# Könnyű álom (5. rész)

## Behálózva

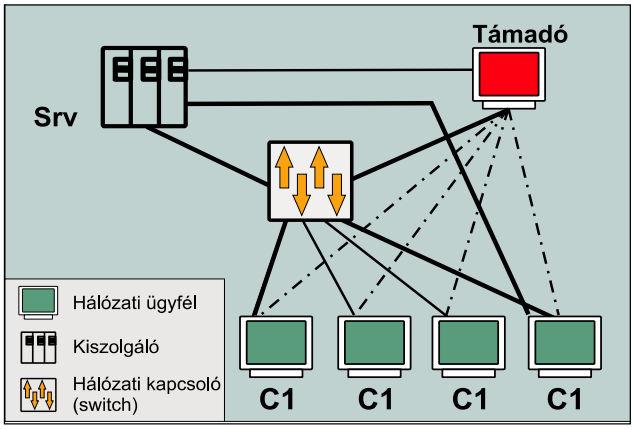
© Kiskapu Kft. Minden jog fenntartva

Ecikkben a hálózatba kötött gépeinket fenyegető veszélyeket és olyan megoldásokat javaslunk, amivel ezek kockázata csökkenthető. A különböző támadásoknak különböző előfeltételeik vannak (például a támadó a célgéppel egy hálózati szakaszon helyezkedik el). Ennek függvényében kell meghatároznunk, hogy milyen támadásokkal szemben védjük gépünket.
A helyi hálózatról gépeinket számos támadás érheti. A támadások kockázata nagymértékben eltér attól függően, hogy a rendszerünk egy otthoni hálózat, kis cég irodája vagy banki rendszer. Míg az otthoni rendszereknél az ilyen támadás esélye roppant kicsi – kivéve, ha az egyik gépünkön egy trójai csücsül –, addig egy banki rendszer esetében fel kell készülnünk minden lehetséges támadásra.

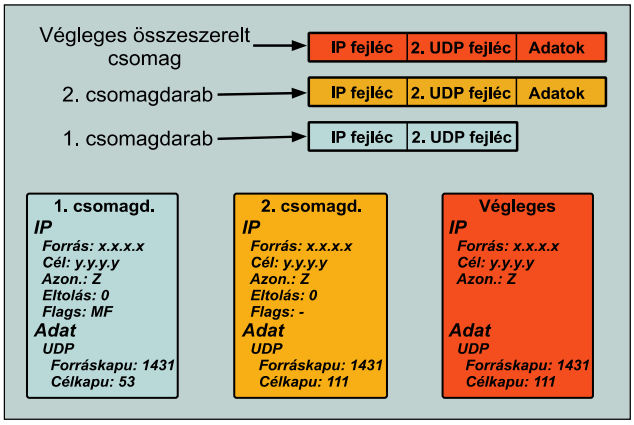
### Lehallgatás

A legegyszerűbb támadás a hallgatózás (snooping). A támadást az teszi lehetővé, hogy a napjainkban elterjedt ethernethálózat esetén egy gép adását a hálózat többi gépe is megkaphatja. A veszély mértékét nagyban befolyásolja a hálózat felépítése. A továbblépéshez először tisztáznunk kell, hogy milyen eszközöket használhatunk a hálózatunk felépítéséhez. A legegyszerűbb eszközök az úgynevezett jelelosztók (hub) és jelismétlők (repeater), melyek egyszerűen csak összekötik a gépeket, forgalomirányítást nem tesznek lehetővé. Számunkra mindkét eszközfajta ugyanazt a szolgáltatást nyújtja, így a későbbiekben bármelyikre hivatkozunk, az vonatkozik a másikra is. Sokan ezeket részesítik előnyben, hiszen áruk igen alacsony.
A jelelosztóknál magasabb szintű szolgáltatást nyújtanak a hidak (bridge), valamint a kapcsolók (switch). Ezek az OSI modell [1.] második szintjén elhelyezkedő eszközök. Itt már kettes szintű (OSI modell adatkapcsolati rétegében zajló) forgalomirányításra nyílik lehetőség. Ha például a kapcsoló egyik csatlakozóján helyezkedik el A és B gép, valamint egy másik csatlakozóján C gép, akkor az eszköz C felé általában nem továbbítja A és B beszélgetését. Az irányítás ebben az esetben az OSI kettes szintű címzés (ethernet esetén például Ethernet-cím) alapján történik (a cikkben végig ethernet hálózatot tételezünk fel, így ha az egyszerűség kedvéért ethernet-címről beszélünk, erre gondoltunk). A kapcsolókat a hidak különleges eseténekt tekinthetjük, így szintén bármelyiket említjük is, vonatkozik mindkét eszközre.
A harmadik osztályt az útválasztó eszközök (router) képezik. Ezen eszközök az OSI modell 3. szintjén helyezkednek el, az ennél alacsonyabb szinten zajló forgalmat közvetlenül nem engedik át (a cikkben feltételezzük, hogy csak IP-alhálózataink vannak).
Amennyiben az egész hálózatot pusztán jelelosztók kapcsolják össze, akkor az egész hálózati forgalom lehallgatható. A lehallgatás útválasztókon át nem lehetséges. A hálózatban elhelyezkedő kapcsolók alapesetben a lehallgatást megakadályozzák, bár bizonyos támadási módszerek felhasználásával a kapcsolók által nyújtott védelem is kijátszható. Hogyan lehetséges ez? Két elterjedt módszer is létezik: az első módszerrel magukat a kapcsolókat támadhatják, a második támadástípus segítségével az egyes gépek IP protokollrétegei ellen indítható támadás. A kapcsolók támadása esetén a behatoló két dologra törekedhet: vagy felügyelői jogokat akar szerezni az eszközön vagy annak megvalósítási, illetve beállítási hibáit próbálja meg kihasználni. Amennyiben egy kapcsolót a telepítés után nem állítottunk be megfelelően, úgy lehetséges, hogy megmaradtak a gyári jelszavak. A különböző kapcsolókban elhelyezett hátsó ajtók (backdoors) ugyancsak veszélyt jelenthetnek. Ezeket a rövidlátó gyártók karbantartási célokra építgetik eszközeikbe a rendszergazda emlékezetkiesésének esetére. Szintén gondot jelenthet a gyárilag engedélyezett SNMP protokolltámogatás, amit elsősorban az eszköz távoli felügyeletéhez használnak. Ennek segítségével az eszköz beállítása letölthető, bizonyos esetekben akár módosítható is. Egyes eszközök tartalmazhatnak olyan biztonsági hibákat is, hogy a gyárilag engedélyezett, csak olvasási jogot biztosító hozzáférés esetén is hozzáférhetők a rendszergazdai jelszavak vagy a módosítást is lehetővé tevő SNMP-azonosítók. Emiatt soha ne felejtsük el a hálózatba kötött kapcsolók jelszavait lecserélni, az SNMP-hozzáférést pedig letiltani, vagy a szükségesre korlátozni. Az SNMP-hozzáférést engedélyező azonosítókat mindig cseréljük le! Látogassuk rendszeresen a gyártó weboldalait, és a vezérlőprogram (firmware) ajánlott javításait (különösen a biztonsági javításokat) telepítsük fel az eszközeinkre. Ez a lépés rendkívül gyakran elmarad, hiszen a kapcsolók a hálózatra kapcsolás után azonnal működnek, látszólag nem igényelnek különösebb beállítást.
A kapcsolók elleni támadás másik módja, hogy megvalósítási vagy felépítésbeli hibáikat próbálják meg kihasználni. Ehhez meg kell ismerni az alapvető működésüket (jelen leírás elég erősen leegyszerűsített). A kapcsoló veszi a csatlakozóin beérkező kereteket (frames), majd megvizsgálja azok ethernet forráscímét. Amennyiben az adott forrás nem, vagy másik csatlakozón szerepel a belső irányító táblázataiban, akkor a táblázatát módosítja. Ezután a célcím vizsgálata következik. Ha a célcím csoportcím vagy üzenetszórásos cím, azokat kiküldi az összes egyéb csatlakozóján. Egyéb esetben a célcímet megkeresi a belső irányítási tábláiban. Sikeres keresés esetén a megadott csatlakozóra, egyéb esetben az összes egyéb csatlakozóra továbbítja. Ezt a működési módot hívjuk a kapcsoló áttetsző (transparent), vagy más néven öntanuló módjának. Ebből is látható, hogy ha a kapcsolót hamisított ethernet forráscímű keretekkel bombázzák, akkor hozzáférhetnek más gépek kereteihez. Előfordulhat, hogy megpróbálják a kapcsoló belső irányítási tábláit megtölteni. Ha a tábla betelik, a kapcsoló bejegyzéseket dobál ki belőle. Ezzel elérhetik, hogy a tábla esetleg hamis címekkel lesz tele, a valódi hálózati forgalmat így kénytelen minden csatornán kiküldeni. Ugyancsak lehetséges, hogy a kapcsoló a processzorának túlterhelése esetén a kereteket nem szűri, hanem minden csatlakozójára továbbítja. Ezek támadási lehetőségek elég erősen gyártó- és megvalósításfüggőek, de elméleti lehetőségként célszerű tisztában lennünk vele. Amennyiben az eszközünk képes rá, a jó nevű gyártók eszközei általában tudják ezt, célszerű lehet az öntanuló módot részben – legalább a kényes gépekre – vagy egészen kikapcsolni. Célszerű korlátozni az engedélyezett forráscímek körét. Így csökkenthetjük annak a lehetőségét, a támadó más gép címével vagy hamis forráscímmel kereteket juttathasson a hálózatba. Amennyiben lehetőség van rá, célszerű a kapcsoló naplózását bekapcsolni, a naplóbejegyzéseket pedig valamelyik kiszolgálón gyűjteni és feldolgozni. A jobb minőségű kapcsolók (általában a nevesebbek) támogatnak egy újabb szolgáltatást is, ez a VLAN (Virtual Local Area Network). A VLAN-ok célja, hogy

© Kiskapu Kft. Minden jog fenntartva




*1. ábra* APR címhamisítás




*2. ábra* IP-darabolási/összeszerelési támadás

a hálózatot virtuálisan nem érintkező részekre oszthassuk. A szolgáltatás létrehozásának a célja az volt, hogy költséghatékony módon kapcsolhassuk össze számítógépeinket, valamint csökkenthessük az ütközési zónákat (collision domains). A keretek nem hagyhatják el a VLAN-t, így például a csoportcímzett keretek is a VLAN-on belül maradnak. A VLAN létrehozása természetesen nem csak egy kapcsolón belül lehetséges, több kapcsoló közösen is kifeszíthet egy VLAN-t. Ilyenkor van a VLAN-oknak igazán értelme – például a cég ugyanazon szervezeti egységei több épületben vannak –, hiszen fizikailag egy vezetéken vihetjük át több különálló hálózat forgalmát. A kapcsolók ennek megvalósításához különleges keretekkel tartanak kapcsolatot, ahol a keret tartalmazza a VLAN azonosítóját. Amennyiben a kapcsolóinkban nem szabályozzuk e keretek elfogadását, akkor a támadó képes a VLAN-ok közötti határ átlépésére. Ha VLAN-okat használunk, mindenképpen tegyünk meg minden lehetséges óvintézkedést. Semmiképpen ne feledjük, hogy a VLAN-ok biztonsági felhasználásával (például: két VLAN között tűzfalazunk) további kockázatot vállalunk, hiszen a kapcsoló feltörése vagy a vezérlőprogram hibája miatt a VLAN-ok átjárhatóvá válhatnak. Az előbbiek figyelembevételével a kapcsolók beállíthatók úgy, hogy a kifejezetten ellenük indított támadások ne járhassanak eredménnyel. Fontos azonban megjegyeznünk, hogy a kapcsolók nem biztonsági eszközök. Tervezéskor a fő cél a teljesítmény növelése és nem a biztonság fokozása volt. A rendszer biztonságát pusztán a kapcsolókra alapozni botorság (például: teljesen kapcsolt hálón Telnet protokoll használata, mondván úgysem tudják lehallgatni).

A másik lehetséges támadási módszernél a támadó úgy kísérel meg csomagokhoz jutni, hogy a feladó gépek IP protokoll rétegét próbálja megtéveszteni. Ehhez az ARP (Address Resolution Protocol) [4.] támadhatóságát használja ki, így a részletes magyarázat előtt nézzük át ezt. Cikksorozatunk harmadik részében [2., 3.] már megismertük az IP protokoll alapvető működését, valamint az általa használt csomagtípusokat és azok szerkezetét. Akkor azonban nem szóltunk arról, hogy az IP-címek miként is azonosítják a számítógépeket. Ethernet-hálózaton a címzés az úgynevezett ethernetcímen alapul. Minden hálózati kártyának saját ethernetcíme van. Az IP-cím alapján az ethernetcím meghatározására szolgál az ARP. Amennyiben az Alfa nevű gép csomagot kíván küldeni Béta gép számára, és Béta ethernetcímét nem ismeri, úgy a hálózatra egy üzenetszórt (broadcast) ARP kérést küld ki, amelyre Béta válaszol, vagy egy harmadik gép (Ubul), amely ismeri Béta címét (proxy arp). A választ Alfa elhelyezi a saját ARP-gyorstárában (ARP cache). A protokoll lehetőséget ad arra is, hogy egy gép bejelenthesse az ethernetcím változását. Ezt a lehetőséget *Gratuitous ARP*-nak hívják [4., 2.].

Most térjünk vissza az eredeti kérdéshez, azaz mit tehet egy támadó az ARP segítségével. A hálózat egy kiszolgálóból (Srv) és több ügyfélből (C*x*) áll. A támadó elkezdi bombázni ARP-válaszokkal és *Gratuitous ARP* csomagokkal az ügyfeleket, amelyben saját ethernetcíméhez Srv IP-címét adja meg. Amennyiben az ügyfelek ARP-gyorstárát sikerül így módosítania, a C4 ügyfél az Srv felé menő csomagját valójában a támadónak küldi. Tehát a támadó képes hozzájutni az ügyfelektől a gazdagép felé menő teljes forgalomhoz. Ugyanezt a trükköt be lehet vetni a gazdagép ellen is. Így az ellenirányú forgalom is lehallgatható. A példa az 1. ábrán látható. Ezek ellen úgy védekezhetünk, ha a fontosabb gépekre az ARP-gyorstárban állandó bejegyzéseket helyezünk el, vagy a teljes ARP-t letiltjuk gépeinken. Ez azonban nem minden operációs rendszernél lehetséges, hiszen az ARP-gyorstár mérete általában korlátozott. Miért ilyen fontos a forgalom lehallgatása? Egyrészt a támadó adatokat nyer a rendszerből (kiszolgálók, ügyfelek, útválasztók), valamint érzékeny adatokat is megszerezhet (pl.: jelszavak). Mint a későbbiekben látni fogjuk, néhány támadásnál fontos szerep jut annak, hogy a támadó képes-e figyelni az ügyfél vagy a gazdagép forgalmát.

## IP-cím hamisítása, kapcsolat eltérítése

Az eddigi támadásoknál áttekintettük, hogy mit érhet el egy támadó, illetve mi ellen kell védekeznünk legfeljebb kapcsolókkal összekapcsolt hálózaton. Ezen támadások ellen védelmet jelentenek az útválasztók, hiszen sem az adatkapcsolati réteg szintű támadások sem az ARP-támadások nem jutnak át az útválasztókon, hiszen azok az OSI modell 3. szintjén helyezkednek el. Azonban itt is követhetünk el beállítási hibákat, amelyek újabb támadásokat tesznek lehetővé. Ismeretek birtokában hozzáláthatunk az újabb lehetséges támadási módszerek megismeréséhez: ezek az IP-címhamisítás (spoofing) és IP-eltérítés (hijacking). Azt a támadást nevezzük IP-címhamisításnak, amikor a támadó nem a saját címét, hanem tetszőleges más címet használ. A használt cím lehet létező gép címe, vagy egy eddig használaton kívüli. A célja lehet a támadóra utaló IP-cím elrejtése, vagy jogosulatlan előnyhöz jutás, például a kiszemelt célgépre csak a 10.6.75.43 címről lehet belépni. Ezeknél a támadásoknál a kalóz gépe nem kap közvetlen választ a hálózatról, hiszen a válasz a hamisított címre érkezne. Feltételezzük, hogy a támadó a válaszhoz mégis hozzájuthat ARP címhamisítás vagy a hálózati forgalom lehallgatása folytán. Amennyiben a támadó a válaszhoz nem fér hozzá, akkor a módszert vak hamisításnak (blind spoofing), vagy vak kapcsolat-eltérítésnek (blind session hijacking) nevezzük. Ennek kivitelezése lényegesen bonyolultabb, erről a későbbiekben ejtünk szót. UDP esetén az IP-címhamisítás roppant egyszerű: a támadó hamisított forráscímű csomagokat juttat a hálózatba. Bizonyos protokollok támadásához több lépcső is szükséges lehet, ekkor a válaszra is

szükség van. A TCP-kapcsolatoknál általában szükség van a visszajövő forgalomra is, az ellenkező esettel a vak hamisításnál foglalkozunk. Mint azt harmadik cikkünkben már leírtuk, a TCP-kapcsolat felépítése háromlépcsős. A kezdeményező gép egy SYN-es csomagot küld a kiszolgálónak, amely erre egy SYN+ACK csomaggal válaszol. A csomag vétele után a kezdeményező egy ACK csomagot juttat a kiszolgálónak, amelyben a SYN+ACK sorozatszámánál eggyel nagyobb nyugtasorszámot használ. A kapcsolat sikeres felépítéséhez mindenképpen a jó nyugtát kell használni. Amennyiben a kiszolgáló gép kezdősorszám-előállítója (ISN – Initial Sequence Number) megfelelő, a SYN+ACK csomagra mindenképpen szükség lesz. A kapcsolateltérítés az IP-címhamisítás egy részesete. Célja, hogy a támadó egy már nyitott kapcsolatba avatkozzon be. Álljon itt erre egy egyszerű példa. A rendszergazda telnet protokollon bejelentkezett a távoli rendszerre. Tételezzük fel, hogy egyszer használatos jelszavakat használ (One Time Password – OTP), például SKEY rendszert. Ebben az esetben a támadó nem ér semmit a forgalom lehallgatásával. Ekkor a támadó megkísérelheti eltéríteni (elrabolni) a rendszergazda kapcsolatát, így az ő nevében tevékenykedhet. Ehhez figyelni kell a hálózati forgalmat, hiszen a kapcsolat eltérítéséhez ismerni kell mind az időszerű csomagsorszámot, mind a nyugta sorszámát. Ezután a következő csomagot már a támadó küldheti el. Amennyiben sikerül, az eredeti rendszergazda kiesik a szinkronból. A támadónak még egy feladata van: lehetetlenné kell tennie, hogy az eltérített munkaállomás érzékelje ezt a hibát és lezárja a kapcsolatot. Ez a feladat az IP-címhamisításnál is fennáll, amennyiben a támadó működő gép címét veszi át. Ezen támadások megvalósítására az Interneten többféle eszköz is rendelkezésre áll, a támadónak pusztán csak le kell töltenie, lefordítania és máris kezdheti „áldásos” tevékenységét.

Vak támadásnak nevezzük azt, ha a támadó nem jut hozzá a számára oly fontos válaszcsomagokhoz. Ezt a támadási formát jóval nehezebb sikeresen kivitelezni és általában könnyebb is védekezni ellene. UDP esetén a vak támadás egyszerű lehet, ha a válaszcsomagok nem szükségesek. TCP esetén a helyzet jóval bonyolultabb, mivel ilyenkor ismerni kell a megfelelő nyugtasorszámot. Ez a feladat megfelelő minőségű IP-alrendszerek esetében szinte lehetetlen. Néhány operációs rendszernél különböző megvalósítási hibák miatt ez a támadás sajnos kivitelezhető. Ilyen hiba volt például a Linux rendszermag 2.0.35-nél korábbi változataiban is [9.]. Itt bizonyos esetekben a rendszermag nem ellenőrizte a nyugtasorszámot, így a vak IP-címhamisítás kivitelezése egyszerű volt. A vak IP-címhamisítás kivitelezhetőségét leggyakrabban a rossz minőségű TCP kezdősorszám-előállító teszi lehetővé. Ez hagyományosan nem biztonsági célokat szolgált, így egyszerű eljárásokkal jól meg lehetett határozni a használandó értéket (eredetileg a hálózaton bolyongó vagy többszöröződött kapcsolatfelépítési kérések kiszűrése volt csak a célja). Elég sok kereskedelmi rendszernek nincs megfelelő minőségű TCP kezdősorszám-előállítója. Akit a téma részletesebben érdekel, kezdésként olvassa el az nmap írójának cikkét [11.]. Egy gyakorlatban is végrehajtott támadás részletes elemzése olvasható *Tsutomu Shimomura* cikkében [8.].

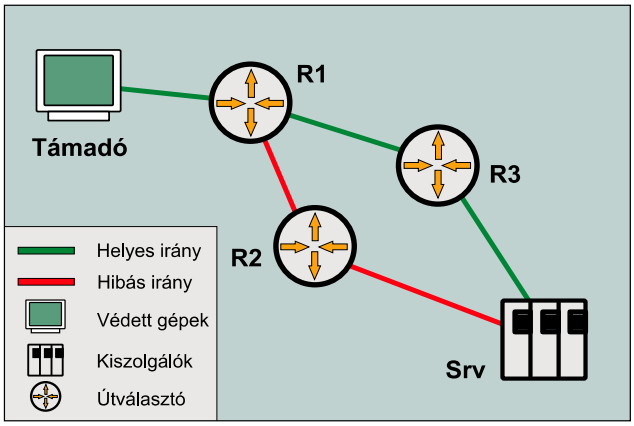
Ugyancsak gondot jelenthet, ha a támadó valamilyen eljárással képes behatárolni a kapcsolat által jelenleg használt sorszám tartományát. A Linux rendszermagban ilyenre is volt példa, ez a 2.0.37-es változatot is érintette [10.]. Ebben az esetben az IP-alrendszer a valódi (várt) sorszám és a hamisított sorszám távolságától függően, eltérően viselkedett. Mivel az IP-azonosítókat a rendszer sorrendben osztotta, egy gyengén terhelt gépen jól be lehetett határolni a szükséges sorszámot.

## Egyéb IP-szintű támadások

Az IP-alapú protokollok nem csak a fenti módokon támadhatók. Az IP összetettségének következtében elég sok megvalósítási hiba volt a legkülönbözőbb operációs rendszerekben. Ki ne emlékezne a *Ping of death* hibára, mikor gépeink könnyen válhattak egy igen hatásos szolgáltatásmegtagadás (DoS, Denial of Service) típusú támadás áldozatává. Az ilyen támadások általában az IP darabolási képességét, valamint a darabok helytelen kezelését használták ki. Jelenleg ezen támadások mérséklődtek, hiszen a mai IP-alrendszerek már védettek ellene. A fent említett *Ping of death* lényege az volt, hogy túlméretes ICMP ECHO_REQUEST csomagra a válasz hosszabb lett, mint 64 k. Mivel a rendszermag feltételezte, hogy egy csomag nem lehet hosszabb, mint 64 k, az eredmény végzetes volt: a rendszermag belső adatszerkezetei károsodtak, az eredménye magpánik lett). A csomagszűrő tűzfalak általában feltételezik, hogy az UDP- vagy TCP-fejléc az első darabban megérkezik. A forrás- és a célkapunak mindkét esetben meg kell érkeznie, hiszen ezek az IP szempontjából az első 8 bájton belül helyezkednek el (darabolás csak 8 bájtos határon lehetséges). A csomagszűrő kiveszi az első darabból a kapuadatokat, és meghozza döntését. Az utána következő darabokat továbbítja. Ha azonban a megcímzett gép helytelenül szereli össze a darabokat, érdekes helyzet állhat elő. Képzeljük el, hogy a támadó küld egy csomagot, amelyben az MF (More Fragment) bit igaz, így a címzett újabb darabra fog várni. A második és egyben utolsó darab viszont ismét eltolási értékkel érkezik, így összeszerelés közben a kapu címe felülíródik. Ezt szemlélteti a 2. ábra. Ebben az esetben a vett csomag nem annak a kapunak adódik át, amelyikre a döntést a csomagszűrő hozta. Ez a hiba már szintén nem létezik a korszerű IP-alrendszerrel rendelkező gépeken, és a csomagszűrők is tartalmaznak alapszintű védelmet ezzel a támadással szemben. Ugyancsak nehézségeket okoz az úgynevezett Source Routing használata. Ez két IP-lehetőség (IP option): (Strict source routing, illetve Loose source routing), amelyek segítségével a feladó a csomag haladási irányát tudja befolyásolni. Segítségével


© Kiskapu Kft. Minden jog fenntartva

© Kiskapu Kft. Minden jog fenntartva




*3. ábra* A Source Routing veszélyei

egy támadó elérheti, hogy csomagokat küldjön olyan gépeknek, amelyekkel nem tarthatna kapcsolatot. Célszerű ezt a lehetőséget minden útválasztón és számítógépen letiltani. A Source Routingra mutat példát a *3. ábra*.

## Általános védekezés IP-szintű támadásokkal szemben

Most nézzük meg, hogy mit is tehetünk e támadások ellen. Az egyszerű IP-hamisítás és eltérítés ellen azonos módon kell védekeznünk, mint a lehallgatás ellen. Az egyetlen különbség az, hogy pusztán a rejtjelezés nem oldja meg a gondot, hiszen a rejtjelezés általában csak az adatokat érinti. Természetesen megoldás lehet valamiféle VPN használata, de ez intraneten belül ritkán használt. Ökölszabályként érdemes használni, hogy az eltérő előjogokkal bíró felhasználókat „fizikailag” is válasszuk el, azaz gépeik különválasztott hálózaton legyenek, amelyeket legalább csomagszűrővel ellátott útválasztók válasszanak el. A kiszolgálókkal egy hálózatra ne helyezzünk ügyfélgépeket. Kisebb cégeknél, ahol csak egy kiszolgáló van néhány munkaállomással, de a munkaállomásokban nem bízunk meg (például az Internetről különböző trójai falovakat hozhatnak be), egyszerű megoldás lehet például több hálózati kártyát helyezni a kiszolgálóba és így elkülöníteni a hálózatot (ez teljesítménynövekedéssel is jár). Amennyiben a hálózatunk felépítése megfelelő, a vak támadások ellen könnyű védekezni. Egyszerűen az útválasztóinkon valósítsuk meg az INGRESS/EGRESS szűréseket [5.]. A megoldás: alhálózatainkba ne engedjünk be olyan csomagokat, amelyek forráscíme belső gépre utal, és ne engedjünk ki olyan csomagokat, amelyek forráscíme nem benti gépé. Az Internettel összekötő tűzfalon ne felejtsük el eldobálni a csak belső hálózati forrás vagy célcímekkel bíró csomagokat (például LINKLOCAL tartomány: 169.254.0.0/16). Ezek után elérhetjük, hogy az IP-címek alapján a kiszolgálókon behatárolható lesz a csomag feladási tartománya. Ennek jelentőségét ne becsüljük le, hiszen a kiszolgálók és a tűzfalak gyakran hoznak cím alapján döntéseket. A címhamisítás elleni védelem kialakítására mutat példát a (*4. ábra*). Hálózatunkat az Internettől célszerű alkalmazásszintű tűzfallal elválasztani. Ezzel azonnal védettséget kapunk a különböző IP-szintű támadások ellen. Az átmenő adatokat a tűzfal saját protokoll alrendszere összemajd újra szétszereli. Ennek köszönhetően – mivel nincs csomagszintű kapcsolat – a csomagszintű hibák, – például gyenge IP-azonosító vagy TCP-sorszám előállító –, által okozottak, vagy például a darabösszeszerelési hibák nem juthatnak át. E lépések megtétele után a sikeres belső támadás esélye jóval kisebb, és többé-kevésbé hitelessé tudtuk tenni a belső hálózaton közlekedő csomagok IP-címeit. A jó védelemhez elengedhetetlen, hogy erős titkosítást alkalmazó protokollokat használjunk. Mint az előbbiekből látható, a rejtjelezés önmagában nem elegendő. Emellett a JRJ (a Jó, a Rossz és a Jó) támadások (Man In The Middle – MITM) kizárásához a kapcsolattartásban részt vevő feleknek tudniuk kell kölcsönösen azonosítani egymást, de legalább az ügyfélnek tudnia kell azonosítani a kiszolgálót.

## Linux rendszerek beállításai

Ebben a szakaszban részletesen kitérünk arra, hogy az előző pontban említett védelmeket Linux-rendszereken miként lehet üzembe helyezni. Amennyiben a gépünk útválasztóként vagy tűzfalként működik, mindenképpen célszerű bekapcsolni a csomagok kötelező összeszerelését. Ha csak egy hagyományos géppel vagy kiszolgálóval állunk szemben, akkor sem ártunk vele:

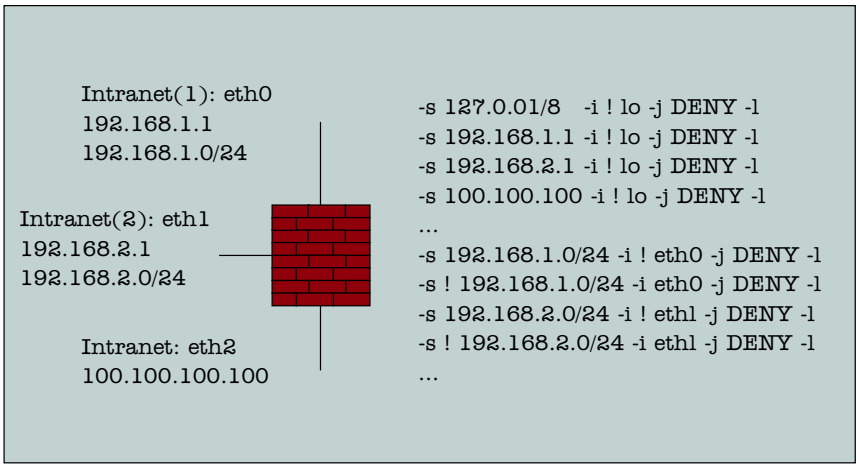
```
(bozo@dragon) ~ # echo 1 >
       /proc/sys/net/ipv4/ip_always_defrag
```

A *source routed* csomagokat ne fogadjuk el. Ugyanígy dobáljuk el a REDIRECT kategóriájú ICMP csomagokat, hiszen egy jól beállított gépen nem kaphatunk ilyeneket (természetesen nagyobb és bonyolultabb hálózaton előfordulhatnak):

```
(bozo@dragon) ~ # echo 0 >
/proc/sys/net/ipv4/conf/all/accept_source_route
(bozo@dragon) ~ # echo 0 >
/proc/sys/net/ipv4/conf/all/accept_redirects
(bozo@dragon) ~ # echo 0 >
/proc/sys/net/ipv4/conf/all/secure_redirects
```

Kapcsoljuk be a gyanús csomagok naplózását. Ehhez a rendszermagot a CONFIG_IP_ROUTE_VERBOSE szolgáltatással kell fordítani (ehhez be kell kapcsolni a CONFIG_IP_ADVANCED_ROUTER szolgáltatást):

```
(bozo@dragon) ~ # echo 1 >
       /proc/sys/net/ipv4/conf/all/log_martians
```




*4. ábra* A hallgatózás elhárítása

Kapcsoljuk be a rendszermagba épített IP-címhamisítás-érzékelőt. Természetesen a második sort ismételjük az összes hálózati csatolóra.

```
(bozo@dragon) ~ # echo 1 >
       /proc/sys/net/ipv4/conf/all/rp_filter
(bozo@dragon) ~ # echo 1 >
       /proc/sys/net/ipv4/conf/eth0/rp_filter
```

Megjegyezzük, hogy ez a megoldás bizonyos más, magasabb szintű biztonsági eszközök működését (például IPSEC), illetve a számozatlan IP-csatoló (unnumbered IP interface) használatát kizárja. Gondot okozhat még egyes csatornaegyesítési (például PPP multilink) eljárások használatában – pedig ez utóbbi megoldással tudunk 2x64kbit/sec ISDN elérést használni. Amennyiben az említett feltételek valamelyike fennáll, a rendszermag csomagszűrő szolgáltatásával tudjuk az *rp_filter* szolgáltatást kiváltani, azokon a csatolókon, ahol alkalmazása szükséges. Ez egyébként mindig hasznos lehet, a többszintű védekezés sosem árt, az egyetlen hátránya a fokozottabb felügyelet.
Két hasznos tanács a fentiekhez: a legtöbb jelenlegi Linuxban nem szükséges „kézzel” kiadni ezeket a parancsokat, induláskor a rendszer a `sysctl(8)` vagy `systune(8)` parancsok valamelyike egy állományból is képes felolvasni és beállítani. A másik hasznos tanács, hogy ne egyesével állítsuk hálózati csatolóinkra, hanem módosítsuk a /proc/sys/net/ipv4/conf/default/ könyvtár alatt levő bejegyzéseket. Amennyiben ez a hálózati csatolók elindítása előtt történik meg, a csatolóra vonatkozó értékeket innen fogja venni.
Nézzük meg, hogy miként állíthatunk be állandó ARP-bejegyzéseket. Erre az `arp(8)` parancs szolgál. Használata az alábbi:

```
(bozo@dragon) ~ # arp -s 192.168.1.1
       11:22:33:44:55:66
```

ahol 192.168.1.1 a gép IP-címe, a második érték pedig az ethernet-címe. Az ARP-gyorstár tartalmát megnézhetjük az alábbi paranccsal:

```
(bozo@dragon) ~ # arp -a
```

Amennyiben szeretnénk kikapcsolni valamely csatolónkon az ARP lehetőséget, adjuk ki az `ifconfig(8)` parancsot a `-arp` kapcsolóval, például:

```
(bozo@dragon) ~ # ifconfig eth0 -arp
```

Az ARP-táblák változásait célszerű figyelni, hiszen így észlelhetjük az újonnan megjelenő gépeket, valamint az IP-címüket megváltoztató gépeinket. Erre hasznos segédeszköz lehet például az `arpwatch(8)` segédprogram. Amennyiben egy megadott gép TCP sorszám-előállítója érdekel minket, adjuk ki az alábbi parancsot:

```
(bozo@dragon) ~ # nmap -O linux
Starting nmap V. 2.54BETA7
(www.insecure.org/nmap/)
Interesting ports on linux.nowhere (192.168.1.1):
(The 1531 ports scanned but not shown below are
in state: closed) Port State Service 22/tcp open
sshTCP Sequence Prediction: Class=random positive
increments Difficulty=1693649 (Good luck!)
Remote operating system guess: Linux 2.1.122 -
2.2.16
Nmap run completed
-- 1 IP address (1 host up) scanned in 2 seconds
```

Szóval ez a jó. Ha az alábbihoz hasonlót látunk, kezdhetünk aggódni:

```
(bozo@dragon) ~ # nmap -O loose95
Starting nmap V. 2.54BETA7
(www.insecure.org/nmap/)
Interesting ports on loose95.nowhere
(192.168.1.2): (The 1522 ports scanned but not
shown below are in state: closed) Port State
Service 139/tcp open netbios-ssn
TCP Sequence Prediction: Class=trivial time
dependencyDifficulty=2 (Trivial joke)
Remote operating system guess: Windows
NT4/Win95/Win98
Nmap run completed
-- 1 IP address (1 host up) scanned in 1 seconds
```

## Irodalomjegyzék


[1.] Andrews S. Tannenbaum: Számítógép-hálózatok
[2.] W. Richard Stevens: TCP/IP Illustrated, Volume 1
[3.] Linuxvilág magazin 2001. február–márciusi száma
[4.] RFC826: An Ethernet Address Resolution Protocol
[5.] RFC2827: Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing.
[6.] CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks
➲ http://www.cert.org/advisories/CA-1996-21.html
[7.] CERT Advisory CA-1995-01 IP Spoofing Attacks and Hijacked Terminal Connections
➲ http://www.cert.org/advisories/CA-1995-01.html
[8.] Tsutomu Shimomura: Technical Details of the Attack Described by Markoff in NYT
➲ http://www.netsys.com/firewalls-9501/0900.html
[9.] Linux Blind TCP Spoofing
➲ http://www.securityfocus.com/templates/archive.pike?list=1&mid=12805
[10.] Linux blind TCP Spoofing, act II + others
➲ http://www.securityfocus.com/templates/archive.pike?list=1&mid=20979
[11.] Fyodor: Remote OS detection via TCP/IP Stack FingerPrinting
➲ http://www.insecure.org/nmap/nmap-fingerprinting-article.html
[12.] Steven M. Bellovin: Security problems in the TCP/IP protocol suite, Computer Communications Review 2:19, pp. 32-48, April 1989 ➲ http://www.research.att.com/~smb/papers/ipext.ps
[13.] IP-spoofing Demystified (Trust-Relationship Exploitation)
➲ http://www.phrack.com/search.phtml


*Mátó Péter* (atya@andrews.hu), informatikus mérnök és tanár. Biztonsági rendszerek ellenőrzésével és telepítésével, valamint oktatással foglalkozik. 1995-ben találkozott először linuxos rendszerrel. Ha teheti, kirándul vagy olvas.

*Borbély Zoltán* (bozo@andrews.hu), okleveles mérnök-informatikus. Főként Linuxon futó számítógépes biztonsági rendszerek tervezésével és fejlesztésével foglalkozik.
A 1.0.9-es rendszermag ideje óta linuxozik. Szabadidejét barátaival tölti.

© Kiskapu Kft. Minden jog fenntartva