# Bezpečnosť sieti

Sieť musí byť bezpečná, preto je dôležité ju po zostavení otestovať. [Link na nástroje (https://tools.kali.org/tools-listing)](https://tools.kali.org/tools-listing) na testovanie siete.

## Typy narušenia bezpečnosti

### Social engineering

Najnebezpečnejšia zraniteľnosť, je to útok na personál, ktorý je menej "odolný" voči hackerom
(vydávanie sa zaniekoho iného, dostať sa blízko k cieľovej osobe, ...).

### DoS (stress)

Preťaženie online služby veľa pripojeniami, v preklade je to zrušenie služby (Denial of Servie).

### DDoS (distribuovaný stress)

DoS s viacerými zariadeniami, v preklade je to distribuované zrušenie služby (Distributed Denial of Servie).

### Data breech

Narušenie serverov organizácii za účelom krádeže dát

### Malware

"Zákerný software", software, ktorý je určený na nekalé činosti na cieli.

### Rootkit

Úplná vzdialená kontrola nad cieľovým zariadením (server, PC, mobil), ak držieľ tohoto zariadenia s kontolou nesúhlasil.

### MitM

"Muž v strede", hacker je uprostred komunikácie medzi dvoma zariadeniami, hacker môže túto komunikáciu sledovať (sniffing) alebo ovplyvňovať (spoofing).

### XSS

"Skrz stránkové skriptovanie", vloženie skriptu (väčšinou JS) na fornt-end stránky, ktorú používajú užívatelia.

### A mnohé iné

## Prevencia pred narušením bezpečnosti

- VPN/Proxy
- Firewall/NGFW
- NAC
- ADBlock (môže zabrániť XSS útoku)
- Up to date software
- SSH, nie telnet
- Personálne audity
- Minimalozovanie výskytu zariadení so systémom Microsoft Windows na sieti

# Zabezpečenie koncových zariadení

## Cisco Email Security Appliance

The Cisco ESA zariadenie je navrhnuté aby monitorovalo SMTP.

Toto sú niektoré z funkcií produktu Cisco ESA:

- Blokovať známe hrozby
- Opravte škodlivý softvér, ktorý sa vyhol prvotnej detekcii
- Zlikvidujte e-mailové adresy so zlými odkazmi
- Blokovať prístup k novo infikovaným stránkam.
- Šifrujte obsah odchádzajúcich e-mailov, aby ste zabránili strate údajov.

## Cisco Web Security Appliance

- Zmierňuje webové hrozby. Pomáha organizáciám riešiť problémy so zabezpečením a riadením webového prenosu.
- Kombinuje pokročilú ochranu pred malvérom, viditeľnosť a kontrolu aplikácií, prijateľné kontroly politík používania a vytváranie prehľadov.
- Poskytuje úplnú kontrolu nad tým, ako používatelia pristupujú k internetu. Niektoré funkcie a aplikácie, ako napríklad čet, správy, video a zvuk, je možné povoliť, obmedziť časovými limitmi a šírkou pásma alebo zablokovať podľa požiadaviek organizácie.
- Môže vykonávať zoznam zakázaných adries URL, filtrovanie adries URL, skenovanie škodlivého softvéru, kategorizáciu adries URL, filtrovanie webových aplikácií a šifrovanie a dešifrovanie prenosu z webu.

# Regulácia prístupu

# Autentifikácia pomocou lokálneho hesla

- Najjednoduchšou metódou overovania vzdialeného prístupu je konfigurácia kombinácie prihlásenia a hesla na konzole, vty lines a aux portoch.

# AAA súčasti

- AAA je skratka pre autentizáciu, autorizáciu a zúčtovanie a poskytuje primárny rámec pre nastavenie riadenia prístupu na sieťovom zariadení.
- AAA je spôsob kontroly toho, kto má povolenie na prístup do siete (autentifikáciu), čo môže robiť, keď je v nej (autorizácia), a na auditovanie toho, aké činnosti vykonali pri prístupe do siete (zúčtovanie).

## Authentication

Lokálne a serverové sú dve bežné metódy implementácie AAA autentifikácie.

**Lokálna autentifikácia AAA:**

- Metóda ukladá používateľské mená a heslá lokálne v sieťovom zariadení (napr. Router Cisco).
- Používatelia sa autentifikujú podľa miestnej databázy.
- Lokálna AAA je ideálna pre malé siete.

**Serverové overenie AAA:**

- Pri serverovej metóde smerovač pristupuje k centrálnemu serveru AAA.
- Server AAA obsahuje používateľské mená a heslo pre všetkých používateľov.
- Router používa na komunikáciu so serverom AAA protokoly Remote Authentication Dial-In User Service (RADIUS) alebo Terminal Access Controller Access Control System (TACACS +).
- Ak je k dispozícii viac routerov a switchov, je vhodnejšie serverové AAA.

## Authorization

- Autorizácia AAA je automatická a nevyžaduje od používateľov, aby po overení vykonali ďalšie kroky.
- Autorizácia určuje, čo môžu a nemôžu používatelia v sieti robiť po overení.
- Autorizácia používa množinu atribútov, ktorá popisuje prístup používateľa do siete. Tieto atribúty používa server AAA na určenie oprávnení a obmedzení pre daného používateľa.

## Accounting

Účtovníctvo AAA zhromažďuje a hlási údaje o použití. Tieto údaje môžu byť použité na také účely, ako je audit alebo fakturácia. Zhromaždené údaje môžu zahŕňať časy začatia a ukončenia pripojenia, vykonané príkazy, počet paketov a počet bajtov.

**Účtovníctvo sa primárne využíva na kombináciu s autentifikáciou AAA.**

- Server AAA vedie podrobný protokol o tom, čo presne autentifikovaný užívateľ v zariadení robí, ako je to znázornené na obrázku. Zahŕňa to všetky EXEC a konfiguračné príkazy vydané používateľom.
- Denník obsahuje početné údajové polia vrátane používateľského mena, dátumu a času a skutočného príkazu, ktorý zadal používateľ. Tieto informácie sú užitočné pri riešení problémov so zariadeniami. Poskytuje tiež dôkazy o tom, kedy jednotlivci páchajú škodlivé činy.

## 802.1X

Štandard IEEE 802.1X je portový protokol kontroly prístupu a autentifikácie. Tento protokol obmedzuje neoprávnené pracovné stanice v pripojení k sieti LAN prostredníctvom verejne prístupných portov prepínačov. Autentifikačný server autentifikuje každú pracovnú stanicu, ktorá je pripojená k portu switcha, pred sprístupnením akýchkoľvek služieb ponúkaných switchom alebo LAN.

Pri overovaní pomocou portu 802.1X majú zariadenia v sieti špecifické úlohy:

- **Klient (Supplicant (najznamejši WPA supplicant))** - Toto je zariadenie, na ktorom je spustený klientsky softvér kompatibilný s normou 802.1X, ktorý je k dispozícii pre káblové alebo bezdrôtové zariadenia.
- **Switch (Authenticator)** - Switch slúži ako sprostredkovateľ medzi klientom a autentifikačným serverom. Vyžiada si od klienta identifikačné informácie, overí ich pomocou autentifikačného servera a odošle odpoveď klientovi. Ďalším zariadením, ktoré by mohlo slúžiť ako autentifikátor, je bezdrôtový prístupový bod.
- **Autentifikačný server** - Server overuje identitu klienta a oznamuje switchu alebo bezdrôtovému prístupovému bodu, že klient má alebo nemá oprávnenie na prístup k sieti LAN a prepínacím službám.

# Nebezpečia layeru 2

## Zranitelnosti

Správcovia sietí bežne implementujú bezpečnostné riešenia na ochranu prvkov vo vrstve 3 až po vrstvu 7. Na ochranu týchto prvkov používajú siete VPN, brány firewall a zariadenia IPS. Ak je však ohrozená vrstva 2, ovplyvnia sa aj všetky vrstvy nad ňou. Napríklad, ak aktér hrozby s prístupom do internej siete zachytil rámce vrstvy 2, potom by všetky zabezpečenia implementované vo vyššie uvedených vrstvách boli zbytočné. Aktér hrozby by mohol spôsobiť veľké škody na sieťovej infraštruktúre LAN vrstvy 2.

## Kategórie útokov na switch

Zabezpečenie je len také silné ako najslabší článok v systéme a vrstva 2 sa považuje za tento slabý článok. Je to tak preto, lebo siete LAN boli tradične pod administratívnou kontrolou jednej organizácie. Vo svojej podstate sme dôverovali všetkým osobám a zariadeniam pripojeným k

našej sieti LAN. Dnes, vďaka BYOD a sofistikovanejším útokom, sa naše LAN stali zraniteľnejšie voči penetrácii.

| Kategória | Príklad |
|---|---|
| MAC Table Attacks | Includes MAC address flooding attacks. |
| VLAN Attacks | Includes VLAN hopping and VLAN double-tagging attacks. It also includes attacks between devices on a common VLAN. |
| DHCP Attacks | Includes DHCP starvation and DHCP spoofing attacks. |
| ARP Attacks | Includes ARP spoofing and ARP poisoning attacks. |
| Address Spoofing Attacks | Includes MAC address and IP address spoofing attacks. |
| STP Attacks | Includes Spanning Tree Protocol manipulation attacks. |

## Migračné techniky útoku na switch

Tieto riešenia vrstvy 2 nebudú účinné, ak nebudú zabezpečené protokoly správy. Odporúčajú sa tieto stratégie:

- Vždy používajte zabezpečené varianty protokolov správy, napríklad SSH, Secure Copy Protocol (SCP), Secure FTP (SFTP) a Secure Socket Layer / Transport Layer Security (SSL / TLS).
- Na správu zariadení zvážte použitie mimopásmovej siete na správu.
- Používajte vyhradenú správu VLAN, kde sa nenachádza nič iné ako prevádzka správy.
- Na filtrovanie nežiaduceho prístupu použite zoznamy ACL.

| Rieěnie | Popis |
|---|---|
| Port Security | Prevents many types of attacks including MAC address flooding attacks and DHCP starvation attacks. |
| DHCP Snooping | Prevents DHCP starvation and DHCP spoofing attacks. |
| Dynamic ARP Inspection (DAI) | Prevents ARP spoofing and ARP poisoning attacks. |
| IP Source Guard (IPSG) | Prevents MAC and IP address spoofing attacks. |

# Útok na tabuľku MAC adries

## Kontrola prevádzky switchu

Pri rozhodovaní o preposielaní switch LAN vrstvy 2 zostavuje tabuľku na základe zdrojových adries MAC v prijatých vo frejmoch. Toto sa nazýva tabuľka MAC adries. Tabuľky MAC adries sú uložené v pamäti a slúžia na efektívnejšie switchovanie frejmov.

## Zaplavenie tabuľky MAC adries

Všetky tabuľky MAC majú pevnú veľkosť a v dôsledku toho môžu switchu dôjsť prostriedky na ukladanie adries MAC. Útoky na zaplavenie adresy MAC využívajú toto obmedzenie bombardovaním prepínača falošnými zdrojovými adresami MAC, kým nie je tabuľka MAC adries prepínača plná.
Keď k tomu dôjde, prepínač zaobchádza s rámcom ako s neznámym jednosmerovým vysielaním a začne zahlcovať všetok prichádzajúci prenos zo všetkých portov na tej istej sieti VLAN bez odkazovania na tabuľku MAC. Táto podmienka teraz umožňuje aktérovi hrozby zachytiť všetky rámce odoslané z jedného hostiteľa do druhého v lokálnej sieti LAN alebo lokálnej VLAN. Traffic je zahltený iba v rámci miestnej siete LAN alebo VLAN. Účastník ohrozenia môže zachytiť iba prenos v rámci miestnej siete LAN alebo VLAN, ku ktorej je účastník ohrozenia pripojený.

## Migrácia tabuľky MAC adries

Vďaka čomu sú nástroje ako macof (https://github.com/WhiteWinterWolf/macof.py) (súčasťou projektu dsniff (https://www.monkey.org/~dugsong/dsniff/)) také nebezpečné, je to, že útočník dokáže veľmi rýchlo vytvoriť útok na pretečenie tabuľky MAC. Napríklad switch Catalyst 6500 môže uložiť 132 000 MAC adries do svojej tabuľky MAC adries. Nástroj ako macof (https://github.com/WhiteWinterWolf/macof.py) môže zaplaviť switch až 8 000 falošných snímok za sekundu; vytvorenie útoku pretečenia tabuľky MAC adries v priebehu niekoľkých sekúnd.

Ďalším dôvodom, prečo sú tieto útočné nástroje nebezpečné, je to, že ovplyvňujú nielen lokálny switch, ale môžu ovplyvňovať aj ďalšie pripojené switche vrstvy 2. Keď je tabuľka MAC adries prepínača plná, začne zaplavovať všetky porty vrátane portov pripojených k iným prepínačom vrstvy 2.

Na zmiernenie útokov na pretečenie tabuľky MAC adries musia správcovia siete implementovať zabezpečenie portu. Zabezpečenie portu umožní na portu zistiť iba zadaný počet zdrojových adries MAC.

# LAN útoky

## VLAN Hopping Attacks

Skokový útok VLAN umožňuje, aby bola prevádzka z jednej VLAN viditeľná inou VLAN bez pomoci routera. Pri základnom preskakovacom útoku VLAN nakonfiguruje aktér hrozby hostiteľa tak, aby fungoval ako switch, aby využil výhodu funkcie automatického portu trunking, ktorá je predvolene povolená na väčšine portov switchu.

Aktér ohrozenia nakonfiguruje hostiteľa tak, aby spoofoval signalizáciu 802.1Q a signalizáciu vlastníckeho Cisco protokolu Dynamic Trunking Protocol (DTP), do trunku pomocou spojovacieho switchu úspešný, switch vytvorí diaľkové spojenie s hostiteľom. Aktér hrozby má teraz prístup ku všetkým sieťam VLAN na switchi. Aktér hrozby môže odosielať a prijímať prenosy na ľubovoľných sieťach VLAN a efektívne preskakovať medzi sieťami VLAN (podobné ako pivoting (technika hackingu)).

## VLAN Double-Tagging Attacks

Aktér hrozby je, že konkrétne situácie môžu vložiť skrytý tag 802.1Q do frejmu, ktorý už tag 802.1Q obsahuje. Tento tag umožňuje frejmu prejsť na VLAN, ktorú pôvodný tag 802.1Q nešpecifikovala.

1. Aktér hrozby pošle prepínaču rámček 802.1Q s dvojitým označením. Vonkajšia hlavička má značku VLAN aktéra ohrozenia, ktorá je rovnaká ako natívna VLAN hlavného portu.

2. Frejm dorazí na prvý switch, ktorý sleduje prvú štvorbajtový tag 802.1Q. Svič vidí, že frejm je určený pre natívnu VLAN. Svič po odstránení tagu VLAN preposiela paket von zo všetkých natívnych portov VLAN. Frejm nie je označený znova, pretože je súčasťou natívnej VLAN. V tomto okamihu je vnútorná značka VLAN stále neporušená a nebol skontrolovaný prvým svičom.

3. Frejm dorazí k druhému sviču, ktorý nevie, že by mal byť pre natívnu VLAN. Nativní prenos VLAN nie je označený odosielacím svičom, ako je uvedené v špecifikácii 802.1Q. Druhý svič sleduje iba vnútornú značku 802.1Q, ktorú vložil aktér ohrozenia, a vidí, že frejm je určený pre cieľovú VLAN. Druhý svič odošle frejm na cieľ alebo ho zaplaví, v závislosti od toho, či pre cieľ existuje záznam tabuľky MAC adries.

Útok dvojitým značkovaním VLAN je jednosmerný a funguje iba v prípade, že je útočník pripojený k portu nachádzajúcemu sa v rovnakej VLAN ako natívna VLAN hlavného portu. Myšlienka je taká, že dvojité tagovanie umožňuje útočníkovi posielať údaje hostiteľom alebo serverom vo VLAN, ktoré by inak boli blokované určitým typom konfigurácie riadenia prístupu. Pravdepodobne bude povolená aj spätná prevádzka, čo útočníkovi umožní komunikovať so zariadeniami na normálne blokovanej sieti VLAN.

Zmiernenie útoku VLAN - Preskakovaniu sietí VLAN a útokom dvojitého značenia VLAN je možné zabrániť implementáciou nasledujúcich bezpečnostných gajdlajnov trunku, ktoré sú popísané v predchádzajúcom module:

- Zakážte kanálovanie na všetkých prístupových portoch.
- Zakážte automatické prepájanie kanálov na spojeniach kufra, aby sa kufre museli povoliť manuálne.
- Uistite sa, že natívna VLAN sa používa iba pre diaľkové spojenia.

# DHCP Messages

Servery DHCP dynamicky poskytujú klientom informácie o konfigurácii adresy IP vrátane adresy IP, masky podsiete, predvolenej brány, serverov DNS a ďalších.

# DHCP Attacks

Dva typy útokov DHCP sú "DHCP hladovanie" a "DHCP spoofing". Oba útoky sú zmiernené implementáciou DHCP snooping.

- **DHCP Starvation Attack** - Cieľom tohto útoku je vytvoriť DoS pre pripojenie klientov. Útoky typu DHCP od hladu si vyžadujú útočný nástroj, napríklad Gobbler. Gobbler má schopnosť pozrieť sa na celý rozsah prenajímateľných IP adries a snaží sa ich všetky prenajať. Konkrétne vytvára správy o zisťovaní DHCP s falošnými MAC adresami.
- **DHCP Spoofing Attack** - Deje sa to, keď je k sieti pripojený podvodný server DHCP a poskytuje legitímnym klientom nesprávne konfiguračné parametre adresy IP. Nečestný server môže poskytnúť rôzne zavádzajúce informácie vrátane nasledujúcich:

- **Nesprávna predvolená brána** - Fejkový server poskytuje neplatnú bránu alebo adresu IP hostiteľa, aby vytvoril útok typu man-in-the-middle. Môže to zostať úplne nezistené, pretože narušiteľ zachytáva tok údajov cez sieť.
- **Chybný server DNS** - Fejkový server poskytuje nesprávnu adresu servera DNS, ktorá nasmeruje používateľa na škodlivú webovú stránku.
- **Chybná adresa IP** - Fejkový server poskytuje neplatnú adresu IP, čo efektívne vytvára útok DoS na klienta DHCP.

# ARP Attacks

- Hostitelia vysielajú ARP požiadavky na určenie MAC adresy hostiteľa s cieľovou IP adresou. Všetci hostitelia v podsiete prijmú a spracujú požiadavku ARP. Hostiteľ so zodpovedajúcou adresou IP v požiadavke ARP odošle odpoveď ARP.
- Klient môže poslať nevyžiadanú odpoveď ARP nazvanú „bezodplatná ARP“. Ostatní hostitelia v podsiete ukladajú adresu MAC a adresu IP obsiahnutú v bezdôvodnom ARP do svojich tabuliek ARP.
- Útočník môže odoslať sviču bezodplatnú správu ARP obsahujúcu sfalšovanú adresu MAC a svič by podľa toho aktualizoval svoju tabuľku MAC. Pri typickom útoku odosiela aktér hrozby nevyžiadané odpovede ARP ďalším hostiteľom v podsieti s MAC adresou aktéra hrozby a IP adresou predvolenej brány, čím efektívne nastavuje útok typu man-in-the-middle.
- Na internete existuje veľa nástrojov na vytváranie útokov typu ARP man-in-the-middle.
- Protokol IPv6 používa na rozlíšenie adries vrstvy 2 protokol ICMPv6 Neighbor Discovery Protocol. Protokol IPv6 obsahuje stratégie na zmiernenie spoofingu so susednou reklamou, podobne ako IPv6 zabraňuje spoofed ARP Reply.
  ARP spoofing a poisoning sú zmiernené implementáciou Dynamic ARP Inspection (DAI).

# Address Spoofing Attacks

- Falošná adresa IP je, keď aktér hrozby unesie platnú adresu IP iného zariadenia v podsiete alebo použije náhodnú adresu IP. Falošné adresy IP je ťažké zmierniť, najmä ak sa používajú v podsieti, do ktorej adresa IP patrí.
- K spoofingovým útokom na MAC adresy dochádza, keď aktéri hrozby zmenia MAC adresu svojho hostiteľa tak, aby zodpovedala inej známej MAC adrese cieľového hostiteľa. Svič prepíše aktuálny záznam tabuľky MAC a priradí adresu MAC novému portu. Potom nechtiac preposiela frejmy určené pre cieľového hostiteľa útočiacemu hostiteľovi.
- Keď cieľový hostiteľ pošle prenos, prepínač opraví chybu a MAC adresu zarovná s pôvodným portom. Ak chcete zabrániť tomu, aby prepínač vrátil priradenie portu do správneho stavu, môže aktér hrozby vytvoriť program alebo skript, ktorý bude neustále posielať frejmy do sviču, aby si prepínač uchoval nesprávne alebo sfalšované informácie.
- Na vrstve 2 nie je žiadny bezpečnostný mechanizmus, ktorý by sviču umožňoval overiť zdroj adries MAC, čo ho robí tak zraniteľným voči falšovaniu.
  Falošné adresy IP a MAC je možné zmierniť implementáciou protokolu IP Source Guard

(IPSG).

## STP Attack

- Sieťoví útočníci môžu manipulovať s protokolom Spanning Tree Protocol (STP) tak, aby vykonali útok spoofingom rootového mosta a zmenou topológie siete. Útočníci potom môžu zachytiť všetku komunikáciu pre doménu s okamžitým prepnutím.
- Na vykonanie manipulačného útoku STP vysiela útočiaci hostiteľ dátové jednotky mosta protokolu STP (BPDU), ktoré obsahujú zmeny konfigurácie a topológie, ktoré vynútia prepočty spanning-tree. Jednotky BPDU zaslané útočiacim hostiteľom oznamujú nižšiu prioritu mosta pri pokuse o zvolenie za koreňový mostík.
- Tento útok STP je zmiernený implementáciou BPDU Guard na všetkých prístupových portoch. BPDU Guard je podrobnejšie diskutovaný neskôr v kurze.

## CDP Reconnaissance

Cisco Discovery Protocol (CDP) je proprietárny protokol na zisťovanie odkazov vrstvy 2. Predvolene je povolená na všetkých zariadeniach Cisco. Správcovia sietí tiež používajú program CDP na konfiguráciu a riešenie problémov so sieťovými zariadeniami. Informácie CDP sa zasielajú na porty podporujúce CDP v pravidelných, nezašifrovaných a neoverených vysielaniach. Informácie CDP zahŕňajú IP adresu zariadenia, verziu softvéru IOS, platformu, možnosti a natívnu VLAN. Zariadenie prijímajúce správu CDP aktualizuje svoju databázu CDP.

- Ak chcete zmierniť využitie CDP, obmedzte použitie CDP na zariadeniach alebo portoch. Napríklad zakážte CDP na okrajových portoch, ktoré sa pripájajú k nedôveryhodným zariadeniam.
- Ak chcete globálne zakázať CDP na zariadení, použite príkaz no cdp run global configuration mode. Ak chcete globálne povoliť CDP, použite príkaz globálnej konfigurácie cdp run.
- Ak chcete zakázať CDP na porte, použite príkaz na konfiguráciu rozhrania bez povolenia cdp. Ak chcete povoliť CDP na porte, použite príkaz konfigurácie rozhrania cdp enable.

Protokol LLDP (Link Layer Discovery Protocol) je tiež zraniteľný pri prieskumných útokoch. Nakonfigurujte žiadne spustenie lldp, aby ste globálne zakázali LLDP. Ak chcete zakázať LLDP na rozhraní, nakonfigurujte žiadny prenos lldp a žiadny príjem lldp.