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

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

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

Tartalomjegyzék

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 biztonságossá tételét. Lehet, hogy valaki vezeték 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 érthetővé 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 megértenénk 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.

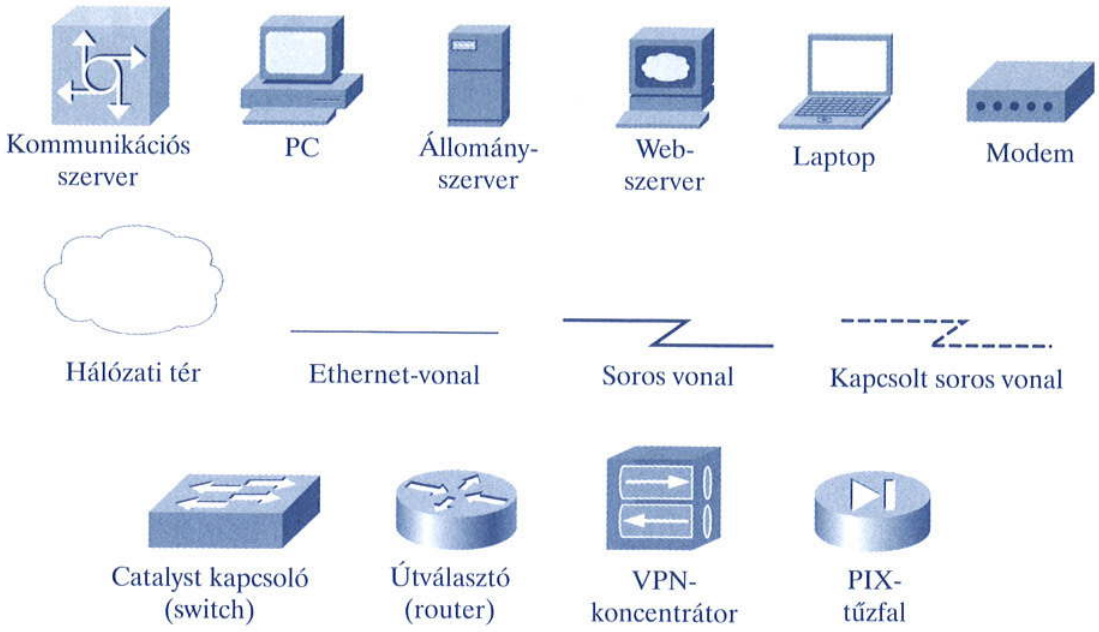
7. fejezet. *A virtuális magánhálózat biztonsága.* A virtuális magánhálózat szerepét és működését vizsgálja. Bemutatja, miként használhatja a nyilvános internetet, titkosítva az ott keresztülhaladó minden továbbított adatát.

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.