

ВЗЛОМ **ДЛЯ НАЧИНАЮЩИХ**

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

ShnLMS | 30.03.2020 | 4 комментария | 41,340 | Добавить в закладки



Первая стадия пентеста — это, как известно, разведка. Только установив, какая система работает на удаленном хосте, можно начинать искать в ней лазейки. Из этой статьи ты узнаешь про семь средств, которые помогут на этом этапе, и заодно увидишь, как именно они вычисляют операционку.

Примерно в тот же исторический период, когда обезьяна слезла с дерева и зачем-то решила стать человеком, она научилась использовать орудия труда. С тех пор так и повелось: каждая маршутка добывает себе пропитание с помощью собственного инструментария, что выгодно отличает ее от прочих представителей фауны. А одним из самых богатых arsenalov сподручных инструментов среди приматов обладаю, безусловно, пентестеры и хакеры.

Оно и не удивительно: изучать удаленные системы и эксплуатировать обнаруженные в них уязвимости голыми руками — все равно что пытаться напугать ежа голым задором и неумным энтузиазмом. То есть и непрактично, и по большому счету бесполезно. Причем даже ежу понятно, что первый и самый важный этап исследования любой системы — это разведка и сбор информации. На нем и заострим наше внимание.

Если ты регулярно читаешь «Хакер», то наверняка уже встречал упоминание многих из этих программ. Возможно, тебе знаком и термин TCP/IP stack fingerprinting, которым обозначается принцип их работы.

Давай же окинем широким взглядом с высоты птичьего полета наиболее актуальные утилиты, пригодные для этой цели, и постараемся оценить их особенности и возможности.

## Пара умных слов

Опытные пентестеры, хакеры и считающие себя таковыми могут смело пропустить пару молочных коктейлей и этот раздел, для остальных же проведем небольшой теоретический экскурс. Очевидно, что на начальном этапе разведки удаленная система представляется для нас «черным ящиком», и в лучшем случае мы знаем только IP-адрес. Как минимум необходимо выяснить, какие на исследуемом хосте открыты порты, под управлением какой операционной системы он работает, какой софт там установлен и способен взаимодействовать с сетью. А уже затем, собрав необходимую информацию, можно искать уязвимости и думать, как обратить их во благо человечества.

В случае с обычным компом или ноутбуком определить операционную систему проще всего. Если при взгляде на экран слегка замутило — значит, там стоит винда, захотелось что-нибудь собрать из исходников — однозначно линукс. С удаленным хостом такой фокус не прокатит, поэтому мы можем оценивать лишь косвенные признаки. Определить, какая операционная система работает на хосте, можно пассивными и активными методами. В первом случае обычно применяется сканинг с помощью тулз вроде Wireshark и последующий анализ трафика. Во втором случае используются принцип паттернов: каждая ОС имеет характерный набор открытых портов, на которые можно поступаться и оценить их доступность. А потом, глядя на эту живописную картину, сделать соответствующие выводы. И в том и в другом случае мы исследуем подобие отпечатков пальцев операционной системы, поэтому совокупность методов так и принято называть — fingerprinting.

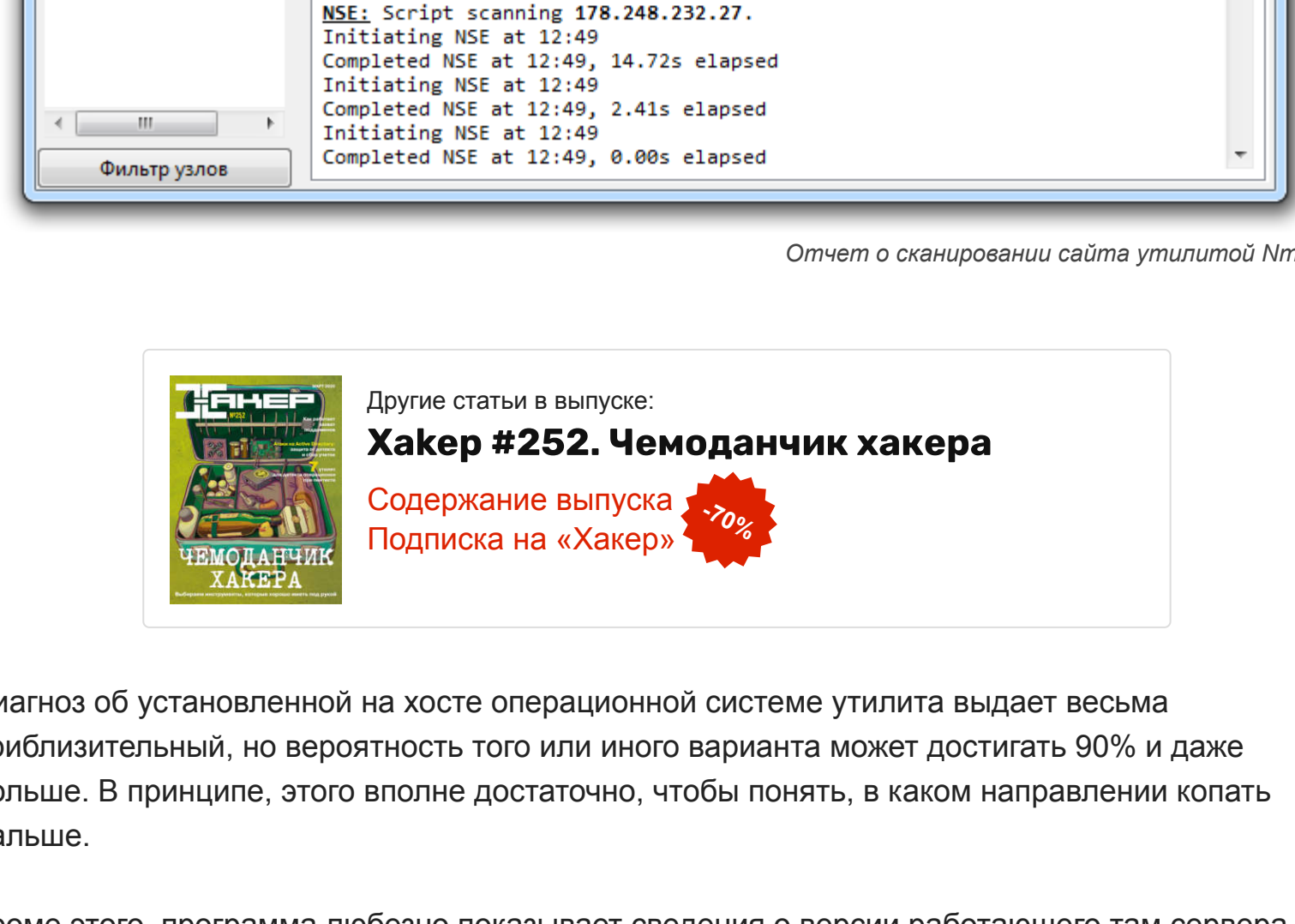
Как правило, все методы пассивного анализа трафика сводятся к изучению стека TCP/IP на удаленной машине. Заголовки пакетов содержат поля, значения которых характерны для строго определенных ОС. Например, время жизни пакета TTL (Time To Live), равное 64, чаще всего встречается в Linux и FreeBSD. Если в заголовке не установлен флаг фрагментации (DF, Don't Fragment), это намекает, что мы имеем дело с OpenBSD. Другими косвенными признаками служат размер окна (window size), значение максимального размера сегмента (maximum segment size, MSS), window scaling value, состояние флага sackOK. Методом исключения мы можем вычислить ОС, которая крутится на интересующем нас хосте. А облегчат это дело утилиты, о которых и пойдет речь.

## Nmap

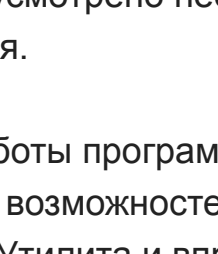
- Сайт: [nmap.org](https://nmap.org)
- Платформа: GNU/Linux, macOS, Windows (x86)

Это очень популярный кросс-платформенный инструмент с богатой историей и широким арсеналом функциональных возможностей. Он умеет многое и помимо фингерпринтинга, но нас интересуют в первую очередь его «разведывательные возможности».

Актуальная версия Nmap 7.80 обладает интуитивно понятным графическим интерфейсом, но для олдфагов предусмотрен режим работы из командной строки. В этом случае можно использовать команду `nmap -O -P [URL]`, где URL — адрес исследуемого сайта. Совсем уверенные упертые могут скомпилировать тулзу из исходников, любезно опубликованных на сайте разработчиков.



Ответ о сканировании сайта утилитой Nmap



Другие статьи в выпуске:

**Хакер #252. Чемоданчик хакера**

Содержание выпуска

Подписка на «Хакер» **70%**

Диагноз об установленной на хосте операционной системе утилита выдает весьма 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.

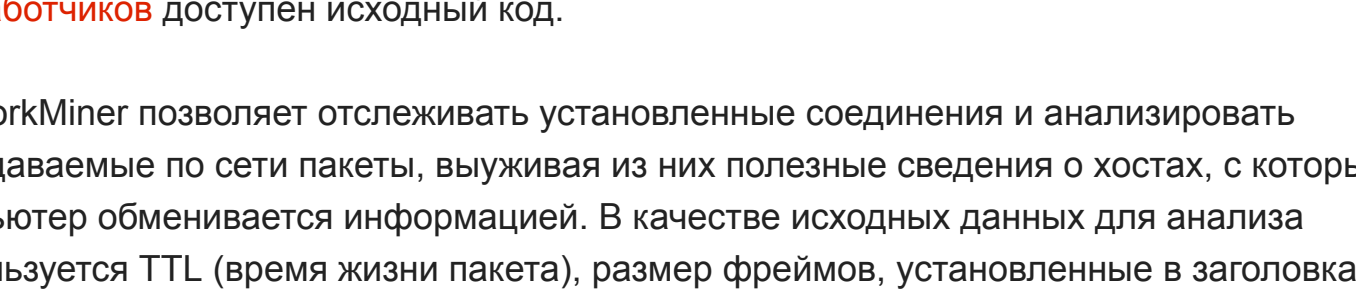
Кроме этого, программа любезно показывает сведения о версии работающего там сервера, об открытых портах, информацию, полученную в результате обработки DNS-запросов, IP- и IPv6-адреса, данные Classless inter-domain routing (CIDR). Софтина может выполнить обратный просмотр DNS (reverse DNS lookup), а также выводит большой объем другой полезной инфы. В Nmap предусмотрено несколько сценариев сканирования, выбор которых зависит от целей исследователя.

Принципы работы программы подробно описаны в документации на официальном сайте, а если базовых возможностей Nmap тебе недостаточно, можно ознакомиться со статьёй об их расширении. Утилита и впрямь очень мощная: она позволяет даже обходить файрволы, выполнять DoS и другие виды атак. Одним словом, полезный инструмент, если знаешь, как с ним обращаться.

## NetworkMiner

- Сайт: <https://www.netressec.com/index.ashx?page=Networkminer>
- Платформа: GNU/Linux, Windows

NetworkMiner — это анализатор трафика, который сами разработчики относят к категории Network Forensic Analysis Tool (NfAT). Тулза использует пассивный метод анализа удаленной системы, а значит, не оставляет никаких следов и позволяет исследователю действовать незаметно.



Интерфейс NetworkMiner достаточно прост и понятен

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

NetworkMiner позволяет отслеживать установленные 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, установленные в заголовках пакетов флаги.

С помощью NetworkMiner можно исследовать и отдельные фреймы. Для этого служит вкладка Frames — здесь представлены данные о размере фрейма, IP-адресах и портах отправителя и получателя, а также прочие полезные сведения. Кроме этого, есть возможность анализировать баннеры демонов. Вся эта информация позволяет воссоздать структуру сети, где выполняется перехват пакетов: особенно это полезно для беспроводных сетей, внутренняя кухня которых тебе неизвестна.

Есть у этой тулзы еще одна шикарная функция: она умеет вытаскивать файлы из трафика, транслируемого по протоколам FTP, FTTP, HTTP, SMB, SMB2, SMTP, POP3 и IMAP. То есть с ее помощью можно перехватывать файлы, передаваемые по электропотоку, FTP, по локалке или попросту в браузере пользователя. Из зашифрованного трафика NetworkMiner может выдергивать сертификаты X.509. Красота, да и только!

В общем, перед нами вполне себе мощный sniffер, способный творить волшебство в умелых руках. Ну а фингерпринтинг и определение ОС — лишь одна из его широчайших возможностей.

## p0f v3

- Сайт: <https://lcamtuf.coredump.cx/p0f3/>
- Платформа: GNU/Linux, Windows, macOS

Это не просто довольно известный sniffер, а программа, объединяющая целый комплекс механизмов для анализа перехваченных пакетов и фингерпринтинга. При этом определение типа ОС на удаленном узле (даже в случаях, когда Nmap с этой задачей не справился, например из-за использования в сети брандмауэра) заявляется разработчиками в качестве одной из основных функций.

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

- режим SYN, подразумевающий исследование входящих соединений;
- режим SYN+ACK — исследование исходящих подключений;
- режим RST+ — подразумевает исследование трафика для узла, находящегося за файрволом, который отклоняет подключения;
- режим MITM — исследование соединения между узлами, трафик которых ты можешь sniffить без вмешательства с твоей стороны.

Кроме того, p0f умеет определять, работает ли в сети NAT, шейперы или файрволы, отслеживать трассировку пакета до заданного узла и вычислять его аптайм. При этом тулза не генерирует никаких собственных запросов и прочего подозрительного трафика, что само по себе неоспоримое преимущество, если исследователь желает оставаться в сети незамеченным.

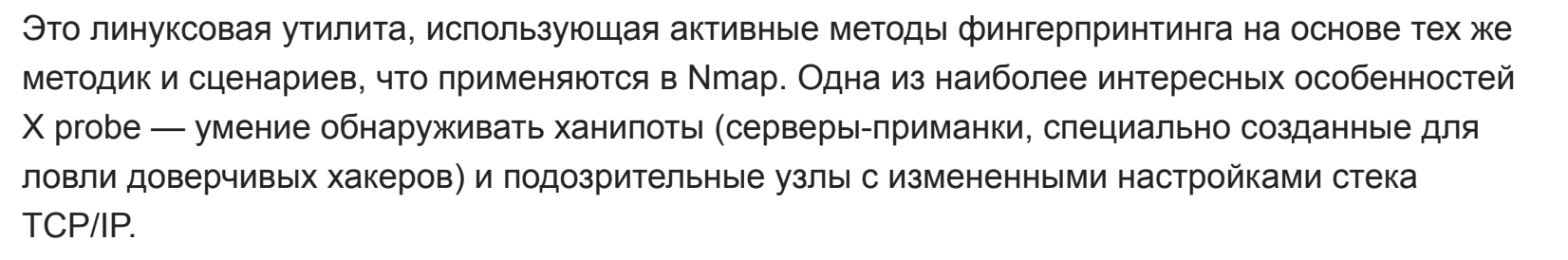
Версия p0f v3 была переписана разработчиками с нуля, поэтому «хвастает отпечатков» там не самая полная. Если верить официальному сайту, программе не хватает данных о старых версиях операционных систем вроде Windows 9x, IRIX и им подобных. Но пользователи могут помочь проекту, добавив в базу результаты собственных экспериментов с программой.

## NetScanTools

- Сайт: [netscantools.com](https://netscantools.com)
- Платформа: Windows

Бесплатная утилита NetScanTools Basic появилась еще в 2009 году и с тех пор претерпела лишь незначительные изменения. Умеет она немного: с ее помощью можно получить данные Whois (а без нее, наверное, никак), выполнить traceroute (для тех, кто не умеет пользоваться командой строкой), отправить DNS-запросы и полигнать удаленные хосты и так, и сяк, и впрямую, то есть управляя параметрами пинга. Негусто.

А вот коммерческая версия Pro может похвастаться более широкими возможностями. Она умеет работать с различными протоколами, включая ARP и SNMP, перехватывать и анализировать пакеты, получать DNS-записи для заданных IP-адресов, искать открытые TCP- и UDP-порты на удаленном хосте, определять поддерживаемые им версии SMB, искать устройства в сети, в том числе SMTP-серверы с открытыми релаями. В сети Active Directory NetScanTools может найти все расширенные пакеты, даже скрытые. В составе софтины есть генератор пакетов TCP, UDP, ICMP, CDP, RAW, в котором можно менять различные параметры, благодаря чему NetScanTools легко и непринужденно превращается во флудер.



NetScanTools — интересный инструмент с кучей функций. Жалко, платный

В целом можно сказать, что NetScanTools Pro довольно интересный проект, включающий инструментарий для активного и пассивного исследования сети. Только вот прайс в 249 долларов немного кусач, особенно если учесть, что вполне себе бесплатные NetworkMiner и Nmap обладают практически тем же набором базовых функций. Впрочем, с сайта разработчиков можно скачать 30-дневную тестовую версию, которая поможет тебе решить, стоит ли искать кржж бэквокс, или лучше воспользоваться фиврайным софтом.

## X probe

- Сайт: <https://sourceforge.net/projects/xprobe/>
- Платформа: GNU/Linux

Это линуксовая утилита, использующая активные методы фингерпринтинга на основе тех же методик и сценариев, что применяются в Nmap. Одна из наиболее интересных особенностей X probe — умение обнаруживать ханипоты (серверы-примани, специально созданные для ловли доверчивых хакеров) и подозрительные узлы с измененными настройками стека TCP/IP.

С использованием заложенных в софтину алгоритмов нечеткой логики X probe позволяет обнаруживать сервисы, скрытые брандмауэром. Помимо определения ОС на удаленном хосте с использованием ICMP-запросов, в возможности программы входит сканирование TCP- и UDP-портов. К сожалению, последняя версия утилиты датирована 2014 годом и, похоже, с тех пор проект практически не развивается.

## Ettercap

- Сайт: <https://www.ettercap-project.org/>
- Платформа: GNU/Linux

Ettercap — это широко известный в узких кругах sniffер, часто используемый для атак типа MITM. Работает он практически во всех линуксах, кроме OpenSuSe, а также на платформах UNIX/BSD, кроме Solaris. Говорят, особо могучие шаманы запускали Ettercap даже на macOS, но документального подтверждения этим слухам нет, ибо те, кому это удалось, погибли, попнув от гордости.

Как и другие sniffеры, этот умеет работать с протоколами Telnet, FTP, IMAP, SMB, LDAP и не только, но с Ettercap можно потрошить и зашифрованный трафик, передаваемый по HTTPS и SSH. Несмотря на то что тулза создавалась с прицелом под MITM, с ее помощью вполне можно идентифицировать удаленные операционные системы методом фингерпринтинга, наряду с такими рутинными процедурами, как определение IP, открытых портов, запущенных на исследуемом узле служб, типа адаптера и MAC-адреса сетевого интерфейса.

После установки и запуска Ettercap начинает sniffить трафик в сети и собирать результат в создаваемых программой профайлах, откуда его можно извлечь для анализа. Этот анализ позволяет установить, в частности, такие данные, как IP-адрес, имя и тип хоста, предположительная версия работающей там ОС, открытые порты и запущенные сервисы. Вполне достаточный стартовый набор для любого исследователя.

## THC-Archive

На гитхабе по адресу <https://github.com/vanhauser-thc/THC-Archive/> лежит богатый архив утилит и скриптов, которые могут стать отличным подспорьем для пентестера. Весь софт долго и кропотливо собирала команда энтузиастов-единомышленников под названием The Hacker's Choice, основанная аж в 1995 году и, судя по активности в Twitter, неплохо чувствующая себя по сей день.

Чуваки предлагают множество интересных проектов, но нас интересуют в основном тулзы из раздела <https://github.com/vanhauser-thc/THC-Archive/tree/master/Tools>. Тут, в частности, можно найти сканер Nmap, позволяющий отслеживать сервисы, работающие на нестандартных портах.

Некоторые наивные иссадмины искренне надеются, что смогут защитить себя от атаки, если поднимут, например, FTP-сервер, SSH или Telnet на каком-нибудь нестандартном порте вместо привычного. Вот с такими хитрежыми админами и призван бороться Amap.

Обычные сканеры стучатся на стандартные порты, анализируют полученные отклики и, если они не соответствуют ожиданиям, объявляются. Амап вместо этого опрашивает весь диапазон портов и сверяет отклики со своей базой данных в поисках соответствия. Таким образом, сервис, работающий на каком-либо порте, идентифицируется по его характерным признакам, содержащимся в ответе.

Чтобы облегчить себе жизнь, можно использовать Amap совместно с любым другим сканером. Сканер определяет список открытых портов на интересующем нас хосте, а Amap потом прощупывает этот диапазон и выясняет, какие именно службы издают эти порты и что полезного из этого может извлечь исследователь. На страничке The Hacker's Choice можно скачать Amap как под винду, так и под Linux, представлены все версии утилиты, начиная с самых ранних.

## Выводы

Статьи в «Хакере» принято завершать кратким заключительным разделом, поэтому не будем этак редактора нарушать добрую традицию. Как ты догадываешься, у большинства описанных здесь утилит возможности гораздо шире, чем просто определение типа ОС на удаленном хосте. Поэтому небезопасно будет попробовать ознакомиться с каждой из них. А