

SADRŽAJ

Predgovor	xv
Uvod.....	xvii

Deo I

Upoznavanje žrtve

Slučaj iz prakse: kako vas ugrožava Google.....	2
1 Snimanje sistema.....	5
Šta je snimanje sistema?.....	6
Zašto je snimanje sistema neophodno?	6
Snimanje Internet sistema	7
Prvi korak: određivanje opsega snimanja	8
Drugi korak: pribavite potrebno ovlašćenje	8
Treći korak: javno dostupne informacije	8
Četvrti korak: popisivanje WHOIS i DNS	18
Peti korak: ispitivanje DNS-a.....	29
Šesti korak: upoznavanje mreže	33
Sažetak	36
2 Skeniranje	37
Otkrivanje živih sistema	38
Otkrivanje usluga koje rade ili oslušuju	47
Vrste skeniranja	48
Identifikovanje aktivnih TCP i UDP usluga	49
Skeneri priključaka koji rade pod Windowsom	55
Skeniranje priključaka – kratko.....	60
Prepoznavanje operativnog sistema	63
Uzimanje otiska aktivnog steka.....	64
Pasivno uzimanje otisaka steka	68
Sažetak	71
3 Popisivanje.....	73
Osnove otimanja zaglavlja	75
Popisivanje uobičajenih mrežnih usluga	77
Sažetak	125

Deo II

Napadanje sistema

Slučaj iz prakse: ja nisam ugrožen – imam Mac!	128
4 Napadanje Windowsa	131
Pregled poglavlja	134
O čemu ne govorimo	134
Napadi bez ovlašćenja	135
Napadi na Windowsove mrežne protokole	135
Realizacije Windowsovih Internet usluga	156
Napadi uz ovlašćenja	164
Proširivanje ovlašćenja	164
Utvrđivanje položaja	166
Daljinsko upravljanje i mala vrata	177
Preusmeravanje priključaka	181
Opšte mere zaštite od zloupotrebe ovlašćenja	183
Prikriivanje tragova	187
Windowsov bezbednosni sistem	190
Neprestano krpljenje sistema	190
Rad s grupama	190
IPSec	192
runas	193
.NET Framework	194
Windowsova zaštitna barijera	195
Sistem šifrovanih datoteka	195
Servisni paket 2 za Windows XP	196
Završnica: breme Windowsove bezbednosti	198
Sažetak	199
5 Napadanje Unixa	201
Potraga za administratorskim ovlašćenjima	202
Kratak pregled	202
Pronalaženje propusta	203
Daljinsko i lokalno pristupanje	203
Daljinsko pristupanje	204
Napadi podacima	208
Hoću svoje komandno okruženje	219
Najčešći tipovi daljinskih napada	224
Lokalno pristupanje	247
Osvajanje administratorskih ovlašćenja samo je početak	261
Oporavljanje sistema od napada administratorskim paketom	272
Sažetak	274

6	Napadanje daljinskih veza i usluge VoIP	277
	Priprema za pozivanje velikog broja telefonskih brojeva	279
	Automatsko pozivanje	281
	Hardver	281
	Zakonske norme	282
	Sporedni troškovi	282
	Softver	283
	Skriptovi za provaljivanje na silu iz domaće radinosti	297
	Napadanje telefonskih centrala	308
	Napadanje glasovne pošte	312
	Napadanje virtuelnih privatnih mreža (VPN)	317
	Napadi na uslugu VoIP	321
	Najčešće vrste napada	322
	Sažetak	328

Deo III

Napadanje mreža

	Slučaj iz prakse: ranjivost bežičnih mreža	330
7	Napadanje mrežnih uređaja	333
	Otkrivanje	334
	Prepoznavanje	334
	Pretraživanje autonomnog sistema	338
	Normalno korišćenje alatke traceroute	339
	traceroute uz ASN informacije	339
	show ip bgp	340
	Javne diskusione grupe	341
	Prepoznavanje usluga	342
	Ranjivost mreže	347
	Sloj 1 prema modelu OSI	348
	Sloj 2 prema modelu OSI	349
	Njuškanje skretnica	350
	Sloj 3 prema modelu OSI	362
	Loše konfiguracije	367
	Hakerisanje protokola za usmeravanje	372
	Hakerisanje protokola za upravljanje	383
	Sažetak	384
8	Hakerisanje bežičnih mreža	385
	Opipavanje bežičnih mreža	386
	Oprema	387
	Skeniranje i popisivanje bežičnih mreža	402
	Programi za njuškanje bežičnih mreža	403
	Alatke za bežično nadgledanje	406

Identifikovanje odbrambenih mera bežičnih mreža	413
SSID	414
Kontrola pristupa zasnovana na MAC adresama	415
Zadobijanje pristupa (hakerisanje mreže 802.11)	418
Kontrola pristupa zasnovana na MAC adresama	419
Napadi na algoritam mehanizma WEP	422
Obezbeđivanje WEP-a	423
Alatke za iskorišćavanje slabih tačaka algoritma WEP	423
Napadi na LEAP	427
Napadi u cilju uskraćivanja usluga	431
Pregled standarda 802.1x	432
Dodatni podaci	433
Sažetak	435
9 Barijere	437
Pejzaž barijera	438
Prepoznavanje barijera	439
Napredne tehnike otkrivanja barijera	443
Skeniranje kroz barijere	446
Filtriranje paketa	450
Slabosti zastupničkih servera aplikacija	453
Slabosti zastupničke barijere WinGate	455
Sažetak	457
10 Napadi u cilju uskraćivanja usluga	459
Uobičajene tehnike DoS napada	461
Tradicionalan DoS: ranjive tačke	462
Savremeni DoS napadi: iscrpljivanje kapaciteta	463
Mere zaštite od DoS napada	470
Osvrt na praktičnu stranu problema	470
Suprotstavljanje DoS napadima	471
Otkrivanje DoS napada	475
Odgovaranje na DoS napade	477
Sažetak	480

Deo IV

Hakerisanje softvera

Slučaj iz prakse: samo elita	482
11 Hakerisanje	483
Uobičajene tehnike zloupotrebe	484
Prelivanje bafera i projektni propusti	484
Napadi na mehanizam provere ulaznih podataka	490

Opšte mere zaštite	494
Ljudi: razvijanje kulture	494
Proces: bezbednost u razvojnom ciklusu softvera (SDL).	496
Tehnologija	504
Preporučena literatura	505
Sažetak	506
12 Hakerisanje Weba	507
Napadanje Web servera	508
Datoteke uzorci	510
Otkrivanje izvornog koda	511
Napadi na kanonizaciju	511
Programska proširenja servera	512
Prelivanja bafera	514
Skeneri ranjivih tačaka Web servera	516
Hakerisanje Web aplikacija	517
Pronalaženje ranjivih Web aplikacija pomoću Googlea.	518
Pretraživanje Weba	519
Seciranje Web aplikacije	520
Uobičajene ranjive tačke Web aplikacija.	532
Sažetak	542
13 Napadanje korisnika	543
Slabosti klijentskog softvera za Internet	544
Kratka istorija napadanja klijenata na Internetu	545
JavaScript i aktivno skriptovanje.	549
Kolačići	550
Zlonamerno skriptovanje dinamički generisanih Web strana	552
Neovlašćeno šetanje kroz okvire i domene	553
Napadi na protokol SSL	554
Ispuštanje zloćudnog tovara	556
Hakerisanje e-pošte	558
Usluga Instant Messaging (IM)	562
Zloupotreba Microsoftovih klijenata za Internet i mere zaštite	563
Opšte mere zaštite Microsoftovog klijentskog softvera.	571
Zašto, osim Microsoftovog, ne treba koristiti drugi klijentski softver?	583
Alternativan klijentski softver za Internet	585
Mrežne službe	590
Socijalno-tehničke metode napadanja: pecanje i krađa identiteta	594
Tehnike pećanja	594
Uznemirujući i lažljivi softver: špijuniranje, propagiranje i zatrpavanje neželjenim porukama	598
Uobičajene tehnike ubacivanja	599
Blokiranje, otkrivanje i uklanjanje uznemirujućeg i lažljivog softvera	601

Zloćudni softver	604
Vrste zloćudnog softvera i uobičajene tehnike napadanja	604
Otkrivanje i uklanjanje zloćudnog softvera	612
Fizičko obezbeđivanje za krajnje korisnike	617
Sažetak	618

Deo V

Dodaci

A Priključci	621
B Četrnaest najopasnijih bezbednosnih propusta	627
Spisak termina korišćenih u knjizi	629
Indeks	633