

A gépek meghódították a világot. Lehet a kijelentésben kételkedni, de az igazság az, hogy meghódították a világot, és mi csupán a működésükhez szükséges energiát szolgáltatjuk. Létezésünk valamiféle energiaforrásra egyszerűsödött. (Eléggé abszurd vagyok?)

Ez most úgy hangzik, mint valami rémálom, esetleg mint a legújabb sci-fi film reklámszövege? Nos, néhány pillanatra azért mégis vegyük fontolóra, hátha az igazat mondjam. Képes lenne Ön feladni a napi 24 órányi kábeltévet, az elektronikus híreket, a videojátékokat? Döntse el, akarja-e hallani az igazságot. Képes vele megbirkózni? Vagy képtelen?

Felébredés után azonnal egy üveggubóban találja magát, amelyik bűzös folyadékkal van tele, és mindenféle szondákkal van teletűzelve a gerince és az agya. Válhat ez a történet még rosszabbá?

Igen, tud, és válik is. Elkezdi kihúzogatni a tüket, egyiket a másik után. Még mielőtt teljesen felismerné, hogy hol is van tulajdonképpen, horrofiztikus géppókok rohanják meg, lefogják, és újra elkábítják.

Most kapcsoljuk fel a lámpát, és gondoljuk végig, hogy mi köze van ennek a történetnek a behatolásérzékeléshez és a mézesbödönhöz (ha van egyáltalán).

Jóllehet a történetet egy sci-fi filmből kölcsönöztük, mégis jól példázza a **behatolásérzékelő rendszerek (IDS – Intrusion Detection System)** működését. Az IDS működésének ugyanis három alapelve van:

- Hol kell figyelni?
- Mit kell figyelni?
- Mit kell tenni?

Az első alapelv, a „hol kell figyelni”, azt mondja meg, hogy az IDS-nek melyik logikai helyen kell észrevennie, ha valami történne. A fenti történetben a „hol kell figyelni” volt az üveggubóba zárt ember. A gonosz gépbirodalom a géppókokat arra utasította, hogy az embert figyeljék, és ne engedjék felkelni.

A második alapelv, a „mit kell figyelni”, azt mondja meg, hogy az IDS-nek pontosan mit kell észlelnie ahhoz, hogy riasztást vagy más akciót kezdeményezzen. Történetünkben a géppókoknak azt kellett észrevenniük, ha az ember felébred, és elkezdi kihúzogatni a tüket.

A harmadik alapelv, a „mit kell tenni”, azt az akciót jelenti, amelyet az IDS-nek végre kell hajtania akkor, ha a helyzet bizonyos paramétereknek felelne meg. A géppókoknak például újra el kellett altatniuk az embert, ha történetesen felébredt volna.

Most tegyük félre a sci-fi történetet, és vizsgáljuk meg egy valós IDS-rendszer működését:

1. Beüzemelünk egy IDS-t, amellyel az internetkapcsolatunkat figyeljük, hogy észlelhessük vele azokat, akik át akarnak hatolni a tűzfalon.
2. Beállítjuk az IDS-t, hogy milyen támadásokat és eseményeket figyeljen. A gyakorlatban azt mondjuk meg az IDS-nek, hogy milyen változás várható a rendszerben az egyes támadástípusok hatására.
3. Utasítjuk az IDS-t, hogy azonnal küldjön nekünk riasztást, ha a figyelt támadások bármelyike megkezdődne. Ezzel megtörtént a rendszer beüzemelése. Egy darabig nem történik semmi, majd folytatódik a történet:
4. Egy támadó „bekopogtat az ajtónkon” egy végpont-letapogatással, amely végigmegy az első 1000 porton.
5. Az IDS észleli a végpontokra való sorozatos csatlakozási kísérletet, ellenőrzi az adatbázisát, és azt olvassa ki belőle, hogy ez a tevékenység magán viseli az általunk beállított végpont-letapogatásra jellemző valamennyi bélyegét.
6. Megpróbál riasztást küldeni minden e-levélben, minden SMS-ben.
7. Hirtelen a végpont-letapogatás intenzitása erősödik, egyidejűleg egy újabb forrás belépésével.
8. Az IDS újabb riasztást küld erről az eseményről is.

Van tehát egy jól beállított behatolásérzékelő rendszerünk, ez 24 órán keresztül csak üldögél, és figyeli a hálózatunkat, minden pillanatban kézen állva a riasztásra, a támadás legelső jelének észlelésekor.

Eddig nagyon jól hangzik, ugye? Észrevette azonban, hogy mi a legfőbb probléma ezzel a módszerrel?

Mindenekelőtt a behatolásérzékelő csak a vele azonos hálózaton haladó forgalmat látja. Ennél nagyobb baj azonban, hogy csupán arra tud figyelni, amit előre beállítottunk. Ha nem állítottuk be, hogy észlelje a „duplán csavart támadás” jeleit, akkor nem fogja észlelni az ilyen támadás bekövetkezését sem. Végezetül az IDS akár szövetségesévé is válhat a támadónak. Lehetetlen? Nos, hányszor fordult elő önnel, hogy az éjszaka közepén kirohant megnézni az autóját, mert annak beindult a gyárilag beépített riasztója? Ugyanez a „kiálts farkast” szituáció az IDS esetén is előfordulhat. Ha a postaládája egyre jobban megtelik különböző riasztásokkal, előbb-utóbb elkezdi figyelmen kívül hagyni azokat, amelyeket „hamis riasztásnak” tart. Ez oda vezethet, hogy figyelmen kívül hagyja majd azt is, amelyik tényleg támadást jelez.

Az IDS telepítésének és beállításának titka a finomhangolás. Előbb össze kell rakni egy laborban, figyelni, hogy milyen normál forgalom okoz riasztást, majd csökkenteni kell az érzékenységét ezeken a helyeken. Ellen kell állni továbbá a késztetésnek, hogy minden eseményt azonnal jelentsen. A legtöbben minden apróságról értesülni akarnak, pedig erre semmi szükség sincs. Az IDS nem lehet tökéletes, és időről időre hamis riasztást fog küldeni. A továbbiakban egy valós példán keresztül vizsgáljuk meg az alapelveket.

## 9.1. A BEHATOLÁS ÉRZÉKELÉSE

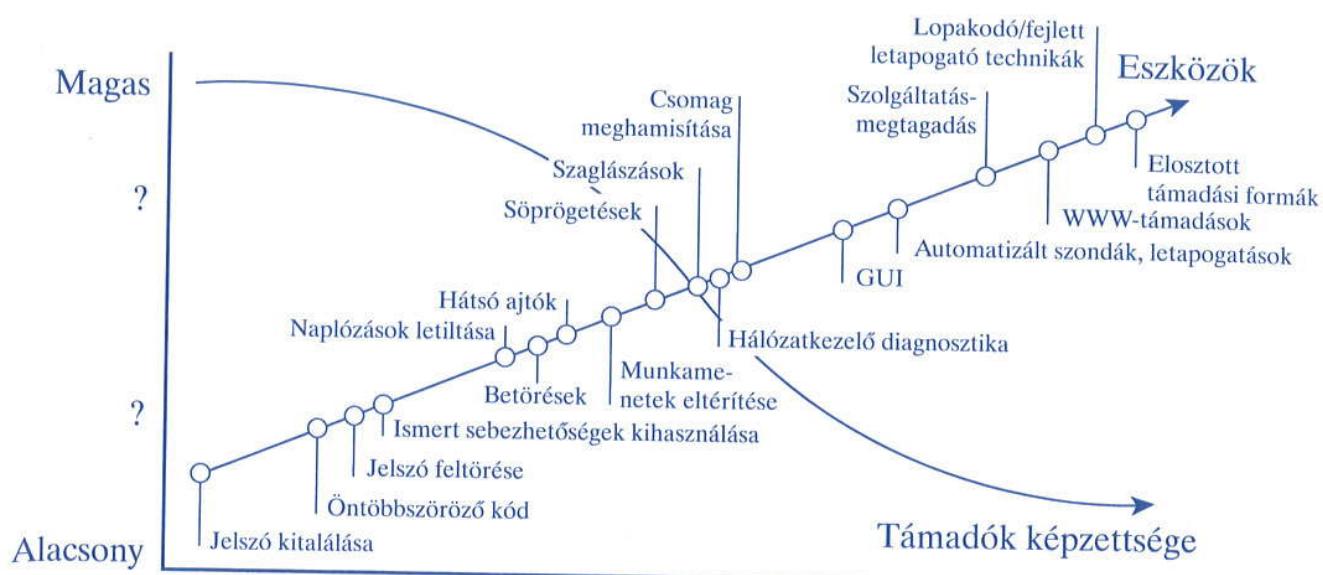
A különböző méretű hálózatokat eredetileg azért hozták létre, hogy lehetővé tegyék az információ megosztását, a biztonság azonban csak ritkán szerepelt a tervezési elvek között. Számos vállalat használja az IP alapú hálózatot, például az internetet arra, hogy a távoli munkahelyeket, utazó munkatársakat és az üzleti partnerek egy részét a saját belső, megbízható hálózatába integrálja. Az internet folyamatosan növekszik, és egyre több és több helyet kapcsol össze. Amint egyre megbízhatóbbá válik, a különböző cégek is átértelmezik, hogyan működtessék üzleti kapcsolataikat. Ennek legnyilvánvalóbb példája az, ahogy a HTML teret hódít. Ez a jelenség lehetővé teszi a vállalkozások számára, hogy egyre jobban működhessenek együtt a vásárlóikkal, hogy egyre akadálytalanabb legyen a működésük, csökkenthessék a költségeket, és megnövelhessék a bevételt, azonban mindennek ára és némi kockázata is van.

Az internet nyíltsága és gazdag tartalma, amely ennyire hatékony üzleti eszközzé teszi, egyben félelmetes tehertétel is. Egyszerűen megfogalmazva, az internetet arra terveztek, hogy összekössön és közössé tegyen, nem pedig hogy biztonságot nyújtson és védjen. A távoli helyeket, mozgó felhasználókat, vásárlókat és üzleti partnereket a megbízható belső hálózatba invitáló webhelyek és portálok a támadókat is hasonló barátságosan fogadják, akik saját személyes hasznuk érdekében kívánják a hálózati erőforrásokat kihasználni. Amint arról a 8. fejezetben már volt szó, a vezeték nélküli hálózati megoldások használatának növekedése csak tovább fokozza ezt a problémát.

A kérdés tehát adott: miként lehet ezt a kiemelkedően kényes, idegen kifejezéssel *mission-critical* kommunikációt megvédeni egy olyan eredendően nem biztonságos közegben, mint az internet? A könyv ezen erőforrások biztonságát megnövelő megoldásokat, a rétegezett védelem kiépítésének módozatait igyekszik bemutatni. A hálózat legalapvetőbb védelmi rétegei a csomagvizsgálatot is végző permi útválasztó, és a mögötte elhelyezett állapotteljes tűzfal. A vállalkozásoknak azonban vannak olyan szerverei, mondjuk a webszerver és a levelezőszerver, melyek működése eredendően megköveteli az internetről való elérhetőségüket. Nem blokkolhatjuk le egyszerűen a felük irányuló forgalmat, mert akkor alapvető céljukat sem képesek megvalósítani, márpedig a vállalkozás sikérében jelentős szerepet játszik a zavartalan működésük. Az is ismert tény, hogy az internet növekedésével párhuzamosan a támadások is egyre kifinomultabbak lettek, miközben a végrehajtásukhoz szükséges szakértelem egyre csökkent, amint az a 9.1. ábrán is jól látható.

Sem az útválasztó, sem a tűzfal nem képes megmondani, hogy egy adott www-csomag egy támadás része-e, vagy egy vásárlótól érkező legális kérés. Sajnálatos módon túlságosan is sokan bízták saját biztonságukat

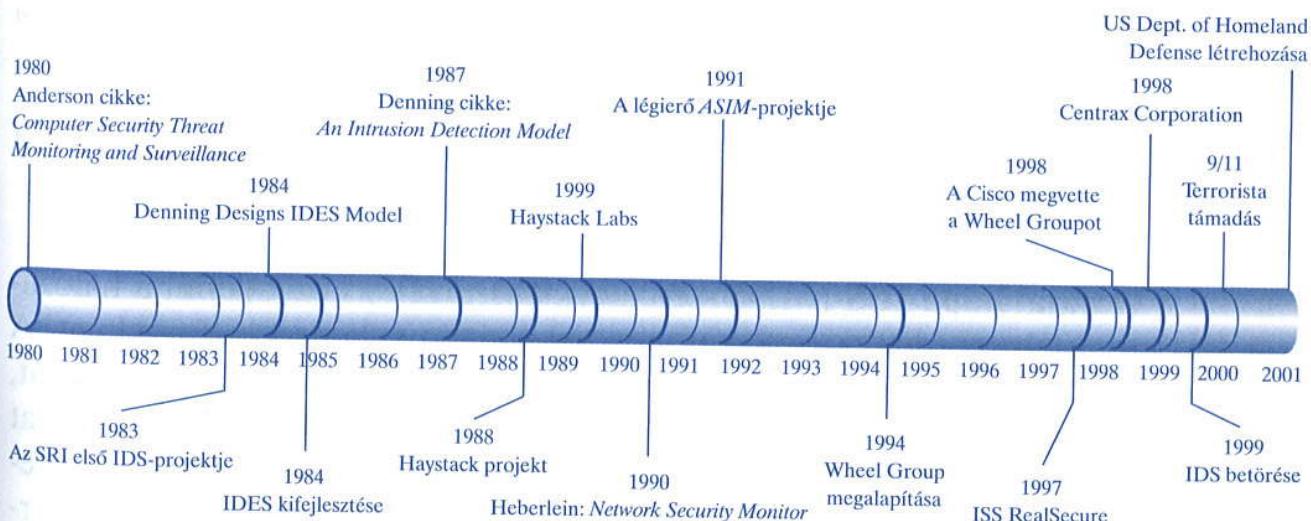
# HÁLÓZATI BIZTONSÁG



9.1. ábra. A támadások kifinomultsága és a szükséges szakértelem

erre a két eszközre, amelyek érzékelési képességei azonban egyre szűkülnek. Lehetséges persze, hogy a vállalatnál van egy kiváló képességű rendszergazda, aki megbízhatóan képes „lezárnai és biztonságba helyezni” ezeket a kényes szervereket, illetve alkalmas az átfogó biztonsági házirend és eljárásrend kidolgozására. Az eddig tárgyalt biztonsági eljárások és módszerek között azonban egyetlen egy sem szerepelt, amely a *támadások vagy betörési kísérletek* észlelésének szükségességét tárgyalta volna!

Az internet szempontjából a behatolásérzékelés viszonylag új fogalom, a kutatások a nyolcvanas években kezdődtek, Anderson és Denning publikációival. Az Egyesült Államok kormányzata ekkor kezdte el az internet elődjén, az ARPA-NET-en alkalmazni az IDS alapvető elveit. A nyolcva-



9.2. ábra. IDS-fejlesztések története

nas évek végén a Haystack-projekt tagjai megalkották a Haystack Labs formációt, amely a gépalapú behatolásérzékelő rendszerek kereskedelmi célú kifejlesztését tűzte ki céljául. A hálózatalapú behatolásérzékelő rendszerek fejlesztése csak a kilencvenes években kezdődött meg, Todd Heberlein vezetésével. Azóta számos cég fejleszti az IDS-eszközöket, amint azt a 9.2. ábra is jelzi.



A 9.2. ábráról annyit érdemes észrevenni, hogy az amerikai légierő ASIM nevű rendszerét kifejlesztő csapat alakította meg 1994-ben a Wheel Group nevű céget, amelyet a Cisco 1998-ban végül megvásárolt, majd ez képezte a Cisco IDS terén végzett fejlesztéseinek magját.

Legyen a támadó motivációja az intellektuális kihívás, kémkedés, politikai, gazdasági vagy csak egyszerűen a zavarkeltés, a hálózatnak mindenkiéppen szembe kell néznie a támadás tényével. Nem csupán a józan ész követeli meg ezen támadások megfigyelését, de sok esetben ez üzleti kényszerűség is. A kilencvenes évek elején új termékek kezdték feltünnedezni a hálózati biztonság

piacán: a behatolásérzékelő rendszerek (IDS). Az IDS a hálózat riasztórendszer. A hálózat ugyan védet, de az IDS (a riasztó) nélkül soha nem vennénk észre, hogy egy támadó megpróbált behatolni. A behatolásérzékelő célja az, hogy a hálózaton megfigyelje a szokásostól eltérő eseményeket, a meg nem engedett tevékenységeket, a valószínű támadásokat, és megakadályozza ezek kiteljesedését és sikereit, valamint lehetőleg a támadó elítéléséhez szükséges információkat szolgáltasson.

Az IDS a hálózaton belül számos helyen elhelyezhető, hogy minél jobb legyen a hálózat biztonsága és védelme. Napjainkban az IDS két formája ismert: hálózatalapú és gépalapú. Az érzékelők mindenkor fajtája más technikák segítségével észleli és késlelteti a rosszindulatú tevékenységeket. A lehető leghatékonyabb mélységi védelem kiépítése érdekében a kettő akár egyszerre is telepíthető:

- **Hálózatalapú IDS (NIDS – Network-based IDS)** közvetlenül a hálózaton helyezkedik el, és figyeli az azon haladó valamennyi forgalmat. A NIDS egyaránt hatékonyan figyeli a kifelé és befelé irányuló forgalmat, valamint a belső gépek és helyi hálózati szolgálok közötti forgalmat is. Jellemzően a túzfalakon és VPN-átjárókon kívül és belül vannak telepítve, mérik ezek hatékonyságát, és együttműködnek velük annak érdekében, hogy a hálózat védelme a lehető legjobb legyen.
- **Gépalapú IDS (HIDS – Host-based IDS)** egy különleges szoftveralkalmazás, amely a gépen (jellemzően a szerveren) van installálva, és ennek

a gépnek a kifelé és befelé irányuló forgalmát figyeli, valamint állandóan monitorozza a gépen lévő állományrendszer változásait is. Különösen hasznosnak bizonyulnak a kényes (mission-critical), internetről is elérhető szerverek, például levelező- vagy webszerverek esetén a gép védelmére.

A NIDS és a HIDS együtt is telepíthető, így megvalósítva a ténylegesen többrétegű védelmet, megfigyelve és ellenőrizve a szervezet minden kommunikációját. Az IDS a beépített különböző védelmi rendszerek hatékonyságának ellenőrzésében, vagy akár finombeállításukban is nagy szerepet játszhat, így biztosítva a biztonságra elköltött összegek tényleges megtérülését. A következő pontban az IDS általános jellemzőivel ismerkedhetünk meg.

### 9.1.1. Az IDS MŰKÖDÉSE

A piacon manapság kapható IDS-eszközök számos képességgel és lehetőséggel rendelkeznek. Amikor szervezetünk számára igyekszünk kiválasztani a legmegfelelőbbet, a következő képességekre célszerű összponosítani figyelmünket:

- Események összefüggése** – Amikor az IDS egy forgalmas hálózatban kerül telepítésre, a hálózat biztonságának szempontjából alapvető fontosságú az a képessége, hogy mennyire képes különböző eseményeket összekapcsolni. Tegyük fel, hogy egy támadás több szegmensben is történhet egyszerre egy feltört gép miatt, amelyet ezután további gépek feltörésére használnak. Az események összefüggéseinek megfelelő feltárása nélkül egy ilyen támadás nagy zavart okozhat, és az okok kiderítésével kapcsolatos erőfeszítések során sok munkaórát és más erőforrást elpazarolhatunk. Az események összefüggésének feltárása segíti az IDS kezelőjét a különböző alhálózatokban telepített szenzorokon bekövetkező történések gyors lekövetésében, történjenek ezek akár időben elnyújtva vagy különböző földrajzi helyeken.
- Központi érzékelő kezelése** – Az események összefüggésének felismerési képessége nagyon fontos, de nem kevésbé fontos a teljes IDS központi kezelhetősége sem. A való életben minden eszköz (szerver, útválasztó, tűzfal) készít naplókat; ezeket a naplókat azonban ritkán ellenőrzik, még ritkábban tanulmányozzák behatóan. A sikeres szempontjából alapvető fontosságú, hogy legyen egy központi kezelői platform, amelyik lehetővé teszi a több szenzoron bekövetkező események összefüggéseinek felismerését és a válaszok központi kezelését, valamint a hálózat biztonságáról készített részletes jelentések elkészítését.

- **Beállítható mintaadatbázis és küszöbértékek** – A vállalati vagy üzleti alkalmazások, szoftverfrissítések, új operációs rendszerek rendszeresen tartalmaznak hibákat, és a vírusok, illetve a támadók állandóan keresik ezeket a sebezhető pontokat. Mindig van valamennyi késleltetés egy sebezhetőség felismerése, és az IDS-fejlesztők által az ehhez kiadott frissített mintaadatbázis bejegyzések megjelenése között. Az IDS ezért tegye lehetővé az adminisztrátorok számára azt, hogy maguk is új mintabejegyzésekkel állíthassanak be.
- **A hamis riasztások kiküszöbölése** – minden operációs rendszer (például a Windows) az összes lehetőség engedélyezésével kerül kibocsátásra, ugyanígy az IDS-ben is alaphelyzetben minden be van kapcsolva. Ez azt jelenti, hogy alapértelmezett telepítésük után túlságosan érzékenyek lesznek, és rengeteg hamis riasztást fognak küldözgetni. Ez egyrészt elbizonytalanítja a kezelőt a hálózat biztonságával szemben, másrészről nehezebbé teszi számára a tényleges támadás felismerését. Éppen ezért minden behatolásérzékelő rendszernek rendelkeznie kell a hamis riasztások kiküszöbölésének lehetőségével. Mindazonáltal óvatosan kell bálni ezzel az opcionális funkcióval – csak olyan riasztásokat kapcsolunk ki, amelyek hamis voltában biztosak vagyunk, és kikapcsolása előtt még ekkor is várunk 24 órát.
- **Szabványalapú implementáció** – Bármely technológia telepítési döntéseknek meghozatala során fontos szempont a szabványoknak való megfelelősége. Számos gyártó készít olyan termékeket, amelyek remek biztonsági szolgáltatásokat adnak, de ezek közül csak kevés képes együttműködni, vagy a későbbi biztonsági rendszerek telepítésének keretét adni. Az IDS sem kivétel e szabály alól, ráadásul jelenleg még csak néhány szabvány létezik vele kapcsolatban. Mivel az IDS integrálásának és kezelésének legfontosabb szempontja a jelentéskészítési képessége, így az egyik szabvány az elterjedt sebezhetőségek és gyenge pontok (*CVE – Common Vulnerabilities and Exposures*) adatbázisa, amely a sebezhetőségeket egy könnyen kezelhető hivatkozási rendszer szerint minősíti és csoportosítja. A CVE-kompatibilitás nagyon fontos szempont az IDS kiválasztásánál, mivel olyan jelentéskészítési lehetőségeket nyújt, amelyek messze meghaladják az ilyen rendszerekben szokásos mértéket. A CVE-kompatibilis IDS integrálásával a vállalatnak lehetősége nyílik más CVE-kompatibilis, mint például a sebezhetőségekről (*VA – Vulnerability Assessment*) eszközök telepítésére, ezzel is növelve az eseményekről készített jelentések pontosságát. A CVE jelenleg széles körben alkalmazott technika, amely egyre inkább a hálózati biztonsági események minősítő és jelentéskészítő szabványává válik (<http://cve.mitre.org/cve>).
- **Behatolásmegelőző képességek** – A behatolásmegelőzési képesség alapjában véve a nem kívánt forgalomra és a támadási kísérletre való

aktív beavatkozási képesség. A „behatolásmegelőzés” kifejezés újabban némi zavart keltett, amely sok hirdetésben úgy jelenik meg, mintha a behatolásérzékelésnek lenne alternatívája. Valójában csupán a piaci behatolásérzékelő rendszerek egyik, ma már kötelezően meglévő képességéről van szó: a valószínűsített támadás elleni fellépés képességeiről.

- **Nyomok összehasonlítása** – A hálózaton áthaladó minden forgalmat figyel, és minden csomagot, vagy csomagok sorozatát összehasonlítja az ismert támadási nyomokkal. Egyezés esetén aktívan vagy passzívan válaszol az eseményre. A válasz lehet egy SNMP-riasztás előállítása, e-lelél üzenet küldése, de akár a támadó tényleges megakadályozása a támadás kiteljesítésében (ez utóbbi a behatolásmegelőzés) is.
- **Eltérés érzékelése** – Lehetővé teszi az IDS számára a normális forgalmi és információáramlási mintázat felmérését, majd az attól egy adott küszöbértéknél nagyobb eltérés esetén a beavatkozást (ilyen lehet például egy új protokoll megjelenése a hálózaton). Az eltérésérzékelés leghatékonyabban akkor használható, ha társítjuk a protokolldekódolási képességgel is, miáltal az IDS képessé válik annak felismerésére, hogy milyen viselkedés várható, és az attól való eltérés – normálistól eltérő parancsok vagy kérések megjelenése – esetén a beavatkozásra.

Meglehetősen elterjedt az IDS-sel kapcsolatban az a téveszme, hogy képes mindennek a megfigyelésére. Ez egyszerűen nem igaz. Az IDS használata a védelem egy újabb rétegeként rendkívül hasznos lehet. Ha azonban egyedül az IDS-re akarnánk csupán hagyatkozni a biztonságunk megteremtése során, súlyos hibát követnénk el.

### Hálózati behatolásérzékelő rendszer (NIDS)

A hálózati behatolásérzékelő rendszer a hozzákapcsolt hálózati szegmens csomagjait „fogja el”. Ez a mondat így hasonlít a csomagszaglászóval kapcsolatban leírtakra; a szaglászás és az elfogás között azonban van különbség. Ez utóbbi a hálózatmegcsapolás koncepciójára épül, és számos különböző módon implementálható. Ezeket a módszereket a hálózati kapcsolók működésének és forgalomszétválasztó módszereinek figyelembe vételével dolgozták ki. Az IDS-nek a hatékony működéshez a lehető legtöbb hálózati forgalmat látnia kell. Az NIDS implementálási módjai az alábbiak:

- **Közébüső hálózatmegcsapolás** – A csomagok elfogásának ezen módszere esetén két hálózati eszköz között helyezünk el egy „csapot”, és az NIDS-t ehhez csatlakoztatjuk.
- **Porttükörözés** – A használt kapcsolótól függően a porttükörözés valószínűleg a leghatékonyabb módszer. E technika szerint a kapcsolót utasít-

.....  
juk arra, hogy a rajta keresztülhaladó valamennyi csomag egy másolatát küldje ki egy meghatározott portjára, és az NIDS-t ehhez a tükröző porthoz csatlakoztatjuk.

Miután az NIDS beolvassa a csomagot, számos különböző módon analizálhatja (az NIDS típusától függően). Némely NIDS az „ujjlenyomat-egyezések” figyeli, összehasonlítva a csomagot az adatbázisában lévő támadási mintákkal. Mások a szokatlan mennyiségek csomagok alapján vonják le azt a következtetést, hogy valószínűleg támadás van folyamatban. Az NIDS egyik legnagyobb előnye az, hogy telepítése után szinte látatlanul képes meglapulni a figyelt hálózaton.

Van néhány olyan, a méretezhetőséggel és időszerűséggel kapcsolatos probléma, amelyet az IDS-ipar jelenleg is próbál leküzdeni. A hálózati sebesség jelentős felgyorsulásával nehezen tud lépést tartani, ráadásul a mostani gigabites hálózatok téryerését látva megjósolható, nincs már messze az idő, amikor a 10 gigabites hálózatok is elterjedtté válnak. A NIDS természetesen minden egyes csomagot el akar fogni, és analizálni kívánja a tartalmát, ám a megnövekedett sebesség olyan kihívást jelent, amely még nincs teljesen megoldva. A támadási minták frissítési gyakorisága sincs még közelében sem a kívántosnak tartott sűrűségnél, így az egyre újabb támadások érzékelése meglehetősen problematikus. Nyilvánvaló, hogy az IDS-szállítók mintafrissítő gyakorisága még nagyon messze van a vírusirtóktól.



*A Cisco nemrégiben kiadott egy új modult a Catalyst 6000 kapcsolójához, amely a behatolásérzékelést magába a kapcsolóba integrálja, ami a csomagok elfogásának nagyobb pontosságát képes nyújtani.*

A NIDS telepítése teljes egészében az egyes helyeken létező hálózati architektúrára alapszik. A hálózati szegmensek száma és helye általában meghatározza a telepítendő NIDS számát és helyét is.

A NIDS-et hagyományosan a leghatékonyabb a hálózat bejárata közelében elhelyezni, mint például a tűzfal minden szélén (kívül és belül egyaránt), vagy a behívószerver mellett, illetve az üzleti partnerek hálózata felé irányuló kapcsolatoknál. Ez az elhelyezés lehetővé teszi a szervezet számára a hálózat peremén elhelyezett előszűrők (tűzfalak és útválasztók) hatékonyságának ellenőrzését is. Ezekben a helyeken a hálózati kapcsolatok általában viszonylag alacsony sávszélességűek (T1 sebességűek), így az IDS könnyen lépést tud tartani a forgalommal. Ez adja az ellenőr-

zésre és a beállításokra a legnagyobb lehetőséget, és különösen jól megfelelnek a biztonságukra ügyelő vállalatoknak, amelyek internetről is elérhető alkalmazásszerverei a tűzfal mögött vannak. Hasonlóan alkalmas az elhelyezésére a vállalat nagy kiterjedésű hálózati gerince (WAN-gerinc). Gyakran felmerülő probléma, hogy a hálózat kihelyezett részeiről indul támadás a főhálózat ellen. Mivel a WAN-kapcsolatok általában viszonylag alacsony sávszélességűek, így kiválóan megfelelnek a NIDS képességeinek.

Az ajánlott biztonsági gyakorlat szerint az IDS-megoldás kiválasztása során minden külső, minden belső NIDS-t érdemes használni. Ez lehetővé teszi számunkra, hogy minden az internetről, minden a belülről kiinduló támadásokat észleljük. Kicsit furcsának tűnhet, hogy kettőt akarunk belőle; nem szabad azonban elfelejteni azt a statisztikai tényt, mely szerint a támadások többsége belülről indul ki. Akár a külső, akár a belső elhelyezés „megtakarítása” nagymértékben csökkenti a védelem hatékonyságát, lerontva ezzel a biztonság szintjét.

### Gépalapú behatolásérzékelő rendszerek

A gépalapú behatolásérzékelő rendszerek az adott gépen figyelik a felhasználói és rendszeraktivitást, észlelik a támadásokat, és beavatkoznak a megakadályozásuk érdekében. A hálózati megfelelőjükkel szemben a megfigyelendő gépen (például levelező- vagy webszerver) vannak installálva, és elsősorban a gép eseménynaplóit figyeli, nem pedig a hálózaton közlekedő csomagokat. Nem a csomagokat hasonlítja össze a támadás mintákkal, hanem megkísérli felismerni azokat a helyi vagy távoli felhasználói és rendszereseményeket, amelyek megfelelnek egy támadás mintának, és ezért nem kellene bekövetkezniük.



**9.**

*Az NIDS a gépről gépre továbbított csomagokat figyeli, míg a HIDS azzal foglalkozik, hogy mi is történik magán a gépen, figyelve a használati mintákat és a naplókat. Az előbbi ezért inkább hasonlít egy parkoló felügyelőjéhez, aki az összes ott parkoló autót figyeli, az utóbbi pedig inkább egy olyan őrhöz, aki csak egy adott autótőriz.*

A HIDS a vírusvédelmi szoftverekhez hasonlóan működik (persze nem csereszabatos vele), azonban olyan fejlett lehetőségei vannak, amelyek nagymértékben megnövelik a biztonság szintjét. Legalkalmasabb a gépek elleni támadások kivédésére, köszönhetően a felhasználói műveleteket és állomány-hozzáféréseket figyelő és elemző képességeinek. A számító-

gépes támadások többsége – amelyek ugyan különböző forrásokból eredhetnek (csalódott, felbosszantott alkalmazott, de akár ipari kémkedés is okozhatja) – a szervezeten belülről ered. A HIDS figyeli a szervereket, és az alábbi információkat szolgáltatja:

- Behatolási kísérletek vagy sikeres behatolások, valamint a feljegosított felhasználók gyanús tevékenysége.
- A gép állandó tesztelése annak biztosítására, hogy állapota megfeleljen az elfogadott biztonsági gyakorlatnak, például elvégezték-e rajta a legújabb frissítéseket, nincsenek rajta szükségtelenül futó szolgáltatások stb.
- Felülvizsgálati szabályok kezelése, adatbizonnyíték-forrás, statisztikai analízis és adatfeltáráás, bizonnyítékgyűjtés, és bizonyos esetekben hozzáférés-ellenőrzés. A jobbak ezeket a lehetőségeket is nyújtják.

A HIDS telepítése meglehetősen nyilvánvaló; ez egy olyan alkalmazás, amely magán a figyelt szerveren foglal helyet, és figyeli az állományrendszer változásait, a rendszerleíró adatbázis módosulását, a nyitott végpontokat, a futó alkalmazásokat, valamint a gépről kiinduló és oda érkező valamennyi forgalmat. A gyakran saját hálózatukon lévő szerverfarmok és az alkalmazásszerverek a HIDS által figyelt leggyakoribb szerverek.

Amennyiben több gépet is figyelnie kell, a HIDS beállítása úgy célszerű, ha egy központi helyre küldi a jelentéseit, megkönyítve az események összekapcsolását és a teljes cég figyelését. Telepíteni a webszervereken, állományszervereken és a nyilvános internet felé más szolgáltatást nyújtó gépeken érdemes.

## 9.2. HOGYAN LEHET ÉSZREVENNI A BEHATOLÁST?

Minden IDS-gyártó (és van belőlük jónéhány) rendelkezik valamilyen divatos kifejezéssel, amellyel a hiszékeny embereknek el akarja magyarázni, miként is végzi a feladatát az IDS. Sajnos ezzel ellentétes hatást ér el, hiszen minden gyártó el akar adni, a világ azonban sajnos ingatag, a biztonsággal kapcsolatban pedig sok hamis ígérettel találkozhatunk. Ebben a pontban ezért nagy vonalakban megvizsgáljuk, hogy mit is kellene a gyártóknak mondaniuk.

Az IDS a TCP/IP-protokoll egy különleges implementációjával rendelkezik, amely lehetővé teszi számára a más címekre küldött csomagok összegyűjtését, majd a vizsgálathoz való újracsoportosításukat. Nem elelegendő egyszerűen megfogni a csomagokat – az IDS-nek meg is kell vizsgálnia azokat. Erre számos lehetőség kínálkozik, amint azt a következőben meglátjuk.

## 9.2.1. A KOMMUNIKÁCIÓFOLYAM ÚJBÓLI ÖSSZEÁLLÍTÁSA

Az IDS képes az egy adott kommunikációhoz tartozó csomagfolyam újbóli összeállítására, hiszen csak így vizsgálhatja meg, mi is történik. Ez a folyamat alapvető fontosságú, mivel ennek alapján lehet az eseménymozaikeket összerakni, és a megfelelő esemény-összefüggéseket visszajelenteni a vezérlőkonzolra. Ez már csak azért is fontos, mert a kutatások szerint a hálózati férgek akkor jutnak be a hálózatba, ha a felhasználók a kliensek hálózatába bedugják a saját laptopjukat, azok ott megfertőződnek, majd visszaérkezve a vállalat hálózatába, elkezdik terjeszteni a fertőzést. Még ennél is rosszabb, ha az alkalmazottak létesítenek egy VPN-csatornát a vállalati hálózatba, ám időnként átlépik a hálózati férgek ellenőrzését szolgáló procedúrát. A fő gondot tehát ezúttal is az jelenti, hogy az alkalmazott a tűzfal megkerülésével beviszi a saját laptopját a céghoz, bedugja és bejelentkezik ezzel a fertőzött gépével a hálózatba. Célszerű lehet tehát a laptopokra is HIDS-t telepíteni, megelőzendő az ilyen eseteket.

## 9.2.2. PROTOKOLLANALÍZIS

A támadások a siker érdekében igyekeznek megváltoztatni az általuk hordozóként használt protokollinformációkat. A *halálra pingelés* például azért lehet sikeres, mert megváltoztatja a csomag méretét – pedig a protokollvizsgálattal ez könnyen felfedhető lenne. Az IDS rendelkezik egy ellenőrző rendszerrel, amely az érvénytelen csomagokat képes megjelölni; ez érintheti viszont azokat a legális csomagokat is, amelyek nagyon szét vannak törölve. Ez ismét csak azt bizonyítja, hogy milyen fontos a kommunikációfolyam visszaállítása.

A protokoll-ellenőrzés fontos szempontja az alkalmazások ellenőrzése, amelynek során az IDS felismeri az alkalmazás helytelen viselkedését vagy a protokolltól való eltérését. A WinNuke például a NetBIOS érvényes protokollt használja ugyan, de vonalon kívüli információt is használ közben, ami elvileg szintén érvényes, azonban kizárolag a gépek támadására használt.

## 9.2.3. AZ ELTÉRÉS FELISMERÉSE

Az eltérés felismerése a szemétlevél-szűrőkhöz hasonlóan a betanítással kezdődik, mivel a tanulási idő alatt az IDS-nek meg kell ismernie, hogy mi tekinthető normális hálózati működésnek. Ez a „normális” természetesen minden rendszer esetén más és más szintet és tevékenysége-

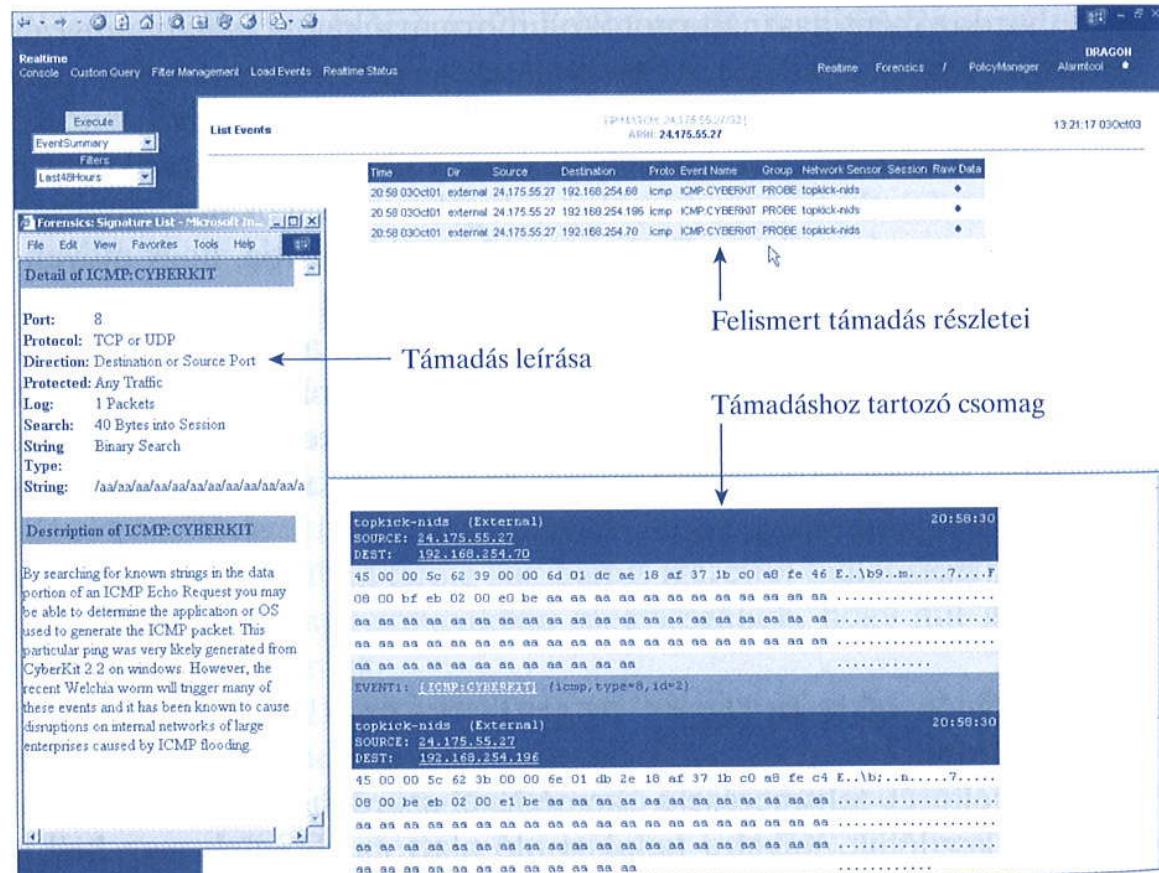
ket jelent. A módszer alapötlete az, hogy az állományokkal, felhasználói bejelentkezésekkel, CPU-használattal, háttértár-aktivitással és még sok egyébbel kapcsolatos működési információkról statisztikai módszerrel megállapítható legyen egy átlagos érték. Miután az átlagos érték megvan, az IDS képes az ettől való eltérést észlelni.

Tegyük fel például, hogy figyeljük a gépek működését, és az IDS azt észleli, hogy minden nap kora hajnalban a hálózaton lévő gépek közül sokuk hirtelen nagyon aktív lesz. Ekkor persze nem tudjuk, hogy valójában mi is történik, de legalább megkaptuk a figyelmeztetést, hogy jó lesz az esetet kivizsgálni.

#### **9.2.4. A MINTA EGYEZŐSÉGE**

A mintaegyeztetés a támadások észlelésének leggyakoribb módszere. A kifejezés azt jelenti, hogy az IDS-nek képesnek kell lennie minden támadási technika felismerésére ahhoz, hogy hatékonyan működhessen. Tartalmaz ezért egy hatalmas adatbázist, amelyben a támadások ujjlenyomatainak ezrei találhatók, s működése során az ezekkel való egyezést vizsgálja.

Például számos IDS-t használnak a visszaélésszerű használat (mondjuk ha a felhasználó pornográf vagy szerencsejáték-oldalakat látogat mun-



9.3. ábra. Egy IDS-észlelő képernyőképe

kaidőben) felfedésére. Az ilyen jellegű visszaéléseket általában kulcs-szavakra alapítjuk. Az is egy lehetőség azonban, hogy valaki elkezdi az ICMP-csomagokkal feltérképezni a hálózatot, ami szintén egy felisme-rendő támadási mintát követ. A bizonyos mintákkal megegyező csoma-gok észlelhetők, amint az a 9.3. ábrán is látszik.

Az ilyen típusú támadásfelismerés a rendszer nagyobb felbontású vizsgálatát követeli meg, mint a protokollanalízis vagy az eltérésfelismerés. Eredményeképpen bizonyos események felismerhetők, amelyek például azt igazolják, hogy sikeresen betörtek egy gépre. Az egyik leggyakrabban felismert minta az, ha egy támadó saját magának adminisztrátori (*root*) jogokat biztosít egy gépen. A gép ekkor küld egy nyugtázó csomagot a támadónak, amelyben jelenti neki, hogy megkapta a „*root*” jogosultságot – a csomagokat tehát vizsgálni kell, hogy szerepel-e bennük a „*root*” szó. Ez persze egy nagymértékben egyszerűsített példa, de jól szemlélteti, hogyan is működik az IDS ezen képessége.

## 9.2.5. NAPLÓANALÍZIS

Az IDS képes számos eszköztől érkező naplózó üzenetek fogadására, és a közük biztonsági eseményekkel kapcsolatosak felülvizsgálatára. Az NIDS például képes egy gépen használt valamennyi alkalmazásiréteg-be-li protokoll naplózására. Az eseménynaplózó rendszerek (WinNT Event, UNIX syslog, SNMP Trap stb.) ezeket a kibővített eseményeket összefogva tudja hasonlítani a hálózat más eseményeivel. A naplóanalízis nem csupán azt a képességet jelenti, hogy a syslog-ot és más eseményeket képes egymáshoz viszonyítani, de jelenti egy olyan mechanizmus meglétét is, amely az IDS-riasztást kiváltó csomagok feljegyzésére képes. Ilyen további hasznos műveletek még például:

- **A vétkes csomagok elfogása** – Az IDS-érzékelő elfogja azt a csomagot, amely kiváltotta a riasztást. Így a csomag tartalmát később lehet analizálni. Az IDS beállítható úgy, hogy ilyenkor a további csomagokat, vagy akár az egész munkamenetet szintén elfogja. Ennek alapvető fontossága van annak megértésében, hogy miért is fogta el a csomagot, és segít a hamis és valós riasztások elkülönítésében.
- **A munkamenet újraépítése** – Az IDS gyakran egyetlen csomagra riaszt, de az a csomag csupán a riasztás kiváltásának végső oka. A teljes kommunikációs munkamenet újraépítése alapvető fontosságú a teljes támadás felismerésében, és segít a hamis riasztások kiszűrésében is, hiszen általánosabb képpel rendelkezünk a tényleges történések ről.

A naplóknak azért is van nagy szerepük, mert egy esemény bekövetkezésekor a riasztás kiváltásának eszközéül szolgálhatnak. A következő lépés pedig minden módszerek kombinálása a hálózat biztonságának növelése érdekében.

## 9.2.6. A MÓDSZEREK KOMBINÁLÁSA

A támadók folyamatosan fejlesztik és javítják képességeiket, ami egyre nehezebben észrevehetővé teszi őket. Az IDS fejlődése így folyamatos, hogy lépést tarthasson a támadók fejlődésével. Egyre intelligensebbek és jobb észlelőképességűek lesznek a behatolásérzékelési módszerek kombinálásával.

Egy IDS például képes lehet a mintaegyezség, a protokollanalízis és az eltérésfelismerés módszerét kombinálni. A többszörös módszer szerinti támadásfelismerés újabb példája annak, hogy az IDS egyre fejlettebb technológiává növi ki magát.

## 9.2.7. A BEHATOLÁS MEGAKADÁLYOZÁSA

A behatolást megakadályozó rendszerek (*IPS – Intrusion Prevention System*) a lehető legkorábbi pillanatban megakadályozzák, hogy a folyamatban lévő felismert támadás sikeres legyen. Az IPS az IDS-sel működik együtt, a gyártók IPS-képességekkel felruházott IDS-t gyártanak. A támadás megakadályozására két technika kínálkozik:

- **Kilövés (sniping)** – Ez lehetővé teszi az IDS számára, hogy a gyanús támadást a TCP reset, vagy az ICMP „nem elérhető” csomag elküldésével befejeztesse.
- **Kitérés (shunning)** – Ez lehetővé teszi az IDS számára, hogy az előszűrő útválasztót vagy tűzfalat dinamikusan konfigurálhassa, így letiltva a felderített támadáshoz tartozó csomagok bejutását, s ezáltal kitérve a további kapcsolat elől. Ahogy az IDS egyre fejlettebb lesz, a kitérés átalakul blokkolássá; ilyenkor az IDS felveszi a kapcsolatot az útválasztóval vagy a tűzfallal, és a támadó IP-cím kiszűrésére létrehoz egy új hozzáférési listát.

Figyelem!



A kitérés hatékony működése nagyon sok finombeállítással jár. A hibás beállítás, vagy az IDS rendszeres karbantartásának hiánya könnyen a hálózat szolgáltatásmegtagadási állapotba kerüléséhez vezethet. Tegyük fel, hogy egy támadó tudja, vagy észlelte, hogy kitérésre konfigurált IDS védi a hálózatot. A támadó ekkor több ezer olyan csomagot állíthat elő, amelyről tudja, hogy az IDS le fogja tiltani a forrás IP-címét. A szolgáltatásmegtagadás akkor következik be, ha a támadó ezt az ezernyi csomagot látszólag minden különböző IP-címekről küldi. Tegyük fel, hogy az egyébként az AOL-hoz vagy más népszerű internetszolgáltatókhoz tartozó tűzfalak címét adja meg – ekkor a hálózatunkat védő IDS egyszerűen letiltja az ezen szolgáltatóktól az e-kereskedelmi oldalunkra érkező valamennyi forgalmat. Ezért alaposan meg kell fontolni, hogy milyen események okozzanak kitérési akciót, és a szűrés mennyi ideig tartson.

### 9.2.8. Az IPS REAKCIÓJA ÉS CSELEKVÉSE

Amint erről már beszélünk, az IDS különböző cselekedetekre képes a támadás felismerésekor. A legjobb megelőző módszerek a kilövés és a kitérés. A kilövést egyedül is végre tudja hajtani, a kitéréshez azonban más eszközökre is szüksége van. Az IDS-érzékelőknek azonban a központi konzolra is célszerű jelentést küldeniük, amely – ha úgy lenne beállítva – szintén képes lehet valamilyen cselekedet végrehajtására. Ilyen cselekedet lehet például a következők egyike:

- **Tűzfal vagy útválasztó újrakonfigurálása** – A kitérés végrehajtására képes IDS újrakonfigurálhatja az útválasztót vagy a tűzfalat, hogy ki-szűresse vele a behatoló IP-címét. A támadó azonban ekkor még minden áttérhet más címekre. A Checkpoint-tűzfalak támogatják a gyanús tevékenységeket megfigyelő protokollt (*SAMP – Suspicious Activity Monitoring Protocol*), amely a tűzfal átkonfigurálását teszi lehetővé a saját OPSEC szabványa szerint.
- **SNMP-eltérülés (trap) küldése** – A HP OpenView, Tivoli, Cabletron Spectrum, és más hasonló kezelői konzolra az így beállított IDS küldhet egy eltérülési megszakítást.
- **Napló készítése** – Az IDS képes a Windows-eseménynaplóba vagy a syslog-szerverre naplózni, vagy akár e-levelet küldeni.

Ne felejtsük el a korábbi figyelmeztetést: az IDS csak akkor legyen képes elővigyázatossági szándékkal megváltoztatni más eszközök beállítá-

sát, ha a kézi átvizsgálást és az aprólékos finomhangolást már korábban elvégeztük. Az IDS még ma is bőven a tervezési fázisban van csupán, az IPS pedig még nála is fiatalabb.

## 9.2.9. IDS-TERMÉKEK

Számos IDS létezik, és számos félreértés övezi őket, mivel még nagyon kevés, a működésük módját érintő szabvány él. Igen nehéz összehasonlítani ezeket a termékeket, mert a használt terminológia, az azonos szavak jelentéstartalma, a jellemzőik és a működési lehetőségeik annyira eltérők, hogy egyszerűen nem összehasonlíthatók. Számos olyan termék is van azonban, amely a nyílt forráskód közössége ezen területen kifejtett erőfeszítéseire alapszik. Ezeknek a termékeknek a zászlóshajója kétségtől kívül a Snort.

### **Snort! (Horkantás)**

Nincs miért aggódni – ez a horkantás nem valamilyen hátborzongató vadállattól származik (bár egy röfi a logójuk), csupán a <http://www.Snort.Org> webhelyen elérhető fejlesztőcsapat nyílt forráskódú IDS-alkalmazásának a neve. Idézzünk a webhelyről:

*A Snort egy nyílt forráskódú behatolásérzékelő rendszer (IDS), amely képes az IP-hálózatok valós idejű forgalomanalízisére és csomagnaplázására. Képes végrehajtani a protokollanalízist, a tartalomkeresést és az egyezőségvizsgálatot, és számos támadási és letapogatási forma, például a puffertúlcordulás, lopakodó portletapogatás, CGI-támadás, SMB-szondázás, OS ujjlenyomat kísérlet, és sok más hasonló felismerésére képes.*

*A program rugalmas szabálynyelvet használ a gyűjtendő vagy átengedhető forgalom leírására, és egy moduláris, bedugaszolható architektúrájú érzékelőmotort tartalmaz. Valós idejű riasztási képességekkel is fel van ruházva, tartalmazza a syslog, egy felhasználó által megadott állomány, egy UNIX-végpont, illetve a WinPopup üzenet formájú riasztási lehetőséget.*

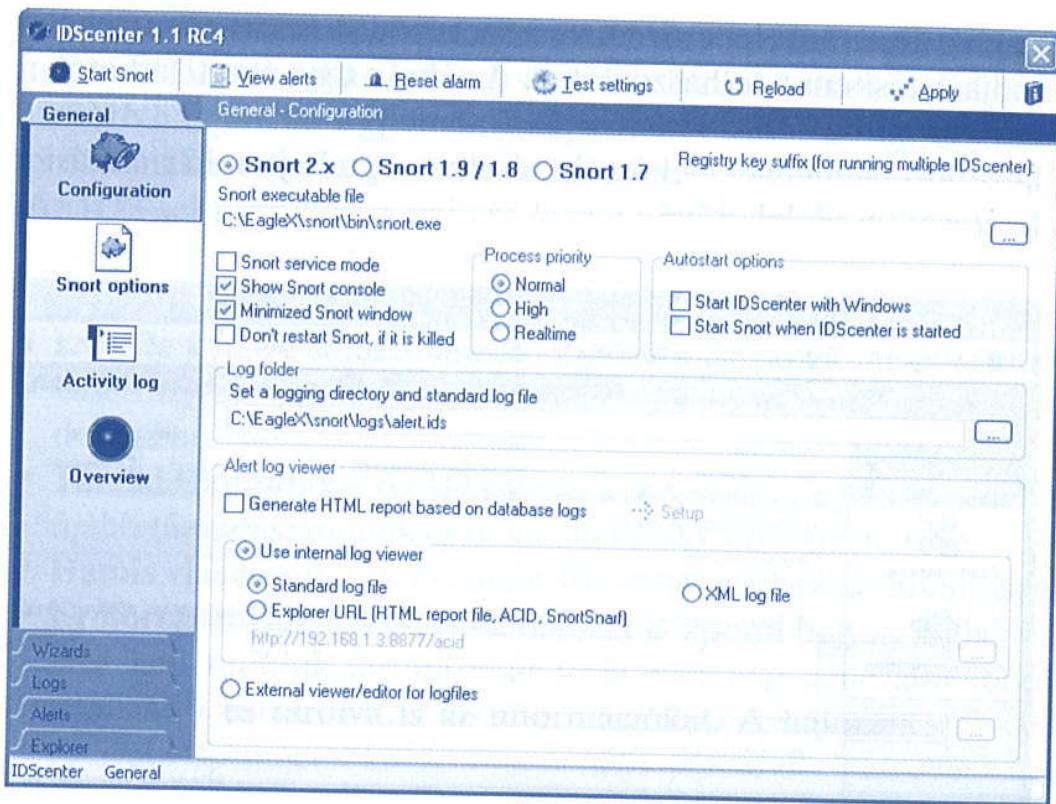
*A programnak három fő felhasználási formája van. Használható egyszerű csomagszaglászként, mint a tcpdump(1) alkalmazás; lehet csomagnaplázó (hasznos lehet például a hálózati hibakeresés során), de alkalmazható teljes képességű hálózati behatolásérzékelő rendszerként is.*

Mielőtt nagyon fellelkesülne a 9.4. ábrán látható grafikus felület láttán, be kell valljam, az nem része a Snort IDS csomagnak, csupán az Engage Security cégnél (<http://www.engagesecurity.com>) dolgozó emberek csoportja készítette.

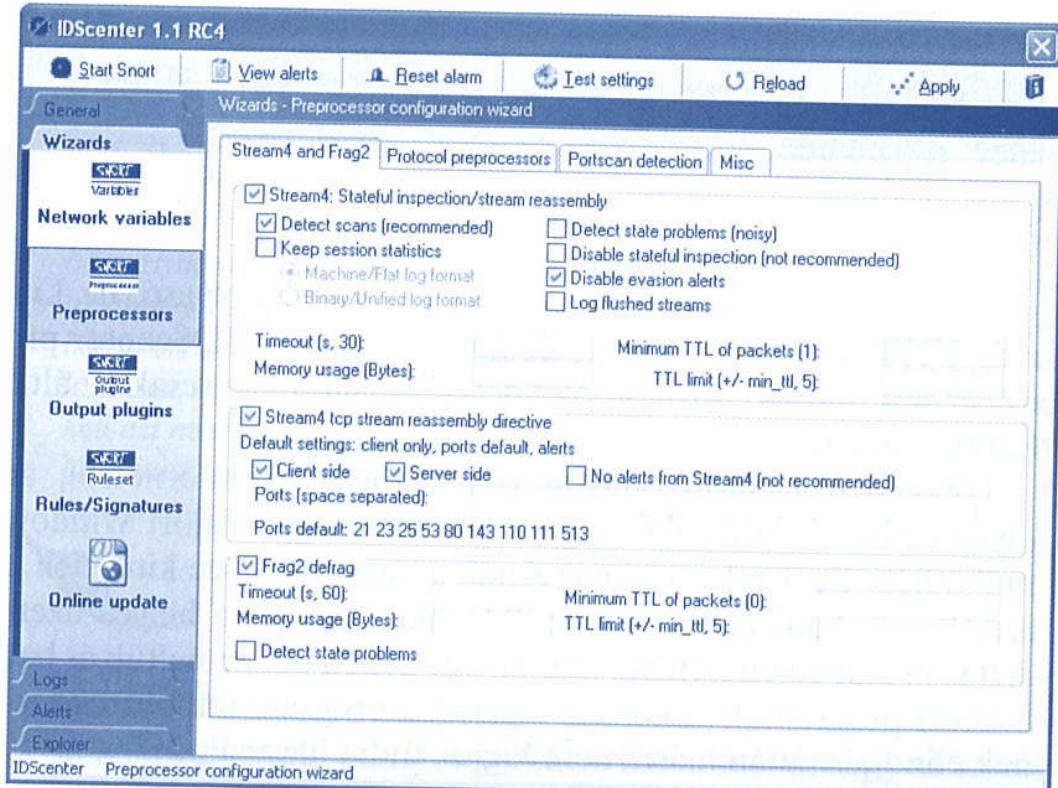
Maga a Snort-alkalmazás egy parancssorból vezérelhető program, amelyet nagyon jól írtak meg, jóllehet néha meglehetősen körülményes

# HÁLÓZATI BIZTONSÁG

a konfigurálása és a monitorozása. Amint az a 9.4. ábrán is látható, az ADScenter GUI vezérlőfelület lehetővé teszi a felhasználók számára a grafikus konfigurálást és monitorozást.



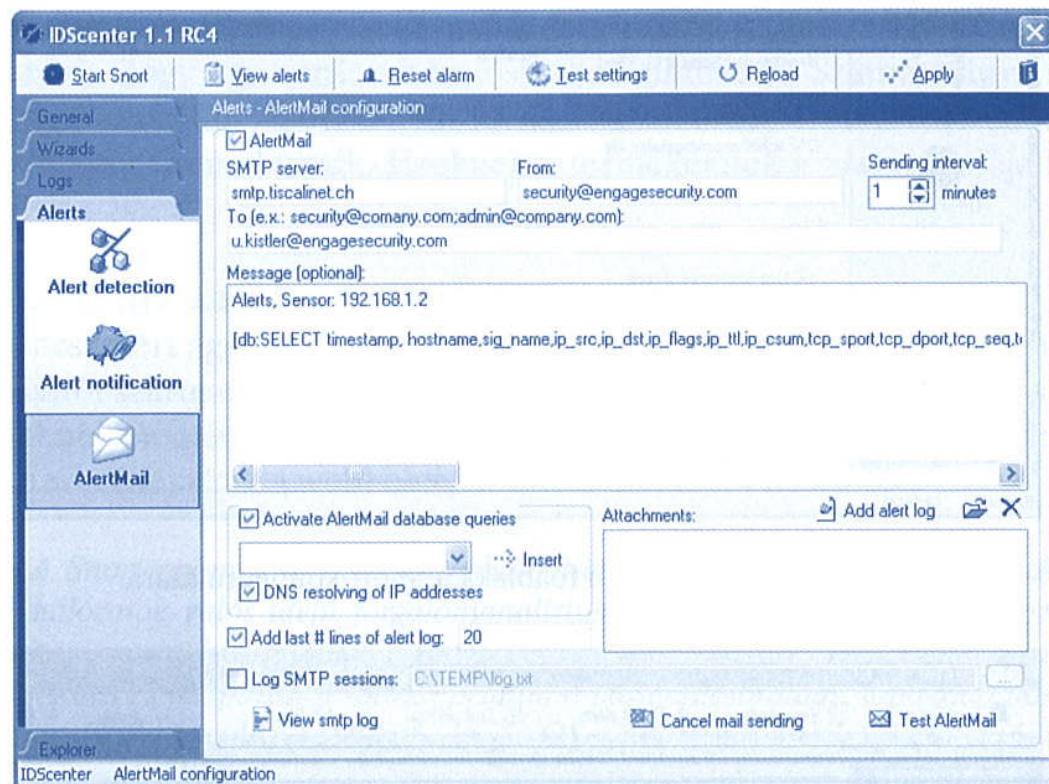
9.4. ábra. Az IDScenter program főablaka a Snort konfigurálására



9.5. ábra. Az IDScenter program szabálybeállító ablaka

A 9.5. ábra a Snort működési lehetőségeit beállító alap konfigurációs opciókról ad némi ízelítőt. Az IDScenter program ezen képernyője alapvető fontosságú a nyilvánvalóan bekövetkező finomhangoláshoz.

A 9.6. ábra mutatja be a felhasználó behatolási vagy támadási profiljainak kiválasztását lehetővé tevő képernyőt. A Snort ezen profilkor alapján tudja értesíteni a felhasználókat. Az ábrán ugyancsak láthatók a riasztási műveletek beállítási lehetőségei is, amelyek az adminisztrátor figyelmét követelő események bekövetkezésekor végrehajtandó riasztási mód kiválasztását teszik lehetővé.



9.6. ábra. Az IDScenter értesítési képernyője

A Snort programot esetleg ismeri a kedves olvasó, ha Linux- vagy más UNIX-féle rendszeren már dolgozott, de az IDScenter programról ekkor sem tudhat, mivel az Windows 32 alapú, akárcsak az általa kezelt Snort-változat.

Több Win32 Snort-változat is letölthető az internetről, amelyeket olyan emberek írtak, akik nagyon akarták, hogy a Snort Windows alatt is működjék. Ezeknek a csomagoknak a nagyobb része kitűnően működik, azonban néhányuk további beállításokat igényel a helyes üzemeléshez. Azt sem szabad elfelejteni, miután egy gépen beüzemeltük és beállítottuk a Snort programot, akkor ezt a gépet a program monitorozó műveleteinek elindítása után másra nem fogjuk tudni használni.

## 9.2.10. Az IDS KORLÁTAI

Mint fejlődő technológiának, hatalmas előnyei mellett van néhány könyen kezelhető hibája is. Telepítésére mindig csak előszűrést végző tűzfalakkal és útválasztókkal együtt kerülhet sor. Ezek az eszközök, és a rajtuk használt titkosítás és hitelesítés már bizonyítottan jó védelmet nyújtanak. Néhány hiba vagy rossz konfigurációs beállítás ugyan gyakran vezet problémákhoz ezeken az eszközökön, de alapelveik már kipróbáltan jók. Az IDS-sel kapcsolatos néhány korlát a következő:

- **HIDS vagy NIDS vita** – Ezen soha nem szabad vitázni; mindenkorre szükség van. A hálózat minél jobb biztonságának megteremtéséhez javasolt együtt használni őket, hiszen különböző szerepet játszanak a védelemben.
- **Támadási minták** – Az IDS-termékek frissítése gyakran elmarad, a legújabb támadási minták csak lassan válnak hozzáférhetővé.
- **Hamis riasztások** – A normális forgalom is okozhat hamis riasztást.
- **Erőforráskorlát** – A NIDS a hálózat központi helyén foglal helyet. Lépéster kell tudniuk tartani akár több ezer gép generálta forgalommal, analizálva és tárolva is az információkat. A hálózati szegmensén keresztül információt küldő valamennyi gépet figyelnie kell. Ennek teljes végrehajtására nyilván nem minden lehet képes, ezért egyszerűsítéseket kell alkalmazni.



*Amikor egy IDS beszerzéséről kell dönten, tájékozódni kell arról is, hogy másodpercenként hány csomag fogadására és feldolgozására képes. Számos gyártó megpróbálja a másodpercenként feldolgozandó bitek számát hangsúlyozni, de a tényleges szűk keresztmetszet mindenkorre a csomagok száma. Nagyból bármelyik gyártó terméke képes megbirkózni az 1500 bájt méretű csomagokat továbbító 100 Mbps sebességű hálózat forgalmával, de csak kevés tudja a 60 bájt méretű csomagokat feldolgozni ugyanezen a hálózaton. Ez elsőre érthetetlen lehet, de gondoljuk meg, az 1500 bájt méretű csomag esetén csak egyszer kell azt megvizsgálni, míg 60 bájt méretű csomagok esetén ugyanezt a vizsgálatot huszonötöszer kellene elvégezni. Ennek végrehajtása pedig nyilván kihat a teljesítményre.*

- **Hosszú időtartamú állapotok** – Klasszikus problémát jelentenek a lassú letapogatások, amelyek esetén a támadó csak nagy időközökkel próbál tájékozódni a hálózatról. Az IDS nem képes ilyen sok információ

hosszú idejű tárolására, így nem fogja tudni együtt ellenőrizni az összetartozó adatokat.

- **Érzékelő vaksága** – Az IDS-t hagyományos számítógépen futó alkalmazásként fejlesztették ki, amelynek nincsenek különleges képességei, így lehetséges válik a hálózati kapcsolatuk telítése és így az IDS elvákitása, amelynek hatására eldobnak olyan csomagokat, amelyeket fel kellene dolgozniuk. Az egyik ilyen módszer az eseménynapló telítése. A nyílt forráskódú *nmap* program pedig tartalmaz egy „csalétekletapogatás” (*decoy scan*) nevű támadási módszert, amely esetén a program több száz letapogató csomagot küld, mindegyiket valamilyen hamisított IP-címről. Ez lehetetlenné teszi az adminisztrátor számára annak kiszűrését, hogy a sok cím közül melyik volt az igazi, és melyek voltak a csalik. Ebben az esetben is megmarad persze a bizonyító adat – ha támadóra gyanakszunk, az adatok továbbra is ott vannak.
- **Tárolási korlátok** – Amikor egy támadó megpróbálja elvakítani az IDS érzékelőjét, akkor még az a szándék is vezérelheti, hogy túltöltse annak adatbázisát vagy háttértárolóját. Ez egyaránt eredményezheti azt, hogy az érzékelő korábbi eseményeket letöröl, vagy akár abbahagyja a további események tárolását.
- **Szolgáltatásmegtagadás** – Az IDS rendkívül bonyolult, hiszen a teljes TCP/IP-implementáció fut benne. Ennek eredményeképp maga is érzékeny a támadásokra. A támadók gyakran maguk is ingyen letöltik a céljuknál futó IDS-alkalmazást, majd igyekeznek olyan csomagokat találni, amelyek lehetetlenné teszik a működését. A támadás során azután ilyen csomagokkal kiiktatják a működését, és további tevékenységük már észrevétlen marad.
- **Széttördelés** – Azt a műveletet hívjuk így, amikor a nagy csomagokat széttördeljük kisebbekre. A fogadó TCP/IP-verem fogja ezeket újra összeállítani. A legtöbb IDS azonban nem képes a csomagok újbóli összeállítására, pedig léteznek olyan egyszerű eszközök, amelyek a támadásokat alkotó csomagokat széttördelik, így játszva ki az IDS figyelmét.



Az IP-csomagok széttördelése a TCP-fejléc közepén már régóta ismert támadási forma a tűzfalak végpontszűrési technikájának kijátszására. Néhány, ipari célra fejlesztett NIDS azonban képes újra összeállítani a forgalmat. Vannak olyan tűzfalak is, amelyek „szabványosítják” a forgalmat, vagyis újból összeállítják a csomagot azok továbbbenedése előtt. Az IDS-érzékelők a monitorozó porton vannak, nincs külön IP-cím hozzájuk rendelve, így nem érzékenyek a szolgáltatásmegtagadási támadásra. A kezelői interfész, amelynek van IP-címe, a többi hálózati forgalomtól leválasztott hálózatban kell elhelyezni.

- **Minta kijátszása/megváltoztatása** – Számos egyszerű NIDS minta szerinti ellenőrzést végez. A támadó parancsállományok jól ismert mintát követnek, így pusztán az ismertek mintáinak adatbázisban tárolása meglehetősen jó felismerési képességet biztosít, bár könnyen kijátszható pusztán a támadó parancsállomány, és ezzel együtt mintázatának megváltoztatásával.
- **IDS „kiértékelő” eszközök** – Különböző szabadon elérhető eszközök, amelyek az IDS használhatóságának és pontosságának tesztelésére lettek kifejlesztve. A két leggyakoribb a „snot” és a „Stick” nevű tesztelő. Ezen szerszámok képesek több ezer támadást előállítani, így ellenőrizve, hogy az IDS vajon felismeri-e őket. Egy támadó is használhatja azonban ezeket a szerszámokat arra, hogy saját támadását elrejtse a többi közé, vagy akár az IDS elvakítására is.

Ezek a korlátok nem jelentik azt, hogy az IDS használhatatlan vagy értékletlen lenne. Manapság annyira sok támadás van, és a támadóeszközök olyan könnyen elérhetők, hogy az IDS impozáns mennyiséggű támadást képes felismerni. Helyesen kezelve és vezérelve, az IDS drámai mértékben meg tudja növelni a hálózat biztonságát. A helyes használat egyik sarkalatos pontját azonban a fejezet végére tartogatjuk.

A biztonsági szabályzat szintén alapvető fontosságú az IDS sikeres használatában. Feltehető a kérdés: „Miért lenne szükség egy újabb szabályzatra és eljárásrendre? Ezek akkora terhet jelentenek!” Nem lehet elégé hangsúlyozni azonban, hogy a biztonsági intézkedések célja az értékek védelme, és nem várható el, hogy a védelmükben érdekelt valamennyi személy ugyanazon normák szerint védje őket – hacsak meg nem mondjuk nekik a követendő szabályzatot. Ellenkező esetben egyetlen, a védelmet hibásan értelmező személy minden lerombolhatna.

## 9.

### 9.3. A MÉZESBÖDÖN

Most nyilván azon tűnődik a kedves olvasó, hogy mit keres Micimackó és kedvenc nyalánkságának tárolására szolgáló eszköze egy, a hálózati védelemről szóló könyvben.

Mindeddig a könyvben nem esett szó a támadókkal folytatott harcról, azonban ebben a pontban erről fogunk szót ejteni – ez a **mézesbödön** (*honeypots*). Így emlegetjük az interneten található azon rendkívül rugalmás számítógéprendszert, amely maga egy gondosan beállított biztonsági eszköz, azzal az egyetlen céllal, hogy vonzó csalátket kínáljon a mások rendszereibe behatolni szándékozó támadók számára, így ejtve őket csapdába.

A mézesbödön nem egy adott biztonsági problémát akar megoldani – bármennyire is furcsa legyen ez. Ehelyett szoros ellenőrzésekkel félrevezetésre, megelőzésre, felismerésre és információgyűjtésre használjuk ezeket, lévén úgy tervezve, hogy a támadók számára kiadják magukat valami másnak, mint amik valójában. A mézesbödönt ezért eleve nem lehet sorozatgyártani, hiszen legfőbb előnye az, hogy folyamatosan próbálják szondázni, támadni vagy akár feltörni is. Elsőre furcsa lehet az ötlet – miért lehet szüksége bárkinek is egy ilyen eszközre a hálózatán? Egy kifejezetten a támadók feltörésére váró eszközt elhelyezni a hálózaton – ennek látszólag semmilyen értelmes célja nincs. A mézesbödönnek azonban számos fontos célja van:

- A mézesbödön elvonja a támadók figyelmét a hálózatban lévő sokkal értékesebb célpontokról, hiszen ők valós célnak hiszik a kifejezetten számukra oda helyezett rendszert.
- Képesek időben figyelmeztetni az új behatolási kísérletekről és támadásokról. Az IDS hamis riasztást is küldhet, a mézesbödön azonban, mivel rajta valódi szolgáltatás nincs, csak akkor generál forgalmat, ha valaki elkezdi támadni.
- Lehetővé teszi egy támadó tevékenységének támadás alatti és utáni alapos vizsgálatát. Elsőre úgy tűnhet, hogy ez csak a biztonsági rendszerek tervezésében érintett kutatók számára fontos, de gondoljuk csak végig, hogy bárki milyen sokat tanulhat belőle. Ezt a tudást később arra is lehet használni, hogy a hálózaton található valódi biztonsági erőforrások beállítása megfelelő legyen.
- Talán legnagyobb előnyük a tényleges vagyon elrejtése (*CYA – Cover Your Assets*). Megvan azon egyedülálló képességük, hogy bebizonyítsák, a hálózati biztonságot sikerült hatékonyan megtervezni.
- Az „ismerd meg az ellenségedet” alapelve szintén fontos célja a mézesbödönnek. Nem elég, ha tudjuk, hogy vannak támadók, hiszen ezt mindenki tudja, csak be kell kapcsolni a tévhíradót. Sokkal fontosabb meghatározni a technikájukat és módszereiket. Miután megvan a támadási profil, a későbbi hasonló kísérletektől nagyobb valószínűséggel védhetjük meg magunkat.



Lance Spitzner, a mézesbödön-rendszerek szakértője írt egy cikksorozatot „Ismerd meg az ellenségedet” címmel, a mézesbödön-projekt részeként (<http://www.honeypot.net>). Ezekben leírja, hogyan lehet lekövetni a támadókat az ilyen rendszereken keresztül, és miként lehet meglehetősen jól megérteni viselkedésüket.

Az IDS részben bemutatott hamis riasztás problémája a mézesbödön-rendszerek esetén szóba sem kerül. Ha az egyébként passzív eszközön bekövetkezik valamilyen támadás, azt könnyű észlelni. Ez nyilván azt jelenti, hogy a támadás érzékelése már egyáltalán nem probléma, ugye? A valódi rendszerek esetén a mézesbödönt gyakran megtaláljuk a demilitarizált zónákban, azonban nincsenek bejegyezve a DNS- vagy WINS-adatbázisokba, és nem kapcsolódnak egyetlen tényleges feladatú géphez sem. Ha ennek ellenére a mézesbödönt elkezdi tapogatni a DMZ valamelyik másik szervere, akkor ennek jelentése van. Na és mi történik akkor, ha a hálózaton belül lévő mézesbödön támadás alá kerül? Ilyen értelemben tehát a mézesbödön passzív eszköz, csak várakozik arra, hogy végre valaki megtámadja.

Ebben a pontban a mézesbödönt annak szemléltetésére mutatjuk be, hogy amint egy aktív eszköznek, például a behatolásérzékelő rendszernek megvan a maga szerepe a hálózatban, ugyanígy egy passzív eszköznek, nevezetesen a mézesbödönnek is megvan, amelynek ráadásul nincsenek olyan korlátai, mint az IDS-nek.

A mézesbödönök tervezésük és szándékolt felhasználásuk szerint két csoportba oszthatók:

- Kutató mézesbödön** – Telepítésük és karbantartásuk meglehetősen bonyolult, és elsődlegesen kutatási, katonai, vagy kormányzati szervek használják.
- Kereskedelmi mézesbödön** – A hálózatuk biztonságáért aggódó vállalkozások által használt eszközök; ebben a könyvben ezekre összpontosítjuk figyelmünket. A kereskedelmi mézesbödön jellemzően egy adott céllal vagy szándékkal kerül telepítésre.



*Az Egyesült Államokban jelenleg felmerülnek kérdések a mézesbödön jog-szerűségével kapcsolatban, hogy vajon a „lehallgató” eszközök családjába tartoznak-e (ugyanis bármilyen információs hálózat lehallgatásához bírói végzésre van szükség). Bármilyen ostobán is hangzik, az FBI és más rendfenntartó szervezetek még mindig csatáznak ezen kérdésben.*

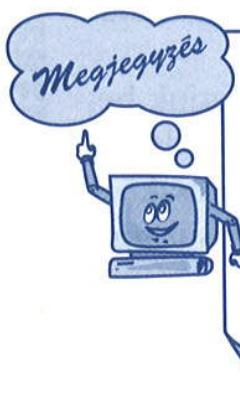
9.

A mézesbödön e két nagy csoport mellett még működése szerint is csoportosítható:

- Végpontfigyelők** – Viszonylag egyszerű eszközök. Azokat a végpontokat figyelik, amelyeket a támadók általában támadni szoktak. Tervezésük fogva válaszolnak a végpont letapogatásra, vagyis megengedik a

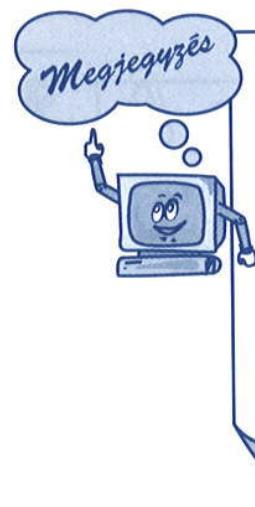
támadónak a hozzájuk való csatlakozást. Az ilyen típusú mézesbödön az általa figyelt végponthoz való csatlakozási kísérleteket naplózza.

- **Megtévesztő rendszerek** – A végpont egyszerű figyelésénél egy lépéssel többet is tesz, és megtéveszti a támadókat azzal, hogy úgy viselkedik irányukba, amint azt a valódi rendszer is tenné. Ez azt jelenti, hogy nem csupán úgy válaszol mondjuk a TCP 110 végpontjára érkező kérésre, amint azt egy POP3 levelezőserver tenné, hanem pontosan úgy viselkedik, mint egy ilyen szerver. Természetesen nem implementálja az imitált szolgáltatás valamennyi feladatát, csak amennyi elegendő ahhoz, hogy a támadó bekapja a csalétket.



A könyv megírásakor az interneten található három leggyakrabban támadott szolgáltatás a régebbi, nem frissített verziójú Linux-rendszerek (Red Hat 5.0), a Solaris 2.6, és a Microsoft IIS 4.0. A mézesbödön megtervezése során ezért érdemes lehet a fenti három szolgáltatás(oka)t imitáló rendszerek felállításáról döntenи.

- **Többszörösen megtévesztő rendszerek** – Ismét egy lépéssel továbbmenve, olyan mézesbödön rendszerek, amelyek nem csupán egyszerre több szolgáltatás imitálására képesek, de szimulálni tudnak különböző operációs rendszereket is. Ezen rendszerek közül a legelterjedtebb a Specter, amelyet a <http://www.specter.com> webhelyen lehet megtalálni.



A mézesbödön rendszerek további jellemvonásait lehet felnérni akkor, ha egész rendszereket állítunk be mézesbödönként. Ilyenkor a behatolásérzékelés még egy lépéssel továbbmehet, ha mellettük az IDS-t is használjuk. A mézesbödönökkel kapcsolatos legjobb információforrás a <http://www.honeypots.net/honeypots/links> webhely.

Win32 gépekre letölthető egy ingyenes mézesbödön is, amelynek neve „Honey Potter”: <http://honeypott4.tripod.com>. Ez egy olyan, viszonylag kis tudású (ám ingyenes) szoftver, amely a mézesbödönök világába képes bevezetni.

### 9.3.1. A MÉZESBÖDÖN TERVEZÉSÉNEK STRATÉGIÁI

A legnyilvánvalóbb veszély az, hogy a helyesen működő mézesbödön a saját hálózatunk és erőforrásai felé irányuló támadást jelez. A gyakorlatban ez azt jelenti, hogy a hálózatunk egy részén már van egy bűnöző. Ennek eredményeként néhány doogról meg kell győződniük a hálózat biztonságának fenntartása érdekében.

Használunk tűzfalat! Igen, tűzfalat – bár a mézesbödön kifejezetten azért van, hogy be lehessen rá hatolni, azért ne tegyük gyanúsan könyűvé a támadó dolgát, s ennek legjobb módja egy tűzfal. Olyan szabálykészletet állítsunk be rajta, amely a mézesbödönről kifelé irányuló alap szolgáltatáskészlet-csomagot megengedi. A szakértők azt ajánlják, hogy érdemes minden befelé irányuló csomag számára engedélyezni a mézesbödön elérését, de kifelé csak az FTP, ICMP és DNS mehessen.

A támadó cselekedeteinek észlelése a különböző naplókon, és a tényleges mézesbödön naplókon alapszik. Amennyiben nem tudjuk biztosítani ezek helyes működését, akkor csupán megnehezítjük az életünket, és gyakorlatilag hatástalaná tettük a mézesbödön felállítására végzett erőfeszítéseinket.



Némelyek úgy vélik, hogy a bűnözők ilyen módon való elfogása a csapdaállítás valamilyen formája. Ez a vélemény azért nem állja meg a helyét, mert a mézesbödön nem egy aktív csalétek – nem hirdeti magát. A jogosult tevékenységet folytató felhasználó soha nem fog beléük botlani, hiszen a jó magaviseletű felhasználó nem próbál meg jogosulatlanul behatolni máshová.



9.

### 9.3.2. A MÉZESBÖDÖN KORLÁTAI

Jóllehet a mézesbödönnek számos előnye van, azért korlátokkal is rendelkezik:

- Ha a rendszerét ténylegesen sikerül megtörni, akkor ugródeszkaként szolgálhat a hálózat többi részébe történő betöréshez.
- Megnöveli a bonyolultságot. A biztonsággal kapcsolatban a bonyolultság már önmagában is azért rossz, mert megnöveli a hibalehetőségek számát.
- A mézesbödöt is karban kell tartani, akárcsak minden más hálózati eszközt és szolgáltatást.

## **9.4. ÖSSZEFoglalás**

A fejezetben a hálózatbiztonsággal kapcsolatos két legújabb technológiát foglaltuk össze – a behatolásérzékelést és a behatolásmegelőzést. Az IDS legalapvetőbb típusainak megismerésével kezdtünk: a szervereken futó gép alapú behatolásérzékelő, és a hálózaton futó hálózati behatolásérzékelő rendszerekkel. A fejezet bemutatta az IDS legalapvetőbb működési elveit, majd a téma kört a mézesbödön tárgyalásával zárta.

## **9.5. ÖSSZEFoglaló KÉRDÉSEK**

1. Mikor és ki tervezett először kereskedelmi IDS-t?
2. Az IDS-nek mely két alapvető típusát ismeri? Egyszerre vagy külön-külön kell-e használni ezeket?
3. Határozza meg és ismertesse az NIDS-t! Hol és hogyan működhetnek hatékonyan a hálózaton?
4. Határozza meg és ismertesse a HIDS-t! Hol és hogyan működhetnek hatékonyan a hálózaton?
5. Mikor a leghatékonyabb az eltérésérzékelés és miért?
6. Milyen behatolásérzékelő módszertan képes az alkalmazások viselkedését is ellenőrizni?
7. Nevezze meg és határozza meg, hogy melyik két technika segítségével válik az IDS képessé a támadás tényleges megakadályozására!
8. Véleménye szerint melyik az IDS három legfontosabb korlátja? Magyarázza meg, miért azokat választotta!
9. A mézesbödön eltéríti a támadókat az értékesebb erőforrások támadásától. Igaz vagy hamis ez az állítás?

# 10. fejezet

## Kereskedelmi eszközök

Azok a boldog emberek, akik valamit előállítanak;  
 azok az unatkozó emberek, akik sokat fogyasztanak,  
 és semmit nem állítanak elő.

(William Ralph Inge)

**A fejezet elolvasása után érteni kell, és el kell tudni magyarázni az alábbi témákat:**

- a hálózatra fenyegést jelentő támadások alapvető típusait;
- hogyan hajtsuk végre vagy hajtassuk végre mással a hálózat biztonsági ellenőrzését;
- miként használhatjuk fel a biztonsági ellenőrzés és sebezhetőség tesztelése során kapott eredményeket a hálózat biztonságosabbá tételeben;
- hogyan hajtsuk végre vagy hajtassuk végre mással a hálózati védelem áttörhetőségének ellenőrzését.

**10.**

Karácsony táján az emberek világszerte megtapasztalják a „házigazdához üzembe helyezhető alkatrész” (HÜHA) érzést. A HÜHA szóval fejezhetjük ki azt az izgatottságot és csodavárást, amelyet számos ember érez egy bonyolultabb készülék, mondjuk az új számítógép kicsomagolásakor. Az új anyagok szaga, a billentyűzet tapintása, a PC első elindításakor hallható hang, a gyönyörű, ragyogó, 1 GB memóriájú, 300 GB háttároló kapacitású, 5 GHz-es processzorú SzuperGép 2010 Turbó Kistorony GTX PC látványa és hangja egyszerűen lenyűgöző – legalábbis így hallottam másoktól.

Könnyen elképzelhető, hogy a fenti jelenet karácsony táján világszerte számos háztartásban lejátszódik. Az előző évben kapott PC-t lefokozzuk „családi géppé”, amelynek háttárolóját soha nem töredézettségmentesenítjük, amelyet nem frissítünk, s amelynek ezért három napra van szüksége az elinduláshoz.

Idén a gépet a kis Jancsi (vagy a kis Juliska, mielőtt még az emancipáció élharcosa szóvá tenné) kapja, hiszen most kezdi meg tanulmányait az egyetemen, és biztosan legfelső fokú disszertációt kell majd írnia biológiából és kémiából (vagy bármilyen más tárgyból). Bárki beláthatja, ezt semmiképpen sem teheti meg egy olyan platformon, amely nincs legalább 150-szer erősebb, mint az ūrsiklók és az Egyesült Államok léghárítása által használt valamennyi számítógép összesen.

A kis Jancsinak/Juliskának persze szüksége van valami igazán erős konfigurációra azért is, hogy nyugodtan játszhassa mindeneket a szélessávú internetcsatlakozáson keresztül elérhető játékokat, amelyeket a karácsonyi ajándékozásra számítva a múlt hónapban bekötött szélessávú internetcsatlakozáson keresztül érhet el. A gépet természetesen a saját kis szobájukban kell elhelyezni, hogy a házi feladatok elkészítése kevésbé legyen a minden nap házimunka, és inkább az önként, örömmel végzett feladat része, amelyet a hálószoba és iroda ötvözésével létrehozott környezetben haborítatlanul végezhet. Lehet persze az is, hogy eleve nem asztali gépet kaptak, hanem egy laptopot; az internetkapcsolat vezeték nélküli kapcsolattal is tartható, így nyugodtan használhatjuk azt munka közben is.

Most gyorsan tegyük néhány dolgot azonnal teljesen világossá. Legelőször is, egy tizenéves gyereknek nincs szüksége olyan számítógépre, amely az RC5 titkosítást két napnál hamarabb is képes megtörni; már vannak erre szakosodott állami intézmények, amelyek erre teljesen képesek, és tényleg nincs szükségük versenytársra az ösztönzésükhez. Másodsor, a „leveled érkezett” szavakat nem fogjuk hallani a kérdéses szuperszámítógép hangszóróból, amikor az a kontinensközi gerinchálózat néhány évevel ezelőtti sávszélességét lassan megközelítő szélessávú internetkapcsolathoz csatlakozik. Ehelyett nyugodtan feltételezhetjük, hogy a kemény metálzene, a rap vagy a gyerek által kedvelt más, MP3 formátumban letöltött, kifejezetten idegesítő zenét fogjuk nagy hangerővel hallani belőle.

Függetlenül attól, hogy a kis egyetemi hallgató mit mond a szüleinek, ha az iskolában bármiféle számítógép-tudománnyal kapcsolatos képzést is kap (és 80%-uk ilyen), valamennyien egyetlen célért küzdenek: elnyerjék bűntársaiktól az „über haxor” koronát. Bizony, a piciny gyermek, aki tegnap még tejbepapit evett az ujjaival, ma már csak néhány egérkattintásnyira van a számítógépes bűnöző törvényi tényállását kimerítő cselekmény elkövetésétől, s a karácsonyra vásárolt csillogó-villogó gép lehet az a szupereszköz, amely a rácsos ablakú hotel hosszabb ideig tartózkodó lakójává teheti őt. Az ebben a könyvben tárgyalt támadások, technikák és eszközök közül mennyi kerül pénzbe? Nem túl sok, és ha valamelyik mégis ilyen lenne, biztosan letölthető valahonnan az internetről a feltört változata is.

Az intelligencia és a hatalom bármilyen formájával szemben megjelenő elutasítás kombinációja (a tizenéves) kezében a korszerű számítástechnikai berendezés könnyen veszélyes eszközzé degradálódhat. Persze sok szülő mondja magának: „Az én gyermekem biztosan nem csinál semmi ilyesmit. Úgy neveltem őt, hogy tisztelete a törvényt, és megtanítottam neki, hogyan különböztesse meg a jót és a rosszat.” Ez mind százszázalékosan igaz lehet, de a kisgyerek nevelése során valószínűleg elfelejtette, hogy az internet ugyanolyan vad és veszélyes, mint az 1800-as években a vadnyugat volt.

Az interneten való kalandozás az utóbbi tíz évben felnövekvő gyermekek számára teljesen természetes cselekedet, míg az interneten az erkölcs még mindig gyerekcipőben jár. Több ezer olyan oldal létezik, és ezt valóban voltak, akik megszámolták, amely a feltörésekkel, betörésekkel, kódtörésekkel és a számítógépes bűnözéssel kapcsolatos információkat tartalmaz. A „hogyan írunk vírust” téma körben könnyebben lehet információt találni (és érdekesebb is), mint a tejkaramellás sütemény készítéséről.

A szélessávú internet-hozzáférés az ismeretlenség olyan kultúráját teremtette meg, amely korábban soha nem létezett a korlátok közül kitörni kívántak, szüleiket bosszantó tizenévesek számára. Az e-levelezés, a webhelyek és a csevegőszobák ellátják a gyerekeket a társadalom korlátainak pillanatok alatti felmérésének képességével, és amikor úgy vélik, hogy ez a társadalom szörnyen kezeli őket, vagy akár szeszélyből is, azonban elkezdik ugyanennek a társadalomnak a határait feszíteni.

A szülő persze még mindig meg lehet győződve a saját gyermekének ártatlanságáról és jószándékáról, amikor az internet használatával kapcsolatos felelősségteljes viselkedésről van szó. Még akár igaza is lehet; de ha megkérdeznénk a hírekben épp az előbb szerepelt, számítógépes bűnözésért perbe fogott tizenéves gépkalóz édesanyját, akkor ő is ugyanezket mondaná, illetve mondta is mindaddig, amíg a tények meghátrálásra nem kényszerítették – ekkor azonban már sajnos késő volt.

**10.**

Ebben a fejezetben azokat a biztonsági eszközöket vesszük sorra, amelyeket a támadók használnak, hogy a kedves olvasó megismerhesse ezeket, és legalább tudja, mivel is áll szemben. Ezután megvizsgáljuk a hálózat gyengeségeinek felfedésére szolgáló eszközöket, majd a biztonsági felülvizsgálat teljes folyamatát ismerjük meg. Ez utóbbi alapvető fontossággal bír számunkra, ha a saját hálózatunk biztonságáról akarunk meggyőződni.

## 10.1. A SEBEZHETŐSÉG ELEMZÉSE

Ebben a részben a támadók által könnyen elérhető eszközöket tekintjük át. Az alapvető mondanivalónk az, hogy a csibészek bizony jó eszközökkel rendelkeznek. A korábbi fejezetekben már számos különféle támadó-eszközt láttunk, a támadók azonban nagyon széles körből választhatnak, amikor többszintű támadást akarnak indítani a hálózatunk ellen. Miután a támadó képes megvetni a lábat a támadott hálózat egyetlen pontján, onnan kiindulva már egyszerűbben kereshet magának egy másik sebezhető pontot.

A támadók például képesek kihasználni a gyenge hitelesítést és feljogsítást, a helytelen lefoglalásokat, a gyenge biztonsági implementációkat, a felhasználók és programok megosztott jogait, de akár az alkalmazottak biztonsági szempontból gyenge vagy eredendően hibás viselkedését is, így nyerve jogosulatlan hozzáférést a kritikus hálózati erőforrásokhoz.

Az egész könyv azt igyekezett súlykolni, hogy még a legjobb biztonsági technológiák és eljárások is számos különböző módon kijátszhatók. Ennek megértéséhez némi időt el kell tölteni a támadók által ténylegesen használt módszerek és eszközök megismerésével. Lehet, hogy izgalmas a támadó eszközeit látni, ha azonban bármilyen hálózati erőforrás is a gondjainkra van bízva, akkor jobb meggyőződni arról, hogy a hálózatunknak legalább ezektől az eszközöktől nincs mit tartania. Rendkívül fontos, hogy saját magunk használjuk ezeket az eszközöket, hogy a sebezhető pontokat felderítsük velük, mielőtt még egy támadó találná meg azokat. Számíthatunk arra, hogy ezeket az eszközöket valaki egyszer használni fogja a hálózatunk ellen – csupán azt áll módunkban meghatározni, hogy ki használja azokat elsőként.

### 10.1.1. ALAPVETŐ TÁMADÁSOK

A legfejlettebb biztonsági technológiák, szabályzatok és eljárások hatékonysága gyorsan nullára csökkenhet, ha a hálózat biztonságáért felelős személyek nem ismerik a hálózatuk támadására használt módszereket és

eszközöket. Ez a fejezet a támadók által használt néhány módszert és különböző eszközöket, ezek működését, valamint az ellenük használható eszközöket és technikákat mutatja be.

Még a legjobb biztonsági technika és eljárás értéke is gyorsan lecsökkenhet, ha nem ismerjük pontosan a hálózat támadására használt módszereket. Alapvető fontosságú ezért a támadók által csereberélt különböző szoftverek, működési elveik, valamint a kivédésükre alkalmas védelmi módszerek ismerete. A továbbiakban bemutatjuk a támadók által használt gyakori technikákat és szoftvereket.

### IP-cím hamisítása és munkamenet-eltérítés

Ilyen jellegű támadásról akkor beszélünk, ha egy támadó a saját IP-címe helyett hamis forráscímet tartalmazó csomagokkal próbál meg bejutni a hálózatba. A támadás a bizalmi viszonyokat támadja, mivel a támadó megpróbálja megbízható gépként feltüntetni a sajátját. A támadás sikereséhez a támadónak meg kell határoznia a célgépen használt „bizalmi mintát” – például azokat az IP-címeket, amelyeket a célgép megbízhatónak tart. Ha a támadó ezt sikeresen megtette, akkor lehet egy lépéssel tovább, vagy valamilyen módon feltörve a gépet, vagy megbénítva a működését. Az ilyen jellegű támadásokat gyakran használják egy átfogó támadási stratégia első lépéseként.

*Mivel a támadó meghamisítja az IP-címet (olyan címet állít be, amelyet a cél megbízhatónak tart – ez lehet például a helyi hálózaton érvényes cím is, ha a támadó nem helyben van), ezért a céltól kapott válasz nem hozzá érkezik vissza. Ez azt jelenti, hogy a támadó nem látja, hogy sikерrel járt-e. Ez az oka annak, hogy ez a támadásfajta általában csak az első lépés. Meglehetősen gyakran lehet vakon megpróbálni kihasználni egy adott sebezhetőséget, majd a támadás következő lépéseivel ellenőrizni, hogy tényleg sikerült-e a támadás.*

10.

### IP-címhamisító és munkamenet-eltérítő eszközök

A módszert egy sereg eszköz támogatja:

- **Dsniff** – Hálózati felülvizsgálat és védelmi képesség tesztelésére szolgáló szoftvercsomag. Ide tartozik maga a Dsniff, a filesnarf, mailsnarf, msgsnarf, urlsnarf és a webspy, melyek passzívan monitorozzák a hálózatot az érdekes adatok (jelszavak, e-levelek stb.) elfogása reményében. A hálózati forgalom elfogását az arp spoof, dsn spoof és macof végzi.

- **Hunt** – Egy kapcsolatba való betörésre, az ott zajló kommunikáció megfigyelésére és erőszakos lezárására szolgáló eszköz. A hasonló, Jugernaut nevű eszközből nőtte ki magát, és számos olyan lehetőséggel rendelkezik, amellyel elődje még nem.
- **Ettercap** – Igen hatékony UNIX-, illetve Apple OS X-alapú program, amelynek szövegmódú grafikus felülete kellően könnyen kezelhető ahhoz, hogy a szkriptcsávók kedvence legyen. minden művelet automatizált, a célszámítógépet pedig a hálózaton felfedezett gépeket tartalmazó legördülő listáról lehet kiválasztani. A szaglászás négy típusát képes alkalmazni: IP, MAC, ARP és nyilvános ARP szaglászást. Számos más automatikus lehetőséggel is rendelkezik.

Az ilyen típusú támadások megakadályozása ugyanolyan fontos, mint a jellegzetességeik és a használt eszközök megismerése. A virtuális magánhálózat (VPN) meglehetősen hatékonyan védi magát az IP-cím hamisításától, hiszen maga a VPN a hálózaton való átvitel előtt titkosítva elhelyezi a csomagban az eredeti IP-címet. Ha akár az adat, akár a forráscím az átvitel során megváltozik, a fogadó oldal ezt észleli, és a csomagot eldobja. Ezzel tehát a támadót megakadályozza abban, hogy a VPN titkosító kulcsok ismerete nélkül betörhessen a hálózatba.

### Csomagszaglászók

Ezek az eszközök a hálózati csatlakozási pontjuk mellett elhaladó valamennyi csomagot összegyűjtik. Lehetnek szoftver- (PC vagy PDA) vagy hardveralapúak (kifejezetten erre kifejlesztett számítógép). A támadók olyan fejlett csomagszaglászó alkalmazások segítségével, amelyek az OSI-modell különböző rétegei által használt protokollokból képesek az adatokat visszafejteni, ellophatják a felhasználóneveket és a jelszavakat, majd ezen tudás birtokában további támadást indíthatnak. A szaglászók használata leginkább úgy lehetséges, ha a támadó képes a vállalat fizikai biztonságát feltörni – mondjuk besétálhat az egyik irodába, és bedughat ott a hálózatba egy laptopot. A vezeték nélküli hálózatok egyre növekvő használata azonban fokozatosan szükségtelenné teszi ezt a követelményt – sokszor a parkolóban álló autóból is elérhető egy vezeték nélküli eszközzel a vállalat hálózata. A szaglászók használatával a támadók értékes információkat nyerhetnek a helyi és magánhálózat-beli jelszavakról, felhasználó nevekről – számos alkalmazás, például az FTP, a Telnet és mások nyílt szövegként küldik el a jelszavakat. Az SMTP, POP3 és IMAP protokollok különösen ki vannak téve ennek a támadásnak, mivel a felhasználók gyakran csatlakoznak kívülről a levelezőszerverhez, hogy elolvassák leveleiket, a levelekhez pedig sokszor az adott gépen érvényes felhasználói névvel és jelszóval férhetnek hozzá. A felhasználók ráadásul

gyakran különböző rendszereken és alkalmazásokban is ugyanazt a jelzést használják, így a támadó egy jelszó megszerzésével nagy valószínűséggel hozzáfér a hálózat más erőforrásaihoz is.

### Szolgáltatásmegtagadási (*DoS – Denial of Service*) támadás

Létezik egyszerű és elosztott változata (ez utóbbi a *DDoS – Distributed Denial of Service*). A csomagvihar, az elárasztás, és más DoS-támadási módszereket a hálózatok túlterhelésére használják: olyan sok kérést intéznek a megbénítandó szolgáltatáshoz, szervergéphez, vagy olyan sok csomaggal árasztják el a hálózatot, hogy a támadás alanyának működése nagymértékben lelassult, esetleg hosszabb-rövidebb időre akár meg is bénul – nem csupán elméletileg, de a gyakorlatban is. A „hagyományos” szolgáltatásmegtagadási támadás általában nem a célgépre való betörést szolgálja – a támadó célja a támadott cél zavarása vagy megbénítása az által, hogy olyan sok hamis kéréssel árasztja el, amelynek feldolgozására az képtelen. Ritkán előfordulhat az is, hogy segít vagy előkészít egy másik támadást.

Ha a cél működése nagymértékben lelassult vagy a cél megbénult, a tényleges felhasználók már nem tudnak hozzá csatlakozni, így a cél „megtagadja a szolgáltatást”. Az elosztott változata a hagyományostól annyiban tér el, hogy nem egy adott forrásból érkező hálózati forgalommal kísérli meg a cél megbénítását (ez a zavaró cél kiszűrésével viszonylag könnyen hárítható lenne), hanem az interneten található számos gépről (ritkábban a nevükben) egyszerre indít támadást. Ehhez az interneten lévő több gépet is meg kell fertőzni egy kis programmal (**DDoS démon**), így **zombi számítógépekké** változtatva ezeket, majd egy adott esemény bekövetkezésekor valamennyi egyszerre kezdi el támadni a célpontot.



*A DDoS démon egy különleges számítógépes program, amelyet a DDoS-támadás vezérlésére és lebonyolítására fejlesztettek ki. A könyv írásakor számos ilyen létezett: Tribal Village (TFN), TFN2K, Trinoo és Stacheldraht (szögesdrót). Ezekről a programokról az alábbi webhelyeken többet is meg lehet tudni:*

<http://staff.washington.edu/dittrich/misc/trinoo.analysis>  
<http://staff.washington.edu/dittrich/misc/tfn.analysis>  
<http://staff.washington.edu/dittrich/misc/stacheldraht.analysis>

10.

Ezek a **zombi hálózatként** együttműködő zombi számítógépek küldik ki a hamis csatlakozási kéréseket, megnövelve a cél által lekezelendő nyitott kapcsolatok mennyiségét, így akadályozva meg a tényleges felhaszná-

lókat a célhoz való kapcsolódásban. A DoS-támadásokat könnyű végrehajtani, és meglehetősen nagy kárt képesek okozni, hiszen szétszilálják a célszámítógép vagy hálózat működését, és gyakorlatilag leválasztják azt az internetről. Az ilyen támadások számos hamis csatlakozási technikát alkalmaznak. A SYN-elárasztás például képzelt, félgy nyitott TCP-kapcsolati kérések segítségével meríti ki a cél erőforrásait. A DoS-támadások kihasználják a támadott rendszer architekturális gyengeségeit; a legutóbbi példa a limitált kapacitást használta ki. Más esetekben a DoS-támadás az interneten használt elterjedt protokollok valamelyikének, például az ICMP-nek a sebezhetőségét használja ki. Egyes DoS-támadások során például nagymennyiségű „ICMP-visszajelzéskérés” (*ping*) üzenetet küldenek meghamisított IP-forráscímmel egy üzenetszóró (*broadcast*) címre. Az üzenetszórásként érkező üzenetet megkapott gépek mindegyike a hamis IP-címre küldi a válaszát, amivel lebéníthatják a célt. Ezeket a támadásokat nevezzük „törpíke támadásnak”.

A **törpíke támadás** (*smurf attack*) egy olyan típusú DoS-támadás, amely az internetvezérlő üzenetprotokoll (*ICMP – internet control message protocol*), például a jól ismert „ping”, valamint az IP-címek és az üzenetszóró címek sebezhetőségeit aknázza ki. A támadás a célgép vagy hálózat lebénítására irányul azzal, hogy minden erőforrását el akarja használni. Más kárt a támadás nem okoz. minden IP-hálózatban van két különleges cím:

- a hálózatcím, amely a hálózat első címe;
- az üzenetszóró cím, amely a tartomány utolsó címe.

A hálózatcím az IP-útválasztó táblában az adott hálózaticím-tartomány azonosítására szolgál. Az üzenetszóró cím arra lett kitalálva, hogy az adott alhálózat valamennyi gépének egyszerre lehessen küldeni egy üzenetet. A legtöbb IP-implementáció válaszol az olyan üzenetekre, amelyknél forrásként a hálózatcím vagy az üzenetszóró cím van feltüntetve. Ezt a lehetőséget nevezzük „irányított üzenetszórásnak”, amelynek megvan a maga haszna.

### **ICMP/Ping támadás**

A ping alapú támadás az ICMP tervezési elvét fordítja a támadó javára. A feltört gépet arra utasítja, hogy a kiválasztott célgépet folyamatosan bombázza a ping csomagokkal. Ezzel hihetetlenül sok ICMP „visszajelzés kérése” (*echo request*) kérés érkezik a feltört gépek ezreitől, ami már mágában is elkezdi megviselni a célpontot. A támadó ráadásul még a csomagokban szereplő forráscímet is megváltoztatja. A forráscím nem a ténylegesen küldő gép lesz, hanem oda is a célgép címét írja (vagyis a csomag cél- és forráscíme ugyanaz lesz). A célrendszer minden ping csomagra az

ICMP „visszajelzés küldése” (*echo reply*), vagyis „pong” üzenetet küldi, méghozzá a hamis cím miatt saját magának, ezzel automatikusan megduplázva a feldolgozandó csomagok számát. A végeredmény az, hogy a cél összeomlik azért, mert nem képes ilyen mennyiségű forgalmat kezelni. Elképzelhető az is, hogy a cél címét forrásdímként használva egy helyi hálózatba engedélyt kapunk az üzenetszórásra. Ezen támadási fajtával az a legnagyobb baj, hogy a forgalom teljesen szabályosnak tűnik,<sup>1</sup> és bárminely hálózatban, illetve tűzfalon keresztül engedélyezett. A támadás lefolyása bármely szondával vagy csomagszaglászóval észlelhető.

### SYN-elárasztásos támadás

A TCP/IP protokoll szerint a felek egy háromutas kézfogásos eljárás szerint veszik fel egymással a kapcsolatot, mielőtt megkezdenék az adatok forgalmazását. Ez a háromutas kézfogásos eljárás az alábbi:

1. A kliens (kezdeményező) küld egy SYN (szinkronizálás) jelzésű csomagot a szolgáltatásnak (kiszolgálónak). Ez a jelzés a TCP-fejrész egy adott helyén található.
2. A kiszolgáló a SYN-ACK (szinkronizálás nyugtázva) üzenettel válaszol.
3. A kezdeményező elküldi a kézfogást a kiszolgálónak (SYN-ACK tranzakció). Ettől kezdve a kapcsolat létrehozottnak tekinthető, és megkezdődhet az adatok forgalmazása.



#### Megjegyzés

*Richard Stevens „TCP/IP Illustrated” című könyvének első fejezete (a protokollok) a 231. oldalon írja le a SYN-csomagok formátumát. Írása kitűnő forrás lehet a téma iránt mélyebben érdeklődőknek.*

10.

A SYN-elárasztásos támadás akkor következik be, ha a kapcsolatot eredetileg kezdeményező gép nem hajtja végre a kiszolgáló SYN-ACK válaszát követő harmadik lépést. Ilyenkor a kiszolgálónak addig kell tarolnia a kapcsolatfelvételi kísérletet, amíg az időtúllépési hiba be nem következik. A támadás folyamán a kliens nem is válaszolhat, hiszen a kiszolgálónak küldött első csomagban a forrás-IP-cím hamisított. A támadó célja az, hogy a kiszolgálónak gyorsabban küldje a SYN-csomagokat,

1 Normális forgalomnak aligha nevezhető az azonos forrás- és célcímű csomag megjelenése, és manapság a legtöbbször az üzenetszórás sem jut át a tűzfalakon, így ez a támadási forma ma már könnyen megelőzhető. (A ford. meg.)

mint amennyi idő alatt az a SYN-ACK válaszra nem érkező harmadik csomag hiánya miatt bekövetkező időtúllépési hiba miatt törölni tudná a kapcsolatkezdeményezési kísérlettel kapcsolatos nyilvántartását. Más-ként megfogalmazva, el akarja használtatni a kiszolgálóval a kapcsolatteremtési kérések kiszolgálásával kapcsolatos erőforrásait. Ez a gyakorlatban azt okozza, hogy a kiszolgáló annyira elfoglalt lesz a sok SYN-csomag nyugtázása és a nem válaszoló kliensre való várakozás miatt, hogy a tényleges felhasználók kapcsolatteremtési üzeneteire már nem lesz képes válaszolni – sikeres lesz tehát a szolgáltatásmegtagadási támadás.

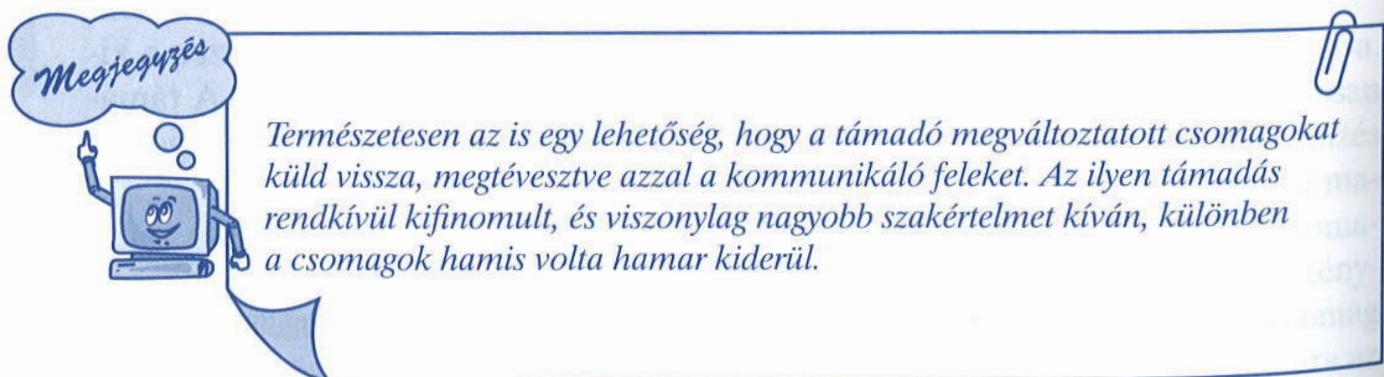
### A DoS-támadások megakadályozása

Felmerülhet a kérdés, miként lehet védekezni a szolgáltatásmegtagadási (DoS) támadások ellen. Ez talán az egyik legnehezebben kivédhető támadási forma, hiszen a támadást végző forgalom legnagyobb része olyan formában érkezik, amely az adott hálózaton teljesen szabályosnak tűnik. Az egyik leggyakoribb védelem a bizonyos típusú forgalmakra kiszabott korlátozás. Így például megengedhetjük a ping-üzeneteket (ICMP vissza-jelzés kérése), ha azonban túl sok érkezne, akkor DoS-támadást feltételezve korlátozzuk a számukat.

Bizonyos típusú forgalom esetén azonban ez a védelmi forma nem használható – például a webkereskés oldalunkra irányuló HTTP-forgalom korlátozása kifejezetten kínos lenne. Az „attól függ” szabály miatt tehát a vállalat IT-csoportjának komoly félelmekkel kell szembesülnie, amikor a DoS-támadások elleni védelmet fontolgatja.

### Beékelődéses támadás

A beékelődéses (*man-in-the-middle*) támadás esetén a támadó két gép közötti kommunikációs láncba ékelődik be: általában a szerver és a kliens közé. Ettől kezdve elfogja az egymással váltott üzeneteiket, és helyettük a sajátjait küldi tovább az eredeti címzettnek. A támadás célja ilyenkor sokféle lehet. Lehet egyszerűen információszerzés – például meg akarja tudni, hogy mennyi pénz van a bankszámlánkon, vagy mi a jelszavunk egy fizetős webszolgáltatásra. Lehet célja a forgalom blokkolása is – ekkor az elfogott csomagokat egyszerűen nem küldi tovább. Aggodalomra legin-

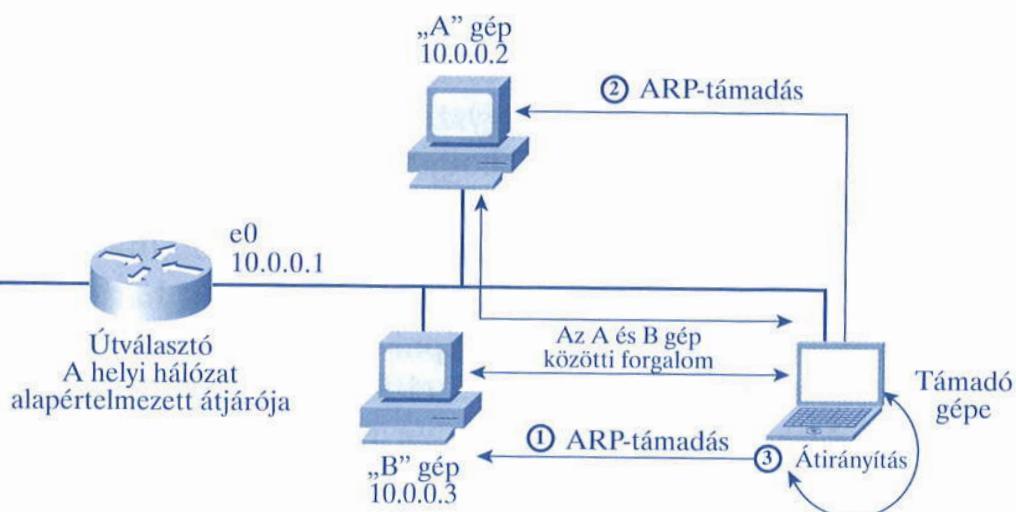


kább az adhat okot, hogy amennyiben a támadó nem változtat meg semmit, csak egyszerűen elfogja a csomagokat, akkor soha nem lehet rájönni, hogy valaki beékelődött a továbbítási útvonalba.

Hálózati szaglászókat, vagy az Ettercap (<http://ettercap.sourceforge.net>) programot gyakran használják az ilyen típusú támadások során. Megjegyzendő, hogy a beékelődéses támadást használják arra is, hogy bizonyos nyilvános titkosító kulcsokat újrakonstruáljanak, ennek tárgyalása azonban meghaladja jelen könyv kereteit. Mégis érdemes megemlíteni, hiszen ebből is látható, a jelszavak és kulcsok védelme mindig hasznos – ezért is van szükség jó jelszókezelési szabályzatra.

### ARP-hamisítás

Mind a vezetékes, mind a vezeték nélküli hálózatban az ARP-hamisítás az egyik olyan módszer, amellyel a beékelődéses támadás sikerre vihető. A célszámítógép ARP gyorsítótárának fabrikált ARP-címekkel való feltöltését nevezük „ARP-mérgezésnek” (*ARP poisoning*). E technika szerint a támadó fabrikált ARP-kérés és -válasz csomagokat állít össze, és így megváltoztatja a második rétegbeli Ethernet MAC-címet az általa választottéra. Mikor a támadó fabrikált ARP-válaszokat küld, a célszámítógép meg lesz győződve arról, hogy a kereteket a másik gépnek küldi, pedig a valóságban azok a támadó gépre irányulnak. Amennyiben helyesen hajtják végre, a gépek nem fogják észrevenni azt, hogy ARP-átirányítás van folyamatban, amint az a 10.1. ábrán látható.



10.1. ábra. Beékelődéses támadás: ARP-hamisítás

### Az IP-hamisítás szerepe a beékelődéses támadás során

Az IP-cím hamisításának is fontos szerepe van a beékelődéses támadások során. Ilyen esetben a támadó először feltöri vagy megbénítja a megbízható gépet. Ezután a megbízható gép nevében az Ő forrásdíját feltüntet-

ve küld csomagokat a célgépnek, eljátszva a megbízható gép szerepét, s így töri föl vagy bénítja meg a célgépet is.

### Hátsó ajtók

A hátsó ajtó (*back door*) vagy csapdaajtó (*trap door*) egy adott programhoz, operációs rendszerhez vagy hálózati szolgáltatáshoz való titkos kapcsolatteremtési mód. Bizonyos számítógépes játékokban is vannak ilyenek elhelyezve, amikor valamilyen billentyűkombináció vagy kulcsszó hatására korlátozás nélkül pénzhez, erőhöz, fegyverhez, egészséghoz vagy más erőforráshoz jut a játékosunk. A hátsó ajtók lehetnek véletlenül vagy szándékasan megnyitva, akár a felhasználók által, akár a program tervezésénél fogva. Az alábbi okok miatt jöhet például létre:

- Szándékasan helyezik el a rendszer fejlesztői azért, hogy a fejlesztés során gyorsan hozzáférhessék a rendszerhez, ám azt a kibocsátás előtt elfelejtik hatástanítani.
- Egy alkalmazott helyezi el a kötelességeinek hatékonyabb teljesítése közben azért, mert a „helyes eljárás” szerinte nehezebbé teszi a munkáját, ezért lennie kell egy gyorsabb és ügyesebb módszernek is. A felhasználók technikailag nincsenek annyira felkészülve, mint az IT-csoport emberei, és gyakran éppen azért találnak hátsó ajtókat, mert nincsenek előzetes elképzeléseiük arról, valaminek miként is kellene működnie.
- Az „alapértelmezett” operációs rendszer egyes részei, amelyeket elfelejtettünk az operációs rendszer „megedzése” során védettebbé tenni – ilyen lehet például egy alapértelmezett felhasználónév–jelszó pár. A gyártók minél kevesebb technikai támogatást kérő hívást akarnak látni, ezért minden annyira egyszerűvé és nyílttá tesznek, amennyire csak lehetséges. Ez azt jelenti, hogy az IT-csoportnak minden egyes szervert át kell vizsgálnia, és meg kell azt „edzeni”, vagyis el kell rajta végezni az összes ajánlott biztonsági óvintézkedést.
- Elégedetlen alkalmazottak által elhelyezett hátsó ajtók, amelyen kilépésük után is be akarnak lépni a rendszerbe. Az alkalmazott a legtöbbször érzi, hogy hamarosan el fogja veszíteni a munkáját. Ez könnyen dühbe hozhatja, nem kellőn méltányoltnak érzi magát, ezért biztos akar lenni abban, hogy idővel majd visszavághat.
- Ártó szándékú kód végrehajtása miatt létrejövő hátsó ajtók. Ilyenek a vírusok vagy a trójai programok, amelyek az operációs rendszer vagy egy alkalmazás sebezhetőségét használják ki.

Amint arról már korábban is volt szó, ezek a támadási formák és eszközök csupán a támadók által használt leggyakoribb módszerek. Megértesük könnyebben érthetővé teszi a későbbi pontokban tárgyalt technikák és eszközök megismerését.

## Különböző más támadások

Ebben a pontban a kevésbé elterjedt, esetleg egyedi támadási fajták közül mutatunk be néhányat.

### „Land” támadás

„Land” támadásnak (*land attack*) nevezük azt az IP-cím-hamisítás jellegű támadást, amikor az IP-csomag forrás- és a célcíme megegyezik. Ez egyes TCP/IP-alkalmazások összeomlását okozhatja, mert nem tudják, hogyan lehet kezelni az ilyen csomagokat. A valóságban ritkán megfigyelhető támadási forma, de számos támadásfelismerő és -elhárító eszköz minta-adatbázisa tartalmazza.

### Karácsonya támadás

Ezen támadási fajta esetén bármely ismert szolgáltatás végpontjára olyan TCP-csomagot küldenek, amelynek valamennyi kódjelzője be van kapcsolva. Alternatív módja a támadásnak, ha egyik jelző sincs beállítva.

### Könnyccsepp támadás

A könnyccsepp támadás (*teardrop attack*) széttördelt UDP-csomagokat használ. Az első töredék még helyes, de a többi minden felülírja az előző egy részét. Ez memóriahibához vezet, amitől a rendszer összeomlik.

### Ping-pong támadás

Két fajtája ismeretes:

- Hamisított, a visszajelző szolgáltatásnak (heteros végpont) címzett csomagok áradata. Ennek a szolgáltatásnak egyetlen feladata, hogy minden kapott csomagot visszaküldjön az eredeti feladónak.
- Hamisított UDP-csomag küldése úgy, mintha azt a karaktergenerátor szolgáltatás küldte volna egy másik rendszer visszajelző szolgáltatásának. A karaktergenerátor bármely kapott csomagra úgy válaszol, hogy visszaküld az eredeti feladónak egy 0 és 512 bájt közötti hosszúságú, véletlenszerűen előállított karakterszorozatot (lásd RFC 864). Ha tehát a támadás miatt a kapcsolat egyszer kialakult, akkor létrejön egy hurok, és egymásnak küldözgetik a csomagokat.

**10.**

Mindkét támadás a CPU-erőforrásokat igyekszik elfogyasztani. Ha kellően erős, a támadás könnyen vezethet a CPU túlterhelődéséhez, s végül a rendszer összeomlásához.

### Halálra pingetés

Akárcsak a könnyccsepp támadás, ez is az IP-csomag feltördelési módszérének sebezhetőségét használja ki. A támadó gép küld egy ICMP vissza-

jelzés kérést, ám a csomag mérete meghaladja az IP-távadat csomag maximális 65 535 bájtos méretét, amely nyilván több töredékként fog kézbesítődni. A támadott gép elkezdi összeállítani a teljes (túlméretes) csomagot, és ezzel hamarosan túlcordul a puffere, amitől a rendszer összeomlik.

### **SYN Flood (SYN elárasztásos) támadás**

Minden TCP kapcsolatfelvételi (SYN) kérés esetén a szervernek a kapcsolathoz le kell foglalnia bizonyos erőforrásokat. A támadás úgy működik, hogy hamisított IP-címekről (ezek lehetnek nyilvános vagy privát címek egyaránt) SYN-kérések tömegét küldik a szolgáltatónak. A szerver fogadja ezeket a SYN-kéréseket, és választ is küld ezekre a címekre, de onnan a valóságban soha nem küldtek ilyen kérést, így azok a választ maguk is támadásnak vélték, egyszerűen eldobták. A rendszertől függetlenül a kapcsolati időzítő egy-három percig várakozik, mielőtt felszabadítána az ekkor lefoglalt erőforrásokat, miközben a SYN-ACK válaszra adott harmadik nyugtázás csupán néhány ezredmásodperc lenne. A SYN-kérések nagy számával való elárasztás megtöltheti a szerver kapcsolati várósorát a be nem fejezett kapcsolatfelvételi kísérletekkel, így az nem lesz képes fogadni a valós felhasználói kéréseket.

### **Tűzjárás**

Sokan úgy vélik, hogy a tűzfalak ellenállóak a támadásokkal és a hagyományos technikákkal szemben, amelyekkel a támadó a tűzfalon beállított szabálykészletet igyekezne kipuhatalni. Ez a hiedelem egy darabig igaz is volt; új technikák azonban állandóan születnek. Ilyen a **tűzjárás** (*firewalking*) is – egy olyan technika, amely lehetővé teszi a támadó számára, hogy mesterségesen fabrikált csomagokat küldjön keresztül a tűzfalon, ezzel felderítve, hogy mely végpontok és szolgáltatások juthatnak rajta keresztül. Ezzel a tudással felvértezve a támadó később rejttet módon elvégezhet egy portletapogatási támadást, feltérképezve ezzel a tűzfal mögötti hálózatunkat.

A tűzjárás azért működhet, mert az IP-csomagok fejrészében található egy bizonyos mező, amely azt hivatott megakadályozni, hogy egy adott csomag állandóan a hálózaton keringjen. Ezt a mezőt nevezzük életidőnek (*TTL – time to live*). Amikor ez a mező nulla, a csomag megsemmisítésre kerül. A tűzjárás esetén ezt a mezőt olyan értékűre állítja be a támadó, hogy az még éppen átjusson a tűzfalon, de a megszólított szolgáltatás vagy gép már megsemmisítse. Ez azért hasznos a támadó számára, mert a mező értékének vizsgálata egyike a legelsőnek elvégzett feladatoknak a csomag feldolgozása során, és amennyiben megsemmisítésre kerül, akkor az eredeti feladó visszajelzést kap erről anélkül, hogy magát a csomagot a célpont valaha is megpróbálta volna feldolgozni.

A továbbiakban a biztonság kiértékeléséről és az áttörhetőség ellenőrzéséről lesz szó.

## 10.2. A BIZTONSÁG KIÉRTÉKELÉSE ÉS AZ ÁTTÖRHETŐSÉG ELLENŐRZÉSE

A biztonsági szolgáltatásokat nyújtó cégek legtöbbjének van egy biztonságkiértékelő szolgáltatása is, amely az első lépés a kliens hálózatának biztonságossá tételere. Ez a technika rendkívül hasznos akkor, ha a kliens meg akarja ismerni a hálózatában telepített biztonsági-védelmi rendszerek hatékonyságát. Erősen ajánlott az a gyakorlat, hogy vállalaton kívüli emberekkel évente végeztessünk el egy ilyen kiértékelést. Ez az egyetlen objektív és valós kiértékelése a biztonságnak, amely őszinte választ adhat a „biztonságban vagyok-e” kérdésre. Mivel új és új sebezhetőségek szinte naponta derülnek ki, ezért a hálózatot is kellő gyakorisággal kell vizsgálni, másként a védelem egy idő után elégtelenné válhat. A biztonsági kiértékelésnek az alábbi típusai léteznek:

- a belső sérülékenység és áttörhetőség ellenőrzése,
- a külső sérülékenység és áttörhetőség ellenőrzése,
- a fizikai biztonság kiértékelése.

Mielőtt megkezdené a biztonság kiértékeltetését, célszerű jobban megismerni a megbízni óhajtott szolgáltató által alkalmazott eljárásokat és folyamatokat. Mivel túlságosan is sok olyan biztonsági cég van, amely nem kellő gondossággal elvégzett munkájával az ön hálózatának biztonságát veszélyezteti, így a következőket érdemes állandóan szem előtt tartani:

*Ismerje meg a biztonsági kiértékelési tervet. Ha nincs ilyen terv, vagy az nem érhető, akkor a tényleges hálózati sérülékenységek kiértékelése akár kárt is okozhat a hálózaton. Meg kell kötni a jogilag is helyes és részletekbe menő szerződést azzal kapcsolatban, hogy mi az ellenőrzés célja és milyen mélységekig lehet el. Ez minden felet védi. Végül nagyon fontos a kiértékelés sikereségének kritériumát is meghatározni, hogy minden felelősségben részesített fél pontosan mit is kell elérni.*

10.

A következő részben megvizsgáljuk a kiértékelés ajánlott módszereit, és mindegyik alkalmazott technika esetén megtárgyaljuk annak a hálózatbiztonsági értékét is.

### 10.2.1. A BELSŐ SÉRÜLÉKENYSÉG ÉS ÁTTÖRHETŐSÉG ELLENŐRZÉSE

Az FBI által nemrég elvégzett felmérés szerint napjaink vállalkozásaiban a hálózatbiztonsági kockázatok 60 százalékánál is több ered a belső fel-

használóktól, illetve folyamatoktól. Ez adódhat a hibás hálózatieszközbeállításból, a hatékony védelmi eljárások hiányából és elavult vagy frissítlen szoftver használatából egyaránt. A biztonsági tanácsadóknak fel kell ismerniük ezeket a kockázatokat annak érdekében, hogy meghatározhassák a hálózat szándékos vagy véletlen támadásokkal szembeni sebezhetőségét.

Napjainkban a cégek nehéznek találhatják, hogy az alkalmazásokban és operációs rendszerekben naponta felfedezett számos új és újabb sebezhetőség ellenére minden a lehető legfrissebb védettségű rendszerrel rendelkezzenek. A biztonsági tanácsadóknak minden ismerniük kell a legfrissebb sebezhetőségeket, és képesnek kell lenniük arra, hogy a megrendelő rendszerének belső hálózatbiztonsági mechanizmusok állapotai kiértékelésében segédkezet nyújtsanak. Képesnek kell lenniük arra is, hogy a vállalat biztonsági céljait előmozdító megfelelő további javító lépések megtételére javaslatot tehessenek.

### A kiértékelés módszertana

A belső hálózatbiztonsági kiértékelést a saját telephelyen kell elvégezni. A figyelemnek elsősorban a szabályzatokkal, eljárásokkal, valamint hálózati gépekkel és alkalmazásokkal kapcsolatos biztonsági kockázatokra kell irányulnia. A biztonsági tanácsadónak legalább az alábbi munkát el kell végeznie:

- Össze kell gyűjtenie a megrendelő által nyújtott hálózati információt (ha van ilyen).
- Össze kell gyűjtenie és dokumentálnia kell a nyilvánosan elérhető információkat a hálózatról azért, hogy a megrendelő azt átnézhesse, hiszen a támadó legalább ennyit bármikor megtudhat.
- Hálózatfeltérképező technikákat kell alkalmaznia a hálózat topológiájának és fizikai tervezésének meghatározásához.
- A hálózati alkalmazások szondázása és letapogatása.
- Az operációs rendszerek nyomelemzése és sérülékenységeik feltérképezése a sebezhető gépek kiszűréséhez.
- A forgalmi minták és folyamok azonosítása, és összehasonlítása a vállalati tevékenységből eredő várható forgalommal.
- A potenciálisan gyenge felhasználóazonosító rendszerek detektálása. Ilyenek például azok, amelyekben a felhasználó soha nem kényszerül (vagy nem is tud) jelszót változtatni, de ilyenek a nem biztonságos vezeték nélküli hálózatok is.
- Sebezhetőségi vizsgálatok nyilvánosan elérhető, saját, és testreszabott eszközök használatával.
- Kézzel ellenőrizni valamennyi felismert sérülékenységet azért, hogy hamis riasztásokat ne jelentsen.

- Megfigyelni a belső biztonsági gyakorlatokat és szabályzatokat a teljes hálózatban.
- Elvégezni a gyűjtött információ analízisét, és leszűrni belőle a további lépéshoz szükséges ajánlásokat.

A belső kockázatelemzés végterméke egy olyan dokumentum, amely tartalmazza a kiértékelés módszertanát, az elvégzett munkát, és minden egyes rendszerről tartalmazza a szükséges részleteket, beleértve a támadásokkal szemben nagyobb kockázatot jelentő rendszereket is, valamit a felismert sebezhetőségek részletes listáját. Az elemzés záródokumentuma tisztább képet ad a hálózat felépítéséről és a biztonsági kockázatokról. Tartalmaznia kell továbbá az elvégzett munkák eredményét, és minden egyes ellenőrzési fázis esetén a szükséges javítások megtételével kapcsolatos következtetéseket, és ezek egymáshoz képest meghatározott fontossági sorrendjét. A dokumentumban természetesen szerepelniük kell a felfedett hálózatbiztonsági kockázatok mérséklésének költséghatékony módon való elvégzéséről szóló ajánlásoknak is.

## 10.2.2. A KÜLSŐ SÉRÜLÉKENYSÉG ÉS ÁTTÖRHETŐSÉG ELLENŐRZÉSE

Amint a hagyományos vállalkozások egyre jobban elosztottá válnak a szervezet földrajzi értelemben vett különböző telephelyei között, a külső támadások veszélye is növekszik. A kockázatot csak tovább növeli a helytelenül beállított tűzfalak és útválasztók, valamint a nem biztonságos, elavult vagy hibásan konfigurált webalapú alkalmazások használata.

Napjaink kis- és közepes vállalkozásai meglehetősen nehezen képesek lépést tartani az operációs rendszerekben és alkalmazásokban naponta felfedezett új és új sérülékenységekkel. A Granite Systems (<http://www.granitesystems.net>) egy világszínvonalú biztonsági cég, amely pontosan ismeri a legújabbakat is. Képesek segíteni önt a jelenlegi hálózati határok védelmi mechanizmusainak állapotfelméréseiben, és lépésekkel tudnak ajánlani szervezetének biztonsági szempontból történő további megújítására.

10.

### A kiértékelés módszertana

A hálózat külső áttörhetőségi és sebezhetőségi kiértékelését azokon a helyeken kell elvégezni, ahol az érintkezésbe kerül a külvilággal. Ez történhet internetkapcsolaton, telefonos vagy vezeték nélküli csatlakozáson, vagy más távoli hozzáférési helyen egyaránt. Ezen kiértékelés célja annak meghatározása, hogy hol és mennyire kitett a hálózat a kívülről jövő támadásokkal szemben.

Számos esetben a külső és a belső kiértékelés ugyanazon típusú dolgozat vizsgálja. A különbség a megközelítésben van, illetve a külső kiértékelés esetén kívülről vizsgáljuk azt, hogy mit is lehet felfedezni. A következő lista foglalja össze a külső kiértékelés során elvégzendő munkákat:

- Össze kell gyűjteni a megrendelő által nyújtott hálózati információt (ha van ilyen).
- Össze kell gyűjteni és dokumentálni kell a nyilvánosan elérhető információkat a hálózatról azért, hogy a megrendelő azt átnéhesse, hiszen a támadó legalább ennyit bármikor megtudhat.
- Lopakodó hálózatfeltérképező technikákat kell alkalmaznia a hálózat topológiájának és fizikai tervezésének meghatározásához, és annak megfigyeléséhez, hogy ezek a szimulált támadások észlelhetők-e.
- A hálózati alkalmazások szondázása és letapogatása.
- Az operációs rendszerek nyomelemzése és sérülékenységeik feltérképezése a sebezheto gépek kiszűréséhez.
- A forgalmi minták és folyamok azonosítása és összehasonlítása a vállalati tevékenységből eredő várható forgalommal.
- A potenciálisan gyenge felhasználóazonosító rendszerek detektálása. Ilyenek például azok, amelyekben a felhasználó soha nem kényszerül (vagy nem is tud) jelszót változtatni, de ilyenek a nem biztonságos vezeték nélküli hálózatok is.
- Sebezhetségi vizsgálatok nyilvánosan elérhető, saját és testreszabott eszközök használatával.
- Kézzel ellenőrizni kell valamennyi felismert sérülékenységet azért, hogy hamis riasztásokat ne jelentsen.
- Elvégzni a gyűjtött információ analízisét, és leszűrni belőle a továbblépéshez szükséges ajánlásokat.

A külső áttörhetőségi és sebezhetségi kiértékelés végdokumentuma megegyezik a belső kiértékelés dokumentumával, de az egyes témaöröket a külső kockázatok szempontjából tárgyalja. Jóllehet a fejezetben elválasztottuk a külső és belső kiértékelést, valójában ezeket legjobb egyszerre végezni. Ez fog a hálózat minden szempontból felmért biztonságáról tisztább képet nyújtani.

### 10.2.3. A FIZIKAI BIZTONSÁG KIÉRTÉKELÉSE

A könyv elsősorban a hálózatok logikai biztonságára összpontosít, amely azonban a biztonsági kiértékelésnek csupán egy része. Számos vagyontárgy azonban fizikailag is megfogható és megrongálható, valószínűleg sokkal durvább és kevésbé ravasz módon, mint amelyekről szót ejtettünk

eddig. Tegyük fel például, hogy az összes IT-eszközünk olyan helyiségben van elhelyezve, amely beépített vízbefecskendezéses tűzoltó rendszerrel van ellátva. Ha ez így van, akkor nincsenek igazán biztonságban, mivel az elektronikai eszközök és a víz nem jól vegyülnek egymással. A legegyszerűbb szolgáltatásmegtámadás az épület tűzjelzőjének beindítása lenne, s csak hagyni kell, hogy a víz végezze el a többet. Már csak abban reménykedhet, hogy legalább a szalagos mentéseit vízbiztos helyen tárolja, és kellően frissek is...

Jóllehet a digitális korban élünk, napjaink IT-rendszeri azért még mindig fizikai helyen vannak elhelyezve, és fizikai berendezéseket használnak. A megfelelő fizikai biztonsági mechanizmusok nélkül az üzemebe helyezett összes többi védelmi rendszer könnyedén áttörhető. Amint a szervezet információinak érzékenysége növekszik, a fizikai biztonság iránti igény egyre nagyobb lesz. Mi értelme is lenne a legújabb tűzfal-, IDS- és VPN-technológiák alkalmazásának, ha bárki által hozzáférhető helyen tartjuk a berendezéseket?

A fizikai biztonságot ellenőrző módszerek lehetnek elrettentő és feldeírő jellegűek egyaránt, amelyeket arra terveztek, hogy csökkentse a szervezet fizikai támadásoknak való kitettségét. A fizikai biztonsági kockázat kiértékelése segítheti a vállalatot abban, hogy költséghatékony módon megtervezze és implementálja a lehetséges támadók elrettentését és felfedezését szolgáló eszközöket, monitorozza a gyanús jelenségeket, végső soron így védelmezve az értékes vállalati erőforrásokat feltörésük, megsemmisítésük és megváltoztatásuk ellen.

### A kiértékelés módszertana

A fizikai biztonsági kockázatelemzést a vállalat telephelyén kell elvégezni, elsősorban a fizikai biztonsági intézkedésekre és a fizikai természetű belső gyakorlatra összpontosítva, amelyek a hálózati erőforrások fizikai védelmét látják el. A következő feladatokat mindenkorban el kell végezni:

10.

- Megfigyelni az épület bejutási pontjait és az elhelyezett őröket.
- Megfigyelni a fizikai biztosítóberendezéseket, mint például a zártláncú kamerákat, a csomagvizsgálatot és a látogatóbejelentkezési eljárást.
- Felülvizsgálni az IT-erőforrások fizikai védelmét ellátó mechanizmusokat, valamint a papíralapú feljegyzések védelmét is.
- Meghatározni az IT-felszerelés közvetlen fizikai védelmét biztosító mechanizmusokat, például a bejutás elleni védelmet, a cserélhető adathordozókat fogadó eszközök zárhatoságát, redundáns feszültségellátást és védett adatkommunikációs csatornákat.
- Megfigyelni az alkalmazottak szokásait, mivel ez kihat a fizikai biztonságra.

- Megfigyelni a kritikus adatokat tartalmazó anyagok fizikai megsemmisítésének folyamatát (idézzük fel a kukabúvárkodásról mondottakat).
- Ajánlásokat adni az IT-erőforrások fizikai behatások elleni védelmének javítására.
- Megismerni a mentési eljárásokat és a kritikus adatok tárolási módszertét.
- Megvizsgálni az üzemeltetők és a látogatók bejutási szabályait (ha ilyenek vannak), ezen keresztül vizsgálva meg az idegenek kezelését.

A fizikai kockázatelemzés végterméke egy dokumentum, amely tartalmazza a követett módszertan leírását, a végrehajtott feladatokat és ezek eredményeit, valamint a felfedett fizikai biztonsági kockázatok mérséklésének költséghatékony módon való elvégzéséről szóló ajánlásokat.

A fenti kiértékelés nem automatizálható, ha bármilyen ésszerű végeredményt akarunk belőlük kapni, így ki kell nyitnunk a hálózatunkat és az erőforrásait egy megbízhatónak tartott külső cég előtt. Amikor kiválasztjuk ezt a szervezetet, az alábbiakat kell megkövetelni:

- Tanulmányozni kell a cégek ipari szabványok terén meglévő bizonyítványait. Így lehet biztosítani azt, hogy a hálózat kiértékelését végző személyek megfelelő szakértelemmel rendelkeznek.
- Fel kell venni a kapcsolatot a cégek referenciaival, és el kell nekik mondanival, hogy alkalmazni kívánjuk a céget. Így meg lehet győződni a referenciaik tényleges létezéséről.
- Kérjen tőlük példakiértékeléseket, és tanulmányozza át azokat figyelmesen. Ez viszonylag nehezen végrehajtható, hiszen a kiértékelések gyakran tartalmaznak érzékeny megrendelői adatokat, de bármely biztonsági szolgáltatások nyújtására képes cégnak rendelkeznie kell legalább egy olyan változattal, amely ezeken a részeken fiktív adatokat tartalmaz.
- Az elvárásokat és a teljesítéseket világosan fogalmazza meg a szerződésben, ezzel védve mind saját magát, mind pedig a biztonsági cégek alkalmazottait. Az érthető, világos beszéd a világ problémáinak 99 százalékát megoldaná.
- Kérje meg tárgyalópartnerét a biztonsági cégnél, hogy menjenek végig a kiértékelési eljárás egyes lépésein még az előtt, hogy kijönnének a telephelyre. Ha nem képesek fejből felsorolni a teendőket, akkor nagy valószínűséggel még nem túl régen űzik ezt a mesterséget – esetleg tárgyalópartnere nem biztonsági szakember.

## 10.2.4. KÜLÖNBÖZŐ KIÉRTÉKELÉSEK

A biztonsághoz bizonyos értelemben kötődő más kockázatelemzéseket is érdemes meglemlíteni, hogy szintén megfontolja a végrehajtásukat:

- **Eljárási kockázat elemzése** – Ennek során a biztonsági szakértők átvizsgálják a biztonsági szabályzatokat és eljárásokat, hogy biztosítsák az ajánlott gyakorlatnak való megfelelőségüket. Az ilyen jellegű szabályzatokat és eljárásokat a második fejezetben tárgyaltuk.
- **Katasztrófa-helyreállítási terv** – Amennyiben a vállalata a föld olyan részén található, amelyen gyakran előfordulnak tornádók, hurrikánok, földrengések, villámcsapások, árvizek, tüzek, akár egyedül, akár más csapásokkal társulva, akkor minden nap elmúltával egyre nagyobb szüksége van egy olyan tervre, amely szerint haladva a természeti csapás bekövetkezése után helyreállítható a hálózati infrastruktúrája, és a kritikus adatai.
- **Információkezelési biztonsági kiértékelés** (bankok és egészségügyi intézmények számára) – Amint a pénzügyi és egészségügyi adatok kezelésével kapcsolatos jogi szabályozás szinte évente változik, az ilyen jellegű adatokat kezelő intézményeknek egyre magasabb biztonsági követelményeknek kell megfelelniük, ellenkező esetben akár büntetőjogilag is felelősségre vonhatók.

### Kiértékeléssel foglalkozó cégek

Egyszerű Google keresés, beírva a „security assessment provider” szavakat, kétnyolc milliónál is több találatot eredményez, s ez a szám egyre növekszik. Nemzetközi szinten az alábbi cégek nagyon jó referenciaikkal rendelkeznek:

- Cisco Secure Consulting Services – <http://www.cisco.com/go/security-consulting>
- INGRI – [http://www.ingri.netindex\\_security.html](http://www.ingri.netindex_security.html)
- Aegis Security – <http://www.aegis-security.com>
- Granite Systems – <http://www.granitesystems.net>

A továbbiakban a kiértékelő és sérülékenység-ellenőrző eszközöket tekintjük át, amelyeket a biztonsági kockázatok keresésének automatizálására használhatunk.

## 10.3. SÉRÜLKÖNYNSÉG-ELLENŐRZŐK

Amikor a támadók réseket keresnek a rendszeren, általában jól ismert biztonsági lyukakat és szoftverhibákat keresnek, hogy ezeket támadhas-

sák. Közülük a leggyakoribbakat a könyv korábbi fejezeteiben már tárgyaltuk. Az igazi támadás, amelynek célja a rendszerbe való betörés és a rendszer feletti uralom megszerzése, a támadó által a szervezet biztonságával kapcsolatos lehető legfontosabb és legátfogóbb tudás megszerzésén alapszik. Amikor a támadó elkezdi felderíteni a rendszert, a sebezhető pontokat akarja kihasználni, hogy pontosan meghatározhassa, miként is férjen hozzá az értékes információkhoz.

A sebezhetőségek támadása régebben meglehetősen időigényes folyamat volt, amelyhez a támadó komoly szakértelmére is szükség volt. Ma már az automata eszközök megjelenése ezt megváltoztatta. Annak az időnek már vége, amikor a hatékony támadáshoz a nyilvánosan is elérhető támadókódokat kellett megfejteni, és megfelelő sorrendben végrehajtatni.

Most felmerülhet a kérdés, vajon a kalózok játszotta szerepről beszélek-e, és együttérznek-e velük abban, hogy milyen nehéz volt az adataik megfelelő kezelése, vagy a hálózati adminisztrátorokról, akiknek egy eny nyire csüggesztő feladattal kellett szembesülniük. Tulajdonképpen minden kettőre gondolok, de amit valójában ki szeretnék hangsúlyozni, hogy ez ma már egyáltalán nem probléma. Napjainkban a jól dokumentált támadások készen megszerezhető parancsállományok segítségével zajlanak, a vállalatok pedig a zajló támadások felderítését és a sebezhetőségek felfedését szintén automatikus működésű eszközökkel végzik. Ebben a fejezetben a legátfogóbb ilyen eszközöket vizsgáljuk meg, amelyek a könyvben korábban már említett egyedi eszközökkel együtt használva kitűnő lehetőséget nyújtanak a hálózat sebezhető pontjainak felderítésére, majd megerősítésükre.

### 10.3.1. A SÉRÜLKENYSÉG-ELLENŐRZŐK JELLEMZŐI ÉS ELÖNYES

A biztonsági letapogatásokat és sebezhetőségi kiértékeléseket végző alkalmazások a letapogatást és a szükséges számításokat a háttérben végzik. A hangsúly nem azon van, hogy miként lehet felismerni a sebezhetőséget, hanem hogy mi az, ami sebezhető. Az ilyen letapogatóeszközök értéke az alábbi négy kategóriába rendezhető:

- **Letapogatási és érzékelési pontosság** – A letapogatásnak és a jelzett sebezhetőségeknek a lehető legkevesebb hamis jelzés mellett pontosaknak kell lenniük. Hamis jelzés az elfogadott tevékenységre vagy konfigurációra tévedésből adott jelzés. Ennek az ellenkezője szintén igaz – a hamis hallgatás is rossz – vagyis ha a rendszer nem ad jelzést az el fogadható állapotról vagy tevékenységről.

- Dokumentáció és támogatás** – Világosnak, tömörnek, olvasmányosnak és könnyen érhetőnek kell lennie. Ideértendő a készített listák leírása, valamint az alkalmazás működésének ismertetése is, hogy a felhasználók megérthessék, miként is működik a program, és milyen információkat tud kiírni.
- Jelentések** – A sérülékenység-ellenőrző eszköz legfontosabb előnye az, hogy használatával megtudhassuk, egy adott sebezhetség felfedezése után mit tehetnénk az elhárítására; éppen ezért a nyomtatásnak testreszabhatónak és pontosnak kell lennie.
- Sebezhetség frissítése** – Állandóan új és új sebezhetső pontokra derül fény, és napjaink technológiai lehetőségeit figyelembe véve a programnak képesnek kell lennie arra, hogy az új résekre kiadott információkat automatikusan letöltsse, és attól kezdve felismerje.

A következő pontban megismerjük a piacon jelenleg megtalálható két legnépszerűbb sérülékenység-ellenőrző szoftvert.

### 10.3.2. NESSUS

A Nessus a sebezhetség-ellenőrzők között olyan, mint a Snort a behatolásérzékelők között: egy nyílt forráskódú alkalmazás, amelyet az internetes önkéntesek egy csoportja támogat. Bővebb információ a <http://www.nessus.com> webhelyen található.

#### Önjellemzés

Az alábbi szöveg a Nessus honlapról elérhető adatlap egy részének magyar fordítása:

*A Nessus projekt célja az internetközösség által elérhető ingyenes, nagy tudású, naprakész és könnyen használható sérülékenység-ellenőrző létrehozása. Lehetővé teszi egy adott hálózat távoli átvizsgálását, kisszürendő, hogy a gonoszok (vagyis a gépkálozok) képesek lehetnek-e betörni rá, vagy bármilyen módon visszaélni vele.*

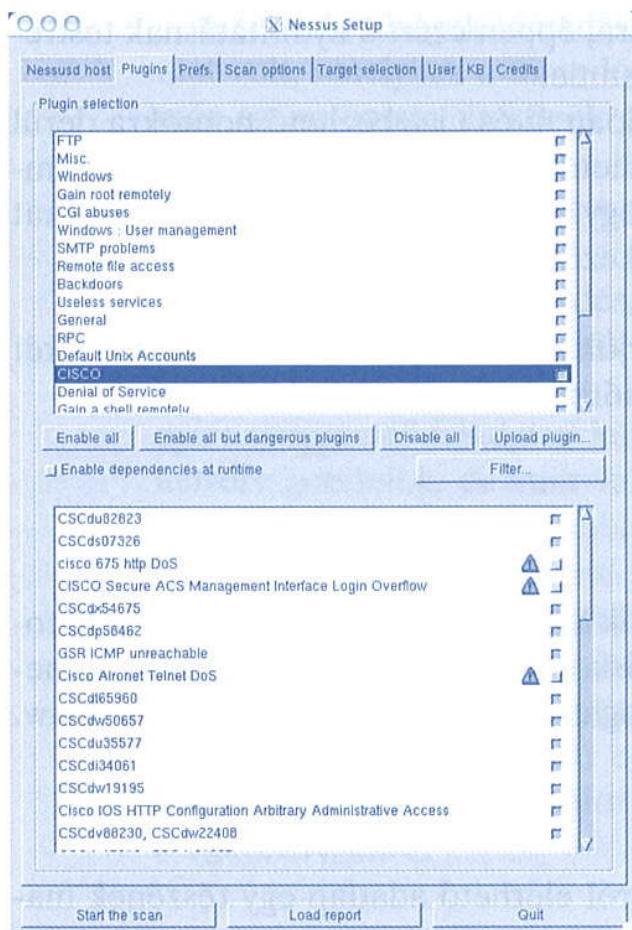
*Számos más biztonsági ellenőrzővel ellentétben a Nessus semmit nem tekint eleve adottnak. Ez például azt jelenti, hogy nem feltételezi egy adott szolgáltatásról, hogy kizárálag a hozzárendelt végponton szolgáltat. Ha például a webszerver az 1234 végponton szolgáltatna, a Nessus ott is meg fogja találni, és ellenőrizni fogja a biztonságát. A biztonsági ellenőrzést sem csupán a távoli szolgáltatás verziószámának ellenőrzésével végzi, hanem ténylegesen meg fogja kísérelni a sebezhetső pont kihasználását.*

#### Felderítési és észlelési pontosság

A letapogatásnak és a jelzett sebezhetségeknek a lehető legkevesebb hamis jelzés mellett pontosaknak kell lenniük. Hamis jelzés az elfogadott tevékenységre vagy konfigurációra tévedésből adott jelzés. Ennek az el-

lenkezője szintén igaz – a hamis hallgatás is rossz –, vagyis ha a rendszer nem ad jelzést az el nem fogadható állapotról vagy tevékenységről.

A programnak a sérülékenységek felderítésével kapcsolatos képességei kitűnők, és az általa megtalált sebezhető pontokról szóló értesítései igen pontosak. Lévén nyílt forráskódú szoftver, állandóan figyelik, tesztelik, tanulmányozzák és fejlesztik. Mivel ennyire kirakatban van, könnyen átkonfigurálható azok számára, akik megértik az alapelveit. A 10.2. ábrán láthatjuk a program beállítási képernyőképét, amelyen felfedezhető, menynyire rugalmas, erős, és milyen sok kiválasztható képességgel rendelkezik.



10.2. ábra. A Nessus program beállítási képernyője

akkor meg kell birkózni azzal a tényel, hogy az a kevés, ami le van írva, az programozók által íródott. Ha valaha megpróbálta már elolvasni a Linux elektronikus kézikönyv oldalait (*man pages*), akkor érti meg igazán, mire próbálom felhívni a figyelmet.

A technikai támogatás szempontjából fontos, hogy lévén nem vállalkozás, a Nessus programhoz nincs egy hivatalos technikai támogatási telefonszáma vagy weboldala. Létezik azonban a Nessus fejlesztői mag által sűrűn látogatott levelezési lista, amely rendkívül nagy segítség lehet.

## Jelentések

A sérülékenység-ellenőrző eszköz legfontosabb előnye az, hogy használataval képesek legyünk megtudni, egy adott sebezhetőség felfedezése után

## Dokumentáció és támogatás

A dokumentációnak világosnak, tömörnek, olvasmányosnak és könnyen érthetőnek kell lennie. Ideértendő a készített listák leírása, valamint az alkalmazás működésének ismertetése is, hogy a felhasználók megérthessék, miként is működik a program, és milyen információkat tud kiírni.

A program dokumentációja egyszerre kiváló, átlagos és nagyon gyenge. Ha egy laptopon akarja első ízben installálni, akkor néhány kitűnő dokumentációforrás segítségével minimális idegeskedéssel képesek leszünk rá.

Ha a dokumentációjából azt kívánjuk megérteni, hogy miként működik a program, vagy egyáltalán mire képes,

akkor meg kell birkózni azzal a tényel, hogy az a kevés, ami le van írva, az programozók által íródott. Ha valaha megpróbálta már elolvasni a Linux elektronikus kézikönyv oldalait (*man pages*), akkor érti meg igazán, mire próbálom felhívni a figyelmet.

mit tehetnénk az elhárítására; éppen ezért a nyomtatásnak testreszabhatónak és pontosnak kell lennie.

A program a nyomtatásokat számos különböző formátumban képes előállítani, melyek közül talán a leghasznosabb a HTML. Az ilyen formátumú nyomtatás tele van követhető hivatkozásokkal, amelyekről megismerhető a felfedett sebezhető pont teljes analízise, a hálózatra vetített kockázati szintje, s mindez kitűnő ábrákkal tarkítva, hogy a sérülékenység szemléletes legyen. Hátránya azonban, hogy a nyomtatások UNIX-centrikusak, és tele vannak fogalmazási és helyesírási hibákkal, vagyis további szerkesztés nélkül nem adható ki a kezünkön. Az információ pontos, csak nem csilllog-villog úgy, mint egy kereskedelmi termék esetén kellene.

### Sebezhetőségi frissítések

Állandóan új és még újabb sebezhető pontokra derül fény, s napjaink technológiai lehetőségeit figyelembe véve a programnak képesnek kell lennie arra, hogy az új résekre kiadott információkat automatikusan letöltsse, és onnantól felismerje.

A program parancsállományok segítségével frissíthető, akár automatikusan is, így biztosítva a legfrissebb sebezhetőségi minták letöltését. Jól lehet a Nessus nem fut Windows alatt, létezik azonban hozzá egy Windows-kliens, amellyel a Nessus-szerverekhez lehet csatlakozni, hogy az ellenőrzés távolról is futtatható legyen.

A program egy nagyon jó sérülékenység-ellenőrző szoftver, amelynek nyílt forráskódú állapotából következően kivételes képességei vannak. Számos vele kapcsolatos kitűnő forrás létezik. További hivatkozások a következő helyeken találhatók: <http://www.securityprojects.org/nessuswx>, <http://list.nessus.org>.

A Nessus ingyenesen elérhető szabad szoftver, amelyet nem kell megvásárolni, és nyílt forráskódú. Ez azt jelenti, hogy kiválóan alkalmas a hálózati adminisztrátorok számára, akik nem akarják a szervezet pénzét feleslegesen költeni. Ez azonban azt is jelenti, hogy a szomszédunkban lakó támadónál a sarokban heverő öreg számítógépre is feltelepíthető egy Linux operációs rendszer (ingyen), és a Nessus (szintén ingyen). Ezek után a szintén ingyen végezhető sebezhetőségi ellenőrzés már a hálózatunk ellen irányulhat.

10.

### 10.3.3. RETINA

Ez a biztonsági ellenőrző program az eEye biztonsági termékeinek zászlóshajója. A vállalat a Microsoft termékcsaládjainak biztonságát növelő számos terméket forgalmaz. Magáról a Retina programról a <http://www.eeye.com> webhelyen lehet többet megtudni.

## Önjellemzés

A következő szöveg az eEye vállalat honlapjáról származik, amelyben ők maguk így írják le a hálózati sérülékenység-ellenőrző terméküket, a Retinát:

*Az eEye Digital Security cég által kifejlesztett Retina hálózati sérülékenység-ellenőrző szoftver a Network World folyóirat által legelső helyre sorolt sérülékenységérzékelő szoftver, amely a gyorsaság, a használhatóság, a nyomtatási és háttérbe húzódási, valamint a fejlett sérülékenységfelderítő képességek mércéjévé vált.*

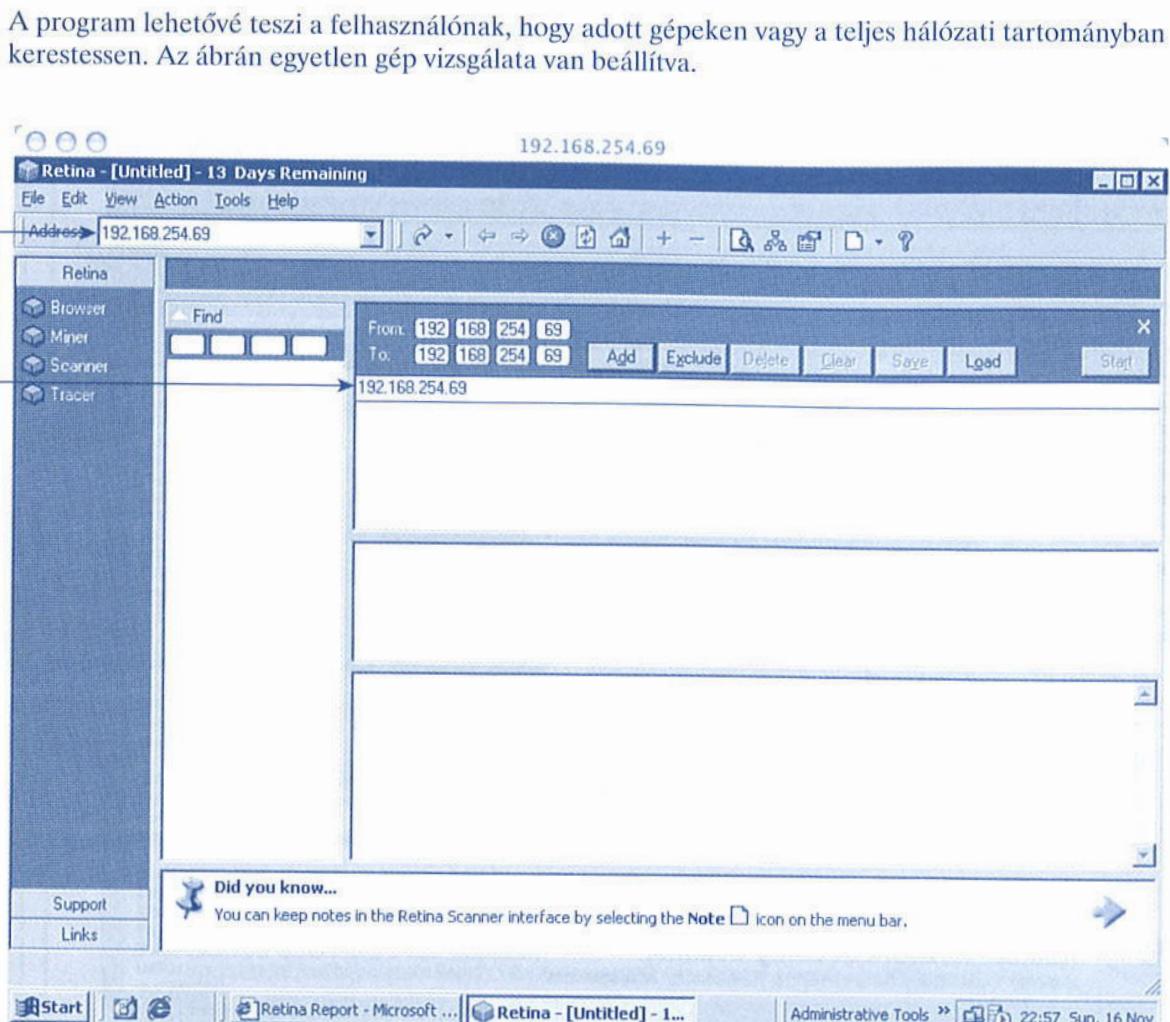
*A program képes a hálózat valamennyi gépét ellenőrizni, beleértve számos különböző operációs rendszert (például Apple, Windows, UNIX, Linux), hálózati eszközöt (kapcsolókat, tűzfalakat, útválasztókat stb.), adatbázisokat és harmadik fél által gyártott, illetve saját fejlesztésű alkalmazásokat is, valamennyit rekordidő alatt. Az ellenőrzés után átfogó nyomtatást állít elő a selfedezett sebezhető pontokról, mellékelve a megfelelő javítási lehetőségek és frissítések listáját is.*

*Az eEye egy elismert, digitális biztonsági kutatásokat folytató intézet. Ennek eredményeként a Retina program is magában foglalja a legátfogóbb és legfrissebb sérülékenységi adatbázist – amely minden Retina ellenőrzési munkamenet elején automatikusan letöltődik. A felismert sebezhetőségek lehető legfrissebb adatbázisa alapján végzett ellenőrzés mellett a felhasználók saját testreszabott vizsgálatokat is végezhetnek a programmal. Az egyedi, mesterséges intelligenciával kiegészített opción (CHAM) segítségével a hálózaton belüli, korábban még nem ismert biztonsági problémák után is lehet vele kutatni.*

## Felderítési és észlelési pontosság

A letapogatásnak és a jelzett sebezhetőségeknek a lehető legkevesebb hamis jelzés mellett pontosaknak kell lenniük. Hamis jelzés az elfogadott tevékenységre vagy konfigurációra tévedésből adott jelzés. Ennek az ellenkezője szintén igaz – a hamis hallgatás is rossz –, vagyis ha a rendszer nem ad jelzést az el nem fogadható állapotról vagy tevékenységről.

A program a felderítés menetét egy kiváló megjelenítő felületen teszi láthatóvá, amely gyakorlatlan felhasználók számára is könnyen kiismerhető, s amely számos más olyan eszköz elérését is lehetővé teszi, amelyek képességei messze túlmutatnak egy sebezhetőségi felderítő eszközén. Egyik legjobb tulajdonsága az egyedi igényekhez való könnyű beállíthatósága, az időzített keresési lehetőség, valamint a behatolási naplók testreszabhatósága. Különösen egyedi a különböző eszközök számára az eltérő keresési lehetőségeket előíró felderítési szabályok létrehozhatósága. Így például az internetről is látható szervereket másként lehet ellenőriztetni, mint a felhasználói gépeket. A 10.3. ábrán látható a program felderítést indító képernyője, amellyel megközelíthető egy adott eszköz, vagy egy teljes hálózat egyaránt.



10.3. ábra. A vizsgált terület kiválasztása a Retina programban

### Dokumentáció és támogatás

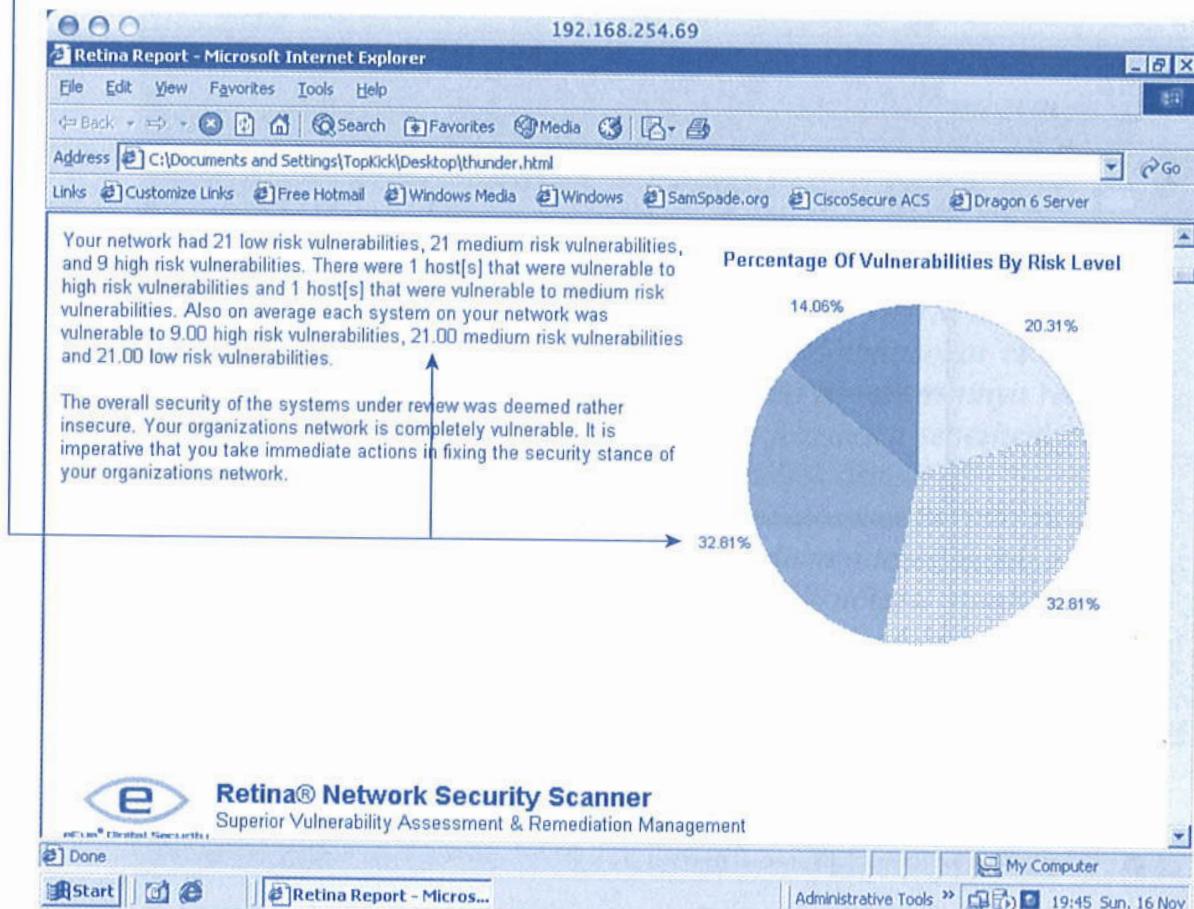
A dokumentációnak világosnak, tömörnek, olvasmányosnak és könnyen érthetőnek kell lennie. Ideértendő a készített listák leírása, valamint az alkalmazás működésének ismertetése is, hogy a felhasználók megérthesék, miként is működik a program, és milyen információkat tud kiírni.

A Retina dokumentációja egy Windows segítségnyújtó állományban található, amely meglehetősen teljesnek tűnik, és az átlagos felhasználóban felmerülő legtöbb kérdésre választ ad. Nincsenek benne alaposabban a részletekbe menő „miként csináljuk” részek, de elegendő példát tartalmaz ahhoz, hogy hiányuk ne jelentsen akadályt. Létezik egy web alapú űrlap is, amelyet az eEye technikai segítségnyújtó ügyfélszolgálata kap meg, a felhasználók számára biztosítva néhány támogatási lehetőséget.

### Jelentések

A sérülékenység-ellenőrző eszköz legfontosabb előnye az, hogy használatával képesek legyünk megtudni, egy adott sebezhetőség felfedezése után mit tehetnénk az elhárítására; éppen ezért a nyomtatásnak testreszabhatónak és pontosnak kell lennie.

A program által felfedett sebezhető pontokat egy képernyőn összegzi, ahol azok átvizsgálhatók, és a szükséges javításokhoz segítséget nyújt. Az összefoglalást egy gördíthető képernyőn szövegesen és grafikusan is nyújtja, kockázati osztályokba sorolva a talált sérülékenységeket.



10.4. ábra. Sérülékenységek összefoglaló oldala kockázati szint szerint

A 10.4. ábrán látható, hogy a program a felderítő munkamenet befejezése után miként számol be a talált sérülékenységekről.

Akárcsak a Nessus, a Retina is megadja minden hasznos hivatkozásokat, amelyeket felkeresve az adott sebezhetőségről még több információt, és kijavításának lehetőségeit is meg lehet ismerni. A 10.5. ábrán egy adott sebezhetőségről szóló beszámoló látszik, megadva a vele kapcsolatos kockázatot, valamint hogy hol található meg a sebezhető eszköz gyártója által kibocsátott javítás.

### Sebezhetőségi frissítések

Állandóan új és még újabb sebezhetőségekre derül fény, s napjaink technológiai lehetőségeit figyelembe véve a programnak képesnek kell lennie arra, hogy az új résekre kiadott információkat automatikusan letöltsse, és onnantól felismerje.

A program ebből a szempontból kivételes: nem csupán a sebezhetőségek listájának, de magának az alkalmazásnak a rendszeres frissítése is

A javításokat tartalmazó különböző helyekre mutató hivatkozások

#### A sebezhetőség leírása

A hálózat szempontjából jelentett kockázati szintje

**Miscellaneous: Internet Explorer 6 SP1 Cumulative Patch 818529**

- Risk Level: High
- Description: Two critical vulnerabilities were discovered in Internet Explorer 6 SP1 and earlier that could allow an attacker to execute arbitrary code upon a victim's machine through malicious HTML. The first is a buffer overflow resulting from a specially-crafted "object" tag with the "type" property, while the second involves the automatic downloading and execution of arbitrary files when IE is flooded with requests to open the file.
- How To Fix: Install the appropriate Microsoft hotfix.
- URL1: [Microsoft Security Bulletin MS03-020](http://www.microsoft.com/technet/security/bulletin/ms03-020.asp)
- URL2: [Microsoft Knowledge Base Article Q818529](http://support.microsoft.com/default.aspx?scid=kb;en-us;Q818529)
- URL3: [eEye Digital Security Advisory on Object Tag Type Bug](http://www.eeye.com/html/research/advisories/)
- CVE: CAN-2003-0309, CAN-2003-0344
- BugtraqID: 7806

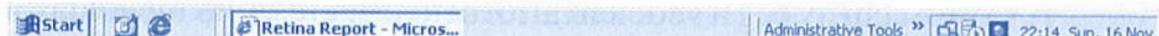
---

**NetBIOS: Null Session**

- Risk Level: High
- Description: A Null Session occurs when an attacker sends a blank username and blank password to try to connect to the IPC\$ (Inter Process Communication) pipe. By creating a null session to IPC\$ an attacker is then able to gain a list of user names, shares, and other potentially sensitive information.
- Note: If you have run this Retina scan with Administrator level access to your network then you will always be able to create a null session and therefore this is a false positive and not a vulnerability.
- How To Fix: Apply the following registry settings:

Hive: HKEY\_LOCAL\_MACHINE  
Key: System\CurrentControlSet\Control\LSA  
Value Name: RestrictAnonymous  
Value Type: REG\_DWORD  
Value Data: 2 (For Windows 2000) or 1 (for Windows NT)

- URL1: [How to Use the RestrictAnonymous Registry Value in Windows 2000](http://support.microsoft.com/default.aspx?scid=kb;en-us;Q246261)
- URL2: [Restricting Information Available to Anonymous Logon Users \(Windows NT\)](http://support.microsoft.com/default.aspx?scid=kb;en-us;Q143474)
- CVE: CVE-2000-1200
- BugtraqID: 494



Az összefoglalást egy gördíthető képernyőn szövegesen és grafikusan is nyújtja, kockázati osztályokba sorolva a talált sérülékenységeket

Hol szerezhető be további információ a sebezhetőséggel kapcsolatban

#### 10.5. ábra. Sebezhetőség részletezése

10.

beállítható rajta. Meglepő, hogy a nyílt forráskódú Nessus ezt nem teszi lehetővé. A Retina programhoz kell némi betanulási idő, azonban rendkívül hatékony sérülékenységérzékelő.

## 10.4. A VÉDELEM ÁTTÖRHETŐSÉGÉT VIZSGÁLÓ TERMÉKEK

A sérülékenységek azonosítása, felderítése, és fontossági sorrendjük kialakítása mind csupán ellenőrzési feladat. Áttörhetőségvizsgálónak csak akkor nevezhető egy program, ha ténylegesen meg is kísérli a megtalált sebezhetőség kihasználását. A sérülékenység ellenőrzése és az áttörhetőség vizsgá-

lata egymást kiegészítő eszközök. Mindegyiknek megvan a maga önálló feladata, ezért két külön csoportba kell őket sorolni. Azért fontos tisztázni ezt a kérdést, mert a kereskedők gyakran összekeverik a kettőt. Az áttörhetőség vizsgálata ott kezdődik, ahol a sérülékenység ellenőrzése abbamaradt.

A sérülékenység ellenőrzése megfelel a hálózat jelenlegi konfigurációjáról készített pillanatfelvételnek. Ez a kép azonban sajnos nem mutatja meg, hogy a szervezet tulajdonához valóban sikeresen hozzá lehet-e férni. Csak azt jelenti ki, hogy milyen sebezhető pontok léteznek; nem próbálja meg mélyebben kielemezni, hogy ténylegesen mi is történik a sérülékeny pont megtámadásakor. A következőkben foglalhatjuk össze a sérülékenység-ellenőrző korlátait:

- Csak részleges információbiztonságot nyújt.
- Kizárálag felismerni képes a sérülékeny pontokat, de nem tudja azokat súlyuk szerint értelmes módon felsorolni, és nem tudja a kiküszöbölésük fontossági sorrendjét felállítani.
- A lehetséges sebezhetőségekről hosszú listát készít, amelyek között általában több hamis is szerepel.
- Nem ismerteti, hogy mely információs vagyontárgyak lehetnek veszélyben.
- Nem képes valódi támadást szimulálni.
- Nem fedi fel a hálózati komponensek közötti bizalmi viszonyokat, és nem is mutatja meg ezek lehetséges befolyását egy adott támadásra.

A Core Security cég a védelem áttörhetőségét tesztelő megoldások piacára a Core Impact nevű feltörő termékével tört be. Igen, *feltörő* termék (alkalmazásokat futtatnak a termékbén). A termék valójában nem foglalkozik a sérülékeny pontok megtalálásával, hanem kihasználja azokat, és a *megcélzott gépen elhelyez egy ügynököt*. Ez az ügynök ezután lehetővé teszi a támadás kiszélesítését, hogy végül át lehessen venni a gép felett az ellenőrzést. Megszűnnek tehát a hamis sérülékenységjelzések. A következő részben áttekintjük a program működését, de a <http://www.coresecurity.com> webhelyen többet is meg lehet tudni róla.

## 10.4.1. CORE IMPACT

### Önjellemzés

A következő bekezdés a Core Security cég honlapjáról való:

*A Core Impact az első átfogó, a védelem áttörhetőségét vizsgáló alkalmazás, amely a vállalatokra leselkedő veszélyek felmérésére szolgál. A termék a költséges, és hiba-lehetőségektől sem mentes kézi ellenőrzés helyettesítésére lett kifejlesztve, mint au-*

tomatikusan működő korszerű, a védelem áttörhetőségét vizsgáló eszköz. A sérülékenység-ellenőrzőkön túl képes az IT-vagyontárgyak elleni valódi támadás végrehajtására. A biztonsági kockázatokkal kapcsolatos információk analízisét egyetlen át fogó alkalmazásban tömöríti.

### Felderítési és észlelési pontosság

A letapogatásnak és a jelzett sebezhetőségeknek a lehető legkevesebb hamis jelzés mellett pontosaknak kell lenniük. Hamis jelzés az elfogadott tevékenységre vagy konfigurációra tévedésből adott jelzés. Ennek az ellenkezője szintén igaz – a hamis hallgatás is rossz –, vagyis ha a rendszer nem ad jelzést az el nem fogadható állapotról vagy tevékenységről.

A program maga azonban nem keresi a sebezhetőségeket, sőt a termék segítségével csupán korlátozott mértékben lehet felderíteni azokat. Fel derítő módba kapcsolva egyszerű végpont-letapogatásra és a cél operációs rendszer felismerésére képes csupán. A rendszer felismerése nagyon fontos, mivel ez az információ a betörés végrehajtását megkönnyíti. Miért beszélünk mégis egy olyan termékről, amely nem deríti fel a lehetséges sérülékenységeket? Nos, mivel használatával elkerülhetők a hamis figyelmeztetések, hiszen ténylegesen végrehajtja a betörést, majd úgy megy tovább a támadás, mintha mi lennének a támadók – így érve el a sérülékenység-ellenőrzés következő lépcsőjét.

### Dokumentáció és támogatás

A dokumentációnak világosnak, tömörnek, olvasmányosnak és könnyen érthetőnek kell lennie. Ideértendő a készített listák leírása, valamint az alkalmazás működésének ismertetése is, hogy a felhasználók megérthesék, miként is működik a program, és milyen információkat tud kiírni.

Amikor új szoftvert vagy alkalmazást kell megismerni, rendkívül fontos, hogy jó dokumentációja és jó terméktámogatása legyen. Ez teszi lehetővé a felhasználók számára, hogy más módszerek, például tanfolyamok és órarend szerinti webszeminariumok helyett saját maguk is képesek legyenek azt megtanulni.

10.

### Jelentések

Az áttörhetőségvizsgáló eszköz legfontosabb előnye az, hogy használatával képesek legyünk megtudni, egy adott sebezhetőség felfedezése után mit tehetnénk az elhárítására; éppen ezért a nyomtatásnak testreszabhatónak és pontosnak kell lennie.

A program számos kitűnő nyomtatást képes előállítani, amely a működés során a program által végzett valamennyi tevékenységet naplózza a letapogatás és a gépek megtámadása során egyaránt. Kétféle nyomtatást készíthetünk vele:

- **Találatok száma** – A megtalált gépek, és a rajtuk felfedezett sérülékenységek listája.
- **Tevékenységtörténet** – A programot használó felülvizsgáló által végzett valamennyi tevékenység időrendi listája.

Ezek a listák csupán a programtól elvárható minimális tudást jelentik. Ami mégis egyedivé teszi őket, az a testreszabhatóságuk, és hogy a felhasználó által elvárt részletességgel nyomtathatók ki. A vállalat igazgatóságának átadott lista például jelentősen el fog tért a beavatkozásra hivatott IT-személyzetnek átadottól. A program által készítendő listák ennyire rugalmasan konfigurálhatók.

### **Sebezhetségi frissítések**

Állandóan új és új sebezhetségekre derül fény, s napjaink technológiai lehetőségeit figyelembe véve a programnak képesnek kell lennie arra, hogy az új résekre kiadott információkat automatikusan letöltsse, és onnantól felismerje.

A program egy kattintással lehetővé teszi az új támadó modulok letöltését. A Core Security rendkívül elkötelezett a program fejlődése és terjedése mellett, így rendkívül agresszív fejlesztési stratégiát alkalmaznak. Nyilván nem található meg benne valamennyi elképzelhető sérülékenység támadómodulja, azonban folyamatosan újabb és újabb modulok kerülnek kibocsátásra. Elég nagy kihívást jelent meghatározni, hogy pontosan milyen sérülékenységekre vannak modulok, és a megfigyelések szerint az igazán jó választások és lehetőségek meglehetősen korlátozottak, azonban ilyen értelemben is gyorsan fejlődik a termék.

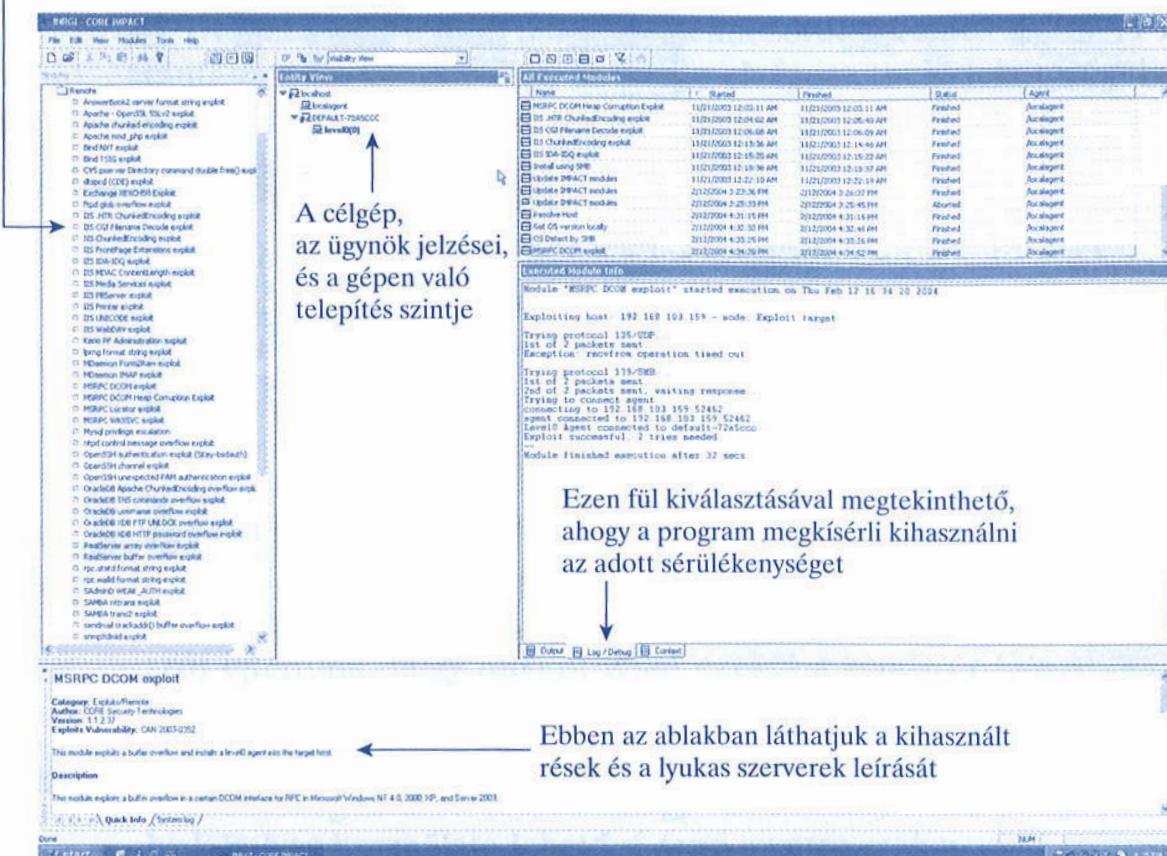
### **A Core Impact működése**

Ebben a pontban azt tekintjük át, hogy a program miként használja ki a támadott sérülékenységet, és hogyan installál egy különleges, felfedezhetetlen szoftverkódöt (ügynököt) a célgépen. Ez az ügynök teszi ezután lehetővé, hogy átvegyük az uralmat a gép felett. Az így megszerezhető uralom szintje az ügynök által kihasznált sérülékenységtől függ. A következő ábrák azt szemléltetik, amikor a kihasznált sebezhetség a célgép feletti teljes uralom megszerzését teszi lehetővé. A 10.6. ábra a Windows 2000 Professional SP3 operációs rendszerben lévő MSRPC DCOM sebezhetség kihasználását mutatja be.

Miután az ügynököt sikerült a célgépre telepíteni, meghatározható a sérülékenység kihasználásával felette szerzett uralom szintje. A 10.7. ábrán az ügynök telepítése sikerült; a jobb egérgomb megnyomása az ügynökön megjeleníti az elérhető opciók lehetséges listáját.

A fenti esetben az egyik legijesztőbb az a lehetőség, hogy az ügynök képes a célgépen lévő valamennyi állomány böngészésére. Amint az a 10.8.

A kiemelt sérülékenységeket lehet kihasználni a célgépen

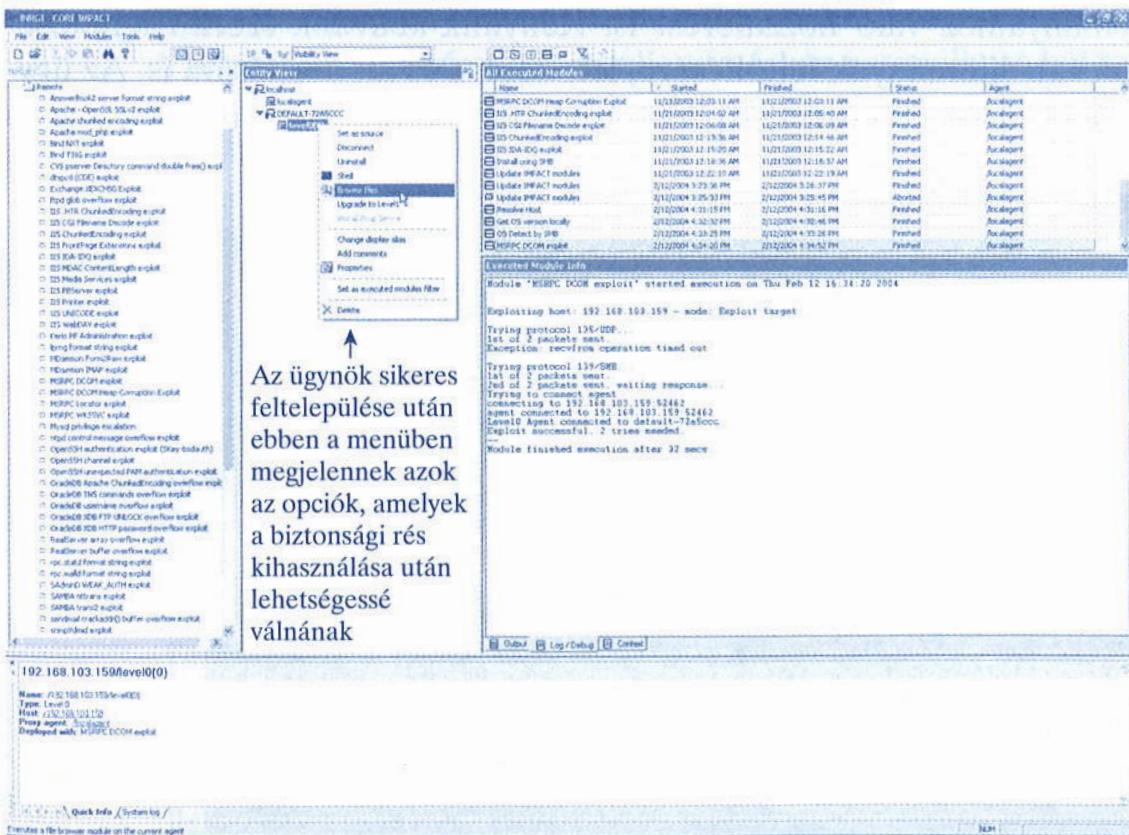


A célgép,  
az ügynök jelzései,  
és a gépen való  
telepítés szintje

Ezen fél kiválasztásával megtekinthető,  
ahogy a program megkísérli kihasználni  
az adott sérülékenységet

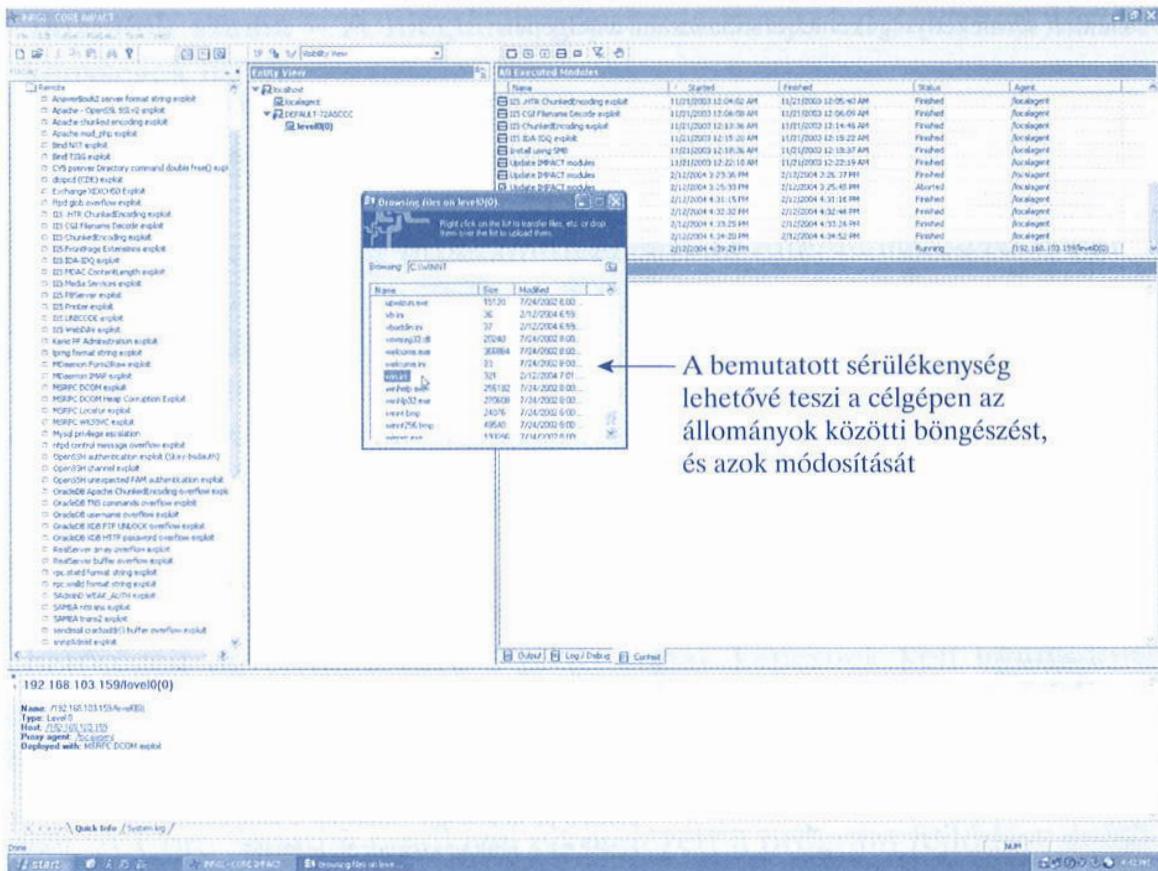
Ebben az ablakban láthatjuk a kihasznált  
rések és a lyukas szerverek leírását

## 10.6. ábra. A Core Impact ügynök telepítése



Az ügynök sikeres  
feltelepülése után  
ebben a menüben  
megjelennek azok  
az opciók, amelyek  
a biztonsági rés  
kihasználása után  
lehetségesse  
válnának

## 10.7. ábra. Az ügynök lehetőségei



10.8. ábra. Az állományok böngészése

ábrán látható, az ügynök lehetővé teszi még a feltört gép legérzékenyebb állományaihoz való hozzáférést is. Kényünk-kedvünk szerint lehetőségünk van állományok feltöltésére, letöltésére és módosítására is. Az ügynököket nem lehet futásuk közben felfedezni a feltört rendszeren, mégis

```
ev mini-shell at default-72a5cc - C:\WINNT\system32
C:\WINNT\system32 # help
Available commands:
  cd [proxied_directory]
  lcd [local_directory]
  pwd
  cat proxied_filename
  rm proxied_filename
  cp src_proxied_filename dst_proxied_filename
  mv src_proxied_filename [dst_proxied_filename]
  get src_proxied_filename [dst_local_filename]
  put src_local_filename [dst_proxied_filename]
  ls [-l]
  id
  hostname
  execute proxied_filename
  exit
  help
C:\WINNT\system32 # ..
```

10.9. ábra. Mini parancsértelmező

jelen vannak, és felruháznak minket azzal a képességgel, hogy kipróbáljuk, a felfedezett biztonsági rés tényleg kihasználható-e.

Utoljára még a mini parancsér telmezőről érdemes szólni. A 10.9. ábra mutatja be a képernyőjét, és a vele elvégezhető lehetőségeket. Amint látjuk, az ügynök telepítése után a feltöltés, letöltés, és az állományok futtatása egyszerű.

Arra is van lehetőség, hogy további ügynököket telepítsünk más célgépekre, ha a felfedezett rés további támadásra ad lehetőséget. A jelen példa esetén a hozzáférés más belső eszközökre is kiterjeszthető. Ebben az a szomorú, ha ezeket a további támadásokat fel is fedeznénk, azok a feltört gépről kiinduló támadásnak tűnnének.

## 10.5. ÖSSZEFOGLALÁS

Az utolsó fejezetben bemutattunk néhány új sérülékenységet, és arról is szót ejtettünk, hogy miként lehet ezeket a rendszer támadására felhasználni. Ezen gyakori támadások megismerése alapvető fontosságú a fejezet többi részének megértéséhez. A biztonsági kiértékelések és a védelem áttörhetőségének ellenőrzése nagyon hatékony eszköz a kezünkben, amelyek helyes használata lehetővé teszi az erre szakosodott mérnökök általi felülvizsgálatot, akik megfelelő biztonsági ellenőrző és analizáló szoftverek segítségével keresik a sebezhető pontokat. Az igazán jó biztonsági kiértékelés azonban többet jelent, mint a hálózat logikai réseinek feltárása. A fejezet további részében az ellenőrzéshez használható különböző eszközöket mutattuk be, amelyek között még ingyenes alkalmazások is voltak.

## 10.6. ÖSSZEFOGLALÓ KÉRDÉSEK

10.

1. Az Ettercap nevű, ingyen letölthető szoftver a csomagszaglászás mely négy típusát képes végrehajtani?
2. Magyarázza el, mi az a DDoS, és miként működik!
3. Nevezze meg és magyarázza el azt a három okot, amely a rendszerben egy hátsó ajtó elhelyezésére ad alkalmat!
4. Határozza meg a tűzjárás alapelveit!
5. Hol kell a külső áttörhetőségvizsgálatot és sérülékenység-ellenőrzést elvégezni a hálózatban?
6. Amikor sérülékenység-ellenőrző szoftvert kíván beszerezni, miért alapvető fontosságú a program precíz felderítési képessége?