A hét vezér: biztonsági eszközök

Attól, hogy újabb és újabb programokkal tömjük meg, a gépünket nem lesz nagyobb biztonságban. Az ajánlott hét csomag segítségével megtanulhatjuk, hogyan állíthatunk össze, például biztonsági házirendet.

Linux alá számtalan kiváló, ingyenes és nyílt forrású biztonsági eszköz érhető el; akár minden hónapban szólhatna valamelyikükről egy cikk. Általában egy vagy két eszközzel szoktam mélyrehatóbban foglalkozni, most azonban inkább áttekintő jelleggel szeretném megismertetni kedvenc linuxos biztonsági eszközeimet. Aki csak most ismerkedik a Linuxszal vagy a hálózati biztonság témakörével, talán először találkozik e programcsomagokkal. Sebaj, reményeim szerint sikerül megtalálniuk azt az irányvonalat, ami mentén haladva elmélyültebb tudásra tehetnek szert. Aki egy vagy több eszközt ismer, de nem mindegyiket, ez alkalommal bővítheti ismereteit és eszközkészletét. Biztosan akadnak olyanok is, akiknek az égvilágon semmi újat nem fogok mondani – ők legfeljebb kikapcsolódnak egy kicsit, miközben azt is megtudják, hogy a saját hordozható gépem processzora miféle dolgokon gondolkodott a legtöbbet az elmúlt időszakban.

Netfilter, illetve iptables

Körsétánkat a legalapvetőbb programmal, a Netfilterrel kezdjük, a Linux-rendszermag beépített tűzfalával. Pontosítsunk egy kicsit: a kérdéses modulok összességének hivatalos neve a Netfilter, az `iptables` pedig a felhasználói térben érvényes parancs, amit a Netfilter magmodulok beállításainak megadására használunk. A két nevet nyugodtan összekeverhetjük, különösebb félreértést nem fogunk okozni vele, kivéve, ha `iptables` parancsokat adunk ki vagy a rendszermag fejlesztőivel társalgunk.

A Netfilter tavaly megnyerte Szerkesztőségi díjunkat a „Legjobb biztonsági eszközök” kategóriában. Azóta is tartom a véleményemet, mely szerint a Netfilter fontos szerepet játszott abban, hogy a linuxos tűzfalak végre túllépjenek az állapotmentes csomagszűrés (stateless packet filtering) némileg meghaladott módszerén, és belépjenek az állapotalapú csomagszűrés korába. Mit is jelent mindez a biztonsággal napi 24 óránál kevesebbet foglalkozók számára? A Netfilter segítségével a linuxos tűzfalak egymással fennálló kapcsolataikat is figyelembe véve vizsgálhatják a hálózati csomagokat, vagyis a létrejött kapcsolatokkal társítják őket; például adott csomagot egy átvitel kezdeteként jelölnek meg. A 2.4-esnél régebbi Linux-rendszermagok a csomagokat különálló egységekként kezelték, a szűrést pedig kizárólag a csomagok forrása, valamint célja alapján végezték.

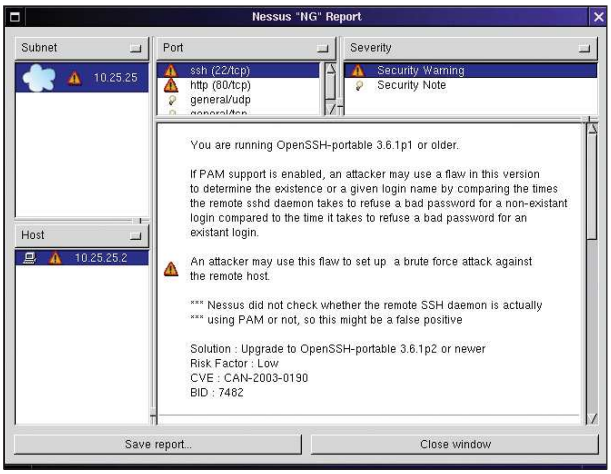
Egy HTTP-kapcsolat csomagjait például a tűzfalak egyenként vizsgálták és szűrték, nem egymáshoz tartozó elemekként kezelték őket.

Az újfajta csomagszűrési eljárás nem csak arra alkalmas, hogy linuxos tűzfalakat állítsunk össze, a Netfilter helyi biztonsági eszközként, kiszolgálókon és munkaállomásokon ugyanolyan jó szolgálatot tehet, mint a hálózati tűzfalakon. (Arról, hogy mindezt miképpen cselekszik a Linuxvilág 2002. decemberi számának 55. oldalán „Biztonság a helyi hálózaton: IP Tables” címmel írtam részletesebben.)

Az `iptables` parancs használata nem nagy ördöngösség, csak egy kis időt kell szánnunk az `iptables(8)` súgóoldal tanulmányozására. Ezenkívül e témában ***Robert Ziegler*** kiváló „Linux Firewalls”című könyvét tudom ajánlani. Az `iptables` kiemelkedő parancsfájl-készítési lehetőségeket kínál a már említett forrásokban, és az interneten rengeteg példát lehet találni, amelyeket könnyedén saját igényeinkhez igazíthatunk.

Mit ajánlhatunk azoknak, akik nem érdeklődnek a csomagszűrés rejtelmei iránt, és inkább ékes angol nyelven beszélő grafikus felületen keresztül szeretnének dolgozni? Semmi gond, a Netfilterhez számos külső fejlesztésű felület létezik. Az egyik legjobb a Firewall Builder (➲ http://www.fwbuilder.org), ami varázslókkal és újrafelhasználható objektumokkal segít bennünket a tűzfalszabályok létrehozásában. A Firewall Builderrel a Linuxvilág hasábjain egy kétrészes sorozatban foglalkoztam 2003. májusában és júniusában.

Másik népszerű `iptables` kiegészítő a Mason, amely az `iptables` parancsfájlokat önműködően, a rendszer mindennapi használatát figyelemmel kísérve készíti el. Elsősorban egyedi, munkaállomásokat védő tűzfalszabályok létrehozására használják. A Mason a ➲ http://users.dhp.com/~whisper/mason címről tölthető le. Szintén érdekes és elterjedt eszköz a Shorewall, amely a ***/etc/shorewall*** könyvtárba helyezett egyszerű szöveges fájlok alapján állítja be az összes `iptables` parancsfájlt. Honlapja a ➲ http://shorewall.net címen található.



1. kép Nessus-példajelentés, amely sebezhető SSH-démon jelenlétéről tudósít

Több Linux-változat saját, egyedi eszközt kínál az `iptables` használatának segítésére. A SuSE 8.2-esben ez a SuSEfirewall2, amely a */etc/sysconfig/SuSEfirewall2* fájlban megadott egyszerű beállítások alapján önműködően hozza létre és futtatja az `iptables` parancsokat. Ha saját terjesztésünk rendelkezik ilyen programmal, akkor érdemes kipróbálni. Valószínűleg már fent csücsül a gépünkön, így a telepítéssel sem lesz gondunk.

Bastille

A Bastille, ***Jay Beale*** és ***Jon Lasser*** alkotása, önmagában is fogalom, külön kategóriát alkot. Lényegében egy parancsfájl, amely a használójának feltett kérdések alapján átfogó jelleggel képes védeni a linuxos rendszert. A többi védelmi parancsfájltól élesen megkülönbözteti, hogy minden kérdéséhez bőséges magyarázat tartozik. Soha nem láttam még olyan biztonsági programot, amely olyan sokat tenne a felhasználók oktatásáért, mint a Bastille. Újoncoknak éppen ezért ajánlom, hogy elsőként mindenképpen a Bastille-t ismerjék meg.
Amikor pár éve a Bastille-ról írtam („Hogyan erősítsük rendszerünk biztonságát?”, Linuxvilág, 2001. április), néhány kérdésemmel megkerestem Jay Beale-t. A Bastille nagyszerűsége jelentős részben Jay nyitott személyiségéből fakad, közvetlen és szórakoztató stílusban segíti hozzá programjának használóit rendszerük biztonságának javításához.
A Bastille hivatalosan Red Hat, Mandrake és Debian GNU/Linux alatt használható. Átültetése HP-UX és Mac OS X alá is elérhető; és a ➲ http://www.bastille-linux.org címről szerezhető be.

Nmap

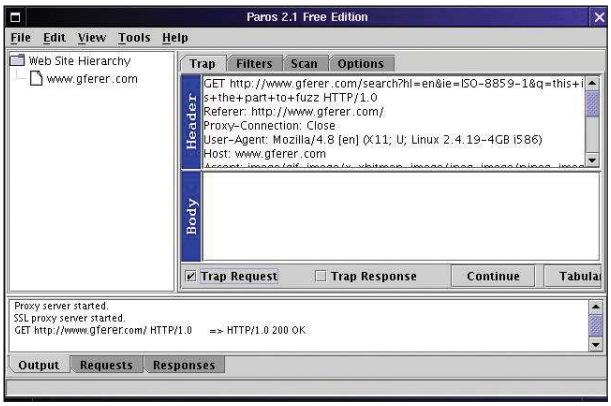
A Netfilter és a Bastille kizárólag védekezésre szolgálnak. Mivel próbálhatjuk ki, hogy valóban biztonságban van-e linuxos gépünk? Az egyik lehetőség, hogy egy kapupásztázót (port scanner) futtatunk le, összesítjük mely kapuk állnak nyitva, és ennek alapján határozzuk meg, mely hálózati alkalmazások futnak.
Ha egy egész telephely vagy iroda biztonságát szeretnénk felmérni, akkor csupán önműködő kapupásztázással nem tudjuk megállapítani, hogy biztonsági szempontból mennyire végzett gondos munkát a vele megbízott személy. A pásztázás mégsem haszontalan, ha mást nem is, legalább a tűzfalak beállításait ellenőrizni tudjuk. Egy jó kapupásztázóval pontosan meghatározhatjuk, hogy a kívülről érkező betyárok (hacker) milyen bejutási pontokat láthatnának rendszerünkön.
Az Nmap (lásd 1. széljegyzetünket az 59. CD-melléklet Magazin/biztonság könyvtárában) kétségbevonhatatlanul a kapupásztázók királya: gyors, kis méretű, ingyenes és nagy tudású. Az Nmap többféle pásztázási módszert ismer, a gyors és feltűnő TCP-csatlakozási próbától egészen a csendes és aljas karácsonyfa-pásztázásig. Az Nmap – bár parancssorból sem nehéz használni – grafikus felülettel is bír. Legújabb változata a ➲ http://www.insecure.org címről tölthető le, de valószínűleg saját Linux-változatunk is tartalmazza valamely változatát. Nem kell mást tennünk, mint a megfelelő korongot elővenni, és pillanatok alatt feltehetjük gépünkre az Nmapot.

Nessus

A kapupásztázók csak végignézik a nyitott kapukat, a biztonsági pásztázók viszont megpróbálnak csatlakozni is hozzájuk, és a lehető legtöbb adatot kísérlik meg beszerezni a kapuk mögött várakozó alkalmazásokról. Ennek legegyszerűbb változata a hirdetménygyűjtés, amikor az alkalmazások által a sikeres kapcsolódást követően megjelenített üzeneteket naplózzuk. Számos alkalmazás névvel, és nem egy esetben, változatszámmal azonosítja magát.
Természetesen a magasabb szintű biztonsági pásztázók jóval többet tesznek a hirdetmények begyűjtésénél. Miután meghatározták, hogy az adott kaput milyen alkalmazás figyeli, és az ismert sebezhetőségeit megpróbálják kihasználni, általában olyan módon, hogy a közismert betörési módszereket kezdik alkalmazni – természetesen nem viszik végig őket. A Nessus (*1. kép*) egy profi, kiválóan testreszabható, ennek ellenére ingyenes biztonsági pásztázó.
Az Nmaphez hasonlóan, a Nessus is felbecsülhetetlen értékű eszköz a biztonsági mérnökök számára. A két program haszna a hétköznapok során is megmutatkozik. Például, ha például a Nessus segítségével egy hobbi-webkiszolgálót akarunk ellenőrizni. A Bastille-hoz hasonlóan a Nessus tervezése során is a célkitűzések között szerepelt a felhasználók oktatása. Ha a jelentéseket gondosan átolvassuk, akkor nemcsak a sebezhetőségekről, de javítási módjaikról is egy csomó dolgot megtudhatunk.

Paros

Mielőtt a biztonsági ellenőrzések témakörén továbblépnénk, szenteljünk némi figyelmet a webes alkalmazások biztonságának is. A webes alkalmazások az interneten keresztül elérhető szolgáltatások bővülésében és a kívülről kihasználható sebezhetőségek számának növekedésében egyaránt elsődleges szerepet játszanak. Vajon hogyan tudnánk ellenőrizni webes alkalmazásaink biztonságosságát? Jó gondolat, hogy a Nessus kezdésnek megfelel, de inkább az általános webdémonok ellenőrizhetők vele. A Nessus jelentései inkább a kiszolgálóra, például az Apache démonra, és nem az általa szolgáltatott webes tartalomra vonatkoznak. A Nessusszal sosem tudjuk megállapítani, hogy vajon saját webes alkalmazásaink kellően ellenőrzik-e a bemeneteket, nem sebezhetők-e a webhelyek között futó parancsfájlokkal



2. kép A Paros ingyenes eszköz a webes alkalmazások ellenőrzésére

végrehajtott támadásokkal szemben (cross-site scripting), esetleg az általuk várt átadott értékek módosításával nem lehet-e megbolondítani őket, és így tovább. A Paros pontosan az ilyen kérdésekre segít megtalálni a választ.

A Paros (*2. kép*) egy ingyenes, Java nyelven írt eszköz, amely Clarified Artistic License (letisztult művészi felhasználói szerződés) hatálya alatt jelenik meg. A Paros használatához telepíteni szükséges a Java futtatási környezetet. A Paros futtatható JAR állománya és teljes forráskódja a ➲ http://www.proofsecure.com címről tölthető le.

A Paros a webes biztonsági eszközök új nemzedékének működési elvét követi. Az ellenőrzésre használt munkaállomáson helyi proxyként fut, a helyi böngésző és a célwebkiszolgáló közötti párbeszédeket bonyolítja le. Ezzel a módszerrel a kimenő kérések a kiszolgálónak való továbbküldés előtt elfoghatók, módosíthatók és összezavarhatók. Tegyük fel, hogy a webes alkalmazásunk lenyíló menüket tartalmazó űrlapot alkalmaz, és meg akarunk győződni arról, hogy alkalmazásunk megfelelően ellenőrzi-e a bemenetet. A Paros segítségével a lenyíló menük pontjait véletlenszerű karakterláncokra cserélhetjük le – így lesz a hétfőből blablabla –, majd megvizsgálhatjuk, hogyan válaszol az alkalmazásunk.

A Paros sokféle pásztázási módszert támogat, például a könyvtárak végigjárását is el tudja végezni. A JRE futtatása a régebbi rendszereket ugyan erősen leterhelheti, de maga a Paros rugalmas és felhasználóbarát program. Mivel Java alapú, nemcsak Linux alatt futtatható, jómagam is többféle Windows-változaton használtam már.

A Paros nem az egyetlen létező összezavaró proxy, ***Dave Aitel*** kiváló Spike nevű proxyprogramját is érdemes megemlíteni. Szintén helyi proxyként működik, de miután a köztünk és a távoli webhely között zajló párbeszédet megfigyelte, önműködő összezavarásos támadások indítására is képes. A Spike Python nyelven készült, vagyis kisebb számítási teljesítményt és kevesebb memóriát igényel, mint a Paros.

F.I.R.E.

Rövidke áttekintésemet egy oknyomozó programmal, ***William Salusky*** F.I.R.E. (Forensics and Incident Response Environment, azaz törvényszéki és esetkezelő környezet) alkalmazásával szeretném zárni. Bármennyire is szeretnénk elhessegetni a gondolatot, mégis tudomásul kell vennünk: hiába vagyunk körültekintőek, hiába próbálunk előre gondolkodni, mégis előfordulhat, hogy egy nem túl szép napon rendszerünket megtörik. Ha tudni szeretnénk a betörés hogyan és miért történt, a F.I.R.E. lehet segítségünkre. A F.I.R.E. egy CD-s Linux-változat, amit feltört rendszerek elemzésére és adataik helyreállítására állítottak össze.

A gépet szükség szerint a F.I.R.E. CD-jéről is indíthatjuk, de ha a rendszerünk még működőképes, azt is megtehetjük, hogy a lemezt befűzzük, és a szükséges programokat róla futtatjuk. Az utóbbi főleg akkor lehet előnyös, ha a gépen található futtatható állományokban nem bízunk meg, mert úgy gondoljuk, hogy a betörő támadócsomagot (rootkit) vagy trójaival fertőzött változatokat telepített fel. A F.I.R.E. a szükséges elemzések elvégzése mellett arra is használható, hogy segítségével a megtört gép adatait más hálózati állomásra másoljuk át. A F.I.R.E. az X Window Systemet is tartalmazza, valamint számos parancssori és X alapú biztonsági programot is magában foglal, többek közt az Nmapet és a Nessust. A F.I.R.E. segítségével akár egy egyszerű windowsos hordozható gépből is félelmetes betörésérzékelő hadigépezetet varázsolhatunk. A F.I.R.E. főbb szolgáltatásai a menürendszerből is elérhetők, ilyen módon még a betörések felderítésében kevésbé jártasak számára is könnyen használható. A F.I.R.E. program a ➲ http://fire.dmzs.com címről tölthető le.

Összegzés

Az volt a szándékom, hogy a teljesség igénye nélkül megemlítsek néhányat a számos kiváló linuxos biztonsági eszköz közül. Az írásban szereplők listája jóval rövidebb, mint a kimaradottaké: Tripwire, AIDE, Nikto, GnuPG, FreeS/WAN, Snort, PSAD, Stunnel, OpenSSL és még sokan mások. Mindössze annyit sikerült elérnem, hogy kedvenc munkaeszközeimet bemutattam. Remélem, mindenki hasznosnak találja majd őket. Ne feledjük, az említett eszközök jókora hatalmat adnak használójuk kezébe, ezért alkalmazásuk során felelősséggel, gondosan és erkölcsösen kell eljárni. Aki így cselekszik, annak jó szórakozást kívánok!

Linux Journal 2004. február 118. szám

KAPCSOLÓDÓ CÍMEK

- ➲ http://www.fwbuilder.org
- ➲ http://shorewall.net
- ➲ http://www.bastille-linux.org
- ➲ http://www.insecure.org
- ➲ http://www.proofsecure.com
- ➲ http://fire.dmzs.com

Mick Bauer (mick@visi.com)
Biztonsági szakember, a Linux Journal biztonsági témákkal foglalkozó szerkesztője, biztonsági tanácsadó a Minnesota állambeli Minneapolisban található Upstream Solutions LLC Inc.-nél.