

Dokumentace pro vyučujícího k laboratorní úloze

Laboratorní úloha č. 3

BEZPEČNOST LINKOVÉ VRSTVY

1. Základní informace k laboratornímu úkolu

Laboratorní úkol č. 3 je zaměřen na problematiku bezpečnosti linkové vrstvy. V teoretické části jsou diskutovány zranitelnosti na úrovni linkové vrstvy RM OSI a v navazující praktické části je **realizován útok ARP spoofing**.

Studenti provádějí simulaci útoku typu MitM s využitím tří virtuálních strojů se systémem Kali Linux, přičemž postupně využijí nástroje `arp spoof`, Ettercap, Wireshark a případně `tcpdump`. Cílem úkolu je porozumět principu fungování ARP protokolu, simulovat útok typu ARP *spoofing*, analyzovat jeho dopad na probíhající komunikaci a navrhnout opatření pro ochranu proti tomuto typu útoku.

2. Očekávané výstupy práce studentů

Úkolem studentů je postupně dle jednotlivých kroků podrobně popsáných v příloženém návodu **simulovat útok ARP spoofing pomocí nástroje arp spoof** v terminálu a následně provést obdobný útok **pomocí nástroje Ettercap**.

V obou případech také sledují ve Wiresharku zachycenou komunikaci mezi VMs, přičemž se zaměřují především na analýzu ARP zpráv. Pro ověření úspěšnosti útoku je třeba zkontrolovat, zda skutečně došlo k ARP *Cache Poisoning*-u („otravě“ ARP tabulek) na zařízení klienta i serveru, tedy zda byly podvrženy ARP odpovědi s MAC adresou útočnickova zařízení.

Úspěšnost samotného ARP *spoofing* útoku se ověřuje **sledováním komunikace procházející přes zařízení útočnicka ve Wiresharku** – ta by měla obsahovat pakety odesílané mezi klientem a serverem (např. ping mezi těmito dvěma zařízeními).

2.1. Řešení samostatného úkolu

V rámci samostatného úkolu mají studenti za cíl navrhnout a implementovat ochranu proti ARP *spoofingu*, například vhodnou **konfigurací statických ARP záznamů**.

Účinnost implementované ochrany se demonstruje neúspěšným pokusem o další *spoofing*, jelikož po nastavení statických ARP záznamů v překladových tabulkách na zařízení klienta a serveru není možné podvrženou MAC adresu útočnicka zapsat do překladové ARP tabulky, a tedy ani přesměrovat komunikaci přes jeho zařízení.

Pro kontrolu správnosti konfigurace statických ARP záznamů je vhodné ověřit výstup příkazu `arp -a` pro zobrazení ARP tabulek (klient a server), případně výstup nástroje `tcpdump` na zařízení útočnicka, který by v tomto případě již neměl zachytit žádnou komunikaci mezi klientem a serverem.

2.2. Odpovědi na 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

2.3. Doplnující otázky

Níže uvedené otázky mohou být využity při kontrole výstupů samostatné práce studentů za účelem ověření, zda skutečně porozuměli řešené problematice v praktické části laboratorního úkolu.

1. Popište, jakou úlohu sehrává ARP protokol v komunikaci mezi zařízeními v lokální síti.

- ARP (*Address Resolution Protocol*) slouží k dynamickému mapování logických IP adres na fyzické MAC adresy v lokální síti, resp. ke zjištění fyzické (MAC) adresy zařízení se známou IP adresou.

2. Co je ARP spoofing a v čem tento útok spočívá?

- ARP spoofing je příkladem útoku typu MitM (*Man-in-the-Middle*), při kterém útočník nejprve posílá do sítě falešné ARP odpovědi, s cílem podvrhnout MAC adresu svého zařízení do překladových záznamů odpovídajících IP adrese důvěryhodného uzlu v síti (např. brány nebo serveru), což má za následek přesměrování komunikace právě přes zařízení útočníka.

3. Jaký je rozdíl mezi dynamickým a statickým ARP záznamem?

- Dynamické záznamy v ARP tabulkách jsou vytvářeny a průběžně aktualizovány automaticky na základě komunikace protokolu ARP, statické záznamy jsou nastaveny ručně administrátorem pomocí příkazu `arp -s <IP> <MAC>`. U statických záznamů nedochází k jejich automatické změně. Jsou jedním ze způsobů ochrany proti *spoofingu* (tedy podvržení MAC adresy), vyžadují však ruční správu.

4. Proč je důležité aktivovat IP forwarding při MitM útoku?

- IP forwarding zajišťuje, že síťové pakety přijaté na jednom rozhraní zařízení útočníka budou automaticky přeposílány na druhé rozhraní směrem k cílovému uzlu. V kontextu MitM útoku to znamená, že útočník je schopen nejen zachytávat, ale i transparentně přeposílat veškerou komunikaci mezi oběťmi (např. klientem a serverem), čímž útok zůstává utajený a zároveň funkční bez přerušení spojení mezi legitimními zařízeními.

5. Vysvětlete, jakým způsobem jste nastavili cíle při použití nástroje Ettercap. Proč jsou jednotlivé kroky důležité?

- Při použití nástroje Ettercap je nejprve nutné provést skenování sítě (*Scan for hosts*) za účelem zjištění dostupných zařízení v síti. Výsledkem je seznam, tzv. *Host List*, ze kterého se následně vyberou cílové IP adresy konkrétních zařízení (např. klient a server), které mají být cílem útoku. Vybraná zařízení se označí jako Target 1 a Target 2. Tato volba je klíčová pro správné nasměrování *spoofingu* na konkrétní zařízení.

6. Jaký filtr Wiresharku použijete k zobrazení pouze ARP paketů?

- Pro filtrování ARP paketů v prostředí nástroje Wireshark je nutné použít filtr `arp`, který zobrazí výhradně ARP požadavky (*Request*) a odpovědi (*Reply*).