

Spis treści

O autorach	15
O redaktorach merytorycznych	17
Podziękowania	18
Przedmowa	19
Wprowadzenie	21
Rozdział 1. Hakowanie jako przypadek biznesowy	29
Wszystkie komputery są zepsute	30
Stawka	32
Co jest kradzione i dlaczego jest to wartościowe?	32
Internet rzeczy podatnych na ataki	32
Niebieskie, czerwone i purpurowe zespoły	33
Niebieskie zespoły	33
Czerwone zespoły	33
Purpurowe zespoły	35
Hakowanie jako część systemu odpornościowego firmy	37
Podsumowanie	39

Rozdział 2.	Etyczne i legalne hakowanie	41
	Prawa wpływające na Twoją pracę	42
	Bezprawne hakowanie	43
	Sąsiedzkie hakowanie	43
	Szara strefa	43
	Metodologie testów penetracyjnych	44
	Autoryzacja	46
	Odpowiedzialne ujawnianie	46
	Programy nagród za błędy	48
	Porady prawne	49
	Kodeks postępowania firmy Hacker House	49
	Podsumowanie	50
Rozdział 3.	Przygotowanie narzędzi do hakowania	51
	Sprzęt do hakowania	52
	Linux czy BSD?	54
	Systemy operacyjne hosta	55
	Gentoo Linux	55
	Arch Linux	56
	Debian	56
	Ubuntu	56
	Kali Linux	57
	Kontrolowanie pobranych plików	57
	Szyfrowanie dysku	59
	Podstawowe oprogramowanie	61
	Zapora sieciowa	62
	Menedżer haseł	63
	E-mail	64
	Konfigurowanie VirtualBoksa	64
	Ustawienia wirtualizacji	64
	Pobieranie i instalowanie VirtualBoksa	65
	Sieć wewnątrz hosta	65
	Tworzenie maszyny wirtualnej Kali Linux	68
	Laboratoria	77
	Dodatki dla systemu gościa	80
	Testowanie wirtualnego środowiska	80
	Tworzenie serwera z podatnościami	82
	Podsumowanie	83

Rozdział 4.	Zbieranie danych z otwartych źródeł	84
	Czy Twój klient potrzebuje analizy OSINT?	85
	Czego należy szukać?	86
	Gdzie znaleźć te dane?	87
	Narzędzia do OSINT	87
	Pobieranie adresów e-mail za pomocą Google	88
	Technika Google dorking	90
	Krótkie wprowadzenie do plików passwd i shadow	90
	Baza danych zapytań Google	93
	Czy już mnie przejęli?	94
	Framework Recon-ng	95
	Jak działa framework Recon-ng?	101
	Zbieranie danych z sieci WWW	102
	Metadane dokumentu	103
	Maltego	106
	Sieci społecznościowe	107
	Shodan	109
	Ochrona przed działaniami OSINT	111
	Podsumowanie	112
Rozdział 5.	System DNS	113
	Implikacje hakowania serwerów DNS	113
	Krótką historią systemu DNS	114
	Hierarchia systemu DNS	114
	Proste zapytanie DNS	115
	Odpowiedzialność i strefy	117
	Rekordy zasobów w systemie DNS	118
	BIND9	120
	Narzędzia do hakowania serwerów DNS	123
	Znajdowanie hostów	124
	WHOIS	124
	Siłowe poznawanie nazw hostów za pomocą Recon-ng	125
	Host	126
	Wyszukiwanie serwerów SOA za pomocą Dig	127
	Hakowanie wirtualnego serwera nazw	129
	Skanowanie portów za pomocą narzędzia Nmap	129
	Wykopywanie informacji	131
	Wybieranie rekordów zasobów	133
	CHAOS ujawnia informacje	136
	Żądania transferu strefy	138
	Narzędzia do gromadzenia informacji	139
	Fierce	139
	Dnsrecon	140
	Dnsenum	140

Poszukiwanie podatności i exploitów	142
Searchsploit	142
Inne źródła	144
Wzmocnienie sieciowego ruchu DNS	144
Metasploit	145
Przeprowadzanie ataku DoS	149
Ataki DoS we frameworku Metasploit	150
Udawanie serwera DNS	151
Zatrucie pamięci podręcznej DNS	152
Węsenie w pamięci podręcznej DNS	154
DNSSEC	155
Rozmywanie	155
Podsumowanie	157
Rozdział 6. Poczta elektroniczna	158
Jak działa poczta?	158
Nagłówki wiadomości	160
Powiadomienia o stanie doręczenia	161
Protokół SMTP	163
Sender Policy Framework	165
Skanowanie serwera pocztowego	167
Wyniki pełnego skanowania programem Nmap (TCP)	171
Sondowanie serwisu SMTP	173
Otwarte serwery przekazujące	175
Protokół POP	176
Protokół IMAP	178
Oprogramowanie do obsługi poczty	179
Exim	180
Sendmail	180
Cyrus	181
PHP Mail	181
Webmail	182
Enumerowanie użytkowników za pomocą usługi Finger	183
Atak siłowy na serwis POP	188
Język skryptowy programu Nmap	190
CVE-2014-0160 — błąd Heartbleed	192
Wykorzystywanie błędu CVE-2010-4345	200
Udało się?	202
Poprawianie powłoki	203
Wykorzystanie błędu CVE-2017-7692	205
Podsumowanie	207

Rozdział 7.	Sieć WWW pełna podatności	209
Sieć WWW		210
Protokół HTTP		211
Metody i czasowniki HTTP		213
Kody odpowiedzi HTTP		214
Protokół bezstanowy		215
Pliki cookie		216
Adresy URI		217
LAMP: Linux, Apache, MySQL i PHP		219
Serwer WWW: Apache		220
Baza danych: MySQL		220
Skrypty po stronie serwera: PHP		221
Nginx		222
Microsoft IIS		223
Pająki i gąsienie		223
Narzędzia hakera serwerów WWW		224
Skanowanie portów serwera WWW		225
Ręczne żądania HTTP		227
Skanowanie podatności		229
Ukryte treści		233
Nmap		233
Przeszukiwanie katalogów		234
Podatności związane z przejściem po katalogach		235
Przesyłanie plików		236
WebDAV		237
Weevely, czyli sieciowa powłoka		238
Uwierzycznianie HTTP		240
Technologia CGI		241
Shellshock		243
Wykorzystywanie błędu Shellshock za pomocą Metasploita		244
Wykorzystywanie błędu Shellshock za pomocą programów cURL i Netcat		245
SSL, TLS i Heartbleed		248
Sieciowe interfejsy administracyjne		254
Apache Tomcat		254
Webmin		256
phpMyAdmin		258
Serwery proxy w sieci WWW		259
Proxychains		259
Podnoszenie uprawnień		262
Podniesienie uprawnień za pomocą ataku DirtyCOW		263
Podsumowanie		265

Rozdział 8.	Wirtualne sieci prywatne	267
	Czym jest sieć VPN?	267
	Protokół IPsec	269
	Protokół IKE	269
	Protokół TLS i sieci VPN	270
	Bazy danych i uwierzytelnianie użytkowników	271
	Baza danych SQL	271
	RADIUS	271
	LDAP	271
	PAM	272
	TACACS+	272
	Agencja NSA i sieci VPN	272
	Narzędzia hakera do pracy z sieciami VPN	273
	Metody hakowania sieci VPN	273
	Skanowanie portów serwera VPN	274
	Hping3	274
	Skanowanie portów UDP za pomocą programu Nmap	276
	Skanowanie portów IKE	277
	Wykrywanie opcji kojarzenia zabezpieczeń	278
	Tryb agresywny	280
	OpenVPN	282
	LDAP	290
	OpenVPN i Shellshock	291
	Wykorzystywanie błędu CVE-2017-5618	292
	Podsumowanie	295
Rozdział 9.	Pliki i współdzielenie plików	296
	Czym są urządzenia NAS?	297
	Uprawnienia do plików	297
	Narzędzia do hakowania urządzeń NAS	300
	Skanowanie portów serwera plików	301
	Protokół FTP	301
	Protokół TFTP	303
	Zdalne wywoływanie procedur	305
	RPCinfo	306
	Protokół SMB	307
	NetBIOS i NBT	308
	Konfigurowanie Samby	310
	Enum4Linux	311
	SambaCry (CVE-2017-7494)	315
	Rsync	317
	System NFS	319

Podniesienie uprawnień w systemie NFS	320
Poszukiwanie przydatnych plików	322
Podsumowanie	323
Rozdział 10. UNIX	324
Administrowanie systemem UNIX	324
Solaris	325
Narzędzia do hakowania systemu Unix	327
Skanowanie portów w systemie Solaris	328
Telnet	329
Secure Shell	332
RPC	334
CVE-2010-4435	336
CVE-1999-0209	337
CVE-2017-3623	338
EBBSHAVE — Święty Graal hakerów	338
Usługi R-services	345
Protokół SNMP	346
Ewok	348
System drukowania CUPS	348
System X Window	350
Usługa Cron i lokalne pliki	354
Środowisko graficzne CDE	357
EXTREMEPARR	358
Podsumowanie	359
Rozdział 11. Bazy danych	361
Typy baz danych	362
Bazy danych w zwykłych plikach	362
Relacyjne bazy danych	362
Nierelacyjne bazy danych	364
Język SQL	364
Funkcje zdefiniowane przez użytkownika	365
Zestaw narzędzi hakera baz danych	366
Typowe używanie baz danych	366
Skanowanie portów serwera baz danych	367
MySQL	368
Badanie baz MySQL	368
Uwierzytelnianie w serwerze MySQL	378
PostgreSQL	379
Ucieczka z serwera baz danych	381
Bazy danych Oracle Database	382
MongoDB	385

Redis	385
Podnoszenie uprawnień za pomocą bazy danych	387
Podsumowanie	395
Rozdział 12. Aplikacje sieciowe	397
OWASP Top 10	398
Narzędzia hakera aplikacji sieciowych	399
Skanowanie portów w serwerze aplikacji sieciowej	399
Korzystanie z przechwytyjącego serwera proxy	400
Konfigurowanie narzędzi Burp Suite Community Edition	400
Używanie programu Burp Suite z protokołem HTTPS	408
Ręczne przeglądanie stron	412
Używanie pająków	415
Wyszukiwanie punktów wejściowych	417
Skanery podatności w aplikacjach sieciowych	417
Zed Attack Proxy	418
Burp Suite Professional	419
Skipfish	419
Poszukiwanie podatności	420
Wstrzykiwanie	420
Wstrzykiwanie SQL	421
SQLmap	426
Drupageddon	431
Ochrona przed atakami wstrzykiwania poleceń SQL	431
Inne błędy wstrzykiwania poleceń	432
Niepoprawne uwierzytelnianie	432
Ujawnianie wrażliwych danych	434
Zewnętrzne encje XML	435
CVE-2014-3660	436
Niepoprawna kontrola dostępu	437
Przechodzenie przez katalogi	438
Niepoprawna konfiguracja zabezpieczeń	439
Strony błędów oraz ślady stosu	440
Cross-Site Scripting	440
Framework BeEF	443
Dodatkowe informacje o podatnościach XSS	447
Unikanie filtrów XSS	448
Niebezpieczna deserializacja	450
Znane podatności	451
Niewystarczające protokołowanie i monitorowanie	451
Podnoszenie uprawnień	452
Podsumowanie	453

Rozdział 13. Microsoft Windows	455
Czym różni się hakowanie Windows od hakowania Linuksa?	456
Domeny, drzewa i lasy	456
Użytkownicy, grupy i uprawnienia	459
Skróty haseł	460
Oprogramowanie antywirusowe	461
Omijanie funkcji Kontrola konta użytkownika	462
Konfigurowanie maszyny wirtualnej z systemem Windows	463
Narzędzia do hakowania systemów Windows	464
Windows i agencja NSA	465
Skanowanie portów systemu Windows Server	466
Microsoft DNS	467
Serwer IIS	468
Kerberos	469
Złote tokeny	470
NetBIOS	472
LDAP	472
Protokół SMB	473
ETERNALBLUE	474
Enumerowanie użytkowników	477
Microsoft RPC	486
Harmonogram zadań	493
Zdalny pulpit	493
Powłoka systemu Windows	495
PowerShell	497
Podnoszenie uprawnień w powłoce PowerShell	498
PowerSploit i AMSI	499
Meterpreter	500
Zbieranie skrótów haseł	501
Używanie skrótów haseł	502
Podnoszenie uprawnień	503
Uzyskanie uprawnień konta SYSTEM	504
Inne metody przesyłania payloadu	505
Unikanie Windows Defendera	507
Podsumowanie	510
Rozdział 14. Hasła	512
Haszowanie	512
Narzędzia do łamania haseł	514
Łamanie haseł	514
Tablice haszy i tablice tęcze	518
Dodawanie soli	519

Badanie pliku /etc/shadow	520
Inne rodzaje skrótów	524
MD5	524
SHA-1	525
SHA-2	525
bcrypt	526
CRC16 i CRC32	526
PBKDF2	526
Kolizje	527
Pseudohaszowanie	527
Haszowanie z firmą Microsoft	529
Zgadywanie haseł	531
Sztuka łamania haseł	532
Generatory liczb losowych	533
Podsumowanie	534
Rozdział 15. Pisanie raportów	536
Czym jest raport z testu penetracyjnego?	536
System CVSS	537
Wektor ataku	538
Złożoność ataku	539
Wymagane uprawnienia	539
Interakcja z użytkownikiem	539
Zakres	540
Wpływ na poufność, spójność i dostępność danych	540
Umiejętność pisania raportów	541
Co powinno znaleźć się w raporcie?	542
Podsumowanie dla dyrektorów	542
Podsumowanie techniczne	543
Ocena wyników	544
Informacje uzupełniające	544
Sporządzanie notatek	545
Dradis Community Edition	545
Sprawdzanie tekstu	549
Przekazanie raportu	550
Podsumowanie	551