A biztonság – életstílus

Rövid, egyszerű recept a biztonság megteremtéséhez, biztonsági mentések készítéséhez, a rendszer figyeléséhez és játékokhoz.

Akik rendszeresen olvassák a rovatomat, tudják, hogy a biztonság a mániám. Ez alkalommal is a rendszer- és hálózati biztonságról olvashattok, de most a David-féle szentírást szeretném megismertetni veletek. Nem engedhetem meg magamnak azt a fényűzést, hogy egy nyugodt irodában üldögélve elmélkedjek a biztonságról, tőlem azt várják az ügyfeleim, hogy a lehető legmagasabb fokú biztonságot teremtsem meg a számukra, és mindezt úgy, hogy közben ne kelljen egy rakás pénzt elköltenük. A receptem roppant egyszerű és rövid, de azt előrevetném, hogy aki jóvágású öltönyössé szeretne válni, szerintem foglalkozzon más területtel.

Először is állíts le minden nélkülözhető hálózati szolgáltatást (kezdve az `inetd`-vel, ha semmi olyan nem fut, amit ez indítana). Az ellenőrzésre megfelel a `netstat -tupan` parancs. Készíts minél szigorúbb */etc/hosts.allow* szabályokat (az ellenőrzést a `tcpdchk` és a `tcpdmatch` segítségével végezheted el), majd a Netfilter szűrőtábláját körültekintően használva tilts le mindent, amit nem akarsz kifejezetten engedélyezni.

Győződj meg arról, hogy a hálózati szolgáltatásokat nyújtó programok (Apache, Sendmail, `wu-ftpd`, `sshd` stb.) lehető legújabb változatát használod. A naplófájlokat minden nap nézd át, és keress bennük rendellenességeket (a megfelelő programokkal a szokásos bejegyzéseket kiszűrheted). A naplók jó esetben egy rendkívül biztonságos központi kiszolgálókra kerülnek.

Ellenőrizd, hogy a felhasználók biztonságos jelszavakat használnak-e. Ügyelj arra, hogy a nyilvánosság a tűzfalon keresztül csak a neki szánt hálózati részeket érje el, az érzékeny adatokat forgalmazó belső hálózathoz az Internetről ne lehessen hozzáférni. Használj VPN-t (FreeS/WAN, OpenSSH), és lehetőleg minden hálózaton keresztül továbbított adatot titkosíts (FreeS/WAN, OpenSSH, GnuPG).

Ne tulajdoníts túl nagy jelentőséget a dolgoknak, ha gond nélkül túlléphetsz rajtuk. A felhasználóid újra és újra meg fognak lepni azzal, hogy mennyire nem értenek bizonyos dolgokhoz, és milyen sokat tapogatóznak a sötétben, amit te akár támadásnak is vélhetsz. Pedig nem az.

A recept segíteni fog, ám semmit nem ér, ha kifelejtjük az egyik nélkülözhetetlen összetevőt: a biztonság életstílus, nem pedig programok vagy tiltások halmaza. Mutass példát, és segíts másoknak munkájuk során a biztonságos eljárások kialakításában. Ők lehetnek szemed fényei, de legszörnyűbb rémálmaid szereplői is. Ha a fentiekhez vallásos elvakultsággal ragaszkodsz, nem fogsz betörés áldozatává válni. Ha mégis baj történne, húzd le a hálózatot, derítsd ki, hogy a támadó hogyan jött be (és mi volt a célja), majd hozd rendbe a rendszert, újra nézz körül javítások után, zárd be az ajtót, és lehetőleg torlaszold el az utat, ahol a betörő bejutott, majd irány a hálózat.

A hatóságokat is lehet értesíteni, de ne ez legyen az első dolgod, hacsak a nyomozásra és a vádemelésre fordított fáradság kifizetődőnek nem bizonyul.

hdup

Rendszeres biztonsági mentéseket kell készítened egy gépről? Mi lenne, ha mindent átmásolnál egy másik gépre? Esetleg titkosítani is lehetne az anyagot, nem? Más nem is kell. Csak add meg a kívánt műveletet – teljes vagy növekményes mentést is végezhetsz – egy beállítófájlban, majd hívd meg a programot havonta, hetente vagy naponta. A futtatásához szükséges: glibc, bash, openssh és mcrypt (elhagyható).

➲ http://www.miek.nl/projects/hdup/hdup.shtml

Nebula Cards

Akar valaki zsugázni? Haverok és gépi játékosok ellen egyaránt játszhatsz. A különféle, négy játékossal folyó játékok – fekete macska, bridzs – megírása sem lehet ördöngösség. A felület egy Java-kisalkalmazásnak köszönhetően webes. Futtatásához Java szükséges.

➲ http://nebulacards.sourceforge.net

User-Friendly IPTables Firewall

Ha gondot okoz az IP Tables szabályok elkészítése, próbáld meg az UIF segítségével. Ugyan a szabályok ellenőrzésére az UIF még nem képes, de legalább segít az elkészítésükben.

A UIF beállítóállománya jóval egyszerűbb, mint maguk az IP Tables szabályok, tehát először írd meg a beállítófájlt, majd az UIF eme jóval érthetőbb bemenet alapján elkészíti a szabályokat. A program az összeköttetés alapú kapcsolatokat is kezeli. Futtatásához szükséges: Perl, NetAddr::IP és Net::LDAP Perl modulok, valamint értelemszerűen IP Tables.

➲ http://lug.mfh-iserlohn.de/uif

Linux Monitor

Remek segédprogram, ha a rendszer létfontosságú jellemzőit akarod szemmel tartani. Ha kezd megtelni valamelyik lemez, vagy nem fut valamelyik szolgáltatás, `syslog`-bejegyzést készít. A Linux Monitor más programot is el tud indítani, neked csak a kívánt időközt kell megadnod, a `linux_mon` mindent lát. Különösen akkor használható hatékonyan, ha nagyszámú gép küldi a jelentéseket egy központi naplónak. Futtatásához libcrypto, libdl és glibc szükséges.

➲ http://sourceforge.net/projects/linux-mon

Linux Journal 2002. október, 102. szám

David A. Bandel (dbandel@pananix.com) jelenleg Panamában él, Linux- és Unix-tanácsadással foglalkozik. Társszerzője a Que Special Edition: Using Caldera OpenLinux című könyvnek.