

Dokumentace pro vyučujícího k laboratorní úloze

Laboratorní úloha č. 4

BEZPEČNOST SÍŤOVÉ VRSTVY

1. Základné informace k laboratorní úloze

Laboratorní úloha č. 4 se zaměřuje na **bezpečnostní aspekty síťové vrstvy** modelu ISO/OSI. Cílem je prakticky demonstrovat, jak lze narušit síťovou komunikaci pomocí techniky IP *spoofing* a následně tuto komunikaci zabezpečit implementací protokolu IPsec.

Studenti pracují v prostředí tří virtuálních strojů s operačním systémem Kali Linux, kde každý stroj plní odlišnou roli – klient, server a útočník. Během úlohy budou studenti **simulovat IP spoofing** útok pomocí nástroje **hping3**, analyzovat přenosy ve Wiresharku a následně implementovat zabezpečenou komunikaci s využitím knihovny strongSwan, která umožňuje **implementaci protokolu IPsec** v transportním režimu. Na závěr budou studenti porovnávat účinnost a základní charakteristiky transportního a tunelového režimu IPsec z hlediska bezpečnosti a výkonnosti sítě.

2. Očekávané výstupy práce studentů

Po úspěšném absolvování této úlohy by měli studenti být schopni popsat a prakticky demonstrovat průběh útoku typu IP *spoofing*. Pomocí nástroje hping3 odešlou pakety s falešnou zdrojovou IP adresou a následně tyto pakety zachytí a analyzují v nástroji Wireshark, kde porovnají IP a MAC adresy v hlavičce zachycených datových jednotek.

Dále by měli studenti správně nakonfigurovat IPsec komunikaci v transportním režimu mezi klientem a serverem, k čemuž využijí *open-source* knihovnu strongSwan a ověří stav spojení pomocí příkazu **ipsec statusall**. Důležitým bodem je i porovnání obsahu zachycené komunikace před a po nasazení zabezpečení IPsec – v případě úspěšné konfigurace by měly být v záznamu komunikace viditelné šifrované ESP pakety. Ověření výstupů a správnosti implementace IPsec probíhá na základě analýzy paketů ve Wiresharku nebo prostřednictvím nástroje **tcpdump** a rovněž kontrolou aktivního IPsec spojení. Úspěšnost úlohy je možné hodnotit podle schopnosti studenta jasně vysvětlit a demonstrovat rozdíly mezi nezašifrovanou a zašifrovanou komunikací.

2.1. Riešenie samostatnej úlohy

V rámci samostatné úlohy mají studenti za úkol simulovat prostředí veřejné sítě, což mohou provést například změnou typu síťového rozhraní ve VMware (NAT nebo bridged). V tomto prostředí následně nakonfigurují IPsec spojení mezi klientem a serverem, tentokrát však v tunelovém režimu. Jejich cílem bude zajistit, aby veškerá IP komunikace procházela šifrovaným tunelem, čímž bude šifrována nejen datová část paketu, ale také původní IP hlavička. V nástroji Wireshark by měly být viditelné pouze

šifrované ESP pakety, jejichž datová část nebude přímo čitelná, což prokazuje úspěšnou implementaci tunelového režimu.

Studenti následně provedou měření výkonnostních parametrů sítě (latence a propustnost) v různých režimech – nezašifrovaná komunikace, IPsec v transportním a v tunelovém režimu. Na základě zobrazených výsledků vypracují stručnou zprávu, ve které porovnají výhody a nevýhody obou bezpečnostních režimů z hlediska výkonu a úrovně zabezpečení. Tato část je důležitá nejen pro ověření praktických dovedností studentů, ale i jejich schopnosti správně analyzovat a vhodně interpretovat dosažené výsledky.

2.2. Odpovědi na kontrolní otázky

1. Co je cílem IP *spoofing* útoku?

- A) Změnit MAC adresu útočníka
- B) Získat neautorizovaný přístup předstíráním cizí IP adresy ☒
- C) Přesměrovat legitimní komunikaci přes vlastní zařízení
- D) Zamezit šifrování dat mezi serverem a klientem

2. Která z následujících tvrzení platí o nástroji hping3?

- A) Umožňuje simulovat IP *spoofing* a různé typy síťových útoků ☒
- B) Je určen k šifrování komunikace pomocí IPsec
- C) Dokáže vygenerovat vlastní TCP/IP pakety dle specifikace ☒
- D) Je to nástroj pro konfiguraci VPN tunelů mezi vzdálenými sítěmi

3. Vyberte nesprávná tvrzení týkající se IP *spoofing* útoku:

- A) IP spoofing automaticky zahrnuje změnu MAC adresy ☒
- B) Má za následek zvýšení přenosové rychlosti v síti ☒
- C) Spoofovaný paket má obvykle neplatný kontrolní součet ☒
- D) Využívá manipulaci s IP záhlavím paketů

4. Jaký je hlavní rozdíl mezi transportním a tunelovým režimem IPsec?

- A) V tunelovém režimu se šifruje pouze hlavička IP paketu
- B) Transportní režim se používá v bezdrátových sítích
- C) V transportním režimu jsou šifrována pouze uživatelská data, IP hlavička paketu zůstává nezměněná ☒
- D) Tunelový režim nemůže být využit v IPv6 síti

5. Co způsobí nastavení parametru `authby=secret` v souboru `ipsec.conf`?

- A) Povolení anonymního přístupu
- B) Vypnutí autentizace
- C) Autentizaci pomocí předsdíleného tajemství (PSK) ☒
- D) Použití certifikátů

6. Protokol AH (Authentication Header) v IPsec:

- A) Umožňuje zašifrovat celý IP paket
- B) Zajišťuje autentizaci a integritu paketu bez šifrování ☒
- C) Poskytuje možnost tunelování přenosu přes HTTPS
- D) Zajišťuje důvěrnost řídicích informací v IP hlavičce

7. Vyberte nesprávná tvrzení o tunelovém režimu IPsec:

- A) Zabezpečuje celý IP paket včetně původní hlavičky
- B) Není vhodný pro spojení mezi dvěma bránami ☒
- C) Používá se zejména při zabezpečení VPN
- D) Přenáší pakety přes šifrovaný SSH tunel ☒

8. V jakých situacích je vhodné použít IPsec v transportním režimu?

- A) Komunikace mezi klientem a serverem ve stejné síti ☒
- B) Propojení dvou vzdálených sítí přes internet
- C) Pro zabezpečení SSH spojení
- D) Ochrana komunikace mezi aplikacemi v rámci jednoho serveru ☒

9. Jak může použití IPsec ovlivnit výkonnost počítačové sítě?

- A) Zvýšená latence v důsledku šifrování a dešifrování paketů ☒
- B) Snížená kvalita přenosu způsobená použitím NAT
- C) Větší objem přenášených dat v důsledku přidání hlaviček ☒
- D) Zablokování komunikace mezi zařízeními, která nepodporují IPsec ☒

10. V konfiguraci IPsec spojení je parametr `left` používán k určení:

- A) Data vypršení platnosti certifikátu
- B) IP adresy vzdáleného serveru
- C) Lokální IP adresy koncového zařízení, kde je konfigurace definována ☒
- D) Sdíleného hesla pro tunelové šifrování

2.3. Doplňující otázky

Níže uvedené otázky lze využít při kontrole výstupů samostatné práce studentů s cílem ověřit, zda skutečně porozuměli řešené problematice v praktické části laboratorní úlohy.

1. Jaký vliv má použití zabezpečení pomocí IPsec na výkon sítě (latenci, rychlost přenosu dat apod.)?

- Použití IPsec může ovlivnit výkon sítě, především zvýšením latence a mírným snížením propustnosti. Tento efekt je způsoben dodatečným zpracováním paketů v procesech šifrování a dešifrování na obou koncích komunikace.

V tunelovém režimu může být vliv ještě výraznější, jelikož dochází k zapouzdření celého IP paketu, čímž se zvětšuje i jeho velikost.

2. Vysvětlete princip útoku IP spoofing.

- Útok IP spoofing spočívá v podvržení zdrojové IP adresy v paketech generovaných útočníkem tak, aby se tyto pakety jevily, jako by pocházely z důvěryhodného zařízení (oběti). Tento typ útoku umožňuje obejít bezpečnostní mechanismy a ACL pravidla a může být také využit jako součást širších útoků, například DDoS.

3. Jaký je rozdíl mezi transportním a tunelovým režimem IPsec?

- Při použití IPsec v transportním režimu se šifruje pouze datová část paketu, přičemž IP hlavička zůstává původní a nezměněná. Tento režim se nejčastěji používá pro zabezpečení komunikace mezi dvěma koncovými body. Naproti tomu tunelový režim šifruje celý původní IP paket včetně hlavičky, který je následně zapouzdřen do nového IP paketu s novou IP hlavičkou. Tunelový režim se využívá zejména pro zabezpečení komunikace mezi dvěma sítěmi nebo bránami.

4. Vysvětlete funkci a účel použití jednotlivých součástí IPsec, konkrétně protokolů AH a ESP.

- Protokol AH (*Authentication Header*) zajišťuje autentizaci a integritu přenášených dat včetně IP hlavičky, ale nešifruje jejich obsah. Protokol ESP (*Encapsulating Security Payload*) umožňuje šifrování, čímž zajišťuje důvěrnost komunikace, a také zajišťuje integritu, avšak pouze datové části paketu. Pro dosažení komplexní ochrany probíhající komunikace, tedy zajištění autenticity, důvěrnosti a integrity datového obsahu, je vhodné používat protokoly AH a ESP současně.

5. Jakým způsobem lze pomocí programu Wireshark ověřit správné fungování IPsec? Uveďte příklad, můžete využít část zachycené datové komunikace.

- Ve Wiresharku je možné filtrovat komunikaci protokolu ESP pomocí filtru **esp**. Po úspěšné konfiguraci zabezpečení IPsec by měly být pakety v tomto formátu nečitelné, což znamená, že jejich obsah (datová část) bude zašifrován. Ve srovnání s nezašifrovanou komunikací, kde jsou data viditelná (např. komunikace protokolů ICMP nebo HTTP), je to jasný důkaz funkčního IPsec spojení. Kromě toho je možné analyzovat i hlavičky paketů a ověřit, že ESP zajišťuje komunikaci mezi správnými zařízeními.