

A mű eredeti címe: NETWORK SECURITY FIRST-STEP, 1st Edition, 1587200996
by Thomas M. Published by Pearson Education, Inc., publishing as Cisco Press,
Copyright © 2004

Hungarian language edition Copyright © 2005 Panem Könyvkiadó

ISBN 963 545 425 2

ISSN 1785-3346

Fordította: Ketler Iván
Lektorálta: Szigeti Szabolcs
Tipográfia: Papp Gyula
Borítóterv: Tóth Attila
Tördelte: Pipaszó Bt.

A kiadásért felel a Panem Kft. ügyvezetője, Budapest, 2005
panem@panem.hu
www.panem.hu

Minden jog fenntartva. Jelen könyvet, illetve annak részeit tilos reprodukálni,
adatrögzítő rendszerben tárolni, bármilyen formában vagy eszközzel –
elektronikus úton vagy más módon – közölni a kiadók engedélye nélkül.

Nyomtatta és kötötte a Kaposvári Nyomda Kft. – 251017
Felelős vezető: Pogány Zoltán igazgató

Tartalomjegyzék

Bevezetés 13

1. fejezet. Itt gépkalózok élnek!	17
1.1. A célpont kiválasztása	18
1.2. Ártalmatlan információk megszerzése	20
1.3. Alkalom szülte célok	22
1.3.1. Alkalom szülte cél a hálózatomban?	23
1.4. Kiválasztott célpontok	24
1.4.1. Kiválasztott célponttá váltunk-e?	25
1.5. A támadás folyamata	26
1.5.1. Felderítés és nyomkeresés (helyszíni szemle)	26
1.5.2. Letapogatás	31
1.5.3. Kiértékelés	35
1.5.4. Hozzáférés megszerzése	39
1.5.5. A jogosultságok kiterjesztése	43
1.5.6. A nyomok elfedése	45
1.6. Hálózatbiztonsági szervezetek	48
1.6.1. CERT Koordinációs Központ	49
1.6.2. SANS	49
1.6.3. Internetbiztonsági Központ (CIS)	50
1.6.4. SCORE	50
1.6.5. Internet Viharközpont	50
1.6.6. ICAT Metabase	51
1.6.7. Security Focus	51
1.6.8. Mit tanulhatunk ezektől a szervezetektől?	51
1.7. Gyakori támadások áttekintése	52
1.8. Összefoglalás	56
1.9. Összefoglaló kérdések	56

2. fejezet. A biztonsági házirend és a felelősség	59
2.1. A bizalmi viszonyok meghatározása	63
2.2. Indokolható használati házirend	66
2.2.1. Áttekintés	66
2.2.2. Célkitűzés	67
2.2.3. Hatályosság	67
2.2.4. Általános használat és tulajdonjog	67
2.2.5. Biztonsági és tulajdonjogi információk	68
2.2.6. Visszaélések	70

2.2.7.	Büntetések	73	
2.2.8.	Következtetések	73	
2.3.	A jelszavak szabályozása	74	
2.3.1.	Áttekintés	74	
2.3.2.	Célkitűzés	75	
2.3.3.	Hatályosság	75	
2.3.4.	Általános szabályok	76	
2.3.5.	A jelszókészítés általános alapelvei	77	
2.3.6.	Jelszóvédelmi szabályok	79	
2.3.7.	Büntetések	80	
2.3.8.	Következtetések	80	
2.4.	A virtuális magánhálózat (VPN) biztonsági szabályzata	81	
2.4.1.	Célkitűzés	82	
2.4.2.	Hatályosság	82	
2.4.3.	Általános szabályok	82	
2.4.4.	Következtetések	84	
2.5.	Az extranet csatlakozás házirendje	85	
2.5.1.	Célkitűzés	85	
2.5.2.	Hatályosság	86	
2.5.3.	Biztonsági átvizsgálás	86	
2.5.4.	A másik fél csatlakozási szerződése	86	
2.5.5.	Üzleti érdek	87	
2.5.6.	Kapcsolattartási pont	87	
2.5.7.	A csatlakozás létrehozása	87	
2.5.8.	A hozzáférés és a csatlakozás módosítása	87	
2.5.9.	A hozzáférés visszavonása	88	
2.5.10.	Következtetések	88	
2.6.	Az ISO-minősítés és a biztonság	89	
2.7.	Példák biztonsági szabályzatokra az interneten	91	
2.8.	Összefoglalás	92	
2.9.	Összefoglaló kérdések	92	

3. fejezet. A biztonsági technológiák áttekintése 95

3.1.	A biztonság fő tervezési elvei	96	
3.2.	Csomagszűrés a hozzáférés-vezérlő lista segítségével	99	
3.2.1.	A bevásárlólista analógiája	101	
3.2.2.	A csomagszűrés korlátai	104	
3.3.	Állapotteljes csomagvizsgálat	105	
3.3.1.	Az SPI használatával kezelt bővített csomagfolyam	106	
3.3.2.	Az állapotteljes csomagvizsgálat korlátai	108	
3.4.	A hálózaticím-fordítás	109	

3.4.1.	A hálózatbiztonság növelése	112
3.4.2.	A címfordítás korlátai	113
3.5.	A közvetítők és az alkalmazásszintű védelem	114
3.5.1.	A közvetítő korlátai	117
3.6.	Tartalomszűrés	118
3.6.1.	A tartalomszűrés korlátai	121
3.7.	Nyilvános kulcsú infrastruktúra	122
3.7.1.	A PKI korlátai	124
3.8.	AAA technológiák	125
3.8.1.	Hitelesítés (azonosítás)	125
3.8.2.	Feljogosítás	126
3.8.3.	Naplózás	127
3.8.4.	RADIUS	128
3.8.5.	TACACS	129
3.8.6.	A TACACS+ és a RADIUS összehasonlítása	131
3.9.	Összefoglalás	131
3.10.	Összefoglaló kérdések	132
4. fejezet.	Biztonsági protokollok	133
4.1.	A DES titkosítás	135
4.1.1.	A titkosítás erőssége	137
4.1.2.	A DES korlátai	138
4.2.	A tripla DES (3DES) titkosítás	138
4.2.1.	A titkosítás erőssége	140
4.2.2.	A 3DES korlátai	140
4.3.	Az MD5 algoritmus	140
4.3.1.	Az MD5 algoritmus működése	143
4.4.	A pont-pont közötti alagútprotokoll (PPTP)	144
4.4.1.	A PPTP működése	145
4.4.2.	A PPTP korlátai	146
4.5.	A második rétegbeli alagútprotokoll (L2TP)	147
4.5.1.	Az L2TP és a PPTP összehasonlítása	148
4.5.2.	Az L2TP előnyei	148
4.5.3.	Az L2TP működése	149
4.6.	A biztonságos távelérés	152
4.6.1.	Az SSH és a telnet összehasonlítása	153
4.6.2.	Az SSH működése	156
4.6.3.	Alagút kiépítése és végpont áthelyezése	157
4.6.4.	Az SSH korlátai	158
4.7.	Összefoglalás	159
4.8.	Összefoglaló kérdések	160

5. fejezet. Tűzfalak 161

5.1.	Gyakran ismételt kérdések a tűzfalakkal kapcsolatban	163
5.1.1.	Kinek van szüksége tűzfalakra?	163
5.1.2.	Miért van szükségem tűzfalakra?	164
5.1.3.	Vannak-e megvédendő értékeim?	165
5.1.4.	Hogyan működik a tűzfal?	166
5.2.	A tűzfal maga a biztonsági házirend	167
5.3.	A tűzfal működésének áttekintése	170
5.3.1.	A tűzfal működése	172
5.3.2.	A tűzfal alkalmazása	173
5.3.3.	A bejövő forgalomra vonatkozó szabályzat meghatározása	175
5.3.4.	A kimenő forgalomra vonatkozó szabályzat meghatározása	177
5.4.	Elsőként az alapelvek: élet a DMZ-ben	177
5.5.	Esettanulmányok	179
5.5.1.	Demilitarizálni vagy nem demilitarizálni?	180
5.5.2.	Levelezőszerver a tűzfallal védett belső hálózatban	181
5.5.3.	A tűzfal beállítása (levelezőszerver a DMZ-ben)	184
5.6.	A tűzfalak korlátai	188
5.7.	Összefoglalás	189
5.8.	Összefoglaló kérdések	190

6. fejezet. Útválasztók 191

6.1.	A peremi útválasztó mint ellenőrző pont	196
6.1.1.	Az ellenőrző pontként működő útválasztók korlátai	198
6.2.	Csomagvizsgáló útválasztó	199
6.2.1.	A tűzfalkészlet előnyei	200
6.2.2.	Tartalomalapú csomagvizsgálat	203
6.2.3.	A behatolás érzékelése a Cisco IOS segítségével	208
6.2.4.	Mikor használjuk a tűzfalkészlet IDS-modulját?	210
6.2.5.	A tűzfalkészlet IDS-moduljának működése	210
6.2.6.	A tűzfalkészlet korlátai	213
6.3.	Biztonságos IOS-sablon	214
6.4.	Összefoglalás	231
6.5.	Összefoglaló kérdések	232

7. fejezet. Virtuális magánhálózatok 233

7.1.	A VPN a biztonságos összeköttetés	236
7.2.	A VPN áttekintése	238
7.2.1.	A VPN előnyei és célja	241
7.2.2.	VPN implementációs stratégiák	242
7.2.3.	Megosztott alagút	245

7.3.	Az IPSec VPN áttekintése	245
7.3.1.	Az adatok hitelesítése és sértetlensége	248
7.3.2.	Alagúttechnika	249
7.3.3.	Titkosító módszerek	250
7.3.4.	IPSec-protokollok	251
7.3.5.	Az IPSec működése	255
7.4.	Az útválasztó beállítása VPN-végpontként	260
7.4.1.	Az ISAKMP beállítása	260
7.4.2.	Az IPSec beállítása	263
7.5.	A tűzfal VPN-beállítása a kliens-hozzáférés számára	267
7.6.	Összefoglalás	270
7.7.	Összefoglaló kérdések	270
8. fejezet.	Vezeték nélküli biztonság	271
8.1.	Vezeték nélküli helyi hálózatok	274
8.1.1.	Mi az a Wi-Fi?	276
8.1.2.	A vezeték nélküli hálózatok előnyei	276
8.1.3.	A vezeték nélküli egyenlő a rádióhullámokkal	277
8.2.	Vezeték nélküli hálózat	278
8.2.1.	Működési módok	278
8.2.2.	Hatósugár	280
8.2.3.	Elérhető sáv szélesség	281
8.3.	Vezeték nélküli háborús játékok	281
8.4.	A drótnélküliség veszélyei	289
8.4.1.	Lehallgatás	289
8.4.2.	Szolgáltatásmegtagadási támadások	291
8.4.3.	Szélhámossá/jogosulatlan elérési pontok	292
8.4.4.	Hibásan beállított elérési pontok	295
8.4.5.	Hálózati visszaélések	296
8.5.	Vezeték nélküli biztonság	296
8.5.1.	Szolgáltatáskészlet-azonosító (SSID)	297
8.5.2.	Az eszközök és az AP csatlakozása	298
8.5.3.	Vezetékessel egyenértékű titkosság (WEP)	298
8.5.4.	MAC-címszűrés	300
8.5.5.	Bővíthető hitelesítőprotokoll	301
8.5.6.	A vezeték nélküli biztonság növelése	304
8.6.	A vezeték nélküli támadók eszközei	305
8.6.1.	NetStumbler	305
8.6.2.	Vezeték nélküli csomagszaglászók	308
8.6.3.	AirSNORT	309
8.7.	Összefoglalás	310
8.8.	Összefoglaló kérdések	310

9. fejezet. A behatolás érzékelése és a mézesbödön	311
9.1. A behatolás érzékelése	314
9.1.1. Az IDS működése	317
9.2. Hogyan lehet észrevenni a behatolást?	322
9.2.1. A kommunikációfolyam újbóli összeállítása	323
9.2.2. Protokollanalízis	323
9.2.3. Az eltérés felismerése	323
9.2.4. A minta egyezősége	324
9.2.5. Naplóanalízis	325
9.2.6. A módszerek kombinálása	326
9.2.7. A behatolás megakadályozása	326
9.2.8. Az IPS reakciója és cselekvése	327
9.2.9. IDS-termékek	328
9.2.10. Az IDS korlátai	331
9.3. A mézesbödön	333
9.3.1. A mézesbödön tervezésének stratégiái	337
9.3.2. A mézesbödön korlátai	337
9.4. Összefoglalás	338
9.5. Összefoglaló kérdések	338
10. fejezet. Kereskedelmi eszközök	339
10.1. A sebezhetőség elemzése	342
10.1.1. Alapvető támadások	342
10.2. A biztonság kiértékelése és az áttörhetőség ellenőrzése	353
10.2.1. A belső sérülékenységi és áttörhetőség ellenőrzése	353
10.2.2. A külső sérülékenységi és áttörhetőség ellenőrzése	355
10.2.3. A fizikai biztonság kiértékelése	356
10.2.4. Különböző kiértékelések	359
10.3. Sérülékenységi-ellenőrzők	359
10.3.1. A sérülékenységi-ellenőrzők jellemzői és előnyei	360
10.3.2. Nessus	361
10.3.3. Retina	363
10.4. A védelem áttörhetőségét vizsgáló termékek	367
10.4.1. Core Impact	368
10.5. Összefoglalás	373
10.6. Összefoglaló kérdések	373

A) függelék. Válaszok az összefoglaló kérdésekre	375
B) függelék. Fogalomtár	387
A szerzőről	400
Tárgymutató	401

Bevezetés

A könyv a hálózatok biztonságával kapcsolatos kérdések jobb megértése iránti igény kielégítésére íródott. Ebben a témakörben már számos szöveg látott napvilágot. Sokan, magánszemélyek és vállalatok egyaránt azonban még csak most fontolgatják, hogyan is kezdjék el hálózatuk biztonságosá tételét. Lehet, hogy valaki vezetékek nélküli hálózatot szeretne telepíteni, és a lehető legbiztonságosabbá akarja azt tenni. Esetleg a tűzfalakkal vagy más biztonsági témakörökkel kapcsolatos információkra kíváncsi. A könyv elegendő információt tartalmaz a hálózati biztonsággal kapcsolatosan ahhoz, hogy ezzel a tudással felvértezve a saját és a cége érdekében is képes legyen a szükséges óvintézkedések megtételére.

A könyv azzal a feltételezéssel íródott, hogy minden olvasójában megvan a biztonság iránti természetes igény, ám jelenleg még nem igazán ismeri a kockázatokat, technikákat, és az elérhető lehetőségeket sem. Ennek megfelelően minden egyes fejezet a többrétegű, komplex biztonsági rendszer egy-egy rétegét igyekszik bemutatni, egyben megválaszolva azt a kérdést is, hogy miért van egyáltalán szükség az adott terület védelmére, mire kell odafigyelni, és hogyan kell az adott területet ténylegesen megvédeni.

CÉLOK ÉS MÓDSZEREK

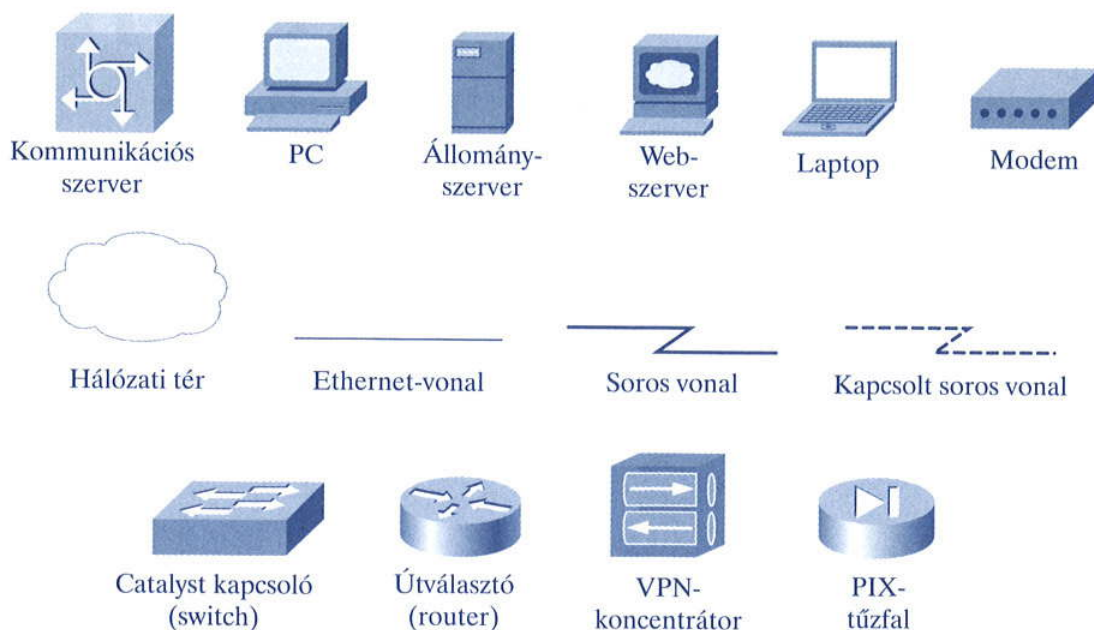
A könyv célja az, hogy a biztonsággal törődni kívánó személyek számára információforrás lehessen. Az olvasónak nem kell hálózati szakembernek vagy informatikai vezetőnek lennie ahhoz, hogy előnyére váljék a könyv elolvasása, bár természetesen az ilyen tudással felvértezett szakemberek is olvashatják. A szerző reményei szerint valamennyi olvasónak, legyen bár egyetemista vagy szakértő, valóban hasznos a könyv elolvasása.

A KÖNYV FELÉPÍTÉSE

A könyv elolvasható az elejétől a végéig, de kellően rugalmasan van felépítve ahhoz, hogy adott esetben mindenki csak az őt érdeklő fejezeteket olvassa el belőle. Ha valamennyit el akarná olvasni, akkor sorrendben célszerű haladni.

1. **fejezet.** *Itt gépkalózok élnek!* Ez a fejezet bepillantást enged azon személyek motivációiba és fejébe, akik rendszereinket támadják. Itt tárgyaljuk a technikákat, a támadási formákat, és a felhasznált eszközöket.
2. **fejezet.** *A biztonsági házirend és a felelősség.* A biztonsági védelem rétegezett felépítésének legelső, a további lépéseket megalapozó témakörét mutatja be, mégpedig a szabályzatokat és házirendeket. A fejezet végére érhetővé válik a szabályzatok fontossága.
3. **fejezet.** *A biztonsági technológiák áttekintése.* A biztonsági technológiákat igyekszik bemutatni, kezdve a valamennyi útválasztóban (routerben) megtalálható hozzáférés-vezérlő listáktól egészen a globális megoldásokig, mint amilyen például a nyilvános kulcsú infrastruktúra (PKI). A technológiák közül többet is lehet ugyan anélkül használni, hogy pontosan megérténénk azokat, a fejezet azonban igyekszik kitérni a hiányosságaikra is, jobb megértésük pedig hatékonyabb használatukat teszi lehetővé.
4. **fejezet.** *Biztonsági protokollok.* Bemutatja a hálózat biztonságossá tétele során használt biztonsági és titkosítási protokollokat. Ismerteti a tárgyalt protokollok korlátait és hiányosságait is, hiszen semmi sem lehet tökéletes.
5. **fejezet.** *Tűzfalak.* A tűzfalak működését mutatja be. Megvizsgálja, hogy egyáltalán kinek van szüksége tűzfalra, és bizonyítja a hálózat biztonságában betöltött alapvető a szerepüket.
6. **fejezet.** *Az útválasztók biztonsága.* Az útválasztók biztonsági képességeit mutatja be. Akinek hálózata van, annak útválasztója is kell legyen. Ezek az eszközök viszont megjelenésük óta sokat fejlődtek, és alapvető feladatukon túl ma már számos biztonsági funkciójuk is van.
7. **fejezet.** *A virtuális magánhálózat biztonsága.* A virtuális magánhálózat szerepét és működését vizsgálja. Bemutatja, miként használhatja a nyilvános internetet, titkosítva az ott keresztülhaladó minden továbbított adatát.
8. **fejezet.** *Vezeték nélküli biztonság.* A vezeték nélküli hálózat biztonságát tárgyalja. A jelenlegi legfrissebb, és ezért még korántsem kiforrott technológia sérülékenységét és biztonságossá tételének korlátait mutatja be.
9. **fejezet.** *A behatolás érzékelése és a mézesbödön.* Megmutatja, miként észlelhetjük egy támadó próbálkozásait, és ismerteti a támadó megtévesztésének kiváló módszerét is, a „mézesbödön” névre hallgató megtévesztő technika alkalmazását.
10. **fejezet.** *Kereskedelmi eszközök.* A támadók által használt biztonsági eszközöket és szoftvereket mutatja be, hogy az olvasó felkészülhessen az ellenük való védekezésre. Megismerésükkel, illetve felhasználásukkal magunk is időben felfedhetjük hálózatunk hiányosságait, és megtehetjük a kellő intézkedéseket ezek kijavítására.

A KÖNYV ÁBRÁIN HASZNÁLT JELÖLÉSEK



PARANCSSZINTAKTIKAI KONVENCIÓK

A könyvben a parancsok szintaxisának bemutatására használt konvenciók az IOS-parancsreferencia által használtakkal egyeznek meg. A parancsreferencia ezeket az alábbiak szerint írja le:

- **Vastag szedés** jelzi a változtatás nélkül beírandó parancsokat és kulcsszavakat. A tényleges konfigurációs példákban és a kimeneti szövegben (amely nem általános parancsszintaxis) a vastag szedés jelöli a felhasználó által kézzel beírt szöveget (mint például a **show** parancs).
- **Dőlt szedés** jelöli azokat az argumentumokat, amelyek helyett a tényleges értékeket kell megadni.
- A függőleges vonalak (|) választják el a vagylagos, egymást kölcsönösen kizáró elemeket.
- Szögletes zárójelek [] közé az opcionális elemeket zártuk.
- A kapcsos zárójelek { } kötelező választást jelölnek.
- Kapcsos zárójelek a szögletes belsejében az opcionális elemen belüli kötelező választást jelölik.