

# 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: Hledání cíle .....	2
<b>1 Hledání stop .....</b>	<b>5</b>
Co to je Vyhledávání stop? .....	6
Proč je hledání stop tak důležité? .....	7
Hledání stop v Internetu .....	7
Krok 1. Určení sféry zájmů .....	8
Krok 2. Mapování sítě .....	12
Krok 3. Zkoumání DNS .....	20
Krok 4. Průzkum sítě .....	25
Shrnutí .....	28
<b>2 Skenování .....</b>	<b>29</b>
Typy skenů .....	38

Identifikace služeb TCP a UDP .....	39
Skenery na platformě Windows .....	44
Automatizované utility .....	58
Shrnutí .....	59
<b>3 Inventarizace systému .....</b>	<b>61</b>
Inventarizace Windows NT/2000 .....	62
Inventarizace síťových prostředků NT/2000 .....	66
Inventarizace uživatelů a skupin v NT/2000 .....	76
Inventarizace aplikací a bannerů NT/2000 .....	83
Automatizované skripty .....	86
Inventarizace Novell NetWare .....	87
Analýza Okolních počítačů .....	87
Inventarizace UNIXu .....	92
Shrnutí .....	99

## ČÁST 2

### HACKOVÁNÍ SYSTÉMU

Studie: Poznej svého nepřítele .....	102
<b>4 Hackování Windows 95, 98 a ME .....</b>	<b>103</b>
Síťové útoky na Win9x .....	104
Přímé připojení ke sdíleným prostředkům .....	105
Zadní vrátka a trojští koně .....	110
Chyby v serverových aplikacích .....	114
Lokální útoky na Win9x .....	115
Windows Millennium (ME) .....	120
Shrnutí .....	121
<b>5 Hackování Windows NT .....</b>	<b>123</b>
Přehled .....	124
Kam míříme .....	125
A co Windows 2000? .....	125
Pátrání po účtu administrátora .....	126

Vzdálené útoky: Odmítnutí služby a přetečení vyrovnávací paměti	140
Zvýšení privilegií	143
Upevnění moci	153
Zneužívání důvěry	162
Sniffery	168
Vzdálené ovládání a zadní vrátka	171
Přesměrování portů	181
Obecná opatření proti kompromitaci přístupových oprávnění	184
Rootkit: Úplná kompromitace	187
Zahlazení stop	189
Vypnutí auditu	190
Odstranění protokolu událostí	190
Skrývání souborů	191
Shrnutí	192
<b>6 Hackování Windows 2000</b>	<b>194</b>
Stopování	197
Skenování	197
Získávání užitečných informací	202
Průnik	204
Hádání hesel NetBIOS-SMB	204
Odposlouchávání haší hesel	204
Útoky na IIS 5	205
Vzdálené přetečení vyrovnávací paměti	207
Odmítnutí služby	208
Zvýšení privilegií	211
Vykrádání údajů	214
Zmocnění se haší hesel ve Windows 2000	214
Šifrovaný souborový systém EFS	219
Zneužívání důvěry	222
Zahlazení stop	224
Vypnutí auditu	224
Odstranění protokolu událostí	224

Skrývání souborů .....	225
Zadní vrátka .....	225
Manipulace při startu systému .....	225
Vzdálené ovládání .....	228
Zaznamenávání stisknutí kláves .....	230
Obecná protiopatření: Nové bezpečnostní nástroje ve Windows .....	230
Group Policy .....	230
runas .....	232
Shrnutí .....	233
<b>7 Hackování Novel NetWare .....</b>	<b>237</b>
Připojit se, ale nedotýkat .....	238
Zmapování Bindery a NDS stromů .....	240
Jak otevřít odemknuté dveře .....	246
Sbírání informací po přihlášení .....	247
Získání Admina .....	251
Zranitelnost aplikací .....	254
Spoofing útoky (Pandora) .....	256
A jste jako Admin na serveru .....	258
Získání NDS souborů .....	260
Ošetření logů .....	265
Další zdroje .....	269
Webové servery (ftp://ftp.novell.com/pub/updates/nw/nw411/) .....	269
Usenet Groups .....	269
Závěr .....	269
<b>8 Hackování UNIXu .....</b>	<b>271</b>
Hledání Roota .....	272
Krátký přehled .....	272
Mapování slabých míst .....	272
Vzdálený versus lokální přístup .....	273
Vzdálený přístup .....	274
Datové útoky .....	277
Já chci shell .....	281

Běžné typy síťových útoků .....	285
Lokální přístup .....	300
Konto superuživatele je naše, co dál? .....	315
Trojské koně .....	316
Uvedení napadeného systému do původního stavu .....	326
Shrnutí .....	327

### ČÁST 3

## HACKOVÁNÍ SÍTĚ

Studie: Sladké drobnosti .....	330
<b>9 Hacking vytáčeného spojení, PBX, hlasové pošty a sítě VPN .....</b>	<b>332</b>
Hromadné vytáčení .....	336
Hardware .....	336
Právní otázky .....	336
Náklady na meziměstské hovory .....	337
Software .....	337
Závěrečná poznámka .....	354
Útoky na pobočkové ústředny .....	356
Útoky na VPN .....	364
Shrnutí .....	368
<b>10 Síťová zařízení .....</b>	<b>369</b>
Objevování .....	370
Detekce .....	370
SNMP .....	377
Zadní dvířka .....	380
Implicitní konta .....	380
Slabá místa .....	383
Sdílení versus přepínání .....	389
Odposlouchávání na síťovém přepínači .....	393
Shrnutí .....	399
<b>11 Firewally .....</b>	<b>401</b>

Typy firewallů .....	402
Identifikace firewallu .....	402
Pokročilé vyhledávání firewallů .....	407
Skenování skrz firewally .....	410
Filtrování paketů .....	414
Zranitelnost aplikačních proxy serverů .....	417
Chyby programu WinGate .....	418
Shrnutí .....	421
<b>12 Útoky typu DoS .....</b>	<b>422</b>
Motivace útočníků .....	424
Typy DoS útoků .....	425
Přivlastnění systémových zdrojů .....	425
Chyby v programech .....	426
Útoky na DNS a systémy směrování paketů .....	426
Obecné DoS útoky .....	427
Cílové systémy .....	429
DoS útoky na UNIX a Windows NT .....	432
Síťové útoky typu DoS .....	433
Distribuované útoky DoS .....	436
Lokální útoky typu DoS .....	440
Shrnutí .....	442

#### ČÁST 4

### HACKOVÁNÍ SOFTWARE

Studie: Použití všech těch špinavých triků .....	444
<b>13 Slabá místa vzdáleného přístupu .....</b>	<b>447</b>
Odhalení softwaru pro vzdálený přístup .....	448
Připojení .....	448
Slabá místa .....	449
Který produkt je z hlediska bezpečnosti nejlepší? .....	455
pcAnywhere .....	455
ReachOut .....	456

	Remotely Anywhere .....	456
	Remotely Possible/ControlIT .....	456
	Timbuktu .....	457
	VNC (Virtual Network Computing) .....	457
	Citrix .....	460
	Shrnutí .....	460
<b>14</b>	<b>Pokročilé metody .....</b>	<b>461</b>
	Přebírání spojení .....	462
	Zadní vrátka .....	465
	Trojští koně .....	484
	Whack-A-Mole .....	485
	Narušení operačního systému: Rootkity a nástroje pro vytváření snímků systému .....	487
	Práce s lidmi .....	489
	Shrnutí .....	491
<b>15</b>	<b>Hackování webů .....</b>	<b>493</b>
	Analýza webového serveru .....	494
	Hledání dobře známých chyb .....	497
	Odhalování bezpečnostních děr ve skriptech .....	497
	Automatizované aplikace .....	499
	Útoky využívající nedostatečné kontroly vstupních dat .....	500
	Chyby v ASP (Active Server Pages) .....	507
	Přeplnění vyrovnávací paměti .....	514
	Špatný návrh stránek .....	519
	Shrnutí .....	522
<b>16</b>	<b>Hackování internetového uživatele .....</b>	<b>523</b>
	Nepřátelský mobilní kód .....	524
	Bezpečnostní díry v Javě .....	534
	Pozor na cookies .....	537
	Chyby rámců HTML (frame) Internet Exploreru .....	541
	Zneužití SSL .....	542
	Zneužívání elektronické pošty .....	544

Generování e-mailů .....	545
Vykonání libovolného kódu prostřednictvím e-mailu .....	548
Outlook a červi šířící se pomocí adresáře .....	554
Útoky pomocí příloh dopisů (attachmentů) .....	557
Útoky na IRC .....	564
Útoky na Napster pomocí Wrapsteru .....	565
Globální obrana proti útokům na internetového uživatele .....	566
Udržujte databáze antivirových programů aktuální .....	566
Sřežení bran do sítě .....	567
Shrnutí .....	567

## ČÁST 5

### PŘÍLOHY

<b>A</b>	<b>Porty .....</b>	<b>571</b>
<b>B</b>	<b>14 nejdůležitějších bezpečnostních děr .....</b>	<b>577</b>
<b>C</b>	<b>0 doprovodném webovém serveru .....</b>	<b>579</b>
	Novell .....	580
	UNIX .....	580
	Windows NT .....	581
	Slovníky a seznamy .....	582
	Hromadné vytáčení telefonních čísel .....	582
	Inventarizační skripty .....	582
	<b>Rejstřík .....</b>	<b>583</b>