

OBSAH

PŘEDMLUVA	XIX
PODĚKOVÁNÍ	XXI
ÚVOD	XXIII
INTERNETOVÁ BEZPEČNOST – SMRT ZPŮSOBENÁ TISÍCI ŠKRÁBNUTÍMI ..	XXIII
Řešení: Více Informací	xxiv
Co je nového ve druhém vydání	xxv

ČÁST 1

PŘÍPRAVA PŮDY

	STUDIE: NOVÉ ZBOŽÍ	2
1	Hledání stop	3
	CO TO JE VYHLEDÁVÁNÍ STOP?	4
	Proč je hledání stop tak důležité?	4
	HLEDÁNÍ STOP V INTERNETU	4
	Krok 1. Určení sféry zájmů	5
	Krok 2. Mapování sítě	8
	Krok 3. Zkoumání DNS	17
	Krok 4. Průzkum sítě	21
	SHRNUTÍ	24
2	Skenování	25
	IDENTIFIKACE FUNKČNÍCH SYSTÉMŮ	26
	IDENTIFIKACE BĚŽÍCÍCH SLUŽEB	32
	Typy skenů	32
	Identifikace služeb TCP a UDP	33
	Skenery na platformě Windows	38

	Obrana proti skenování portů	42
	IDENTIFIKACE OPERAČNÍHO SYSTÉMU	45
	Aktivní identifikace operačního systému	45
	Pasivní identifikace operačního systému	48
	AUTOMATIZOVANÉ UTILITY	50
	SHRNUTÍ	51
3	Inventarizace	53
	INVENTARIZACE WINDOWS NT/2000	54
	[§] Inventarizace síťových prostředků NT/2000	57
	Inventarizace počítačů s NT/2000	67
	Inventarizace aplikací a bannerů NT/2000	77
	INVENTARIZACE NOVELL NETWARE	81
	Analýza Okolních počítačů	81
	INVENTARIZACE UNIXU	84
	INVENTARIZACE BGP	93
	SHRNUTÍ	95

ČÁST 2

HACKOVÁNÍ SYSTÉMU

	STUDIE: ZASTAVTE SE A PŘIVOŇTE K RŮŽÍM	98
4	Hackování Windows 95, 98 a ME	99
	SÍŤOVÉ ÚTOKY NA WIN9X	100
	Přímé připojení ke sdíleným prostředkům	101
	Zadní vrátka a trojští koně	105
	Chyby v serverových aplikacích	109
	DoS útoky na Win9x	109
	LOKÁLNÍ ÚTOKY NA WIN9X	110
	WINDOWS MILLENIUM (ME)	115
	Síťové útoky na WinMe	115
	Lokální útoky na WinMe	116
	WINDOWS XP HOME EDITION	117
	ICF (Internet Connection Firewall – firewall pro připojení do Internetu)	118
	Integrovaný MS Passport – jednorázový login pro Internet	118
	Vzdálené řízení	118
	SHRNUTÍ	119
5	Hackování Windows NT	121
	PŘEHLED	122

Kam míříme	123
A co Windows 2000?	123
PÁTRÁNÍ PO ÚČTU ADMINISTRÁTORA	124
Vzdálené útoky: Odmítnutí služby a přetečení vyrovnávací paměti	136
Zvýšení privilegií	139
UPEVNĚNÍ MOCI	149
Zneužívání důvěry	157
Sniffery	163
Vzdálené ovládání a zadní vrátka	166
Přesměrování portů	176
Obecná opatření proti kompromitaci přístupových oprávnění	179
ROOTKIT: ÚPLNÁ KOMPROMITACE	182
ZAHLAZENÍ STOP	184
Vypnutí auditu	184
Odstranění protokolu událostí	185
Skrývání souborů	185
SHRNUTÍ	187
6 Hackování Windows 2000	189
STOPOVÁNÍ	190
SKENOVÁNÍ	191
ZÍSKÁVÁNÍ UŽITEČNÝCH INFORMACÍ	195
PRŮNIK	197
Hádání hesel NetBIOS-SMB	197
Odposlouchávání hašů hesel	198
SMBRelay	198
Útoky na IIS 5	205
Vzdálené přetečení vyrovnávací paměti	205
ODMÍTNUTÍ SLUŽBY	205
ZVÝŠENÍ PRIVILEGIÍ	210
VYKRÁDÁNÍ ÚDAJŮ	214
Zmocnění se hašů hesel ve Windows 2000	214
Šifrovaný souborový systém EFS	219
Zneužívání důvěry	224
ZAHLAZENÍ STOP	226
Vypnutí auditu	226
Odstranění protokolu událostí	226
Skrývání souborů	227
ZADNÍ VRÁTKA	227

	Manipulace při startu systému	227
	Vzdálené ovládání	229
	Zaznamenávání stisknutí kláves	231
	OBCENÁ PROTIPATŘENÍ: NOVÉ BEZPEČNOSTNÍ NÁSTROJE VE WINDOWS	232
	runas	234
	BUDOUCNOST SYSTÉMU WINDOWS 2000	235
	.NET FRAMEWORK	235
	KÓDOVÉ OZNAČENÍ WHISTLER	236
	Verze Whistler	236
	Bezpečnostní vlastnosti Whistlera	236
	Poznámka o Raw Sockets a dalších nedoložených tvrzeních	239
	SHRNUTÍ	239
7	Hackování Novell NetWare	243
	PŘIPOJIT SE, ALE NEDOTÝKAT	244
	ZMAPOVÁNÍ BINDERY A NDS STROMŮ	246
	JAK OTEVŘÍT ODEMKNUTÉ DVEŘE	252
	ZÍSKÁNÍ ADMINA	257
	ZRANITELNOST APLIKACÍ	259
	SPOOFING ÚTOKY (PANDORA)	262
	A JSTE JAKO ADMIN NA SERVERU	264
	ZÍSKÁNÍ NDS SOUBORŮ	266
	OŠETŘENÍ LOGŮ	270
	Záznamy konzoly (Console Logs)	272
	ZÁVĚR	275
8	Hackování UNIXu	277
	HLEDÁNÍ ROOTA	278
	Krátký přehled	278
	Mapování slabých míst	278
	VZDÁLENÝ VERSUS LOKÁLNÍ PŘÍSTUP	279
	VZDÁLENÝ PŘÍSTUP	280
	Datové útoky	283
	Já chci shell	289
	Běžné typy síťových útoků	292
	LOKÁLNÍ PŘÍSTUP	311
	KONTO SUPERUŽIVATELE JE NAŠE, CO DÁL?	327
	Rootkity	327
	Uvedení napadeného systému do původního stavu	337
	SHRNUTÍ	338

HACKOVÁNÍ SÍTĚ

	STUDIE: POUŽITÍ VŠECH TĚCH ŠPINAVÝCH TRIKŮ	342
9	Hacking vytáčeného spojení PBX, hlasové pošty a sítě VPN	345
	PŘÍPRAVA K ÚTOKU	347
	HROMADNÉ VYTÁČENÍ	348
	Hardware	348
	Právní otázky	349
	Náklady na meziměstské hovory	349
	Software	349
	ÚTOKY HRUBOU SILOU	361
	ÚTOKY NA POBOČKOVÉ ÚSTŘEDNY	370
	SYSTÉMY HLASOVÉ POŠTY	374
	ÚTOKY NA VPN	378
	SHRNUTÍ	382
10	Síťová zařízení	385
	OBJEVOVÁNÍ	386
	Detekce	386
	SNMP	393
	ZADNÍ DVÍŘKA	396
	Implicitní konta	396
	Slabá místa	399
	SDÍLENÍ VERSUS PŘEPÍNÁNÍ	406
	Identifikace média	406
	Hesla na stříbrném podnosu: Dsniff	407
	Odposlouchávání na síťovém přepínači	409
	ÚTOKY NA BEZDRÁTOVÉ SÍTĚ	416
	Bezdrátová LAN IEEE 802.11	416
	WAP (Celulární telefon)	418
	SHRNUTÍ	419
11	Firewally	421
	TYPY FIREWALLŮ	422
	IDENTIFIKACE FIREWALLU	422
	Pokročilé vyhledávání firewallů	427
	SKENOVÁNÍ SKRZ FIREWALLY	430
	FILTROVÁNÍ PAKETŮ	434

ZRANITELNOST APLIKAČNÍCH PROXY SERVERŮ	437
Chyby programu WinGate	438
SHRNUTÍ	441
12 Útoky typu DoS	443
MOTIVACE ÚTOČNÍKŮ	444
TYPY DOS ÚTOKŮ	445
Obsazení přenosové kapacity linky	445
Přivlastnění systémových zdrojů	446
Chyby v programech	446
Útoky na DNS a systémy směrování paketů	446
OBECNÉ DOS ÚTOKY	447
Cílové systémy	449
DOS ÚTOKY NA UNIX A WINDOWS NT	452
Síťové útoky typu DoS	453
Distribuované útoky DoS	456
Lokální útoky typu DoS	461
SHRNUTÍ	462

ČÁST 4

HACKOVÁNÍ SOFTWARE

STUDIE: TICHÝ A SMRTÍCÍ	464
13 Slabá místa vzdáleného přístupu	465
ODHALENÍ SOFTWARE PRO VZDÁLENÝ PŘÍSTUP	466
PŘIPOJENÍ	466
SLABÁ MÍSTA	467
VNC (VIRTUAL NETWORK COMPUTING)	473
TERMINAL SERVER OD MICROSOFTU A CITRIX ICA	476
Server	476
Klient	476
Datové spojení	476
Vyhledávání cílů	477
Útok na Terminal Server	478
Další úvahy o bezpečnosti	481
SHRNUTÍ	483
14 Pokročilé metody	485
PŘEBÍRÁNÍ SPOJENÍ	486
ZADNÍ VRÁTKA	489

TROJŠTÍ KONĚ	508
KRYPTOGRAFIE	510
Terminologie	510
Třídy útoků	511
Útoky na Secure Shell (SSH)	511
NARUŠENÍ OPERAČNÍHO SYSTÉMU: ROOTKITy	
A NÁSTROJE PRO VYTVÁŘENÍ SNÍMKŮ SYSTÉMU	513
PRÁCE S LIDMI	515
SHRNUTÍ	517
15 Hackování webů	519
ANALÝZA WEBOVÉHO SERVERU	520
HLEDÁNÍ DOBRĚ ZNÁMÝCH CHYB	523
Odhalování bezpečnostních děr ve skriptech	523
Automatizované aplikace	525
ÚTOKY VYUŽÍVAJÍCÍ NEDOSTATEČNÉ KONTROLY VSTUPNÍCH DAT	528
Chyby v CGI	531
IIS a chyby v ASP (Active Server Pages)	533
Chyby serveru Cold Fusion	542
PŘEPLNĚNÍ VYROVNÁVACÍ PAMĚTI	544
ŠPATNÝ NÁVRH STRÁNEK	550
NÁSTROJE URČENÉ K ÚTOKŮM NA WEB	552
SHRNUTÍ	555
16 Hackování internetového uživatele	557
NEPŘÁTELSKÝ MOBILNÍ KÓD	558
Microsoft ActiveX	559
Bezpečnostní díry v Javě	568
Pozor na cookies	571
Chyby rámců HTML (frame) Internet Exploreru	574
ZNEUŽITÍ SSL	576
ZNEUŽÍVÁNÍ ELEKTRONICKÉ POŠTY	578
Generování e-mailů	578
Vykonání libovolného kódu prostřednictvím e-mailu	581
Outlook a červi šířící se pomocí adresáře	592
Útoky pomocí příloh dopisů (attachmentů)	594
Iniciování odchozích spojení	601
ÚTOKY NA IRC	604
ÚTOKY NA NAPSTER POMOCÍ WRAPSTERU	605
GLOBALNÍ OBRANA PROTI ÚTOKŮM NA INTERNETOVÉHO UŽIVATELE	606