Linuxos kiszolgálót mindenkinek! (2. rész)

A SuSE Linux mint kiszolgáló – kisvállalati és otthoni környezetben.

Az elmúlt alkalommal eljutottunk oda, hogy – elsősorban kiszolgálói feladatok ellátására – feltelepítettünk egy SuSE Linuxot. Most ezt a kiszolgálót fogjuk finomhangolni: felhasználókat, felhasználói csoportokat készítünk, beállítjuk a kiszolgáló biztonsági szintjét, felügyelhetővé tesszük a gépet és tűzfalat készítünk.

Felhasználók és felhasználói csoportok

Felhasználók létrehozásakor ökölszabályként alkalmazandó, hogy a felhasználókat a működési területüknek megfelelő felhasználói csoportokba tegyük, a felhasználói csoportokat pedig úgy hozzuk létre, hogy jól elkülöníthetőek legyenek egymástól. Minden felhasználónak csak a működéséhez, a munkája elvégzéséhez szükséges jogosultságokat adjuk meg. Felhasználókat vagy a `useradd` paranccsal vehetünk fel, vagy a YaST rendszergazdai felületen keresztül. A `useradd` parancsról bővebb leírást kaphatunk a megfelelő súgóoldal megnyitásával. A YaST-on keresztül egy olyan felülethez juthatunk, ami az összes felhasználót és felhasználói csoportot megmutatja nekünk, így grafikusan is jó áttekintést kapunk a felhasználókról. A YaST-on belül a ***Biztonság és felhasználók*** menüpontban találjuk a felhasználók felügyeletével foglalkozó részt. A ***Csoportok létrehozása és módosítása*** menüpontot kiválasztva megjelenik a ***Felhasználók és csoportok adminisztrációja*** ablak, ezen belül pedig egy lista a már létező felhasználói csoportokról. Az ablak alján található ***Szűrő beállítása*** és ***Egyedi szűrő*** gombbal szűrési feltételeket adhatunk meg, így téve még átláthatóbbá a listát. A ***Hozzáadás*** gombbal új csoportot hozhatunk létre. Ekkor meg kell adnunk egy csoportnevet, egy egyedi csoportazonosító számot, megadhatunk továbbá jelszót a csoporthoz, és rögtön ki is jelölhetjük, hogy mely felhasználókat társítsuk a csoporthoz.

Felhasználók hozzáadásához a ***Felhasználók létrehozása és módosítása*** menüpontot válasszuk. Ekkor az előbbihez hasonló ablak jelenik meg, ahol szintén meghatározhatunk szűrőket és a ***Hozzáadás*** gombbal új felhasználót adhatunk a rendszerhez. A megjelenő ablakban meg kell adnunk a felhasználó teljes nevét, az azonosítóját, illetve a jelszavát. A ***Jelszóbeállítások*** gombra kattintva a jelszó lejáratával kapcsolatos adatokat adhatjuk meg, úgymint figyelmeztetés, az érvényesség időtartama, a lejárat pontos időpontja. A ***Részletek*** gombra kattintva beállíthatjuk a felhasználó egyedi azonosítószámát, saját könyvtárának a helyét – amit egyébként a felhasználói csoportoknak megfelelően érdemes elhelyezni, és ez alapján csoportosítani a felhasználókat –, megadhatunk kiegészítő felhasználói adatokat, a bejelentkezési héjat (shellt), alapértelmezett és további csoportokat. Héjnak érdemes a felhasználó szükségleteinek megfelelő héjat megadni. Így amennyiben felhasználónk csak levelezést vagy megosztott könyvtárakat használ, úgy héjnak a */**bin**/**false***-t adjuk, így megakadályozzuk, hogy ez a felhasználó a kiszolgálóra akár helyileg, akár távoli eléréssel (SSH, Telnet stb.) közvetlenül bejelentkezzen. Amennyiben a felhasználó munkája során szükség van konzolra, ráadásul párhuzamosan több felületet is használnánk, úgy használjuk

a */**usr**/**bin**/**screen*** héjat, amit a ***screen*** csomag telepítése után érhetünk el. Ha ezzel végeztünk, kattintsunk a ***Következő*** gombra, majd fogadjuk el az eddig elkészített beállításainkat.

Biztonsági beállítások

A YaST ***Biztonság és felhasználók*** menüpontjának biztonsági beállításai közül először foglalkozzunk a ***Biztonsági beállítások***kal. Ezt a modult indítva három előre meghatározott biztonsági összeállítás közül választhatunk, vagy létrehozhatjuk a sajátunkat. Beállíthatjuk, hogy a felhasználói jelszavak létrehozásakor a rendszer egy szótárral hasonlítsa össze a megadott jelszót, és ha megtalálja, akkor figyelmeztesse a felhasználót, hogy egy ilyen jelszót esetleg könnyen ki lehet találni. A ***Jelszó elfogadhatóságának ellenőrzése*** lehetőség pedig biztosítja, hogy a felhasználónak megfelelően bonyolult jelszót gépeljen ahhoz, hogy a rendszer elfogadja. Megadhatjuk továbbá a jelszó titkosításának eljárását, a legfeljebb figyelembe vett karakterek számát, a legkisebb jelszóhosszt, valamint a jelszó lejárata előtti figyelmeztetést napokban.

Tűzfalak

Rendszerünk védelme szempontjából nagyon fontos szerepet kap egy jól beállított tűzfal. Tűzfalunkra hárul ugyanis az a feladat, hogy elválassza a biztonságos belső hálózatot a nem biztonságos külső hálózattól, például az internettől.

A tűzfalaknak többféle összeállítása létezhet az alkalmazott hálózat topológiájától, szolgáltatásától, biztonsági követelményeitől függően. A megfelelő összeállítás kiválasztása mind a rendszer biztonsága, mind a rendszerre fordított anyagiak szempontjából kényes kérdés. Mielőtt nekiállunk tűzfalat készíteni, érdemes kockázatelemzést készíteni, hogy a megfelelő biztonságot garantálni tudjuk, de azért ne szaladjon el velünk a ló.

A legegyszerűbb eset, amikor egy kiszolgáló védelméről kell csak gondoskodni. Ekkor elég felmérnünk azt, hogy a kiszolgálón milyen szolgáltatások fognak futni, és a tűzfalat ehhez

mérten tudjuk beállítani. Ilyenkor elég a szolgáltatások által igényelt kapuk kinyitása, természetesen a kapuk forgalmának monitorozása mellett.
Kicsit bonyolultabb a helyzet, ha olyan hálózatunk van, ami egy adott gépen (hálózati átjárón) keresztül éri el mondjuk az internetet. Ekkor a tűzfalunkat úgy kell beállítani, hogy az védelmet nyújtson az átjárónak és a mögötte lévő hálózatnak is úgy, hogy a hálózati ügyfelek munkáját ne akadályozza. Különös esetben elképzelhető, hogy a hálózati átjárót a belső hálózat oldaláról is védeni kell – ez csak tovább bonyolítja a dolgunkat. A SuSE Linuxba épített tűzfalszolgáltatás akár háromrétegű tűzfalszerkezetet is támogat. Így lehetőségünk van a belső hálózat–DMZ–külső hálózat felépítés kialakítására. Belső hálózatunk értelemszerűen a biztonságos helyi hálózat; a külső hálózat a nem biztonságos hálózati szakasz, ahonnan a támadások várhatóak; s a DMZ pedig nem más, mint a szabad zóna

Frissítés SuSE 9.0-ra

Magyarországon is bemutatták a SuSE Linux 9.0-s kiadását, amely a fejlesztők szerint az utóbbi idők egyik legkiforrottabb Linux-változata. Sok olyan szolgáltatást kínál, ami miatt egy kiszolgálót is érdemes lehet frissíteni az új kiadásra. Ilyen szolgáltatás például a YaST-ba épített Samba, DHCP, DNS vagy Apache modul, hogy csak párat említsek. Természetesen a frissítés szükségességét mindenkinek saját magának kell megítélnie, de én úgy döntöttem, hogy frissítek, és a cikksorozatban a továbbiakban a SuSE 9.0-s kiadás nyújtotta lehetőségeket is bemutatom.
A frissítés maga nem túl bonyolult dolog, de azért körültekintést igényel. A telepítés a megszokott módon kezdődik: először behelyezzük a CD-t vagy a DVD-t a meghajtóba, és a gép indítása után kiválasztjuk a *Telepítés* menüpontot. A telepítő a megszokott módon először a telepítés nyelvét állítja be, itt válasszuk a magyart. A következő lépésben a telepítő rákérdez a telepítés típusára. Amennyiben már meglévő SuSE Linux-rendszerünk van, úgy válasszuk a Meglévő rendszer frissítése lehetőséget, s ha új rendszert szeretnénk telepíteni, akkor természetesen az *Új telepítés* menüpont a megfelelő választás.
Miután a telepítés menetét az előző cikkemben már leírtam, és ez a 9.0-s kiadásnál sem különbözik lényegesen, most a frissítés menetével foglalkozom.
Miután a telepítő ellenőrizte a meglévő rendszert és a csomagadatbázist frissítette az új változatra, megjelenik a *Telepítési beállítások* ablak. Itt az új rendszer telepítéséhez hasonlóan megadhatjuk a telepítendő rendszer nyelvét, billentyűzetkiosztását, de amire mi most a figyelmünket összpontosítjuk, az a *Frissítési mód* és a *Biztonsági mentés* menüpontok.
A *Frissítési mód* menüpont alatt adhatjuk meg, hogy egy előre összeállított csomaglista alapján kívánjuk-e frissíteni a rendszert, vagy a meglévő csomagjainkat kívánjuk frissíteni. Az előbbi előnye, hogy felteszi a legfrissebb, legújabb szolgáltatásokat, az utóbbié, hogy nem változtat a meglévő csomag-összeállításon. Én az utóbbit javaslom, mert az új csomagokat később is tudjuk telepíteni, viszont ezzel a beállítással biztosított, hogy a rendszer frissítés után is a már összeállított kiépítésnek megfelelően fog működni. Fontos még odafigyelni az ablak alján lévő *Karbantartás nélküli csomagok törlése* jelölőnégyzetre. Ezt javasolm kikapcsolni, mert ha nem tesszük meg, az olyan csomagokat, amelyekről a rendszer úgy ítéli meg, hogy nem fogjuk használni, egyszerűen letörli, ez pedig meglepetéseket okozhat a későbbiekben.
A *Biztonsági mentések* menüpont alatt lehetőségünk van a régi rendszerről készítendő mentések beállítására. Mindenképpen jelöljük be a biztonsági mentés készítését a módosítandó állományokról és a teljes */etc/sysconfig* könyvtárról. A mentés később a */var/adm/backup* könyvtárban lesz található, ahonnan akár törölni is lehet.
Ha ezekkel a beállításokkal végeztünk, indíthatjuk a frissítést.
A SuSE saját bevallása szerint a 7.3, 8.0, 8.1 és 8.2 rendszerekről történő frissítés zökkenőmentes lesz. Ettől függetlenül készítsünk az adatainkról, beállításokról biztonsági másolatot, és ahogy mondani szokták: mindenki a saját felelősségére csinálja!
Ha a telepítő végzett a csomagok telepítésével, akkor hátravan még az internetkapcsolatunk kipróbálása és a frissített csomagok letöltése az internetről. Frissítéshez válasszuk a *suselinux.hu* kiszolgálót, és ha gondoljuk, akkor bízzunk meg a rendszer önműködő csomagtelepítésében.
Ezzel végeztünk is, feltettük a legfrissebb SuSE Linuxot, egy ajánlott újraindítás után dolgozhatunk is tovább.

(demilitarized zone), vagy elsődleges hálózat (perimeter network), ami egy köztes, elkülönített réteg a biztonságos belső hálózat és a külső hálózat között vagy mellett. Itt szokták elhelyezni az olyan gépeket, amelyek például az internet felől elérhető szolgáltatásokat nyújtanak. Mivel a szabad zónát mindkét oldalról tűzfal határolja, az esetlegesen a szabad zónában megtámadott gépről a belső hálózaton keresztül nem tudnak további adatokat szerezni – sikeres támadás esetén a támadó nem jut rögtön hozzáféréshez a belső hálózathoz. Ez a kiépítés a legbiztonságosabb megoldás, de elég drága, hiszen további eszközök beszerzését teszi szükségessé, illetve a kiépítése bonyolultabb, mint egy belső hálózat–külső hálózat felépítésű rendszeré.
Otthoni, kisvállalati felhasználási körben – megfelelő biztonsági kockázatelemzést követően – dönthetünk úgy, hogy ez az utóbbi felépítés megfelelő biztonságot nyújt számunkra. Ebben az esetben a belső hálózat–külső hálózat kiépítésére a YaST megfelelő eszközöket nyújt.
A YaST ***Biztonság és felhasználók*** menüpontja alatt található a ***Tűzfal*** modul, amelynek az indításával kezdhetjük meg a tűzfalunk beállítását. Az első lépésben meg kell adnunk a kiszolgáló külső és belső hálózatához tartozó hálózati csatoló nevét. Figyeljünk rá oda, hogyha ADSL kapcsolatot használunk, akkor nem a hálózati kártyát kell megadnunk, hanem az adott eszközhöz tartozó PPP-csatolót (általában a `ppp0`-t).
Következő lépésben megadhatjuk, hogy milyen szolgáltatásokat akarunk elérhetővé tenni a kiszolgálón, így például a HTTP, SMTP, egyéb levelezési protokollok, SSH. Érdemes arra odafigyelni, hogy a HTTP, SMTP, POP3, IMAP, `telnet` protokollok a teljes adatforgalmat titkosítás nélkül bonyolítják le, így ha valaki egy arra alkalmas helyen lehallgatja a hálózatunkat, akkor felhasználói nevekhez, jelszavakhoz is hozzájuthat. Ezért ahol lehet, érdemes az SSL-es szolgáltatásokat használni. Ezeknek a beállításához majd tanúsítványokat kell létrehozni, amivel a protokoll a titkosítást fogja végezni, de erről még szólunk a későbbiekben.
A ***Szakértő*** gombra kattintva további kapukat adhatunk meg elérésre, nevük a */etc/services* állományban találhatók meg.
Következő lépésben négy fontos beállítást végezhetünk el.
Az első az ***Útvonalkövetés engedélyezése***, amely lehetővé teszi, hogy a távoli gépről úgynevezett „ICMP time to live exceeded” csomagokat küldjünk a gépnek. Ez egyfelől hasznos, mert a `ping` parancs segítségével megállapíthatjuk, hogy a gép pillanatnyilag elérhető-e, ugyanakkor ez támadási felületet ad a szolgáltatásmegtagadásos (Denial of Service, DoS) támadásokhoz. DoS támadás alkalmával például ICMP csomagokkal árasztják el a kiszolgálót, ami – mivel a nagy terhelés miatt nem fogja tudni kiszolgálni a csomagokat – elérhetetlenné válik. Ezt a kockázatot mindenképpen figyelembe kell vennünk.
A második beállítási lehetőség a ***Forgalomtovábbítás és álcázás*** (NAT – Network Address Translation), amire akkor lesz szükségünk, ha a tűzfal mögött elhelyezett hálózatnak saját IP-tartományt akarunk adni, és az ügyfelek számára elérhetővé kívánjuk tenni a külső hálózatot. Ekkor a belső hálózati gépekről indított forgalom úgy fog látszani, mintha azt a kiszolgáló indította volna. Ez arra jó, hogy elrejtsük, hogy a kiszolgáló mögött helyi hálózatot hoztunk létre, valamint ennek segítségével takarékoskodni tudunk a rendelkezésünkre álló nyilvános IP-címekkel. Amennyiben otthoni hálózatot szeretnénk üzemeltetni, ennek a lehetőségnek használata szükséges például egy ADSL kapcsolat megosztására. (Figyelem, a szolgáltatók az ***Előfizetői szerződés*** keretében az ADSL és a kábeltévés internetelérések megosztását korlátozhatják, sőt akár tilthatják is!)
A harmadik beállítási lehetőség a ***Minden futó szolgáltatás védelme*** lehetőség. Ha ezt bekapcsoljuk, úgy az engedélyezett szolgáltatásokon kívül minden más szolgáltatáshoz érkező kérés vissza lesz utasítva – hasznos például DoS támadások ellen.
A negyedik pedig a már említett ***Védelem a belső hálózattal szemben***. Ekkor a belső hálózatról is csak a kijelölt szolgáltatások lesznek elérhetők.
Negyedik lépésben lehetőségünk van beállítani, hogy a tűzfal futása alatt milyen biztonsági események legyenek a helyi naplóba bejegyezve. Alapesetben a kényes csomagok kerülnek naplózásra, mind az elfogadott, mind az eldobott csomagok. Mivel ezek a bejegyzések a többi rendszerbejegyzéssel együtt a */var/log/messages* naplóállományba kerülnek, ez a naplózás eléggé meg fogja növelni a napló méretét, amely így elérheti

Kockázatelemzés adatbiztonsági szempontból

A biztonság az egyik legfontosabb dolog napjainkban – erre érdemes költeni, mert adataink elvesztése óriási gondokat idézhet elő, és ez ma már nem csak üzleti környezetben van így. Otthoni felhasználókat is fájdalmasan érinthet, mondjuk a családi fényképek elveszítése, amiket az elmúlt években az újonnan vásárolt digitális kamerával készítettek, vagy éppen egy egyetemi házi feladat, munkahelyi leírás eltűnése. Éppen ezért érdemes odafigyelni a biztonságra, költeni rá. És itt szokott felmerülni a kérdés, hogy mennyit is áldozzunk a biztonságra? A kevés adott esetben olyan, mintha semmit nem tettünk volna, a sok pedig felesleges kiadásként jelentkezik. A kulcsszó: felmérés és tervezés.
Megtehetjük, hogy az adatainkat többszörözött lemezrendszeren tároljuk, ahogy azt az előző cikkemben be is mutattam, megtehetjük, hogy rendszeres mentéseket készítünk, amit aztán a számítógép mellett tartunk. Mit ér mindez egy tűz alkalmával? Semmit. Elveszik a gép, megsemmisül a mentés.
Beállíthatunk akármilyen jó tűzfalat, készíthetünk szigorú felhasználói beállításokat – mindez semmit nem ér, ha a kiszolgáló fizikailag hozzáférhető és el lehet vinni a merevlemezeket.
Meg kell tehát teremteni a fizikai és logikai védelmet, az adatok biztonságos tárolásának feltételeit, és fel kell készülnünk egy esetleges rendszer-helyreállításra. Ehhez készíthetünk vésztervet, meghatározhatjuk, hogy ilyen esetben kinek mi a feladata. Amire pedig semmiképpen nem lehet felkészülni, olyan esetekre köthetünk biztosítást. Ezzel ismét eljutottunk oda, hogy határt kell szabnunk, mire és mennyit akarunk költeni. Körültekintés és alapos tervezés, ez a megfizethető biztonság kulcsa.

a napi 3–4 MB-ot is. Hibakeresési céllal bekapcsolhatjuk, hogy minden egyes csomag naplózásra kerüljön, de ez tényleg csak rövid idejű használatra ajánlott, mert így akár több 10 MB-os naplóállomány is előállhat. Ha minden beállítással végeztünk, akkor elindíthatjuk tűzfalunkat, így ezek után már nagyobb biztonságban érezhetjük magunkat.
Tűzfalunk összetettebb beállítása érdekében vessünk egy pillantást a ***Rendszer*** menüpont ***/etc/sysconfig*** szerkesztőmoduljára. A bal oldali fában a ***/network/firewall/SuSEfirewall2*** alatt találhatóak a SuSE-tűzfal további beállítási lehetőségei. Ezek módosítása csak haladó felhasználóknak ajánlott, mert csúnyán elszúrhatjuk vele a tűzfal beállításait. Ezekre a beállításokra egyszerű irodai, otthoni kiszolgálók esetén ritkán van szükség. Az egyik ilyen beállítási terület például az UDP-csomagok forgalmának a szabályozása, amelyre például DNS-kiszolgáló üzemeltetésekor vagy IPSEC titkosított csatorna létrehozásakor lehet szükség. Itt tudunk beállítani kaputovábbítást (port forward) a belső hálózat felé, és itt tudjuk beállítani a már említett három rétegű tűzfalszerkezetet is.

Naplóállományok kezelése

A SuSE 9.0 a rendszer futása alatt keletkező naplóeseményeket a */var/log/* könyvtárban tárolja. A könyvtárban további mappák is találhatók, amelyekben bizonyos telepített szolgáltatások külön naplóállományokat hoznak létre, például az Apache webkiszolgáló a ***http*** könyvtárat, a Samba fájl- és nyomtatókiszolgáló a ***samba*** könyvtárat. Rendszerünk biztonságos üzemeltetéséhez elengedhetetlen, hogy a naplóállományokat figyelemmel kísérjük, hiszen az üzemzavar vagy a támadási kísérlet ezekből derül ki egyértelműen. A */var/log* könyvtárban találhatók a ***messages*** és a ***mail*** állományok, ahová a rendszer és a levelező az elkészült naplóbejegyzéseket gyűjti.
Ezeknek az állományoknak az állandó szemmel tartása fontos, ugyanakkor elég kényelmetlen dolog. A SuSE Linuxban erre létezik egy `logdigest` nevű csomag, ami minden éjszaka kigyűjti az aznapi naplóbejegyzéseket és egy megadott elektronikus címre juttatja el őket. A `logdigest` csomag egyik legfőbb erénye, hogy a naplózott események megjelenítését szabályos kifejezésekkel saját magunk csoportosíthatjuk, így előtérbe helyezhetünk olyan bejegyzéseket, amelyek fontosak számunkra. A */etc/logdigest* könyvtárban találhatók az ***alarming*** és az ***ignore*** állományok. Az előbbibe tegyük az olyan kifejezéseket, amelyek fontos, riasztásértékű adatokkal szolgálnak, például a rendszermaghibára utaló bejegyzéseket. Az utóbbi állományba tegyük az olyan bejegyzéseket, amelyeket fontosnak tartunk menteni, de adott esetben nem akarunk minden nap átböngészni. A ***config*** állomány a `logdigest` beállítására szolgál. Itt adhatjuk meg, hogy mely naplóállományok kerüljenek feldolgozásra, mely felhasználó kapja meg a kiküldött elektronikus levelet, illetve, hogy egyéb rendszeradatok feldolgozásra kerüljenek-e.
Ha idáig eljutottunk, akkor van egy működő, alapjában véve biztonságosnak tekinthető kiszolgálónk.

Illés Viktor (viktor@ei.hu)
23 éves, a BME műszaki informatikus szakának hallgatója, mellette weblapokkal, linxos és windowsos rendszerekkel foglalkozik. Szabadidejét legszívesebben a szabadban tölti, teniszezik és kerékpározik.