Hatósági eljáráshoz szükséges bizonyítékok gyűjtése

Windows

Alapok[1]: http://www.securityfocus.com/infocus/1653 (Windows Forensics: A Case Study, Part One, December 31, 2002), és http://www.securityfocus.com/infocus/1672 (Windows Forensics: A Case Study, Part Two, March 5, 2003) by Stephen Barish

Amikor a nemkívánatos esemény bekövetkezik, rendelkeznünk kell a megfelelő eszközökkel és eljárásokkal, hogy rögzítsük az esemény minden nyomát a későbbi eljárás sikerességéért.

1 Észlelés és lehetséges incidensek

A leginkább problémára mutató jel a hálózati forgalom váratlan megnövekedése. Amennyiben ez a támadók miatt van, akkor mélyen bent vannak a rendszerben, és a legkülönfélébb dolgokat művelhetik: szerzői jogvédelem alá tartozó alkotásokat cserélnek, másokat támadnak (persze, a mi nevünkben), reklámlevelekkel árasztják el a hálózatot.

A másik jellemző problémára utaló jel, amit erős behatolásérzékelő vagy tűzfal nélkül is észre lehet venni, az a váratlan forgalom megjelenése. A SANS ezt nevezi a „hazai pálya előnyének", vagyis, a saját rendszerben előforduló eseményeket ismerve hamar feltűnik, ha valami az eddigiektől eltérően működik. Amennyiben a forgalom mennyisége tér el, annak okát kell kideríteni, de amennyiben számos NetBIOS kommunikáció megy végbe egy menedzsment interfészen, ami normális esetben kódolt kapcsolaton keresztül szokott menni, akkor biztonsági problémánk van.

Annak megértéséhez, hogy egy esemény normális vagy sem, ismerni kell a normális működés tulajdonságait. Ehhez szabadon elérhető eszközök állnak rendelkezésre, melyek egy Linuxos laptopról futtathatók a legegyszerűbben. Mivel ez nem egy integrált vállalati rendszer, szükséges egy saját készlet összeállítása, melyben a hasznos alkalmazások megtalálhatók. Az Internetről letölthető többféle ilyen összeállítás, de idővel úgyis saját szükségletek szerint válogatjuk össze magunknak, ami bevált. Néhány alapeszköz, amit a legtöbb készlet tartalmaz, és méltán neves eszközök[2]:

- *Ethereal*: Windows és Linux rendszerre szabadon elérhető grafikus felülettel rendelkező hálózati forgalom-elemző.

  http://www.ethereal.com/

- *EtherApe*: Jelenleg csak Linux rendszerre elérhető hálózati kommunikációs térkép-készítő, és kiváló segítség a normális hálózati kommunikáció meghatározásában.

  http://etherape.sourceforge.net/

- *tcpreplay*: elmentett hálózati kommunikáció „újrajátszásához" való eszköz, mellyel az újrajátszás sebessége is állítható, így segítve a tesztelés-elemzés menetét.

  http://tcpreplay.sourceforge.net/

- Dan Farmer és Wietse Venema gyűjteménye feltört UNIX-ok elemzésére.

  http://www.porcupine.org/forensics/tct.html

Az egyes eszközöket valamilyen kombinációban is lehet használni (pl. tcpreplay és EtherApe a hálózati forgalom anomáliák felderítésére). Mára olyan mértékű szolgáltatás-palettával rendelkeznek ezek az alkalmazások, hogy minden lehetőségük kihasználása csak idővel válik lehetségessé a megfelelő számú és mélységű használat után.

Nagyon fontos, hogy legyen legalább egy ember, aki használja ezeket az eszközöket, és figyeli a kiugró jelenségeket, hogy idejében nyomozni lehessen az okok után, és azonosítani lehessen a támadást.

1 Átfogalmazta és billentyűzte: kincses zoli, támogatta: Hun-CERT (http://www.cert.hu/). 2005. június.

2 Itt említjük meg az MTA-SZTAKI Hálózatbiztonsági Osztálya által készített ToReS (Tools Related to Security) CD-t, melyről bővebb információ a http://nsd.sztaki.hu/ címen érhető el.

1.1 A támadás azonosítása

Minden hálózatra kötött számítógép támadásnak lesz kitéve, hiszen manapság az automatikus pásztázó és sebezhetőség-kereső eszközök nem is foglalkoznak azzal, hogy kié a célgép. Felmérik egy-egy tartomány összetételét, felépítését, és amint megjelenik egy sebezhetőség, a felmérés eredményei közül keresik ki a támadható gépet.

A károk csökkentésének kulcsa a támadás azonosítása és megértése, valamint a helyreállítás és a következő támadás elkerülésének lehetőségei. Tekintsük a Web-szerver szolgáltatás példáját, amikor a Web4sale.com cég hálózatán kimagasló forgalmat észlelünk. A cég egy központi pontból menedzseli a hálózatot privát hálózatot használva (10.20.0.0/24). Ebből a C osztályú hálózati címtartományból várjuk el a hálózati kommunikációban résztvevők címeit. Ebből kiindulva térképezzük fel, hogy mi történhetett a cég hálózatán.

Az első lépés a gyanús forgalom okának felderítése. Az elvárt címtartományon belül is SSH-val kódolt kommunikációt várunk el, így minden, ami nem ennek megfelelően zajlik, az gyanús. Egy Linuxos laptoppal és a tcpdump programmal felszerelve kiszemelünk egy hosztot, melyet megfigyelünk és csomagjait elkapjuk (sniff). A switch-elt hálózatban a router mirror portjára csatlakozva a számunkra érdekes forgalmat tükrözzük:

```
tcpdump –i eth0 –s 1500 host winbox.private.com
```

ahol eth0 a lehallgató felület és winbox.private.com a megfigyelt szerver menedzsment felülete.

A kapott adatokból két anomáliát észlelünk. Elsőként a nagymértékű NetBIOS forgalmat a privát felületen:

```
10/02/02  08:27:18  netbios.public_ip.com  137   ->   winbox.private.net  137
10/02/02  08:27:19  netbios.public_ip.com  137   ->   winbox.private.net  137
10/02/02  08:27:20  netbios.public_ip.com  137   ->   winbox.private.net  137
```

Második anomáliaként egy nyilvános IP-cím szerepel az adatokban (netbios.public_ip.com).

Első szabály: a hazai pálya előnyének kihasználása. Mivel e két anomáliának nem szabadna előfordulnia a hálózati forgalomban, biztosak lehetünk a jogosulatlan hozzáférésben. A következő lépés a Winbox gépen történt események feltárása, miszerint kívülről vagy belülről történik a jogosulatlan használat. Ehhez magát a hosztot kell vizsgálni.

1.2 Hoszt-alapú vizsgálat

Nagyon fontos tudatosítani, hogy egy vizsgálat alatt lévő hoszton semmiben sem szabad megbízni. Úgy kell tekinteni, hogy a hosztot feltörték, root-kit-et helyeztek el rajta, és figyelik azt is, hogy valaki vizsgálja-e a rendszert[3]. Elsőként el kell dönteni, hogy a gépet lekapcsoljuk a hálózatról vagy sem. Nincs egyértelmű válasz, mert ha úgy ítéljük meg, hogy a tevékenység további károkat okozhat, akkor kapcsoljuk el, míg ha a jogosulatlan felhasználó működését megfigyelve tudunk több információt szerezni és felderíteni a tevékenységét és a kilétét, akkor ne kapcsoljuk le a gépet a hálózatról.

Az igazságügyi vizsgálat a bűncselekménnyel kapcsolatos információ megszerzésének, rögzítésének és követésének a művészete annak érdekében, hogy egy lehetséges bírósági ügyben használni lehessen ezeket az adatokat. Ennek érdekében minden elővigyázatosságot meg kell tennünk azért, hogy az adatok pontosak, megbízhatóak, és nem módosultak az adatgyűjtés előrehaladtával. Az adatok gyűjtésének és feldolgozásának menetét rögzítve és az adatmozgatást követve (ki kezdeményezte, erre mi történt) támogatjuk a „felügyeleti lánc" megőrzését. Ez nem egy egyértelmű feladat, melyet a szakkönyvek is hosszasan taglalnak. A jó gyakorlat a bizonyítékok gyűjtésére a *megbízható eszközök használata*, *a mobil adathordozóra történő adatrögzítés* és *az adatok hitelességének biztosítása*.

Az első kihívás a megbízható eszközök használata. Alapjában véve minden szükséges eszköz megtalálható egy Windows 2000 rendszerben is, de mivel nem bízhatunk egy kompromittáltnak tekintett rendszerben, ezért össze kell állítanunk a magunk eszközkészletét. Egyszerűen szükségünk van egy (lehetőleg hálózatra nem kötött) operációs rendszer másolatra, melyet CD-re írunk. A CD tartalmazza a következő eszközöket is:

3 Klasszikus példa: A azt hiszi, hogy B-vel, B azt hiszi, hogy A-val kommunikál, és C azt hiszi, hogy csak ő egyedül ékelődött be és hallgat le mindent...

- at.exe – időzítetten futó alkalmazások
- cmd.exe – parancsablak
- dir.exe – könyvtártartalom listázása (win2k alatt nem külön fájl!)
- ipconfig.exe – Internet-beállítások lekérdezése, módosítása
- nbtstat.exe – TCP/IP feletti NetBIOS kapcsolatok statisztikái
- net.exe – a lokális hálózat lekérdezései (net help parancs ad részletezést a lehetőségekről)
- netstat.exe – hálózati kapcsolatok részletei és statisztikája
- nslookup.exe – Name Server lekérdezése
- route.exe – a routing tábla lekérdezése, módosítása
- tracert.exe – a géptől a paraméternek adott gépig vezető út lekérdezése

Az Interneten több hasznos szabadon használható biztonsági eszköz is elérhető. Ilyen az integritás-ellenőrzéshez használható md5sum.exe (nekem 49152 byte, Unix alatt a /usr/bin/md5sum 17032 byte :-)). A program generálja vagy ellenőrzi egy fájl MD5 lenyomatát, így ellenőrizhetjük, hogy az általunk ismert (pl. honlapon közzétett) lenyomattal rendelkezik-e az adott fájl.

A legjobb módszer forgalomfigyelés során a forgalom lemezre mentése és egy MD5 lenyomat készítése. Fontos, hogy a lenyomat nem garantálja az adatok manipulálatlanságát a lenyomat készítése alatt, így ezen a ponton kikezdhető az eljárás. Ezért szükséges a külső gépről arra a gépre történő mentés, és a lenyomat azon történő képzése, nem a feltört gépen végezve mindezt.

Windows rendszerekhez a legjobb eszközök a **Sysinternals.com** címén érhetők el[4]. Ezek közül néhány eszköz (az oldalon többféle operációs rendszerre sokkal több eszköz található), mely az egyes művelet monitorozására (innen a 'mon' végződések) alkalmazhatók:

- Diskmon – lemezműveletek
- Filemon – fájlrendszer műveleteinek
- PMon – futó eljárások és szálak
- Process Explorer – fájlok, registry kulcsok (a Regmon valós időben mutatja a bejegyzések változásait), objektumok, DLL-ek betöltése stb. Az egyes eljárások tulajdonosait is megmutatja.
- PsTools – Parancssori eszközök helyi vagy távoli gépen futó eljárások listázására, távoli eljárások futtatására, gép-újraindításra, naplófájlok lementésére stb.

Az elkezdett esetben azt kell meghatároznunk, hogy ki lépett be a rendszerbe, milyen erőforrások kerültek megosztásra és milyen eljárások futnak. Minden parancs CD-ről (pl. E:\) fut, és az eredmények lemezre (A:\) kerülnek:

```
E:\nbtstat -a winbox.private.com > a:\nbtstat-a_output.txt
E:\md5sum a:\nbtstat-a_output.txt > a:\nbtstat-a_output.md5
```

Ez az eljárás minden elkövetkező parancs esetén követendő, így később lehet elemezni az elmentett válaszokat. Az egyes eljárásokról hasznos könyvek[5] is elérhetők különböző eszközök felsorolásával, de ez az anyag inkább a technikákról szól, mint az elérhető eszközökről.

1.3 Mit keressünk?

A legelső feladat annak kiderítése, hogy mi történt, ki volt a vétkes és milyen hatása van az eseménynek. Sokan a megérzésre, tapasztalatra vagy éppen szerencsére hivatkoznak, de vannak mindenki által elfogadott célok és eszközök, melyeket lehet alkalmazni.

Cél	Eszköz / Módszer
Szokatlan eljárások azonosítása	pslist, psinfo, psfile
Szokatlan nyitott portok azonosítása	netstat, Fport, psservice
Szokatlan nyitott fájlok azonosítása	psfile, listdlls, Fport
Belépett felhasználók azonosítása	psloggedon, nbtstat
Eljárások tulajdonosainak azonosítása	psloggedon
Routing táblák vizsgálata	netstat, route
Időszakos fájlok vizsgálata	dir, type
Gyanús alkönyvtárak/mappák azonosítása	dir, Explorer

4 Az eredeti cikkben a Foundstone.com szerepelt, de azóta felvásárolták a céget, termékei pénzesek.
5 *Pl. Keith Jones: Anti-Hacker Toolkit, Kevin Mandia: Incident Response, cikkek a SecurityFocus-on.*

Rekonstruálni kell az eseményt. Ismerve a normális körülményeket rövid idő alatt le tudjuk folytatni a helyszíni vizsgálatot és egyben az adatgyűjtést. A későbbi vizsgálatok már hosszabbak lehetnek. Ráadásul folyamatosan a nyomok után kell kutatnunk, hogy azonosítsuk a támadók tevékenységét. Az ideiglenes fájlokat olyan szektor-szerkesztővel (sector editor) kell vizsgálni, melyekkel a részben felfedezett nyomokat is észlelhetjük. A kötegelt fájlok (*.bat) esetén azt kell vizsgálni, hogy módosultak-e, vagy olyan tartalmuk van, mely a támadó további lépéseit segíti. Végül, a Windows rendszerekben az eseménynapló (Event Log) és a biztonsági napló (Security Log) is vizsgálható.

A **winbox.private.com** esetében a következő rendszereszközökre van szükség a vizsgálat során: netstat, route, nbstat, hostname, net, dir. Ezeken felül szükség van az Fport, pslist, psloggedon és a pssservice segédeszközökre, hogy azonosítsuk a felfedezett gyanús eljárások tulajdonosait. A következő rész egy kivonat az eljárás során kiadott parancsokból és gyűjtött adatokból:

E:\hostname
```
Winbox.private.com
```

E:\nbtstat -a winbox.private.com
```
NetBIOS Remote Machine Name Table
Name                 Type       Status
---------------------------------------------
WINBOX               <00>       UNIQUE Registered
WINBOX               <02>       UNIQUE Registered
PROD                 <00>       GROUP  Registered
PROD                 <1E>       GROUP  Registered
..__MSBROUWS__       <01>       GROUP  Registered
ADMINISTRATOR        <03>       UNIQUE Registered
MAC ADDRESS = XX-XX-XX-XX-XX-XX
```

E:\net session
```
Computer  User name  Client Type     Opens   Idle time
-------------------------------------------------------------
\\TGT1  ADMINISTRATOR           0       00:00:27
\\TGT2  ADMINISTRATOR           0       00:00:15
\\TGT3  ADMINISTRATOR           0       00:00:23
\\TGT4  ADMINISTRATOR           0       00:00:05
```

E:\Fport.exe
```
Fport v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc
http://www.foundstone.com

Pid  Process    Port  Proto     Path
420  svchost ->  135   TCP      C:\WINNT\system32\svchost.exe
8    System  ->  445   TCP
888  MSTask  -> 1025   TCP      C:\WINNT\system32\MSTask.exe
8    System  -> 1027   TCP
8    System  ->  445   UDP
430  svchost ->   80   TCP      C:\Program Files\Apache\httpd.exe
1625 servu   -> 3215   TCP      C:\Client_Data\Inetpub\_vti-bin\ \servu.exe
```

Elsőként a célgép nevét ellenőriztük le, majd azt néztük meg, hogy ki van bejelentkezve a rendszerbe, milyen eljárások futnak és milyen szolgáltatások figyelnek az eszközön. A kimenetek között a nyomozás szempontjából több figyelembe veendő adat is van. Az első a NetBIOS megosztás a célgép és több más gép között a szerverek belső címének használatával. Tudjuk, hogy ez nem természetes, mivel a belső hálózati címek csak menedzsment célokat szolgálnának, és az erőforrás-megosztás a Fájl és Nyomtató-megosztással tételesen tilos a szabályzat szerint.

Minden esetben láthatjuk a tiltott kapcsolódásokat a helyi rendszergazda (Administrator) jogköréhez, és ez aggasztó esemény. Ennél is aggasztóbb az **Fport** kimenete szerint az, hogy a célgép olyan FTP szervert futtat egy ideiglenes porton (1024 feletti), melynek szokatlan helyen van a forrása (**C:\Client_Data\Inetpub_vti-bin** \) és egy rejtett alkönyvtárnak tűnik. Ez különösen gyanús, mivel a célgép Apache Web-szervert futtat, és az FTP-szerver könyvtárszerkezete egy olyan alkönyvtárban került elrejtésre, melynek struktúrája a Microsoft IIS szerver könyvtárstruktúrájára hasonlít.

Rekurzív módon listázva a rejtett alkönyvtárt megtaláltuk az FTP-szerver futtatható változatát, saját konfigurációs fájlját, több érdekes kötegelt fájlt, más konfigurációs fájlokat és eszközöket.

E:\dir /s /a C:\Client_Data\Inetpub_vti-bin\" "\ /p

Különösen érdekes volt a VFS_MNT.BAT nevű fájl (részlet a fájlból):

```
net use F \\tgt1\c$\WINNT\system32\ \_vti-bin\ /user:Administrator AdminPass
net use G \\tgt2\c$\WINNT\system32\ \_vti-bin\ /user:Administrator AdminPass
net use H \\tgt3\c$\WINNT\system32\ \_vti-bin\ /user:Administrator AdminPass
net use I \\tgt4\c$\WINNT\system32\ \_vti-bin\ /user:Administrator AdminPass
```

Először a támadó mount-olt egy rejtett alkönyvtárt helyi rendszergazdai jogokkal minden célgépen, megengedve a virtuális fájlrendszer létrehozását a tiltott FTP-szervernek. Ilyen módon megosztani a rendszergazdai jelszót természetesen nagyon igénytelen megoldás, de ebben az esetben ez történt. Nagyobb gond, hogy a támadó ezek után egy vagy több gépen keresztül is továbbíthat adatokat a gépekre telepített rejtett FTP-szervereken keresztül.

1.4 Kapcsoljuk össze az eredményeket

Minden incidensnek megvannak a tanulságai és jellegzetességei: 1) a nagy cégek rendkívül nagy sávszélességű Internet-kapcsolattal rendelkeznek; 2) nagyméretű Windows NT és 2000 hálózatok működnek a cégeknél; 3) folyamatosan sérül a rendszergazdai és domain gazdai azonosítók bizalmassága; 4) olyan elosztott kétlépcsős FTP-szerverek széleskörű használata történik, ahol a szerver gyökérkönyvtára több gép megosztott meghajtói fölött létrehozott virtuális fájlrendszert alkot. Az esetünk is ezekkel a jegyekkel rendelkezik, és mint a legtöbb alkalommal, a támadók warez és pornó tartalmat terjesztettek.

Az eljárásnak ebben az állapotában felfedésre került a kompromittálódás, a támadás lényege és megértettük, hogy mi történik a cégben, de még ki kell deríteni a támadók módszerét, amivel ezt elérték. Először néhány alapintézkedést el kell végezni: a rendszergazda jelszavát meg kell változtatni, csomagszűrőkkel korlátozni kell a NetBIOS használatát a cégen belül működő switch-ekben. Ki kell derítenünk a támadási módszer lényegét vagy hatáskörét. Ennek érdekében a következő fázisban a hálózati forgalmat elemezzük ki.

2 A cél

A warez és pornó tartalmak nagy forgalmat generálnak, így az erőforrás költsége is nagy, ezért fontos a támadóknak ingyen hozzájutni a megfelelő erőforrásokhoz (gépek megfelelő számban, hálózati kapacitás megfelelő sávszélességgel). A megfelelő beállításokhoz a helyi és a cégszintű rendszergazda jogokat is megszerezték a támadók. Célunk kideríteni a következőket: 1.) mennyire terjedt a támadók hatásköre a helyi hálózaton belül? 2.) mi volt az eredendő kompromittáló eljárás? és 3.) ki(k) volt(ak) a támadó(k), ha kideríthető mindez?

2.1 Eszközfejlesztés

Ideális esetben teljes mértékben felügyelt környezet és megfelelő személyzet áll rendelkezésre, akik figyelik az eseményeket, elemzik a naplókat, és megteszik a szükséges intézkedéseket. A legtöbb eset nem ideális: nem áll rendelkezésre hoszt vagy hálózati behatolásérzékelő, lépcsőzetes tűzfalrendszer, megfelelően erős azonosító és felruházó rendszer, és általában a naplózás is hiányos. Nagyobb intézmények esetében a helyzet még rosszabb, mert a rendszer és adatainak mérete és mennyisége nem teszi lehetővé az események valós idejű elemzését. Így az elkerülhetetlenül bekövetkező eseménykor szükség van egy gyors eszközre és eljárásra a hálózaton folyó események felméréséhez és a helyrehozatali intézkedésekhez.

Az ideális összetétel egy laptop Windows (+ Windows 2000 Resource Kit) és Linux operációs rendszerekkel és olyan eszközökkel, melyek mindkét rendszerhez elérhetők. Ezek a következők:

Eszköz	Windows	Unix
Hálózati lehallgatók	Windump, Ethereal	Tcpdump, Ethereal, dsniff
Betörésészlelők	Snort	Snort
Elemzők	–	EtherApe, tcpreplay
Port pásztázók	Fscan, nmapwin	Nmap

Ezen kívül létezhet még sok más eszköz is, de ezekkel már el lehet kezdeni a munkát.

2.2 Első lépések, a munka kezdete

Mielőtt elindítunk egy lehallgató programot, meg kell határoznunk, hogy milyen adatokat keresünk a hálózati forgalomban. Egy 100 Mbps switch-elt hálózatban természetes, hogy elárasztható egy lehallgató, egy elemző hoszt vagy egy elemző. Elsőként az áldozattá vált gépet érdemes figyelni, olyat, melyről tudható, hogy a támadó még használja.

Egy switch-elt hálózatban (a hálózati forgalom elemzése szempontjából a legrosszabb) legjobb a swicth és az áldozat közé a mirror portra csatlakozva lehallgatni a forgalmat. Nem kell a hálózati kapcsolatot megszakítva beékelődni, mert ezt a szakadást a támadó is észlelheti. Másik megoldás lehet az Ethernet aljzaton keresztüli csatlakozás. Az előbbi előnye, hogy megfelelő switch esetén gyorsan átállítható, hogy engedje megfigyelni a másik önálló hosztot vagy VLAN-t. Annak ellenére, hogy a tükrözés széles körben alkalmazott, biztosra vehető, hogy a VLAN csomagvesztést és ütközést fog okozni egyes switch-eken. Nem a legkívánatosabb megoldás, de használható, amit a következőkben mutatunk be.

2.3 Beépített Windows eszközök

A tcpdump (http://www.tcpdump.org) néven ismert Unix eszközök elérhetők Windows alatt is Windump (http://windump.polito.it) név alatt. A Windump a libpcap (WinPcap, http://winpcap.polito.it) segítségével kommunikál a különböző hálózati eszközökkel. A Windump olvasni és írni is tudja a tcpdump bináris kimeneti formátumát, így az adatgyűjtés és elemzés történhet különböző rendszereken is.

A Windump telepítése után a switch mirror portjára csatlakozva elkezdődhet a forgalom lehallgatása. A forgalom megjelenítési formája lehet szöveges, ASCII vagy hexa formátumú. A megfelelő módon alkalmazott szűrők segítségével a nagy mennyiségű forgalomból a számunkra érdekes részt tudjuk kicsemegézni. Például a következő parancs az **áldozat** és **cél** közötti forgalmat szűrve menti a kimenetként adott fájlba:

```
C:\> Windump -i1 host aldozat and cel -w kimenet.txt
```

A valóságban az elején nem tudjuk, hogy mit keresünk, ezért *minden forgalmat* mentsünk el. Az Ethernet maximális átviteli egysége (MTU) 1500 byte, a snaplength változót (-s kapcsoló) is erre állítjuk. Végül a -n kapcsolóval megelőzzük, hogy a Windump konvertálja a hoszt címeket és port számokat, mert ez megkímél attól, hogy a DNS-nek küldjünk címfeloldási kéréseket, miközben a DNS is lehet, hogy már a támadók kezében van.

```
C:\> Windump -i1 -s1500 -n -w output
```

A Windump a kimenetet is el tudja olvasni, és különféle szűrőkön át értelmezzük a kapott eredményt, bár sokkal intuitívebb egy grafikus elemzéssel is rendelkező eszközben vizsgálódni. Ehhez az egyik legjobb alkalmazás az Ethereal (http://www.ethereal.com).

Az Ethereal olyan grafikus felülettel rendelkezik, melyen kényelmes keresztugrások is végrehajthatók az elkapott csomagokon, azok fejlécén keresztül le magukig a kommunikációban átvitt adatokig. Ugyancsak alkalmas protokollelemzésre és TCP folyamok feltérképezésére.

Az Ethereal tartalmaz egy sokoldalú szűrőnyelvet, így sokkal könnyebb a begyűjtött adatokból azokat kiszűrni, amelyekre szükségünk van, de ez a szűrés arra is jó, hogy különböző szempontok szerinti szűréssel vizsgáljuk ugyanazt az adatmennyiséget.

2.4 Mit keressünk?

Annak ellenére, hogy minden támadásnak van valami sajátossága, vannak minden támadás esetén alkalmazható, vagyis ellenőrizendő technikák és jelenségek. Ezek a következők:

- Legnagyobb forgalmúak (kimenet)
- Legnagyobb forgalmúak (bemenet)
- Leginkább használt portok és protokollok
- Összehasonlítás ismert és valós forgalommal
- Koordináció / korreláció az igazságügyi vizsgálattal

Az első négy elem természetesnek tűnik, míg az utolsót gyakran el szokták felejteni. Emlékezzünk a példaesetre, amikor egy olyan fájlt találtunk az egyik feltört gépen, mely végrehajtásakor kapcsolatot akart létesíteni több más géppel is, mint rendszergazda jogú felhasználó. Teljes tartalomfigyeléssel és az Ethereal segítségével hozzáfoghatunk további anomáliák kereséséhez.

```
C:> Windump -i2 host TGT1 -s1500 -w output
```

Egy ideig gyűjtjük a forgalmi adatokat (jellemzően egy órai blokkot érdemes gyűjteni pár perces átfedésekkel), majd elemezzük őket. Az Etherealba töltött adatokra szűrőket alkalmazunk, hogy az SMB csomagokat (ezt alkalmazza a Windows Fájl Sharing) külön vizsgálhassuk, és megtaláljuk a TGT1-től és a TGT1-hez menő kapcsolatokat (mind a menedzsment interfészen, ami a windump -D szerint a 2. számú a mi esetünkben). Amint feltételeztük a TGT1 felé egy sor kapcsolódást találunk:

Nr.	Idő	Forrás	Cél	Protokoll	Infó
27	4.7277	winbox.victim.com	TGT1.victim.com	SMB	TREE CONNECT ANDX REQUEST, NTLMSSP AUTH
35	5.2552	winbox.victim.com	TGT1.victim.com	SMB	TREE CONNECT ANDX REQUEST, NTLMSSP AUTH
42	6.3521	winbox.victim.com	TGT1.victim.com	SMB	TREE CONNECT ANDX REQUEST, NTLMSSP AUTH

Ezek Windows fájlmegosztáshoz való hozzáférési kéréseknek tűnnek. Valójában gyors kapcsolódásokat látunk a winbox.victim.com felől a TGT1.victim.com felé, ami szintén gyanús, mert automatikus kapcsolódási kísérleteket jelent. Tovább szűrve az adatokat és az Ethereal natív protokoll dekódolóját használva a következő szekvenciákat tudjuk rekonstruálni:

```
FILTER:  (ip.addr eq 192.168.254.2 and ip.addr eq 192.168.254.205) and (tcp.port eq 1095
and tcp.port eq 445)

Resulting Stream (Excerpt1)

00000389  00 00 01 48 ff 53 4d 42  73 00 00 00 00 18 07 c8 ...H.SMB s.......
00000399  00 00 00 00 00 00 00 00  00 00 00 00 00 00 ff fe ........ ........
000003A9  01 08 50 00 0c ff 00 48  01 04 11 0a 00 01 00 00 ..P....H ........
000003B9  00 00 00 a6 00 00 00 00  00 d4 00 00 a0 0d 01 4e ........ .......N
000003C9  54 4c 4d 53 53 50 00 03  00 00 00 18 00 18 00 66 TLMSSP.. .......f
000003D9  00 00 00 18 00 18 00 7e  00 00 00 0c 00 0c 00 40 .......~ .......@
000003E9  00 00 00 0e 00 0e 00 4c  00 00 00 0c 00 0c 00 5a .......L .......Z
000003F9  00 00 00 10 00 10 00 96  00 00 00 15 82 88 e0 4c ........ .......W
00000409  00 41 00 50 00 54 00 4f  00 50 00 73 00 62 00 61 .I.N.B.O .X.A.d.m
00000419  00 72 00 69 00 73 00 68  00 4c 00 41 00 50 00 54 .i.n.i.s .t.r.a.t
00000429  00 4f 00 50 00 a0 22 69  06 b4 2d 12 7f 00 00 00 .o.r.."i ..-....
00000439  00 00 00 00 00 00 00 00  00 00 00 00 00 8b e9 d5 ........ ........
00000449  b8 26 a1 f2 01 06 6b 6c  e3 62 0d 7f fa 63 15 7f .&....kl .b..c.
00000459  7d d6 64 30 5e d0 ca 7d  5f 30 5f 13 a4 a7 c3 15 }.d0^..} _0_.....
00000469  d1 fb 87 33 8b 00 57 00  69 00 6e 00 64 00 6f 00 ...3..W. i.n.d.o.
00000479  77 00 73 00 20 00 32 00  30 00 30 00 32 00 20 00 w.s. .2. 0.0.2. .
00000489  32 00 36 00 30 00 30 00  20 00 53 00 65 00 72 00 2.6.0.0.  .S.e.r.
00000499  76 00 69 00 63 00 65 00  20 00 50 00 61 00 63 00 v.i.c.e.  .P.a.c.
000004A9  6b 00 20 00 31 00 00 00  57 00 69 00 6e 00 64 00 k. .1... W.i.n.d.
000004B9  6f 00 77 00 73 00 20 00  32 00 30 00 30 00 32 00 o.w.s. . 2.0.0.2.
000004C9  20 00 35 00 2e 00 31 00  00 00 00 00              .5...1. ....
```

Amikor az Ethereal dekódolja az SMB adatfolyamot, '.' jeleket illeszt be az egyes karakterek közé, mivel a legtöbb alacsony szintű naplózás és kommunikáció Unicode karaktereket használ a Windowsban. A Unicode-ban az 'US' karakterek felső byte-ján '00' karaktereket tartalmaznak. Az Ethereal minden nem ASCII karaktert '.' jelként dekódol. A „W.I.N.B.O.X.A.d.m.i.n.i.s.t.r.a.to.r.” sorozat a Winbox gép rendszergazdájának csatlakozási szándékát jelzi a TGT1-hez.

A rendszergazdai azonosítóval történő csatlakozási kísérleteken kívül egyéb azonosítókkal történő próbálkozásokat is lehet észlelni az adatokból, ilyenek az INET_GLOBAL, a Web-szerver beállításaihoz használt megosztott azonosító, a HELPTECH1, a helpdesk egyik munkatársának azonosítója, és a USERCHUCK, mely a cég egyik magas szintű programozójának az azonosítója. Egyszerű lenne az utóbbi két azonosítóra gyanakodni, de ezen a ponton még nincs bizonyítékunk ellenük.

Annak ellenére, hogy sok esetben ez az elemző munka a segítség a támadók által végzett kommunikáció felderítésére, léteznek olyan eszközök, melyek még kényelmesebbé teszik az elemzést végző életét. Ilyen a dsniff (http://naughty.monkey.org/~dugsong/dsniff) is, mely Windows rendszerre is elérhető

(http://www.datanerds.net/~mike), és azonosító-jelszó dekódolásra képes a legtöbb internetes protokoll esetén (FTP, Telnet, HTTP, POP, NNTP, IMAP, SNMP, LDAP, Rlogin, NFS, SOCKS, X11, IRC, AIM, CVS, ICQ, Napster, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB, és Oracle SQL).

2.5 Behatolás után kutatva

Látható, hogy a Windump és Ethereal sokat segít, de nem észleli a behatolást, csak a hálózati adatforgalom elemzésében használhatók egy gép esetén. Ha az egész hálózati forgalmat akarjuk elemezni, akkor az adatok mennyisége miatt ez nem egyszerű feladat. Ebből kifolyólag szükségünk van sokkal összetettebb eszközökre.

Snort (http://www.snort.org)

Egy csomagszűrő alkalmazás és behatolásérzékelő rendszer. Elérhető Win32 platformra is, beleértve a naplózási képességet MySQL vagy MSSQL adatbázisba. Grafikus kezelőfelülettel (pl. ACID – http://www.andrew.cmu.edu/user/rdanyliw/snort/snortacid.html) támogatva azonnali statisztikák készíthetők (legnagyobb forgalom, protokollok stb. szerint). Az igazsághoz hozzátartozik, hogy a háttérben kerül legenerálásra a forgalmi adatok alapján az adatbázis, amire a grafikus felület „felfekszik" és a lekérdezéseket végzi (ekkor már gyors válaszidőkkel). Ezen felül a snort szignatúra adatbázisát (előre megadott szabályok) saját szignatúrával bővítve meghatározhatjuk, hogy mit naplózzon, mit szűrjön, milyen eseményekre figyeljen. Például a következő szignatúrák minden NetBIOS kapcsolatot észlelni fognak a távoli gép F, G, H és I meghajtóin (ld. az esetünkben említett batch fájlban látottakat).

```
alert tcp any -> $HOME_NET 139 (msg:"NETBIOS SMB F$access"; flow:to_server,established; content:"\\F$|00
41 3a 00|";)
alert tcp any -> $HOME_NET 139 (msg:"NETBIOS SMB G$access"; flow:to_server,established; content:"\\G$|00
41 3a 00|";)
alert tcp any -> $HOME_NET 139 (msg:"NETBIOS SMB H$access"; flow:to_server,established; content:"\\H$|00
41 3a 00|";)
alert tcp any -> $HOME_NET 139 (msg:"NETBIOS SMB I$access"; flow:to_server,established; content:"\\I$|00
41 3a 00|";)
```

Ezek a szabályok riasztást váltanak ki, ha bármelyik hoszt megkísérli bemountolni az adott meghajtót a hálózaton keresztül a HOME_NET változót alkalmazva. A HOME_NET változót megváltoztatva, ahogy a forgalmat a mirror portra tereltük, folyamatosan kiterjeszthetjük keresésünk határait, mígnem az egész menedzsment VLAN-ban figyeljük a NetBIOS kísérleteket.

A szabályok megváltoztatásával vagy új szabályok megadásával több hálózati erőforrást, meghajtót stb. figyelve felépíthetjük a támadás mértékének térképét. Amióta tudjuk, hogy a helyi szabályok szerint NetBIOS (vagy bármilyen más kódolatlan) forgalom nem lehet a VLAN-on, minden riasztás támadó tevékenységnek feltételezhető.

Tanácsos kétféle monitorozó eszközt használni, a Snort valósidejű megfigyelést végez a számára megadott szignatúrák alapján, de szükség van egy teljes tartalom-elemzésre is akár off-line módban is. Fontos az eljárásban, hogy minél tovább tart, annál többet fedezünk fel a támadók cselekményeiből. Az eredeti adathalmazt megtartva újraelemezhetjük az időközben hasznosnak tűnő új szabályokkal:

```
C:\SNORT> snort -r Windumpfile -c C:\SNORT\snort.conf
```

Mivel a NetBIOS forgalom nem fordulhatott volna elő a hálózaton, ezért ezek mindenképpen gyanúsak, sőt osztályozhatjuk súlyosabban is őket. Az Ethereal segítségével a Windumpfile-ban a Snort által észlelt IP címeket vehetjük kézi vizsgálat alá, hogy felderítsük a feltört azonosítókat.

3 Megoldás

Elemzőként meg kell tudni különböztetni a normális forgalmat a gyanús és/vagy rosszindulatú forgalomtól. Ha ismerjük hálózatunkat, akkor nálunk a hazai pálya előnye, de sajnos ez nem mindig van így.

Sokáig nehéz volt a Windows rendszerek vizsgálata, de a Sysinternals-nak köszönhetően ma már számos eszköz rendelkezésünkre áll (pl. az előzőekben is említett PS* eszközök). Említésre méltó a Foundstone, az @Stake, a nyílt forráskódú szoftverek világából a WinPcap, Windump, Ethereal, Snort stb.

Léteznek adatforrások, melyek nem kerültek vizsgálat alá ebben az anyagban (pl. Windows esemény és biztonsági naplók, Web-szerver naplók stb.), pedig egy valós incidens során ezeket is teljes mértékben vizsgálni kell. A legtöbb esetben elég adat áll így is rendelkezésre az incidens kivizsgálásához, sokszor kardinális szabályok alapján egyértelműsíthetők a történtek.

Az elején említett batch fájl nem lehetett volna olyan sikeres, ha nem lett volna a Rendszergazda azonosító minden gépen ugyanaz (Global Domain Administrator = Local Administrator tovább csökkentve a teljes céges hálózat biztonságát). A második nagy probléma a rossz figyelő környezet, melyek strukturális változásokat és koncepcionális átalakításokat követeltek. Az említett eszközök segítségével és minimális költséggel lehetséges egy alapvető IDS képesség kiépítése, bár a felügyelet jelentős emberi erőforrást igényel majd.

A Windows biztonságáról nem nyitva vitát megjegyezzük, hogy minden széles körben elterjedt rendszer terjedésével arányosan több támadásnak van és lesz kitéve. Ennek köszönhetően a sebezhetőségei is gyakran és hatásosan kerülnek kihasználásra, így nagyméretű Windows rendszer esetén számítani kell a biztonsági eseményekre. Ezért nem árt felkészülni a következőképpen.

- Készítsünk egy eszközkészletet:
  - PS Utilities a Systinternals lapjáról
  - A rendszerben lévő Windows verziókról egy megbízható verzió (alap-összeállítások image-i is hasznosak lehetnek, mert minden újratelepítése sem kevés idő manapság)
  - Dual-boot-os Windows / Linux laptop Winpcap, Windump, Ethereal, és Snort+MySQL valamint Acid és ezek Linux változatai a Linuxos partíción.
- Windump/tcpdump és tcpreplay használata + EtherApe a hálózat felmérésére
- IDS implementálása – legalább egy kezdetleges változatban.

Végül, de nem utolsó sorban szánjunk időt saját felkészülésünkre. Ma már elérhetők olyan könyvek vagy internetes források, melyekből ez önképzéssel is elvégezhető. A legfontosabb, hogy az eszközökkel leássunk a dolgok mélyére, ismerjük meg a tulajdonságaikat és gyakoroljuk használatukat.

---

4 Kiegészítések

a http://www.securityfocus.com/infocus/1661 és 1665 – *Jamie Morris cikkei (2003. január 28. és 2003. február 11) alapján.*

4.1 Előzetes felkészülés

Minden eljárás első lépése a felkészülés, mely legjobb esetben még azelőtt történik, hogy gond lenne. Ide kell érteni a rendszergazdák által megtehető megelőző lépéseket is.

4.1.1 Törvények

A számítógépes törvényszéki eljárások két fő témakörre helyezik a hangsúlyt: 1. bírósági bizonyító eljáráshoz szükséges és elfogadott módszerek, 2. az eljáró azon igénye, hogy elkerülje az ellene, vagy az általa képviselt szervezet ellen irányuló jogi lépések lehetőségét. Ezek az elemek egyúttal a gyanúsított személyiségi jogait is védik. Egy adott eljárásban mindig mérlegelni és konzultálni kell arról, hogy a törvényszéki eljárás és az adatvédelmi szabályok mely pontokon keresztezik egymást, és melyiknek van nagyobb prioritása illetve mire és milyen feltételekkel van törvényi szabályozás.

4.1.2 Szabályok és eljárások

Amennyiben léteznek adatvédelmi szabályok, ezek behatárolják az adatok vizsgálati mélységét és milyenségét is. Az ilyen szabályzat a munkaadó és a munkavállaló számára is hasznos, hogy a keretekben megegyezve, a szabályokat aláírva állapodjanak meg a részletekben. Ez azért is fontos az eljárás során, hogy lehessen tudni, ki mit tudott, hogy egy-egy cselekedet megengedett-e számára vagy sem.

Az incidens jelentésének szabályai azt biztosítják, hogy a jelentés a megfelelő helyre érkezik, és ha már észlelték, nem kallódik el a szervezeten belül.

4.1.3 Naplózás

Csak az vonható eljárás alá, ami elérhető, tehát a megfelelően felülírt, törölt vagy más okból elérhetetlen adatok nem vonhatók eljárás alá. A nem naplózott eseményeket is nehéz kitalálni a végállapotból, de sokszor a naplózás beállításait nem ismerik és nem alkalmazzák a rendszergazdák.

A naplózásnál (mit és hogyan naplózzunk) fontos megtalálni az optimumot, hogy milyen előnyökkel jár a naplózás beállítása (milyen adatok lesznek meg), és milyen hátrányokat jelent (rendszer lassulása, lemezterület-foglaltság, kiegészítő erőforrások igénye stb.). A naplózás szabályai is rögzíthetők, így a naplók rögzítésének és őrzésének módja, ideje és hozzáférési jogosultságai is tisztázottak lehetnek.

Egyes rendszerek biztosítják, hogy előre beállított események riasztást vagy adott módú értesítést, netán reakciót váltsanak ki, így a naplózás átmehet behatolásérzékelésbe is. Az automatikus eszközök intelligenciája még sokáig nem lesz arra alkalmas, hogy a humán elemzést kiváltsák, így a naplókból kikövetkeztethető összefüggéseket, egy-egy a vizsgálat során intuitív forrásból felmerülő gyanút emberi elemzéssel kell ellenőrizni.

4.1.4 Az eszköztár összeállítása

A választék elég széles, de csak idővel alakul ki a saját bevált (és jól megismert!) eszköztár, valamint az adott vizsgálandó rendszer esetén alkalmazandó eszközök tára. Jelen esetben a szabadon elérhető eszközökre helyezzük a hangsúlyt. A 3. fejezetben felsoroltakon kívül a következőkre lesz még szükségünk.

Az eszközök közül a The Sleuth Kit (TSK, http://www.sleuthkit.org/sleuthkit/) és a hozzá tartozó Autopsy Forensic Browser (AFB, http://www.sleuthkit.org/autopsy/) emelendő ki, mely 2005 áprilisában is még frissített volt (több hasonló termék már nem érhető el régi címén vagy a készítők már nem frissítik). A TSK készlet biztosítja, hogy a 'dd'-vel lemásolt merevlemezen vizsgálatot végezzünk, míg az AFB egy HTML-alapú megjelenítést ad, hogy az eredményeket kezelhetőbb formában vizsgálhassuk.

Az eszközök használhatók a különböző Linux, MacOS és Windows fájlrendszereken történő vizsgálatokhoz is. Ezen kívül is léteznek szabadon elérhető eszközök, melyek hasznosak lehetnek (ld. ToReS CD az 1 lábjegyzetben). A legfontosabb szabály, hogy bármilyen eszközzel is dolgozunk, és bármit cselekszünk is, az eredeti bizonyítékokat ne változtassuk meg! Ne használjuk a feltételezhetően kompromittált rendszert önmaga vizsgálatára, hanem a kikapcsolt gépről mentsük le a merevlemezt (image készítés, teljes másolás), és csak ezt a másolatot használjuk a vizsgálódásra.

Igazságügyi eljárás esetében az eredeti adathordozóról készült másolat kerül tárolásra, és az eredeti eszköz kerül vizsgálatra!

4.1.5 Másolat (image) készítés

Az első lépés a teljes másolat hiteles elkészítése, melyhez sokféle eszköz létezik[6]. A legtöbb nyomozó által használt eszköz a fizetős EnCase nevű termék (http://www.guidancesoftware.com/). A másik említendő fizetős termék a SafeBack (http://www.forensics-intl.com/safeback.html), de a cég honlapjáról elérhetők ingyenes termékek is.

Nem szükséges pénzt költeni a fizetős termékekre, ha technikai szempontból megfelelő megoldást keresünk, mert a data dumper (dd) a Linux rendszereken megtalálható. A man dd megmutatja a parancssoros eszközök használatát, de léteznek olyan paraméterei is, melyek kifejezetten az igazságügyi eljárás céljából történő munkát segítik. Érdemes megjegyezni, hogy ha fizikai hibás a lemez (bad sector), akkor előfordul, hogy a másolat használhatatlan lesz (nem boot-ol és nem mount-olható).

A másolat megfelelőségét (ugyanaz, mint az eredeti) és sértetlenségét (nem változott meg) hash algoritmussal tudjuk biztosítani. Ilyen az MD5 és az SHA-1 algoritmus, de hamarosan áttérés várható ezeknél biztonságosabb változatokra (pl. SHA-256 és nagyobb számú névtársai). Az ilyen algoritmusok lényege, hogy akár 1 bit megváltozása esetén is más hash-t fognak eredményezni, így jelzik, hogy az adat megváltozott-e vagy sem. Az eljárás alkalmazható egy-egy fájlra is. Az md5sum.exe szabadon elérhető, de legyünk körültekintőek, hogy megbízható forrásból szerezzük be.

6 fontos, hogy a helyi hatóságok elfogadják-e az adott eszközzel történő másolatkészítést!

4.2 Keresés a rendszerben

Az image elkészülte után indulhat a bizonyítékok utáni keresés, melyet többnyire az image készítő szoftverek is támogatnak. A következőkben nézzük meg egy Windows rendszer esetén hogyan érdemes a keresést végezni.

Amikor egy felhasználó belép egy Windows 2000 vagy NT rendszerbe, először egy teljes könyvtárstruktúra jön létre az egyéni fájlok és beállítások tárolására (profile[7]). Ez a struktúra egy főkönyvtárból ágazik el, és ennek a neve megegyezik a felhasználó azonosítójával. Ebben a struktúrában található pl. az NTUSER.DAT fájl, melyben a felhasználóra vonatkozó beállítási információk találhatók. A fájl rejtett, így csak akkor látható, ha a rejtett fájlok megmutatását is beállítottuk a fájlböngészőnkben. Ez a fájl minden kilépéskor frissítésre kerül, így az utolsó írás időpontjából következtethetünk a felhasználó kilépési idejére.

A Cookies mappában a meglátogatott Internet oldalak tárolnak adatokat, ha a böngésző cookie tárolási szabályai ezt engedik (alapból engedélyezett, de letiltható). Együtt az ideiglenes Internet fájlokkal (ld. később) egész jó képet nyerhetünk a felhasználó böngészési tevékenységéről. A cookie-k kezelhető megjelenítését segíti több eszköz, közülük a CookieView-t említjük meg, mely szabadon letölthető a http://www.digital-detective.co.uk/ lapról a FreeTools alól. A böngészési eseményeket a NetAnalysis szoftverrel lehet nagyon jól elemezni, de ez már nem ingyenes terméke a cégnek.

Az operációs rendszer által különböző célokra létrehozott fájlok (*windows artefacts*) is hasznos támpontot jelentenek a nyomozásban. Ilyenek pl. az .lnk fájlok, melyek pl. a Munkaasztalon, a Küldés vagy a Start menüben jelennek meg. Ezek olyan hivatkozások, melyekkel a gyakran használt fájlok vagy alkalmazások könnyebben elérhetők.

Ezeknek a fájloknak a vizsgálata segíthet kideríteni egyes fájlok, mappák, alkalmazások vagy eszközök valamikori létezését, melyek már nem léteznek a rendszerben. Ez akkor hasznos, amikor egyes fájlok már törlésre kerültek és már nem állíthatók vissza, vagy hálózati meghajtókon voltak. Ilyen esetben, ha egy hivatkozás egy ZIP, JAZZ vagy USB meghajtóra mutat, hasznos útmutatást kapunk ezen médiák utáni keresésre majd megtalálásuk esetén tartalmuk elemzésére.

Hasznosak még a telepítés során vagy egy alkalmazás használata során keletkező ideiglenes fájlok. Ezek többnyire törlésre kerülnek, amikor a telepítés vagy az alkalmazás befejeződik vagy a számítógépet megfelelően kapcsolják ki (shutdown). Amennyiben egy alkalmazás lefagy, úgy ez a törlés nem megy végbe, így sok olyan bizonyíték maradhat, melyekről a felhasználó nem tudhat.

Azok, akik úgy nyomtatnak egy fájlt, hogy nem mentik el a gépre, szintén ellenőrizhetők, mert a nyomtatás során keletkezett .spl és .shd fájlok tartalmazzák a nyomtatott fájl nevét, tulajdonosát, a használt nyomtatót, és a nyomtatandó adatokat (vagy egy listát az ilyen adatokat tartalmazó fájlokról).

4.3 Mélyebbre ásás – törölt, rejtett, titkosított fájlok

A fájlok törlése után (a Kuka ürítése után is) a fájl adatai nem kerülnek törlésre, csak a fájlt töröltként, elfoglalt területét pedig szabadként kezeli a rendszer, így a terület felülírásáig ez elérhető marad. Egyes esetekben a felülírás után is elérhetők az adatok (ld. Kürt Rt. ez irányú munkássága).

A törölt fájlok behatárolására és teljes vagy legalább részleges visszaállítására elérhető eszközök közül a EasyRecovery Pro (http://www.ontrack.com/software) az egyik legjobb, de ez nem ingyenes. Interneten rákeresve a 'freeware file recovery' szavakra több találat közül is választhatunk, de egyet külön is megemlítünk: http://www.pcinspector.de.

A Kuka a felhasználó által törölt, de még visszaállítható fájlok tárháza, mely különösen nagy figyelmet kap a nyomozásokkor. Például a Windows98 rendszereken egy INFO vagy INFO2 fájl tartalmazta a Kukába került fájlok részleteit (többek között az eredeti helyüket, a törlés időpontját). A Kuka ürítésekor ez is törlésre kerül, de a már említett módon visszaállítható, ha még nem került felülírásra. Megemlítendő, hogy a SHIFT billentyűvel támogatott törlés (SHIFT+Del) nem helyezi a Kukába a törölt adatot, hanem valóban törlésre kerül (persze a fentiekben említett módon visszaállíthatók).

7 fontos, hogy 'roaming profile' esetén a cache ne a profile-ban legyen, mert egyrészt a profile mentés és betöltés hosszú időt vesz igénybe, másrészt a

Amikor alkalmazás végzi a törlést (nem fájlkezelő), az alkalmazásbeli tárolástól és a visszaállítás támogatásától (ha van egyáltalán) függ a visszaállíthatóság. Ez történhet az alkalmazásból vagy olyan eszközökkel, melyeket az igazságügyi vizsgálatokat végzők írtak... Megtörténhet, hogy a nyomok eltüntetése érdekében egész partíciót törölnek, vagy formázzák a lemezt, de ebben az esetben sem tűnik el fizikailag az adat a lemezről.

Azok, akik el akarnak rejteni egy fájlt, annak jellemzőit módosítják (pl. átnevezik a kiterjesztését exe-ről txt-re), de a fájl jellemzőjét így is vizsgálhatjuk szignatúraelemzéssel. Ekkor a fájl fejléce és kiterjesztése között felfedhetők ellentmondások, melyek alapján tovább ellenőrizhetjük az adott fájlt. Ilyen elemző Linux alatt a file parancs, míg Windows alatt a „File for Windows" szabadon használható (http://gnuwin32.sourceforge.net/packages/file.htm).

Ha a visszaállított adat titkosított információ, akkor ez egy újfajta kihívást jelent a szakértőnek. Nincs egyértelmű mindent törő alkalmazás, de lehetnek rosszul megválasztott jelszavak vagy tárolási módok, így az eljáró felfedezhet ilyen adatokat, melyekkel dekódolhatja a kódolt adatokat. Az is lehet, hogy az adott alkalmazás gyenge titkosítást használ, és a megfelelő megfejtő-programmal, elég erőforrással és idővel siker érhető el. Egyes esetekben a végigpróbálgatásos módszer is működhet, más esetben a háromszori rossz próbálkozás miatti védelem ezt nem engedi meg.

A jövőre nézve elmondható, hogy a folyamatos változásra kell felkészülni, hiszen az új és újabb lehetőségeket a támadók ki fogják használni, így sohasem késő megkezdeni a felkészülést az új és újabb védekezésekre és nyomozásokra az igazságügyi eljárás sikere de egyben tévedhetetlensége érdekében.

4.4 Amire nem szoktak gondolni...

A betörést elkövetők sokszor letöltenek valamilyen egyéb alkalmazást is, és az amatőrök elkövetik azt a hibát[8], hogy a böngésző beállításait megtartva teszik ezt, így a nyomozás számára hasznos adatokat hagynak maguk után. Ezek az adatok az adott felhasználóhoz tartozó cache, cookie, history stb. fájlokban található meg.

Windows rendszeren az egyes alkalmazások alkönyvtárait is érdemes átböngészni, pl. Firefox böngésző használata esetén keressük meg a downloads.rdf nevű fájlt, és érthető lesz, amiről beszélünk... Hasonlóan más böngészőben is elérhetők a felhasználó tevékenységét tároló fájlok, egyes rendszerek alatt még a begépelt parancsok is (pl. Linux rendszeren előfordul, hogy a RootKit (http://www.rootkit.com/) felrakása előtt elfelejtenek a támadók a .bash_history tartalmáról gondoskodni, így a rootkit felrakása után már nem is emlékeznek rá, illetve nem látják maguk sem...a nyomozást végzőnek pedig rendelkezésére áll majd minden parancs, amit a támadók gépeltek be a betörés után.

A fontosabb fájlok után lehet globális keresést indítani (pl. Cache mappa több helyen is lehet több különböző alkalmazásban), míg a speciális keresések a Documents and Settings mappában végzendők, de a ravasz vagy egyedi beállításokat alkalmazó felhasználók ellen érdemes a böngészőprogram beállításait ellenőrizni, mert lehet, hogy a böngésző cache mégis nem szabványos, hanem általa beállított külön helyen található a háttértáron.

A hibalehetőségek, melyeket elkövethetnek a támadók, szinte korlátlanok, mert a sok egyszerűen használható automatikus eszközt futtató amatőr (script kiddie) nem gondol mindenre, ezért szélsőséges esetben az is előfordulhat, hogy a helyi rendszerből ír levelet, ami a levelező beállításaitól függően másolatban is elérhető lesz később a kiküldött levelek mappában. Másik példa, ha SSH kapcsolat esetén a távoli gép kulcsát elmenti a helyi kliens, így azt is tudni lehet, hogy melyik gépre léptek be a támadók, és fel lehet venni annak a gépnek a gazdájával a kapcsolatot, hogy az ottani helyi logokból adjon információt a belépő azonosítójáról. Ha amatőrök voltak, akkor az már nem feltört azonosító volt, és ott sem töröltek maguk után minden adatot, és így még közelebb jutunk a valós belépési ponthoz, akár a személyhez is.

Természetesen ezen a területen is léteznek olyan munkák, melyek a rootkit-ek felfedését tűzték ki célul (Rootkit Detection – http://research.microsoft.com/rootkit/ Linux alatt ld. *chrootkit*), de a verseny folyamatos lesz az írók és a felfedők között. Az igazságügyi szakértőnek csak arra kell figyelni, hogy a személyes beállításokat (Profiles) tartalmazó adatokat lementse úgy az operációs rendszer, mint az egyes alkalmazások (főleg böngészők) megfelelő mappáiból.

* * *

8 Ugye mostanra világos lett az olvasó számára, hogy mindkét fél a másik hibájából él?