3.b Ismertesse a behatolás érzékelő és megelőző rendszerek (IDS/IPS) célját, típusait, működési elveit!

IDS és IPS rendeltetés, alapfunkciók, tervezési megfontolások, lehetőségek, szolgáltatások

IPS és IPS rendeltetése

- Behatolás érzékelő eszközöknek a hálózat kritikus forgalmat átbocsátó pontjaira helyezésével a nem kívánt vagy jogosulatlan forgalom érzékelése és valós idejű beavatkozás is elvégezhető.

IDS és IPS alapfunkciók

- **Érzékelik**
  - Gyanús csomagokat
  - Illegális tevékenységre utaló adattartalmakat
  - Normálistól eltérő forgalom mintákat
  - Küszöb értékeket meghaladó mennyiségű csomagokat
  - IDS jelzi a behatolás tényét
  - IPS valós időben ellenintézkedéseket tesz a támadás megelőzésére

Tervezési megfontolások

- **Védelem:** Biztonsági politika kialakítása és megvalósítása megfelelő technológia alkalmazásával.
- **Érzékelés:** Támadások észlelése
- **Elhárítás:** Válaszlépés megtétele
- **Értékelés:** Kockázatelemzés, ellenintézkedések és költség/haszon elemzés
- **Javítás:** Kiválasztott ellenintézkedések megvalósítása

Szolgáltatások és lehetőségek

IDS

- **Előnyei:** Nem érinti negatívan a hálózati forgalmat.
- **Hátrányai:** Nem skálázható és a rosszindulatú csomag célba juttatását nem akadályozza meg.

IPS

- **Előnyei:**
  - Single-packet támadásokat megállítja
  - Real-time figyeli a forgalmat
  - Harmadik és negyedik rétegben figyel
- **Hátrányai:**
  - Negatívan érinti a hálózati teljesítményt (latency, jitter)
  - Kieséskor megszakad a forgalom

Host alapú IPS megoldások jellemzői, alkalmazása, előnyök és hátrányok

Host alapú IPS megoldás lényege

- Lényege, hogy a kliensre egy szoftvert telepítenek, ami monitorozza a gépen végzett tevékenységeket.
- **Előnyei:**
  - Oprendszerre tipikus támadásokat figyeli
  - Szokásostól eltérő műveleteket is detektálja
- **Hátrányai:**
  - Csak lokális
  - Minden gépen implementálni kell
  - Nem ismeri az egész hálózatot, mivel a hálózat legvégén van

A hálózat alapú IPS megoldások jellemzői, alkalmazása, eszközei, előnyök és hátrányok

Hálózat alapú IPS megoldás lényege

- Host-based szenzorok nem tudják megvédeni a hálózatot, ezért fontos a hálózati szenzorok alkalmazása.
  - Ezeket a szenzorokat a hálózat megfelelő pontjaira kell telepíteni a maximális biztonság elérése céljából.
- **Előnyei:**
  - Költséghatékony
  - Hálózaton transzparens
  - Alacsony szintű hálózati eseményeket is látja
- **Hátrányok**
  - Titkosított forgalmat nem látja
  - Nem tudja a támadás sikerességét

Hálózati alapú IPS megoldások eszközei

- **Port mirroring:** A bejövő csomagokat tovább küldi a cél felé és le is másolja és elküldi egy meghatározott portján az analizáló eszköz felé.
  - CISCO SPAN (switched port analyzer) egy cisco implementációja

A „signature” alapú IPS rendszerek működése, jellemzői, alkalmazása

- Olyan biztonsági megoldások, amik a hálózati forgalom ellenőrzésére használnak aláírásokat.
- Ezek az aláírások egyedi azonosítók, amik a hálózati támadásokra jellemző mintákat és jellemzőket tartalmazzák.
- Figyelik a hálózati forgalmat és ha találnak egy aláírást, akkor riaszt. (Rendszergazdának szól)
- Gyors reakcióideje van
- Magas fokú pontosság és könnyű kezelhetőség.
- Javasolt olyan környezetekben használni, ahol a hálózati forgalom ellenőrzése és szabályozása fontos szempont.

A minta-, az anomália-, a policy es a „Honeypot” alapú érzékelés sajátosságai

Minta alapú

- Előre definiált mintákat keres a forgalomban.
- Atomi és összetett mintákat is felismer.
- **Előnye:** Könnyen konfigurálható és kevesebb hibás pozitív eredmény.
- **Hátrányai:**
    - Eddig nem ismert hibákat nem tudja felismerni.
    - Kezdetben sok a hibás pozitív eredmény.
    - Mintákat folyamatosan frissíteni kell.

Anomaly/Anomália

- Normál profilt létre kell hozni, ahol meg kell határozni mi a normális működés és minden ami attól eltér, az negatív.
- **Előnyei:**
    - Ismeretlen támadási fajta detektálható
    - Elég normális mintát meghatározni, nem kell minden támadási fajtára mintát írni.
- **Hátrányai:**
    - Nem mondja meg pontosan milyen támadás történik.
    - Meg kell határozni a normál működést.
    - Tanulási időszakban biztosan támadásmentesnek kell lenni a hálózatnak, különben az lesz a normális.

Policy alapú

- Nem mintákat határoz meg, hanem viselkedéseket.
- Riaszt, ha x csinál y-t.
- Mindenre alkalmazkodik.
- **Előnye:** Ismeretlen támadások detektálása
- **Hátrányai:**
    - Nehéz nagy profilokba kategorizálni a hálózati forgalmat nagy hálózaton
    - Nem változhat a hálózati forgalom profilja

HoneyPot

- Álszervereket állít a hálózatba, hogy azt támadják.
- Adatokat gyűjt a különböző támadásokról, így finom hangolva az IDS, IPS szenzorait.
- Biztonsági cégek alkalmazzák kutatás céljából.
- **Előnyei:**
    - Megtéveszti, lelassítja a támadókat
    - Információkat gyűjt a támadásról
- **Hátrányai:** Dedikált szervert, eszközt igényel

A riasztások veszélyességi fokozatai, a riasztások kezelése, téves riasztás típusok

Riasztások típusai

- **False positive:** Elvárt, de nem kívánt riasztás.
- **False negatíve:** Rendszer nem ismeri fel a támadást.
- **True positive:** Helyesen ismeri fel a támadást.
- **True negatíve:** Helyes működésnél nem riaszt.

Riasztások kezelése

- Figyelmeztetés
- Logolás
- Aktivitás megszakítása
- TCP kapcsolat reset
- Jövőbeli kapcsolat blokkolása
- Engedélyezés