

# Содержание

<b>Введение .....</b>	<b>9</b>
<b>В.1. ТИПИЧНЫЕ ОШИБКИ ХАКЕРОВ .....</b>	<b>9</b>
Лень .....	9
Самоуверенность .....	10
Глупость .....	11
<b>В.2. ИСТОЧНИКИ ИНФОРМАЦИИ .....</b>	<b>11</b>
<b>В.3. КАК ЧИТАТЬ ЭТУ КНИГУ .....</b>	<b>12</b>
<b>Глава 1. Посещаем анонимно закрытые сайты .....</b>	<b>15</b>
<b>1.1. СПОСОБЫ ОБХОДА ЗАПРЕТА.....</b>	<b>15</b>
<b>1.2. СМЕНА СЕТИ.....</b>	<b>17</b>
<b>1.3. АНОНИМАЙЗЕР.....</b>	<b>19</b>
<b>1.4. АНОНИМНЫЕ ПРОКСИ-СЕРВЕРЫ .....</b>	<b>20</b>
<b>1.5. ТРИ ЗАВЕТНЫЕ БУКВЫ - VPN.....</b>	<b>24</b>
1.5.1. Основная информация.....	24
1.5.2. Обзор популярных VPN-провайдеров .....	28
<b>Глава 2. Как взломать сайт .....</b>	<b>33</b>
<b>2.1. ЗАЧЕМ ВЗЛАМЫВАЮТ САЙТ .....</b>	<b>33</b>
<b>2.2. КАК ВЗЛАМЫВАЮТ САЙТЫ .....</b>	<b>34</b>
<b>2.3. РЕАЛЬНЫЙ ПРИМЕР: ВЗЛАМЫВАЕМ ГОЛОСОВАЛКУ .....</b>	<b>36</b>
2.3.1. Выбираем оптимальный способ.....	36
2.3.2. Накрутка с помощью анонимайзеров .....	38
2.3.3. Анонимные прокси .....	39
2.3.4. Ломаем голосовалку .....	43
2.3.5. Автоматизируем .....	47
2.3.6. Как защититься от взлома? .....	48
<b>Глава 3. Как взломать электронную почту.....</b>	<b>50</b>
<b>3.1. ТРОЯНСКИЙ КОНЬ .....</b>	<b>50</b>
<b>3.2. ВЗЛОМ ПО НОМЕРУ ТЕЛЕФОНА .....</b>	<b>53</b>
<b>3.3. ФИЗИЧЕСКИЙ ДОСТУП К КОМПЬЮТЕРУ .....</b>	<b>55</b>

<b>3.4. СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ ИЛИ ПРОСТО ОБМАН</b> .....	57
<b>3.5. МОДНОЕ СЛОВО "ФИШИНГ"</b> .....	58
<b>3.6. ВОССТАНАВЛИВАЕМ ПАРОЛЬ</b> .....	62
<b>3.7. КРАЖА COOKIES</b> .....	62
<b>3.8. XSS-УЯЗВИМОСТИ</b> .....	63
<b>3.9. МЕТОД ГРУБОЙ СИЛЫ</b> .....	64

## **Глава 4. Как отправлять электронную почту и другие электронные сообщения анонимно** .....

65

<b>4.1. ЗАПОВЕДИ ПАРАНОИКА</b> .....	65
<b>4.2. ЦЕЛИ АНОНИМНОСТИ ПОЧТОВОГО ЯЩИКА</b> .....	66
<b>4.3. ПОЛУЧАЕМ АНОНИМНУЮ ПОЧТУ</b> .....	68
<b>4.4. КАКОЙ МЕССЕНДЖЕР САМЫЙ АНОНИМНЫЙ</b> .....	75
4.4.1. Telegram .....	76
4.4.2. Viber.....	76
4.4.3. WhatsApp .....	77
4.4.4. Signal .....	78
4.4.5. Briar .....	78
4.4.6. Мессенджеры социальных сетей .....	79
4.4.7. WickrMe .....	80
4.4.8. Wire.....	82

## **Глава 5. Анонимность в Интернете. Возможно ли?**.....

83

<b>5.1. ЧАСТИЧНАЯ АНОНИМНОСТЬ</b> .....	83
<b>5.2. ЦЕПОЧКИ ПРОКСИ</b> .....	85
<b>5.3. ПРОЕКТ TOR</b> .....	87
5.3.1. Что такое Tor .....	87
5.3.2. Как работает браузер Tor.....	88
5.3.3. Кто и зачем использует Tor? .....	90
5.3.4. Что лучше VPN или Tor?.....	91
5.3.5. Tor и VPN.....	93
5.3.6. Использование браузера Tor в Windows .....	94
5.3.7. Тонкая настройка Tor .....	98
5.3.8. Установка Tor в Android .....	105
<b>5.4. VPN ДЛЯ LINUX</b> .....	107
<b>5.5. ЧТО ТАКОЕ DARKNET?</b> .....	109

5.6. НА ПУТИ К ПОЛНОЙ АНОНИМНОСТИ .....	110
---	-----

## Глава 6. Что такое Kali Linux и как его использовать для взлома..... 112

6.1. ВКРАТЦЕ О KALI .....	112
---------------------------	-----

6.2. ГДЕ СКАЧАТЬ И КАК УСТАНОВИТЬ KALI LINUX .....	116
--	-----

6.3. ОБСЛУЖИВАНИЕ СИСТЕМЫ .....	126
---------------------------------	-----

6.3.1. Обслуживание источников пакетов.....	126
---	-----

6.3.2. Ошибка «The disk contains an unclean file system (0, 0). Metadata kept in Windows cache, refused to mount» .....	127
---	-----

6.3.3. Регулярная очистка системы.....	127
--	-----

6.3.4. Задание пароля <i>root</i> . Вход как <i>root</i> .....	129
--	-----

6.4. ОБЗОР ЛУЧШИХ ИНСТРУМЕНТОВ KALI LINUX .....	130
---	-----

6.4.1. WPScan.....	130
--------------------	-----

6.4.2. Nmap.....	132
------------------	-----

6.4.3. Lynis .....	133
--------------------	-----

6.4.4. Aircrack-ng .....	134
--------------------------	-----

6.4.5. Hydra .....	134
--------------------	-----

6.4.6. Wireshark.....	136
-----------------------	-----

6.4.7. Metasploit Framework.....	136
----------------------------------	-----

6.4.8. Skipfish .....	136
-----------------------	-----

6.4.9. Sqlmap .....	139
---------------------	-----

6.4.10. Взлом пароля Windows. John the Ripper .....	144
---	-----

6.4.11. Wireshark – захват трафика .....	147
--	-----

6.4.12. Autopsy Forensic Browser: профессиональный инструмент правоохранительных органов .....	149
--	-----

6.4.13. Nikto .....	161
---------------------	-----

6.4.14. Snort.....	164
--------------------	-----

6.4.15. Airflood.....	164
-----------------------	-----

6.4.16. Apktool .....	164
-----------------------	-----

6.4.17. Nessus – лучший сканер уязвимостей.....	167
---	-----

6.4.18. fcrackzip – взлом пароля Zip-архива .....	168
---	-----

## Глава 7. Секреты Metasploit..... 170

7.1. ЧТО ТАКОЕ METASPLOIT .....	170
---------------------------------	-----

7.2. СТРУКТУРА ФРЕЙМВОРКА .....	172
---------------------------------	-----

7.3. БАЗОВАЯ ТЕРМИНОЛОГИЯ.....	173
--------------------------------	-----

7.4. КОНФИГУРАЦИИ ФРЕЙМВОРКА И ОСНОВНЫЕ КОМАНДЫ .....	175
---	-----

7.5. КОНФИГУРАЦИЯ МОДУЛЕЙ .....	176
---------------------------------	-----

<b>7.6. ПЕРВЫЙ ЗАПУСК METASPLOIT .....</b>	<b>176</b>
<b>7.7. ПРАКТИЧЕСКОЕ ИСПОЛЬЗОВАНИЕ КОМАНД METASPLOIT .....</b>	<b>180</b>
7.7.1. Команда <i>help</i> – получение справки .....	180
7.7.2. Команда <i>use</i> – выбор модуля для использования.....	181
7.7.3. Команда <i>show</i> – показ сущностей.....	182
7.7.4. Команды <i>set</i> и <i>setg</i> – установка значений переменных .....	186
7.7.5. Команда <i>check</i> – проверка целевой системы .....	187
7.7.6. Команда <i>back</i> – возврат .....	188
7.7.7. Команда <i>run</i> – запуск эксплойта.....	188
7.7.8. Команда <i>resource</i> – определение ресурса .....	189
7.7.9. Команда <i>irb</i> .....	189
<b>7.8. ПРАКТИЧЕСКИЙ ПРИМЕР 1: ВЗЛАМЫВАЕМ СТАРЕНЬКИЙ СЕРВЕР     WINDOWS 2008 С ПОМОЩЬЮ ЭКСПЛОЙТА АНБ .....</b>	<b>190</b>
<b>7.9. ПРАКТИЧЕСКИЙ ПРИМЕР 2: ХАКАЕМ СОВРЕМЕННЫЕ СИСТЕМЫ –     WINDOWS SERVER 2016 И WINDOWS 10 .....</b>	<b>194</b>

## **Глава 8. Взлом и защита аккаунтов в социальных сетях 198**

<b>8.1. КТО И ЗАЧЕМ ВЗЛАМЫВАЕТ АККАУНТЫ.....</b>	<b>198</b>
<b>8.2. СБОР ИНФОРМАЦИИ .....</b>	<b>200</b>
<b>8.3. МЕТОДЫ ВЗЛОМА.....</b>	<b>204</b>
8.3.1. Взлом электронной почты.....	204
8.3.2. Социальный инжиниринг .....	204
8.3.3. Перебор пароля .....	205
8.3.4. Фишинг или фейковая страничка. Очень подробное руководство	208
8.3.5. Клавиатурный шпион.....	220
8.3.6. Подмена DNS .....	221
<b>8.4. КАК УБЕРЕЧЬСЯ ОТ ВЗЛОМА .....</b>	<b>221</b>

## **Глава 9. Взлом паролей и получение доступа к зашифрованным данным .....223**

<b>9.1. СБРОС ПАРОЛЯ WINDOWS 10 .....</b>	<b>223</b>
9.1.1. Сброс пароля с помощью PowerShell .....	223
9.1.2. Взлом пароля с помощью утилиты Lazesoft Recover My Password	224
9.1.3. Сброс пароля Windows 10 через режим восстановления.....	225
<b>9.2. ПОЛУЧЕНИЕ ДОСТУПА К ФАЙЛАМ, ЗАШИФРОВАННЫМ С ПОМОЩЬЮ     EFS .....</b>	<b>228</b>
9.2.1. Что такое EFS? .....	228
9.2.2. Включение EFS-шифрование .....	230

9.2.3. Использование программы Advanced EFS Data Recovery для расшифровки зашифрованных EFS файлов.....	231
<b>9.3. ВОССТАНОВЛЕНИЕ ДОСТУПА К BITLOCKER .....</b>	<b>237</b>
9.3.1. Особенности реализации .....	238
9.3.2. Технические подробности .....	239
9.3.3. Включение шифрования и восстановления доступа с помощью ключа восстановления.....	240
9.3.4. Дополнительные возможности взлома BitLocker .....	246
<b>9.4. ВЗЛОМ ПАРОЛЯ ROOT В LINUX.....</b>	<b>249</b>
<b>9.5. УТИЛИТА CRUNCH: ГЕНЕРАТОР ПАРОЛЕЙ.....</b>	<b>255</b>
<b>Глава 10. Взламываем соседский WiFi-роутер.....</b>	<b>257</b>
<b>10.1. ПРИЧИНЫ ВЗЛОМА.....</b>	<b>257</b>
<b>10.2. УЗНАЕМ СВОЙ ПАРОЛЬ WIFI.....</b>	<b>259</b>
<b>10.3. СМЕНЯЕМ MAC-АДРЕС .....</b>	<b>259</b>
<b>10.4. ВЗЛОМ РОУТЕРА С ИСПОЛЬЗОВАНИЕМ УЯЗВИМОСТИ .....</b>	<b>261</b>
10.4.1. Установка и запуск инструмента.....	262
10.4.2. Проверка на уязвимость по всем эксплоитам .....	263
10.4.3. Проверка на конкретную уязвимость .....	264
10.4.4. Использование эксплойтов .....	265
<b>10.5. ВЗЛОМ WPA2-РОУТЕРА. МИФЫ И РЕАЛЬНОСТЬ.....</b>	<b>266</b>
<b>10.6. АВТОМАТИЗИРУЕМ ВЗЛОМ С ПОМОЩЬЮ WIFITE.....</b>	<b>275</b>
<b>10.7. ANDROID-ПРИЛОЖЕНИЕ ДЛЯ БРУТФОРСИНГА WIFI-СЕТИ.....</b>	<b>281</b>
<b>10.8. КАК РАЗДОБЫТЬ ХОРОШИЙ ХАКЕРСКИЙ СЛОВАРЬ.....</b>	<b>282</b>
<b>10.9. РЕАЛИИ .....</b>	<b>287</b>
<b>Глава 11. Заметаем следы.....</b>	<b>289</b>
<b>11.1. ОЧИСТКА СПИСКОВ НЕДАВНИХ МЕСТ И ПРОГРАММ.....</b>	<b>289</b>
<b>11.2. ОЧИСТКА СПИСКА USB-НАКОПИТЕЛЕЙ .....</b>	<b>292</b>
<b>11.3. ОЧИСТКА КЭША И ИСТОРИИ БРАУЗЕРОВ.....</b>	<b>294</b>
<b>11.4. УДАЛЯЕМ ЗАПИСИ DNS.....</b>	<b>296</b>
<b>11.5. ОЧИСТКА FLASH COOKIES.....</b>	<b>296</b>
<b>11.6. УДАЛЕНИЕ СПИСКА ПОСЛЕДНИХ ДОКУМЕНТОВ MS OFFICE .....</b>	<b>296</b>
<b>11.7. АВТОМАТИЗИРУЕМ ОЧИСТКУ С ПОМОЩЬЮ CCLEANER.....</b>	<b>297</b>

11.8. РЕАЛЬНОЕ УДАЛЕНИЕ ФАЙЛОВ..... 297  
11.9. СОЗДАЕМ ВАТ-ФАЙЛ ДЛЯ ОЧИСТКИ ВСЕГО..... 299  
11.10. СОЗДАЕМ АУТОНОТКЕУ-СКРИПТ ДЛЯ ОЧИСТКИ ВСЕГО..... 300

**Глава 12. Швейцарский нож хакера .....301**

12.1. КАК ВОССТАНОВИТЬ ПАРОЛЬ TOTAL COMMANDER..... 301  
12.2. БЕСПЛАТНАЯ ОТПРАВКА SMS ПО ВСЕМУ МИРУ ..... 302  
12.3. ЗАПУТЫВАЕМ СЛЕДЫ В ЛОГАХ СЕРВЕРА ..... 303  
12.4. ВОРУЕМ WINRAR ..... 304  
12.5. ПРИВАТНАЯ ОПЕРАЦИОННАЯ СИСТЕМА KODACHI..... 305  
12.6. ПЛАГИН PRIVACY POSSUM ДЛЯ FIREFOX..... 305  
12.7. ПОЛУЧАЕМ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ О ПОЛЬЗОВАТЕ-  
ЛЕ FACEBOOK ..... 306  
12.8. УЗНАЕМ МЕСТОНАХОЖДЕНИЕ ПОЛЬЗОВАТЕЛЯ GMAIL..... 306  
12.9. ОБХОД АВТОРИЗАЦИИ WI-FI С ГОСТЕВЫМ ДОСТУПОМ. ЛОМАЕМ  
ПЛАТНЫЙ WI-FI В ОТЕЛЕ..... 307  
12.10. САЙТ ДЛЯ ИЗМЕНЕНИЯ ГОЛОСА..... 308  
12.11. СПАМИМ ДРУГА В TELEGRAM С ПОМОЩЬЮ TERMUX ..... 308  
12.12. УЗНАЕМ IP-АДРЕС ЧЕРЕЗ TELEGRAM ..... 309  
12.13. КАК УБИТЬ ANDROID-ДЕВАЙС ВРАГА..... 309  
12.14. ШИФРУЕМ ВИРУС ДЛЯ ANDROID ..... 310  
12.15. МСТИМ НЕДРУГУ С ПОМОЩЬЮ CALLSPAM .....311  
12.16. ЕЩЕ ОДНА БОМБА-СПАММЕР ТВОМВ..... 312  
12.17. ВЗЛОМ INSTAGRAM..... 315  
12.18. DDOS-АТАКА РОУТЕРА..... 316  
12.19. SPLOITUS – ПОИСКОВИК СВЕЖИХ УЯЗВИМОСТЕЙ ..... 317  
12.20. УГОН TELEGRAM-АККАУНТА..... 318  
12.21. КАК ПОЛОЖИТЬ WIFI СОСЕДА ИЛИ КОНКУРЕНТА ..... 319