

Spis treści

O autorach	9
O recenzentach	11
Wstęp	15
Co znajdziesz w tej książce?	16
Czego potrzebujesz do pracy z książką?	17
Dla kogo przeznaczona jest ta książka?	17
Konwencje	18
Errata	18
Piractwo	19
Rozdział 1. Przygotowania	21
Podstawowe założenia testów penetracyjnych aplikacji internetowych	23
Metodologia przeprowadzania testów penetracyjnych	24
Ocena ryzyka	30
Testy penetracyjne z wykorzystaniem systemu Kali Linux — założenia	34
Etap 1. Rekonesans	34
Etap 2. Wyszukiwanie podatności	35
Etap 3. Wykorzystywanie zidentyfikowanych podatności	36
Etap 4. Podnoszenie uprawnień	37
Etap 5. Utrzymanie zdobytego przyczółka	37
Wprowadzenie do systemu Kali Linux	38
Konfiguracja systemu Kali Linux	39
Uruchamianie systemu Kali Linux z nośnika zewnętrznego	39
Instalowanie systemu Kali Linux	40
Kali Linux i pierwsze uruchomienie w maszynie wirtualnej	46
Przegląd narzędzi dostępnych w systemie Kali Linux	46
Podsumowanie	49

Rozdział 2. Rekonesans	51
Zadania rekonesansu	52
Rozpoznanie wstępne	53
Strona internetowa firmy	53
Źródła przechowujące historyczne wersje witryn internetowych	54
Regional Internet Registries, czyli regionalni administratorzy adresów IP	57
System EDGAR	57
Zasoby serwisów społecznościowych	58
Zaufanie	59
Oferty pracy	59
Lokalizacja	60
Wyszukiwarka Shodan	60
Google hacking	61
GHDB, czyli Google Hacking Database	63
Badanie zasobów sieci komputerowych	65
Rekonesans z wykorzystaniem protokołu ICMP	69
Rekonesans z wykorzystaniem serwerów DNS	71
Nmap	76
FOCA — wyszukiwanie i analiza metadanych	83
Podsumowanie	89
Rozdział 3. Ataki na serwery aplikacji internetowych	91
Wyszukiwanie podatności i luk w zabezpieczeniach	92
Webshag	92
Skipfish	95
ProxyStrike	98
Vega	101
Owasp-Zap	105
Websploit	112
Wykorzystywanie znalezionych luk w zabezpieczeniach (exploity)	113
Metasploit	113
w3af	120
Wykorzystywanie luk w zabezpieczeniach systemów poczty elektronicznej	123
Ataki typu brute-force	125
Hydra	125
DirBuster	128
WebSlayer	131
Łamanie haseł	137
John the Ripper	137
Ataki typu man-in-the-middle	139
SSLStrip	140
Podsumowanie	145

Rozdział 4. Ataki na klienty aplikacji internetowych	147
Inżynieria społeczna	148
Pakiet SET — Social Engineer Toolkit	149
Zastosowanie pakietu SET do ataku z klonowaniem	151
MitM Proxy	161
Skanowanie hostów	162
Skanowanie hostów za pomocą pakietu Nessus	162
Przechwytywanie i łamanie haseł użytkowników	169
Hasła w systemie Windows	171
Hasła w systemie Linux	173
Narzędzia do łamania haseł dostępne w systemie Kali Linux	174
Johnny	174
Programy hashcat i oclHashcat	177
samdump2	178
chntpw	180
Ophcrack	183
Crunch	185
Inne narzędzia dostępne w systemie Kali Linux	188
Hash-identifier	188
dictstat	189
RainbowCrack (rccrack_mt)	189
findmyhash	190
phrasendrescher	190
CmosPwd	190
creddump	191
Podsumowanie	191
Rozdział 5. Ataki na metody uwierzytelniania	193
Ataki na zarządzanie sesjami	195
Clickjacking	196
Przechwytywanie ciasteczek sesji	197
Narzędzia do przechwytywania sesji	198
Wtyczki przeglądarki Firefox	198
Cookie Cadger	203
Wireshark	206
Pakiety Hamster i Ferret	208
Atak typu man-in-the-middle	211
Narzędzia dsniff i arpspoof	212
Ettercap	214
Driftnet	217
Wstrzykiwanie kodu SQL	218
sqlmap	221
Ataki typu XSS (cross-site scripting)	223
Testowanie podatności na ataki XSS	224
Techniki XSS cookie stealing i Authentication hijacking	225

Inne narzędzia	227
urlsnarf	227
acccheck	228
hexinject	228
Patator	229
DBPwAudit	229
Podsumowanie	229
Rozdział 6. Ataki na aplikacje internetowe i serwery WWW	231
BeEF — Browser Exploitation Framework	232
FoxyProxy — wtyczka przeglądarki Firefox	236
BURP Proxy	238
OWASP-ZAP	245
Przechwytywanie haseł — pakiet SET	249
Fimap	254
Ataki typu DoS	255
THX-SSL-DOS	257
Scapy	259
Slowloris	261
LOIC, czyli Niskoorbitalne Działo Jonowe...	263
Inne narzędzia	266
DNSChef	266
SniffJoke	267
Siege	268
Inundator	269
TCPReplay	270
Podsumowanie	270
Rozdział 7. Przeciwdziałanie i zapobieganie	271
Testowanie mechanizmów obronnych	273
Podstawowe wymogi bezpieczeństwa	273
STIG	274
Zarządzanie aktualizacjami i poprawkami zabezpieczeń	275
Polityka zarządzania hasłami	277
Klonowanie środowiska	278
HTTrack	279
Inne narzędzia do klonowania witryn	281
Obrona przed atakami typu man-in-the-middle	281
Obrona przed atakami SSLstrip	284
Obrona przed atakami typu DoS	285
Obrona przed przechwytywaniem ciasteczek	286
Obrona przed atakami typu Clickjacking	287
Informatyka śledcza	287
Uruchamianie systemu Kali Linux w trybie Forensics	290
Analiza systemu plików za pomocą narzędzi systemu Kali Linux	291
Inne narzędzia śledcze w systemie Kali Linux	295
Podsumowanie	300

Rozdział 8. Tworzenie raportów końcowych	301
Zgodność ze standardami i procedurami	303
Usługi profesjonalne	304
Dokumentacja	306
Format raportu	307
Strona tytułowa	307
Oświadczenie o zachowaniu poufności	307
Zarządzanie wersjami dokumentacji	308
Ramy czasowe projektu	308
Streszczenie raportu	309
Metodologia	310
Szczegółowe procedury testowania	312
Podsumowanie ustaleń	313
Podatności i luki w zabezpieczeniach	315
Wnioski i rekomendacje dla środowiska sieciowego	316
Dodatki	319
Glosariusz	319
Wykaz prac	319
Zewnętrzne testy penetracyjne	321
Dodatkowe elementy wykazu prac	323
Narzędzia wspomagające tworzenie raportów	325
Dradis	325
KeepNote	326
Maltego CaseFile	326
MagicTree	327
CutyCapt	327
Podsumowanie	327
Skorowidz	329