

Text laboratórnej úlohy

Laboratórna úloha č. 3

BEZPEČNOST SPOJOVEJ VRSTVY

Úvod k laboratórnej úlohe

Cieľom laboratórnej úlohy je analyzovať zraniteľnosti na úrovni spojovej vrstvy referenčného modelu ISO/OSI a demonštrovať možné riziká a útoky.

V prvej časti laboratórnej úlohy s využitím vhodných nástrojov vo virtuálnom stroji Kali Linux realizujete **simuláciu sieťového útoku ARP spoofing**, počas ktorej sa pokúsíte podvrhnúť falošné záznamy do ARP tabuľky klienta, presmerovať sieťovú komunikáciu cez zariadenie útočníka a analyzovať jej obsah. Okrem vykonania samotného útoku, kedy si vyskúšate prácu s nástrojmi **arp spoof** a **Etttercap**, sa tiež naučíte analyzovať a vhodne interpretovať zachytené sieťové dáta v prostredí **sieťového analyzátoru Wireshark**. Následne budete implementovať ochranné opatrenia (statické ARP záznamy, monitorovanie ARP záznamov) a testovať ich účinnosť.

Požiadavky pre vypracovanie úlohy:

- software: VMware Workstation Player pre virtualizáciu staníc,
- virtuálne stroje: tri virtuálne stroje s Kali Linux.

1. Teoretický úvod

V tejto laboratórnej úlohe budete oboznámení s **protokolom ARP**, ktorý slúži k prekladu logických adries zariadení na adresy fyzické. Ďalšia časť bude zameraná na problematiku týkajúcu sa bezpečnostných hrozieb na úrovni spojovej vrstvy referenčného modelu ISO/OSI. Vysvetlený bude **princíp útoku ARP spoofing**, u ktorého bude uskutočnená tiež jeho praktická realizácia.

1.1. ARP protokol

ARP protokol (z angl. *Address Resolution Protocol*) je protokol pracujúci na úrovni spojovej vrstvy referenčného modelu ISO/OSI, ktorý zabezpečuje mapovanie („preklad“) logickej IP adresy zariadenia na jeho fyzickú adresu (spravidla MAC). Protokol ARP teda slúži zariadeniam v lokálnej sieti k nájdeniu odpovedajúcej adresy druhej úrovne (t. j. fyzickej adresy) iného zariadenia na základe jeho sieťovej IP adresy (t. j. adresy tretej úrovne). [1], [2]

Keď zariadenie potrebuje odoslať IP paket inému uzlu nachádzajúcemu sa v tej istej lokálnej sieti, najprv prostredníctvom ARP požiadavky zisťuje, aká MAC adresa prislúcha k požadovanej IP adrese. Po získaní odpovede odosielateľ vytvorí ethernetový rámec so správnou cieľovou MAC adresou, ktorú mu dané zariadenie poskytlo v zaslanej ARP odpovedi, a odosiela ho na úrovni spojovej vrstvy.

Pre ARP protokol sú známe nedostatky determinujúce zraniteľnosti, v dôsledku ktorých je ARP protokol náchylný na sieťové útoky. Medzi podstatné zraniteľnosti ARP protokolu možno zaradiť nasledujúce:

- **Chýbajúca autentifikácia:** ARP protokol nemá zabudovaný žiadny mechanizmus autentifikácie, v čoho dôsledku môže ktorékoľvek zariadenie v sieti odosielať ARP odpovede bez overenia identity. Tento nedostatok umožňuje útočníkovi podvrhnúť falošnú MAC adresu pre konkrétnu IP adresu a docieľiť tak „otravu“ ARP tabuľky na zariadení odosielajúcom žiadosť *ARP Request* (tzv. *ARP Cache Poisoning* útok).
- **Dynamická ARP tabuľka:** ARP tabuľka je dynamická, čo znamená, že zariadenia automaticky aktualizujú svoje záznamy na základe prijatých ARP odpovedí. Útočník môže popísaný mechanizmus zneužiť tak, že zariadeniu poskytne falošné údaje a prepíše pôvodné hodnoty fyzických adries iných zariadení zaznamenané v ARP tabuľke.
- **ARP odpovede bez vyžiadania:** Zariadenia v sieti môžu prijímať a ukladať ARP odpovede, aj keď si ich samé nevyžiadali (t. j. keď tieto zariadenia neodoslali konkrétnu žiadosť *ARP Request*). Útočník môže využiť uvedenú vlastnosť ARP protokolu k rozosieleniu nesprávnych, falošných ARP odpovedí (tzv. „*gratuitous ARP replies*“), čím môže ovplyvniť obsah ARP tabuliek u zariadení a celkovo manipulovať s priebehom sieťovej komunikácie.
- **Zraniteľnosť voči Man-in-the-Middle útokom:** Vzhľadom na absenciu zabezpečenia môžu útočníci presmerovať dátovú komunikáciu medzi zariadeniami cez svoje vlastné zariadenie úplne transparentne z pohľadu obete. To umožňuje odpočúvanie komunikácie, modifikáciu paketov alebo realizáciu útokov typu *Denial-of-Service* (DoS) o odopretie poskytovania služby.
- **Neexistuje vstavaná ochrana:** Nakoľko ARP protokol pracuje na spojenej vrstve OSI modelu, samotný nemá zabudované mechanizmy, ktoré by umožnili kontrolovať autentickosť prijatých ARP odpovedí, čo môže podnietiť útoky súvisiace s podvrhnutím falošných informácií a „otravou“ ARP tabuľky (viď vyššie). Preto je nutné implementovať dodatočné ochranné opatrenia, medzi ktoré patria: konfigurácia statických ARP záznamov, využitie nástrojov pre ARP monitoring (napr. Arpwatch) alebo definícia pravidiel firewallu obmedzujúcich prijímanie neoprávnených ARP odpovedí.

ARP tabuľka

Každé zariadenie v sieti si vo svojej pamäti aktívne udržiava tabuľku obsahujúcu záznamy o dvojiciach k sebe prislúchajúcich logických IP adries a fyzických (MAC) adries, tzv. ARP tabuľku (tiež *ARP cache*). Záznamy v ARP tabuľke majú zvyčajne krátku životnosť (napr. 5 minút) a sú v stanovených intervaloch pravidelne

aktualizované¹. Záznamy k sebe prislúchajúcich dvojíc IP adresy a fyzickej adresy pre jednotlivé zariadenia v danej sieti sa do ARP tabuľky ukladajú buď na základe činnosti samotného ARP protokolu, alebo je možné potrebné informácie zadať do ARP tabuľky aj manuálne.

Štruktúra ARP správ

ARP správy sú prenášané na spojovej vrstve ISO/OSI modelu, t. j. nevyužívajú žiadny protokol vyššej (IP alebo TCP) a sú zapuzdrené priamo do ethernetového rámca. Protokol ARP funguje nezávisle od vyšších vrstiev a práve vďaka tomu môžu byť ARP správy odosielané aj v prípade, kedy ešte nepoznáme MAC adresu cieľového zariadenia, nakoľko úvodná správa ARP Request, ako bude popísané ďalej, je odoslaná na všesmerovú fyzickú adresu v príslušnej lokálnej sieti.

Protokol ARP definuje dva základné typy správ:

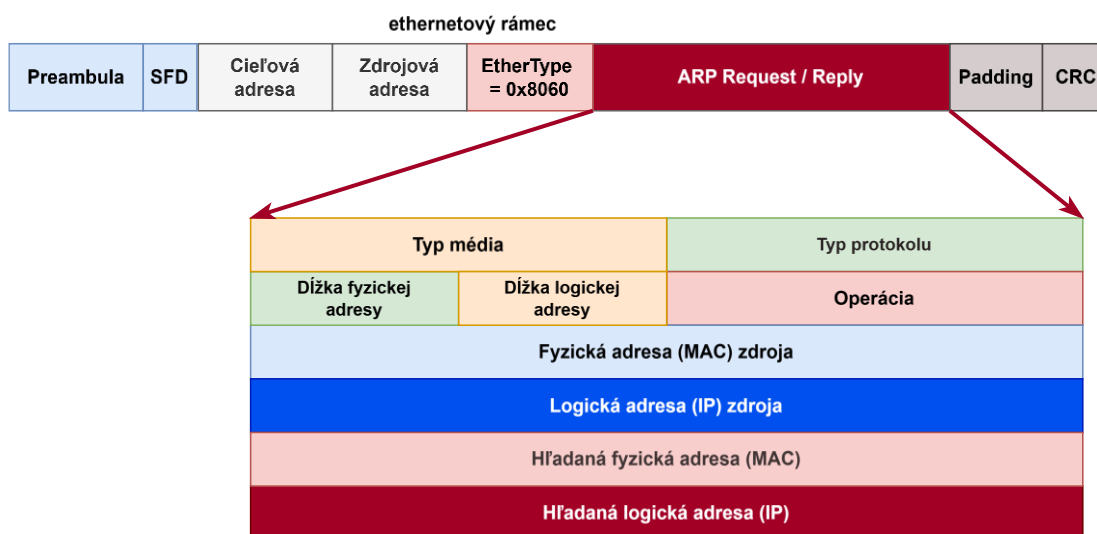
- **ARP Request (žiadosť)** – vysielaná do siete v prípade, že zariadenie potrebuje zistiť MAC adresu príjemcu pre známu IP adresu;
- **ARP Reply (odpoveď)** – odpoveď na žiadosť obsahujúca príslušnú MAC adresu.

Každá z uvedených ARP správ (*request* alebo *reply*) obsahuje nižšie uvedené polia, jej štruktúra je schematicky znázornená na obr. 1.1:

- **Typ média** (16 b): určuje typ protokolu na spojovej vrstve (napr.: 1 = Ethernet),
- **Typ protokolu** (16 b) – určuje protokol vyššej vrstvy, ktorý využíva ARP (napr. 0x0800 pre IPv4),
- **Dĺžka fyzickej adresy** (8 b) – určuje dĺžku MAC adresy v bajtoch (typicky 6 B);
- **Dĺžka logickej adresy** (8 b) – určuje dĺžku IP adresy v bajtoch (typicky 4 B);
- **Operácia** (16 b) – označuje typ správy (1 = ARP Request, 2 = ARP Reply);
- **Fyzická adresa zdroja** (48 b) – MAC adresa zariadenia, ktoré odosiela ARP správu;
- **Logická adresa zdroja** (32 b) – IP adresa zariadenia, ktoré odosiela ARP správu;
- **Hľadaná fyzická adresa** (48 b) – MAC adresa cieľového zariadenia (v prípade správy ARP Request je toto pole prázdne);
- **Hľadaná logická adresa** (32 b) – IP adresa cieľového zariadenia, pre ktoré sa zisťuje MAC adresa.

ARP správa je následne na spojovej vrstve vložená do ethernetového rámca, ktorého **EtherType pole** je nastavené na hodnotu 0x0806, čím sa indikuje, že dáta prenášané v dátovej časti rámca sú typu ARP.

¹ V prípade, kedy nie je záznam v stanovenej dobe aktualizovaný, dochádza k jeho trvalému odstráneniu z prekladovej ARP tabuľky v pamäti zariadenia.



Obrázok 1.1 Všeobecná štruktúra správy ARP protokolu a jej zapuzdrenie do ethernetového rámca.

Popis fungovania ARP protokolu, výmena správ

1. ARP Request (Žiadosť):

Zariadenie, ktoré pre svojho komunikačného partnera (iné zariadenie) potrebuje zistiť fyzickú MAC adresu pre konkrétnu IP adresu tohto zariadenia, najprv skontroluje svoju ARP tabuľku. V prípade, že požadovaný záznam nie je v ARP tabuľke obsiahnutý, vyšle žiadosť *ARP Request* vo forme broadcastu na adresu **FF:FF:FF:FF:FF:FF**, ktorú prijmu všetky zariadenia v lokálnej sieti. V žiadosti uvedie svoju IP a MAC adresu spolu s IP adresou cieľa, ktorú chce nájsť.

2. ARP Reply (Odpoveď):

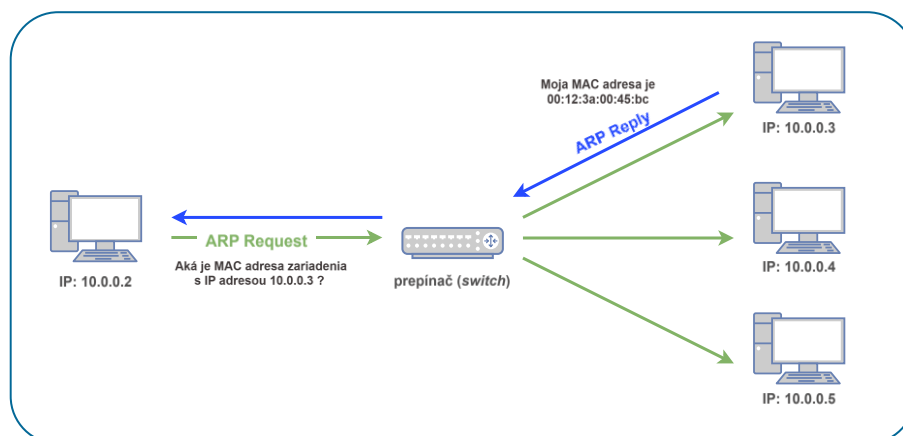
Zariadenie s požadovanou (hľadanou) IP adresou odpovedá unicastovou správou *ARP Reply* adresovanou priamo zariadeniu iniciujúcemu ARP komunikáciu, ktoré odoslalo do siete správu *ARP Request*. V tejto odpovedi odosiela informáciu o svojej MAC adrese vyplnením príslušného poľa v ARP záhlaví. Ostatné stanice v sieti prijatú správu *ARP Request* ignorujú a zahodia.

3. Vytvorenie záznamu v ARP tabuľke:

Po prijatí odpovede si žiadajúce zariadenie uloží IP a k nej odpovedajúcu hľadanú MAC adresu cieľového zariadenia do ARP tabuľky vo svojej pamäti. Ak už zariadenie pozná MAC adresu z predchádzajúcej komunikácie, použije pri ďalšej komunikácii uložený záznam bez nutnosti opakovaného odosielania obdobnej ARP žiadosti.

4. Timeout a obnova:

Záznamy v ARP tabuľke majú obmedzenú platnosť (typicky napr. 5 minút). Po uplynutí času sa z ARP tabuľky vymažú, aby sa predišlo neaktuálnym údajom pri zmene konfigurácie siete.



Obrázok 1.2 Schematické znázornenie výmeny správ ARP protokolu².

V prípade záujmu o rozšírenie poznatkov ohľadom ARP protokolu a jeho fungovania je odporúčené nahliadnuť do ďalšej literatúry, ktorú poskytujú napr. zdroje [3], [4].

1.2. Hrozby na spojenej vrstve: ARP spoofing

ARP spoofing je typ sieťového útoku používaný útočníkmi k presmerovaniu komunikácie v lokálnej sieti (LAN) prostredníctvom manipulácie s ARP protokolom (*Address Resolution Protocol*). Tento protokol sa využíva na mapovanie sieťových IP adries na fyzické adresy zariadení v rámci danej lokálnej siete. Útok *ARP spoofing* patrí do skupiny tzv. MitM útokov, kedy sa útočník dostáva do pozície prostredníka v rámci komunikácie dvoch komunikujúcich strán.

Základný princíp útoku *ARP spoofing* teda spočíva v tom, že útočník po zachytení žiadostí *ARP Request* od iných zariadení vyšle do siete podvrhnuté ARP odpovede, v ktorých uvedie falošné mapovanie požadovanej IP adresy na fyzickú adresu svojho zariadenia, vďaka čomu sa môže vydávať za očakávané zariadenie (napr. za východziu bránu zo siete alebo server). Cieľové zariadenie, ktoré pôvodnú ARP žiadosť o mapovanie odoslalo, si zapíše tento podvrhnutý zápis do svojej ARP tabuľky, a tak bude všetka ďalšia komunikácia odoslaná na zadanú IP adresu príjemcu následne presmerovaná na zariadenie útočníka. Týmto spôsobom môže útočník zachytávať a manipulovať sieťovú prevádzku.

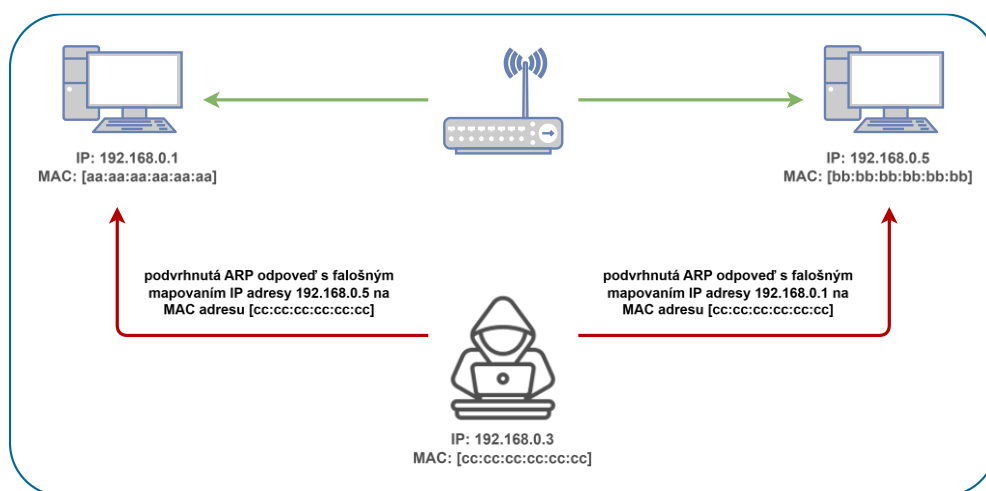
² Prevzaté z [3].

Priebeh útoku

Pri útoku *ARP spoofing* útočník najskôr identifikuje cieľové zariadenia v sieti, napríklad klienta a bránu (*gateway*). Následne začne odosielať falošné ARP odpovede, v ktorých informuje obeť (klienta), že jeho MAC adresa patrí bráne, a zároveň druhé zariadenie, t. j. bránu v podvrhnutých ARP odpovediach informuje, že jeho MAC adresa patrí klientovi. Týmto spôsobom dôjde k presmerovaniu celej sieťovej komunikácie cez útočnickovo zariadenie.

Pokiaľ sa útočníkovi podarí popísaný útok úspešne realizovať, jeho zariadenie sa dostáva do pozície MitM, kedy je cez dané zariadenie preposielaná všetka legitímna komunikácia medzi klientom a bránou, vďaka čomu môže útočník zachytávať, modifikovať alebo blokovat' sieťovú komunikáciu medzi týmito dvoma zariadeniami. V závislosti na ďalších použitých nástrojoch môže útočník ďalej napríklad sledovať prihlasovacie údaje, odpočúvať nešifrovaná dáta, presmerovať prebiehajúce dátové prenosy na iný cieľový server alebo realizovať útoky typu DoS (*Denial of Service*) s cieľom útočiť na celkovú dostupnosť siete.

Podrobný popis *ARP spoofing* útoku možno nájsť v [5], [6].



Obrázok 1.3 Schematické znázornenie priebehu *ARP spoofing* útoku.³

Ochranné opatrenia proti *ARP spoofing* útoku

Útoky typu *ARP spoofing* možno do značnej miery obmedziť, resp. zmierniť ich dopad prostredníctvom implementácie vhodných ochranných mechanizmov.

Jedným zo základných preventívnych opatrení je **statické nastavenie ARP záznamov** na dôležitých zariadeniach v sieti, čím sa zabráni ich prepísaniu v dôsledku prijatia neočakávaných ARP odpovedí s falošne priradenou dvojicou IP ↔ MAC adresa.

³ Prevzaté z [7].

Medzi doplnkové ochranné opatrenia, ktoré je možné proti *ARP spoofing* útokom nasadiť, patrí mechanizmus filtrovania MAC adries, tzv. **MAC filtering**, a to najmä v menších alebo staticky konfigurovaných sieťach. Ide o bezpečnostný mechanizmus, pri ktorom sieťové zariadenie (napr. prepínač alebo smerovač) povoľuje pripojenie len tým zariadeniam, ktorých MAC adresy sú vopred povolené v zozname. Týmto spôsobom je možné zamedziť neoprávnenému zariadeniu (napr. útočníkovi) prístup do siete, čím sa znižuje riziko manipulácie s obsahom ARP tabuliek.

V sieťovej infraštruktúre podporujúcej pokročilejšie funkcie je možné nasadiť **Dynamic ARP Inspection** (DAI) na sieťových prvkoch (typicky prepínačoch), ktorá porovnáva ARP odpovede so známymi, dôveryhodnými údajmi a v prípade nenájdenia zhody blokuje podozrivú prevádzku, resp. povolí prijatie len legitímnych odpovedí.

Ďalšou možnosťou je **segmentácia siete a použitie VLAN**, čím sa obmedzí dosah potenciálneho útočníka vďaka izolovaniu vybraných zariadení do virtuálnej siete. A taktiež je možné využiť nástroje umožňujúce detekciu podozrivej aktivity, spomedzi ktorých možno spomenúť napríklad **arpwatch**, ktoré dokážu upozorniť správcu siete na náhle zmeny MAC adries v ARP tabuľkách. Pravidelné monitorovanie a analýza sieťovej prevádzky pomocou Wiresharku tiež prispieva k rýchlej identifikácii potenciálnych nežiadúcich hrozieb.

1.3. Ďalšie hrozby na úrovni spojenej vrstvy

Útok *ARP spoofing* nie je jedinou známou hrozbou vyskytujúcou sa v počítačových sieťach na úrovni spojenej vrstvy. Existuje množstvo ďalších útokov, ktoré môžu byť vykonané na spojenej vrstve. Nižšie bude uvedených niekoľko z nich.

MAC Flooding

MAC Flooding je útok cielený najmä na sieťové prepínače (switch), ktorý spočíva v „zaplavení“ tabuľky MAC adries na prepínači veľkým množstvom falošných MAC adries. Pamäť prepínača disponuje obmedzenou kapacitou pre ukladanie informácií mapovania MAC adries na príslušné porty, a v prípade, kedy dôjde k prekročeniu dostupnej kapacity, degraduje prepínač svojou funkčnosťou na hub, čo bude mať za následok, že prepínač začne preposielať prijaté rámce ďalej do všetkých portov, čo umožní útočníkovi odpočúvať celú sieťovú komunikáciu.

Vhodnou obranou proti MAC Flooding útoku môže byť použitie a správna konfigurácia mechanizmu **Port Security** na prepínači, ktorý obmedzuje počet pripojených MAC adries na jednom porte a ďalej umožňuje stanoviť zoznam povolených MAC adries na príslušnom porte.

VLAN Hopping

VLAN Hopping je útok, ktorý umožňuje útočníkovi získať neoprávnený prístup k iným VLAN segmentom v sieti. VLAN (*Virtual Local Area Network*) je technológia

umožňujúca logické oddelenie sieťovej prevádzky celej siete v rámci jedného fyzického prepínača alebo skupiny viacerých prepínačov. Každá VLAN sieť tak predstavuje samostatný segment siete, čo prakticky znamená, že zariadenia v rôznych VLAN sa nemôžu medzi sebou priamo dorozumievať (i keď sa fyzicky nachádzajú v spoločnej lokálnej sieti) bez použitia smerovača alebo špeciálne definovaných pravidiel. Siete VLAN sa používajú najmä za účelom zvýšenia bezpečnosti, zjednodušenie managementu a správy siete a tiež pre rozdelenie celkovej prevádzky a záťaže v počítačovej sieti, vďaka čomu je možné minimalizovať riziko preťaženia, resp. nežiadúceho zahltenia siete.

Útok VLAN Hopping obchádza túto segmentáciu a umožňuje útočníkovi komunikovať s VLAN, do ktorej by nemal mať prístup. Pri útoku dochádza k zneužitiu nesprávnej konfigurácie sieťového prepínača, ktorého úlohou je prenos dát medzi VLAN. VLAN Hopping môže byť vykonaný dvoma hlavnými spôsobmi: **switch spoofing**, kedy sa útočník vydáva za dôveryhodný, legítimný prepínač a získava prístup k viacerým VLAN, a tzv. **double tagging**, pri ktorom útočník manipuluje so značkami VLAN (tzv. VLAN tag) v záhlaví ethernetových rámcov, čo bude mať za následok presmerovanie paketov do inej VLAN siete.

Za účelom zaistenia vhodnej ochrany pred VLAN Hoppingom je potrebné dbať na správne nastavenie konfigurácie sieťových prepínačov, zakázať možnosť automatického vytvárania trunkov a obmedziť VLAN *tagging* len na dôveryhodné zariadenia.

Útoky na Spanning Tree Protocol

Spanning Tree Protocol (STP) je sieťový protokol, ktorého použitie umožní zamedziť vzniku sieťových slučiek v ethernetových sieťach s redundantnými spojeniami. Nesprávna konfigurácia preposielania rámcov, v ktorej dôsledku dochádza k využívaniu záložných ciest pre komunikáciu, môže mať za následok zahltenie siete, opakované preposielanie paketov a celkovo nežiadúcim spôsobom ovplyvniť komunikáciu v danej sieti. Protokol STP umožňuje zariadeniam, resp. prepínačom aktívne identifikovať redundantné cesty v sieti a dočasne niektoré porty deaktivovať, aby bolo možné zabrániť vzniku smerovacích slučiek.

Protokol STP používa na výmenu informácií medzi sieťovými prepínačmi špeciálne správy nazývané **BPDU (Bridge Protocol Data Unit)**. BPDU správy pomáhajú určiť hierarchiu prepínačov a vybrať tzv. **root bridge**, t. j. hlavný prepínač, ktorý predstavuje referenčný bod pre výpočet najefektívnejších ciest v sieti s redundantnými spojeniami, teda pre vytvorenie kostry siete slúžiacej pre vytvorenie prenosových ciest medzi uzlami s cieľom eliminovať vznik smerovacích slučiek.

Útočník môže popísaný mechanizmus zneužiť odosielaním falošných BPDU správ s nižšou prioritou, v dôsledku čoho sa bude jeho zariadenie pre ostatné prepínače v sieti ako root bridge. Následne môže ovplyvniť konštrukciu kostry siete a docieľiť vedenie komunikácie cez svoje zariadenie, čím neoprávnene získa možnosť odpočúvať a prípadne i manipulovať s dátovým obsahom. Okrem toho môže útočník opakovane meniť

topológiu siete neustálym posielaním podvrhnutých BPDU správ, čo môže mať za následok narušenie prevádzky, celkovú nestabilitu siete, časté zmeny v prepojeniach medzi portami a nakoniec môže viesť až k fatálnym výpadkom alebo úplnému narušeniu sieťovej komunikácie.

1.4. Kali Linux a použité nástroje

V rámci tejto laboratórnej úlohy budú pre útok ARP spoofing a analýzu komunikácie postupne využité nižšie uvedené nástroje:

- **arpspoof**: jednoduchý nástroj umožňujúci posielanie falošných ARP odpovedí.
- **Ettercap**: pokročilý MitM nástroj s možnosťou ARP *spoofingu* a schopnosťou cieľenej modifikácie sieťovej komunikácie.
- **Wireshark**: sieťový analyzátor určený pre monitorovanie prebiehajúcej sieťovej komunikácie (resp. jednotlivých dátových paketov) a možnú následnú analýzu manipulovaných ARP odpovedí.
- **Arpwatch**: nástroj na monitorovanie ARP zmien a detekciu podvrhnutých MAC adries.

Nástroj arpspoof

Arpspoof je jednoduchý nástroj integrovaný v systéme Kali Linux, ktorý môže byť vhodným prostriedkom k vykonaniu útoku typu ARP spoofing. S pomocou tohto nástroja je možné doceliť presmerovanie sieťovej prevádzky (resp. komunikácie) medzi zariadeniami v sieti tým, že útočník predstiera identitu iného zariadenia (zvyčajne brány) a rozosiela falošné ARP odpovede s cieľom modifikovať záznamy obsiahnuté v ARP tabuľkách príslušných zariadení. Nástroj arpspoof môže byť využitý pre testovanie zraniteľností ARP protokolu a na analýzu prebiehajúcej komunikácie.

Nástroj arpspoof je v Kali Linux integrovaný ako súčasť balíčka `dsniff`. Jeho inštalácia do prostredia Kali Linux je možná pomocou príkazu:

```
sudo apt update && sudo apt install dsniff -y
```

Štruktúra príkazu nástroja arpspoof je nasledujúca:

```
arpspoof [-i interface] [-t target] host
```

kde pomocou prepínača **-i** špecifikujeme konkrétne rozhranie, ktoré je využité pre ARP *spoofing* (v prípade napr. ethernetu sa použije typicky rozhranie `eth0`), ďalej prepínač **-t** určuje IP adresu „obete“, t. j. cieľového zariadenia, ktorému má byť odoslaná falošná ARP odpoveď. A nakoniec parameter **host** určuje adresu zariadenia, pre ktoré chce útočník monitorovať a zachytávať prichádzajúcu sieťovú komunikáciu na danej linke (resp. pre ktoré podvrhne falošnú ARP odpoveď). [8]

Príklad použitého príkazu nástroja arpspoof pre simuláciu útoku ARP spoofing:

```
arpspoof -i eth0 -t <cieľová_IP> <IP_brány>
```

čo značí, že k realizácii útoku je použité ethernetové rozhranie **eth0**, falošné ARP odpovede sú odoslané zariadeniu s IP adresou **<cieľová_IP>** a útočník odchyťava komunikáciu prichádzajúcu na zariadenie predstavujúce východziu bránu s IP adresou **<IP_brány>** danej (lokálnej) siete.

Nástroj ettercap

Ettercap predstavuje komplexný nástroj, ktorý je taktiež súčasťou Kali Linux, vhodný pre analýzu sieťovej prevádzky a realizáciu MitM útokov, a to vrátane ARP *spoofingu*. Ponúka väčšie spektrum funkcií v porovnaní s nástrojom arpspoof a podporuje interaktívne sledovanie a manipuláciu s paketmi v reálnom čase. Môže byť použitý prostredníctvom príkazového riadku (terminál) alebo je možné pre prácu s nástrojom využiť užívateľsky prívetivé grafické rozhranie⁴. Medzi hlavné poskytované funkcie nástroja ettercap patrí:

- automatická detekcia zariadení v sieti,
- realizácia MitM útokov vrátane ARP spoofingu a DNS spoofingu a tiež možnosť manipulácie s obsahom správ HTTPS a iných protokolov,
- možnosť používania vlastných filtrov na zmenu obsahu paketov. [9]

V rámci praktickej časti laboratórnej úlohy budú postupne použité oba zmienené nástroje k simulácii útoku ARP *spoofing*. Zásadné rozdiely medzi predstavenými nástrojmi uvádza priložená tabuľka:

Tabuľka 1.1 Porovnanie nástrojov arpspoof a ettercap.

<i>Funkcia:</i>	arpspoof	ettercap
<i>Úroveň komplexnosti</i>	Jednoduchý nástroj vhodný pre simuláciu útoku ARP <i>spoofing</i> .	Komplexný nástroj poskytujúci viaceré možnosti, ako napr.: analýza sieťových parametrov, dostupnosť zariadení, ...
<i>Podpora filtrov</i>	Nie	Áno
<i>Grafické rozhranie</i>	Nie	Áno
<i>Typy útokov</i>	ARP <i>spoofing</i>	ARP <i>spoofing</i> , DNS <i>spoofing</i> , generovanie vlastných paketov, možnosť neoprávnenej manipulácie s obsahom, ...

⁴ Pre účely vypracovania úloh tohto laboratórneho cvičenia bude nástroj ettercap v Kali Linux používaný v jeho grafickom režime.

Analyzátor sieťovej komunikácie

Wireshark je jeden z najpoužívanějších nástrojov na zachytávanie a analýzu sieťových paketov. Používa sa na sledovanie prebiehajúcej dátovej komunikácie s cieľom diagnostiky problémov v sieti, odhaľovanie podozrivej aktivity a skúmanie prípadných bezpečnostných incidentov v monitorovanej sieti. Tento nástroj umožňuje používateľovi detailne sledovať sieťovú komunikáciu a analyzovať dátové jednotky jednotlivých protokolov na všetkých vrstvách ISO/OSI modelu.

Pre účely vypracovania tejto laboratórnej úlohy bude nástroj Wireshark použitý na monitorovanie komunikácie ARP protokolu, identifikáciu podvrhnutých ARP odpovedí počas útoku ARP spoofing a na overenie správnosti implementácie ochranných opatrení a ich efektivity v ochrane voči uvedenému typu útoku.

Nástroj Wireshark umožňuje nasledovné:

- **Zachytávanie sieťovej prevádzky** – Wireshark umožňuje sledovať všetku komunikáciu prebiehajúcu cez vybrané sieťové rozhranie (Ethernet, Wi-Fi, tunelované pripojenia, virtuálne adaptéry atď.).
- **Analýza paketov** – Umožňuje detailné skúmanie obsahu paketov na všetkých vrstvách OSI modelu, vrátane podrobného zobrazenia a analýzy záhlavia protokolov ako napr. ARP, TCP, UDP, ICMP, DNS či HTTP.
- **Filtrovanie paketov** – Pomocou použitia filtrov umožňuje zobrazit' len potrebné, relevantné dáta, napríklad iba zachytenú ARP komunikáciu alebo HTTP požiadavky. Filtrovanie je možné na základe protokolov, IP adries, MAC adries, portov a ďalších parametrov.
- **Rekonštrukcia sieťovej komunikácie** – Wireshark umožňuje analyzovať kompletný priebeh komunikácie medzi zariadeniami v sieti, a to vrátane jej obsahu (napr. sledovanie obsahu nezašifrovanej komunikácie protokolu HTTP, analýza požiadaviek a odpovedí).
- **Sledovanie podozrivej aktivity, detekcia útokov a bezpečnostných hrozieb** – Nástroj Wireshark je možné využiť i k odhaľovaniu podvrhnutých ARP odpovedí, MitM útokov, DoS útokov a iných bezpečnostných incidentov.
- **Exportovanie a spracovanie dát** – Zachytené dátové pakety (komunikáciu) je možné uložiť do .pcap súborov a analyzovať neskôr.

Základné príkazy Wiresharku (CLI verzia – TShark)

Nástroj Wireshark je možné využiť aj v jeho „príkazovej“ podobe **TShark**, ktorá umožňuje monitorovať a analyzovať sieťovú komunikáciu v systéme Linux z prostredia terminálu `$_`. Nižšie je uvedených niekoľko užitočných príkazov:

- Zachytávanie paketov na konkrétnom rozhraní:

```
tshark -i eth0
```

Uvedený príkaz spustí zachytávanie sieťovej prevádzky na rozhraní `eth0`.

- Použitie filtra k zobrazeniu len paketov ARP protokolu:

```
tshark -i eth0 -Y "arp"
```

- Zachytenie paketov a uloženie do súboru:

```
tshark -i eth0 -w nazov_saboru.pcap
```

- Zobrazenie iba požadovaných polí v paketoch:

```
tshark -r zachyt.pcap -T fields -e ip.src -e ip.dst
```

Uvedený príkaz zobrazí len zdrojovú **ip.src** a cieľovú **ip.dst** IP adresu zachytených paketov.

V rámci tejto laboratórnej úlohy bude využitá verzia nástroja Wireshark umožňujúca využitie všetkých jeho funkcionalít prostredníctvom grafického užívateľského rozhrania. Podrobnejší popis možností Wiresharku a ich využitia pre potreby tejto úlohy bude uvedený neskôr v praktickej časti tohto návodu.

ARPwatch

Nástroj ARPwatch sa využíva pre **sledovanie zmien a detekciu anomálií v ARP tabuľkách** na sieťových rozhraniach zariadení a sieťových prvkov a umožňuje vytvárať hlásenia (*alerts*) v prípade výskytu nežiadúcich a/alebo neočakávaných zmien. Použitie tohto nástroja je obzvlášť výhodné najmä v prostredí s veľkým počtom zariadení, kde môže byť užitočným prostriedkom pre rýchlu detekciu potenciálnych sieťových ARP *spoofing* útokov.

2. Praktická časť

V rámci praktickej časti bude **realizovaný útok typu MitM, konkrétne ARP spoofing**. Simulovaný útok bude prebiehať vo virtuálnej sieti pozostávajúcej z troch virtuálnych strojov s Kali Linux (klient, server a útočník), ktorej topológia je schematicky znázornená nižšie na obr. 2.1. Komunikácia medzi uvedenými virtuálnymi strojmi prebieha skrz virtuálny switch VMware virtual switch, ako je znázornené na uvedenom obrázku. Cieľom úspešnej realizácie ARP spoofing útoku je modifikovať sieť tak, aby všetka komunikácia medzi virtuálnymi strojmi klienta a serveru prebiehala výhradne cez zariadenie útočníka.

2.1. Topológia virtuálnej siete a nastavenie virtuálnych strojov

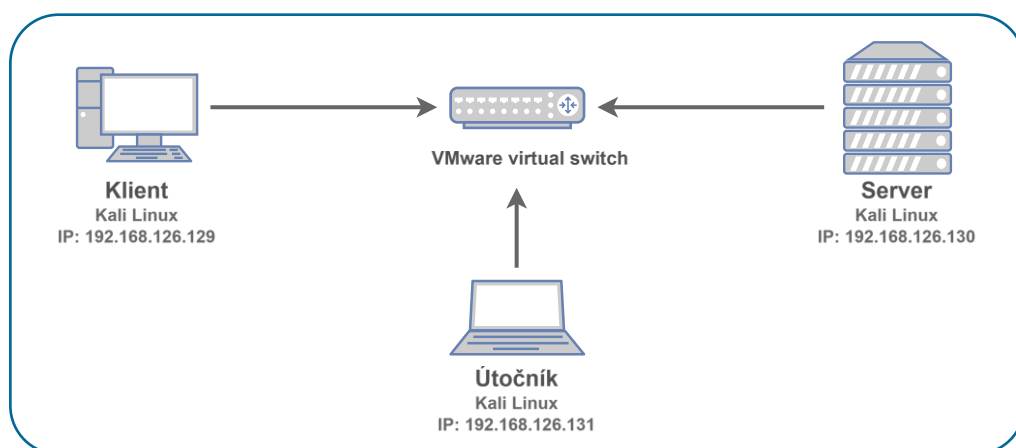
Použité virtuálne stroje:

- obeť (klient): bežný počítač v sieti, cieľ útoku
- server: poskytovateľ sieťovej služby (napr. webserver, *gateway* = brána)
- útočník: vykonáva ARP spoofing, zachytáva sieťovú komunikáciu medzi klientom a serverom

Sieťová konfigurácia:

- obeť: 192.168.126.129
- server: 192.168.126.130
- útočník: 192.168.126.131

Všetky virtuálne stroje budú pripojené do rovnakej virtuálnej siete (nastavenie sieťového adaptéra v režime napr. **Bridged** alebo **Host-Only**), aby mohlo byť na VM predstavujúcom „útočníka“ realizované zachytávanie dátových prenosov (komunikácie) medzi klientom a serverom.



Obrázok 2.1 Topológia siete laboratórnej úlohy.

2.2. Zoznámenie sa s použitými nástrojmi

Prehľad základných príkazov pre jednotlivé používané nástroje

- Zobrazenie ARP tabuľky:

```
arp -a
```

Dobrovoľné: Pred zahájením praktickej časti si vyskúšajte použitie uvedeného príkazu na zariadeniach klienta a severu. Pozorujte záznamy uvedené v ARP tabuľke na oboch zariadeniach.

- ARP spoofing pomocou nástroja arpspoof:

```
sudo arpspoof -i eth0 -t 192.168.1.10 192.168.1.1
```

- Spustenie Ettercapu cez terminál:

```
sudo ettercap -Tq -M arp:remote /192.168.1.10/ /192.168.1.1/
```

Použitie Wiresharku na analýzu ARP spoofing útoku

1. Spustenie zachytávania sieťovej prevádzky

Po spustení programu Wireshark je potrebné vybrať monitorované sieťové rozhranie, cez ktoré prebieha komunikácia (napr. eth0 pre Ethernet). Po jeho výbere kliknutím na tlačidlo **Start** spustíte zachytávania paketov.

2. Filtrovanie paketov ARP protokolu

Pre zobrazenie dátových jednotiek prislúchajúcich ku komunikácii ARP protokolu, je vhodné použiť filter pre komunikáciu: **arp**. Tento filter zobrazí len ARP žiadosti a ARP odpovede odosielané v monitorovanej sieti.

3. Identifikácia podvrhnutých ARP odpovedí

V rámci analýzy zachytenej dátovej komunikácie je nutné zamerať sa na rôzne prvky podozrivej aktivity, ktorá môže indikovať prebiehajúci ARP spoofing útok. Môže sa jednať napr. o:

- neočakávané ARP odpovede bez predchádzajúcich ARP žiadostí,
- rovnaké IP adresy priradené k rôznym fyzickým MAC adresám,
- časté opakovanie ARP odpovedí smerujúcich na jedno cieľové zariadenie (obet').

4. Ukladanie a analýza dát

Zachytené pakety zaznamenanéj ARP komunikácie je možné vo Wiresharku uložiť do samostatného .pcap súboru a analyzovať neskôr pomocou príkazu:

```
tshark -r subor.pcap | grep ARP
```

2.3. Postup pre vypracovanie laboratórnej úlohy

A) Príprava prostredia

Spustenie virtuálnych strojov:


- Otvorte VMware Workstation Pro (umiestnený na ploche).
- Spustíte postupne všetky tri virtuálne stroje (klient, server, útočník). Uistite sa v správnosti konfigurácie sieťových parametrov, overte priradenie IP adries.
- Prihláste sa do prostredia Kali Linux na VM útočníka.

VM „útočník“ – prihlasovacie údaje: **Username: kali**, **Password: kali**

VM „klient“ – prihlasovacie údaje: **Username: klient**, **Password: kali**

VM „server“ – prihlasovacie údaje: **Username: server**, **Password: kali**

Overenie sieťovej konektivity:

- Otvorte **terminál** (kliknite na ikonu terminálu  v záhlaví horného pracovného panelu alebo stlačte **Ctrl + Alt + T**).
- Na každom VM si zobrazte priradené IP adresy (na rozhraní **eth0**) pomocou príkazu:

```
ip a
```

- Z klienta vyskúšajte pripojenie na server pomocou príkazu **ping**.

```
ping <ip_adresa_servera>
```

Ak prichádza odpoveď **ping echo reply** zo strany servera, sieťová komunikácia medzi zariadeniami funguje.

- Obdobným spôsobom overte možnosť spojenia v opačnom smere komunikácie.
- Po overení funkčnosti spojenia si **zobrazte prekladové ARP tabuľky** na oboch zariadeniach pomocou príkazu:

```
arp -a
```

Spustenie Wiresharku a sledovanie ARP paketov

- Na klientovi spustíte Wireshark pomocou príkazu:

```
sudo wireshark &
```

Prepínač **'sudo'** spustí nástroj Wireshark s oprávneniami administrátora, čo je nevyhnutné pre zachytávanie sieťovej prevádzky v Kali Linux.

- V hlavnom okne vyberte sieťové rozhranie (napr. **eth0**).
- Do okna pre filtrovanie napíšte **arp** a použitie zvoleného filtra komunikácie potvrdíte stlačením **Enter**.
Použitie filtra **'arp'** zaistí, že spomedzi všetkých zachytených dátových jednotiek prenesených v rámci komunikácie cez zvolené rozhranie, budú zobrazené len správy protokolu ARP.
- Kliknite na **Start Capturing Packets**.

B) Vykonanie ARP spoofing útoku

Princípom simulácie útoku bude dosiahnuť „otravu“ ARP tabuliek na zariadení klienta a na serveri, a to v dôsledku podvrhnutia falošných ARP odpovedí zo strany útočníka, ktoré budú oznamovať skutočnosť, že server so sieťovou IP adresou **192.168.126.130** má priradenú fyzickú MAC adresu odpovedajúcu MAC adrese zariadenia útočníka [**cc: cc: cc: cc: cc: cc**] a obdobne v druhom smere komunikácie bude serveru poskytnutá informácia, že klient s IP adresou **192.168.126.129** tak isto disponuje fyzickou MAC adresou zariadenia útočníka [**cc: cc: cc: cc: cc: cc**] (viď obr. 1.3).

Podvrhnutie ARP odpovedí obom komunikujúcich zariadeniam bude mať za následok odosielanie všetkej komunikácie v smere **server → klient** a tak isto v opačnom smere **klient → server** na zariadenie útočníka. Útočník môže zachytené správy modifikovať a následne v zmenenej podobe preposlať koncovému adresátovi, čo bude mať za následok narušenie integrity komunikácie.

Použitie nástroja arpspoof

- Pred spustením samotného útoku je potrebné povoliť presmerovanie IP paketov na zariadení útočníka, aby mohol správne sprostredkovať komunikáciu medzi klientom a serverom:

```
echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
```

Použitie uvedeného príkazu zabezpečí, že útok nebude spôsobovať výpadok prebiehajúceho legitímneho spojenia medzi klientom a serverom, no zároveň bude útočník schopný komunikáciu zachytávať a preposielať – čo je *typický priebeh Man-in-the-Middle útoku*.

- Na útočnickovom stroji ďalej otvorte terminál (nové terminálové okno) a spustíte nasledujúce príkazy pre vykonanie ARP *spoofing* útoku postupne pre oba smery komunikácie. **Pre podvrhnutie ARP odpovede klientovi použijete príkaz:**

```
sudo arpspoof -i eth0 -t 192.168.126.129 192.168.126.130
```

*** do príkazu arpspoof vstupujú ako parametre jednotlivých prepínačov hodnoty na základe uvedenej topológie vytvorenej pre túto laboratórnu úlohu*

- Následne opakujte postup, ale tentokrát **pre podvrhnutie ARP odpovedí serveru:**

```
sudo arpspoof -i eth0 -t 192.168.126.130 192.168.126.129
```

Po použití uvedených příkazů budou generované falošné ARP odpovědi a následně odeslané ze stroje útočníka zařízením s uvedenými IP adresami, vďaka čomu sa útočník sa dostane do pozície prostredníka komunikácie MitM medzi klientom a serverom.

- Po zadání příkazů začne nástroj **arpspoof** opakovaně odosielať na uvedené cieľové IP adresy žiadosti ARP Request. **Je nutné nechať tento príkaz na oboch zariadeniach (klient, server) spustený po celú dobu trvania útoku!** Akékoľvek ďalšie príkazy je vhodné spustiť v samostatnom okne terminálu.
- Zadanie postupne oboch **arpspoof** príkazů zaručí, že je útok ARP *spoofing* kompletný. Všetka komunikácia prebiehajúca v smere *klient* → *server* a tiež *server* → *klient* bude od tohto momentu prechádzať cez zariadenie útočníka.

Presmerovanie komunikácie – overenie útoku

- Po spustení **arpspoof** z klienta na server aj zo servera na zariadenie klienta je možné overiť úspešnosť útoku jednoduchým príkazom **ping**. Na klientovi spustíte:

```
ping 192.168.126.130
```

- Na zariadení útočníka sledujte, či sa generované pakety protokolu ICMP objavujú v zachytenej komunikácii vo Wiresharku. Alternatívne je možné overiť úspešnosť útoku aj prostredníctvom nástroja **tcpdump**, a to nasledovným príkazom:

```
sudo tcpdump -i eth0 icmp
```

Uvedený príkaz zobrazuje **všetky ICMP pakety** (napr. *ping*), ktoré prechádzajú cez rozhranie **eth0**. Ak útok prebieha správne a je zapnuté IP forwarding, na zariadení útočníka budú zachytené odeslané správy ICMP echo a príslušné a odpovede (*reply*) medzi klientom a serverom.

Overenie zmien v ARP tabuľke klienta

- Na zariadení klienta si zobrazte ARP tabuľku zadáním príkazu do nového terminálového okna a pozorujte zmeny porovnaním obsahu tabuľky pred vykonaním útoku:

```
arp -a
```

Ak je útok ARP *spoofing* úspešný, MAC adresa prislúchajúca k IP adrese serveru bude v prekladovej ARP tabuľke zmenená na MAC adresu zariadenia útočníka.

- Obdobne postupujte i pri kontrole ARP tabuľky na serveri.

```
(klient@kali-klient)-[~]
$ arp -a
? (192.168.142.2) at 00:50:56:f0:7a:e5 [ether] on eth0
? (192.168.142.254) at 00:50:56:ec:e3:69 [ether] on eth0
? (192.168.142.130) at 00:0c:29:80:63:d6 [ether] on eth0
? (192.168.142.128) at 00:0c:29:b6:d3:cc [ether] on eth0

(klient@kali-klient)-[~]
$ arp -a
? (192.168.142.2) at 00:50:56:f0:7a:e5 [ether] on eth0
? (192.168.142.254) at 00:50:56:ec:e3:69 [ether] on eth0
? (192.168.142.130) at 00:0c:29:b6:d3:cc [ether] on eth0
? (192.168.142.128) at 00:0c:29:b6:d3:cc [ether] on eth0
```

Obrázok 2.2 Zmeny v ARP tabuľke klienta.

Overenie detekcie útoku pomocou nástroja arpwatch

- Po úspešnom spustení útoku ARP *spoofing* môžete overiť detekciu zmien v ARP tabuľke aj pomocou nástroja arpwatch.
- Na jednom z napadnutých strojov (klient/server) otvorte terminálové okno a nainštalujte arpwatch pomocou príkazov:

```
sudo apt update
sudo apt install arpwatch -y
```

- Spustíte arpwatch na sieťovom rozhraní, ktorým je napadnuté zariadenie pripojené do siete, v ktorej prebieha útok:

```
sudo arpwatch -i eth0
```

- Počas toho, kým prebieha simulovaný útok pomocou arpspoof, sledujte výstup arpwatch v termináli alebo kontrolujte logovací súbor:

```
sudo tail -f /var/log/syslog
```

alebo:

```
sudo cat /var/lib/arpwatch/arp.dat
```

- Všímajte si správy, ako napríklad:

```
changed ethernet address for 192.168.126.130
ethernet address 00:0c:29:b6:d3:cc found at 192.168.126.130
```

alebo:

arpwatch: ethernet address for **192.168.126.130** changed from **00:0c:29:d6:30:5b** to **00:0c:29:b6:d3:cc**

Zobrazené správy (a zmeny v ARP tabuľke klienta) indikujú, že uvedená IP adresa (server) bola spárovaná s novou MAC adresou (útočníka) – čo je typický dôsledok ARP spoofingu útoku.

Zachytávanie a analýza dát vo Wiresharku

V rámci tejto laboratórnej úlohy bude nástroj Wireshark využitý primárne za účelom **monitorovania prebiehajúcej ARP komunikácie** vo vytvorenej virtuálnej sieti a k následnej analýze zachytených správ (žiadostí a odpovedí) ARP protokolu.

- Vráťte sa do Wiresharku.
- Pozorujte podvrhnuté ARP odpovede a analyzujte ich obsah.

Kliknutím na paket zobrazíte jeho detaily. Skontrolujte, **ako sa zmenili riadiace informácie v záhlaví ARP protokolu** po vykonaní ARP *spoofing* útoku (zdrojová a cieľová MAC adresa by mali byť zmenené na útočnickovu).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	VMware_b6:d3:cc	VMware_80:63:d6	ARP	60	192.168.142.129 is at 00:0c:29:b6:d3:cc
2	0.000448276	VMware_10:dd:3a	Broadcast	ARP	42	ARP Announcement for 192.168.142.129 (du
3	0.108476963	VMware_b6:d3:cc	VMware_10:dd:3a	ARP	60	192.168.142.130 is at 00:0c:29:b6:d3:cc
4	2.001248686	VMware_b6:d3:cc	VMware_80:63:d6	ARP	60	192.168.142.129 is at 00:0c:29:b6:d3:cc
5	2.111381306	VMware_b6:d3:cc	VMware_10:dd:3a	ARP	60	192.168.142.130 is at 00:0c:29:b6:d3:cc
6	4.003394116	VMware_b6:d3:cc	VMware_80:63:d6	ARP	60	192.168.142.129 is at 00:0c:29:b6:d3:cc
7	4.113794142	VMware_b6:d3:cc	VMware_10:dd:3a	ARP	60	192.168.142.130 is at 00:0c:29:b6:d3:cc
8	6.005818128	VMware_b6:d3:cc	VMware_80:63:d6	ARP	60	192.168.142.129 is at 00:0c:29:b6:d3:cc
9	6.116295402	VMware_b6:d3:cc	VMware_10:dd:3a	ARP	60	192.168.142.130 is at 00:0c:29:b6:d3:cc
10	8.008090986	VMware_b6:d3:cc	VMware_80:63:d6	ARP	60	192.168.142.129 is at 00:0c:29:b6:d3:cc
11	8.118940653	VMware_b6:d3:cc	VMware_10:dd:3a	ARP	60	192.168.142.130 is at 00:0c:29:b6:d3:cc
12	10.009960213	VMware_b6:d3:cc	VMware_80:63:d6	ARP	60	192.168.142.129 is at 00:0c:29:b6:d3:cc
13	10.010518955	VMware_10:dd:3a	Broadcast	ARP	42	ARP Announcement for 192.168.142.129 (du
14	10.122068398	VMware_b6:d3:cc	VMware_10:dd:3a	ARP	60	192.168.142.130 is at 00:0c:29:b6:d3:cc
15	12.012443986	VMware_b6:d3:cc	VMware_80:63:d6	ARP	60	192.168.142.129 is at 00:0c:29:b6:d3:cc
16	12.123850907	VMware_b6:d3:cc	VMware_10:dd:3a	ARP	60	192.168.142.130 is at 00:0c:29:b6:d3:cc
17	14.014704906	VMware_b6:d3:cc	VMware_80:63:d6	ARP	60	192.168.142.129 is at 00:0c:29:b6:d3:cc
18	14.126084138	VMware_b6:d3:cc	VMware_10:dd:3a	ARP	60	192.168.142.130 is at 00:0c:29:b6:d3:cc

Frame 3: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on
Ethernet II, Src: VMware_b6:d3:cc (00:0c:29:b6:d3:cc), Dst: VMware_10:dd:3a (00:0c:29:10:dd:3a), Address Resolution Protocol (reply)
[Duplicate IP address detected for 192.168.142.130 (00:0c:29:b6:d3:cc)]
[Duplicate IP address detected for 192.168.142.129 (00:0c:29:10:dd:3a)]

Obrázok 2.3 Ukážka zachytenej komunikácie (Wireshark)

ARP spoofing pomocou nástroja Ettercap

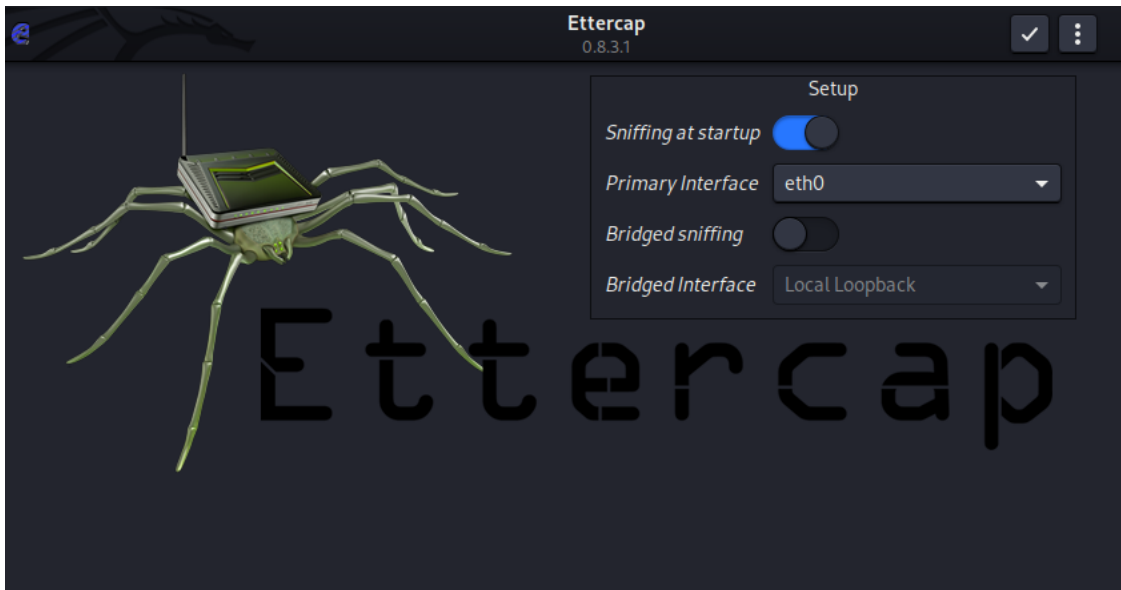
- Na stroji útočníka spustíte Ettercap cez terminál:

```
sudo ettercap -G
```

- Ako primárne sieťové rozhranie vyberte eth0.

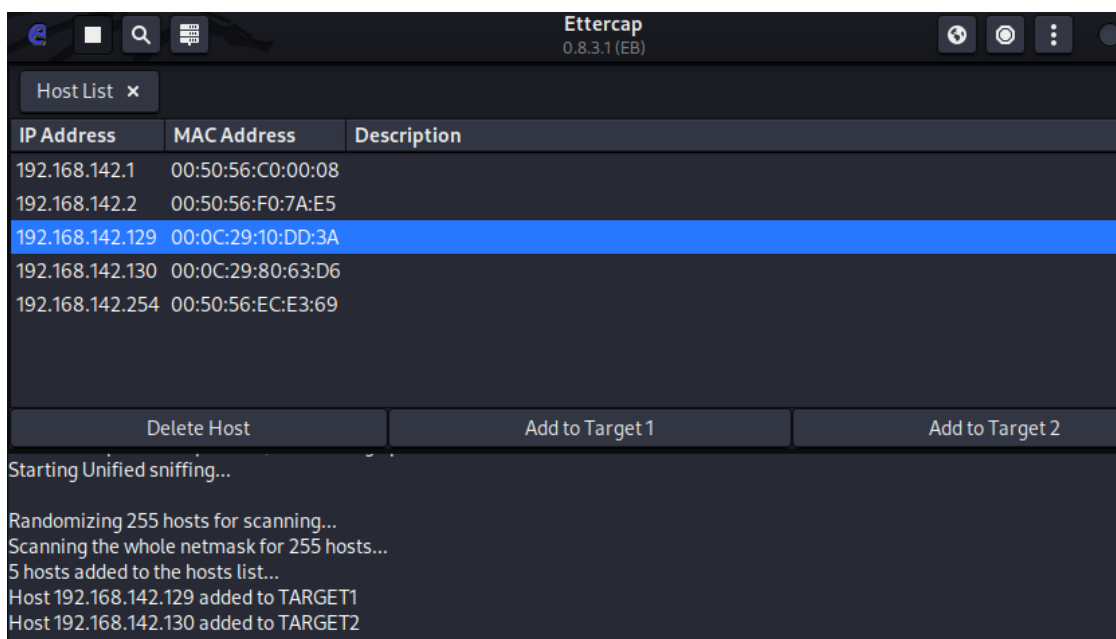
- Po spustení ponechajte všetky nastavenia bez zmeny (viď obr. 2.4) a pokračujte kliknutím na ☒ v záhlaví zobrazeného okna.

Kliknutím na **Options** (tri bodky v záhlaví) sa uistite, že je zaškrtnutá voľba **Promisc mode**, čo v priebehu simulácie zabezpečí, že zariadenie útočníka bude pracovať v promiskuitnom režime, vďaka čomu bude možné odchyťovať všetku komunikáciu na lokálnej linke prechádzajúcu cez zvolené rozhranie.



Obrázok 2.4 Nástroj Ettercap: úvodné grafické rozhranie.

- Pred výberom cieľových zariadení je potrebné vykonať *sken* siete. Kliknite na „tri bodky“ v záhlaví, ďalej zvolíte **Hosts > Scan for hosts**, čím naplníte zoznam dostupných zariadení v sieti.
- Po dokončení skenovania si zoznam zariadení zobrazíte cez **Hosts > Hosts List** (viď obr. 2.5).
- Z tohto zoznamu vyberte cieľové zariadenia *ARP spoofing* útoku a pridajte ich postupne do **Target 1** (klient) a **Target 2** (server).
- Ďalej pokračujte kliknutím na MitM Menu (ikona zemegule) záhlaví grafického rozhrania, z ponuky vyberte na **MitM > ARP Poisoning**, zaškrtnite **Sniff remote connections** a túto voľbu potvrdíte pomocou **OK**, čím zahájite útok.



Obrázok 2.5 Nástroj Ettercap: výpis nájdených zariadení v sieti.

Overenie úspešnosti MitM útoku pomocou Ettercap

- Po spustení útoku v prostredí nástroja Ettercap v režime MitM, môžete jeho úspešnosť overiť obdobne ako v prípade prvého útoku: pomocou aplikácie **ping** (resp. odoslaním ICMP *echo request* správy z klienta na server):

```
ping 192.168.126.130
```

Ak odosielané správy ICMP protokolu prechádzajú cez zariadenie útočníka (resp. ak sú tieto pakety viditeľné v zachytenej komunikácii vo Wiresharku alebo ak program Ettercap zobrazí záznam o komunikácii medzi týmito IP adresami), znamená to, že ARP *spoofing* útok prebehol z pohľadu úspešne a komunikácia bola presmerovaná.

2.4. Samostatná úloha

C) Implementácia ochranných opatrení

V poslednej časti laboratórnej úlohy si prakticky vyskúšate možnosti ochrany proti útoku ARP *spoofing*.

Cieľom vašej samostatnej práce bude implementovať statické ARP záznamy, ktoré predstavujú jeden z možných druhov ochranných opatrení proti zmienenému typu útokov, a následné otestovanie účinnosť tejto ochrany.

Konfigurácia statických ARP záznamov

- Na klientovi a serveri zadefinujte statické ARP záznamy:

```
sudo arp -s 192.168.1.1 00:11:22:33:44:55  
sudo arp -s 192.168.1.20 AA:BB:CC:DD:EE:FF
```

*** **Poznámka:** ako fyzické MAC adresy a sieťové IP adresy voľte **konkrétne adresy** vami používaných VMs.*

- Overte uloženie vami zadaných statických záznamov zobrazením ARP tabuľky na oboch zariadeniach výpisom aktuálneho obsahu ARP tabuľky.

Testovanie účinnosti ochrany

- Opakujte útok pomocou nástroja `arpspoof` podľa predošlého postupu a overte, či nedochádza ku zmene MAC adres v ARP tabuľke.
- V prípade nemennosti informácií v záznamoch v ARP tabuľke na oboch VMs (klient, sever) je implementovaná ochrana voči podvrhnutiu falošných MAC adres vďaka nastaveniu statických záznamov v ARP tabuľke účinná.

3. Záver

V tejto laboratórnej úlohe ste sa zoznámili s problematikou bezpečnosti spojovej vrstvy počítačových sietí. Prakticky ste overili **priebeh útoku ARP spoofing**, v rámci ktorého útočník podvrhnutím falošných ARP odpovedí docieli uvedenie nesprávnych informácií o fyzických MAC adresách v prekladových ARP tabuľkách komunikujúcich zariadení, čo môže mať za následok presmerovanie komunikácie práve skrz zariadenie útočníka.

Účinnou ochranou proti útokom založených na „otrave“ prekladovej ARP tabuľky je **konfigurácia statických záznamov** pre mapovanie medzi sieťovými a fyzickými adresami, ktorá zamedzí získavaniu informácií o MAC adresách s využívaním ARP protokolu medzi zariadeniami v sieti, a tým aj nežiaducim zneužitím ARP odpovedí k podvrhnutiu falošnej fyzickej (MAC) adresy.

3.1. Kontrolné otázky

1. Akú funkciu plní ARP protokol v rámci sieťovej komunikácie?
 - A) Zabezpečuje preklad fyzickej adresy na logickú v lokálnej sieti
 - B) Priradzuje porty k IP adresám
 - C) Zisťuje fyzickú adresu zariadenia na základe jeho známej IP adresy
 - D) Poskytuje kryptografickú ochranu komunikácie medzi dvoma zariadeniami
2. Ktoré z nasledujúcich tvrdení správne popisujú útok typu ARP spoofing?
 - A) Útočník odosiela do siete falošné ARP odpovede, aby dosiahol zmenu IP adresy v ARP tabuľke zariadenia
 - B) Jedná sa o typ útoku, pri ktorom útočník podvrhne svoju MAC adresu namiesto skutočnej MAC adresy zariadenia s hľadanou IP adresou v odpovedi na ARP žiadosť iného zariadenia
 - C) Cieľom útoku je presmerovať sieťovú komunikáciu cez zariadenie útočníka
 - D) ARP spoofing sa využíva primárne za účelom narušenia dostupnosti cieľovej služby
3. Aký je rozdiel medzi dynamickým a statickým ARP záznamom?
 - A) Dynamický záznam je uložený trvalo, statický len dočasne
 - B) Statický je uložený manuálne, dynamický sa generuje automaticky
 - C) Dynamický záznam sa nikdy neaktualizuje podľa aktuálnej situácie v sieti
 - D) Dynamický je bezpečnejší ako statický
4. Prečo je pri MitM útoku dôležité zapnúť IP forwarding?
 - A) Aby bolo možné odosielať pakety cez zabezpečené HTTPS spojenie
 - B) Pretože umožní odosielanie a prijímanie ICMP správ
 - C) Aby útočník mohol presmerovať sieťovú komunikáciu cez svoje zariadenie
 - D) Umožňuje zakázať použitie MAC filtering mechanizmu

5. Ktorý z nasledujúcich nástrojov slúži primárne na analýzu sieťovej komunikácie?
- A) arpspoof
 - B) Ettercap
 - C) Wireshark
 - D) arping
6. Ktoré z nasledujúcich javov môžu naznačovať prebiehajúci ARP *spoofing* v sieti?
- A) Znížená latencia a zvýšená prenosová rýchlosť v sieti
 - B) Výskyt ARP odpovedí, ktoré priradujú rovnakú MAC adresu k viacerým IP adresám
 - C) Výskyt "duplicate IP" varovaní v systéme
 - D) Výskyt viacerých ARP odpovedí bez predchádzajúcich požiadaviek
7. Ktoré tvrdenia vystihujú rozdiely medzi nástrojmi arpspoof a Ettercap?
- A) Ettercap dokáže analyzovať a upravovať dáta vyšších vrstiev (napr. HTTP)
 - B) arpspoof je jednoduchý CLI nástroj bez možnosti manipulácie so samotnými dátami
 - C) Ettercap neumožňuje vizualizáciu MitM útokov cez GUI rozhranie
 - D) arpspoof automaticky obnovuje ARP tabuľky po útoku
8. K čomu slúži nástroj arpspoof počas útoku typu MitM?
- A) Odosiela falošné ARP odpovede, aby sa útočník dostal do pozície medzi dvoma zariadeniami (MitM)
 - B) Skenuje sieť pre zistenie aktívnych služieb
 - C) Skenuje sieť pre zistenie pripojených koncových zariadení
 - D) Blokuje komunikáciu medzi routerom a klientom
9. Ktoré z nasledujúcich opatrení môžu pomôcť chrániť sieť pred ARP *spoofingom*?
- A) Použitie šifrovania TLS
 - B) Konfigurácia statických ARP záznamov
 - C) Nasadenie *Dynamic ARP Inspection* (DAI)
 - D) Použitie VLAN segmentácie
10. Aký filter vo Wiresharku použijete na zobrazenie len ARP paketov (požiadaviek aj odpovedí)?
- A) arp
 - B) ip.arp == 1
 - C) eth.type == 0x0806
 - D) arp.request

4. Literatúra

- [1] *ARP (Address Resolution Protocol)*. *SecuriaPro.sk* [online]. Dostupné z: <https://www.secu-riapro.sk/slovník-pojmov/arp/> [cit. 2024-11-23].
- [2] Noite.pl. *ARP Protocol – Address Resolution Protocol*. In: *Network Basic. AL0- 012* [online]. 2016. s. 118–130. Dostupné z: <https://books.google.sk/books?id=wcFxCwAAQBAJ> [cit. 2024-11-23].
- [3] *What Is Address Resolution Protocol (ARP)?* *fortinet.com* [online]. Dostupné z: <https://www.fortinet.com/resources/cyberglossary/what-is-arp> [cit. 2024-11-23].
- [4] ATKINSON, RJ. *Address Resolution Protocol (ARP) for the Identifier-Locator Network Protocol for IPv4 (ILNPv4)*. In: *Internet Requests for Comments*. [online]. RFC Editor, 2012. Dostupné z: <https://datatracker.ietf.org/doc/html/rfc6747> [cit. 2024-11-23].
- [5] WAGNER, R. *Address Resolution Protocol Spoofing and Man in the Middle Attacks*. SANS Institute. 2001. [online]. Dostupné z: <https://www.sans.org/reading-room/whitepapers/threats/address-resolution-protocol-spoofing-man-in-the-middle-attacks-474> [cit. 2024-11-23].
- [6] Al Sukkar, G. Saifan, R. Khwaldeh, S. Maqableh, M. et Jafar, I. *Address Resolution Protocol (ARP): Spoofing Attack and Proposed Defense*. In: *Communications and Network*. 2016. s. 118–130. [online]. Dostupné z: <http://hdl.handle.net/123456789/856> [cit. 2024-11-23].
- [7] MORSY, Sabah M. and NASHAT, Dalia. *D-ARP: An Efficient Scheme to Detect and Prevent ARP Spoofing*. In: *IEEE Access*. 2022. s. 49142–49153. [online]. Dostupné z: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9766351> [cit. 2024-11-23].
- [8] *arp spoof(8) – Linux man page*. In: *Linux Documentation*. [online]. Dostupné z: <https://linux.die.net/man/8/arp spoof> [cit. 2024-11-26].
- [9] Ettercap project. [online]. Dostupné z: <https://www.ettercap-project.org/> [cit. 2024-11-26].