Книга "Взлом с помощью Kali Linux: Проникновение в беспроводные сети" авторства Эдди Арнольда посвящена изучению методов взлома беспроводных сетей с использованием программы Kali Linux. Автор предупреждает о запрете воспроизведения, хранения и передачи книги без письменного согласия издателя. В книге представлены главы, включающие введение, знакомство с беспроводными сетями и их ролью в рабочем процессе, основы беспроводного взлома и необходимые инструменты, обход шифрования Wi-Fi, эксплуатация беспроводных сетей, работа с DoS и изучение VPN и брандмауэров. Также в книге рассматривается основы кибербезопасности, понимание работы вредоносных программ и кибератак, а также последствия кибернападения. Завершается книга главой о защите сетей с помощью эффективного сканирования, а также заключением.

Содержание

1Введение

Поздравляем вас с приобретением книги "Проникновение в беспроводные сети

в Kali Linux", и мы искренне признательны вам за ваш выбор. В предстоящих

разделы будут всесторонне охватывать основные знания, необходимые для

чтобы начать наше путешествие по проникновению в беспроводные сети. В современном

технологическом ландшафте многие компьютеры перешли от традиционных проводных

подключения к беспроводным сетям. Этот переход обеспечивает повышенную мобильность и

удобство, но в то же время подвергает нас повышенному риску потенциальных

атак на беспроводные сети. Необходимо, чтобы все понимали эти

уязвимости и быть бдительным в отношении потенциальных угроз.

Хакеры заинтересованы в распространении беспроводных сетей. Эти

сети предоставляют хакерам возможность проникнуть в сеть и посеять

хаос в сетях, к которым у них не должно быть доступа. Очень важно, чтобы мы

понять, как работают эти системы, и развить навыки противодействия этим

атакам.

В этом руководстве мы рассмотрим сложные компоненты беспроводных

сетей, выявлять уязвимости и использовать их в своих интересах.

преимущества. Чтобы эффективно бороться с потенциальными угрозами, мы должны принять

хакерскую точку зрения, распознавая общие проблемы, которые могут возникнуть, и

разрабатывать стратегии для предотвращения этих злонамеренных действий.

Например, мы изучим основы современных

беспроводных сетей, различные методы шифрования, способы взлома и

методы перехвата данных, передаваемых между устройствами. Мы также

вникнем в тонкости ключей подписи и четырехстороннего рукопожатия.

используемых компьютерами для обеспечения безопасности.

Кроме того, мы уделим внимание стратегиям укрепления

наших систем. Мы обсудим беспроводные методы отказа в обслуживании, использование VPN и брандмауэров.

использование VPN и брандмауэров для защиты от хакеров, а также

методы борьбы с вредоносным ПО и кибератаками.

В свете этого мы должны осознать серьезные последствия

кибератак как для частных лиц, так и для предприятий. Данное руководство

В заключение мы узнаем, какие шаги необходимо предпринять для эффективного сканирования наших

сетей и одновременно защитить их от потенциальных вторжений хакеров.

Расширение наших знаний о собственных системах, принятие хакерского

Мышление хакера и понимание потенциальных уязвимостей могут значительно

существенно повлиять на нашу способность противостоять надвигающимся угрозам. Хакеры

неустанно ищут любые слабые места для получения несанкционированного доступа, будь то

для кражи информации или получения финансовой выгоды. С помощью этого руководства мы

сможем вооружиться знаниями о тестировании беспроводных сетей на проникновение

и заранее выявлять проблемы до того, как они поставят под угрозу наши компьютеры

и сети.

Хотя этой теме посвящено множество книг, мы искренне признательны вам за то, что

за то, что вы выбрали именно эту книгу. Мы приложили все усилия, чтобы снабдить ее

максимально ценной информацией. Мы надеемся, что вы извлечете из нее огромную пользу.

из нее. Приятного чтения!

2Глава 1: Введение в беспроводные сети и их роль в нашем рабочем процессе

Рабочий процесс

В первые годы развития компьютерных сетей практически все соединения

между узлами осуществлялись с помощью медных кабелей. Этот тип проводки был известен

своей эффективностью, доступностью и долговечностью и служил основой

раннего интернета. Однако по мере роста спроса на широкополосную связь оптоволокно

оптоволокно постепенно заменило значительную часть интернет-магистрали.

магистрали. Тем не менее локальные сети все еще полагались на медные соединения.

Недавний рост числа мобильных устройств и использование ноутбуков вместо

менее портативных настольных компьютеров в качестве основных устройств потребовало широкого использования

беспроводных сетей, которые теперь нам хорошо знакомы. Хотя эти беспроводные сети

сети обеспечивают удобство и гибкость, они по своей сути менее безопасны

по сравнению с их жесткими проводными аналогами. Это связано в первую очередь с тем, что беспроводные

сигналы передаются во всех направлениях, а не ограничиваются кабелями.

Чтобы уменьшить эти уязвимости, были разработаны протоколы шифрования.

для защиты беспроводной связи. Хакеры, которым удается

взломать эти алгоритмы шифрования, могут получить несанкционированный доступ к своим

цели.

Беспроводные технологии

Важно понимать, что различные стандарты беспроводной связи

различаются по назначению, радиусу действия, скорости и пропускной способности. Каждый

Каждый стандарт работает на основе своего набора протоколов, хотя все они используют

TCP/IP для обеспечения сетевого взаимодействия.

Из-за всенаправленной природы беспроводных сигналов их качество

быстро ухудшается по мере увеличения расстояния от источника сигнала. Это

Это ограничивает скорость передачи данных, которую можно поддерживать на определенных расстояниях.

Кроме того, беспроводные сигналы подвержены воздействию электромагнитных

помехам, которые ухудшают качество сигнала.

Wireless Fidelity, широко известный как Wi-Fi, - это стандарт беспроводной связи.

Стандарт беспроводной связи, используемый как в локальных, так и в коммерческих сетях. Wi-Fi

обычно обеспечивает эффективное покрытие в радиусе 100 метров без помех.

но в большинстве жилых и городских районов радиус действия сокращается

до 30 метров.

Еще одна беспроводная технология - Bluetooth, предназначенная для небольших

аксессуаров и устройств в персональных сетях с радиусом действия не более

не более 10 метров. Для передачи данных на короткие расстояния в пределах 0,1 метра и менее

используется стандарт связи ближнего поля (NFC), который иногда

для работы которого иногда требуется физический контакт между устройствами.

Сети Wi-Fi

Давайте рассмотрим Wi-Fi - технологию, которая настолько распространена, что сложно

найти современный город без частных или общественных точек доступа Wi-Fi.

Однако такая широкая распространенность также представляет собой серьезную проблему с точки зрения безопасности.

проблему.Любой человек в радиусе действия может отслеживать сигналы Wi-Fi без

физического подключения или авторизации, даже из другого места внутри

локальной сети (LAN).

Хакеры иногда используют незащищенные сети Wi-Fi, просто проходя или проезжая по городским улицам.

просто прогуливаясь или проезжая по городским улицам, выявляя уязвимые

сети для потенциального использования. Эта уязвимость подчеркивает

необходимость шифрования сетей Wi-Fi для защиты конфиденциальных данных.

Первоначальный стандарт Wi-Fi, разработанный Институтом инженеров по электротехнике и электронике, - это стандарт 802

и инженеров электроники, был стандарт 802.11. С течением времени этот

стандарт претерпел изменения, направленные на повышение безопасности, скорости и

радиуса действия. Известны следующие версии стандарта: 802.11g и 802.11n, а самая последняя - 802.11ac.

последняя - 802.11ac. Эти стандарты поддерживают различные частотные диапазоны, включая 900 МГц, 2,4 ГГц, 3,6 ГГц, 60 ГГц и 5 ГГц.

Сеть Wi-Fi, согласно стандартам, состоит как минимум из двух беспроводных станций, связь между которыми регулируется функцией координации функция. Набор станций, управляемых одним CF, образует базовый сервисный набор базовых услуг локальной сети Wi-Fi.Каждая станция предлагает четыре основных сервиса:

Аутентификация: Проверяет личность станции в сети.

Деаутентификация: Аннулирует ранее аутентифицированную станцию.

Конфиденциальность:Использует шифрование для защиты кадров сообщений MAC Service.

Доставка единиц данных: Доставляет кадры данных к месту назначения.

Станция, функционирующая в качестве точки беспроводного доступа, как правило, маршрутизатор обычно маршрутизатор, должна предоставлять пять дополнительных услуг. К ним относятся:

Ассоциация: Этот процесс включает в себя сопоставление аутентифицированной станции с точке доступа.

Разъединение: Здесь ранее ассоциированная станция деаутентифицируется, разрывая соединение.

Повторная ассоциация: Позволяет переназначить станцию на другую точку доступа точке доступа.

Распределение: Обеспечивает доставку кадров MSDU в пределах локальной сети.

Интеграция: Эта служба управляет передачей кадров MSDU между локальной сетью и внешней проводной сетью.

Операции с сетью Wi-Fi

Сети Wi-Fi определяются тремя ключевыми параметрами, которые отличают их от соседних сетей. Этими параметрами являются имя сети (Service Set Identifier или SSID), режим работы и рабочий канал. Хотя маршрутизаторы поставляются с SSID по умолчанию, большинство пользователей предпочитают настраивать их.

Можно скрыть SSID для обеспечения конфиденциальности, но опытные хакеры все равно могут обнаружить скрытые имена сетей.

Сети Wi-Fi работают в одном из двух режимов: инфраструктурном или ad-hoc.

Инфраструктурные сети, наиболее распространенные, имеют центральную точку доступа обслуживающая множество клиентских станций, обычно используется в домашних и рабочих локальных сетях.

локальных сетях. В отличие от них, сети Wi-Fi ad-hoc представляют собой прямое двустороннее соединение

между двумя станциями, например, между компьютером и

беспроводным принтером.

Если несколько сетей пересекаются, желательно, чтобы они использовали

отдельные подчастоты в общем диапазоне. Каждой сети может быть

назначить определенный канал либо вручную, либо настроить автоматическое

переключения каналов во избежание помех.Сеть с непересекающимися

каналов обеспечивает оптимальную производительность.

Процесс аутентификации и квитирования очень важен для обеспечения

безопасности и целостности данных в беспроводной локальной сети. Взаимная аутентификация

необходима для проверки личности как точки доступа (AP), так и

клиентов.Клиент называется супликантом, а точка доступа выступает в качестве

аутентификатор.

Для завершения аутентификации требуется четырехстороннее рукопожатие.

Стандарт IEEE 802.1X требует создания и обмена

криптографическим ключом. Это может быть предварительный общий ключ, конкатенированный ключ

(парный переходный ключ), а также криптографический nonce - случайное значение, используемое

однократно и отбрасываемое. Криптографические несы предотвращают перехват и последующее

перехват и последующее использование хакерами сообщений, передаваемых по рукопожатию.

Четырехстороннее рукопожатие происходит следующим образом:

Точка доступа генерирует nonce и отправляет его на станцию (STA) для

аутентификации.

STA строит парный переходный ключ (PTK) из предварительно распределенного

ключа, полученного nonce, своего собственного nonce, MAC-адресов и генерирует

код целостности сообщения (MIC). Он отправляет SNonce и MIC для проверки

подлинности сообщения.

Используя SNonce, точка доступа строит тот же PTK, что и STA, и

генерирует групповой временной ключ (GTK) для многоадресных операций. Она отправляет

GTK на STA вместе с MIC.

STA подтверждает стандартным подтверждением (ACK),

завершая рукопожатие.

Хотя значение криптографических несов может быть не сразу очевидным

значение криптографических несов не сразу становится очевидным, но в следующих главах будет показано, как они

как они используются для компрометации протоколов Wi-Fi и как хакеры могут взламывать

беспроводные сети для достижения своих целей.

3Глава 2: Создание беспроводной сети и необходимые инструменты

Получив некоторое представление о том, как функционируют беспроводные сети, давайте

рассмотрим основные шаги, необходимые для начала беспроводного взлома и

и подготовимся к выполнению поставленной задачи. Для взлома беспроводной сети требуются особые

программных и аппаратных средств из-за уникальных характеристик этих

сетей и их схем шифрования. Программные средства легко доступны

доступны и часто входят в стандартный пакет Kali Linux, что делает их легкодоступными.

что делает их легкодоступными. Что касается необходимых беспроводных сетевых адаптеров,

хотя они могут потребовать некоторого поиска, их обычно легко найти

и доступны по цене.

Инструменты для Kali Linux

Прежде всего, нам нужно определить инструменты, необходимые для начала

взлома с помощью программы Kali Linux. Набор aircrack служит

важной отправной точкой. Этот набор представляет собой коллекцию инструментов на базе Linux

инструментов с открытым исходным кодом, специально разработанных для тестирования на проникновение и

мониторинга беспроводных сетей.

Все программы пакета выполняются через командную строку терминала Linux

строку. Официально известный как aircrack-ng, этот набор специально разработан для

стандарта 802.11, позволяя нам отслеживать и атаковать как WPA/WPA2

и WEP-шифрования, если у нас есть соответствующее оборудование. Он

включает в себя 16 программ, способных выполнять различные задачи, в том числе сниффинг,

инъекции, анализ, дешифрование, взлом паролей и др.

Флагманской программой пакета является инструмент для взлома ключей шифрования

которая незаменима для перехвата сообщений, передаваемых между

двумя компьютерами.Для работы с различными

типами ключей. Например, метод взлома ключа WEP основан на

атака на потоковый шифр, которая предполагает объединение перехваченных пакетов

для получения необходимого ключа. Этот метод использует уязвимости в

векторах инициализации, используемых в WEP. Он также может использоваться совместно с

атакой по словарю для взлома ключей WPA/WPA2, если они слабые.

Инструмент airmon-ng необходим для перевода беспроводного адаптера атакующей машины в режим

беспроводной адаптер атакующей машины в режим монитора, что является необходимым условием для любого значимого Wi-

Fi мониторинга. Также есть airodump-ng, пакетный анализатор пакетов беспроводной сети

сниффер и сетевой анализатор, способный перехватывать необработанные кадры с

подключенного беспроводного адаптера. В основном он используется для извлечения векторов инициализации

векторов инициализации для взлома ключей WEP.

Наконец, aireplay-ng, инструмент для инъекции пакетов, использует подключенный

беспроводной адаптер для трансляции в канал точки доступа, подвергающейся атаке. Это

особенно полезен для деаутентификации клиентов в сети, чтобы увеличить

трафика и решения других проблем, таких как поддельная аутентификация и инъекция

поддельных пакетов.

Это одни из наиболее часто используемых инструментов для взлома, хорошо известных

благодаря своей эффективности при взломе различных беспроводных сетей. Однако,

существует множество других инструментов, в зависимости от ваших конкретных потребностей

и целей.

Еще один инструмент, который стоит изучить, - Macchanger. Уязвимость сигналов Wi-Fi

является их всенаправленное вещание, предоставляющее хакерам

широкие возможности для перехвата сетевого трафика. Мониторинг в этом

в этом контексте по своей сути пассивен, поэтому хакерам крайне важно оставаться

незаметным. Пассивные атаки предпочтительнее, когда это возможно, однако важно отметить, что

важно отметить, что пассивные атаки на WEP все чаще

обнаруживаются, что приводит к постепенному отказу от этого типа шифрования. Большинство

эффективных беспроводных атак требуют определенного уровня инжекции пакетов или

для достижения своих целей.

IP-пакеты, изменение MAC-адресов и беспроводные адаптеры

В сфере взлома беспроводных сетей все IP-пакеты должны содержать

важнейшую информацию в своих заголовках: сведения об источнике и

узлах назначения, включая MAC-адреса и IP-адреса.

Когда хакер приступает к атаке на беспроводную сеть, используя свой собственный

беспроводной сетевой адаптер вместо Интернета, необходимо принять особые меры предосторожности.

должны быть приняты особые меры предосторожности. Они должны манипулировать информацией об IP-адресе в

заголовке пакета таким образом, чтобы скрыть свою личность и гарантировать, что атака

не может быть отслежена до машины или местоположения по IP-адресу источника, как это обычно бывает при атаках через Интернет.

как это обычно бывает при атаках через Интернет.

Однако проблема заключается в том, что карты сетевого интерфейса

по своей природе обладают уникальным MAC-адресом, который идентифицирует как производителя, так и отдельное устройство, передающее информацию.

производителя и отдельное устройство, передающее сообщение. Даже

даже решительные и хорошо финансируемые сотрудники правоохранительных органов или службы безопасности могут

извлечь этот идентификатор при выявлении подозрительного заголовка пакета,

что может привести к раскрытию личности злоумышленника. Это может произойти, например, если

хакер открыто приобрел интерфейсную карту, что позволяет производителю

отследить продавца устройства, дату покупки и, возможно, покупателя по

любой финансовый след.

Чтобы сохранить анонимность, целесообразно и относительно просто

изменить MAC-адрес в заголовках пакетов. Хотя MAC-адрес оборудования

MAC-адрес оборудования является постоянным и неизменным, то адресом, передаваемым в

в заголовках пакетов, можно изменить с помощью инструмента Linux под названием

"macchanger", который прост в использовании и находится в свободном доступе. С помощью

одной строкой кода, этот инструмент может изменить MAC-адрес, связанный с

сетевым интерфейсом, позволяя задать его вручную или сгенерировать

случайный адрес.

Однако изменение MAC-адреса, скрывающее вашу личность,

может вызвать подозрения и потенциально спровоцировать вмешательство систем обнаружения вторжений или сетевых мониторов.

системы обнаружения вторжений или сетевых мониторов, которые могут заблокировать ваши пакеты

от входа в систему. Таким образом, необходимо найти баланс между

анонимностью и тем, чтобы не вызывать подозрений.

Изменение MAC-адреса в Kali Linux

Чтобы изменить MAC-адрес в адаптере Kali Linux, необходимо

сначала вывести его из эксплуатации. Этого можно добиться, выполнив следующие действия

команда:

```hell
# ifconfig eth0 down
```

В этом коде "eth0" обозначает адаптер, который вы хотите изменить. Чтобы изменить

MAC-адрес вашего адаптера на случайный, вы можете использовать

"macchanger" с тегом "-r" следующим образом:

```hell
# macchanger -r eth0
```

Такой подход позволяет контролировать MAC-адрес.

передаваемым на целевой компьютер, что повышает вероятность получения

доступа без обнаружения и последующего отслеживания.

Беспроводные адаптеры

В сфере компьютерного взлома большинство начинаний не требуют

специализированного оборудования, кроме компьютера, необходимых программных средств и

сетевого интерфейса. Однако для взлома беспроводных сетей, особенно в контексте

стандарта Wi-Fi 802.11, как правило, требует наличия специального беспроводного сетевого адаптера.

адаптер. Кроме того, для достижения конкретных целей хакерам может потребоваться

внешний адаптер с увеличенным радиусом действия или направленными возможностями. Таким образом, очень важно

очень важно учитывать типы адаптеров, которые лучше всего подходят для решения поставленных задач.

Один из важнейших аспектов, на который следует обратить внимание, - это режим монитора. В рамках стандарта 802.11

стандарт 802.11, сетевые адаптеры могут работать в семи различных режимах, причем выбор режима зависит от

Выбор режима зависит от предназначения адаптера. Два режима, представляющие

представляющие особый интерес для анализа сети, - это режим монитора и

режим промискуитета. Режим монитора перехватывает все пакеты Wi-Fi в пределах

в пределах своей зоны действия, что делает его незаменимым для взлома стандартов шифрования, поскольку

в защищенной сети необходимо перехватить несколько зашифрованных пакетов, прежде чем

чтобы попытаться расшифровать. Инструмент "airmon-ng" облегчает

переход подключенного адаптера в этот режим.

Однако не все операционные системы, драйверы и беспроводные сетевые

Однако не все операционные системы, драйверы и адаптеры беспроводных сетей поддерживают все семь режимов работы Wi-Fi. Чтобы максимально повысить

эффективности набора aircrack, хакеры должны убедиться, что их беспроводной

адаптер поддерживает режим монитора. Большинство внутренних беспроводных радиомодулей, используемых в

мобильных устройствах, ноутбуках и настольных компьютерах не поддерживают этот режим.

Поэтому часто приходится приобретать внешнее USB-устройство, способное

перед попыткой взлома беспроводных сетей. Выбор

подходящего оборудования является относительно простым процессом, несмотря на

потенциальные проблемы.

Для начала необходимо составить список контроллеров беспроводных адаптеров

чипсетов, поддерживаемых выбранной операционной системой. Этот список периодически

периодически обновляется, а поддерживаемые чипсеты часто меняются. Поэтому

рекомендуется дважды проверить, поддерживается ли тот или иной чипсет.

После того как вы определили совместимые чипсеты для вашей операционной системы,

можно приступать к выбору адаптера с одним из этих наборов микросхем. А

рекомендуемый производитель для приобретения беспроводного USB-адаптера с

Alfa Network, Inc.

Понимание основ работы беспроводных сетей, знание шагов

необходимых для обхода системы, а также владение рядом инструментов и программного обеспечения

Для успеха хакера очень важно знать, какие шаги необходимо предпринять для обхода системы, и владеть набором инструментов и программного обеспечения. В данном контексте мы в первую очередь

сфокусируемся на взломе стандартов шифрования WPA/WPA2, поскольку WEP, более слабый WEP, более слабый вариант шифрования, постепенно отменяется в пользу более надежных мер безопасности. Если ваша сеть все еще использует WEP, вы можете столкнуться с больше уязвимостей, чем ожидалось изначально, что свидетельствует о необходимости проактивных мер информационной безопасности и потенциального перехода на более надежный протокол шифрования.

4Глава 3: Обход шифрования Wi-Fi

В этой главе мы погрузимся в развивающуюся сферу методов шифрования Wi-Fi методы. Как уже говорилось, шифрование WEP, некогда популярное, теперь считается устаревшим и уязвимым. Хакеры легко используют его слабые места, что делает его небезопасным выбором для защиты сетей. Сегодня большинство компьютеров используют протоколы WPA/WPA2 для онлайн-общения. При этом WPA2 является преобладающим вариантом.

В этой главе рассматриваются расширенные протоколы и их уязвимости. Важно важно отметить, что по мере распространения методов взлома уязвимости либо быстро устраняются, либо целевые сети хакеры отказываются от них. Опытный хакер должен оставаться бдительным, постоянно узнавая о новейших методах атак.

Сети Wi-Fi представляют собой отличную платформу для безопасного взлома.

Получив доступ к беспроводному маршрутизатору, хакеры могут манипулировать протоколами шифрования протоколами шифрования, сложностью паролей и другими параметрами безопасности. Взлом своей сети - это безопасная среда для оттачивания навыков без юридических последствий.

WEP:

Сначала рассмотрим WEP, сокращение от Wired Equivalent Privacy.

Введенный для преодоления разрыва в безопасности между проводными и беспроводными сетями, WEP шифрует беспроводные передачи данных. Однако его зависимость от одноразового вектора инициализации (IV) создает уязвимости.

Хакеры могут пассивно перехватывать пакеты данных, использовать короткую длину IV, и восстановить ключ шифрования. Специальные беспроводные адаптеры, поддерживающие

режим монитора, в сочетании с такими инструментами, как airodump-ng, airmon-ng и

aircrack-ng из Kali Linux, облегчают эксплуатацию WEP. Хотя

несмотря на усовершенствования, WEP остается небезопасным и устаревшим.

WPA:

Чтобы устранить недостатки WEP, была разработана технология WPA (Wi-Fi Protected Access).

разработан. WPA динамически изменяет ключ шифрования в каждом пакете,

повышая уровень безопасности. Однако хакеры разработали такие методы, как перехват пакетов.

инъекции пакетов с использованием aireplay-ng для сетей WPA. Несмотря на улучшения

по сравнению с WEP, WPA стал уязвим для более продвинутых атак, что послужило толчком к разработке WPA2.

разработку WPA2.

WPA2:

WPA2, или Wi-Fi Protected Access II, является текущим стандартным протоколом шифрования

протокол шифрования для сетей Wi-Fi. Он предлагает три метода распределения ключей в зависимости от

в зависимости от размера и типа сети: Предварительный общий ключ (для домашних/малых офисов

сетей), Enterprise (для крупных/корпоративных сетей, требующих наличия сервера аутентификации) и Wi-Fi Protected Access II.

сервер аутентификации), а также Wi-Fi Protected Setup (упрощенный, но менее безопасный вариант).

безопасный вариант). Если говорить о взломе беспроводных сетей, то в WPA2 используется предварительный

Shared Key (WPA-PSK).

Взлом сети WPA2:

Несмотря на усовершенствование WPA2, уязвимости сохраняются. Слабые

слабые пароли остаются серьезной угрозой, подверженной атакам по словарю и

методам перебора. Aircrack, инструмент, нацеленный на слабые системы, пытается

взломать предварительно распределенные ключи. Другая продвинутая техника, Nonce Krack,

использует уязвимости в 4-стороннем процессе рукопожатия WPA2. С помощью

перехватывая и манипулируя несами во время аутентификации, хакеры могут

расшифровать клиентские пакеты, раскрыв конфиденциальные данные.

Таким образом, методы шифрования Wi-Fi различаются по степени уязвимости. В то время как

WEP легко эксплуатируется и устарел, более новые протоколы, такие как WPA2, предлагают

повышают уровень безопасности, но не защищены от современных атак. Постоянное

Постоянное обучение и бдительность необходимы как хакерам, так и владельцам сетей, чтобы для защиты информации в постоянно меняющемся ландшафте безопасности Wi-Fi.

5Глава 4: Эксплуатация беспроводных сетей

В этом разделе мы погрузимся в искусство эксплуатации беспроводных маршрутизаторов и сетей. Получение доступа к беспроводной сети является значительным

достижение для многих хакеров, и эта задача становится все более

сложнее, так как меры сетевой безопасности продолжают совершенствоваться. Однако, важно понимать, что это лишь начальный шаг на пути к достижению

более продуктивных целей. При атаке на беспроводную сеть хакеры

обычно преследуют одну из трех основных целей:

Проникнуть в один из клиентов, подключенных к сети.

Получение доступа к основной точке доступа.

Осуществление атаки типа "отказ в обслуживании".

Стоит отметить, что для атаки типа "отказ в обслуживании" не всегда требуется

доступа к сети; она может быть выполнена с помощью того же набора инструментов.

которые мы рассмотрели в этом руководстве. В этой главе мы рассмотрим различные

аспекты безопасности беспроводных маршрутизаторов и обзор

необходимых инструментов для анализа и эксплуатации участников сети.

Безопасность маршрутизатора

Взлом шифрования беспроводной сети позволяет получить доступ к

самой сети, но не обязательно к подключенным узлам. Клиенты и

Клиенты и точки доступа имеют свои собственные меры безопасности, с которыми хакеры должны бороться

с которыми приходится бороться. Маршрутизаторы, используемые в качестве точек доступа в локальной сети Wi-Fi, предназначены в основном

для административного доступа и имеют встроенные средства защиты.

Однако, как и в других обсуждаемых нами темах, в маршрутизаторах есть

уязвимости, которые при использовании могут предоставить хакерам обширный контроль

над сетью. Получив доступ к маршрутизатору, хакеры могут изменять

протоколы шифрования, перехватывать привилегированные данные или запрещать доступ даже

легитимным пользователям.

Программное обеспечение для настройки беспроводных маршрутизаторов обычно поставляется в виде

в виде встроенной микропрограммы. Эта программа, известная как шлюз, доступна

Доступ к ней осуществляется через веб-интерфейс клиента путем ввода IP-адреса маршрутизатора в адресную строку веб-браузера.

IP-адрес маршрутизатора в адресную строку веб-браузера. IP-адрес маршрутизатора можно

обычно можно найти в документации к продукту или на этикетке, прикрепленной к устройству.

устройстве. Существует два распространенных формата IPv4-адресов для маршрутизаторов:

192.168.X.X

10.0.X.X

Когда вы получаете доступ к веб-приложению, оно запрашивает у вас имя пользователя

и пароль. Некоторые шлюзы также предоставляют информацию о сети

и подключенных к ней клиентах.

Имя пользователя и пароль администратора по умолчанию обычно можно найти

в документации к продукту или на устройстве. Многие маршрутизаторы, особенно

особенно старых моделей, поставляются со стандартными учетными данными для входа в систему, что облегчает администраторам сброс пароля, если они не хотят входить в систему.

администраторам легко сбросить пароль, если они его забыли. Хотя это

удобство выгодно администраторам, оно представляет собой уязвимость для хакеров.

которые имеют физический доступ к маршрутизатору. Если пользователи не изменят пароль по умолчанию

пароль по умолчанию, его можно легко найти в Интернете, поскольку многие модели имеют общие,

легко угадываемые учетные данные.

Картирование сети с помощью Nmap

Получив доступ к беспроводной сети, следующим шагом хакеров становится

выявление уязвимостей в клиентах сети. Обзор

сети и подключенных к ней клиентов помогает определить потенциальные цели. Kali

Linux предоставляет бесплатное приложение для картографирования сети с открытым исходным кодом

под названием Nmap, которое сканирует сеть, отправляя специальные пакеты для пинга

узлов и получения ответов.

Nmap анализирует эти ответные пакеты и создает карту сети,

обнаруживая узлы, сканируя их порты и определяя операционную систему и версию, запущенную на каждом устройстве.

операционной системы и ее версии, установленной на каждом устройстве. Чтобы понять и практического применения Nmap, рекомендуется использовать его на своей собственной персональной сети.

Nmap предлагает различные опции для задания функций. Например, опция "-sn" выполняет простое сканирование на наличие открытых хостов в сети, сообщая их MAC-адреса и связанных с ними производителей. Результаты показывают целый ряд устройств, включая подключенные приборы, принтеры, маршрутизаторы, планшеты и смартфоны. Названия некоторых производителей могут могут соответствовать сетевым адаптерам на возможных компьютерах.

Хотя Nmap работает через командную строку и предоставляет текстовый вывод, сопутствующие приложения, такие как Zenmap, входящие в состав Kali Linux, предлагают более наглядное представление топологии сети.

Использование опции "-O" в Nmap помогает определить операционную систему объекта. операционной системы, что очень важно для планирования эксплойтов. Nmap предоставляет ряд опций для управления объемом информации, собираемой во время сканирования. Важно важно отметить, что Nmap - это не пассивная деятельность; он обменивается пакетами с узлами целевой системы. Некоторые машины могут обнаружить сканирование и реагировать на это предупреждениями, сбором данных о заголовках входящих пакетов или блокировкой IP блокировка IP-адресов, если они подозревают наличие злого умысла.

Metasploit

Еще один важный инструмент в арсенале хакера - Metasploit, фреймворк для обнаружения и использования уязвимостей в целевых портах. Metasploit использует обновляемую базу данных известных уязвимостей и соответствующих эксплойтов. По состоянию на 2017 года в ней насчитывалось более 1600 эксплойтов, и это число, скорее всего, будет расти. и это число, вероятно, будет расти.

Для запуска Metasploit требуется внешний интерфейс. Существуют различные варианты интерфейса, включая msfconsole (Metasploit Framework Console) в Kali Linux, который служит стандартным стандартным интерфейсом для запуска Metasploit. Чтобы запустить Metasploit, необходимо использовать определенные опции которые необходимо использовать.

Эти методы полезны для взлома беспроводных сетей, которые

которые обеспечивают гибкость, но в то же время сопряжены с проблемами безопасности. Необходимо найти баланс

между использованием беспроводных сетей для удобства и защитой

их от потенциальных угроз, очень важно для обеспечения безопасности

вашей информации.

6Глава 5: Работа с беспроводными сетями Отказ в обслуживании (DoS)

Отказ в обслуживании (DoS) - это тип кибератаки, при которой

хакер проникает в систему и нарушает доступ для законных пользователей, вызывая

простоя сети и лишения доступа к сайту даже администраторов сайта.

доступа к своему сайту. Во время такого простоя хакеры могут воспользоваться ситуацией

ситуацией, похитить данные и совершить различные вредоносные действия, создавая дополнительную работу для администраторов сайта.

дополнительную работу для администраторов сайта после восстановления работоспособности сети.

и работы.

DoS-атаки могут иметь различные мотивы, начиная от желания хакеров

стремящихся создать хаос или содействовать политической или социальной активности, до более серьезных действий, таких как электронная война.

более серьезных действий, таких как электронная война или шантаж. Что делает

эти атаки особенно опасными, так это то, что их относительно легко

и не обязательно требуют доступа к целевой системе, сложной

расшифровки или внедрения полезной нагрузки.

Эти атаки могут быть осуществлены через Интернет из различных

анонимных мест, некоторые из которых могут захватывать нежелательные хосты.

Такая атака известна как распределенный отказ в обслуживании (DDoS), и ее эффективное предотвращение является сложной и дорогостоящей задачей.

Эффективное предотвращение этой атаки является сложной и дорогостоящей задачей.

Беспроводные DoS-атаки отличаются от традиционных проводных DoS-атак тем.

тем, что атакующий или, по крайней мере, конечная точка атакующего узла должны находиться в пределах

радиочастотного диапазона целевой точки доступа. Беспроводные DoS-атаки

могут происходить путем глушения сигнала Wi-Fi на целевом канале или путем принуждения

точку доступа неоднократно отключать легитимного клиента.

Это не пассивные атаки, поэтому очень важно оставаться незаметным и маскироваться.

Могут возникнуть споры о том, можно ли технически квалифицировать это как

хакерство, поскольку оно не обязательно связано с получением доступа к ресурсам.

Однако DoS-атаки требуют навыков и инструментов, схожих с другими формами

взлома и приводят к нежелательному поведению системы.

Специалистам по безопасности необходимо понимать, как осуществляются эти атаки

чтобы лучше защититься от них. Атака деаутентификации, например

например, служит предвестником более навязчивых действий, в конечном итоге

заставляя клиентов подключаться к скомпрометированным точкам доступа.

Понимание отказа в обслуживании

Прежде чем приступить к работе с DoS-атаками, необходимо понять

концепцию. DoS-атака - это форма кибератаки, при которой злоумышленник

хакер делает компьютер или устройство недоступным для предполагаемого пользователя. Это

Обычно это происходит, когда хакер нарушает нормальную работу устройства.

DoS-атаки осуществляются путем перегрузки целевого компьютера

множеством запросов, эффективно препятствуя прохождению нормального трафика

через него. Система становится перегруженной из-за притока фальшивого трафика,

не оставляя места для законных пользователей. В DoS-атаках обычно участвует один

компьютер в качестве атакующего.

Цель хакера - помешать регулярному использованию целевой

системы, позволяя им выполнять свои действия без помех. Это

Это гарантирует, что никто не сможет получить доступ к системе по назначению, что облегчает

хакеру нарушить нормальную работу веб-сайта или компьютера.

DoS-атаки в первую очередь направлены на перенасыщение пропускной способности

перегрузить пропускную способность атакуемого компьютера, заставив его отказать в обслуживании дополнительных входящих

запросам. Эти атаки можно классифицировать по их сходству.

Как правило, выделяют две основные категории:

1. Атаки на переполнение буфера: Эти атаки связаны с перегрузкой

перегрузку буфера памяти цели, потребляя свободное место на жестком диске, процессорное время,

и память. Такие атаки часто приводят к заторможенности системы, сбоям,

и другим деструктивным поведением серверов, которые отказывают в обслуживании легитимным пользователям.

2. Флуд-атаки: Флуд-атаки предполагают насыщение целевого сервера

многочисленными пакетами, превышающими возможности сервера и приводящими к

отказ в обслуживании. Эти атаки более успешны, когда у хакера

больше доступной пропускной способности, чем у цели.

Исторически сложилось так, что эти атаки направлены на уязвимости в безопасности

сети, программного обеспечения или аппаратного обеспечения. DDoS-атаки стали более

распространенными из-за их разрушительного характера и доступности инструментов. На сайте

На практике многие DoS-атаки при необходимости можно превратить в DDoS-атаки.

К историческим DoS-атакам относятся атаки Smurf, Ping flood и Ping

смерти.

Обнаружение DoS-атаки может быть сложной задачей, поскольку ее можно принять за

другие проблемы с подключением к сети или высоким потреблением полосы пропускания.

Однако есть несколько индикаторов, на которые следует обратить внимание, например замедление работы сети в обычном режиме

сети, длительное время загрузки веб-сайтов или файлов, невозможность

доступа к определенному веб-сайту (особенно вашему собственному), а также потеря

связи между устройствами в одной сети. Очень важно быть

быть бдительным и реагировать на эти проблемы.

Прежде чем завершить эту тему, важно провести различие между DoS

и DDoS-атаками. Основное различие заключается в количестве соединений

используемых в атаке. Некоторые DoS-атаки, такие как низкие и медленные атаки, черпают

свою силу из простоты и минимальных требований, что делает их

высокоэффективными.

Атака деаутентификации

Ранее мы рассмотрели процесс рукопожатия в сетях Wi-Fi,

в ходе которого происходит аутентификация клиентов. Этот процесс включает в себя многоступенчатый обмен пакетами

обмен пакетами между агентом аутентификации, обычно маршрутизатором или точкой доступа

точкой доступа, и клиентом. Одной из обязанностей точки доступа является повторная аутентификация

клиентов, которые на короткое время теряют связь с сетью, что часто случается в беспроводных сетях.

частое явление в беспроводных сетях.

Атака на деаутентификацию - это техника, используемая хакерами, чтобы нарушить этот процесс. Атака успешна, поскольку она посылает поток пакетов как на точку доступа, так и на клиента. Эти пакеты побуждают ответы от точки доступа и клиента, которые отклоняются от стандартной процедуры рукопожатия. Пока атака продолжается, клиент не может правильно аутентифицировать себя в сети.

Эта атака похожа на атаку "человек посередине", когда хакер располагается между компьютером и маршрутизатором или точкой доступа, перехватывая информацию или перенаправляя ее до того, как она достигнет цели. назначения. Атака деаутентификации требует только поддельных пакетов и не требует включения атакующей машины в сеть или доступа к ключам шифрования.

Базовая атака на деаутентификацию в сети Wi-Fi может быть выполнена используя пакет aircrack и совместимый беспроводной адаптер, способный работать в режим монитора. Выполнив действия, описанные в предыдущей главе, вы можно перевести подключенный Wi-Fi адаптер на атакующей машине в необходимый режим монитора и начать сбор пакетов с помощью airodumpng.

Кроме того, для анонимности рекомендуется подменить MAC-адрес.

Выберите в списке airodump целевого клиента, которому нужно запретить обслуживание для него. Помните, что для этой атаки необходимо знать BSSID и MAC BSSID и MAC-адреса клиента и связанной с ним точки доступа.

7Глава 6: Знакомство с VPN и брандмауэрами

В следующей главе мы погрузимся в царство виртуальных частных сетей (VPN) и брандмауэров. сетей (VPN) и брандмауэров. Поскольку Интернет постоянно сталкивается с постоянно растущие угрозы для его активов, нам становится все более важным понимать, как защитить наши сети от известных и неизвестных рисков. Одним из незаменимых инструментов для достижения этой цели является брандмауэр.

Технология брандмауэров со временем претерпела значительные изменения. Те, кто ответственные за разработку VPN, понимают, что простое блокирование нежелательного трафика и разрешить авторизованный трафик в сети недостаточно для обеспечения безопасности.

обеспечения безопасности. Нам требуются более надежные функции безопасности, включая

защита от атак типа "отказ в обслуживании" (DoS) и системы обнаружения вторжений

системы обнаружения вторжений, чтобы укрепить безопасность нашей сети. Давайте углубимся в эти

темы и поймем, как приспособить их к нашим потребностям.

Что такое брандмауэр?

Брандмауэр - это, по сути, маршрутизатор, расположенный между определенным веб-сайтом

и остальной частью сети. Эти специализированные брандмауэры действуют как маршрутизаторы

поскольку они соединяют две или более физических сетей и передают пакеты данных

из одной сети в другую. Кроме того, они служат в качестве фильтров, позволяя

сетевым администраторам применять централизованную политику безопасности.

Среди типов брандмауэров брандмауэры на основе фильтров являются наиболее управляемыми

и широко распространены. Они настраиваются с помощью таблицы адресов, которая

определяет, какие пакеты разрешены, а какие запрещены. Две основные

категории современных брандмауэров:

Аппаратные брандмауэры или брандмауэры на базе устройств используют специализированное оборудование для

защиты.

Программные брандмауэры используют обычное оборудование и операционные системы, такие как

например, Windows NT Server 4.0, которая усилена для минимизации потенциальных

угроз безопасности.

Аппаратный брандмауэр - это физическое устройство, похожее на сервер,

способное фильтровать входящий и исходящий трафик до того, как он достигнет вашего

сервера. При такой настройке брандмауэр располагается между восходящим каналом и вашим

компьютером, эффективно действуя как барьер. Эти устройства, как и обычные

компьютеры, используют вычислительную мощность, память и сложное программное обеспечение.

программное обеспечение, что позволяет им тщательно проверять весь трафик на соответствие

настраиваемым правилам, тем самым разрешая или запрещая доступ.

К распространенным примерам программных брандмауэров относятся FirewallD, IPTables,

UFW и Windows Firewall. В отличие от них, аппаратные брандмауэры располагаются

вне вашего сервера и подключаются непосредственно к каналу связи. При использовании

новых брандмауэров, обычно требуется плановое обслуживание для

физических соединений.

Как только сервер устанавливает соединение, весь входящий и исходящий

трафик должен проходить через брандмауэр для проверки. Такой подход позволяет

полный контроль над трафиком, входящим и выходящим из вашей системы.

Как аппаратные, так и программные брандмауэры служат для защиты сети.

меры безопасности. Многие организации используют VPN наряду с брандмауэрами, чтобы

чтобы упростить администрирование системы безопасности.

Однако брандмауэры имеют свои ограничения. Они не могут различать

между типами данных, что позволяет пропускать потенциально опасные пакеты данных.

если они выглядят безобидными. Для борьбы с этим брандмауэры VPN

специально разработанные для защиты VPN-соединений от злоумышленников.

Аппаратные, программные и универсальные брандмауэры разработаны таким образом, чтобы

разрешать доступ только к легитимному VPN-трафику. Это особенно важно в

сетях с большим количеством систем под управлением различных операционных систем.

При возникновении бреши в системе безопасности все потенциально затронутые системы должны быть

все потенциально затронутые системы должны быть оперативно обновлены, что требует масштабируемого управления конфигурацией и

проактивного исправления, что усиливает важность брандмауэров в сетевой безопасности.

безопасности.

Брандмауэры стратегически размещаются между внутренней сетью и

Брандмауэры стратегически размещаются между внутренней сетью и Интернетом, чтобы установить безопасную связь и создать внешний слой защиты

для вашей сети. Эта концепция согласуется с военным принципом

обороны в глубину, что является важным аспектом интернет-безопасности. Доверенные компьютерные

Доверенные компьютерные системы, особенно в правительственных приложениях, подходят для размещения брандмауэров,

В них используются четыре общих правила работы с брандмауэром:

1. Контроль услуг определяет типы интернет-услуг, к которым можно получить доступ

1. Контроль служб определяет типы интернет-услуг, к которым можно получить доступ, используя фильтры на основе протокола, IP-адреса или номера порта. Это

Также может использоваться прокси-программное обеспечение для интерпретации запросов на услуги или программное обеспечение хост-сервера.

серверное программное обеспечение.

2. Контроль направления регулирует направление, в котором запросы на обслуживание

разрешено передавать в сети.

3. Контроль пользователей ограничивает доступ к сервисам на основе идентификации пользователя, часто

Применяется для локальных пользователей или внешних пользователей с надежной аутентификацией.

4. Контроль поведения отслеживает функционирование служб, позволяя

такие действия, как уменьшение количества спама и выборочный внешний доступ к локальным серверным

данным.

Брандмауэры создают единую точку пресечения, что упрощает управление безопасностью

управление, консолидируя возможности защиты на одной или нескольких

системах. Помимо обеспечения безопасности, брандмауэры могут поддерживать различные небезопасные

Интернет-функции, такие как трансляция сетевого расположения и IPsec.

Брандмауэр может служить платформой для реализации IPsec, коммуникационного протокола, который туннелирует данные из сети в сеть.

коммуникационного протокола, который туннелирует данные из одной сети в другую.

Туннелирование облегчает передачу данных из частной сети через

открытой сети, такой как Интернет, с инкапсуляцией, чтобы скрыть

характер трафика.

Несмотря на возможности туннелирования, брандмауэры имеют свои ограничения. Они

Они не могут защитить от атак, которые их обходят, например от внутренних систем

с возможностью выхода в сеть, недовольных сотрудников или атак с использованием портативных устройств хранения данных.

портативных устройств хранения данных. Брандмауэры действуют как пакетные фильтры, проверяя и разрешая или

запрещая пакеты данных на основе определенных критериев. Брандмауэры с фильтрацией пакетов

поставляются с правилами для входящих и исходящих IP-пакетов и оценивают

пакеты на основе содержащейся в них информации, включая IP-адреса источника и

IP-адреса источника и назначения, адреса транспортного уровня и поля IP-протокола.

Интерфейсные брандмауэры работают на основе совпадений с заголовками IP или TCP,

немедленно разрешая или запрещая доступ в соответствии с заранее определенными правилами.

Если совпадений не обнаружено, они выполняют действия по умолчанию: отбрасывают или

пересылка пакета. Брандмауэры обычно придерживаются консервативной политики,

блокируя все и разрешая доступ только в каждом конкретном случае,

поэтому они кажутся препятствиями. В отличие от этого, политика пересылки по умолчанию

приоритет отдается удобству пользователя, но при этом может быть нарушена безопасность.

Виртуальные частные сети (VPN)

Переходя к виртуальным частным сетям (VPN), следует отметить, что эти сети

обеспечивают безопасную связь через общедоступные сети, такие как

Интернет. В VPN используются IP-туннели, которые представляют собой виртуальные соединения "точка-точка", соединяющие узлы различных сетей.

виртуальные каналы "точка-точка", соединяющие узлы различных сетей.

VPN - это экономически эффективное решение, соединяющее множество компьютеров

используя шифрование и специальные протоколы в изначально небезопасной

сети. Это позволяет обеспечить взаимосвязь между базами данных,

рабочими станциями, серверами и корпоративными сайтами через Интернет и другие общедоступные сети, что позволяет сократить расходы.

сети, что позволяет сократить расходы. Однако управление частной сетью может быть

более сложным, чем управление сетью общего пользования.

VPN снижают риски несанкционированного доступа за счет использования шифрования

и аутентификации для создания безопасных соединений через, казалось бы.

небезопасные сети. Они обладают теми же преимуществами, что и частные сети, но по

но по более низкой цене, при условии, что идентичные методы аутентификации и шифрования

на обоих концах. Маршрутизаторы и брандмауэры реализуют IP-шифрование, причем

IPsec является наиболее распространенным механизмом для этой цели.

Для понимания VPN необходимо разобраться с самим термином. "Сеть"

означает совокупность устройств, взаимодействующих друг с другом с помощью

различных методов, будь то принтеры, маршрутизаторы или компьютеры, независимо от

географического расположения. Термин "частная" означает виртуализацию и

конфиденциальность, гарантирующую, что общение в сети остается

конфиденциальным и скрытым от внешних наблюдателей.

VPN бывают разных типов, каждый из которых призван виртуализировать определенную часть

коммуникаций внутри организации и сделать некоторые или все эти

связь незаметной для внешних субъектов. Они используют

эффективность общей коммуникационной инфраструктуры, скрывая при этом

конфиденциальную информацию от посторонних глаз.

Типы VPN

Существует несколько типов VPN, каждый из которых обладает своими уникальными характеристиками.

Выделяются две основные категории:

1. VPN сетевого уровня, которые находятся в наборе протоколов TCP/IP,

охватывают систему IP-маршрутизации, отвечающую за передачу данных по сети.

сети. К ним относятся два подтипа:

- Одноранговые VPN: Включают в себя вычисление пути от одного узла к другому, где каждый

узел на пути передачи данных является одноранговым с узлом следующего хопа. Они обычно

используются в традиционно маршрутизируемых сетях.

- Оверлейные VPN: Используют промежуточную сеть канального уровня для

определения маршрутов пересылки, служащих в качестве сквозного канала

к граничным узлам на другой стороне сети.

2. VPN с контролируемой утечкой маршрутов: Эта модель предполагает управление

распространением маршрута, выполняемое внутри VPN-маршрутизатора сайта. В отличие от пограничных

маршрутизации, этот подход фильтрует маршруты, подключенные к

конкретным сетям, обеспечивая конфиденциальность, но вызывая опасения по поводу потенциальных

уязвимости.

Хотя это основные типы VPN, существует множество других вариантов, каждый из которых

со своими преимуществами и потенциальными проблемами. Выбор подходящей VPN

имеет решающее значение для обеспечения сетевой безопасности, особенно при использовании таких инструментов, как Kali

Linux для этического взлома. Важно тщательно изучить возможности брандмауэра и VPN

чтобы эффективно защитить свою сеть.

8Глава 7: Взгляд на основы кибербезопасности

В этой главе основное внимание уделено кибербезопасности - важнейшему аспекту в современном

цифровом мире, где деятельность в Интернете стала неотъемлемой частью нашей жизни.

жизни. В начале главы подчеркивается обширность Интернета и

уязвимость личной информации в сети. В ней подчеркивается

что большинство пользователей не являются экспертами в области защиты своих онлайн-данных, что делает их легкой мишенью для хакеров.

что делает их легкой добычей для хакеров.

Что такое кибербезопасность?

Кибербезопасность определяется как процесс защиты аппаратных средств,

программного обеспечения и данных от онлайн-атак. Она обеспечивает конфиденциальность,

доступность и целостность данных. Надежная система кибербезопасности

включает в себя несколько уровней защиты, распространяющихся на сети, компьютеры,

программы и данные. Подчеркивается, что ключевую роль играет профилактика, поскольку гораздо

гораздо легче предотвратить кибератаки, чем бороться с их последствиями.

Общие угрозы кибербезопасности

В главе рассматриваются распространенные угрозы кибербезопасности, такие как

ransomware, рекламное и шпионское ПО. В частности, атаки на программы-вымогатели

отмечается, что они происходят каждые 10 секунд, поэтому пользователям крайне важно

быть бдительными в вопросах сетевой безопасности. Рекламное и шпионское ПО может

проникать в системы, нарушать конфиденциальность пользователей и наносить значительный ущерб.

Преимущества кибербезопасности

Описано несколько преимуществ кибербезопасности, включая предотвращение

атак вымогателей, рекламного и шпионского ПО, улучшение SEO-функционала сайтов и

предотвращение финансовых потерь. В главе подчеркивается, что кибератаки могут

привести к значительным финансовым потерям для предприятий, особенно небольших,

и даже могут привести к закрытию стартапов. Укрепление доверия

Построение доверительных отношений с клиентами имеет жизненно важное значение, и кибербезопасность играет решающую роль в обеспечении целостности данных

Кибербезопасность играет решающую роль в обеспечении целостности данных и доверия клиентов.

Основы кибербезопасности

В этой главе представлены ключевые термины, необходимые для понимания

Кибербезопасность:

Аутентификация: проверка источника информации с помощью таких факторов.

таких как знание, владение или присущие характеристики.

Авторизация: Определение разрешений и привилегий пользователя после

аутентификации.

Неотрицание: Установление договора между пользователями и

для предотвращения отказа в обработке данных.

Конфиденциальность: Обеспечение защиты данных от несанкционированного

Конфиденциальность: Обеспечение защиты данных от несанкционированного доступа и ограничение доступа к информации даже авторизованных пользователей.

Целостность: Обеспечение точности и надежности хранимых данных,

предотвращение несанкционированных изменений.

Доступность: Обеспечение доступа пользователей, необходимого для функционирования системы.

Доступность:** Обеспечение доступа пользователей, жизненно важного для функционирования системы, и предотвращение атак типа "отказ в обслуживании" (DoS).

Важность кибербезопасности

В этой главе подчеркивается важность кибербезопасности в эпоху

когда личная информация легко доступна в Интернете. С увеличением

количества времени, проводимого в сети, люди становятся уязвимыми для дезинформации

и вредоносным атакам. Кибербезопасность можно сравнить с тормозом автомобиля,

обеспечивая контроль и безопасность при перемещении по онлайн-миру.

В заключение главы подчеркивается необходимость для частных лиц и

предприятий активно внедрять меры кибербезопасности, подчеркивая, что

что понимание и следование рассмотренным принципам является важнейшим условием

обеспечения безопасной работы в Интернете.

9Глава 8: Понимание операций вредоносного ПО и кибератак

После изучения информации, представленной в этом руководстве, настало время

углубиться во внутреннюю работу вредоносных программ и кибератак.

Защита наших систем требует бдительности при выборе веб-сайтов, которые мы посещаем.

посещать, следить за тем, кто получает доступ к нашей сети, и многое другое. Пренебрежение

Эти аспекты могут привести к значительному ущербу и финансовым потерям. Таким образом,

соблюдение предельной осторожности имеет первостепенное значение для защиты нашей цифровой

среды. В этой главе мы изучим тонкости вредоносного ПО

и различные методы взлома, угрожающие нашим сетям, а также вооружимся знаниями, необходимыми для защиты

знаниями, необходимыми для противостояния этим угрозам.

Разновидности вредоносного ПО

Сфера вредоносного ПО включает в себя широкий и разнообразный спектр

вредоносных программ, в зависимости от целей и методов хакера. Очень

крайне важно сохранять бдительность в отношении нескольких различных типов, включая:

1. Ransomware: Эта вредоносная программа захватывает контроль над вашими файлами,

требуя выкуп за их сохранение. Платить выкуп зачастую бесполезно,

и это может усугубить ситуацию.

2. Рекламное ПО: Рекламное ПО наполняет вашу систему нежелательной рекламой и

перенаправляет поисковые запросы на определенные веб-сайты.

3. Боты: Эти автоматизированные скрипты завладевают вашим компьютером, превращая его

его в зомби для проведения онлайн-атак, как правило, без ведома пользователя.

пользователя.

4. Руткиты: Созданные для сокрытия присутствия вредоносного ПО, руткиты

имитируют обычные файлы, позволяя вредоносному ПО действовать скрытно.

5. Шпионские программы: Эти вредоносные программы скрытно передают данные с вашего жесткого диска.

5. Шпионские программы: эти вредоносные программы скрытно передают данные с жесткого диска, оставляя вас в неведении относительно их кражи.

6. RAT (Remote Access Tool): После взлома системы RAT

помогает злоумышленникам сохранить контроль над сетью. Она может перехватывать

нажатия клавиш, делать фотографии с помощью камеры и проникать на другие машины.

незаметно передавая информацию злоумышленнику.

7. Вирусы: Вирусы внедряются в компьютерные программы и

распространяются по устройствам, оставляя после себя заражения.

8. Черви: Подобно вирусам, черви самовоспроизводятся, но для их распространения не требуется

Для их распространения не требуется программа-хост или вмешательство человека. Они используют уязвимости системы

уязвимости системы или используют социальную инженерию, чтобы обмануть пользователей и заставить их

выполнения программы.

Чтобы оценить природу подозрительного файла, его сканирование с помощью автоматических

Это прагматичный подход. Некоторые инструменты имеют открытый исходный код, другие

являются коммерческими. Эти утилиты быстро оценивают потенциальное влияние файла на

системы, генерируя подробные отчеты о ключах реестра, активности файлов,

значениях мьютексов и сетевом трафике.

Этапы анализа вредоносного ПО

Анализ вредоносного ПО предполагает изучение различных свойств и этапов, каждый из которых

каждая из которых позволяет понять природу угрозы. Начальный этап - это

статический анализ свойств, предполагающий внимательное изучение подозрительного файла

без выполнения. Изучаются строки, хэши, ресурсы, упаковщик

сигнатуры упаковщика, сведения о заголовках и метаданные, такие как дата создания, могут помочь

выявить фундаментальные признаки компрометации.

После того как автоматизированные инструменты проанализируют статические свойства, аналитики решают

необходимо ли более детальное изучение образца вредоносной программы.

необходимо. Комплексный анализ предполагает заражение изолированной системы

с вредоносным ПО, чтобы проследить за его поведением. Аналитики должны понять

процессы вредоносной программы, сетевые действия, взаимодействие с файловой системой и изменения в реестре.

изменения в реестре. Также может быть использована экспертиза памяти, чтобы понять.

как программа использует системную память. Этот этап позволяет наблюдать

попытки вложения, что является важным аспектом, отсутствующим в автоматизированных

расследованиях.

Следующим шагом является ручное восстановление кода, позволяющее получить ценные сведения путем

препарирования скомпрометированного кода. Дизассемблеры, отладчики и

декомпиляторы - инструменты, позволяющие проникнуть в логику вредоносной программы,

обеспечивая более глубокое понимание, чем поведенческий анализ.

Предотвращение кибератак

Теперь, когда мы познакомились с вредоносным ПО и его различными

различных аспектов, давайте сосредоточимся на стратегиях предотвращения, чтобы эффективно защитить наши системы

эффективно. Основные шаги по предотвращению атак вредоносного ПО включают:

1. Просветите себя и пользователей о лучших методах предотвращения

вредоносного ПО.

2. Не загружайте и не запускайте неизвестные программы и не вставляйте

непроверенных носителей в компьютер.

3. Научитесь распознавать потенциальные вредоносные программы, например, фишинговые письма.

4. Проводите необъявленные учения, например, намеренные фишинговые

4. Проводите необъявленные учения, например намеренные фишинговые кампании, для повышения осведомленности пользователей.

В дополнение к этим мерам безопасность сети можно повысить

с помощью контролируемого доступа, используя такие проверенные технологии, как

брандмауэры, VPN, IDS, IPS и другие. Хотя физическое разделение систем

остается крайним средством, оно все равно имеет уязвимые места.

Использование надежного антивирусного программного обеспечения повышает уровень безопасности, поскольку оно обнаруживает

и удаляет вредоносные программы. Необходимо проводить регулярные проверки безопасности

для выявления и устранения уязвимостей системы, таких как ошибки в программном обеспечении или

небезопасные приложения. Регулярное резервное копирование обеспечивает сохранность важных данных, гарантируя

восстановление в случае атак вымогателей или потери данных.

Типы кибератак

Понимание многообразия видов кибератак крайне важно для

защиты вашей системы. Кибератаки могут принимать различные формы, и при

бдительности их можно предотвратить:

1. Кибератаки: Эти интернет-операции направлены на получение

интеллектуальной собственности или финансовой выгоды, нарушая при этом работу компании-цели.

нарушая при этом работу целевой компании. Кибератаки, спонсируемые государством, могут быть политически

политически мотивированными.

2. Фишинг: злонамеренные хакеры используют уловки, чтобы обманом заставить цель

действий в соответствии с их желаниями. Это включает выдачу себя за доверенных

лиц или организаций, чтобы завоевать доверие.

3. Несанкционированное разглашение: Несанкционированное разглашение происходит, когда организация раскрывает вашу информацию без вашего согласия.

организация раскрывает вашу информацию без вашего согласия.

4. Китобойство: Китобойство - это более изощренная форма фишинга, которая направлена на

высокопоставленных лиц, собирая обширную информацию для создания

убедительных электронных писем.

5. Атаки вредоносного ПО: Вредоносное ПО проникает в системы через вредоносные

Вредоносное ПО проникает в системы через вредоносные вложения или загрузки, причиняя вред после активации.

6. Атаки типа "человек посередине": Эти атаки перехватывают и манипулируют

коммуникациями между клиентом и сервером.

7. Атаки на пароли: Пароли являются распространенной мишенью, доступ к которой осуществляется с помощью

различных методов, включая перебор и атаки по словарю.

Чтобы защититься от таких атак, следует использовать надежные и уникальные пароли.

следует использовать сложные уникальные пароли, а пользователи должны избегать предоставления личной информации в Интернете

или по электронной почте. Физическая безопасность, брандмауэры, системы обнаружения вторжений и

регулярное обновление программного обеспечения - все это играет важную роль в укреплении вашей защиты.

Защита системы от вредоносных программ и потенциальных атак зависит от

принятия проактивного и комплексного подхода. Знания, полученные

полученные в этой главе, в сочетании со стратегиями, изложенными в данном руководстве,

позволят вам эффективно ориентироваться в сложном ландшафте кибербезопасности.

10Глава 9: Последствия кибернетического нападения

В этом руководстве мы уделили значительное время рассмотрению

различных тактик проникновения хакеров в компьютерные системы. Многие из

Эти методы могут показаться обманчиво простыми,

но они могут нанести серьезный ущерб и привести к краже конфиденциальной

информации. Кибератаки представляют собой серьезную угрозу для предприятий

по всему миру. По данным одного исследования, глобальные компании ежегодно теряют более 400 миллиардов долларов из-за кибератак.

ежегодно теряют более 400 миллиардов долларов из-за кибератак. Более того, среди

предприятий, ежегодно подвергающихся крупным утечкам данных, не менее 40

не менее 40 процентов сталкиваются с неплатежеспособностью в течение того же года.

Поэтому, чтобы обезопасить свои финансы и предотвратить крах бизнеса, необходимо

всестороннее понимание угроз и методов, используемых

хакеров, необходимо для эффективной защиты ваших активов.

Разновидности кибератак

Основная цель кибератаки - скомпрометировать компьютерную

сети или уничтожить компьютерную систему. Хакеры используют различные методы

для достижения этой цели. Четыре основные схемы, используемые для совершения

кибератаки, следующие:

1. Ransomware: Как следует из названия, ransomware - это тип

Программное обеспечение, предназначенное для блокирования доступа к важным данным и информации до тех пор, пока не будет выплачена определенная сумма денег.

пока не будет выплачена определенная сумма денег. Многочисленные частные лица и даже крупные

корпорации становятся жертвами этой формы атак, неся значительные

финансовые затраты. Хакер, как правило, обещает раскрыть информацию

после получения оплаты, но иногда они этого не делают, оставляя после себя

нераскрытые проблемы.

2. Вирусы: Среди наиболее распространенных методов кибератак - использование

вирусов. Как правило, они проникают на компьютер через зараженные электронные письма

вложения или файлы общего доступа. Как только один компьютер в сети оказывается заражен,

вирус быстро распространяется по всей сети, нанося существенный ущерб.

3. Шпионские программы: Загрузка некоторых типов программ из Интернета может

шпионского ПО в вашу систему. Шпионские программы предназначены для перехвата и

передачи конфиденциальной информации, такой как пароли и поведение в Интернете, хакеру.

хакеру.

4. Кража личных данных: Когда люди думают о кибератаках, кража личных данных часто

приходит на ум в первую очередь. Похитители личных данных получают доступ к персональной идентифицирующей

информации, такой как номера социального страхования или данные кредитных карт, чтобы

выдавать себя за других людей и совершать мошенничества и кражи.

Последствия кибератаки могут значительно отличаться для каждого предприятия.

В зависимости от таких факторов, как продолжительность, время и отрасль, последствия кибератаки могут значительно отличаться для каждого предприятия.

Тем не менее, необходимо учитывать несколько общих последствий при оценке

Тем не менее при оценке уровня безопасности и возможных последствий необходимо учитывать несколько общих последствий:

1. Ущерб репутации: Нарушение кибербезопасности или кибератака может

подрывает доверие клиентов и заинтересованных сторон. Серьезность нарушения

прямо пропорциональна потере доверия, что иногда приводит к

значительный удар по репутации компании. Заинтересованные стороны и клиенты

могут не захотеть сотрудничать с компанией, подвергшейся утечке, особенно если она не смогла защитить их данные.

компания не смогла защитить их данные. Это может привести к потере бизнеса

и помешать привлечению инвесторов, поставщиков и талантливых специалистов.

2. Кража: В то время как кибератака на крупный банк может принести значительную

хакеры могут получить значительную прибыль, но малые предприятия часто оказываются менее подготовленными, что делает их более легкой мишенью.

что делает их более легкой мишенью. Мошенничество с использованием кибертехнологий может привести к значительным денежным

а похищенные данные могут быть выгодны хакерам, особенно в "темной паутине".

Темной паутине. Кража интеллектуальной собственности также может иметь далеко идущие

последствия, поскольку может привести к потере многолетних инвестиций в исследования и разработки.

инвестиций в исследования и разработки.

3. Финансовые потери: Киберпреступность может оказать непропорционально большое

финансовое воздействие на малые предприятия по сравнению с крупными.

Малые компании могут тратить значительные суммы на восстановление после

что ставит под угрозу их финансовую стабильность. Пренебрежение мерами кибербезопасности

может привести к краху бизнеса небольших компаний.

4. Штрафы: Утечки данных могут привести к штрафам и поборам за нарушение

за нарушение правил защиты данных, которые призваны обеспечить сохранность информации о клиентах.

информации клиентов. Многие мировые власти рассматривают возможность ужесточения правил для

защиты потребителей, что создает дополнительное финансовое бремя для компаний, которые

не соблюдающих их.

5. Скрытые расходы: Помимо прямых финансовых потерь, компания должна

бороться с нематериальными издержками после кибератаки, такими как операционные

сбои в работе. Компании, не имеющие надежных стратегий обеспечения устойчивости и непрерывности бизнеса

могут столкнуться с дополнительными проблемами, а небольшие компании могут

могут увеличиться страховые взносы или долговые обязательства. Нарушение операционной деятельности может

усугубить существующие финансовые трудности и потенциально привести к краху бизнеса

краху.

Чтобы снизить риск кибератак, компании должны принимать упреждающие меры.

шаги. К ним относятся разработка внутренних политик для обучения сотрудников

риски безопасности и информирование о возникающих угрозах. Регулярно

Регулярное обновление программного обеспечения и использование надежных облачных сервисов могут повысить уровень кибербезопасности.

кибербезопасность. Также рекомендуется обращаться за советом к экспертам и взаимодействовать с

профессиональными экспертами по безопасности. Число кибератак растет, и

защита информации и систем от потенциальных угроз имеет решающее значение для

предприятий любого размера.

11Глава 10: Защита сетей с помощью эффективного сканирования

Стремясь обеспечить безопасность наших сетей, необходимо

изучить практику сканирования сетей. Это включает в себя изучение

нет ли в наших сетях вредоносных объектов или уязвимостей, которые

которые могут быть использованы потенциальными хакерами. Чтобы начать, нам нужно погрузиться

в образ мышления хакера, понять его стратегию проникновения в

наши системы.

Взлом начинается с этапа, известного как "отпечаток". На этом

На этом этапе хакеры собирают первоначальную информацию о предполагаемых целях.

Однако одной этой предварительной информации недостаточно. Она служит

фундаментом, а дальнейшие, более сложные методы сбора данных

на последующем этапе, который называется "сканирование".

Сканирование сети - важнейший компонент сбора разведданных. Оно

позволяет получить информацию о различных аспектах, в том числе о конкретном IP-адресе

детали, операционную систему и архитектуру объекта, а также сервисы.

запущенные в сети. Кроме того, злоумышленники ищут информацию о
сети и хост-системе. Чем больше у вас информации о
цели, тем больше шансов обнаружить слабые места и получить
доступ к сети. Производительность сканирования и глубина информации
зависят от мотивов хакера, которые могут включать в себя:
Определение IP-адресов хостов и открытых портов в сети.
Обнаружение открытых портов, наиболее желанных точек входа для хакеров.
Выявление уязвимых открытых портов для эксплуатации.
Определение операционной системы и архитектуры системы для использования
слабые места.
Классификация уязвимостей и угроз на основе слабых мест системы
слабых мест системы.
Одним из существенных рисков, связанных с активным наблюдением, является возможность
возможность обнаружения цели. Чтобы минимизировать этот риск, хакеры должны использовать
скрытные методы, оставаясь незаметными, чтобы не вызывать подозрений и не
чтобы не вызвать подозрений или тревоги. Эти методы включают в себя сокрытие атаки в
легитимного трафика и изменение IP-адреса источника, использование сетей анонимности
сети и изменение параметров пакетов, часто с помощью таких инструментов, как Nmap.
Прежде чем хакер или испытатель на проникновение приступит к исследованию системы
прежде чем хакер или тестер проникновения приступит к исследованию системы, необходимо
отключить ненужные службы в своей
системе (Kali), поскольку они могут случайно взаимодействовать с целевой
сети, предупредив цель о вторжении.
Изменение параметров пакетов - один из основных шагов при проведении
сканирования сети с целью выявления уязвимостей. Типичный подход включает
выполнение "целевого сканирования", отправку определенных пакетов и анализ
ответы. Network Mapper (Nmap) - это хорошо известный инструмент для этой цели.
и, как и многие другие инструменты для работы с пакетами, он наиболее эффективен
при запуске с привилегиями root-уровня. Различные скрытные техники, позволяющие избежать
Различные скрытные методы, позволяющие избежать обнаружения и тревоги в целевой сети,
включают:
1.определение цели сканирования заранее и отправка минимального
минимальное количество пакетов, необходимых для достижения цели.

2.Избегание сканирования, которое может вызвать тревогу или нарушить работу целевой системы.

3.Случайное определение или подмена IP-адресов источников, адресов портов и MAC-адресов

адресов.

4.Настройка времени для замедления передачи пакетов.

5.Изменение размеров пакетов путем фрагментации или добавления

случайных данных.

Помимо манипуляций с пакетами, мы можем работать с прокси-серверами

такими как Tor и Privoxy. Tor, сокращение от "The Onion Router", облегчает

анонимное общение по сети. Сообщения, передаваемые через

через луковую сеть, покрыты слоями шифрования, напоминающими слои лука.

лука. Эта технология позволяет пользователям оставаться скрытыми, шифруя свой

трафика и маршрутизации его через ряд узлов, что защищает от атак, связанных с анализом трафика

атак на анализ трафика. Использование скрипта Tor Buddy еще больше усиливает

анонимность за счет частой смены IP-адреса Tor, что затрудняет отслеживание личности пользователя.

отследить личность пользователя.

После того как хакер обеспечил свою анонимность, следующим шагом будет

выявление сетевой инфраструктуры, особенно устройств в доступной через Интернет

части сети. Эта информация может быть использована для того, чтобы

запутать или исключить результаты тестера. Она включает в себя такие устройства, как брандмауэры

и системы проверки пакетов. Кроме того, эти данные помогают хакерам

определить уязвимые машины и предпосылки для скрытного сканирования,

Получение информации об уровне безопасности объекта.

Перечисление хостов - еще один важный этап, позволяющий хакеру

собрать конкретную информацию о целевом узле, например открытые порты,

запущенные службы, приложения и базовая операционная система. Этот

Этот процесс должен выполняться незаметно, чтобы не насторожить цель.

Восстановление хоста в реальном времени также может быть полезным, и основной техникой для этой цели является

для этого является "пинговое сканирование". Эта техника помогает выявить живые узлы или

компьютеров путем отправки пакетов на IP-адреса и ожидания ответов,

указывая на их присутствие. Выбор используемого протокола - TCP,

UDP, ICMP или ARP - зависит от конкретных потребностей сканирования.

Сканер безопасности Nmap - ценный инструмент для проведения пингового сканирования

и определения IP-адресов "живых" узлов. Этот сканер позволяет

одновременную оценку нескольких узлов и может выполняться

удаленно через Интернет, чтобы определить живые узлы.

Хотя Nmap не является эксклюзивным инструментом для Kali, это очень эффективный инструмент для

картирования сетей. Он управляется из командной строки, что обеспечивает гибкость и

широкий спектр возможностей. Для тех, кто предпочитает графический интерфейс, Zenmap

доступен в виде фронтенда. Тем не менее, версия с командной строкой

предоставляет больше опций и возможностей для адаптации.

Nmap упрощает задачу администратора по быстрому изучению

сетевых системах. Его способность определять живые хосты и связанные с ними сервисы

повышает его функциональность. Механизм создания сценариев Nmap Scripting Engine (NSE) еще больше

позволяет администраторам создавать скрипты для обнаружения уязвимостей.

Чтобы приступить к сканированию сети, необходимо выполнить определенные системные требования

чтобы приступить к сканированию сети, должны быть выполнены определенные системные требования, в том числе:

1.Kali Linux в качестве операционной системы.

2.вторичная машина с соответствующими правами для запуска сканирования Nmap

сканирования, что часто достигается с помощью виртуальной машины.

3.стабильное сетевое соединение или надежное внутреннее сетевое соединение

для виртуальных машин.

Регулярное сканирование очень важно, так как новое программное обеспечение и обновления могут

могут появляться уязвимости. Обнаружение этих уязвимостей на ранней стадии может

значительно повысить безопасность сети и защитить конфиденциальную информацию

от попадания в чужие руки.

Проведение сканирования сети, своевременное обнаружение потенциальных угроз и

проактивное устранение уязвимостей - важнейшие шаги в поддержании

сетевой безопасности и защиты личной информации. Регулярное сканирование

позволяют всегда быть в курсе состояния сети и всех потенциальных

слабых местах, которыми она может обладать.

12 Заключение

Спасибо, что дошли до конца статьи "Взлом в Kali Linux: Беспроводная сеть

Проникновение в беспроводные сети". Мы надеемся, что это руководство дало вам ценные сведения

и необходимыми инструментами для достижения ваших целей, какими бы они ни были. Следующий

Следующий шаг - начать применять рассмотренные в этом руководстве методы для

повышения безопасности вашей собственной системы. Никогда не стоит

самоуспокаиваться, когда речь идет об устройствах, подключенных к Интернету и

беспроводным сетям. Хотя легко чувствовать себя в безопасности и считать, что ваша система

неуязвимой, реальность такова, что хакер потенциально может использовать ваш

компьютер в своих целях. Необходимо быть хорошо подготовленным и осведомленным

о своей сети и способах ее защиты крайне важно.

В этом руководстве мы рассмотрели основы

беспроводного проникновения и изучили, на что обращают внимание хакеры при попытке

проникнуть в вашу сеть. Хотя переход на беспроводные технологии

несомненно, предоставил потребителям больше свободы и мобильности, он также

также открыл новые возможности для хакеров по взлому систем и созданию проблем

проблемы.

Применяя идеи и методы, описанные в этом руководстве, мы можем

мы сможем сосредоточиться на защите наших систем и обеспечить их максимальную

безопасность. Хотя всегда существует риск того, что хакер получит доступ к вашей системе

и причинить неприятности, но при должной подготовке и использовании методов и стратегий сканирования

методов и стратегий, описанных здесь, мы сможем выявить и устранить

уязвимости до того, как ими воспользуются хакеры. Такой проактивный подход

обеспечивает безопасность вашей информации и информации других пользователей системы.

системы.

Работа с беспроводным проникновением - это процесс, который может потребовать времени

и самоотдачи, и он не всегда так прост, как может показаться.

Однако научиться использовать эти методы и обращать внимание на

Однако научиться использовать эти методы и обращать внимание на потенциальные уязвимости в вашей сети очень важно. Когда вы будете готовы

работать с беспроводным проникновением с помощью операционной системы Kali Linux,

обратитесь к этому руководству.

Если вы нашли эту книгу полезной, мы будем очень признательны за

за отзыв на Amazon! Ваши отзывы бесценны для нас.