

Dokumentácia pre vyučujúceho k laboratórnej úlohe

Laboratórna úloha č. 4

BEZPEČNOSŤ SIEŤOVEJ VRSTVY

1. Základné informácie k laboratórnej úlohe

Laboratórna úloha č. 4 sa venuje bezpečnostným aspektom sieťovej vrstvy ISO/OSI modelu. Cieľom je prakticky demonštrovať, ako je možné narušiť sieťovú komunikáciu pomocou techniky IP *spoofing* a následne túto komunikáciu zabezpečiť implementáciou protokolu IPsec.

Študenti pracujú v prostredí troch virtuálnych strojov s operačným systémom Kali Linux, kde každý stroj zohráva inú úlohu – klient, server a útočník. V priebehu úlohy budú študenti **simulovať IP spoofing** útok pomocou nástroja **hping3**, analyzovať prenosy vo Wiresharku a následne implementovať zabezpečenú komunikáciu pomocou knižnice **strongSwan**, ktorá umožňuje **implementovať IPsec protokol** v transportnom režime. Nakoniec budú študenti porovnávať účinnosť a základné charakteristiky transportného a tunelového režimu IPsec z hľadiska bezpečnosti a výkonu siete.

2. Očakávané výstupy práce študentov

Po úspešnom absolvovaní tejto úlohy by mali študenti byť schopní popísať a prakticky demonštrovať priebeh útoku typu IP spoofing. Pomocou nástroja hping3 odošlú pakety s falošnou zdrojovou IP adresou a následne tieto pakety zachytia a analyzujú v nástroji Wireshark, kde porovnajú IP a MAC adresy v záhlaví zachytených dátových jednotiek.

Ďalej by mali študenti správne nakonfigurovať IPsec komunikáciu v transportnom režime medzi klientom a serverom, pre dosiahnutie toho využiť *open-source* knižnicu strongSwan a následne overiť stav spojenia pomocou príkazu **ipsec statusall**. Dôležitým bodom je aj porovnanie obsahu zachytenej komunikácie pred a po nasadení zabezpečenia IPsec, kde by v prípade úspešnej konfigurácie mali byť v zázname komunikácie viditeľné šifrované ESP pakety. Overenie výstupov a tiež správnosti implementácie zabezpečenia IPsec prebieha na základe analýzy paketov vo Wiresharku alebo prostredníctvom nástroja **tcpdump** a zároveň kontrolou aktívneho IPsec spojenia. Úspešnosť úlohy je možné hodnotiť podľa schopnosti študenta jasne vysvetliť a demonštrovať rozdiely medzi nezašifrovanou a zašifrovanou komunikáciou.

2.1. Riešenie samostatnej úlohy

V rámci samostatnej úlohy majú študenti za úlohu simulovať prostredie verejnej siete, čo môžu dosiahnuť napríklad zmenou typu sieťového rozhrania v prostredí VMware (NAT alebo bridged). V tomto prostredí následne nakonfigurujú IPsec spojenie medzi klientom a serverom, tentokrát však v tunelovom režime. Ich cieľom bude zaistiť, aby celá IP komunikácia prechádzala cez šifrovaný tunel, čím sa zaistí, že šifrovaná bude nielen dátová časť paketu, ale tiež pôvodné IP záhlavie. V nástroji Wireshark by mali byť viditeľné iba šifrované ESP pakety, ktorých dátovú časť nebude

možné priamo zobrazit', resp. čítať v otvorenej podobe, čím sa preukáže úspešná implementácia tunelového režimu.

Študenti následne vykonajú meranie výkonnostných parametrov siete (latencia a priepustnosť) v rôznych režimoch – nezašifrovaná komunikácia, IPsec v transportnom a v tunelovom režime. Na základe zobrazených výsledkov vypracujú jednoduchú krátku správu, v ktorej porovnávajú výhody a nevýhody oboch bezpečnostných režimov z pohľadu výkonu a úrovne zabezpečenia. Táto časť je dôležitá nielen pre overenie praktických zručností študentov, ale aj schopnosti správne analyzovať a vhodným spôsobom interpretovať dosiahnuté výsledky.

2.2. Odpovede na kontrolné otázky

1. Čo je cieľom IP *spoofing* útoku?

- A) Zmeniť MAC adresu útočníka
- B) Získať neautorizovaný prístup predstieraním cudzej IP adresy ☒
- C) Presmerovať legitímnu komunikáciu cez vlastné zariadenie
- D) Zamedziť šifrovaniu dát medzi serverom a klientom

2. Ktoré z nasledujúcich tvrdení platia o nástroji hping3?

- A) Umožňuje simulovať IP *spoofing* a rôzne typy sieťových útokov ☒
- B) Je určený na šifrovanie komunikácie pomocou IPsec
- C) Dokáže vygenerovať vlastné TCP/IP pakety podľa špecifikácie ☒
- D) Je to nástroj na konfiguráciu VPN tunelov medzi vzdialenými sieťami

3. Vyberte nesprávne tvrdenia týkajúce sa IP *spoofing* útoku:

- A) IP spoofing automaticky zahŕňa zmenu MAC adresy ☒
- B) Má za následok zvýšenie prenosovej rýchlosti v sieti ☒
- C) Spoofovaný paket má zvyčajne neplatný kontrolný súčet ☒
- D) Využíva manipuláciu s IP záhlavím paketov

4. Aký je hlavný rozdiel medzi transportným a tunelovým režimom IPsec?

- A) V tunelovom režime sa šifruje len záhlavie IP paketu
- B) Transportný režim sa používa v bezdrôtových sieťach
- C) V transportnom režime sú šifrované len užívateľské dáta, IP záhlavie paketu ostáva nezmenené ☒
- D) Tunelový režim nemôže byť využitý v IPv6 sieti

5. Čo spôsobí nastavenie parametra `authby=secret` v súbore `ipsec.conf`?

- A) Povolenie anonymného prístupu
- B) Vypnutie autentizácie
- C) Autentizáciu pomocou predzdieľaného tajomstva (PSK) ☒
- D) Použitie certifikátov

6. Protokol AH (Authentication Header) v IPsec:

- A) Umožňuje zašifrovať celý IP paket
- B) Zaisťuje autentizáciu a integritu paketu bez šifrovania ☒
- C) Poskytuje možnosť tunelovania prenosu cez HTTPS
- D) Zaisťuje dôvernosť riadiacich informácií v IP záhlaví

7. Vyberte nesprávne tvrdenia o tunelovom režime IPsec:

- A) Zabezpečuje celý IP paket vrátane pôvodného záhlavia
- B) Nie je vhodný pre spojenie medzi dvoma bránami ☒
- C) Používa sa najmä pri zabezpečení VPN
- D) Prenáša pakety cez šifrovaný SSH tunel ☒

8. V akých situáciách je vhodné použiť IPsec v transportnom režime?

- A) Komunikácia medzi klientom a serverom v rovnakej sieti ☒
- B) Prepojenie dvoch vzdialených sietí cez internet
- C) Na zabezpečenie SSH spojenia
- D) Ochrana komunikácie medzi aplikáciami v rámci jedného servera ☒

9. Ako môže použitie IPsec ovplyvniť výkonnosť počítačovej siete?

- A) Zvýšená latencia v dôsledku šifrovania a dešifrovania paketov ☒
- B) Znížená kvalita prenosu spôsobená v dôsledku použitia NAT
- C) Väčší objem prenášaných dát v dôsledku pridaných záhlaví ☒
- D) Zablokovanie komunikácie medzi zariadeniami, ktoré nepodporujú IPsec ☒

10. V konfigurácii IPsec spojenia je parameter left používaný na určenie:

- A) Dátumu vypršania platnosti certifikátu
- B) IP adresy vzdialeného servera
- C) Lokálnej IP adresy koncového zariadenia, kde je konfigurácia definovaná ☒
- D) Zdieľaného hesla pre tunelové šifrovanie

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. Aký vplyv má použitie zabezpečenia pomocou IPsec-u na výkon siete (latenciu, rýchlosť pre-nosu dát, atď.)?

- Použitie IPsec-u môže ovplyvniť výkon siete, a to predovšetkým zvýšením latencie a miernym znížením priepustnosti. Tento efekt je spôsobený dodatočným spracovaním paketov v procesoch šifrovania a dešifrovania na

oboch koncoch komunikácie. V tunelovom režime môže byť vplyv ešte výraznejší, keďže dochádza k zapuzdreniu celého IP paketu, čím sa zväčšuje aj jeho veľkosť.

2. Vysvetlite princíp útoku IP spoofing.

- Útok IP spoofing spočíva v podvrhnutí zdrojovej IP adresy v paketoch generovaných na strane útočníka tak, aby sa tieto pakety javili, že pochádzajú z dôveryhodného zariadenia (obete). Tento typ útoku umožňuje obchádzať bezpečnostné mechanizmy a ACL pravidlá a môže byť tiež využitý ako súčasť širších útokov, napríklad DDoS.

3. Aký je rozdiel medzi transportným a tunelovým režimom IPsec?

- Pri použití IPsec v transportnom režime sa šifruje iba dátová časť paketu, pričom IP záhlavie zostáva pôvodné, nezmenené. Tento režim sa najčastejšie využíva za účelom zabezpečenia komunikácie medzi dvoma koncovými bodmi. Naopak, tunelový mód šifruje celý pôvodný IP paket vrátane záhlavia, ktorý je následne zapuzdrený do nového IP paketu s priradeným novým IP záhlavím. Využitie tunelového režimu je zväčša pre zabezpečenie komunikácie medzi dvoma sieťami alebo bránami.

4. Vysvetlite funkciu a účel použitia jednotlivých súčastí IPsec-u, a to konkrétne protokolov AH a ESP.

- Protokol AH (*Authentication Header*) zabezpečuje autentizáciu a integritu prenášaných dát vrátane IP záhlavia, pričom ale nešifruje ich obsah. Protokol ESP (*Encapsulating Security Payload*) umožňuje šifrovanie, čím zabezpečuje dôvernosť komunikácie, a zaisťuje tiež integritu, avšak len dátovej časti paketu. Za účelom dosiahnutia komplexnej ochrany prebiehajúcej komunikácie, t. j. zaistenia autentickosti, dôvernosti a integrity dátového obsahu, je vhodné používať protokoly AH a ESP súčasne.

5. Akým spôsobom je možné s využitím programu Wireshark overiť správnosť fungovania IPsec? Demonštrujte na príklade, môžete využiť časť zachytenej dátovej komunikácie.

- Vo Wiresharku je možné filtrovať komunikáciu protokolu ESP s použitím filtra **esp**. Po úspešnej konfigurácii zabezpečenia IPsec by mali byť pakety v tomto formáte nečitateľné, čo znamená, že ich obsah (dátová časť) bude zašifrovaný. V porovnaní s nezašifrovanou komunikáciou, kde sú údaje viditeľné (napr. komunikácia protokolov ICMP alebo HTTP), je to jasný dôkaz funkčného IPsec spojenia. Okrem toho je možné analyzovať aj záhlavia paketov a overiť, že ESP zabezpečuje komunikáciu medzi správnymi zariadeniami.