

Linux rendszerek biztonságosabbá tétele a gyakorlatban

Mátó Péter <atya@fsf.hu>

Telepítés

■ Megfelelő disztribúció

- Lehetőleg legyen szerver telepítés
- A csomagkezelő tegye lehetővé a könnyű frissítést

■ Partícionálás

- A /, /tmp, /var, /home, /var/log, /var/spool legyen külön partíció
- Legyen az adatoknak külön hely
- Csatolási opciók: noexec, nodev, nouser, nosuid

A csomagok átvizsgálása

- A rendszerre telepített csomagokat át kell vizsgálni
- Csomagkezelő függő, Debian és Ubutnu rendszereken:

```
# dpkg --get-selections | \  
    awk '!/deinstall/ {print $1}' > packages  
# cp packages packages.needed  
# vi packages.needed  
# apt-get remove --purge \  
    `fgrep -vf packages.needed packages`
```

Felesleges szerverek eltávolítása

- `'ps ax'` parancs használata
 - a parancs kiírja a rendszeren futó programokat
 - minden olyat érdemes eltávolítani, amit nem ismerünk
- `'netstat -nlp'` parancs használata
 - ha az előző szitán átcsúszott valami, akkor itt meg lehet találni
 - egy asztali gépen semminek nem kell figyelnie
 - szerveren pedig csak a szükséges szolgáltatások

Felesleges szerverek eltávolítása

- A rendszer indulásakor induló szerverek módosítása óvatosságot igényel
- Az init konfigurációja: `etc/inittab`
- A `/etc/rc.*` könyvtárak módosítása
`update-rc.d remove/add`
- `/etc/defaults/...` beállítások

A Netfilter tulajdonságai

- A Netfilter állapotartó csomagszűrő
- Az IP, ICMP, TCP és UDP csomagok jellemzői alapján lehet döntéseket hozni
- Lehetővé teszi a forgalom befolyásolását (--limit)
- Szűrhetünk a kapcsolat tulajdonosára és csoportjára (--owner)
- Könnyen lementhető és betölthető (iptables-save és iptables-restore)

A csomagszűrő beállítása I

- Szolgáltatás nélküli számítógép
 - --state NEW/ESTABLISHED/RELATED/INVALID
 - Az INPUT chain-ben csak az ESTABLISHED és a RELATED csomagokat kell beengedni
 - A chain default policy-ja legyen DROP
- Szolgáltatások beengedése
 - Elegendő a NEW állapotú csomagok beengedése a megfelelő portokra
 - Szükség esetén feladatok szerint chain-eket hozhatunk létre, ezzel áttekinthetőbb lesz a konfiguráció

A csomagszűrő beállítása II

■ Gateway rendszer beállítása

- Érdemes minden hálózat-kapcsolatnak létrehozni egy-egy chain-t
- Minden chain végén legyen egy -j LOG, és utána egy -j DROP
- Az előző beállítás fail-safe megoldás, tehát amit nem engedünk át explicit módon, azt a chain végén lévő szabály kiszűri
- Érdemes megvizsgálni, hogy az adott forgalom a megfelelő csatolón jön-e be
- Az érdektelen forgalmat ki kell szűrni a logból

Mentési rendszer elkészítése

- A find parancs megfelelő paraméterezésével szinte kész is vagyunk
- Teljes mentés

```
# find / /var ... -mount ! -path '/var/backups*' -depth -print0 |  
    cpio -o0Hcrc | gzip > /var/backups/2005.10.21.cpio .gz
```

- Inkrementális mentés

```
# find -newer /var/backups/stamp \  
    -depth -print0 | ...  
  
# touch /var/backups/stamp
```

Jail-ek használata

- A jail Linux-on a chroot rendszerhívásra épül (nem valódi jail, mint BSD-ken)
- A chroot eltakarja a rendszer kívül eső részeit
- Használata a chroot paranccsal lehetséges
- A szerverek indító scriptjeit módosítani kell
- A naplózásra nagyon figyelni kell

`syslog -a <új socket>`

Köszönöm a figyelmet

(az előadás kiegészített, szöveges változata hamarosan elérhető lesz a <http://kolab.fsf.hu> oldalon)

Linux rendszerek biztonságosabbá tétele a gyakorlatban

Mátó Péter <atya@fsf.hu>