



Spis treści

O autorze	17
O korektorze merytorycznym	18
Podziękowania	19
Wstęp	20
Rozdział 1. Praca z oknem terminala	25
System plików w Kali Linux	26
Podstawowe polecenia okna terminala	27
Okno terminala Tmux	30
Uruchamianie terminala Tmux	30
Skróty klawiszowe w oknie terminala Tmux	30
Zarządzanie sesjami terminala Tmux	31
Nawigacja wewnątrz okna terminala Tmux	32
Opis poleceń terminala Tmux	33
Zarządzanie użytkownikami i grupami w systemie Kali Linux	33
Polecenia związane z zarządzaniem użytkownikami	34
Polecenia związane z zarządzaniem grupami	37
Zarządzanie hasłami w systemie Kali Linux	37

Zarządzanie plikami i katalogami w systemie Kali Linux	38
Wyświetlanie plików i folderów	38
Prawa dostępu	40
Operacje na plikach w systemie Kali Linux	41
Wyszukiwanie plików	42
Kompresowanie plików	44
Operowanie na katalogach w systemie Kali Linux	45
Montowanie katalogów	45
Praca z plikami tekstowymi w systemie Kali Linux	46
Edytor vim kontra nano	48
Wyszukiwanie i filtrowanie tekstu	49
Połączenia z systemami zdalnymi	50
Protokół RDP	51
Secure Shell	51
Połączenie SSH z danymi uwierzytelniającymi	52
Połączenia SSH bez używania hasła	53
Zarządzanie systemem Kali Linux	56
Informacje o nazwie hosta systemu Linux	58
Informacje o systemie operacyjnym Linux	58
Informacje o sprzęcie	58
Zarządzanie usługami	60
Zarządzanie pakietami	61
Zarządzanie procesami	62
Połączenia sieciowe w systemie Kali Linux	63
Interfejs sieciowy	63
Zakresy adresów prywatnych IPv4	64
Statyczne adresy IP	65
DNS	66
Wyświetlanie listy aktywnych połączeń	67
Przesyłanie plików	68
Podsumowanie	69
Rozdział 2. Skrypty powłoki bash	70
Tworzenie prostych skryptów powłoki bash	71
Wyświetlanie informacji i danych na ekranie	71
Zmienne	73
Zmienne zawierające polecenia	74
Parametry wywołania skryptów	75
Dane wejściowe wprowadzane przez użytkownika	76
Funkcje	77

Instrukcje warunkowe i pętle	77
Instrukcje warunkowe	79
Pętle	80
Iteracje po plikach	81
Podsumowanie	83
Rozdział 3. Skanowanie hostów sieciowych	84
Podstawy działania sieci	84
Protokoły sieciowe	85
TCP	85
UDP	86
Inne protokoły sieciowe	86
Adresowanie IP	88
IPv4	88
Podsieci i notacja CIDR	88
IPv6	89
Numery portów	90
Skanowanie sieci	90
Identyfikacja aktywnych hostów w sieci	90
Ping	90
ARP	91
Nmap	92
Skanowanie portów i identyfikacja usług	93
Skanowanie portów — TCP SYN Scan	93
Skanowanie portów — UDP Scan	93
Podstawy skanowania z użyciem programu Nmap	94
Identyfikacja usług	95
OS Fingerprinting — identyfikacja systemu operacyjnego	97
Silnik skryptowy skanera Nmap	98
NSE Category Scan	99
Argumenty wywołania skryptów NSE	101
Wyliczanie DNS	101
DNS brute force	102
Transfer stref DNS	103
Narzędzia do wyszukiwania subdomen DNS	103
Pakiet Fierce	104
Podsumowanie	104

Rozdział 4.	Zbieranie informacji z internetu	105
	Pasywne zbieranie informacji i rekonesans	106
	Wyszukiwarki internetowe	107
	Wyszukiwarka Shodan	107
	Zapytania Google	108
	Zbieranie informacji przy użyciu systemu Kali Linux	110
	Baza danych Whois	111
	TheHarvester	112
	DMitry	114
	Maltego	114
	Podsumowanie	118
Rozdział 5.	Ataki socjotechniczne	119
	Ataki typu spear phishing	119
	Wysyłanie wiadomości e-mail	120
	Pakiet SET	120
	Wysyłanie wiadomości e-mail przy użyciu języka Python	122
	Kradzież poświadczeń	123
	Ładunki i procesy nasłuchujące	124
	Czym się różni powłoka Bind Shell od Reverse Shell	124
	Powłoka dowiązana (Bind Shell)	125
	Powłoka odwrócona (Reverse Shell)	126
	Tworzenie połączenia typu Reverse Shell za pomocą pakietu SET	127
	Ataki socjotechniczne z wykorzystaniem klucza USB Rubber Ducky	129
	Praktyczny przykład nawiązania połączenia Reverse Shell z wykorzystaniem klucza USB Rubber Ducky i powłoki PowerShell	131
	Generowanie skryptu powłoki PowerShell	132
	Uruchamianie listenera	132
	Hostowanie skryptu powłoki PowerShell	132
	Uruchomienie powłoki PowerShell	133
	Pobieranie i uruchamianie skryptu powłoki PowerShell	134
	Odwrócona powłoka	135
	Replikacja ataku przy użyciu klucza USB Rubber Ducky	135
	Podsumowanie	135
Rozdział 6.	Zaawansowane wyszukiwanie usług sieciowych	137
	Protokoły przesyłania plików	138
	FTP (port 21)	138
	Scenariusze ataków na serwer FTP	138
	Jak wyszukiwać działające usługi sieciowe?	139
	Skanowanie w poszukiwaniu usług	139

Zaawansowane skanowanie z wykorzystaniem skryptów Nmapa	140
Inne rodzaje ataków typu brute force	141
SSH (port 22)	142
Scenariusze ataków na serwer SSH	142
Zaawansowane skanowanie z wykorzystaniem skryptów Nmapa	142
Atak brute force na SSH za pomocą pakietu Hydra	143
Zaawansowane ataki typu brute force	144
Telnet (port 23)	145
Scenariusze ataków na serwer Telnet	146
Wykrywanie i identyfikacja usługi telnet	146
Skanowanie w poszukiwaniu usługi	146
Zaawansowane skanowanie z wykorzystaniem skryptów Nmapa	146
Atak brute force za pomocą pakietu Hydra	147
Protokoły poczty elektronicznej	147
Protokół SMTP (port 25)	147
Podstawowe skanowanie Nmapem	148
Zaawansowane skanowanie z użyciem skryptów Nmapa	148
Wyliczanie użytkowników	148
Protokoły POP3 (Port 110) i IMAP4 (Port 143)	151
Atak brute force na konta e-mail POP3	152
Protokoły baz danych	152
Microsoft SQL Server (port 1433)	152
Serwer bazy danych Oracle (port 1521)	153
Baza danych MySQL (port 3306)	153
Protokoły CI/CD	153
Docker (port 2375)	154
Jenkins (Port 8080/50000)	155
Atak brute force na portal WWW przy użyciu Hydry	157
Krok 1 — ustaw proxy	158
Krok 2 — przechwytywanie żądania logowania	159
Krok 3 — wyciąganie danych z formularza i atak brute force za pomocą Hydry	159
Protokoły sieciowe na portach 80/443	161
Protokoły wykorzystywane do zdalnych połączeń GUI	161
RDP (port 3389)	161
Atak typu brute force na usługę RDP	162
VNC (Port 5900)	162
Protokoły współdzielenia plików	163
SMB (port 445)	163
Atak typu brute force na SMB	165
SNMP (port UDP 161)	166
Wyliczanie SNMP	166
Podsumowanie	167

Rozdział 7. Faza eksploracji	168
Ocena podatności	169
Przebieg procesu oceny podatności	169
Skanowanie podatności za pomocą pakietu OpenVAS	171
Instalacja pakietu OpenVAS	171
Skanowanie przy użyciu OpenVAS	172
Wyszukiwanie exploitów	176
SearchSploit	178
Wykorzystywanie podatności i luk w zabezpieczeniach usług	179
Wykorzystywanie podatności usługi FTP	179
Logowanie do serwera FTP	180
Zdalne wykonanie kodu	181
Wywoływanie sesji powłoki	183
Wykorzystywanie podatności usługi SSH	184
Logowanie do SSH	184
Wykorzystywanie podatności usługi Telnet	185
Logowanie przez telnet	185
Wyszukiwanie informacji przesyłanych otwartym tekstem	186
Wykorzystywanie podatności serwera poczty elektronicznej	189
Wykorzystywanie podatności Dockera	191
Testowanie połączenia z Dockerem	192
Tworzenie nowego zdalnego kontenera Kali	192
Uruchamianie powłoki w kontenerze Kali	193
Wykorzystywanie podatności hosta Docker	193
Wykorzystywanie podatności Jenkinsa	195
Odwrócone powłoki	198
Wykorzystanie powłok z pakietu Metasploit	199
Wykorzystywanie podatności protokołu SMB	201
Uzyskiwanie dostępu do udziałów SMB	201
Exploit SMB Eternal Blue	202
Podsumowanie	202
Rozdział 8. Podatności i luki w zabezpieczeniach aplikacji internetowych	203
Podatności w aplikacjach internetowych	204
Instalacja pakietu Mutillidae	204
Instalacja serwera WWW Apache	204
Konfiguracja zapory sieciowej	205
Instalacja PHP	205
Instalacja i konfiguracja bazy danych	205
Instalacja pakietu Mutillidae	206

Podatności typu XSS (Cross-Site Scripting)	206
Podatność typu Reflected XSS	207
Podatność typu Stored XSS	208
Wykorzystywanie podatności XSS przy użyciu nagłówka	209
Omijanie walidacji w skryptach JavaScript	210
Wstrzykiwanie kodu SQL	212
Zapytania do bazy danych	212
Obchodzenie strony logowania	214
Wykonywanie poleceń w bazie danych za pomocą SQLi	216
Automatyzacja wstrzykiwania kodu SQL za pomocą programu SQLMap	219
Testowanie podatności na ataki SQL Injection	219
Wstrzykiwanie poleceń	220
Podatność na dołączanie plików	221
LFI — dołączanie plików lokalnych	221
RFI — dołączanie plików zdalnych	222
Podatności typu CSRF	224
Przebieg ataku z punktu widzenia napastnika	224
Przebieg ataku z punktu widzenia ofiary	226
Przesyłanie plików	226
Proste przesyłanie plików	227
Omijanie walidacji	228
Kodowanie	231
Lista OWASP Top 10	231
Podsumowanie	232

Rozdział 9. Testy penetracyjne aplikacji sieciowych i cykl tworzenia bezpiecznego oprogramowania	233
Wyszukiwanie i wykorzystywanie podatności aplikacji sieciowych	234
Burp Suite Pro	234
Testy penetracyjne aplikacji sieciowych z użyciem pakietu Burp Suite	234
Jeszcze więcej wyliczania	248
Nmap	248
Crawling	248
Ocena podatności na zagrożenia	249
Lista kontrolna wspomagająca przeprowadzanie testów penetracyjnych aplikacji sieciowych	250
Wspólna lista kontrolna	250
Lista kontrolna dla stron specjalnych	251
SDLC — cykl tworzenia i rozwoju bezpiecznego oprogramowania	252
Faza analizy i planowania	253
Modelowanie zagrożeń aplikacji	253
Aktywa	253

Punkty wejścia	254
Elementy i podmioty trzecie	254
Poziomy zaufania	254
Diagram przepływu danych	254
Faza tworzenia/rozwoju	255
Faza testowania	256
Wdrożenie w środowisku produkcyjnym	256
Podsumowanie	257
Rozdział 10. Eskalacja uprawnień w systemie Linux	258
Wprowadzenie do exploitów jądra systemu i błędów w konfiguracji	259
Exploity jądra systemu	259
Exploit jądra — Dirty Cow	259
Wykorzystywanie uprawnień SUID	262
Nadpisywanie pliku passwd	263
CRON — eskalacja uprawnień zadań	265
Podstawy CRON	265
Crontab	265
Anacrontab	266
Wyliczanie zadań i wykorzystywanie podatności CRON-a	266
Plik sudoers	268
Eskalacja uprawnień z wykorzystaniem sudo	268
Wykorzystanie polecenia Find	268
Edycja pliku sudoers	269
Wykorzystywanie działających usług	269
Zautomatyzowane skrypty	270
Podsumowanie	271
Rozdział 11. Eskalacja uprawnień w systemie Windows	272
Pozyskiwanie informacji o systemie Windows	273
Informacje o systemie	273
Architektura systemu Windows	274
Wyświetlanie listy napędów dyskowych	274
Lista zainstalowanych aktualizacji	275
Whoami, czyli kim jestem?	275
Lista użytkowników i grup	275
Informacje o sieci	278
Wyświetlanie niepoprawnych (słabych) uprawnień	280
Wyświetlanie listy zainstalowanych programów	280
Wyświetlanie listy zadań i procesów	281

Przesyłanie plików	281
Cel — komputer z systemem Windows	282
Cel — komputer z systemem Linux	282
Wykorzystywanie podatności i luk w zabezpieczeniach systemu Windows	283
Exploity dla jądra systemu Windows	284
Sprawdzanie wersji systemu operacyjnego	285
Wyszukiwanie odpowiedniego exploita	285
Uruchamianie exploita i uzyskanie powłoki na prawach administratora	286
Eskalacja uprawnień — magia Metasploita	286
Wykorzystywanie podatności i luk w zabezpieczeniach aplikacji Windows	289
Uruchamianie poleceń w kontekście innego użytkownika systemu Windows	292
Program PSEXec	292
Wykorzystywanie podatności i luk w zabezpieczeniach usług w systemie Windows	293
Interakcja z usługami Windows	293
Nieprawidłowo skonfigurowane uprawnienia usług	294
Nadpisywanie pliku wykonywalnego usługi	295
Niepoprawnie skonfigurowana ścieżka usługi	295
Nieprawidłowe uprawnienia w rejestrze	297
Wykorzystywanie podatności i luk w zabezpieczeniach zaplanowanych zadań	297
Zautomatyzowane narzędzia wspomagające eskalację uprawnień	298
PowerUp	298
WinPEAS	299
Podsumowanie	299
Rozdział 12. Pivoting i ruch poprzeczny	300
Wyodrębnianie skrótów haseł w systemie Windows	301
Skróty NTLM haseł w systemie Windows	301
Plik SAM i wyodrębnianie skrótów haseł	302
Korzystanie ze skrótów haseł	303
Mimikatz	303
Pobieranie skrótów haseł z Active Directory	304
Ponowne wykorzystanie haseł i ich skrótów	305
Atak z przekazywaniem skrótu hasła	306
Pivoting z przekierowywaniem portów	306
Koncepcje przekierowywania portów	307
Tunelowanie SSH i lokalne przekierowywanie portów	308
Przekierowywanie portów zdalnych przy użyciu SSH	309
Dynamiczne przekierowywanie portów	310
Dynamiczne przekierowywanie portów przy użyciu SSH	310
Podsumowanie	311

Rozdział 13. Kryptografia i łamanie skrótów haseł	312
Podstawy kryptografii	312
Podstawy haszowania	313
Jednokierunkowe funkcje skrótu	313
Zastosowania funkcji skrótu	314
Algorytmy haszujące	314
Algorytm MD5	314
Algorytm SHA	316
Haszowanie haseł	316
Zabezpieczanie haseł za pomocą haszowania	317
Algorytm HMAC	318
Podstawy szyfrowania	319
Szyfrowanie symetryczne	319
Algorytm AES	319
Szyfrowanie asymetryczne	321
Algorytm RSA	322
Łamanie haseł za pomocą programu Hashcat	324
Testowanie wydajności	324
Łamanie haszy w praktyce	326
Tryby ataku	328
Tryb prosty	328
Atak kombinatoryczny	329
Maski i ataki typu brute force	330
Ataki typu brute force	333
Ataki hybrydowe	333
Łamanie skrótów — jak to wygląda w praktyce	334
Podsumowanie	334
 Rozdział 14. Raportowanie	 335
Znaczenie raportów w testach penetracyjnych	335
Ocena poziomu krytyczności podatności i luk w zabezpieczeniach	336
CVSS v3.1 — otwarty system oceny podatności na zagrożenia	336
Prezentacja raportu	340
Strona tytułowa	340
Dzienniki zmian	340
Podsumowanie raportu	341
Sekcja podatności	341
Podsumowanie	341

Rozdział 15. Język assembler i inżynieria odwrotna	342
Rejestry procesora	342
Rejestry ogólnego przeznaczenia	343
Rejestry indeksowe	344
Rejestry wskaźnikowe	344
Rejestry segmentów	345
Rejestr flag	345
Instrukcje języka assembler	347
Kolejność bajtów — little endian	349
Typy danych	349
Segmenty pamięci	350
Tryby adresowania	350
Przykład inżynierii odwrotnej	351
Pakiet Visual Studio Code dla języka C/C++	351
Pakiet Immunity Debugger do inżynierii odwrotnej	352
Podsumowanie	357
 Rozdział 16. Przepełnienia bufora i stosu	 358
Jak działa przepełnienie stosu?	358
Jak działa stos?	358
Instrukcja PUSH	359
Instrukcja POP	359
Przykład programu w języku C	360
Analiza bufora za pomocą programu Immunity Debugger	360
Przepełnienie stosu	364
Mechanizm przepełnienia stosu	365
Wykorzystywanie podatności na przepełnienie stosu	367
Wyposażenie naszego laboratorium	367
Aplikacja podatna na przepełnienie bufora	367
Faza 1. Testowanie	367
Testowanie szczęśliwej ścieżki	368
Testowanie awarii serwera	369
Faza 2. Rozmiar bufora	369
Tworzenie wzorca	370
Lokalizacja przesunięcia	370
Faza 3. Sterowanie wskaźnikiem EIP	371
Dodawanie instrukcji JMP	373
Faza 4. Wstrzyknięcie ładunku i uzyskanie zdalnej powłoki	373
Generowanie ładunku	374
Niepoprawne znaki	374
Shellcode w skrypcie Pythona	375
Podsumowanie	376

Rozdział 17. Programowanie w języku Python	377
Podstawy języka Python	377
Uruchamianie skryptów języka Python	378
Debugowanie skryptów w języku Python	379
Instalowanie pakietu Visual Studio Code w systemie Kali Linux	379
Programowanie w języku Python	380
Podstawowa składnia poleceń języka Python	381
Wiersz shebang w języku Python	381
Komentarze w języku Python	381
Wcięcia wierszy i importowanie modułów	382
Wprowadzanie danych i wyświetlanie informacji na ekranie	382
Wyświetlanie argumentów przekazanych w wierszu wywołania	383
Zmienne	383
Zmienne numeryczne	383
Operatory arytmetyczne	384
Ciągi znaków	385
Formatowanie ciągów znaków	385
Funkcje tekstowe	385
Listy	387
Odczytywanie wartości z listy	387
Aktualizowanie elementów listy	387
Usuwanie elementów listy	387
Krotki	387
Słowniki	388
Inne techniki programowania w języku Python	388
Funkcje	388
Zwracanie wartości	389
Argumenty opcjonalne	389
Zmienne globalne	389
Zmiana wartości zmiennych globalnych	389
Instrukcje warunkowe	390
Instrukcja if-else	390
Operatory porównania	391
Pętle	391
Pętla while	391
Pętla for	392
Zarządzanie plikami	392
Obsługa wyjątków	393
Znaki specjalne	394
Niestandardowe obiekty w języku Python	394
Podsumowanie	395

Rozdział 18. Automatyzacja testów penetracyjnych za pomocą Pythona	396
Program Pentest Robot	396
Sposób działania aplikacji	397
Pakiety dla języka Python	398
Uruchamianie aplikacji	399
Walidacja danych wejściowych	399
Refaktoryzacja kodu	401
Skanowanie w poszukiwaniu aktywnych hostów	402
Skanowanie portów i usług	403
Atak na dane uwierzytelniające i zapisywanie wyników działania	406
Podsumowanie	409
 Dodatek A Kali Linux Desktop w skrócie	 410
Pobieranie i uruchamianie maszyny wirtualnej z systemem Kali Linux	411
Pierwsze uruchomienie maszyny wirtualnej	411
Pulpit środowiska Xfce w systemie Kali Linux	412
Menu interfejsu graficznego Xfce w systemie Kali Linux	413
Pasek wyszukiwania	414
Menu Favorites	414
Menu Usual Applications	415
Inne polecenia menu	416
Menedżer ustawień środowiska Xfce	417
Zaawansowana konfiguracja ustawień sieci	417
Okno Appearance	418
Okno Desktop	421
Okno Display	424
File Manager	425
Okno Keyboard	428
Okno MIME Type Editor	429
Okno Mouse and Touchpad	430
Panel górny	431
Okno Workspaces	433
Okno Window Manager	433
Praktyczny przykład dostosowywania pulpitu do własnych potrzeb	435
Edycja górnego panelu	435
Dodawanie nowego panelu dolnego	437
Zmiana wyglądu pulpitu	439
Instalowanie systemu Kali Linux od podstaw	441
Podsumowanie	447

Dodatek B	Tworzenie środowiska laboratoryjnego przy użyciu Dockera	448
	Technologia Docker	449
	Podstawy pracy z Dockerem	449
	Instalacja Dockera	449
	Obrazy i rejestry obrazów	451
	Kontenery	451
	Dockerfile	453
	Woluminy	453
	Praca w sieci	454
	Kontener Mutillidae	454
	Podsumowanie	456
	 Skorowidz	 457