

Dokumentácia pre vyučujúceho k laboratórnej úlohe

Laboratórna úloha č. 3

BEZPEČNOSŤ SPOJOVEJ VRSTVY

1. Základné informácie k laboratórnej úlohe

Laboratórna úloha č. 3 je zameraná na problematiku bezpečnosti spojovej vrstvy. V teoretickej časti sú diskutované zraniteľnosti na úrovni spojovej vrstvy RM OSI a v nadväzujúcej praktickej časti je **realizovaný útok ARP spoofing**.

Študenti realizujú simuláciu útoku typu MitM s využitím troch virtuálnych strojov so systémom Kali Linux, pričom postupne využijú nástroje **arp spoof**, Ettercap, Wireshark a prípadne **tcpdump**. Cieľom laboratórnej úlohy je porozumieť princípu fungovaniu ARP protokolu, simulovať útok typu ARP *spoofing*, analyzovať jeho dopad na prebiehajúcu komunikáciu a navrhnúť ochranné opatrenia proti tomuto typu útoku.

2. Očakávané výstupy práce študentov

Úlohou študentov je postupne podľa krokov podrobne popísaných v priloženom návode **simulovať útok ARP spoofing s využitím nástroja arp spoof** v prostredí terminálu, a následne obdobný typ útoku realizovať aj s **pomocou nástroja Ettercap**.

V oboch prípadoch taktiež sledujú vo Wiresharku zachytenú komunikáciu VMs, v ktorej sa zamerajú najmä na analýzu ARP správ. Pre overenie úspešnosti útoku je potrebné skontrolovať úspešnosť ARP *Cache Poisoning*-u („otravy“ ARP tabuliek) na zariadení klienta a na serveri, t. j. či naozaj došlo k podvrhnutiu ARP odpovedí s MAC adresou útočnickovho zariadenia.

Úspešnosť samotného ARP *spoofing* útoku sa overí **sledovaním komunikácie prechádzajúcej cez zariadenie útočníka vo Wiresharku**, ktorá by mala obsahovať pakety odosielané medzi klientom a serverom (napr. ping medzi týmito doma zariadeniami).

2.1. Riešenie samostatnej úlohy

V rámci samostatnej úlohy majú študenti za cieľ navrhnúť a implementovať ochranu voči ARP *spoofingu*, a to napr. vhodnou **konfiguráciou statických ARP záznamov**.

Účinnosť implementovanej ochrany je demonštrovaná neúspešnosťou ďalšieho *spoofingu*, nakoľko po nastavení statických ARP záznamov v prekladových tabuľkách na zariadení klienta a na serveri nie je možné docieľiť zápis podvrhutej MAC adresy útočníka do prekladovej ARP tabuľky, a teda ani presmerovanie komunikácie cez jeho zariadenie.

Pre kontrolu správnosti implementácie statických ARP záznamov je vhodné overiť výpis príkazu **arp -a** pre zobrazenie ARP tabuliek (klient a server), prípadne výstup nástroja **tcpdump** u útočníka, ktorý by v tomto prípade už nemal zachytiť žiadnu komunikáciu klienta so serverom.

2.2. Odpovede na 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 priradzujú 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

2.3. Dopĺňajúce otázky

Nižšie uvedené otázky môžu byť využité pri kontrole výstupov samostatnej práce študentom s cieľom overiť, či skutočne porozumeli riešenej problematike v praktickej časti laboratórnej úlohy.

1. Popíšte, akú úlohu zohráva ARP protokol v komunikácii medzi zariadeniami v lokálnej sieti.

- ARP (*Address Resolution Protocol*) slúži na dynamické mapovanie logických IP adries na fyzické MAC adresy v rámci lokálnej siete, resp. na zistenie fyzickej (MAC) adresy zariadenia so známou IP adresou.

2. Čo je ARP spoofing a v čom tento útok spočíva?

- ARP *spoofing* je príkladom MitM (Man-in-the-Middle) útoku, pri ktorom útočník najskôr posiela do siete falošné ARP odpovede, s cieľom podvrhnúť MAC adresu svojho zariadenia pre prekladové záznamy prislúchajúce IP adrese dôveryhodného uzlu v sieti (napr. bráne alebo serveru), čo má za následok presmerovanie komunikácie práve cez zariadenie útočníka.

3. Aký je rozdiel medzi dynamickým a statickým ARP záznamom?

- Dynamické záznamy v ARP tabuľkách sú vytvárané a tiež priebežne aktualizované automaticky na základe komunikácie ARP protokolu, statické záznamy sú nastavené manuálne administrátorom, pomocou príkazu `arp -s <IP> <MAC>`. Pri použití statických záznamov nedochádza k ich automatickej zmene. Sú jedným zo spôsobov ochrany proti *spoofingu* (resp. proti podvrhnutiu falošnej MAC adresy), no vyžadujú ručnú správu.

4. Prečo je dôležité aktivovať IP forwarding pri MitM útoku?

- IP *forwarding* zabezpečuje, že sieťové pakety prijaté na jednom rozhraní útočnickovho zariadenia budú automaticky preposielané na druhé rozhranie smerom k cieľovému uzlu. V kontexte MitM útoku to znamená, že útočník dokáže nielen zachytávať, ale aj transparentne preposielať všetku komunikáciu medzi obeťami (napr. klientom a serverom), čím zostáva útok utajený a pritom funkčný bez akéhokoľvek prerušenia sieťového spojenia medzi legitímnymi zariadeniami.

5. Vysvetlite, akým spôsobom ste nastavili ciele pri použití nástroja Ettercap. Prečo sú jednotlivé kroky dôležité?

- Pri použití nástroja Ettercap je potrebné najprv vykonať sken siete (*Scan for hosts*) za účelom zistenia dostupných zariadení v danej sieti. Výsledkom bude zoznam, tzv. *Host List*, z ktorého sa následne vyberú cieľové IP adresy konkrétnych zariadení (napr. klient a server), ktoré majú byť cieľom útoku. Vybrané zariadenia sa označia ako *Target 1* a *Target 2*. Táto voľba je kľúčová pre správne nasmerovanie *spoofingu*, na konkrétne zariadenia

6. Aký filter Wiresharku použijete na zobrazenie len ARP paketov?

- Pre filtrovanie paketov ARP protokolu v prostredí nástroja Wireshark je nutné použiť filter `arp`, ktorý zobrazí výlučne len ARP požiadavky (*Request*) a odpovede (*Reply*).