

Spis treści

Podziękowania	xix
Przedmowa	xx
Wstęp	xxiii
Kto powinien przeczytać tę książkę	xxiii
Struktura książki	xxiii
Wymagania systemowe	xxiv
Pomoc techniczna	xxiv

Część I Planowanie i wdrażanie systemu zabezpieczeń

1 Wprowadzenie do przeprowadzania oceny zabezpieczeń	3
Rola oceny bezpieczeństwa w zabezpieczeniach sieci	4
Dlaczego zabezpieczenia zawodzą?	5
Czynnik ludzki	5
Czynniki dotyczące zasad	7
Niewłaściwa konfiguracja	8
Błędne założenia	10
Niewiedza	11
Nieaktualny system lub oprogramowanie	11
Rodzaje ocen zabezpieczeń	12
Skanowanie w poszukiwaniu podatności	12
Testy penetracji	14
Audyt bezpieczeństwa IT	15
Często zadawane pytania	15
2 Kluczowe zasady bezpieczeństwa	17
Zapewnianie prostoty zabezpieczeń	17
Utrzymanie działania usług	18
Zezwalanie właściwym użytkownikom na dostęp do właściwych informacji	18
Ochrona każdej warstwy, jakby była ostatnią linią obrony	18
Rejestrowanie prób dostępu do informacji	19
Rozdzielenie i izolowanie zasobów	19

Unikanie błędów popełnianych przez innych.....	20
Kontrola kosztów wcześniej wymienionych celów.....	21
Zarządzanie ryzykiem.....	21
Nauka zarządzania ryzykiem.....	22
Strategie zarządzania ryzykiem.....	24
Niezmienne prawa bezpieczeństwa.....	25
Często zadawane pytania.....	28

3 W poszukiwaniu podatności 31

Określanie zakresu projektu.....	32
Definiowanie rodzaju docelowych obiektów.....	32
Definiowanie zakresu docelowych obiektów.....	35
Definiowanie wyszukiwanych typów podatności.....	36
Określanie celów.....	37
Wybór technologii.....	38
Narzędzia i obiekty zarządzane oraz niezarządzane.....	39
Lista kontrolna wyboru narzędzi.....	41
Tworzenie procedur skanowania w poszukiwaniu podatności na ataki.....	42
Wykrywanie podatności.....	42
Klasyfikowanie wykrytych słabych punktów ze względu na poziom ryzyka.....	44
Identyfikowanie podatności, których nie można naprawić.....	44
Rozpoznawanie udoskonaleń zabezpieczeń sieci dokonywanych z upływem czasu.....	45
Tworzenie procedur analizy wyników.....	45
Często zadawane pytania.....	45

4 Prowadzenie testu penetracji 47

Myśleć jak napastnik.....	48
Dążenie do rozgłosu i uznania.....	49
Korzyści finansowe.....	49
Wyzwanie.....	51
„Aktywiści”.....	51
Zemsta.....	51
Szpiegostwo.....	52
Wojna informatyczna.....	52
Definiowanie stopnia zaangażowania testu penetracji.....	53
Definiowanie celów.....	53

Definiowanie zakresu	57
Wykonanie testu penetracji	58
Lokalizowanie słabszych obszarów w obronie sieci lub aplikacji	58
Ustalanie sposobów wykorzystania wykrytych podatności	59
Lokalizowanie zasobów, do których można uzyskać dostęp, które można zmienić lub zniszczyć	59
Ustalanie, czy atak został wykryty	59
Identyfikowanie tropów ataku	60
Sporządzanie zaleceń	61
Często zadawane pytania	61
 5 Wykonywanie audytów zabezpieczeń	63
Składniki audytu zabezpieczeń IT	63
Zasady	64
Metodologie i procedury	65
Praktyka wykonawcza	66
Wstępne decyzje	67
Uwarunkowania prawne	67
Uwarunkowania operacyjne	68
Uwarunkowania organizacyjne	68
Planowanie i wykonanie audytu	69
Tworzenie ram audytu	69
Definiowanie zakresu i harmonogramu audytu	72
Uzyskanie akceptacji	72
Wykonanie audytu	73
Analiza i przedstawienie wyników audytu	73
Często zadawane pytania	73
 6 Raportowanie spostrzeżeń	75
Ogólne wskazówki dotyczące tworzenia raportów	75
Zwięzłość i profesjonalizm	75
Dokładność techniczna	76
Obiektywizm	77
Mierzalność	77
Ramy raportu spostrzeżeń	77
Definiowanie podatności na atak	78
Dokumentowanie planów neutralizacji	80

Identyfikowanie potencjalnych zmian	81
Określenie odpowiedzialności za implementację zaakceptowanych zaleceń	82
Często zadawane pytania	82

7 Rozwijanie umiejętności oceny zabezpieczeń 83

Budowanie podstawowych umiejętności	83
Podnoszenie umiejętności dotyczących sieci, systemów operacyjnych i aplikacji	83
Rozwijanie umiejętności programistycznych	85
Ćwiczenia w zakresie oceny zabezpieczeń	87
Aktualność wiedzy	89
Znajdowanie odpowiedniego kursu	89
Konferencje	93
Zasoby dostępne w Internecie	94
Biuletyny zabezpieczeń	95
Witryny poświęcone bezpieczeństwu	95
Często zadawane pytania	96

Część II

8 Rekonesans informacyjny 101

Istota rekonesansu informacyjnego	101
Informacje rejestrowe	103
Ustalanie informacji o firmie rejestrującej	104
Środki zaradcze	105
Przydziały bloków adresów IP	106
Ustalanie przydziału bloku adresów IP dla organizacji	106
Środki zaradcze	108
Strony WWW	108
Przeglądanie zawartości serwera Web	108
Środki zaradcze	111
Mechanizmy wyszukiwania	112
Przeglądanie witryny firmowej przy użyciu wyszukiwarek	112
Środki zaradcze	114
Publiczne fora dyskusyjne	115
Ocena stopnia odsłonięcia organizacji	115

Środki zaradcze	116
Często zadawane pytania	117
9 Wykrywanie hostów przy użyciu DNS i NetBIOS.....	119
Wykorzystanie DNS	119
Standardowe typy rekordów	120
Analiza transferu strefy	127
Korzystanie z NetBIOS.....	129
Korzystanie z LDAP.....	131
Często zadawane pytania	132
10 Ustalanie struktury sieci i hostów.	133
Techniki przeczesywania sieci	134
Przeczesywanie przy użyciu ICMP	136
Przeczesywanie wykorzystujące UDP	137
Przeczesywanie sieci przy użyciu TCP	138
Przeczesywanie sieci przy użyciu rozgłaszania.....	139
Środki zaradcze	139
Odkrywanie topologii sieci.....	141
Śledzenie tras	142
Firewalking	143
Środki zaradcze	144
Często zadawane pytania	144
11 Skanowanie portów	145
Skanowanie połączeniowe TCP	145
Niestandardowe skanowanie TCP	149
Skanowanie pakietami SYN.....	149
Skanowanie pakietami FIN	150
Skanowanie pakietami SYN/ACK i ACK	150
Skanowanie pakietami XMAS.....	150
Skanowanie puste	150
Skanowanie przy użyciu niemego hosta	151
Skanowanie UDP	152
Skanowanie przekierowaniem odpowiedzi serwera FTP	153
Skanowanie portów: sztuczki i chwyt	154
Fragmentacja pakietów i skanowanie portów	155

Środki zaradcze	155
Często zadawane pytania	156
12 Uzyskiwanie informacji z hosta.....	157
Fingerprinting.....	157
Fingerprinting przy użyciu IP i ICMP	158
Fingerprinting przy użyciu TCP.....	159
Środki zaradcze	160
Fingerprinting aplikacji.....	161
Środki zaradcze	161
Co działa na danym porcie?	162
Odpytywanie hosta	163
Środki zaradcze	168
Często zadawane pytania	169
13 Ataki typu war dialing, war driving i Bluetooth	171
Wykrywanie modemów – war dialing	171
Anatomia ataku war dialing	174
Środki zaradcze	177
Wykrywanie sieci bezprzewodowych – war driving.....	178
Filtrowanie adresów MAC	179
Wylączenie rozgłaszania nazwy sieciowej (Service Set ID – SSID).....	180
Wired Equivalent Privacy	181
Anatomia ataku war driving.....	185
Środki zaradcze	186
Ataki Bluetooth.....	188
Wykrywanie urządzeń.....	191
Kradzież danych	191
Kradzież usług	192
Podśluchiwanie sieci	192
Często zadawane pytania	193
 Część III	
14 Zautomatyzowane wykrywanie słabych punktów.....	
Techniki skanowania	198

Odczytywanie transparentów i fingerprinting	199
Wykorzystanie podatności	199
Testy oparte na wnioskowaniu	200
Ponowne przesyłanie podsłuchanych pakietów	200
Wykrywanie poprawek	201
Wybór skanera	201
Sprawdzanie podatności	202
Szybkość skanera	203
Niezawodność i skalowalność	203
Dokładność sprawdzania	204
Częstotliwość aktualizacji	205
Funkcje raportowania	206
Podejścia do skanowania	206
Skanery oparte na hostach	206
Skanery oparte na sieci	207
Niebezpieczeństwa wynikające ze stosowania zautomatyzowanych skanerów	207
Wskazówki dotyczące bezpiecznego korzystania ze skanerów	209
Często zadawane pytania	209

15 Ataki na hasła 211

Gdzie szukać hasel	211
Ataki brute force	212
Testowanie hasel online	213
Testowanie hasel offline	215
Strategie ataków offline	216
Środki zaradcze	217
Ataki wykorzystujące ujawnienie hasel	219
Hasła w systemie plików	219
Hasła zaszyfrowane	220
Podsłuchiwanie hasel	220
Programy rejestrujące naciśnięcia klawiszy	221
Środki zaradcze	221
Często zadawane pytania	222

16 Odmowa usługi 223

Atak przez zalewanie	224
Testowanie ataków przez zalewanie	227

Środki zaradcze	227
Wyczerpywanie zasobów	228
Ataki przez wyczerpywanie CPU	228
Ataki przez wyczerpywanie pamięci	229
Atak przez wykorzystanie przestrzeni dyskowej	230
Przerwanie usług	232
Często zadawane pytania	233
 17 Ataki na aplikację	235
Przepełnienie bufora	236
Przepełnianie stosu	236
Przepełnianie sterty	239
Błędy formatowania łańcuchów	241
Środki zaradcze	242
Przepełnienie całkowite	243
Środki zaradcze	244
Wyszukiwanie przepełnienia bufora	244
Często zadawane pytania	245
 18 Ataki na bazy danych	247
Wykrywanie serwerów baz danych	248
Wykrywanie serwerów baz danych w sieci	248
Środki zaradcze	252
Brakujące poprawki	253
Wykrywanie brakujących poprawek	253
Środki zaradcze	255
Nieautoryzowany dostęp	256
Wykrywanie możliwości nieautoryzowanego dostępu	256
Środki zaradcze	257
Słabe hasła	258
Wykrywanie słabych haseł	258
Środki zaradcze	259
Podsłuchiwanie sieci	259
Wykrywanie zagrożenia podsłuchem sieci	260
Środki zaradcze	260
Iniekcja SQL	260
Wykrywanie dróg iniekcji SQL	262

Środki zaradcze	262
Często zadawane pytania	263
19 Podśluchiwanie sieci	265
Istota podśluchiwania sieci	265
Demaskowanie mitów	267
Mit 1: Napastnik może zdalnie przechwycić ruch sieciowy	267
Mit 2: Switche są odporne na ataki podśluchiwania sieci	268
Wykrywanie zagrożeń podśluchiwania sieci	271
Wykrywanie ręczne	271
Przegląd architektury sieci	272
Monitorowanie zapytań DNS	272
Mierzenie opóźnień	273
Wykorzystanie sfałszowanych adresów MAC i pakietów ICMP	273
Wykorzystanie kont-pułapek	274
Wykorzystanie nierozgłaszanych pakietów ARP	274
Automatyczne narzędzia wykrywające	274
Wykrywanie instalacji Microsoft Network Monitor	274
Środki zaradcze	275
Często zadawane pytania	277
20 Podszywanie się (spoofing)	279
IP Spoofing	279
Środki zaradcze	281
Falszowanie poczty elektronicznej	282
Środki zaradcze	284
Falszowanie DNS	284
Atakowanie klienta	285
Atakowanie serwera DNS	286
Atak poprzez aktualizację strefy	287
Atak za pośrednictwem rejestru nazw	287
Środki zaradcze	288
Często zadawane pytania	289
21 Przechwytywanie sesji	291
Istota przechwytywania sesji	291
Przechwytywanie sesji na poziomie sieci	293

Przechwytywanie sesji TCP	293
Przechwytywanie sesji UDP	295
Ustalanie podatności na zagrożenie	296
Środki zaradcze	296
Sztuczki i techniki	297
Przechwytywanie sesji na poziomie hosta	301
Przechwycenie sesji użytkownika	302
Przechwycenie portu serwera	302
Przechwytywanie na poziomie aplikacji	307
Wykrywanie ataków	308
Środki zaradcze	308
Często zadawane pytania	309

22 Unikanie wykrycia 311

Zalewanie dzienników	312
Mechanizmy rejestrujące	313
Mechanizmy wykrywające	314
Fragmentacja	316
Zapis niekanoniczny	319
Wabiki	320
Unikanie wykrycia po włamaniu	322
Narzędzia typu rootkit	322
Ukrywanie danych	323
Zniekształcanie plików dzienników	329
Często zadawane pytania	330

23 Pozasieciowe metody uzyskiwania dostępu. 333

Uzyskiwanie fizycznego dostępu do zasobów informatycznych	333
Fizyczna infiltracja	334
Zdalna inwigilacja	336
Kradzież upatrzonego sprzętu	339
Zawartość pojemników na śmieci	340
Zwroty sprzętu poleasingowego, aukcje i wyprzedaż sprzętu	340
Socjotechnika	341
Przekupstwo	342
Sugerowanie posiadania uprawnień	343
Falszerstwo	343

Schlebianie.....	344
Często zadawane pytania	345

Część IV Ocena bezpieczeństwa: analizy przypadków

24 Zagrożenia dotyczące WWW.....349

Zagrożenia na poziomie klienta	349
Cross-site scripting	350
Luki zabezpieczeń w programach klienckich.....	355
Zagrożenia na poziomie serwera	356
Wypieranie się.....	356
Ujawnienie informacji	358
Podwyższenie uprawnień.....	362
Odmowa usługi	372
Zagrożenia na poziomie usługi.....	373
Nieautoryzowany dostęp	373
Podsluchiwanie sieci	374
Zniekształcanie danych.....	374
Ujawnienie informacji	374
Często zadawane pytania	375

25 Zagrożenia dla poczty elektronicznej377

Zagrożenia na poziomie klienta	378
Dołączanie złośliwych plików.....	378
Wykorzystanie braku poprawek	383
Zagnieżdżanie złośliwej treści	384
Nadużycie zaufania użytkowników	384
Zagrożenia na poziomie serwera	387
Złośliwe załączniki	388
Fałszowanie poczty elektronicznej.....	388
Nadużycie nieaktualizowanych serwerów pocztowych	391
Spam.....	392
Dlaczego należy się przejmować spamem?	392
Sztuczki i techniki	393
Co można zrobić ze spamem?.....	397
Często zadawane pytania	398

26 Zagrożenia dla kontrolerów domeny 399

Ataki na hasła	399
Środki zaradcze	400
Podwyższanie uprawnień	404
Wykorzystanie niekoniecznych usług	404
Wykorzystanie zbędnych kont	407
Wykorzystanie braku poprawek	408
Złamanie zabezpieczeń uprzywilejowanych kont i grup domenowych	409
Odmowa usługi	411
Środki zaradcze	412
Zagrożenia dla fizycznego bezpieczeństwa	412
Środki zaradcze	413
Często zadawane pytania	414

27 Zagrożenia dotyczące sieci ekstranet i VPN 415

Podstawy projektowania bezpiecznych sieci	416
Hosty o podwójnym podłączeniu	417
Host ekranowany	418
Podsieci ekranowane	419
Rozdzielone podsieci ekranowane	420
Testy penetracyjne sieci ekstranet	420
Przykład testu penetracji ekstranetu	421
Gromadzenie informacji	422
Pierwsza próba wejścia	422
Badanie sieci wewnętrznej	423
Rozszerzanie wpływów	426
Często zadawane pytania	429

Część V Dodatki**A Listy kontrolne 433**

Listy kontrolne testów penetracyjnych	433
Rozdział 8: Rekonesans informacyjny	433
Rozdział 9: Wykrywanie hostów przy użyciu DNS i NetBIOS	433
Rozdział 10: Ustalanie struktury sieci i hostów	434
Rozdział 11: Skanowanie portów	434

Rozdział 12: Uzyskiwanie informacji z hosta	435
Rozdział 13: Ataki typu war dialing, war driving i Bluetooth	436
Rozdział 14: Zautomatyzowane wykrywanie słabych punktów	436
Rozdział 15: Ataki na hasła	437
Rozdział 16: Odmowa usługi	438
Rozdział 17: Ataki na aplikację	438
Rozdział 18: Ataki na bazy danych	438
Rozdział 19: Podśluchiwanie sieci	438
Rozdział 20: Podszywanie się (spoofing)	439
Rozdział 21: Przechwytywanie sesji	439
Rozdział 22: Unikanie wykrycia	439
Rozdział 23: Pozasieciowe metody uzyskiwania dostępu	439
Rozdział 24: Zagrożenia dotyczące WWW	440
Rozdział 25: Zagrożenia dla poczty elektronicznej	440
Rozdział 26: Zagrożenia dla kontrolerów domeny	441
Rozdział 27: Zagrożenia dotyczące sieci ekstranet i VPN	441
Listy kontrolne środków zaradczych	441
Rozdział 8: Rekonesans informacyjny	441
Rozdział 9: Wykrywanie hostów przy użyciu DNS i NetBIOS	442
Rozdział 10: Ustalanie struktury sieci i hostów	442
Rozdział 11: Skanowanie portów	442
Rozdział 12: Uzyskiwanie informacji z hosta	443
Rozdział 13: Ataki typu war dialing, war driving i Bluetooth	443
Rozdział 15: Ataki na hasła	444
Rozdział 16: Odmowa usługi	444
Rozdział 17: Ataki na aplikację	444
Rozdział 18: Ataki na bazy danych	444
Rozdział 19: Podśluchiwanie sieci	445
Rozdział 20: Podszywanie się (spoofing)	445
Rozdział 21: Przechwytywanie sesji	446
Rozdział 22: Unikanie wykrycia	446
Rozdział 23: Pozasieciowe metody uzyskiwania dostępu	446
Rozdział 24: Zagrożenia dotyczące WWW	446
Rozdział 25: Zagrożenia dla poczty elektronicznej	447
Rozdział 26: Zagrożenia dla kontrolerów domeny	447
Rozdział 27: Zagrożenia dotyczące sieci ekstranet i VPN	448

B Źródła.....	449
Rozdział 1: Wprowadzenie do wykonywania oceny zabezpieczeń	449
Rozdział 2: Kluczowe reguły bezpieczeństwa	449
Rozdział 3: W poszukiwaniu podatności.....	449
Rozdział 4: Prowadzenie testu penetracji.....	450
Rozdział 5: Wykonywanie audytów zabezpieczeń	450
Rozdział 6: Raportowanie spostrzeżeń.....	450
Rozdział 7: Rozwijanie umiejętności oceny zabezpieczeń	450
Rozdział 8: Rekonesans informacyjny	450
Rozdział 9: Wykrywanie hostów przy użyciu DNS i NetBIOS	451
Rozdział 10: Ustalanie struktury sieci i hostów	451
Rozdział 11: Skanowanie portów	451
Rozdział 12: Uzyskiwanie informacji z hosta	452
Rozdział 13: Ataki typu war dialing, war driving i Bluetooth.....	452
Rozdział 14: Zautomatyzowane wykrywanie słabych punktów.....	452
Rozdział 15: Ataki na hasła	452
Rozdział 16: Odmowa usługi.....	453
Rozdział 17: Ataki na aplikację.....	453
Rozdział 18: Ataki na bazy danych.....	453
Rozdział 19: Podsluchiwanie sieci.....	455
Rozdział 20: Podszywanie się (spoofing)	455
Rozdział 21: Przechwytywanie sesji.....	456
Rozdział 22: Unikanie wykrycia.....	456
Rozdział 23: Pozasieciowe metody uzyskiwania dostępu.....	456
Rozdział 24: Zagrożenia dotyczące WWW	457
Rozdział 25: Zagrożenia dla poczty elektronicznej.....	457
Rozdział 26: Zagrożenia dla kontrolerów domeny	458
Rozdział 27: Zagrożenia dotyczące sieci ekstranet i VPN	458
 Indeks	 459