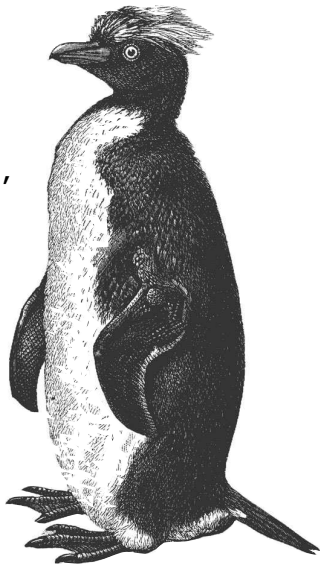
DMZ hálózatok tervezése és használata

Bemutatjuk, hogyan gondoskodhatunk azokról a szolgáltatásainkról, amelyek sérülékeny hálózatokkal is kapcsolatba kerülhetnek.



A DMZ-típusú (DeMilitarized Zone – szabad terület) hálózati felépítés manapság a tűzfalak egyik leghasznosabb kiegészítő eszköze. Olyan hálózatrészről van szó, amelyben elhelyezhetjük az összes nyilvánosan hozzáférhető szolgáltatásunkat. Egyrészt így könnyebben szemmel tarthatjuk ezen szolgáltatások működését, másrészt pedig elszigetelhetjük azokat a belső hálózattól. A szabad területek, a bástyakiszolgálók és a Linux együtt kifejezetten jó csapatot alkotnak.

Mit is jelent a szabad terület? Megtervezhető-e többféleképpen is? Vajon minden internet-szolgáltatónak szüksége van szabad területekre? Ezekkel a kérdésekkel régebben nem foglalkoztunk, éppen ezért most átfogóbban vizsgáljuk a szabad területek biztonsági kérdéseit.

Ha esetleg úgy gondoljuk, hogy a jelenleg használt tűzfalrendszer, szabad terület nélkül tökéletesen megfelel az igényeinknek, akkor is célszerű végigolvasni ezt a cikket. Minden olyan gép és szolgáltatás – akár szabad területen helyezkedik el, akár nem –, amely nem megbízható hálózatokkal is kapcsolatba kerülhet, különleges odafigyelést igényel, és a cikkben bemutatott ötletek között számos olyan is van, amelyik DMZ-, és szokványos környezetben egyaránt használható.

A szóhasználatról

Mielőtt továbblépünk tisztázzunk néhány kifejezést. Elképzelhető, hogy a felsorolt meghatározások némelyikét korábban másképp használtuk, éppen ezért szeretném már az elején leszögezni, hogy ebben a cikkben milyen értelemben hivatkozom rájuk:

- *Szabad Terület (DMZ):* nyilvánosan is elérhető kiszolgálókat tartalmazó hálózatrész, amely megfelelő módon elszigetelt a „belső” hálózattól.
- *Belső hálózat:* az a hálózatrész, amelyet szeretnénk megvédeni – a végfelhasználók rendszerei, a bizalmas adatokat tartalmazó kiszolgálók és az összes többi olyan rendszer, amelyet szeretnénk elzárni a kívülről érkező kapcsolatok elől. Védett területnek is nevezhetjük.
- *Tűzfal:* olyan rendszer vagy eszköz, amely az egyik hálózatot elszigeteli a másiktól. Ez lehet egy útválasztó, azaz olyan számítógép, amely hálózati forgalmat irányító programot futtat, esetleg egy ilyen rendeltetésű egyedi eszköz, vagy bármilyen más rendszer, amely csomagszűrésre, proxyszolgáltatások biztosítására és egyéb, hozzáférés-vezérléshez tartozó feladatok elvégzésére alkalmas. A cikk során egyetlen, többkártyás számítógépre gondolunk.
- *Többkártyás* számítógép: egy olyan számítógép, amely egynél több hálózati csatlakozóval rendelkezik.
- *Bástyagép:* olyan rendszer, mely nyilvánosan hozzáférhető szolgáltatásokat nyújt, de önmaga nem tűzfal. Általában a bástyagépeket a szabad területen helyezzük el (bár máshol is elhelyezhetjük). A bástya kifejezés arra vonatkozik, hogy az operációs rendszer valamilyen módon megerősített, ez a feltétel azonban nem mindig teljesül.
- *Csomagszűrés:* olyan eljárás, mely az IP-csomagok fejlécében tárolt adatok (forrás IP-cím, cél IP-cím, forráskapu és célkapu) megvizsgálása után továbbengedi, vagy pedig eldobja az adott csomagot. Ez az eljárás a csomagok tartalmával nem foglalkozik, azaz a hibás felépítésű csomagokat nem feltétlenül veszi észre (feltéve, hogy a csomag fejléce megfelelő adatokat tartalmaz). Szinte minden tűzfal végez csomagszűrést, ez azonban önmagában még nem ad elegendő védelmet minden támadással szemben. A legtöbb útválasztó (és sok gyenge tűzfal) kizárólag csomagszűréssel védelmezi a rábízott hálózatot. (Lásd e témával kapcsolatban a 34. oldalon található Könnyű álom című cikket.)
- *Proxy:* olyan szolgáltatás, mely közvetítő szerepet tölt be a belső és a külső gépek között. Proxy használata közben a felhasználó nem közvetlenül a kiszolgálóval tartja a kapcsolatot, a proxy „közvetít”. Az eljárás lehetőséget ad kifinomultabb szűrések használatára, mivel itt az alkalmazási réteg adatait elemezhetjük (ez a módszer hatékonyabb az egyszerű csomagszűrésnél). Vannak olyan tűzfalak, amelyek kifejezetten proxykra épülnek.
- *Állapotvizsgálat:* legegyszerűbb formájában arra a háromlépéses kézfogásnak a megfigyelésére vonatkozik, amely egy adott TCP-kapcsolat felépülésekor zajlik a gépek között (gép1: SYN, gép2: SYN+ACK, gép1: ACK). Kifinomultabb változata magában foglalja ennek és az ezeket követő összes többi állapot adatainak nyomon követését. Az utóbbi változat sokkal kevésbé elterjedt, mint az első.

Ez a rengeteg szakkifejezés elsőre talán egy kicsit nagy falatnak tűnhet, viszont nagyon hasznos az ismeretük. Most már készen állunk arra, hogy beássuk magunkat a Szabad Területek felépítésébe.

A tűzfaltípusok és a DMZ hálózatok lehetséges szerkezete

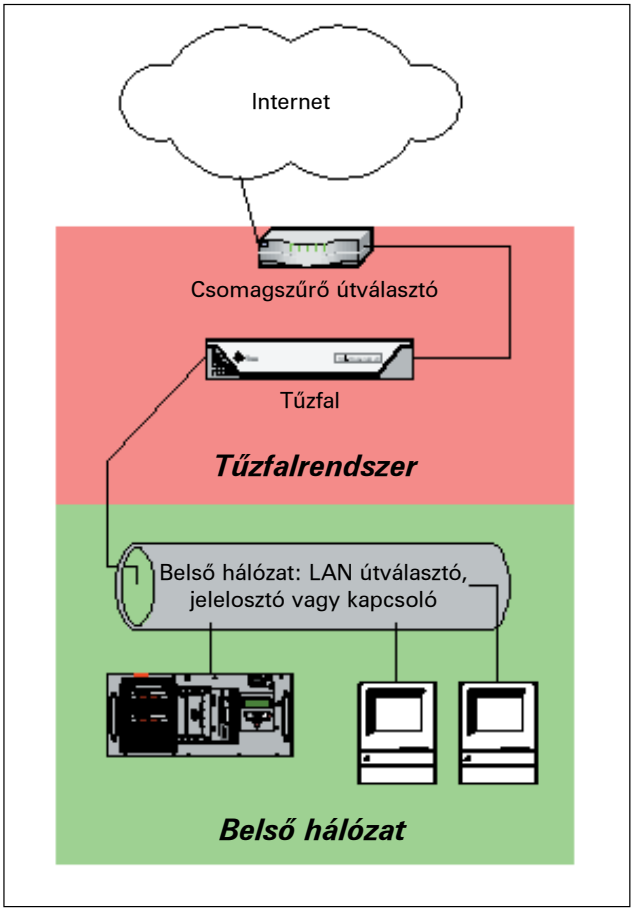
A drága kereskedelmi tűzfalak világában a tűzfal kifejezés szinte mindig egyetlen olyan számítógépet vagy különleges eszközt jelöl, amely több hálózati csatlakozással bír. Ez a meghatározás a gyengébb megoldásokra is ráhúzható: a hálózati kártyák manapság már igen olcsók, akárcsak a PC-k.

Már elmúltak azok a napok, amikor egyetlen számítógép önmagában nem volt képes arra, hogy egy nagyobb hálózatban nyomon kövesse az összes bejövő és kimenő csomagot. Akkoriban még kizárólag az útválasztók kaphattak helyet a hálózatok elleni támadások első védelmi vonalában (az egyszerű számítógépek nem).

Mára a helyzet teljesen megváltozott. Manapság már az erős internet-kapcsolatokkal rendelkező szervezetek is többkártyás tűzfalakkal igyekeznek megvédeni hálózataikat. Jelenleg már a viszonylag lassú PC-k is képesek arra, hogy kifinomult ellenőrzést végezzenek akár T1-es (1,544 Mb/mp) hálózati kapcsolatokon is.

Az *1. ábrán* azt a tűzfalszerkezetet láthatjuk, amellyel manapság a leggyakrabban találkozhatnunk. Ahogy azt az ábrán is láthatjuk, a biztonság első, de nem kizárólagos védelmi vonalában egy csomagszűrő útválasztó kap helyet. Közvetlenül az útválasztó mögött találhatjuk magát a tűzfalat (ez lehet Sun SparcStation is), melyen RedHat fut. A belső hálózatnak sem az Internettel, sem

pedig a külső útválasztóval nincs közvetlen kapcsolata: minden hálózati forgalomnak át kell haladnia a tűzfalon.
Véleményem szerint minden külső útválasztónak tartalmaznia kell valamilyen csomagszűrést. Még ha az útválasztóhoz drága, és lehetőség szerint jól beállított és karbantartott tűzfal csatlakozik, akkor sem árt, ha bizonyos veszélyekkel szemben többszörösen is biztosítjuk magunkat.
Mi a baj az első ábrával? Mi hiányzik róla? Mindössze annyit állítottam, hogy ez a szerkezet igen elterjedt, azt viszont nem mondtam, hogy tökéletes. Az olyan nyilvános szolgáltatásoknak, mint az SMTP (elektronikus levelezés), a DNS vagy a HTTP szintén át kell menniük a tűzfalon, vagy pedig magán a tűzfalon kell elhelyezni ezeket.
Az a tény, hogy az ilyen jellegű hálózati forgalmat is a tűzfalon keresztül bonyolítjuk, önmagában még nem növeli meg annak az esélyét, hogy a belső hálózat számítógépeit támadás érje, jelentősen súlyosbítja azonban az ilyen támadás következményeit. A nyilvános szolgáltatásoknak a tűzfalon történő elhelyezése nem feltétlenül rossz ötlet, mert hol lehetnének nagyobb biztonságban ezek a szolgáltatások, mint magán a tűzfalon. Ebben az esetben azonban nyilvánvaló, hogy a megfelelő teljesítmény eléréshez a tűzfalnak minden létező erőforrását a csomagok ellenőrzésére és továbbítására kell fordítania. (Ez alól van néhány kivétel, amiről rövidesen részletesebben is beszélünk majd.) Emellett ilyenkor kényesebbé válik a tűzfal karbantartása is, hiszen érzékeny programok is futnak rajta.
Hol tudjuk tehát elhelyezni nyilvános szolgáltatásainkat úgy, hogy azok sem közvetlenül, sem pedig közvetve ne jelentsenek veszélyt a belső hálózatra, és ne terheljék túl a tűzfalat sem? Pont erre való a szabad terület. Legegyszerűbb formájában Szabad Területnek tekinthetünk minden olyan hálózatot, amely kívülről elérhető, a belső hálózattól azonban el van szigetelve. Eszményi esetben azonban a szabad terület is egy tűzfal védelmét élvezi. A *2. ábrán* ezt az eszményi szerkezetet láthatjuk. Ezen az ábrán a tűzfal szerepét egy háromkártyás számítógép tölti be. A nyilvános szolgáltatásokat biztosító gépek egy saját hálózatban helyezkednek el, amely a tűzfalhoz kapcsolódik. A hálózat többi része is ezt a tűzfalat használja, azonban másik hálózati felületen keresztül csatlakozik ahhoz. Ha megfelelően van beállítva, akkor a tűzfal más és más szabályokat alkalmaz bármelyik hálózati részből bármelyik rész felé áramló forgalom kiértékelésére.
Úgy tűnik, hogy ez a megoldás sokkal nagyobb felügyeleti költséggel jár, mintha a nyilvános szolgáltatásokat a belső hálózatban, vagy pedig magán a tűzfalon helyeznénk el, valójában azonban sokkal egyszerűbb, mivel a DMZ-t egyetlen egységként kezelhetjük. Ilyen jellegű hálózatot természetesen sokféleképpen összeállíthatunk, a *3. ábrán* rögtön két példát is láthatunk. A védett alhálózat (Screened Subnet) biztonsága teljes egészében a külső és a belső útválasztók biztonsági rendszerétől függ. A hálózat belseje közvetlen kapcsolatban áll a külvilággal, és ezen az úton a csomagok szabad áramlását kizárólag egy útválasztó csomagszűrő szabályai gátolhatják meg.
A 3. ábra jobb oldalán látható kiépítésnek a „Vergődés a szél-ben” nevet adtam. Ebben az esetben a belső hálózatot teljes értékű tűzfal választja el az Internettől, a szabad terület azonban a tűzfalon kívül helyezkedik el, valamint védelmét kizárólag a csomagszűrő útválasztó biztosítja.
Mindkét megoldással találkozhatunk a tűzfalakkal foglalkozó könyvekben (elképzelhető, hogy ott más néven szerepelnek), véleményem szerint azonban ezek a rendszerek túlságosan nagy bizalmat fektetnek az útválasztóba. Ez a túlzott bizalom több okból is veszélyes: egyrészt elképzelhető, hogy a tűzfal és az útválasztó nem ugyanannak a rendszerfelügyelőnek a hatáskörébe tartozik. Lehet, hogy az útválasztóért felelős személy nem használ kellőképpen erős jelszavakat, nem fektet elegendő hangsúlyt a hozzáférés-szabályozási listákra. Sőt, még modemet is elhelyezhet az útválasztóban mondván, így a gyártó könnyebben karbantarthatja. Ezenkívül az útválasztóra



1. ábra Többkártyás tűzfal

általában sokkal könnyebb behatolni, mint egy jól beállított számítógépre (az útválasztókat például szinte minden esetben el lehet érni telnet protokoll segítségével, ami egyáltalán nem nevezhető biztonságosnak). Továbbá a csomagszűrés valójában nem alkalmas arra, hogy segítségével kifinomult módon szabályozhassuk a hálózati forgalmat. Még egy nyílt forráskódú, ingyenes tűzfalprogram is támogathatja az IPSEC, az alkalmazásszintű proxyk, az állapotvizsgálat, a Radius hitelesítés és még sok más olyan szolgáltatás használatát, amelyekkel az útválasztókon nem találkozhatunk. Egyszerűen összefoglalva: az útválasztókat arra tervezik, hogy irányítsák a forgalmat, nem pedig arra, hogy megvédjék a hálózatot.
Mi a helyzet a Cisco Pixszel? A Pix tűzfal is útválasztó ugyan, amit azonban a Cisco IOS operációs rendszer megerősített, biztonságközpontú változatával szereltek fel. Habár erősen támaszkodik az egyszerű csomagszűrésre, rengeteg olyan kiegészítő szolgáltatással is ellátták, amelyek alkalmassá teszik arra, hogy jól beállítva nagyszerű tűzfal lehessen. Amikor megkérdőjelezem az útválasztók tűzfalként történő felhasználását, akkor az általános célú útválasztókra gondolok.
Összefoglalva, a szabad terület szerkezete elsősorban a tűzfal(ak) felépítésétől függ. Egy többkártyás tűzfal köré olyan hálózatot építhetünk, amelyben a DMZ hálózatrész az Internettől és a belső hálózattól egyaránt teljes mértékben el van választva (lásd 2. ábra).

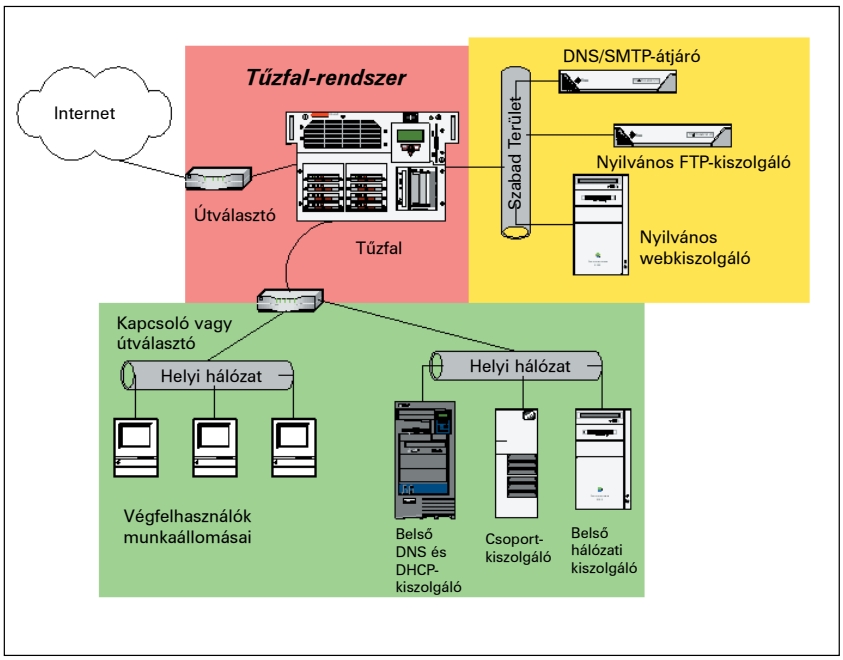
Mi legyen a Szabad Területen?

Ha már eldöntöttük, hogy hol helyezzük el a DMZ hálózatot, pontosan meg kell határoznunk azt is, hogy mit fogunk elhelyezni benne. Célszerű minden nyilvánosan elérhető szolgáltatást ide helyezni. Túlságosan sokszor találkozom olyan hálózatokkal, amelyekben egy

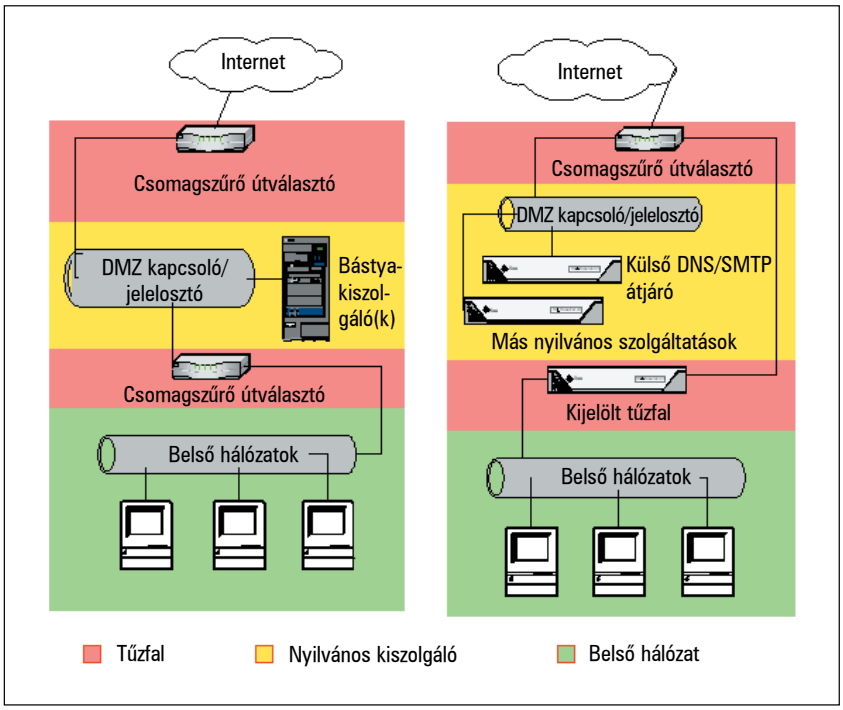
vagy több – biztonsági szempontból nézve kényes – szolgáltatást a tűzfalon keresztül juttatnak el belső géphez annak ellenére, hogy a rendszerben helyet kap egyébként nagyszerűen működő DMZ hálózatrész is. Általában olyan programokról van szó, mint amilyen például az MS-Exchange, amit nem láttak el az internetes alkalmazásoknál megkövetelhető biztonsági alrendszerrel.

Egyetlen ilyen alkalmazás elég ahhoz, hogy rést nyisson az egyébként biztonságos rendszeren: mindössze annyi kell, hogy valamelyik alkalmazásunkat egy egyszerű átmeneti tártúlcsordulással meg lehessen támadni, és a hívatlan látogató máris hozzáférhet az összes olyan géphez, amely az adott gépről elérhető. Egy ilyen esetben nem mindegy, hogy a megtámadott gépről csak a szabad terület gépeihez lehet hozzáférni, vagy pedig a belső hálózat összes gépéhez. Ezt a szempontot nem lehet eléggé kihangsúlyozni: a szabad terület legnagyobb értéke az, hogy szétválaszthatjuk a külvilág és a belső hálózat számára szükséges szolgáltatásokat.

Elképzelhető, hogy az a személy, aki a tűzfalon keresztüláramló szolgáltatásért felelős, más, mint a tűzfalat és a szabad terület kiszolgálóit kezelő szakember. Meglehet, hogy az előbbi nem ügyel annyira a biztonságra, mint amennyire kellene. Ez már önmagában is elegendő ok arra, hogy a nyilvános kiszolgálókat a Szabad Területen helyezzük el, mivel így ezek a gépek a tűzfal rendszergazdájának felügyelete alá kerülnek, aki ideális esetben rendkívül kényes a gépek biztonságára. Ez azt jelenti, hogy a vállalati levelezést, a névszolgáltatást és a többi fontos szolgáltatást szintén a DMZ hálózatban kell elhelyezni? Egyáltalán nem! A megoldás ebben az esetben az, hogy a szolgáltatást szétválasztjuk külső és belső részre (lásd 2. ábra). A DNS-t például fel kell bontanunk külső és belső DNS-re. A külső DNS adatbázisa, amely az Internetről is elérhető, csak a nyilvánosan is hozzáférhető gépekről tartalmazhat adatokat. A nem nyilvános gépek adatait pedig a másik, belső DNS adatbázisba kell elhelyeznünk, amely a külső gépek számára tökéletesen láthatatlan. Ugyanez a helyzet az elektronikus levelezéssel is. A belső levelezést (a belső gépekről belső gépekre elküldött leveleket) szigorúan belső gépeknek kell kezelniük, az Internetre kimenő vagy onnan beérkező leveleket pedig egy szabad területen elhelyezett kiszolgálónak (ezt a gépet SMTP-átjárónak is szokás nevezni).



2. ábra Többkártyás tűzfal szabad területtel



3. ábra A védett alhálózat és a „Vergődés a szélben" változatok

Szinte minden olyan szolgáltatás szétbontható két részre, amely saját és nyilvános módon egyaránt használható. Míg ez látszólag sok többletmunkával jár, valójában egyáltalán nem jelent külön megterhelést, sőt szabadságot ad, mivel lehetővé teszi, hogy a belső szolgáltatások kialakításakor a kényelemi szempontokra, a külső szolgáltatások esetében pedig a teljesítményre és a biztonságra összpontosítsunk. Fontos szempont az is, hogy ily módon Linux, OpenBSD és más nyílt forráskódú programokat is beépíthetünk az egyébként kereskedelmi programokra épülő környezetünkbe. Mondani sem kell, hogy a nyilvános használatra szánt szolgáltatásoknak kizárólag a szabad területen kell megjelenniük. Összegezve az eddigieket: az összes nyilvános szolgáltatást, beleértve a kívül és belül egyaránt használt szolgáltatások nyilvános részét is (feltéve, hogy az adott szolgáltatás felbontható két részre), kivétel nélkül a DMZ hálózatrészben kell elhelyezni.

Az erőforrások megosztása a DMZ hálózatban

Minden nyilvános szolgáltatás a szabad területre kerül. De külön gépre lesz szükség minden egyes szolgáltatáshoz? Esetleg bizonyos szolgáltatásokat elhelyezhetünk magán a tűzfalon is? Használjunk-e jelelosztót vagy hálózati kapcsolót a szabad területen?

Az utolsó kérdés a legkönnyebb: mivel a kapcsolt kapuk ára évről évre csökken, a kapcsolók használata minden hálózatban, így a DMZ hálózatrészekben is ajánlott. A kapcsolók két tekintetben is nagyon hasznosak: biztonsági szempontból vizsgálva használatuk azért előnyös, mert lehetetlen lehallgatni azt a forgalmat, amely el sem jut a kapcsoló adott kapujához. Mivel a szabad területen lévő gépeket nagyobb valószínűséggel éri majd támadás, mint a belső hálózat gépeit, ez a nézőpont igen fontos. Nemcsak azt kell végiggondolnunk, hogyan védhetjük meg ezeket a gépeket a támadástól, hanem tisztán kell látnunk az esetleg sikeres támadás következményeit is. A kapcsoló természetesen a teljesítmény tekintetében is jobb választás, mint a jelelosztó. Ne feledkezzünk meg azonban arról, hogy a kapcsolók teljesítménye korlátozott. Ha például a kapcsolónk másodpercenként legfeljebb 800 megabit továbbítására képes, akkor hiába van rajta tíz, egyenként 100 Mb/mp sebességű kapu, akkor sem fog tudni másodpercenként 1000 megabitet feldolgozni. Mindezek ellenére leszögezhetjük, hogy még az alacsonyabb osztályba tartozó kapcsolók is bőven túlszárnyalják a velük egy szinten lévő jelelosztók teljesítményét. Ettől még elképzelhető, hogy szabad területünk kiszolgálásához egy jelelosztó is elegendő. Ez elsősorban attól függ, hogy hány gép van a hálózatrészben, ezek mekkora forgalmat bonyolítanak, és mennyire aggódunk amiatt, hogy az egyik gépen keresztül esetleg a hálózat többi gépét is feltörhetik.

A másik két kérdést általában úgy is megválaszolhatjuk, hogy a biztonsági szempontok helyett más tényezőket helyezünk előtérbe (például költség, várható terhelés, hatékonyság stb.), feltéve természetesen, hogy a szabad területen lévő gépek már megfelelően biztonságosak. Figyeljünk arra is, hogy a Szabad Területről kimenő, illetve az oda beérkező hálózati forgalmat szabályozó tűzfal is a lehető legszigorúbb módon legyen beállítva.

A DMZ gépek biztosításának irányelvei

Nyilvánvalónak tűnik, hogy a szabad terület gépeit is védenünk kell. Ennek ellenére sokszor találkozom olyan szervezetekkel, amelyek kellőképpen igényesek ahhoz, hogy szabad területet tartsanak fenn, annyira azonban nem, hogy gondoskodjanak ennek a hálózatnak a biztonságáról. A jó hír az, hogy egy kis időráfordítással jelentős mértékben csökkenthetjük rendszerünk sebezhetőségét.

Az operációs rendszerből, a programokból és a rendszermagból is mindig a legfrissebb megbízható változatot használjuk, és azonnal telepítsük a különböző biztonsági hézagokat befoltozó javítócsomagokat, amint azok megjelennek!

Ha mindenki megfogadná ezt az egyszerű és magától értetődő tanácsot, akkor a ➲ www.hackernews.com lapon megtalálható feltört weblapok listája valószínűleg sokkal rövidebb lenne. Általában elmondható, hogy a hálózatokba történő betörést a legtöbb esetben az teszi lehetővé, hogy az adott hálózatban valamely programnak nem a legfrissebb változata fut. Mindannyian tisztában vagyunk ezzel, azonban nem mindig vagyunk hajlandók időt szánni a gondok orvoslására.

Kapcsoljuk ki az összes olyan szolgáltatást és démont, amelyekre nincs szükségünk. A használaton kívüli programok karbantartása általában nem megfelelő, így nyilvánvaló támadási felületet biztosítunk a betörők számára. A gond nagyon könnyen megoldható. A rendszer telepítésekor egyszerűen töröljük le, vagy pedig nevezzük át az összes felesleges hivatkozást a /etc/rc.d/ megfelelő könyvtárában.

Ha például webkiszolgálót szeretnénk telepíteni, de nincs szükség arra, hogy a gép DNS-szolgáltatást is nyújtson, akkor kiadhatjuk a következő parancsot:

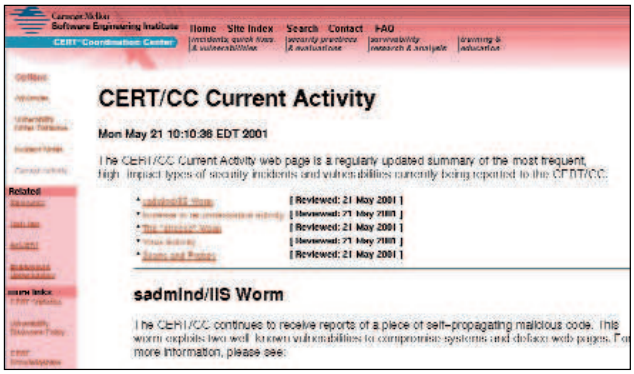
```
mv /etc/rc.d/rc2.d/S30named
/etc/rc.d/rc2.d/disabled_S30named
```

➲ http://www.atstake.com/security_news/

(A szolgáltatások a különböző Linux-változatok alatt más és más helyen engedélyezhetők, illetve tilthatók le.)

Amikor a felesleges szolgáltatások letiltásán dolgozunk, különösen figyeljünk oda az alábbi szolgáltatásokra:

- *RPC:* a Sun távoli eljárásvezérlés (Remote Procedure Control – RPC) protokollja – ez manapság szinte minden Unix-változatban megtalálható – lehetővé teszi, hogy az rsh, rcp, rlogin, nfs stb. programok segítségével utasításokat hajtsunk végre távoli rendszerben. Ez a protokoll sajnos nem biztonságos, főleg nem a szabad területeken. Ne nyújtsunk tehát ilyen szolgáltatásokat a külvilág számára. Ha szükségünk van ezekre a szolgáltatásokra, akkor használjuk az ssh-t, ezt ugyanis kifejezetten az rpc szolgáltatások felváltására tervezték. Töröljük (vagy nevezzük át) az nfsd és az nfsclientd állományokat a /etc/rc.d könyvtár alatt fellelhető összes alkönyvtárban, és távolítsuk el az r* parancsokra vonatkozó sorokat a /etc/inetd.conf fájlból is.
- *inetd:* az Internet démon (inetd) kiválóan alkalmas arra, hogy figyelje a rábízott kapukat, és szükség esetén elindítsa a kapukhoz tartozó szolgáltatásokat. Ez a hasznos kis szolgáltatás azonban még az igen részletes naplózási lehetőség ellenére sincs olyan biztonságos, mintha az egyes szolgáltatásokat démonként futtatnánk. Egy FTP-kiszolgáló esetében például semmi okunk nem lehet arra, hogy ne futtassuk állandóan az FTP-folyamatokat. Sőt, a legtöbb olyan szolgáltatás, amely az inetd.conf fájlban alapértelmezés szerint engedélyezve van, teljesen felesleges vagy pedig nem biztonságos (esetleg mindkettő). Ha mindenképpen szükségünk van az inetd használatára, akkor a /etc/inetd.conf fájl átszerkesztésével tiltsuk le az összes olyan szolgáltatást, amelyre nincs szükségünk (és azokat is, amelyekről még soha sem hallottunk). Sok olyan rpc szolgáltatás van, amely az inetd.conf-ból indul.
- *linuxconfd:* annak ellenére, hogy a linuxconf (olyan eszköz, melynek segítségével a rendszergazdák távolról is hozáférhetnek a géphez) jelenlegi változata egyetlen olyan ismert hibát sem tatalmaz, amit esetleges támadás során fel lehetne használni, a CERT jelentése szerint a szolgáltatás pásztázásával felfedhetők a rendszer egyéb gyengeségei
  ➲ http://www.cert.org/current/current_activity.html
- *sendmail:* sokan azt gondolják a sendmail szolgáltatásról – amely alapértelmezés szerint engedélyezve van a legtöbb Unix-változatban –, hogy azokon a gépeken is szükséges, amelyek kizárólag saját maguknak küldenek leveleket (felügyeleit célból). Ez azonban nem igaz, a sendmail (vagy postfix, qmail stb.) szolgáltatásra csak azokon a gépeken van szükség, amelyek más gépekkel is váltanak leveleket. A sendmail szolgáltatás általában a /etc/rc.d/rc2.d vagy a /etc/rc.d/rc3.d alatt kerül elindításra.
- *telnet, FTP és POP:* Ennek a három protokollnak megvan az a közös vonása, hogy mindegyikük egyszerű szöveg formájában



➲ http://www.cert.org/current/current_activity.html

továbbítja a felhasználók nevét és jelszavát a hálózaton keresztül. A telnet és az FTP helyett használhatjuk az ssh-t, illetve ennek a fájlátvitelre alkalmas scp nevű segédprogramját. Az elektronikus leveleket önműködően továbbíthatjuk egy másik géphez, meghagyhatjuk a szabad területtel bíró gépen úgy, hogy csak ssh-n keresztül lehessen hozzáférni, vagy a POP felhasználásával továbbíthatjuk az ssh-hoz. Mindhárom szolgáltatást az inetd indítja el.

Használjunk chroot-ot, ahol csak lehet!

Egyes démonokat (ilyen például named) a chroot börtönében is futtathatunk (ebben az esetben a démon a chroot mellett megadott könyvtárat tekinti gyökérkönyvtárnak, és nem is tud kilépni abból). Ez nagyon értékes biztonsági szolgáltatás, ha ugyanis a chroot-tal futtatott szolgáltatást sikerül is feltörni valahogy, a betörő akkor sem fog hozzáférni a szolgáltatás gyökérkönyvtárán kívül eső fájlokhoz. Linux alatt bármilyen parancsot futtathatunk ezzel a módszerrel: egyszerűen adjuk ki a `chroot` *`elérési_út`* utasítást. Ha például a `bubba -v plop` parancsot úgy szeretnénk futtatni, hogy az ne tudjon kilépni a /var/bubba könyvtárból, akkor gépeljük be a következőt:

```
chroot /var/bubba /usr/local/bin/bubba -v plop
```

Ebben az esetben azokat a rendszerfájlokat, amelyekre a programnak szüksége van, be kell másolnunk egy olyan könyvtárba, amelyhez a program hozzáférhet. Ha például a fenti parancs olvasni szeretne a /etc/passwd fájlból, akkor ezt a fájlt át kell másolnunk a /var/bubba/etc könyvtárba. A másolatnak természetesen elég azokat az adatokat tartalmaznia, amelyekre valóban szükségünk van. Ha például a bubba parancsot csak az „anonymus” nevű felhasználó fogja futtatni, akkor a /var/bubba/etc/passwd fájlnak csak egyetlen sort kell tartalmaznia (például nobody::50:50:Anonymous user::/bin/noshell).

Futtassuk a szolgáltatásokat a lehető legalacsonyabb jogosultsági szinten!

Vannak ugyan olyan démonok, amelyeket csak rendszergazdaként futtathatunk, manapság azonban egyre több olyan program létezik, amelyeket alacsonyabb jogosultsággal rendelkező felhasználók is futtathatnak. Például a Postfix (mely a sendmail szolgáltatást hivatott felváltani) általában egy postfix nevű, alacsony jogosultsági szinttel rendelkező felhasználóként fut.

A módszer előnye hasonló, mint a chroot esetében: ha az esetleges betörő ilyen szolgáltatáson keresztül jut be a rendszerbe, akkor alacsonyabb jogosultságokkal rendelkezik majd (remélhetőleg jóval alacsonyabbakkal), mint a rendszergazda.

Töröljük vagy tiltsuk le a felesleges azonosítókat!

Egyes Linux-változatok alapértelmezés szerint meglehetősen hosszú /etc/passwd fájlokat tartalmaznak olyan programcsomagok kedvéért, amelyeket többnyire még csak nem is telepítettünk. A hordozható számítógépemre telepített SuSE Linux /etc/passwd fájljában például 22 felesleges bejegyzést találtam. Távolítsunk el minden olyan bejegyzést, amelyekre nincs szükségünk.

A naplózás beállítása és a naplók ellenőrzése:

Szintén olyan dolog, amiről tudjuk, hogy mennyire fontos, sokszor mégis megfeledkezünk róla. A nem létező naplókat nem is lehet átnézni, azokból a naplókból pedig, amelyeket nem olvasunk át, semmit sem fogunk tanulni. Gondoskodjunk róla, hogy a fontos szolgáltatások működését megfelelő módon naplózzuk. Tudnunk kell, hogy hol tárolódnak a létrehozott naplófájlok és azt is, hogy mi történik velük, amikor túlságosan nagyra nőnek. Nézzük át rendszeresen az éppen használatos naplófájlokat!

Ez utóbbi feladatban a `grep` parancs nagy segítséget jelenthet, a `cat` pedig önmagában általában túlságosan sok adatot zúdít ránk.

A naplók figyelését különböző parancsfájlok segítségével önműködően is elvégezhetjük. A parancsfájlok arra is alkalmasak, hogy figyeljük a fontosabb rendszerbeállításokat tartalmazó fájlok változásait. Ha több DMZ gép működését szeretnénk szemmel tartani, akkor nem kell egyesével végignéznünk az egyes gépeken létrehozott naplófájlokat, mivel a syslogd segítségével egyetlen rendszerbe is összegyűjthetjük azokat. A syslog démon a helyi folyamatok naplózása mellett képes távoli gépekről érkező naplóbejegyzések fogadására is. Ha például DMZ hálózatunk két gépből áll (Bobo és Rollo), és a naplófájlokat egyetlen helyen szeretnénk összegyűjteni, akkor módosítsuk a Bobo gépen a /etc/syslogd.conf fájlt úgy, hogy kizárólag a következő sort tartalmazza:

```
*.*      @rollo
```

Ennek hatására a Bobo gépen futó syslogd minden naplóbejegyzést a Rollohóz továbbít majd.

Annak ellenére, hogy az imént bemutatott szolgáltatás nagyon hasznos, megvannak a maga kis biztonsági gondjai. Ha valakinek sikerül betörnie a Rollo rendszerbe, akkor hozzájut a Bobo naplófájljaihoz is, és így akár olyan adatok is megszerezhet, amelyek felhasználásával azután a másik rendszert is könnyedén feltörheti.

Használjuk a tűzfal biztonsági házirendjét és az IP-hamisításokat megelőző szolgáltatásait!

Teljesen természetes, hogy szeretnénk odafigyelni arra, hogy milyen adatok kerülnek be kívülről a szabad területre. Ugyanolyan fontos azonban az is, hogy megfelelően korlátozzuk a szabad területről a belső, illetve a külső hálózatba áramló adatforgalmat is. Az előzőre azért van szükség, hogy a szabad terület megtámadása esetén meg tudjuk védeni a belső hálózatot, az utóbbi pedig azért fontos, hogy elejét vehessük annak, hogy valaki egyetlen, a szabad területen található feltört gépről támadjon meg más hálózatokat.

Természetes, hogy nem szeretnénk, ha bármi bejutna az Internetről a belső hálózatba. Bármi történjen is, a tűzfal biztonsági rendszere hatékonyabban működik majd, ha a tűzfal különbséget tud tenni a megbízható és a kétes eredetű IP-címek között. Ha erre nem képes a rendszerünk, akkor előfordulhat, hogy külső felhasználó az IP-cím meghamisításával csomagokat csempésszen be a rendszerünkbe.

A legtöbb tűzfalon nincs alapértelmezés szerint engedélyezve ez a szolgáltatás. Még ha támogatja is a tűzfal ennek használatát, valószínűleg külön engedélyeznünk kell azt.

Igazán megéri az erőfeszítést.

Mick Bauer (mick@visi.com) hálózati biztonsággal foglalkozó szaktanácsadó. 1995 óta a Linux elkötelezett híve, 1997 óta pedig OpenBSD prófétaként tevékenykedik. Mick szívesen fogad minden kérdést, és megjegyzést.