

5. lépés. A dinamikus leképzési bejegyzést hozzáadja egy statikus leképzési készlethez. Mindig győződjünk meg arról, hogy a dinamikus bejegyzéseknek legyen a legkisebb prioritásuk (legnagyobb sorszámuk) a készletben.

```
crypto map leképzés-név sorszám ipsec-isakmp dynamic  
dinamikus-leképzés-neve
```

Példa:

```
crypto map mymap 200 ipsec-isakmp dynamic dyn1
```

7.6. ÖSSZEFoglalás

Ebben a fejezetben megtárgyaltuk, hogy mi is az a VPN, és milyen általános előnyökkel jár a használata. A VPN implementálásának legnagyobb előnye a költségek csökkentése és az általános gazdasági megtakarítás. A sávszélességi költségek megtakarítása tette a VPN-t az elérhető legjobb megoldássá.

Ebben a fejezetben a legjobb létező VPN-ekre koncentráltunk: az IPSec-alapú VPN-re. Az adatvédelmi képesség megértése érdekében megvizsgáltuk mindeneket a különböző szinteket, meneteket és eljárási típusokat, amelyek az IPSec-alapú VPN-ben az adatok biztonságának megőrzéséhez szükségesek. Ez valóban lenyűgöző feladat volt, hiszen az érintett problémák bonyolultsága gyorsan növekszik.

7.7. Összefoglaló kérdések

1. Van-e lehetőség titkosítás nélküli VPN felállítására?
2. Sorolja fel a VPN három típusát!
3. Válassza ki a VPN három jellemzőjét és előnyét, és mutassa meg, hogy az ön vállalata miként tud belőlük használ húzni!
4. A VPN-koncentrátorokat sok felhasználó igényeihez alakították ki. Mutassa be, hogy hány felhasználóhoz és mikor célszerű a használtuk!
5. Mikor következik be az alagút megosztása?
6. Milyen szerepe van a hitelesítésnek az adatfolyam biztonságában?
7. Milyen protokollok játszanak szerepet, amikor az adatot az IPSec-alagútban küldjük?
8. A telephelyközi VPN esetén melyik a két különböző csomagoló protokoll, és mi közöttük a különbség?
9. Nevezze meg az IKE előnyeit!

8. fejezet

Vezeték nélküli biztonság

A vég közeledtével nem ellenségeink szavára, hanem barátaink hallgatására fogunk emlékezni.

(ifj. Martin Luther King)

A fejezet elolvasása után érteni kell, és el kell tudni magyarázni az alábbi témákat:

- A vezeték nélküli helyi hálózat alapelveit, beleértve az előnyeit és a biztonsági kockázatát
- A vezeték nélküli hálózattal szembeni komolyabb fenyegetéseket
- A támadók számára elérhető lehetséges támadások és lehetőségek lényegét és határait

Mikor tudott a kedves olvasó utoljára úgy elmenni szabadságra, hogy mindenről megszabaduljon? Esetleg valami távoli helyre, egy másik országba? Képzelje most el, hogy kisétál a szállodai szobájának ajtaján (amely szoba természetesen a tengerre néz), hogy megcsodálja az óceánba lenyugvó nap káprázatos színjátékát. A levegő egy kicsit hűvös, így alaposan beburkolódzik egy pokrócba, lefekszik a kedvenc nyugágyára, és figyeli a tengeri sirályok játékos röptét és a hullámok ritmikus morajlását – és ekkor bíp-bíp-bíp, SMS érkezését jelzi a mobiltelefonja!

Ki lehet az az elvetemült, aki ilyenkor hívja, amikor végre egy kicsit ki-pihenhetné magát, és elszakadhatna a minden napoktól? Micsoda vész-helyzet lehet annyira súlyos, hogy a vakáció alatt is meg kell miatta zavarni vele a nyugalmát?

Az SMS szövegéből az derül ki, hogy úgy tűnik, valamilyen probléma lépett fel a vállalat tűzfalán/VPN-jén/levelezőszerverén/más ön által felügyelt eszközön. Meglehetősen komolynak tűnik a probléma, így sajnos arra a következtetésre kell jutnia, hogy valamiképpen be kell jelentkezni a vállalati hálózatba, és meg kell vizsgálnia a problémát.

Nagy szerencse, hogy a szálloda rendelkezik szélessávú internettel, önnig pedig elhozta magával a vezeték nélküli kapcsolódáshoz szükséges hozzáférési pontot. A hozzáférési pont már csatlakoztatva van az internetre, így nyugodtan élvezheti tovább a csodás látványt. A laptop bekapcsolása sajnos nem kerülhető el, hiába fogadta meg a szabadsága elején, hogy egy pillantást sem fog vetni rá – a vész helyzet feloldja az ígéret betartása alól.

Ott üldögél tehát a szoba előtti verandán, és éppen indul a laptopja. Látja a vezeték nélküli kapcsolatot jelző led villogásán, hogy minden rendben van, a kapcsolat feléledt.

Beizzítja a távoli parancsér telmezőt, majd bejelentkezik az útválasztóra/tűzfalra, és elkezd körbevizsgálódni, hogy mi is okozhatja a problémát. Ez nem tarthat soká, mondja magának. Még mindig elég idő marad az est további részének kellemes eltöltésére, beleértve egy remek vacsorát. Egy óra elteltével a probléma meg is oldódott. Ön teljesen elégedett magával, mert zseniálisan sikerült felismerni és kiküszöbölni a bajt, minden össze néhány apró beavatkozással.

Állítsuk meg egy pillanatra ezt a filmet, és nézzünk kicsit a színfalak mögé. Ez a szabadságát töltő szupertechnikus épp most okozott a vállalatának többmillió dolláros veszteséget. „Hogyan?” – üti fel a fejét most a kedves olvasó. Miként okozhatott ez a fickó többmillió dolláros veszteséget csupán azzal, hogy bejelentkezett a vállalat tűzfalára/útválasztójára, és megoldott egy problémát?

A bajt nem az okozta, hogy bejelentkezett a vállalat hálózatára, hanem az, hogy ehhez vezeték nélküli kapcsolatot használt. Az a vállalat, amelynek ez a szupertechnikus dolgozott (múlt időben, mert az incidens után

(persze kirúgták), egy olyan multinacionális vállalat, amely kifejlesztett egy olcsó technológiát arra, miként lehet használt pizzásdobozokból memóriamodulokat gyártani, és éppen ennek bejelentésére készült. Erre a forradalmian új technológiára persze erősen fájt a foga a vállalat versenytársának is, aki nem csupán a bejelentést kívánta lehetőleg megakadályozni, de szerették volna a terveket is megszerezni a saját részlegük számára, hogy ők jelenhessenek meg elsőként a piacon ezzel a termékkel.

A versenytárs valószínűleg alkalmazott egy számítógépes kalózt, és fizette neki az útját, hogy követhesse a fenti szupertechnikust. Ez a kalóz egy alkalmas pillanatban betört a szupertechnikus szobájába, és a laptop teljes tartalmát lemásolta egy mobil tárolóeszközre abban a reményben, hogy talál a gépen valamilyen hasznos információt erről az új technológiáról. Amikor észrevette, hogy a szupertechnikus bekapcsolja a gépet, és a vezeték nélküli kapcsolaton keresztül elkezd dolgozni, a támadó is felismerte, hogy váratlanul aranybányára bukkant, gyorsan betört a vállalat hálózatába, és elkezdett ott kerestgálni. Mindez a szupertechnikus nem biztonságos vezeték nélküli kapcsolata révén tehette meg. A távolról elkövetett betörés és szaglászás – kicsit a „lehetetlen küldetéshez” hasonlít, ugye? Meglehetősen kis esély van arra, hogy valaha is sikerüljön, ugye? Nos, a valóság az, hogy a fenti élethelyzet szinte naponta megtörténik valahol. A vezeték nélküli kapcsolatra is képes laptopokkal felszerelt támadók igen kicsiny erőfeszítéssel értékes információkhoz juthatnak közvetlenül a „levegőből”. Ehhez olyan szoftvereket használnak, amelyek könnyen elérhetők az interneten, és számos bajt okoznak azoknak a vállalatoknak, amelyek nem ismerik fel a nem biztonságos vezeték nélküli hálózat jelentette veszélyt.

Ebben a fejezetben a vezeték nélküli hálózat biztonságával kapcsolatos számos kérdésre keressük a választ, hogy felvértezzük az olvasót a vezeték nélküli hálózatokat kívülről fenyegető lehetséges behatolási kísérletek különböző típusainak felismeréséhez, megértéséhez és megakadályozásához szükséges ismeretekkel. Elsődlegesen a vállalatok számára készített vezeték nélküli berendezésekkel foglalkozunk, nem pedig a Cisco alvállalata, a Linksys által otthoni használatra gyártott eszközökkel. Nagyon fontos felismerni a különbséget: a Cisco Linksys felvásárlásáról írt alábbi szövegben világos és egyértelmű üzenet található:

Vegyük például a Cisco Aironet vezeték nélküli termékcísaládját. Ezek az eszközök a Cisco iparvezető WLAN- és hálózati technológiába fektetett jelentős beruházások végtermékei. A teljes bonyolult hálózat részét képezve a biztonság, hatótávolság, kezelhetőség, teljesítmény, használhatóság és a birtokba vétel költségei szempontjából egyaránt kiemelkedő értéket képviselnek. Ezzel szemben a Linksys termékei létező hardver- és szoftvermegoldásokon alapulnak, és elsősorban a könnyű kezelhetőség, olcsóság és a használhatóság követelményének kívánnak megfelelni.

Ebből a példából is látható, hogy ezeket a termékeket más piacokra és más igények kielégítésére szánták. (http://newsroom.cisco.com/dlls/hd_032003.html)

8.1. A VEZETÉK NÉLKÜLI HELYI HÁLÓZATOK

Ebben a fejezetben a vezeték nélküli helyi hálózatok (*WLAN – wireless LAN*) használatát igyekszünk bemutatni, amelyek ma már környezetünkben a legtöbb helyen megtalálhatók, a repülőterektől kezdve az éttermekben, kávézókon át egészen az otthonokig. A személyi számítógépek nyolcvanas években bekövetkezett nagyméretű elterjedését elsőként a helyi hálózatok (*LAN – Local Area Network*) megjelenése, majd az internet gyors kialakulása követte a kilencvenes években. Mindez lehetővé tette a földrajzi helytől független kapcsolatot. A WLAN a kétezres évekre a következő gyorsan terjedő technológia nagy ígérete. Az üzleti életben természetesen hamar felismerték a WLAN előnyeit, és egyre növekvő mértékben alkalmazzák is. Ahogy a vállalkozások rákényszerültek az internettel és a személyi számítógépekkel kapcsolatos biztonsági intézkedések bevezetésére és fokozódó használatára, ugyanígy a legtöbb felismerték azt is, hogy az általuk nyújtott termelékenységnövelés és mobilitás mellett a WLAN-hoz megoldandó biztonsági problémák is társulnak.

A WLAN a rézalapú hálózatok gyors és hatékony kiterjeszhetőségét teszik lehetővé. A rézalapú hálózatban megfelelően elhelyezett hozzáférési pontok (*access point*) segítségével a vezeték nélküli csatolókártyával felszerelt asztali és hordozható számítógépek akár a hozzáférési ponttól mért 300 méter távolságból is szélessávú hozzáféréssel érik el a vezetékes hálózatot. Ez azt jelenti, hogy a számítógépek nincsenek többé a kábelezési infrastruktúrához kötve – felszabadító érzés, ugye?

A WLAN-telepítések többségét a 802.11b vezeték nélküli átviteli szabványnak megfelelően építették ki. Az IEEE 802.11b szabvány a 2,4 GHz-es rádiófrekvencia használatát követeli meg – erre a „szabad” sávra nem vonatkoznak kormányzati előírások. Legfeljebb 11 Mbps átviteli sebesség elérését teszi lehetővé, ami a nagyméretű e-levél-csatolmányok és komoly sávszélességet igénylő alkalmazások, például videokonferenciák működését is lehetővé teszi. Jóllehet jelenleg ez a szabvány uralja a vezeték nélküli hálózati piacot, ugyanezen szabványnak más változatai is fejlesztés alatt állnak, némelyek már meg is szerezték a szükséges jóváhagyást, mivel a sávszélesség növelése állandó követelményként jelentkezik. Jelenleg a 802.11g a legutolsó ilyen szabványváltozat, amely 56 Mbps átviteli sebességet tesz lehetővé.

A különböző vezeték nélküli szabványok más piaci szegmenseket céloznak, amint az a 8.1. és 8.2. táblázatban látható.

HÁLÓZATI BIZTONSÁG

8.1. táblázat. A 802.11a/WLAN szabványos karakterisztikája

Szabvány	IEEE 802.11a, WLAN
Hullámhossz-frekvencia	5 GHz
Adat-sávszélesség	54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 12 Mbps, 6 Mbps
Biztonsági kiegészítők	WEP, OFDM
Optimális működési távolság	50 méter beltérben, 100 méter kültéren
Legjobb alkalmazási területe (célpont vagy eszköz típusa)	Mozgó laptop számítógépekhez otthoni vagy üzleti használatra; számítógéphez, ha a kábelezés akadályokba ütközik.

A 802.11a soha nem lett kiadva, a legfrissebb 802.11g viszont a sebesség és a biztonság tekintetében néhány érdekes lehetőséggel rendelkezik (lásd 8.2. táblázat).

8.2. táblázat. A 802.11g/Wi-Fi szabványos karakterisztikája

Szabvány	IEEE 802.11g, Wi-Fi
Hullámhossz-frekvencia	2.4 GHz
Adat-sávszélesség	54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 12 Mbps, 6 Mbps
Biztonsági kiegészítők	WEP, OFDM, AES, és lehetséges a WPA/Wi-Fi védett hozzáférés
Optimális működési távolság	300 méter ideális feltételek esetén; normál működés 30 méter beltérben, 100 méter kültéren
Legjobb alkalmazási területe (célpont vagy eszköz típusa)	Mozgó laptop számítógépekhez otthoni vagy üzleti használatra; számítógéphez, ha a kábelezés akadályokba ütközik.

Jegyezzük meg, ha a 802.11b-klienseknek működniük kell a 802.11g hozzáférési ponttal, a biztonsági beállításokat gyengíteni kell. A WEP-nek és biztonsági problémáinak köszönhetően ekkor a teljes hálózat biztonsága a legkisebb közös szintre csökken.

8.1.1. MI AZ A WI-FI?

A Wi-Fi¹ (*wireless fidelity*) kifejezést gyakran használjuk a 802.11 hálózatok megnevezésére. A vezeték nélküli hálózatról beszélve ez a kifejezés egyértelműen a legnépszerűbb marketinges szó. Egyre inkább elterjed a használata, s mivel sokkal gyorsabban és könnyebben lehet kimondani, mint a „vezeték nélküli hálózat” kifejezést, így ezúttal a marketingesek megkaphatják a méltó elismerést a bevezetéséért.

A Wi-Fi utal továbbá a Wi-Fi Szövetség által kiadott igazolásra. Ez a szövetség a 802.11 gyártók nonprofit szervezete. Az igazolást megszerzett termékek tesztelése megtörtént, és így bizonyítottan képesek az együttműködésre más, ugyanezen igazolást megszerzett termékekkel. Ez azt jelenti, hogy az igazolt termék használható a 802.11 Wi-Fi igazolású hálózatban, legyenek azok Apple számítógépek vagy Windows-alapúak. Bár az igazolással nem rendelkező termékek is jól együttműködhetnek az igazoltakkal, a Wi-Fi igazolás jelzése az együttműködés biztosítéka. A Wi-Fi Szövetségről a <http://www.weca.net> webhelyen lehet többet megtudni.

8.1.2. A VEZETÉK NÉLKÜLI HÁLÓZATOK ELŐNYEI

Mostanában nem kellett sokat utaznom repülőgépen, de egy fontos családi esemény, a testvérem esküvője ismét rákényszerített. Mivel egyetlen nagyobb repülőtér sincs a környékemen, így négy különböző repülőteret próbálhattam ki. Ezek mindegyike biztosított vezeték nélküli hálózati elérést az utasok számára, így a repülőtéri holtidőket kihasználva értelmesen tölthetik az idejüket. Világszerte számos vállalkozás használja a vezeték nélküli lehetőséget, amely viszonylag kis költséggel bevezethető. A vezeték nélküli hálózatok előnyei az alábbiakban összegezhetők:

- **Kedvező ár** – A vezeték nélküli hálózat telepítése sokkal olcsóbb lehet, mint a rézalapúé, hiszen elmarad a kábelek és a kábelezés költsége. Egyszerűen üzembe kell helyezni egy hozzáférési pontot, amely egyszerre több számítógépet is ki tud használni.
- **Mobilitás** – A felhasználói termelékenység megnövelhető pusztán azval, hogy képessé válnak a hálózathoz való csatlakozásra bárhol egy hozzáférési pont közelében.

¹ A kifejezés nyilvánvalóan a hangtechnikából ismert Hi-Fi (*high fidelity* – magas hanghűség) kifejezés átalakítása, amely már korábban a jó minőségű hang jelzőjévé vált a közönségben. (A ford. meg.)

- Gyors és rugalmas telepítés** – A rézalapú hálózat gyorsan és könnyen kiterjeszhető pusztán azzal, hogy elérési pontokat helyezünk üzembe a megfelelő pontjain.
- Alkalmazásfüggetlen** – A rézalapú hálózat kiterjesztéseként a WLAN minden létező alkalmazással kompatibilis. Amint arról már esett szó, a szabványos protokoll a TCP/IP, amely a vezeték nélküli hálózatok minden formája által támogatott.
- Teljesítmény** – A WLAN nagy sebességű átvitelt biztosít, amely megfelel az Ethernet nyújtotta szolgáltatásnak, és az új fejlesztésekkel egyre növekszik a sebessége.

A WLAN előnyeit mind a felhasználók, mind a vállalkozások gyorsan felismerték. A Gartner Group szerint 2005-ben a legnagyobb 1000 vállalat fele nagymértékben kibővített vezeték nélküli hálózatot fog használni, és 2010-re közülük a legtöbb üzleti és hálózati céljai elérésében leginkább a vezeték nélküli technológiára fog támaszkodni.

8.1.3. A VEZETÉK NÉLKÜLI EGYENLŐ A RÁDIÓHULLÁMOKKAL

A vezeték nélküli hálózatokra leselkedő veszélyekről értekezve az első megértendő technikai kérdés az, hogy a 802.11 hálózatok a végpontok között az adatok minden irányú átvitelére rádióhullámokat használnak, akárcsak a vezeték nélküli telefonok vagy a rádiókészülékek. Közöttük a különbség a frekvenciában van, amelyen a jeleket továbbítjuk.

A rádióhullámok nagy távolságot is áthidalhatnak, ez azonban a használt frekvenciától függ. Némely frekvencia 300–400 láb áthidalására képes rendkívül kicsiny adóteljesítmény mellett is. A régebbi vezeték nélküli telefonok az Egyesült Államokban a 900 MHz-es sávot használják hordozófrekvenciának, amely sokkal nagyobb távolság átvitelére képes, mint azt a legtöbben gondolnák. Még egy otthoni báziskészülékkel is előfordulhat, hogy egy-két háztömbnyi távolságból is tartja a kapcsolatot a kézibeszélővel, ami 100–150 méternyi távolságot jelent.

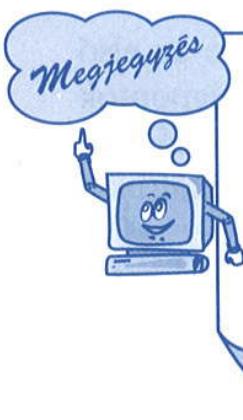
8.

Ha egy otthoni telefon is képes lehet 400–500 láb átívelésére, akkor a vezeték nélküli hálózat is megteheti ezt. Ha van egy vezeték nélküli hozzáférési pontunk (*WAP – Wireless Access Point*) otthon vagy az irodában, nagy biztonsággal lefogadhatjuk, hogy az utcán sétáló emberek is a hatósugarán belül vannak. Ha egy átlagos WAP van a nappalinkban, és társasházban lakunk, akkor tudtunk nélkül nyújthatunk internetszolgáltatást másoknak is.

8.2. VEZETÉK NÉLKÜLI HÁLÓZAT

A vezeték nélküli hálózat kifejezés arra a rádiótechnológiára utal, amely két vagy több számítógép számára lehetővé teszi a szabványos hálózati protokollok (például IP) segítségével történő kommunikációt anélkül, hogy kábelekkel kellene összekötni őket. A vezeték nélküli hálózati hardver egy olyan technológia használatát követeli meg, amely rádiófrekvenciát használ az adatátvitelhez. A legszélesebb körben használt szabvány a 802.11, amelyet az IEEE vezetett be. Ez a szabvány meghatározza a rádiófrekvenciás vezeték nélküli hálózati technológia minden aspektusát.

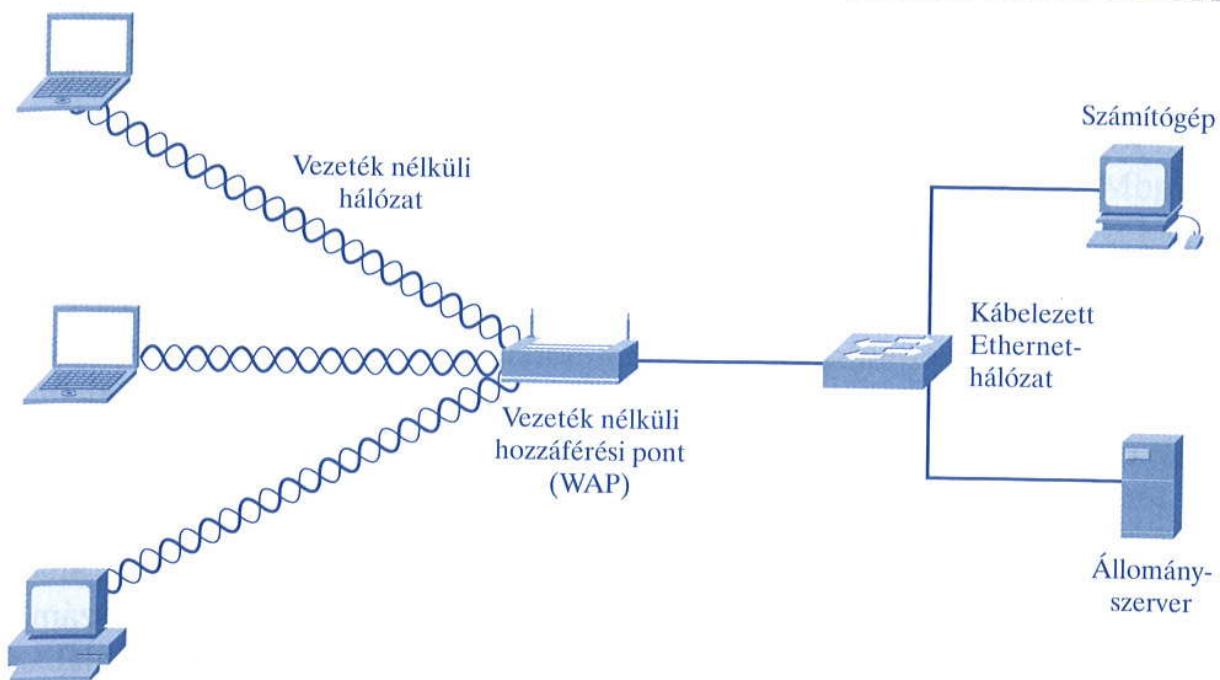
A 802.11b szerint a rádiók az engedély nélkül használható 2,4 GHz-es sávban forgalmazhatnak 11 Mbps átviteli sebességgel, mégpedig 15 meghatározott csatorna valamelyikén (az Egyesült Államokban csak 11 csatorna használható a kormányzati előírások miatt). A vezeték nélküli hálózati kártyák a WLAN-elérés után kutatva automatikusan is végigkereshetik ezeket a csatornákat, így nincs szükség a kliensállomások adott csatornához való előzetes beállítására. Amikor a hálózati kártya megtalálja a megfelelő csatornát, megkezdi a párbeszédet a hozzáférési ponttal. Amennyiben a kliens és a hozzáférési pont biztonsági beállításai meggyeznek, a kapcsolat kiépül és a felhasználó elérheti a hálózatot.



A 802.11g egy új, megnövelt sebességi vezeték nélküli szabvány, amely a felhasználók számára lehetővé teszi akár 54 Mbps átviteli sebesség elérését is – csaknem ötször gyorsabban, mint a 802.11b lehetővé tenné. Mivel ugyanabban a 2,4 GHz-es sávban forgalmaz, így a 802.11g teljesen kompatibilis a 802.11b-vel, és világszerte használják is. Ma már a legtöbb gyártó támogatja ezt az újabb szabványt.

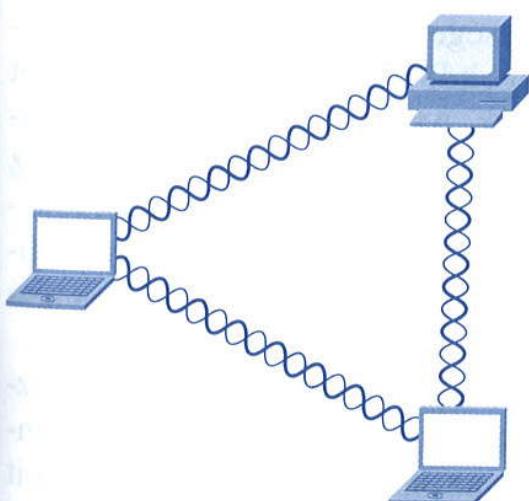
8.2.1. MŰKÖDÉSI MÓDOK

A vezeték nélküli hálózatoknak két típusa létezik, amelyek egymástól a vezeték nélküli eszközök egymás közötti kommunikációjának módszerében térnek el. A WLAN működhet eseti (*ad-hoc*) vagy kiépített (*infrastructure*) módon. Az eseti hálózatokban az egyes vezeték nélküli kliensek közvetlenül egymással, gép–gép kapcsolat keretében oszthatják meg adatokat bármiféle elérési pont használata nélkül. A kiépített WLAN esetén ezzel szemben a kliensek egy központi eszközzel, a hozzáférési ponttal kommunikálnak, amely eszköz általában a kábelezett otthoni vagy vállalati hálózathoz csatlakozik.



8.1. ábra. Kiépített módú vezeték nélküli hálózat

- **Kiépített** – Ehhez a működési módhoz szükség van egy alap szolgáltatás-készletre (*BSS – Basic Service Set*), más néven a hozzáférési pontra (AP). A hozzáférési pont feladata nem csupán az, hogy az egyes vezeték nélküli számítógépek egymással kommunikáljanak, hanem egyúttal biztosítja a kábelezett hálózathoz való hozzáférésüket is (8.1. ábra). A legtöbb vállalati WLAN kiépített módban üzemel, hiszen szükség van a kábelezett hálózat bizonyos erőforrásainak (például nyomtatók, állománszerverek) elérésére is.
- **Eseti** – Ez a gép–gép néven is ismert vezeték nélküli hálózat, amely a 8.2. ábrán látható módon néhány vezeték nélküli csatlakozású számítógépből áll, amelyek egymással akarnak kommunikálni. Ezen működési módot alap szolgáltatás-készlettől független (*IBSS – Independent Basic Service Set*) néven is szokták emlegetni. Az eseti mód úgy jegyezhető meg, hogy nincs szükség hozzáférési pontra. Bárminely számítógép közvetlenül kommunikálhat a többi vezeték nélküli csatlakozású számítógéppel. Egymással tehát megoszthatnak adatokat, vagy akár hozzájuk közvetlenül csatlakozó nyomtatókat is, de nem képesek a kábelezett hálózat szolgáltatásainak igénybe vételére, hacsak a részt vevő számí-



8.2. ábra. Eseti vezeték nélküli hálózat

tógépek egyike egy külön szoftver segítségével nem kezd el hídként működni a kábelezett és az eseti működésű vezeték nélküli hálózatok között.

8.2.2. HATÓSUGÁR

Ma már túlságosan sokféle vezeték nélküli hozzáférési pont létezik ahoz, hogy valamennyit sorra vehessük, így ebben a pontban az általában elérhető lefedettségi szintekre összpontosítunk. A tényleges értékek elérhetnek, így érdemes mindenkor meggyőzően a gyártóval, esetleg terepróbát is tartani a végleges beüzemelés előtt.

Minden egyes hozzáférési pontnak megvan a maga hatósugara, amelyen belül még képes fenntartani a kapcsolatot a hozzá csatlakozó számítógéppel. A tényleges távolság a környezettől is függ; a gyártók általában a szabadtéri és a beltéri hatósugarat egyaránt megadják, így viszonylag jól felmérhetők a tényleges lehetőségek. Nem szabad elfelejteni azt sem, ha a készüléket a hatósugarának határán használjuk, a teljesítménye leromlik, hiszen a jel minősége ekkor már meglehetősen gyenge. A jellemző hatósugarak a következők:

- A szokásos beltéri távolság 50–100 méter, de jóval rövidebb is lehet akkor, ha az épület szerkezete zavarja a rádióhullámok terjedését. Bizonyos esetekben nagyobb távolság is elérhető, de a távolság növelésével a teljesítmény gyorsan romlik.
- A kültéri hatósugarat 300 méter körül szokták megadni, de a ténylegesen elérhető érték nagyban függ a helytől és a környezettől.

A leggyakoribb esetben több hozzáférési pont van összekötve kábeles kapcsolattal, így biztosítva a teljes lefedettséget a hivatalban vagy osztálytermekben. A hozzáférési pont képességeitől függően a hatótávolságot az adóteljesítmény növelésével fokozhatjuk. Az olcsóbb felhasználói hozzáférési pontok esetén ez a lehetőség hiányozhat, a Cisco Aironet 350, 1100 és 1200 termékcsalád esetén azonban erre is van lehetőség. A teljesítmény 5 mW és 100 mW között állítható, így arra is lehet némi ráhatásunk, hogy a vállalat falain kívül még milyen távolságban legyen fogható a jelzés.

Amennyiben egy adott hely túlságosan nagy ahoz, hogy egyetlen hozzáférési ponttal lefedhető legyen, használhatunk több hozzáférési pontot vagy vezeték nélküli átjátszókat egyaránt. Amennyiben ezt az utóbbit akarnánk választani, mindenkor meg kell győződni arról, hogy a hozzáférési pontjaink ténylegesen rendelkeznek-e ezzel a lehetőséggel, mert vannak olyanok is, amelyek erre nem alkalmasak.

8.2.3. ELÉRHETŐ SÁVSZÉLESSÉG

A 802.11b hálózatban a sávszélesség hozzáférési pontonként 11 Mbps lehet. Rögtön el kell oszlatni egy gyakori félreértést: ez a 11 Mbps az elérhető maximális sávszélességet jelenti. Sokan hozzá vannak szokva a kábelles hálózatokhoz, ahol kapcsolókkal biztosítják a hálózat megosztását, és minden egyes munkahely és eszköz rendelkezésére áll a teljes 100 Mbps sávszélesség. A vezeték nélküli hálózat esetén ez a 11 Mbps azonban megoszlik a hozzáférési pontot ténylegesen használó eszközök között. Ha ugyanazon eszközözhöz egyszerre tízen csatlakoznak, akkor a kommunikáció nagyjából személyenként 1 Mbps sávszélességű lehet.

Növelhető-e a sávszélesség egy további hozzáférési pont telepítésével? Nos, az „attól függ” kifejezést a 4. fejezet óta nem használtuk, így most nyugodtan megtehetjük. A 802.11b szabvány semmilyen specifikációt nem tartalmaz a több hozzáférési pont közötti terhelésmegosztással kapcsolatban. A szigorúan a szabvány szerint működő berendezések esetén nincs olyan megoldás, amely kizárná a vezeték nélküli hálózat egyes részeinek nagymértékű terhelődését.

A megoldás az lehet, hogy ugyanazon a területen beüzemelünk egy másik hozzáférési pontot, de eltérő hálózatnevet állítunk be rajta (és a frekvenciasáv másik csatornájára állítjuk). Ezzel gyakorlatilag egynél több vezeték nélküli hálózatot helyezünk üzembe. Azonos terület esetén legfeljebb három párhuzamos hálózat építhető ki. Megismételjük azonban, hogy erre csak akkor van szükség, ha eszközeink működése szigorúan a 802.11 szabványt követi. A valóságban számos gyártó felismerte, hogy ez a hiányosság nagymértékben korlátozná az általuk eladott hozzáférési pontok számát, ezért különböző, saját terhelésmegosztási megoldásokat dolgoztak ki. Ezeknek a megoldásoknak a további tárgyalása azonban meghaladja jelen könyv kereteit, így szükség esetén a kiválasztott gyártónál kell tájékozódni.

8.

8.3. VEZETÉK NÉLKÜLI HÁBORÚS JÁTÉKOK

Mint a könyvben tárgyalt számos más előnyös technológia, a vezeték nélküli hálózat is ki van téve számos veszélynek. Mindazonáltal egyre gyorsabban terjed, és ma már megvan a lehetőség arra, hogy megvédjük és biztonságossá tegyük a vezeték nélküli hálózatunkat. Ebben az alfejezetben nagy vonalakban áttekintjük a veszélyek többségét, és felvázoljuk a hálózat biztonságossá tételenek szükségessége melletti érveket is.

Talán még többen emlékeznek az 1983-ban készült „Háborús játékok” c. mozi-filmre, amelyben egy fiatal kalóz bejut egy katonai számítógépre, és véletlenül elindítja a III. világháborút kirobbantó program visszaszám-

lálását. A filmbeli támadó mindezt egy modem segítségével viszi véghez, kialakítva így egy új szót: CsataHívás (WarDialing).

Lépjünk most előre az időben húsz évet, amikor egy Londonban élő szerző, Ben Hammersley írás közben meg akart inni egy kávét, esetleg bekapott valamit az utca túloldalán lévő kávézóban. Beüzemelt ezért egy vezeték nélküli hozzáférési pontot. Adakozó természetű lévén, a szomszédainak is elárulta, hogy onnantól ingyenes internet elérésük lehet. Sajnálatos módon ezért egyikük sem volt különösebben hálás, viszont Ben egyik barátja, Matt Jones elhelyezett néhány titkos jelet egy weboldalon (www.blackbeltjones.com) azzal a szándékkal, hogy olyan nemzetközi jeleket honosítson meg, amelyek segítségével az emberek láthatják, hogy van a közelben egy hozzáférhető vezeték nélküli összeköttetés. Ben fogott egy darab krétát is, és felrajzolta a megfelelő jelet a kávézó előtt a járdaszegélyre, így ő lett az első CsataRajzoló (WarChalker, lásd 8.3. ábra).

Nem sokkal Matt jeleinek az interneten való megjelenése után elkezdett terjedni ez a divat, így ez a két ember elindított egy olyan internetes jelenséget, amely hamarosan új szavak kialakulását eredményezte: CsataRajzoló, CsataKémkedés, CsataSzemetelő, CsataVezető (WarChalking, WarSpying, WarSpamming, WarDriving) – végső soron mindegyik a vezeték nélküli hozzáférés fejlődésének részévé vált. Ezek olyan egyszerű fogalmak, amelyekkel a támadók leírják a saját tevékenységüket. A továbbiakban röviden áttekintjük ezeket a fenyegetéseket.

CsataRajzolunk!	
KULCSSZÓ	JELZÉSE
NYITOTT CSOMÓ-PONT	ssid  Sávszélesség
ZÁRT CSOMÓ-PONT	ssid 
WEP-CSOMÓ-PONT	ssid  Hozzáférési csatalkozás Sávszélesség

blackbeltjones.com/warchalking

8.3. ábra. CsataRajzoló jelek

CsataRajzolás

Ha valaha is látott már olyan kalózos mozifilmet, amelyben egy kincses térképen a nagy piros X jelölte azt a helyet, ahol a rabolt kincsek voltak elásva, akkor már van némi elképzelése arról, hogy a szimbólumok mi-lyen szerepet játszottak az emberiség kincs utáni vágyakozásában. Amint ez a nagy kereszт jelölte az arannyal, ezüsttel, ékszerrel teli kincsesláda rejtekhelyét, úgy más hasonló jelek a különböző veszélyeket jelölhetik. A nagy társadalmi visszaesés alatt a hobók ilyen jelekkel jelölték, hogy melyik házban lakik rendőr, vagy mely házakat találták vonzónak. A kettőskereszttel jelölték például más hobók számára, hogy a környéken nemrég bűnt követtek el, és így jobb azt elkerülni; egy hanyagul felszínen álló szög pedig azt jelezte, hogy már jelenleg is túl sok hobó tevékenykedik az adott körzetben, így a területen nem sok jót lehet már találni.

Ezek a „hobó hieroglifák” inspirálták Bent és Mattot arra, hogy megalapításuk a CsataRajzolás (WarDrawing) néven elhíresült szokást. Ezek-

kel a jelekkel azt szándékozták más vezeték nélküli harcosok tudtára adni, hogy a közelben van egy hozzáférhető vezeték nélküli vállalati vagy magánhálózat. A művelői által kidolgozott jelrendszer azt is tudtára adja a hozzáértőnek, hogy a hozzáférési pont „nyitott” vagy „zárt” (előbbi esetben a két félkör egymásnak háttal áll, utóbbi esetben pedig kört alkot), illetve hogy milyen védelemmel van ellátva az adott elérési pont.

A CsataRajzolás eredeti formája csupán rövid életű kultusznak bizonyult, amely mindenkit lenyűgözött. A gyakorlatban azonban hamarosan jelentősen megváltozott, alkalmazkodva a művelői által valójában elérni kívánt célohoz. Igen kevesen mászkálnak fel-alá a városban, krétával rajzolatva a házakat; sokan vannak azonban olyanok, akik GPS-koordinákkal ellátott térképeken mutatják meg, hogy a vezeték nélküli szolgáltatások pontosan hol érhetők el. Az internetet keresve ráakadhatunk jónéhány ilyen, használatra kész térképre (www.netstumbler.com/nation.php). A letölthető térképek egyik további előnye a krétajelekkel szemben például az is, hogy az eső nem mossza le őket.

Biztonsági szempontból rendkívül valószínűtlen persze, hogy valaha is ténylegesen látni fogjuk a saját házunk oldalán a CsataRajzot, az viszont könnyen előfordulhat, hogy a nem megfelelően védett vezeték nélküli hálózat esetén koordinátái felbukkannak valakinek a térképen, ahol azután bárki elérheti. Lehet, hogy most azon tüntődik, a támadók miként derítik fel a nem kellően védett elérési pontokat. Nos, látott-e már a kedves olvasó valakit laptopjal és GPS-egységgel sétálni? Valószínűleg nem, ez a fajta tevékenység mégis viszonylag gyakori, művelői azonban szeretik hálózásban rejtve tárolni a szükséges felszerelésüket. Ha ehhez még hozzávesszük az akkumulátorok biztosította korlátozott működési időtartamot, könnyen kijöhét a számításból, hogy az ilyen tevékenység eléggé fárasztó. Ez viszont elvezet minket a következő, a vezeték nélküli világot fenyegető veszélyhez, a CsataVezetéshez – ilyenkor az autó nem csupán helyváltoztatásra használható, de energiaforrásként is üzemel.

8

Megjegyzés



A CsataRajzolás egy válfaja a „WapChalking”, amely a „vezeték nélküli elérési helyet megosztó közösség” (Wireless Access Point Sharing Community) nevű csoportosulás tevékenysége. E csoport tagjai szigorúan tartják magukat a szabályhoz, hogy engedély nélkül nem használnak elérési pontokat. A szimbólumokat felhívásként használják, amellyel más vezeték nélküli tagokat invitálnak meg a közösségiükbe. A „nyitott csomópont” szimbólum esetükben azt jelenti, hogy egy gyári beállítású elérési pont van a közelben.

CsataVezetés

A **CsataVezetés** (WarDriving) a hozzáférhető vezeték nélküli hálózatok megtalálását rendkívül egyszerűvé teszi, ráadásul a keresési területet is nagymértékben megnöveli. Maga a cselekvés egyszerű: be kell ülni egy autóba, és fel-alá kell járkálni vele az utcákon, keresve a hálózatokat. Vonzereje az is, hogy így könnyen használható az autó energiaforrásáról üzemelő laptophoz kötött GPS-rendszer. Ez a felderítést rendkívül pontossá teszi. A vezeték nélküli hálózatot keresők számára rendkívül gyümölcsöző ez a tevékenység, hiszen az autóval nagyon nagy területeket is hamar bejárhat.

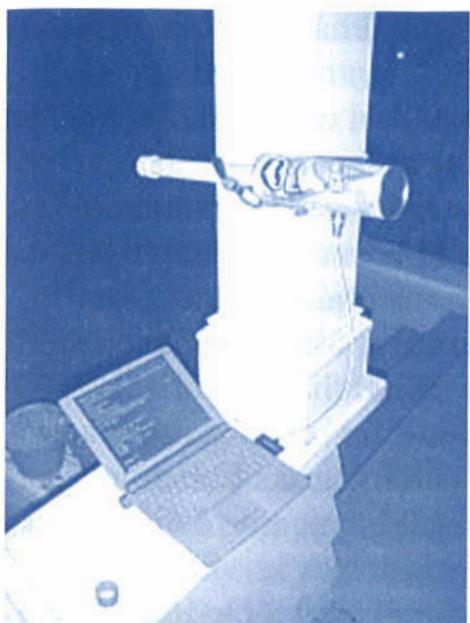


Mielőtt túl mélyen belemérülnénk ebbe a téma körbe, fontos megjegyezni, hogy csatavezetéssel keresni egy gyanúltan fél vezeték nélküli elérési pontjait illegális cselekedet is lehet, az adott ország törvényeitől függően. Akár a hálózatok felderítési távolságának növelésére szolgáló antenna felszerelése is illegális lehet. A tevékenységgel kapcsolatos jogi szabályozást érdemes a tevékenység megkezdése előtt megvizsgálni.

Meglehetősen zavaró, hogy bárki ennyire könnyen megtalálhatja a vezeték nélküli hálózatokat. A gyártók alapértelmezésben minden bekapcsolnak, függetlenül a hálózatbiztonsági megfontolásoktól; éppen ez teszi könnyűvé a csatavezetők dolgát. Alapértelmezés szerint a hozzáférési pontok például minden századmásodpercben sugároznak egy szignált, amelyben közlik az egység azonosítóját (SSID).

A vezeték nélküli PCI hálózati kártyák antennája nem elég érzékeny ahhoz, hogy az elérési pontok alacsony vagy közepes erősségű szignáljaira ráálljanak, így számos csatavezető USB-porthoz csatlakozó vezeték nélküli hálózati eszközt használ, kiegészítve azt egy házilag fabrikált yagi antennával (lásd 8.4. ábra). Az ilyen antennák méretezésével és összeszerelésével kapcsolatos tudnivalók számos honlapon megtalálhatók (például <http://www.wlan-ok.hu>), de készen megvásárolva is csupán fillérekbe kerülnek. Az ilyen antennák a letapogatni kívánt frekvenciatartománytól függően jobb vagy rosszabb eredményt adnak, de mindenkorban növekklik a hatósugarat. A vezeték nélküli hálózatot egy harminckét karakteres névjegy, az úgynevezett szolgáltatáskészlet-azonosító (*SSID – Service Set Identifier*) azonosítja. A csatavezető a legkönnyebben azokat a hálózatokat találja meg, amelyek rendszeresen sugározzák az azonosítójukat. Semmilyen bonyolult felszerelésre nincs szükség, mivel egy Windows XP rendszert futtató laptop is elegendő. Ez az operációs rendszer ugyanis tá-

mogatja a vezeték nélküli hálózatokat, talán túlságosan is, mivel könnyen felismeri a különböző SSID-ket, és automatikusan megpróbál csatlakozni hozzájuk. Egy ennyire készséges operációs rendszer esetén kinek lenne szüksége bármilyen speciális eszközre?



8.4. ábra. Sósmogyorós dobozból készített yagi antenna

Alapértelmezés szerint a hálózatazonosító megjelenik a hozzáférési pontok által század-másodpercenként sugárzott szignálban. Az SSID különbözteti meg az egyes vezeték nélküli hálózatokat (*WLAN – wireless LAN*) egymástól, így az adott WLAN-t alkotó hozzáférési pontoknak ugyanazt az azonosítót kell sugározniuk. Egy eszköz csak akkor csatlakozhat a vezeték nélküli hálózathoz, ha meg tudja adni ezt az egyedi azonosítót. Az SSID azonban a sugárzott csomag fej-részéből nyílt szövegként kiolvasható, így semmilyen biztonsági szerepe nincs, jóllehet a hálózat eléréséhez szükséges jelszóként funkcionál. Éppen ezért nyomatékosan javasolt a hozzáférési pontokban letiltani az SSID automatikus szétsugárzását.

Az SSID megjelenése a vezeték nélküli hálózatban azt okozza, hogy az ilyen hálózatokat kereső személyeknek jó antennákkal kell rendelkezniük, amely lehetővé teszi számukra a gyengébb rádiójelzések fogását is. Ha 802.11b (2,4 GHz) hálózatot keresünk, akkor valószínűleg egy helikális antennára van szükség (ez egy függőlegesen szerelt, cső alakú antenna, ahol a központi mag köré van feltekerve némi vezeték). Az ilyen antennát elég nehéz ugyan házilag jó minőségben legyártani, azonban igen alacsony áron beszerezhetők (két-háromezer forintért már kaphatók). Az irányantennák, amilyen a yagi is, még otthon is könnyen és olcsón előállíthatók, gyakorlatilag háztartási szemét (sósmogyorós doboz, kávédoboz stb.) felhasználásával.

Ezeket az antennákat el kell helyezni az autó tetején vagy a csomagtartó fedelén, hozzá kell kapcsolni a vezeték nélküli hálózati eszközhöz, és körbe kell autózni a várost, figyelve a vezeték nélküli szignálokat. Ne feledjük azonban, hogy az internet-hozzáférés ellopása vagy akár az erre alkalmas hálózatok felderítése illegális cselekmény, amely kékbe öltözött, humorérzékkel nem rendelkező emberek látogatását eredményezheti a lakásunkban. A CsataVezetést egy Peter Shipley nevű ember „találta ki”, aki a csatarajzolást akarta magasabb szinten úzni:

„Nemrég kitaláltam a csatavezetést. Jóllehet nem én vagyok az első, aki elindul hozzáférhető vezeték nélküli hálózatokat keresni (már jónéhányan rótták az utcákat előttem is laptoppal, papírral és ceruzával megjelölve az ígéretes helyeket), azonban én vagyok az első, aki az egészet

automatizálta egy GPS és az erre felhasználható szoftver felhasználásával. Amikor elkezdtem ezt a tevékenységet, a vezeték nélküli hálózatok alig 15%-a használta a WEP-titkosítást, az eredményeim megjelentetése után azonban ez az érték 33%-ra nőtt. Jó tudni, hogy az emberek veszik az üzenetet. Az ezen tevékenység közben rajzolt néhány térképem letölthető a <http://www.dis.org/wl/maps> címről.”

A háttérétől függően (s hogy milyen indíttatásból olvassa e könyvet) az olvasó most esetleg eltűnődik azon, hogy a csatavezetés vajon bűncselekmény-e. Akik úzik, azok szerint persze nem az, a vezeték nélküli hálózatok tulajdonosainak természetesen más lehet a véleménye. Az alábbi valószínűleg az Egyesült Államok egyik FBI-nyomozójától ered:

„A vezeték nélküli hálózat jelenlétének azonosítása önmagában valószínűleg nem bűncselekmény, azonban azzá válhat, ha szolgáltatások jogosulatlan megszerzése, a rajta zajló kommunikáció lehallgatása, a számítástechnikai eszközökkel való visszaélés miatt végzik. Ebben az esetben ugyanis a különböző szövetségi törvényeket megsértő bűncselekménnyé is válhat.”²

Minden esetre érdemes megfontolni, ha vezeték nélküli hálózatot telepítünk, nagyon valószínű, hogy valaki megkíséri azt megtalálni. A biztonságunk tehát attól függ, hogy az ezt megkísérlő személy mennyire van tisztában a saját felelősségevel, és mennyire tisztei az adott helyen érvényes törvényi szabályozást. Röviden: rengeteg vesződséggel megvásároltuk az eszközöket, megszereztük a szükséges tudást, összeraktuk a berendezéseket és minden beállítottunk, a szükséges biztonsági intézkedéseket azonban nem tettük meg, a törvény őrei pedig semmi kivetnivalót nem látnak a csatavezetésben. Tényleg minden, a törvényt kevésbé tisztelő lehetséges támadó által sebezhetőnek kívánjuk meghagyni a hálózatunkat? Ha most igennel válaszolna, akkor javasolt újra elolvasnai az 1. fejezetet.

A fenti, FBI-nyomozónak tulajdonított idézet nagyjából tükrözi a rendvédelmi szervek csatavezetéssel kapcsolatos állásfoglalását. Nyugodtan lehet akár versenyt is rendezni, hogy ki képes megtalálni a legtöbb vezeték nélküli hálózatot. A vezeték nélküli hálózati iparban érintett személyek nyilván nemileg egyoldalú véleménnyel rendelkeznek ebben a kérdésben, a nyilvánvalóan általuk fenntartott alábbi webhelyeket azonban érdemes tanulmányozni: <http://www.worldwidewardrive.org>, <http://www.wardriving.com>.

Találhatók különböző, csatarajzokkal kiegészített térképek, amelyek megadják a GPS-koordinátákat, és számos esetben világszerte megadnak

2 Magyarországon is nagyjából ugyanez a jogi megítélés: ha a tulajdonos szándéka és akarata ellenére lép be valaki a hálózatába, akkor ez büntetendő cselekmény akkor is, ha a hálózat semmilyen védelemmel sem volt ellátva. (A lektor meg.)

teljesen védtelen hálózatokat. Vannak már olyan személyek is, akik a csatavezetést akarják még magasabb szinten űzni. Ők a CsataPilóták.

CsataPilóták

Mindössze két ismert esetről sikerült tudomást szeretni, a kérdéskör azonban annyira érdekes, hogy érdemes megemlíteni. A CsataPilóták (WarFlying) a csatavezetőkhöz hasonlóan a vezeték nélküli hálózatokat keresik, azonban autó helyett repülővel teszik mindezet. Egyelőre kevés embernek van lehetősége kis repülőgépekhez jutni, és közülük még kevesebben vannak azok, akik rendelkeznek a tudással, és képesek a kéréshöz szükséges eszközökkel ellátni a gépeket, ezért jelentősége nyilván sokkal kisebb, mint a csatavezetésé. A vezeték nélküli hálózatok korlátozott elérési távolsága miatt a repülővel 1500 méter alatt kell repülni. Elsőként Ausztráliában, Perth városában jegyeztek fel ilyen esetet.

A csatapilótáknak számos problémával kell megküzdeniük, hiszen ma még nem képesek háromszöggeléssel meghatározni az elérési pont helyét, amely az észlelési helytől akár kilométerekre is lehet. Mindazonáltal a jelenség érdekes, és javasolt elolvasni az alábbi cikkeket is, amelyek bemutatják, hogy a Szilícium-völgyet hogyan „csatarepülték meg”. A kifejezés nyelvtani helyességéről nem vagyok ugyan meggyőződve, de a cikket mindenki által érdemes elolvasni: <http://www.arsTechnica.com/wanker-desk/3q02/warflying-1.html>.

CsataSzemetelés

Manapság mindenki kap szemétleveleket; az internet ezen pestise mindenkinél a postaládáját megfertőzi. Hiszek a szólásszabadságban, ami azonban nem jelentheti azt, hogy mindenkit kötelező meghallgatni. Szerencsére a politikusok és a törvényalkotók világszerte kezdik felismerni az ezzel kapcsolatos közhangulatot, és egyre jobb törvényeket gyártanak a szemétlevelek feladói ellen. Ezek a törvények vagy hatékonyak, vagy nem – ezt csak idővel lehet majd megmondani. Mindenesetre egyre nehezebbé válik az ezekkel a törvényekkel már rendelkező országokban lakó feladók számára a szemét küldése. Vannak olyan szervezetek is, amelyek tárolják a szemétárasztó gépek vagy hálózatok IP-címét, így az innen eredő levelek kitilthatók. Mit tehetnek tehát a szemetelők? Sokan közülük olyan országból adják fel a leveleiket, amelyek még nem alkottak ezzel kapcsolatos törvényeket. Ez persze némi logisztikai problémát, esetleg további költségeket jelent a szemetelők számára. A szemetelő számára tehát egyre vonzóbbá válik az a lehetőség, hogy felbéréljen valakit, aki keres neki egy hozzáférhető vezeték nélküli hálózatot, majd csatlakozzék ehhez, és onnan küldözesse a szemétleveleit.

Talán még rémlík a 3. fejezetben említett felelősségi probléma? Egyszerűnek tűnhet találni egy hozzáférhető vezeték nélküli hálózatot, és csatla-

kozni hozzá a szemetelés érdekében. A támadó leülhet az utca túloldalán lévő kávézóban anélkül, hogy a hálózat tulajdonosa tudomást szerezne róla. Ezáltal viszont a szemét kijut néhány ezer emberhez, akik a szemét érkezéséről feljegyzést készítenek. Legyen ez a szemét mondjuk pornográf jellegű. Lehetne persze még ennél is rosszabb (ne feledjük, most erkölcs nélküli vagy kifacsart erkölcsű emberekről beszélünk, akiknek furcsa céljaik és szükségleteik lehetnek). A szemét forrásának keresése során gyorsan kibukik a vezeték nélküli hálózathoz tartozó hálózat IP-címe, amely nyilván feketelistára kerül, amit az internetszolgáltató is megkap – és ne feledjük el az új, szeméttel elleni törvényeket sem. Az eredmény minden esetre az, hogy a hálózatot üzemeltető vállalattól származó kimenő forgalom feketelistára kerül. Mármost meglehetősen bosszantó, ha a vállalat vásárlói olyan visszapattanó értesítésekkel kapnak, hogy a vállalat szemétleveleket küld, ezért a szolgáltatója letiltotta az internet-hozzáférést, ráadásul még a rendőrség is bekopogtat a vállalat ajtaján! Ha az internetszolgáltató ráadásul a forgalom arányában állítja ki a szolgáltatás számláját, akkor ebben a hónapban jó nagy összegre lehet még számítani.

A **CsataSzemetelés** (WarSpamming) mögötti igazság minden képpen az, hogy az adott vállalat ténylegesen szeméttel árasztott el másokat. Ez ugyan egy támadó számlájára írható, de a vállalat is felelős, hiszen nem tette kellően biztonságossá a vezeték nélküli hálózatát. Mit gondol, ki lesz az, akit végső soron felelőssé tesznek mindezért, aki kereshet majd új állandót? A szemétlevezéssel kapcsolatos törvények szigorodásával és a körülmenyek nehezedésével párhuzamosan számíthatunk a csataszemelés egyre nagyobb méretű elterjedésére. Akik megkerdőjelezhető dolgokat akarnak művelni, mindig meg fogják találni rá a módot; egyesek a körülmenyek nehezedésével felhagynak ugyan vele, mások azonban nem.

CsataKémkedés

A csataszemelésnél is kellemetlenebb a **CsataKémkedés** (WarSpying), amely a vezeték nélküli hálózatainkra leselkedő viszonylag új veszélyek egyike. A csatakémkedés legnépszerűbb formája a vezeték nélküli (például X10) kamerák használata. Ilyen kamerák ma már nagy számban, különböző átviteli technológiát használva kaphatók a piacon, tárgyalásuk azonban messze meghaladja e könyv kereteit.

A csatakémkedés elsőként a 2600 magazinban jelent meg (<http://www.2600.com>), amelyben gyakran érdekes olvasmányok találhatók. A cikkben felvázoltak egy olyan eszközt, amely a vezeték nélküli felügyeleti rendszerek továbbította videofolyam megszolgáltatását teszi lehetővé. Az óta sokan felfedezték és rögzítették maguknak ezt a cikket, s ma már számos jelentés szól olyan emberekről, akik a vezeték nélküli rendszereken továbbított képeket csapolják meg. A csatakémkedés ezen formáját lásd például a <http://rhizome.org/RSG/RSG-X10-1> weboldalon.

A téma további részletes tárgyalásától ezúttal eltekintünk. A kulcsszó mindenkorban a fenyelőt ismerete legyen, és annak biztos tudása, miként lehetük a saját rendszerünket védetté ezekkel a veszélyekkel szemben.

Számos olyan hely van ma már, ahonnan minden szükséges felszerelés megvásárolható ahoz, hogy valaki megkezdje a fenti csatatevékenységek bármelyikét – térképek, eszközök, szoftverek minden könnyen beszerezhetők. Egyszerű internetkeresés után csak hármat mutatnánk be: <http://www.kenneke.com>, <http://www.wi-fi-hotspotlist.com>, <http://www.wi-fi-planet.com>.

Ebben a fejezetben azt igyekeztünk bemutatni, miként találhatók meg a vezeték nélküli hálózatok, illetve némi kisebb mértékben, hogy milyen veszélyek leselkednek rájuk. Ezekben kívül persze még számos más fenyelővel is számolni kell. Ha pedig egy támadó egyszer sikeresen csatlakozott a vezeték nélküli hálózatunkhoz, számos más problémával is számolnunk kell majd. A következőkben igyekszünk kicsit mélyebben foglalkozni ezekkel a kérdésekkel.

8.4. A DRÓTNÉLKÜLISÉG VESZÉLYEI

A vezeték nélküli rendszerekre leselkedő veszélyek sokfélék lehetnek, kezdve az elérési pontunk (WAP) jogosulatlan elérésétől egészen a rádióhullámokkal továbbított csomagok lehallgatásáig és visszafejtéséig. Számos, a vezeték nélküli technikát alkalmazó felhasználó egyszerűen nincs tisztában azzal, hogy milyen típusú veszélyekkel kell szembenéznie pusztán amiatt, hogy egy vezeték nélküli hozzáférési pontot csatlakoztatnak a hálózatukhoz. Ebben a fejezetben az ezzel kapcsolatos leggyakoribb veszélyeket mutatjuk be.

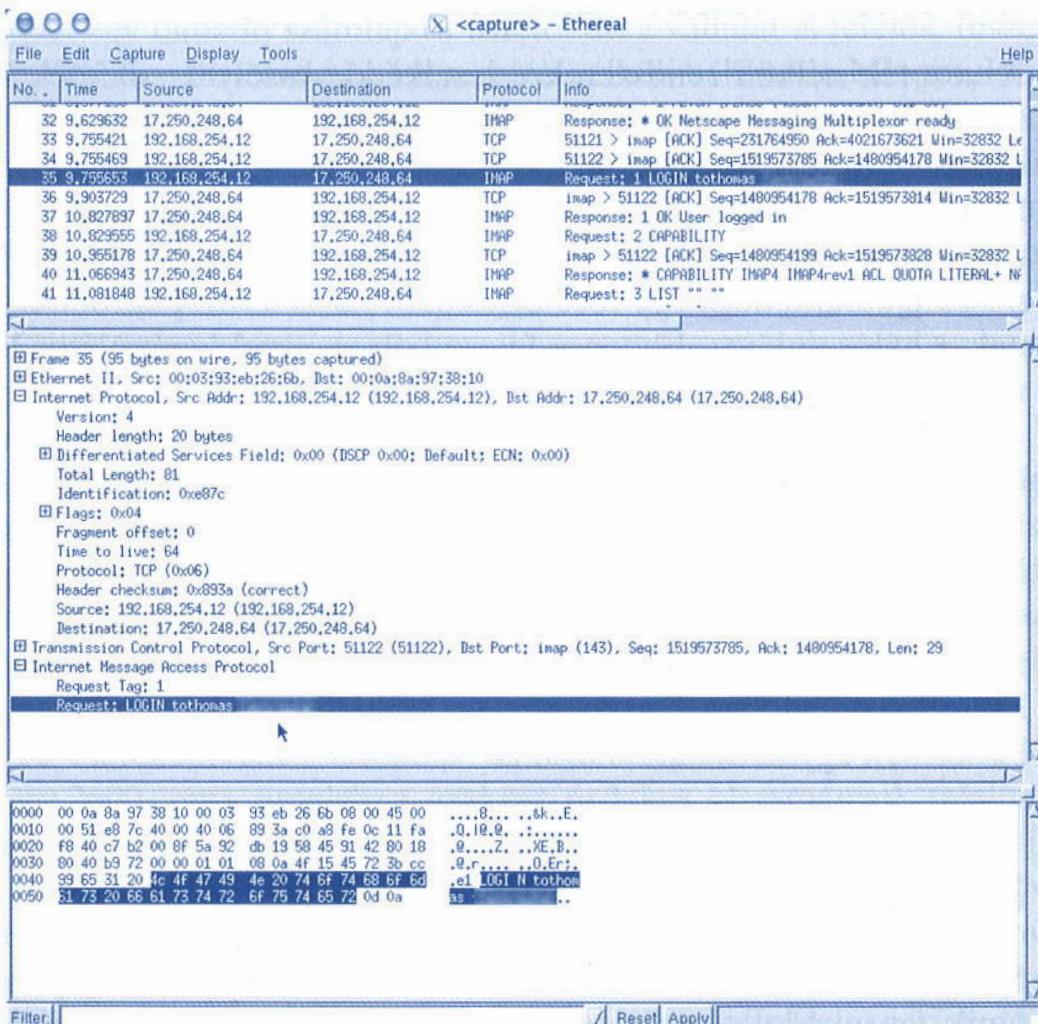
A WLAN-átvitel rádióhullámok segítségével történik, ami a hálózatunkat a bárhonnan érkező behatolók és támadók számára nyitottá teszi. Ezeket a rádióhullámokat az épület fala sem állítja meg, s bárki által foghatók. Az alkalmazottaknak ugyan örömet szerezhet, ha laptopjaikkal a vállalat parkjának egy csendes zugában dolgozhatnak, azonban így a támadók, mondjuk az épület előtti parkolóban állva vagy az utca túloldalán egy vendéglőben ülve is könnyen foghatják a jeleket, akár egy házilag barkácsolt egyszerű antennával is.

8.4.1. LEHALLGATÁS

Mivel a vezeték nélküli kommunikáció a rádióhullámok segítségével történik, így a kódolatlan üzeneteket a rádióhullámok felfogására képes berendezés segítségével bárki lehallgathatja. A vezetékes hálózattal ellen-

tétben a vezeték nélküli elérhetősége nem korlátozódik a vállalat tényleges területére, vagy egy adott hozzáférési helyre – kivételt csak azok a bosszantó helyek jelentenek, ahol nincs meg a kellő lefedettség, ezek azonban szinte kivétel nélkül olyan helyen vannak, ahol az alkalmazottak jogosan szeretnék, ha lenne. A vezeték nélküli LAN hatótávolsága meglehetősen távol is lehet a hivatal vagy az épület határától, így a jogosulatlan felhasználók számára a nyilvánosság számára megnyitott helyről is elérhetővé válnak. A védtelen vezeték nélküli hálózatba betörni szándékozó támadónak minden össze a cél közelében kell elhelyezkednie, és a támadás sikéréhez nincs szüksége különleges képességekre vagy eszközökre sem. Valahányszor ki kell értékelnem egy vezeték nélküli hálózatot egy bérelhető irodákat tartalmazó épületben, szinte minden az alábbi két eset egyike következik be:

- van olyan szomszédos vállalkozás, amelynek védtelen a vezeték nélküli hálózata;
- valamelyik szomszédos vállalkozás felhasználója csatlakozott a kiértékeltek hálózathoz.



8.5. ábra. Vezeték nélküli csomag elfogása

Ha egy (vezeték nélküli vagy vezetékes) Ethernet-kapcsolaton keresztülhaladó információt akarunk megvizsgálni, a legjobban egy **csomagszaglászó** (*packet sniffer*) programmal tehetjük. Ezek a csomagok egy adott (vagy több) Ethernet-kapcsolaton keresztülhaladó csomagokat képesek elfogni. Elfogják a csomagot, analizálják, majd felfedik a benne található adatot. A legnagyobb fenyegetést ilyenkor egy feljegosított felhasználó azonosítónak ellopása jelenti. A 8.5. ábrán az *Ethereal* nevű, ingyenesen használható csomagszaglászó képernyőképe látható, amelyet egy Apple Powerbook G4 laptopon futtattunk egy levelezőalkalmazás által küldött csomag felfedésére. (A neveket és a jelszavakat persze már megváltoztattuk.)

Ezzel azt igyekszünk bemutatni, hogy a csomagszaglászókat miként lehet ismert viselkedésű felhasználók ellen használni. Ebben az esetben, amikor a felhasználók bekapsolják a gépüket, az általuk végzett egyik legelső dolog a levelek ellenőrzése. A legtöbb levelezőszerver nem követeli meg bármiféle titkosítás használatát sem, s mivel a vezeték nélküli hálózat sem titkosítja a forgalmat, az adatokat nyílt szövegként továbbítja. A csomagszaglászóval felfegyverkezett támadó tehát később bármikor képes lesz belépni a felhasználó nevében a levelezőszerverre.

Ha már vizsgáltatott korábban is ilyen elfogható csomagokat, és tudja az így felfedhető információk mennyiségét, akkor nyilván rémülettel tölti el a felfedezés, hogy a vezeték nélküli hálózatokhoz számos szaglászó létezik, melyek közül több is ingyenes. Ha most lát először csomagszaglászókat, akkor valóságos sokként érheti az elfogott csomagok adattartalmának mennyisége és minősége. Képzelje el azt a helyzetet, amikor egy tartomány adminisztrátoraként bejelentkezik a hálózatba, és lekéri az internetes bankszámláját vagy más hasonló olyan információt, amelynek bárki illetéktelen által való ellopása valóságos katasztrófával ér fel az Ön számára.

8.

8.4.2. SZOLGÁLTATÁSMEGTAGADÁSI TÁMADÁSOK

A vezeték nélküli hálózatba behatolni képtelen támadók továbbra is fenyegetést jelentenek azáltal, hogy a vezeték nélküli hálózatot valamilyen statikus zajjal árasztják el, miáltal a valódi csomagok eltorzulnak, és CRC-hibákkal érnek célba. Az ilyen szolgáltatásmegtagadási (*DoS – Denial of Service*) támadás hatékonyan megbéníthatja, vagy jelentősen lelassíthatja a vezeték nélküli hálózatot, mint ahogy más DoS-támadások a vezetékes hálózattal tehetik ezt. Ez a sérülékenység nyilvánvaló; ahogy a biztonság növelésével a vezetékes hálózaton sem csökken a vírusoknak, egyéb támadásoknak való kitettség, úgy a vezeték nélkülin is hiába növeljük azt, sőt könnyebb zavarhatósága miatt csak rosszabbá válik a helyzet.



Éttermek, szállodák, üzleti központok, apartmankomplexumok és magánszemélyek gyakran nyújtanak vezeték nélküli hozzáférést kevés, vagy éppen semmilyen védelemmel. Ilyenkor hozzá lehet féni más, ugyanezen vezeték nélküli hálózathoz csatlakozó számítógépekhez, megteremtve ezzel a lehetőséget a jogosulatlan információszerzsének, erőforrások megszerzsének, és az ilyen rendszerekbe való hátsó ajtók beépítésének. Amikor a felhasználók a vállalati laptopokat viszik haza és használják az otthoni vezeték nélküli hálózatukon, a vállalati hálózat sérülékenysége is növekszik. Számos, a vezeték nélküli hálózatot kiértékelő hálózatvizsgálaton vettet részt, ahol kiderült, hogy sok vezető beosztású munkatárs beállítatott az IT-csoporttal otthoni használatra szánt olyan vezeték nélküli eszközöket, amelyek minden tekintetben meggyeztek a vállalati beállításokkal (SSID stb. azonos). Ezzel egyszerűbben tudtak otthon is dolgozni, a hálózat sérülékenysége azonban megnövekedett, mivel egy támadó az otthoni hálózatba betörve a vezető munkatárs gépét feltörheti, azon kémprogramokat húlyezhet el. Amikor ez a munkatárs bemegy dolgozni, viszi magával a támadó programjait is, amelyek már bejutást biztosítanak a támadó számára a vállalati hálózatba is. A józan paraszti ész tehát azt diktálja, és ezt a hálózat biztonságáért végső soron felelős vezetőségnek is tudnia kell, hogy az otthoni és a vállalati biztonságot ne keverjük össze.

Ennél talán gyakoribb, ha más vezeték nélküli eszközök szándékolatlanul okozzák a saját vezeték nélküli adathálózat szolgáltatáskiesését – mondjuk egy új, szintén 2,4 GHz frekvencián működő vezeték nélküli telefon, vagy más, a hozzáférési pont közelében elhelyezett eszközök (például mikrohullámú sütők) rontják le a működésüket. A vezeték nélküli kapcsolat romlása nem minden vezethető vissza tényleges támadásra. Soha ne feledjük, a vezeték nélküli hálózat a rádióhullámokon alapszik, amelyek terjedését számos különböző doleg (falak, időjárás, boszorkányság) befolyásolhatja.

8.4.3. SZÉLHÁMOS/JOGOSULATLAN ELÉRÉSI PONTOK

Elérési pontot bárki könnyen telepíthet, aki rendelkezik hálózati eléréssel, bárhol a vállalat területén. A valóságban a legtöbb vezeték nélküli kapcsolatot éppen az otthonokban találjuk, hogy a lakók a lakás bármely helyiségében elérhessék laptopjukkal a hálózatot. A vezeték nélküli hálózat telepítésének egyszerűsége azonban minden hálózatadminisztrátort aggodalommal töltelhet el.

Mivel az egyszerű WLAN könnyen beüzemelhető egy gyakran néhány ezer forintos elérési pont vezetékes hálózathoz való csatlakoztatásával, mire a saját laptopjuk egy még olcsóbb kártya segítségével alkalmassá vá-

lik a vezeték nélküli működésre, így egyes vállalati felhasználók jogosulatlanul vezeték nélküli hálózatokat helyezhetnek üzembe, ha az IT-csoport csak lassan vezeti be ezt az új technológiát. Az ilyen jogosulatlan elérési pontokat szoktuk **szélhámos WAP** (rogue WAP) néven emlegetni.

Egy nagy technológiai konglomerátum egyik vezetője mondott nemrég valami olyasmit, hogy „a vezeték nélküli fenyegetésekkel szemben legnehezebben azokat a hálózatokat lehet biztonságossá tenni, amelyek egyáltalán nem tartalmaznak vezeték nélküli elérési lehetőséget”. Ezalatt azt értette, hogy ha egy vállalat nem vásárol és telepít vezeték nélküli eszközöket, még nem feltétlenül jelenti azt, hogy ilyenek nem jelennek meg a hálózatában.

A vezeték nélküli technológia mögötti elképzelés az, hogy az embereknek lehetővé tegyük a szabad mozgást anélkül, hogy elveszítenék a kapcsolatukat a hálózattal. Ezen szabadság csábereje azonban annyira vonzó, hogy a vállalatok számos alkalmazottja vásárolja meg saját pénzén a vezeték nélküli eszközöket, és illeszti hozzá azokat a vállalat hálózatához. Ez a jelenség az Egyesült Államokban már komoly méreteket öltött, és itthoni terjedése is egyre valószínűbbé válik.

Megjegyzés



2001-ben a Gartner Group kutató és statisztikai vállalat arról számolt be, hogy „legalább a vállalkozások 20 százalékánál megtalálható a szélhámos elérési pont”, amelyet erre fel nem jogosított alkalmazottaik telepítettek. A kockázatérzékeny vállalatoknak, amelyek a megnövekvő kockázat miatt tudatosan készletetek az új technológia bevezetését, rendszeresen figyeliük kell a saját légterüket, nehogy véletlenül szélhámos WAP-ok nyissanak ajtót a behatolóknak. Persze ha elhalásodik rajtunk az üldözési mánia, akár azt is feltehetjük, hogy a takarítószemélyzet valamelyik tagja este, takarítás közben üzemel be egy ilyen készüléket – amit percek alatt könnyen megtehet.

8.

Ha elképzeljük azt, mennyire nehéz az embereket megakadályozni abban, hogy otthonról különböző szoftvereket hozzanak be és futtassanak a saját munkahelyi gépükön, akkor biztosak lehetünk abban, hogy ennél tízszer nehezebb megakadályozni őket abban, hogy saját maguknak telepítsenek vezeték nélküli eszközöket a vállalati hálózatba.

Persze feltehető a kérdés, „tulajdonképpen mi ezzel a baj?” A válasz természetesen az, hogy az ilyen jogosulatlan telepítésű eszközök megövelik a cég 200 méternyi körzetében tartózkodó bármely támadó sikérének valószínűségét, aki internet-hozzáférést akar, vagy el akarja érni a vállalat állományait, nyomtatói vagy bármely más, a hálózaton elérhető eszközét.

A hálózati rendszergazdák komoly erőfeszítéseket tesznek azért, hogy megvédjék a vállalati hálózatot a támadásoktól és más gonoszterőktől, mire valaki jogosulatlanul egyenesen a szentélyek legbelőbbikébe – a vállalati hálózatba – vezető teljesen védtelen nyílást üt ezen a védelmen.

A megfelelően felkészült vállalatnak különböző biztonsági szabályzatai vannak, amelyek a felhasználók hálózathoz való csatlakozásának különböző módozatait szabályozzák. A szélhámos elérési pontok kijátszák ezeket a szabályokat, és lehetővé teszik, hogy a hálózattal bármiféle szörnyűség megtörténhessen.

Az ezen végső bűnt elkövetni képes alkalmazottakkal szemben akkor járhatunk el, ha a következő információt számukra teljesen világossá tesszük:

- Kizárolag az erre feljogosított számítástechnikai munkatárs csatlakoztatthat a hálózathoz bármiféle eszközt.
- A hálózathoz csatlakozó minden eszköznek, különösen a vezeték nélküli elérési pontoknak bizonyos biztonsági szabályoknak meg kell felelniük.
- Bármely olyan eszköz, amelyet nem a vállalat erre feljogosított munkatársa csatlakoztat a hálózathoz, azonnal elköbozható vagy megsemmisíthető.
- A vállalat hálózatához szélhámos elérési pontokat kizárolag támadók csatlakoztatnak, mégpedig olyan célból, hogy üzleti titkokat lophassanak el és tönkretehessenek adatokat – mivel ez a vállalat üzleti sikereit veszélyezteti, így az ezt a tettet elkövetőkkel szemben azonnal a legsúlyosabb büntetést kell kiszabni.

A szélhámos elérési pontokat mostanában némileg egyszerűbb felfedni, mint a múltban volt, mivel megjelent egy szabadon elérhető szoftver (lásd 8.6.1. NetStumbler című alfejezet). Ugyanez a szoftver, amely korábban a támadók dolgát könnyítette meg, most a hálózatbiztonsági szakemberek kedvelt eszköze lett, amikor a jogosulatlanul beüzemelt elérési pontokat keresik.

A támadók szélhámos WAP telepítési szokásai

Ennek a pontnak eredetileg a „támadók szélhámos WAP hozzáférési pontok telepítési szabályai” volt a címe, de meglehetősen ostobán festett a bűncselekményeket ténylegesen elkövetni szándékozó személyekkel kapcsolatban bármiféle szabályokról beszélni. A támadók mindenkorral kifejlesztették az ajánlott végrehajtás „kézikönyvét”, amelyet a saját közösségekön belül elterjesztettek. Mostanra már minden becsületes hálózati mérnök a csatavezetést a hálózat védelmében meglehetősen gyakran használja is. A következő listán röviden összefoglaljuk azokat a teendőket, amelyekben a támadók írják le az általuk követett elveket:

- Mérjük fel, mit akarunk elérni, mielőtt elhelyezünk egy hozzáférési pontot.
- Tervezzük meg az elérési pont használatát; ez azt jelenti, hogy úgy kell azt elhelyeznünk, hogy ne tűnjünk gyanúsnak akkor, amikor hozzá csatlakozva a laptopunkon „dolgozunk”.
- A lehető legkevésbé látható helyen helyezzük el az elérési pontot, egyúttal maximalizáljuk a hozzá való csatlakozási képességünket.
- Tiltsuk le az SSID sugárzását, így a célpont IT-csoportjának külön vezeték nélküli nyomozóeszközre van szüksége a felderítéséhez.
- Tiltsuk le a hozzáférési pont minden hálózati kezelhetőségi opciónját, mint az SMTP-, HTTP-, Telnet-hozzáférést.
- Ha lehetséges, tiltsuk le az elérési pont MAC-címének ARP-táblákban való megjelenését.

Amennyiben hálózat-ellenőrzési munka során akarjuk a hálózat védeottségét (esetleg az IT-csoport felkészültségét) felmérni, a fenti műveleteket csak a célpont vállalat vezetősége által kiadott írásos engedély birtokában tegyük. Számos vállalat még a vezeték nélküli hálózatához való véletlen csatlakozást is támadásként értékeli, így rajtakapás esetén nyilván bűnösen fogják tartani az elérési pontot telepítő személyt, hacsak nem képes bizonyítani az ártatlanságát.

Szintén fontos észben tartani, hogy bizonyos rádiófrekvenciák elnyomására szolgáló berendezések már jóval a vezeték nélküli hálózati szabvány megjelenése előtt is léteztek. Mivel a vezeték nélküli hálózat is rádióhullámokat használ, így könnyen zavarható.

8.4.4. HIBÁSAN BEÁLLÍTOTT ELÉRÉSI PONTOK

8.

A hibásan beállított elérési pont elkerülhető, ám jelentős lyukat jelent a WLAN biztonsági ernyőjén. Számos elérési pont úgy van beállítva, hogy nyíltan kisugározzák az SSID-t az erre feljogosított felhasználóknak. Számos becsületes hálózati rendszergazda hibásan használta az SSID-t arra, hogy a feljogosított felhasználókat jelszóként azonosítsa vele. Mivel azonban az elérési pont rendszeresen közli az SSID-t a világgal, így ez a komoly beállítási hiba lehetővé teszi a behatoló számára annak egyszerű ellopását, majd megtéveszti az elérési pontot, mintha ő is jogosult lenne a csatlakozáshoz.

Az SSID ennek ellenére jelszónak tekinthető, amelyet gyakran használunk a feljogosított eszközök felismerésére is. Ennek megfelelően a vállalat jelszókezelési szabályzatában foglaltak szerint kell megválasztanunk, és jelszóként is kell kezelnünk. Amennyiben a vállalatnak nincs ilyen sa-

bályzata, akkor térjen vissza a 2. fejezethez, és olvassa el a biztonsági házirendekről és felelősségekről szóló pontot. mindenéppen biztosítsa, hogy a vállalat az SSID alapján ne legyen azonosítható.

8.4.5. HÁLÓZATI VISSZAÉLÉSEK

A jogosult felhasználók fenyegethetik a hálózat biztonságát az olyan, viszsaélésnek minősülő tevékenységekkel is, amelyek a hálózati kapcsolatok sebességét lerontják, felélik a rendelkezésre álló sávszélességet, vagy lerontják a WLAN teljesítményét. Néhány olyan felhasználó, aki MP3-ál-lományokat cserélget, befolyásolhatja a vezeték nélküli hálózathoz csatlakozó valamennyi munkatárs hatékony munkavégzését. Ez végső soron oda vezet, hogy a munkájukat hatékonyan elvégezni nem tudó felhasználók állandóan panaszkodni fognak a hálózat lassúságára, és a kapcsolat gyakori elvesztésére. A gyakorlatban ezeket a problémákat meglehetősen nehéz azonosítani és lecsökkenteni, különösen ha a vállalat azáltal akart pénzt megtakarítani, hogy az olcsóbb, otthoni használatra kifejlesztett elérési pontokat vásárolta meg a vállalati eszközök helyett. Az otthoni használatú elérési pontok nem rendelkeznek azokkal az eszközökkel, amelyekre szükség lenne az ilyen problémák kiküszöbölésére.

Az elégedetlen és a lojális vállalati alkalmazottak csaló szándékú és gondatlan viselkedése szintén biztonsági kockázatot jelent, amely vezethet a jogosulatlanul telepített elérési pontokhoz, a biztonsági szempontból helytelen viselkedéshez és a hálózati visszaélésekhez egyaránt. Fel kell ismernünk azt a tapasztalati tényt, hogy a biztonsági problémák legnagyobb része belülről, a megbízhatónak feltételezett személyektől ered.

8.5. VEZETÉK NÉLKÜLI BIZTONSÁG

Ennyi veszély felsorolása után mindenki eltűnődhet, miért is akarna bárki vezeték nélküli hálózatot használni, ha egyszer ennyire nem biztonságos a működése. Szerencsére ennyire azért nem elveszett még a helyzet, köszönhetően a vezeték nélküli titkosítási protokollnak (*WEP – Wireless Encryption Protocol*). Némelyek vezetékkel egyenértékű protokollnak (*Wired Equivalent Protocol*), mások vezetékkel egyenértékű biztonság-nak (*Wired Equivalent Privacy*) is nevezik. A „vállalati szakértők” körében ugyanis dül némi vita a pontos jelentéséről. Attól függetlenül azonban, hogy melyik jelentését fogadjuk el, a WEP egy olyan titkosítási algoritmus, amelyet a vezeték nélküli felhasználó és az általa használt elérési pont közötti forgalom védelmére használunk.

A 802.11b szabványba a vállalati biztonsági eszközök kimerítő készletét már a kezdetekben sem akarták belefoglalni. Mindazonáltal tartalmaz néhány olyan alapvető biztonsági intézkedést, amelynek segítségével a hálózat biztonságosabbá tehető. Mindegyik biztonsági jellemző esetén megvan arra a lehetőség, hogy a hálózatot még biztonságosabbá vagy még sérülékenyebbe tegyük.

A mélységi, többrétegű védelem elvein dolgozva a következő pontokban mindenekelőtt megismerjük, hogy a vezeték nélküli eszköz miként is csatlakozik az elérési ponthoz, és hogyan lehet ezt az első lehetséges helyet is némi védelemmel ellátni.

8.5.1. SZOLGÁLTATÁSKÉSZLET-AZONOSÍTÓ (SSID)

Alapértelmezés szerint az elérési pont másodpercenként többször is ki-sugározza a hálózatazonosítót (*beacon*). Ez persze könnyebbé teszi a jogosult felhasználók számára a megfelelő hálózat megtalálását, azonban azt is lehetővé teszi, hogy a jogosulatlan felhasználók megtudják a hálózat nevét. Ez a jellemző teszi lehetővé a vezeték nélküli hálózatokat felderítő szoftverek számára a hálózatok megtalálását anélkül, hogy ismernék azok azonosítóját.

Az SSID helyes beállítása a hálózat biztonságának legelső lépése, így ennek megfelelően kezelendő. A szabványból következően az SSID nem ké-

8.1. táblázat. Alapértelmezett SSID

Gyártó	Alapértelmezett SSID
3COM	101, comcomcom
Addtron	WLAN
Cisco	Tsunami, WaveLAN Network
Compaq	Compaq
DLink	WLAN
Intel	101, 195, xlan, intel
Linksys	Linksys, wireless
Lucent/Cabletron	RoamAbout
NetGear	Wireless
SMC	WLAN
Symbol	101
Teletronics	any
Zcomax	any, mello, Test
Zyxel	Wireless
Mások	Wireless

pes védelmet nyújtani azzal kapcsolatban, hogy ki érheti el a hálózatot, de ha úgy állítjuk be, hogy nem lehet könnyen kitalálni, és a névből nem lehet következtetni a hálózat tulajdonosára sem, akkor a beható számára megnehezítjük annak felismerését, hogy pontosan kinek a hálózatát is látják.

Ha a vezeték nélküli hálózat SSID-je a 8.1. táblázatban található alapértelmezett értékek bármelyike, akkor azonnal változtassa meg.

A gyártók által beállított alapértelmezett SSID-k és egyéb hálózati eszközök alapértelmezett jelszavainak listája megtalálható az interneten, a <http://www.cirt.net> webhelyen. Amint látható, ezek az azonosítók az interneten is megtalálhatók, így legelső lépésként a szignálként való rendszeres kisugárzásának megtiltása mindenféle hasznos.

8.5.2. AZ ESZKÖZÖK ÉS AZ AP CSATLAKOZÁSA

Mielőtt a vezeték nélküli kliens és a vezeték nélküli elérési pont között bármiféle kommunikáció megkezdődhetne, a kettőnek előbb meg kell kezdenie a párbeszédet. Ezt a folyamatot nevezzük csatlakozásnak. Amikor a 802.11b szabványt terveztek, az IEEE lehetővé tette a vezeték nélküli hálózatok számára, hogy rögtön az eszköz csatlakozása után, de még a forgalmazás megkezdése előtt megkövetelje az eszköz hitelesítését. Ennek a követelménynek az az oka, hogy így egy újabb biztonsági védelmi vonal helyezhető üzembe. Ez a hitelesítés egyaránt lehet „nyílt kulcsú” (*open key*) vagy megosztott kulcsú (*shared key*).

Célszerű a nyílt kulcsú hitelesítést használni, mivel a közös kulcsú hitelesítés sajnos hibás. Ez az ajánlás egyáltalán nem nyilvánvaló, de azon alapszik, hogy más titkosítást is alkalmazni fogunk.

8.5.3. VEZETÉKESSEL EGYENÉRTÉKŰ TITKOSSÁG (WEP)

Számos tévhit övezi a WEP-technológiát, ezért mindenki az elején tisztázunk egy fontos kérdést. A WEP nem titkosító algoritmus, és soha nem is volt annak szánva. Tervezési elvei között soha nem szerepelt célként az adatok biztonságának megőrzése a szcriptcsávókkal szemben, még kevésbé a titkainkat felfedő intelligensebb támadókkal szemben. A WEP nem védelmi eszköz, csupán annyi érhető el a segítségével, hogy ne legyünk kevésbé védtelenek pusztán azáltal, hogy a forgalmat nem vezetéken továbbítjuk. A félreértés nyilván abból ered, hogy az emberek látják a „titkosítás” szót, és hibás feltételezéseket vonnak le belőle. A WEP-et arra terveztek, hogy a vezeték nélküli átvitel vezetékessel szembeni öröklletes sebezhetőséget kiküszöbölje, és az átvitt adatokat annyira biztonságossá

tegye, amennyire azok a titkosítatlan vezetékes Ethernet-hálózaton lennének. Mindössze ennyi a feladata, s ezzel a tévhítet eloszlattuk, és továbbhaladhatunk. A WEP jellemzően háromféleképpen állítható be:

- nincs titkosítás,
- 64 bites titkosítás,
- 128 bites titkosítás.

A WEP egy előre megbeszélendő, opcionális titkosítási szabvány, amelyet még az előtt be kell állítani, hogy a vezeték nélküli felhasználó csatlakozna az elérési ponthoz. Miután mind az elérési ponton, mind a kliensgépen beállítottuk, a levegőben továbbított üzenetek mindegyike titkosított lesz, így biztosítva a kellően biztonságos, elegendően nehezen feltörhető kapcsolatot (jóllehet a támadók mostanra már kifejlesztettek olyan eszközöket, amelyek egyre könnyebbé teszik a feltörését). A WEP használatának mellékhatása az is, hogy az elérési ponthoz csatlakozni kívánó felhasználóknak a saját gépükön előzetesen engedélyezni kell azt, amihez ismerniük kell az elérési pont és a végfelhasználó közös jelszavát.

A WEP-et (*Wired Equivalent Privacy*) tehát arra terveztek, hogy a vezeték nélküli felhasználóknak a vezetékkessel egyenértékű biztonságot nyújtsanak. Amikor be van kapcsolva, akkor az elérési pont a kliensgépre irányuló minden egyes csomagot elsőként titkosít úgy, hogy veszi a csomag adatait, valamint egy titkos 40 bites számot, és mindenkor átküldi az RC4 névre hallgató titkosító algoritmuson. Az eredményül kapott titkosított csomagot csak ezután sugározza ki a kliensnek. Amikor a kliens megkapja a WEP-titkosítású csomagot, ugyanezt a 40 bites számot adja át a csomaggal együtt az RC4 algoritmusnak, amely visszafejti az információt. Természetesen ugyanez a folyamat játszódik le a visszafelé irányú átvitel során is, amikor a kliens küld adatot a hozzáférési pontnak. A fenti példában 64 bites titkosító kulcsot feltételeztünk, de természetesen ugyanígy használható a 128 bites is. Mivel ismertek a WEP hibái és a vele kapcsolatos tévhitek is, így mindenkor ajánlott a 128 bites kulcsot használni a 64 bites helyett.

A WEP korlátai és gyengeségei

A WEP a vezeték nélküli forgalmat a „titkos” WEP-jelszó és egy véletlenszerűen előállított 24 bites szám (inicializáló vektor, IV) kombinálásával védi, így biztosítva a titkosítási szolgáltatást. Ezt a 24 bitet kell kombinálni a 40 vagy 104 bit hosszú WEP-jelszóval, ami így együtt 64 vagy 128 bites titkosítást ad – avagy mégsem? A WEP jelenlegi hibás implementációjával kapcsolatban érdemes néhány gondot megérteni:

- A WEP első gyengesége a 24 bites inicializáló vektor nyilvánvaló matematikai gyengesége, amely alig 16 777 216 (2^{24}) lehetséges értéket jelent. Ez így elsőre nagynak tűnhet, de ha visszaemlékszünk a 4. fejezetben mondottakra, akkor bizony kitűnik, mennyire nem az. Ezzel a kicsiny számmal az a legnagyobb baj, hogy az értékek és a kulcsok egy idő után ismételni kezdik egymást; a támadók pontosan ezt kihasználva törik fel a WEP-kulcsokat.
- A második gyengeség a lehetséges 16 millió érték mellett még az is, hogy ezek nem mindenike jó. Például az 1-es szám sem túl jó. Ha egy támadó képes használni egy olyan eszközt, amely a gyenge IV-értékeket megtalálja, akkor a WEP könnyen feltörhető.
- A harmadik gyengesége a 64 és 128 bites titkosítás közötti különbségben rejlik. Azt feltételeznénk, hogy az utóbbi kétszer olyan biztonságos. Ez azonban nem igaz, mert minden két szinten ugyanazt a 24 bites IV-t használja, amelytől egyben örökli is a gyengeségét. Ha tehát valaki azt is gondolná, hogy a 128 bites kulcs biztonságosabb, akkor téved, a valóságban semmilyen előnyvel nem jár a hálózat szempontjából az erősebb jelszó választása.

Természetesen számos szabadon elérhető eszköz áll a támadók rendelkezésére, hogy kihasználják ezeket a gyengeségeket, amint azt később be is mutatjuk. Mindenesetre a WEP használata a semminél azért jobb, de a biztonság növelését csak a többrétegű védelem jelentheti, amint a könyvben már többször is hangsúlyoztuk. A „bővíthető hitelesítő protokoll” (*EAP – Extensible Authentication Protocol*) a biztonság következő rétege, amelyet az azonos nevű pontban később ismertetünk.

8.5.4. MAC-CÍMSZŰRÉS

A MAC-címszűrés is az egyik módja annak, ahogy néhányan megpróbálják biztonságosabbá tenni a 802.11b szabvány szerinti hálózatukat. A hálózati kártya MAC-címe egy 12 jegyű hexadecimális szám, amelyet a gyártó állít be, és amely az egész világon egyedi. Mivel minden egyes vezeték nélküli Ethernet-kártyának megvan a maga saját MAC-címe, így az elérési ponthoz való hozzáférést is korlátozhatjuk csak azokra a gépekre, amelyek MAC-címe megfelel egy listán felsoroltak valamelyikének. Az itt nem szereplő MAC-című eszközök hozzáférését pedig az elérési pont visszautasítja.

A MAC-címszűrés sem teljesen biztonságos azonban, és ha egyedül erre bíznánk magunkat, hamis biztonságérzetbe ringatjuk magunkat. Soha ne feledjük a következőket:

- Valakinek karban kell tartania a hálózatban engedélyezett valamennyi eszköz MAC-címét. Ha csupán 10–20 ilyen van, akkor ez nem túl nehéz. Ha azonban több száz MAC-címet kell karbantartani, akkor ez a kötelezettség hamar rémálommá válhat.
- A MAC-címeket meg lehet változtatni, így egy kellően elszánt támadó lehallgathatja a vezeték nélküli kommunikációt az erre szolgáló szaglászó eszközökkel, és kitalálhatja belőlük az engedélyezett MAC-címeket, majd beállíthatja a saját gépén ezek bármelyikét. Ne feledjük, hogy a titkosítás csak a második rétegen történik, így a MAC-címek továbbra is láthatók maradnak a lehallgató számára.

8.5.5. BŐVÍTHETŐ HITELESÍTŐPROTOKOLL

A 802.1X az IEEE által jóváhagyott végpontszintű biztonsági szabvány. A jóváhagyás eredetileg a vezetékes hálózati végpontok biztonságának szabványosítására szolt, azonban alkalmazható a vezeték nélküli hálózatokban is. A bővíthető hitelesítő protokoll (*EAP – Extensible Authentication Protocol*) egy 2-es rétegbeli (MAC-címréteg) biztonsági szabvány, amely a biztonsági folyamat hitelesítési fázisát szabályozza, s amely az eddig tárgyalt biztonsági óvintézkedésekkel együtt használva a vezeték nélküli hálózat harmadik, és egyben utolsó védelmi vonalát alkothatja. A 802.1X esetén ha egy eszköz el akarja érni a hozzáférési pontot, az EAP során a következők játszódnak le:

1. Az elérési pont a klienst felszólítja a hitelesítési információk elküldésére.
2. A felhasználó megadja a kívánt hitelesítő információt.
3. Az elérési pont a kapott hitelesítő információt továbbítja egy szabványos RADIUS-szervernek, amely elvégzi a hitelesítést és a jogosultság-ellenőrzést.
4. Ha a RADIUS-szerver megállapítja a jogosultságot, a kliens engedélyt kap a csatlakozásra, és az adatátvitelre.

Napjainkban az EAP során használt négy leggyakoribb módszer:

- EAP-MP5,
- EAP-Cisco Wireless (LEAP néven is ismert),
- EAP-TLS,
- EAP-TTLS.

A következő pontokban röviden sorra vesszük az egyes eljárásokat.

EAP-MP5

A módszer az MD5 kivonatoló algoritmuson alapszik. Veszi a felhasználó azonosítóját és a jelszavát, kivonatolja azt, és az eredményt elküldi a RADIUS-szervernek. Az algoritmus nem használ kulcskezelési vagy dinamikus WEP-kulcsgenerálási lehetőséget, így állandó WEP-kulcsok beállítására van szükség. Ennek a módszernek van néhány korlátja:

- Mivel nincs lehetőség dinamikus WEP-kulcs előállítására, így a módszer a WEP-hez képest nem növeli meg a biztonságot. A támadók továbbra is lehallgathatják a forgalmat, és visszafejthetik a WEP-kulcsot.
- A kliens semmilyen módon nem biztosíthatja azt, hogy a megfelelő elérési pontnak továbbítsa az üzeneteit, akár egy szélhámos elérési ponttal is felveheti a kapcsolatot.

Mivel az EAP-MD5 a 802.1X szabványban előírthoz képest semmilyen többletbiztonságot nem nyújt, így a fenti módszerek közül a legkevésbé nevezhető biztonságosnak.

LEAP (EAP-Cisco)

Az EAP-Cisco Wireless, vagy a szélesebb körben használt elnevezés szerint a LEAP a 802.1X szabvány Cisco általi továbbfejlesztése, amely az EAP számos más jóváhagyott továbbfejlesztésének alapját képezi. Akár csak az EAP-MD5, a LEAP is a felhasználói nevet és a jelszót kéri be a klienstől, és továbbítja azokat a RADIUS-szervernek jóváhagyásra. A Cisco azonban a szabvány megkövetelte előírásokon kívül további feltételeket is támaszt, amelyek a biztonság szempontjából az alábbi előnyökkel járnak:

- A LEAP hitelesíti a klienst; minden egyes klienskapcsolathoz dinamikusan előállít egy csak ezen kapcsolathoz használt WEP-kulcsot. Ez azt jelenti, hogy a hálózat minden egyes eszköze más-más WEP-kulccsal éri el a vezeték nélküli hálózatot, ráadásul egy olyan kulcs segítségével, amelyet senki nem tud – még a felhasználó sem.
- A LEAP támogatja a RADIUS „munkamenet időtúllépés” lehetőséget, amely megköveteli a kliensektől a bizonyos időnkénti, jellemzően néhány percenkénti újra bejelentkezést. Szerencsére mindez úgy teszi, hogy a felhasználónak semmit nem kell tennie. Ez a jellemző párosul a dinamikus WEP-kulcsok használatával, így a kapcsolatban a dinamikus WEP-kulcsok annyira gyakran változnak, hogy egyetlen támadó sem lesz képes a kulcs ennyire gyors feltörésére.
- A LEAP-protokoll során kölcsönös hitelesítés történik, az elérési pont azonosítja a klienst, a kliens pedig az elérési pontot, így a támadók nem tudnak szélhámos elérési pontokat elhelyezni a hálózatban.

Jelenleg csupán egyetlen ismert hiányossága van a LEAP használatának. A kliens és az elérési pont hitelesítésére az MS-CHAPv1 módszert használja, amelynek van néhány ismert sérülékenysége.

Megjegyzés



Nem mindenki rendelkezik RADIUS-szerverrel, amelyet a LEAP használhatna; a Cisco elérési pontok azonban rendelkeznek egy AAA hitelesítés nevű lehetőséggel is, amely lehetővé teszi a felhasználók helyi azonosítását. Ilyenkor nincs szükség külső RADIUS-szerverre, hanem maga az AP végzi a hitelesítést.

EAP-TLS

A Microsoft fejlesztette ki ezt a protokollt, amelyet az RFC 2716 ír le. Ez a felhasználónév–jelszó pár helyett X.509 tanúsítványok segítségével végzi a hitelesítést. A módszer a szállítási réteg biztonságára épít, amikor az EAP számára átadja a PKI-információt. Az alábbiakat lehetővé:

- dinamikus, kapcsolatonként egyszeri WEP-kulcs előállítása,
- kölcsönös hitelesítés.

Hátrányai az alábbiak:

- PKI-ra (nyilvános kulcsú infrastruktúrára) van szükség a használatához, a legtöbb vállalat azonban ilyet nem telepít magának.
- A hitelesítő szerverrel kiegészített Microsoft Active Directory létét feltételezi, és ennek megváltoztatása rendkívül nehéz.
- Amennyiben nyílt LDAP vagy Novell Directory Services is található a rendszerben, szükség lesz egy RADIUS-szerverre is, illetve azonban nem mindenki áll a rendelkezésére.
- Amennyiben a VeriSign-tanúsítványok használatára állítottuk be a saját PKI-szerverünket, akkor az EAP-TLS által megkívánt néhány mező hiányozni fog.

Hacsak nem kívánjuk az EAP-TLS protokollt pontosan a Microsoft előírásainak megfelelően telepíteni, valószínűleg más módszer után kell néznünk.

EAP-TTLS

A Funk Software cég (<http://www.funk.com>) volt az EAP-TLS alternatívájának szánt EAP-TTLS kidolgozásának úttörője. A vezeték nélküli elérési pont továbbra is azonosítja magát a kliens felé egy szervertanúsítvánnyal, de

a felhasználó a saját hitelességét a név/jelszó párral igazolja. Az EAP-TTLS ezután átadja ezt az igazolást a felhasználó által beállított tetszés szerinti számú kihívás–válasz típusú mechanizmusnak (PAP, CHAP, MS-CHAPv1, MS-CHAPv2, PAP/Token Card, vagy EAP). A módszer hátrányai:

- Némileg kevésbé biztonságos, mint az EAP-TLS által használt kettős hitelesítés.
- Használata megkérdőjelezhető a Microsoft és a Cisco által közösen jelenleg is kidolgozás alatt álló Protected EAP (PEAP = védett EAP) módszer miatt, amely pontosan ugyanígy működik.

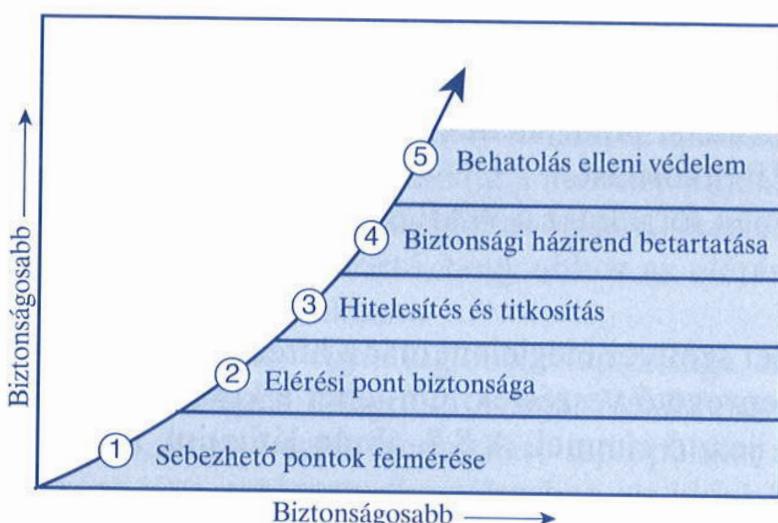
8.5.6. A VEZETÉK NÉLKÜLI BIZTONSÁG NÖVELÉSE

Amint arról már szó volt, a vezeték nélküli hálózatot a WEP használata kívül több módszerrel is biztonságosabbá tehetjük. Nem nagyon valószínű azonban, hogy mindenki rendelkezésére állna egy telepített RADIUS-szerver, így olyan lépések megtételére is sort kell keríteni, amelyek ilyen szerver hiányában is azonnal biztonságosabbá tehetik a hálózatot. A vezeték nélküli hálózattal kapcsolatos számos biztonsági probléma arra indított több vállalatot is, hogy a technológiát mindenestől száműsse a saját hálózatából. A biztonságukra figyelő cégek azonban a saját vezeték nélküli hálózatukat is megerősíthetik a többrétegű biztonsági rendszer kiépítésével, amely az alábbi lépések megtételét jelenti:

- A teljes vezeték nélküli hálózatot a saját egyetlen útválasztója mögé helyezi el, így baj esetén csak egyetlen ponton kell beavatkozni a nagyobb kár megelőzése érdekében.
- A szélhámos elérési pontok rendszeres felderítése, így a hozzájuk kapcsolódó lehetséges sebezhetőségek megelőzése.
- Az elérési pontok fizikai és logikai biztonságának megteremtésével, megelőzve azt, hogy bárki odamehessen a tudtunk nélkül egy elérési ponthoz, és megváltoztassa annak konfigurációját.
- Az alapértelmezett SSID megváltoztatása egy véletlenszerűen előállított olyan értékre, amely semmilyen formában nem utal a hálózatunkra vagy a cégbünkre.
- Az SSID jelzésként való rendszeres kisugárzásának megtiltása.
- A WEP-kulcsok tízpercenkénti vagy gyakoribb rotálása.
- Titkosítás és hitelesítés beüzemelése, amely jelentheti a vezeték nélküli hálózaton kialakított VPN használatát is.
- 802.1X kulcskezelés és hitelesítés használata.
- A létező EAP-protokollok megvizsgálása, és közük a megfelelő kiválasztása.

- A munkamenetek időtúllépési értékének 10 perces vagy annál kisebb értékre való beállítása.
- A vezeték nélküli hálózatbiztonsági házirendek kidolgozása és betartatása.
- Különböző megelőző biztonsági intézkedések megtétele, beleértve például a behatolásérzékelőket.

Amint azt a 8.6. ábra is szemlélteti, ezek a lépések és ajánlások egy menetekre bontott módszernek tekinthetők, amely betartja az alapvetet: mindenekelőtt ismerni kell a sebezhető pontot, kidolgozni a lehetséges legjobb védelmet, és továbblépni a következő menetre.



8.6. ábra. A vezeték nélküli hálózat biztonságossá tételenek lépései

8.6. A VEZETÉK NÉLKÜLI TÁMADÓK ESZKÖZEI

Ebben a pontban megvizsgálunk néhány olyan lehetőséget, amely a korábbiakban említett néhány fenyegetés kivédésében lehet segítségünk. Elméletileg minden eszközök a saját hálózat kezelésében segítik a hálózati rendszergazdákat, és az interneten mindegyikük így is van meghirdetve. A valóságban azonban ezek némelyikét a támadók is képesek és akarják is használni, így még fontosabb a hálózati rendszergazdák számára, hogy használatukkal ellenőrizzék a saját hálózatuk biztonságát.

8.6.1. NETSTUMBLER

Vezeték nélküli hálózatot mindenhol! Ez nem csupán üres frázis – már valóban mindenhol felfedezhető a vezeték nélküli hálózat. A vezeték nélküli technológia az adatok átvitelére rádióhullámokat használ, így kük-

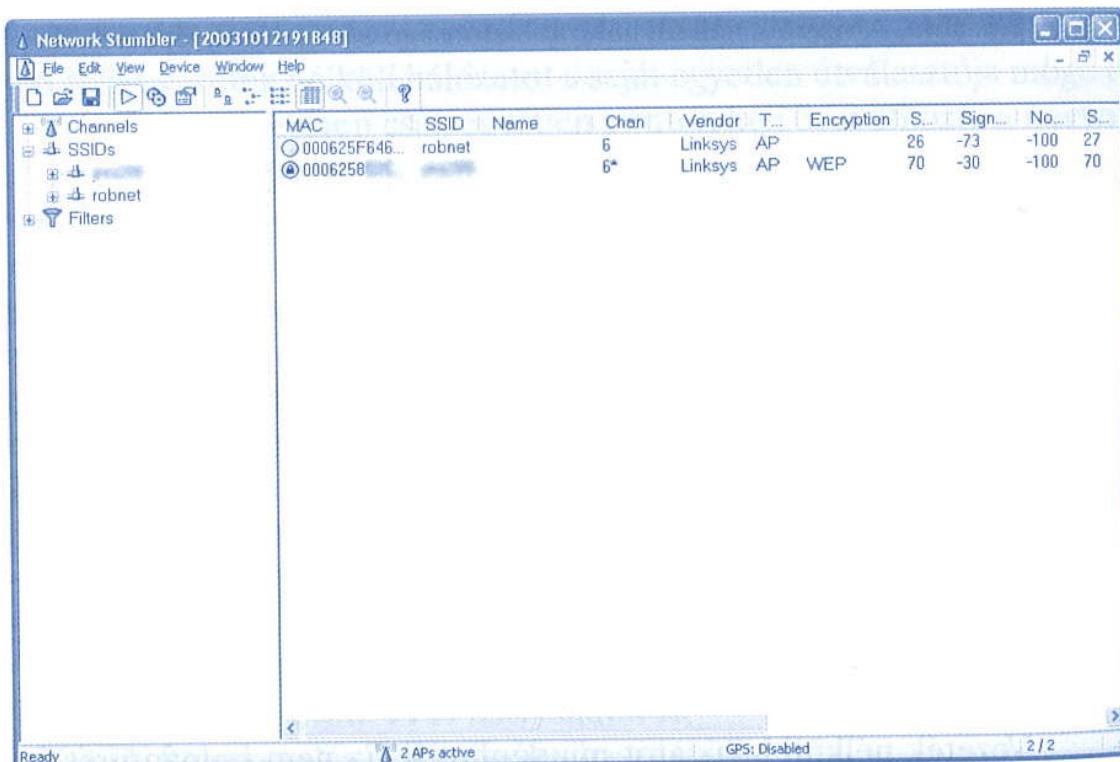
lönböző vezeték nélküli csomagok valószínűleg a könyv olvasása alatt is ott röpködnek az orrunk előtt.

Amint mostanra már mindenki megértheti, ahol vezeték nélküli csomagok röpködnek, ott biztosan megtaláljuk az őket röptető vezeték nélküli elérési pontokat is (ahol füstöt látunk, ott valami biztosan ég). Bár csak lenne arra mód, hogy megmondhassuk, van-e valahol a közelben elérési pont. Szerencsére (vagy szerencsétlenségre) tényleg van erre módnunk.

Az interneten is elérhető egy kisebb szoftver, a neve NetStumbler (megtalálható a <http://www.netstumbler.com> webhelyen), amely az alábbi „titkos” információmorzsák megszerzését teszi lehetővé számunkra:

- A vezeték nélküli elérési pont SSID-jét (azt az egyedi azonosítót, ami a vezeték nélküli hálózatot azonosítja).
- A felfedezett elérési pont jelének erősségét, és hogy az adott eszköz használ-e WEP-titkosítást.
- Melyik csatornán forgalmaz a WAP, és még néhány más apró információt.

A NetStumbler szoftver megjelent már a hírekben is, a „vezeték nélküli biztonságot fenyegető veszélyek: Ön lehet a következő áldozat”, vagy más hasonlóan ijesztő címmel. A 8.7. ábrán láthatjuk a program képernyőképét.



8.7. ábra. A NetStumbler program képernyőképe

A program valamennyi csatornán kiküld egy csatlakozási kérést, és várja a válaszokat. Ha a WAP úgy van beállítva, hogy válaszoljon az ilyen általános üzenetekre („SSID broadcast” engedélyezett), akkor a program bejelentkezik erre a WAP-ra, és a felhasználót egy bimm-bamm hangüzenettel tájékoztatja egy cél megtalálásáról. A NetStumbler jelenlegi változata azonban csak a 802.11b és egyes 802.11a-kompatibilis elérési pontokat képes felderíteni.

Az igazság az, hogy a program nem mond meg sokkal többet annál, mint amit a vezeték nélküli hálózati kártya is közölne. A trükk azonban az, hogy minden olyan információt megad, amelyre szükség van valaki más hálózatába való belépéshez.

A legtöbb vezeték nélküli hálózati kártya konfigurálása lehetővé teszi számunkra a „**helylekérdezés**” funkciót, amely a kártyával azonos csatornán forgalmazó valamennyi elérési pont megtalálására szolgál. Ha találunk ezek között olyat, amely az alapértelmezett SSID-re van beállítva (LinkSys egység esetén például a nehezen kitalálható „linksys” az alapértelmezés), tehát ha a program az alapértelmezett SSID-k egyikét jeleníti meg, akkor feltételezhető, hogy ahhoz az elérési ponthoz kevés vesződseggel tudunk csatlakozni.

A NetStumbler egyik legjobb tulajdonsága, hogy a laptopalapú GPS-egységeket képes integrálni a saját WAP-felderítési módszerébe. Képzeljük el, hogy a saját megbízható laptopunkat a saját autónk utasoldali székére téve autózgatunk a városban, és időnként meghalljuk a „bimm-bamm” jelzést, valahányszor a program talál a vételi körzetében vezeték nélküli hálózatot. Mindannyiszor, amikor a laptop kiadja ezt a hangot, a program lekérdezi a géphez csatolt GPS-egységet is, és feljegyzi a koordinátáit a megtalált WAP-információk mellé. Később betölthetjük ezeket a koordinátákat a saját térképező szoftverünkbe, és lesz egy gyönyörű térképünk arról, hogy merrefelé találhatók elérhető hálózatok. Ki merné azt állítani, hogy a jelenkor technológiája nem teszi az életünket sokkal érdekesebbé?

Eltekintve a GPS használatának lehetőségétől, a NetStumbler valójában nem a támadók eszköze, mivel az általa felderített információk alig jelentenek többletet a hálózati kártya által megadottól. Az ilyen szoftverek inkább a „felderítő” eszközök családjába tartoznak, mivel olyan problémákra vethetnek fényt, amelyek nélkülük nem lennének nyilvánvalóak. A NetStumbler egyik feladata manapság a szélhámos elérési pontok felderítése.

8.6.2. VEZETÉK NÉLKÜLI CSOMAGSZAGLÁSZÓK

A csomagok „szaglászása” (elfogása és vizsgálata) egyaránt lehet érdekes és értékes, ha tudjuk, hogy mit és hogyan szaglásszunk. Bármely hálózati rendszerben másodpercen belül szert tehet egy csomagszaglásra, és elfoghat vele néhány száz csomagot még rövidebb idő alatt, mint ahogy ezt a bekezdést végig lehetne olvasni. A csomagok tartalma olyan hálózati titkokat rejthet, amelyeket szorosan kell védeni. A „szaglászás” (*sniffing*) olyan forgalom elfogását és rögzítését jelenti, amely eredetileg csak a feladó és a címzett által olvasható volt feltételezve.

A laikus számára a „szaglászás”, illetve „elfogás” vagy „elcsórás” (*snagging*) fogalmak – egyesek így is nevezik – meglehetősen idegenül hangzanak, így magát az alapelvet is érdemes egy kicsit jobban megvizsgálni:

1. A csomagok a forrástól a cél felé haladnak az Ethernet-kapcsolaton keresztül.
2. A „válogatás nélküli” (*promiscuous*) módba kapcsolt hálózati kártya minden „helyi” forgalom fogadására képes (alaphelyzetben csak a közvetlenül neki címzett forgalmat fogadná).
3. A csomagszaglászó is látja és rögzíti a teljes forgalmat, bármely címre is irányuljanak azok eredetileg.
4. A csomagszaglászó a csomag dekódolására is képes, és olyan érdekes információkat képes feltárnivalni és megmutatni, mint a forrás és a cél MAC-címe, valamint a csomag által tartalmazott adatok.
5. A csomagok gyakran tartalmaznak kódolatlan információkat, például Windows LanMan v1 jelszavakat, egyéb nyílt szövegként továbbított titkos információkat, amelyek a támadók számára remek csemegéül szolgálnak.

Most, hogy már ismeri a vezetékes csomagszaglászókat, ismerkedjünk meg a vezeték nélküli rokonaikkal is. S hogy miként lehetséges, hogy vannak ilyen rokonai? Nos, el tudjuk fogni a vezeték nélküli forgalmat? Könnyen el tudjuk azt fogni? Tudják a támadók, hogy mennyire könnyű ezt elfogni? Az utóbbi három kérdésre a válasz egyaránt igen, amiből egyenesen következik az első kérdésre adandó válasz is.

Bizony, a támadók ismerik a vezeték nélküli csomagok szaglásának lehetőségét, és alaposan ki is használják azt. Bekapcsolta a MAC-cím szerinti szűrést a saját elérési pontján? A csomag elfogásával viszont a támadó is megtudhatja ezt a címet, mivel a csomagban megtalálható a forrás címe. Bármely vezeték nélküli hálózati kártya MAC-címe könnyen át-állítható, különösen ha az embernek rendelkezésére áll egy SMAC-hoz hasonló szoftver is, amelyet a KLC Consulting cég munkatársai alkottak meg nagy szeretettel. Elkészítették a programnak mind a Windows32-, mind a Linux-változatát, és segítségével látszólag (bár nem ténylegesen,

de ez nem látszik) megváltoztatható a hálózati kártya címe. Ha egy támadó elfogja az általunk küldött vezeték nélküli csomagot, dekódolhatja belőle a küldő MAC-címét, amellyel már más hozzájutott az elérési pont tábólázatában szereplő információhoz. Ezt a címet megadja az SMAC programnak, és a saját gépét már a mi géünknek kiadva képes az elérési ponthoz való csatlakozásra. Mindezt egy percnél is rövidebb idő alatt meg lehet tenni. Igen, jól látja – 60 másodpercnél rövidebb idő alatt. Anynyi idő alatt, amennyi egy keksz elrágcsálásához kell, a támadó már behatolhat a rendszerünkbe. S mi történik akkor, ha még a WEP-titkosítás is be van kapcsolva? Nos, olvassa el a fejezet hátralévő részét, és ezeket a kérdéseket tegye el a végére – bár addigra már valószínűleg a válaszokat is tudni fogja.

8.6.3. AIRSNORT

Mostanra már biztosan tudja, hogyan végzi a WEP a feladatát, és milyen titkosítást használ, s ezáltal mennyire sérülékeny a vezeték nélküli hálózat. A vezeték nélküli világban viszonylag jól mentek a dolgok egészen 2001-ig – ekkor megjelent az interneten egy AirSNORT nevű szoftver. A 802.11 protokoll támadás alá került, és ez a támadás azóta is tart.

Maga a program elsőként 2001. augusztus 20-án kapott szélesebb nyilvánosságot a Wired folyóiratban. A csomagok elfogása és az őket védelmező titkosítás feltörése nem volt már új ötlet – tulajdonképpen a biztonsági szakértők már ismerték a WEP gyengeségét egy ideje. Az AirSNORT csupán egy támadó „kombinált menüje” volt, amely a csomag elfogását és a titkosítás feltörését maga végezte, mindezt egy könnyen használható alkalmazás formájában. Az egyetlen hátránya az volt, hogy kizártlag Linux alatt futott (és fut ma is), amelynek akkor még korántsem volt meg az a viszonylag széles körű elismertsége, amit ma élvez.

A programot kifejlesztő csapatot a kibocsátás idején megkérdezték az okaikról. Azt állították, hogy nem a támadók univerzális szerszámának szánták, hanem annak demonstrálására, hogy mennyire gyenge védelmet nyújt a WEP-titkosítás.

A becslés szerint a szoftvernek el kell fognia öt- vagy hatmillió csomagot, amelyeken néhány percet vagy legfeljebb egy-két órát dolgozva képes megtörni a titkosítást és felfedni a WEP-kulcsot. Akkoriban ezek az időtartamok még elég hihetetlenek voltak, azonban a mai 2–3 GHz-es órajelű gépek elképzelhetetlenül gyorsabban végzik egy ekkora mennyiségi adat feldolgozását – legfeljebb néhány másodperc alatt végeznének. A nehézség szempontjából az egyetlen problémát a néhány millió csomag elfogása jelenti, mert ez azért elég hosszú ideig is tarthat – de ha egyszer ezt megszereztek...

Vannak még további szoftverek, mint például az AirSNORT-tal azonos célra szolgáló WEPcrack, amely még korántsem fejlett annyira, de már jelen van a hálózaton. Van továbbá a KisMET (illetve Apple-n futó párja, a KisMAC), amelyek szintén a vezeték nélküli hálózat felderítésére szolgálnak, GPS-helymeghatározással kiegészítve, amelyek segítségével a város elérhető vezeték nélküli hálózatait lehet feltérképezni. A különböző szoftverekből azonban ennyi is elég ahoz, hogy felismerjük a problémát. Az AirSNORT megtalálható a <http://airsnort.smhoo.com/> oldalon.

8.7. ÖSSZEFoglalás

A fejezet remélhetőleg nyújtott némi betekintést a vezeték nélküli hálózatok világába, és a biztonságossá tételek problematikájába. A kérdés-körnek számos olyan területe van, amelyet ismernünk kell; vannak azonban olyan nyilvánvaló, egymásra épülő lépések, amelyek segítségével a felhasználók dolgának minimális megnehezítésével a vezeték nélküli hálózat biztonságossá tehető. Vannak a biztonság növelésére tett olyan lépések is, amelyek ma még valójában nem jelentik a biztonság tényleges javítását. A fejezetet azon szabadon elérhető szoftverek ismertetésével zártuk, amelyekkel a vezeték nélküli hálózat támadható, s így a sérülékeny pontok felismerésével és későbbi megszüntetésével a biztonság növelését szolgálják. A támadók is gyakran használják ezeket a programokat, azonban a hálózat biztonságosabbá tétele érdekében tevékenykedőknek szinte kötelezően használniuk kell őket, hogy felismerhessenek és megelőzhessenek minden későbbi támadást.

8.8. Összefoglaló kérdések

1. Mikor használjuk a 802.11 és a Wi-Fi fogalmakat? Ezek mennyiben tekinthetők azonos vagy eltérő fogalmaknak?
2. Mi az az öt fontos szempont, ami a vállalat számára a vezeték nélküli hálózat beüzemelése mellett szól?
3. A CsataVezetés a vezeték nélküli hálózatok felderítésének leggyakoribb eszköze. Mire van szüksége a csatavezetőnek, és miért jelent akkoras hasznat a támadók számára?
4. Nevezzen meg egy szabadon elérhető csomagszaglászó szoftvert!
5. A vezeték nélküli hálózatok is ki vannak-e téve ugyanazon szolgáltatásmegtagadási (DoS) támadásoknak, mint a vezetékesek? Ki vannak-e téve olyan további DoS-támadásoknak is, amelyeknek a vezetékesek nem?
6. Sorolja fel az EAP négy, jelenleg használható fajtáját!

9. fejezet

A behatolás érzékelése és a mézesbödön

Az „érintett” és az „elkötelezett” közötti különbséget legjobban a sonkás tojásrántottával mutathatjuk be: a csirke „érintett”, a disznó viszont „elkötelezett”.

(Ismeretlen szerző)

A fejezet elolvasása után érteni kell, és el kell tudni magyarázni az alábbi témákat:

- a behatolásérzékelés alapelveit, valamint szükségeségét annak ellenére, hogy rendelkezik tűzfallal;
- a hálózati behatolásérzékelő rendszer és a gép behatolásérzékelő rendszere közötti különbséget;
- miként érzékelik ezek a rendszerek a behatolást (vagyis a támadást), és az erre való válaszolás lehetőségeit;
- a napjainkban elérhető behatolásérzékelő rendszerek némelyikét.