**13.a Ismertesse a 2. (adatkapcsolati) rétegbeli hálózati támadások fajtáit! Milyen protokollok biztonsági réseit használják ki ezek a támadások?**

Támadás fajtái:

* **CAM Table Attack** : hamis MAC-címek áradatát küldik a switch-nek. Ez az adatáradat arra készteti a switch-et, hogy a CAM-adatbázis tábláiban lévő érvényes címeket kidobja, hogy helyet csináljon a hamis információknak.
* **VLAN Attack**:
* **VLAN Hopping**: A VLAN hálózati erőforrásainak támadására szolgáló módszer, amely csomagok küldésével történik egy olyan portra, amely általában nem érhető el egy végrendszerből. A támadás ezen formájának fő célja, hogy hozzáférést szerezzen más VLAN-okhoz ugyanabban a hálózatban.
* **STP Attacks:** Az STP-támadás során a támadó meghamisítja a root bridge-t a topológiában. A támadó egy STP konfiguráció/topológiaváltás BPDU-t sugároz ki, hogy megpróbálja kikényszeríteni az STP újraszámítását. A kiküldött BPDU azt jelenti, hogy a támadó rendszere lower bridge prioritással rendelkezik.
* **DHCP Attack**:
* **DHCP starvation**: A DHCP starvation támadás egy olyan támadás, amely a DHCP-kiszolgálókat célozza, és amelynek során a támadó hamisított DHCP-kérelmeket készít azzal a céllal, hogy kimerítse a DHCP-kiszolgáló által kiosztható összes rendelkezésre álló IP-címet. E támadás során a törvényes hálózati felhasználók számára megtagadható a szolgáltatás.
* **DHCP Snooping**: A DHCP snooping egy olyan biztonsági funkció, amely tűzfalként működik a nem megbízható állomás és a megbízható DHCP-kiszolgálók között. A DHCP snooping funkció a következő tevékenységeket végzi: - Érvényesíti a nem megbízható forrásokból érkező DHCP-üzeneteket, és kiszűri az érvénytelen üzeneteket.
* **ARP Attacks**:

-**ARP spoofing**: A hacker hamis ARP-csomagokat küld, amelyek összekapcsolják a támadó MAC-címét egy már a LAN-on lévő számítógép IP-címével.

-**ARP Poisoning**: A sikeres ARP-spoofing után a hacker megváltoztatja a vállalat ARP-tábláját, így az hamisított MAC-térképeket tartalmaz. A fertőzés terjed.

* **Address Spoofing Attacks**:

-**MAC address spoofing**: A MAC spoofing egy olyan technika, amely egy hálózati eszköz hálózati interfészének gyárilag kiosztott MAC-címét változtatja meg. A hálózati interfész-vezérlőn (NIC) keményen kódolt MAC-cím nem módosítható. Sok illesztőprogram azonban lehetővé teszi a MAC-cím megváltoztatását.