

STRUČNÝ OBSAH

ČÁST 1

PRONIKÁME DO LINUXU

- | | | |
|------|--|-----|
| ▼ 1. | Přehled zabezpečení v Linuxu | 11 |
| ▼ 2. | Proaktivní bezpečnostní opatření | 49 |
| ▼ 3. | Mapování počítače a sítě | 101 |

ČÁST 2

PRŮNIK ZVENČÍ

- | | | |
|------|---|-----|
| ▼ 4. | Sociální inženýrství, trojské koně a další triky útočníků | 165 |
| ▼ 5. | Fyzické útoky | 199 |
| ▼ 6. | Útoky přes síť | 223 |
| ▼ 7. | Pokročilé útoky přes síť | 263 |

ČÁST 3

LOKÁLNÍ ÚTOKY

- | | | |
|------|--------------------------------------|-----|
| ▼ 8. | Zvýšení uživatelských práv | 307 |
| ▼ 9. | Autentizace v Linuxu | 351 |

ČÁST 4

PROBLÉMY SERVERŮ

- | | | |
|-------|--|-----|
| ▼ 10. | Bezpečnost pošty | 373 |
| ▼ 11. | Bezpečnost protokolu FTP | 397 |
| ▼ 12. | Webové servery a dynamický obsah | 423 |
| ▼ 13. | Řízení přístupu a firewally | 469 |
| ▼ 14. | Útoky typu DoS | 491 |

ČÁST 5**PO PRŮNIKU**

▼ 15.	Maskování přístupu	511
▼ 16.	Zadní vrátka	535
▼ 17.	Pokročilá zneužití systému	567

ČÁST 4**PŘÍLOHY**

▼ A.	Odhalení a obnova systému po útoku	585
▼ B.	Aktualizace používaných programů	593
▼ C.	Vypnutí nepotřebných programů	609
▼ D.	Rozbory reálných případů	621
	Rejstřík	627

OBSAH

Poděkování	1
Úvod	3

ČÁST 1

PRONIKÁME DO LINUXU

▼ 1. Přehled zabezpečení v Linuxu	11
Proč chtějí získat přístup k účtu root?	12
Hnutí Open Source	13
Open Source a bezpečnost	14
Uživatelé v Linuxu	15
/etc/passwd	17
Typy uživatelů	19
Skupiny uživatelů	20
Jak řídit práva uživatelů	21
Přístupová práva k souborům	22
Změna práv souboru	23
Příznaky souborů	29
Další bezpečnostní mechanismy	31
Signály	31
Privilegované porty	31
Správa virtuální paměti	32

Mechanismus logování	32
/etc/security	32
chrootované prostředí	34
Použití Capabilities k omezení práv uživatele root	37
Chybně napsaný kód	37
Program neodloží privilegia	38
Přeplnění bufferu	39
Chyby formátovacího řetězce	41
Souběh (race condition)	43
Auditovací nástroje	46
Shrnutí	47
▼ 2. Proaktivní bezpečnostní opatření	49
Bezpečnostní skenery	50
Systémové skenery	50
Síťové bezpečnostní skenování	56
Detektory skenů	58
Zvýšení odolnosti systému	60
Analýza logovacích souborů	66
Syslog	67
Syslog-ng	70
Kontrola logů	70
Nástroje pro kontrolu logů	71
Běžné útoky na logy	76
Kontrola integrity souborového systému	86
Vytváření databází kontrolních součtů a práv	90
Nástroje pro kontrolu integrity souborového systému	92
Shrnutí	99
▼ 3. Mapování počítače a sítě	101
Online hledání	102
Databáze whois	104
Průzkum pingem	109
Problémy související s DNS	113
Příklad DNS hledání	114
Bezpečnostní problémy DNS dotazů	114
Zjištění charakteristik jmeného serveru	121
DNSSEC	123
Traceroute	123
Skenování portů	125

Detekce operačního systému	134
Aktivní průzkum síťové vrstvy	136
Pasivní průzkum síťové vrstvy	140
Zjištění RPC služeb	143
Sdílení souborů přes NFS	145
Simple Network Management Protocol (SNMP)	148
Skenování slabých míst sítě	152
Shrnutí	162

ČÁST 2

PRŮNIK ZVENČÍ

▼ 4. Sociální inženýrství, trojské koně a další triky útočníků	165
Sociální inženýrství	166
Kategorie útočných metod	166
Ochrana před sociálním inženýrstvím	171
Útočníci plní domácí úkoly	171
Trojské koně	172
Metody šíření trojských koňů	172
Příklady trojských koňů	174
Další trojské koně	186
Viry a červi	191
Jak si viry a červi šíří	192
Viry a Linux	192
Červi a Linux	193
Shrnutí	197
▼ 5. Fyzické útoky	199
Kancelářské útoky	200
Možnost naboťovat znamená být root	206
Zavaděče OS	210
Restart z terminálu	220
Šifrované souborové systémy	221
Shrnutí	222
▼ 6. Útoky přes síť	223
Používání sítě	225
Síť TCP/IP	225
Veřejné telefonní síť	230

Sítové zneužitelné slabiny	232
Programátorské chyby v síťových démonech	232
Výchozí nebo špatné konfigurace	236
Systém X Window	239
Útoky proti OpenSSH	244
Útoky proti síťovým klientům	248
Výchozí hesla	253
Odposlouchávání provozu	255
Jak odposlech funguje	255
Běžné programy pro odposlech	256
Další programy pro odposlech	260
Hádání hesel	261
Shrnutí	262
▼ 7. Pokročilé útoky přes síť	263
Útoky na DNS	264
Směrovací problémy	269
Pokročilý odposlech a únos spojení	275
Hunt	275
Dsniff	280
Útoky man-in-the-middle	281
Zneužití vztahu důvěry	291
Průniky do bezdrátových sítí	293
Ochrana bezdrátových sítí prostřednictvím VPN	300
Implementace hraniční filtrace	302
Shrnutí	304

ČÁST 3

LOKÁLNÍ ÚTOKY

▼ 8. Zvýšení uživatelských práv	307
Uživatelé a práva	308
Zvýšení práv	309
Průzkum systému	310
Špatná práva domovských adresářů	310
Ukládání a práce s hesly	316
Vyhledávací cesty a trojské koně	319
SUDO	323
Lokálně zneužitelné programy	328

sXid programy	328
Souběhy	333
Pevné a symbolické odkazy	337
Ověřování vstupu	342
Útoky proti jádru	344
Přímý přístup k zařízením	348
Shrnutí	349
▼ 9. Autentizace v Linuxu	351
Jak hesla v Linuxu fungují	352
Klíče a salt	352
Algoritmus DES	353
Algoritmus MD5	353
Další algoritmy	354
Programy pro luštění hesel	354
Spuštění programu Crack	355
Spuštění programu John the Ripper	357
Režimy programu	358
Dostupnost slovníků	359
Pluggable Authentication Modules	359
Konfigurace PAM	360
Hádání hesel hrubou silou	361
Ochrana hesel	362
Špatná hesla	362
Pravidla pro vytváření dobrých hesel	363
Autentizace ostatních programů	366
Soubory hesel serveru Apache	367
Samba	367
MySQL	368
Shrnutí	369

ČÁST 4

PROBLÉMY SERVERŮ

▼ 10. Bezpečnost pošty	373
MTA	374
Sendmail	374
Qmail	375
Postfix	376

Exim	376
Rizika poštovních serverů	377
Shrnutí	395
▼ 11. Bezpečnost protokolu FTP	397
Historie FTP přenosů	398
Popis protokolu FTP	400
Příklad FTP komunikace	400
FTP v aktivním režimu	401
FTP v pasivním režimu	402
Skenování portů prostřednictvím třetích serverů	406
Třístranná FTP komunikace	413
Nebezpečná stavová pravidla firewallů	417
Problémy s anonymním přístupem	419
Shrnutí	420
▼ 12. Webové servery a dynamický obsah	423
Vytvoření požadavku HTTP	424
Webový server Apache	430
Konfigurace serveru Apache	431
Logy serveru Apache	438
Problémy s programy CGI	441
Nebezpečné programy CGI	442
Důvěřování uživatelskému vstupu	443
Nebezpečné konfigurace CGI	461
PHP	463
Další linuxové webové servery	466
Shrnutí	467
▼ 13. Řízení přístupu a firewally	469
Démony inetd a xinetd	470
Inetd	470
Xinetd	471
Firewall: řízení přístupu na úrovni jádra	482
Filtrace paketů v Linuxu	483
Blokování konkrétních přístupů	484
Někdy je REJECT lepší než DROP	487
Strategie nastavení firewallu	488
Vytvoření firewallu pomocí iptables	489
Další nástroje	490
Shrnutí	490

▼ 14. Útoky typu DoS	491
Útoky DoS na jádro	492
Síťové zahlcení	494
Útoky nárůstem paketů	497
Distribuované útoky DoS	501
Útoky vedoucí k vyčerpání lokálních prostředků	505
Shrnutí	507

ČÁST 5

PO PRŮNIKU

▼ 15. Maskování přístupu	511
Maskování stop	512
Trojanizované systémové programy	514
Triky s operačním systémem	519
Maskování síťového přístupu	524
Shrnutí	533
▼ 16. Zadní vrátka	535
Autentizace podle vzdáleného systému a uživatelský přístup	536
Vytváření a modifikace účtů	540
Zadní vrátka v existujících účtech	543
Přihlášení bez hesla pomocí SSH	551
Síťově přístupné příkazové interprety uživatele root	554
Zadní vrátka prostřednictvím trojských koňů	559
Shrnutí	565
▼ 17. Pokročilá zneužití systému	567
Úpravy jádra	568
Oslabení jádra	572
Rootkity	575
Shrnutí	581

ČÁST 4

PŘÍLOHY

▼ A. Odhalení a obnova systému po útoku	585
Jak poznáte, že se někdo dostal do systému	586

Co dělat po průniku	588
Možné modifikace postupu obnovení	590
Nepřípustný výpadek	590
Nalezení útočníka	590
Nezjištěná příčina	590
Pravidla o mlčenlivosti	590
Shrnutí	592
▼ B. Aktualizace používaných programů	593
Aktualizace balíčků RPM	594
Aktualizace balíčků systému Debian	596
Aktualizace balíčků systému Slackware	600
Aktualizace jádra	601
Překlad jádra	601
Restart systému	608
▼ C. Vypnutí nepotřebných programů	609
Další informace týkající se jádra	608
Úroveň běhu	610
Adresáře /etc/rc#.d	611
Vypnutí určitých služeb	611
Red Hat	612
Debian	613
Síťové služby spouštěné démony inetd/xinetd	613
Inetd	613
Xinetd	615
Služby spouštěné přes svscan	616
Identifikace síťových démonů	617
Netstat	618
Lsof	619
▼ D. Rozbory reálných případů	621
Případová studie	622
Rejstřík	627