

10.b Mutassa be a biztonság tervezési elveit! Határozza meg az információbiztonsági célok elérésére használható intézkedés típusokat, adjon példát ezekre intézményi környezetben!

### Tervezés

1. A rendszerterv és a használt biztonsági protokoll legyen nyilvános.
2. Alapértelmezés legyen az, hogy valaki valamihez nem férhet hozzá.
3. A security-vel kapcsolatos kérdéseket a rendszer tervezésének korai fázisában tisztázni kell és a security csomagot a rendszer magjába integrálni kell.
4. Legyen a rendszer felhasználóbarát.
5. Ha lehet, akkor kerüljük az egész rendszer felett „teljes hatalommal bíró” (superuser, supervisor) rendszergazda koncepciót.
  - a. A rendszert bontsuk moduljaira, például egy-egy modul egy-egy fontosabb erőforrás kezelését végezze és az egyes moduloknak legyenek külön-külön felügyelői.

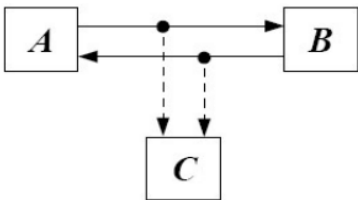
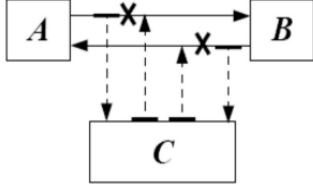
### Legfontosabb nézőpontok

- Központi vírusvédelem
- Virtuális magánhálózatok (VPN) konfigurálása
- Jogosultságkezelés (hitelesítés, azonosítás)
- Tartalomszűrés (dokumentálás, logolás)
- Tűzfalak
- Behatolás detektáló rendszerek (intrusion-detection)
- Felhasználó és hozzáférés menedzsment
- Adatmentés

### Hálózat védelme

- Támadó célja
  - o Információs szerzés
  - o Illetéktelen hozzáférés
  - o Szolgáltatások megbénítása
  - o Rendszer feltörése
  - o Rosszindulatú programok bejuttatása

## Aktív és passzív támadások

Passzív	Aktív
A lehallgatás (evesdropping, wire-tapping), az érzékeny információ megszerzésére irányul, a támadó nem módosítja az átviteli csatorna tartalmát.	A támadó maga is forgalmaz a csatornán <ul style="list-style-type: none"> <li>• üzenetmódosítás</li> <li>• megszemélyesítés</li> <li>• visszajátszás</li> <li>• szolgáltatás megtagadás (DoS – denial of service) típusú támadások</li> </ul>
	

## Csomag szintű támadások

### IP spoofing

- IP cím hamisítása
- **Védekezés:** A tűzfalak bizonyos forrás IP címeket csak bizonyos irányból fogadnak el.

### Smurf

- DoS típusú támadás, ami a megtámadott gép nevében ICMP echo request üzenetet küld egy irányított IP broadcast címre.
- **Védekezés:** A routerek IP broadcast-ot ne engedje át, IP broadcast címre ICMP echo request-re a gépeink ne válaszoljanak.

### SYN flood

- DoS támadás
- Ha a rosszindulatú **C** támadó az **A** nevében nagy mennyiségű SYN csomagot küld **B**-nek (**C** nem kapja meg a válaszokat), akkor ezzel kimeríti **B** erőforrásait és az nem lesz képes fogadni a valódi kéréseket.
- **Védekezés:**
  - o Mikro blokkok használatával:
    - A szabványos adatstruktúráknál lényegesen kisebb helyet foglalunk le, és ha a kapcsolat kérés valódinak bizonyul, csak akkor foglaljuk le a szükséges erőforrásokat (10x annyi támadó csomagot bírunk el).
    - SYN cookie használatával.

### Xmas, Ymas

- A TCP fejrészben az URG bittől balra levő két bitet 2003 májusában az IANA (Internet Assigned Numbers Authority) az ECN (Explicit Congestion Notification) mechanizmus céljára osztotta ki.
- A korábbi TCP implementációk azt várják el, hogy ez a 2 bit 0 értékű legyen.
- A bitek 0-tólkülönböző értékre állításával és a TCP implementáció viselkedésének megfigyelésével a támadó információt szerezhet a TCP/IP protocol stack implementációjáról.

## Hálózati szintű támadások

### Switchek elleni támadás

- **Switch normál működése:** Keretek továbbítása csak arra a portra, ahol a címzett található.
- **Portokhoz MAC címek beállítása:**
  - o Statikusan, munkaigényes konfiguráció változásánál át kell vezetni (hálókártya csere)
  - o Öntanuló módban, megjegyzi, hogy az egyes MAC címekkel forráscímként melyik portján találkozott.
- Ha a támadó sok különböző MAC címmel való forgalmazással, megtelíti a switch táblázatát, akkor a működés fenntartása érdekében minden keretet minden portjára kiküld (fail open). Ezzel a forgalom lehallgathatóvá válik.

### ARP poisoning

- A támadó kéretlen és hamis ARP válaszokat küld, amiben a kérdéses IP címhez a saját MAC címét tünteti fel.
- **ARP (Address Resolution Protocol):** Címlekérdező protokoll. Üzenetszórásos hálózatokon broadcast (minden gépnek szóló) üzenettel megszerzi az információt (IP cím – fizikai cím összerendelés) és elraktározza (cache).

### ICMP redirect

- Az ICMP redirect üzenettel egy router egy számítógép számára egy jobb útvonalat tud megadni. A támadó ezzel maga felé tudja irányítani a megtámadott gép forgalmát.
- Használhatja pl:
  - o Lehallgatásra: A csomagokat tovább küldi a címzettnek, hogy a támadás észrevétlen maradjon.
  - o IP spoofing támogatásra: A redirecttel elérte, hogy az A válaszai őhozzá érkezzenek, a TCP kapcsolat ténylegesen felépül.
- **Védekezés: accept\_redirects** kikapcsolása.

### RIP (Routing Information Protocol) távolságvektor hamisítása

- RIP: Distance-vector protokoll, ami egy célponthoz (hálózatok, subnetek, állomások vagy a default router) táblázatában tárolja:
- A célpont IP címét.
- Az odavezető út költségét (egy csomagnak az adott linken való átküldésének költsége alapján).
- Az odavezető út első routerét.
- Időzítőket
- Mivel a RIP nem használ autentikációt, a támadó számítógépe hamis távolságvektorral becsaphatja a routereket azt állítva, hogy rajta keresztül rövidebb út vezet a cél felé.

### Source route IP opció

- A forrás megadhatja, hogy adott IP című állomás felé mely routereken keresztül haladjon a csomag.
- Támadó: privát IP című hálózatok elérésére.
- A **C** támadó az **R1** routernek megmondja, hogy **R2**-n keresztül kell a csomagot küldenie. **R2** privát IP címmel rendelkező hálózat gateway-e, a datagrammot már a cél IP cím alapján küldi a címzettnek.
- A visszaút: A támadó publikus IP címmel rendelkezik.
- **Védekezés: accept\_source\_router** kikapcsolása.

### DNS (cache) ellen való támadás

- Kihasználja, hogy lejár az ns.myisp.com által tárol [www.mybank.com](http://www.mybank.com) TTL (Time To Live) ideje.

### Felhasználók védelme

- Legnagyobb probléma a jelszavak.
- Erős jelszó megkötése:
  - o Több karakter
  - o Kis-nagybetű
  - o Számok
  - o Speciális karakterek
- Kerberos, LDAP, NIS
- Jelszavakat védett fájlban tároljuk
- Jelszavak titkos kezelése, például nem írjuk fel publikus cetlire.

### Szerverek védelme

- Folyamatos vizsgálat
  - o Rajta futó programok
  - o Hozzáférések naplózása
- Tűzfalak használata
  - o Alapértelmezetten portok tiltása
- Naplózás
  - o Külön partícióra
- Fájrendszer megfelelő kialakítása
  - o Jogosultságok kezelése
  - o Írás jogokat nem adunk mindenkinek
- Külön szerverek a szolgáltatásoknak
  - o FTP, DNS, WEB
- Virtualizáció
- Biztonsági frissítések és adatmentések