Szokatlan azonosítók

Nézz bele a **/etc/passwd** fájlba új és főként 0-ás UID vagy GID azonosítók után kutatva:

 # less /etc/passwd

 # grep :0: /etc/passwd

A normális azonosítók is a listában lesznek, de az új, nem várt azonosítókat kell észlelni. Az elütő jogosultságok és tulajdonosok is kitűnnek a /bin és /lib alatt az **ls –la** kimenetében (default **chmod/chown** rootkit beállítások)

Szokatlan naplóbejegyzések

Nézd át a rendszer naplófájljait gyanús események után kutatva, beleértve ezeket is:

Promiscuous (válogatás nélküli csomagelkapás) mód: „entered promiscuous mode", azaz minden csomagot elkapó módba lépett

Nagyszámú sikertelen hitelesítés vagy belépés helyi vagy távoli belépést adó eszközzel (pl. telnetd, sshd stb.)

A naplóbejegyzéseket takarítani is szokták a támadók a nyomok eltűntetésére, ezért érdemes szokatlanul hosszú hiányzó időintervallumokat keresni a naplókban.

Web-szerverek esetében: nagyszámú Apache „error" szót tartalmazó naplóbejegyzésre kell keresni.

Kiegészítő segédeszközök

A következő eszközök legtöbbször be vannak építve a Linuxba, de a rendszer biztonsági állapotának részletesebb elemzésére is használhatók:

A Chrootkit a felhasználói vagy kernel-szintű RootKit-ek által eredményezett anomáliákat kutatja a rendszerben (utólag is segíthet)

http://www.chkrootkit.org – ingyenes

A Tripwire a kritikus rendszerfájlok változásait kutatja (utólag már kevésbé hasznos)

http://www.tripwire.org (szabadon elérhető verzió: http://sourceforge.net/projects/tripwire)

Az AIDE is a kritikus rendszerfájlok változásait figyeli (ez sem segít sokat utólag)

http://www.cs.tut.fi/~rammer/aide.html

A Tripwire és az AIDE használatát el kell kezdeni már a telepítés után, még a hálózatra kapcsolódás előtt.

Nagyon fontos, hogy feltört vagy gyanús gépről ne lépjünk be másik gépre még SSH-val sem, és ha megtettük, akkor azokon a gépeken is vizsgálódjunk, és változtassunk jelszót!

Ha az adott gépen nem tudunk dolgozni, akkor kívülről is lehet vizsgálódni (portscan, nmap), de a kapott válaszokban ekkor sem kell feltétel nélkül megbízni (pl. lehet hátsó bejárat a kívülről nézve normálisan szolgáltató Web-szerverben is).

Hun-CERT
HUNGARIAN NATIONAL COMPUTER EMERGENCY RESPONSE TEAM

CERT.HU zsebsorozat*

http://www.cert.hu/ismert

Betörésészlelés Linux Rendszerekben

(v1)

Valamilyen rendszerességgel (pl. hetente, naponta) érdemes átfutni az itt részletezett lépéseken, és használni az ismertetett eszközöket akkor is, ha „nem történt semmi gyanús" a rendszerben.

Amennyiben valami gyanús történt, fontos, hogy nem szabad pánikba esni, az csak növelheti a bajt. Incidens esetén kapcsolatba kell lépni az incidenskezelő szervezettel (céges, helyi vagy országos), ezért írd ide az elérési adataikat, és inkább ne legyen rá szükséged, minthogy ne legyen kéznél, ha kell:

Név: ----------
Telefon: ----------
E-mail: ----------
Web: ----------

Időnként látogasd meg a Hun-CERT lapját is, az újabb verziókért vagy egyéb hasznos anyagokért, információkért. Szívesen vesszük a visszajelzéseket is, hogy mit tartasz hasznosnak, vagy mi szorul kiegészítésre!

a Hun-CERT csapat

* A SANS „Pocker Reference Guide" anyaga alapján.

Készítők: Rigó Ernő, Kincses Zoli és külön köszönet Mátó Péternek

Szokatlan processzek

Futó alkalmazások megtekintése (ha a támadó a lekérdező parancsokat lecserélhette, akkor a /proc bejegyzéseket kell vizsgálni):

 # ps –aux

Ismerni kell a „normális” működés során futó alkalmazásokat. Kutatni kell a szokatlan alkalmazásokat, különösen a root jogokkal (UID 0) futó alkalmazásokat kell figyelni.
Ha kiszúrunk egy ismeretlen alkalmazást, vizsgáljuk ki a szokatlanságot ezzel:

 # lsof –p [pid]

Betöltött rosszindulatú kernelmodul ellen csak a clean reboot véd, ezért legyen egy ilyen rendszerünk kéznél (pl. Knoppix boot CD).

Szokatlan fájlok 1.

Utánanézünk: a szokatlan SUID root fájloknak és nagy fájloknak (ismerni kell a normális SUID és nagy fájlokat):

 # find / –type f –perm +7000 –ls vagy inkább:

 # find / \(–uid 0 –or –gid 0 \) –perm +7000 –ls

 # find / –size +10000k –ls

Utánanézünk a ponttal kezdődő nevű fájloknak kivéve a /home és /tmp mappákat:

 # find / \(–not \(–path '/home/*' –or –path '/tmp/*' \) \) –name '.*' –ls

Mindenféle szokatlan állománynév kiszűrése:

 # find / \(–not \(–path '/home/*' –or –path '/tmp/*' \) \) –name '*[^a–zA–Z0–9_.]*' –ls

Szokatlan fájlok 2.

Egy RPM-mel telepített (pl. RedHat) Linux esetén futtassuk ezt a parancsot:

 # rpm –Va //Debian esetén: **debsums**

Különös figyelemmel kell lenni az eltérésekre a (/usr)/sbin és a (/usr)/bin alkönyvtárakban. Pl. nem man formátumú fájl a /man alatt, vagy nem a csomagba tartozva felkerült fájlok. 1-1 példa:

 # find /bin –exec file {} \; | grep –v ELF

 # find /*bin /usr/*bin –exec dpkg –S {} \; | grep 'not found'

Könyvtári függvény felülbírálást lehetővé tevő LD_PRELOAD környezeti változók beállításának keresése legalább a /etc-ben és a cron-ban.

SSH host-kulcsok változásának figyelése (továbblépés másik gépre veszélyes)!

Szokatlan hálózati működés 1.

A „válogatás nélkül” módot kell kutatni, mert ez lehallgatóra (sniffer) utalhat:

 # ip link | grep PROMISC

A nem elsődleges routing tábla is fontos. Minden routing paraméter lekérdezése (nem kellemes olvasmány, de a támadó tehet routing bejegyzéseket, amit átlagos felhasználó sose nézne meg):

 # ip route ls table 0

Sok levelet küld-e a gép (spam küldésre használják, csak azért törték fel):

 # tcpdump –i eth0 dst port 25

Szokatlan hálózati működés 2.

Keresés szokatlan portokon-figyelőkre:

 # lsof –i

 # netstat –nlp

Ismerni kell, mely TCP és UDP portokon figyel egy normális alkalmazás, és az ettől való eltérést kell figyelni.

Figyelni kell a szokatlan ARP bejegyzésekre, a MAC címre leképzett IP címekre, melyek nem szabályosak a LAN-nak:

 # arp –a

Szükséges ismerni, hogy mi feltételezhető, hogy a LAN-on van.

Szokatlan időzített processzek

Ellenőrizni kell a cron-ból futó root vagy bármelyik UID 0 azonosítójú felhasználó által időzített feladatokat:

 # crontab –u root –l

Figyelni kell a szokatlan rendszert-érintő cron feladatokra:

 # cat /etc/crontab

 # ls /etc/cron.*

Szokatlan időzített processzeket az atd is indíthat (ld. még **at** és **atq** parancsok leírását a man-ban), így ezekre is figyelni kell (a root által indított **atq** minden futó processzt kilistáz).