

Obsah

Úvod	21
Proč jsme napsali tuto knihu?	21
Požadavky na systém	21
Absolutní požadavky	22
Archivační nástroje	22
Prohlížeče různých textových souborů	23
Programovací jazyky	24
O příkladech v této knize	25
O odkazech v této knize	27
Poznámka na závěr	28

ČÁST I Koncepce bezpečnosti

Kapitola 1 Plánování zabezpečení vašeho podniku	33
Porovnání reaktivního a proaktivního modelu	33
Poznávání podniku	34
Workflow a bezpečnost	36
Vyhodnocení rizika: Určení stavu bezpečnosti vašeho podniku	37
Identifikace digitálních aktiv	39
Ochrana aktiv	40
Identifikace a odstranění zranitelností	42
Standardizace a proaktivní zásady	43
Zásady reakce na incident	45
Školení uživatelů a správců	46
40 000 stop dlouhá revize	46
Shmutí	50
Kapitola 2 Situace Internetu: Svět ve válce	51
Hacking, cracking a jiné zlomyslné jednání	51

Vlády ve válce.....	52
Může být Internet využíván pro špionáž?.....	54
Lze využívat Internet k terorismu?.....	55
Hrozba se týká všech.....	56
Kdo má v rukou trumfy?	57
Mohou Spojené státy chránit národní informační infrastrukturu?	58
Jak by vypadal informační útok?.....	60
Situace vlády.....	62
NIPC (National Infrastructure Protection Center).....	63
Shrnutí bezpečnostní situace vlády.....	63
Stav podnikatelského sektoru.....	64
Krádeže kreditních karet: incident StarWave.....	64
Další krádeže kreditních karet.....	65
Trendy.....	67
Varování.....	68
Shrnutí.....	68
Doplňkové informace	69
Zdroje informací o informační válce na Internetu.....	69
Knihy o informační válce.....	70
Kapitola 3 Hackeři a crackeři.....	73
Rozdíl mezi hackery a crackery.....	73
Nástroje útočníků.....	74
Rekognoskace	74
Pasivní identifikace operačního systému – Fingerprinting.....	82
Zneužití a 20 nejčastějších zranitelností definovaných institutem SANS.....	86
Zneužití slabín (Exploits)	86
20 nejkritičtějších hrozeb.....	89
Shrnutí.....	94
Kapitola 4 Zdroje informací	95
Informační přetížení	95
Kolik informací o bezpečnosti potřebujete?.....	97
Obecné zdroje.....	98

CERT (Computer Emergency Response Team).....	98
CIAC (Computer Incident Advisory Capability) Ministerstva pro energii USA.....	99
NIST CSRC (National Institute of Standards and Technology Computer Security Resource Clearinghouse).....	100
Konference.....	102
Diskusní skupiny v síti Usenet.....	104
Konference o bezpečnosti pořádané výrobcí, deponitáři záplat a zdroje.....	105
Bezpečnostní ústředí společnosti Silicon Graphics.....	105
Archív bezpečnostní bulletinů společnosti Sun.....	105
Shrnutí.....	107
Kapitola 5 Interní bezpečnost.....	109
Interní bezpečnost: vzdorovitě nevlastní dítě.....	109
Interní rizika: Typy škod a škůdců.....	110
Zaměstnanci bez zlého úmyslu.....	112
Zaměstnanci porušující nařízení.....	113
Zaměstnanci IT oddělení.....	114
Zásady pro zmírnění rizik.....	115
Fyzické zabezpečení.....	115
Proces přijímání zaměstnanců.....	117
Záměrné omezení funkčnosti stolních počítačů – <i>lockdown</i>	118
Omezení obsahu.....	119
Spolupráce při správě.....	121
Produkty.....	121
Správa stolních počítačů.....	121
Bezpečnost notebooků/PDA.....	122
Fyzická bezpečnost.....	123
Řízení obsahu.....	124
Zdroje informací na Internetu.....	125
Shrnutí.....	126

ČÁST II Hackování 101

Kapitola 6 Stručný úvod do protokolů TCP/IP	129
Co je TCP/IP	129
Referenční model OSI	129
Historie TCP/IP	132
RFC	132
Implementace protokolů TCP/IP	133
Jak fungují protokoly TCP/IP?	134
Jednotlivé protokoly	135
Protokoly na síťové úrovni	135
Protokoly na aplikační úrovni – porty	143
IPsec, IPv6, VPN a budoucnost	151
Shrnutí	153
Kapitola 7 Spoofing aneb klamání cíle	155
Co je spoofing?	155
Základy Internetové bezpečnosti	155
Metody autentizace	156
RHOSTS	156
Mechanismus spoofing útoku	158
Ingredience úspěšného spoofing útoku	161
Otevření brány do systému	162
Koho lze oklamat?	162
Jak časté jsou spoofing útoky?	163
Spoofingové nástroje	166
Dokumenty týkající se falšování IP adres	165
Jak se mohu bránit proti spoofingu?	165
Další zvláštní a nekonvenční spoofingové útoky	167
ARP Spoofing	167
DNS Spoofing	168
Web spoofing	169
Shrnutí	171

Kapitola 8 Osobní soukromí.....	173
Úrovně ohrožení.....	173
Výzvědná činnost.....	173
Prohlížení obsahu Internetu a narušení soukromí.....	176
Architektura Internetu a soukromí.....	176
Ukládání uživatelských dat na serverech.....	176
Nástroj <i>finger</i>	177
Řešení problému <i>finger</i>	180
Nástroj MasterPlan.....	181
Za hranicemi nástroje <i>finger</i>	182
Zabezpečení prohlížeče.....	183
Slídění s využitím IP adres a vyrovnávací paměti prohlížeče.....	183
Soubory cookie.....	184
Reklamní proužky a webové štěnice.....	188
Spyware.....	191
Adresa elektronické pošty a síť Usenet.....	192
Skupiny na serveru Google.....	195
Služba WHOIS.....	196
V práci.....	202
Varování.....	202
Zdroje informací na Internetu.....	203
Články a související webové stránky.....	205
Kapitola 9 Vyvracení pověr.....	207
Kdy mohou nastat útoky?.....	207
Jak se stát cílem útočníka?.....	208
Dial-up (vytáčené) versus trvalé připojení.....	211
Které operační systémy jsou zranitelné?.....	211
Můj firewall crackery zastaví!.....	213
Jaké typy útočníků existují?.....	214
Největší hrozba – script kiddies.....	214
“Černé klobouky” -strana zla.....	214
“Bílé klobouky” – strana dobra.....	215
Operační systémy, které hackeři používají.....	215
Operační systémy Windows.....	215

Linux/NetBSD/FreeBSD	216
OpenBSD.....	217
Existuje typický útok?.....	217
Útok typu zablokování služby (denial-of-service)	218
Viry, trojské koně, zákeřné skripty a obsah webových stránek.....	218
Diskreditace webových stránek (značkování).....	219
Útoky zevnitř.....	220
Kdo je nejčastěji cílem?	221
Domácí uživatelé Internetu a uživatelé Internetu v malých firmách.....	221
Větší společnosti a korporace.....	221
Vládní a vojenské instituce	222
Finanční instituce.....	222
Jaká je motivace k útokům?	223
Proslulost.....	223
Destruktivní žerty nebo bezdůvodné ničení.....	224
Uveřejnění politického prohlášení.....	225
Finanční zisk.....	225
Cracking jako touha po vědomostech.....	228
Průnik za účelem průniku.....	229
Shrnutí.....	229

ČÁST III Výbava obránce

Kapitola 10 Firewally	233
Co je to firewall?.....	233
Další funkce firewallových produktů.....	234
Firewall není neprůstřelný.....	236
Firewallové produkty z blízka.....	237
Firewally založené na filtrování paketů.....	238
Firewally založené na stavovém filtrování paketů.....	239
Firewally založené na principu proxy.....	240
Programátoři obcházející firewall.....	242
Úskalí používání firewallu.....	242
Možnosti nasazení firevallů.....	243

Nasazení firewallů v reálném světě.....	244
Identifikace topologie sítě, aplikací a protokolů	246
Analýza důvěryhodnosti vazeb a komunikačních cest v organizaci	247
Vyhodnocení a výběr firewallu.....	248
Nasazení a testování firewallu.....	249
Příklady selhání firewallu	250
Problém typu “Kam se poděl můj webový server?”	250
Použití SSH při obcházení zásad zabezpečení.....	252
Komerční firewally.....	253
BlackICE	254
BorderManager	254
FireBOX.....	254
Firewall-1.....	254
FireWall Server.....	255
GNAT Box Firewall.....	255
Guardian.....	255
NetScreen.....	255
PIX Firewall.....	256
SideWinder.....	256
Sonicwall	256
Symantec Enterprise Firewall.....	256
Tiny Personal Firewall	256
ZoneAlarm Pro.....	257
Shrnutí.....	257
Knihy a publikace.....	257
Zdroje informací na Internetu.....	258

Kapitola 11 Analyzátoři zranitelných míst systémů259

Historie analyzátorů zranitelných míst.....	259
Jak fungují analyzátoři zranitelných míst.....	261
Na co se zaměřit při výběru analyzátoru.....	263
Základní nedostatky.....	265
Nejlepší analyzátoři.....	266
Retina	267
NetRecon.....	267

ISS Internet Scanner.....	268
Cybercop Scanner.....	268
Open source projekt Nessus.....	269
Whisker.....	270
Ostatní analyzátory.....	270
HackerShield.....	270
Update.....	270
Cisco Scanner.....	270
SAINT.....	271
SARA, TARA a WebMon.....	271
STAT.....	271
Security Analyzer.....	271
Shnutí.....	271
Kapitola 12 Systémy pro detekci průniku	273
Princip detekce průniku.....	273
Kdo by měl detektory průniku používat.....	275
Síťové detekční systémy.....	276
Hostitelské detekční systémy.....	277
Detekční systémy s vyhledáváním anomálií.....	278
Na co se zaměřit při výběru detektoru průniku.....	279
Kritéria vyhodnocování.....	279
Nástroj Snort a jiná open source řešení.....	282
Seznam produktů pro detekci průniku.....	282
Cisco Secure IDS.....	283
Computer Associates eTrust Intrusion Detection.....	283
Enterasys Dragon.....	283
Intrusion SecureNet a SecureHost.....	284
Intruvert IntruShield.....	284
ISS RealSecure.....	285
ISS BlackICE.....	285
NFR Security Intrusion Detection System.....	285
nSecure Software nPatrol.....	286
Symantec NetProwler a Intruder Alert.....	286
Shnutí.....	286

Kapitola 13 Nástroje protokolování	289
Proč protokolovat?	289
Protokolování z pohledu crackera.....	289
Vytváříme strategii protokolování.....	290
Monitoring sítě a sběr dat.....	293
SWATCH (The System Watcher).....	293
Watcher	293
lsof (List Open Files).....	294
Private – I.....	294
WebSense.....	295
Win – Log verze 1.....	295
SNIPS.....	295
Nástroje pro analýzu protokolových souborů.....	295
NetTracker.....	296
LogSurfer.....	296
WebTrends for Firewalls and VPNs.....	296
Analog.....	296
Shrnutí.....	297
 Kapitola 14 Zabezpečení hesly	 299
Cracking hesel.....	299
Základy šifrování hesel.....	301
Jak cracking hesel probíhá.....	308
Nástroje pro cracking hesel.....	309
Nástroje pro cracking hesel na systémech Windows	309
L0pthCrack/LC4.....	309
John the Ripper od firmy Solar Designer.....	310
NTCrack.....	311
Nástroje pro cracking hesel na systémech Unix.....	312
Nástroj Crack.....	314
John the Ripper od firmy Solar Designer.....	316
PaceCrack 95.....	316
Star Cracker od autora Sorcerer.....	316

Cracking hesel zařízení Cisco, aplikačních hesel i jiných typů hesel.....	317
Cracking hesel systému Cisco IOS.....	317
Nástroj pro cracking hesel komerčních aplikací.....	318
ZipCrack Michaela A. Quinlana.....	319
AMI Decode (autor neznámý).....	319
PGPCrack Marka Millera.....	320
Zdokonalení hesel.....	321
Windows NT/2000.....	321
Passfilt Pro.....	321
Password Bouncer.....	322
Unix.....	322
Servery LDAP.....	322
Další zdroje informací.....	322
Zdroje informací na Internetu.....	323
Publikace a zprávy.....	324
Shrnutí.....	325
Kapitola 15 Analyzátoři paketů aneb sniffery	327
Analyzátoři paketů jako bezpečnostní riziko.....	328
Sítě LAN a datový provoz.....	328
Přenos a doručení paketů.....	328
Jakou úroveň rizika analyzátoři představují?.....	329
Už někdo viděl útok s využitím analyzátoru?.....	329
Jaké informace analyzátoři získávají?.....	330
Kde se dají analyzátoři najít?.....	331
Jak můžu analyzátor získat?.....	332
Komerční analyzátoři paketů.....	332
Zdarma dostupné analyzátoři.....	335
Obrana proti útokům s využitím analyzátorů.....	336
Odhalení a eliminace snifferu.....	336
Bezpečná topologie.....	338
Šifrovaná připojení.....	339
Shrnutí.....	340
Zdroje informací na Internetu.....	340

ČÁST IV Zbraně hromadného ničení

Kapitola 16 Útoky typu odepření služby.....	343
Co to je odepření služby?	343
Jak útoky typu odepření služby fungují.....	344
Exploits a odepření služby	347
Útoky pomocí emailových bomb.....	348
Útoky na protokoly.....	355
Rejstřík útoků typu odepření služby.....	355
Aktuální útoky typu odepření služby.....	356
Historický seznam známých útoků typu odepření služby.....	358
Distribuované útoky typu odepření služby.....	362
Souhrn	365
Jiné zdroje odepření služby.....	365
Kapitola 17 Viry a červy	367
Seznámení s viry a červy.....	367
Co to je počítačový virus?	369
Co to je počítačový červ?.....	371
Objekty, které mohou být infikovány viry.....	372
Kdo píše viry a proč.....	373
Jak viry vznikají?	375
Co vlastně znamená virus typu ItW (In the Wild)?.....	377
Jak viry fungují?.....	378
Memetické viry	384
Jak fungují červy?.....	387
Vlastnosti virů.....	388
Antivirové nástroje	391
Network Associates.....	393
Norton Anti-Virus.....	394
eSafe.....	394
Antigen.....	394
PC-Cillin.....	394
Sophos Anti-Virus.....	394
F-PROT Anti-Virus.....	394

Integrity Master.....	395
Budoucí trendy ve virovém malwaru	395
Publikace a weby.....	396
Souhrn	399
Kapitola 18 Trojské koně	403
Co to je trojský kůň?.....	403
Původ druhu.....	403
Definice.....	404
To jsem nechtěl.....	405
Klasifikace trojských koní.....	408
Odkud trojské koně pocházejí?	421
Jak často jsou trojské koně zjištěny?.....	422
Jaké riziko trojské koně znamenají?.....	424
Jak lze trojské koně detekovat?.....	425
MD5.....	427
Tripwire	429
TAMU/TARA.....	430
Jiné platformy.....	430
Zdroje.....	431
Souhrn	433
Rejstřík	435