

Adatkapcsolati rétegbeli támadások védelméhez módjai

• CAM Table Attack

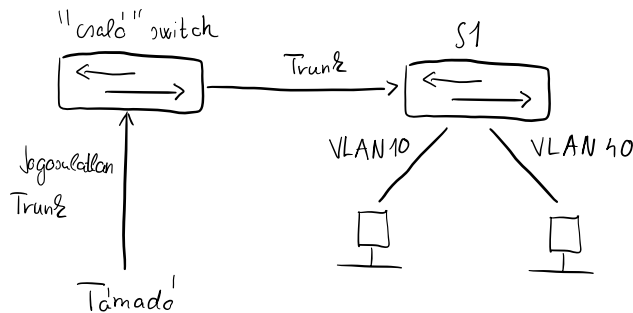
- CAM → Content-addressable memory
- Hamis MAC címek átadását küldi a switch-nek?
- Ez az adatátvitel arra készteti a switch-et, hogy a CAM-adatbázis táblájában lévő érvényes címet lecserélje, hogy helyet csináljon a hamis információknak.
- **Támadás** → macof linux parancs
macof -i <Interfész>
- **Kivédés**
 - Port security, vagyis a port nem továbbít olyan csomagokat, amik a forráscímei nem tartoznak a meghatározott címek csoportjába.
 - # shutdown (MAC címek kiürítése)
 - # no sh
 - # switchport mode access
 - # switchport port-security maximum <MAX> (Max MAC címek)
 - # switchport port-security
- Hibaüzenet → SecurityViolation

• VLAN Attacker → VLAN Hopping

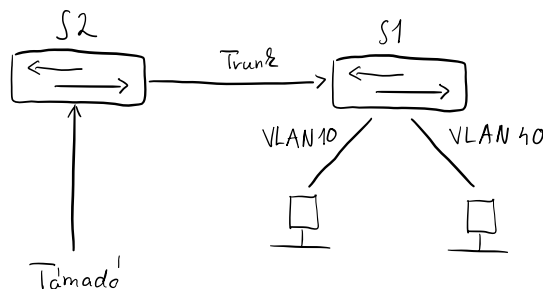
- A VLAN hálózati erőforrásainak támadására szolgáló módszer, ami csomagok küldésével történik egy olyan portra, ami általában nem érhető el egy végrendszerből.
- Fő célja, hogy hozzáférést szerezzen más VLAN-okhoz ugyanabban a hálózatban.

• Támadás

1. Switch spoofing → A támadó trunk vonalat hoz létre egy "csaló" switch hálózatba kapcsolódással.



2. Double tagging → A támadó hozzáad / módosítja a tag-ét az Ethernet-frame-ben.
(802.1Q tagging)

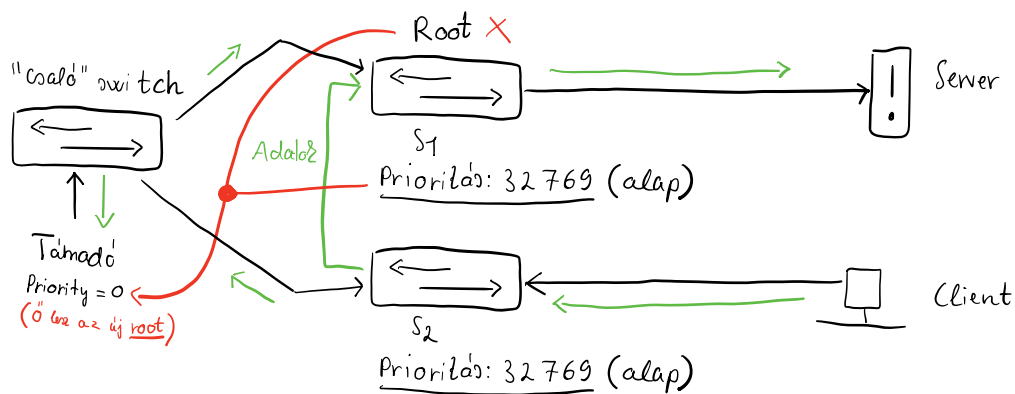


• Kivédése

- DTP (automatikus trunk) negotiation letiltása a nem trunk (switchport mode access) és trunk portokon (switchport non-negotiate).
- Nem használt portok letiltása és külön VLAN-ba helyezése.
- Trunk port engedélyezése manuálisan (switchport mode trunk).
- VLAN 1 ne legyen natív, használaton kívüli VLAN-ra állítsa be.

• STP Attack

- STP → Spanning Tree Protocol
 - Loop-ök (hurkök) ellen → ∞
- Az STP támadásakor a támadó meghamisítja a root bridge-t a topológiában.
 - A támadó egy STP konfiguráció/topológiaváltozás BPDU (Bridge Protocol Data Unit) sugároz ki, hogy megpróbálja zavarba ejteni az STP újraszámítását.
 - A elküldött BPDU azt jelenti, hogy a támadó rendszere lower bridge priority rendelkezik.
- Minden BPDU-nak van id-je → Bridge ID (BID) = Bridge Priority + MAC
- **Támadás**



• Kivédése

- BPDU Guard
- Root Guard
- Loop Guard

• Address Spoofing Attack → MAC address spoofing

- Hálózati eszközök hálózati interfészeinek általában rögzített MAC címet változtatja meg.
- A hálózat interfészvezérlő (NIC) "hard" kódolt MAC cím nem módosítható.
- Szűz illendőprogram (driver) ezt megakadályozza.

• Támadás

- Victim MAC cím megszerzése, majd a támadó a saját eszközhöz MAC címet átírja. ↓

• 11:CC:55:AA:77:BB

33:AA:99:DD:44:FF ↓

Támadó új MAC címe → 11:CC:55:AA:77:BB

• Kivédése

- Port Security
- Max MAC címek számának korlátozása
- # shutdown (MAC címek törlése)
- # no sh
- # switchport mode access
- # switchport port-security maximum <MAX> (Max MAC címek)
- # switchport port-security

• DHCP Attack

• DHCP starvation

- DHCP szolgálatot célzza és aminek során a támadó hamisított DHCP kéréseket küld az adott a céllal, hogy kimerítse a DHCP szolgáltató által kiosztható összes rendelkezésre álló IP címet.

• Támadás → Yersinia Linuxon

- DISCOVER csomagok küldésével

show ip dhcp pool → Hiba! (Nem hajtod ki végre a parancs)

↳ Letérhelte a DHCP adatbázist

show ip dhcp binding → Rengeteg IP cím, hamis MAC címmel.

• DHCP snooping

• Támadás

- Érvényesíti a nem megbízható forrásból érkező DHCP üzeneteket és kiszűri az érvénytelen üzeneteket.

• Kivédése

- DHCP snooping megbízható port beállítása
- DOT1x autentizáció
- Port Security
- Nem használt portok lezárása

• ARP Attacker → Address Resolution Protocol

• ARP spoofing

- A támadó hamis ARP csomagokat küld, amik összekapcsolják a támadó MAC címét a LAN-on lévő számítógép IP címével.

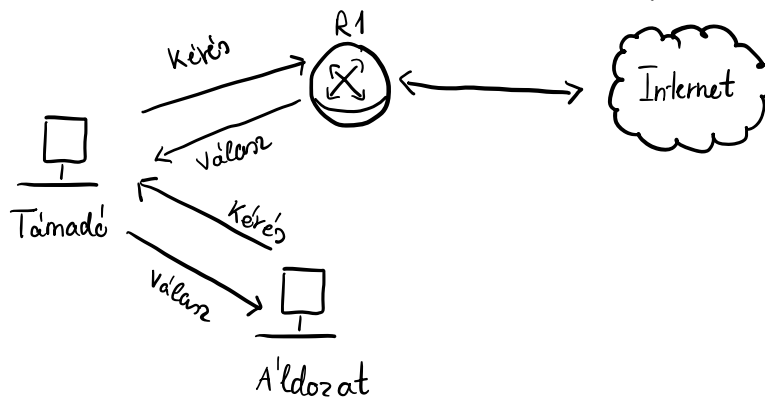
• Támadás → Arpspoof

- Szkenelés
- Hamis ARP-válaszok küldése, ami tartalmazza a támadó MAC címét.
- Az adatok most már a támadóhoz érkeznek meg.

• ARP poisoning

• Támadás

- A sikeres ARP spoofing után a támadó megváltoztatja az ARP táblát, így a hamisított MAC címet tartalmaz és a fertőzés elterjed.



• Kivédése

- Dynamic ARP Inspection használata
- ARP forgalom monitorozása