

14.a Ismertesse a 2. (adatkapcsolati) rétegbeli hálózati támadások kivédésének módjait!

Támadás fajtái

CAM Table Attack

- Hamis MAC címek áradatát küldi a switch-nek.
- Ez az adatáradat arra készíti a switch-et, hogy a CAM- adatbázis tábláiban lévő érvényes címeket kidobja, hogy helyet csináljon a hamis információknak.
- **Kivédése**
 - o Port security, vagyis a port nem továbbít olyan csomagot, amik forráscímei nem tartoznak a meghatározott címek csoportjába.

VLAN Attack

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

- Az STP támadásakor a támadó meghamisítja a root bridge-t a topológiában.
 - o A támadó egy STP konfiguráció/topológiaváltás BPDU-t sugároz ki, hogy megpróbálja kikényszeríteni az STP újraszámítását.
 - o A kiküldött BPDU azt jelenti, hogy a támadó rendszere lower bridge prioritással rendelkezik.
- **Kivédése:**
 - o BPDU Guard
 - o Root Guard
 - o Loop Guard

Address Spoofing Attack

- **Mac address spoofing**
 - o A Mac address spoofing egy olyan technika, ami egy hálózati eszköz hálózati interfészének gyárilag kiosztott MAC címét változtatja meg.
 - A hálózat interfészvezérlő (NIC) keményen kódolt MAC-cím nem módosítható.
 - Sok illesztőprogram lehetővé teszi a MAC cím megváltoztatását.
 - o **Kivédése**
 - Port security
 - Megengedett MAC-címek számának korlátozása egy porton.

DHCP Attack

- **DHCP starvation**
 - A DHCP starvation támadás egy olyan támadás, ami a DHCP kiszolgálókat célozza és aminek során a támadó hamisított DHCP kérelmeket készít azzal a céllal, hogy kimerítse a DHCP kiszolgáló által kiosztható összes rendelkezésre álló IP címet.
- **DHCP snooping**
 - A DHCP snooping egy olyan biztonsági funkció, ami tűzfalként működik a nem megbízható állomás és a megbízható DHCP kiszolgálók között.
 - A DHCP snooping érvényesíti a nem megbízható forrásokból érkező DHCP üzeneteket és kiszűri az érvénytelen üzeneteket.
- **Kivédése**
 - DHCP snooping megbízható port beállítása
 - DOT1x autentikáció
 - Port security
 - Nem használt portok lekapcsolása

ARP Attack

- **ARP spoofing**
 - A támadó hamis ARP csomagokat küld, amik összekapcsolják a támadó MAC címét a LAN-on lévő számítógép IP címével.
- **ARP poisoning**
 - A sikeres ARP spoofing után a támadó megváltoztatja a vállalat ARP táblát, így a hamisított MAC térképeket tartalmaz és a fertőzés elterjed.
- **Kivédése:**
 - Dynamic ARP Inspection használata
 - DHCP snooping validálja