Könnyű álmok (1. rész)

Avagy hogyan maradjunk nyugodtak a sok veszély ellenére.

Omne principium difficile...
Bolygónk új fajjal gazdagodott: a homo szájberszpésszel. Gigabájtokkal ébred és nem is talál ki hatvannégy bites világából egész álló nap. Nos igen, a számítástechnika napjaink csillaga. Nap mint nap hallani, hogyan teszi életünket egyszerűbbé, szebbé és hatékonyabbá, persze a rossz oldalai sem maradhatnak rejtve. Gonosz számítógépes bűnözők ülnek naphosszat mindentudó gépeik előtt, és azon dolgoznak, hogy százcsillió dollárt utaljanak át a szegény árvák bankszámláiról sajátjukra. Eddig a mese. Mi a valóság? Akad néhány fülsértően hozzáértő, aki túl gyakran és sokat beszél az informatikáról. Az ember azonnal megtudhatja tőlük, hogy mi a helyzet manapság, mi a „trendi" és mi nem. Van azonban egy apró gond: a félrevezetett felhasználók tartanak az Internet kalózaitól anélkül, hogy bármit is tudnának róluk és ismernék a védekezés lehetőségeit. A cégek felelős vezetői hihetetlen összegeket költenek méregdrága védelmi rendszerekre, amelyek biztonsági szintjét azonban senki sem tudja hitelt érdemlően bizonyítani. A biztonsági rendszerek felépítését és működését belső emberek ritkán látják át, mivel kevés cég engedheti meg magának hivatásos biztonsági szakember alkalmazását. Mások hajlamosak lebecsülni a nehézségeket, mivel ők hozzáértők és mindenkinek be tudják bizonyítani, hogy miért nincsenek veszélyben. Ez a hamis biztonságérzet természetesen kihat az egész cégre, amikor pedig becsap a villám, mindenki csak néz és csodálkozik.
Érdemes tehát a biztonságról beszélni, és kicsit többet megtudni róla. A Linux-rendszerek mind az otthoni, mind a céges felhasználási területen rohamosan terjednek, így egyre többen fedezik fel az ingyenes rendszerek előnyeit. Kevesen tudják azonban, hogy kis odafigyeléssel és némi tapasztalattal kitűnő védelmi rendszer építhető belőlük. Szándékaink szerint írásunk egy olyan sorozat kezdete, melynek célja, hogy érthetővé tegye a rendszerek sérülékenységének okait, valamint elősegítse azok elhárítását. Nem cél azonban minden lehetséges rés feltárása, hiszen ez messze túllépi kereteinket. Fontos cél a figyelem felhívása a veszélyekre, de emellett mindenhol igyekszünk megmutatni az adott bajok megakadályozásának módszereit is. A sorozat előrehaladtával egyre mélyebbre hatolunk a Linux-rendszer védelmének rejtelmeibe, és mire vég-zünk, egy alapos áttekintő képet kapunk a biztonságos rendszerről. Terveinkben szerepel, hogy mélyebben foglalkozzunk adott rendszer hálózat felőli védelmével, egy hosszabb lélegzetű részben pedig a helyi biztonság növelésével. Ezek után következik a legérdekesebb témakör: a tűzfalak. Bemutatjuk a fajtáit, azok sajátosságait, milyen eszközök léteznek Linuxra a hálózati határvédelem kialakítására. Mire ide elérünk, addigra valószínűleg végleges lesz a 2.4-es rendszermag első példánya, így megismerkedhetünk annak lehetőségeivel. Végül bemutatjuk egy Linux-alapú védelmi rendszer tervezését és kivitelezését, mindezt ingyenes tűzfalalkalmazás segítségével. Így már érthető a főcím mondanivalója: védd magad és légy nyugodt.

Az első nyugodt álom: hálózati rendszerek biztonsága

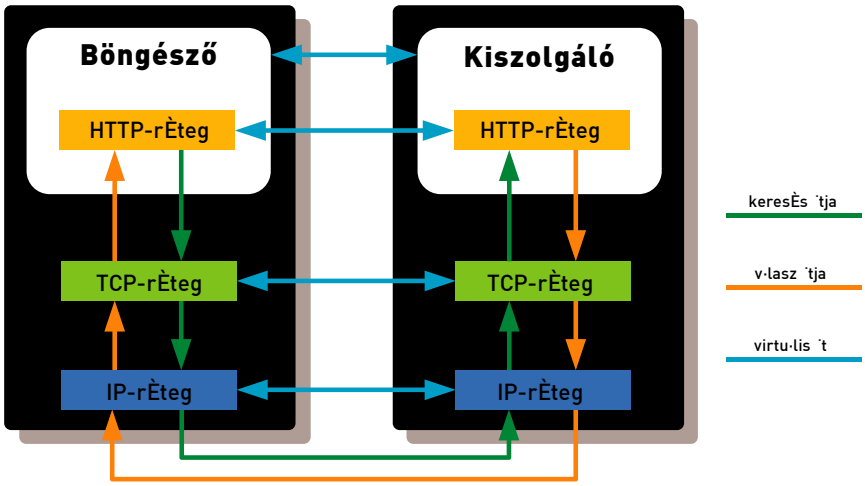
Manapság mindenki a szupersztrádáról beszél, a nagytudásúak és a hangos elektronikus üzleti (e-business) reklámok azt azonban elfelejtik megemlíteni, hogy az új szabadság veszélyeket is rejt magában. Más összefüggésben ugyan sokat hallhatunk emlegetni a számítógépes bűnözésről, a kettő összefüggéseit azonban tudatosan elfelejtik említeni. A sajtó döntő többségét olvasva nem is fedezzük fel az összefüggést. Balgaság lenne azt gondolni, hogy ha a kalózok a NASA számítógéprendszerét is feltörik, pont a mi otthoni banki átutalásokra használt kis programunkat hagyják békén. Az is kósza tévhit, hogy gonoszok csak az Interneten vannak. Sőt! A számítógépes bűnelkövetők többsége a cég belső emberei közül kerül ki, legyen az multicég vagy egyetemi kollégium. A komolyabb támadásokat általában az anyagiak ösztönzik, de az indítékok között előfordul bosszú, erőfitogtatás, kalandvágy és ki tudja, mi még. Mivel nem tekinthetünk el a belső emberek által elkövetett ténykedésektől, így a hálózati támadásokat nem célszerű csak az Internetre értelmezni. A belső hálózat ugyanolyan támadási felület, azon belül is a lehető legnagyobb védelemről kell gondoskodnunk. A cikksorozat első néhány részének célkitűzése, hogy megvilágítsuk, miként mérsékelhető annak az esélye, hogy valaki sikeres hálózati támadást intézzen az otthoni rendszer vagy a cég kiszolgálója ellen.

Mekkora az egészséges veszélyérzet?

Általában elmondható, hogy a védelem ereje arányos a ráfordított energiával és az erőforrásokkal. Azt, hogy egy rendszert mennyire kell, vagy érdemes védeni, kizárólag a rendszer felhasználói tudják eldönteni. Gyakran hangzik el az a kijelentés: „Hozzánk nem érdemes betörni, itt nincs semmi értékes..." Ezzel kapcsolatban két dolgot vizsgáljunk meg közelebbről.

Érdemes védekezni?

Nincs olyan rendszer, amit ne lenne érdemes feltörni. Mindig védekezz!
Példaként említeném a következő elképzelt esetet: a cégnél van egy nyomtató, amit többen is használnak. Az elérhetőség céljából egy éve összeraktak egy régi elavult számítógépből, valamint egy linuxos nyomtatókiszolgálóból álló rendszert. Mivel a Linux-alapú kiszolgáló megbízható, sőt, a gép áramkimaradás esetén CD-ről indul, így hozzá sem kell nyúlni. Biztonsági intézkedéseket sem hozta, hiszen nincsen rajta semmi fontos, csak egy egyszerű nyomtatókiszolgáló. Egy nap a rendőrség kíséretében néhány Interpol-nyomozó érkezik, lefoglalják a nyomtatókiszolgálót és kihallgatják a cég összes alkalmazottját. Mi történt? Az értéktelen kiszolgáló biztonsági rendszerén valaki könnyedén keresztülhatolt, és ezen keresztül törte fel a Pentagon honlapját, majd ott malac képeket helyezett el.
A kalóz konkrét cél nélkül csak akkor tör be valahová, ha az egyszerű. Ugyanis ha egy rendszerben nincs olyan érték, ami miatt érdemes lenne feltörni, akkor a betörés leggyakoribb oka a rendszer védtelensége. Ha az erdő körül nincs kerítés, és a tóhoz az erdőn keresztül vezet egy rövidebb út, akkor mindenki arra fog menni, ha viszont van egy erdőkerülő két hatalmas kutyával, akkor inkább a hosszabb utat fogják választani. Így működik ez a számítógépes rendszerek esetében is. Ha nem fordítunk kellő figyelmet a biztonságra, akkor a rendszerbe könnyű lesz behatolni, és a kalózok átjárónak fogják használni rendszerünket, vagy használják erőforrásainkat. Mindenki érti, hogy a kalózok miként használják fel gépünket, amikor tovább akarnak lépni, nem egyértelmű viszont az, hogyan lehet az erőforrásokat kihasználni. Ahogy egyre több felhasználónak van elektronikus levélcíme, úgy az árucikkek Interneten zajló reklámozásában is egyre



1. ábra A webkiszolgáló és az ügyfél közti kapcsolat

nagyobb üzleti lehetőségek rejlenek. A legegyszerűbb megoldás a célközönség által olvasott levelezőlisták irattáraiból a levélcímek kigyűjtése, azután már gyerekjáték egy reklámlevél (más szóval levélszemét, angolul spam) elküldése. Ez azonban nem etikus, ráadásul óriási hálózati forgalmat okoz, így nem célszerű közvetlenül a cég levelezőrendszerét erre felhasználni. Ha egy kalóz feltör egy rendszert, akkor ott olyan programot helyezhet el, amely a továbbítandó levelet egy előre megadott címlistára a feltört rendszer erőforrásait felhasználva juttatja el. Eközben a rendszer tulajdonosa hálózati keresztmetszetének egy részét nem tudja kihasználni, nem beszélve az erkölcsi kárról, ha az eset kiderül (mert általában kiderül, csak már régen késő).
Ha a behatolás nem könnyű, akkor inkább másik áldozatot keres a kalóz, úgyis minden egyes biztonságosabb rendszerre harminc könnyű préda jut. Ha azonban a kalóz határozott céllal támad meg egy rendszert, akkor a komolyabb biztonsági rendszer is kevésnek bizonyulhat. Itt következik annak a mérlegelése, hogy rendszerünk mennyire értékes. Ha elég erős a védelmi rendszer – például jó minőségű a tűzfal –, akkor a támadóknak annyi energiát kellene befektetni annak kikerülésébe, hogy inkább feladják. Ennek ellenére be kell vallani, hogy van olyan támadó, aki ellen nem lehet védekezni. Ha például egy másik földrész hárombetűs hivatala akar behatolni...

Tévedni emberi?

Nem tudsz olyan kevés időt tölteni az Interneten, hogy ne találjanak meg. Mindig számíts támadásra!
Az alábbi példa velem esett meg: egy barátomnak segítettem Linuxot telepíteni. Beállítottuk a behívást, éppen azt magyaráztam, hogy mire jók a naplóállományok, és... Mit látok? Valaki megpróbálta feltörni a még csak négy perce az Interneten lógó névtelen rendszert. Hogyan találhattak meg? Egyszerű: nem ezt a gépet keresték, hanem egy tetszőlegeset, amit rosszul állítottak be az adott szolgáltató címtartományában. A naplóállományokból látszott ugyan, hogy a támadó program nem Linux-rendszert keresett, hiszen olyan porton (kapun) próbálkozott, amely egy másik rendszer tipikus hibáját rejtheti, de nem szabad megfeledkezni arról, hogy a Linux terjed. Egyre gyakrabban keresnek majd rosszul beállított Linux-rendszert is.
Foglalkozzunk két újabb tévhittel: a rövid idő és az ismeretlen cím biztonságnövelő hatásaival. Egyesek hajlamosak azt gondolni, hogy ha nem futtatnak nyilvános szolgáltatást – vagy senkinek sem szólnak róla –, és csak napi fél órát szörföznek, akkor nincsenek veszélyben. Ha helyesen állítjuk be a csomagszűrőt és figyeljük a naplóállományokat, akkor gyorsan rájövünk, hogy ez bizony önámítás. Vannak rosszindulatú emberek által írt olyan programok, úgynevezett férgek (worm), melyeknek fő célja a terjedés (úgy, mint a vírusoknak), és egyszerű próbálkozással keresik leendő áldozataikat. Ezek ellen nem véd semmilyen névtelenség, különösen ha eleve olyan Internet-címtartományokkal dolgoznak, amelyeket a nagy szolgáltatók az oda behívó gépeknek osztanak ki. Azért dolgoznak gyakran éppen ezekkel a címekkel, mert a behívó rendszerek nagy része rosszul van beállítva, a biztonság a fent felsoroltak miatt e rendszerek gazdáinak nem túl fontos szempont. Ha sikerült bejuttatni a támadó programot, akkor már csak a rendszer újratelepítése adhat biztonságos megoldást. Mivel a legtöbb Linux-rendszer behívással kapcsolódik az Internetre, fontosnak tartjuk újra felhívni a figyelmet: *a behívással kapcsolódó gépek biztonságának is figyelmet kell szentelni!*

Mennyibe kerül mindez?

Egy rendszer legkevesebb annyit ér, amennyibe a helyreállítása kerülne. Számolj!
Például az ügyvezető úgy gondolja, nincs szükség külön tűzfalra, mert a rendszeren tárolt legértékesebb információ a tavalyi könyvelés, annak a végeredményét pedig már úgyis nyilvánosságra hozták... Egyszer egy tréfás kedvű kölyök egy friss biztonsági rés működését bemutató program segítségével betör a kiszolgálóra. A támadó ráébredve arra, hogy mit követett el, gyökértől letörli az összes állományt a rendszerről, hogy eltüntesse saját nyomait. Mi történt? Mivel nem volt a könyvelést újra el kell készíteni. Ha ekkor jönne egy adóellenőr, az nagyon kellemetlen és drága mulatság lenne. Sokkal drágább, mint amennyire a rendszer kiegészítése lett volna.
Rendszerünk, legyen az kiszolgálórendszer a hozzá tartozó adatokkal, vagy erőforrás-szolgáltató, mindenképpen okkal van a hálózatban. Azt lehet mondani, hogy másnak nem fontos, de ez nem jelenti azt, hogy nem kell óvni. Célszerű a következő szempontokat szem előtt tartani a védelmi rendszerre fordított eszközök meghatározásánál:

- fel kell mérni, hogy mennyit ér a rendszer nekünk, valamint azt is, hogy mennyit érhet a rendszer egy esetleges támadónak,
- figyelembe kell venni a jelenlegi átlagos védekezési erőfeszítéseket a hasonló jellegű rendszereken,
- fel kell mérni, kit tesznek felelőssé egy tőlünk kiinduló számítógépes bűncselekmény miatt,
- át kell gondolni, hogy mekkora erkölcsi kárt jelenthet, ha a gépet feltörik, és a kalóz saját céljaira használja fel.

Csak mindezek figyelembevételével szabad a rendszer védelméről dönteni. A rendszer védelme a vas és az operációs rendszer védelmével kezdődik, erre a későbbiek során részletesebben kitérünk. Ha a hálózat felől szeretnénk biztonságosabbá tenni rendszerünket, akkor meg kell ismerni a hálózatszintű és alkalmazásszintű támadásokat.

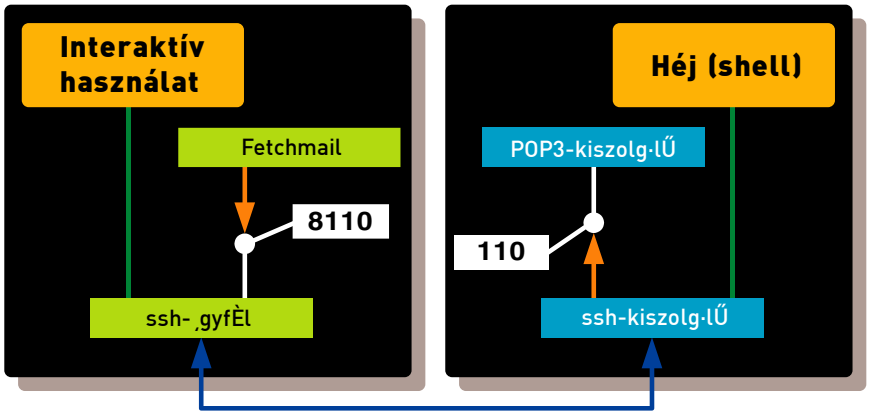
Hálózatszintű támadások

A számítógépes hálózatok hőskorában a biztonság nem volt tervezési szempont, így a kapcsolattartó protokollok általában könnyen támadhatók. A számítógépek közti információcsere jelenleg a leggyakrabban

TCP/IP protokollon keresztül folyik. Ez egy protokollcsoport, amely mindig tartalmazza az IP-t (Internet Protocol) és feladatától függően néhány egymásba ágyazott egyéb protokollt. Például amikor letöltök a kedvenc honlapomról egy képet, az alábbi rétegek működnek:

- A két gép között az IP gondoskodik az adatok továbbításáról. Az IP egy megbízhatatlan hálózatokra tervezett csomagkapcsolt protokoll, amelynél az egyetlen tervezési szempont az volt, hogy az adatok eljussanak A-ból B-be. Minden csomag tartalmazza a feladó és a címzett gép címét, ezek a címek azonban jelenleg nem hitelesítettek.
- A TCP létrehoz egy, a felsőbb protokollok számára folytonosnak és hibamentesnek tűnő kapcsolatot. A felettes protokollok adatait a TCP feldarabolja, sorszámozott csomagokba teszi, és elküldi. Így a túloldali rendszer ellenőrizni tudja, hogy minden csomag pontosan egyszer érkezzen meg. Továbbá ő gondoskodik arról, hogy a csomagok a megfelelő sorrendben össze legyenek állítva. Lehetővé teszi még a célgép egy adott szolgáltatásának megcímzését is.
- A HTTP protokollt kifejezetten állománytovábbításra fejlesztették ki, az ő adatrészébe kerül be a tulajdonképpeni adat – jelen esetben a kép.

Ezt a folyamatot az első ábra mutatja be. Ez a séma csak szemléltető jellegű, a rendszer a valóságban lényegesen összetettebb. A szemléltetésre néhány később bemutatott támadás átláthatóbbá tétele miatt van szükség. Az adatátvitel közbeni támadásoknak alapvetően kétfélék: passzív és az aktív.



2. ábra Titkosított csatorna létrehozása ssh segítségével

Passzív támadásformák

Ha van rá mód, titkosítsd kapcsolataidat!

Példaként lássuk a következőket: *Sára* rendszergazda egy *Kft.*-nél. A személyzeti vezető nem bízik meg benne, ezért a levelezőrendszer üzemeltetői jogát elveszi tőle. Mivel tisztázni szeretné, hogy valóban megbízhatatlan-e a munkatárs, elektronikus levélben megkeresi Sára előző munkahelyét. A kérdésre megírták, hogy valóban gondok voltak vele. Sajnos lopott és megbízhatatlan. A személyzeti vezető elhatározza, hogy már másnap megválik, de éjszaka a cég teljes bevételének lába kél, és Sárát sem látják soha többé. Mi történt? A személyzeti vezető nem volt tisztában azzal, hogy a levelek továbbítására szolgáló SMTP (Simple Mail Transfer Protocol) protokoll nem titkosított, így Sára tudomást szerezhetett a levelek tartalmáról.

A két gép közti adatáramlás alapesetben semmilyen titkosítással nincs védve, így ha valaki azt le tudja hallgatni, akkor az átáramló adatok birtokába jut. Ezt a támadási módot hallgatózásnak hívják (sniffing), és klasszikus esete a hálózati szintű támadások egyik fajtájának, a passzív támadásnak. Ezeknél a támadó semmilyen úton nem szól bele a két gép közti adatátvitelbe, csak figyeli azt.

Mivel az Interneten jelenleg használatos protokollokat viszonylag régen tervezték, általában nincs beépített titkosítási lehetőségük, így ezzel a támadási móddal még sokáig számolnunk kell. Néhány jelentősebb protokoll támogat valamilyen szintű titkosítást, de ez viszonylag ritka, és nem minden esetben kielégítő erősségű. Jó példa erre az elektronikus kereskedelem dinamikus terjedésével egyre gyakrabban használt HTTPS protokoll, amely a HTTP titkosítással kiterjesztett változata.

Ne figyelj ide!

Könnyen lehallgatható például a jelenleg kis- és közepes méretű hálózatoknál leggyakrabban használt Ethernet, ahol egyszerűbb esetben az azonos hálózaton lévő eszközök egymás közti forgalmát láthatják. Így, ha egy cég vagy iskola rendszerébe egy támadó képes bejutni, akkor a hálózaton áramló titkosítatlan adatokat megszerezheti. A hálózati forgalom irányítását ígérő eszközök (például hálózati kapcsolók – switchek) hamis biztonságérzetet adhatnak, hiszen gyakran korántsem olyan biztonságosak, mint amilyennek kikiáltják őket. Az Internet felé irányuló forgalmat mind a szolgáltató alkalmazottai, az oda behatoló kalózok lehallgatják. Ha valaki elég rámenős, a bérelt vonali forgalmat is lehallgathatja egy telefonpóznára szerelt eszközzel. Tehát a hálózati rendszerekről nem feltételezhetjük, hogy e támadás ellen hatékony védelmet tudnak adni. Az egyetlen biztos megoldás a hálózaton átáramló bizalmas adatok valamilyen módon történő titkosítása.

Titkok

Ha a protokoll nem támogatja a titkosítást, akkor kiegészítő eszközzel elérhető, hogy a két fél titkosított csatornán beszélgessen. A leggyakrabban használt ilyen kiegészítők az úgynevezett SSL (Secure Socket Layer – titkosított csatolóréteg) programozási könyvtárra épülő eszközök, ezek segítségével a titkosításra nem képes protokoll egy titkosított virtuális csatornán halad át. Például a levelek letöltését lehetővé tevő kiszolgáló, mely az egyszerű POP3 (Post Office Protocol) protokollt használja, kiegészíthető egy olyan réteggel, amivel a levelek letöltése titkosítva történik. Ezt a kiegészítést a levelezőprogramok jó része már támogatja, illetve a letöltés alkalmas eszközzel egyszerűen megoldható. Ez Linux alatt például stunnel, valamint a fetchmail segítségével könnyen kivitelezhető.

Csatornázás

Jó megoldás egy rendszer távoli elérésére az ssh (secure shell) használata, amely titkosított csatornán keresztül viszi át az adatokat, és újabb csatornák létrehozását is lehetővé teszi. Ha a távoli gép POP3 portját (kapuját) szeretnénk saját gépünk helyi csatolóján látni, akkor a következő paranccsal kezdeményezhetjük a kapcsolat felépítését:

```
$ ssh -L 8110:localhost:110 -l atya -v gep.neve.hu
```

Ha a távoli ssh-kiszolgáló beállítása lehetővé teszi a port továbbítását (port forwarding), akkor a helyi gép 8110-es portjához kapcsolódáskor, az ssh ügyfél ezt a kapcsolatot továbbítja a távoli gép 110-es portjára (lásd a *2. ábrát*). Azért kell a helyi gépen 8110-es portot használni, mert az egyszerű felhasználóknak nincs joguk a gép első 1024 portját megnyitni. Így egy nem titkosított protokollt,

ami a hálózaton való keresztülhaladáskor lehallgatható lett volna, egy titkosított csatornán vezetünk keresztül. Ez a titkosított csatorna kialakításának legegyszerűbb módja, és jelenleg már aligha találunk olyan rendszert, amit ne érhetnénk el ssh protokollon keresztül.
Egy másik lehetőség az átvitelre kerülő adatok titkosítása, erre jó példa a gpg (GNU Privacy Guard), amely a gpg adatállományok titkosítására vagy hitelesítésére szolgál, leggyakrabban bizalmas adatok levélben való továbbításakor használják a Sárával kapcsolatos gondot megoldotta volna. Megfelelően nagy méretűre választott titkosító kulcs segítségével a titkosítás olyan erős, hogy bizonyos országokban használata még ma is tiltott, ugyanis az államhatalom nem tudja megfejteni...

Végső megoldás

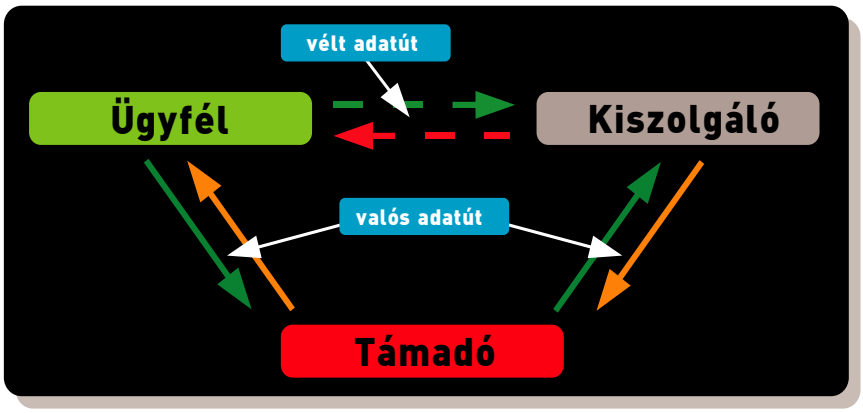
Ha több csatornát akarunk továbbítani, melyek különböző protokollokon beszélgetnek, akkor célszerű lehet egy úgynevezett VPN (Virtual Private Network), azaz egy virtuális magánhálózat kiépítése. A VPN olyan – célszerűen titkosított – csatornát hoz létre két független hálózati rendszer között, amely lehetővé teszi a két rendszer védett, bizalmas kapcsolattartását. Felépíthetünk tehát egy olyan rendszert, amely az Interneten keresztül kapcsolódik össze, mégsem kell tartani a lehallgatás veszélyétől, mert a végpontok közti adatátvitel titkosított. Virtuális magánhálózatot általában egy nagyobb cég telephelyei között szokták kiépíteni, hiszen így megtakarítható a telephelyeket összekötő bérelt vonal költsége.

Aktív hálózati támadások

Akkor beszélünk aktív támadásról, ha a támadó valamilyen szinten beleszól a két fél közti adatáramlásba. Például a támadó a két gép között helyezkedik el, a forgalom rajta keresztül folyik és az átáramló adatfolyamot módosíthatja. Az aktív támadások sokfélesége, valamint a védekezés különleges volta miatt itt csak néhány formájáról ejthetünk szót.

A jó, a rossz és a jó

Bizalmas adatok továbbítására mindig használj titkosított csatornát!
Tegyük fel, egy cégnek Linux-alapú könyvelőrendszere van. Az arra illetékesek telnet protokoll segítségével belépnek a kiszolgálóra, és ott végzik el a cég könyveléssel, illetve átutalással kapcsolatos tevékenységeit. A cégnél dolgozó *Terep Járó* úgy szeretne némi pluszjövedelemhez jutni, hogy amikor a főkönyvelő belép a könyvelési rendszerbe, akkor a főkönyvelő gépével elhiteti, hogy ő a könyvelést tartalmazó kiszolgáló, a kiszolgálóval pedig azt, hogy ő a főkönyvelő gépe. Így mindkét gép úgy fog hozzá fordulni, hogy azt hiszi, a másik rendszerrel beszél. Így Járónak lehetősége nyílik a könyvelő által végrehajtott utasítások közé csempészni néhány kisebb átutalást. Hogyan történhet ez meg? Az Ethernet hálózat mindamellett, hogy könnyen lehallgatható, könnyen meg is téveszthető.
A példában szereplő helyzetet a szaknyelv „IP spoofing”-ként (IP-megtévesztés) emlegeti, és a „man-in-the-middle” (középre belépő) támadások kategóriájába tartozik (lásd *3. ábra*). A hiba oka egyértelműen az Ethernet hálózati protokolljának hiányossága. Ha a rendszerben meg tudnánk teremteni annak feltételeit, hogy a két gép közt áramló adatokhoz más ne férhessen hozzá, a közöttük lévő hálózati elemek biztonsága sérthetetlen legyen, akkor már csak kis valószínűséggel támadható a rendszer alacsony szinten. Újra figyelmeztetek azonban mindenkit: a hálózati eszközök (jelelosztók, hálózati kapcsolók) nem biztonsági eszközök. Ha az eszköz alkalmas is a biztonsági feladatok ellátására, a beállításainak tökéleteseknek kell lenniük ahhoz, hogy biztonságosnak lehessen mondani, és még így is kerülnek a felszínre olyan hibák a biztonsági levelezőlistákon, amelyek elgondolkodtatóak. Ha azonban az adatátvitelt titkosított csatornára bízzuk, ahol a két rendszer mindenekelőtt azonosítja egymást (ilyen például az ssh), akkor egy középen elhelyezkedő támadónak csak akkor van esélye, ha már az első kapcsolatfelvétel előtt a két gép között van, és folyamatosan felügyeli a két gép közt zajló forgalmat. Ez igen komoly előkészítést igényel, és kikerülhető, ha a két gép egymás azonosítására szolgáló kulcsait első alkalommal nem a hálózaton át cseréli ki, hanem a két rendszer gazdája a kulcsokat független fizikai csatornán – például lemezen – juttatja el a egymáshoz, valamint használat előtt hitelesíti. Utóbbi megoldás biztonsági szakemberhez méltó jól fejlett paranoiáról árulkodik. :)



3. ábra A gépek megtévesztésével a támadón keresztül zajlik az adatátvitel

Záró szavak

Hálózati szintű támadásokkal foglalkozunk a következő alkalommal is, akkor azonban már a Linux-rendszer beállításaira is kitérünk. Megtárgyaljuk, hogy milyen beállításokkal és intézkedésekkel csökkenthető a sikeres hálózati támadások esélye. Szó lesz arról, hogy miként tanácsos beállítani egy Linux-rendszer csomagszűrőjét behívás esetén, valamint a cégek szolgáltatásokat is adó kiszolgálóin.

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.

A főszerkesztő ezúton kér elnézést a tisztelt olvasótól és a szerzőktől, ha úgy érzik, hogy a szerzők „technicus terminusainak” magyarítása csorbította a szöveg érthetőségét.