Egy nyomozás története

Ugye, mindenki elképzelte már a következő helyzetet: valami gond van a kiszolgálóval, amelyet üzemeltetünk – szerencsésebb, ha a karbantartását nem magunk végezzük, hiszen így nem mi hibáztunk –, és nekünk ki kell nyomoznunk a tettest.

Egyből rohanunk, hogy megoldjuk az esetet: esetleg már otthonról elkezdhetjük a munkát, de semmiképpen sem fejezhetjük be. El kell mennünk a kiszolgálóhoz, mert a gépeknél is szükség van „személyes kapcsolat"-ra, továbbá jobban látszik, hogy mennyire súlyos a gond.
A helyszínen azután belefutunk egy-két ügyes félrevezetésbe és csapdába, melyeket azonban megoldunk. Egy-két leleményes eljárás – amikor már a remény is elfogyott, természetesen csakis ekkor! –, és váratlan fordulatokkal dűlőre visszük az ügyet. A rossz ember lebukik, mi pedig besöpörhetjük az elismerést, a kollégák elismerő pillantásai nyomán pedig jó érzés tölt el minket.
Na, eddig tartott a mese.

```
[ago@mdk ago]$ telnet mail.ceg.hu 25
Trying X.Y.W.Z
Connected to X.Y.W.Z
Escape character is '^]'.
220 mail.ceg.hu ESMTP Postfix
MAIL FROM: ago@lsc.hu
250 Ok
RCPT TO: bill@microsoft.com
551 Reciepent address rejected. Relay access denied...
QUIT
```

A valóság: kétórás modemes kapcsolat otthonról, sok káromkodás és infarktusközeli élmény, egy fél tábla Boci csoki elfogyasztása szigorúan a stresszoldás végett, és befejezésképpen az áhított siker is megérkezik, amelyre azonban a frissen szerzett tapasztalatok birtokában már nem is vágyakoztunk annyira. Amennyiben választani lehetne, szívesebben szavaznék a nyugodt életre. A továbbiakban elolvashatjuk, mi is történt pontosan, milyen intézkedéseket foganatosítottam, és mi lett a következménye. A szereplők természetesen névtelenek maradnak, hogy senki személyiségi jogait ne sértsük meg.

Első felvonás

Éppen egy tanároknak szóló tanácskozáson tartózkodtam és az előadásomra készültem. Egy órával a nevezetes esemény előtt hangüzenet érkezett a telefonomra, de nem volt térerő, amikor hívni próbáltak. Az üzenetben egy barátom közölte, hogy levélszemetet (spam) kapott, és mit tudok mondani az info@gepnev címről, ugyanis tudomása szerint minket bíztak meg a karbantartásával. Kicsit elcsodálkoztam, mert az említett gépen levelezőszolgáltatások nem futottak, csupán egy átjárógép volt két alhálózattal. Ezen keresztül érhetik el az adott cég számítógépei a külső címtartományban lévő levelező- és egyéb kiszolgálókat. Felhívtam az említett cég telephelyén tartózkodó rendszergazdánkat, hogy nézze meg, nem fut-e az átjárón levelezőkiszolgáló (MTA). Természetesen nem futott, viszont célszerű volt rákérdezni, hiszen sohasem árt. Ezután már megnyugodva hívtam fel a hangüzenethagyót és közöltem, hogy valószínűleg meghamisították a levél fejlécét – ezért gondolhatta, hogy a levelet tőlünk kapta. Aznap este könnyű szívvel tértem nyugovóra.

Második felvonás

Másnap hazaérés és rövid pihenés után modemen keresztül csatlakoztam a Világhálóra. Amint beléptem, és elolvastam a beérkezett leveleket, az ellazultság legalább annyira távol került tőlem, mint a gonosz kismalactól a jóindulat. Többen is visszajeleztek, hogy levélszemetet kaptak, amely a fejlécek tanulsága szerint valóban tőlünk származott. Ezt megerősítette a levelezési forgalomról készült előző napi kimutatás, ami egyébként mindig lefut. Valaki – akkor még ismeretlen személy – 7241 kéretlen levelet továbbított a kiszolgálón keresztül! Mi is erősítette ezt meg? A visszajelzések között akadt olyan, amely a teljes levelet idézte a fejléccel együtt. Az eredetileg kiküldött levélben a `From:` szó után az a levélcím állt, amelyet a küldő a levelezőprogramba írt be. A továbbítókiszolgálókat azonosító fejlécrészlet pedig az ügyfelet kiszolgáló átjárót, valamit a tényleges levelezőkiszolgálót azonosította. A jelentés és az eredeti levél tehát egyértelművé tette: tényleg rajtunk keresztül küldték a levelet. A következőt kellett kiderítenem: valóban nyílt levéltovábbító-e a kiszolgáló vagy egyéb módon került meg a levél? Az egyéb lehetőségek közé soroltam még: a kiszolgálót feltörték és egy telepített program segítségével küldték ki a leveleket vagy a törés után nyílt levéltovábbítót csináltak belőle. Amennyiben nyílt levéltovábbítóként működik, akkor is meg kell vizsgálnom, nem történt-e valami sokkal rosszabb a háttérben. Ha megtörték, és nyílt levéltovábbító lett, valaminek futnia kellett ott. A nyomozást a lehető legegyszerűbben kezdtem: kipróbáltam, lehet-e nem engedélyezett címre levelet küldeni. Ennek legegyszerűbb módja a Telnet program használata. A segítségével csak rá kell kapcsolódni a levelezőkiszolgáló 25-ös kapujára és ellenőrizni. Aki követte a cikkeimet, annak már ismerős az a folyamat, amit az *1. lista* szemléltet.
Ez kicsit megnyugtatott, eszerint tehát rajtunk keresztül nem lehet akárkinek levelet küldeni. Ekkor számba vettem a második lehetőséget: a számítógépet megtörték. Mit tesz ilyenkor az előrelátó ember? Elővarázsolja a kiszolgáló „tiszta állapotát" tartalmazó fájlt, és az AIDE program segítségével összehasonlítja a rendszer binárisait. Kicsit morogni kezdtem, ugyanis az elutazásom előtti napon általános programfrissítést hajtottak végre. A rendszeren Debian Woody fut, amelyhez az újabb csomagokat is letöltöttem. Az új fájlt viszont mindig helyileg szeretem elkészíteni, ami azonban az utazás miatt elmaradt. Ez bizony balszerencse volt, nem engedhettem volna meg – le is szidtam magam. A következő lépésben meghívtam a `debsum` nevű programot, ami a telepített programokhoz tartozó ellenőrzőösszegeket – az úgynevezett `MD5 summ`-okat – hasonlítja össze a binárisok jelenlegi állapotával. Ha bármelyik futtatható fájlt lecserélték,

ez a program kideríti. Ámde hogyan bízhatnánk meg az esetlegesen gyanúba keveredett gépen lévő ellenőrzőösszegekben? Sehogy. Mindenesetre egyelőre tisztának tűnt minden, tehát meghívtam a `netstat` programot. Ez a program a hálózathoz kapcsolódó programok állapotáról ad tájékoztatást. Megmutatja, hogy a kiszolgáló milyen kapcsolatot kezel jelenleg. Én a *2. listán* látható módon indítottam el. Természetesen a kimeneten kívül több más érték is szerepel itt. A program ezekkel a kapcsolókkal mutatja meg, hogy melyik program vár kapcsolatot melyik kapun, és milyen IP-címen teszi azt. Itt ért az első szívroham, ugyanis egy számomra ismeretlen kaput fedeztem fel ismeretlen démonnal. Majd megnyugodtam, mert csupán az otthoni gépemen futó kísérleti program várta a kapcsolatokat. Még otthon kezdtem el kipróbálni és a gépemen maradt. Másodszor már a kiszolgálón sikerült lefuttatnom a programot, ahol mindent rendben lévőnek találtam. A biztonság kedvéért azonban tovább piszkáltam a rendszert. Átnéztem az összes parancsfájlt, amely a `cron`, az `at` és a Postfix programokhoz kapcsolódik, ugyanis ezeket a szolgáltatásokat le akartam állítani. Azt azonban mindenképpen el szerettem volna kerülni, hogy amennyiben a kiszolgálót mégis feltörték, és esetleg huncut `rm -rf /` parancsot írtak a vezérlő parancsfájlba, annak következményei legyenek. Miután mindent rendben találtam, a szolgáltatásokat leállítottam. Miért volt ez fontos? Ha a rendszert feltörték, és egy olyan binárist módosítottak, amelyet a `cron` is használ, a rendszer esetleg önműködően újra meg újra megnyílik. Ráadásul a Postfix még számos helyre el akarta küldeni a leveleket. Ezeket a leveleket a leállítás után töröltem. Jó néhány akadt, ezért miután meggyőződtem róla, hogy „rendes" levél nincs a sorban, az egész várakozási sort töröltem (szerencsére hétvége volt, ezért ez csaknem természetesnek tekinthető). Ezután a ➲ http://www.debian.org-ról leszedtem a binárisokhoz tartozó MD5-ös ellenőrző összegeket és átmásoltam őket a gépre, majd így ellenőriztem a binárisokat. Ezt az átjárón is megismételtem. Mindkét rendszer teljesen rendben volt, tehát a törést és a nyílt levéltovábbító gondokat elfelejthettem. Már csak egyetlen lehetőség maradt.

2
```
[ago@mdk ago]$ netstat -antl
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address     Foreign Address         State
tcp        0      0     0.0.0.0:25          0.0.0.0:*           LISTEN
```

Harmadik felvonás

Mivel a kiszolgáló csak egy helyről fogadott el leveleket továbbításra, nem volt nehéz dolgom, hogy behatároljam a következő keresési területet. Ez a gép az átjáró volt – az egyetlen gép, amely felől a küldés engedélyezett. Ezen az átjárón igazából nem fut semmi, csak címeket fordít és kapcsolatokat továbbít. A támadás tehát a mögötte lévő egész belső hálózatról jött. Hogyan lehet megkeresni a saját berkeinkben megbúvó támadót? Miután ismét elindítottam minden szolgáltatást a levelezőkiszolgálón, figyelmemet az átjáróra, pontosabban a naplófájlokra összpontosítottam. Mivel a levelezőkiszolgáló eléréséhez címet kell fordítanom, vagyis álcáznom (masquerading) kell, a csomagszűrővel az erre vonatkozó szabály volt beállítva. Csakhogy a szabály végén megadtam, hogy fordításnál *minden* kimenő csomagról írjon jelentést a naplófájlba. A parancs hasonlóan néz ki:

```
/sbin/ipchains -A forward -i -p tcp
➥-s 192.168.1.0/24 -d mail.ceg.hu 25
➥-j MASQ -l
```

Ez fordította át a belső hálózat címeit az átjáró IP-címére, amennyiben az ügyfelek kapcsolatba akartak kerülni a levelezőkiszolgálóval. A `-l` kapcsolta be a naplózást. Az előző napi naplófájlból kikerestem – természetesen a segédprogramok használatával –, hogy melyik ügyfél kapcsolódott kiemelkedően sokszor a levelezőkiszolgálóhoz. A segédprogram saját készítésű volt, ezért a kiosztott címtartomány minden ügyfelére összesítést készített, és hogy hány bejegyzést talál az adott IP-címhez. Majd a kiemelkedően nagy számú küldő címét felhasználva kikerestem a listából, hogy kihez tartozik a cím. Ekkor csörrent meg a telefon. Maga az elkövető volt. Honnan tudta meg, hogy nyomozok? Az egyik felháborodott partner ugyanis nemcsak nekem küldte el panaszát, hanem a levél küldőjének is – mármint arra a címre, amit az elkövető írt be, és ahova a válaszleveleket a megrendelésekkel együtt várta (ugyanis egy szolgáltatást hirdetett). Mivel csoportos választ nyomtam, ő is megkapta válaszomat – ez idegességemben fel sem tűnt nekem. Nos, próbálta magát mentegetni, hogy nem gondolta, mekkora baj lesz ebből, és különben is otthonról akarta végezni. Ennek azonban jócskán ellentmondott, hogy a saját bevallása szerint is mailbomber programot használt. A következő héten hétfőn leadtam a jelentést a cég vezetőjének és szóban is tájékoztattam az eseményekről. Ennek eredményeképpen az illetőt még aznap elbocsátották.

Miért is? A cég erőforrásait használta és mivel levélszemét jött a levelezőkiszolgálóról, néhány másik levelezőkiszolgálóról kitiltották a tőle érkező *összes* levelet. Ezenkívül a céget erkölcsi kár is érte.

Összegzés

Egyszer minden „csínytevésre" fény derül, és egy ilyen nyomozás inkább fárasztó és idegesítő, semmint jó móka. Gondolom, jövője ismeretében a vétkes is másképp cselekedett volna.

Deim Ágoston (ago@lsc.hu)
Kedveli a sört, szereti a futást és imádja Szabó Lőrinc verseit. Nem hisz vakon egyik rendszerben sem. Vonzódik a BSD-hez is. Tagja az LME-nek és a MBE-nek. Mottója: a gép nem lehet fontosabb az embernél.