

# 1. fejezet

## Itt gépkalózok élnek!

▼ ITT GÉPKALÓZOK ÉLNÉK!

Amikor régen a térképészek  
lerajzolták az általuk ismert világot,  
a szélre minden odaírták:  
Itt sárkányok élnek!

(Ismeretlen szerző)

**A fejezet végére az alábbi kérdésekre kell tudnunk választ adni:**

- **Mi a különbség az alkalom szülte cél és a kiválasztott célpont között?**
- **Mi a támadás hat legfontosabb összetevője, és mi az egyes összetevők célja?**
- **Melyek a számítógépes biztonsági szervezetek, és miként segíthetnek ezek minket?**
- **A támadók milyen mélységben és milyen terjedelemben támadhatják és használhatják ki hálózatunkat?**

**1.**

Napjaink „behálózott” világára is igaz az egyének személyes tudásán túlmutató ilyen ōsi megjelenítése. Amikor az otthoni gépet vagy a vállalati hálózatot csatlakoztatjuk az internethez, akkor a saját hálózatunkon kívüli vadon a szó szoros értelmében a világ vége, egyben a világháló kezdete, ahol a gépkalózok (*cracker*)<sup>1</sup> leselkednek, hogy kihasználják az óvatlanokat.

A hálózati biztonság megértését célzó könyvben a legelső lépés nyilván annak bemutatása, hogy ki is az a gépkalóz, és milyen módon is fenyegetheti a mi hálózatunk biztonságát.

A fejezet – kezdve a támadás végrehajtásához kiválasztandó megfelelő célponttal – bemutatja a gépkalózok támadásának anatómiáját. Megismerhetjük a kalózok jellemzőit és hátrahagyott nyomait, ezzel is segítve a saját hálózaton kívül leselkedő veszélyek jobb megértését.

## 1.1. A CÉLPONT KIVÁLASZTÁSA

A világhálón csupán néhány milliárd lehetséges nyilvános IP-cím lehet, így mennyire lehet nehéz megtalálni az alkalmas célt? A legtöbbet valószínűleg a biztonság ezen területével foglalkoznak legelőször. A hálózat csatlakoztatása az internethez lehetővé teszi, hogy a kalózok megtalálják azt, így aztán célszerű gondoskodnunk a saját hálózatunk biztonságáról. Tegyük fel, hogy megvásároltuk a gép védelmére szolgáló elérhető legjobb védelmi technológiát, és rendszeresen (továbbá gyakran) megbizonyosodunk arról, hogy alkalmaztuk rá a legfrissebb biztonsági javításokat is. Ide értendő a tűzfalunk (*firewall*), a monitorozást is lehetővé tevő útválasztónk (*router*), a virtuális magánhálózatunk (*VPN – virtual private network*), a vírusirtó szoftverünk, a közvetítő kiszolgálónk (*proxy server*), a biometriai azonosító eszközeink, és általában a pénzért megvehető legjobb védelmi technológiáink. Ezt már mind megvettük és alkalmazzuk.

Természetes az a hiedelem, hogy a védelmi technológiák képesek megvédeni minket a gépkalóz technikák rosszindulatú fenyegéseitől. Az előbbi esetben például nagyon vágytunk arra, hogy biztonságban érezhessük magunkat, azonban megfeledkeztünk a leggyengébb láncszemről: az emberről.

1 Az angol eredetiben szereplő „hacker” kifejezés valójában más jelentéssel is bír. Ez jelöli például az egyáltalán nem rosszindulatú, bizonyos területen komoly szakérlelmemmel bíró szakembereket, míg a rosszindulatú támadókat inkább a „cracker” kifejezéssel jelölnek. Az eredetiben a „hacker” kifejezést használta a szerző, azonban a legtöbb esetben „támadó” értelemben tette ezt, s ennek megfelelően lett lefordítva is. Ahol mégis valódi értelmében használta, ott „etikus támadó” megjelöléssel szerepel. (A lektor meg.)

Tegyük fel egy pillanatra, hogy alkalmazottaink minden átestek a legjobb biztonsági képzésen. Tudhatjuk-e róluk, hogy mit fognak tenni akkor, ha valaki az érzékeny információk megszerzése érdekében megpróbálja becsapni őket? Az épületnek összesen hány kulcsmásolata létezik? Mit csinál a takarítószemélyzet, ha nem vagyunk jelen? Az előírásoknak megfelelően semmisítik meg a papírosárunk tartalmát, vagy csak bezsákolják és a szemetbe dobják azt? Betörhet-e valaki észrevétlenül az ablakon keresztül vagy egy zár feltörésével? S ekkor vajon mennyire védhet minket az a kitűnő tűzfal?

Hihetjük azt is, hogy kiváló IT-csapatunk van, vagy akár kifejezetten hálózatbiztonságra specializálódott szakembergárdánk, ami természetesen helyes. A biztonsági szakemberektől elvárható a magas szintű technikai hozzáértés, ami általában igaz is. Sajnos ezek a szakemberek gyakran nem feltételezik ugyanezt a hozzáértést és képességeket azon támadóról, akikkel szemben védeni akarják a területüket. Sokan nem veszik figyelembe az örökök érvényű állítást: „*Mindig van nálunk okosabb, többet tudó, vagy jobban felszerelt támadó*”. A katasztrófa bekövetkezésének csak nem biztos módja, ha egy olyan mérnök van a csapatunkban, aki saját magát hiszi a legokosabbnak.

Vegyük az elterjedt **kukabúvárkodás** (*dumpster diving*) fogalmát. A nevét arról kapta, hogy némely rajongó (a kukabúvár) a neves filmcsillag vagy ismert tévés személyiségek szemetében is keresgélte az „ereklyéket”. A pszichomérnökök szerint tehát a vállalat szemétbén elhelyezett anyagai egyáltalán nem tekinthetők biztonságosan megsemmisítettnek. A módszer segítségével annak idején az AT&T telefonrendszerébe is betörtek, őket persze még nem gépkalózoknak hívták, hanem „vonaltolvajoknak” (*phone phreak*)<sup>2</sup>.

A biztonság gyakran csupán egy illúzió, amelyet a vállalat alkalmazottainak tudatlansága és naivitása táplál és tesz hihetővé. Nem szabad kizárálag a biztonsági termékekben megbízni; ha ezt tennénk, akkor csupán a biztonság csalóka érzetébe ringatnánk magunkat. minden biztonsági óvintézkedést meg kell tennünk – ez a technológián kívül a szabályok kidolgozását is jelenti. (Természetesen a vállalat valamennyi munkatársának be is kell tartania ezeket a szabályokat.) Ajánlatos továbbá véletlenszerű vizsgálatokat is végezni, azt ellenőrzendő, hogy a vállalatnál bizonyos személyek (például a főnökség tagjai), akik magukat sokszor felmentve érzik a szabályok alól, betartják-e ezeket. A főnökség tagjai általában hozzáférnek a titkokhoz, s így a kalózok elsődleges célpontjai. Amennyiben megengedjük, hogy a vezető beosztású személyek áthágjanak bizonyos

<sup>2</sup> Magyarországon kevésbé ismert jelenség, olyanokat jelöltek így, akik különböző eszközökkel képesek voltak a telefonhálózat egy része fölött átvenni az uralmat, és fizetési kötelezettség nélkül kapcsolatokat tudtak létesíteni segítségükkel. (A ford. megj.)

biztonsági szabályokat, akkor egyértelműen meggyengítjük a biztonsági rendszerünket.

Összefoglalva tehát, a „valódi” biztonság sokkal több egy megvásárolható terméknél, inkább a folyamatok olyan sorozata, amely felöleli a szervezethez tartozó személyek és termékek mindegyikét. A következő részben annak fontosságát vizsgáljuk meg, hogy a szervezethez tartozó személyek valóban figyelembe vegyék a biztonsági folyamatokat.

## 1.2. ÁRTALMATLAN INFORMÁCIÓK MEGSZERZÉSE

Figyelembe véve a fejezet bevezetőjében elmondottakat, a témát az ártalmatlan információk megszerzési módszerének megvizsgálásával folytathatjuk. Ezt nevezzük **pszichomérnöki** (*social engineering*)<sup>3</sup> tevékenységnak. Sokkal könnyebb a pszichomérnöki tevékenység segítségével megszerezni az ártalmatlan információt, mint átjutni a tűzfalon.

Az emberek alapjában véve bíznak másokban, és segíteni akarnak nekik, ezért erősen ki vannak téve a pszichomérnököknek. Ezen legalapvetőbb támadási forma ellen folytatott küzdelem egyike a legnagyobb kihívásoknak, amellyel a biztonságért felelős személyeknek szembesülniük kell.

Jóllehet el sem hisszük, hogy az ártalmatlan információt egyáltalán védeni kellene, az mégis nagyon fontos lehet a pszichomérnök támadó számára. Az így szerzett információval felfegyverkezve ugyanis később még hihetőben adhatja ki magát bennfentesnek. A gyakorlatban a kalóz sokszor azzal kezdi a támadását, hogy egy ártalmatlannak tűnő és könnyen elérhető dokumentumot szerez. Vigyázni kell tehát az „ártalmatlan” információkkal is, mert ezek értékes segítséget nyújthatnak a későbbi támadásokhoz.

Tanulmányozzuk a következő beszélgetést, amit egy biztonsági vizsgálat során folytattam. Meg akartam tudni, hogy az alkalmazottak mennyi információt hajlandóak kiadni magukról egy „hivatalosan” hangzó személynek, ezért felhívtam az IT-főmérnököt:

– Üdvözölöm, Tom vagyok a SzélSzárny utazási irodától. A San Joséba szóló repülőjegyek elkészültek. Kérdez, hogy kipostázzuk-e önnel, vagy inkább letétbe helyezzük őket a repülőtéren az információs pultunknál?

– San Joséba? – kérdezte Daniel. – Nem tudok róla, hogy oda akarnék repülni.

– Ön Daniel Thomas? – kérdeztem.

3 Szó szerinti fordítása „társadalomkutató” vagy „szociológus” lenne, azonban már csak szakmájuk iránti tiszteletből is illetlen lenne ezt a fajta támadást így nevezni. A „pszichomérnök” kifejezéssel arra igyekeztünk utalni, hogy némi lélektani ismerettel és színjátékkal, de gondos terv alapján végzett és jól előkészített tevékenységről van szó. (A ford. meg.)

– Igen, én vagyok, de nincs más utazásom beütemezve, csak a San Franciscó-i SunOne konferencia, majd néhány hónap múlva.

– Nos – kérdeztem nevetve –, biztos ön abban, hogy nem akar elutazni San Joséba?

Daniel is felnevetett, így reagálva a humoros helyzetre, amely a szokássos napi munkájába egy kis színt hozott: – Sajnos, biztos vagyok, ha csak meg nem győzi a főnököt...

– Hát, úgy tűnik, hogy a számítógépünk már megint tévedett – mondtam, majd ismét kuncogva folytattam –, pedig azt hinné az ember, hogy a számítógépeknek meg kellene könnyíteni az életünket. – Daniel is nevet.

– A számítógépes rendszerünkben a foglalásokat az önkö munkáltatói törzsszáma szerint tartjuk nyilván. Lehet, hogy valaki hibás számot adott meg, amikor lefoglalta a repülőjegyet. Megmondaná a saját törzs számát?

Daniel tudja, hogy a vállalatán belül több csoport is ismeri az ő törzs számát: a biztonságiak, a személyzetisek, a főnöke, és nyilván a bérszám fejtés is, így hát miért ne használhatná akár egy utazási iroda is ezt a számot az ő azonosítására. Ebben semmi veszély nincs, ugye?

A pszichomérnöki tevékenységben jártas kalóz ezután az így megszerzett apró információt hozzákapcsolja a hasonlóan könnyen megszerzett további adatokhoz, hogy megkezdhesse a következő szinten is a támadást. Képzeljük el, mennyi mindenhez hozzáférhet akkor, ha sikerült megszereznie a törzssámot, a teljes nevét, mellékének számát, e-levél-címét, osztályának a nevét, szobájának a számát, s még akár a főnökének a hasonló adatait is. A fenti információk bármelyike önmagában ártalmatlannak tűnik, de meglehetősen riasztó képnek tűnik, hogy ezek ilyen könnyen összegyűjthetők.

Az ártatlan információkat is védeni kell tehát, és az alkalmazottaknak tudniuk kell, hogy azon adatok hibás kezelése, amelyeknek soha nem kel lene nyilvánosságra jutniuk, komolyan veszélybe sodorhatja a vállalatot, de akár magát az alkalmazottat is. Tegyük fel, hogy az előbbi beszélgetést így folytattam volna:

– Daniel, a törzsszám alapján nem találom a rendszerünkben. Nyilván valami hiba van, hadd próbáljam meg kideríteni másként. Mi az ön TAJ száma?

Az ökolszabály értelmében minden vállalati adatot természeténél fogva érzékenynek kell tekintenünk, és soha senkinek nem szabad kiadnunk, ha csak az információt kérő az adott adat kapcsán nincs jogosultként fel tüntetve az adatkezelési szabályzatban.

## 1.3. ALKALOM SZÜLTE CÉLOK

Számon sem tudom tartani, hányszor hallottam már a vevőimtől a következő állítást, miközben a hálózatáról és a biztonságáról beszélgettünk: „Mi a »nem IT« üzleti körben tevékenykedünk, és semmi nincs a hálózatunkon, amiért egy kalóz ide betörne. Miért aggódnék hát?”

Micsoda állítás! Valahányszor hallom, minden ámulatba ejt. Sokféleképpen lehet persze válaszolni erre a felvetésre – ezek nemelyike udvarias, más részük azonban nem. Mivel a fenti kijelentést általában egy reménybeli vevő teszi, így nyilván ennek megfelelő választ kell adni neki.

Ezt a hiedelmet a **titokra alapozott biztonság** (*security through obscurity*) néven ismerjük.<sup>4</sup> Ebben a könyvben éppen azt próbáljuk bizonyítani, hogy a biztonság titoktartásra alapozásában megbízni rendkívül veszélyes, függetlenül a vállalat méretétől és tevékenységi körétől.

Lehet, hogy a szóban forgó vállalat nem bank, de a hálózatában nyilván találhatók kiszolgálók, szabad lemezterület, internetes sávszélesség és az alkalmazottakról személyes információk. Abban hinni, hogy ezek az információk nem fontosak a támadó számára, végzetes lehet. Vizsgáljuk meg, mire lehet képes egy kalóz ezekkel az információkkal:

- **Kiszolgálók** – Ha sikerült betörni egy kiszolgálóra, akkor nyert vele egy olyan eszközt, amelyet más, sokkal fontosabb célok támadására használhat közvetítőként. Képzeljünk el egy fekete ruhába öltözött, morcos embertől érkező telefonhívást, aki egyáltalán nem találja viccesnek azt, mivel is próbálkozik a szerverünk az ő hálózatában. Megvan?
- **Szabad lemezterület** – minden hálózatban van ki nem használt lemezterület. Mi van akkor, ha sikerült betörni a hálózatunkba, és megkérdőjelezhető vagy éppen illegális tartalmú állományokat sikerült feltölteni? Gondoljuk meg, hogy a szerzői jogokat betartani szándékozó ügyvédek mit fognak tenni. Tegyük fel, hogy a feltöltött állományok pornográf vagy éppen terrorista anyagok. Ma már jó néhány gigabájt méretű lemezeket szoktunk használni, ami vonzó lehet azok számára, akik egy frissen kijött mozi film kalózmásolatát akarják valahol elhelyezni, csupán néhány órára vagy napra.
- **Sávszélesség** – minden támadónak jól jön némi extra sávszélesség és alternatív hozzáférés, amelyek segítségével más vállalatokhoz próbálhat betörni.

4 A biztonságot ilyenkor arra alapozzuk, hogy valamilyen információt titokban tartunk, például nem hozzuk nyilvánosságra a titkosítást végző algoritmust, esetleg bizonyos kódszavakat. Számos példa bizonyítja, hogy ilyen esetekben a biztonság a titokban tartott információ felfedése miatt igen rövid idő alatt (néha heteken belül) sérül. (A ford. megij.)

- **Alkalmazottak személyi adatai** – Felfegyverkezve minden információval, amit egy munkáltatónak tárolnia kell az alkalmazottairól, a támadó bármikor képes lehet saját személyazonosságát meghamisítani.

Ezek a támadói tevékenységek tehát az IT-személyeket, a vállalatvezetést, vagy akár magát a vállalatot is jogi vagy bűnvádi eljárás veszélyébe sodorják, s még nem is tértünk ki arra a rendkívül rossz sajtóvisszhangra, ami egy ilyen mértékben feltört vállalatról nyilván megjelenik.

Az igazán fontos kérdés tehát nem az, hogy „miért akarna bárki is betörni a hálózatomba?”, hanem „nem vagyok-e túlságosan sérülékeny egy ilyen támadással szemben?”.

A kalózok legkönnyebben a „felkínált” célokra törhetnek be, hiszen ezeken valamit elmulasztottak, vagy valami olyat tettek, ami könnyen felismerhetővé teszi őket, s így képes lesz hozzáférni egy olyan vállalati hálózathoz, amelyen a tulajdonos szerint *nincs semmi értékes*.

### 1.3.1. ALKALOM SZÜLTE CÉL A HÁLÓZATOM?

Számos esetben a gépkalózok az interneten barangolnak, különböző eszközök (ezekről később lesz szó a könyvben) használatával próbálva feldeíteni a lehetséges célokat, és általában van elképzelésük arról, mit fognak tenni, ha találnak egyet. Ezeken a kalózokon kívül ráadásul még a **szkriptcsávónak** (*script kiddie*) nevezett támadóktól is tartanunk kell.

A biztonsági infrastruktúra pontos ismeretében lehet eldönteni, hogy a saját hálózat vajon alkalom szülte célnak tekinthető-e. Ökoliszabályként azt mondhatjuk, ha egyáltalán nem védjük a hálózatunkat tűzfallal, vagy ha a tűzfalat nem frissítjük rendszeres (gyakori) időközönként, akkor nagy valószínűséggel célpontnak tekinthetjük a hálózatunkat. Mivel automatikus eszközökkel tesztelik állandóan az ismertté váló biztonsági réseket, az alkalom szülte célként minősíthető hálózatokra a leggyakoribb veszélyt a szkriptcsávók jelentik. Az egyik legegyszerűbb módszer az alkalom szülte célként való minősítés elkerülésére az, ha minden felte tessük a legutolsó biztonsági frissítéseket. El kell kerülni önmagunk becsapását, és nem szabad megelégedni azzal, hogy csupán egy vagy két szervert frissítünk. Ha nem is minősülünk alkalom szülte célnak, még mindig előfordulhat, hogy kiválasztott célponttá válunk.



A szkriptcsávó lekicsinylő fogalom, amely a képzett gépkalózoktól származik. Ezzel jelöljük azokat a sokkal képzetlenebb, ám gyakran ugyanolyan veszélyes támadókat, akik a szoftverek ismert biztonsági réseit használják ki. Jellemzően létező, gyakran igen jól ismert és könnyen megtalálható technikákat és programokat vagy parancsállományokat, más néven szkripteket használnak (innen származik a fogalom neve), így felfedezve és kihasználva az internetre csatlakozó gépek gyengeségeit. Teszik ezt véletlenszerűen, keveset vagy egyáltalán nem törődve a lehetséges káros következményekkel. A gépkalózok lenézik a szkriptcsávókat, és némi aggodalommal is figyelik őket, mivel az utóbbiak semmit nem tesznek a gépfeltörés „művészetteléért”, viszont nagyon gyakran felingerlik a hatóságokat, ami a teljes gépkalóz-társadalmat sújtja. Amíg a gépkalóz büszke a támadás minőségére – például hogy ne hagyjon nyomot maga után –, addig a szkriptcsávók elsősorban a nagyobb mennyiségre elérésére törekszik, amelynek segítségével ismertségre és hírnévre kíván szert tenni. A médiában gyakran unatkozó, magányos tinédzserként ábrázolják őket, akik társaik körében kívánnak elismertséget kivívni (<http://www.searchsecurity.com>). Általában csak a kihívás kedvéért támadnak, nem pedig gazdasági előnyök kedvéért, bár néha ez utóbbi is lehet ösztönző. Mivel kezdők, általában nincsenek tisztában azzal, hogy mit is csinálnak, és gyakran gondatlanságból okoznak szolgáltatásmegtagadást (DoS – Denial of Service). Állítólag a legtöbb gépkalóz a maga idején szintén szkriptcsávóként kezdte.

## 1.4. KIVÁLASZTOTT CÉLPONTOK

A támadóknak gyakran van valami céljuk a célpont kiválasztásakor. Elsőként vizsgáljuk meg, hogy a média milyen befolyással bír arra a képre, amit a gépkalózokról alkotunk magunkban. Sokan hiszik azt, hogy a gépkalózokra az alábbi jellemvonások igazak:

- elégedetlen, elutasító és haragszik a világra,
- keserű, kevés baráttal és alacsony önbecsüléssel,
- különlegesen okos, mégsem képes hagyományos karriert felépíteni,
- problémái vannak a kapcsolatok, barátságok, szerelmek kiépítésével,
- elutasítja a hatóságokat, aszociális,
- fiatal, tapasztalatlan a nőkkel,
- 5zám0kat ha5zná1 a szavakban, h0gy királyabbnak 1átszódjék.

Ezek a sablonok időnként igazak lehetnek, ettől függetlenül létezik viszont egy gépkalóz-szubkultúra, amelyhez bizonyos támadók tartoznak. Azt hinni azonban, hogy a hálózatunk elleni minden fenyegetés ilyen egyénektől jön, hiba lenne.

## 1.4.1. KIVÁLASZTOTT CÉLPONTTÁ VÁLTUNK-E?

A következő feltételezett helyzetek esetén gyanakodhatunk arra, hogy a vállalatunk – esetleg mi személyesen – adott esetben kiválasztott célpont-tá lehetünk:

- Vállalatunknak van egy olyan új terméke, amely forradalmasítani fogja az üzleti területét – különösen, ha az valamelyen áttörés az adott területen.
- Késhegyig menő fontos vitába bonyolódunk tágabb értelemben vett családunk valamelyik tagjával, és valami olyan információval rendelkezünk, amelyet ő meg akar szerezni.
- Felbosszantottunk valakit, aki ismer egy gépkalózt.
- Jó hitelbesorolásunk van, ami a személyazonosságunkat különösen vonzóvá teszi.
- Vállalatunk olyan üzleti területen dolgozik, hogy súlyosabb üzemszava-ra segítene valamelyen csoportnak (vagy valakinek) abban, hogy egy el-képzeli-süket, állításukat hangsúlyosabbá tegyék.
- Vállalatunk olyan információval rendelkezik egy másik vállalatról, ami valaki másnak fontos.
- Vállalatunk valamelyik alkalmazottja elégedetlen, és elvi kérdésnek tekinti a visszavágást.
- Egy elkeseredett válási folyamat során valamit el akarunk rejteni az ügyvédek elől (lehet mosolyogni ezen a kitételen, de valóban előfordulhat ilyen helyzet).
- Vállalatunk a világ olyan részén (is) folytatja üzleti tevékenységét, amely szociális vagy politikai forrongások színtere – napjaink egyes gépkalózai geopolitikai öntudattal is rendelkeznek.

A fenti esetekben, és számos ezekhez hasonlóban, „hivatalosan” is kiválasztott célpont lehetünk. A gépkalóz nyilván a korábban említett szubkultúrához fog tartozni, de nem feltétlenül viselkedik úgy, mint egy amerikai filmben. Megemlíthetjük még a magánnyomozókat és az ügyvédeket is, közöttük is lehet olyan, akit a vállalatunk vagy általunk birtokolt információ érdekel.

Mivel olyanok bízzák meg őket, akik számos különböző dolgot akarnak megtudni, ezért a magánnyomozók is egyre újabb képességeket kell kifejlesszenek, így például akár az internethez is fordulhatnak ezen „titkok” megszerzése érdekében. Említsük meg a volt katonai vagy különleges biztonsági kiképzést kapott személyeket is, igen kétséges, hogy a filmbeli gépkalózsablonba illenének. Vegyük az elutasított szeretőt vagy házastársat, aki rendelkezik valamennyi számítógépes ismerettel. Vegyük a vállalat azon alkalmazottját, aki minden tud a vállalatunkkal kapcsolatban

álló cégekről. Ezen csoportok egyike sem illik bele a filmen látható sabinba, jólehet ténylegesen veszélyt jelenthetnek a hálózatunkra.

Azt is meg kell értenünk, hogy a gépkalóznak nem kell minden saját magának végeznie, és nem feltétlenül kell minden elektronikusan csinálnia. Emlékezzünk vissza a kukabúvár tevékenységre.

A kukabúvárkodás legális tevékenység, amelynek segítségével a gépkalóz számára hasznos információk különböző fajtáit lehet könnyedén be- szerezni.

A következő részben azt vizsgáljuk meg, hogyan kezdődhet egy támadás, és megfigyeljük azt a folyamatot, amellyel a támadó megkezdheti a célrendszer biztonságának feltörését.

## 1.5. A TÁMADÁS FOLYAMATA

Számos különböző módon kísérelheti meg a támadó a rendszerhez való hozzáférési jogosultság megszerzését. Ez a rendszer lehet egyszerű házi számítógép, amely modemmel csatlakozik az internetre, de lehet egy bonyolult vállalati hálózat is. A gépkalóz által támadni kívánt rendszer fajtájától függetlenül, a támadás során végrehajtott lépések a következők:

1. felderítés és nyomkeresés,
2. letapogatás,
3. kiértékelés,
4. hozzáférés megszerzése,
5. jogosultság kiterjesztése,
6. hátsó ajtók létrehozása és a nyomok elfedése.

A következő pontokban ezeket a lépeket vizsgáljuk meg részletesen. Rendkívül fontos annak megértése, hogy egy támadó az egyes lépések során mit csinál, és mi a célja vele.

### 1.5.1. FELDERÍTÉS ÉS NYOMKERESÉS (HELYSZÍNI SZEMLE)

„A csatamező felderítése” – ezzel a katonai fogalommal egy olyan módszert definiálunk, amely bármilyen katonai művelet megkezdése előtt az ellenséggel, a környezettel és a felszínnel kapcsolatos bizonytalanságokat van hivatva kiküszöbölni. A napjaink katonai cselekményei során használt távirányított repülőgépek is jól demonstrálják ezt, hiszen ezek teszik lehetővé a katonai vezetés számára, hogy kiválaszthassa a támadás idő-

pontját, illetve a még lényegesebb módját. A csatamező megismerése, és ezáltal az ellenség megtámadási módszerének pontosabb elképzelése hasonlít arra, amit a gépkalózok is tesznek.

A támadók is különböző felderítő akciókat folytatnak a vállalatunk és hálózata ellen. Ez egy folyamatos tevékenység, amely minden tervezett és végrehajtott cselekmény során használható. A hálózatbiztonsági szakemberek által biztonsági védelemmel ellátott hálózati környezet felel meg a csatamezőnek. A semmiből felbukkanó támadók és behatolók tízezrei azok az agresszorok, akik állandóan offenzívában vannak. A biztonsági szakértők a védekezők, akik bizalmi feladata az adatok bizalmasságának és sérтetlenségének megőrzése.

A hálózatbiztonsági szótárban ezt a tevékenységet nevezük felderítésnek és nyomkeresésnek, a filmekben ezt hívják „betörés előtti terepszemlének”. A valóságban számos bűnöző valószínűleg tényleg megteszi ezt, de külön nem nevezi el ezt a tevékenységet. A bűnöző például ilyenkor méri fel a kiválasztott üzlet biztonsági védelmét, hogy megismerje, hol tartják a pénzt, hol vannak a biztonsági kamerák, merre vannak a lehetséges kijáratok és hasonló információkat gyűjt, amelyek a bűn elkövetésében később majd segítségére lesznek. Amint az 1.1. táblázatban is látható, ebben a fázisban a gépkalózok is minden össze információt gyűjtenek.

#### 1.1. táblázat. A felderítés és nyomkeresés célja

Technológia	Megszerzett tudás
Hálózati jelenlét	<p>Ideális esetben a célnak az Internetre kell csatlakoznia, így a támadó az alábbi információkat akarja megszerezni:</p> <ul style="list-style-type: none"> <li>• A céltartományban használt neveket és a tartományinév-szolgáltatók címét, valamint a kiosztott nyilvános IP-címtartományt?</li> <li>• A kiosztott IP-címek közül melyek érhetők el az internetről?</li> <li>• Az internetről elérhető IP-című gépeken milyen szolgáltatások (www, ftp, email stb.) támadhatók?</li> <li>• A megtalált szolgáltatások milyen számítógépen (hardver és operációs rendszer egyaránt) futnak? Operációs rendszer esetén melyik verzió és melyik fordítás, hogy a lehetséges sérülékenységekre lehessen következtetni. Lehet például Windows, Linux, UNIX, Solaris stb., és ezek különböző változatai – mindegyiknek megvannak a maga gyenge pontjai.</li> <li>• Van-e valamilyen, a hálózati hozzáférést szabályozó mechanizmus a rendszerben?</li> <li>• Milyen típusú tűzfalra, illetve behatásjelző rendszerre (<i>IDS – intrusion detection system</i>) lehet számítani?</li> <li>• A rendszer kiértékelése a rendszer és bizonyos adatai (felhasználói és csoportnevek, útválasztó táblák, SNMP információk) azonosítását teszi lehetővé.</li> <li>• Az eszközök és rendszerek fizikailag hol helyezkednek el?</li> <li>• Milyen hálózati protokollok (kommunikációs és útválasztó) létezik (például IP, IPX, OSPF vagy RIP)?</li> </ul>

Technológia	Megszerzett tudás
Hálózati jelenlét	<ul style="list-style-type: none"> <li>Egyszerű hálózati térkép összeállítása a fenti információk és a hálózati hozzáférést biztosító cég feltüntetésével.</li> <li>Minden olyan ismeret megszerzése, amely megkönnyíti a pszichomérnöki tevékenységet.</li> <li>A rendszerekkel kapcsolatba kerülő személyek adatai: neve, telefonszáma, beosztása, címe, milyen adatokat ismerhet stb.</li> </ul>
Belső hálózat jellegzetességei	A hálózati szakemberek tisztában vannak azzal, hogy a gépkalózok az internethez való hozzáférés megszerzését kísérlik meg, így a legtöbb hálózatnak kettős infrastruktúrája van: a tűzfalon belül és kívül. Ezt viszont a támadók is tudják, így az alapos gépkalóz megismétli a fenti nyomozati munkát a belső hálózaton (intranet) is.
Távoli hozzáférés	<p>A legtöbb vállalatnak nem csupán a szokásos szélessávú vonali Internetelérése van, de létezik telefonos behívó csatlakozási pontja is. Ez egy további lehetőséget nyújt a támadó számára a hálózatba való belépésre, ezért a gondos gépkalóz az alábbi információkat is kinyomozza:</p> <ul style="list-style-type: none"> <li>Milyen típusú távoli elérés létezik?</li> <li>Hova csatlakozik a távoli elérési pont, és hol van a csatlakozó célállomás?</li> <li>Miként szabályozzák a hálózati hozzáférést (RADIUS, TACACS stb.)?</li> </ul>

Nyilvánvaló, hogy a támadónak számos lehetősége van a hálózatunkról szóló információk tudomásunk nélkül való megszerzésére. Vegyük például a hálózatunkról csupán a tartományi névszolgáltató rendszerből (*DNS – Domain Name System*) megtudható információkat, amelyeket egy egyszerű program (*nslookup*) segítségével kaphatunk meg (lásd 1.1. példa).

#### 1.1. példa. A DNS használata passzív felderítésre

```
E:\>nslookup
Alapértelmezett kiszolgáló: ceres.ik.bme.hu
Address: 10.0.0.2
```

```
> www.cisco.com
Kiszolgáló: ceres.ik.bme.hu
Address: 10.0.0.2
```

Nem mérvadó válasz:  
 Név: www.cisco.com  
 Address: 198.133.219.25

```
> set querytype=mx
> cisco.com
Kiszolgáló: ceres.ik.bme.hu
Address: 10.0.0.2
```

Nem mérvadó válasz:

cisco.com	MX preference = 20, mail exchanger = sj-inbound-2.cisco.com
cisco.com	MX preference = 20, mail exchanger = sj-inbound-3.cisco.com
cisco.com	MX preference = 20, mail exchanger = sj-inbound-4.cisco.com
cisco.com	MX preference = 30, mail exchanger = proxy9.cisco.com
cisco.com	MX preference = 50, mail exchanger = proxy6.cisco.com
cisco.com	MX preference = 10, mail exchanger = sj-inbound-0.cisco.com
cisco.com	MX preference = 20, mail exchanger = sj-inbound-1.cisco.com
sj-inbound-2.cisco.com	internet address = 128.107.250.143
sj-inbound-3.cisco.com	internet address = 128.107.250.144
sj-inbound-4.cisco.com	internet address = 128.107.250.145
proxy9.cisco.com	internet address = 192.135.250.71
proxy6.cisco.com	internet address = 64.104.252.245
sj-inbound-0.cisco.com	internet address = 128.107.250.141
sj-inbound-1.cisco.com	internet address = 128.107.250.142
>	

Láthatjuk, hogy csak a DNS-eszközök segítségével a támadó felfedheti a Cisco webszerverének címét, valamint a névszolgáltató és a levelezőszervereit, valamint az is kiderül, hogy közvetítő szerverek is vannak. Másik egyszerű eszköz a whois (jelentése: ki az), amelyet számos szabadon elérhető alkalmazás nyújt, de az alábbi helyeken az interneten is elérhető. A kedves olvasó próbálja ki a megfelelőt a saját tartományára!

- <http://www.networksolutions.com/> – a whois webfelülete
- <http://www.arin.net> – ARIN Whois
- <http://www.ripe.net/whois> – Európai Whois
- <http://whois.apnic.net> – Ázsia Csendes-óceáni IP-címek kiosztása (Asian Pacific IP Address Allocations)
- <http://whois.nic.mil> – U.S. hadsereg
- <http://whois.nic.gov> – U.S. kormányzat

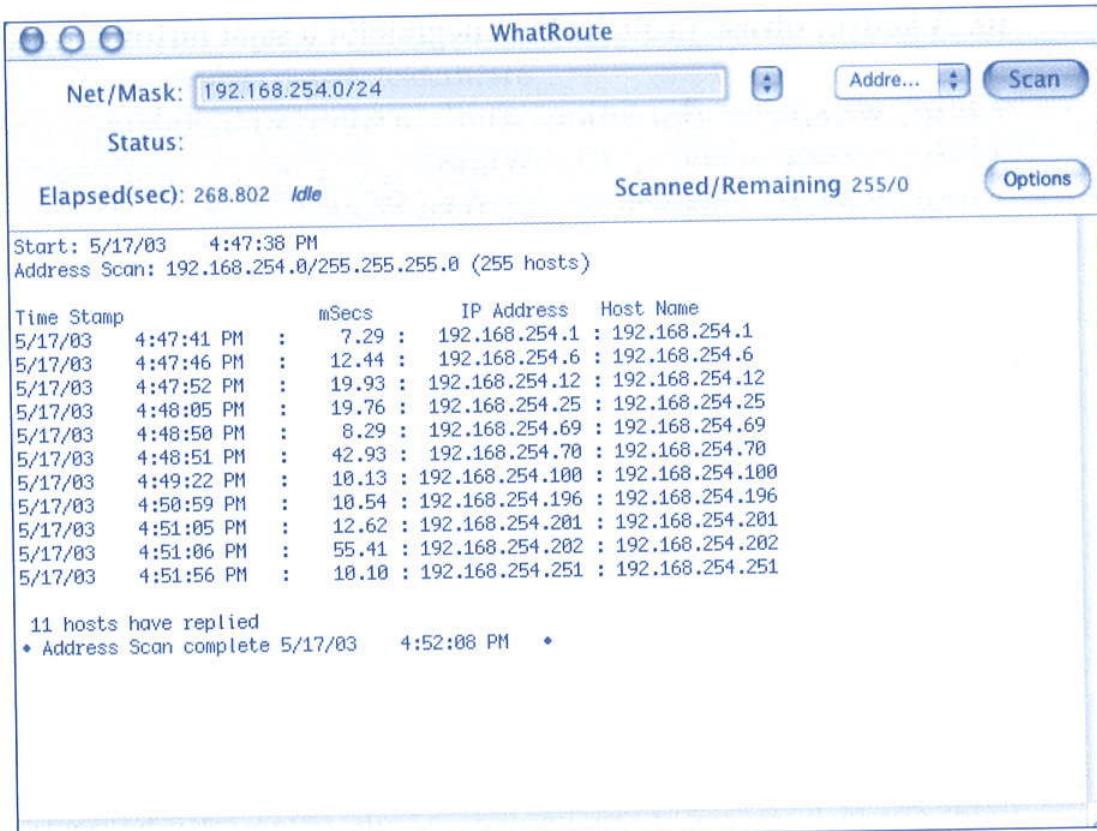
Mivel a DNS-lekérdezések minden naposak minden rendszerben, így a Cisco biztonsági érzékelőit nem aktiválja az előbb ismertetett **passzív feldeírás** (*passive reconnaissance*). Ne feledkezzünk meg a cégek honlapján megtalálható információkról sem: mennyire hasznos lehet ismerni a vállalat nevét, telefonszámait, faxszámait, leányvállalatait, kiadványait, és a vezérkar összetételét (beleértve a tagok rövid életrajzát is). A célok kereskedelmi honlapja olyan információforrássá vált, amelyből a támadó rengeteg információt gyűjthet össze. Az így szerzett tudást fel lehet használni a pszichomérnöki tevékenység során, valamint a hálózati rendszerek és rendszergazdák azonosításához, egyebekhez. A gépek lekérdezé-

sével a technikai kapcsolattartó személyek és a rendszergazdák könnyen azonosíthatók. Ezen információk lenyomozására kellő időt szánva a támadó a célhálózatot sokkal alaposabban ismerheti meg.

Számos támadó a passzív mellett **aktív felderítést** (*active reconnaissance*) is végez, hogy meghatározhassa a nyilvános IP-című gépeken futó szolgáltatásokat.

Sajnálatos módon a legtöbb vállalat nincs felkészülve arra, hogy felfedje ezen letapogatásokat vagy próbákat. Ennek oka semmiképpen sem az, hogy nem állnak rendelkezésre az ehhez szükséges alapvető eszközök, sokkal gyakoribb, hogy az eszközök nem naplózzák, mi is történik rajtuk – vagy ha mégis naplózzák, akkor senki nem olvassa ezeket a naplókat. Tegyük fel, hogy a következő lépések egyike az IP-címtartomány megpinggetése, az interneten ingyen elérhető (és a legtöbb operációs rendszerben alapértelmezésként rendelkezésre álló) számos eszköz egyikével. Az 1.1. ábrán a WhatRoute alkalmazás segítségével történő lekérdezés eredménye látható (ez a kitűnő eszköz megtalálható a <http://www.whatroute.net> címen).

A támadók tudják, hogy a legtöbbször észrevétlenek maradnak, azonban azzal is tisztában vannak, hogy minél tevékenyebben tapogatják le a hálózatot, annál nagyobbra növekszik a felfedezésük kockázata. A támadó tehát az aktív felderítést addig folytatja, amíg elegendő ismeretet nem gyűjt a hálózatról a felderítés megkezdhetőségehez. Ha ez a felderítés si-



1.1. ábra. Egy C osztályú hálózaticím-tartomány pingetéssel való letapogatása

kerrel jár, a támadó megkezdi a következő lépést, ha nem, akkor visszatér a további adatgyűjtéshez.

A támadás ezen fázisa során a gépkalózok óvatos és visszafogott módszerekkel próbálkoznak tehát, amelyek remélhetőleg nem eredményezik a támadás tényének felismerését. A támadó meg akarja határozni a vele kapcsolatba kerülő hálózat, és az esetleg érintett személyek fajtáját: a rendszert, a hálózatot és a biztonságért felelős személyeket. A cél tehát az, hogy elkészülhessen a hálózat részletes, információgazdag térképe, amely a nyomkeresés során megtalált adatokat tartalmazza. E térkép alapján lehet kitalálni, hogy mely eszközök üzemelnek tűzfalként és útválasztóként (*router*), melyek a kulcsrendszerek (például levelezőszerverek, névszerverek, állományszerverek stb.). A támadó azt is meg akarja tudni, hogy a célrendszernek honnan biztosítják az internet-hozzáférését, hátha az internetszolgáltató felől is meg lehetne próbálni a célohoz való hozzáférést.

### Megjegyzés



*A kedves olvasó végezzen el egy google-keresést, rákeresve a „Welcome to IIS 4.0” kifejezésre, s rögtön meg fogja látni, milyen sok IIS-kiszolgáló üzemel szerte a nagyvilágban. Maga a tény, hogy ilyen sok találat van, rendkívül sokatmondó, és nagyon jól példázza, mennyire nemtörődöm módon installálják és telepítik a cégek a webszervereiket. Amíg ez így marad, a gépkalózoknak kimeríthatlen készletük lesz a kiválasztható és támadható szerverekből.*



## 1.5.2. LETAPOGATÁS

Elérve ezt a mérföldkövet a támadónak már meglehetősen pontos elképzelése van a hálózaton elhelyezkedő gépekről, ezek operációs rendszereiről, tudja, kik a rendszergazdák, feltehetőleg ismeri a különböző hírcsoportokban az általuk postázott üzenetek tartalmát, irodájuk címét és nagy vonalakban a behatolást megakadályozó rendszerük (*IPS – intrusion prevention system*) felépítését is. A támadó azt is tudja, hogy ettől kezdve minden lépése nagy valószínűséggel naplózásra kerül, erre legalábbis számítania kell. Rendelkezésére áll a hálózat és az eszközök térképe, és készen áll a válaszadásra kész kiszolgáló programok és a nyitott portok azonosítására. A gépkalóz elsőként meghatározza, mekkora a még elfogadható kockázat mértéke. Ezen belül mekkora veszélyt jelent, ha naplózzák a letapogatási tevékenységét; a támadás későbbi szintjein elfogadható-e a lelepleződés veszélye; szükség van-e az eredeti támadási hely későbbi elrejtésére; ha másvalaki kérésére tevékenykedik, mennyire fedi fel a meg-

bízó kilétét a támadás során? Ilyenkor számos hasonló kérdés merül fel a támadóban. Egyesek tervvázlatot készítenek, mások csak fejben tartják ezeket a szempontokat, amint lépésről lépésre haladnak előre.

Az 1.2. példán a támadó az nmap ingyen elérhető program ([www.insecure.org](http://www.insecure.org)) segítségével sokkal aktívabb letapogatási támadást indított a célrendszer ellen. Ezt a programot mind a gépkalózok, mind az etikus támadók (*hacker*) gyakran használják. Lévében ingyenes, egyetlen szkriptcsávó eszköztárából sem hiányzik!

#### 1.2. példa. Aktív port letapogatás eredménye

```
[AppleKick:/Users/topkick] topkick# nmap -sS -O 192.168.254.69
```

```
Starting nmap V. 3.00 ( www.insurance.org/nmap/ )
Interesting ports on  (192.168.254.69):
(The 1579 ports scanned but not shown below are in state: closed)

```

Port	State	Service
7/tcp	open	echo
9/tcp	open	discard
13/tcp	open	daytime
17/tcp	open	qotd
19/tcp	open	chargen
25/tcp	open	smtp
42/tcp	open	nameserver
53/tcp	open	domain
80/tcp	open	http
119/tcp	open	nntp
135/tcp	open	loc-srv
139/tcp	open	netbios-ssn
443/tcp	open	https
445/tcp	open	microsoft ds
563/tcp	open	snews
1025/tcp	open	NFS-or-IIS
1027/tcp	open	IIS
1031/tcp	open	iad2
1033/tcp	open	netinfo
3372/tcp	open	msdtc
3389/tcp	open	ms-term-serv

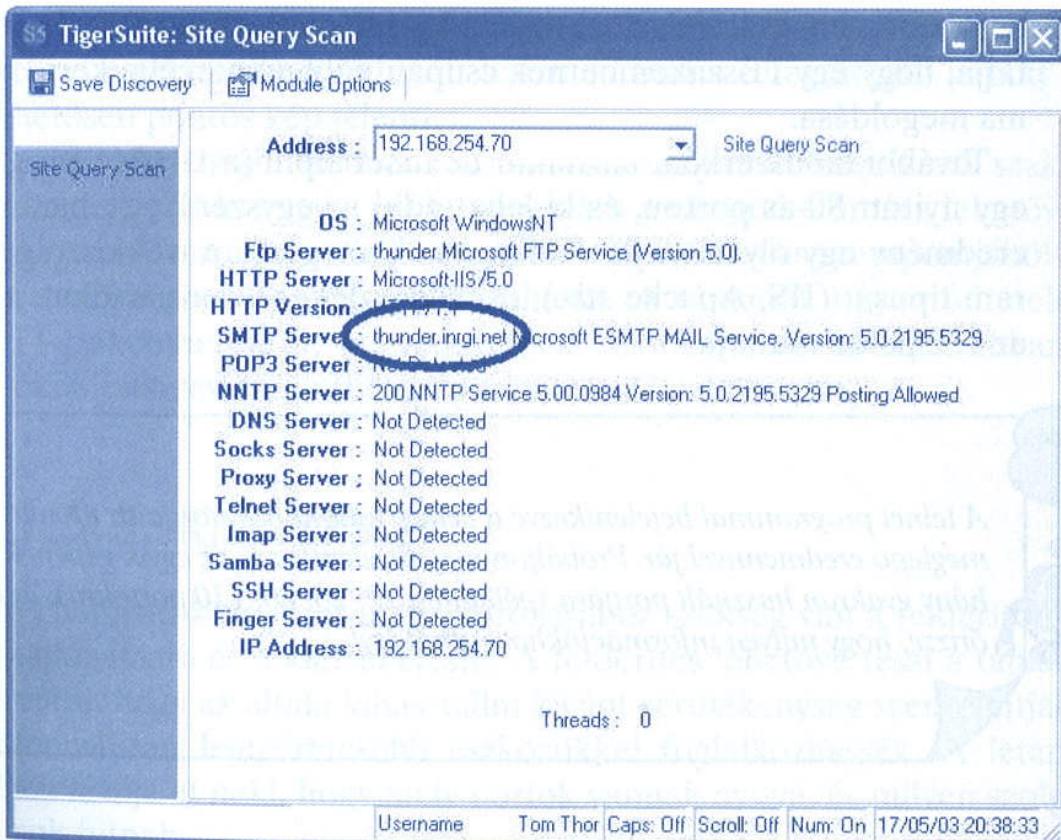
```
Remote operating system guess: Windows 2000/XP/ME
```

```
Nmap run completed - 1 IP address (1 host up) scanned in 5 seconds
[AppleKick:/Users/topkick] topkick#
```

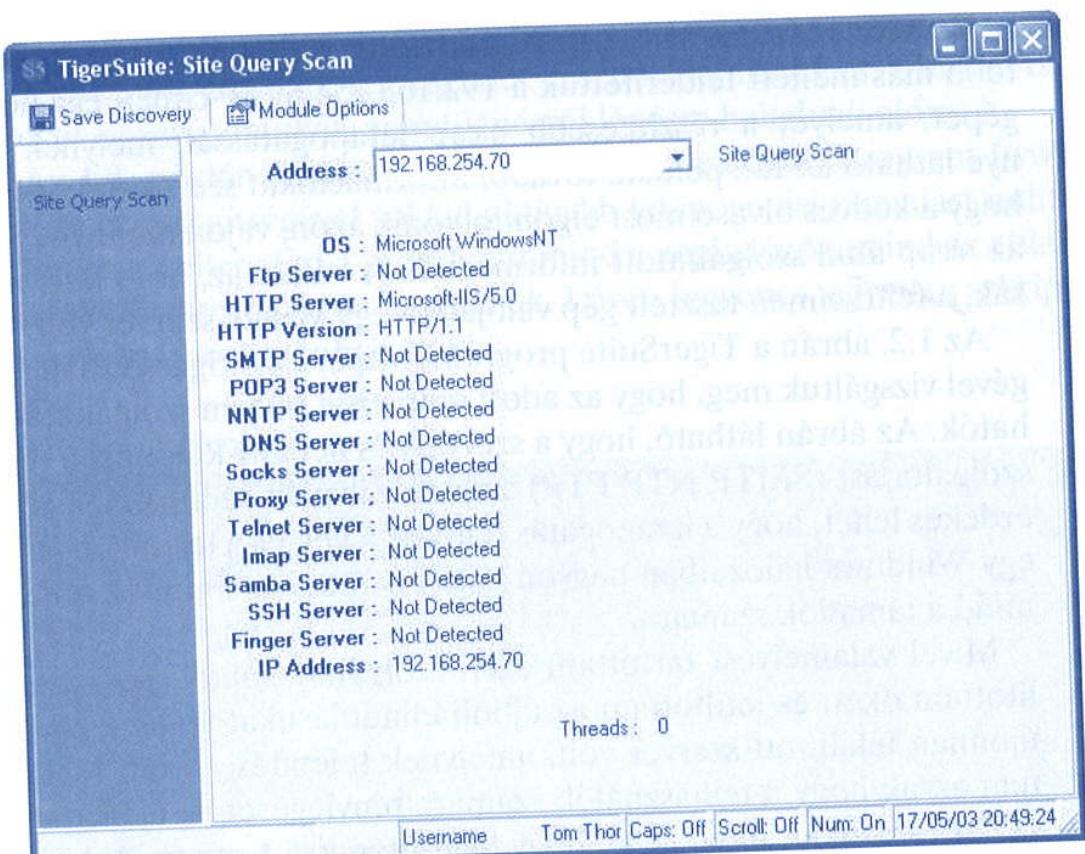
Ha visszanézünk az 1.1. példára, akkor láthatjuk, hogy a pingetéssel több más mellett felderítettük a 192.168.254.69 IP-címen egy bekapcsolt gépet, amelyet a részletesebb nmap letapogatással, melynek eredménye látható az 1.2. példán, további információkat szereztünk róla. Lehet, hogy a kedves olvasó most elgondolkodik azon, vajon mennyire pontosak az nmap által szolgáltatott információk. A válasz az, hogy *nagyon* pontosak, a fenti címen tesztelt gép valójában egy Win2k szerver volt.

Az 1.2. ábrán a TigerSuite program (<http://www.tigertools.net>) segítségével vizsgáltuk meg, hogy az adott szerveren milyen szolgáltatások találhatók. Az ábrán látható, hogy a szervert és néhány különösen sérülékeny szolgáltatást (SMTP, NTP, FTP) azonnal sikerült azonosítani. Különösen érdekes lehet, hogy a letapogatás felfedte a gép és a tartomány nevét, ami egy Windows-hálózatban nagyon hasznos tudnivaló minden felhasználók, mind a támadók számára.

Mivel valamelyest tartottam ezen szolgáltatásoktól, így azonnal leálítottam őket, és letiltottam az újbóli elindulásukat is. Ez egy viszonylag újonnan felállított szerver volt, amelynek telepítése során többet törődtem azzal, hogy a felhasználók számára ténylegesen nyújtásak a megígért szolgáltatásokat, mint azzal, hogy biztonságossá tegyem. A szíve mélyén az operációs rendszerek legtöbb szállítója segítőkész, és a kezdetektől fogva beüzemeli a rendszer minden lehetőségét és szolgáltatásait, lecsökkenve így a (számukra) költséges ügyfélszolgálati hívásokat. Ennek a



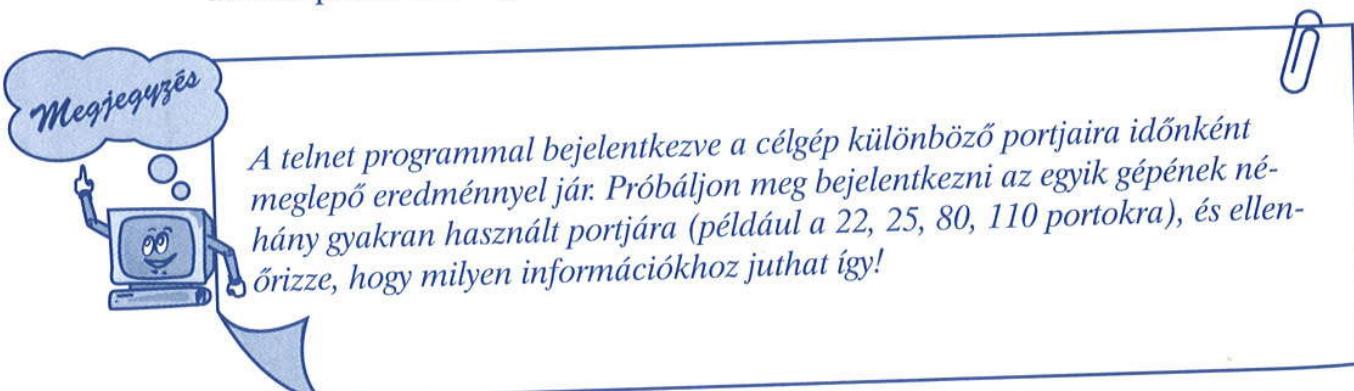
1.2. ábra. Szervert lekérdező letapogatás



1.3. ábra. Biztonságosabbá tett szerver lekérdező tapogatásának eredménye

döntésnek a meghozatala során kicsit sem törődtek a biztonsággal, csak a pénzzel. Nyilván azt akarják, hogy a főnökük a világ leggazdagabb embere lehessen. Felelőtlen motivációiktól függetlenül az 1.3. ábra azt mutatja, hogy egy IT-szakembernek csupán néhány percébe kerül a probléma megoldása.

További módszerként bármikor be lehet lépni (a telnet programmal) egy nyitott 80-as porton, és ki lehet adni az egyszerű get parancsot. Az eredmény egy olyan „fejléc” lesz, amely megadja a webkiszolgáló program típusát (IIS, Apache stb.), és más érdekes információkat, amint azt az 1.3. példa mutatja.



1.3. példa. A telnet használata a 80-as porton a szerver azonosításához

```
[AppleKick:~] topkick% telnet 192.168.254.69 80
Trying 192.168.254.69...
Connected to 192.168.254.69.
Escape character is '^']'.

get

HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Tue, 20 May 2003 00:43:14 GMT
Content-Type: txt/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is incorrect.
</body></html>Connection closed by foreign host.
[AppleKick:~] topkick%
```

A letapogatás egy másik fajtáját nevezzük a **gyenge pontok letapogatásának** (*vulnerability scanning*). Ezt legtöbbször kívülről, az internetről hajtják végre. Célja annak ellenőrzése, hogy mennyire jól van védve a rendszer.

Láthatjuk tehát, hogy a felderítési fázis során alkalmazott valamennyi technikának megvan a maga gyümölcse, de a támadó számára az igazi értéket a technikák kombinált használatával a céleszközről kapott meglehetősen pontos kép jelenti.

Mielőtt továbbmennénk a támadási folyamat következő szakaszára, megjegyezzük, hogy a cél letapogatása a támadó számára lehetővé teszi, hogy erőfeszítéseit a hálózatunkba való behatolás szempontjából legígéretesebb pontokra összpontosíthassa. A támadók ugyan feltételezik az IT-szakemberekről, hogy figyelnek, azonban kételkednek abban, hogy őket is észrevennék (bár ez a feltételezés változhat is).

### 1.5.3. KIÉRTÉKELÉS

A hálózati környezet meghatározásához szükség van a felderítésre, a letapogatásra és a kiértékelésre. A felderítés lehetővé teszi a támadó számára, hogy az általa kihasználni kívánt sérülékenység szempontjából potenciálisan legígéretesebb eszközökkel foglalkozhassék. A letapogatás azt árulja el neki, hogy mely portok vannak nyitva, és milyen szolgáltatások futnak.

A kiértékelés az elérhető erőforrások és érvényes témaszám<sup>5</sup> információk (valid account information) beszerzését jelenti. Az előző két lépésben szemben a kiértékeléshez már arra van szükség, hogy az adott rendszerekhez aktív csatlakozásokat hozhasson létre, és kifejezetten ezeknek címzett közvetlen parancsokat adhasson ki.



*Az előzőekben arra a következtetésre jutottunk, hogy a támadók számítanak ugyan arra, hogy észreveszik őket a felderítés során, ám azt reméljük, hogy figyelmen kívül hagyják a tevékenységüket. Amint megkezdődik azonban a kiértékelés, a helyzet megváltozik – ezeket a támadási próbálkozásokat meg kell állítani, vagy legalább naplózni kell őket, és válaszlépésekkel kell tenni ellenük!*

Akárcsak a támadás többi szintjén, minél több részműveletet végezhet el a támadó, annál nagyobb a valószínűsége a sikерnek. A hálózaton belül az alábbi négy kategória található:

- hálózati erőforrások és megosztások,
- felhasználók és csoportok,
- alkalmazások,
- eszközök üdvözlő szövegei.

A fenti kategóriák természetesen minden operációs rendszerben különbözőképpen vannak megvalósítva. Így például mindegyik elterjedt operációs rendszer lehetővé teszi a megosztások létesítését, de mindegyikük – Mac OS, Windows, Linux és Novell – másként kezeli ezeket. Ez azt jelenti, hogy – a támadó szempontjából – minden operációs rendszert másként kell kezelni.

A többszintű megközelítésre adott korábbi példa most nyer igazi értelmet, hiszen egy korábbi szinten az nmap program adott jó becslést arra vonatkozóan, hogy milyen operációs rendszert is kell támadni.

### A Windows kiértékelése

A számítógépes operációs rendszerek piacvezetőjeként valószínűleg a Microsoft Windows a legtöbbet tárgyalt rendszer, így érdemes már most kissé közelebbről megvizsgálnunk. A Windows-rendszer még ma is erősen függnek a NetBIOS használatától (UDP 137 port), ráadásul számos olyan eszköz, amit a támadó egy Windows-alapú hálózat felderíté-

<sup>5</sup> Windows-környezetben ismert neve: „bejelentkezési fiók”.

sére akarhat használni, eleve be van építve magába az operációs rendszerbe.

Az 1.4. példában a Windows-rendszer alatt üzemelő gépen parancssor-ból kiadott net view parancs futásának eredménye látható. Ebben az esetben a tartománynév (*domain name*) ismert volt, ezért a parancssal ezen tartomány gépeit tudtuk felfedni, ha a tartománynév nem ismert, akkor a parancs a helyi hálózaton elérhető tartományok neveit listázta volna ki.

#### 1.4. példa. A Windows net view parancsának használata

E:\>net view	
Kiszolgálónév	Megjegyzés

\ATHENE	
\CERES	
\CHAOS	
\DEFACTO	
\HERA	Hera Samba Server
\ITRUST	
\JUPITER	
\MARS	
\VIDEO	Gergő gépe
\WKSABA	
\WKSBD	
\WKSFA	Zoli gépe
\WKSIVAN	Iván gépe
\WKSKO	
\WKSPET	
\WKSPISTA	

A parancs sikeresen végrehajtódott.

1.

Ez a kiértékelési technika még hasznosabb, ha kombináljuk azt a korábbi pingelési letapogatás eredményével. Az IP-címek és a NetBIOS-nevek ugyanis egyaránt használhatók a Windows-hálózatban. Egy másik számítógéphez tehát hozzá lehet férni a névvel: \SZÁMÍTÓGÉP\_NÉV, de ugyanígy hozzáférhetünk az IP-címével is: \192.168.254.69. A támadók természetesen tisztában vannak ezzel, ezért eleve úgy módosítják a saját rendszereiket, hogy azok automatikusan „gyorsítótárazzák” a NetBIOS-neveket.

Egy másik remek beépített Windows-eszköz az nbtstat, amely egy másik számítógép NetBIOS névtáblájának lekérdezését teszi lehetővé. Ez azt jelenti, hogy egy támadó lekérdezheti akár a szervertől is a névtáblákat, amint az 1.5. példán is látható.

### 1.5. példa. Lekérdezés az nbtstat segítségével

```
E:\>nbtstat -A 10.0.0.3
```

Helyi kapcsolat:

Csomópont IP-címe: [10.0.2.36] Hatókör azonosítója: []

NetBIOS távoli számítógépnév táblázat

Név	Típus	Állapot
JUPITER	<00> EGYEDI	Regisztrált
JUPITER	<20> EGYEDI	Regisztrált
IK	<00> CSOPORT	Regisztrált
IK	<1C> CSOPORT	Regisztrált
IK	<1B> EGYEDI	Regisztrált
IK	<1E> CSOPORT	Regisztrált
IK	<1D> EGYEDI	Regisztrált
..._MSBROWSE_.<01>	CSOPORT	Regisztrált
ConfigServer	<1C> CSOPORT	Regisztrált
jupiter	<2D> EGYEDI	Regisztrált

MAC-cím = 00-00-0D-00-89-4C

Ha nem ismernénk az IP-címét valamelyik gépnek, amelynek tudjuk a NetBIOS-nevét, akkor használhatjuk az nbtstat -c parancsot, amely megadja a gyorsítótárban található valamennyi NetBIOS-névhez a hozzá tartozó IP-címet (1.6. példa). Ugye milyen kedvesek ezek a barátságos operációs rendszerek?

### 1.6. példa. Az nbtstat -c parancs használata

```
E:\>nbtstat -c
```

Helyi kapcsolat:

Csomópont IP-címe: [10.0.2.36] Hatókör azonosítója: []

NetBIOS távoli gyorsítótár névtáblázat

Név	Típus	Állomáscím	Élettartam [mp]
ATHENE	<20> EGYEDI	10.0.0.5	470
JUPITER	<20> EGYEDI	10.0.0.56	422
IK	<1B> EGYEDI	10.0.0.56	422

A támadót ezen információk megszerzésében úgy lehet a legkönnyebben megakadályozni, hogy az útválasztón (router) és a tűzfalon megtiltjuk a NetBIOS-csomagok áthaladását mind befelé, mind kifelé. Legjobb, ha minden kettőt lezárjuk, ezzel is nehezítve még a többszintű támadásokat is. Az alábbi portokat kell bezárni:

- TCP és UDP 135...139 portok,
- TCP és UDP 445 port Windows 2000 és XP esetén.

Ezen portok blokkolása nem teszi működésképtelennek a NetBIOS-t, csupán nem engedi meg azt, hogy kívülről a hálózatunkba léphessenek be vele. Több különböző módon is letiltható lenne egyébként a NetBIOS a számítógépen, azonban a nyújtott szolgáltatásai miatt ez nem mindig engedhető meg. Az 1.2. táblázatban soroljuk fel a támadó által végrehajtott leggyakoribb feladatokat és a hozzájuk felhasznált eszközöket.

1.2. tábla. A támadó feladatai, eszközei és technikái

Támadó feladata	Eszközök és technikák
Állománymegosztások listázása	A helyszínen kell lenni (a belső hálózatban)
Felhasználónevek listázása	NetBIOS és NetBEUI
Alkalmazások azonosítása	Telnet segítségével az alapértelmezett üdvözlő szövegek olvasása
Operációs rendszerek azonosítása	Windowsos „null szakaszok” (null sessions)

Amint azt korábban már említettük, minden egyes operációs rendszerhez megvannak a megfelelő kiértékelési technikák. Ezúttal csak a Windows ellen használhatók közül vizsgáltunk meg néhányat, de van még több is. A fejezet későbbi részében található néhány ajánlott irodalmi hivatkozás, amelyekből többet is megtudhatunk a további kiértékelési lehetőségekről.

1.

#### 1.5.4. HOZZÁFÉRÉS MEGSZERZÉSE

Sokan tévesen azt gondolják, hogy a támadók át akarják venni az uralmat a céleszköz fölött, vagy hogy ez lenne a támadás végső célja. Ez azonban nincs teljesen így. Sokkal valószínűbb, hogy a támadó csupán hozzáférést akar a célként kiválasztott számítógépre. Miután a kiértékelés felfedte az igéretes belépési pontokat, megkezdődhet a sokkal intenzívebb támadás az érvényes témaszámok és a gyengén védett erőforrás-megosztások felfedése, és végső soron a behatolási lehetőség megszerzése érdekében.

A támadónak a rendszer valamelyen jellemzőjét kihasználva be kell tudnia lépni abba a rendszerbe. A felderítésnek alapvetően négy fő típusa van, amelyek a támadó által megtámadott rendszer különböző lehetőségeire vezethetők vissza:

- operációs rendszer támadása,
- alkalmazás támadása,
- konfigurációs hiba támadása,
- szkripttámadás.

Ezen különböző lehetőségeken belül is kétféle módon folytatható a támadás:

- **Automatikus támadás** – Ez a támadástípus (mely jellegénél fogva alkalomszerű) általában a cél egy vagy több lehetőségét igyekszik kihasználni. Az automatikus támadás olyan értelemben alkalomszerű, hogy az IP-címek egy adott csoportját tapogatja le, a sérülékeny pontokat megtalálandó. Példaként vegyük egy olyan automatikus támadást, amely egy C osztályú IP-címtartomány címeit támadja egymás után, minden egyiken megvizsgálva a 80-as portot, hogy kihasználhassa a webszerverek egy ismert gyengeségét. Ha a letapogatás sikeres, akkor a támadás megkezdődik a megtalált címen, ha sikertelen, akkor folytatja a következő címmel.
- **Célzott támadás** – Ezen típusú támadások veszélyesebbek az automatikusnál, mivel ilyenkor a támadás kifejezetten az adott rendszerre összpontosul. Másként megfogalmazva, a támadó tudja, hogy van valamink, aminek megszerzésére nagyon vágyik, esetleg elérheti valamely célját azzal, hogy sikerre viszi a támadását. Ez utóbbi esetben a támadót egyre inkább politikai vagy társadalmi célok vezérelhetik. Szerencsére a célzott támadások képezik az internetes cselekmények kisebb részét. Lehangoló azonban az a tudat, hogy amennyiben mégis célzott támadás áldozataivá válnánk, akkor minél képzettebb a támadó, annál kissebb valószínűséggel vesszük észre a támadás tényét.

Amikor azt vizsgáljuk, hogy a támadás a rendszer mely lehetőségeit érintheti, ne feledkezzünk meg e kétféle támadási módról.

### Operációs rendszerek megtámadása

Az operációs rendszert arra terveztek, hogy a felhasználókat támogassa végrehajtandó feladataik megvalósításában, többek között tehát valami-lyen szinten képesnek kell lennie a hálózati működésre is. Amint növekszenek a hálózati működéssel szembeni elvárások, annál több szolgáltatás aktiválódik ezen igények kielégítésére. Ez egyre több nyitott portot, vala-

mint aktív és látható szolgáltatást jelent, ami nyilván a lehetséges támadásoknak is szélesebb teret nyit.

A felhasználók és a rendszergazdák ráadásul gyakran azt hiszik, hogy munkájuk befejeződött azzal, hogy az operációs rendszert feltelepítették, és bekapcsolták az összes szükséges szolgáltatást. Ez a hibás hozzáállás eredményezi azután, hogy a rendszerük a támadók kitűnő célpontjává válik. Tegyük fel, hogy támadóként találunk egy olyan szervet, amelyre az operációs rendszert a létező biztonsági javítások nélkül tették fel, ráadásul valamennyi alapértelmezett szolgáltatást is bekapcsolták. Ezt a szervet perceken belül fel lehet törni!

### Alkalmazások megtámadása

Régebben dolgoztam egy olyan vállalatnak, amely egyik termékeként egy hálózati alkalmazást árult. Ez egy nagy, nemzetközi vállalat volt, széles körű telekommunikációs tapasztalattal a háta mögött. Ennyi háttérinformációból bárki azt gondolná, hogy egy ilyen cég szoftvere magán viseli a vállalat technológiai és biztonsági tapasztalatainak nyomát.

Sajnos, egyáltalán nem ez volt a helyzet: a programozók állandóan hihetetlenül szoros határidők nyomása alatt voltak, és újabb szolgáltatások megvalósítását követelték tőlük. Sokukat ismertem – valamennyien a helyes utat kívánták követni, de a külső körülmények egyszerűen nem tettek ezt számukra lehetővé. A szoftverek például egyáltalán nem voltak a megfelelő módon leteszelve.

Ez a tény, párosulva az állandó új szolgáltatások megkövetelésével, számos lehetőséget teremtett a támadók számára. Ez elég szörnyen hangzik, azonban a felhasználók néhány éve még egyáltalán nem törődtek a biztonsággal, kizártólag azt vizsgálták, hogy a szoftver megvalósítja-e mindeneket a szolgáltatásokat, amelyekre szükségük van. Lehet, hogy ha a vevők jobban megfontolják, mire is költik a pénzüket, akkor a szoftver biztonsága sokkal nagyobb súllyal fog a latba esni.

### Hibás konfigurációk megtámadása

A rendszergazdák, miközben biztonságosabbá akarják tenni a rendszert vagy be akarnak állítani a felhasználók számára fontos szolgáltatásokat, bekapcsolnak bizonyos lehetőségeket. A kívánt eredményt akkor érik el, amikor a megfelelő lehetőségeket mind bekapcsolták – de a munka közben gyakran bekapcsolnak olyanokat is, amelyekre nem lenne feltétlenül szükség.

Kikapcsolják-e ezeket a lehetőségeket később? Valószínűleg nem. A gond az, hogy a rendszergazda nem megy vissza a korábbi műveletekre, és nem ellenőrzi, hogy minek a hatására kezdett el működni a kívánt szolgáltatás – s így nem kapcsolja ki a szükségtelenül bekapcsolt lehetőségeket sem. Ez azért zavaró, mert a rendszer félrekonfigurálási problémái-

nak ellenőrzése egyszerű módja lenne annak, hogy a helyes működését biztosíthassuk. Ökölszabálynak azt tekinthetjük, hogy minden szükségtelen szolgáltatást ki kell kapcsolni, a bekapcsolva maradtak esetén pedig a megfelelő konfigurálásukra és biztonságossá tételekre kell összpontosítanunk.

Tartsuk nyilván írásban, hogy mely szolgáltatások és lehetőségek engedélyezettek, illetve tiltottak. A pillanat hében (különösen hajnali háromkor, miközben azon gondolkodunk, hogy mivel érdemeltük ki azt, hogy betörjenek a rendszerünkbe) ez az írásos lista segíthet majd abban, hogy a korábban szükségtelenül bekapcsolt opciókat visszaállíthassuk.

Szintén a félrekonfigurálás témakörébe tartozik egy szolgáltatás olyan módon való telepítése, hogy nem állítjuk át az eszközbe beépített alapértelmezett felhasználó nevet és jelszót. Ha a kedves olvasó most elgondolkodna azon, hogy pontosan miről is van szó, akkor javaslom a mindenutád csillogó-villogó tűzfalával együtt kapott felhasználói kézikönyv fellapozását. A mai felhasználói kézikönyvek legtöbbjének van egy „gyors beállítások” című fejezete, amely az első alkalommal történő bejelentkezést és az eszköz beállítását is ismerteti. A legtöbb ilyen biztonsági eszköznek vagy nincs kezdeti jelszava, vagy a név-jelszó pár valami admin-admin párhoz hasonló egyszerű szó. Valószínűleg nem nehéz elhinni, hogy a gépkalózok is ismerik a kézikönyveket, s különösen nagy érdeklődéssel olvassák az útválasztók, tűzfalak, hozzáférési pontok és egyéb internetes eszközök alapértelmezett jelszavait tartalmazó fejezeteit.

## Szkripttámadások

A UNIX- és Linux-rendszerök a szkripttámadásoknak kétségkívül jó találját biztosítják. Ezen rendszerek legtöbbje példaszkripteket és parancsállományként megírt programokat tartalmaz, amelyek álcázott bejáratként várják a rendszer elleni támadásokat, ha nem kapcsoljuk ki őket.

A támadás ezen fázisában a gépkalóz az alábbi támadások valamelyikével fog próbálkozni:

- **Puffermemória túlcordulása** – Az adatoknak nyilvánvalóan valahová kerülniük kell, és a támadó adott esetben úgy is irányíthatja őket, hogy segítségükkel feltörhesse a rendszert. Amikor egy memóriaterület túlcordul, az operációs rendszerek olyasmit is megtehetnek, amit a tervező álmában sem gondolt volna.
- **Jelszavak feltörése nyers erővel** – A támadó egy olyan programot indít el, amely egy szótár minden egyes szavát kipróbálja. Ez lehet egy nyelvi szótár (angolok esetén például a Webster), de lehet nevek, sportegyesületek, filmcímek, egyéb hasonló tematikus gyűjtemények listája is.
- **Jelszavak kiszimatolása** – mindenki be kell valamikor jelentkeznie, s ha egy támadó le tudja olvasni ilyenkor a jelszót, már be is jutott! Kép-

zeljük el, hogy munkakezdéskor mekkora mennyiségű jelszót lehetne leolvasni a megfelelő eszközök segítségével!

- **Jelszóállomány elfogása** – Ebben az esetben a támadó a jelszóállományt akarja megszerezni, amelyet később, a pihenőidejében megfejthet és feltörhet, méghozzá nagy valószínűsséggel nem a feltörni kívánt rendszeren, hanem a saját gépén. A támadó tehát igyekszik átmásolni ezt az állományt a saját gépére, ahol – miközben például alszik, esetleg elmegy dolgozni – a megfelelő eszközök segítségével igyekszik megfenni a benne tárolt jelszavakat.

A használt technikák, eljárások és eszközök a támadó képzettségi szintjétől, valamint program- és szkriptírási képességétől függően változhatnak. Mindenesetre rengeteg nyílt forráskódú eszközt lehet találni. A támadó nagy valószínűsséggel használja például az alábbiak valamelyikét (vagy akár többet is közülük):

- nmap – <http://www.insecure.org>
- strobe – <http://www.deter.com/unix/index.html>
- nessus – <http://www.nessus.org>
- satan – <http://www.cerias.purdue.edu/coast/satan.html>
- WinScan, Sam Spade és más hasonló eszközök Windowshoz

A CyberCop Scanner, illetve az Internet Security Scanner (ISS) programokhoz hasonló eszközök használatát sem szabad kizártani, hiszen – bár fizetni kell értük – szabadon megvásárolhatók a kereskedelemben.

A következőkben azt vizsgáljuk meg, hogy a támadó, miután sikerült behatolnia a rendszerbe, miként dolgozik azon, hogy minél több minden megtehessen (vagyis minél több jogosultsága legyen).

1.

### 1.5.5. A JOGOSULTSÁGOK KITERJESZTÉSE

A rendszer feltörése során a gépkalóz eléri azt a pontot, amikor már képes belépni a rendszerbe. Valószínűleg képes volt kitalálni/megismerni/feltörni egy felhasználó jelszavát, mivel az egyszerű volt (például a kedvenc sportegyesületének neve vagy a kedvenc filmjének a címe). Egy közönséges felhasználónak azonban nincsenek meg azok a jogosultságai, amelyekre a támadónak szüksége van a céljai eléréséhez. A támadás ezen fázisában ezért a támadó elkezd további jogosultságokat szerezni. Mivel már sokkal jobban ismeri a rendszert, így valószínűleg a következőkkel próbálkozhat:

- Mivel be tud lépni a rendszerbe, így futtathatja a rendszert feltörő megfelelő programokat, amelyek több jogosultság megszerzésével kecsegéteknek.
- Megpróbálhatja megfejteni a jelszavakat, ehhez számos ingyenesen hozzáférhető jelszótörő eszközt használhat.
- Megpróbálhat kódolatlan, vagyis nyílt szövegként (*clear text*) tárolt jelszavakat keresni a rendszerben.
- Kihasználhatja a feltört és a hálózaton található más rendszerek közötti bizalmi viszonyokat. Lehet, hogy ott további lehetőségei vannak.
- Kihasználhatja a helytelenül beállított állomány-hozzáférési és a megosztási jogosultságokat.

A támadó, miután sikerült alapszintű hozzáférést szereznie a rendszerhez, a fenti típusú tevékenységekkel fog próbálkozni. Nem azért vállalt fel annyi kockázatot és küzdött annyit, hogy most félbehagyja anélkül, hogy végső célját elérte volna.

Ha mindezek sikertelennek bizonyulnak, vagy ha a támadó eleve szolgáltatásmegtagadási (*DoS – Denial of Service*) támadást akart indítani, akkor a rendszer működésképtelenné tételehez különleges **túlterhelő kódot** (*exploit code*) futtathat. Ezek használata függ az operációs rendszertől, de függhet az alkalmazott javításuktól (*patch*) is. Ez azt jelenti, hogy az X rendszer sérülékeny a 666 túlterhelő kódossal szemben, de ha installálták rá az ötös szervizcsomagot, akkor már nem sérülékeny. A túlterhelő támadás lehet például a SYN-árادat, különböző ICMP-technikák, átlapoló szegmensekkel/offszetekkel kapcsolatos rendszerhibákat kihasználó vagy puffert túltöltő megoldások. Hatékonyságuk nagymértékben függ attól, hogy mennyire vannak installálva a rendszerben a legfrissebb javítások. A támadó tisztában van azzal, hogy amint egy túlterhelő technika ismertté válik, az hamarosan hatástanlan lesz azokkal a rendszerekkel szemben, amelyeknek a rendszergazdái rendesen ellátják feladataikat. Azzal viszont nekünk is tisztában kell lennünk, hogy naponta találnak újabb és újabb túlterhelési lehetőségeket. A támadó egyébként is tudja, hogy kutatásokra és kísérletezésre van szükség a leghatékonyabb technikák és eszközök megtalálásához.

A még hátralevő lépések már nyilvánvalóak és egyszerűek. Miután a támadónak sikerült adminisztrátori jogosultságra szert tennie (tulajdonképpen birtokolva a rendszert), végrehajtja azt, amiért az egész feltörési folyamatot megkezdte, majd megkezdi elrejteni tevékenységének nyomait, esetleg valamilyen módon lehetővé teszi későbbi visszatérését is.

### 1.5.6. A NYOMOK ELFEDÉSE

Miután a támadó képes uralni a megtámadott rendszert, ezt a tényt el kell rejtenie a rendszerelődő elől. Ez a rendszerfeltörés egyik legalapvetőbb szabálya, szerencsére egyben a legnehezebben kivitelezhető tevékenység is. A Windows-alapú rendszerekben a nyomok elfedését az eseménynapló és a rendszerleíró adatbázis (*registry*) bizonyos bejegyzéseinek törlése vagy felülírása jelenti. UNIX-alapú rendszerekben a támadó kiüríti a parancstörténeti állományt (*history file*), és lefuttat egy naplótisztító (*log wiper*) eszközt, hogy bizonyos bejegyzéseket kivegyen az *utmp*, *wtmp* és *lastlog* állományokból.



Megjegyzés

Jegyezzük meg, hogy a támadó a naplók egyes bejegyzéseit távolítja el, és nem letörli az állományokat. A naplóállományok törlésének hatására olyan értesítés következhet be, amely ráírányíthatja a támadó szempontjából nem kívánt figyelmet arra a tényre, hogy a rendszert feltörték.

Ha a támadó a rendszer eredeti feltörése után is meg akarja tartani hozzáférését, akkor a későbbi belépésekhez **rejtekajtót** (*backdoor*) helyez el. Ennek módszere, eszközei és technikája erősen rendszerfüggő, de az elérődő cél mindenkor az, hogy témaszámokat, időzítetten lefutó programokat, fertőzött indítóállományokat helyezzen el, bekapsoljon különböző távoli elérést biztosító szolgáltatásokat/szoftvereket, és a legitim alkalmazások és szolgáltatások egy részét trójaikra cserélje le. Lehetséges eszközök például a következők:

- netcat – Egyszerű UNIX-os alkalmazás, amely a TCP és UDP protokollt használva képes adatot írni és olvasni a hálózaton keresztül.
- VNC (Virtual Network Computing) – Egy távoli képernyős rendszer, amely a rendszer grafikus kezelői felületéhez való hozzáférést teszi lehetővé, nem csupán az adott gépen, hanem bárholnan az internetről, még hozzá különböző gépi környezetekben. Erre számos program képes – talán a VNC a legnépszerűbb, lévén ingyenes, és működik Windows, Linux és UNIX alatt egyaránt (<http://www.realvnc.com/>).
- **Billentyűlenyomás naplózók** – Az internetről százával töltethetők le az erre képes programok. Vannak hardver- és vannak szoftveralapúak. A billentyűlenyomás naplózók a számítógéphez csatlakozó billentyűzeten minden lenyomott billentyűt megjegyeznek, és némelyek e-levélben akár el is küldhetik a feljegyzett sorozatokat.

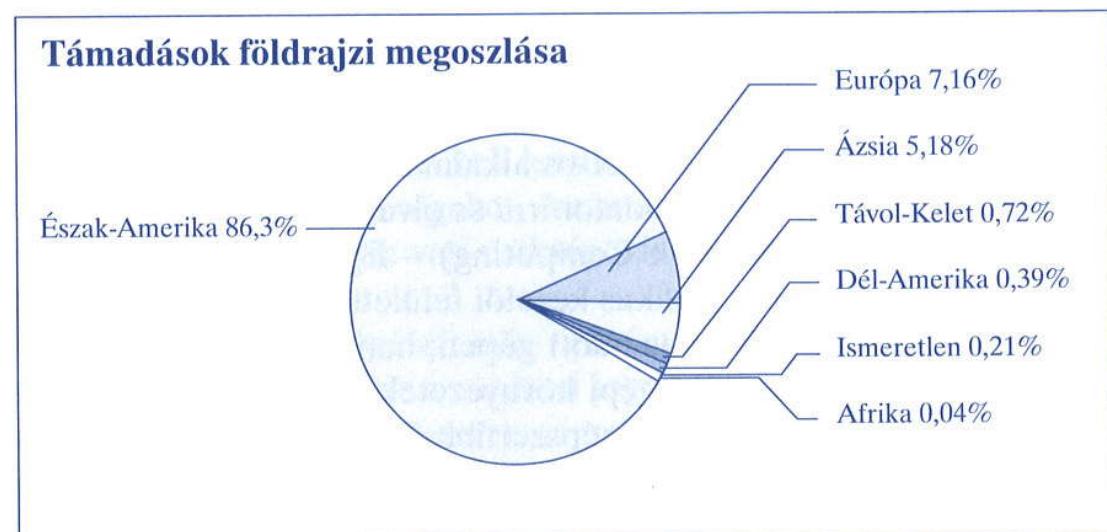
- **Testreszabott programok** – Ezeket el lehet helyezni a Windows indítókönyvtárában vagy a konfigurációs állományaiiban (`system.ini`, `win.ini`, `autoexec.bat`, `config.sys` stb.). UNIX-alapú rendszerek esetén a `/etc/rc.d` katalógusban lehetnek elhelyezve.

Előfordulhatnak olyan esetek is, amikor a támadó nem akar „művészbejárót” elhelyezni a rendszerben. Az ipari kémkedés során például a támadó a betörés után megszerzi a kívánt információt, majd távozik. Ilyenkor a támadó pontosan tudja, mit is akar, és egyáltalán nem akar később visszatérni a feltört rendszerbe. Az ilyen jellegű támadások során a támadó sokkal inkább arra törekszik, hogy teljesen elfedje a nyomait, hogy soha senki ne vegye észre a betörés tényét.

### Honnan jönnek a támadások?

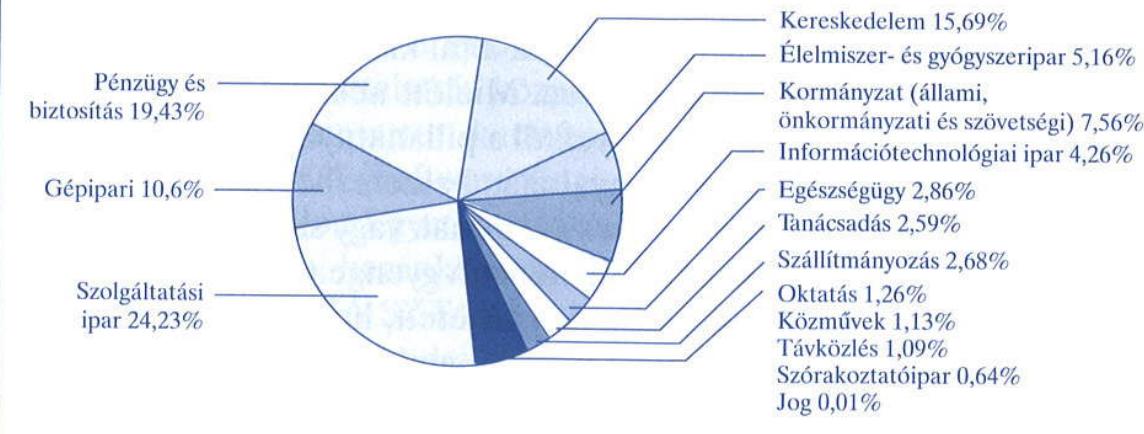
Mostanra már világossá kellett válnia, hogy a rossz fiúk kint lapulnak az interneten, és mindenféle eszközökkel támadnak minket – kezdve az automatikus letapogatásuktól egészen a kifejezetten célzott támadásokig. Mindenki tisztában van azzal, hogy az internethöz való csatlakozáshoz szükség van egy nyilvános IP-címre. A címek a világ adott tájaira vannak kiosztva, így nyilván képesek vagyunk arra is, hogy megvizsgálhassuk, pontosan honnan jönnek a támadások.

Ez valóban igaz, és az ISS biztonsági cég (<http://www.iss.net>), melynek van egy távfelügyelő biztonsági szolgáltatása (*Managed Security Services*) a 2003. április 1. és június 20. között feljegyzett 5052 biztonsági eseményt az 1.4. ábrán látható grafikonon ábrázolta. Ez azt mutatja be, hogy a világ mely részéről kezdeményezték őket.



1.4. ábra. 2003. április 1. és június 20. közötti támadások megoszlása a Földön  
(Forrás: Internet Security Systems, 2003)

### Megcélzott üzleti területek



1.5. ábra. Megtámadott üzleti területek eloszlása

(Forrás: Internet Security Systems)

A fenti felmérés további érdekessége az, hogy – mivel az ISS az ügyfelei részére végzi távfelügyeleti biztonsági szolgáltatását – pontosan tudható az is, hogy milyen üzleti szektorban tevékenykedő ügyfelek ellen irányultak a támadások. Ezt szemlélteti az ugyancsak általuk közzétett 1.5. ábra is.

Az üzleti tevékenységek szerinti megoszlás meglehetősen érdekes. Vélhetőleg mindenkit érdekel, hogy a biztosítási társaságok hogyan állapítják meg díjszabásukat, és mire alapozzák döntéseiket!

További érdekesség, hogy a támadások túlnyomó része az Egyesült Államokból indul ki. Ne feledjük el azonban azt a tényt sem, hogy az internet elterjedtsége is éppen ott a legnagyobb. Ezek a számok valamennyit egyébként is csalhatnak, hiszen számos támadó feltörhetett az USA-ban található gépeket, és másokat már ezek közvetítésével támadhat. Ez utóbbi állítás valószínűleg igaz, azonban semmilyen módon nem lehet megmondani, hogy az pontosan hány százalékot jelenthet. A hálózati üzletában a biztonság megteremtése bizony komoly kihívást jelent.

Ez a tény azonnal felveti a felelősség kérdését is – a **közvetítői felelősség** (*downstream liability*) fogalma világszerte mostanában kezd bekerülni a jogászok szótárába. Dióhéjban megfogalmazva, ha vállalatunk nem tesz meg a saját védelme érdekében bizonyos lépéseket, miáltal a mások ellen vérehajtott támadások közvetítőjévé válik, akkor bizony felelőssé tehető a támadásért.

A hálózati biztonság megteremtésében érintett valamennyi szereplőt aggodalommal töltheti el a felelősség ilyen kiterjesztése, s valószínűleg nincs már messze az a pillanat, amikor egy jogász bíróság elé visz egy ilyen ügyet. A hálózati biztonság témakörének bizony számos területe egyáltalán nincs jogi szempontból kidolgozva, de még felmérve sem, ez azonban hamarosan meg fog történni – ennyiben biztosan bízhatunk a jogászokban!

## 1.6. HÁLÓZATBIZTONSÁGI SZERVEZETEK

A következő részben a támadók által kihasználható sérülékeny pontokat vizsgáljuk meg részletesebben. Mielőtt nekilátnánk, érdemes megismerni azokat a helyeket, amelyektől a pillanatnyilag ismert sebezhetőségekre vonatkozó információk egyáltalán beszerezhetők.

Egy időben minden egyes gyártónak vagy szállítónak a saját felelőssége volt, hogy a termékét érintő minden gyenge ponttal kapcsolatos információt nyomon kövessen. Ez oda vezetett, hogy különböző cégek ugyanazt a sérülékeny pontot jelentették be, ami kisebb zűrzavarhoz vezetett. Más esetekben a cégek nem is szereztek tudomást a gyenge pontokról mindaddig, amíg nyilvánosságra nem hozta őket valaki más. A hálózatbiztonsági üzletág szereplői hamar észrevették, hogy ez a módszer nem túl hatékony, ezért létrehozták az elterjedt sérülékeny és gyenge pontok listáját, a CVE-t. Ez nem a gyenge pontok adatbázisa, hanem egy szótár. A honlapja (<http://www.cve.mitre.org>) a következőkben foglalja össze a szerepét:

A CVE (*common vulnerabilities and exposures*) a sérülékeny helyek és más biztonsági fenyegetettséggel kapcsolatos információk szabványos elnevezésgyűjteménye. Célja tehát a közismert gyenge pontok és biztonsági fenyegetettségek nevének szabványosítása.

A szótár fő célja az, hogy a különböző sérülékenységi adatbázisok és biztonsági eszközök közötti információáramlás könnyebb legyen. Jól lehet a szótár könnyebbé teheti a más adatbázisokban való információ visszakeresését, önmagában mégsem tekinthető sérülékenységi adatbázisnak.

Tartalma a CVE csapata önkéntes közös munkájának eredménye, amely csapatnak tagja számos, a biztonsági üzletágban érintett vállalat képviselője, mint például a biztonsági eszközök kibocsátói, felsőoktatási intézmények és kormányzatok, valamint a biztonsági terület más kiemelkedő szakértői. A MITRE vállalat tartja karban a szótárt és vezeti a csoport megbeszéléseit.

Fejlődésével párhuzamosan a CVE egyre nagyobb elismertségre tesz szert, ami remélhetőleg egyre fokozódni fog. Teljes kifejlődéséig azonban a hálózati biztonságban érintettek alapvető információforrásának a különböző adatbázisok és ellenőrző listák tekinthetők. Ezek a szervezetek számos cikket, e-levelezési csoportot, fórumot, figyelmeztető üzenetet, gyakorlati tanácsot és képzési lehetőséget kínálnak az érdeklődők számára a tudásuk növeléséhez.

## 1.6.1. CERT KOORDINÁCIÓS KÖZPONT

A CERT (<http://www.cert.org>) önmagát úgy határozza meg, mint az internetbiztonsági tapasztalatok központját. Helyileg az USA Szövetségi Kormánya által fenntartott kutatási és fejlesztési központnál, a Szoftvermérnöki Intézetnél (Software Engineering Institute) található, amelyet a Carnegie Mellon Egyetem működtet. A legtöbb országnak van saját CERT szervezete, hazánkban az ISZT, IHM, és HIF szervezetekkel együttműködve az MTA SZTAKI üzemelteti (<http://www.cert.hu>). Az itt található információk a rendszerünkben található potenciális problémák elleni védelemtől kezdve a jelenlegi problémákra való helyes cselekvéssel át egészzen a jövőben várható problémák megjósolásáig terjednek. A CERT tevékenységi köre felöleli a számítógépes biztonsággal kapcsolatos események és sebezhetőségek kezelését, a biztonsági figyelmeztetések közzétételét, a hálózati rendszerek nagyobb lélegzetű változásaival kapcsolatos kutatásokat, valamint az oktatási anyagok kifejlesztését is, segítve mindezzel a helyi biztonság növeléséért felelősök munkáját.

## 1.6.2. SANS

A SANS (*Sysadmin, Audit, Network, Security*) (<http://www.sans.org>) önmeghatározása szerint az információbiztonsággal kapcsolatos kutatások, képzések, és hitelesítések megbízható vezetője. A SANS Intézet kutatási és oktatási együttműködésként 1989-ben alakult. Lehetővé teszi, hogy százötvenhazezenél is több biztonsági szakember, ellenőr, rendszergazda és hálózatüzemeltető megoszthassa az általa tanultakat, és megoldásokat találhasson azokra a problémákra, amelyekkel éppen küzd. A SANS magját a világszerte megtalálható kormányzati ügynökségek, vállalatok és egyetemek számos tevékeny biztonsági szakembere alkotja, akik minden évben több száz órát fordítanak kutatásra és oktatásra, ezzel segítve az egész biztonsági közösséget. A SANS számos erőforrása, mint például a publikációk szemléje, kutatási összegzések, biztonsági figyelmeztetések és a díjnyertes cikkek ingyen rendelkezésére állnak bárkinek, aki ezt kéri. A nyomtatott publikációkból származó bevételek néhány egyetemi kutatási program finanszírozását teszik lehetővé. A SANS oktatási tevékenységeből származó bevételből pedig magát a képzési programot, valamint különleges biztonsági kutatásokat ösztönöznek.

### 1.6.3. INTERNETBIZTONSÁGI KÖZPONT (CIS)

A CIS (*Center for Internet Security*) (<http://www.cisecurity.com>) deklarált célja szerint a világ bármely pontján található vállalatok segítése az információs biztonsággal kapcsolatos kockázati tényezők hatékony kezelésében. Olyan módszereket és eszközöket kínál, amelyek növelik, mérik, figyelik és összehasonlítják az internetre kapcsolódó rendszerek és gépek biztonsági állapotát, beleértve az üzleti partnerekét is. A CIS nem kapcsolódik egyetlen kereskedelmi termékhez vagy szolgáltatáshoz sem. Az általa vezetett egyeztetési eljárás keretében a tagok azonosítják a legnagyobb veszélyt jelentő biztonsági fenyegetéseket, és részt vesznek olyan gyakorlati módszerek kifejlesztésében, amelyek ezt a kockázatot csökkentik. Ez az egyeztetési folyamat már most is működik, és működőképességét az internetes biztonsági mérések létrehozásával bizonyította, amelyeket széles körben testre szabtak és alkalmaztak mások.

### 1.6.4. SCORE

A Score (<http://www.sans.org/score/>) saját magát a SANS/GIAC és az Internetbiztonsági Központ (CIS) együttműködéseként definiálja. Ez a különböző háttérrel rendelkező és különböző területeken tevékenykedő biztonsági szakemberek közössége, akik a legalapvetőbb szabványok, valamint ajánlott módszerek gyűjteményének kialakításán fáradoznak. Túlajdonképpen ez a CIS kutatói tevékenységének motorja. Miután a szakemberek egyetértésre jutottak valamely kérdésben, és ellenőrizték az ajánlásra kerülő módszert, a CIS formálisan is kidolgozza azt alapvető szabvánként és ajánlott módszerként, amelyet ezután az ipar átvehet.

A Score céljai:

- Biztonsági ellenőrző listák reklámozása, kifejlesztése és publikálása.
- Ezen ellenőrző listák szakmai egyeztetések és a Score levelezési listáin történő nyílt párbeszédek segítségével történő összeállítása.
- Már létező hivatkozások felhasználása, GIAC-bizonyítvánnyal rendelkező szakemberek verbuválása és adott témakörök szakértőinek toborzása, amikor és ahol csak szükséges.

### 1.6.5. INTERNET VIHARKÖZPONT

Az Internet Viharközpont (*Internet Storm Center*) (<http://isc.sans.org>) önmagát napi több mint 3 millió behatolási kísérlet naplózóközpontjáért határozza meg. Egyre bővülő kutatásokkal igyekszik minél ham-

rabb felismerni a készülő új „viharokat”, elkülönítve azokat a helyeket, amelyeket a támadások során használnak, illetve hivatalos adatokat szolgáltatni azokkal a támadásokkal kapcsolatban, amelyek a világ különböző területein található régiók és iparágak ellen irányulnak. Az Internet Viharközpontról a hálózati közössége számára ingyenes szolgáltatás. A SANS Intézet a SANS biztonsági képzési programjaiban fizetett tandíjakból támogatja a munkáját.

### 1.6.6. ICAT METABASE

Az ICAT (<http://icat.nist.gov/icat.cfm>) a számítógépek sebezhető pontjait felsoroló kereshető adatbázisként határozza meg önmagát. Az adatok nagyon részletes szempontok alapján katalogizáltak, így visszakereshetőségük is jó. A felhasználókat hozzásegítik a sebezhető pontok megtalálásához, illetve azok biztonságossá tételehez.

### 1.6.7. SECURITY FOCUS

Évi 2,5 millió egyedi felhasználójával a Security Focus (jelentése: biztonsági gócpont) (<http://www.securityfocus.com>) a biztonsági szakértők legnagyobb közösségeit alkotja. Számos, a biztonsági iparágban komoly technikai vagy vezetői beosztást betöltő, magasan képzett biztonsági szakértő is tagja. A Security Focus állandóan elérhető nyilvános oldala kilenc területet, ha úgy tetszik, csatornát tartalmaz: **honlap** (*home*), **alapok** (*foundations*), **Microsoft**, **UNIX**, **IDS** (információvédelmi rendszerek), **események** (*incidents*), **vírus**, **íráspróbák** (*Pen-Test*) és **tűzfalak** (*firewalls*). Ezekben a csatornákon együttesen havonta több millió oldalnyi információ keletkezik. Az információt különböző jellemzők szerint tovább csoporthoz kötött (például sebezhetőség, InFocus cikkek, eszközök stb.). Ez a napi frissítésű honlap világszerte a biztonsági szakértők reggeli „újságának” szerepét tölti be.

### 1.6.8. MIT TANULHATUNK EZEKTŐL A SZERVEZETEKTŐL?

Ezen szervezetek egyike sem létezett öt évvel ezelőtt. Megszületésüket és megerősödésüket az interneten fellelhető legkülönbözőbb gépkalózok tevékenysége jelentette fenyegetés váltotta ki. Mindegyik fent említett honlapot érdemes átböngészni, mert számos olyan információra tehetünk hasznat.

tünk szert, amelyeket könyvünk nem, vagy nem annyira részletesen érint. A következő részben a sebezhető pontokon keresztül történő támadásokat tekintjük át.

Manapság a gyártók egyik nagyon hasznos szolgáltatása, hogy a felhasználók és az etikus támadók (*hacker*) számára lehetővé teszik a termékkel kapcsolatosan felfedett biztonsági problémák bejelentését, illetve azok megtekintését. Például a Cisco cég az alábbi weblapon teszi ezt lehetővé: [http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a00801d2d9d.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a00801d2d9d.shtml)

## 1.7. GYAKORI TÁMADÁSOK ÁTTEKINTÉSE

Ez a pont a támadók által leggyakrabban használt támadásokat tekinti át. A lista semmiképpen sem tekinthető teljesnek vagy kimerítőnek, hiszen naponta egyre ijesztőbb számban fedezhetők fel új támadási formák. Az itt fel nem sorolt támadási fajtákról, illetve a felsoroltakról bővebb információk találhatók az előző pontban megadott szervezetek honlapjain.

- **Szolgáltatásmegtagadás (DoS: Denial of Service)** – Szolgáltatásmegtagadási támadásról akkor beszélünk, ha a támadás a cél hibás állapotba vezérlésére irányul, miáltal mások számára megtagadja a szolgáltatás nyújtását. Ez a hibás állapot számos különböző módon elérhető, közülük csupán egy a cél: csatlakozási kísérletekkel való elárasztása.
- **Elosztott szolgáltatásmegtagadás (DDoS: Distributed Denial of Service)** – Azt a támadástípust hívjuk így, amikor számos különböző helyen található „bűnrészes” gépek segítségével egyidejűleg támadjuk a célt. Egy ilyen jellegű támadásról részletes ismertetés olvasható a <http://grc.com/dos/grcdos.htm> weblapon.
- **SYN-elárasztásos támadás** – Ez a fajta támadás akkor következik be, ha egy hálózat annyira túltelítődik a be nem fejezett kapcsolatteremtési kéréseket kezdeményező SYN-csomagokkal, hogy nem képes feldolgozni a valódi kapcsolatteremtési kéréseket (oka lehet a CPU, memória, vagy hálózati interfészkartya túlterhelése). Ez tulajdonképpen a DoS-támadás egy fajtája.
- **UDP-elárasztásos támadás** – Akárcsak a később ismertetett ICMP-elárasztásos támadás, UDP-elárasztásról akkor beszélünk, ha nagymennyiségű UDP-csomagot kifejezetten azért küldenek a megcélt zott hálózatba, hogy azok a rendszert a valódi kapcsolatok kiépítésének ellehetetlenüléséig lelassítsák. Például az 53-as portra érkező DNS-elárasztás iskolapéldája ennek a támadásfajtanak.
- **Portletapogatási támadás** – Portletapogatással akkor állunk szemben, ha különböző portokra egymás után az üzemelő szolgáltatások megtá-

lálásának szándékával küldenek csomagokat. A támadó ezt annak reményében teszi, hogy a valamelyen szolgáltatást kiszolgáló portra érkező csomagra választ fog kapni.

- **Halálra pingetés** – A TCP/IP-specifikáció meghatározza a távadat-(datagram) átvitel maximális csomagmérétét. Számos pingelő alkalmazás azonban lehetővé teszi azt is, hogy a felhasználó nagyobb csomagmérét írjon elő. A túlméretes ICMP-csomagokra a rendszer többféle ártalmas módon reagálhat. Előfordulhat szolgáltatásmegtagadás, összeomlás, lefagyás és újraindulás egyaránt.
- **IP-hamisítás (IP spoofing)** – Ilyen típusú támadásról van szó akkor, ha a támadó a tűzfal biztonsági beállításait hamisítással (érvényes kliens IP-címének, e-levélcímének, vagy felhasználói azonosítójának megadásával) akarja megkerülni. Ez a módszer különösen akkor vállhat fontossá, ha a támadó a különböző számítógépek közötti bizalmi viszonyokat (*trust relationship*) akarja kihasználni. A rendszergazdák ugyanis gyakran kiépítenek ilyen bizalmi viszonyokat, hiszen ennek egyik előnye például a felhasználók csupán egyszeri bejelentkezési kötelezettsége.
- „**Land**” támadás – A SYN elárasztásos támadás és az IP-csalás együttes alkalmazása. Akkor következik be, ha a támadó egy olyan mehamisított IP-csomagot küld a célnak, amely feladóként és célként egyaránt a cél IP-címét tartalmazza. A megtámadott rendszer erre azzal válaszol, hogy önmagának küld egy SYN-ACK csomagot, létrehozva ezzel egy olyan üres kapcsolatot, amely az üresjárat időtúllépés bekövetkeztéig fennmarad. A rendszer ilyen üres kapcsolatokkal való elárasztása túlterheli azt, s így bekövetkezik a szolgáltatás megtagadása.
- „**Teardrop**” támadás – Ez a támadásfajta a részekre tördelt IP-csomagok újra összeállításával kapcsolatos sérülékenységet használja ki. Az IP-fejléc egyik mezője az eltolási cím (*offset*). Ha az egyik részcsomag eltolási címe és a hossza eltér a másik részcsomagétől, akkor a csomagok átlapolása következne be, amire a teljes csomagot összeállítani próbáló gép összeomlással válaszolhat.
- **Pingelő letapogatás** – A portletapogatási támadáshoz hasonlóan a pingelő letapogatás akkor következik be, ha a támadó ICMP válaszkérő (*echo request*) csomagokat (vagyis „ping” csomagokat) küld különböző címekre annak reményében, hogy valamelyik majd csak válaszol – így próbálva felfedni a megcélzott címtartományban a lehetséges célok IP-címeit.
- **Java/ActiveX/Zip/Exe támadás** – Rosszindulatú Java- vagy ActiveX-komponensek rejthetők el a weblapokon. Amikor ezeket letölti valaki, ezek a betöltődő kódok trójai falovat installálhatnak a számítógépén. Ugyanilyen trójai programok rejthetők el a zip, gzip, tar és a végrehajtható (exe, com) állományokban is.

- **WinNuke támadás** – WinNuke egy gépkalóz program, amelynek kifejezetten célja a hálózatról elérhető, Windows operációs rendszer alatt üzemelő gép összeomlása. A program – általában a NetBIOS 139-es portra – egy olyan kötőgen kívüli (*out of band*) adatot küld a kapcsolat kiépítése után a célgépre, amely NetBIOS-részüzenet átlapolását, s ezzel számos gép összeomlását okozza. Ez a támadásfajta egy újabb okkal szolgálhat arra, miért nem célszerű a NetBIOS-üzenetek kívülről a helyi hálózatba való bejutását, vagy éppen az onnan történő kijutását engedélyezni.
- **Törpike (*smurf*)** – A kis hupikék törpikék nevét nem éppen felvidításunk miatt kapta ez a fajta támadás, amely tulajdonképpen a támadó gép által egy közvetítő segítségével történő ping (ICMP) támadást jelent. A tényleges támadó így rejte maradhat. Erről a támadásfajtról többet is meg tudhatunk a <http://www.cert.org/advisories/CA-1998-01.html> weblapon.
- **Nyers erővel támadás (*brute force*)** – A támadó célja a jelszavak olyan technikával való feltörése, mint például egy szótárban szereplő lehetséges jelszavak egymás utáni megadásával megkísérelt ismételt bejelentkezések.
- **Forrásirányítás (*source routing*)** – Az IP-fejléc egyik mezője meghatározhatja, hogy a csomag miként legyen irányítva. Számos túzfalon a szabályok megkerülhetők az ilyen módon beállított IP-csomagokkal, illetéktelen hozzáférést engedve így a védett hálózathoz. Az IP-fejlében például megadható egy olyan útválasztási információ, amely a fejléc forrásától eltérő IP-forráscímet ad meg. Ez azt okozhatja, hogy a csomagok más irányba továbbítódhatnak. Kövessük le az ICMP-csomagok útválasztásának vezérlésére szolgáló különböző lehetőségeket:
  - **Útvonal feljegyzése** – A támadó olyan IP-csomagot küld, amelyben az irányítási opció az útvonal feljegyzése. Ezt arra használjuk, hogy a csomag útját végig lehessen követni. A feljegyzett útvonalat a kívülálló tanulmányozhatja, miáltal megismerheti a hálózat címzési sémáját és topológiáját.
  - **Laza forrásútvonal** – A támadó által küldött csomag ezen irányítási opciója a csomag cél felé továbbítását végző útválasztónak adhat javaslatokat. Azért nevezzük laza útvonalnak, mert a továbbító eszköz az útvonal következő állomásának eléréséhez akárhány közbeeső útválasztót is felhasználhat.
  - **Szigorú forrásútvonal** – A támadó által küldött csomag ezen opciója lehetővé teszi a csomag forrásának, hogy a cél felé vezető útvonal pontos leírását adja. Azért nevezzük szigorú útvonalnak, mert a továbbító eszköz kizárolag közvetlenül a forrás által megadott következő címre továbbíthatja a csomagot, méghozzá kizárolag a következő cél által jelölt közvetlenül csatlakozó hálózaton keresztül.
  - **ICMP-elárasztás** – Ez a támadásfajta akkor következik be, ha az ICMP-pingetések nagy száma annyira túlterheli a célrendszert, hogy

- az minden erőforrását a válaszadásra fordítja, s így nem képes a valódi hálózati forgalmat feldolgozni. Különböző típusú ICMP-üzenetek léteznek, melyek mindegyikének megvan a maga sajátos célja (lásd RFC 792), a támadó azonban bármelyiküket felhasználhatja.
- **ICMP-válaszküldés (echo reply)** – A pingre adott válasz. Számos tűzfal átengedi a válaszokat, hogy lehetővé tegye a védett tartománybeli felhasználók számára a külső erőforrások elérhetőségének ellenőrzését, így az ilyen típusú csomagok gyakran alkalmasak az elárasztásos támadásra.
  - **ICMP-gép nem elérhető (host unreachable)** – Az eszköz ezzel a hibaüzenettel jelzi, hogy a küldött csomag nem érte el a megjelölt célt.
  - **ICMP-lefojtócsomag (source quench)** – Az internetes forgalom torlódását jelző üzenet. A támadó megkísérelheti ilyen csomagok küldésével rábírni a megcélzott gépet az adatátvitel lelassítására.
  - **ICMP-átirányítás (redirect)** – A forgalom átirányítását javasló üzenet (mondjuk az X hálózat forgalmát közvetlenül a G2 átjáróra, mert az rövidebb útvonal lenne a cél felé). A támadó így próbálhatja meg átirni az alapértelmezett útválasztónkat, például a **beékelődéses támadás (man in the middle)** során, hogy az útválasztó minden kifelé irányuló forgalmat az ő gépen keresztül küldjön el.
  - **ICMP-válaszkérés (echo request)** – Ez a gyakran használt ping kérés. Beérkezése jele lehet egy ellenséges letapogatási kísérletnek, de a normál hálózati működés részeként is kaphatunk ilyen csomagokat.
  - **ICMP-távadat időtúllépése (time exceeded for a datagram)** – Ezzel az üzenettel jelzik, hogy a csomag valahol időtúllépés miatt megsemmisült (rendszerint hurokba került), soha el nem érve a célját.<sup>6</sup>
  - **ICMP-távadat paraméterhibája (parameter problem on datagram)** – Az üzenet azt jelzi, hogy valami szokatlan jelenség következett be. Ez valószínűleg egy éppen folyó támadás jele.
  - **Túlméretes ICMP-csomag (large ICMP packet)** – Az 1024 bájtnál hosszabb ICMP-csomagok számos eszköz számára problémát jelentenek, mivel valós forgalom esetén soha nem érik el ezt a méretet.
  - **Csomag lehallgatása** – A lehallgatás (*sniffing*) a passzív támadás során használható módszer, egy hálózati interfészkartya különleges „szűrő” (*promiscuous*) módba állításával. Ne becsüljük le a veszélyt csak azért, mert ez csupán passzív támadás. Valójában ha a támadónak sikerül egy lehallgatót (*sniffer*) elhelyeznie a belső hálózatunkban, akkor a biztonságunk már ismét veszélyesen sértült, hiszen a támadó a hálózatunk forgalmát alkotó csomagok szinte mindegyikét láthatja vele – ez pedig kifejezetten fenyegető lehetőség.

<sup>6</sup> A traceroute program is ilyen csomagok segítségével követi az átviteli utat. (A lektor meg.)

Ez csupán egy rövid ízelítő a ma ismert több ezer különböző sérülékenységből. Képzeljünk el egy összehangolt támadást, amely akár csak ezek közül is egyszerre több módszert felvonultat. Mindjárt más színben látjuk a hálózati biztonság témakörét, ugye?

## 1.8. ÖSSZEFoglalás

A fejezetben megvizsgáltuk azokat a lehetőségeket, amelyekkel a támadó kiválasztja a célját, nevezetesen az alkalom szülte és a célzott támadást. Sikerült bizonyítani, hogy bárki célponttól válthat, s a valódi vízválasztó csak az lehet, hogy a támadó pusztán kényelmesen besétál a védtelen célba, vagy mélyebb és sokkal rosszindulatúbb szándék húzódik meg a hátterben.

Miután a támadó kiválasztott minket célpontjaként, hat elterjedt lépést hajt végre. Ezek együtt alkotják azt a támadást, amelynek célja végső soron a rendszer feltörése.

A fejezetben röviden ismertettük azokat az állandóan elérhető helyeket, ahol a hálózatbiztonsággal kapcsolatos ismereteinket mélyíthetjük el. Ezek a helyek a „jó emberek”, amelyeket azért is célszerű ismertetni, mert az interneten a legtöbb hely a „gonoszok birodalma”; mindig óvatosan közelítsük meg ez utóbbi webhelyeket! A fejezet befejezéseként a lehetséges támadási módszerek közül ismertünk meg néhányat. A következő fejezetben a hálózatbiztonság témakörének megismerése felé vezető út első állomását vesszük szemügyre – a biztonsági házirendeket, amelyek a védelem kialakítása felé vezető út első lépését alkotják.

## 1.9. Összefoglaló kérdések

Az összefoglaló kérdések segítségével a fejezetben tárgyalt alapvető elvek és fogalmak megértése ellenőrizhető. A kérdésekre adott válaszok helyessége az A) függelékben ellenőrizhető.

1. Mi az alkalom szülte cél?
2. Mi a kiválasztott célpont?
3. Mi a nyomkeresés célja?
4. Mely módszerekkel nyerhet bebocsátást egy rendszerbe a támadó a következők közül?
  - a) Operációs rendszer támadása.
  - b) Alkalmazások támadása.
  - c) Hibás konfigurációk támadása.

- d) Szkripttámadások.
  - e) A fentiek mindegyike.
5. Soroljon fel négy hálózatbiztonsági szervezetet!
  6. Röviden ismertesse, miért fontos a támadó számára a nyomainak el-fedése.
  7. A pszichomérnöki tevékenység akkor is káros lehet, ha a nyilvánvaló támadás soha nem következne be. Mondja el, miért igaz ez az állítás!
  8. Milyen jellegű információkat találhatna a támadó, ha az Ön munkahelyén kezdene el kukabúvárkodni?
  9. Milyen típusú felderítés során használhatók a Whois adatbázisból nyerhető DNS-információk?
  10. Melyik két ingyenes felderítő eszköz található meg a legtöbb Windows operációs rendszerben, alapértelmezés szerint?