IT biztonság
2020/2021 tanév

BEHATOLÁS VÉDELEM

Intrusion (Behatolás)

- Valaki megpróbál betörni, vagy visszaélni a meglevő jogaival
- Bármilyen tevékenység, amellyel a CIA-hoz kapcsolódó visszaélés történik
  - Confidentiality - Bizalmasság
  - Integrity - Sértetlenség
  - Availability – Rendelkezésre állás

Intruders (Behatolók)

- Külsősök
  - Minden olyan személy vagy program, amely nem kapott engedélyt a hálózatunkon bármilyen rendszer és/vagy adat hozzáféréshez
- Belsősök
  - Legálisan hozzáfér a hálózathoz és az alkalmazásokhoz/adatokhoz, de nem jogosult felhasználás a célja

Hogyan jutnak be?

- Fizikai betörés
- Rendszer betörés
- Távoli betörés

Fogalmak

"An **intrusion detection system** (**IDS**) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a Management Station."

Fogalmak

"Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. **Intrusion detection and prevention systems** (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization."

IDPS architektúra

- Minden IDPS-ben van
  - Szenzor – adat begyűjtés (hálózati, felhasználói)
  - Analítika – adatelemzés, jellemzően a menedzsment is
  - Adminisztrátori interfész – Üzemeltetés, jellemzően az analítikai is

Az utolsó kettő két jogosultsági szint!

Történelem

- 1972 US Air Force tanulmány
- Log analítika helyett hálózati analítíka
- Első kereskedelmi megoldás ‘90-es évek
- Felderítés + megakadályozás ‘90-es évek vége (IPS)

Félreértések

- Van vírusírtóm, megtalálja a trójai falovat is!
- Van tűzfalam, az elég!
- Csak jelszóval lehet belépni a rendszerbe!

IDS/IPS elvárások

- Rendszeres definíció (pattern) frissítés
  - Automatikusan is
- Tudatosság
- Egy technikailag/technológiailag képzett személy (csapat)
- Riasztások, riportok

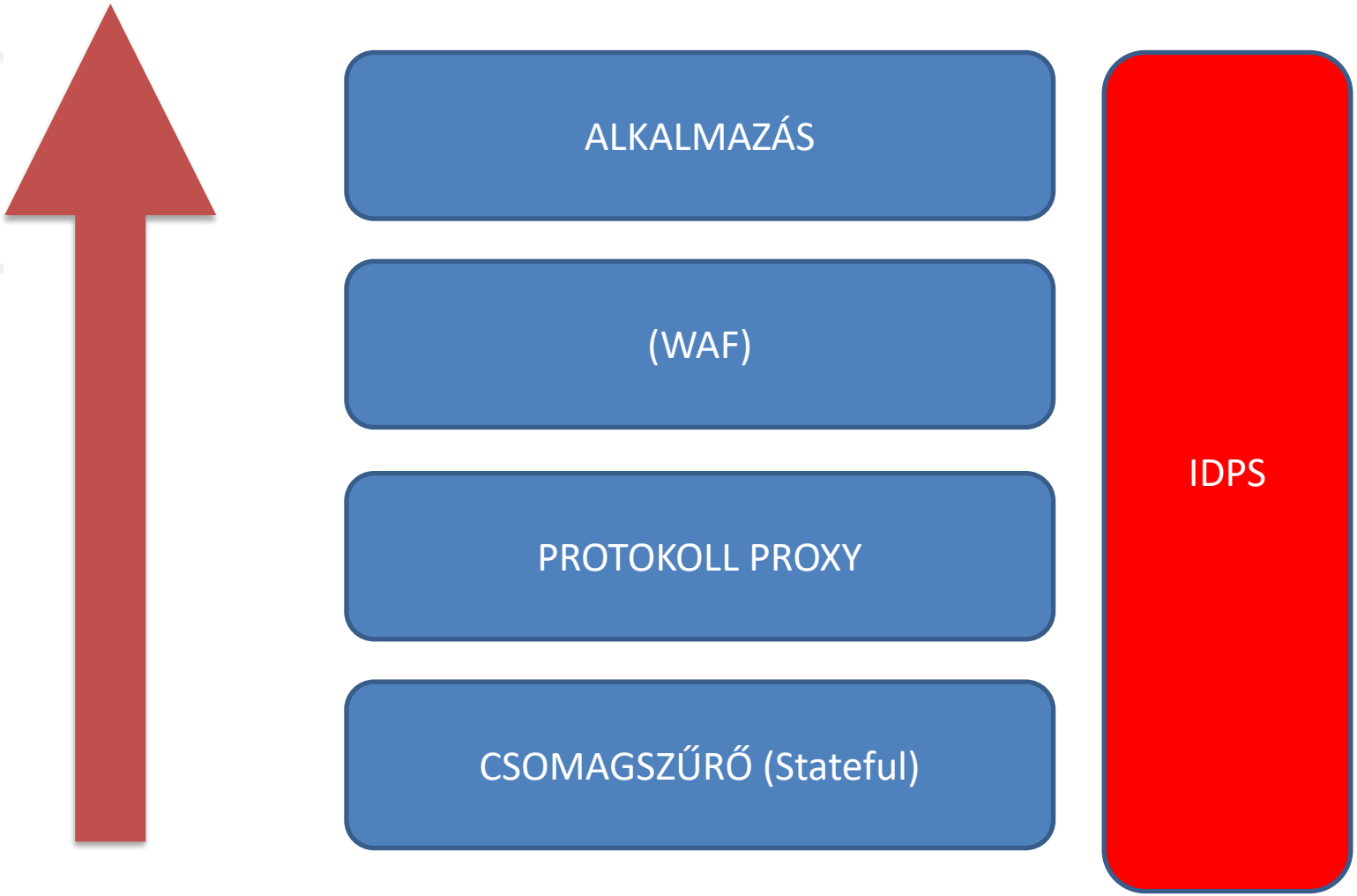
Mi NEM IDS/IPS?

- Antivírus
- Biztonsági scannerek
  - Nessus
- Log management
- Security/authentikációs rendszerek
- Tűzfalak, DLP rendszerek
  - Nos…

Támadások menete

- Külső felderítés
- Belső felderítés
  - “Legális” feltérképezés (pl. e-mail)
  - Social Engineering
- Betörés
- Jogosultság emelés
  - További rendszerek feltörése
- Fun and Profit

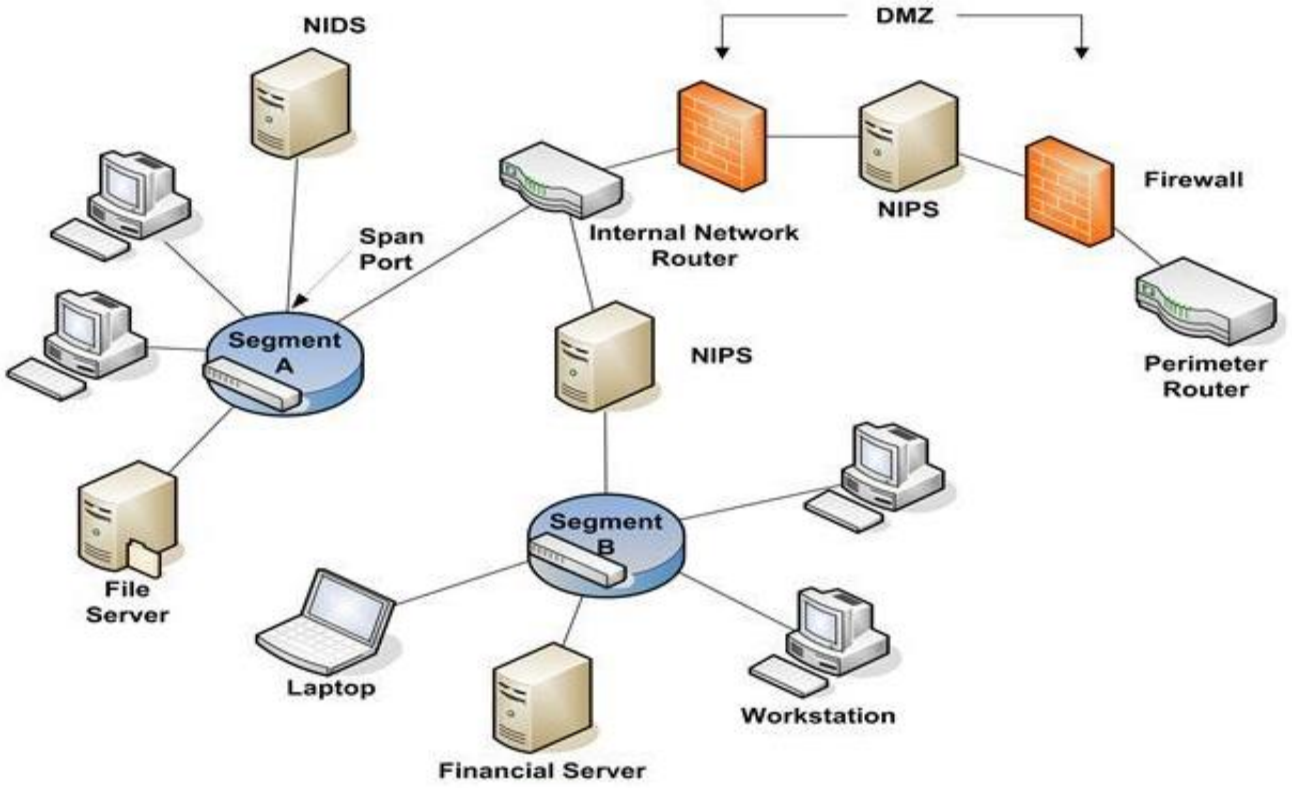
IDPS mint igény



Hol helyezhetjük el?

- Internet tűzfal előtt
- Tűzfalak mögött
- TűzfalakON
- Gerinc vonalakon
- Kritikus zónák ki és belépési pontjai
- Végpontokon

Architektúra



Az IDS karakterisztikái

- Találja meg az “összes” biztonsági eseményt
- Képes legyen gyorsan jelezni ezeket
  - Emberi beavatkozás nélkül
  - Ne “dőljön” össze
  - Védje meg saját magát
    - Management hálózat
  - Kis erőforrás igény
  - “Normál” minták

Motor

- Az “agy” az IDS mögött
  - Felismeri a támadó tevékenységeit
- Felismerés után
  - Riaszt (és/vagy)
  - Beavatkozik

IDS típusok

- Hogyan?
  - Szabály alapú
  - Anomália alapú
- Hol?
  - Host IDS – HIDS
  - Network IDS – NIDS
    - Tap/Span
    - In-line
    - Wireless IDS

Szabály alapú IDS

- Előre definiált szabályok
- Gyártói támogatás
- Felhasználók saját szabályai

Anomália alapú IDS

- “Normál” viselkedés feltérképezése
  - Mi a normális?
    - Heurisztika alapján
    - Statisztika alapján
    - Szabályok alapján

A betörés eltér a “normál” hálózati forgalomtól

HIDS

- Adott gép működését monitorozza
  - Hálózati forgalom
  - Lokális erőforrások
  - Logok vizsgálata (nincs korreláció)
- Ami gyanús egyik rendszerben, nem biztos hogy gyanús egy másikban
  - Folyamatos, diverz adatbázis karbantartás

NIDS

- Hálózati forgalom monitorozás
- Egyszerű telepíteni
  - TAP
  - SPAN
  - In-Line
- Kevés eszközt kell telepíteni

IDS esetén jellemzően erről a megközelítésről beszélünk

WIDS

- Nincs fizikai korlát
- Támadásokhoz nem kell közel lenni!
- RF monitorozás
- WIDS
  - Wireless – Wireless
  - Wireless – Wired
- Layer 3 felett normál IDS?

Előnyök és hátrányok

- A hálózati zaj jelentősen megnehezíti a rendszer működését
- Ez hamis riasztásokat eredményez
  - Túl sok riasztás -> szabály/trigger csökkentés -> a támadás bejut!
- Új támadásokat találhat meg
- Nem kifejezetten exploit jellegű támadásokat is felfedezhet
- Furcsa kommunikációkat is felfedez (kapcsolati adatok alapján)

Incidens kezelési terv

SSL/TLS

Mi a helyzet a titkosított forgalommal?

Jellemző IDS implementáció

- Csak NIDS
  - UTM
- NIDS + HIDS
  - Korreláció (közös management)

Honeypot/Honeynet

- Szándékosan gyenge rendszer
  - Izolált környezet (!!!!!!!)
- Alapértelmezett/gyenge jelszavak
- Hibás szoftver verziók

- Monitorozzuk a támadásokat
  - Kiváló 0-day exploit gyűjtésre ☺

IDPS jövőkép

- Komplex vagy specializált rendszerek, átfedő funkcionalitás
  - IDPS – Web Application Firewall (WAF)
  - HIDPS – DLP szenzorok
  - HIDPS – UBA rendszerek
  - IDPS network – SIEM analítika
- Miért nem használunk mindenhova IDPS-t?
  - Használunk (vagyis kellene)
  - Nem specializált

IDPS jövőkép

- IoT – Internet of Things
- Esetenként kiszorítják az egyéb technikai megoldások

Termékek

- Ingyenes
  - SNORT (1998!) (SourceFire)
  - Suricata
  - Bro (anomália is)
  - Kismet (WiFi)
  - OSSEC (Host)
- Elterjedt nagyvállalati megoldások
  - SourceFire
  - McAfee IPS
  - IBM Network Intrusion Prevention System
  - UTM (Checkpoint, Paloalto Networks)

DEMO

Hogyan tovább?

- Linux
  - Tcpdump
  - Wireshark
  - Bármilyen OpenSource megoldás
- Honeypot
- Google
  - DE ne fogadjatok el mindent, ellenőrizzétek!
    - Ja. Sok idő. ☺

horvath.tamas@brightdea.hu

KÖSZÖNÖM A FIGYELMET!