

ПЕНТЕСТ

СЕКРЕТЫ ЭТИЧНОГО ВЗЛОМА

Библиотека журнала

ЭТТЕР

ПЕНТЕСТ

СЕКРЕТЫ ЭТИЧНОГО ВЗЛОМА

Санкт-Петербург

«БХВ-Петербург»

2022

УДК 004.056
ББК 16.8
П25

П25 Пентест. Секреты этичного взлома. — СПб.: БХВ-Петербург, 2022. — 160 с.:
ил. — (Библиотека журнала «Хакер»)
ISBN 978-5-9775-6823-4

В сборнике избранных статей из журнала «Хакер» представлены материалы о тестировании на проникновение, используемых пентестерами дистрибутивах Linux и другом инструментарии. Дана информация об организации и принципах работы команд Red Team, раскрыты способы получения доступа к беспроводным сетям и данным на ПК с помощью протокола Network Time Protocol. Представлены сведения о способах постэксплуатации Windows, закрепления в системе, методах удаленного исполнения кода. Описаны приемы разведки на основе открытых источников информации (OSINT).

Для читателей, интересующихся информационной безопасностью

УДК 004.056
ББК 16.8

Группа подготовки издания:

Руководитель проекта	<i>Павел Шалин</i>
Зав. редакцией	<i>Людмила Гауль</i>
Компьютерная верстка	<i>Ольги Сергиенко</i>
Дизайн обложки	<i>Карины Соловьевой</i>

Подписано в печать 30.07.21.

Формат 70×100^{1/16}. Печать офсетная. Усл. печ. л. 12,9.

Тираж 1000 экз. Заказ №

"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20.

Отпечатано с готового оригинал-макета

ООО "Принт-М", 142300, М.О., г. Чехов, ул. Полиграфистов, д. 1

ISBN 978-5-9775-6823-4

© ИП Югай А.О., 2022
© Оформление. ООО "БХВ-Петербург", ООО "БХВ", 2022

Оглавление

Вместо предисловия.....	9
1. Боевой Linux. Обзор самых мощных дистрибутивов для пентестов и OSINT (Михаил Артюхин, Марк Бруцкий-Стемпковский)	11
NST	11
Kali	12
DEFT	14
Tsurugi.....	15
Parrot	17
BlackArch.....	18
BackBox	20
Выводы	22
2. Арсенал пентестера. Утилиты для детекта ОС на удаленном хосте (Валентин Холмогоров)	23
Пара умных слов.....	23
Nmap	24
NetworkMiner	26
p0f v3.....	27
NetScanTools	28
X probe.....	29
Ettercap.....	29
THC-Archive	30
Выводы	30
3. Арсенал пентестера. Выбираем инструмент для перехвата и анализа трафика (Валентин Холмогоров)	31
Немного теории	31
Wireshark	32
CommView	33
Interceptor-NG.....	35
SmartSniff.....	37
tcpdump	38
Burp Suite.....	38
Заключение.....	39

4. Воздушные ловкости. Простые трюки, которые выручают при пентесте Wi-Fi (Иван Пискунов)	41
Смена и автоматическая генерация нового MAC-адреса при новом подключении к Wi-Fi	41
Зачем менять MAC?	41
Практика	42
Включаем автоматическую генерацию случайных MAC-адресов	43
Устанавливаем определенный MAC	44
Другие способы программно поменять MAC	44
Изменение MAC с помощью iproute2	45
Изменение MAC с помощью macchanger	45
Обнаружение скрытого SSID	46
Получаем скрытый SSID при помощи Airodump-ng	46
Обход MAC-фильтрации путем заимствования адреса из белого списка	47
Глушение сети Wi-Fi	47
Еще эффективный скрипт для глушения Wi-Fi	48
5. Туннель во времени. Выводим данные с компьютера через Network Time Protocol (Марк Бруцкий-Стемковский)	51
Что такое NTP	51
Структура пакета NTP	52
Ограничения на трафик по порту UDP-123	54
Концепт	55
Реализация	56
Сервер	56
Клиент	59
Тестирование с Wireshark	62
О производительности и скрытности	63
Применение	64
Выводы	64
6. Пингвин-супершпион. Используем виртуалку с Linux для постэксплуатации Windows (Андрей Жуков)	65
Реализация	66
Делаем гостевую систему	66
Тихая установка и запуск VirtualBox	70
Деплой на удаленном хосте	72
Уходим красиво	73
Пример из жизни	73
7. Кунг-фу pivoting. Выжимаем максимум из постэксплуатации (Андрей Жуков)	75
Передача файлов (инфильтрация и эксфильтрация)	76
Эксфильтрация через TCP	76
Эксфильтрация через SMB	77
Эксфильтрация через HTTP	77
Эксфильтрация с использованием FTP	77
Эксфильтрация с помощью TFTP	78
Эксфильтрация через ICMP	78

Экспфильтрация через DNS	78
Экспфильтрация plaintext	79
Проброс портов	80
Local port forwarding	81
Remote port forwarding	81
Обход сразу двух файрволов	83
dns2tcp	85
Проксирование	85
Зпроху	85
SSH	86
Используем прокси	87
VPN-туннели	88
VPN-туннель через TCP в одну команду (L3-туннель)	89
VPN туннель через SSH (L2/L3-туннели)	89
VPN-туннели на Windows	90
VPN-туннель через ICMP	90
VPN-туннель через DNS	90
Организация GUI	91
Быстрая GUI-сессия	91
Параллельный доступ по RDP	93
Выводы	93

8. Гид по Lateral. Изучаем удаленное исполнение кода в Windows

<i>(Андрей Жуков)</i>	95
Стратегия бокового перемещения	96
Удаленное выполнение кода в Windows	97
MSRPC	97
psexec.exe	97
psexec.py	98
winexe	98
smbexec.py	99
services.py	99
atexec.py/at.exe	100
reg.exe	100
DCERPC	100
wmiexec.py	101
dcomexec.py	101
wmis	101
wmic.exe	102
sc.exe	102
WinRM	102
Evil-WinRM	102
RDP	103
GP	103
Локальные учетные записи	105
Pass-the-Hash	106
Bruteforce	107
Билеты Kerberos	108
Kerberoasting	108

Извлечение Kerberos-билетов через дампы виртуальной памяти	109
Извлечение Kerberos-билетов через дампы физической памяти.....	109
Извлечение Kerberos-билетов из сетевого трафика	110
Bruteforce TGS.....	110
Pass-the-Ticket	110
Доменные учетные записи	111
Кеш хешированных доменных учетных записей	111
Учетные данные запущенных сессий.....	112
Lateral movement	115
Credentials spraying.....	115
Массовое исполнение кода	116
Заключение.....	117

9. Шпаргалка по persistence. Как надежно прописаться на хосте

или выявить факт компрометации (Андрей Жуков)	119
Шелл	121
Автозагрузка	121
# Сервисы	122
Задачи	123
In-memory	123
Конфиги.....	125
Особые приемы в Linux.....	126
LD_PRELOAD.....	126
rc.local	126
Особые приемы в Windows.....	126
Дебаггер.....	126
Gflags.....	127
WMI	127
AppInit.....	128
Lsass	128
Winlogon	129
Netsh.....	129
Office	130
Выводы	130

10. Целенаправленные атаки: разведка на основе открытых источников

(OSINT) (Денис Макрушин)	131
Поиск незакрытых дверей.....	131
Просканировать, отметить, повторить.....	132
OSINT без интерактива	135
Сбор информации для социальной инженерии.....	138
Reson как искусство	139

11. Проект Red Team: организация, управление, скоуп

(Денис Макрушин)	141
Красная, синяя и пурпурная команды.....	141
Виды наступательной безопасности	143
Red Team: задачи	145

Red Team: ключевые показатели эффективности	146
Управление командой и доставка результатов	147
Выводы	147

12. Проект Red Team: роли и области экспертизы (Денис Макрушин) 149

Области экспертизы	149
Роли Red Team	151
Разработчик	152
Исследователь уязвимостей (багхантер).....	152
Администратор (DevOps-инженер)	152
Penetration Testing	152
Reporting	153
Training	153
Оттенки красного.....	153

«Хакер»: безопасность, разработка, DevOps..... 154

Предметный указатель 157

Вместо предисловия

Тестирование на проникновение — пожалуй, единственный легальный и абсолютно законный способ заниматься хакерским ремеслом, не опасаясь угодить за решетку. Действительно, спрос на услуги специалистов по информационной безопасности, способных проверить надежность и защищенность IT-инфраструктуры предприятия, в последние годы растет. А с переходом многих компаний на удаленный режим работы в период коронавирусной эпидемии это направление стало еще более актуальным.

Penetration testing, или пентест, — явление неоднородное. Под этим термином понимается комплекс средств и методов оценки безопасности информационных систем или сетей путем моделирования атаки злоумышленников. В первом приближении пентестеров часто делят на две «команды» согласно их функциям: «красная» команда, Red Team, это группа атакующих — такие специалисты воспроизводят действия хакеров, пытающихся взломать целевую сеть, службу или сервер. «Синяя» команда, Blue Team, наоборот, защищается от атак, воспроизводя действия системных администраторов, сотрудников техподдержки или службы безопасности и определяя таким образом уязвимые места в «периметре обороны». Разумеется, все эти действия выполняются с ведома и согласия «атакуемой» стороны. Часто для пентестеров заранее определяются цели исследования — что в инфраструктуре предприятия можно трогать, а что, наоборот, нельзя, и критерии работы — используемый инструментарий, методы и средства для проведения испытаний. Реже жесткие условия не задаются, и атакующей стороне фактически предоставляют полную свободу действий в выборе целей атаки, а также средств и методов в достижении поставленных целей.

На практике среди пентестеров тоже принято своеобразное «разделение полномочий». Кто-то специализируется на сборе информации из открытых источников, кто-то — на методах социальной инженерии, есть эксперты в сфере поиска уязвимостей в веб-приложениях и во взломе сетей, работающих под управлением Active Directory. Кто-то лучше разбирается в Samba, Exchange, в системах SCADA. Помимо людей, знакомых с инструментарием вроде Metasploit и Mimikatz, в команде пентестеров обязательно нужны специалисты с навыками программирования, способные набросать скрипт для автоматизации каких-либо рутинных процессов. А в процессе подготовки отчетов нужен некто, обладающий скиллами технического писателя. Иногда все эти навыки удачно сочетает в себе один человек, но такие «универсалы» — буквально нарасхват.

Вот почему уложить абсолютно все аспекты, связанные с тестированием на проникновение, в объем одного небольшого издания практически невозможно. В данной книге мы собрали лучшие статьи из журнала «Хакер», посвященные пентестингу. Авторы этих статей — специалисты в сфере информационной безопасности, практикующие пентестеры, профессиональные эксперты по защите данных. Написанные ими материалы, которые мы включили в эту книгу, — результат их многолетнего труда и отражение накопленного опыта.

Помимо текста, фрагментов кода и иллюстраций некоторые разделы книги содержат специальные врезки. В них есть дополнительная информация, перекликающаяся с темой текущего раздела, а также ссылки на интернет-ресурсы, где читатель сможет отыскать полезные информационные материалы.

Эта книга необычна и по своей стилистике. В журнале «Хакер» принят своеобразный неформальный стиль, а к читателям обращаются на «ты». Кроме того, на страницах журнала очень часто встречается компьютерный сленг, а манеру изложения в статьях можно назвать ироничной и шутливой. Все эти добрые традиции в полной мере распространилась и на книгу. Потому не удивляйся, встретив на страницах издания слово «тулза» вместо «утилита» или «пофиксить» вместо «исправить выявленную ошибку в коде». У нас так заведено.

Поскольку тема этой книги весьма специфичная, мы не можем не опубликовать в предисловии несколько важных предупреждений. Вот они:

ВНИМАНИЕ!

Вся приведенная на страницах этой книги информация, код и примеры публикуются исключительно в ознакомительных целях. Ни издательство «БХВ», ни редакция журнала «Хакер», ни авторы не несут никакой ответственности за любые последствия использования информации, полученной в результате прочтения книги, а также за любой возможный вред, причиненный информацией из этого издания.

Помните, что несанкционированный доступ к компьютерным системам и распространение вредоносного ПО преследуются по закону. Все рассмотренные в книге методы представлены в ознакомительных целях. Каким-либо образом используя представленную в книге информацию, вы действуете исключительно на собственный страх и риск.

Искренне надеюсь, что этот сборник поможет читателям ознакомиться с тематикой тестирования на проникновение, изучить приемы пентестеров, понять принципы их работы. Возможно, для кого-то книга станет первым шагом в новую, увлекательную и крайне интересную профессию.

*Валентин Холмогоров,
редактор рубрики «Взлом» журнала «Хакер»*

<http://xakep.ru>
<http://holmogorov.ru>

1. Боевой Linux.

Обзор самых мощных дистрибутивов для пентестов и OSINT

Михаил Артюхин, Марк Бруцкий-Стемпковский

Дистрибутивов для пентеста существует множество. Одни популярны, другие — не очень, но все они преследуют цель дать хакеру удобный и надежный инструмент на все случаи жизни. Большинство из программ в составе таких кастомизированных сборок средний хакер никогда не воспользуется, но для статусности их добавляют («Смотри, у тебя 150 утилит, а у меня — 12 000!»). Сегодня мы постараемся сделать обзор большинства интересных дистрибутивов, как популярных, так и незаслуженно забытых.

NST

- ❑ Первый релиз: 2003 год
- ❑ Основан на: Fedora
- ❑ Платформы: x64
- ❑ Графическая оболочка: MATE

Ссылка: <https://www.networksecuritytoolkit.org/nst/index.html>

Начнем с малоизвестного, но оттого не менее интересного дистрибутива. NST (Network Security Toolkit) основан на Fedora и предназначен для сетевых атак. В основе интерфейса — MATE, который вызывает ощущение начала нулевых (рис. 1.1). В комплекте идет несколько десятков самых важных инструментов, в основном сетевые сканеры, клиенты для всевозможных служб и разного рода перехватчики трафика. Но не хватает таких полезностей, как, например, masscan, и даже банального aircrack, хотя airtsnort имеется.

Больше всего вкусоностей можно найти в папке **Applications** → **Internet**. Тут у нас и Angry IP Scanner, написанный, кстати, на Java, и Ettercap, и даже OWASP ZAP. Есть неплохой сборник модулей для всевозможного спуфинга и скана у пакета netwag. В деле он показал себя неплохо, жаль только — не очень удобен и жутко устарел.

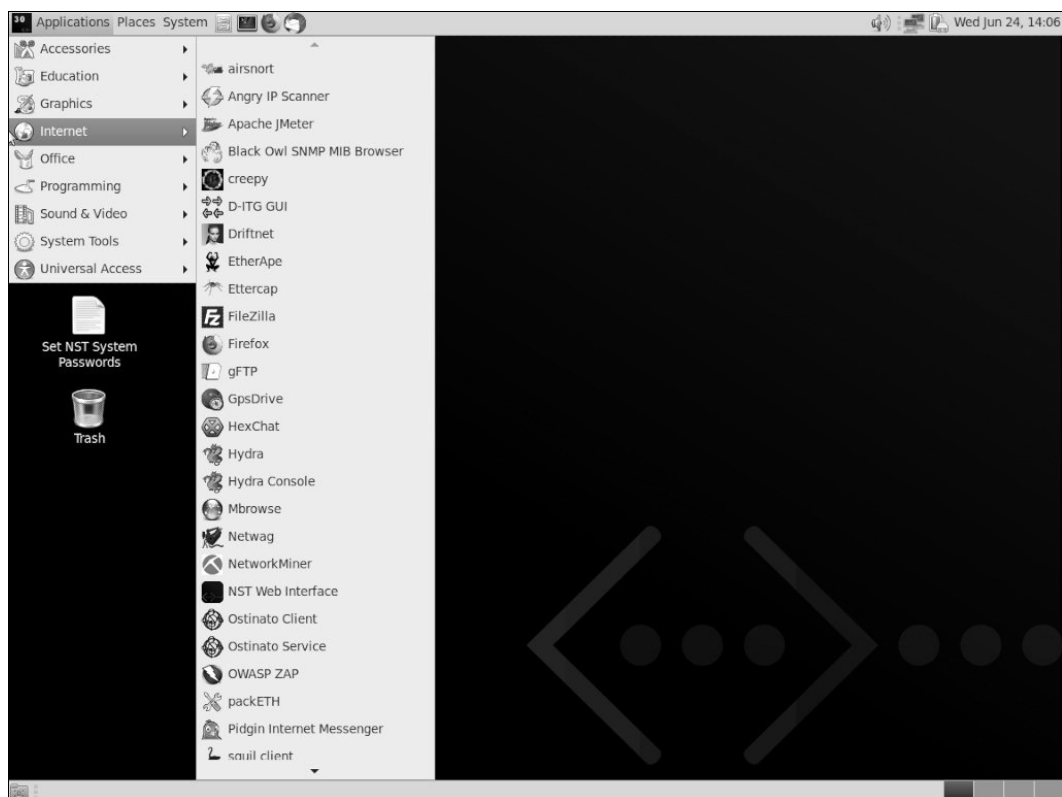


Рис. 1.1. NST (Network Security Toolkit)

Весь проверенный нами софт работает прекрасно. В общем, всем скучающим по древнему интерфейсу и привычным инструментам рекомендуем этот дистрибутив.

Kali

- Первый релиз: 2013 год
- Основан на: Debian
- Платформы: x86, x64, ARM, VirtualBox
- Графическая оболочка: Xfce

Ссылка: <https://kali.org/>

Как ты, конечно, знаешь, Kali — один из самых распиаренных дистрибутивов для хакеров, и было бы странно, если бы мы про него не написали. О нем знают даже школьники, а с относительно недавних пор он доступен в виде приложения прямо из Microsoft Store (рис. 1.2)! Конечно, доступность — несомненный плюс, но система слегка перегружена набором инструментов (хотя и не так сильно, как BlackArch), к тому же часть из них из коробки работает криво или не работает вообще.

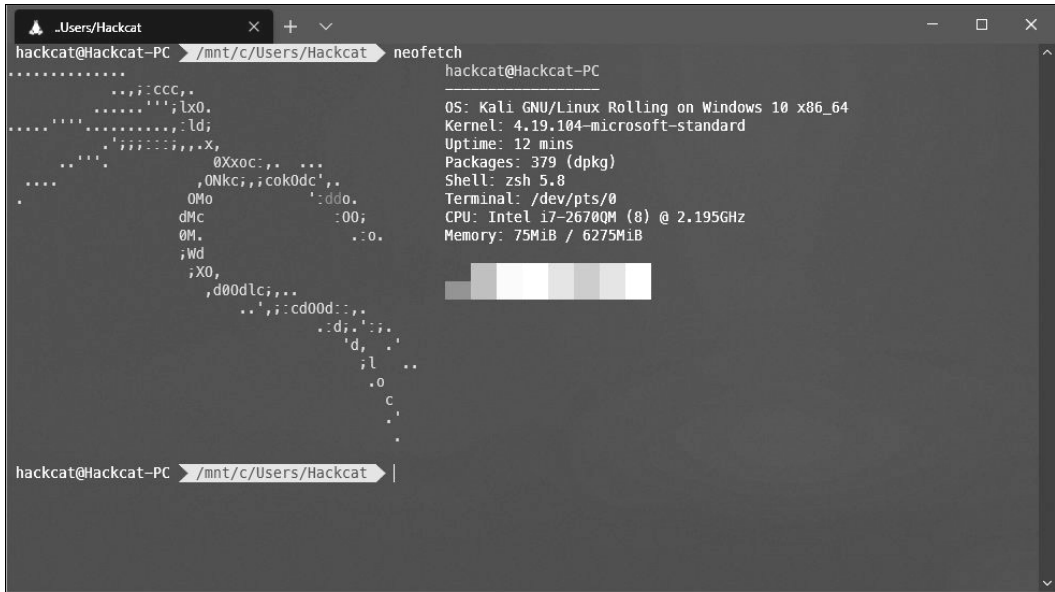


Рис. 1.2. Kali работает в Windows Subsystem for Linux

Защиты от дурака в Kali тоже не предусмотрено. Как показывает практика, не всем пользователям понятно, что не стоит делать эту систему основной. От ядра до оболочки она была создана и оптимизирована для выполнения боевых задач на фронтах ИБ и плохо пригодна для спокойной ежедневной работы. Многие нужные в быту механизмы там попросту отсутствуют, а попытка их установить, скорее всего, вызовет сбой в нормальной работе ОС, если не выведет ее из строя полностью.

Короче, Kali как спички — мощная штука в умелых руках, ее легко достать, но детям лучше не давать. Охватить разом все возможные официальные и неофициальные утилиты (а их, на минуточку, больше 600) этой системы не представляется возможным хотя бы потому, что постоянно появляются новые и новые модули, фреймворки, утилиты и прочие прибабасы.

Kali предназначена для широкого спектра задач, но основная из них — атаки в сетевой среде, например, поиск уязвимостей в веб-приложениях и получение доступа к беспроводным сетям. Как наследник BackTrack, Kali вообще неплохо приспособлена для работы с беспроводными каналами связи, в особенности Wi-Fi. Проверка на прочность удаленных хостов тоже возможна с помощью, например, Metasploit, но именно на работу с Wi-Fi ориентировано ядро и значительная часть инструментов.

Еще из плюсов отмечу наличие в штатной поставке большого количества словарей для различных атак, не только на Wi-Fi, но и на аккаунты в Интернете и на сетевые службы.

Для еще большего удобства использования на официальном сайте предлагается версия дистрибутива для виртуальных машин, ведь при взломе куда разумнее использовать систему без установки — мало ли кто потом будет копаться в твоём

компе! Вердикт такой: если умеешь пользоваться — классная штука, но не вздумай показывать ее ребенку. Один из авторов видел, что будет, если нарушить эту рекомендацию.

DEFT

- Первый релиз: 2005 год
- Основан на: Ubuntu
- Платформы: x86
- Графическая оболочка: LXDE

Ссылка: <https://archive.org/details/deft-8.2>

Родина DEFT — солнечная Италия, и он щедро, как пицца сыром, посыпан разнообразными инструментами для разведки и взлома. При этом они не примотаны к дистрибутиву синей изолентой, а вполне гармонично встроены в него. Все вместе напоминает интересный и полезный в жизни швейцарский нож.

Разработан DEFT на платформе Lubuntu (<https://ru.bmstu.wiki/Lubuntu>) и снабжен удобным графическим интерфейсом. В продукт входит набор профильных утилит, начиная с антивирусов, систем поиска информации в кеше браузера, сетевых сканеров и других полезностей и заканчивая инструментами, которые необходимы при поиске скрытой информации на диске.

Используя эту ОС, не составит труда получить доступ к стертым, зашифрованным или поврежденным данным на различных видах физических носителей. Основной инструментарий прячется в разделе DEFT, который, в свою очередь, находится в некотором подобии меню «Пуск» (рис. 1.3).

Изначально этот дистрибутив был предназначен для нужд сетевой полиции и специалистов по реагированию на инциденты в области ИБ, поэтому еще одна сильная сторона DEFT — это конкурентная разведка, в том числе анализ взаимосвязей аккаунтов соцсетей. Есть даже интересная утилита для обнаружения геолокации заданного аккаунта LinkedIn или Twitter. Я не смог проверить, насколько эффективно это работает в данный момент, но с определением принадлежности аккаунта к стране и городу она справляется.

В отличие от Kali Linux или Tsurugi, в DEFT защита от дурака встроена. Без должной подготовки почти ни один инструмент попросту не запустить, а без глубокого понимания работы защитных механизмов тут вообще делать нечего. Буквально каждое приложение или опция требует прав root, так что не спеши сразу запускать все подряд или создавать непривилегированного пользователя.

Также мы обнаружили «подарочек»: несколько репозиториев, откуда DEFT берет обновления, закрыты ключами. Пару дней мы рылись по форумам, пока не нашли, откуда запросить данные, да и сами ключи тоже отыскались.

В итоге эта система хороша для форензики и расследования инцидентов, в особенности если есть физический доступ к носителям информации — будь то диск,

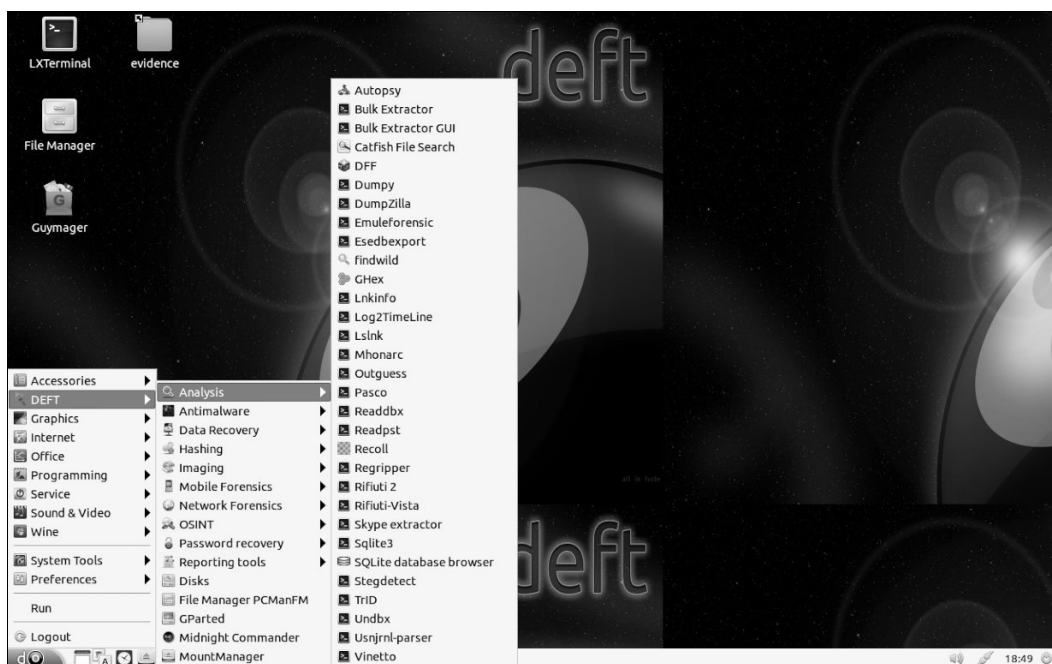


Рис. 1.3. DEFT

флешка или смартфон (хакера, начальника, сотрудника, конкурента, жены, любовницы, ее бати — нужное подчеркнуть).

Tsurugi

- Первый релиз: 2018 год
- Основан на: Ubuntu
- Платформы: x86 (частично), x64
- Графическая оболочка: MATE

Ссылка: <https://tsurugi-linux.org/downloads.php>

Этот дистрибутив вообще не очень известен в кругах ИБ-специалистов — возможно, из-за своей молодости. Однако Tsurugi — детище, рожденное совместными усилиями создателей DEFT и Kali. Что из этого вышло? Давай посмотрим!

Tsurugi (это слово означает двуручный японский меч) создан на основе Ubuntu, в качестве GUI используется MATE. Предназначен он больше для форензики или OSINT, нежели для пентеста, однако его инструментарий, как и некоторые особенности, позволяют использовать его и в этом направлении. Изначально система поставляется в режиме live-образа, но при желании можно произвести постоянную установку.

После входа в систему мы видим несложный GUI, предусмотрительно обвешанный со всех сторон виджетами показателей загрузки процессора, жестких дисков, опе-

ративной памяти, скорости сети и прочего. Да, рука создателей Kali тут довольно сильно заметна. В глаза сразу бросается обилие предустановленных инструментов, которые нужны далеко не всегда. При этом интерфейс системы выглядит более чем минималистично и компактно. А вот логика работы системы безопасности, как и работы с вебом или защиты от отслеживания, основана на лучших практиках DEFT.

Весь основной арсенал расположен в **Applications** → **TSURUGI** (рис. 1.4).

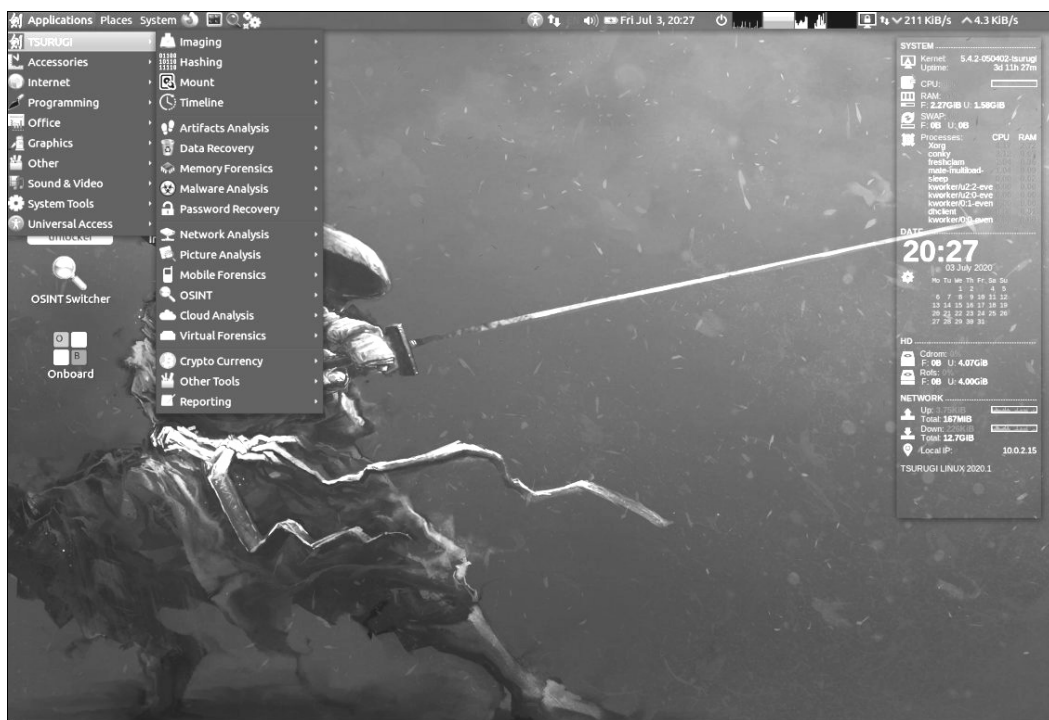


Рис. 1.4. Tsurugi

Здесь и работа с образами, и анализ вредоносных, и восстановление данных, и, как упоминалось, набор утилит для OSINT. Стоит иметь в виду, что эта ОС, как и Kali, не имеет защиты от кривых рук. Она подойдет тем, кто имеет хорошие навыки работы с Linux и действует предусмотрительно и вдумчиво. Как и положено острому японскому мечу!

Обширный инструментарий позволяет использовать систему как мультитул для широкого спектра задач. Пусть Tsurugi и немного смахивает на Kali, серьезные различия все равно имеются. Притом что некоторые из утилит так же, как и в Kali, работают некорректно или не работают вообще, процент проблемных тулз здесь намного меньше, и видно, что об этом кто-то заботится.

Если по каким-то причинам ты не хочешь использовать Kali, то Tsurugi станет достойным инструментом в твоём наборе. Пять звезд не поставим как минимум пото-

му, что один из авторов этого обзора отложил кирпич от звука меча при старте ОС... Впрочем, давай не будем о грустном.

Parrot

- Первый релиз: 2013
- Основан на: Debian
- Платформы: x86, x64, ARM
- Графическая оболочка: MATE

Ссылка: <https://parrotsec.org/download/>

Этот красивый дистрибутив Linux основан на Debian и разработан командой Frozenbox специально для тестов безопасности компьютерных систем, поиска и оценки различного ряда уязвимостей. Что же внутри? В качестве окружения рабочего стола здесь все тот же MATE (рис. 1.5).

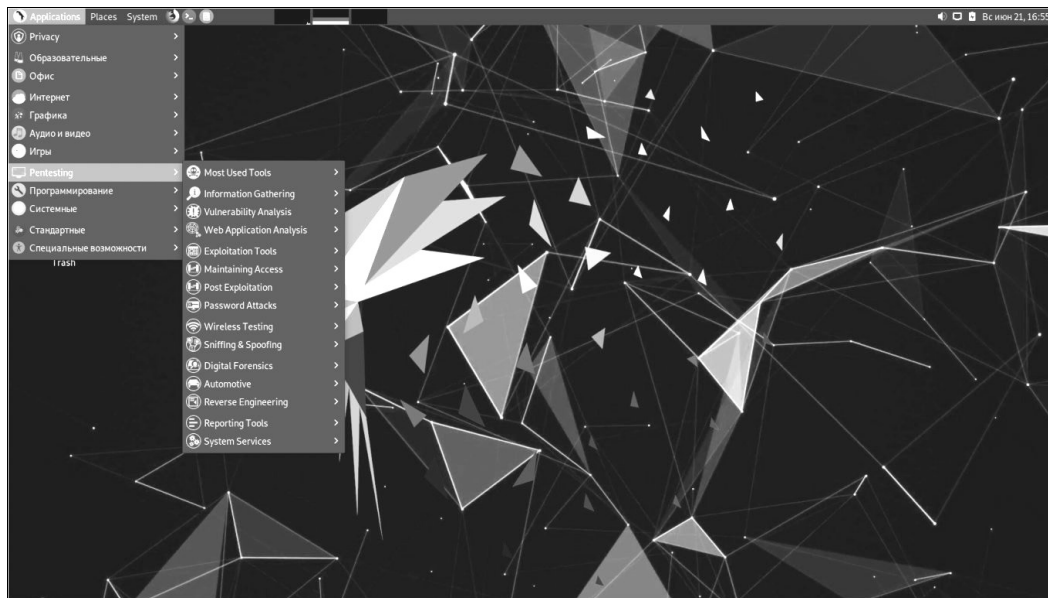


Рис. 1.5. Parrot

Сверху, в разделе **Application**, ты найдешь утилиту Anon Surf. Одна из особенностей Parrot — в ней предустановлены некоторые средства анонимизации, и при выборе Anonsurf Start весь трафик системы будет перенаправлен через Tor. В этом же разделе есть возможность использовать DNS проекта OpenNIC — это внеадресная альтернатива реестрам доменов верхнего уровня. Здесь же, выбрав параметр **Check IP**, можно проверить текущий внешний IP.

Второй раздел — **Cryptography**. Здесь стоит обратить внимание на утилиту GPA — это графический интерфейс программы GnuPG, предназначенной для шиф-

рования информации и создания электронных цифровых подписей. Это, по сути, альтернатива шифрованию PGP. А если тебе нужен GPG, то под рукой будет утилита **zuluCrypt** — аналог **VeraCrypt**, который позволяет шифровать папки, разделы, флешки и прочее.

Следующий (и самый интересный) раздел — **Parrot**. В нем собраны именно те утилиты для тестирования защищенности компьютерных систем, из-за которых эта ОС попала в наш обзор. Многие из представленных утилит нам уже известны по **Kali Linux**, но есть и уникальные.

Подробнее хотелось бы остановиться на вкладке «Интернет». Здесь мы видим предустановленный **Tor Browser** и биткойн-кошелек **Electrum**, а также утилиту **XSSer** — фреймворк для обнаружения и эксплуатации XSS-уязвимостей в веб-приложениях. Тут же есть почтовый клиент **Claws Mail**, это полноценный почтовый клиент с поддержкой шифрования GPG. Бонусом идет **Ricochet IM** — децентрализованный анонимный мессенджер, работающий через сеть **Tor**.

Это, пожалуй, все особенности **Parrot Security OS**, о которых хотелось бы рассказать. Как видно, **Parrot OS** подходит не только для тестов на проникновение, она может и служить ОС для ежедневного использования тем, кто знает, зачем им это нужно. Нам **Parrot** показалась качественно и удобно сделанной ОС. Приятно работать с системой, где не нужно предварительно чинить инструменты.

BlackArch

- Первый релиз: неизвестно
- Основан на: Arch
- Платформы: x64
- Графическая оболочка: отсутствует, есть несколько менеджеров рабочего стола

Ссылка: <https://blackarch.org/downloads.html>

BlackArch — самый крупный по объему образа дистрибутив. Актуальная версия занимает больше 14 Гбайт! Загружать, кстати, при желании можно через торрент, и сидов всегда много. Оцени дружелюбие интерфейса: если тебе удалось выкачать этого монстра и запустить его, нужно ввести логин и пароль, о которых ты должен прочесть на сайте в инструкции по установке (это **root/blackarch**, если что). Про **live**-пользователей, видимо, забыли.

Дальше: после логина не видно никаких намеков на меню или что-то в этом роде. Перед нами практически голый **Fluxbox**, поэтому оно вызывается по клику правой кнопкой мыши в любом месте рабочего стола (рис. 1.6).

Все приложения удобно разложены по категориям в подменю **blackarch** основного меню. Представлены 49 категорий, в которых есть инструменты на любой случай жизни. Навигация по меню с помощью мыши, как в **Windows**? О нет, в этом дистрибутиве про мышь смело можно забыть. Только клавиатура, только хардкор! С другой стороны, раз ты решил связаться с ***nix**-системами и взломом, глупо рассчитывать на что-то другое.

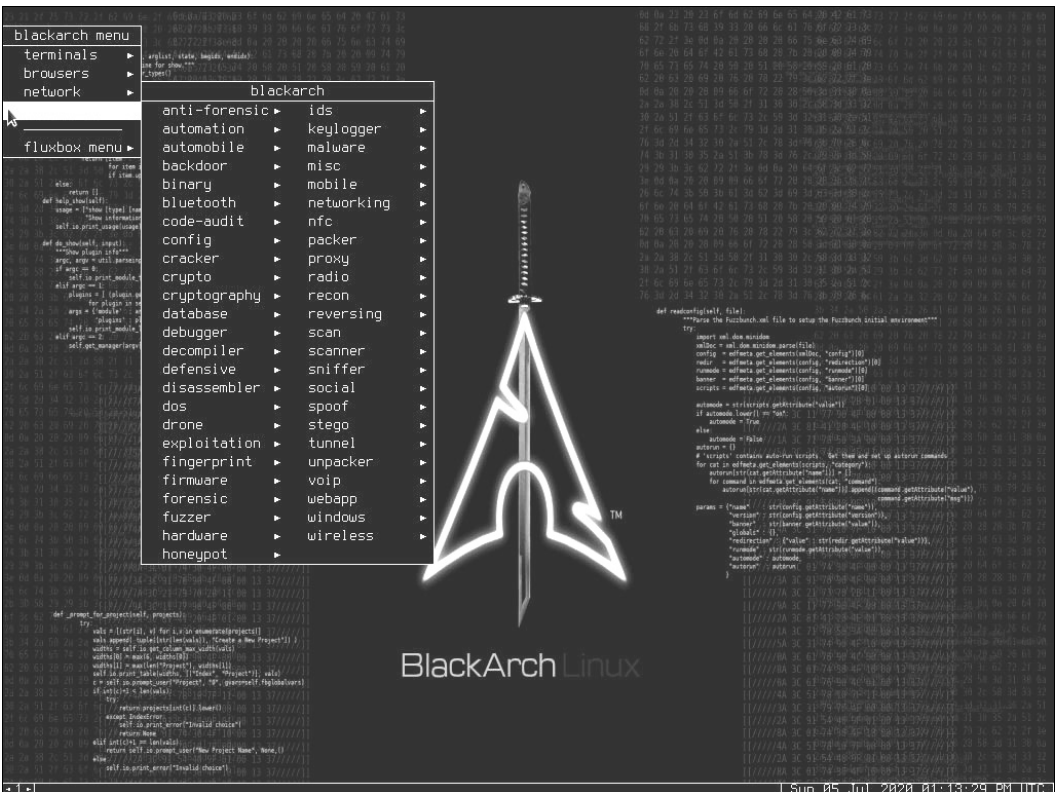


Рис. 1.6. Группы приложений BlackArch

Что касается собственно инструментов, то тут представлены все популярные и не очень тулзы для взлома, включая, конечно, такие знаковые, как Metasploit и BeEF XSS. Делать обзор всех инструментов этого поистине огромного набора — занятие еще более безнадежное, чем в случае с Kali и Parrot. Так что я пройдусь по верхам, а ты, если будет интересно, сможешь углубиться в чтение документации настолько, насколько посчитаешь нужным.

BlackArch не стесняется использовать Wine для запуска некоторых «неродных» приложений. В качестве примера — mft2csv (на рис. 1.7), который парсит MFT файловой системы NTFS для дальнейшего анализа. В наличии имеется и Java (OpenJDK 14.0.1).

Терминал, как и в целом графическая оболочка системы, выглядит уныло, зато версии софта актуальные. С одной стороны, кажется, что хотели сделать как в кино про хакеров, с другой — система все же вполне юзабельна, хотя и требует серьезных навыков.

В общем, если ты не готов пробираться через минное поле конфигов, аргументов при запуске софта, гугленья на каждый чих и прочие престели этого мультитула — смотри в сторону Kali и Parrot, там хоть что-то можно сделать без настольного справочника. К новичкам BlackArch более чем недружелюбна. И ясен пень, не вздумай ставить ее как основную ОС.

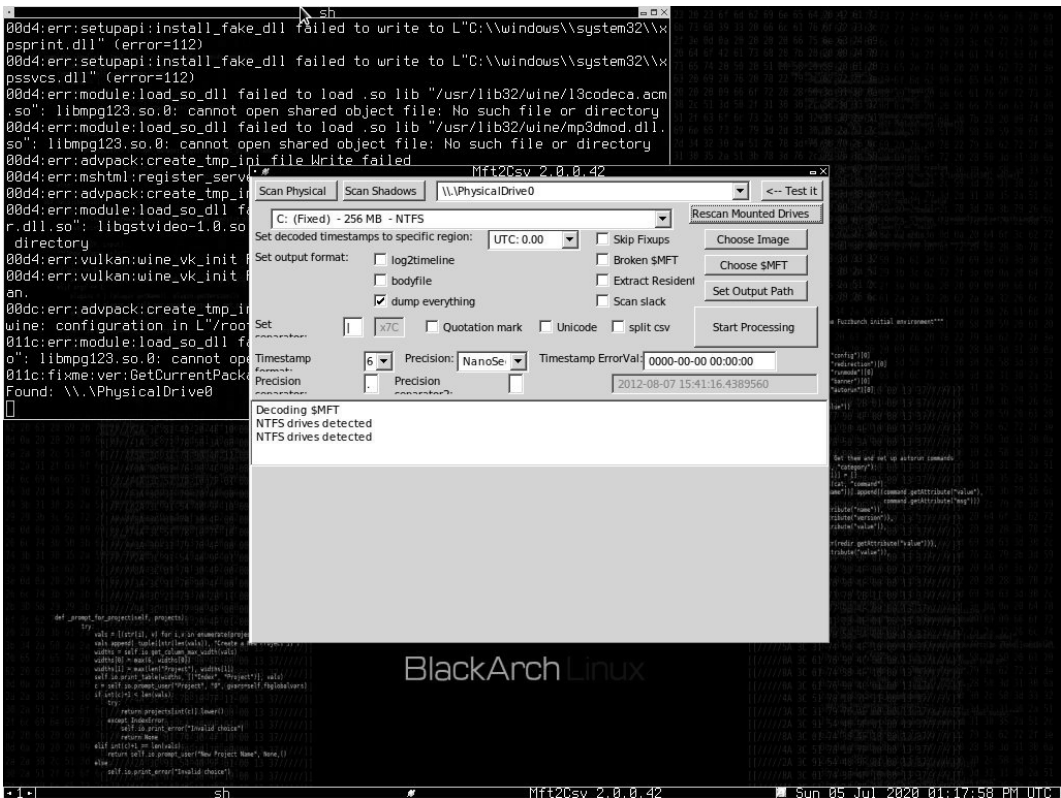


Рис. 1.7. Запуск приложения в Wine

BackBox

- Первый релиз: 2010
- Основан на: Ubuntu
- Платформы: x64
- Графическая оболочка: Xfce

Ссылка: <https://www.backbox.org/download/>

И под конец — еще один дистрибутив, стоящий особняком от остальных. BackBox не претендует на звание лучшего хакерского мультитула, зато он как нельзя лучше подходит для повседневного использования. Графическая оболочка тут Xfce, что минимизирует потребление системных ресурсов. С сайта доступны для скачивания два варианта — ISO и Torrent. Образа для виртуальных машин нет.

BackBox основан на Ubuntu (точнее, Xubuntu), что делает удобным его использование как домашней ОС, к тому же по Ubuntu доступна куча документации и форумов с ответами на распространенные вопросы. Тут нет каких-то твиков ядра, так что никакие махинации ничего не испортят. Такие особенности делают этот дистр прекрасным выбором для начинающего пентестера (рис. 1.8).



Рис. 1.8. Меню BackBox Linux 7

Инструментов из коробки поставляется не так и много, всего около 200 штук, но для первых шагов в ИБ вполне достаточно. В остальном BackBox — это просто Xubuntu со всеми ее фишками и функциями. Важный плюс, на который я не могу не обратить внимание, — все инструменты очень удобно сгруппированы в меню. Даже если ты не знаешь ни одного инструмента, например, для атак на Wi-Fi, ты с легкостью найдешь их.

Сказать больше особо нечего, все достоинства и недостатки описанных в этом разделе дистрибутивов мы свели в табл. 1.1 для сравнения. Пользуйся на здоровье.

Таблица 1.1

Дистрибутив	Графическая оболочка	Основан на	Год выпуска	Платформы
NST	MATE	Fedora	2003	x64
Kali	Xfce	Debian	2013	x86, x64, ARM, VirtualBox
DEFT	LXDE	Ubuntu	2005	x86
Tsurugi	MATE	Ubuntu	2018	x86 (частично), x64
Parrot	MATE	Debian	2013	x86, x64, ARM

Таблица 1.1 (окончание)

Дистрибутив	Графическая оболочка	Основан на	Год выпуска	Платформы
BlackArch	—	Arch	?	x64
BlackBox	Xfce	Ubuntu	2010	x64

Выводы

Тут должна была быть лекция о том, что недопустимо использовать большинство из этих дистрибутивов как основную ОС, но ее не будет. Пробуй разные варианты, выбирай тот, что ближе твоему сердцу, и желаем тебе удачи.

2. Арсенал пентестера. Утилиты для детекта ОС на удаленном хосте

Валентин Холмогоров

Первая стадия пентеста — это, как известно, разведка. Только установив, какая система работает на удаленном хосте, можно начинать искать в ней лазейки. В этом разделе ты узнаешь про семь средств, которые помогают 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 мартышка добывает себе пропитание с помощью собственного инструментария, что выгодно отличает ее от прочих представителей фауны. А одним из самых богатых арсеналов сподручных инструментов среди приматов обладают, 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 от-

крыты 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 sniff-финг с помощью тулз вроде Wireshark и последующий анализ трафика. Во втором случае используется принцип паттернов: каждая ОС имеет характерный набор открытых портов, на которые можно постучаться 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

□ 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 (рис. 2.1) обладает интуитивно понятным графическим интерфейсом, но для олдфагов предусмотрен режим работы из командной строки. В этом случае можно использовать команду `nmap -O -PN [URL]`, где URL — адрес исследуемого сайта. Совсем упертые могут скомпилировать тулзу из исходников, любезно опубликованных на сайте разработчиков (<http://nmap.org/>).

Диагноз об установленной на хосте операционной системе утилита выдает весьма приблизительный, но вероятность того или иного варианта может достигать 90% и

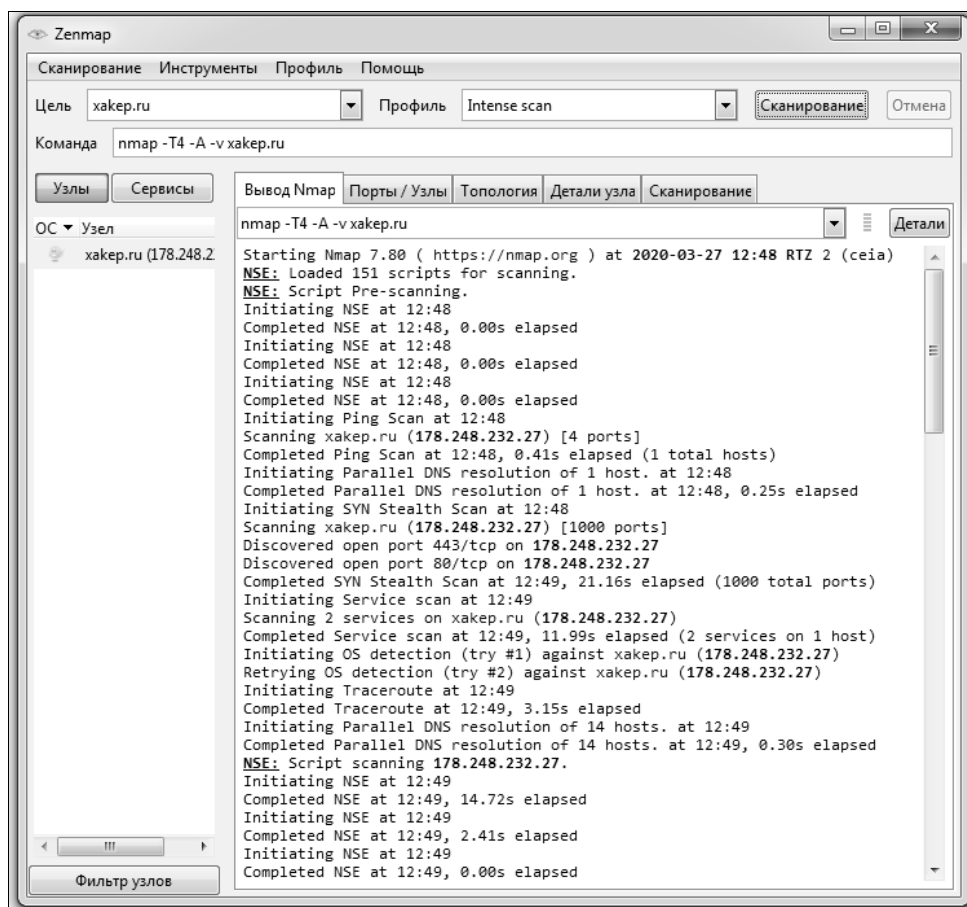


Рис. 2.1. Отчет о сканировании сайта утилитой Nmap

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 статьей об их расширении (<https://xakep.ru/2016/02/25/pimp-my-nmap/>). Утилита и впрямь очень мощная: она позволяет даже обходить файрволы, выполнять DoS и другие виды атак (<https://xakep.ru/2017/03/31/nmap-for-hackers/>). Одним словом, полезный инструмент, если знаешь, как с ним обращаться.

NetworkMiner

□ Сайт: <https://www.netresec.com/index.ashx?page=Networkminer>

□ Платформа: GNU/Linux, Windows

NetworkMiner (рис. 2.2) — 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.

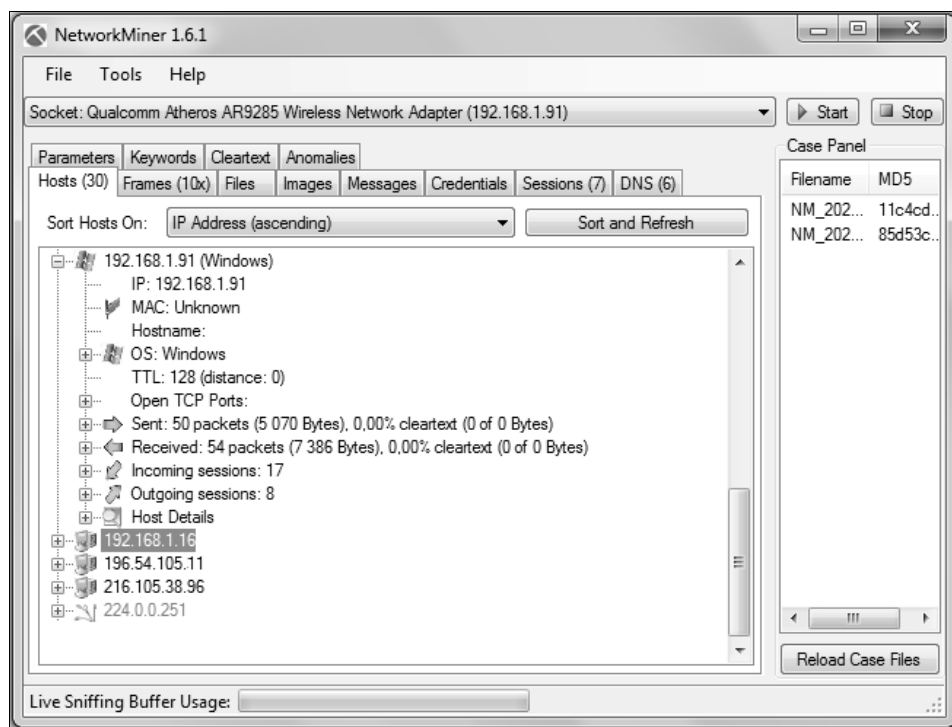


Рис. 2.2. Интерфейс NetworkMiner достаточно прост и понятен

Утилиту можно скачать с сайта <http://sourceforge.net/projects/networkminer>, а на страничке разработчиков (<https://www.netresec.com/>) 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 незнакома.

Есть у этой тулзы еще одна шикарная функция: она умеет вытаскивать файлы из трафика, транслируемого по протоколам FTP, TFTP, HTTP, HTTP/2, SMB, SMB2, SMTP, POP3 и IMAP. То есть с ее помощью можно перехватывать файлы, передаваемые по электронной почте, 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 сниффер, способный творить волшебство в умелых руках. Ну а фотопечать 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 сниффер, а программа, объединяющая целый комплекс механизмов для анализа перехваченных пакетов и фотопечати. 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 сниффить 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 «база отпечатков» там не самая полная. Если верить официальному сайту, программе не хватает данных о старых версиях операционных систем вроде Windows 9x, IRIS и им подобных. Но пользователи могут помочь проекту, добавив в базы результаты собственных экспериментов с программой.

NetScanTools

□ Сайт: netscantools.com

□ Платформа: Windows

Бесплатная утилита NetScanTools Basic (рис. 2.3) 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 командной строкой), отправить DNS-запросы и попинговать удаленные хосты и так и сяк, и вприсядку, т. е. управляя параметрами пинга. Негусто.

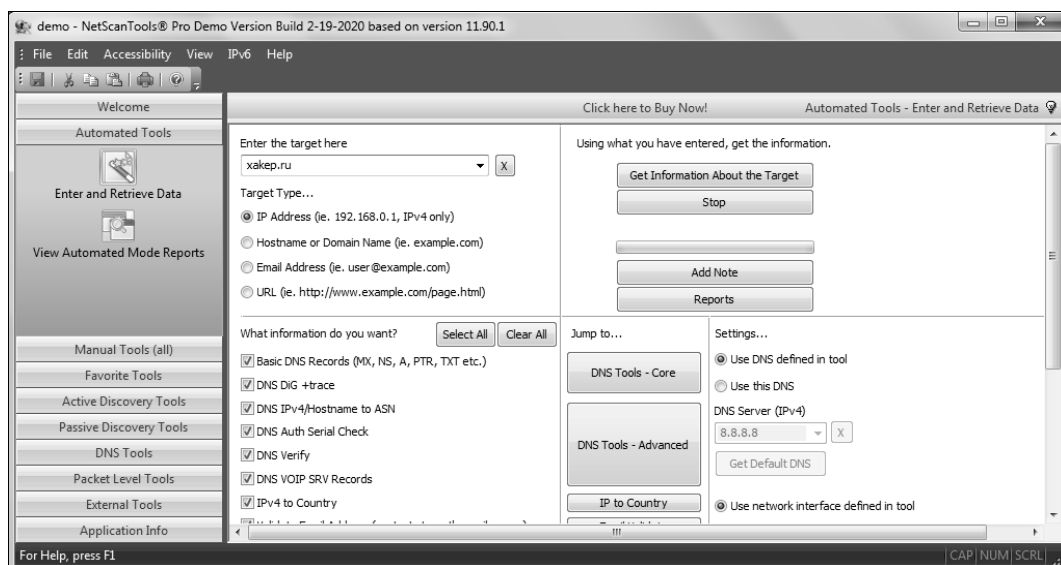


Рис. 2.3. NetScanTools — интересный инструмент с кучей функций. Жалко, платный

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 реляями. В сети Active Directory NetScanTools может найти все расшаренные папки, 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.

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 триальную

версию, которая поможет тебе решить, стоит ли искать пачку баксов, или лучше воспользоваться фриварным 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-приманки, специально созданные для ловли доверчивых хакеров) и подозрительные узлы с измененными настройками стека TCP/IP.

С использованием заложенных в софтинку 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, лопнув от гордости.

Как и другие sniffеры, этот умеет работать с протоколами Telnet, FTP, IMAP, SMB, LDAP и несколькими другими, 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 спloitов, которые могут стать отличным подспорьем для пентестера. Весь софт долго и кропотливо собирала команда единомышленников под названием The Hacker's Choice (<https://twitter.com/hackerschoice>), 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 Амар, позволяющий отследить сервисы, работающие на нестандартных портах.

Некоторые наивные сисадмины 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 хитрыми админами и призван бороться Амар.

Обычные сканеры стучатся на стандартные порты, анализируют полученные отклики и, если они не соответствуют ожидаемому, обламываются. Амар 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 Амар совместно с любым другим сканером. Сканер определяет список открытых портов на интересующем нас хосте, а Амар потом прощупывает этот диапазон и выясняет, какие именно службы юзают эти порты и что полезного из этого может извлечь исследователь. На страничке The Hacker's Choice можно скачать Амар как под винду, так и под Linux, представлены все версии утилиты, начиная с самых ранних.

Выводы

Как ты догадываешься, у большинства описанных здесь утилит возможности гораздо шире, чем просто определение типа ОС на удаленном хосте. Поэтому бесполезно будет попробовать ознакомиться с каждой из них. А уж что ты будешь в итоге использовать в деле — решать тебе.

«Хакер»: безопасность, разработка, DevOps

История журнала «Хакер» началась задолго до февраля 1999 года, когда увидел свет первый номер издания. Еще в ноябре 1998 в сети DALnet появился русскоязычный IRC-канал #хакер, где активно обсуждались компьютерные игры и приемы их взлома, а также прочие связанные с высокими технологиями вещи. Тогда же в недрах основанной Дмитрием Агаруновым компании Gameland зародилась идея выпускать одноименный журнал, правда, изначально он задумывался, как геймерский. Новое издание должно было подхватить выпавшее знамя нескольких закрывшихся компьютерных журналов, не переживших кризис 1998 года. В отличие от популярного «глянца» первой половины «нулевых», идея «Хакера» не была заимствована у какого-либо известного западного издания, а изначально являлась полностью оригинальной и самобытной.

Читатели приняли журнал более чем благосклонно: первый номер «Хакера» был полностью раскуплен в Москве за несколько часов, даже несмотря на то, что он поступил в продажу в 6 вечера. Журнал быстро набрал вирусную популярность, а одной из самых читаемых рубрик «Хакера» стал раздел «западлостроение», в котором авторы щедро делились с аудиторией практическими рецептами и проверенными способами напасть на ближнего своему при помощи различных технических средств разной степени изощренности.

Вскоре под влиянием читательских откликов тематика журнала стала меняться, постепенно смещаясь от игровой индустрии в сторону технологий взлома и защиты информации, что, в общем-то, вполне логично для издания с таким названием. Один из отцов-основателей «Хакера», Денис Давыдов, посвятивший свое творчество компьютерным играм, вскоре покинул редакционный коллектив, чтобы встать во главе собственного журнала: так появилась на свет легендарная «Игромания». Ну а «Хакер» с тех пор сосредоточился на вопросах, изначально заложенных в его ДНК — хакерство, взлом и защита данных. В марте 1999 года был запущен сайт журнала, на котором публиковались анонсы свежих номеров — этот сайт и по сей день можно найти по адресу xakep.ru.

Уже в 2001 году тираж «Хакера» составил 50 тыс. экземпляров. Вскоре после своего появления на свет журнал уверенно завоевал звание одного из самых популярных компьютерных изданий в молодежной среде — по крайней мере, именно так считает русскоязычная «Википедия». «Хакер» регулярно взрывал читательские

массы веселыми статьями о методах взлома домофонов, почтовых серверов и веб-сайтов, временами вызывая фрустрацию у производителей программного обеспечения и прочих представителей крупного бизнеса. На «Хакер» писали жалобы, а благодарные читатели приносили в редакцию пиво. Его сотрудников приглашали на телевидение и радио, а само издание в то же самое время называли «вестником криминальной субкультуры». В общем, и авторы, и читатели развлекались, как могли.

«Хакер» развивался и рос, продолжая публиковать интересные статьи об операционных системах, программах, сетях, гаджетах и компьютерном «железе». Очень скоро все присылаемые авторами материалы перестали помещаться под одну обложку, и некоторые сугубо технические тексты постепенно перекочевали в отдельное тематическое приложение под названием «Хакер Спец».

В 2006 году объем «Хакера» едва не стал рекордным — 192 полосы. Выпустить номер такой толщины не получилось исключительно по техническим причинам. Со временем редакционная политика стала меняться: в журнале появлялось все меньше хулиганских статей, посвященных всевозможным компьютерным безобразиям, и все больше — аналитических материалов о секретах программирования, администрирования, информационной безопасности и защите данных. Но взлому компьютерных систем на страницах «Хакера» по-прежнему уделялось самое пристальное внимание.

Ключевым для истории журнала стал 2013 год, когда параллельно с традиционной бумажной версией стала выходить электронная, которую можно было скачать в виде PDF-файла. А последний бумажный номер журнала увидел свет летом 2015 года. С той поры «Хакер» издается исключительно в режиме онлайн и доступен читателям по подписке.

Сегодняшний «Хакер» — это популярное электронное издание, посвященное вопросам информационной безопасности, программированию и администрированию компьютерных сетей. Основу аудитории **xakep.ru** составляют эксперты по кибербезопасности и IT-специалисты. Мы пишем как о трендах и технологиях, так и о конкретных темах, связанных с защитой информации. На страницах «Хакера» публикуются подробные HOWTO, практические материалы по разработке и администрированию, интервью с выдающимися людьми, создавшими технологические продукты и известные IT-компании, и, конечно, экспертные статьи об информационной безопасности. С подборкой таких статей ты имел возможность ознакомиться на страницах этой книги. Аудитория сайта **xakep.ru** составляет 2 500 000 просмотров в месяц, еще несколько сотен тысяч подписчиков следят за новинками журнала в социальных сетях.

Современный «Хакер» отличается непринужденная, веселая атмосфера. Участники сообщества «Хакер.ru» получают несколько материалов каждый день: мануалы по кодированию и взлому, гайды по новым возможностям и новым эксплоитам, подборки хакерского софта и обзоры веб-сервисов. На сайте «Хакера» ежедневно публикуются знаковые новости из мира компьютерных технологий, рассказывающие о самых интересных событиях в сфере IT. Мы еженедельно готовим дайджесты, делаем подборки советов и полезных программ, изучаем свежие уязвимости.

В рубрике «Взлом» выходят интересные статьи о хакерских технологиях и утилитах, раздел «Кодинг» посвящен хитростям программирования, в рубрике «Приватность» собраны советы и мануалы по сетевой безопасности и сохранению своего инкогнито в Интернете. Статьи из раздела «Трюки» расскажут о недокументированных возможностях софта и нестандартных аппаратных решениях, системные администраторы найдут массу полезных рекомендаций по настройке ОС и прикладного ПО в разделе «Админ», а любители гаджетов и новомодного «железа» смогут насладиться рубрикой «Geek».

Присоединяйся к сообществу «Хакера» прямо сейчас! Материалы журнала выходят в нескольких форматах на выбор. Ты можешь подписаться в приложении на iOS или Android и читать ежемесячные выпуски, либо оформить подписку на сайте и получать статьи каждый будний день — сразу, как только они выходят. Подписка на сайте также дает возможность скачивать ежемесячный PDF и читать на любом удобном устройстве.

Когда «Хакер» только создавался, мы сказали себе: «Наша цель — чтобы среди наших ребят программирование стало самой популярной профессией». Мы использовали для этого все, что могли придумать, — развлекались, дурачились, как могли популяризировали ИБ, нашу субкультуру и тягу к IT в любых ее проявлениях. И мы считаем, что во многом достигли своей цели.

Присоединяйся, мы будем рады видеть тебя в нашей тусовке!

С самыми теплыми пожеланиями,
редакция журнала «Хакер»

Предметный указатель

3

3proxy 85

A

Admins hunting 96
Aircrack 11
Airodump 46
Airodump-ng 47
Airsnot 11
Amap 30
Angry IP Scanner 11
Anon Surf 17
AppInit 128
ARP spoofing 73
Arpspoof 65
ARP-сканирование 48
Atftpd 78
Attack Kill Chain 146
Autoruns 120

B

BackBox 20
BackTrack 13
BeEF XSS 19
BlackArch 18
Blue Team 141
Bring your own device (BYOD) 132
Burp Suite 38

C

Classless inter-domain routing (CIDR) 25
CommView 33
CrackMapExec 115

D

Dcc1 (mscash1) 112
Dcc2 (mscash2) 112
DCERPC 97, 101, 106
DEFT 14
DLP 55
DMZ 65
DNS (reverse DNS lookup) 25
Dns2tcp 85
Dnscat 79
DNS-туннелирование 63, 91
Domain Credential Cache 111

E

ESSID 46
Ettercap 11, 29
Evasion 75
Evil-winrm 102
Exploit Prevention 152
Exploitation 152

F

Fingerprinting 24
FreeSSHd 87

G

Gathering 75
GnuPG 17
Golden ticket 115
GPA 17
GRE 67
GUI 91

H

Hans 90
Hashcat 108
Heartbleed 36
HTTP 106

I

IMAP 106
Impacket 77, 97, 105, 112
In-memory 124
Interceptor-NG 35
Iodine 90
IP forwarding 66
Iptables 88

K

Kali Linux 12, 38, 66
Kerberoasting 108
Kerberos 108
Kirbi 111

L

L2-доступ 65
LANs 47
Lateral movement 75
LDAP 106
LM-хеш 106
Local Port Forwarding 82
LSASS 113, 128

M

MAC (Media Access Control) 41
Macchanger 45
Masscan 11, 132
Maximum segment size, MSS 24
Metasploit 13, 19, 82
Meterpreter 85, 124
mft2csv 19
MiTM 27, 29, 35, 65
MITRE ATT&CK 146
MS SQL 106
MSRPC 97, 106
Multirdp 93

N

NetBios spoofing 73
Netcat 76
NetScanTools 28
Netsh 129
Netwag 11
Network Forensic Analysis Tool (NFAT) 26
NetworkManager 43, 44
NetworkMiner 26
Nmap 24, 48, 86, 132
NPcap 35
NST (Network Security Toolkit) 11
NTLM-relay 106
NTLM-хеш 105, 106
NTP (Network Time Protocol) 51

O

OpenVPN 66, 67, 70, 90
Ophcrack 107

P

p0f 27
Parrot 17
Pass-the-Hash 103, 106, 107, 117
Pass-the-Ticket 103, 110, 117
PcapNet 60
Penetration Testing 143
Persistence 75, 119
Pivoting 75
Privilege escalation 75
Promiscuous mode 31
Psexec 97
Ptftpd 78
Purple Team 142
Pyftplib 77

R

Rc.local 126
RCE 100, 101
RDP 106
Rdpwrap 93
Recall 109
Red Team 141, 143, 149
Remote port forwarding 81
Remote registry 106
Responder 65
Reverse shell 120
Rubeus 109

S

SAM (Security Account Manager) 105
 Sc.exe 102
 Service Manager 122
 Shodan 135
 SIEM 104
 SmartSniff 37
 SNTP (Simple Network Time Protocol) 52
 Socat 80
 Spear phishing 131
 Spoofing 36
 SSH 86
 Sticky keys 114
 SYN 27
 SYN+ACK 27

T

Tactics, techniques and procedures, TTPs 131
 TCP/IP stack fingerprinting 23
 Tcpdump 38
 TermService 93
 TGS-билет 108
 THC-Archive 30
 Tsurugi 15
 TTL (Time To Live) 24, 26

V

VDS 70
 VeraCrypt 18
 VirtualBox 66

Volatility 113
 VPN-туннели 88
 Vulnerability Assessment 143
 Vulnerability Research 152

W

Weaponization 152
 Wifijammer 48
 Window scaling value 24
 Window size 24
 Windows Remote Management (WinRM) 102
 WinDump 38
 Winexe 98
 Winlogon 129
 WinPcap 35, 37
 WINRM 106
 WinRS.exe 103
 Wireshark 24, 32, 62
 WMI 101
 Wmic.exe 102
 Wmis 101

X

X probe 29
 XSSer 18

Z

ZMap 132
 zuluCrypt 18

A

Анализаторы трафика 31

Б

Боковое перемещение 95

Г

Генератор пакетов 34
 Групповые политики 103

Д

Доменные учетные записи 111

П

Постэксплуатация 75
 Проброс портов 85

С

Снифферы 31
 Соксификация 88

Т

Туннелирование портов 87

ХАКЕР

Подпишись на «Хакер» и прокачай свои скиллы в ИБ!

Оформи подписку на xaker.ru, и ты сможешь:

- читать новые актуальные материалы об информационной безопасности, реверс-инжиниринге, хаках и компьютерных трюках;
- получить доступ к статьям, опубликованным на сайте за всё время;
- скачать PDF со всеми вышедшими номерами.

Доступны годовой и месячный варианты подписки.

Внимание: для тех, кто постоянно продлевает подписку, мы стараемся сохранять прежнюю цену. Даже когда доступ к «Хакеру» дорожает, это не затрагивает наших постоянных читателей.

<https://xaker.ru/about-magazine/>

ПЕНТЕСТ

СЕКРЕТЫ ЭТИЧНОГО ВЗЛОМА

В книге собраны лучшие, тщательно отобранные статьи из легендарного журнала «Хакер», посвященные этичному взлому и тестированию на проникновение. Авторы этих статей — специалисты в сфере информационной безопасности, практикующие пентестеры, профессиональные эксперты по защите данных. Написанные ими материалы — результат их многолетнего труда и отражение накопленного опыта.

Вы узнаете:

- какой инструментарий используется для тестирования на проникновение;
- как тестировать беспроводные сети;
- как выводить ценные данные с использованием Network Time Protocol;
- как организованы и как действуют команды Red Team;
- способы постэксплуатации Windows при помощи виртуальной машины с Linux;
- практические приемы pivoting;
- методы удаленного исполнения кода в Windows;
- способы обеспечения persistence;
- приемы разведки на основе открытых источников (OSINT).

Андрей Жуков
Денис Макрушин
Валентин Холмогоров
Марк Бруцкий-Стемпковский
Михаил Артюхин
Иван Пискунов

«Хакер» — легендарный журнал об информационной безопасности, издающийся с 1999 года. На протяжении 20 лет на страницах «Хакера» публикуются интересные статьи об операционных системах, программах, сетях, гаджетах и компьютерном «железе». На сайте «Хакера» ежедневно появляются знаковые новости из мира компьютерных технологий, мануалы по кодигу и взлому, гайды по новым эксплойтам, подборки хакерского софта и обзоры веб-сервисов. Среди авторов журнала — авторитетные эксперты по кибербезопасности и IT-специалисты.



191036, Санкт-Петербург,
Гончарная ул., 20
Тел.: (812) 717-10-50,
339-54-17, 339-54-28
E-mail: mail@bhv.ru
Internet: www.bhv.ru

ISBN 978-5-9775-6823-4



9 785977 568234