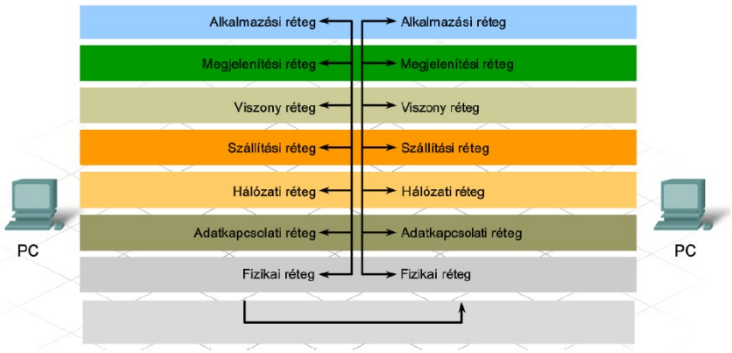
Hálózat dolgozta

1. **TCP/IP**
   a. **TCP/ip**
      - Felépítése:
        - A TCP/IP felépítése a rétegződési elven alapul, minden egyes réteg egy jól definiált fel-adatot végez el, és a rétegek egymás között szolgálatelérési pontokon keresztül kommu-nikálnak. Minden réteg csak a vele szomszédos réteggel képes kommunikálni, mivel ezek egymásra épülnek. Alapvetően négy réteg alkotta, melyet ötre bővítettek.
        - Alkalmazási réteg
        - Szállítási réteg
        - Hálózati (Internet) réteg
        - Adatkapcsolati réteg
        - Fizikai réteg
2. **OSI modell**
   a. **Céljai:**
      - modellje a különböző protokollok által nyújtott funkciókat egymásra épülő rétegekbe sorolja
      - Minden réteg csak és kizárólag az alsóbb rétegek által nyújtott funkciókra támaszkodhat
      - A rendszert, amelyben a protokollok viselkedését az egymásra épülő rétegek valósítják meg, gyakran nevezik 'protokoll veremnek' vagy 'veremnek'.
      - A rendszert, amelyben a protokollok viselkedését az egymásra épülő rétegek valósítják meg, gyakran nevezik 'protokoll veremnek' vagy 'veremnek'.
      - A legfontosabb eredmény az volt, hogy olyan specifikációkat határoztak meg, amelyek pontosan leírták, hogyan léphet egy réteg kapcsolatba egy másik réteggel.
      - Az OSI közösségben használt szabványokat itt lehet megtalálni: ISO szabványok. (ok)
   b. **Előnyei:**
      - Csökkenti a bonyolultságot
      - Szabványosítja az interfészeket
      - Támogatja a moduláris tervezést
      - Biztosítja a különféle technológiák együttműködését
      - Felgyorsítja a fejlődést
      - Egyszerűsíti a tanulást és az oktatást



   c. **A fizikai réteg**
      - felépíteni és lezárni egy csatlakozást egy kommunikációs médiummal.
      - feladata a bitek kommunikációs csatornára való juttatása
      - részt venni egy folyamatban, amelyben a kommunikációs erőforrások több felhasználó közötti hatékony megosztása történik.

- moduláció, vagy a digitális adatok olyan átalakítása, konverziója, jelátalakítása, ami biztosítja, hogy a felhasználó adatait a megfelelő kommunikációs csatorna továbbítani tudja. A jeleket vagy fizikai kábelen – réz vagy optikai szál, például – vagy rádiós kapcsolaton keresztül kell továbbítani.

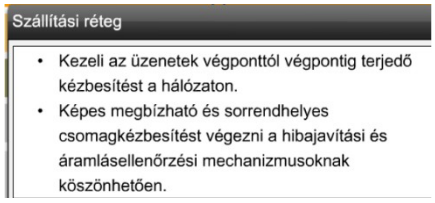
d. Adatkapcsolati réteg



e. Hálózati réteg

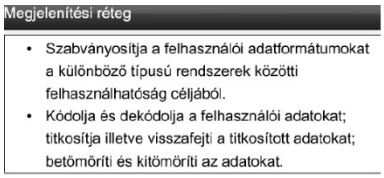
- biztosítja a változó hosszúságú adat sorozatoknak a küldőtől a címzetthez való továbbításához szükséges funkciókat és eljárásokat, úgy, hogy az adatok továbbítása a szolgáltatási mi-nőség függvényében akár egy vagy több hálózaton keresztül is történhet.
- A hálózati réteg biztosítja a hálózati útvonalválasztást, az adatáramlás ellenőrzést, az adatok szegmentálását/deszegmentálását, és főként a hiba ellenőrzési funkciókat.

f. A szállítási réteg



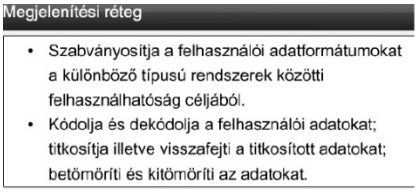
g. A viszony réteg

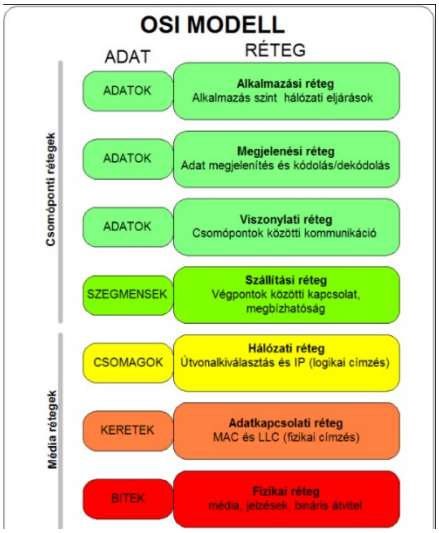
Feladatai:



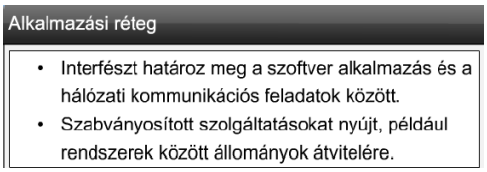
- két számítógép között logikai kapcsolat létesítése
- párbeszéd szervezése
- vezérjelkezelés
- szinkronizálás

h. Megjelenítési réteg





i. Alkalmazási réteg



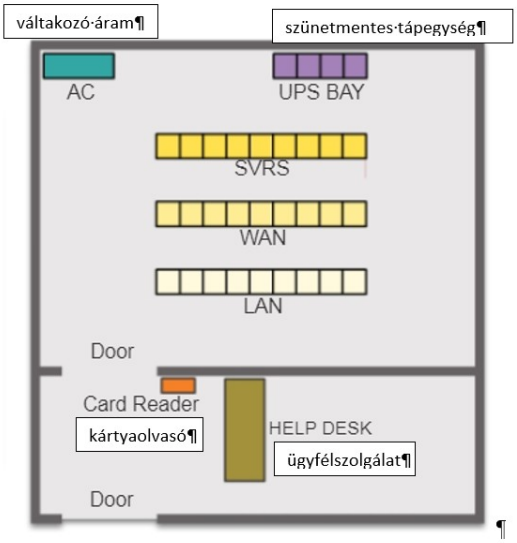
3. Hálózatbiztonság

a. Miért fontos?

- Mer: 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 hackernek (hekker, számítógépkalóz) nevezik.
- Fenyegetések, amikkel fenyegetnek
    - Információlopás
    - Azonosító lopás
    - Adatvesztés és manipuláció
    - Szolgáltatás megszakítása

b. Fizikai fenyegetések

- 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



1. Valami random kép ami gondolom jó valamire

c. Három fontos hálózatbiztonsági tényező:

- sebezhetőség
    - A gyengeség fokmérője
    - hálózatban és eszközben eredendően benne rejlik
    - a forgalomirányítókat, kapcsolókat, szervereket, munkaállomásokat, és még a biztonsági eszközöket is.
- fenyegetés
    - beleszámítanak azok az emberek, akik érdekeltek és kellőképpen képzettek is a bizton-sági sebezhetőségek kihasználására
- támadás

d. Három elsődleges sebezhetőségi pont:

- Technológiai
- Konfiguráció
- Biztonsági házirend

e. Sebezhetőségi pont

- 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 ha-tást okoz egy munkaállomáson.
  - A Trójai ló annyiban különbözik ettől, hogy az alkalmazás egészen másnak látszik, mint ami valójában, miközben igazából egy támadási eszköz.
  - 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.

f. 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.

g. Három fő támadási kategória

- 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

h. Felderítéses támadások

- Egy külső támadó internetes eszközöket használva, például nslookup vagy whois segéd-programok segítségével könnyen megállapíthatja egy adott szervezet IP-címtartományát. Ezután a támadó a tartomány publikus IP-címeinek megpingelésével ki tudja választani az aktív állomásokat.

i. Hozzáférési támadások

- A hozzáférési támadások a hitelesítési, FTP és web szolgáltatások ismert sebezhetőségi pontjait használják ki a bejelentkezési adatok, bizalmas információk megszerzéséhez.
- Négy csoportja:
    - jelszó elleni támadás
    - a megismételt bejelentkezési próbálkozások
    - Adathalászat

- Port átirányítás

- Port átirányítás
  - A port-átirányítás egyfajta bizalom-kihasználási támadás, amely egy veszélyeztetett gazdagépet használ a forgalom átadásához egy tűzfalon, amelyet egyébként elvetnének.

j. Szolgáltatás megtagadás

- A DoS (Denial of Service, szolgáltatás megtagadás) támadás a legismertebb és a legnehezebben kiküszöbölhető támadásforma. Még a hekker társadalomban is jelentéktelennek és helytelennek számítanak a DoS-támadások, mivel csekély erőfeszítés árán végrehajthatók. mindegyik a rendszer erőforrásainak felemésztésével akadályoz meg jogosult felhasználókat egy szolgáltatás használatában.
- Halálos ping ☠

  Halálos ping: egy olyan csomag kerül elküldésre az eszköznek, melynek mérete meghaladja az IP által megengedett méretet (65.535 bájt). Ez a fogadó rendszer összeomlását okozza.

- Szinkron elárasztás

  SYN (szinkron) elárasztás - egy csomagáradat kerül elküldésre a kiszolgálóhoz kérve az ügyfél kapcsolódását. A csomagok érvénytelen forrás IP-címet tartalmaznak. A kiszolgálót teljesen lefoglalja az, hogy megpróbálja megválaszolni ezeket a hamis kéréseket és így nem képes válaszolni a valódiakra.

- DDOS

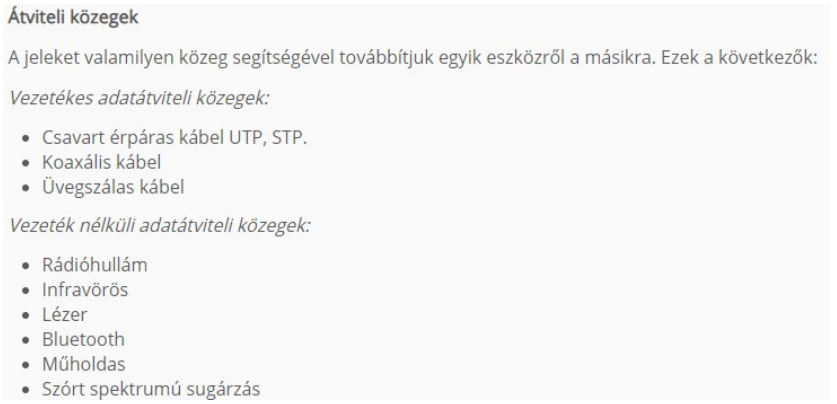
  A támadók sok köztes állomást, úgynevezett zombikat használnak a támadás elindításához.

4. <u>Fizikai átviteli jellemzők és módszerek</u>

a. Az átviteli közeg feladata, hogy bitfolyamokat szállítson egyik géptől a másikhoz

b. A fizikai közeg a jelek hordozója, fémvezeték, fényvezeték vagy a puszta „éter”.

c. Az átvitel történhet vonalszerűen, pl. vezeték, lézersugár; infravörös vagy mikrohullá-mú nyaláb útján, és történhet térben, irányítatlan rádióhullámmal.



Átviteli közegek

A jeleket valamilyen közeg segítségével továbbítjuk egyik eszközről a másikra. Ezek a következők:

Vezetékes adatátviteli közegek:

- Csavart érpáras kábel UTP, STP.
- Koaxális kábel
- Üvegszálas kábel

Vezeték nélküli adatátviteli közegek:

- Rádióhullám
- Infravörös
- Lézer
- Bluetooth
- Műholdas
- Szórt spektrumú sugárzás

d. Aktív és passzív eszközök

- az eszköz lehet aktív és passzív abból a szempontból, hogy a rajta átfolyó jelekkel mit csinál. Ha csak simán továbbadja/szétosztja, akkor passzív eszköz
- Amennyiben ezen jeleket erősíti is, akkor már aktív
- Repeater:
  - Az ismétlő feladata a hálózati jelek bit szintű erősítése és újbóli időzítése.

    - Az azonos típusú sínhálózatok egyszerű jelismétlőkkel kapcsolhatók össze na-gyobb hálózattá.

    - Három nagy csoporja
        - sodrott érpáras repeaterek
        - üvegszálas átviteli támogatók
        - vékony Ethernet repeaterek
- Router
    - Feladata:
        - a bejövő csomagok megvizsgálása,
        - a legjobb hálózati útvonal kiválasztása, és
        - a csomagok átkapcsolása a megfelelő kimenő portra.
    - Lehetővé teszik gyakorlatilag bármely típusú számítógép számára), hogy kommunikálhasson a világ szinte bármelyik számítógépével.
- HUB
    - feladata a hálózati jelek bit szintű erősítése és újraidőzítése sok felhasználó számára.
    - Feladata:
        - a munkaállomások, szerverek és egyéb hálózati eszközök közti adatforgalom biztosítása.
        - Csavart érpáras csillag topológiájú hálózatok esetén használnak az útvonal elosztására hub-okat, melyek meghatározott számú port-tal rendelkeznek.
    - Három nagy csoportja
        - passzív hub: nem végez jelismétlést, feladata az adattovábbítás
        - aktív hub: jelismétlést is végez
        - intelligens hub: feladata a forgalomirányítás, csomagkapcsolás
        -
- Bridge
    - Feladata a forgalom szűrése a LAN-on. A bridge nem továbbítja a lokális (helyi) forgalmat, de a LAN más részeire (szegmenseire) tartó forgalmat átengedi. Minden hálózati eszköz rendelkezik egy egyedi MAC-címmel; a híd ez alapján dönti el, hogy továbbítja-e az adatot.
    - Két nagy csoportja:
        - 1.Az első esetben a fentebb már leírt transzparens és tanuló módszer segítségével a híd figyeli a rajta átmenő adatforgalmat, majd egy listát (forgalomirányítási tábla) állít össze arról, hogy az adatcsomag melyik állomásról érkezett.
        - 2.A másik módszer a célcím forrásának meghatározására a forgalomirányítás, amikor az adatcsomag a teljes útvonalat tartalmazza.
    - Miben tér el a router-től?
        - Bár mindkét eszköz számítógép-hálózatokat kapcsol össze, más módon teszik azt. A há-lózati híd az OSI modell második, tehát az Adatkapcsolati rétegében operál, míg a router az OSI modell 3. más szóval a hálózati rétegében tevékenykedik.
- Gateway

    - Ez a legbonyolultabb hálózat összekapcsolási módszer. Akkor alkalmaznak átjárót, ha egymástól teljesen különböző hálózatot akarnak összekapcsolni.
    - Üzenetformátum átalakítása: A hálózatok különböző üzenetformátumokat, eltérő maximális üzenetméretet és karakterkódokat alkalmaznak. Az átjáró át tudja alakítani az üzeneteket az üzenetet fogadó állomás számára.
    - Címátalakítás: A hálózatok eltérő címzési szerkezetet használnak. A gateway képes átalakítani minden üzenethez a rendeltetési hálózat által megkívánt címszerkezetet.
    - Protokoll-átalakítá
    - Az átjáró képes arra, hogy felcserélje az egyik hálózatból érkező információt a másik hálózat, hasonló feladat elvégzéséhez szükséges információjára.
- Switch
    - A kapcsolók (angolul: switches) jóval fejlettebbek, mert az egyszerű adattovábbítás he-lyett a switch mindig ellenőrzi a cél MAC-címét és csak utána továbbítja a megfelelő üzenetet. Így a switch csökkenti a domainek közötti forgalmat
    - Feladata a hálózat szegmensei közötti összeköttetés biztosítása és a hálózat terheltségé-nek csökkentése.

5. <u>MAC és IP cím</u>

Az összehasonlítás alapja	**MAC**	**IP**
Teljes alak	Media Access Control cím.	Internet protokoll címe.
Célja	Meghatározza az interneten lévő számítógép fizikai címét.	A számítógép internetes kapcsolatát azonosítja.
bit	Ez 48 bites (6 byte) hexadecimális cím.	Az IPv4 egy 32 bites (4 bájt) cím, és az IPv6 egy 128 bites (16 bájt) cím.
Cím	A MAC-címet a NIC-kártya gyártója adja meg.	Az IP-címet a hálózati rendszergazda vagy az internetszolgáltató adja meg.
Cím letöltése	Az ARP protokoll képes egy eszköz MAC-címének letöltésére.	A RARP protokoll egy eszköz IP-címét lekérheti.
	fizikai	logikai
	nem változtatható meg	megváltoztatható

	kapcsoló (switch)	forgalomirányító (router)