

Содержание

ВВЕДЕНИЕ	11
ГЛАВА 1. ОСНОВЫ LINUX	15
1.1. ПРОЦЕСС ЗАГРУЗКИ ОС. ЯДРО	16
1.1.1. Загрузчики Linux.....	17
1.1.2. Загрузчик GRUB2	17
Конфигурационные файлы	17
Выбор метки по умолчанию	24
Пароль загрузчика GRUB2.....	24
Установка загрузчика.....	26
1.1.3. Система инициализации	27
Принцип работы.....	28
Конфигурационные файлы <i>systemd</i>	30
Цели.....	32
Управление сервисами при использовании <i>systemd</i>	34
1.2. УЧЕТНЫЕ ЗАПИСИ ПОЛЬЗОВАТЕЛЕЙ	35
1.2.1. Введение в учетные записи Linux	35
1.2.2. Получение полномочий <i>root</i>	38
1.2.3. Управление учетными записями пользователей	44
Файлы <i>/etc/passwd</i> и <i>/etc/shadow</i>	45
Изменение и удаление учетных записей	49
Группы пользователей.....	53
1.2.4. Модули PAM.....	53
Ограничиваем доступ к системе по IP-адресу.....	57
Ограничиваем время входа в систему.....	58
Ограничение системных ресурсов с помощью PAM	59
1.3. ПРАВА ДОСТУПА К ФАЙЛАМ И КАТАЛОГАМ	61
1.3.1. Общие положения.....	61
1.3.2. Смена владельца файла	62
1.3.3. Определение прав доступа	62
1.3.4. Специальные права доступа	65
1.3.5. Атрибуты файла.....	65
1.4. МОНТИРОВАНИЕ ФАЙЛОВЫХ СИСТЕМ	67
1.4.1. Монтируем файловые системы вручную	67
1.4.2. Имена устройства	69



1.4.3. Монтируем файловые системы при загрузке.....	72
1.4.4. Автоматическое монтирование файловых систем.....	73
1.4.5. Работа с журналом.....	74
1.4.6. Преимущества файловой системы ext4.....	74
1.4.7. Специальные операции с файловой системой.....	75
Монтирование NTFS-разделов.....	75
Создание файла подкачки.....	76
Файлы с файловой системой.....	77
Создание и монтирование ISO-образов.....	78

ГЛАВА 2. ЛОКАЛЬНЫЙ ВЗЛОМ – ЛОМАЕМ ПАРОЛЬ ROOT..... 81

2.1. ИСПОЛЬЗУЕМ ПОДМЕНУ ОБОЛОЧКИ.....	82
2.2. ИСПОЛЬЗУЕМ ЗАГРУЗОЧНЫЙ ДИСК.....	84
2.3. УТИЛИТА <i>CRUNCH</i> : ГЕНЕРАТОР ПАРОЛЕЙ.....	89

ГЛАВА 3. ПОЛУЧАЕМ ПРАВА ROOT НА VDS 91

3.1. СБОР ИНФОРМАЦИИ.....	92
3.2. КРИТИЧЕСКИЕ ДАННЫЕ.....	94
3.3. ФЛАГИ SUID/SGUID.....	94
3.4. АНАЛИЗ ИСТОРИИ КОМАНД.....	95
3.5. ВОЗМОЖНОСТИ LINUX.....	96
3.6. ПЛАНИРОВЩИК <i>CRON</i>	97
3.7. УЯЗВИМОСТИ ЯДРА.....	98
3.8. БРУТФОРС SSH.....	99
3.8.1. Использование Patator.....	99
3.8.2. Инструмент Hydra.....	100
3.8.3. Инструмент Medusa.....	100
3.8.4. Metasploit.....	100

ГЛАВА 4. УЯЗВИМОСТИ ECRYPTFS	103
4.1. ВЫБОР СРЕДСТВ ШИФРОВАНИЯ В LINUX	104
4.2. АТАКА НА ECRYPTFS: ПОЛУЧАЕМ ПРИВИЛЕГИИ <i>ROOT</i>	107
ГЛАВА 5. ВЗЛОМ ПОПУЛЯРНЫХ СЕТЕВЫХ СЕРВИСОВ ..	109
5.1. УЯЗВИМОСТЬ В АРАСНЕ.....	110
5.1.1. Общее описание уязвимости	110
5.1.2. Примеры использования уязвимости.....	111
Пример 1	111
Пример 2	111
Пример 3	111
Пример 4	112
5.2. ВЗЛОМ MYSQL.....	112
5.2.1. SQL-инъекции	112
5.2.2. Поиск жертвы	115
5.2.3. Брутфорс	117
5.2.4. Что делать дальше?.....	118
5.3. ВЗЛОМ WORDPRESS.....	119
ГЛАВА 6. СБОР ИНФОРМАЦИИ.....	121
6.1. ОБЩЕДОСТУПНЫЕ САЙТЫ.....	122
6.2. ПОЛУЧЕНИЕ ИНФОРМАЦИИ О ДОМЕНЕ	123
6.3. КОМАНДА <i>HOST</i>	125
6.4. КОМАНДА <i>DIG</i>	126
6.5. ОЧЕНЬ ПОЛЕЗНЫЙ ИНСТРУМЕНТ - <i>DEERMAGIC INFORMATION GATHERING TOOL (DMITRY)</i>	127
6.6. КОМАНДА <i>TRACEROUTE</i>	131
6.7. ИНСТРУМЕНТ <i>METAGOOFIL</i>	133

ГЛАВА 7. ЧТО ТАКОЕ *KALI LINUX* И КАК ЕГО ИСПОЛЬЗОВАТЬ ДЛЯ ВЗЛОМА 135

7.1. ВКРАТЦЕ О <i>KALI</i>	136
7.2. ГДЕ СКАЧАТЬ И КАК УСТАНОВИТЬ <i>KALI LINUX</i>	140
7.3. ОБСЛУЖИВАНИЕ СИСТЕМЫ	152
7.3.1. Обслуживание источников пакетов	152
7.3.2. Ошибка " <i>The disk contains an unclean file system (0, 0). Metadata kept in Windows cache, refused to mount</i> "	153
7.3.3. Регулярная очистка системы	153
7.3.4. Задание пароля <i>root</i> . Вход как <i>root</i>	155

ГЛАВА 8. ОБЗОР ЛУЧШИХ ИНСТРУМЕНТОВ *KALI LINUX*..... 157

8.1. <i>WPSCAN</i>	158
8.2. <i>NMAP</i>	160
8.3. <i>LYNIS</i>	162
8.4. <i>AIRCRAK-NG</i>	163
8.5. <i>HYDRA</i>	164
8.6. <i>WIRESHARK</i>	165
8.7. <i>METASPLOIT FRAMEWORK</i>	165
8.8. <i>SKIPFISH</i>	166
8.9. <i>SQLMAP</i>	169
8.10. ВЗЛОМ ПАРОЛЯ <i>WINDOWS</i> . <i>JOHN THE RIPPER</i>	175
8.11. <i>WIRESHARK</i> – ЗАХВАТ ТРАФИКА	177
8.12. <i>AUTOPSY FORENSIC BROWSER: ПРОФЕССИОНАЛЬНЫЙ ИНСТРУМЕНТ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ</i>	179
8.13. <i>NIKTO</i>	194
8.14. <i>SNORT</i>	197
8.15. <i>AIRFLOOD</i>	197

8.16. APKTOOL.....	197
8.17. NESSUS – ЛУЧШИЙ СКАНЕР УЯЗВИМОСТЕЙ	200
8.18. FCRAKZIP – ВЗЛОМ ПАРОЛЯ ZIP-АРХИВА	201

ГЛАВА 9. ИСПОЛЬЗОВАНИЕ METASPLOIT ДЛЯ ВЗЛОМА... 203

9.1. ЧТО ТАКОЕ METASPLOIT	204
9.2. СТРУКТУРА ФРЕЙМВОРКА	206
9.3. БАЗОВАЯ ТЕРМИНОЛОГИЯ.....	207
9.4. КОНФИГУРАЦИИ ФРЕЙМВОРКА И ОСНОВНЫЕ КОМАНДЫ	209
9.5. КОНФИГУРАЦИЯ МОДУЛЕЙ	210
9.6. ПЕРВЫЙ ЗАПУСК METASPLOIT	211
9.7. ПРАКТИЧЕСКОЕ ИСПОЛЬЗОВАНИЕ КОМАНД METASPLOIT	215
9.7.1. Команда <i>help</i> – получение справки	215
9.7.2. Команда <i>use</i> – выбор модуля для использования	215
9.7.3. Команда <i>show</i> – показ сущностей	216
9.7.4. Команды <i>set</i> и <i>setg</i> – установка значений переменных	221
9.7.5. Команда <i>check</i> – проверка целевой системы.....	222
9.7.6. Команда <i>back</i> – возврат	222
9.7.7. Команда <i>run</i> – запуск эксплоита	223
9.7.8. Команда <i>resource</i> – определение ресурса.....	223
9.7.9. Команда <i>irb</i>	224
9.8. ПРАКТИЧЕСКИЙ ПРИМЕР 1: ВЗЛАМЫВАЕМ СТАРЕНЬКИЙ СЕРВЕР WINDOWS 2008 С ПОМОЩЬЮ ЭКСПЛОИТА АНБ	224
9.9. ПРАКТИЧЕСКИЙ ПРИМЕР 2: ХАКАЕМ СОВРЕМЕННЫЕ СИСТЕМЫ – WINDOWS SERVER 2016 И WINDOWS 10	228

ГЛАВА 10. ВЗЛОМ И ЗАЩИТА АККАУНТОВ В СОЦИАЛЬ- НЫХ СЕТЯХ..... 233

10.1. КТО И ЗАЧЕМ ВЗЛАМЫВАЕТ АККАУНТЫ.....	234
10.2. СБОР ИНФОРМАЦИИ	236

10.3. МЕТОДЫ ВЗЛОМА	241
10.3.1. Взлом электронной почты.....	241
10.3.2. Социальный инжиниринг	242
10.3.3. Перебор пароля	242
10.3.4. Фишинг или фэйковая страничка. Очень подробное руководство.....	245
10.3.5. Клавиатурный шпион	256
10.3.6. Подмена DNS	257
10.4. КАК УБЕРЕЧЬСЯ ОТ ВЗЛОМА	257
ГЛАВА 11. АНОНИМНОСТЬ В ИНТЕРНЕТЕ	259
11.1. ЧАСТИЧНАЯ АНОНИМНОСТЬ	260
11.2. ЦЕПОЧКИ ПРОКСИ	262
11.3. ПРОЕКТ TOR	263
11.3.1. Что такое Tor.....	263
11.3.2. Как работает браузер Tor.....	264
11.3.3. Кто и зачем использует Tor?.....	267
11.3.4. Что лучше VPN или Tor?.....	267
11.3.5. Tor и VPN.....	269
Tor через VPN.....	269
VPN через Tor.....	270
11.3.6. Использование браузера Tor в Windows.....	271
11.3.7. Тонкая настройка Tor.....	274
Установка выходных узлов	274
Фиксирование входных узлов.....	275
Исключение подозрительных узлов.....	276
Запрещаем использовать комп в качестве выходного узла.....	276
Установка прокси-сервера в Tor	277
Другие параметры конфигурационного файла	277
11.4. VPN ДЛЯ LINUX	282
11.5. ЧТО ТАКОЕ DARKNET?	284
11.6. НА ПУТИ К ПОЛНОЙ АНОНИМНОСТИ	285
11.7. ЗАМЕТАЕМ СЛЕДЫ	287
11.7.1. Приложения для безопасного удаления данных с жестких дисков.....	287

11.7.2. Удаление инфы с SSD	288
11.7.3. Запутываем следы	291

ГЛАВА 12. КАК МОЖНО ВЗЛОМАТЬ ANDROID..... 293

12.1. ПРИБОРЫ И МАТЕРИАЛЫ	294
12.2. ВСКРЫВАЕМ АРК.....	298
12.3. ВНОСИМ ИЗМЕНЕНИЯ В ПРОГРАММУ.....	302
12.4. УСТАНОВКА ANDROID STUDIO В LINUX.....	304

ГЛАВА 13. СКРИПТИНГ ДЛЯ ХАКЕРА.....309

13.1. ВЗЛОМ FTP.....	310
13.2. ПРОВЕРКА ПОРТОВ	311
13.3. СКАНИРОВАНИЕ MYSQL.....	312
13.4. ТСР-СЕРВЕР НА PYTHON.....	314
13.5. КАК ЗАПУСКАТЬ СКРИПТЫ ИЗ ЭТОЙ ГЛАВЫ?.....	315

Данная книга показывает, как использовать Linux для несанкционированного доступа к информационным системам. Попросту говоря для взлома. Первая часть книги показывает, как взломать саму Linux, вторая – как использовать различные инструменты, доступные в Linux, для взлома других систем, опять-таки, в том числе и Linux.

Мы предупреждаем читателя: материал носит информационный характер и каждый сам решает, как его использовать. Вся ответственность по использованию материала данной книги в противозаконных целях ложится на самого читателя. В книге не показываются примеры взлома каких-то реальных систем и сервисов.

В первой главе приводятся основы Linux. Ты не сможешь взломать Linux, не понимая, как она работает. Это относится не только к Linux, а и к любой другой системе. Нужно понимать, как работает та или иная система, знать ее тонкости и нюансы и только потом возможен ее взлом. Поэтому если ты не знаком с Linux, то чтение этой книги нужно начать именно с первой главы, не пропуская ее.

Далее будет показано, как взломать локальную Linux-систему и получить права *root*. Когда нет доступа к "железу", все усложняется, но нет ничего невозможного. И такой случай рассматривается в главе 3.

Четвертая глава посвящена различным уязвимостям в системе шифрования файлов и папок eCryptfs. Пятая глава будет самой интересной в этой части книги, поскольку будет показано, как взломать Apache, MySQL, а также CMS WordPress.

Следующая часть книги посвящена хакерским инструментам в Linux, которые можно использовать как для взлома самой Linux, так и для взлома других систем. В главе 7 состоится знакомство с хакерским дистрибутивом Kali Linux, а в главе 8 будут описаны популярные инструменты из этого дистрибутива. Один из этих инструментов заслуживает отдельного разговора, и он состоится в главе 9.

В главе 10 попытаемся взломать аккаунт в социальной сети, а в главе 11 – научимся скрывать свою деятельность с помощью Tor.

Дальнейший материал посвящен взлому Android-приложения посредством инструментов, входящих в состав Linux. Также немного поговорим про скриптинг для хакера.

Добро пожаловать на темную сторону!