Běžné hrozby, zranitelnosti a útoky v lokální síti mohou zahrnovat:

- Odposlech komunikace: Útočník může odposlechnout komunikaci mezi zařízeními v lokální síti, což může způsobit únik citlivých informací, jako jsou uživatelská jména, hesla nebo data.
- Podvržení zpráv: Útočník může podvrhnout zprávy nebo data v síti a získat tak neoprávněný přístup nebo provést útok na cílové zařízení.
- ARP spoofing: Útočník může podvrhnout ARP odpovědi a změnit mapping MAC adres na IP adresy, což může vést k odklonění komunikace nebo snadnému odposlechu komunikace.
- MAC flooding: Útočník může zaplavit přepínač (switch) falešnými MAC adresami, což může způsobit zahlcení přepínače a odepření služeb legitimním zařízením.
- Neautorizovaný přístup: Útočník může se pokusit získat neautorizovaný přístup k lokální síti fyzickým nebo logickým způsobem, například připojením neautorizovaného zařízení nebo použitím neplatných autentizačních údajů.
- Problematika autentizace a řízení přístupu k lokální síti je důležitá zejména z hlediska zabezpečení sítě. Hlavním cílem je zajistit, aby pouze oprávněné osoby a zařízení měly přístup do sítě a mohly využívat její služby. K tomu se používají různé metody autentizace a autorizace.

AAA (Authentication, Authorization, Accounting)

- je koncept zabezpečení sítě, který kombinuje tři funkce – autentizaci, autorizaci a účtování. Autentizace ověřuje totožnost uživatele nebo zařízení a ověří, zda mají oprávnění k přístupu do sítě. Autorizace stanovuje, jaké zdroje v síti jsou pro uživatele nebo zařízení dostupné a jaké operace mohou provádět. Účtování sleduje použití sítě a zaznamenává informace o tom, kdo a jakou síťovou službu používá.

802.1x

- je standard pro autentizaci a řízení přístupu k lokální síti. Tento standard umožňuje zabezpečit přístup do sítě pomocí autentizace uživatelů a zařízení. Při použití 802.1x se uživatelé musí přihlásit pomocí svých uživatelských jmen a hesel a pouze ti, kteří jsou úspěšně autentizováni, mají přístup do sítě.
- Použití autentizace a řízení přístupu k lokální síti je klíčové pro zabezpečení sítě. Bez těchto opatření by mohlo dojít k neoprávněnému přístupu k citlivým informacím, ke zneužití sítě nebo k útoku na síťovou infrastrukturu.

Bezpečnostní funkce přepínače (switch) mohou zahrnovat:

- Port Security: Tato funkce umožňuje definovat, které MAC adresy jsou povoleny na konkrétním portu přepínače, což pomáhá chránit síť před neautorizovaným přístupem a MAC flooding útoky.
- DHCP Snooping: Tato funkce monitoruje provoz DHCP (Dynamic Host Configuration Protocol) v síti a chrání ji před
- neautorizovaným DHCP serverem, který by mohl distribuovat neplatné konfigurační informace nebo získávat citlivé informace od klientů. (Funguje tak že připnač filtruje dhcp zprávy)
- DAI (Dynamic ARP Inspection): Tato funkce monitoruje provoz ARP (Address Resolution Protocol) v síti a chrání ji před ARP spoofing útoky tím, že ověřuje, že MAC adresy v ARP zprávách odpovídají IP adresám registrovaným v tabulce ARP.
- Port-Based Access Control (802.1x): Tato funkce umožňuje autentizaci uživatelů nebo zařízení na konkrétním portu přepínače na základě protokolu 802.1x, což umožňuje řízení přístupu do sítě na základě identifikace a autentizace uživatelů nebo zařízení.

- VLAN Segmentation: Tato funkce umožňuje rozdělení sítě na různé virtuální sítě (VLANy), což umožňuje izolaci provozu mezi různými segmenty sítě a snižuje možnost neoprávněného přístupu nebo odposlechu komunikace.
- Je důležité, aby byly tyto bezpečnostní funkce správně nakonfigurovány a spravovány, aby byla zajištěna ochrana lokální sítě před potenciálními hrozbami, zranitelnostmi a útoky. Správná konfigurace a aktualizace firmware a softwaru přepínače je rovněž důležitá pro zabezpečení sítě.