

Spis treści

Część I Wprowadzenie	1
Rozdział 1 Dlaczego napisałem tę książkę?	3
Protokół PPTP firmy Microsoft	4
Przyczyna problemu	5
Zła konfiguracja obiektu ataku	6
O znaczeniu szkoleń w dziedzinie bezpieczeństwa	9
Rozdział 2 Jak korzystać z książki?	15
Struktura książki	15
Programy FTP	16
Języki programowania	19
Sposoby korzystania z książki	20
Ograniczenia niniejszej książki	21
Podział książki na części i rozdziały	22
Część II Poznajemy teren	25
Rozdział 3 Narodziny Internetu	27
Początki: 1962-1969	27
Narodziny UNIX-a: 1969-1973	30
Język C	30
Lata kształtowania się Internetu: 1972-1975	31
UNIX osiąga pełnoletność	32
UNIX rozwija się wraz z Internetem	33
Ogólna charakterystyka systemu UNIX	35
System X Window	36
Jakie aplikacje można uruchomić w systemie UNIX?	38
UNIX a bezpieczeństwo internetowe	38
Internet dzisiaj	40
Dostawcy usług internetowych	41
Przyszłość	41
Rozdział 4 Krótkie wprowadzenie do protokołu TCP/IP	43
Czym jest TCP/IP	43
Protokoły pakietu TCP/IP	43
Historia TCP/IP	44
Które platformy obsługują TCP/IP?	45
Jak działa TCP/IP?	46
Opis poszczególnych protokołów	47
Protokoły działające na poziomie sieci	47

Protokół komunikacyjny sterowania siecią Internet (ICMP)	49
Protokół internetowy (IP)	49
Protokół kontroli transmisji (TCP)	50
inetd: obsługa połączeń	52
Porty	53
Telnet	54
Protokół przesyłania plików (FTP)	56
TCP/IP to jest Internet	61
Rozdział 5 Hakerzy i Krakerzy	63
Czym się różni haker od kraker?	63
Gdzie się to wszystko zaczęło?	67
Dzisiaj: wojna w Internecie	71
Rozdział 6 Zagrożenie - kogo dotyczy?	75
Definicja włamania	75
Rząd	76
Sieć obronnych systemów informacji DISN	78
Marynarka Wojenna Stanów Zjednoczonych i NASA	79
Ataki na Pentagon	80
Inne zaatakowane komputery rządowe	80
Bezpieczeństwo sieci rządowych	81
Prezydencka Komisja Ochrony Infrastruktur	82
Krajowy Ośrodek Ochrony Infrastruktur (NIPC)	84
Przedsiębiorstwa	84
Incydent StarWave	85
Więcej o kartach kredytowych	86
Badania Farmera	87
Statystyka firmy Ernst & Young	88
Rozdział 7 Wojna w Internecie	89
Różne oblicza Internetu	89
Przyjaciół czy wróg?	89
Czy Internet może służyć szpiegom?	90
Zagrożenie coraz bardziej realne	91
O dostępie do technologii	92
Bezpieczeństwo w Stanach Zjednoczonych	92
Jak wyglądałby atak informacyjny?	93
Y2K	94
Najbliższa przyszłość	96
Materiały dotyczące wojny informacyjnej	97
Materiały dotyczące problemu roku 2000 (Y2K)	99
Część III Programy narzędziowe	103
Rozdział 8 Programy destrukcyjne	105
Czym są programy destrukcyjne?	105

Programy destrukcyjne jako zagrożenie dla bezpieczeństwa systemu	105
Bomby pocztowe	106
Oprogramowanie umożliwiające listowne „bombardowanie”	106
Bomby pocztowe jako zagrożenie bezpieczeństwa systemu	108
Zapisywanie użytkownika do wielu list dyskusyjnych	109
Przekazywanie poczty elektronicznej (e-mail relay)	111
Ataki powodujące blokowanie usług DoS (denial of service)	111
Gdzie spotkamy się z atakami DoS	112
Spis programów powodujących blokowanie usług (DoS)	113
Ataki DoS przeciw sprzętowym elementom sieci	122
Inne narzędzia wymuszające blokadę usług	123
Wysyłanie dużych pakietów Ping	124
SynFlood	124
DNSKiller	124
arnudp100.c	124
cbcb.c	125
Wirusy	126
Czym jest wirus komputerowy?	126
Pliki narażone na infekcję wirusową	127
Kto i dlaczego pisze wirusy?	127
Jak powstają wirusy	128
W jakim języku programuje się wirusy	129
Jak działają wirusy	129
Wirusy głównego modułu rozruchowego (MBR)	130
Programy antywirusowe	135
Publikacje i adresy źródłowe	137
Rozdział 10 Programy skanujące	139
Jak działają programy skanujące	139
Platformy, dla których dostępne są programy skanujące	139
Wymagania systemowe skanerów	140
Czy trudno jest stworzyć program skanujący?	140
Czy programy skanujące są legalne?	141
Znaczenie programów skanujących dla bezpieczeństwa sieci	141
Wpływ programów skanujących na bezpieczeństwo Internetu	142
Programy skanujące	142
Nessus	143
NSS (Network Security Scanner)	149
Strobe	151
SATAN	153
Ballista	156
Jakal	156
IdentTCPscan	157
Ogre	158
WebTrends Security Scanner (Asmodeus)	159
Internet Security Scanner i SAFESuite	159

Druga strona medalu	164
CONNECT	165
FSPScan	165
XSCAN	165
Inne platformy	166
Network Toolbox	166
Rozdział 10 Programy łamiące hasła	171
Charakterystyka „łamacza hasel”	171
Znaczenie programów do łamania hasel	178
Proces łamania hasła	179
Programy łamiące hasła	179
Programy deszyfrujące dla Windows NT	179
L0phtCrack 2.0	179
ScanNT firmy Midwestern Commerce	180
NTCrack firmy Somarsoft	181
Password NT firmy Midwestern Commerce	181
Programy łamiące hasła systemu operacyjnego UNIX	183
Crack	183
CrackerJack	185
PaceCrack95	186
Qcrack	186
John the Ripper	187
Hades	187
Star Cracker	188
Hellfire Cracker	188
XIT	189
Claymore	189
Guess	190
Merlin	190
Inne rodzaje „łamaczy hasel”	191
ZipCrack	191
Fast Zip 2.0	192
Decrypt	192
Glide	192
Ami Decode	192
NetCrack	192
PGPCrack	193
Zestaw narzędzi ICS Toolkit	194
EXCrack	194
CP.EXE	194
Źródła	195
Rozdział 11 Konie trojańskie	199
Czym są konie trojańskie?	199
Skąd pochodzą konie trojańskie?	200
Gdzie można znaleźć konie trojańskie?	203

Jak często możemy spotkać konia trojańskiego	204
Jakie ryzyko stanowią konie trojańskie?	205
Jak wykryć konia trojańskiego?	206
Źródła	214
Rozdział 12 Programy analizy ruchu w sieci komputerowej (Sniffery)	217
Analizatory ruchu w sieci komputerowej (sniffers), jako zagrożenie dla bezpieczeństwa	218
Lokalne sieci komputerowe a przesyłanie danych	218
Transmisja i dostarczanie pakietów danych	219
Jak dużym zagrożeniem są programy typu sniffer ?	219
Programy typu sniffer a bezpieczeństwo sieci	220
Jakie informacje przechwytyują programy typu Sniffer?	221
Gdzie lokowane są programy typu sniffer?	222
W jaki sposób pozyskać program typu sniffer?	222
Sniffery komercyjne	223
ATM Sniffer Network Analyser z firmy Network Associates	223
Ogólnie dostępne programy typu sniffer	227
Obrona przed atakami wykorzystującymi programy typu sniffer	232
Wykrycie i unieszkodliwienie sniffiera	232
Bezpieczna topologia	234
Szyfrowanie sesji	235
Inne źródła wiedzy o sniffierach	236
Rozdział 13 Zapory sieciowe (firewalle)	239
Czym jest firewall?	239
Inne zadania realizowane przez zapory sieciowe	239
Z czego składa się zaporę sieciową?	240
Typy zapór sieciowych	241
Zapory sieciowe na poziomie sieci/pakietu	241
Zapory sieciowe realizowane w oparciu o aplikacje bramy	242
Konstrukcja zapory sieciowej	246
Rozpoznanie topologii sieci oraz potrzeb w zakresie aplikacji i protokołów	247
Analiza zależności służbowych	247
Stworzenie reguł dostępu do zasobów i znalezienie odpowiedniego firewall-a	248
Czy zapory sieciowe są niezawodne?	248
Luka w zaporze Cisco PIX	249
Firewall-1 - zastrzeżone słowa kluczowe	249
Komercyjne zapory sieciowe	250
AltaVista Firewall 98	250
ANS InterLock	250
Avertis	250
BorderManager	251

Conclave	251
CSM Proxy/Enterprise Edition	251
CyberGuard Firewall	252
CyberShield	252
Elron Firewall/Secure	252
FiraWalla 3.0	253
Gauntlet Internet Firewall	253
GNAT Box Firewall	253
Guardian	254
IBM eNetwork Firewall	254
Interceptor Firewall Appliance	254
NETBuilder	254
NetRoadTrafficWare Firewall	255
NetScreenAO	255
PIX Firewall 4.1	255
Raptor Firewall	256
SecureAccess	256
SecurIT Firewall	256
SunScreen	257
Źródła	257
Rozdział 14 Dzienniki systemowe (logi)	261
Dzienniki systemowe - czemu służą?	261
Monitorowanie sieci i zbieranie danych	263
SWATCH (The System Watcher)	263
Watcher	264
Isoft (List Open Files)	264
WebSense	265
WebTrends for Firewalls and VPNs	265
Win-Log version 1	266
MLOG	266
NOCOL/NetConsole v4.0	266
PingLogger	267
Narzędzia do analizy dzienników systemowych	267
NestWatch	267
NetTracker	267
LogSurfer	268
VBStats	268
Netlog	268
Analog	269
Wyspecjalizowane narzędzia monitorujące	269
Courtney	269
Gabriel	270

Część IV Platformy systemowe a bezpieczeństwo	271
Rozdział 15 Luka w ochronie systemu	273
Pojęcie luki	273
Gra na czas	273
Proces ujawniania luki	274
Poruszanie się po morzu danych	275
Wymagany poziom bezpieczeństwa systemu	277
Źródła ogólne	278
CERT - The Computer Emergency Response Team	278
Rada do spraw Bezpieczeństwa Systemów Komputerowych	
Departamentu Energii Stanów Zjednoczonych (Computer Incident Advisory Capability)	280
Zasoby Bezpieczeństwa Komputerowego Ośrodka Uzgadniania Informacji (CSRC) przy Narodowym Instytucie Standaryzacji i Technologii (NIST)	281
Centrum Informacji ds. Sieci Departamentu Obrony USA	282
Archiwa BUGTRAQ	283
Forum Zespołów ds. Bezpieczeństwa i Szybkiego Reagowania FIRST	283
Archiwum błędów Windows 95	284
Listy dyskusyjne	285
Grupy dyskusyjne Usenetu	287
Listy wysyłkowe producentów oprogramowania, zbiory pakietów korygujących i inne zasoby	288
Kwatera ds. Bezpieczeństwa Silicon Graphics	288
Archiwum biuletynów nt. bezpieczeństwa firmy Sun	289
Lista dyskusyjna dotycząca bezpieczeństwa systemu Windows NT utrzymywana przez ISS	289
Narodowe Instytuty Zdrowia	289
Spis odnośników do stron o tematyce bezpieczeństwa sieci i systemów	290
Gorąca lista Eugene Spafford	290
Rozdział 16 Microsoft	291
DOS	291
Komputery zgodne z IBM	292
Oprogramowanie pozwalające na kontrolę dostępu do systemu DOS	294
Zasoby sieciowe zawierające oprogramowanie narzędziowe pod DOS zwiększające poziom zabezpieczenia systemu	296
Windows for Workgroups i Windows 95	296
Formuła zabezpieczenia hasłem w oparciu o plik PWL (Password List)	297
Odczytywanie hasła z pamięci	298
Oprogramowanie kontroli dostępu pod Windows 95	299
Zagrożenia bezpieczeństwa systemu w oprogramowaniu Microsoftu	304
Microsoft Internet Explorer	304
Microsoft FrontPage	308

Microsoft Exchange	310
Inne aplikacje i dodatki	312
Inne aplikacje Microsoftu	314
Microsoft Access	316
Pozostałe aplikacje	317
Podsumowanie platform DOS, Windows i Windows 95	317
Windows NT	317
IIS (Internet Information Server)	318
Luki w bezpieczeństwie Windows NT - Zagadnienia ogólne	322
Luki o mniejszym znaczeniu dla bezpieczeństwa systemu	323
Wewnętrzna ochrona systemu Windows NT	324
Wewnętrzna ochrona w ogólności	324
Jak utworzyć bezpieczny serwer Windows NT	326
Narzędzia	327
Źródła informacji w sieci Internet	333
Ramy bezpieczeństwa internetowego wg Microsoftu - FAQ	334
Książki o tematyce związanej z bezpieczeństwem systemu Windows NT	337
Rozdział 17 UNIX: Wielkie wyzwanie	339
Od czego należy zacząć?	339
Kilka słów na temat fizycznej ochrony serwera	339
Bezpieczeństwo konsoli	341
Hasła konsoli	341
Hasło administratora („roota“)	343
Zabezpieczenie pakietu instalacyjnego systemu	343
Ustawienia domyślne	343
Kontrola dostępu za pomocą haseł	344
Instalujemy password shadowing	345
Pakiety korekcyjne („łaty“)	350
Wybrane luki i usterki systemowe	350
Poważne luki w ochronie zewnętrznej systemu: AIX	351
Poważne luki w ochronie zewnętrznej systemu: IRIX	353
Poważne luki w ochronie zewnętrznej systemu: SunOS i Solaris	354
Poważne luki w ochronie zewnętrznej systemu: Linux	356
Następny krok: analiza usług	356
Usługi zdalnego dostępu typu „r“	357
Usługa finger	358
Telnet	359
FTP	362
O usłudze FTP ogólnie	363
Gopher	366
Sieciowy system plików (NFS)	368
HTTP	370
Ogólne aspekty bezpieczeństwa HTTP	372
Protokół SSL	372
Śledzenie zmian w systemie plików	373

TripWire	373
X Windows	373
Podręczniki i przewodniki	376
Wybrane luki i sposoby ich wykorzystania w systemach typu UNIX	378
Publikacje i źródła	400
Książki	400
Publikacje internetowe	401
Rozdział 18 Novell	403
Novell – bezpieczeństwo wewnętrzne	403
Domyślne hasła	405
Luka programu FLAG	406
Skrypt logowania	406
Programy typu „sniffer” a Novell	407
Zdalne ataki na sieć NetWare	408
Luka w module PERL	408
Atak wykorzystujący procedurę logowania nowego użytkownika	409
Podszywanie (spoofing)	410
Blokowanie usług (DoS)	412
Blokada usług z wykorzystaniem TCP/IP w systemie	
Novell NetWare 4.x	412
Serwer FTP podatny na ataki DoS	413
Problemy w oprogramowaniu innych producentów	413
Luka Windows 95	413
Luka Windows NT	414
Programy do zabezpieczenia i administracji sieci Novell	414
AuditTrack	414
ProtecNet for NetWare	415
System administracyjny LattisNet	415
LT Auditor+ v6.0	416
Kane Security Analyst	416
Zbiór reguł i procedur bezpieczeństwa systemu	417
Menu Works	417
AuditWare for NDS	417
WSetPass 1.55	418
WnSyscon 0.95	418
BindView EMS	418
SecureConsole	419
GETEQUIV.EXE	419
Programy do testowania bezpieczeństwa sieci NetWare	419
Getit	419
Burglar	420
Setpass	421
NWPCrack	421
IPXCntrl	421
Crack	421
Snoop	422

Część V Zaczniemy od początku**427****Rozdział 19 Kto tu dowodzi ?****429**

Zarys ogólny	429
Kontrola dostępu	431
Osiągnięcie przywilejów root-a	433
Zalety i wady systemu zezwoleń	433
Działania krakerów w celu osiągnięcia przywilejów root-a	434
Root może należeć do przeszłości	434
Root na innych systemach operacyjnych	435
Kraker, który uzyskał przywileje roota	435

Rozdział 20 Bezpieczeństwo wewnętrzne**437**

Bezpieczeństwo wewnętrzne	437
Czy bezpieczeństwo wewnętrzne jest rzeczywiście potrzebne?	437
Dlaczego wewnętrzne ataki są tak powszechne?	437
Zasady postępowania	439
Dostęp do sprzętu	439
Modemy	439
Napędy, katalogi i pliki	441
Ogólna ocena bezpieczeństwa wewnętrznego	443
SysCAT	443
SQLAuditor	444
System Security Scanner (S3)	446
RSCAN	447
Kontrola dostępu pracowników do Internetu	447
N2H firmy Bess School and Business Filters	448
WebSENSE	448
X-STOP	449
Sequel Net Access Manager	449
SmartFilter	450
Najlepsze zestawienia kontrolne	451

Część VI Atak zdalny**453****Rozdział 21 Atak zdalny****455**

Co to jest atak zdalny?	455
Pierwsze kroki	455
Spojrzenie na sieć	456
WHOIS	458
finger i rusers	460
System operacyjny	461
Faza analiz	462
Identyfikacja najsłabszych punktów systemu zabezpieczeń	463
Zbiór danych o słabych punktach systemu	464

Oficjalne źródła omawiające zagadnienia bezpieczeństwa	464
Faza testów	466
Podsumowanie	467
Rozdział 22 Poziomy ataku	469
Kiedy atak może nastąpić?	469
Jakiego rodzaju systemy operacyjne wykorzystują włamywacze?	470
Sun	471
UNIX	472
Microsoft	472
Źródła ataku	473
Kim jest typowy kraker ?	473
Jaki jest typowy cel ataku?	474
O atakach	475
Poziomy ataków	478
Poziomy czułości	479
Poziomy reakcji	485
Źródła	486
Rozdział 23 Ataki podszywania	489
Co to jest atak podszywania?	489
Podstawy bezpieczeństwa w Internecie	489
Metody uwierzytelniania	490
RHOSTS	490
Mechanizmy ataku podszywania	492
Składniki pomyślnego ataku podszywania	494
Odgadywanie numeru sekwencyjnego	494
Otwarcie bardziej dogodnej luki	495
Kto jest podatny na atak podszywania?	495
Jak często występują ataki podszywania?	496
Dokumenty poświęcone podszywaniu na bazie IP	498
Jak zabezpieczyć się przed podszywaniem opartym o adresy IP?	498
Inne odmiany ataku podszywania	500
Podszywanie oparte o ARP	500
Podszywanie oparte na DNS	501
Rozdział 24 Ataki wykorzystujące usługę Telnet	503
Telnet	503
Terminal wirtualny	504
Historia bezpieczeństwa usługi Telnet	505
Zmienianie środowiska	508
Emulacja terminala	510
Czy ataki te nie są już skuteczne?	515
Telnet jako broń	515
Podsumowanie	519

Rozdział 25 Języki, rozszerzenia i bezpieczeństwo	523
Rozwój sieci WWW	523
CGI i bezpieczeństwo	524
Perl (Practical Extraction and Report Language)	524
Bezpieczeństwo Perla	525
Wywołanie systemowe	525
Uruchamianie skryptów w trybie uprzywilejowanym	528
Tworzenie plików	528
Pliki dołączalne po stronie serwera	529
Java	530
ActiveX	535
Na czym polega problem z ActiveX?	536
Języki skryptów	537
JavaScript	537
VBScript	539
Uwagi końcowe	539
Rozdział 26 Ukrywanie tożsamości	541
Stopnie ujawniania tożsamości	541
Wywiad ludzki	541
Przeglądanie stron WWW a prywatność	543
Architektura Internetu i prywatność	543
Jak przechowywane są dane użytkowników na serwerach	543
Finger	544
MasterPlan	547
Nie tylko finger...	549
Bezpieczeństwo przeglądarki	549
Cookies	551
Rozwiązania z Lucent Technologies	556
Używanie programu Lucent's Personalized Web Assistant	556
Nasz adres poczty elektronicznej i Usenet	560
Usługa WHOIS	563
Ostrzeżenie	569
Dodatek A Dodatkowe źródła informacji	573
Źródła oficjalne	573
Źródła podziemne	585
Dodatek B Zawartość CD-ROM-u	587
Oprogramowanie dla komputerów Macintosh	587
Oprogramowanie dla platformy Windows - Narzędzia sieciowe	587
Oprogramowanie dla systemu UNIX	596
Dokumenty	598