

# Obsah

PODĚKOVÁNÍ .....	23
PŘEDMLUVA .....	25
ÚVOD .....	27

## ČÁST I SŽÍVÁME SE S LINUXEM

KAPITOLA 1 PŘEHLED ZABEZPEČENÍ SYSTÉMU LINUX .....	37
Proč se chtějí dostat k vašim právům superuživitele .....	38
Hnutí open source .....	39
Open source a bezpečnost .....	39
Klady modelu open source .....	40
Stinná stránka otevřeného softwaru .....	40
Uživatelé Linuxu .....	41
/etc/passwd .....	41
Typy uživatelů .....	42
Linuxové skupiny .....	43
Jak uživatele kontrolovat .....	44
Přístupová práva souborů .....	44
Atributy souborů .....	50
Kvóty .....	51
Limity .....	52
Schopnosti v Linuxu .....	54
Další možnosti zabezpečení .....	54
Signály .....	55
Privilegované porty .....	55
Správa virtuální paměti .....	56
Systémové protokolování .....	56
Shrnutí .....	57
KAPITOLA 2 AKTIVNÍ PREVENTIVNÍ OPATŘENÍ A ZOTAVENÍ Z PRŮNIKU .....	59
Aktivní opatření .....	60
Zjišťování bezpečnostních nedostatků .....	60
Skenery bezpečnosti systému .....	61
Jednoduchý příkaz find .....	61
COPS .....	62
Tiger .....	62
Nabou .....	63
Předved'te své vlastní síťové zvědy .....	64

Detekce skenování .....	65
Klaxon .....	66
Courtney .....	66
Scanlogd .....	67
PortSentry .....	67
Upevnění vašeho systému .....	69
Bastille .....	69
Linuxová záplata Openwall .....	70
LIDS .....	71
Analýza protokolových souborů .....	73
Nastavení programu syslogd .....	73
Sledování protokolových souborů .....	76
Soupravy protokolových analyzátorů .....	78
Logcheck .....	78
Swatch .....	79
Logsurfer .....	81
Dohlížení na integritu systému souborů .....	83
Kontrolní součty .....	84
Přístupová práva souborů .....	85
Generování databází kontrolních součtů a přístupových práv .....	86
Úskalí nástrojů souborové integrity .....	87
Existující nástroje souborové integrity .....	88
Tripwire .....	88
AIDE .....	89
Nabou .....	96
Zotavení z úspěšného útoku .....	96
Umění zjistit, kdy jste napadeni .....	97
Jak na průnik odpovědět .....	99
Zastavit ničení .....	99
Dostat se k průlomů .....	99
Návrat na síť .....	100
Další faktory .....	101
Odvětné útoky a protiúder .....	102
Černé díry .....	103
Shrnutí .....	103
<b>KAPITOLA 3 MAPOVÁNÍ VAŠEHO POČÍTAČE A VAŠÍ SÍŤE .....</b>	<b>105</b>
Online průzkum .....	107
Prohledávání newsgroups a mailing listů .....	107
Ochrana před průsakem informací do news a konferencí .....	109
Databáze Whois .....	109
Informace o registraci doménového jména .....	109
Seznamy domén .....	112
Vyhledávání sítí .....	112
Opatření proti zneužití whois .....	113
Hromadný ping .....	114
ICMP Ping .....	114
Echo port ping .....	114

Ohlašování přihlašování .....	375
Protokolování .....	376
Ohlašování procesů .....	377
Ohlašování souborů .....	378
Ohlašování síťového provozu .....	380
Bezpečnostní nástroje .....	380
Zadní vrátka .....	381
Síťové služby .....	381
Omezení síťového přístupu .....	381
Pravidla pro ověřování .....	382
Knihovny PAM .....	382
Modifikace síťových démonů .....	384
Lokální setXid programy .....	385
CGI .....	387
Opatření proti programům typu trójský kůň .....	388
„Vylepšení“ jádra .....	389
Nahrátelné jaderné moduly .....	389
Opatření proti jaderným modulům .....	395
Modifikace samotného jádra .....	395
Opatření proti pozměňování jádra .....	399
Rootkity .....	399
LRK – The Linux Root Kit .....	400
Opatření proti rootkitům .....	401
Shrnutí .....	402

## ČÁST IV PROBLEMATICKÉ OTÁZKY SERVERŮ

KAPITOLA 11 BEZPEČNOST POŠTY A FTP .....	407
Bezpečnost pošty .....	408
Poštovní servery .....	409
Sendmail .....	409
Qmail .....	410
Postfix .....	411
Bezpečnostní netěsnosti poštovních serverů .....	411
Superuživatelský přístup přes váš poštovní server .....	412
Provozování poštovního serveru pod zvláštním UID .....	412
Hlavičky poštovního serveru .....	413
Změna SMTP hlavičky u Sendmailu .....	413
Změna SMTP hlavičky u Qmailu .....	414
Změna SMTP hlavičky u Postfixu .....	414
Příkaz SMTP VRFY .....	414
Odstavení VRFY u Sendmailu .....	415
Odpovědi VRFY u Qmailu a Postfixu .....	416
Příkaz SMTP EXPN .....	416
Odstavení EXPN u Sendmailu .....	417
Odpovědi EXPN u Qmailu a Postfixu .....	417
Nevhodná přístupová práva .....	418

Kontrola přístupových práv souborů poštovního serveru .....	418
Předávání pošty .....	419
Opatření proti přeposílačům .....	420
Spam .....	421
Blokování spamu .....	422
Mailbomby a jiné útoky DoS .....	423
Vynucování omezení zdrojů v Sendmailu .....	423
Vynucování omezení zdrojů v Qmailu .....	423
Vynucování omezení zdrojů v Postfixu .....	424
Všemi zapisovatelný adresář pro poštu určenou k odeslání .....	425
Opatření pro všem přístupný adresář odesílané pošty .....	426
Otevřenost SMTP .....	426
Šifrování elektronické pošty a SMTP .....	426
Otevřená hesla u POP a IMAP .....	428
Opatření pro otevřená hesla POP a IMAP .....	428
File Transfer Protocol (FTP) .....	429
Protokol FTP .....	430
Ukázková FTP relace .....	430
Aktivní režim FTP .....	431
Pasivní režim FTP .....	432
Otevřená hesla .....	433
Opatření pro otevřená hesla .....	433
Informační FTP hlavičky .....	434
Změna FTP hlavičky u wu-ftpd .....	435
Změna FTP hlavičky u ProFTPD .....	435
Sledování portů přes FTP servery třetích osob .....	436
Nmap a průzkum přes FTP .....	437
Opatření proti průzkumu přes FTP servery .....	438
Únos dat pasivního FTP .....	440
Opatření proti unášení dat pasivního FTP .....	441
Únosy dat aktivního FTP .....	442
Opatření proti unášení dat aktivního FTP .....	443
Umožnění zprostředkovaného FTP .....	444
Útoky odrážené přes FTP .....	446
Opatření proti útokům odráženým přes FTP .....	447
Nepořádná pravidla pro FTP na firewallech .....	448
Přístup k zapovězeným portům FTP serverů za firewallem .....	448
Ochrana FTP serverů za firewallem .....	449
Nepovolený přístup k portům FTP klientů za firewally .....	450
Ochrana FTP serverů za firewallem .....	451
Potíže s anonymním FTP .....	451
Zkazitelné anonymní FTP servery .....	451
Opatření proti zkazitelným anonymním FTP serverům .....	451
Shrnutí .....	452
Poštovní servery .....	452
FTP .....	453
Opatření: nepoužívat FTP .....	453
KAPITOLA 12 WEB SERVERY A DYNAMICKÝ OBSAH .....	455
Vznesení HTTP požadavku .....	456

Získávání informací z hlavičky .....	457
Změna výchozí hlavičky .....	457
V případě potřeby aktualizujte starý software .....	458
Přístup k důvěrným datům .....	458
Ochrana webových dat IP omezeními .....	458
Použití HTTP autentizace .....	459
Odchycení autentizačního řetězce .....	459
Používejte bezpečné HTTP spojení .....	460
Umožnění .. v URL .....	462
Opatření pro ..: Používejte Apache .....	463
Web server Apache .....	463
Konfigurace Apache .....	464
Nebezpečné symbolické odkazy .....	465
Bezpečné nastavení symbolických odkazů .....	466
Získávání obsahu adresářů .....	466
Zabránění výpisům adresářů .....	467
Když tajemství není tajemstvím .....	467
Nespoléhejte se na tajemství .....	468
Děravé nastavení CGI .....	468
Vymezení CGI do určitých adresářů .....	469
Nepovolte spouštění CGI podle názvu souboru .....	469
Spouštění starších verzí CGI .....	470
Omezení přístupu k souborům podle jejich jména .....	470
Neschovávejte si staré kopie CGI programů .....	471
Děravé CGI programy ovlivňující další webová místa .....	471
CGI spouštějte pod různými uživateli .....	471
Útoky na špatně nastavenou HTTP autentizaci .....	472
Bezpečné použití souborů .htaccess pro HTTP autentizaci .....	472
Bezpečné použití httpd.conf pro HTTP autentizaci .....	473
Zneužití problémů výchozí konfigurace .....	474
Odstranění online příruček .....	474
Odstranění výchozí uvítací stránky .....	475
Zrušení spouštění CGI skriptů podle přípony .....	475
Bezpečné nastavení serverem zpracovávaných HTML souborů .....	475
Bezpečné nastavení zobrazování stavu serveru a dalších informací .....	476
Nastavení adresářů public_html .....	476
Zneužití výchozího nastavení proxy cache .....	476
Direktivy pro zabezpečení proxy serveru .....	477
Problémy se CGI programy .....	478
Zneužití dodaných a stažitelných CGI programů .....	478
Nedůvěřujte dodaným a staženým CGI programům .....	479
Děravé CGI programy .....	480
Předpoklad, že budou přijata jen očekávaná vstupní pole .....	480
Vždy kontrolujte obdržaná pole .....	482
Zneužití důvěry ve skrytá pole .....	482
Pro kontrolu skrytých polí použijte MD5 .....	483
Zneužití důvěry v délku uživatelem zadávaného vstupu .....	484
Vždy kontrolujte délku dat .....	485
Zneužití důvěry v hlavičky „Referer“ .....	485
Nespoléhejte se na hlavičky „Referer“ .....	486
Zneužití důvěry v cookies .....	486

Nespoléhejte se na cookies .....	487
Pro cookies používejte SSL .....	487
Zneužití důvěry v názvy souborů .....	487
Explicitní otevírání souborů v režimu pro čtení .....	488
Kontrola znaků v názvech souborů .....	488
Zaslaný vstup obsahuje znak „null“ .....	488
Kontrolujte znaky na vstupu .....	489
Zneužití předzpracování JavaScriptem .....	489
Nikdy nepředpokládejte, že došlo k předzpracování .....	490
Zneužívání trubek a volání systému .....	490
Nikdy nepoužívejte nezkontrolovaný vstup z formulářů pro systémová volání a trubky .....	491
Funkci system() volejte s parametry v seznamu .....	492
Použijte fork() a exec() .....	492
Zneužívání webových velkochovů .....	493
Poskytovatele vyberte rozvážně .....	494
Další web servery pro Linux .....	494
Shrnutí .....	495
<b>KAPITOLA 13 ŘÍZENÍ PŘÍSTUPU A FIREWALLY .....</b>	<b>497</b>
Přehled inetd a xinetd .....	498
inetd .....	498
Nastavení inetd .....	499
xinetd .....	499
Nastavení xinetd .....	500
Nežádoucí připojení hackera .....	502
Implementujte řízení přístupu s inetd a TCP wrappery .....	502
Pravidla pro TCP wrappery .....	503
Zavádění řízení přístupu u xinetd .....	505
Padělání „důvěryhodných“ odpovědí DNS .....	507
Opatření proti padělání zpětných DNS dotazů .....	507
Útočník v důvěryhodné doméně .....	508
Zablokování konkrétních hostitelů v doméně s inetd .....	508
Zablokování konkrétních hostitelů v doméně s xinetd .....	509
Útoky na služby nespojené s inetd/xinetd .....	509
Zakompilování podpory TCP wrapperů .....	509
Požádání správce programu o podporu TCP wrapperů .....	510
Implementujte si TCP wrappery sami .....	510
Zneužití nepořádně napsaných pravidel TCP wrapperů .....	511
Kontrola platnosti pravidel TCP wrapperů .....	511
Útoky na služby spouštěné z inetd založené na přetížení .....	513
Na obranu před přetížením použijte tcpserver .....	513
Na obranu před přetížením použijte xinetd .....	513
Firewally: řízení přístupu na úrovni jádra .....	514
Druhy firewallů .....	514
Proxy servery .....	515
Firewally filtrující pakety .....	515
Filtrování paketů na Linuxu .....	515
Přijetí paketu .....	516

Odmítnutí paketu .....	516
Popření paketu .....	516
V čem se iptables liší od ipchains .....	517
Blokování konkrétního síťového přístupu .....	518
Pokusy o ping nebo traceroute vašeho stroje .....	518
Popření ICMP pingu a traceroute s ipchains .....	519
Popření spojení na firewallu s iptables .....	520
Pokusy o připojení na port telnet .....	521
Popření spojení na firewallu s ipchains .....	521
Strategie pro firewall .....	521
Stavba firewallu s ipchains .....	522
Stavba firewallu s iptables .....	523
Firewallové produkty .....	524
Nástroje na konfiguraci firewallů .....	524
Open source firewally .....	524
Komerční firewally .....	524
Shrnutí .....	525

## ČÁST V DODATKY

DODATEK A ABY VAŠE PROGRAMY BYLY VŽDY ČERSTVÉ .....	529
RPM společnosti Red Hat .....	530
Dpkg a Apt na Debianu .....	533
Baličky Slackware .....	536
DODATEK B ZAKAZOVÁNÍ NEPOTŘEBNÝCH SLUŽEB .....	537
Úrovně běhu .....	538
Adresáře /etc/rc#.d .....	539
Vypínání služeb .....	539
Red Hat .....	540
SuSE .....	541
Síťové služby inetd .....	544
DODATEK C ONLINE ZDROJE .....	545
Mailing listy společností .....	546
Ostatní mailing listy zaměřené na bezpečnost .....	546
Stránky o bezpečnosti a hackingu .....	547
Newsové skupiny .....	548
Stránky Hacking Linux Exposed .....	548

DODATEK D PŘÍPADOVÉ STUDIE .....	549
Případová studie A .....	550
Pozadí .....	550
Pátrání .....	551
Pokus o přihlášení .....	552
Hledání dalších vrátek .....	552
Vetřelec vyhnán .....	554
Případová studie B .....	555
Sledování cíle .....	555
Mapování sítě .....	556
Cesta dovnitř .....	556
Návštěva místnosti serverů .....	557
Průnik do dohlížejícího hostitele .....	557
Prošetřování dobytého hostitele .....	558
Čmuchání po síti .....	561
Sledování protokolů .....	561
Zrušení čmuchání .....	562
Kam teď? .....	562
Hon .....	563
Nashledanou, ne však sbohem .....	563
Případová studie C .....	564
Skenování stroje .....	564
Ořukávání Sedmailu .....	565
Ořukávání web serveru .....	565
Hledání CGI programů .....	566
Útok na CGI programy .....	567
Zametání stop .....	569
Založení trvalého spojení .....	571
Průchod firewallem .....	572
Útoky z místního účtu .....	573
Skenování síťových služeb, pokus druhý .....	574
Útok na FTP server .....	575
Konec dobrý, všechno dobré .....	575



Fping .....	115
Hromadný ping s pomocí Nmap .....	115
Opatření proti hromadným pingům .....	116
DNS .....	117
Příklad vyhledávání v DNS .....	118
Bezpečnostní problémy DNS dotazů .....	118
Informační pole .....	119
Opatření proti zneužití informací z DNS .....	120
Přenosy zón .....	120
Opatření pro přenosy zón .....	121
Reverzní dotazy .....	123
Opatření pro reverzní dotazy .....	123
DNSSEC .....	124
Trasování .....	124
UNIX Traceroute .....	125
MTR .....	126
Opatření proti trasování .....	127
Sledování portů .....	127
Skener Netcat .....	127
Strobe .....	128
Nmap – sledování portů .....	130
Opatření proti sledování portů .....	135
Detekce OS .....	136
Otevřené porty .....	136
Opatření pro otevřené porty .....	137
SNMP .....	137
Opatření pro SNMP .....	137
Síťové hlavičky .....	137
Opatření pro síťové hlavičky .....	138
Aktivní testování síťového rozhraní (stack fingerprinting) .....	139
Queso .....	139
Nmap – detekce OS .....	139
Opatření proti aktivnímu testování síťového rozhraní .....	141
Pasivní testování síťového rozhraní .....	142
Siphon .....	142
Opatření proti pasivním testům síťového rozhraní .....	143
Výčet služeb RPC .....	143
Dotazování mapovače portů pomocí Rpcinfo .....	144
Zjišťování RPC služeb s Nmapem .....	145
Opatření proti výčtu služeb RPC .....	146
Sdílení souborů přes NFS .....	146
Dotazování NFS pomocí Showmount .....	147
Opatření pro Showmount .....	148
Protokol SNMP (Simple Network Management Protocol) .....	149
Dotazování SNMP pomocí Net-snmp .....	150
Opatření pro SNMP .....	152
Síťové bezpečnostní skenery .....	152

ISS .....	153
Satan/SAINT .....	153
SARA .....	155
Nessus .....	156
Opatření pro síťové skenery .....	160
Shrnutí .....	160

## ČÁST II ZVENKU DOVNITŘ

KAPITOLA 4 OVLIVŇOVÁNÍ, DANAJSKÉ DARY A JINÉ HACKERSKÉ ZÁLUDNOSTI .....	163
Sociální inženýrství .....	164
Kategorie sociálního inženýrství .....	165
Falšování postavení .....	165
Vydávání se za konkrétní osobu .....	166
Soucit .....	167
Osobní zájem .....	167
Sázka na samolibost .....	168
Nenápadná povolání .....	168
Odměna .....	169
Jakými kroky odrazit manipulaci .....	170
Buďte paranoidní .....	170
Ptejte se na všechno .....	170
Ověřte si zdroj .....	170
Odmítněte .....	170
Trénink uživatelů .....	171
Hackeři jsou vždy připraveni .....	171
Trójští koně .....	172
Programy – trójští koně .....	172
Opatření proti trójským koním .....	173
Ztrójštěný zdrojový kód .....	173
Prohlížejte kódy .....	174
Ověřujte kontrolní součty .....	175
Ověřujte PGP podpisy .....	177
Metody roznášky trójských koní .....	177
Fiktivní exploit skript .....	179
Viry a červi .....	180
Jak se viry a červi šíří .....	181
Viry a Linux .....	181
Existují tedy vůbec na Linuxu viry? .....	182
A co takhle skenovací software na linuxové viry? .....	182
Červi a Linux .....	183
Morrisův internetový červ .....	183
Červ Ramen .....	183
Opatření proti červu Ramen .....	186
Červi dnes .....	186
Zadní vrátka IRC .....	186

Shrnutí .....	187
KAPITOLA 5 FYZICKÉ ÚTOKY .....	189
Útok na kancelář .....	190
Pracovní plocha .....	191
Opatření proti ohrožení pracovního prostoru .....	192
Odpadní hospodářství .....	193
Opatření proti prohledávání odpadků .....	193
Atakování síťových tajemství .....	194
Prevence cizích objevů v oblasti vašich síťových tajemství .....	194
Zneužití přístupu ke konzoli .....	195
Opatření pro konzoli .....	196
Krádež laptopu .....	196
Opatření proti krádežím laptopů .....	197
Znovuzavedený systém = superuživatelský přístup .....	198
Dual booting .....	198
Opatření proti zneužití dual bootingu .....	199
Zaváděcí zařízení .....	199
Obrana proti zneužití zaváděcích zařízení .....	200
Prolamování BIOSu .....	201
Ochrana BIOSu .....	202
Zneužití LILO .....	202
Opatření proti zneužití LILO .....	204
Zašifrované systémy souborů .....	208
Shrnutí .....	210
KAPITOLA 6 NAPADENÍ PŘES SÍŤ .....	213
Použití sítě .....	214
Sítě TCP/IP .....	214
Protokol IP (Internet Protocol) .....	215
Protokol TCP (Transmission Control Protocol) .....	216
Protokol UDP (User Datagram Protocol) .....	217
Protokol ICMP (Internet Control Message Protocol) .....	218
Protokoly aplikační vrstvy .....	218
Veřejné telefonní sítě .....	219
Hromadné vytáčení (Wardialing) .....	219
Opatření proti hromadnému vytáčení .....	220
Výchozí nebo špatné nastavení .....	221
Sdílené souborové systémy NFS .....	221
Útok na špatně nastavené NFS .....	221
Opatření pro sdílené systémy souborů NFS .....	222
Výchozí nastavení produktů Netscape .....	222
Útok na výchozí nastavení produktů Netscape .....	222
Opatření pro výchozí nastavení produktů Netscape .....	223
Squid .....	223
Útok na špatně nastavený server Squid .....	223
Opatření proti špatnému nastavení serveru Squid .....	223
Systém X-Window .....	224

Útok na špatně nastavené X-Window .....	224
Opatření proti špatnému nastavení X-Window .....	224
Výchozí hesla .....	225
Výchozí heslo serveru Piranha .....	225
Opatření pro výchozí hesla serveru Piranha .....	226
Výchozí hesla síťových zařízení .....	226
Opatření pro výchozí hesla síťových zařízení .....	227
Sledování provozu .....	227
Jak sniffery fungují .....	227
Sniffery mohou zachytit uživatelská jména a hesla .....	228
Opatření proti sniffěrům .....	228
Obvyklé sniffery .....	229
Tcpcdump .....	229
Hunt .....	230
Linux-Sniff .....	230
Další sniffery .....	231
Hádání hesel .....	231
Získání přístupu uhodnutím hesel .....	231
Opatření proti hádání hesel .....	232
Slabá místa .....	234
Přetečení vyrovnávacích pamětí .....	234
Zranitelné služby .....	234
Přetečení vyrovnávacích pamětí služeb .....	235
Opatření pro přetečení vyrovnávacích pamětí .....	236
Zranitelné skripty .....	236
Slabá místa skriptů .....	236
Opatření pro skripty .....	236
Nepotřebné služby .....	237
Útoky přetížením (Denial-of-Service) .....	237
Opatření proti útokům přetížením .....	237
Netstat .....	237
Netstat může být vyměněn, aby poskytoval nesprávné informace .....	239
Opatření proti výměně Netstatu .....	239
Lsof .....	239
Identifikace služeb pomocí Nmapu .....	240
Vypínání služeb .....	242
Shrnutí .....	243
<b>KAPITOLA 7 ZNEUŽITÍ SAMOTNÉ SÍTĚ .....</b>	<b>245</b>
Zneužití DNS .....	246
Otrava cache BIND (cache poisoning) .....	246
Opatření proti otravě cache BIND .....	248
DNS spoofing s Dnsspool .....	250
Opatření proti Dnsspoof .....	250
Směrování (routing) .....	251
Směrování zdrojem (source routing) .....	251
Potlačení směrování zdrojem .....	252

Nevhodné IP přeposílání (IP forwarding) .....	252
Zrušení IP přeposílání .....	253
Doplňování nových síťových cest .....	253
Znemožnění doplňování nových cest .....	254
Pokročilý sniffing a unášení relací .....	254
Hunt .....	254
Sniffing na přepínaných sítích s Huntem .....	255
Unášení relací pomocí Huntu .....	257
Opatření proti Huntu .....	259
Dsniff .....	260
Útoky s prostředníkem (man-in-the-middle) .....	261
Sshmitm .....	261
Opatření proti Sshmitm .....	262
Webmitm .....	263
Opatření proti Webmitm .....	264
Útoky směřující k vyřazení z provozu (denial-of-service) .....	265
Záplavy (floods) .....	266
ICMP (ping) záplavy .....	266
Opatření proti ICMP záplavám .....	267
UDP záplavy .....	267
Opatření proti UDP záplavám .....	268
Smurf .....	268
Opatření proti Smurfu .....	268
Distribované DoS (DDoS) útoky .....	269
Opatření proti distribuovaným DoS útokům .....	269
TCP/IP útoky .....	270
Ping smrti (Ping of death) .....	270
Opatření proti pingu smrti .....	270
Teardrop („slza“) .....	270
Opatření proti Teardrop .....	271
Záplavy SYN .....	271
Opatření proti záplavám SYN .....	272
Zneužívání vztahů důvěry .....	272
IP závislosti v TCP wrapperech, příkazech r* a filtrech paketů .....	273
Odstranění protokolů používajících IP .....	273
NFS .....	273
Opatření pro NFS .....	274
NIS .....	274
Opatření pro NIS .....	275
Implementace filtrování egress .....	275
Shrnutí .....	277

### ČÁST III

## ÚTOKY PŘES LOKÁLNÍHO UŽIVATELE

KAPITOLA 8 ROZŠÍŘOVÁNÍ UŽIVATELSKÝCH PRÁV .....	281
Uživatelé a práva .....	282

Rozšiřování privilegií .....	283
Důvěryhodné cesty a Trojské koně .....	284
Zneužití uživatelů, kteří mají v PATH „“ .....	285
Odstraňte ze své cesty „“ .....	286
Trojské koně spuštěné z ošálených setuserid programů .....	286
Opatření pro nezabezpečená systémová volání .....	287
Uchování a používání hesel .....	287
Hesla uložená v uživatelských souborech .....	287
Likvidace hesel v souborech uživatelů .....	288
Hesla umístěná v systémových souborech .....	288
Ochrana systémových souborů s hesly .....	289
Zjistitelná podoba uložených hesel .....	289
Opatření pro rekonstruovatelná hesla .....	290
Hesla na příkazovém řádku .....	290
Odstranění hesel na příkazové řádce .....	291
Prohledávání souborů s historií .....	291
Opatření proti prohledávání souborů s historií .....	291
Příslušnost ke skupinám .....	292
Právo zápisu pro skupinu .....	292
Opatření pro příslušnost ve skupině .....	292
Účelové skupiny a přístup k zařízením .....	293
Útoky přes účelové skupiny .....	293
Opatření pro účelové skupiny .....	293
Skupina „wheel“ .....	294
Sudo .....	294
Útok změnou hesla přes Sudo .....	295
Opatření pro změny hesla přes Sudo .....	295
Spouštění editoru přes Sudo .....	295
Opatření pro editory spouštěné přes Sudo .....	296
Další programy zranitelné přes Sudo .....	298
Sudo konfiguruje s maximální podezřívavostí .....	298
Programy se setuserid .....	299
Útoky přeplněním vyrovnávacích pamětí .....	299
Opatření proti přetečení vyrovnávacích pamětí .....	301
Útoky přes formátové řetězce .....	302
Opatření pro formátovací řetězce .....	302
Útoky přes pomocné aplikace .....	303
Opatření pro pomocné aplikace .....	303
Útoky přes setuserid hry .....	303
Opatření pro setuserid hry .....	304
Obecná opatření pro setuserid programy .....	304
Hackerovy setuserid programy na připojených svazcích .....	304
Setuserid binárky na svazcích NFS .....	305
Chyba v Novell NFS .....	305
Zamezení setuserid přístupu na připojených svazcích .....	306
Útoky na špatně napsané programy .....	307
Závodění .....	307
Opatření proti závodům .....	308

Pevné a symbolické odkazy .....	309
Pevné odkazy .....	310
Symbolické odkazy .....	310
Otevírání souborů přes symbolické odkazy .....	311
Souborové operace přes symbolické odkazy .....	312
Obrana před útoky přes symbolické odkazy .....	313
Útoky přes pevné odkazy .....	314
Opatření proti útokům přes pevné odkazy .....	315
Kontrola vstupu .....	315
Kontrola vstupu od uživatele .....	316
Podmíněné vkládání skriptů .....	316
Opatření pro podmíněné skripty .....	317
Shrnutí .....	317
KAPITOLA 9 PROLAMOVÁNÍ HESEL .....	319
Jak fungují hesla v Linuxu .....	320
/etc/passwd .....	320
Šifrovačí algoritmy Linuxu .....	322
Algoritmus DES .....	323
Algoritmus MD5 .....	324
Nástroje na prolamování hesel .....	325
Crack .....	326
Instalace Cracku .....	326
Použití Cracku .....	327
John the Ripper .....	331
Instalace programu John the Ripper .....	331
Použití programu John the Ripper .....	332
Režimy programu John the Ripper .....	333
Oznámení o prolomení .....	333
Další programy na hádání hesel .....	334
Viper .....	334
Slurpie .....	334
Opatření proti prolamování hesel .....	335
Dostupnost slovníků .....	335
Slovník Linuxu .....	335
Packetstorm .....	335
Freie Universität Berlin .....	336
Zastíněná hesla a /etc/shadow .....	336
Jak zastínění funguje .....	336
Aktivace zastínění hesel .....	337
Pwck – kontrola integrity /etc/passwd .....	338
Pwconv – převod na zastíněná hesla .....	338
Pwunconv – odstranění zastínění .....	338
Sada programů pro zastíněná hesla .....	338
Příkaz change .....	339
Další užitečné příkazy .....	339
Soubory s hesly Apache .....	339
Doplnitelné autentizační moduly (PAM) .....	341

Ochrana hesel .....	342
Zásady tvorby efektivních hesel .....	342
Nejdříve špatná hesla .....	342
Pravidla pro tvorbu dobrých hesel .....	343
Na různých systémech používejte různá hesla .....	345
Použití zastíněných hesel .....	346
Jak vynutit dobrá hesla .....	346
Passwd+ .....	346
Npasswd .....	347
Anlpasswd .....	347
PAM .....	347
Omezení platnosti hesel .....	348
Jednorázová hesla .....	348
MD5 .....	349
Pravidelné spuštění hadačů hesel .....	349
Shrnutí .....	349
KAPITOLA 10 JAK SI HACKEŘI UDRŽUJÍ PŘÍSTUP .....	351
Ověřování podle jména hostitele a uživatelský přístup .....	352
Změny v souborech hosts.allow a hosts.deny .....	353
Opatření proti zneužívání souborů hosts.allow a hosts.deny .....	354
Nezabezpečená exportování NFS .....	354
Opatření proti zneužití NFS exportu .....	355
Vytváření a modifikace účtů .....	356
Opatření proti zneužívání a nelegálnímu zavádění účtů .....	357
Shelly se setuserid root .....	357
Opatření proti setuserid shellům .....	359
Bezheslový vzdálený přístup pomocí příkazů r* .....	360
Modifikace /etc/hosts.equiv .....	360
Modifikace souborů rhhosts .....	361
Opatření proti zneužívání příkazů r* .....	362
Bezheslové přihlašování pomocí Ssh .....	362
Modifikace souborů hosts.equiv a rhhosts .....	363
Opatření proti zneužívání „hosts“ souborů Ssh .....	364
Totožnosti u Ssh .....	365
Opatření proti zneužívání totožnosti u Ssh .....	366
Přes síť přístupné superuživatelské shelly .....	366
Přidávání superuživatelských shellů do inetd .....	366
Opatření proti nepatřičným root shellům v inetd .....	367
Spouštění dalších démonů inetd .....	368
Opatření proti neoprávněně spouštěným inetd serverům .....	369
Poskytování přichozích root shellů pomocí programu Netcat .....	369
Opatření proti přichozím root shellům .....	372
Nepřímý přichozí přístup .....	372
Opatření proti nepřímým přichozím přístupům .....	374
Ztržštěné systémové programy .....	375
Zahlazování stop .....	375