

Kratak sadržaj

Uvod	1
Deo I: Koncepti sigurnosti	9
1. Izgradnja putne karte za obezbeđivanje Vašeg preduzeća	11
2. Država Net: rat u svetu	27
3. Hakeri i krekeri	47
4. Iskopavanje podatka "monstruma"	67
5. Unutrašnja sigurnost	79
Deo II: Hacking 101	95
6. Kratak TCP/IP bukvar	97
7. Spoofing napadi	121
8. Lična sigurnost	139
9. Razbijanje nekih mitova	171
Deo III: Skup alata zaštite	193
10. Firewalls	195
11. Alati za procenu ranjivosti (skeneri)	219
12. Sistemi za otkrivanje napada	231
13. Alati prijavljivanja	245
14. Sigurnost lozinke	255
15. Njuškala (sniffers)	281
Deo IV: Oružje za masovno uništenje	295
16. Alati za lišavanje servisa	297
17. Virus i crvi	319
18. Trojanci	351
Deo V: Arhitekture, platforme i sigurnost	379
19. Razmatranja mrežne arhitekture	381
20. Microsoft	409
21. Unix	445

22.	Novell NetWare	527
23.	Routeri, switchevi i hubovi	547
24.	Macintosh	563
25.	Načela, procedure i primenjivanje	615

Deo VI: Sigurnost i integrisani servisi **643**

26.	Sigurni razvoj aplikacija, jezici i proširenja	645
27.	Revidiranje bežične sigurnosti	687

Deo VII: Preporuke **729**

A.	Bibliografija sigurnosti - dalje čitanje	731
B.	Kako da dobijete više informacija	745
C.	Informacije proizvođača i sigurnosni standardi	761
D.	Šta je na CD-ROM-u	781
E.	Rečnik	835

Indeks	871
--------------	-----

Deo IV: Oruđe za masovno uništenje

16.	Alti za lišavanje servisa
17.	Virusi i čvci
18.	Trojanci

Deo V: Arhitekture platformi i alati

19.	Razmatranje mrežne arhitekture
20.	Microsoft
21.	Unix

Sadržaj

Uvod	1
------------	---

Deo I: Koncepti sigurnosti

1. Izgradnja putne karte za obezbeđivanje Vašeg preduzeća	11
Reaktivni nasuprot proaktivnih modela	11
Shvatanje inicijative	12
Rad i sigurnost	14
Procena rizika: Izračunavanje sigurnosnog stava preduzeća	15
Identifikovanje digitalnog preimućstva	16
Zaštita preimućstva	17
Identifikovanje i izbacivanje ranjivosti	19
Standardizacija i proaktivne politike	20
Načelo odgovora na incident	22
Treniranje korisnika i administratora	22
Pregled	23
Zaključak	26
2. Država Net: rat u svetu	27
Hakovanje, kreovanje i drugo zlobno ponašanje	28
Vlade u ratu	28
Da li se može Internet koristiti za špijunažu?	30
Da li se Internet može koristiti za terorizam?	31
Pretnja je više lična	31
Ko skriva kartice?	33
Da li mogu Sjedinjene Američke Države zaštititi informacije o nacionalnoj infrastrukturi?	34
Kako izgledaju informacije o napadu?	36
Vlada	37
National Infrastructure Protection Center (NIPC)	38
Zaključak o ranjivostima vlade	38
Korporativno odeljenje	39
Ukradena kreditna kartica Cyber: StarWave incident	39
Ukradena kreditna kartica brzo se pronalazi	39
Trendovi	41
Zaključak	43
Dodatna informacija	43
Internet resursi informacionog rata	43
Knjige o informacionom ratu	44

3. Hakeri i krekeri	47
Razlika između hakera i krekeri	47
Alati trgovine	48
Izviđanje	48
Identifikacija otiskom prstiju pasivnog operativnog sistema	55
Eksploatacije i SANS Top 20	59
Eksploatacije	59
SANS Top 20	62
Zaključak	66
4. Iskopavanje podatka "monstruma"	67
Informacija prekoračenja	68
Koliko sigurnost Vam je potrebna?	69
Opšti izvori	70
Computer Emergency Response Team (CERT)	70
Odeljenje energetike SAD za Computer Incident Advisory Capability	71
Nacionalni institut za standarde i tehnologiju Computer Security Resource Clearinghouse	72
Mejling liste	73
Usenet diskusionih grupa	75
Prodavac sigurnosnih mejling lista, mesta zakrpe i resursi	76
Silicon Graphics štabovi sigurnosti	76
Sun sigurnosni arhivski bilten	77
Zaključak	78
5. Unutrašnja sigurnost	79
Unutrašnja sigurnost: Red-hedovo pastorče	79
Unutrašnji rizici: Tipovi štete i vektora	80
Dobronamerni/nesvesni radnici	82
Zaposleni koji krše zakon	82
IT radnici	83
Načela ublaženja rizika	84
Fizička sigurnost	84
Proces unajmljivanja	86
Zaključavanje desktopa	86
Smanjenje sadržaja	87
Administrativna saradnja	89
Proizvodi	89
Upravljanje desktopom	89
Laptop/PDA sigurnost	90
Fizička sigurnost	91
Upravljanje sadržajem	92

Resursi 93
 Zaključak 94

Deo II: Hacking 101 95

6. Kratak TCP/IP bukvar 97

- Šta je TCP/IP? 97
 - Open System Interconnection (OSI) referentni model 98
 - Istorija TCP/IP 100
 - RFC-ovi 100
 - Implementacije TCP/IP 101
- Kako radi TCP/IP? 101
- Individualni protokoli 103
 - Protokoli mrežnog sloja 103
 - Protokoli nivoa aplikacije-portovi 110
- IPsec, IPv6, VPN i pogled dalje 117
- Zaključak 118

7. Spoofing napadi 121

- Šta je spoofing? 121
- Fundamenti Internet sigurnosti 122
 - Metode autentičnosti 122
 - RHOSTS 123
- Mehanike napada ismevanja 125
 - Sastojci uspešnog spoofing napada 127
 - Otvaranje pogodnije rupe 128
 - Ko može biti spoofer? 128
 - Koliko su česti spoofing napadi? 129
 - Pomoćni programi spoofing/otmice 129
- Dokumenti koji se odnose specijalno na IP spoofing 131
- Kako sprečiti IP spoofing napade? 132
- Drugi nepoznati i neuobičajeni spoofing napadi 133
 - ARP spoofing 133
 - DNS spoofing 134
 - Web Spoofing 135
- Zaključak 137

8. Lična sigurnost 139

- Stepeni izloženosti 139
 - Ljudska obaveštajna delatnost 140
- Web pretraživanje i invazija na privatnost 142
 - Internet arhitektura i privatnost 142
 - Kako se smešta korisnička informacija na serverima 142
- Finger 143
- MasterPlan 146

Iza fingera	147
Sigurnost pretraživača	148
IP adresa i njuškanje keša	148
Cookies	149
Reklamni baneri i web greške	152
Spyware	155
Vaša e-mail adresa i Usenet	156
Google Groups	159
WHOIS servis	159
Na poslu	164
Upozorenje	165
Članci, novine i web sajtovi koji se na to odnose	168
9. Razbijanje nekih mitova	171
Kada se napadi mogu pojaviti?	172
Kako postajem meta hakera?	172
Dial-up nasuprot istrajnim konekcijama	175
Koji operativni sistemi računara su ranjivi?	175
Moj firewall će zaustaviti Pesky krekeri!	177
Koje vrste napadača postoje?	177
Korisnici skripti - Vaša najveća pretnja?	178
Crni šeširi - "Tamna strana"	178
Beli šeširi - Dobri momci	179
Operativni sistemi koje koriste krekeri	179
Windows operativni sistemi	179
Linux/NetBSD/FreeBSD	179
OpenBSD	180
Da li postoji tipičan napad?	181
Denial-of-service napadi	181
Virusi, trojanci i zlobni skriptovi ili web sadržaj	182
Web nagrđenost/"etiketiranje"	183
Napadi iznutra	183
Ko je najčešće napadnut?	184
Kućni i korisnici malog Internet biznisa	184
Ogromni poslovi i korporacije	184
Vlada i vojne institucije	184
Finansijske institucije	185
Koji je motiv napada?	185
Ozloglašenost, ili faktor "elite"	186
Zlobnost i destrukcija	186
Pravljenje političke izjave	187
Finansijska zarada	188
Krekovanje radi saznanja	191
Lomljenje radi ulaska	191
Zaključak	191

Deo III: Skup alata zaštite 193

10.	Firewalls	195
	Šta je firewall?	195
	Druge pronađene karakteristike proizvoda firewall	196
	Firewall nije neprobojan	198
	Pogledajmo proizvode firewalla	199
	Firewalls bazirani na paketu filtra	199
	Firewalls bazirani na potpunom paketu filtra	201
	Firewall baziran na proksiju	201
	Programeri koji zaobilaze firewall	202
	Zamke za firewall	203
	Uređaji firewalla	204
	Izgradnja firewalls u stvarnom svetu	205
	Identifikovanje topologije, aplikacije i potreba protokola	206
	Analiza odnosa kojima se veruje i putevi komunikacije u Vašoj organizaciji	208
	Procena i izbor proizvoda firewalla	208
	Razvoj i testiranje Vašeg firewalla	209
	Primer nedostataka firewall tehnologije	210
	"Kuda ide moj web server?" problem	211
	Korišćenje SSH za zaoblazanje skupa pravila	212
	Komercijalni firewalls	213
	BlackICE	214
	BorderManager	214
	FireBOX	214
	Firewall-1	214
	FireWall Server	215
	GNAT Box firewall	215
	Guardian	215
	NetScreen	215
	PIX firewall	216
	SideWinder	216
	Sonicwall	216
	Symantec Enterprise firewall	216
	Tiny Personal firewall	217
	ZoneAlarm Pro	217
	Zaključak	217
	Knjige i publikacije	217
	Internet resursi	218

11.	Alati za procenu ranjivosti (skeneri)	219
	Istorija skenera ranjivosti	219
	Kako rade skeneri ranjivosti	221
	Šta tražiti kada se bira skener	223
	Osnovne mane	225
	Najbolji skeneri ranjivosti	226
	Retina	226
	NetRecon	227
	ISS Internet Scanner	227
	Cybercop Scanner	228
	Open Source Nessus Project	228
	Whisker	229
	Drugi skeneri ranjivosti	229
	HackerShield	229
	Update	229
	Cisco skener	230
	SAINT	230
	SARA, TARA i WebMon	230
	STAT	230
	Analizator sigurnosti	230
	Zaključak	230
12.	Sistemi za otkrivanje napada	231
	Uvod u otkrivanje napada	231
	Ko treba da koristi IDS	233
	IDS bazirani na mreži	233
	ID sistemi bazirani na hostu	235
	IDS bazirani na anomaliji	236
	Šta tražiti kada se bira IDS	236
	Opšti kriterijum ocene	237
	Snort i druga Open Source IDS rešenja	239
	Listing proizvoda za otkrivanje napada	240
	Cisco Secure IDS	240
	Computer Associates eTrust Intrusion Detection	240
	Enterasys Dragon IDS	240
	Intrusion SecureNet NID/SecureHost HID	241
	IntruVert IntruShield	241
	ISS RealSecure	241
	ISS BlackICE	242
	NFR Network Intrusion Detection System	242
	nSecure softver nPatrol	243
	Symantec NetProwler i Intruder Alert	243
	Zaključak	243

13.	Alati prijavljivanja	245
	Zašto prijava?	245
	Prijave iz perspektive krekovanja	245
	Formiranje strategije prijavljivanja	246
	Nadgledanje mreže i prikupljanje podataka	248
	SWATCH (sistemski posmatrač)	249
	Watcher	249
	Isof (lista otvorenih fajlova)	250
	Private-I	250
	WebSense	250
	Win-Log verzija 1	251
	SNIPS	251
	Alati za analiziranje fajlova prijave	251
	NetTracker	251
	LogSurfer	251
	WebTrends za firewalls i VPN	252
	Analog	252
	Zaključak	252
14.	Sigurnost lozinke	255
	Uvod u krekovanju lozinke	255
	Šifrovanje lozinke 101	257
	ROT-13	258
	DES i Crypt	259
	Proces krekovanja lozinke	263
	Krekeri lozinke	265
	Krekeri lozinke za Windows	265
	L0phtCrack/LC4	265
	John the Ripper proizveo je Solar Designer	266
	NTCrack	266
	Krekovanje Unix lozinke	268
	O Unix sigurnosti lozinke	268
	Crack	269
	John the Ripper proizveo je Solar Designer	271
	PaceCrack95 (pacemkr@bluemoon.net)	271
	Star Cracker proizveo je Sorcerer	272
	Krekovanje Cisco, aplikacije i drugih tipova lozinke	272
	Krekovanje Cisco IOS lozinki	272
	Komercijalna aplikacija krekeri lozinke	273
	ZipCrack proizveo je Michael A. Quinlan	274
	AMI Decode (Autor nepoznat)	274
	PGPCrack proizveo je Mark Miller	275
	Poboljšanje Vaših lozinki sajta	275
	Windows NT/2000	276
	Passfilt Pro	276

	Password Bouncer	276
	Unix	277
	LDAP serveri	277
	Drugi resursi	277
	Internet resursi	278
	Publikacije i knjige	279
	Zaključak	280
15.	Njuškala (sniffers)	281
	Njuškala kao rizici sigurnosti	282
	Lokalne mreže i saobraćaj podataka	282
	Transport paketa i raznošenje	283
	Koji nivo rizika predstavljaju njuškala?	283
	Da li neko stvarno vidi napad njuškala?	283
	Koju informaciju njuškala hvataju?	284
	Gde možemo pronaći nešto nalik njuškalu?	285
	Gde mogu pronaći njuškalo?	286
	Komerijalna njuškala	286
	Besplatna njuškala	289
	Poražavanje napada njuškala	290
	Otkrivanje i eliminisanje njuškala	290
	Sigma topologija	292
	Sesije enkripcije	292
	Zaključak	293
	Deo IV: Oružje za masovno uništenje	295
16.	Alati za lišavanje servisa	297
	Šta je lišavanje servisa?	297
	Kako radi lišavanje servisa	298
	Eksploatisanje i lišavanje servisa	301
	Napadi resursa bombom elektronske pošte	301
	Napadi protokola	308
	Indeks napada lišavanja servisa	308
	Skorašnji DoS napadi	309
	Istorijska lista dobro poznatih DoS napada	311
	Distribuirani napadi lišavanja servisa	315
	Zaključak	318
	Drugi DoS resursi	318
17.	Virusi i crvi	319
	Razumevanje virusa i crva	319
	Šta je kompjuterski virus?	321
	Šta je kompjuterski crv?	323
	Rizik infekcije objekata virusom	323

	Ko piše viruse i zašto?	324
	Kako se kreiraju virusi?	326
	Šta znači stvarno "In the Wild"?	328
	Kako rade virusi?	329
	Memetic virusi	335
	Kako rade crvi?	337
	Karakteristike virusa	338
	Pomoćni antivirusni programi	341
	Network Associates	343
	Norton Anti-Virus	343
	AVG AntiVirus	343
	eSafe	343
	Antigen	343
	PC-Cillin	343
	Sophos Anti-Virus	344
	F-PROT Anti-Virus	344
	Integrity Master	344
	Budući trendovi u Viral Malware	344
	Publikacije i sajtovi	345
	Zaključak	348
18.	Trojanci	351
	Šta je trojanac?	351
	Poreklo vrste	352
	Definicije	352
	Nisam to mislio	353
	Klasifikacija trojanaca	355
	Odakle dolaze trojanci?	366
	Koliko često se trojanci stvarno otkrivaju?	367
	Koji nivo rizika predstavljaju trojanci?	369
	Kako detektovati trojanca?	370
	MD5	372
	Tripwire	373
	TAMU/TARA	374
	Na drugim platformama	375
	Resursi	376
	Zaključak	377
- Deo V:	Arhitekture, platforme i sigurnost	379
19.	Razmatranja mrežne arhitekture	381
	Mrežna arhitektura	381
	Mrežne komponente	382
	Pretnje	385
	Približavanje mrežnoj arhitekturi	386

	Sigurnosne zone	387
	Zaštita zamka	390
	Izolacija i odvajanje	390
	Odvajanje mreža	398
	Mrežna izolacija	401
	Zaključak	407
20.	Microsoft	409
	Windows 9x i Windows Me	410
	Šema lozinki za listu lozinki	410
	Zaključak za Windows 9x i Windows Me	411
	Windows NT	412
	Opšte sigurnosne ranjivosti Windows-a NT	412
	Druge značajne ranjivosti manjeg značaja	415
	Unutrašnja sigurnost Windows NT-a	415
	Uopšteno o unutrašnjoj sigurnosti	415
	Postizanje dobre unutrašnje sigurnosti	416
	Savet za postavljanje od nule sigurnog Windows NT Servera	417
	Zaključak za Windows NT	417
	Windows 2000	417
	Poboljšanja sigurnosti	418
	Pregled distribuirane sigurnosti Windows 2000	419
	Opšte sigurnosne ranjivosti Windows 2000	420
	Zaključak za Windows 2000	423
	Windows XP	423
	Sigurnosna poboljšanja Windows XP	423
	Moderne ranjivosti u aplikacijama Microsoft	424
	Microsoft Internet Explorer	424
	Microsoft Exchange Server	427
	Internet Information Server	430
	Alati	434
	Softver za kontrolu pristupa	439
	Dobri online izvori informacija	442
	Knjige za Windows 2000 i Windows NT sigurnost	443
	Zaključak	444
21.	Unix	445
	Tura istorijom Unixa sa kratkim zadržavanjem	446
	Klasifikovanje distribucija Unixa	448
	Nerazvijena	448
	Glavna struja	448
	Koliko je siguran otvoreni izvorni kod?	450
	Ojačani operativni sistemi	452
	Linux Kernel Patch	455
	Poverljivi sistemi u više nivoa	456

118	24	Sigurnosna razmatranja pri izboru distribucije	460
118		Sigurnosni rizici Unixa	461
118		Korisnički računi	463
118		Sigurnost fajl sistema	466
118		Rizici fajl sistema	470
118		Protivmere fajl sistema	471
118		Problem set-uid-a	473
118		Razbijanje programa set-uid zbog zabave i profita	477
118		Korisni alati za istraživača	479
118		Rootkit-ovi i odbrane	481
118		Protivmere za rootkit-ove	482
118		Rootkit-ovi kernel-a	484
118		Zaštita protiv napada na kernel	486
118		Mrežna sigurnost na hostu	487
118		Mrežni servisi: opšte svrhe u odnosu na "podesni za svrhu"	487
118		Rizici pokretanja mrežnih servisa	489
118		Osiguravanje mrežnih servisa	490
118		Onemogućavanje mrežnih servisa	491
118		Reč o privilegovanim portovima	492
118		Zaštićivanje od napada oćimanja servisa	494
118		Detektovanje lažnih servera	494
118		Telnet	495
118		Rizici protokola TELNET	496
118		Osiguravanje Telnet-a	498
118		Osnovni alat: Secure Shell	499
118		SSH protokoli	499
118		SSH serveri	499
118		SSH klijenti	500
118		Resursi SSH-a	501
118		FTP	501
118		Rizici FTP-a	502
118		Osiguravanje FTP-a	503
118		r servisi	504
118		Rizici r servisa	505
118		Kontramere	505
118		REXEC	505
118		Rizici REXECREXEC-a	505
118		Osiguravanje REXEC-a	506
118		SMTP	506
118		Rizici SMTP-a	506
118		Osiguravanja SMTP-a	507
118		DNS	508
118		Rizici DNS-a	508
118		Osiguravanje DNS-a	510
118		finger	511

	SNMP	511
	Rizici SNMP-a	511
	Osiguravanje SNMP-a	512
	Network File System	513
	Rizici NFS-a	513
	Osiguravanje NFS-a	513
	Upozorenja chroot-a	514
	Bolje samostartujući program koji znate... ..	515
	Procenjivanje Unix sistema u odnosu na ranjivosti	517
	Zaključavanje hosta	519
	Resursi za ojačavanje hosta	519
	GNU/Linux	523
	Zaključak	525
22.	Novell NetWare	527
	Činjenice o životu OS-a	527
	Posmatranje velike trojke	528
	Serversko okruženje	529
	Klijentsko okruženje	536
	Okruženje Novell Directory Services-a (NDS)	537
	Dalje čitanje	545
	Zaključak	546
23.	Routeri, switchevi i hubovi	547
	Problemi sa infrastrukturnom opremom	548
	Držanje koraka sa revizijom OS-a	549
	Osiguravanje hub-ova	550
	Osiguravanje switcheva	550
	Osiguravanje i konfigurisanje routera	550
	Osiguravanje mesta logovanja	551
	Držanje administratora odgovornim	553
	Onemogućavanje nepotrebnih servisa	553
	Razmatranja mrežnog upravljanja	554
	Centralizovanje logovanja	555
	Razmatranja o smeštanju lozinki	555
	Vreme sinhronizacije	556
	Razmatranja SNMP-a	557
	Sprečavanje ometanja i drugih igara sa paketima	558
	Filtriranje izlaza (egress filtering)	558
	Filtriranje ulaza	559
	Zaustavljanje budalastih igara sa paketima	560
	Zaključak	561
	Dalje čitanje i referenciranje	561

24.	Macintosh	563
	Mac OS X - Apple-ov novi operativni sistem	564
	Uspostavljanje Macintosh-a kao servera	565
	WebSTAR serverski skup regrutovan od strane armije SAD-a	566
	Vruća linija za deljenje ideja i fajlova	567
	Moć Mac OS X Server-a	567
	Ranjivosti na Macintosh platformi	568
25.	AtEase-ov bug pristupa (AtEase Acces Bug)	569
	AtEase-ov bug PowerBook-a 3400 (AtEase PowerBook 3400 Bug)	570
	Odbijanje servisa pomoću prekoračenja portova (Denial of Service by Port Overflow)	570
	Sigurnost DiskGuard-a (DiskGuard Security)	570
	Ranjivost FWB Hard Disk Toolkit-a 2.5	571
	Bug MacDNS	572
	Network Assistant	572
	Sigurnost lozinke na unapređivanjima programa Mac OS 8.0	573
	Sequence of Death i WebSTAR	573
	Mac OS X-ove softverske ranjivosti	574
	Sigurnosna zabrinutost za lokalni host	575
	O deljenju fajlova i sigurnosti	575
	Sigurnost fajlova Mac OS-a 9	576
	Sigurnost fajlova Mac OS X-a	577
	Upravljanje i sigurnost servera	578
	EtherPeek	580
	InterMapper 3.6	581
26.	MacAnalysis	581
	MacSniffer - Mac OS X	582
	ettecap	583
	HenWen sa Snort-om	583
	StreamEdit	584
	MacRadius	584
	Network Security Guard	585
	Oyabun Tools	586
	Silo 1.03	587
	Nmap	587
	Timbuktu Notes	588
	Zaštita firewall-om	588
	IPNetSentry	589
	NetBarrier	590
	Norton Personal Firewall	590
	Unutrašnja sigurnost	590
	Mac OS X-va zaštita pomoću screensaver-a sa lozinkom	591
	Logovanje na Mac OS X	591
	BootLogger	592
	DiskLocker	592

Empower	593
Ferret	593
Filelock	593
FullBack	594
Invisible Oasis	594
TypeRecorder	594
KeysOff i KeysOff Enterprise	595
LockOut	595
OnGuard-ove lozinke za opasnost	595
Password Key	596
Lozinke za opasnost za Password Security Control Panel	596
Aladdin Secure Delete	597
Zaključavanja pomoću SecurityWare-a	597
Stealth Signal	597
Mac OS X-ov root mod za jednog jedinog korisnika	598
Super Save 2.02	598
SubRosa Utilities	599
Open Firmware-ova zaštita lozinkom	599
Krekeri lozinki i povezani uslužni programi	601
FMP Password Viewer Gold 2.0	601
FMPProPeeker 1.1	601
Radionica Macintosh Hacker-a (Macintosh Hacker's Workshop)	602
John the Ripper	602
Killer Cracker	602
MacCrack	603
MagicKey 3.2.3a	603
MasterKeyII	603
McAuthority	603
Meltino	604
Password Killer	604
Anonimni mail-ovi i bombardovanje mail-ovima	604
Caem	604
Bomba	605
NailMail X	605
Spic & Spam	605
ATT Blitz	605
Virusi, crvi i antivirusna rešenja za Macintosh	605
MacVirus.Info	606
.Mac	607
Naorton Anti-Virus	607
Intego VirusBarrier	608
Disinfectant	608
AutoStart uklanjač crva	609
Little Dutch Moose	609
Pregled virusa za Mac OS X	609

188	Softver za špijuniiranje (spyware) i detekcija	610
188	MacScan	611
189	Resursi	612
189	Knjige i izveštaji	612
280	Sajtovi sa alatima i ratnom opremom	613
282	E-zine-ovi i web sajtovi	613
188	25. Načela, procedure i primenjivanje	615
188	Značaj sigurnosnih načela	615
190	Sigurnosna načela sajta i infrastrukture	616
191	Objektna i fizička sigurnosna razmatranja	616
192	Infrastruktura i kompjutersko okruženje	619
192	Prijvatljiva upotreba	637
198	Administrativna sigurnosna načela	637
197	Načela prihvatljive upotrebe za korisnike	638
198	Primenjivanje načela	639
199	Zaključak	641
200	Sigurnost lozinki	641
200	Revidiranja i analize	641
200	Sigurnosna načela za lokaciju	642
201	Upravljanje incidentima	642
202	Konfiguracija sistema	642
102	Deo VI: Sigurnost i integrisani servisi	643
102	26. Sigurni razvoj aplikacija, jezici i proširenja	645
102	Sigurnost i softver	645
102	Šta je sigurna aplikacija?	646
102	Neprijatelj unutar (Vašeg koda)	647
102	Sporna pitanja vezana za konfiguraciju	647
102	Uslovi trke	648
102	Prekoračenja bafera	650
102	Zaštita podataka	653
102	Privremeno smeštanje	653
102	Odbijanje servisa	654
102	Ulazne i izlazne metode	655
102	Sigurnosna arhitektura	656
102	Komponente sigurnosne arhitekture	656
102	Sigurnosni zahtevi	660
102	Identifikacija oblasti rizika	666
102	Sigurnosna reakcija	667
102	Dizajn sa svesnošću za sigurnost	667
102	Analize u fazi dizajna	668
102	Prakse sigurnosnog kodiranja	675
102	Zamke C-a	676

Perl aplikacije	681
Mi Java Es Su Java	683
C#/ .NET	684
Shell igra i Unix	684
Internet uređaji	685
Zaključak	685

27. Revidiranje bežične sigurnosti	687
Bežična LAN topologija	688
Tačke pristupa	690
NetGear-ova pristupna tačka ME102	691
Antene	692
Nasumično ograničena Yagi antena: HyperLink HG2415Y	695
Antena sa paraboličnom mrežom: Hyperlink HG2419G	696
SigMax-ova usmerena od tačkastog izvora: Signull SMISMCO10	697
SigMax-ov kružni Yagi: Signull SMISM CY12	698
TechnoLab-ov Log Periodic Yagi (Logaritamski periodični Yagi)	699
Bežične mrežne kartice	700
Kartica ORiNOCO PC	700
Uređaji koji mogu da se drže u ruci	700
Compaq iPAQ	701
Konstruisanje bežične laboratorije za testiranje	702
Bežični napadi	703
Prismostra	705
Ratna vožnja (war driving)	708
Hakovanje sa klijenta na klijent	716
Tačke pristupa-varalice (rogue access point)	721
Ometanje (odbijanje servisa)	723
Praktično krekovanje WEP-a	726
Zaključak	727

Deo VII: Preporuke **729**

A. Bibliografija sigurnosti - dalje čitanje	731
Opšta sigurnost na Internetu	731
TCP/IP	740
Na NetWare-u	742
B. Kako da dobijete više informacija	745
Ustanovljeni resursi	745
Sajtovi na WWW-u	745
Izveštaji i publikacije	747
Java	747
Baze podataka i sigurnost	748

Članci	749
Alati	749
Tehnički izveštaji, vladini standardi i radovi	753
Detekcija upada	757
Mailing liste	758
Podzemni resursi	759
C. Informacije proizvođača i sigurnosni standardi	761
Sigurnosne informacije prodavaca	761
Hewlett-Packard	761
IBM	762
Linux	763
Microsoft	763
Sun Microsystems	763
RFC dokumenti bitni za sigurnost	764
D. Šta je na CD-ROM-u	781
E. Rečnik	835
Indeks	871