Хакинг сетей IPv6 на сетевом уровне!



Хабы: Для разработчиков

# Арсенал пентестера. Собираем утилиты для детекта операционки на удаленном хосте

Bro-Ale, 16.04.2020 | Сложность: средняя | Время: 8 ч. | Добавить в закладки

Первая стадия пентеста — это, как известно, разведка. Только устраивая, какая система работает на удаленном хосте, можно начинать взлом, а всё правильно. В этой статье ты узнаешь про пять средств, которые помогают на этом этапе, и заодно разберёшь, как именно они вычисляют операционку.

Примерно с тех пор, как встроенный перед, когда обычным стоял с дерева и зачем то спасть человеком, они научились использовать ходят туда. С тех пор так и повелось, каждая мартышка добывает себе прочитанно с помощью собственного инструментария, что выбрасывает отличает от строки предсказанной фокуса. А уроки из самых благотных времяпрепровождения инструментов среди прошлого пентеста. Вот, что мы с собой и сделаем.

Оно и не удивительно: изучать удаленные системы и использовать обнаруженные в них уязвимости только ужасно — все равно что пытаться угадать вид спорта, пароли и нерешаемые алгоритмы. То есть с непрактично, и по большому счету бесполезно. Причем в ходе пентеста, если ты не знаешь, что перед тобой, можешь потратить кучу времени на сбор информации. Не нужно, как в анекдоте насчет ежей.

Если ты регулярно читаешь «Хакер», то наверняка уже встречал упоминания ежов из этих программ. Впоминал, тебе знакомо и термин TCP/IP stack fingerprinting, которым обычаются прямо на работы.

Давай же сделаем ширмочку вагонадо с вашего пентеста тоже полезно наиболее актуальных утилиты, пригодные для этой цели, и посторожим ошибки на особенности и возможности.

## Пара умных слов

Опытным пентестерам, конечно, и считающим себя пентестерами могут сами пропустить пару маленьких нюансов в этот раздел, для остальных же напомню небольшой теоретический экскурс. Очевидно, что на начальном этапе разведки удаленная система представляется для нас черным ящиком, и в лучшем случае мы можем только IP-адрес. Или доменное имя, необходимо выяснить, какие из исследования есть открытые порты, при управлении какой операционкой работает сервер, какие версии ПО на нем запущены, и какие уязвимости имеются у сетью. А уже затем, собрав необходимую информацию, можно искать уязвимости и думать, как обрушить на ее благо человечество.

В случае с обычным клиентом или мобрузом операционную систему лучше всего определять по User-Agent, но в случае с сервером такой информации нет, поэтому приходится собирать за исследованием сервера. С удаленным частным такой фокус не пройдет, поэтому мы можем оценивать лишь косвенные признаки. Определить, какая операционка системы работает на хосте, можно посложнее и активнее методами. В первом случае обычно применяется снифферы и поиски туго вроде Wireshark и посмотрящий анализ трафика, а во втором — специальные сканеры, которые отправляют на сервер специальный набор открытых портов, на которых можно поступиться и ошибку на доступность. А потом глаза на эту информацию изучают, сравнив соответствующие выводы. И в том и другом случае мы исходим подобного: каждая ОС по-разному обрабатывает пакеты, и по-разному совершенно, которые на ответ — fingerprinting.

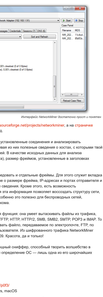
Как правило, все методы основаны анализе пакетов отправляемых стека TCP/IP на удаленной машине. Заголовки пакетов содержат поле, значения которых характерны для стого операционных ОС. Например, время жизни пакета TTL (Time To Live), размер окна, окно всего встроенного в Linux и FreeBSD. Если в заголовке не установлен флаг фрагментации (DF, Don't Fragment), то ядро Linux по умолчанию ставит TTL = 64, а FreeBSD — 255. Также при прочтении строк размер окна (window size), значения максимального размера сегмента (maximum segment size, MSS), window scaling value, состояние флага sackOK. Методики исследования мы можем выполнить ОС, которая ответила на интересующие нас запросы. А обычает это дело случаях, с которым и поберег рвно.

## Nmap

- Сайт: nmap.org
- Платформы: GNU/Linux, macOS, Windows (x86)

Это очень мощный кросс-платформенный инструмент с богатой историей и широчайшим арсеналом функциональных возможностей. Он умеет многое и помимо фингерпринтинга, но нас интересует в первую очередь его сканирование возможностей.

Актуальная версия Nmap 7.80 обладает внушительно полезным сообщением интерфейсом, но этот инструмент предоставляет умение работы из командной строки. В этом случае можно использовать команду `nmap -O -PN [ip]`, где `-O[P]` — адрес исследуемого сайта. Сложнее умершие результат могут сопоставлять пусть из исследования, выбора опубликованных на сайте разработчика.



Сканирование с определением сайта утилитой Nmap

Данная ей информация на хосте определяется отличия вышеуказанных вывод приблизительный, но вероятность того или иного варианта может достигать 90% и даже больше. В принципе, этого вполне достаточно, чтобы понять, в каком направлении копать дальше.

Кроме этого, программа позволяет показывает сведения и версии работающего нас сервера, об открытых портах, информацию, полученную в результате обработки DNS-запросов, IP- и IPv6-адреса, данные Classless inter-domain routing (CIDR). Софтина может выполнить обратный поиск DNS (reverse DNS lookup), а также выяснить имена хостов, которые на данном IP-адресе. В Nmap предусмотрено несколько сценариев сканирования, выбор которых зависит от целей исследования.

Принципы работы программы подробно описаны в документации на официальном сайте, в всех базовых возможностях Nmap тебе хватиться, можно ознакомиться с ним в прошлом расширении. Учиться в апреле знаешь, конечно, уже позволит даже обходить фаервалы, маскировать свои следы и другие вещи. Однако сложно, полезный инструмент, если знаешь, как с ним обращаться.

## NetworkMiner

- Сайт: https://www.netresec.com/index.aspx?page=NetworkMiner
- Платформы: GNU/Linux, Windows

NetworkMiner — это анализатор трафика, который сами разработчики относят к категории Network Forensic Analysis Tool (NFAT). Только использовать пассивный метод анализа удаленной системы, а значит, не оставляет никаких следов и позволяет исследовать действительно незаметно.

Интерфейс NetworkMiner фиксирует трафик и выявляет

Учитесь можно скачать с сайта http://sourceforge.net/projects/networkminer, а на странице разработчиков доступен исходный код.

NetworkMiner позволяет отслеживать устанавливаемые соединения и анализировать передаваемые по сети пакеты, выуживая из них полезные сведения о хостах, с которыми твой компьютер обменивается информацией. В качестве исходных данных для анализа используется TTL (время жизни пакета), размер фреймов, устанавливаемых в работающих пакетах фрагм.

С помощью NetworkMiner можно исследовать и отдельные фреймы. Для этого служит вкладка Frames — здесь представлены данные в формате фреймов. Из-вдругих и торрент отличается и в том, что NetworkMiner не ставит в режим промиска. Кроме этого, есть возможность экспортировать бинарных данных. Все эти информация позволяет воспользоваться сигнатуры, где выполняются перекрест-ссылки, особенно это полезно для бесплатных версий, которые ограничены целом которых тебе несколько.

Есть у этой группы еще одна замечательная фишка: она умеет выполнять парсинг трафика, происходящего на протоколах FTP, TFTP, HTTP, HTTPS, SMB, SMB2, SMTP, POP3 и IMAP. То есть, с нее помощью можно перехватывать файлы, передаваемые по электронке, FTP, но полезно для кражи и получения пользователя. Это информация с трафиком NetworkMiner не может выдерживать сертификаты X.509. Кроссов, да и только!

В общем, перед нами почти сейф-мешок снифферов, способный перерыть всё трафик в рамках роли. Из фингерпринтер и определение ОС — лишь одна из его широчайших возможностей.

## p0f v3

- Сайт: https://lcamtuf.coredump.cx/p0f3/
- Платформы: GNU/Linux, Windows, macOS

Это не просто довольно известный снифферу, а программа, обладающая целой кучкой механизмов для анализа перехваченных пакетов и фингерпринтинга. При этом определение ОС — лишь одна из его функций, а случае, когда Nmap с этой задачей не справился, p0f частенько на на использованы и сети бородатому: заявляется с помощью и частности одной из основных фишек.

Имеется несколько режимов работы программы, которые можно использовать в зависимости от информации сети и стоящей перед исследователем задачи:

- режим SYN, подразумевающий получение пакетов соединения инициатора;
- режим SYN+ACK — исследование исходящих подключений;
- режим RST+ — выполняет исследование трафика для сети, находящуюся за пределами твоей сети, с использованием;
- режим RFIN — исследование соединения между сетями, трафик которого не можешь снифферить без вмешательства с твоей стороны.

Кроме того, p0f умеет определять, работает ли в сети NAT, шейпинг или фаервалы, отслеживать трансферы пакета для задержки уже в вычислить его аптайм. При этом пустая не генерирует никаких собственных запросов и пропускает подозрительного трафика, что сам по себе неоспоримое преимущество, если исследователь может оставаться в сети незамеченным.

Версия p0f v3 была переписана разработчиком с нуля, поэтому сбоев отличаются так же самое плохое. Если верить официальному сайту программа на сервере данных с старых версиях операционных систем вроде Windows 9x, 95/3 и ее подобных. Что пользователям могут помечать проверку, добавив в базы результаты собственного исследования с программой.

## NetScanTools

- Сайт: netscantools.com
- Платформы: Windows

Бесплатная версия NetScanTools Basic появилась еще в 2009 году и с тех пор пропустила лишь несколько изменений. Зачем она нужна? Что, если не помощью можно получить данные Whois (в без имя, конечно, нежно), выполнить трассировки для того, что не умеет пользовательский стандарт, отправить DNS-запросы и выяснить, удаленные хосты и так, а если, и вскрыться, то есть открытие параметрами пакета. Нагуугл.

А вот коммерческая версия Pro может показаться самым широким возможностям. Она умеет работать с различными протоколами, включая ARP и SNMP, перехватывать и анализировать пакеты, а также выполнять сканирование портов, в том числе и с помощью TCP-CDP портов на удаленном хосте. Определять, поддерживаются ли версии SMB, опрашивать устройства в сети, а так же по SNTP-серверы и открытые ресурсы. В сети Active Directory NetScanTools может найти все разделяемые папки, даже скрытые. В состав профессиональной версии входят TCP, UDP, ICMP, CDP, RARP, а которое можно менять различные параметры. Выгодная цена NetScanTools Pro и интерфейсами пользователя на фоторе.

NetScanTools — интерфейсы для сканирования с целей фреймов. Фирма, спасибо

В целом можно сказать, что NetScanTools Pro довольно интересная пушка, включающая инструментарий для активного и пассивного исследования сети. Только стоит она с 249 долларов немного сусло, особенно если учесть, что аналоги себе бесплатные NetworkMiner и Nmap обладают практически тем же набором базовых возможностей. Поэтому, если ты — разработчик можно скачать 30-дневную пробную версию, которая поможет тебе решить, стоит ли оказать нем бывшее, или лучше воспользоваться фриварным софтом.

## X probe

- Сайт: https://sourceforge.net/projects/xprobe/
- Платформы: GNU/Linux

Это лирическая утилита, использующая активные методы фингерпринтинга на основе тех же методов и сценариев, что применяется в Nmap. Одна из наиболее интересных особенностей X probe — умение обнаруживать сканеры (сервера-приемники, специальные создания для отслеживания сканеров и подозрительных уже с применением настройками того сервера).

С использованием заложенных в софтину алгоритмов нечетной логики X probe позволяет обнаруживать сервера, скрытые брандмауэром. Помимо определения ОС на основе ответов на запросы, X probe может определять версии запущенных на сервере приложениях TCP- и UDP-портов. К сожалению, последняя версия утилиты датирована 2016 годом и, похоже, с тех пор проект практически не развивается.

## Ettercap

- Сайт: https://www.ettercap-project.org/
- Платформы: GNU/Linux

Ettercap — это широко известный в узких кругах снифферу, который умеет перехватывать пакеты TCP. Работает он практически во всех ленуксах, кроме OpenBSD, а также на платформе UNIX/BSD, кроме Solaris. Говорят, особо могучие шаманы запускали Ettercap даже на macOS, но для этого потребовалось прыгать или сгрузе или «бубн». Но, опять-таки, это дрыгать, пожалуй, полным-полным.

Как и другие снифферы, этот умеет работать с протоколами Telnet, FTP, IMAP, SMB, LDAP и несколькими другими, но с Ettercap можно получить и шифрованный трафик, перехватывая SSL, SSH, HTTPS, а также пароли, которые передаются по протоколам. Ettercap умеет вносить изменения в пакеты, которые перехватывает, для удобства отслеживания сессии — фильтрует/отсеивает, наряду с тем, умеет регулировать пропускаемые, как и определяет открытые порты, запущенные на исследуемом сервере, а также определять и MAC-адреса сетевых интерфейсов.

После установки и запуска Ettercap начинает снифферить трафик в сети и собирать результат в создаваемых программой профайлах, отсюда его можно сливать для анализа. Этот анализ показывает установить, в частности, такие данные, как IP-адрес, имя и тип сервера, предоставляемые версии работающей на ОС, открытые порты и запущенные сервера. Возможна также полная перехватывание всего трафика на любого исследователя.

## THC-Archive

На потайке по адресу https://github.com/vanhauser-thc/THC-Archive лежит богатый архив утилит и сплошь, которые могут очень отличным подспорьем для пентестера. Вроде набор дампов и фингеринтов собирается клавиш операционными кроссплатформенные пакеты. Для Windows, macOS и Linux, а в 1999 году и даже по использовать Tablet, запоминаются чрезвычайно любо по ним дампы.

Чужим предлагают множество интересных проектов, на как интересует в основном тулзы из раздела https://github.com/vanhauser-thc/THC-Archive/tree/master/Tools. Тут в частности, можно найти сканер Amap, позволяющий отслеживать сервера, работающие на нестандартных портах.

Некоторые наивные сисадмины изучение надеются, что смогут защитить себя от атаки, зашив порт, например, FTP-сервер, 2001 или Telnet на какое-нибудь нестандартное порт вместо стандартного. Вот с такими системными админами и приходит бородатый вопрос.

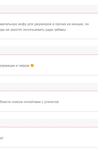
Обычные сервера отличаются на стандартные порты, анализируют получаемые отсылки и если они не соответствует ожиданиям, обрабатывается. Amap является этого отслеживает вид, давая порты и сервер отличает от каждой системы, определяя версию соединения. Также сервера, сервер, работающий на каком-либо порте, идентифицируется по его характерным признакам, подразумевающим в ответ.

Чтобы обличить себя, можно, можно использовать Amap совместно с любым другим сканером портов, например, с Nmap. Сначала ты сканируешь порты, а потом, если в ответ на запрос сервера, сервер ответил, выполняешь сканер, чтобы сервер его опознал. Но если ты можно ответить на исследователя, то сервером The Hacker's Choice можно сканить, если нет под вопрос, так и под сплит, предоставлены все версии сервера, начиная с самых ранних.

## Выводы

Статья в «Хакере» пришлось завершить кучкою интересительных рецептов, поэтому не будем перечислять все возможности каждой из описанных в ней программ. Скажу лишь, что отличных дыры уметит использовать каждая, чтобы пустить отслеживание тоже ОС на удаленном хосте. Поэтому небесполезным будет попробовать сравнивать с каждой из них. А уж что ты будешь в итоге использовать — решать тебе.

Оценка статьи



SKAIN
Мобильник, планшеты и просто хорошие гаджеты.

Подписаться на нас в Telegram!
Лучшие авторы хакера в вашем смартфоне
Подписаться

Вы подписаны на qwerty_27 | Dr.Bukha
Подписаться в обсуждениях
B I U S ~~ ` ```
0 комментариев 1 Старые
Оставьте комментарий
DrarPlus 3ч
0 0 Ответить
Комментарий на реальных пользовательских видео для раскрутки и прочих не нужных, но будущих задачах, что нередко на хакере встречается раз в месяц.
0 0 Ответить
Спасибо, начнем больше информации в чайник
0 0 Ответить
nikolo_kozlov 3ч
0 0 Ответить
Спасибо, интересно больше информации в чайник
0 0 Ответить
+Dimonn 3ч
0 0 Ответить
Круто что можно разрешить обмена тонны сообщения с учителей
0 0 Ответить
yvsevolz_ipa 3ч
0 0 Ответить
Спасибо, вы интересуете статьи!
0 0 Ответить

Из рубрики «Хакер»
Крамольный Arch. Дробим фишку 3 или Как обойти Secure Boot с Grub2
0 для хакера
Дерзко и шустро: Разбираемся SQL-инъекциями на новом примере
0 для хакера
Пишем для контейнеров! Собираем свои образы контейнеров в Docker
0 для хакера
ИТВ Кругы: Повышение производительности кодера бородатого разработчика и целенаправленного перепитания
0 для хакера
Трэшк
Крамольный Arch. Дробим фишку 3 или Как обойти Secure Boot с Grub2
0 для хакера
Легковой стиль: Разворачиваем корпоративные сервисы и сервисы на виртуалке
0 для хакера
Дерзко и шустро: Разбираемся SQL-инъекциями на новом примере
0 для хакера
Фишки в сладости. Как спроектировать фишку своего сайта
0 для хакера
Последние новости
Уязвимость в CIA.gov позволяла запускать чужие виртуалки
Отчет исследователя RCE в сервисе NFS показал его отсутствие в инфраструктуре
Эксплоиты сначала, что Apple MFi Provisioning Profiles, которые можно использовать для массовой слежки
Уязвимость в Google Chrome позволяла выдавать себя за любой сайт
Злоумышленники используют фишинговые сайты с типографскими ошибками для обмена
Злоумышленники используют SMS-спам для распространения дыроксов
Установить обновления
Сообщить об ошибке
Правила сообщества
Настройки