

Spis treści

O autorze	15
O recenzentach	16
Wstęp	17
CZĘŚĆ 1. Wprowadzenie do testów penetracyjnych	
Rozdział 1	
Wstęp do etycznego hakowania	25
Identyfikacja złośliwych aktorów i ich zamierzeń	26
Co ma znaczenie dla złośliwych aktorów	29
Czas	29
Zasoby	29
Czynniki finansowe	30
Wartość hakowania	30
Terminologia związana z cyberbezpieczeństwem	30
Dlaczego trzeba przeprowadzać testy penetracyjne i na jakie etapy można je podzielić	33
Tworzenie planu bitwy testu penetracyjnego	34
Podejścia stosowane w testach penetracyjnych	38
Rodzaje testów penetracyjnych	39
Etapy hakowania	41
Rekonesans, czyli zbieranie informacji	42
Skanowanie i enumeracja	42
Uzyskanie dostępu	43
Utrzymanie dostępu	43
Zacieranie śladów	44
Platforma Cyber Kill Chain	44
Rekonesans	45
Zbrojenia	46

Dostarczanie	46
Eksploatacja	48
Instalacja	48
Połączenia Command and Control (C2)	48
Działanie	49
Podsumowanie	49
Dalsza lektura	50

Rozdział 2

Tworzenie laboratorium do testów penetracyjnych	51
Wymagania techniczne	52
Ogólny opis laboratorium i wykorzystywanych w nim technologii	52
Konfiguracja hipernadzorcy i odizolowanych sieci wirtualnych	54
Część 1. Wdrażanie hipernadzorcy	55
Część 2. Tworzenie odizolowanych sieci wirtualnych	56
Konfiguracja systemu Kali Linux i praca w nim	57
Część 1. Konfiguracja systemu Kali Linux na maszynie wirtualnej	57
Część 2. Dostosowanie maszyny wirtualnej z systemem Kali Linux oraz kart sieciowych	60
Część 3. Początki pracy w systemie Kali Linux	64
Część 4. Aktualizowanie źródeł i pakietów	66
Wdrażanie podatnego na atak systemu Metasploitable 2	68
Część 1. Wdrażanie systemu Metasploitable 2	68
Część 2. Konfigurowanie ustawień sieciowych	70
Implementacja systemu Metasploitable 3 za pomocą Vagranta	72
Część 1. Konfigurowanie wersji dla systemu Windows	72
Część 2. Konfiguracja wersji dla Linuksa	75
Konfigurowanie systemów z aplikacjami WWW podatnymi na ataki	77
Część 1. Wdrażanie projektu OWASP Juice Shop	78
Część 2. Konfigurowanie projektu OWASP Broken Web Applications	82
Podsumowanie	84
Dalsza lektura	85

Rozdział 3

Konfiguracja dla zaawansowanych technik hakerskich	86
Wymagania techniczne	86
Budowanie laboratorium AD czerwonego zespołu	87
Część 1. Instalowanie systemu Windows Server 2019	89
Część 2. Instalowanie systemu Windows 10 Enterprise	93
Część 3. Konfigurowanie usług AD	95
Część 4. Podnoszenie do poziomu kontrolera domeny	96

Część 5. Tworzenie kont użytkowników i administratora domeny	98
Część 6. Wyłączanie ochrony przed złośliwym oprogramowaniem oraz zapory sieciowej domeny	99
Część 7. Konfiguracja przygotowująca do ataków na mechanizmy udostępniania plików i uwierzytelniania	101
Część 8. Przyłączanie klientów do domeny AD	103
Część 9. Konfiguracja na potrzeby przejścia lokalnego konta i ataków SMB	104
Konfigurowanie laboratorium do bezprzewodowych testów penetracyjnych	105
Implementowanie serwera RADIUS	107
Podsumowanie	115
Dalsza lektura	116

CZĘŚĆ 2. Rekonesans i testy penetracyjne sieci

Rozdział 4

Rekonesans i footprinting	119
Wymagania techniczne	119
Znaczenie rekonesansu	120
Footprinting	120
Pasywne zbieranie informacji	122
Oprogramowanie wywiadowcze open source	122
Strategie OSINT w zbieraniu danych wywiadowczych	123
Znaczenie pacynki	124
Anonimizacja ruchu sieciowego	125
Profilowanie infrastruktury IT docelowej organizacji	133
Pozyskiwanie danych pracowników	136
Rekonesans w mediach społecznościowych	149
Zbieranie danych o infrastrukturze organizacji	153
Podsumowanie	165
Dalsza lektura	165

Rozdział 5

Aktywne zbieranie informacji	166
Wymagania techniczne	167
Zasady aktywnego rekonesansu	167
Przegląd strategii Google hacking	168
Rekonesans DNS	174
Enumerowanie DNS	177
Sprawdzanie błędnej konfiguracji transferu stref DNS	178
Automatyzacja zbierania danych OSINT	181

Enumerowanie subdomen	186
Korzystanie z programu DNSmap	186
Używanie programu Sublist3r	187
Profilowanie witryn WWW za pomocą programu EyeWitness	189
Korzystanie z technik aktywnego skanowania	190
Spoofing adresów MAC	192
Wykrywanie systemów uruchomionych w sieci	193
Sondowanie otwartych portów usług, uruchomionych usług i systemów operacyjnych	196
Unikanie wykrycia	199
Enumerowanie popularnych usług sieciowych	203
Skanowanie za pomocą platformy Metasploit	204
Enumerowanie usługi SMB	205
Enumerowanie usługi SSH	208
Enumerowanie użytkowników poprzez hakaśliwe uwierzytelnianie	209
Znajdowanie wycieków danych w chmurze	212
Podsumowanie	216
Dalsza lektura	217
Rozdział 6	
Ocena podatności	218
Wymagania techniczne	218
Nessus i jego zasady	219
Konfiguracja Nessusa	219
Skanowanie za pomocą Nessusa	223
Analiza wyników Nessusa	225
Eksportowanie wyników Nessusa	230
Wykrywanie podatności programem Nmap	232
Korzystanie z programu Greenbone Vulnerability Manager	236
Używanie skanerów aplikacji internetowych	242
WhatWeb	242
Nmap	243
Metasploit	244
Nikto	247
WPScan	248
Podsumowanie	249
Dalsza lektura	250

Rozdział 7

Testy penetracyjne sieci	251
Wymagania techniczne	251
Wprowadzenie do testów penetracyjnych sieci	252
Korzystanie z technologii bind shell i reverse shell	255
Zdalna powłoka z użyciem Netcata	257
Tworzenie powłoki bind shell	259
Konfiguracja mechanizmu reverse shell	261
Techniki omijania zabezpieczeń antywirusowych	262
Kodowanie ładunków programem MSFvenom	263
Tworzenie ładunków programem Shellter	266
Obsługa bezprzewodowych kart sieciowych	272
Łączenie bezprzewodowej karty sieciowej z systemem Kali Linux	274
Podłączanie bezprzewodowej karty sieciowej z mikroukładem RTL8812AU	277
Zarządzanie trybami bezprzewodowymi i monitorowanie ich	280
Ręczne konfigurowanie trybu monitorowania	280
Włączanie trybu monitorowania za pomocą pakietu Aircrack-ng	283
Podsumowanie	285
Dalsza lektura	286

Rozdział 8

Przeprowadzanie testów penetracyjnych sieci	287
Wymagania techniczne	288
Wykrywanie działających systemów	288
Profilowanie systemu docelowego	291
Ataki z wykorzystaniem haseł	293
Wykorzystanie protokołu Remote Desktop Protocol w systemie Windows	295
Tworzenie listy haseł na podstawie słów kluczowych	297
Tworzenie list słów z użyciem programu Crunch	299
Znajdowanie i wykorzystywanie podatnych usług	299
Wykorzystywanie podatnej usługi w systemie Linux	299
Wykorzystanie usługi SMB w systemie Microsoft Windows	303
Przekazywanie wartości skrótów	314
Uzyskiwanie dostępu za pośrednictwem usługi SSH	318
Wykorzystanie protokołu Windows Remote Management	321
Wykorzystywanie luk w usłudze Elasticsearch	325
Wykorzystywanie protokołu Simple Network Management Protocol	326
Ataki z wykorzystaniem taktyki wodopoju	328
Podsumowanie	329
Dalsza lektura	330

CZĘŚĆ 3. Techniki czerwonego zespołu

Rozdział 9

Zaawansowane testy penetracyjne sieci — posteksploatacja	333
Wymagania techniczne	334
Posteksploatacja za pomocą programu Meterpreter	334
Główne operacje	335
Operacje w interfejsie użytkownika	338
Przesyłanie plików	339
Eskalacja uprawnień	341
Kradzież tokenów i podszywanie się	342
Utrwalanie dostępu	345
Eskalacja pozioma i używanie hosta pośredniczącego	349
Zacieranie śladów	353
Kodowanie i eksfiltracja danych	354
Kodowanie plików wykonywalnych za pomocą programu exe2hex	354
Eksfiltracja danych za pomocą programu PacketWhisper	357
Ataki MITM i przechwytywanie pakietów	364
Przeprowadzanie ataków MITM za pomocą programu Ettercap	367
Podsumowanie	369
Dalsza lektura	369

Rozdział 10

Ataki na usługę Active Directory	371
Wymagania techniczne	371
Czym jest usługa Active Directory	372
Enumerowanie Active Directory	376
Korzystanie z programu PowerView	378
Korzystanie z programu Bloodhound	387
Wykorzystanie relacji zaufania w sieci	392
Wykorzystywanie protokołów LLMNR i NetBIOS-NS	393
Wykorzystywanie zaufania między protokołem SMB a NTLMv2 w usłudze Active Directory	399
Podsumowanie	406
Dalsza lektura	407

Rozdział 11

Zaawansowane ataki na Active Directory	408
Wymagania techniczne	408
Zasady działania Kerberos'a	409

Wykorzystanie zaufania w sieci IPv6 w usłudze Active Directory	411
Część 1. Konfiguracja potrzebna do ataku	412
Część 2. Uruchamianie ataku	414
Część 3. Przejmowanie kontroli nad domeną	417
Atakowanie Active Directory	418
Eskalacja pozioma za pomocą programu CrackMapExec	418
Eskalacja pionowa z wykorzystaniem Kerberosa	421
Eskalacja pozioma za pomocą programu Mimikatz	423
Przejmowanie kontroli nad domeną i trwała obecność	427
Złoty bilet	428
Srebrny bilet	431
Klucz szkieletowy	433
Podsumowanie	436
Dalsza lektura	437
Rozdział 12	
Taktyki Command and Control	438
Wymagania techniczne	438
Zasady operacji C2	439
Konfigurowanie operacji C2	440
Część 1. Konfiguracja serwera Empire	442
Część 2. Zarządzanie użytkownikami	445
Posteksploatacja za pomocą platformy Empire	447
Część 1. Konfigurowanie nasłuchiwania	448
Część 2. Tworzenie stagera	449
Część 3. Korzystanie z agentów	450
Część 4. Tworzenie nowego agenta	454
Część 5. Lepsza emulacja zagrożeń	455
Część 6. Konfiguracja stałego dostępu	457
Używanie Starkillera	458
Część 1. Uruchamianie programu Starkiller	459
Część 2. Zarządzanie użytkownikami	459
Część 3. Korzystanie z modułów	462
Część 4. Tworzenie listenerów	463
Część 5. Tworzenie stagerów	464
Część 6. Korzystanie z agentów	466
Część 7. Dane dostępowe i raportowanie	468
Podsumowanie	471
Dalsza lektura	471

Rozdział 13

Zaawansowane bezprzewodowe testy penetracyjne	473
Wymagania techniczne	474
Wprowadzenie do sieci bezprzewodowych	474
SISO i MIMO	476
Standardy bezpieczeństwa sieci bezprzewodowych	479
Rekonesans sieci bezprzewodowej	481
Ustalanie klientów powiązanych z określoną siecią	486
Włamywanie się do sieci WPA i WPA2	488
Przeprowadzanie ataków AP-less	492
Włamywanie się do bezprzewodowych sieci firmowych	497
Część 1. Konfiguracja przygotowująca do ataku	498
Część 2. Określanie celu	500
Część 3. Rozpoczynanie ataku	503
Część 4. Pobieranie danych dostępowych użytkownika	505
Tworzenie bezprzewodowego honeypota	508
Wykrywanie ataków na sieci WPA3	513
Przeprowadzanie ataków typu downgrade i słownikowych	514
Zabezpieczanie sieci bezprzewodowych	518
Zarządzanie identyfikatorami SSID	518
Filtrowanie adresów MAC	519
Poziomy mocy w antenach	520
Silne hasła	520
Zabezpieczanie firmowej sieci bezprzewodowej	521
Podsumowanie	522
Dalsza lektura	522

CZĘŚĆ 4. Inżynieria społeczna i ataki na aplikacje internetowe

Rozdział 14

Ataki na klienta — inżynieria społeczna	525
Wymagania techniczne	525
Podstawowe zasady inżynierii społecznej	526
Elementy inżynierii społecznej	527
Rodzaje ataków z wykorzystaniem inżynierii społecznej	529
Techniki oparte na interakcjach z ludźmi	529
Ataki z wykorzystaniem komputerów	530

Ataki z wykorzystaniem urządzeń mobilnych	531
Witryny społecznościowe	532
Obrona przed inżynierią społeczną	533
Planowanie ataków z wykorzystaniem inżynierii społecznej	534
Narzędzia i techniki wykorzystywane w inżynierii społecznej	535
Tworzenie witryny phishingowej	536
Tworzenie urządzeń infekujących	539
Podsumowanie	542
Dalsza lektura	543

Rozdział 15

Bezpieczeństwo aplikacji internetowych 544

Wymagania techniczne	544
Charakterystyka aplikacji WWW	545
Podstawowe zasady protokołu HTTP	546
Lista OWASP Top 10: 2021	549
Zapoznanie z programami FoxyProxy i Burp Suite	551
Część 1. Konfigurowanie programu FoxyProxy	552
Część 2. Konfiguracja pakietu Burp Suite	554
Część 3. Zapoznanie z możliwościami programu Burp Suite	556
Ataki przez wstrzykiwanie	561
Przeprowadzanie ataku przez wstrzykiwanie SQL	562
Ataki wykorzystujące błędy w mechanizmach kontroli dostępu	569
Wykorzystanie błędów w mechanizmach kontroli dostępu	569
Wykrywanie usterek kryptograficznych	572
Wykorzystywanie usterek kryptograficznych	573
Zagrożenia związane z projektowaniem z pominięciem zasad bezpieczeństwa	578
Błędna konfiguracja zabezpieczeń	578
Wykorzystywanie błędnej konfiguracji	579
Podsumowanie	582
Dalsza lektura	583

Rozdział 16

Zaawansowane testy penetracyjne witryn internetowych 584

Wymagania techniczne	585
Wykrywanie podatnych i przestarzałych komponentów	585
Wykrywanie podatnych komponentów	585
Wykorzystywanie usterek w identyfikacji i uwierzytelnianiu	588
Wykrywanie usterek uwierzytelniania	589

Usterki w integralności oprogramowania i danych	594
Usterki w monitorowaniu i rejestracji zdarzeń związanych z bezpieczeństwem	594
Przeprowadzanie ataków typu server-side request forgery	595
Automatyzacja ataków przez wstrzykiwanie SQL	599
Część 1. Wykrywanie baz danych	599
Część 2. Pobieranie poufnych informacji	603
Ataki cross-site scripting	606
Część 1. Wykrywanie ataków typu reflected XSS	608
Część 2. Wykrywanie ataków stored XSS	611
Przeprowadzanie ataków po stronie klienta	613
Podsumowanie	619
Dalsza lektura	619
Rozdział 17	
Najlepsze praktyki dla rzeczywistych testów	620
Wymagania techniczne	620
Wskazówki dla pentesterów	621
Uzyskiwanie pisemnej zgody	621
Postępowanie etyczne	621
Kontrakt dotyczący testów penetracyjnych	621
Zasady zaangażowania	622
Lista kontrolna dla testów penetracyjnych	622
Zbieranie informacji	623
Skanowanie sieci	623
Enumeracja	624
Uzyskiwanie dostępu	624
Zacieranie śladów	625
Pisanie raportów	625
Tworzenie przybornika hakera	626
Konfigurowanie zdalnego dostępu	631
Następne kroki	635
Podsumowanie	636
Dalsza lektura	636
Skorowidz	638