Szokatlan naplóbejegyzések

A naplóbejegyzések megtekintéséhez futtassd:

```
C:\> eventvwr.msc
```

Gyanús bejegyzések lehetnek:

„Az Eseménynapló szolgáltatás leállt” (Event log service was stopped). A naplózás leállt, de ha a gép tovább működött, akkor ez nem rendeltetésszerű.

„A Windows fájlvédelem nem aktív a rendszerben” (Windows File Protection is not active on this system). Több fájlt is „figyel” a rendszer, és illetéktelen változás esetén helyrehozza őket (egy cache-ből visszamásolja az eredetit), így gyanús a kikapcsolt állapot, ld. Sajátgép→Eszközök→Mappa beállításai→Nézet→Az operációs rendszer védett fájljainak elrejtése (My Computer→Tools→Folder Options→View→Hide protected operating system files).

„A Microsoft Telnet szolgáltatás sikeresen elindult” (*The MS Telnet Service has started successfully*). Alaphelyzetben nincs szükség a szolgáltatásra, így ha elindult, akkor gyanús, hogy kapcsolódást akarnak a gépünkkel.

Nézz utána a nagyszámú hibás bejelentkezésnek vagy kizárt azonosítónak (jogosulatlan jelszópróbálkozások jelei).

A listában az egyes oszlopok fejlécein kattintva egyet vagy kettőt növekvő ill. csökkenő sorrendbe állíthatók az adott oszlop szerint az események, így könnyebb átnézni őket.

A Művelet (Action) és Nézet (View) menükben beállíthatók a naplózás paraméterei.

Kiegészítő segédeszközök

A következő eszközök nem részei az operációs rendszernek, de a rendszer mélyebb biztonsági elemzésére használhatók. Mindegyik szabadon letölthető és használható.

- Nagyon sok rendkívül hasznos eszköz és webhopp:
`http://www.sysinternals.com`

Különösen a *mon eszközök hasznosak (Filemon, PMon, Regmon, Portmon), de a PsTools és a Process Explorer is jó, ha a CD-re írt túlélőkészlet része.

- Fájlok sértetlenségének (központi, több gépre alkalmazható) ellenőrzéséhez:
`http://osiris.shmoo.com/download.html`

- Windows rendszerekhez elérhető az MBSA nevű eszköz, mellyel sok biztonsági beállítás tesztelhető le, és a helyes beállításokhoz segítséget is az elemzés után:
`http://tinyurl.com/2e5fe`

- Windows 2000 Resource Kit Tools:
`http://tinyurl.com/1px9`

Különösen a **`pulist`** és a **`pstat`** parancsok mutatnak részletes információt a futó processzekről, de sokszor (ha nem elég profi a támadó, hogy elrejtse tevékenységét) a CTRL+ALT+DEL billentyűk sorrendben történő lenyomására előbukkanó ablak Feladatkezelő (Task Manager) részében is észrevehető, hogy mi okozza a nagy terhelést. Parancssorból:

```
C:\> taskmgr.exe
```

Hun-CERT
HUNGARIAN NATIONAL COMPUTER EMERGENCY RESPONSE TEAM

CERT.HU zsebsorozat*
http://www.cert.hu/ismert

Betörés-felfedezés Windows 2000-ben (XP és 2003 megoldásokkal is)

(v1)

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

Amennyiben valami gyanús történt, fontos, hogy *nem szabad pánikba esni*, az csak növelheti a bajt, és lehetőleg *csak abban az időben kapcsolódjunk a hálózatra, amíg jelen vagyunk*, így észlelhetjük a gyanús jelenségeket.

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 „Pocket Reference Guide” anyaga alapján.

Szokatlan processzek

Szokatlan processzek után lehet kutatni a Feladatkezelőben (Task Manager) (CTRL+ALT+DEL, vagy **`taskmgr.exe`**)

Érdemes megjegyezni, hogy mi fut alapból (telepítés után). Amelyiknek nem tudjuk a szerepét, arra keressünk rá egy internetes keresőben a 'security' szóval együtt.

Windows XP és 2003 rendszerekben a „SYSTEM" vagy „Rendszergazda (Administrator)" és az utóbbi csoportba tartozó felhasználókra kell jobban figyelni.

Nézz utána a szokatlan hálózati forgalomnak:

```
C:\> net start
```

Érdemes megnézni a parancs kimenetét hálózat nélküli időben és hálózati kapcsolat során többször is (egy-egy alkalmazás indítása előtt, közben, után).

Szokatlan fájlok

Ellenőrizd a fájlok méretét és a lemeztelítettséget (a feltört gépekre sokszor felkerülnek nagyméretű fájlok, melyeket másoknak kínálnak fel letöltésre, ezek többnyire szerzői jogot is sértő fájlok). Jobb klikk a partíción állva az egérrel, vagy: **`C:\> dir c:\`** (az utolsó sor kiírja a szabad lemezterületet).

A *Start→Keresés (Search)→Fájlok és mappák (For Files or Folders...)* segítségével adott méretnél (ld. Keresési opcióknál) nagyobb fájlokat kereshetsz.

Szokatlan hálózati jelenségek

Nézd meg a megosztásaidat, és ellenőrizd, hogy szükséges-e mindnek a fenntartása, de törölni is csak akkor törölj egy megosztást, ha utánajártál, hogy mi a következménye ennek.

```
C:\> net view \\computer_name
```

```
C:\> net share
```

Nézd meg, ki nyitott kapcsolatot a gépeddel:

```
C:\> net session
```

Nézd meg, géped kivel nyitott kapcsolatot:

```
C:\> net use
```

TCP/IP feletti NetBIOS tevékenység:

```
C:\> nbtstat –S
```

Gyanús készenlét TCP és UDP portokon:

```
C:\> netstat –na |more
```

Folyamatos frissítés 5 mp-enként (CTRL+C-vel leállítható)

```
C:\> netstat –na 5
```

Az XP és 2003 verziókban van '**–o**' kapcsoló, mely megmutatja a saját processz számát:

```
C:\> netstat –nao 5
```

Ezek esetében is ismerni kell a normális működést, hogy észlelhessük az eltéréseket.

Érdemes a help-et is használni a további lehetőségek megismeréséhez:

```
C:\> net help
```

```
C:\> netstat help
```

Szokatlan időzített feladatok

Nézd meg az időzített feladatokat a helyi rendszerben:

```
C:\> at
```

Használható a grafikus felület is:

Start→Programok→Kellékek (Accessories)→ Rendszereszközök (SystemTools)→ Ütemezett feladatok (Scheduled Tasks)

A szokatlan feladatokat kell keresni, különösen azokat, amelyek az Rendszergazdák (Adminisztrátor) csoportba tartozók nevében fut SYSTEM-ként vagy üres felhasználói névvel.

Szokatlan azonosítók

Adminisztrátorok csoportja:

```
C:\> lusrmgr.msc
```

Klikk a Csoportok (Groups), majd azon belül az Rendszergazdák (Administrator) sorra, melyen belül megtekinthető a tagok listája.

Ajánlatos a programtelepítéseket a rendszergazdai azonosító alól végezni, de a mindennapi használat során egy másik azonosító alól dolgozni. Ez a másik azonosító ne legyen a rendszergazda-jogú csoport tagja, így ha ezt az azonosítót feltörik, még nem férnek hozzá a teljes rendszerhez.