Harc a kibernetikai bűnözés ellen: technikai alapok

Összeállította: Drencsán János
a Puskás Tivadar Közalapítványnál

Köszönetnyilvánítás

Szeretném megköszönni Mrs. E. van Geest LL.M.-nek és GOVCERT.NL technikai csoportnak a munkáját, akik a From Recognition to Reporting, Cyber Crime Manual című kézikönyvet készítették. "Harc a kibernetikai bűnözés ellen: technikai alapok" a holland kézikönyv magyar változata, és erősen támaszkodik a GOVCERT.NL munkájára.

Harc a kibernetikai bűnözés ellen: technikai alapok

1 Bevezetés

A kibernetikai bűnözés komplex fogalom és sokak számára nem világos, hogy mit is takar ez a fogalom. Ez a dokumentum a kibernetikai bűnözés több formáját meghatározza és ismerteti az olvasóval. Az olvasó számára nyújt némi technikai információt az egyes bűnözési formákról, és az ellenük tehető lehetséges biztonsági intézkedésekről.

Jelenleg a kibernetikai bűnözők kinyomozása, és büntetőjogi eljárás indítása számos technikai, jogi és politikai akadályba ütközik. Mivel a számítógépes adat könnyen változtatható, a naplók, és az egyéb bizonyítékként szolgáló adatok is könnyen hamisíthatók (a támadó, és akár az áldozat által is). A törvénykönyvek nem írják le, hogy milyen adatok, milyen körülmények között fogadhatók el bizonyítékként a bíróság előtt; szerencsés esetben – mint például a magyar jogban – szabad bizonyítás van, azaz a vád bizonyítása során a bizonyítás és a bizonyítékok értékelésének szabadsága érvényesül. Ennek értelmében a hatóságok a bizonyítási eszközök és bizonyítékok felhasználásáról szabadon döntenek. Ebben őket kizárólag azt köti, hogy a felderítésre váró tényállás szempontjából mi a jelentős adat, vagy tény. A bizonyítékok értékelésének szabadsága folytán a bizonyítási eszközök és bizonyítékok egyenként és összességükben kerülnek értékelésre és elbírálásra. A szabad értékelés a büntetőeljárásban mindenfajta bizonyítékra kiterjed.

Vannak javaslatok arra, hogyan kell az adatokat kezelni annak érdekében, hogy megállják helyüket bizonyítékként. Sajnos ezek csak javaslatok, és sok függ a szakértő véleményétől, hogy mi számít hiteles adatnak büntetőjogi eljárás esetén. Viszont még akkor se biztos, hogy tudunk eljárást indítani a támadó ellen, ha bizonyítéknak minősülő hiteles adataink vannak a támadó ellen. Nemzetközi egyezmények hiányában, egy külföldi támadó ellen eljárást indítani nagyon nehéz, és költséges lehet. Sőt az is lehet, hogy jogi úton nem is támadható a bűnöző.

2 Spam

2.1 Meghatározás

A spam kéretlen e-maileket jelent. Ezeket a kéretlen e-maileket általában egyszerre nagyon sok e-mail címre küldik el. Gyakran használnak közvetítő szervereket a kéretlen e-mailek küldésére (*lásd:* 3. fejezet Nyitott továbbító (open relay)), ami megbéníthatja a valós e-mailek küldését egy e-mail szerveren (*lásd:* 7. fejezet (Elosztott) szolgáltatásmegtagadásos támadás).

Egy spammernek[1] csak a megcélzott személyek e-mail címeire van szüksége. Hatalmas címlistákat képesek felhalmozni erre specializálódó ügynökségektől, hírcsoportokból, weblapokról, csevegő fórumokról, LDAP[2] címtárakból és egyéb helyekről. Spam megelőzése érdekében óvatossággal járjunk el, amikor az e-mail címünket kiadjuk.

2.2 Technikai megkülönböztetés

Annak meghatározása, hogy a kéretlen e-mail egyben spam-e, az e-mailezés természetéből kifolyólag nem egyértelmű. Sokszor küldünk úgy e-mailt, hogy a fogadó fél nem várja, nem kérte, vagy akár nem is akar felőlünk hallani. A spamnek vannak bizonyos technikai tulajdonságai, amik megkülönböztetik a normális e-mail[3] forgalomtól:

- **Érvénytelen feladó cím**

  Gyakran, de nem mindig, a feladó címe vagy tartománya érvénytelen spam levelek esetén.

- **Érvénytelen 'received' fejléc**

  A spamhez gyakran adnak érvénytelen 'received' sorokat, hogy nehezítsék a spam felismerését.

2.3 Lehetséges biztonsági intézkedések

A spamek elkerülése érdekében a következőket lehet tenni:

- **DNS ellenőrzés**

  Ezzel a módszerrel a következőket tudjuk ellenőrizni:
  - A feladó címben lévő tartomány valóban létezik
  - A feladó e-mail szerver az, akinek állítja magát.

- **Fekete lista**

  A fekete listába olyan e-mail szerverek kerülnek, amelyeket gyakran használnak spam küldésére. Ezzel nagy mennyiségű spamtől megóvja a felhasználót, de azoktól a szerverektől jövő rendes e-mail forgalom nem jut el a felhasználóhoz.

- **Fehér lista**

  A fehér lista egy szervezet saját listája e-mail címekkel és szerver tartományokkal. Csak az ebben a listában szereplő feladóktól kapott e-maileket tartjuk hitelesnek. A spam úgy

[1] Spammer: spamet küldő egyén vagy szervezet.
[2] LDAP (Lightweight Directory Access Protocol) címtárak a telefonkönyv elektronikus formájához hasonlító adattár e-mail címek keresésére.
[3] A normális e-mail alatt kifejezetten azokat az e-maileket értjük, ami nem spam. Egy technikai megkülönböztetés a(z) 2. oldalon található.

kerülheti meg ezt a védelmi rendszert, hogy a feladó meghamisítja a feladó címet egy olyan címre, ami a fehér listán található.

- **Tartalomvizsgálás**

Az e-mail tartalmának vizsgálata az emberi gondolkodást és döntést próbálja szimulálni. Ha elolvasunk egy e-mailt, mi azonnal el tudjuk dönteni, hogy spam-e vagy sem. A tartalomvizsgálásnak kétféle megoldása van:

- **Minta analízis.** Ilyenkor az e-mailt megvizsgáljuk, hogy tartalmaz-e bizonyos „tiltott" szavakat. Amennyiben a tiltott szó szerepel az e-mailben, akkor azt a program spamnek minősíti. A probléma ezzel a megoldással az, hogy normális e-mailek is tartalmazhatnak „tiltott" szavakat.
- **Tanuló rendszer.** Szabályok alapján működik, de hibás döntés esetén módosítja a szabályokat.

2.4 Büntethetőség

Spam esetén nincs illetéktelen behatolás számítógépes rendszerekbe. Spam nem okoz adatkárosodást vagy adatváltozást, sem a továbbításra használt szervereken, sem a címzett számítógépén. Spamek küldése önmagában nem számít bűncselekménynek. Viszont nagy mennyiségű e-mailek küldése, illetve továbbítása megbéníthatja az e-mail szervereket. Ez főként a továbbító szervereknél okoz gondot, ugyanis normális e-mail forgalom kezelése ideiglenesen megszűnhet, vagy jelentősen lecsökkenhet a nagy mennyiségű spam továbbítása miatt. Ez úgynevezett szolgálatmegtagadásos támadásnak minősülhet, ami viszont büntethető.

3 Nyitott továbbító (open relay)

3.1 Meghatározás

Ez nem támadási forma, hanem konfigurációs hiba egy e-mail szerveren, ami lehetővé teszi spam továbbítását. Tehát aki beállította az e-mail szervert, nem tette meg a megfelelő biztonsági lépéseket a helytelen használat megelőzésére. Mint ahogy már említettem az előző fejezetben, nagy mennyiségű spam továbbítása szolgáltatás megtagadást hozhat létre a továbbító szerveren.

Amennyiben az e-mail szerverünk az alábbi e-maileket továbbküldi, akkor a nyitott továbbítóként működik:

- Ha a feladó és a címzett e-mail címe ugyanaz.
- Ha a feladó tartománya nem létezik.
- A levelet a „localhost" tartományból küldik.
- Ha a feladó tartománya nincs megadva.
- Ha a feladó címe nincs megadva.
- Az e-mailen a célszerver van megadva, mint feladó szerver.
- Az e-mailen a feladó szerver IP címe szögletes zárójelben van megadva.
- E-mail továbbítása a % karakterrel. Például címzett%szerver.com@továbbítószerver.com címzésű e-mailt a címzett@szerver.com címre továbbítja a nyitott továbbító szerver.
- A címzett e-mail címe dupla idézőjelben van megadva.
- A címzett e-mail címe inverz jelöléssel van megadva. Pl. @továbbítószerver.com:címzett@szerver.com címzésű e-mailt a címzett@szerver.com címre továbbítja a nyitott továbbító szerver.
- … vagy a szerver.com!címzett címzésű e-mailt a címzett@szerver.com címre továbbítja a nyitott továbbító szerver.
- A fentiek bármelyik kombinációja.

3.2 Lehetséges biztonsági intézkedések

- Az e-mail szerver beállítása úgy, hogy e-mailek továbbítása ne legyen lehetséges kívülállók számára. Tehát a szervernek fel kell ismernie a felül említett, és egyéb jól ismert továbbítási módszereket. Természetesen amennyiben a szerver felismerte a továbbítási szándékot, akkor azonnal szakítsa meg a kapcsolatot a feladóval, és küldjön egy hibaüzenetet (pl. „550 relaying not allowed" azaz a „továbbítás nem engedélyezett").

- SMTP[4] kapcsolatot csak bizonyos, meghatározott IP címekről engedjünk. Ez lehetséges az e-mail szerver konfigurációjával, vagy pedig a tűzfal beállításával. Ezt akkor érdemes tenni, amikor az e-mailt csak néhány ismert szervertől fogadunk el.

- Ellenőrizzük, hogy a feladó vagy címzett mező olyan címet tartalmaz, amelyekre a továbbítás engedélyezett. Ezt a szerver konfigurációs fájljában lehet beállítani.

- Vannak olyan esetek, amikor nincs szükség SMTP kapcsolatra az e-mail szerver és az internet más e-mail szerverei között. Ezt a korlátozást a tűzfalon lehet beállítani.

[4] SMTP (Simple Mail Transfer Protocol) az e-mailek küldésére, továbbítására, és kézbesítésére használt protokoll.

4 Hacking / cracking[5]

4.1 Meghatározás

A hacking és a cracking angol kifejezések, adathoz vagy számítógéphez történő jogosulatlan hozzáférést, és az arra való törekvést jelentik. Azokat a személyeket, akik ilyen tevékenységekben részt vesznek hackernek (vagy crackernek) hívjuk.

4.2 Behatolási technikák

Háromféleképen lehet betörni egy rendszerbe:

- *Fizikai betörés*
  Ebben az esetben a behatolónak van fizikai hozzáférése a rendszerhez. A betörés történhet konzolról vagy adathordozók eltávolításával.

- *Helyi betörés*
  A hackernek már van felhasználói joga, és bővíti a hozzáférési jogait, akár jelszómásolással, akár valami sérülékenység kihasználásával.

- *Távoli betörés*
  A hackernek nincs semmilyen hozzáférési joga a rendszerhez, viszont sérülékenységek kihasználásával képes behatolni a rendszerbe.

4.2.1 Sérülékenységek kihasználása

A sérülékenységek olyan szoftver-, beállítási vagy egyéb hibák, amiket egy hacker kihasználhat számítógépes rendszerek támadásához. A sérülékenységek alábbi fajtái léteznek:

- **Szoftver sérülékenység**

A szoftver sérülékenységek programozási hibák, amiket a hacker kihasznál. A leggyakoribb kihasználási technikák:

  - Puffer túlcsordulás
    A puffer egy lefoglalt memória blokk, amit a program adatok bevitelére és küldésére használ ideiglenes tárolás céljából. A puffernek van egy előre meghatározott mérete. Puffer túlcsordulás akkor történik, amikor megpróbálunk (és sikerül) a puffer méreténél nagyobb adatot beírni a pufferbe. Ilyenkor a puffer utáni memória területre is írunk adatokat (azt nem lehet tudni, hogy milyen adatokat írunk át). Ezzel a hacker elérheti, azt hogy az alkalmazás összeomoljon, vagy pedig lefutathat egy program kódot. Ha sikerül egy programkódot lefutatni, a hacker hozzáférést nyerhet a rendszerhez.
  - Váratlan kód kombináció
    Számítógépes rendszereken egyszerre több alkalmazás is futhat az operációs rendszer mellett. Egy ártatlannak tűnő parancs kiadásával egy programnak, befolyásolhatunk más programokat. Egy példával a legkönnyebb bemutatni ezt a sérülékenységet:
    A Perl egy programozási nyelv, amit gyakran használnak web-alkalmazásokhoz. Gyakran használt trükk valamilyen parancs futtatása a web-alkalmazáson keresztül. Például „| mail user < /etc/passwd”. Ezzel a karakterlánccal a Perl nyelven írt web-

[5] A hacking és a cracking kifejezések felcserélhetők, és alapjába véve ugyanazt jelentik. A hacker és a cracker, illetve a hacking és cracking között egyes szakértők megkülönböztetést tesznek, azonban jogszabályilag nincs különbség a két kifejezés között. Továbbiakban a hacker szót fogjuk használni az illegális kibernetikai behatolók megnevezésére.

alkalmazás megkéri az operációs rendszert, hogy e-mailben küldje el a jelszavakat tartalmazó fájlt. A hacker felhasználhatja a jelszavakat, hogy hozzáférést nyerjen a rendszerhez.

- **Hibás beállítások**

Sérülékenység fakadhat a hibás beállításokból, vagy pedig az alapértelmezett beállítások használatából. Alapértelmezett beállítások nem nyújtanak kellő biztonságot a rendszernek. Ilyen esetekben a hacker hozzáférést nyerhet alapértelmezett jelszavakkal. A hacker szintén kihasználhat egy feleslegesen futó szolgáltatást.

- **Gyenge jelszavak**

Könnyen kitalálható jelszavak, egyszerű behatolási lehetőséget adhat egy hacker számára. Például amikor a felhasználónév és a jelszó megegyezik. *(További információ érdekében lásd:* 13. fejezet: Jelszótalálgatás*).*

- **Titkosítatlan adat**

A hálózatot több számítógép és egyben felhasználó is használja egyszerre. Bizonyos programokkal egy hacker képes lehallgatni a forgalomban lévő adatokat, ha titkosítatlanul küldjük át őket a hálózaton. Így a hacker hozzájuthat fontos adatokhoz, illetve jelszavakhoz. *(További információ érdekében lásd:* 12. fejezet: Sniffing*).*

4.2.2 Felderítés

Ahhoz hogy egy hacker a fent említett sérülékenységeket ki tudja használni, ismernie kell a rendszert. Tehát behatolás előtt minél többet meg kell tudni a célba vett rendszerről. Egy rendszerről meg lehet tudni sok mindent anélkül, hogy kapcsolatba lépnénk vele. Információkat a hacker szerezhet útadó táblázatokból, internetes keresőktől, és DNS[6] szerverektől. Nehéz a hacker nyomon követése, ha ilyen nyilvános információkat használ.

A hacker használhat közvetlen vizsgálati technikákat is a rendszer megismerésére. Egyes esetekben az ilyen vizsgálatok észlelhetők. A portok[7] letapogatásával (port scanning) a hacker megtudhatja, milyen szolgáltatások futnak egy távoli számítógépes rendszeren. *(További információ érdekében lásd:* 8. fejezet: Portok letapogatása*).* A hacker további információt is megtudhat a rendszerről, mint például:

- az operációs rendszer, és annak verziója
- a rendszeren futó alkalmazások, és azok verziói
- egyes folyamatok tulajdonosai
- a rendszerkönyvtár szerkezete
- stb.

4.3 Lehetséges biztonsági intézkedések

A hackernek minden fent említett sérülékenység kihasználására vannak eszközei. Tehát a sérülékenységeket sorra vesszük és megtárgyaljuk az azok kihasználása ellen tehető biztonsági intézkedéseket.

[6] DNS (Domain Name System) a tartomány nevekhez (pl. neti.hu) megadja a hozzá tartozó IP címet.
[7] Port: A hálózaton lévő számítógépeken egyszerre több hálózati szolgáltatás is futhat. Ezekhez a szolgáltatásokhoz egyedi számokat, ún. „port”-ot rendelünk. Így tudja a számítógép, hogy melyik csomagot, melyik szolgáltatásnak (programnak) kell továbbítani.

- **Szoftver sérülékenység**

Ezeket a sérülékenységeket programozási hibák hozzák létre. Sajnos a szoftverek kiadásával nem szoktak várni addig, amíg tökéletesen nem működik. Viszont kiadásuk után a fejlesztők tovább javítják a programokat. Ezek a javítások általában díjtalanul megszerezhetők. Mihelyt egy felismert problémát megjavítanak, a fejlesztők kiadnak egy úgynevezett patch-et. Ritkább időközönként pedig úgynevezett upgrade[8] csomagokat adnak ki, amik tartalmazzák az addig kiadott patch-eket és esetleg további javításokat is.

A szoftverfejlesztők és egyéb szervezetek tesztelik a szoftver termékeket, hogy a hackerek előtt felfedezzék hibáikat. Így a javítások hamarabb nyilvánosságra kerülhetnek, mint a bizonyos sérülékenységet kihasználó hacker eszközök.

A szoftver sérülékenységek ellen tehető legjobb és legegyszerűbb lépés a patchek és upgrade csomagok használata. Sok esetben ez már szinte automatizált. Az alkalmazás saját maga, vagy egy segédprogram figyeli, mikor jönnek ki a patchek, és azonnal jelzi a felhasználónak. Csak egy katintás és letölti, illetve installálja a legfrissebb javításokat. Mindezek ellenére sajnos kevesen frissítik[9] az operációs rendszert, és az alkalmazásokat. Tehát sok számítógépes rendszer marad támadható.

- **Hibás beállítások**

A hibás beállítások elkerülése érdekében olyan személy végezze a telepítést és a beállítást, aki jól ismeri a rendszert, az alkalmazást, és rendelkezik kellő szaktudással a rendszer biztonságos beállításához. Amennyiben saját magunk szeretnénk elvégezni a beállításokat, meg kell ismerni a számítógépes rendszert, a rajta futó operációs rendszert, és egyéb alkalmazásokat. Legfőképpen olvassuk el a dokumentációkat, továbbá derítsük ki, milyen egyéb eszközökre (pl. tűzfal) van szükség ahhoz, hogy a rendszer biztonságos legyen. Semmiféleképpen ne használjuk az alapértelmezett beállításokat, mert azok nem biztonságosak.

- **Gyenge jelszavak**

Először is, soha se használjunk alapértelmezett jelszavakat. A rendszergazda által megadott jelszavakat se használjuk, hiszen azokat csak azzal a céllal adják, hogy be tudjunk jeletkezni és módosítani tudjuk a jelszót egy általunk kiválasztott biztonságos jelszóra. Az szintén nem jó, ha a jelszavunk tartalmazza a nevünket, a felhasználónevet, telefonszámot, lakcímet, születési dátumot, vagy egyéb szavakat, illetve számokat, amik valamilyen közeli kapcsolatba hozhatók velünk. Továbbá a jelszó tartalmazzon kisbetűket, nagybetűket, és számokat egyaránt. A fokozottabb biztonság érdekében változtassuk meg a jelszavunkat bizonyos időközönként (pl. hetente, havonta). Minél hosszabb a jelszó, annál biztonságosabb. Természetesen sose írjuk le a jelszót papírra, tehát olyan jelszót válasszunk, amire fogunk is emlékezni, és ne adjuk ki a jelszavunkat senkinek sem. Továbbá különböző rendszerekhez más-más jelszót használjunk.

A jelszóval kapcsolatos szabályokat ismertetni kell a felhasználókkal, és azok betartását rájuk kell kényszeríteni. Használhatunk scripteket, vagy programokat, amik a jelszó beírásakor ellenőrzik a jelszót a szabályok értelmében. A felhasználónak így nem lesz hozzáférése a számítógépes rendszerhez addig, amíg nem ad megfelelő jelszót. Utólagosan is lehet a jelszavakat ellenőrizni. A hackerek eszköztárában lehetnek a jelszavak kitalálására szolgáló eszközök. Ugyanezeket az eszközöket egy rendszergazda is használhatja (természetesen ehhez kell engedély a feletteseitől) a jelszavak ellenőrzésére. Tehát ha a

[8] Upgrade helyett, szokás a Szerviz Csomag (Service Pack) kifejezést is használni.
[9] Frissítés alatt a patchek és upgrade csomagok letöltését, illetve installálását értjük.

program kitalálja a jelszót, akkor az gyenge jelszónak minősül és azonnal meg kell változtatni.

- **Titkosítatlan adat**

Ez könnyen megoldható olyan programok használatával, amik titkosítva küldik az adatokat, vagy legalább a jelszavakat. Az FTP és TelNet programok például sima karakterláncként küldi el a jelszavakat. Használjuk inkább az SSH és SCP programokat, amik titkosítva küldik az adatokat. A lényeg, hogy tudjuk, milyen biztonságot nyújtanak azok a programok, amiket használunk.

4.4 Büntethetőség

Egy számítógéphez való jogosulatlan hozzáférés a betörés számítógépes megfelelője. Adathoz való jogosulatlan hozzáférés pedig lehet a lopás számítógépes megfelelője. A megszerzett adatokat (pl. hitelkártyaszám, jelszó stb.) tovább lehet használni, akár nem számítógépes bűncselekmények elkövetésére is. A feltört számítógépet pedig fel lehet használni egyéb számítógépes bűncselekmények lebonyolítására is, mint például (elosztott) szolgáltatás megtagadás típusú támadásokra, betörés más számítógépes rendszerekbe stb.

Jogosulatlan hozzáférés esetén a hackernek módjában áll az adatok másolása (lopás), módosítása (hamisítás), tönkretétele (vandalizmus). Sőt képes az egész számítógépes rendszer tönkretételére.

Azt is tudni kell, hogy a számítógépes rendszer működtetője köteles biztonsági lépéseket tenni a rendszer és a rajta tárolt adatok védelme érdekében. Amennyiben nem tesz eleget ennek a kötelezettségnek, jogilag támadható lesz. Itt nem csak szervezetek nagy számítógépes rendszereiről van szó, hanem az otthoni személyi számítógépes rendszerekről is. Viszont a törvény nem határozza meg, mi számít megfelelő biztonsági intézkedésnek, a döntés a tulajdonos/rendszergazda kezében van.

5 Elcsúfítás

5.1 Meghatározás

Elcsúfítás egy weboldal jogosulatlan változtatása, kicserélése, tönkretétele és/vagy az internet forgalom átirányítása egy másik weboldalra DNS hacking vagy tartománynév hamisítás által.

Ahhoz, hogy egy weboldalt megváltoztasson, kicseréljen vagy tönkretegyen, a hackernek be kell hatolnia a webszerverbe vagy a hozzá kapcsolódó egyéb szerverekbe, például adatbázis szerverbe.

DNS hacking esetén a hacker a DNS szerverbe hatol be és a tartománynévhez tartozó IP címet változtatja meg. Tartománynév hamisítás esetén a hacker nem hatol be a DNS szerverbe, viszont a hatás ugyanaz; a DNS szerver a weboldal látogatóját más címre küldi. A látogató számára ez veszélyes lehet, ugyanis azt hiszi, hogy egy hiteles cég weboldalán van. A rosszakaró ilyenkor elkérhet jelszót, e-mail címet, lakcímet, és akár hitelkártya-számot is a gyanútlan látogatótól.

5.2 Lehetséges biztonsági intézkedések

Mivel az elcsúfítás hacker technikákkal is történhet a saját webszerverünk ellen, az előző fejezetben megtárgyalt biztonsági lépések is meg kell tennünk *(lásd* 4. fejezet: Hacking / cracking*)*. További biztonsági intézkedések elcsúfítás ellen:

- A weboldal forgalmának figyelése. DNS hacking / tartománynév hamisítás nyomai nem találhatók a mi rendszerünkben. Ilyen típusú elcsúfítás esetén hirtelen, nagymértékű forgalomcsökkenés vehető észre a weboldalon. Ha úgy érezzük, hogy gond van, lépjünk kapcsolatba a DNS szerver működtetőjével.
- Figyeljük a 401 (jogosulatlan), 403 (tiltott) és 405 (eljárás nem engedélyezett) jelentéseket. Ezek a jelentések az mutatják, hogy valaki megpróbált elérni olyan fájlokat, amik nem léteznek, vagy nincsen hozzáférési engedélyük. Vegyük fel a naplóba az időt, a forrás IP címet és az URL[10]-t, amit megpróbáltak elérni.
- Rendszerinformáció ne legyen nyilvánosan látható weboldalakon.
- A rendszer könyvtárai ne legyenek láthatók az internet böngésző számára.
- Ne használjon szimbolikus kapcsolatokat mappákhoz és fájlokhoz a weboldalon.
- A webszervernek ne engedélyezze az SSI (Server Side Include)[11] aktiválását.
- Használjon biztonságos kapcsolatot (HTTPS), amikor adatokat kér a felhasználótól.

5.3 Büntethetőség

A magyar törvények szerint a számítógépes rendszerekbe való behatolás, és ott az adatok és fájlok illetéktelen megváltoztatása bűncselekménynek számít. Ezt már a 4. Hacking / cracking fejezetben is megtárgyaltuk. A tartománynév hamisítás szintén bűncselekménynek számít, ugyanis egy rendszert hozzáférhetetlenné teszünk.

[10] URL (Uniform Resource Locator) az interneten megtalálható objektumok (weboldal, kép, fájl, stb.) címe egy megadott forma szerint. Pl. http://www.példa.com/János/képek/egyszépkép.jpg

[11] Az SSI lehetővé teszi a weboldal számára, hogy parancsokat futtason a webszerveren mielőtt az oldal megjelenik a látogató Internet böngészőjén.

6 Scriptek futtatása weboldalon keresztül

6.1 Meghatározás

Hibásan beállított webszereverek kihasználásával egy támadó lefuttathat rosszindulatú kódokat az internetböngészőn. Az alábbi hibákat tartalmazó webszervereket lehet ily módon kihasználni:

- A webszerver bekér adatot a böngészőtől (pl. űrlapon keresztül), és visszaküldi ezt az adatot a böngészőnek.
- A webszerver nem szűri az adatot, amit bekér a böngészőtől, majd feldolgoz és visszaküld.

A támadó úgy formálja a szervernek küldött adatokat, hogy az speciális karaktereket tartalmaz. Amikor azt a szerver visszaküldi, a böngésző elindít egy rosszindulatú scriptet. A támadó elhelyezhet egy linket egy weboldalon vagy elküldheti azt e-mailben. A link tartalmazza a webszervernek elküldendő adatot, és egy scriptet a rosszindulatú kóddal.

Például: http://www.példa.com/neve=Janos<script>támadás</script>. A weboldal a 'neve' után lévő nevet felhasználja a látogató személyes üdvözlésére. Viszont ahogy az adatokat visszaküldi a szerver a böngészőnek, a rosszindulatú scriptet is visszaküldi. A scriptet pedig a böngésző lefuttatja. További fenyegetést jelent, hogy úgy tűnik, mintha a script a kihasznált weboldaltól származna. Komoly kár okozható, ha a látogató a weboldalt megbízhatónak tartja.

6.2 Lehetséges biztonsági intézkedések

6.2.1 A böngésző oldalán

- Az internetböngészőnek ne engedélyezzük a scriptek automatikus lefuttatását. Amennyiben a script futtatása szükséges a weboldal (és azt megbízhatónak tartjuk) használatához, csak a honlapról kiindulva engedélyezzük azt.

- Ellenőrizzük a hivatkozások tartalmát és forrását mielőtt arra klikkantanánk. Vigyázzunk, mert a státuszsor a legtöbb böngészőn megváltoztatható. HTML forráskód szinten lehet csak biztosra menni a hivatkozás tartalmáról. Ehhez némi szakértelemre van szükség.

6.2.2 A webszerver oldaláról

- Korlátozzuk a böngészőnek visszaküldött adatokat. Ez elérhető minimális adatbekéréssel.
- Legyen a lekért adatoknak egy felső korlátja, és ellenőrizzük a korlát betartását.
- Töröljük a <script>, <object>, és <embed> beágyazott elemeket, ha nem szükségesek.
- Ha lehetséges, csak a HTTP POST-tól fogadjunk el adatbevitelt. HTTP POST leválasztja az adatot az URL-től, míg a HTTP GET esetében az URL tartalmazza az adatot is. Bár scriptek futtatása weboldalon keresztül lehetséges a HTTP POST használatával is, de az sokkal ritkább.
- Ellenőrizzük a sütik tartalmát, mielőtt elküldjük a böngészőnek.
- Használjunk viszonyazonosítást. Adjunk minden látogatónak egy viszonyazonosítót, amit csak egyetlen lapról (pl. a honlapról) kaphat a látogató. Érvénytelen viszonyazonosító esetén, küldjük a látogatót a honlapra. Viszonyazonosítót tehetünk az URL-be vagy egy sütibe. Ennek az a hátránya, hogy a weblap mélyebb szintjeire nem lehet hivatkozni.

- A weboldalon egy meghatározott kódolást használjunk (pl. ISO-8859-1), hogy egyértelműek legyenek a speciális karakterek.
- Szűrjük ki a speciális karaktereket a böngésző által szolgáltatott adatokból. Határozzuk meg, mik az engedélyezett karakterek és semmi mást ne engedjünk be.
- Hivatkozásokat csak bizonyos forrásoktól engedélyezzünk. És ellenőrizzük a hivatkozó mező tartalmát a HTTP fejlécben. Ezzel vigyázni kell, ugyanis ez a mező hamisítható.
- Szűrjük ki a speciális karaktereket a böngészőnek küldött adatokból. Annak ellenére, hogy ez úgy tűnik, mint a bejövő adatok szűrésének ismétlése, szükség lehet rá. A bejövő és kimenő adatok formátuma különbözhet. Tehát lehetséges, hogy a bejövő adatoknál egyes speciális karakterekre szükség van, míg azok elküldésére viszont semmi szükség nincs.

6.3 Büntethetőség

Az ilyen esetekben használt scriptek általában kárt okoznak a célrendszerben. Adatok módosulhatnak, sőt behatoláshoz is vezethet. Az adatok módosítását és a behatolást a törvény bünteti.

7 (Elosztott) szolgáltatásmegtagadásos támadás

7.1 Meghatározás

Szolgáltatásmegtagadásos támadás esetén az a cél, hogy egy számítógépes rendszert, hálózatot, vagy szolgáltatást elérhetetlenné tegyenek, úgy hogy azt túlterhelik. A támadás jöhet egy vagy akár egyszerre több számítógépről. Egyetlen számítógépről indított támadást **szolgáltatásmegtagadásos támadásnak (DoS[12])** nevezünk. Több számítógépről indított támadást **elosztott szolgáltatásmegtagadásos támadásnak (dDoS[13])** nevezünk.

A dDoS támadásokat árasztásos DoS támadásokra használják. Viszont a hatásuk sokkal nagyobb, ugyanis egyszerre több számítógépről indul a támadás. A korlátozott készletek felfalásához és árasztásához használt DoS támadásokat fel lehet használni dDoS támadások végrehajtására is, csak jóval nagyobb hatásfokkal.

dDoS támadás esetén a támadó sok daemont, továbbá néhány vezérlő programot is küld a gyanútlan felhasználók számítógépeire. A támadó a vezérlőket irányítja, a vezérlők pedig a daemonokat irányítják. A daemonok pedig a támadást hajtják végre. Mivel sok daemon van, ezért súlyos támadást lehet indítani bármilyen célszámítógép ellen.

A daemonokat és mastereket főként személyi számítógépekre telepítik. Ezeknek a gépeknek a biztonsága minimális (vagy nincs) ugyanis az átlag felhasználó nem rendelkezik a számítógépek biztonságos beállításához szükséges szaktudással. Továbbá a széles sávú internet szolgáltatások elterjedése az otthonokban nagy támadási erőt biztosít minden egyes daemonnak.

Modern dDoS eszközök könnyen használhatóak és magas fokon automatizáltak. Egyes eszközöknél pedig a masterek képesek a vándorlásra is. Ez a jelenség nagyon megnehezíti a támadó lenyomozását.

A szolgáltatásmegtagadásos támadásnak három alapvető eleme van:

- Korlátozott készletek felfalása, és árasztása.
- Beállítások tönkretétele.
- A rendszer fizikai tönkretétele (nem kimondottan kibernetikai bűncselekmény).

7.2 Támadási típusok

7.2.1 Korlátozott készletek felfalása, és árasztása

Egy rendszer működésének szüksége van bizonyos készletekre, hogy rendeltetésszerűen tudjon működni (pl. memóriára, CPU-ra, lemezterületre, hálózati sávszélességre stb.). Egy támadó ezeket a készleteket felhasználhatja, vagy elárasztathatja. Ennek következtében a rendszer összeomlik vagy nem lesz elérhető a támadás ideje alatt.

Néhány ilyen támadási példa:

a. SYN árasztás
b. Smurf támadás
c. Fraggle támadás
d. Syslog támadás
e. e-mail bomba

[12] DoS (Denial of Service) Szolgáltatásmegtagadás.
[13] dDoS (distributed Denial of Service) Elosztott Szolgáltatásmegtagadás.

a. SYN árasztás

A SYN árasztás a TCP kapcsolat kialakításához szükséges háromkézfogásos eljárást használja ki. Egy TCP kapcsolat kialakításához hoszt A küld egy SYN csomagot hoszt B-nek. Hoszt B válaszol egy SYN/ACK csomaggal, amire hoszt A válaszol egy ACK csomaggal.

Támadás során hoszt B nagy mennyiségű SYN csomagot kap, ami hamisított IP címet tartalmaz. Hoszt B mindegyikre válaszol egy SYN/ACK csomaggal, és lefoglal egy memóriaterületet a kapcsolat részére. Utána hoszt B vár a válaszra, ami nem fog jönni. Egy idő után hoszt B feladja a várást, és felszabadítja a lefoglalt memóriát.

- A támadás felemészti a memóriát, és hiteles folyamatok nem tudják a dolgukat végezni. A rendszer összeomolhat. A támadás hiteles TCP kapcsolatokat nem képes kialakítani.
- A SYN árasztás felismerhető jelei:
  - hoszt B szokatlanul sok SYN csomagot kap egy vagy több IP címről
  - hoszt B-n hirtelen megnő a forgalom
  - hoszt B átlag csomagmérete lecsökken.

b. Smurf támadás

A Smurf támadás az úgynevezett irányított adatszórás elvét használja ki. Ez azt jelenti, hogy csak egy megcélzott hálózat lokális hálózatán belül lesz az adat elküldve minden számítógépnek (minden hálózatnak van úgynevezett adatszórási címe). Amíg a hálózatot el nem éri, egyetlen csomagként továbbítódik.

Smurf támadás esetén egy ICMP[14] 'echo request' csomagot küld a cél hálózatnak. Ez a csomag egy hamis forrás IP címet tartalmaz, ami a támadni kívánt számítógép IP címe. A csomagra válaszolva minden számítógép a hálózatban (egyszerre) 'echo reply' csomagot küld a hamis forráscímre. A megtámadott számítógép nem lesz képes hiteles hálózati forgalom lebonyolítására, mert a támadásból kifolyóan nagy mennyiségű ICMP csomagot kap. 1 ICMP 'echo request' csomag egy 254 számítógépes hálózaton, 254 ICMP 'echo reply' csomagot fog produkálni.

A smurf támadás felismerhető jelei:

- a rendszer szokatlanul sok ICMP csomagot kap
- a rendszeren hirtelen megnő a forgalom
- a csomagok átlagmérete lecsökken
- az aktív kapcsolatok elakadnak, vagy nagyon lelassulnak
- a lokális hálózatot az internethez kapcsoló útválasztó ICMP 'echo request' csomagokat kap a lokális hálózaton kívülről.

c. Fraggle támadás

Majdnem ugyanaz, mint a smurf támadás, de ICMP 'echo request' csomag helyett UDP 'echo request' csomagot küld.

d. Syslog támadás

Hálózati eszközök úgy vannak beállítva, hogy egyes eseményeket (pl. magas hőmérséklet, beállítás változtatás stb.) jelentse a Syslog-nak. Ezeket a jelentéseket az 514-es UDP portra küldik. Egy úgynevezett Network Management Station (NMS), fogadja, feldolgozza, és ha kell, figyelmezteti a rendszer működtetőjét a SYSLOG üzenet tartalma alapján.

[14] ICMP (Internet Control Message Protokol) az Internet hiba és vezérlő üzenet továbbító protokollja.

Sajnálatos módon ezeket az üzeneteket is lehet hamisítani, ami vaklármát okoz a rendszer működtetője számára.

Ennek a támadásnak az ismertető jele: sok üzenet az 514-es UDP portra.

e. E-mail bombák

Ez régebbi jelenség, ami mostanában nem nagyon elterjedt. E-mail bombázás esetén egy e-mail szervert vagy csak egy fiókot elárasztanak e-mail üzenetekkel. Ez megakadályozza a személyt vagy szervezetet a levelekhez való hozzáférésben.

E-mail bombázás akaratlanul is történhet, spamből kifolyólag. Spamet küldenek hamisított feladó címmel, de ez a feladó cím létezik (valaki másnak a címe). Minden spammel kapcsolatos hibaüzenetet (pl. ha nem létezik a cím) ez a harmadik gyanútlan fél kap meg.

7.2.2 Beállítások tönkretétele

Azok a rendszerek, amelyek nincsenek jól beállítva, nem tudnak rendesen működni. Hackerek tönkretehetik vagy módosíthatják a rendszer beállításait. Ennek következményeként a rendszer nem fog (rendeltetésszerűen) működni. A hackernek be kell hatolnia a rendszerbe, hogy meg tudja változtatni a beállításait (vagy éppen tönkretegye, kitörölje). A beállítások tönkretétele nagyon sokféle módon elvégezhető, ezért a módszereket nem tárgyaljuk meg részletesebben.

7.3 Lehetséges biztonsági intézkedések

- SYN sütik használata a SYN árasztás ellen. Egy kapcsolat sorszámmal ellátott SYN csomagot küld válaszként a SYN csomagra, hogy meggyőződjön a kapcsolatkiépítés tényleges szándékáról. Addig nem készítjük elő a kapcsolatot, és nem foglalunk le memóriát, amíg meg nem győződtünk a kapcsolatkiépítés tényleges szándékáról.

- RST sütik használata a SYN árasztás ellen (ez a megoldás nem annyira elterjedt, mint az előző; elég az egyik megoldás használata). Az RST csomag egy hibás SYN/ACK csomag.

- Tiltsuk le az irányított adatszórást a hálózatban minden egyes gépen.

- Figyeljük a hálózat sávszélességét.

- Figyeljük az átlagos csomagméreteket a hálózaton.

- Szolgáltatás minőség (QoS) nyújtása érdekében korlátozzuk a szerver számára kevésbé szükséges protokollok (pl. ICMP) használatát, sávszélességét.

7.4 Büntethetőség

Egyes DoS támadások során a támadó behatol a támadott rendszerbe (pl. beállítások tönkretétele esetén), ami a magyar törvények szerint számítógépes bűncselekmény. Illetéktelen adatmódosítás is történik ebben az esetben.

dDoS támadások során a támadó megakadályozza egy rendszer rendeltetésszerű működését. Természetesen a támadások célja, hogy üzemképtelenné tegye a célba vett rendszert.

Elosztott szolgáltatásmegtagadásos támadás esetében több számítógép indít valamilyen DoS támadást egyszerre egy célgép ellen. Emiatt dDoS támadások sokkal hatásosabbak és veszélyesebbek. Viszont legtöbb esetben a támadó számítógépek tulajdonosai nem tudják,

hogy az ő gépüket támadásra használják. A támadást indító program a tudtuk nélkül lett telepítve a számítógépükre, ami szintén behatolásnak számít. Sőt, a számítógépen tárolt adatokat (fájlokat) is meg szokták a hackerek változtatni.

8 Portok letapogatása

8.1 Meghatározás

Portok letapogatásának célja, hogy kiderítsük, futnak-e szolgáltatások egyes portokon, és milyen operációs rendszer fut a számítógépen. A letapogatást felderítő akcióként lehet felfogni egy behatolási kísérlet előtt.

A letapogatás úgy történik, hogy a célgépnek küldenek bizonyos csomagokat. A számítógép reakciójából (válaszol a csomagra vagy nem, és ha válaszol, akkor mit tartalmaz a csomag) el lehet dönteni, hogy fut-e szolgáltatás egy bizonyos porton. A letapogatás felismerhető bizonyos eszközökkel, tehát a célba vett számítógépes rendszer működtetője tehet lépéseket a behatolás megelőzésére.

Vannak úgynevezett „stealth scannerek". Eredetileg ezeket nem lehetett felismerni, de mostanára már kidolgoztak technikákat a felismerésükre. Ennek ellenére ezek a letapogatások még mindig nehezen felismerhetők, ugyanis nagyon hasonlítanak a hiteles forgalomra. Amikor megkapunk egy csomagot, nem mindig lehet eldönteni, hogy az a csomag hiteles forgalom része vagy nem. Egyes esetekben ezt csak utólagosan lehet eldönteni.

8.2 Letapogatási technikák

Az alábbi lista tartalmazza a leggyakoribb port-letapogatási technikákat:

- **TCP connect scan**

Ebben az esetben a TCP kapcsolatot teljesen kiépíti a két számítógépes rendszer (a támadó és az áldozat). A teljes kézfogási eljárás végrehajtódik: SYN → SYN/ACK → ACK. Ez az eljárás nagyon megbízható és nehezen észlelhető, ugyanis a kapcsolat kiépítése hiteles TCP/IP fejlécet tartalmaz és a kapcsolat kiépítését sem szakítja félbe. Ezt csak utólag lehet azonosítani.

- **SYN scan**

Ez a letapogató nem hajtja végre a teljes kézfogási eljárást, és így nem építi ki a kapcsolatot. A támadó megszakítja a kapcsolatot: SYN → SYN/ACK → RST. Ezt a letapogatási módszert is csak utólagosan lehet észlelni.

- **SYN/ACK scan**

A SYN/ACK scan nem használja ki a kézfogási eljárást. Ebben az esetben a támadó küldi először a SYN/ACK csomagot. A nyitott portok erre nem adnak választ, de ha nincs szolgáltatás a megadott porton, akkor egy RST csomagot küld vissza a gép.

- **FIN scan**

A támadó először egy FIN csomagot küld. A nyitott portok erre nem adnak választ, de ha nincs szolgáltatás a megadott porton, akkor egy RST csomagot küld vissza a gép.

- **NULL scan**

A NULL scan esetében a csomagoknak nincs egy jelzőjük sem bejelölve. A nyitott portok erre nem adnak választ, de ha nincs szolgáltatás a megadott porton, akkor egy RST csomagot küld vissza a gép.

- **XMAS scan**

Az XMAS scan esetén a csomagok összes jelzője meg van jelölve. A nyitott portok erre nem adnak választ, de ha nincs szolgáltatás a megadott porton, akkor egy RST csomagot küld vissza a gép.

- **UDP ICMP_PORT_UNREACHABLE scan**

TCP helyett az UDP portokat tapogatja le. Egy UDP datagram elküldése egy portra kimutatja, hogy azon a porton fut-e szolgáltatás. A nyitott portok erre nem adnak választ, de ha nincs szolgáltatás a megadott porton, akkor egy „port unreachable" (port nem elérhető) ICMP üzenetet küld vissza a gép.

- **Félrevezető letapogatás**

Ez a letapogatáshoz használt technika egyike. A félrevezetés azon alapszik, hogy a csomagok nagy részét hamis IP címmel küldjük el. Ez megnehezíti a támadó IP címének lenyomozását, főként ha a hamis IP címek léteznek. Minél több hamis IP címet használunk, annál nehezebb a támadó IP címét azonosítani. Viszont szükség van olyan csomagra, ami a letapogató valódi IP címét tartalmazza, ugyanis a célgép által adott válasz neki is meg kell kapnia.

8.3 Lehetséges biztonsági intézkedések

Valójában a letapogatás nem előzhető meg, bár a letapogatás által nyert információk hasznossága csökkenthető. Tűzfalak és IDS[15]-ek képesek észlelni bizonyos letapogatásokat a tulajdonságai alapján, viszont stealth scan esetén nem hatásosak. Letapogatás ellen a következő technikákat érdemes bevetni:

- Csak használt portokhoz küldött csomagokat engedjünk be a rendszerbe. A többi porthoz irányított csomagokat ne engedje át a tűzfal.

- Figyeljük a csomagokat a szállítási szinten[16] és szűrjük ki SYN/RST/ACK hibás használatát.

- Szűrjük ki az ICMP 3-as (destination unreachable) és 8-as (echo request) típusú üzeneteket.

- Szűrjük a csomagokat az alkalmazási szinten[17] is a csomagok tartalma alapján.

- Portsentry használata. Program a letapogatások észlelésére. Képes a stealth scan felismerésére is. A scan felismerése után automatikusan tilthatja a forráscímet, figyelmeztethet, és akár más programokat is képes elindítani a további letapogatás és behatolás megelőzése érdekében.

- Nyilvános szolgáltatások (pl. SSH) ne fussanak magas (1024 felett) portokon.

[15] IDS (Intrusion Detection System) Behatolás észlelő rendszer.
[16] A 7-szintű OSI (Open Systems Interconnection) modell 4.-ik szintje.
[17] A 7-szintű OSI (Open Systems Interconnection) modell 7.-ik szintje.

8.4 Büntethetőség

A portok letapogatása során csak információszerzés történik. Nem tesz kárt számítógépes rendszerekben, nem módosít adatokat, és nincs behatolás. Tehát a portok letapogatása nem bűncselekmény.

9 Spoofing[18]

9.1 Meghatározás

A spoofing, azaz hamisítás azt jelenti, hogy valaki másnak a személyiségét (azonosítóját) vesszük magunkra; másnak adjuk ki magunkat. Ezt az eljárást a támadók szívesen használják, ugyanis nagyon megnehezítheti a lenyomozásukat.

Az interneten használt azonosítók formáját szabványok határozzák meg, és az azonosítókat hivatali szervek osztják szét és adják ki. Sajnos mivel ezek a szabványok nyilvánosan is elérhetők, az azonosítók hamis használatát lehetővé tevő szoftvereszközöket (elegendő szaktudással) bárki létre tud hozni. Ilyen eszközökhöz bárki ingyen hozzáférhet, és használatuk nem igényel komoly számítógépes szaktudást.

Az interneten több azonosító információt is lehet hamisítani. Sőt, egy támadó ezeket kombinálhatja is. Így fokozza a nyomozás nehézségét. Következőként a spoofing típusait ismertetjük a hamisított információ alapján.

9.2 IP spoofing

9.2.1 Meghatározás és használat

A támadó az IP csomagoknak a célszámítógép által megbízhatónak tartott IP címet ad meg forrás IP címként. Ezt az illetéktelen hozzáférés elnyerése érdekében teszi. IP cím hamisítás esetén csak egyirányú forgalom lehetséges (hacker → célgép), ugyanis a hacker nem kap meg semmilyen választ. Minden választ a hamis IP címre küld a célba vett gép.

9.2.2 Felismerés

Az IP spoofing felismerésére lehet hálózatfigyelő alkalmazásokat használni (pl. net log). Például, ha a külső hálózati interfészen (ami a belső hálózatot az internethez kapcsolja) küldött csomagok forrás és cél IP címe belső hálózati cím, akkor hamis IP címmel van dolgunk.

Sikeres támadás IP spoofing használatával a következő módon ismerhető fel. Az áldozatul esett gépen van naplózási bejegyzés távoli bejelentkezésről. Ezzel ellentétben a látszólagos forráscímet használó gépen nincs naplózási bejegyzés a távoli bejelentkezés kezdeményezéséről. Tehát a hamisításra használt címről senki nem jelentkezett be a feltört gépbe.

9.2.3 Lehetséges biztonsági intézkedések

A leggyakrabban használt megoldás ilyen támadások ellen a forráscím szerint irányított (source-routed) csomagok tiltása és belső címekkel rendelkező (az internet felől) beérkező csomagok ejtése, továbbá azon csomagok ejtése, amelyeknél a forrás- és célcím megegyezik.

A routerek ismernek egy úgynevezett „verify unicast reverse path” eljárást. Ez egy spoofing ellen használt eszköz. A router tudja, milyen IP címek vannak az egyes interfészek mögött. Ellenőrzi a forrás IP címet a routing táblázat alapján. Ha az interfész mögött nem létezik a megadott forráscím, akkor a csomag hamis IP címet tartalmaz.

[18] A „spoofing” angol kifejezés magyar megfelelője a „hamisítás”.

9.3 ARP[19] spoofing

9.3.1 ARP gyengesége

A hálózaton egy számítógépnek két címe van, MAC[20] címe és IP címe. Az IP címet szoftveres úton adjuk meg. A MAC címet pedig a gyártó adja meg az ethernet hálózati interfész kártyának. Ez egy hardver cím és minden hálózati eszköz egyedi MAC címet kap gyártáskor. Ahhoz hogy a hálózaton átküldött adatokat megkapja a célgép, a MAC és IP címet egyaránt tudni kell.

Amennyiben tudjuk egy számítógép IP címét, a hozzá tartozó MAC címet ki lehet deríteni úgynevezett „ARP request" küldésével. Az „ARP request" tartalmazza a célgép IP címét és adatszórással (az adatszórás MAC címe FF:FF:FF:FF:FF:FF:FF:FF) minden számítógép megkapja a hálózaton (még kapcsolt hálózaton is). A keresett IP cím tulajdonosa válaszol a kérésre és elküldi a MAC címét. A MAC-IP címpárt az operációs rendszer egy ARP táblázatban tárolja.

Az ARP gyengesége abban jelentkezik, hogy a számítógép tárolja az ARP válaszban küldött MAC-IP párt akkor is, ha azt nem kérte. Ez az adatszórásos ARP request üzenetek minimalizálása érdekében működik így. Viszont egy támadó ezt kihasználhatja és küldhet kéretlen ARP válaszokat. Ezzel azt tudja elérni a támadó, hogy egy másik gépnek szánt üzenetet a támadónak küld az áldozat gépe.

9.3.2 ARP spoofing céljai

- **sniffing**

Sniffinget avagy a hálózati forgalom lehallgatását lehetővé tudja tenni egy támadó, még kapcsolt hálózaton keresztül is. Az ARP lekérdezésre a válasz a hálózati adatszórási címét párosítja a kért IP címhez. Így az IP címhez küldött adatokat mindenki megkapja a hálózaton, a támadót is beleértve. Ez szolgáltatásmegtagadást idézhet elő a hálózaton, ugyanis az adatszórás miatt megnő a forgalom.

- **klónozás**

A MAC címeknek elvileg egyedinek kell lenniük a világon. Régen a hálózati kártya ROM-ja tárolta a MAC címet, viszont a mostani kártyák MAC címeit már meg lehet változtatni. A MAC klónozás azt jelenti, hogy a támadó megváltoztatja a MAC címét egy másik számítógép címére. Így a számítógép lehallgathatja a klónozott számítógépnek küldött üzeneteket.

- **MiM (man-in-the-middle)**

Ebben a támadási módszerben egy támadón (T) keresztül megy minden internet forgalom két hoszt (A és B) között.

- T küld egy ARP választ A-nak. Az ARP válasz tartalmazza B IP címét, és T MAC címét.
- A bejegyzi az új IP-MAC párost.
- T küld egy ARP választ B-nek. Az ARP válasz tartalmazza A IP címét, és T MAC címét.
- B bejegyzi az új IP-MAC párost.
- A és B közötti forgalom T-n keresztül megy, így T megvizsgálhatja annak tartalmát.

[19] ARP (Address Resolution Protocol) Címfeloldási protokol.
[20] MAC (Media Access Control) Közeg hozzáférési vezérlő cím. A világon minden ethernet kártyának az egyedi azonosító száma.

Az MiM támadás nagyon veszélyes, ugyanis nem csak hosztok, hanem routerek és gatewayek ARP táblázata is megváltoztatható. Ráadásul nyilvános kulcs forgalom (pl. SSL) esetén a kulcsokat is meg tudja a támadó szerezni. Tehát titkosított információ is könnyen visszafejthető.

9.3.3 Lehetséges biztonsági intézkedések

ARP spoofing ismertető jelei:

- IP címhez társított MAC cím hírtelen megváltozik.
- Egy MAC cím többször is megtalálható az ARP táblázatban.

Sajnos ezek az ismertető jelek nem egyértelműen az ARP spoofing jelei. Például DHCP használata esetén az IP címekhez társított MAC címek megváltoznak, akárhányszor a DHCP szerver új IP címet ad egy számítógépnek. Proxy-ARP használata esetén pedig egyszerre több IP címhez lehet ugyanaz a MAC cím társítva egy ARP táblázatban. Például a routerek esetén a router a külső IP címekhez a router MAC címe lesz párosítva a belső hálózat számítógépeinek ARP táblázatában.

Valójában az egyetlen biztonságos megoldás ARP spoofing ellen a statikus ARP táblázatok használata. Az ARP táblázat adatai nem változhatnak, ezért az ARP válaszokról nem vesz tudomást a számítógép. Mivel karbantartásuk nehéz és lassú (ember által végzett munkát igényel), használatuk legtöbb hálózat esetén nem ajánlott.

Kapcsolt hálózat esetén egyes kapcsolóknál megoldható a „MAC binding” (hívják még „Port Binding”-nak vagy „Port Security”-nek). Ez azt jelenti, hogy a kapcsoló ARP táblázatát csak a rendszergazda változtathatja meg.

Általános biztonságos megoldást nyújt érzékeny adatok továbbítására a nyilvános kulcsú titkosítást használó adatforgalom, megbízható harmadik fél által aláírt hitelesítési tanúsítványok átadásával. Ez főként a MiM támadások ellen hatásos. Ez sajnos közel sem eléggé elterjedt ahhoz, hogy mindenféle kommunikáció esetén használható legyen.

ARPsec az ARP biztonsági bővítése. Ez kompatíbilis az eredeti ARP protokollal is, viszont képes az információk hitelesítésére és sértetlenségének ellenőrzésére. Tehát az ARP csomagokat nem lehet majd hamisítani. Ez az ARP jövője és (remélhetőleg) az elterjedésével megszűnnek az ARP által lehetővé tett támadások. Az ARPsec-re egyenlőre még várnunk kell, ugyanis jelenleg fejlesztés alatt áll.

9.4 DNS spoofing

9.4.1 Meghatározás és használat

A DNS szerverek és a cache name-szerverek manipulálása. A hacker rendszere küldhet hamisított információt a DNS vagy cache szervernek. Ennek következtében azt hiszi a szerver, hogy az információ megbízható forrásból jön. Így a hacker megváltoztathatja a szerveren tárolt adatbázis tartalmát.

A hacker több módon is megvalósíthatja a DNS hamisítást:

- A hacker behatol a DNS szerverbe és megváltoztatja a hoszt szerver nevéhez tartozó IP címet. Az új IP cím egy olyan számítógép címe, ami a hacker irányítás alatt áll, vagy az interneten nem létező cím[21]. Ennek az a következménye, hogy az adat nem a megcélzott címre megy.

[21] RFC1918 IP címek vagy nem-kiosztott IP címek.

- A támadó meghamisítja a cache szerver válaszát, mielőtt a hiteles válasz megérkezne. A későn érkező választ a számítógép eldobja. A weboldal karbantartója nem mindig tudja meg az átirányítást, mivel a cache szervert nem ő vezérli, és nem jelentik neki.

- A támadó meghamisítja a cache szerver által tárolt információt. Ezt kétféle képen tudja megtenni:
  - A hacker által küldött információnak magasabb a TTL (Time-To-Live) jelzője, mint a cache szerveren tárolt adatoké. A cache szerver kicseréli a tartománynévhez tartozó bejegyzést a hamis információra.
  - A hacker elrejti a hamis információt egy weboldal domain nevéről (pl. domain A) egy másik domain név (pl. domain B) zóna fájljába. Amikor domain B-ről kérnek információt, akkor domain A hamis információját is elküldi.

9.4.2 Lehetséges biztonsági intézkedések

Az alábbi biztonsági intézkedések egy bizonyos weboldal hivatalos DNS szerverére vonatkoznak. A legkomplikáltabb a cache szerverek biztonsága, ugyanis nagyon sok cache szerver létezik a világon, amik független szervezetek irányításai alatt álnak.

- IDS és tűzfal használata behatolás ellen.
- A behatolások észlelésére használjunk fájl-integritás ellenőrző programokat, mint például a Tripwire.
- Biztosítsuk azt, hogy zóna átadások csak hiteles névszerverek között engedélyezett.
- Tiltsuk a domainek dinamikus frissítését.
- Hiteles névszervereknek engedélyezzük az inverz lekérdezést.
- Elosztott DNS használata. Ez azt jelenti, hogy a cache szervert a belső hálózaton használjuk. A belső hálózaton kívül helyezkedik el a DNS szerver, ami csak a szervezethez tartozó tartományokat referál. Így a hacker nem tudja megváltoztatni a DNS cachetárját.
- Naplózzuk a lekérdezések teljes adatát.
- Naplózzuk a zóna átadásokat IDS-el vagy tűzfallal, ha nem hivatalos névszervertől jön.
- Titkosítsuk a TLD[22]-kel cserélt információt (pl. crypt, MD5 vagy PGP).

9.5 E-mail spoofing

9.5.1 Meghatározás és használat

Az e-mail spoofing azt használja ki, hogy a legtöbb ember azt hiszi, hogy a feltüntetett feladó a tényleges feladó. Hamisított e-maileket főként arra használnak, hogy rávegyenek felhasználókat olyan adatok kiadására, amit nem kéne kiadniuk. E-mail spoofingot gyakran használják spam és e-mail bouncing[23] esetén.

A hamisított e-mailt nem lehet 100%-os bizonyossággal megkülönböztetni a hiteles e-mailektől. Azt lehetséges ellenőrizni, hogy a feladó tartománya létezik-e. Amennyiben a tartomány nem létezik, az e-mail spoofing egyértelmű. Viszont egy támadó könnyedén használhat létező tartományt, sőt létező e-mail címet is. Az e-mail címek létezésének ellenőrzése sajnos szinte lehetetlen.

[22] A TLD a Top-Level Domain rövidítése. Az ezek által szolgáltatott tartományok például: .com, .hu, .org, .net
[23] E-mail üzenetek visszaküldését jelenti.

9.5.2 Lehetséges biztonsági intézkedések

E-mail spoofing ellen nem létezik biztonságos védekezés. Emiatt minden felhasználó kellő óvatossággal járjon el, amikor az e-mailjeit kinyitja és a benne lévő információt, és linkeket használja.

9.6 Büntethetőség

Általában spoofing esetében illetéktelen behatolás történik egy számítógépes rendszerbe, ami büntethető. Továbbá adatok módosulhatnak és rongálódhatnak, sőt egy számítógépes rendszer működésében is okozhatnak meghibásodást. Mindezt bünteti a törvény.

10 Férgek és vírusok

10.1 Meghatározások

A férgeknek nincs általánosan elfogadott meghatározásuk. A férgek és vírusok közötti különbség meghatározása vitatott.

10.1.1 Férgek

Általában a férgek olyan programok, amik többszörösítik magukat. Ez történhet automatikusan, emberi beavatkozás nélkül, vagy valamilyen minimális emberi beavatkozással.

Más meghatározások szerint pedig a férgek csak a számítógép memóriájában léteznek. Nem teszik be magukat a számítógép fájlrendszerébe, és nem változtatnak meg fájlokat a fájlrendszerben.

10.1.2 Vírusok

A vírus általában olyan program, ami a saját kódját hozzáadja már létező programok kódjaihoz. Ezt az eljárást fertőzésnek nevezzük.

10.1.3 Közös tulajdonságok

Vannak férgek és vírusok, amik képesek megváltoztatni saját magukat, így megnehezítik az észlelésüket. Az ilyeneket polymorph férgeknek és vírusoknak nevezzük.

Férgeket és vírusokat kombinálhatnak trójai falovakkal a terjesztés elősegítése érdekében.

10.2 Többszörösítés

10.2.1 Hálózaton keresztül

A hálózaton keresztüli többszörösítés emberi beavatkozás nélkül történik.

- **Sérülékenység által**

A többszörösítés történhet valamilyen szoftver sérülékenység kihasználásával. Például puffer túlcsordulással aktiválhatja magát a féreg vagy vírus egy távoli számítógépen (pl. Slammer az SQL szervereken, vagy Ramen FTP szervereken).

Ez a terjedési mechanizmus nem rugalmas, ugyanis puffer túlcsordulás csak bizonyos körülmények között történhet. Ennek következtében a terjedés észlelhető a hálózati forgalom analizálásával (IDS és hálózat figyelő eszközök segítenek az észlelésben).

Amennyiben a féreg vagy vírus agresszív, a forgalom leterhelheti a hálózatot és DoS-t okozhat.

- **Fájlok megosztása által**

A többszörösítés történhet a hálózaton megosztott fájlok által vagy egy belső hálózaton keresztül. Például egy hibás beállítás írási jogot ad jogosulatlan felhasználók számára. A vírus vagy féreg átmásolja magát egy másik helyre a hálózaton belül.

A terjedés automatikus, de az aktiváció általában újraindításkor történik meg. A féreg vagy vírus beírhat egy linket saját magához az alábbi helyekre, és a rendszer újraindításakor a vírus is elindul:

  - Start-up. Minden Windowsban van egy olyan hely, ahova a felhasználó tehet programokat, amiket szeretne minden induláskor elindítani.

- Registry. A registry-ből is lehet programokat indítani bekapcsoláskor, illetve újraindításkor. Nem annyira feltűnő a felhasználó számára, mint a Start-up.

10.2.2 E-mailen keresztül

E-mailen keresztül történő többszörösítés úgy történik, hogy a féreg vagy vírus e-mail címeket keres egy megfertőzött gépen. Több helyről is gyűjt címeket: címjegyzékekből, levél mappákból és helyi fájlokból is. Az összegyűjtött címekre elküldi magát a féreg vagy vírus.

Legtöbbjük tartalmaz algoritmusokat az e-mail felismerésének nehezítésére. A téma szövegét megváltoztatják, sőt a csatolt fájlokat is dinamikusan módosítják. Ezeket az e-maileket nagyon nehéz felismerni. A legjobb védekezés az, hogy az ismeretlen csatolt fájlokat ne nyissuk ki.

Nagymennyiségű e-mailek továbbítása leterhelheti az e-mail szervereket és a hálózatot. Egyes szerverek akár összeomolhatnak a szokatlanul magas e-mail forgalom miatt. Ezek a férgek és vírusok DoS-t okozhatnak.

10.2.3 További fájlok fertőzésével

Egy vírus többszörösítheti magát más fájlok megfertőzésével, bár ez az eljárás eléggé lassú. A vírusok hozzáadhatják magukat programokhoz, de scriptekhez és makrókhoz is. Ilyen változások esetén a fájl méretének növekedése a jellemző. Néhány antivírus szoftver a fájlok méretének változásait figyeli. A vírusirtó programok nagy része megvizsgálja a fájlok sérülékeny pontjait, és vírusok jellemző kódjait keresik.

10.3 Lehetséges biztonsági intézkedések

- Antivírus programok használata automatikus napi frissítéssel.
  - A hálózati átjárókon figyeljék a http, ftp, smtp stb. protokollokat.
  - Vizsgálják az e-maileket.
  - A szervereken és klienseken az ellenőrzés a fájlrendszer szinten folyjék.

- IDS bevetése; figyelje a hálózatot vírus- és féregforgalom észlelésére.

- Scriptek és makrók futtatásának letiltása.

- A felhasználók közötti tudatosság növelése a számítógépek biztonságos kezelésével kapcsolatosan. Ez különösen fontos az e-mail vírusok (és férgek) esetében, ugyanis sok esetben a vírus aktiválásához meg kell nyitni egy csatolt dokumentumot.

10.4 Büntethetőség

A férgek és vírusok jellemzője, hogy módosítanak, és kárt tesznek fájlokban és adatokban. Továbbá egyes esetekben jogosulatlan behatolás is történik. Mindkettő törvényellenes és büntethető.

11 Trójai falovak

11.1 Meghatározás

Trójai falovakat először a görögök használtak a trójai háborúban. A görögök a békeség jeléül egy falovat adtak ajándékba az ellenségüknek, a trójaiaknak. A trójaiak ezt a lovat hazavitték. Az éjszaka leple alatt görög harcosok jöttek elő a ló belsejéből, és kinyitották a város kapuit. A görögök így tudták bevenni Tróját.

Az informatikában használt trójai falovak ugyanezen az elven működnek. A felhasználó letölt egy számára hasznosnak tűnő programot (pl. egy vírusirtó program, vagy szoftverfrissítés). A hacker elrejtett vírusokat vagy kiskapukat megnyitó kódokat, vagy egyéb rosszindulatú kódokat ebben a programban. A gyanútlan felhasználó aktiválja ezeket a rosszindulatú kódokat. Az elrejtett vírusok megtámadják a gépeket. A kiskapuk pedig szabad uralmat adnak a hackernek a gép felett.

A trójai falovak felinstallálhatnak root-kiteket, ami a kernel egyik fontos részét helyettesíti. Ezután a fájlrendszer szinten nem észlelhető a trójai falovak jelenléte a rendszerben. A root-kitek kinyithatnak kiskapukat a hacker számára.

11.2 Ismertető jelek

A trójai falovakat nehéz felismerni. Az egyik gyakori ismertető jele, hogy egyszerre több folyamat fut a rendszeren, amit a felhasználó nem lát. A program által létrehozott hálózati forgalom is lehet ismertetőjele, bár azt el is lehet rejteni, ha kis mennyiségű adatot küldünk standard portokon.

Trójai falovak linkeket tesznek magukhoz az operációs rendszerbe, hogy a rendszer újraindításakor őket is elindítsa. Tehát jó kiindulópontok a felderítésükhöz a rendszer olyan pontjai, ahonnan programokat lehet indítani automatikusan.

11.3 Lehetséges biztonsági intézkedések

A trójai falovak az emberek bizalmát használják ki, ezért minden esetben fő az óvatosság. A felhasználó számára vannak lehetőségek a letöltött programok hitelességének ellenőrzésére. A programok MD5 lenyomatát ellenőrizzük installálás előtt, és ellenőrizzük, hogy az aláírt kulcs valójában a program fejlesztőjéhez tartozik. Továbbá antivírus programok is képesek észlelni trójai falovakat. Tehát az antivírus programmal is ellenőrizzük a programot installálás előtt.

11.4 Büntethetőség

A büntethetőség szempontjai ugyanazok, mint a férgek és vírusok esetén.

12 Sniffing

12.1 Meghatározás

A sniffing a hálózati forgalom lehallgatását jelenti. Ez történhet hálózati analízis miatt, például amikor a rendszergazda fel szeretné deríteni, van-e vírusforgalom a hálózaton. A sniffing történhet rosszindulatú hackerek által, aminek a célja lehet jelszavak és egyéb bizalmas információk elfogása. Egy sniffer[24] futhat a gépen a felhasználó tudta nélkül is. Trójai faló telepítése lehallgathatja a hálózati forgalmat, majd az adatokat elküldheti a hackernek. A wireless[25] hálózatok és a bluetooth elterjedése miatt a lehallgatás még egyszerűbb lett, ugyanis nem kell fizikai hozzáférés a hálózathoz.

12.2 Sniffer észlelés

Elvileg a sniffing észlelése nem lehetséges egy hálózaton. Hardver snifferek olyan hordozható gépek, amiket kizárólag a lehallgatásra készítettek. Ezeket a gépeket nem lehet észlelni, hiszen csak egyirányú adatforgalom van rajtuk, befelé.

Azokat a sniffereket, amiket általános gépekre telepítettek, néha lehetséges észlelni. Mivel általános gépekre vannak telepítve az operációs rendszer akaratlanul is küldhet csomagokat, ami elárulja a sniffer működését a gépen. Azt figyelembe kell venni, hogy 100%-os pontossággal nem lehet ezeket a sniffereket sem észlelni. Lehetnek „hamis pozitív” és „hamis negatív” eredmények. Észlelésük az alábbi módszerekkel történhet:

- **Ping módszer**

Amennyiben a sniffer egy általános gépre van telepítve, a gép válaszolni fog a pingekre. Küldjünk egy pinget a gyanús számítógép IP címére, de hamisítsuk meg a MAC címet egy, a hálózaton nem szereplő címre. Ha a gép válaszol a pingre, akkor a gép promiscous módban működik és hallgatózik. A ping módszer megkerülhető szoftver alapú MAC filterrel.

- **Ping módszer változatai**

Ping (ICMP) helyett lehet más protokollt is használni, ami általában választ ad.

- **DNS módszer**

Sok, nem kereskedelmi forgalomban lévő sniffer megpróbálja megkeresni a lehallgatott hosztok nevét inverz DNS lekérdezéssel. Ezek a snifferek észlelhetők az inverz lekérdezés figyelésével. Inverz lekérdezés akkor is történik, ha egy csomagot nem létező IP címre küldünk, ami ping sweep esetén is történhet. Ha ezeken az eseteken kívül történik inverz DNS lekérdezés, akkor valószínűleg egy sniffer dolgozik a hálózaton.

- **Csapda**

Ebben az esetben közvetve próbáljuk megállapítani snifferek létezését a hálózaton. Egy titkos (rajtunk kívül senki ne tudjon róla) felhasználói fiók felvétele a rendszerbe. Ebbe a fiókba gyakran belépünk, és feljegyezzük a belépések idejét. A fiókban naplózzuk a bejelentkezések idejét. Ha a számlánkra bejelentkezett valaki rajtunk kívül, akkor egy sniffer van a hálózaton. Sőt mi több, a lehallgatott információt felhasználva belépett a titkos fiókba. Ez a módszer csak akkor működik, ha tényleg senki nem tud a fiók létezéséről rajtunk kívül.

[24] Sniffer a lehalgatást (sniffing) végrehajtó eszköz.
[25] Wireless LAN a drótnélküli lokális hálózat.

12.3 Lehetséges biztonsági intézkedések

A hálózati forgalom lehallgatása nem megelőzhető a hálózatok felépítése és működése miatt (az információk megosztása céljából jöttek létre a hálózatok). Viszont a lehallgatás által nyert információ és annak használhatósága illetéktelen személyek által minimalizálható:

- Kapcsolók használata hubok helyett. Minden hálózati interfész, ami egy hubhoz van csatlakoztatva, megkap minden hálózati forgalmat. Így egy hálózati kártya promiscous módban lehallgathat minden forgalmat a hálózaton. A kapcsoló csak a célgépnek küldi csak el az adatokat. Sniffing hálózati kapcsoló esetén még mindig lehetséges, de komplikált.

- Titkosítás használata a leghatásosabb védekezés a sniffing ellen. Az információ, amit a snifferek megszereznek szinte használhatatlan. Wireless LAN esetén használjunk erősebb titkosítást.

12.4 Büntethetőség

Sniffing esetén adatok elfogása történik. Amennyiben a sniffing során valaki olyan adatokhoz jut, amik őt nem illetik meg (pl. üzleti, banki, szolgálati, állami titkok), akkor az törvényellenes. Viszont például hálózati analízis céljából történő sniffing esetén nincs bűncselekmény. Sniffing büntethetősége esetén a cél és a megkapott adatok felhasználása a mérvadó.

13 Jelszótalálgatás

13.1 Meghatározás és használat

A jelszótalálgatás alatt azt értjük, hogy egy program segítségével a hacker megpróbálja eltalálni egy ismert felhasználó jelszavát. A program adja meg a felhasználónevet és jelszót a bejelentkezéshez.

A program a jelszavakat veheti egy szótárból. Ebben az esetben a program a szótárban lévő szavakat sorra megpróbálja jelszóként használni. A szótár egy olyan szöveges fájl, ami gyakran használt és alapértelmezett jelszavakat tartalmaz. Egy szótárban általában nagyon sok szó szerepel, minél több szót tartalmaz, annál nagyobb az esély a jelszó eltalálására. Egy szótár tartalmazhatja az alábbi gyakori jelszavakat:

password
sesame
changeme
secret
sex
qwerty
money
pass
abc123
private
admin
123456
god
hello
111111

A jelszavak eltalálására használhatja a program a nyers erő megoldást is. Ebben az esetben nincs szótár. A program maga alkotja a jelszavakat a felhasználható karakterekből.

13.2 Lehetséges biztonsági intézkedések

Idővel a legnagyobb akadály is leküzdhető. Egy cracking program heteken keresztül is próbálkozhat a bejutással. Ez az idő bőven elegendő lehet a betörési kísérlet észlelésére. Viszont tennünk kell annak érdekében, hogy a jelszavak kitalálása minél tovább tartson. A jelszavak megadására (hogy nehezen kitalálható legyen) ki kell dolgozni egy szabályt, és annak pontjait tudatni a felhasználókkal és rávenni őket, hogy alkalmazzák ezeket a szabályokat a jelszavak kiválasztásánál. Ez csak is a felhasználók közreműködésével oldható meg. A felhasználók biztonsági tudatosságát növelni kell, hogy ők is megértsék a nehezen kitalálható jelszavak fontosságát.

Ajánlott szabályok a jelszavak kiválasztására:

- mindenkinek külön jelszava legyen (ne használjanak csoportos jelszavakat)
- jelszó hosszának meghatározása (minimum és maximum)
- jelszóváltás gyakorisága
- karakter változatosság (a jelszó tartalmazzon kisbetűt, nagybetűt és számot egyaránt)
- ne tartalmazza a felhasználói azonosítót, a felhasználó neveit és egyéb, a felhasználóra utaló szavakat, illetve számokat
- más jelszó használata titkos (üzleti) rendszer és más a nyilvános rendszereken

A szabályok betartását rákényszeríthetjük a felhasználókra olyan jelszókezelő program használatával, ami lehetővé teszi a jelszavak biztonságosságát. Ez a jelszavak megadásakor nem fogadja el a jelszót, ha nem felel meg a szabályoknak. Természetesen amíg nincs biztonságos jelszó megadva, a felhasználó nem férhet hozzá a rendszerhez. A fent felsorolt szabályok közül az utolsó kivételével mindegyik pontot ellenőrizni tudjuk.

A rendszergazda utólag is ellenőrizheti a jelszavak biztonságosságát jelszótalálgató programokkal. Ebben az esetben ugyanazt csinálja, mint egy cracker, ezért ilyet csak akkor szabad csinálni, ha ahhoz rendelkezik a rendszergazda a megfelelő jogokkal. A legbiztosabb az, ha van írásos engedélye. Amennyiben egy felhasználói fiókot sikerül feltörni, a felhasználót figyelmeztetni kell, hogy azonnal változtassa meg a jelszavát. Sőt, amennyiben lehetséges, erre rá kell őt kényszeríteni a biztonság érdekében. (Bármennyire is nagy a kísértés, más fiókjában ne turkáljunk.)

A biztonság érdekében bizonyos számú (általában 3) hibás bejelentkezés után a fiók hozzáférését tiltsuk le. Ezzel nagyon meg tudjuk nehezíteni a cracker dolgát. Továbbá rendszeresen figyeljük és naplózzuk a hibás bejelentkezéseket. Rendszeres hibás bejelentkezés egy felhasználói fiókba jelszótalálgatást jelenthet.

13.3 Büntethetőség

A jelszavak találgatása magában nem bűncselekmény, de ez a behatolás előzménye szokott lenni (mi másért kellene egy másik felhasználó jelszava?). Mint már előzőleg is említettük, a behatolás bűncselekménynek számít.

A hacker akkor tudja meg, hogy sikeres volt a próbálkozása, ha sikeresen belép a felhasználói fiókba. Amennyiben a felhasználói fiók hozzáféréséhez nincs jogosultsága, az illetéktelen hozzáférést, avagy behatolást jelent. Tehát ez csak siker esetén büntethető.

14 Néhány jó tanács

A biztonságos számítógépes környezet megteremtésében mindenkinek részt kell vennie. Egy számítógépes rendszert minden lehetséges oldalról védeni kell, és a védelmi rendszerek működését állandóan figyelni kell. Tudnunk kell, hogy a támadónak elég csak egyetlen egy gyenge pont a rendszer biztonságában. A biztonság megteremtése nehéz feladat, minden érintettnek segítenie kell a biztonság megteremtésében. Ez a munkatársak nagy részének azt jelenti, hogy a biztonsági szabályokat tartsák be, és használjanak józan észt a számítógépek használata közben (pl. fájlok megnyitásánál).

A különböző támadási formákhoz megadtam a lehetséges biztonsági intézkedéseket a támadások ellen. Most néhány általános dolgot szeretnék említeni, ami nélkülözhetetlen a számítógépek biztonságának megteremtéséhez.

- Tűzfalak felállítása a nemkívánatos csomagok szűrésére, és DMZ-k kialakítására.
- IDS használata a hálózat védelme érdekében.
- Anti-vírus program használata, és gyakori frissítése.
- A szoftverek frissítése.
- Mindent tiltsunk, majd mindenkinek csak arra adjunk engedélyt, amire szüksége van.
- Szükségtelen szolgáltatások eltávolítása a rendszerről.
- A biztonsági szabályzatot mindenkivel tudassuk.
- A biztonsági szabályokat mindenki tartsa be.
- A weboldalak eléréséhez ne használjunk linkeket. Mindig a honlapról indítsuk a böngészést.
- Titkosítás használata távoli bejelentkezéshez és érzékeny dokumentumok továbbítására.
- A felhasználók hitelesítése bejelentkezéskor. Nyilvános kulcson alapuló hitelesítés biztonságosabb, mint a név-jelszó kombináció.
- Hálózati forgalom naplózása.
- Naplózás az egyedi számítógépeken.
- A naplók figyelése és különleges események kinyomozása.
- A rendszer teljesítményének figyelése.
- Biztonsági mentések készítése, és ellenőrzése.
- Fontos rendszerfájlok sértetlenségének rendszeres ellenőrzése (pl. MD5 hashkódok ellenőrzése Tripwire-al).

- A szoftverek futtatásához hozzunk létre külön felhasználói fiókokat, és korlátozzuk a szoftver jogosultságait.

- Rejtsük el a szoftverek nevét és verziószámát. Így nem tudja a támadó, milyen gyengeségeket tud kihasználni.

- Korlátozzuk a lemezterületek használatát.

Referenciák

2000 Linux Symposium: arpsec. *http://www.linuxsymposium.org/2000/arp.php*

DNSSEC - DNS Security Extensions, Securing the Domain Name System. *http://www.dnssec.net*

Jerome Etienne. ARPsec: An ARP Securty Extension.

Mrs. E. van Geest LL.M. és a GOVCERT.NL technikai csoport. From Recognition to Reporting, Cyber Crime Manual. Dan Haag, 2003 augusztus 11.

Teemu Koponen és Juha Mynttinen. DNS Spoofing. 2001, április 21. *http://www.hut.fi/~tkoponen/dnsspoof.html*

Teemu Koponen és Juha Mynttinen. Secure Sockets Layer (SSL) Man-in-the-middle attack. 2001, április 18. *http://www.hut.fi/~tkoponen/vaihe2/ssl-mitm.html*

Yegappan Lakshamanan. ARP: Questions and Answers. Az oldal készült 1999, február 17.-én és utoljára frissült 1999, október 20.-án. *http://www.geocities.com/SiliconValley/Vista/8672/network/arp.html*

Mit érdemes tudnom a spam elkerüléséhez? *http://www.microsoft.com/hun/biztonsag/mitkell_10_spam.mspx*

Geoffrey Sisson. A Brief Introduction to DNSSEC. 2004, július 8.

Tartalomjegyzék