

Obsah

Předmluva překladatele	15
Předmluva	17
I Začínáme	21
1 Úvod	23
1.1 Proč bezpečnost?	23
1.2 Výběr bezpečnostní politiky	24
1.2.1 Postoj	26
1.3 Strategie pro bezpečnou síť	27
1.3.1 Bezpečnost připojeného počítače	27
1.3.2 Brány a firewally	29
1.3.3 Ochrana hesel	30
1.3.4 Šifrování	33
1.4 Etika počítačové bezpečnosti	34
1.5 Varování	35
2 Přehled TCP/IP	37
2.1 Jednotlivé vrstvy	37
2.1.1 IP	37
IP adresy	39
Bezpečnostní návěští v IP	39
2.1.2 ARP	40
2.1.3 TCP	40
2.1.4 UDP	42
2.1.5 ICMP	43

2.2	Směrovače a směrovací protokoly	43
2.3	Domain Name System	44
2.4	Standardní služby	46
2.4.1	SMTP	46
2.4.2	telnet	49
2.4.3	Network Time Protocol	50
2.4.4	Vyhledávání lidí	51
2.5	Protokoly založené na RPC	51
2.5.1	RPC a <i>portmapper</i>	51
2.5.2	NIS	54
2.5.3	NFS	54
2.5.4	Andrew	56
2.6	Protokoly pro přenos souborů	56
2.6.1	TFTP	56
2.6.2	FTP	57
2.6.3	FSP	59
2.7	Příkazy „r“ – vzdálené provádění příkazů	59
2.8	Informační služby	61
2.8.1	World Wide Web	61
2.8.2	NNTP	62
2.8.3	Multicasting a MBone	62
2.9	Systém X11	63
2.10	Proletence důvěry	64

II Sestavujeme vlastní firewall

67

3	Firewally	69
3.1	Podstata firewallů	69
3.1.1	Cena	69
3.2	Umístění firewallů	70
3.3	Brány filtrující pakety	72
3.3.1	Zpracování IP fragmentů	74
3.3.2	Filtrování FTP	74
3.3.3	Filtrování X Window	75
3.3.4	Kročení DNS	78
3.3.5	Protokoly bez pevných adres	80
3.3.6	Umístění filtru	81
3.3.7	Topologie sítě a falšování adres	83
3.3.8	Filtr paketů a UDP	86
3.3.9	Filtrování dalších protokolů	86
3.3.10	Filtrujeme směrování	87

3.3.11	Ukázkové konfigurace	89
3.3.12	Výkon při filtrování paketů	90
3.3.13	Implementace paketového filtru	90
3.3.14	Shrnutí	90
3.4	Brány na aplikační úrovni	91
3.5	Brány na úrovni okruhů	92
3.6	Podpora příchozích služeb	94
3.7	Dobré i špatné o tunelech	94
3.8	Společné podniky	96
3.9	Co firewally nedokáží	97
4	Jak sestavit bránu na aplikační úrovni	99
4.1	Bezpečnostní politika	99
4.2	Možnosti pro konfiguraci hardware	100
4.3	Počáteční instalace	102
4.4	Nástroje brány	104
4.4.1	<i>TCP wrapper</i>	104
4.4.2	Relay	106
4.4.3	Lepší <i>telnetd</i> démon	107
4.4.4	Podpora pro odchozí FTP	107
4.5	Instalace služeb	107
4.5.1	Doručování pošty	108
4.5.2	Příchozí <i>telnet</i>	109
4.5.3	Proxy služby	111
4.5.4	Menu služeb brány	112
4.5.5	Anonymní FTP	114
4.5.6	MBone	116
4.5.7	X11	117
4.5.8	WAIS, WWW a spol.	119
4.5.9	Proxy NFS	119
4.5.10	Instalace NTP	121
4.6	Ochrana ochránců	121
4.7	Správa brány	122
4.7.1	Záznamy	122
4.7.2	Integrita souborů	123
4.7.3	Další záležitosti	123
4.8	Bezpečnostní analýza – aneb proč je naše nastavení bezpečné a chráněné proti selhání	125
4.9	Výkon	126
4.10	TIS Firewall Toolkit	127
4.11	Hodnocení firewallů	128
4.11.1	Paketové filtry	128
4.11.2	Aplikační brány	128

4.11.3	Brány na úrovni okruhů	129
4.12	Život bez firewallu	129
5	Autentizace	131
5.1	Autentizace uživatele	131
5.1.1	Hesla	131
5.1.2	Jednorázová hesla	132
5.1.3	Čipové karty	134
5.1.4	Biometricky	134
5.2	Autentizace mezi počítači	135
5.2.1	Autentizace podle síťových adres	135
5.2.2	Kryptografické techniky	135
6	Užitečné nástroje	137
6.1	<i>proxylib</i>	137
6.1.1	<i>socks</i>	139
6.2	<i>syslog</i>	139
6.3	Sledování sítě: <i>tcpdump</i> a spol.	140
6.3.1	Použití <i>tcpdump</i>	140
6.3.2	<i>ping</i> , <i>traceroute</i> a <i>dig</i>	142
6.4	Rozšíření protokolování u standardních démonů	142
7	Pasti, léčky a návnady	145
7.1	Co protokolovat	145
7.1.1	Sondování adresového prostoru	149
7.1.2	Sledování ICMP	149
7.1.3	Kontrašpionáž	149
7.1.4	Nástroje pro sledování záznamů v protokolech	151
7.2	Nastrčené účty	151
7.3	Stopování spojení	152
8	Hackerova dílna	155
8.1	Úvod	155
8.2	Nalezení cíle	156
8.2.1	<i>pinglist</i>	159
8.2.2	Mapovací nástroje: <i>fremont</i>	160
8.3	Sondování počítačů	160
8.4	Nástroje kontrolující spojení	161
8.5	Hry se směrováním	162
8.6	Síťové monitory	162
8.7	Metastázy	164
8.8	Tygfí týmy	166
8.9	Další informace	167

III	Ohlédnutí	199
9	Druhy útoků	171
9.1	Krádeže hesel	171
9.2	Lidský faktor	172
9.3	Chyby a zadní vrátka	173
9.4	Selhání autentizace	175
9.5	Selhání protokolu	175
9.6	Únik informací	176
9.7	Odepření služby	177
10	Večer s Berferdem	179
10.1	Úvod	179
10.2	Nepřátelské skutky	179
10.3	Večer s Berferdem	182
10.4	Den poté	186
10.5	Vězení	187
10.6	Pátrání po Berferdovi	189
10.7	Berferd se vrací	190
11	Co se kde skrývá: Pohled do protokolovacích souborů	193
11.1	Rok práce	193
11.1.1	Záznamy přihlašování	195
11.1.2	Zvídavý <i>finger</i>	196
11.1.3	Hackerův rozvrh hodin	198
11.1.4	Jiné sondy	200
11.2	Použití proxy	201
11.3	Zdroje útoků	201
11.4	Šum na lince	204
IV	Závěrem něco navíc	207
12	Právní aspekty	209
12.1	Zákony počítačové kriminality	209
12.2	Protokolovací soubory jako důkaz	211
12.3	Je monitorování legální?	214
12.4	Otázky zodpovědnosti za škody	218
13	Bezpečná komunikace přes nezabezpečené sítě	221
13.1	Úvod do kryptografie	221
13.1.1	Značení	223
13.1.2	Symetrická kryptografie	223

13.1.3	Módy činnosti	224
	Mód elektronické kódovací knihy	224
	Mód řetězení šifrovaných bloků	224
	Mód zpětného vstupu pro výstup	225
	Mód zpětného vstupu pro šifru	225
	Jednorázová hesla	226
	Jak bezpečný je DES	226
13.1.4	Kryptografie veřejnými klíči	227
13.1.5	Exponenciální výměna klíčů	228
13.1.6	Digitální podpis	229
13.1.7	Bezpečné hašovací funkce	230
13.1.8	Časová razítka	231
13.2	Autentizační systém Kerberos	232
	13.2.1 Omezení	234
13.3	Šifrování na spojové úrovni	235
13.4	Šifrování na síťové a transportní úrovni	235
13.5	Šifrování na aplikační úrovni	238
	13.5.1 Protokol <i>telnet</i>	239
	13.5.2 Autentizace SNMP	239
	13.5.3 Bezpečná elektronická pošta	240
	PEM	240
	RIPEM	241
	PGP	241
	13.5.4 Rozhraní obecných služeb bezpečnosti pro aplikační programy	242
14	A kam dál?	243
A	Užitečné a bezplatné	247
	A.1 Budování firewallů	248
	A.1.1 TCP wrapper a <i>potmapper</i>	248
	A.1.2 <i>securelib</i>	248
	A.1.3 <i>socks</i>	248
	A.1.4 TIS Firewall Toolkit	249
	A.1.5 Proxy X11	249
	A.1.6 Bellcore <i>S/Key</i>	249
	A.1.7 Démon <i>ident</i>	249
	A.1.8 <i>swatch</i> – monitor souborů s protokoly	249
	A.1.9 Zdrojové kódy síťových démonů	249
	A.1.10 <i>screend</i>	250
	A.1.11 NFS	250
	A.1.12 <i>karlbridge</i>	250
	A.2 Nástroje pro správu a sledování sítě	250

A.2.1	<i>tcpdump</i>	250
A.2.2	<i>traceroute</i>	250
A.2.3	<i>dig</i>	251
A.2.4	<i>host</i>	251
A.2.5	<i>bind 4.9</i>	251
A.2.6	<i>SNMP</i>	251
A.2.7	<i>fremont</i> pro mapování sítí	251
A.3	Balíky pro audit	251
A.3.1	<i>TAMU</i>	251
A.3.2	<i>COPS</i>	252
A.3.3	<i>Tripwire</i>	252
A.3.4	<i>ISS</i>	252
A.3.5	<i>SATAN</i>	252
A.3.6	<i>crack</i>	252
A.3.7	<i>SPI</i>	253
A.4	Kryptografický software	253
A.4.1	<i>RIPEM</i>	253
A.4.2	<i>RSAREF</i>	253
A.4.3	<i>PEM</i>	253
A.4.4	<i>PGP</i>	253
A.4.5	<i>Kerberos</i>	253
A.4.6	<i>MD2</i> a <i>MD5</i>	253
A.4.7	<i>snefru</i>	254
A.5	Zdroje informací	254
A.5.1	Nástroje a doporučení <i>CERTu</i>	254
A.5.2	Konference <i>firewalls</i>	254
A.5.3	Konference <i>bugtraq</i>	254
A.5.4	<i>RISKS Forum</i>	254
A.5.5	Diskuzní skupiny <i>USENETu</i>	255
A.5.6	Bezpečnostní archiv <i>COAST</i>	255
B	Porty TCP a UDP	257
B.1	Pevně dané porty	257
B.2	<i>MBone</i>	260
C	Doporučení výrobčům	261
C.1	Všichni	261
C.2	Stanice	261
C.3	Směrovače	262
C.4	Protokoly	262
C.5	<i>Firewally</i>	263

Obsah

Literatura	265
Seznam hrozeb	279
Seznam obrázků	281
Seznam tabulek	283
Rejstřík	284

Obsah

Předmluva překladatele	15
Předmluva	17
I Začínáme	21
1 Úvod	23
2 Přehled TCP/IP	37
II Sestavujeme vlastní firewall	67
3 Firewally	69
4 Jak sestrojít bránu na aplikační úrovni	99
5 Autentizace	131
6 Užitečné nástroje	137
7 Pasti, léčky a návnady	145
8 Hackerova dílna	155
III Ohlédnutí	169
9 Druhy útoků	171
10 Večer s Berferdem	179
11 Co se kde skrývá: Pohled do protokolovacích souborů	193
IV Závěrem něco navíc	207
12 Právní aspekty	209
13 Bezpečná komunikace přes nezabezpečené sítě	221
14 A kam dál?	243
A Užitečné a bezplatné	247
B Porty TCP a UDP	257
C Doporučení výrobcům	261
Literatura	265
Seznam hrozeb	279
Seznam obrázků	281
Seznam tabulek	283
Rejstřík	284
