**Hálózatbiztonság**

## **Hálózati eszközök biztonsága**

A vezetékes vagy vezeték nélküli számítógép hálózatok mindennapi életünk fontos kellékei. Mind a magánszemélyek, mind a szervezetek egyaránt függenek számítógépeiktől és hálózatuktól. Egy jogosulatlan személy behatolása költséges hálózati leállást és a munka elvesztését eredményezheti. Egy hálózat elleni támadás lehet végzetes, valamint a fontos információk és eszközök megrongálása vagy ellopása okozhat idő- és pénzveszteséget.

**A behatolók hozzáférést szerezhetnek a hálózathoz a szoftver sebezhető pontjain keresztül, hardver elleni támadással vagy egy felhasználó nevének és jelszavának kitalálásával. Azt a behatolót, akik a szoftver módosításával vagy sebezhető pontjainak kihasználásával jut hálózati hozzáféréshez gyakran hacker-nek (hekker, számítógépkalóz) nevezik.**

A hacker hozzáférése a hálózathoz négyféle fenyegetést jelenthet:

* Információlopás
* Azonosító lopás
* Adatvesztés és manipuláció
* Szolgáltatás megszakítása



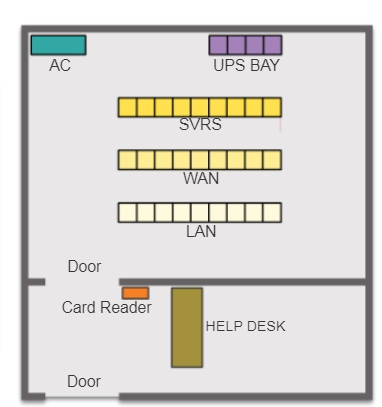
**Kis hálózatok tervezése és megvalósítása során is szükség van a biztonsági fenyegetések és sebezhetőségek áttekintésére**.

Amikor hálózati vagy számítógép biztonságról beszélünk, **általában a szoftverek sebezhetőségét kihasználó támadóra gondolunk**. Ugyanennyire fontos azonban az eszközök **fizikai biztonsága is**, hiszen **egy támadó megakadályozhatja a hálózati erőforrások használatát, ha azokat fizikailag képes veszélyeztetni**.

A fizikai fenyegetések négy formája:

* **Hardver fenyegetések**- szerverek, munkaállomások, forgalomirányítók, kapcsolók és a kábelezés fizikai megrongálása.
* **Környezeti fenyegetések**- szélsőséges hőmérséklet (túl meleg vagy hideg) vagy szélsőséges páratartalom (túl nedves vagy száraz)
* **Elektromos veszélyek**- feszültség tüskék, alacsony feszültségszint (feszültségesés), szűrés nélküli tápellátás (zaj), áramszünet
* **Karbantartási veszélyek**- az elektromos összetevők hanyag kezelése (elektrosztatikus feltöltődés), kritikus alkatrészek hiánya, hibás kábelezés és hiányos feliratozás

Ezen problémák egy részének szerepelni kell a vállalat házirendjében, más részük megoldása a szervezet vezetőségének hatáskörébe tartozik.



váltakozó áram

ügyfélszolgálat

kártyaolvasó

szünetmentes tápegység

*biztonságos számítógépes szoba alaprajza*

**A három fontos hálózatbiztonsági tényező: sebezhetőség, fenyegetés és támadás**.

**A sebezhetőség a gyengeség fokmérője**, mely minden **hálózatban és eszközben eredendően benne rejlik**, beleértve **a forgalomirányítókat, kapcsolókat, szervereket, munkaállomásokat, és még a biztonsági eszközöket is**.

**Fenyegetésekbe beleszámítanak azok az emberek, akik érdekeltek és kellőképpen képzettek is a biztonsági sebezhetőségek kihasználására**. Az ilyen személyek folyamatosan keresik az új lehetőségeket és gyengeségeket.

**A fenyegetések különféle segédeszközök, szkriptek és programok formájában jelennek meg, melyek alkalmasak a hálózatok és a hálózati eszközök megtámadására**. Ezek a **hálózati eszközök általában végberendezések**, például **szervere**k vagy **asztali számítógépek**.

**A három elsődleges sebezhetőségi pont:**

* Technológiai
* Konfiguráció
* Biztonsági házirend

**Mindhárom sebezhetőség vagy gyengeség különféle támadásokra ad lehetőséget, ilyenek például a rosszindulatú programok vagy a hálózati támadások.**

Információ lopás Személyazonosság lopás

megszemélyesít valakit hitel megszerzése érdekében

tudományos kutatási jelentése ellopása

egy cég felhasználói adatbázisának ellopása

illegális online vásárlások

Adatvesztés/manipuláció Szolgáltatás megzavarása

hálózat túlterhelése a felhasználók távol tartása érdekében

adatrekordok megváltoztatása

vírus küldése merevlemez formázására

megakadályozza, hogy a legális felhasználók hozzáférjenek az adatszolgáltatásokhoz

## **Sebezhetőségi pontok és hálózati támadások**

**A rosszindulatú kód támadások** (malicious code attack) **közé azokat a számítógép programokat soroljuk, melyeket adatvesztés vagy sérülés okozása céljából hoztak létre**. Három fő típusuk:

* a vírusok,
* a trójai lovak és
* a férgek.

**A vírus egy rosszindulatú szoftver, mely más programokba ágyazva nemkívánatos hatást okoz egy munkaállomáson.** **Vírus** például **egy program**, amely beágyazódik a command.com állományba (ez a Windows rendszerek elsődleges parancsértelmezője), letöröl bizonyos fájlokat és megfertőz minden más command.com állományt, amit talál.

**A Trójai ló annyiban különbözik ettől, hogy az alkalmazás egészen másnak látszik, mint ami valójában, miközben igazából egy támadási eszköz**. **Trójai ló például** egy olyan alkalmazás, mely **egyszerű játékként fut a munkaállomáson**. Miközben *a felhasználót lefoglalja a játék, a trójai elküldi saját másolatát a felhasználói címjegyzékben szereplő összes címre. A címzettek megkapják és futtatják a játékot, ezáltal tovább terjesztik a Trójai lovat a saját címjegyzékükben szereplőknek.*

**A vírusoknak a víruskód más rendszerbe való átviteléhez egy továbbító mechanizmusra, például egy levélhez csatolt zip vagy exe fájlra van szükségük**. **A vírusok és férgek közötti alapvető különbség az, hogy a vírus továbbterjedéséhez emberi közreműködés szükséges**.

**A férgek önálló programok, melyek megtámadják a rendszert és megpróbálják kihasználni annak sebezhető pontjait**. **A sikeres támadás után a féreg átmásolja önmagát a megtámadott rendszerbe, és a folyamat kezdődik elölről**.

Egy féregtámadás anatómiája a következő:

* **A sebezhetőség**- A féreg feltelepíti magát a rendszer egy ismert gyenge pontját kihasználva, például amikor egy naiv felhasználó megnyit egy futtatható e-mail csatolmányt.
* **Terjesztési mechanizmus**- Az állomáshoz való hozzáférés megszerzése után a féreg másolatot készít önmagáról, majd új célpontot választ.
* **Hasznosítás** - A megfertőzött állomáshoz a támadó gyakran olyan jogosultságot szerez, mellyel a helyi lehetőségeket kihasználva adminisztrátorrá válhat.

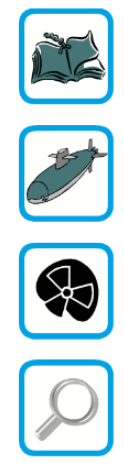
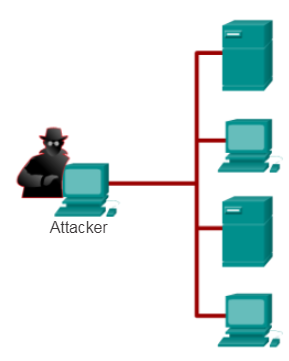
**A rosszindulatú szoftver támadásokon kívül a hálózat áldozatul eshet különféle hálózati támadásoknak is**.

**A hálózati támadások három fő kategóriába sorolhatók**:

* **Felderítéses támadások**- a rendszerek, szolgáltatások és sebezhetőségek jogosulatlan feltérképezése
* **Hozzáférési támadások**- adatok, rendszerhozzáférések és felhasználói jogok illetéktelen kezelése
* **Szolgáltatásmegtagadás**- hálózatok, rendszerek és szolgáltatások megbénítása vagy elrontása

**Felderítéses támadások**

**Egy külső támadó internetes eszközöket használva**, például nslookup vagy whois **segédprogramok segítségével könnyen megállapíthatja egy adott szervezet IP-címtartományá**t. **Ezután a támadó a tartomány publikus IP-címeinek megpingelésével ki tudja választani az aktív állomásokat**. Ez a feladat egy "ping sweep" (ping pásztázás) segédprogrammal, mint például az fping vagy a gping automatizálható is, hiszen ezek a programok szisztematikusan végig pingelik a összes címet egy adott tartományban vagy alhálózatban. Ez pont olyan, mint egy telefonkönyvben végighívni az összes számot azt figyelve, hogy melyiket veszik fel.



csomagszippantók

port keresések

ping pásztázás

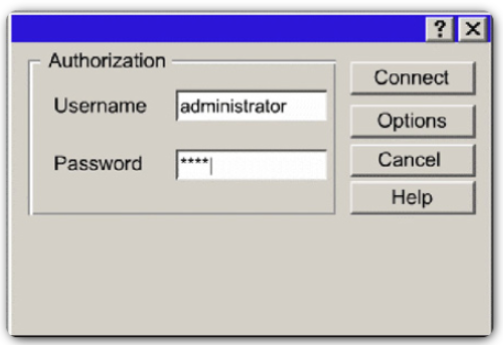
internetes lekérdezés

**Hozzáférési támadások**

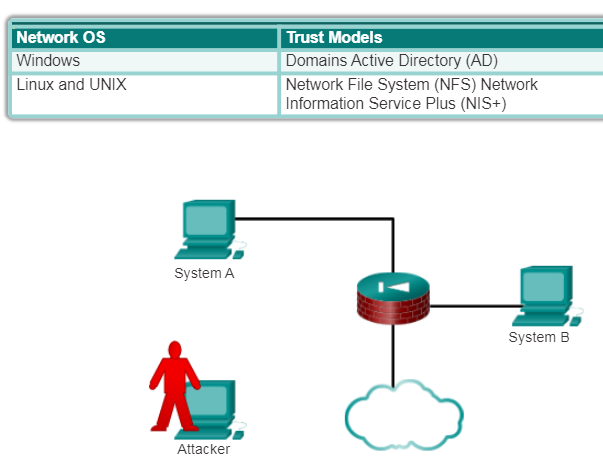
**A hozzáférési támadások a hitelesítési, FTP és web szolgáltatások ismert sebezhetőségi pontjait használják ki a bejelentkezési adatok, bizalmas információk megszerzéséhez**. Ennek eredményeképpen **a támadó személy jogosulatlan hozzáférés által jut hozzá számára titkos adatokho**z.

A hozzáférési támadások négy csoportba oszthatók.

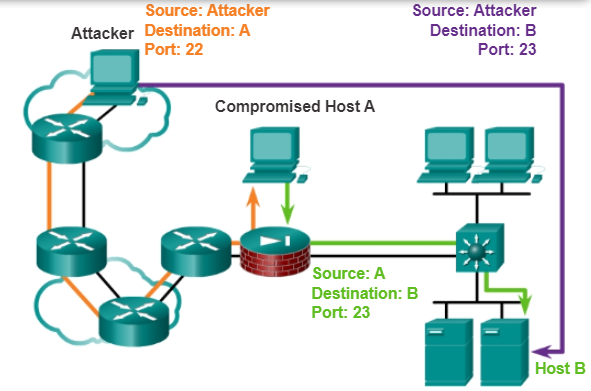
* egyik leggyakoribb támadástípus a **jelszó elleni támadás**, amely egy protokollelemző segítségével is végrehajtható, elfogva az egyszerű szövegként továbbított felhasználóneveket és jelszavakat.
* a **megismételt bejelentkezési próbálkozások**, melyek osztott erőforrások, például szerverek vagy forgalomirányítók felhasználónevének és jelszavának megszerzésére irányulnak. **Az ismétléses támadásokat nevezik még szótár (dictionary) vagy nyers erő (brute-force) támadásoknak** is.

**Jelszó támadás:**

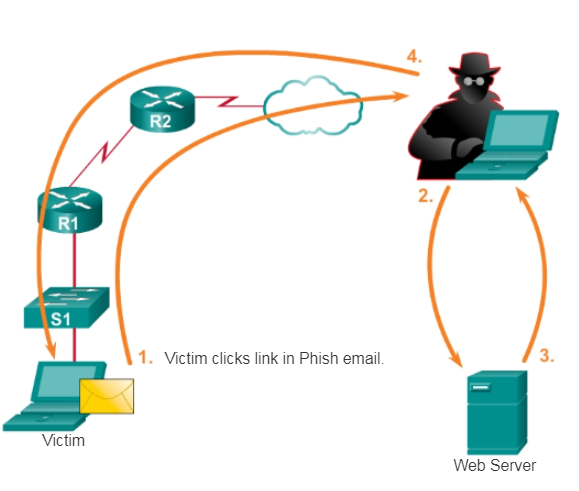
**Bizalom megszerzése:**



**Port átirányítás: A port-átirányítás egyfajta bizalom-kihasználási támadás, amely egy veszélyeztetett gazdagépet használ a forgalom átadásához egy tűzfalon, amelyet egyébként elvetnének.** Ezt elsősorban a megfelelő bizalmi modellek alkalmazásával enyhítik. A víruskereső szoftver és a gazdagép-alapú IDS segíthet felismerni és megakadályozni a támadókat, amelyek telepítik a port átirányító segédprogramokat a gazdagépre.



**Adathalász:**



az áldozat a linkre kattint az adathalász e-mailjében.

áldozat