

Text laboratorní úlohy

Laboratorní úloha č. 3

BEZPEČNOST LINKOVÉ VRSTVY

Úvod k laboratorní úloze

Cílem této laboratorní úlohy je analyzovat zranitelnosti na úrovni linkové vrstvy referenčního modelu ISO/OSI a demonstrovat možná rizika a útoky.

V první části úkolu provedete s využitím vhodných nástrojů ve virtuálním stroji Kali Linux **simulaci síťového útoku ARP spoofing**. Během tohoto útoku se pokusíte podvrhnout falešné záznamy do ARP tabulky klienta, přesměrovat síťovou komunikaci přes zařízení útočníka a analyzovat její obsah. Kromě samotné realizace útoku, při které si osvojíte práci s nástroji **arp spoof** a **Ettercap**, se zároveň naučíte analyzovat a vhodně interpretovat zachycená síťová data v prostředí **síťového analyzátoru Wireshark**. Následně implementujete ochranná opatření (statické ARP záznamy, monitorování ARP záznamů) a otestujete jejich účinnost.

Požadavky pro vypracování úkolu:

- software: VMware Workstation Player pro virtualizaci stanic,
- virtuální stroje: tři virtuální stroje s Kali Linux.

1. Teoretický úvod

V rámci tohoto laboratorního úkolu se seznámíte s **protokolem ARP**, který slouží k překladu logických adres zařízení na adresy fyzické. Následující část je zaměřena na problematiku bezpečnostních hrozeb na úrovni linkové vrstvy referenčního modelu ISO/OSI. Bude vysvětlen **princip útoku ARP spoofing**, který si rovněž prakticky vyzkoušíte.

1.1. ARP protokol

ARP protokol (z angl. *Address Resolution Protocol*) je protokol pracující na úrovni linkové vrstvy referenčního modelu ISO/OSI, který zajišťuje mapování (tzv. překlad) logické IP adresy zařízení na jeho fyzickou adresu (obvykle MAC adresu). Protokol ARP tedy slouží zařízením k vyhledání odpovídající adresy druhé vrstvy (tj. fyzické adresy) jiného zařízení na základě jeho síťové IP adresy (tj. adresy třetí úrovně). [1], [2]

Když zařízení potřebuje odeslat IP paket jinému uzlu ve stejné lokální síti, nejprve prostřednictvím ARP požadavku zjistí, jaká MAC adresa odpovídá požadované IP adrese. Po získání odpovědi odešle odesílatel ethernetový rámec s příslušnou cílovou MAC adresou, kterou mu zařízení sdělilo v odpovědi na ARP požadavek, a přenesení ho na úrovni linkové vrstvy.

Protokol ARP má několik známých nedostatků, které jej činí zranitelným vůči různým typům síťových útoků. Mezi nejvýznamnější zranitelnosti ARP protokolu patří:

- **Chybějící autentizace:** Protokol ARP nemá implementovaný žádný autentizační mechanismus. To znamená, že jakékoliv zařízení v síti může zasílat ARP odpovědi bez ověření identity. Tento nedostatek umožňuje útočníkovi podvrhnout falešnou MAC adresu pro určitou IP adresu a tím „otrávit“ překladovou ARP tabulku zařízení, které odesílá požadavek *ARP Request* (útok typu *ARP Cache Poisoning*).
- **Dynamická ARP tabulka:** ARP tabulka je dynamická – zařízení do ní automaticky zapisují nové záznamy na základě přijatých ARP odpovědí. Útočník může tohoto mechanismu zneužít tím, že zařízení poskytne nepravdivé informace a přepíše původní záznamy s fyzickými adresami v ARP tabulce.
- **ARP odpovědi bez vyžádání:** Zařízení v síti mohou přijímat a ukládat ARP odpovědi i v případě, že si je samy nevyžádaly (tj. neodeslaly žádný ARP požadavek). Útočník může této vlastnosti využít k šíření falešných ARP odpovědí (tzv. *gratuitous ARP replies*), což mu umožňuje ovlivnit obsah ARP tabulek u zařízení a manipulovat se sítíovou komunikací.
- **Zranitelnost vůči Man-in-the-Middle útokům:** Kvůli absenci jakéhokoliv zabezpečení mohou útočníci přesměrovat datovou komunikaci mezi zařízeními přes své vlastní zařízení, aniž by to oběť zaznamenala. Tím získávají možnost komunikaci odposlouchávat, upravovat pakety nebo dokonce realizovat útoky typu *Denial-of-Service* (DoS) za účelem odepření služby.
- **Neexistence vestavěné ochrany:** Jelikož protokol ARP funguje na linkové vrstvě OSI modelu, sám o sobě neobsahuje mechanismy pro ověřování autenticity přijatých ARP odpovědí. To otevírá prostor pro útoky související s podvržením falešných informací a „otravou“ ARP tabulek (viz výše). Z tohoto důvodu je nutné implementovat dodatečná ochranná opatření, jako jsou například: konfigurace statických ARP záznamů, nasazení nástrojů pro ARP monitoring (např. Arpwatch) nebo definování pravidel na firewallu, které omezí přijímání neoprávněných ARP odpovědí.

ARP tabulka

Každé zařízení v síti si ve své paměti udržuje aktivní tabulku obsahující záznamy o dvojicích odpovídajících si logických IP adres a fyzických (MAC) adres – tzv. ARP tabulku (také nazývanou *ARP cache*). Záznamy v ARP tabulce mají obvykle krátkou životnost (např. 5 minut) a v definovaných intervalech se pravidelně aktualizují¹. Záznamy o dvojicích IP adres a příslušných fyzických adresách jednotlivých zařízení

¹ Pokud záznam v ARP tabulce není v daném časovém intervalu aktualizován, dochází k jeho trvalému odstranění z překladové ARP tabulky v paměti zařízení.

v dané síti se do ARP tabulky ukládají buď automaticky na základě činnosti samotného ARP protokolu, nebo je možné potřebné informace do tabulky zadat ručně.

Struktura ARP zpráv

ARP zprávy jsou přenášeny na linkové vrstvě modelu ISO/OSI, tzn. nevyužívají žádný protokol vyšší vrstvy (IP nebo TCP) a jsou přímo zapouzdřeny do ethernetového rámce. Protokol ARP funguje nezávisle na vyšších vrstvách, a právě díky tomu mohou být ARP zprávy odesílány i v situaci, kdy zatím neznáme MAC adresu cílového zařízení – protože úvodní zpráva ARP Request, jak bude popsáno dále, je vysílána na všesměrovou (*broadcastovou*) MAC adresu v příslušné lokální síti.

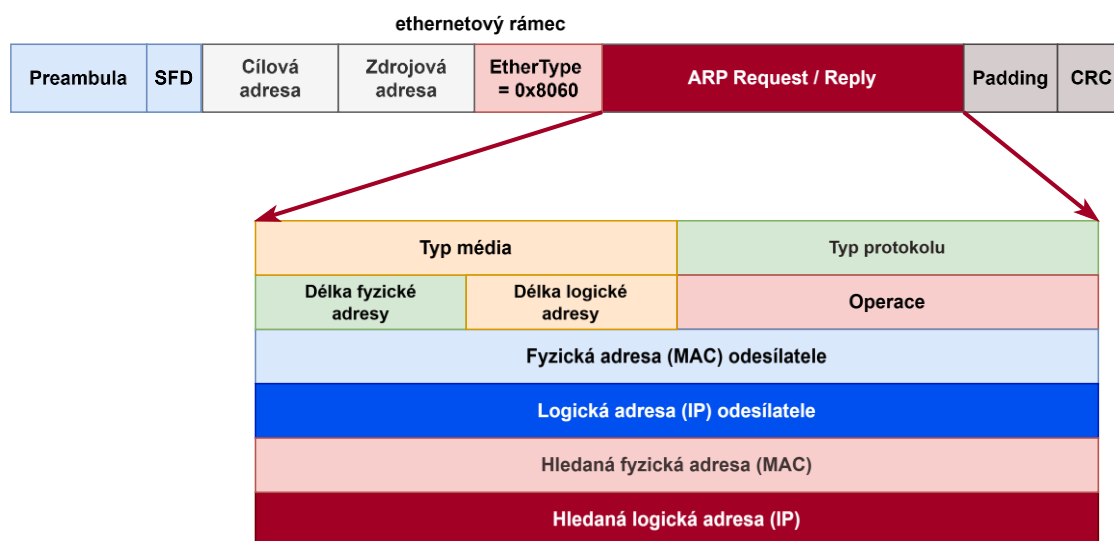
Protokol ARP definuje dva základní typy zpráv:

- **ARP Request (požadavek)** – vysílá se do sítě ve chvíli, kdy zařízení potřebuje zjistit MAC adresu příjemce pro známou IP adresu;
- **ARP Reply (odpověď)** – odpověď obsahující požadovanou MAC adresu.

Každá z těchto ARP zpráv (*request* nebo *reply*) obsahuje následující pole. Jejich struktura je schematicky znázorněna na obr. 1.1:

- **Typ média** (16 b): určuje typ protokolu na linkové vrstvě (např.: 1 = Ethernet),
- **Typ protokolu** (16 b) – definuje protokol vyšší vrstvy, který využívá ARP (např. 0x0800 pro IPv4),
- **Délka fyzické adresy** (8 b) – určuje délku MAC adresy v bajtech (typicky 6 B);
- **Délka logické adresy** (8 b) – určuje délku IP adresy v bajtech (typicky 4 B);
- **Operace** (16 b) – označuje typ správy (1 = ARP Request, 2 = ARP Reply);
- **Fyzická adresa odesílatele** (48 b) – MAC adresa zařízení, které ARP zprávu odesílá;
- **Logická adresa odesílatele** (32 b) – IP adresa zařízení, které odesílá ARP správu;
- **Hledaná fyzická adresa** (48 b) – MAC adresa cílového zařízení (v případě správy ARP Request je toto pole prázdné);
- **Hledaná logická adresa** (32 b) – IP adresa cílového zařízení, pro které se má MAC adresa zjistit.

Zpráva ARP je následně na linkové vrstvě vložena do ethernetového rámce, přičemž pole **EtherType pole** je nastaveno na hodnotu **0x0806** – tím se identifikuje, že datová část rámce obsahuje ARP zprávu.



Obrázek 1.1 Obecná struktura zprávy ARP protokolu a její zapouzdření do ethernetového rámce.

Popis fungování ARP protokolu, výměna zpráv

1. ARP Request (Požadavek):

Zařízení, které potřebuje zjistit fyzickou MAC adresu jiného zařízení pro známou IP adresu tohoto cílového zařízení, nejprve zkontroluje svou ARP tabulku. Pokud požadovaný záznam v tabulce nenajde, vyšle *ARP Request* zprávu formou broadcastu na adresu **FF: FF: FF: FF: FF: FF**, kterou obdrží všechna zařízení v lokální síti. V žádosti uvede svou vlastní IP a MAC adresu spolu s cílovou IP adresou, kterou se snaží zjistit.

2. ARP Reply (Odpověď):

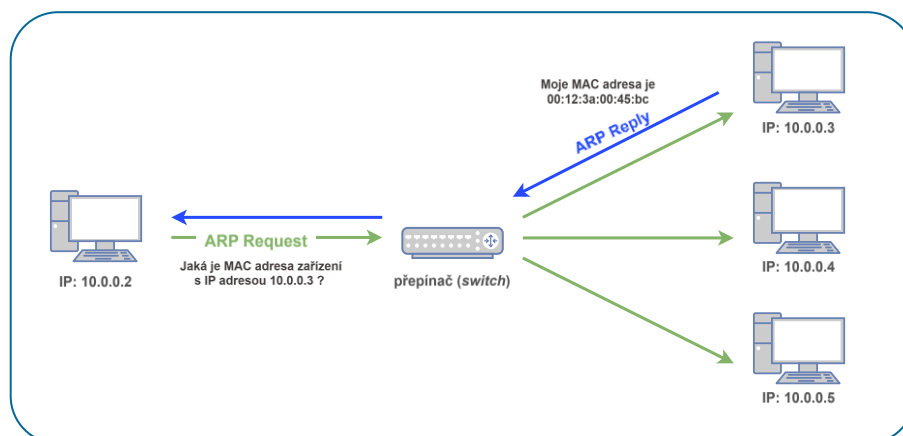
Zařízení, jehož IP adresa odpovídá požadované (hledané), reaguje unicastovou *ARP Reply* zprávou adresovanou přímo zařízení, které ARP komunikaci iniciovalo a vyslalo do sítě *ARP Request*. V této odpovědi odešle informaci o své MAC adrese prostřednictvím příslušného pole v ARP hlavičce. Ostatní stanice v síti přijatou *ARP Request* zprávu ignorují a zahazují.

3. Vytvoření záznamu v ARP tabulce:

Po přijetí odpovědi si žádající zařízení uloží IP adresu spolu s odpovídající MAC adresou cílového zařízení do své ARP tabulky v paměti. Pokud zařízení zná MAC adresu z předchozí komunikace, při dalším kontaktu využije uložený záznam bez nutnosti znovu odesílat ARP žádost.

4. Timeout a obnova:

Záznamy v ARP tabulce mají omezenou platnost (typicky např. 5 minut). Po uplynutí této doby jsou z ARP tabulky odstraněny, aby se předešlo použití neaktuálních údajů při změnách konfigurace sítě.



Obrázek 1.2 Schematické znázornění výměny zpráv ARP protokolu².

V případě zájmu o rozšíření znalostí týkajících se fungování ARP protokolu doporučujeme nahlédnout do literatury uvedené např. ve zdrojích [3], [4].

1.2. Hrozby na linkové vrstvě: ARP spoofing

ARP spoofing je typ síťového útoku využíváný útočníky k přesměrování komunikace v rámci lokální sítě (LAN) prostřednictvím manipulace s ARP protokolem (*Address Resolution Protocol*). Tento protokol slouží k mapování IP adres na fyzické adresy zařízení v rámci dané sítě. Útok *ARP spoofing* patří do skupiny tzv. MitM útoků, při kterých se útočník staví do role prostředníka mezi dvěma komunikujícími stranami.

Základní princip *ARP spoofingu* spočívá v tom, že útočník po zachycení *ARP Request* žádosti od jiných zařízení rozesílá do sítě podvržené ARP odpovědi. V těchto odpovědích uvádí falešné mapování požadované IP adresy na MAC adresu svého zařízení, čímž se vydává za důvěryhodný uzel (například za výchozí bránu nebo server). Cílové zařízení, které původní ARP žádost o mapování odeslalo, si následně tento podvržený údaj uloží do své ARP tabulky – a veškerá další komunikace směřující na danou IP adresu je pak ve skutečnosti přesměrována na zařízení útočníka. Tímto způsobem může útočník komunikaci a zachytávat a manipulovat síťový provoz.

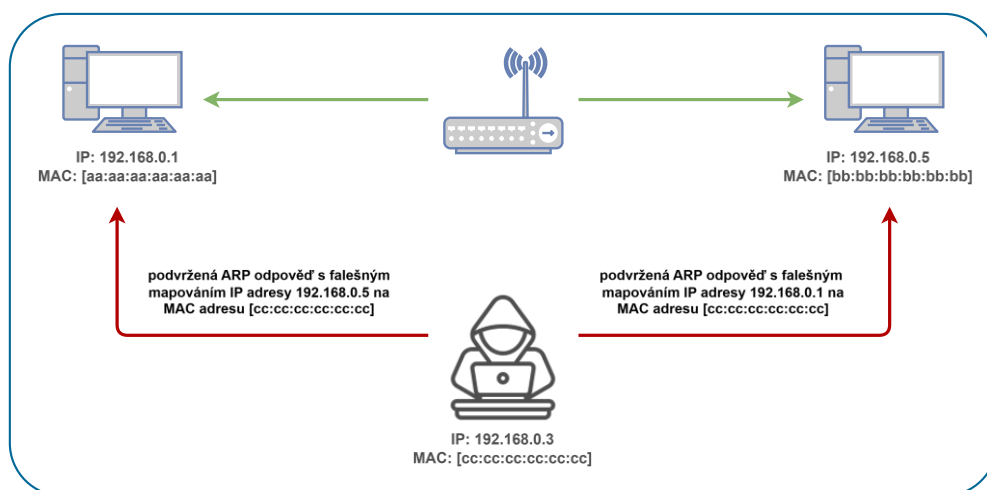
² Převzato z [3].

Průběh útoku

Při útoku *ARP spoofing* útočník nejprve identifikuje cílová zařízení v síti, například klienta a výchozí bránu (*gateway*). Následně začne do sítě rozesílat podvržené ARP odpovědi, ve kterých informuje oběť (klienta), že jeho MAC adresa patří bráně, a zároveň druhému zařízení – tedy bráně – oznamuje, že jeho MAC adresa náleží klientovi. Tímto způsobem dochází k přesměrování veškeré síťové komunikace přes útočnickovo zařízení.

Pokud se útočnickovi podaří takto popsany útok úspěšně realizovat, jeho zařízení se dostává do pozice MitM, tedy prostředníka, přes kterého je přeposílána veškerá legitimní komunikace mezi klientem a bránou. Díky tomu je útočník schopen tuto komunikaci zachytávat, modifikovat nebo zcela blokovat. V závislosti na dalších použitých nástrojích může útočník dále například monitorovat přihlašovací údaje, odposlouchávat nešifrovaná data, přesměřovávat probíhající datové přenosy na jiný cílový server nebo provádět útoky typu DoS (*Denial of Service*) s cílem narušit celkovou dostupnost sítě.

Podrobný popis útoku typu *ARP spoofing* lze nalézt v [5], [6].



Obrázek 1.3 Schematické znázornění průběhu *ARP spoofing* útoku.³

Ochranná opatření proti útoku *ARP spoofing*

Útoky typu *ARP spoofing* lze do značné míry omezit, resp. zmírnit jejich dopad prostřednictvím implementace vhodných bezpečnostních opatření.

Jedním ze základních preventivních kroků je **statické nastavení ARP záznamů** na důležitých zařízeních v síti, čímž se zabrání jejich přepsání v důsledku přijetí nevyžádaných ARP odpovědí s falešně přiřazeným párem IP ↔ MAC adresa.

Mezi doplňková bezpečnostní opatření, která lze nasadit proti útokům typu *ARP spoofing*, patří mechanismus filtrování MAC adres, tzv. **MAC filtering**, a to především

³ Převzato z [7].

v menších nebo staticky konfigurovaných sítích. Jedná se o bezpečnostní techniku, při níž síťové zařízení (například přepínač nebo směrovač) povoluje připojení pouze těm zařízením, jejichž MAC adresy jsou předem uvedeny v seznamu povolených. Tímto způsobem lze zabránit neoprávněnému zařízení (například útočníkovi) v přístupu do sítě, čímž se snižuje riziko manipulace s obsahem ARP tabulek.

V síťové infrastruktuře podporující pokročilejší bezpečnostní funkce lze nasadit mechanismus **Dynamic ARP Inspection** (DAI), který bývá dostupný na síťových prvcích (zejména přepínačích). Ten porovnává přijaté ARP odpovědi s databází důvěryhodných údajů a v případě nesouladu zablokuje podezřelý provoz, resp. povolí pouze odpovědi, které odpovídají známým a legitimním záznamům.

Další možností je **segmentace sítě a využití technologie VLAN**, která umožní oddělení jednotlivých částí sítě a tím výrazně omezí působnost potenciálního útočníka v rámci konkrétního segmentu. Doporučuje se rovněž nasazení nástrojů pro detekci podezřelé činnosti, mezi které patří například nástroj **arpwatch**, jenž dokáže správce sítě upozornit na náhlé změny MAC adres v ARP tabulkách. Pravidelné monitorování a analýza síťového provozu pomocí nástroje Wireshark rovněž významně přispívá k rychlé identifikaci potenciálních hrozeb a nežádoucích událostí v síti.

1.3. Další hrozby na úrovni linkové vrstvy

Útok ARP spoofing není jedinou známou hrozbou, která se v počítačových sítích vyskytuje na úrovni linkové vrstvy. Existuje celá řada dalších typů útoků, které mohou být na této vrstvě provedeny. Níže jsou uvedeny některé z nich.

MAC Flooding

MAC Flooding je útok zaměřený na síťové přepínače (switche), jehož cílem je „zaplavení“ MAC tabulky přepínače velkým množstvím falešných MAC adres. Vzhledem k tomu, že přepínač má omezenou paměťovou kapacitu pro uložení záznamů mapujících MAC adresy na konkrétní porty, dojde při jejím překročení ke ztrátě původní funkčnosti přepínače. V takovém případě začne přepínač fungovat podobně jako hub – přijaté ethernetové rámce budou preposílány na všechny porty. To umožňuje útočníkovi odposlouchávat síťový provoz a potenciálně získávat citlivé informace.

Vhodnou obranou proti tomuto typu útoku je nasazení a správná konfigurace mechanismu **Port Security** na síťovém přepínači. Ta umožňuje omezit počet MAC adres, které mohou být aktivní na konkrétním portu, a definovat seznam povolených MAC adres, jejichž přítomnost na portu je považována za legitimní.

VLAN Hopping

VLAN Hopping je typ útoku, který umožňuje útočníkovi neoprávněný přístup do jiných VLAN segmentů v rámci jedné fyzické sítě. VLAN (*Virtual Local Area Network*) je technologie umožňující logické oddělení síťového provozu – a to buď na jednom

přepínači, nebo v rámci propojené infrastruktury více síťových prvků. Každá VLAN představuje samostatný logický segment, přičemž zařízení v různých VLAN spolu nemohou přímo komunikovat bez použití směrovače nebo jinak speciálně definovaných pravidel. VLAN se často používají za účelem zvýšení bezpečnosti, usnadnění správy sítě a rozdělení síťového provozu a zátěže, což umožňuje předcházet přetížení sítě nebo vzniku nežádoucí kolize.

Útok VLAN Hopping obchází tuto segmentaci a umožňuje útočnickovi komunikovat s VLAN, ke které by běžně neměl mít přístup. Během útoku dochází ke zneužití nesprávné konfigurace síťového přepínače, jehož úkolem je zajišťovat přenos dat mezi jednotlivými VLAN. VLAN Hopping může být proveden dvěma hlavními způsoby: **switch spoofing**, kdy se útočník vydává za důvěryhodný, legitimní přepínač a tím získává přístup k více VLAN, a tzv. **double tagging**, při kterém útočník manipuluje se značkami VLAN (tzv. VLAN tagy) v hlavičce ethernetových rámců, což vede k tomu, že jsou pakety chybně přesměrovány do jiné VLAN.

Ochrana proti VLAN Hoppingu spočívá ve správné konfiguraci přepínačů, zákazu automatického vyjednávání trunkových spojení a omezení VLAN *taggingu* pouze na ověřená zařízení.

Útoky na Spanning Tree Protocol

Spanning Tree Protocol (STP) je síťový protokol, jehož použití umožňuje zabránit vzniku síťových smyček v ethernetových sítích s redundantními spoji. Nesprávná konfigurace přeposílání rámců, v jejímž důsledku dochází k využívání záložních cest pro komunikaci, může vést k zahlcení sítě, opakovanému přeposílání paketů a celkově nežádoucímu ovlivnění komunikace v dané síti. Protokol STP umožňuje zařízením (přepínačům), aktivně identifikovat redundantní cesty v síti a dočasně deaktivovat některé porty, aby se zabránilo vzniku směrovacích smyček.

Protokol STP využívá pro výměnu informací mezi síťovými přepínači speciální zprávy nazývané **BPDU** (**Bridge Protocol Data Unit**). BPDU zprávy pomáhají určit hierarchii přepínačů a zvolit tzv. **root bridge**, tedy hlavní přepínač, který představuje referenční bod pro výpočet nejefektivnějších cest v síti s redundantními spoji a pro vytvoření tzv. páteřní sítě, sloužící k přenosu dat mezi uzly, a tím k eliminaci směrovacích smyček.

Útočník může tento mechanismus zneužít odesláním falešných BPDU zpráv s nižší prioritou, v důsledku čehož bude jeho zařízení ostatními přepínači považováno za **root bridge**. Následně může ovlivnit strukturu páteřní sítě a docílit toho, že veškerá komunikace bude procházet jeho zařízením, čímž získá neoprávněnou možnost odposlouchávat, a případně i manipulovat s přenášenými daty. Kromě toho může útočník opakovaně měnit topologii sítě neustálým zasíláním podvržených BPDU zpráv, což může vést k narušení provozu, celkové nestabilitě sítě, častým změnám v propojeních mezi

porty a v krajním případě až k fatálním výpadkům nebo úplnému přerušení síťové komunikace.

1.4. Kali Linux a použité nástroje

V rámci této laboratorní úlohy budou pro útok typu ARP *spoofing* a analýzu komunikace postupně využity následující nástroje:

- **arp spoof:** jednoduchý nástroj umožňující odesílání falešných ARP odpovědí.
- **Etttercap:** pokročilý MitM nástroj s možností ARP *spoofingu* a schopností cílené manipulace se síťovou komunikací.
- **Wireshark:** síťový analyzátor určený pro monitorování probíhající síťové komunikace (resp. jednotlivých datových paketů) a následnou analýzu manipulovaných ARP odpovědí.
- **Arpwatch:** nástroj pro sledování změn v ARP tabulkách a detekci podvržených MAC adres.

Nástroj arpspoof

Arpspoof je jednoduchý nástroj integrovaný v distribuci Kali Linux, který může být vhodným prostředkem pro realizaci útoku typu ARP spoofing. S pomocí tohoto nástroje lze docílit přeměrování síťového provozu (komunikace) mezi zařízeními v síti tím, že útočník předstírá identitu jiného zařízení (obvykle výchozí brány) a rozesílá falešné ARP odpovědi s cílem upravit záznamy v ARP tabulkách dotčených zařízení. Nástroj arpspoof může být využit pro testování zranitelností ARP protokolu a pro analýzu síťové komunikace.

V systému Kali Linux je nástroj arpspoof integrován jako součást balíčku dsniiff. Instalace do prostředí Kali Linux se provádí následujícím příkazem:

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

Struktura příkazu nástroje arpspoof je následující:

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

kde přepínač **-i** specifikuje síťové rozhraní, které bude použito pro ARP spoofing (např. rozhraní **eth0** u ethernetu), dále přepínač **-t** určuje IP adresu „oběti“, tj. cílového zařízení, jemuž má být odeslána falešná ARP odpověď. A poslední parametr **host** označuje IP adresu zařízení, vůči kterému útočník podvrhne falešné údaje, a jehož komunikaci chce na dané lince zachytit. [8]

Příklad použitého příkazu pro simulaci útoku ARP *spoofing*:

```
arp spoof -i eth0 -t <cílová_IP> <IP_brány>
```

což značí, že útok bude proveden na síťovém rozhraní **eth0**, přičemž falešné ARP odpovědi budou odesílány zařízení s IP adresou **<cílová_IP>**, a útočník bude zachytávat komunikaci určenou pro výchozí bránu s IP adresou **<IP_brány>** dané (lokální) sítě.

Nástroj **ettercap**

Ettercap je komplexní nástroj taktéž obsažený v Kali Linux, vhodný pro analýzu síťového provozu a realizaci MITM útoků včetně útoku ARP spoofing. Nabízí širší spektrum funkcí než nástroj **arp spoof** a umožňuje interaktivní sledování i manipulaci s pakety v reálném čase. Lze jej používat přes příkazovou řádku, nebo – výhodněji – pomocí uživatelsky přívětivého grafického rozhraní⁴. Mezi hlavní funkce nástroje **Ettercap** patří:

- automatická detekce zařízení v síti,
- realizace MITM útoků včetně ARP spoofingu, DNS spoofingu a manipulace s obsahem protokolů typu HTTPS a jiných protokolů,
- možnost využití vlastních filtrů pro úpravu obsahu přenášených dat. [9]

V praktické části této laboratorní úlohy budou použity oba výše uvedené nástroje pro simulaci útoku ARP *spoofing*. Zásadní rozdíly mezi nimi shrnuje následující tabulka:

Tabulka 1.1 Porovnání nástrojů **arp spoof** a **ettercap**.

<i>Funkce:</i>	arp spoof	ettercap
<i>Úroveň komplexnosti</i>	Jednoduchý nástroj vhodný pro simulaci útoku ARP <i>spoofing</i> .	Komplexní nástroj poskytující pestré možnosti, jako např.: analýza síťových parametrů, dostupnost zařízení, ...
<i>Podpora filtrů</i>	Ne	Ano
<i>Grafické rozhraní</i>	Ne	Ano
<i>Typy útoků</i>	ARP <i>spoofing</i>	ARP <i>spoofing</i> , DNS <i>spoofing</i> , generování vlastních paketů, možnost neoprávněné manipulace s obsahem, ...

⁴ Pro účely vypracování úloh tohoto laboratorního cvičení bude nástroj **Ettercap** v systému **Kali Linux** používán v jeho **grafickém režimu**.

Analyzátor síťové komunikace

Wireshark je jedním z nejpoužívanějších nástrojů pro zachytávání a analýzu síťových paketů. Používá se pro sledování probíhající datové komunikace s cílem diagnostiky problémů v síti, odhalování podezřelé aktivity a zkoumání možných bezpečnostních incidentů v monitorovaném síťovém prostředí. Tento nástroj umožňuje uživateli detailně sledovat síťovou komunikaci a analyzovat datové jednotky jednotlivých protokolů na všech vrstvách referenčního modelu ISO/OSI.

Pro účely této laboratorní úlohy bude nástroj Wireshark využit pro monitorování ARP komunikace, identifikaci podvržených ARP odpovědí během útoku ARP spoofing a pro ověření správnosti implementace ochranných opatření a posouzení jejich účinnosti vůči tomuto typu útoku.

Nástroj Wireshark umožňuje:

- **Zachytávání síťového provozu** – Wireshark umožňuje sledování veškeré komunikace probíhající přes zvolené síťové rozhraní (Ethernet, Wi-Fi, tunelované připojení, virtuální adaptéry apod.).
- **Analýzu paketů** – Umožňuje detailní rozbor obsahu paketů na všech vrstvách OSI modelu, včetně zobrazení a analýzy hlaviček protokolů jako ARP, TCP, UDP, ICMP, DNS nebo HTTP.
- **Filtrování paketů** – pomocí filtrů lze zobrazit pouze požadovaná a relevantní data, například zachycenou ARP komunikaci nebo HTTP požadavky. Filtrování může probíhat podle protokolů, IP adres, MAC adres, portů a dalších parametrů.
- **Rekonstrukce síťové komunikace** – Wireshark umožňuje analyzovat kompletní průběh komunikace mezi zařízeními v síti, včetně obsahu zpráv (např. sledování nešifrované HTTP komunikace, analýza požadavků a odpovědí).
- **Monitorování podezřelé aktivity, detekce útoků a bezpečnostních hrozeb** – Nástroj Wireshark je možné použít k odhalení podvržených ARP odpovědí, útoků typu *Man-in-the-Middle*, DoS útoků a dalších bezpečnostních incidentů.
- **Export a zpracování dat** – zachycené pakety (komunikaci) lze uložit do .pcap souborů pro následnou analýzu.

Základní příkazy Wiresharku (CLI verze – TShark)

Wireshark je možné používat také v textové verzi zvané **TShark**, která umožňuje sledovat a analyzovat síťovou komunikaci přímo z terminálu `$-` v systému Kali Linux. Zde jsou uvedeny užitečné příkazy:

- Zachytávání paketů na konkrétním rozhraní:

```
tshark -i eth0
```

Uvedený příkaz spustí zachytávání síťového provozu na rozhraní `eth0`.

- Použití filtru pro zobrazení pouze ARP paketů:

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

- Zachycení paketů a uložení do souboru:

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

- Zobrazení pouze vybraných polí v paketech:

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

Uvedený příkaz zobrazí pouze zdrojovou **ip.src** a cílovou **ip.dst** IP adresu zachycených paketů.

Pro potřeby této laboratorní úlohy bude použita grafická verze nástroje Wireshark, která umožňuje využít všechny jeho funkcionality prostřednictvím uživatelského rozhraní. Podrobnější popis možností nástroje a jeho využití bude uveden později v praktické části tohoto návodu.

ARPwatch

Nástroj ARPwatch slouží k **monitorování změn a detekci anomálií v ARP tabulkách** na síťových rozhraních zařízení a aktivních síťových prvcích. Umožňuje vytvářet upozornění (*alerts*) v případě výskytu nežádoucích nebo neočekávaných změn. Jeho použití je obzvlášť výhodné v prostředí s velkým množstvím zařízení, kde může být cenným nástrojem pro rychlou detekci potenciálních útoků typu ARP *spoofing*.

2. Praktická část

V rámci praktické části bude **realizován útok typu MitM, konkrétně ARP spoofing**. Simulovaný útok proběhne ve virtuální síti sestávající ze tří virtuálních strojů s Kali Linux (klient, server a útočník), jejíž topologie je schematicky znázorněna níže na obr. 2.1. Komunikace mezi uvedenými virtuálními stroji probíhá prostřednictvím virtuálního přepínače VMware virtual switch, jak je znázorněno na uvedeném obrázku. Cílem úspěšné realizace útoku *ARP spoofing* je modifikovat síť tak, aby veškerá komunikace mezi virtuálními stroji klienta a serveru probíhala výhradně přes zařízení útočníka.

2.1. Topologie virtuální sítě a nastavení virtuálních strojů

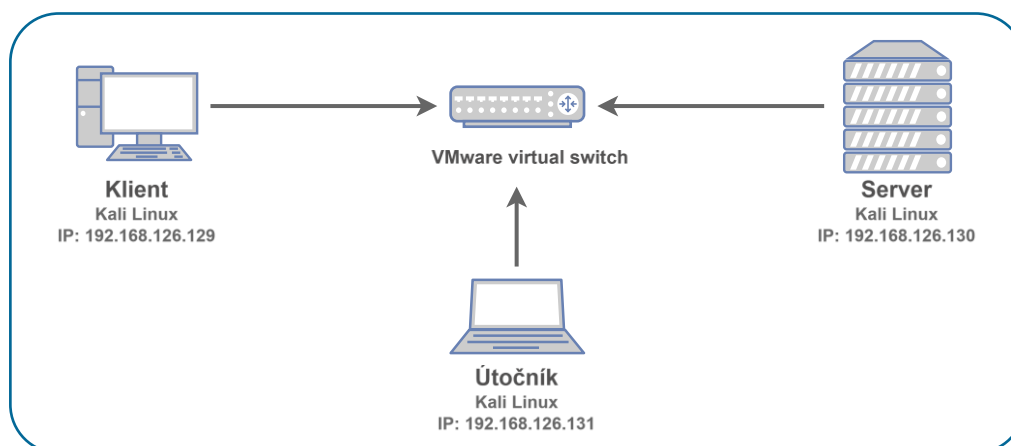
Použité virtuální stroje:

- oběť (klient): běžný počítač v síti, cíl útoku
- server: poskytovatel síťové služby (např. webserver, *gateway* = brána)
- útočník: provádí *ARP spoofing*, zachytává síťovou komunikaci mezi klientem a serverem

Síťová konfigurace:

- oběť: 192.168.126.129
- server: 192.168.126.130
- útočník: 192.168.126.131

Všechny virtuální stroje budou připojeny do stejné virtuální sítě (nastavení síťového adaptéru v režimu např. **Bridged** alebo **Host-Only**), aby bylo možné na VM představujícím „útočníka“ realizovat zachytávání datových přenosů (komunikace) mezi klientem a serverem.



Obrázek 2.1 Topologie sítě laboratorní úlohy.

2.2. Seznámení s použitými nástroji

Přehled základních příkazů pro jednotlivé používané nástroje

- Zobrazení ARP tabulky:

```
arp -a
```

Dobrovolné: Před zahájením praktické části si vyzkoušejte použití uvedeného příkazu na zařízeních klienta a serveru. Sledujte záznamy uvedené v ARP tabulce na obou zařízeních.

- ARP spoofing pomocí nástroje arpspoof:

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

- Spuštění Ettercapu přes terminál:

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

Použití Wiresharku pro analýzu ARP spoofing útoku

1. Spuštění zachytávání síťového provozu

Po spuštění programu Wireshark je nutné vybrat monitorované síťové rozhraní, přes které probíhá komunikace (**eth0** pro Ethernet). Po jeho výběru kliknutím na tlačítko **Start** spustíte zachytávání paketů.

2. Filtrování paketů ARP protokolu

Pro zobrazení datových jednotek odpovídajících komunikaci protokolu ARP je vhodné použít filtr: **arp**. Tento filtr zobrazí pouze ARP žádosti a ARP odpovědi odesílané v monitorované síti.

3. Identifikace podvržených ARP odpovědí

V rámci analýzy zachycené datové komunikace je nutné zaměřit se na různé prvky podezřelé aktivity, které mohou indikovat probíhající útok ARP *spoofing* útok. Může se jednat např. o:

- neočekávané ARP odpovědi bez předchozích ARP žádostí,
- stejné IP adresy přiřazené různým fyzickým MAC adresám,
- časté opakování ARP odpovědí směřujících na jedno cílové zařízení (oběť).

4. Ukládání a analýza dat

Zachycené pakety zaznamenané ARP komunikace je možné ve Wiresharku uložit do samostatného .pcap souboru a analyzovat později pomocí příkazu:

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

2.3. Postup pro vypracování laboratorní úlohy

A) Příprava prostředí

Spuštění virtuálních strojů:


- Otevřete VMware Workstation Pro (ikona na ploše).
- Postupně spusťte všechny tři virtuální stroje (klient, server, útočník).
- Zkontrolujte správnost síťové konfigurace, ověřte přiřazení IP adres.
- Přihlaste se do systému Kali Linux na VM útočníka.

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

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

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

Ověření síťové konektivity:

- Otevřete **terminál** (kliknutím na ikonu terminálu  v horní liště nebo pomocí klávesové zkratky **Ctrl + Alt + T**).
- Na každém VM zobrazte přidělené IP adresy (na rozhraní **eth0**):

```
ip a
```

- Z klienta odešlete testovací požadavek (ping) a vyzkoušejte připojení na server pomocí příkazu:

```
ping <ip_adresa_serveru>
```

Pokud se vrací odpovědi **ping echo reply** ze strany serveru, komunikace mezi zařízeními funguje.

- Stejným způsobem ověřte spojení i v opačném směru.
- Po ověření funkčnosti spojení **zobrazte překladové ARP tabulky** na obou zařízeních pomocí příkazu:

```
arp -a
```

Spuštění Wiresharku a sledování ARP paketů

- Na klientském zařízení spusťte Wireshark příkazem:

```
sudo wireshark &
```

Přepínač **'sudo'** spustí nástroj Wireshark s oprávněními správce, což je nezbytné pro zachytávání síťového provozu v Kali Linuxu.

- V hlavním okně vyberte síťové rozhraní (např. **eth0**).
- Do pole pro filtraci zadejte **arp** a potvrďte stisknutím klávesy **Enter**.
Použití filtru **'arp'** zajistí, že mezi všemi zachycenými datovými jednotkami přenášenými přes zvolené rozhraní budou zobrazeny pouze zprávy protokolu ARP.
- Klikněte na **Start Capturing Packets**.

B) Provedení ARP spoofing útoku

Cílem simulace útoku je dosáhnout „otravy“ ARP tabulek na klientském zařízení a na serveru prostřednictvím podvržených falešných ARP odpovědí od útočníka. Tyto odpovědi budou oznamovat, že server s IP adresou **192.168.126.130** má přiřazenou fyzickou MAC adresu odpovídající MAC adrese útočnickova zařízení [**cc: cc: cc: cc: cc: cc**]. Obdobně bude serveru poskytnuta informace, že klient s IP adresou **192.168.126.129** má také fyzickou MAC adresu útočnickova zařízení [**cc: cc: cc: cc: cc: cc**] (viz obr. 1.3).

Podvržení ARP odpovědí oběma komunikujícím zařízeními způsobí, že veškerá komunikace v směru **server → klient** a taky v opačném směru **klient → server** na zařízení útočníka. Útočník může zachycené zprávy modifikovat a následně je v upravené podobě přeposlat koncovému adresátovi, čímž dojde k narušení integrity komunikace.

Použití nástroje arpspoof

- Před spuštěním samotného útoku je nutné povolit přesměrování IP paketů na zařízení útočníka, aby mohl správně zprostředkovat komunikaci mezi klientem a serverem:

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

Tento příkaz zajistí, že útok nezpůsobí výpadek probíhajícího legitimního spojení mezi klientem a serverem, ale zároveň umožní útočnickovi komunikaci zachytávat a přeposílat – což je typický průběh **Man-in-the-Middle** útoku.

- Na útočnickově zařízení otevřete nové terminálové okno a spusťte následující příkazy pro provedení ARP *spoofing* útoku postupně pro oba směry komunikace.
Pro podvržení ARP odpovědi klientovi použijte příkaz:

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

*** do příkazu arpspoof vstupují jako parametry jednotlivých přepínačů hodnoty na základě síťové topologie vytvořené pro tuto laboratorní úlohu.*

- Následně opakujte postup **pro podvržení ARP odpovědi serveru:**

```
sudo arp spoof -i eth0 -t 192.168.126.130 192.168.126.129
```

Po použití uvedených příkazů budou generovány falešné ARP odpovědi a následně odeslány ze zařízení útočníka na zařízení s uvedenými IP adresami, čímž se útočník dostane do pozice prostředníka komunikace (MitM) mezi klientem a serverem.

- Po zadání příkazů začne nástroj **arp spoof** opakovaně odesílat na uvedené cílové IP adresy žádosti ARP Request. **Je nutné nechat tento příkaz na obou zařízeních (klient, server) spuštěný po celou dobu trvání útoku!** Jakékoli další příkazy je vhodné spustit v samostatném okně terminálu.
- Zadání obou příkazů **arp spoof** zaručí, že je útok ARP *spoofing* kompletní. Veškerá komunikace probíhající mezi klientem a serverem bude od tohoto momentu procházet přes zařízení útočníka.

Přesměrování komunikace – ověření útoku

- Po spuštění **arp spoof** z klienta na server i ze serveru na klienta je možné ověřit úspěšnost útoku jednoduchým příkazem **ping**. Na klientovi spusťte:

```
ping 192.168.126.130
```

- Na zařízení útočníka sledujte, zda se generované pakety protokolu ICMP objevují v zachycené komunikaci ve Wiresharku. Alternativně je možné ověřit úspěšnost útoku i prostřednictvím nástroje **tcpdump** následujícím příkazem:

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

Uvedený příkaz zobrazuje **všechny ICMP pakety** (napr. *ping*), které procházejí přes rozhraní **eth0**. Pokud útok probíhá správně a je zapnuté IP forwarding, na zařízení útočníka budou zachyceny odeslané zprávy ICMP echo a příslušné odpovědi (*reply*) mezi klientem a serverem.

Ověření změn v ARP tabulce klienta

- Na zařízení klienta zobrazte ARP tabulku zadáním příkazu do nového terminálového okna a porovnejte obsah tabulky před a po provedení útoku:

```
arp -a
```

Pokud je útok ARP spoofing úspěšný, MAC adresa příslušející k IP adrese serveru bude v překladové ARP tabulce změněna na MAC adresu zařízení útočníka.

- Obdobně postupujte i při kontrole ARP tabulky na serveru.

```
(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
```

Obrázek 2.2 Změny v ARP tabulce klienta.

Detekce změn v ARP tabulce pomocí nástroje arpwatc

- Po úspěšném spuštění útoku ARP *spoofing* můžete ověřit detekci změn v ARP tabulce i pomocí nástroje arpwatc.
- Na jednom z napadených strojů (klient/server) otevřete nové terminálové okno a nainstalujte arpwatc pomocí příkazů:

```
sudo apt update
sudo apt install arpwatc -y
```

- Spustěte arpwatc na síťovém rozhraní, kterým je napadené zařízení připojeno do sítě, ve které probíhá útok:

```
sudo arpwatc -i eth0
```

- Během probíhajícího simulovaného útoku pomocí arpspoof, sledujte výstup arpwatc v terminálu nebo kontrolujte logovací soubor:

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

nebo:

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

- Všimněte si zpráv, jako například:

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

nebo:

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

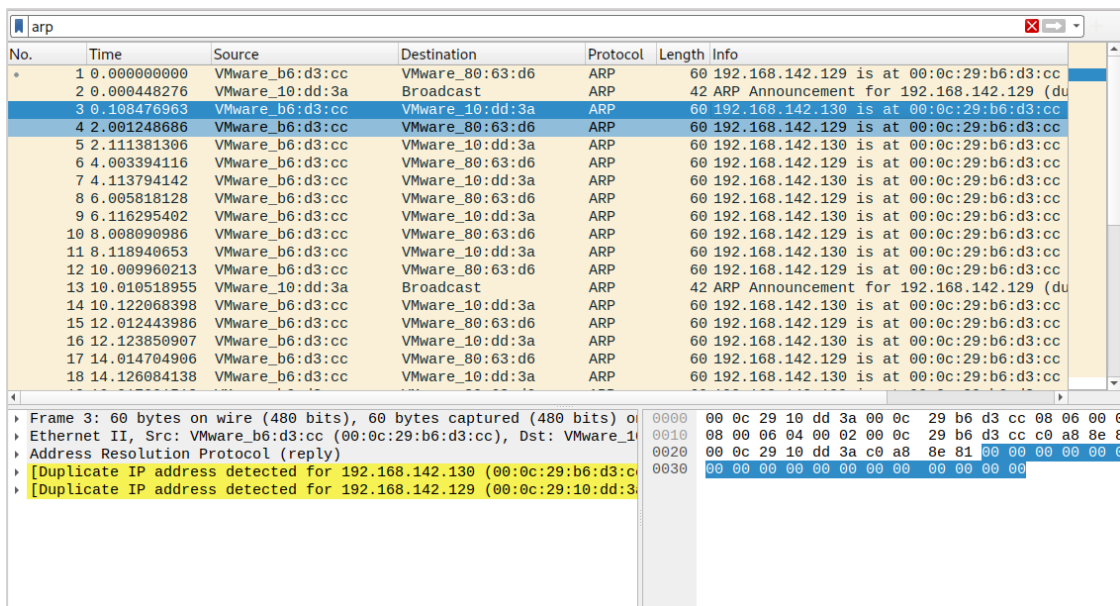
Zobrazené zprávy (a změny v ARP tabulce klienta) indikují, že uvedená IP adresa (server) byla spárována s novou MAC adresou (útočníka) – což je typický důsledek ARP spoofingu útoku.

Zachytávání a analýza dat ve Wiresharku

V rámci této laboratorní úlohy bude nástroj Wireshark využit především za účelem **monitorování probíhající ARP komunikace** ve vytvořené virtuální síti a k následné analýze zachycených zpráv (žádostí a odpovědí) protokolu ARP.

- Vraťte se do Wiresharku.
- Sledujte podvržené ARP odpovědi a analyzujte jejich obsah.

Kliknutím na paket zobrazíte jeho detailní strukturu. Zkontrolujte, **jak se změnila řídící informace v hlavičce protokolu ARP** po provedení útoku ARP spoofing útoku (zdrojová a cílová MAC adresa by měly být nahrazeny MAC adresou útočníka).



Obrázek 2.3 Ukázka zachycené komunikace (Wireshark)

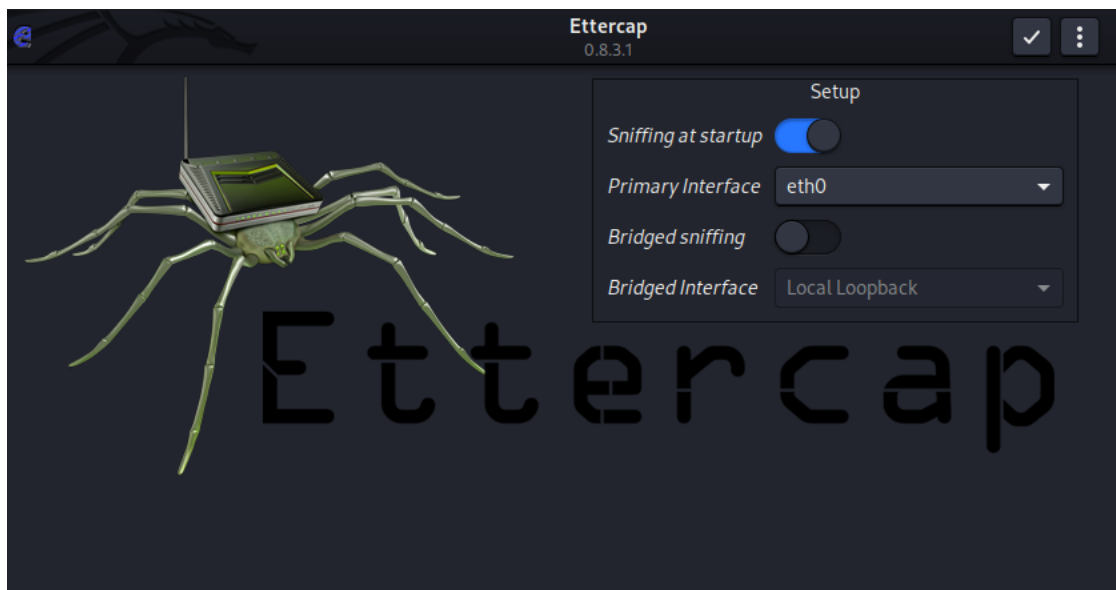
ARP spoofing pomocí nástroje Ettercap

- Na zařízení útočníka spusťte Ettercap v terminálu:

```
sudo ettercap -G
```

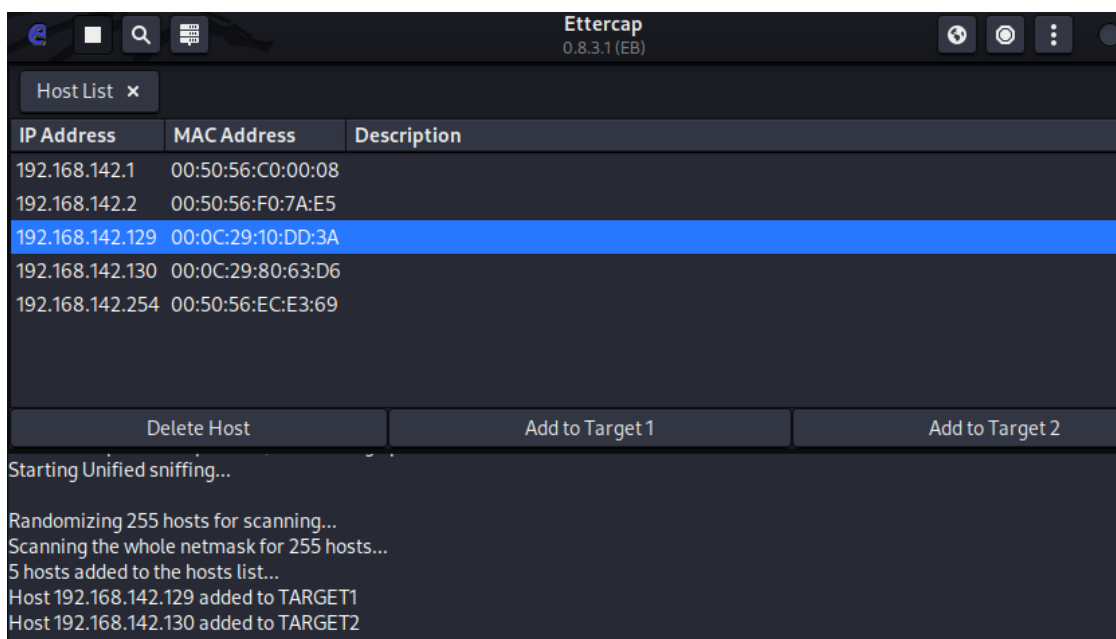
- Jako primární síťové rozhraní zvolte **eth0**.
- Po spuštění ponechte všechna výchozí nastavení beze změn (viz obr. 2.4) a pokračujte kliknutím na ☒ v horní části zobrazeného okna.

Kliknutím na **Options** (tři tečky v záhlaví) se ujistěte, že je aktivní volba **Promisc mode**. Tato volba zajistí, že zařízení útočníka bude během simulace pracovat v promiskuitním režimu, což umožní zachytávat veškerou komunikaci na lokální lince probíhající přes zvolené rozhraní.



Obrázek 2.4 Nástroj Ettercap: úvodní grafické rozhraní.

- Před výběrem cílových zařízení je třeba provést *skenování* sítě. Klikněte na „tři tečky“ v horní liště a zvolte **Hosts > Scan for hosts**, čímž naplníte seznam dostupných zařízení v síti.
- Po dokončení skenování zobrazíte seznam zařízení přes **Hosts > Hosts List** (viz obr. 2.5).
- Z tohoto seznamu vyberte cílová zařízení pro ARP *spoofing* útok a přidejte je postupně do **Target 1** (klient) a **Target 2** (server).
- Pokračujte kliknutím na nabídku *MitM Menu* (ikona zeměkoule v záhlaví grafického rozhraní), zvolte **MitM > ARP Poisoning**, zaškrtněte volbu **Sniff remote connections** potvrďte kliknutím na **OK**. Tím dojde k zahájení útoku.



Obrázek 2.5 Nástroj Ettercap: výpis nalezených zařízení v síti.

Ověření úspěšnosti MitM útoku pomocí Ettercap

- Po spuštění útoku v prostředí nástroje Ettercap v režimu MitM lze jeho úspěšnost ověřit obdobně jako u prvního útoku – pomocí aplikace **ping**, respektive odesláním zprávy ICMP *echo request* z klienta na server:

ping 192.168.126.130

Pokud zprávy protokolu ICMP procházejí přes zařízení útočníka (a tedy jsou viditelné v zachycené komunikaci ve Wiresharku, nebo je Ettercap zaznamená jako komunikaci mezi uvedenými IP adresami), znamená to, že ARP *spoofing* útok proběhl úspěšně a komunikace byla přesměrována.

2.4. Samostatný úkol

C) Implementace ochranných opatření

V závěrečné části laboratorní úlohy si prakticky vyzkoušíte možnosti ochrany proti útoku typu ARP *spoofing*.

Cílem vaší samostatné práce bude implementovat statické ARP záznamy, které představují jeden z možných způsobů obrany proti tomuto typu útoku, a následně otestovat účinnost této ochrany.

Konfigurace statických ARP záznamů

- Na klientovi a serveru zadefinujte statické ARP záznamy následujícím způsobem:

```
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.**: Použijte konkrétní MAC adresy a IP adresy odpovídající vašim používaným VMs.*

- Ověřte uložení zadaných statických záznamů zobrazením ARP tabulky na obou zařízeních prostřednictvím výpisu jejího aktuálního obsahu.

Testování účinnosti ochrany

- Opakujte útok pomocí nástroje `arp spoof` podle předchozího postupu a ověřte, zda nedochází ke změnám MAC adres v ARP tabulce.
- V případě, že se záznamy v ARP tabulce na obou VMs (klient, server) nezmění, je implementovaná ochrana proti podvržení falešných MAC adres účinná díky nastavení statických záznamů v ARP tabulce.

3. Závěr

V tomto laboratorním úkolu jste se seznámili s problematikou bezpečnosti linkové vrstvy počítačových sítí. Prakticky jste si ověřili **průběh útoku ARP spoofing**, při kterém útočník podvržením falešných ARP odpovědí dosáhne zavedení nesprávných informací o fyzických MAC adresách do překladových ARP tabulek komunikujících zařízení, což může mít za následek přesměrování komunikace právě přes zařízení útočníka.

Účinnou ochranou proti útokům založeným na „otravě“ překladové ARP tabulky je **konfigurace statických záznamů** pro mapování mezi síťovými a fyzickými adresami. Tato konfigurace zabrání získávání informací o MAC adresách prostřednictvím ARP protokolu mezi zařízeními v síti, a tím i nežádoucímu zneužití ARP odpovědí k podvržení falešné fyzické (MAC) adresy.

3.1. Kontrolní otázky

1. Jakou funkci plní ARP protokol v rámci síťové komunikace?
 - A) Zajišťuje překlad logické IP adresy na fyzickou MAC adresu v lokální síti
 - B) Přiřazuje porty k IP adresám
 - C) Zjišťuje fyzickou adresu zařízení na základě jeho známé IP adresy
 - D) Poskytuje kryptografickou ochranu komunikace mezi dvěma zařízeními
2. Která z následujících tvrzení správně popisují útok typu ARP spoofing?
 - A) Útočník odesílá do sítě falešné ARP odpovědi, aby dosáhl změny IP adresy v ARP tabulce zařízení
 - B) Jedná se o typ útoku, při kterém útočník podvrhne svou MAC adresu místo skutečné MAC adresy zařízení s hledanou IP adresou v odpovědi na ARP žádost jiného zařízení
 - C) Cílem útoku je přesměrovat síťovou komunikaci přes zařízení útočníka
 - D) ARP spoofing se využívá primárně za účelem narušení dostupnosti cílové služby
3. Jaký je rozdíl mezi dynamickým a statickým ARP záznamem?
 - A) Dynamický záznam je uložený trvale, statický pouze dočasně
 - B) Statický záznam je nastaven ručně, dynamický je generován automaticky
 - C) Dynamický záznam se nikdy neaktualizuje podle aktuální situace v síti
 - D) Dynamický je bezpečnější než statický
4. Proč je při útoku typu MitM důležité zapnout IP forwarding?
 - A) Aby bylo možné odesílat pakety přes zabezpečené HTTPS spojení
 - B) Protože umožní odesílání a přijímání ICMP zpráv
 - C) Aby útočník mohl přesměrovat síťovou komunikaci přes své zařízení
 - D) Umožňuje zakázat použití mechanismu MAC filtering

5. Který z následujících nástrojů slouží primárně k analýze síťové komunikace?
- A) arpspoof
 - B) Ettercap
 - C) Wireshark
 - D) arping
6. Které z následujících jevů mohou naznačovat probíhající ARP *spoofing* v síti?
- A) Snížená latence a zvýšená přenosová rychlost v síti
 - B) Výskyt ARP odpovědí, které přiřazují stejnou MAC adresu více IP adresám
 - C) Výskyt "duplicate IP" varování v systému
 - D) Výskyt více ARP odpovědí bez předchozích požadavků
7. Která tvrzení vystihují rozdíly mezi nástroji arpspoof a Ettercap?
- A) Ettercap dokáže analyzovat a upravovat data vyšších vrstev (např. HTTP)
 - B) arpspoof je jednoduchý nástroj pro použití v CLI bez možnosti manipulace s vlastními daty
 - C) Ettercap neumožňuje vizualizaci MitM útoků pomocí GUI rozhraní
 - D) arpspoof automaticky obnovuje ARP tabulky po útoku
8. K čemu slouží nástroj arpspoof během útoku typu MitM?
- A) Odesílá falešné ARP odpovědi, aby se útočník dostal do pozice mezi dvě zařízení (MitM)
 - B) Skenuje síť pro zjištění aktivních služeb
 - C) Skenuje síť pro zjištění připojených koncových zařízení
 - D) Blokuje komunikaci mezi routerem a klientem
9. Která z následujících opatření mohou pomoci chránit síť před ARP *spoofingem*?
- A) Použití TLS šifrování
 - B) Konfigurace statických ARP záznamů
 - C) Nasazení *Dynamic ARP Inspection* (DAI)
 - D) Použití VLAN segmentace
10. Jaký filtr ve Wiresharku použijete pro zobrazení pouze ARP paketů (požadavků i odpovědí)?
- A) arp
 - B) ip.arp == 1
 - C) eth.type == 0x0806
 - D) arp.request

4. Literatura

- [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. ALO- 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].