

Obsah

Předmluva	.xxiv
Poděkování	.xxv
O autorovi	.xxvii

Kapitola 1

Úvod	1
1.1 Úvod do druhého vydání.....	1
1.2 Pro koho je tato kniha určena?.....	3
1.3 Uspořádání této knihy	4
1.3.1 Použité konvence.....	6
1.3.2 Předpoklady ke studiu.....	7
1.4 Proti čemu se bráníme?	8
1.5 Kdo jsou naši nepřátelé?.....	10
1.6 Čeho chtějí dosáhnout?.....	12
1.7 Náklady: ochrana versus vloupání.....	13
1.8 Ochrana hardwaru	13
1.9 Ochrana přístupu po síti a přes modem.....	14
1.10 Ochrana celkového přístupu k systému.....	14
1.11 Ochrana souborů	15
1.12 Příprava na průnik a jeho detekce	16
1.13 Odstraňování následků průniku.....	16

Část I – Zabezpečování systému17

Kapitola 2

Rychlá náprava obvyklých problémů	21
2.1 Celkový pohled na bezpečnost Linuxu.....	22
2.1.1 V bludišti krivolakých úzkých chodeb.....	22
2.1.2 Cesty možného útoku.....	26
2.1.3 Zavedení bezpečnostních bariér	29
2.2 Sedm nejhorších smrtelných hříchů.....	31
2.2.1 Nebezpečně slabá hesla (hřích 1).....	31
2.2.2 Otevřené síťové porty (hřích 2)	33
2.2.3 Staré verze softwaru (hřích 3).....	35
2.2.4 Nebezpečné a chybně konfigurované programy (hřích 4).....	36
2.2.5 Nedostatečné prostředky a chybně stanovené priority (hřích 5).....	43
2.2.6 Zastaralé a nepotřebné účty (hřích 6)	45
2.2.7 Co můžeš odložit... (hřích 7)	46
2.3 Hesla – klíč k dobrému zabezpečení.....	46

2.3.1 Jak zabránit slabým a implicitním heslům	47
2.4 Pokročilé techniky pro správu hesel	52
2.4.1 Zvýšení bezpečnosti se stínovými hesly MD5	52
2.4.2 Opakované zadání hesla	53
2.4.3 Má být platnost hesel omezená?	55
2.4.4 Jména účtů	56
2.5 Ochrana systému před omyly uživatelů	57
2.5.1 Nebezpečí doneseného softwaru	61
2.5.2 Výchova uživatelů v Čechách	61
2.6 Promíjet je lepší než úplně dovolit	62
2.6.1 Adresáře a bit „sticky“	64
2.6.2 Jak hledat problémy s oprávněním	65
2.6.3 Umask ve spouštěcích skriptech	70
2.7 Nebezpečí při prvotní instalaci systému a opatření proti nim	71
2.7.1 Roztočte kola Red Hat 7.3	72
2.8 Omezení bezdůvodného přístupu	76
2.8.1 Omezení terminálů, z nichž se může přihlásit root	76
2.8.2 Vytáčení telefonních čísel (násilné vytáčení)	78
2.8.3 Zastavení nekontrolovaného přístupu k datům	79
2.8.4 Omezení serverových rozhraní	79
2.9 Firewally a vnější opevnění firemní sítě	80
2.9.1 Jak zastavit cílené nájezdy na firewally	81
2.9.2 Tunelování přes firewally	84
2.9.3 Přepínače protokolů v jádře	87
2.9.4 Filtrování odchozího provozu	88
2.9.5 Miny v lokální síti LAN	89
2.9.6 Vnitropodnikový firewall, který odolá požáru	92
2.10 Vypnutí nepotřebných služeb	95
2.11 Vysoká bezpečnost vyžaduje minimum služeb	101
2.12 Tyto chatrné dveře je třeba zazdít	102
2.12.1 Nepovolujte finger	102
2.12.2 Vypněte démon rwhod	104
2.12.3 Vypněte démon rwalld	104
2.12.4 Vypněte protokol SNMP	105
2.12.5 Vypněte NFS, mountd a portmap	106
2.12.6 Přepněte NFS nad protokol TCP	107
2.12.7 Vypněte příkazy rsh, rcp, rlogin a rexec	108
2.12.8 Vypněte echo a chargin	109
2.12.9 Vypněte příkazy talk a ntalk	109
2.12.10 Vypněte TFTP	109
2.12.11 Vypněte příkazy systat a netstat	110
2.12.12 Vypněte interní služby démonu inetd	110
2.13 Vyměňte staré lampy za nové	110
2.13.1 Aktualizujte jádro verze 2.4	114

14.2.1 Konfigurace pasti Cracker Trap.....	602
14.3.1 Soubor /etc/services.....	603
14.2.3 Soubory /etc/xinetd.d/*	605
14.2.4 Soubor /etc/inetd.conf	606
14.2.5 Soubor /etc/hosts.allow	609
14.2.6 Soubor /etc/hosts.allow	610
14.2.7 Zachycení útoků na servery s přesměrováním portů	610
14.2.8 Spolupráce nástrojů Cracker Trap a PortSentry	614
14.3 Likvidace crackerských serverů pomocí úpravy jádra.....	615
14.4 Cvičný poplach.....	616
14.4.1 Letadlo nouzově přistálo	617
14.4.2 Toto je pouze test!	618
14.4.3 Nebezpečí testů a opatření proti nim	618
14.4.4 Plánování výcviku	619
14.4.5 Testovací systémy.....	619
14.4.6 Bezpečné trojské koně	620
14.4.7 I na velikosti záleží	622
14.4.8 Jak působit další problémy.....	623
14.5 Zkuste se do vlastního systému prolomit s pomocí „tygrího týmu“.....	623
14.5.1 Testování rizika průniku	625

Kapitola 15

Pozorování vlastního systému627

15.1 Bezpečnostní hlídač Nessus	627
15.2 Bezpečnostní auditory SARA a SAINT.....	628
15.3 Mapování sítě a nmap	628
15.4 Detektor útoků Snort	634
15.5 Pozorování a analýza s programem SHADOW.....	635
15.6 John Rozparovač – John the Ripper	635
15.7 Ukládání kontrolních součtů databáze RPM	636
15.7.1 Uživatelské záchranné disky	637

Část III – Detekce případů vniknutí639

Kapitola 16

Monitorování aktivit641

16.1 Soubory protokolů	641
16.2 Soubory protokolů: opatření a protiopatření.....	642
16.3 Programem Logcheck kontrolujete soubory protokolů, které nikdy nekontrolujete.....	644
16.4 Zabránění přístupu crackerům pomocí nástroje PortSentry.....	650
16.5 Nástroj HostSentry	656
16.6 Okamžitá zpráva administrátorovi: cracker se dobývá!	657

16.7 Příklad automatického zaslání zprávy	657
16.8 Jak rozvíjet příklad automatického zasílání zprávy	660
16.9 Oznamování o použití programů telnet a rsh.....	662
16.10 Podchycení útoku na protokol ARP a adresy MAC s nástrojem Arpwatch.....	663
16.11 Monitorování práce s porty	667
16.12 Monitorování útoku s nástrojem Ethereal	668
16.12.1 Sestavení nástroje Ethereal	669
16.12.2 Práce s nástrojem Ethereal.....	670
16.13 Monitorování sítě s utilitou tcpdump.....	670
16.13.1 Sestavení programu tcpdump.....	671
16.13.2 Práce s programem tcpdump	672
16.14 Monitorování „narušitelů“ s nástroji DTK	674
16.15 Monitorování procesů	678
16.15.1 Monitorování zátěže systému	680
16.16 Cron: na stopě crackerům	681
16.17 Identifikace volajícího (Caller ID).....	681

Kapitola 17

Jak v systému vyhledávat odchylky od normálu683

17.1 Hledání podezřelých souborů.....	683
17.1.1 Analýza podezřelých souborů.....	685
17.1.2 Pravidelné porovnávání obsahu souborů.....	686
17.2 Nástroj Tripwire.....	687
17.2.1 Instalace Tripwire.....	689
17.2.2 Práce s programem Tripwire.....	690
17.2.3 Před čím nás Tripwire neochrání.....	692
17.2.4 Možné náhrady Tripwire	692
17.3 Detekce odstraněných spustitelných souborů	693
17.4 Detekce promiskuitních karet síťového rozhraní.....	694
17.4.1 Program Lóphit AntiSniff.....	697
17.5 Vyhledání promiskuitních procesů	698
17.6 Automatická detekce pozměněných webových stránek	699

Část IV – Odstraňování následků útoku

Kapitola 18

Jak nad systémem znovu získat ztracenou kontrolu . . .709

18.1 Vyhledání běžících procesů crackera	709
18.1.1 Co dělat s odstraněnými spustitelnými soubory	710
18.2 Co dělat s crackerskými běžícími procesy	711
18.2.1 Oblíbené trojské koně	717
18.3 Ihned shodit modemy, sítě, tiskárny a celý systém.....	720

Kapitola 19

Jak zjistit rozsah škod a jak je napravit723

19.1 Kontrola protokolů v adresáři /var/log	724
19.2 Démony syslogd a klogd.....	724
19.3 Vzdálený záznam do protokolu	724
19.4 Interpretace záznamů v souboru protokolu.....	725
19.4.1 Soubor lastlog.....	726
19.4.2 Soubor messages.....	726
19.4.3 Soubor syslog	730
19.4.4 Soubor kernlog.....	730
19.4.5 Soubor cron.....	730
19.4.6 Soubor xferlog.....	731
19.4.7 Soubor daemon.....	731
19.4.8 Soubor mail	731
19.5 Kontrola dalších informací	733
19.6 Kontrola reakcí TCP Wrappers.....	733
19.7 Jak může být poškozen souborový systém.....	734
19.8 Podstrčení falešných dat.....	734
19.9 Změny v monitorovacích programech	735
19.10 Ztracení v zrcadlovém bludišti	736
19.11 Opět máme kontrolu nad systémem	736
19.12 Jak vyhledat soubory změněné crackerem	737
19.12.1 Interpretace výsledků volání tar -d	739
19.12.2 Urychlení kontrol s RPM.....	740
19.12.3 Opravy poškozených balíků RPM.....	741
19.12.4 Oprava databází	742
19.12.5 Poškození periférií	743
19.12.6 Elektronická krádež.....	744
19.12.7 Jak může být poškozeno jádro systému.....	744
19.13 Cracker je usvědčen.....	744
19.13.1 Stopy v poškozených datech.....	745
19.14 Vyhledání programů s příznakem set-UID.....	746
19.15 Vyhledání trojského koně mstream	746

Kapitola 20

Na stopě systému útočníka749

20.1 Vypátrání číselné IP adresy příkazem nslookup.....	749
20.2 Vypátrání číselné IP adresy příkazem dig.....	750
20.3 Podívej, kdo to přišel: hledání vlastníků domén .com.....	750
20.4 Hledání entit přímo z IP adresy.....	751
20.5 Hledání vetřelce přes vládní systémy .gov.....	752
20.6 Program ping.....	753
20.7 Program traceroute.....	754
20.8 Výsledky ze sousedních systémů.....	755

20.9 Nedávňý případ mezinárodního honu na crackera.....	756
20.10 Našli jste určité skutečného útočníka?	756
20.11 Ostatní systémoví administrátoři: zajímá je to vůbec?	759
20.11.1 Sepište případ pro administrátory	760

Kapitola 21

Zločin a trest761

21.1 Policie: obávaná síť na zločince, nebo smečka neschopných?	762
21.1.1 FBI.....	762
21.1.2 Americká tajná služba	764
21.1.3 Ostatní federální úřady	765
21.1.4 Úřady jednotlivých států	765
21.1.5 Místní policie	766
21.1.6 Pečlivě si svůj případ připravte	767
21.1.7 Vystopujte osud odcizených dat	768
21.1.8 Péče o usvědčující důkazy	768
21.2 Soudní stíhání	769
21.3 Odpovědnost poskytovatelů internetových služeb za nezabránění nezákonným aktivitám	770
21.4 Nejlepší obrana je útok.....	771
21.4.1 Který postup je zákonný	771
21.4.2 Masivní spam.....	772
21.4.3 Smrtelný ping	773
21.4.4 Nepřátelské javové applety	773
21.4.5 Vyřídím si to s ním sám.....	774

Příloha A

Internetové zdroje nedávňých případů průníků a obrany proti nim775

A.1 Poštovní konference – povinné.....	776
A.1.1 Americké vládní koordinační centrum CERT	777
A.1.2 Americký vládní úřad CIAC	777
A.1.3 Bugtraq.....	777
A.1.4 ISS X-Force	778
A.1.5 Stránky mail-abuse.org.....	778
A.2 Poštovní konference – nepovinné	778
A.2.2 Poštovní konference SSH	779
A.2.3 Poštovní konference Network World Fusion	779
A.3 Diskusní skupiny zpráv Usenet News	779
A.4 Webové adresy URL věnované bezpečnosti.....	779
A.4.1 Stránky Kurta Seifrieda	779
A.4.2 Security Focus	780
A.4.3 Forensics.....	780

A.4.4	Webový server hackerwhacker	780
A.4.5	Čísla crackerských portů	780
A.4.6	Jak fungují linuxové viry	780
A.4.7	Centrum FBI NIPC	780
A.4.8	FIRST	780
A.4.9	Bezpečnostní stránky Linux Weekly News	781
A.4.10	Linux Today	781
A.4.11	SANS Institute	781
A.5	Adresy URL bezpečnostních nástrojů	781
A.5.1	Autorovy stránky	781
A.5.2	Jak stáhnout bezpečný shell (Secure SHell, SSH)	783
A.5.3	Jak stáhnout Bastille Linux	783
A.5.4	Jak stáhnout skript pro zvýšení bezpečnosti SuSE	783
A.5.5	Jak stáhnout systém Linux Intrusion Detection System	784
A.5.6	Pretty Good Privacy (PGP)	784
A.5.7	GNU Privacy Guard (GPG)	784
A.5.8	Utilita tcpdump	785
A.5.9	Grafický nástroj Ethereal pro sledování paketů	785
A.5.10	Utilita sniffit	785
A.5.11	Jak stáhnout utilitu Tripwire	785
A.5.12	Jak stáhnout alternativy ke Tripwire	786
A.5.13	Jak stáhnout bezpečnostní auditor Nessus	786
A.5.14	Jak stáhnout bezpečnostní auditor SARA	786
A.5.15	Jak stáhnout nástroj nmap	787
A.5.16	Jak stáhnout detektor útoků Snort	787
A.5.17	Jak stáhnout nástroj SHADOW	787
A.5.18	Jak stáhnout bezpečnostní auditor SAINT	787
A.5.19	Jak stáhnout nástroj pro konfiguraci IP Chains	788
A.5.20	Jak stáhnout SSL	788
A.5.21	Jak stáhnout program sslwrap	789
A.5.22	Webová stránka pro rozšíření CVS o SSH	789
A.5.23	Jak stáhnout ovladač šifrovaných disků	789
A.5.24	Sendmail bez uživatele root	789
A.5.25	Jak stáhnout program postfix	789
A.5.26	Knihovna Libsafe	789
A.5.27	Skutečně pozorované útoky	790
A.5.28	Analýza útočníka na stránkách Sam Spade	790
A.6	Adresy URL s dokumentací	790
A.6.1	Dokumentace k Linuxu	790
A.6.2	Jak psát bezpečné programy	791
A.7	Adresy URL s obecnými nástroji	791
A.7.1	Debugger ddd	791
A.7.2	Počítač časového pásma	792
A.8	Adresy URL s různými specifikacemi a definicemi	792
A.8.1	Oranžová kniha	792

A.8.2 RFC 1813: NFS verze 3.....	793
A.8.3 Slovníček pojmů z počítačové bezpečnosti u NSA.....	793
A.8.4 Slovníček počítačových pojmů CNET.....	793
A.9 Software a aktualizace od dodavatelů	793
A.9.1 Red Hat	793
A.9.2 Slackware	793
A.9.3 SuSE.....	794
A.9.4 Mandrake.....	794
A.9.5 Caldera	794
A.9.6 Debian	794
A.9.7 Yellow Dog.....	794
A.10 Ostatní softwarové aktualizace	794
A.10.1 Jak stáhnout program sendmail.....	794
A.10.2 Databáze PostgreSQL	795
A.10.3 Zdroje Open Source softwaru	795

Příloha B

Knihy, CD-ROM a video797

B.1 Linux System Security	797
B.2 OpenBSD Firewalls	797
B.3 Samba: Integrating Unix and Windows	797
B.4 Linux Sendmail Administration.....	797
B.5 Secrets and Lies: Digital Security in a Networked World.....	798
B.6 The Cuckoo's Egg.....	798
B.7 Hackers.....	798
B.8 UNIX Complete.....	799
B.9 The Computer Contradictionary	799
B.10 Zdroje agentury DISA amerického Ministerstva obrany	799
B.10.1 CD-ROM CyberProtect.....	800
B.10.2 Výuková videokazeta o bezpečnosti 101.....	800
B.10.3 Videokazeta o bezpečnosti 201	800
B.10.4 Videokazeta Understanding Public Key Infrastructure (PKI).....	800
B.10.5 Videokazeta agentury NSA.....	800
B.10.6 Ears Looking at You	801
B.10.7 CD-ROM Information Assurance (IA) for Auditors & Evaluators.....	801
B.10.8 CD-ROM Incident Preparation & Response	801
B.10.9 CD-ROM ministerstva obrany INFOSEC Awareness.....	801
B.10.10 CD-ROM Operational Information Systems Security (OISS), svazky 1 a 2.....	801
B.11 Internetworking with TCP/IP, svazky I, II a III.....	801
B.12 Linux Application Development.....	802
B.13 Konzultanti: dobří, špatní a falešní	802

Příloha C

Síťové služby a jejich porty	805
---	------------

Příloha D

Stupně nebezpečí	813
-------------------------------	------------

Příloha E

O disku CD-ROM	823
E.1 Veřejný klíč GPG autora	826

Příloha F

Seznam zkratk	827
Licenční ujednání a omezení záruky	831

Obsah disku CD-ROM	833
Rejstřík	835

2.13.2 Aktualizujte jádro verze 2.2	114
2.13.3 Aktualizujte sendmail	115
2.13.4 Posilte sendmail, aby odolal útokům odepření služeb	117
2.13.5 Aktualizujte shell SSH	120
2.13.6 Aktualizujte WU-FTPd	120
2.13.7 Aktualizujte Netscape	121
2.13.8 Zablokujte webové reklamy	122
2.14 Společně zahyneme, samostatně přežijeme	122

Kapitola 3

Snadné a rychlé hackerské příuky do systému a jak jim předcházet125

3.1 X Window znamenají díru	125
3.2 Zákony džungle – fyzická bezpečnost	130
3.3 Fyzické zásahy do systému	134
3.3.1 Zavedení systému z diskety nebo CD-ROM vetřelce	135
3.3.2 Změna konfigurace paměti CMOS	135
3.3.3 Doplnění hesla CMOS	136
3.3.4 Obrana proti jednoruživatelskému módu	137
3.3.5 Proti krádežím s disketou	138
3.3.6 Ochrana před útoky Ctrl-Alt-Delete	139
3.4 Vybraná drobná témata	139
3.4.1 Kabelové modemy	139
3.4.2 Proměnná \$PATH: hodnoty s tečkou vedou do záhuby	140
3.4.3 Blokování zdrojového směrování IP	142
3.4.4 Blokování falešné komunikace IP	143
3.4.5 Automatické uzamykání obrazovky	143
3.4.6 Soubor /etc/mailcap	145
3.4.7 Program chatter a bit nezměnitelnosti	146
3.4.8 Bezpečné odstraňování souborů	146
3.4.9 Synchronní I/O operace	147
3.4.10 Příznaky připojování pro zvýšení bezpečnosti	148
3.4.11 Obalení UDP do TCP a SSH	149
3.4.12 Kočka škrábe svého pána	150
3.4.13 Omezený úspěch s voláními *limit	152
3.4.14 Historie shellu na veřejných terminálech	153
3.4.15 Jak funguje protokol ARP (Address Resolution Protocol)	154
3.4.16 Jak zabránit poškození cache protokolu ARP	155
3.4.17 Hackerské útoky na přepínače	156
3.4.18 Opatření proti útokům na systém a přepínače, způsobeným útoky v protokolu ARP	160
3.4.19 Wireless Equivalent Privacy (WEP)	162
3.4.20 Hacking diod LED	164
3.4.21 Únik do příkazového interpretu	165

3.4.22 Poskytovatel internetových služeb.....	166
3.4.23 Odposlech terminálu (ttysnoop)	168
3.4.24 Star Office	169
3.4.25 VMware, Wine, DOSemu a jejich přátelé.....	169
3.5 Útoky na terminálová zařízení	169
3.5.1 Únos funkčních kláves	170
3.5.2 Zranitelnost klávesy Compose	171
3.5.3 Hrozba změny protokolového souboru xterm	171
3.6 Slídění po disku	171
3.6.1 Skutečné vymazání souborů.....	172
3.6.2 Zničení starších důvěrných dat ve volných blocích	175
3.6.3 Vymazání celého disku.....	178
3.6.4 Zničení pevného disku	179

Kapitola 4

Nejčastější hackerské průniky podle subsystemů 181

4.1 NFS, mountd a portmap	181
4.2 Sendmail	184
4.2.1 Samostatné nebo další poštovní servery pro zvýšení bezpečnosti	185
4.2.2 Základní bezpečnost programu sendmail	186
4.2.3 Možnosti zabezpečení programu sendmail	189
4.2.4 Falšování pošty a adresa odesílatele zpráv	193
4.2.5 Odkud přichází všechna ta hromadná pošta?	193
4.2.6 Přeposílání hromadné pošty	195
4.2.7 Blokování hromadné pošty	195
4.2.8 Jak obelstít roboty pro hromadnou poštu	196
4.2.9 Povolení řízeného přeposílání	196
4.2.10 Povolení odesílání pošty klientům POP a IMAP	198
4.2.11 Zákaz otevřených poštovních konferencí	199
4.2.12 Útok odepráním služeb sendmail při zaplnění disku	199
4.3 Telnet	200
4.4 FTP	201
4.4.1 Konfigurace anonymního FTP	203
4.4.2 Nebezpečí z proxy-serverů FTP	209
4.5 Služby rsh, rcp, rexec a rlogin	209
4.5.1 Bezpečně s příkazy R*	211
4.5.2 Nebezpečí příkazů R*	211
4.6 DNS (démon named neboli BIND)	213
4.6.1 Jak omezit důsledky narušení named	213
4.6.2 Sloužíme lidstvu	214
4.7 Servery POP a IMAP	215
4.7.1 Hesla na příkazovém řádku – ó můj bože!	218
4.8 Systém Samba	220
4.8.1 Co je to Samba?	220

4.8.2 Verze Samby	221
4.8.3 Je Samba na počítači nainstalována?	221
4.8.4 Jakou verzi Samby v systému mám?	221
4.8.5 Soubor smb.conf	221
4.8.6 Soubor smbpasswd	223
4.8.7 Soubor mapování uživatelů	224
4.8.8 Protokolové soubory	225
4.8.9 Dynamické datové soubory	226
4.8.10 Bezpečný provoz Samby	226
4.8.11 Síťová bezpečnost Samby	226
4.8.12 Bezpečnost souborů pod Sambou	229
4.8.13 Zabezpečení uživatelů	234
4.8.14 Bezpečnost správy Samby	238
4.8.15 Volání SSH ze Samby	239
4.9 Aby vám squid nemohl ušpinit prsty	240
4.10 Služba syslogd	243
4.11 Tisková služba lpd	244
4.12 Služba ident	245
4.13 Démon INND a news	246
4.14 Ochrana registrace v DNS	246

Kapitola 5

Nejčastější typy útoků crackerů251

5.1 Útoky s nástroji rootkit (skriptové útoky)	251
5.2 Jak funguje falšování paketů	253
5.2.1 Proč je falšování paketů UDP tak úspěšné	255
5.2.2 Falšování pořadových čísel TCP	257
5.2.3 Únos běžící relace	258
5.3 Útok záplavou paketů SYN	259
5.4 Ochrana před útokem záplavou paketů SYN	260
5.5 Ochrana před falšováním pořadových čísel TCP	260
5.6 Paketové bouře, šmoulí útoky a tříštivé bomby	261
5.6.1 Nechci být zesilovačem	263
5.6.2 Jak odrazit útok paketové bouře	264
5.6.3 Směrovače Cisco	266
5.6.4 Útoky distribuovaného odepření služby: webové zdroje obrany	266
5.7 Přetečení bufferu neboli pošlapání paměti voláním gets()	267
5.8 Techniky falšování	268
5.8.1 Falšování pošty	268
5.8.2 Útok na adresu MAC	270
5.8.3 Zásah do cache protokolu ARP	271
5.8.4 Zásah do cache DNS	271
5.9 Útok s mužem uprostřed	272

Kapitola 6

Pokročilé otázky bezpečnosti275

6.1 Konfigurace zvýšeného zabezpečení prohlížeče Netscape.....	275
6.1.1 Důležité preference Netscape	276
6.1.2 Hlídejte si své cookies	279
6.1.3 Preference jednotlivých uživatelů v Netscape	280
6.1.4 Správce zabezpečení Netscape	281
6.1.5 Netscape a bezpečnost Javy	281
6.2 Zastavení přístupu k I/O zařízením.....	283
6.2.1 Proč má zařízení /dev/tty mód 666	288
6.2.2 Ohrožení bufferu virtuální konzoly	289
6.2.3 Ovladač šifrovaného disku	289
6.3 Na stopě problémům se serverem Apache (httpd)	290
6.3.1 Vlastnictví a oprávnění v Apache	290
6.3.2 Soubory Server-Side Include	291
6.3.3 Direktiva ScriptAlias	292
6.3.4 Jak uživatelům zabránit ve změně nastavení pro celý systém	292
6.3.5 K jakým adresářům smí Apache přistupovat	293
6.3.6 K jakým typům souborů smí Apache přistupovat	293
6.3.7 Různé	294
6.3.8 Odčerpání databáze	294
6.3.9 Jak vykázat nepřijatelné uživatele	298
6.3.10 Odkazy na vaše stránky	298
6.4 Zvláštní postupy pro webové servery	299
6.4.1 Postavit samostatnou pevnost	300
6.4.2 Nevěřte skriptům CGI	300
6.4.3 Skryté proměnné formulářů a nebezpečné cookies	301
6.4.4 Vezměte si, prosím, naše zaměstnance	301
6.4.5 Vyloučení robotů z webových stránek	302
6.4.6 Všude se povalují nebezpečné programy CGI	303
6.4.7 Zneužití programu query v CGI	304
6.4.8 Dekódování adres URL z hexadecimálního formátu	305
6.4.9 Zneužití programu counterfiglet v CGI	306
6.4.10 Zneužití CGI programu phf	307
6.4.11 Skripty a programy CGI	307
6.4.12 Jak vynutit blokování adres URL	316
6.4.13 Jak detekovat pozměnění webových stránek	316
6.5 Jednosměrné putování dat o kreditních kartách pro nejvyšší bezpečnost	318
6.6 Velmi vysoká bezpečnost si žádá další opevnění	322
6.7 Omezení povoleného místa a času pro přihlášení	332
6.8 Těžko odhalitelné, ale závažné problémy	333
6.8.1 Ochrana proti útokům přetečení bufferu	334

6.8.2 Ochrana proti ohrožení systémového volání chroot()	336
6.8.3 Útok na symbolické odkazy	338
6.8.4 Problém díry s adresářem lost+found	341
6.8.5 Souběh s rm -r	342
6.9 Ochrana proti simulovanému přihlášení	342
6.9.1 Aktualizace souboru /etc/issue	345
6.9.2 Úpravy programu /bin/login	347
6.9.3 Podpora jádra (bezpečnostní kombinace kláves SAK)	347
6.10 Jak zastavit přetečení bufferů s knihovnou Libsafe	350

Kapitola 7

Zavádění bezpečnostní politiky 356

7.1 Obecná politika	354
7.2 Politika osobního používání	355
7.3 Politika pro účty	356
7.4 E-mailová politika	358
7.5 Politika okamžité výměny zpráv	359
7.6 Politika webového serveru	360
7.7 Politika souborových serverů a databází	361
7.8 Politika firewallu	362
7.9 Politika stolních počítačů	362
7.10 Politika přenosných počítačů	363
7.11 Politika likvidace zařízení	367
7.12 Politika síťové topologie	368
7.12.1 Politika interní síťové topologie	369
7.13 Politika oznamování problémů	371
7.14 Politika vlastnictví	371
7.15 Politika politiky	372

Kapitola 8

Jak a kdy důvěřovat jiným počítačům 373

8.1 Bezpečné systémy a nebezpečné systémy	374
8.2 Nevěřit nikomu – to je nejvyšší zabezpečení	374
8.3 Linuxové a unixové systémy v rámci vaší sféry vlivu	376
8.4 Střediskové počítače ve vaší sféře vlivu	377
8.5 Jedno okno je jako tisíc kanonů	378
8.6 Ohrožení firewallů	380
8.7 Virtuální privátní sítě	383
8.8 Viry a systém Linux	384

Kapitola 9

Nejdrastičtější průniky 387

9.1 Techniky „Mission Impossible“	387
9.2 Špionáž	390
9.2.1 Průmyslová špionáž	391

9.3 Fanatické a sebevražedné útoky	391
--	-----

Kapitola 10

Případové studie393

10.1 Výpověď „krtka“ v systému Berkeley	393
10.2 Královští rytíři (soudnička)	397
10.3 Vloupání Kena Thompsona do námořnictva	399
10.4 Trojský kuň ve virtuálním počítači	400
10.5 Neúspěšný pokus o změnu DNS v AOL	401
10.6 Já jsem nevinný, říkám vám!	403
10.7 Crackeri s laptopem v telefonní budce	404
10.8 Stačí jen pár haléřů	405
10.9 Neziskové organizace mají smůlu	406
10.10 Neústupnost vůči vzpurným systémovým administrátorům se vyplácí	408
10.11 Produkt .NET se dodával s virem Nimda	409

Kapitola 11

Nedávné případy průníků411

11.1 Fragmentační útoky	411
11.2 U protokolu ICMP maskování IP selhává	412
11.3 Smrtelný ping potopil holandskou námořní společnost	413
11.4 Kapitáne, sleduj nás! (neviditelné sledování)	414
11.5 Kabelové modemy: crackerův sen	415
11.6 Blokování e-mailových útoků pomocí programu sendmail	415
11.7 Uhodnutí jmen účtů pomocí sendmail	416
11.8 Záhadný zámek ingreslock	417
11.9 Jdou po vás!	417
11.9.1 Výrobní číslo Pentium III	417
11.9.2 Globální identifikátor GUID od Microsoftu umožňuje vaše sledování	418
11.10 Distribuované (koordinované) útoky odeprání služby	419
11.11 Neviditelné trojské koně	422
11.11.1 Proč a jak pakety odpovědí na opakování ICMP?	424
11.11.2 Budoucí směry „vývoje“ neviditelných trojských koňů	425
11.11.3 Zprávy jádra systému při promiskuitním módu	425
11.12 Konfigurace programem linuxconf přes TCP port 98	427
11.13 Zákeřné značky a skripty jazyka HTML	427
11.14 Problémy s formátováním rutiny syslog()	428

Část II – Příprava na průnik do systému429

Kapitola 12

Další posílení bezpečnosti systému431

12.1 Ochrana uživatelských relací se SSH.....	431
12.1.1 Sestavení SSH2	433
12.1.2 Konfigurace SSH.....	435
12.1.3 Používání SSH	439
12.1.4 Jak postavit SSH okolo X Window	440
12.1.5 Program sftp	441
12.1.7 Program scp.....	441
12.1.8 Jak postavit SSH okolo dalších služeb založených na TCP	442
12.1.8 Ohrožení, proti kterým se SSH nedokáže bránit	444
12.2 Virtuální privátní síť (VPN)	444
12.2.1 Nebezpečí sítí VPN	445
12.2.2 Virtuální privátní síť se SSH, PPP a Perlem	449
12.2.3 Mechanismus CIPE (Crypto IP Encapsulation).....	451
12.2.4 Virtuální privátní síť s FreeS/WAN IPSec	451
12.2.5 PPTP (Point-to-Point Tunneling Protocol).....	452
12.2.6 Zbedee	452
12.2.7 Měření výkonnosti sítí VPN	452
12.3 PGP (Pretty Good Privacy).....	453
12.4 Snadné šifrování souborů pomocí GPG	454
12.4.1 Jak si GPG stáhnout.....	455
12.4.2 Jak GPG sestavit	456
12.4.3 K čemu je dobré	457
12.4.4 Generování klíčů	458
12.4.5 Vzájemná výměna klíčů	460
12.4.6 Rozeslání veřejného klíče	463
12.4.7 Soubory s podpisem	464
12.4.8 Šifrované a podepsané poštovní zprávy.....	466
12.4.9 Šifrované záložní a jiné soubory	167
12.4.10 Velmi vysoká bezpečnost GPG	468
12.5 Firewally s IP Tables a s demilitarizovanou zónou	469
12.5.1 Neustálá štvance: ochrana jednoduché domácí nebo firemní sítě	470
12.5.2 Výhody IP Tables proti IP Chains.....	484
12.5.3 Nevýhody IP Tables proti IP Chains.....	485
12.5.4 Sledování spojení v IP Tables: mýty a skutečnost.....	489
12.5.5 Boj proti únosům spojení a útokům na ICMP	491
12.5.6 Konfigurace firewallu s distribucí Red Hat 7.3	493
12.5.7 Konfigurace firewallu v systému SuSE 8.0	495
12.5.8 Triky a techniky k firewallům	496
12.5.9 Vytvoření firewallu s demilitarizovanou zónou postaveného na IP Tables.....	516

12.5.10 Co IP Tables dělat nemohou	518
12.5.11 Jak funguje maskování IP (převody síťových adres NAT) ..	520
12.5.12 Příkazy IP Tables	525
12.5.13 Spuštění firewallového skriptu	527
12.5.14 Vytvoření demilitarizované zóny	530
12.5.15 Tajemství mechanismů směrování	535
12.5.16 Méně používané funkce IP Tables	537
12.5.17 Stavové firewally	537
12.5.18 Nebezpečí SSH	539
12.5.19 Přístup k šifrované poště	541
12.6 Firewally s IP Chains a s demilitarizovanou zónou	542
12.6.1 Co IP Chains dělat nemohou	544
12.6.2 Jak funguje maskování IP (převody síťových adres NAT, pro IP Chains)	546
12.6.3 Příkazy IP Chains	551
12.6.4 Spuštění skriptu pro firewall	554
12.6.5 Základní využití firewallu s IP Chains	558
12.6.6 Odražení vnějšího nepřítele	558
12.6.7 Maskování IP	567
12.6.8 Vytvoření demilitarizované zóny	569
12.6.9 Stavové firewally	571
12.6.10 Nebezpečí SSH	573
12.6.11 Přístup k šifrované poště	575

Kapitola 13

Příprava hardwaru577

13.1 Nejdůležitější je přesný čas	577
13.2 Přípravy pokračují	580
13.3 Přechod na záložní zařízení (horká záloha)	581
13.3.1 Ke kterým systémům je potřeba vytvořit záložní systém? ..	582
13.3.2 Dva typy záložních systémů	583
13.3.3 Návrh bezpečnostního záložního systému	583
13.3.4 Udržování bezpečnostního záložního systému v pohotovosti	585
13.3.5 Kontrolování cache	587
13.3.6 Příteli, mohl bys postrádat jeden disk?	588

Kapitola 14

Příprava konfigurace589

14.1 TCP Wrappers	589
14.1.1 Používání TCP Wrappers	590
14.1.2 TCP Wrappers pro pokročilé	592
14.2 Adaptivní firewally: most se rozevírá s pastí na crackery – Cracker Trap	593