

Text laboratórnej úlohy

Laboratórna úloha č. 4

BEZPEČNOSŤ SIEŤOVEJ VRSTVY

Úvod k laboratórnej úlohe

Cieľom laboratórnej úlohy je zoznámiť sa s možnými hrozbami a analyzovať zraniteľnosti, ktoré ohrozujú sieťovú vrstvu počítačových sietí, predovšetkým s útokom *IP spoofing*, a tiež demonštrovať spôsoby kryptografického zabezpečenia dátových prenosov s využitím technológie IPsec.

V prvej časti laboratórnej úlohy pomocou vhodných nástrojov vo virtuálnom stroji Kali Linux najskôr realizujete **simuláciu sieťového útoku *IP spoofing*** s cieľom demonštrovať spôsob manipulácie s riadiacimi informáciami obsiahnutými v IP záhlaví prenášaného dátového paketu, a to konkrétne generovaním paketov s podvrhnutou zdrojovou IP adresou zariadenia, ktoré má byť cieľom tohto útoku. Okrem vykonania samotného útoku budete jeho priebeh monitorovať a následne analyzovať v prostredí sieťového analyzátoru Wireshark. Nakoniec sa budete venovať **implementácii bezpečnostného rozšírenia IPsec** za účelom zabezpečenia dátových prenosov na úrovni sieťovej vrstvy, a to najskôr v transportnom a neskôr i v tunelovom režime.

Požiadavky pre vypracovanie úlohy:

- software: VMware Workstation Player pre virtualizáciu staníc,
- virtuálne stroje: tri virtuálne stroje s Kali Linux.

1. Teoretický úvod

V tejto laboratórnej úlohe budete oboznámení s problematikou týkajúcou sa možných bezpečnostných hrozieb na úrovni sieťovej vrstvy referenčného modelu ISO/OSI. Budete oboznámení so základným princípom **útoku *IP spoofing***, u ktorého si vyskúšate aj jeho praktickú simuláciu. V druhej časti počítačového cvičenia sa pokúsite za účelom ochrany prebiehajúcich dátových prenosov na úrovni sieťovej vrstvy implementovať **bezpečnostné rozšírenie IPsec**, ktoré prostredníctvom kryptografických mechanizmov zaisťuje dôvernosť a tiež autentickosť IP prenášaných paketov.

1.1. Hrozby na sieťovej vrstve: IP spoofing

IP spoofing je typ sieťového útoku, ktorý spočíva vo falšovaní (resp. podvrhnutí) zdrojovej IP adresy v IP záhlaví odosielaných paketov v snahe vzbudiť dojem, že tieto pakety sú odosielané z iného zariadenia než je zariadenie útočníka. Táto technika umožňuje útočníkovi obísť určité bezpečnostné opatrenia, akými môžu byť pravidlá firewallu pre filtrovanie komunikácie alebo mechanizmy autentifikácie, ktoré používajú ako identifikátor v procese overovania identity práve IP adresu. *IP spoofing* môže byť

útočníkom využitý napr. pri realizácii DDoS útokov¹, kedy je spravidla cieľom útočníka dosiahnuť zahltenie cieľovej stanice (obete) v dôsledku generovania a odosielania falošných požiadaviek s podvrhnutými IP adresami. [1]

Základný mechanizmus IP *spoofing* útoku spočíva odosielaní takých IP paketov, v ktorých IP záhlaví útočník manuálne, cielene upraví informácie prenášané v poli zdrojovej IP adresy napr. na skutočnú IP adresu obete (t. j. konkrétneho zariadenia v sieti) alebo legitímneho servera. [1].

Vhodnou ochranou proti popísanému typu útoku môže byť použitie techník ako napr. *ingress filtering*², ktoré umožnia blokovat' príjem prichádzajúcich paketov so zdrojovou IP adresou, ktorá nezodpovedá očakávanej adrese pre dané rozhranie, alebo **použitie bezpečnostného rozšírenia IPsec (*Internet Protocol Security*)** pre zabezpečenie komunikácie pomocou mechanizmov autentizácie a šifrovania prenášaných dát. Zabezpečeniu dátových prenosov pomocou IPsec rozšírenia bude venovaná ďalšia časť tejto laboratórnej úlohy.

1.2. Technológia IPsec

IPsec (*Internet Protocol Security*) predstavuje bezpečnostné rozšírenie sieťového IP protokolu. Jedná sa o sadu protokolov, ktoré spoločne poskytujú kombináciu bezpečnostných mechanizmov pre komplexné zabezpečenie dátových prenosov prebiehajúcich na úrovni sieťovej vrstvy počítačových sietí s využitím IP protokolu. IPsec je používaný v rôznych prostrediach, spravidla sa s jeho implementáciou môžeme stretnúť napr. pri zabezpečovaní virtuálnych privátnych sietí VPN.

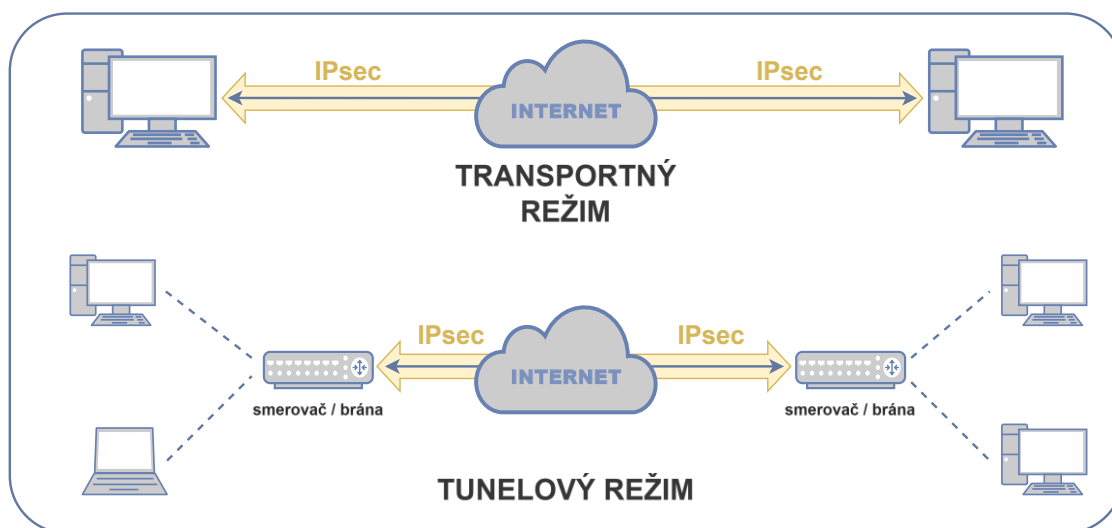
IPsec umožňuje zaistiť **integritu a autentizáciu** prenášaných IP paketov a tiež ich **šifrovanie**, a to na úrovni IP protokolu, čím chráni dátové prenosy pred neoprávneným prístupom a manipuláciou.

Protokol IPsec môže byť implementovaný pre fungovanie v dvoch základných módoch. Rozlišujeme:

- **transportný mód:** šifrovaný je iba obsah prenášaného IP paketu, pričom IP záhlavie paketu zostáva nezmenené, nie je šifrované. Transportný mód býva spravidla používaný pre zabezpečenie komunikácie medzi koncovými bodmi v sieti.
- **tunelový mód:** šifrovaný je celý pôvodný IP paket vrátane IP záhlavia, ktorý je následne vložený do nového IP paketu s novým IP záhlavím. Tento režim sa používa pri vytváraní tunelov medzi sieťami, napríklad medzi dvomi bránami.

¹ Typicky sa s IP *spoofingom* môžeme stretnúť pri realizácii SYN flood útoku, viac vid' [2], [3], alebo pri útoku ICMP flood či Smurf útoku.

² Pre viac informácií o technike *Network Ingress Filtering* vid' [5]20.



Obrázok 1.1 IPsec: transportný a tunelový režim³.

Súčasti protokolu IPsec

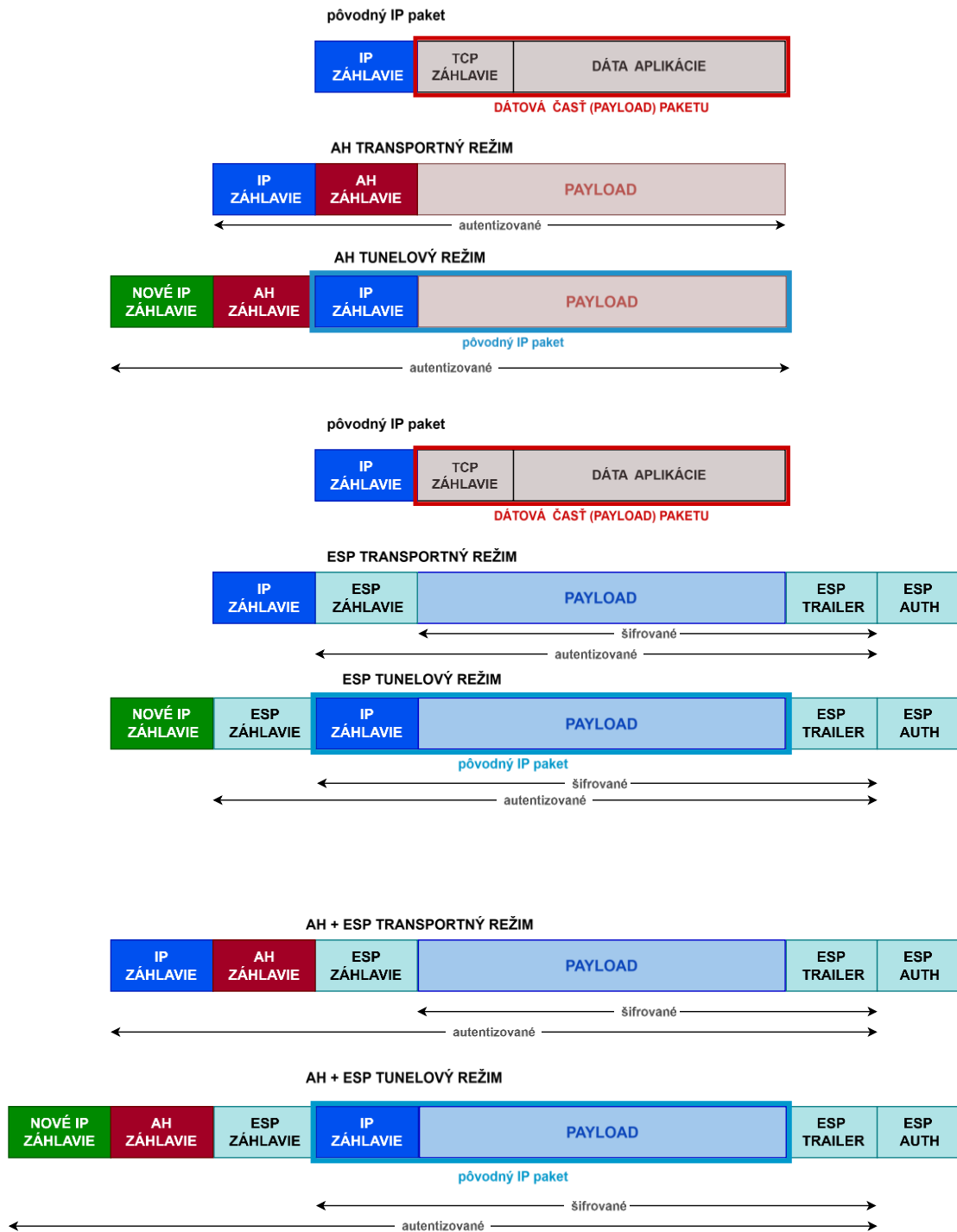
Bezpečnostné rozšírenie IPsec poskytuje možnosti komplexného zabezpečenia prenášaných dátových jednotiek prostredníctvom dvoch hlavných protokolov:

- **Authentication Header (AH):** používa sa za účelom overenia autenticity prenášaných IP paketov. Poskytuje ochranu prenášaných dát pred neoprávnenou zmenou, ale nezaist'uje ich šifrovanie, a teda ochranu informačného obsahu dát pred neoprávneným odposluchom.
- **Encapsulating Security Payload (ESP):** zaist'uje šifrovanie prenášaného dátového obsahu (resp. celého IP paketu v tunelovom režime) a súčasne zaist'uje i overenie autenticity obsahu IP paketu. Autenticita IP záhlavia je zaistená len v prípade použitia ESP súčasne s AH protokolom.

Zapuzdrenie prenášaného IP paketu, ktoré spočíva v pridaní odpovedajúcich záhlaví a zápätí nesúcich riadiace informácie, pri použití AH a/alebo ESP protokolu pre zabezpečenie ním prenášaného dátového obsahu, je znázornené pre oba prenosové IPsec režimy (transportný o tunelový) na obr. 1.2.

Podrobnejší popis technológie IPsec možno nájsť napr. v [4].

³ Prevzaté z [3].



Obrázok 1.2 Schematické znázornenie zapuzdrovania IPsec paketu.

1.3. Kali Linux a použité nástroje

V tejto laboratórnej úlohe budú pre útok IP *spoofing*, záznam a analýzu prebiehajúcej dátovej komunikácie a neskôr pre implementáciu bezpečnostného rozšírenia IPsec postupne využité nižšie uvedené nástroje:

- **hping3**: pokročilý nástroj určený ku generovaniu a odosielaniu vlastných IP paketov, ktorého použitie je vhodné napr. práve pre účely simulácie IP spoofing útoku.
- **Wireshark**: sieťový analyzátor určený pre sledovanie a záznam prebiehajúcej sieťovej komunikácie (resp. jednotlivých paketov) s možnosťou následnej analýzy zachytených paketov.
- **strongSwan**: *open-source* knižnica vhodná pre implementáciu bezpečnostného rozšírenia IPsec, používaná tiež pre konfiguráciu bezpečných VPN spojení.

Nástroj hping3

hping3 je flexibilný nástroj vhodný pre použitie ku generovaniu TCP/IP paketov. Umožňuje simuláciu rôznych typov útokov, ako sú napríklad IP spoofing, *port scanning* či rôzne typy DoS útokov, môže byť použitý tiež za účelom testovania firewallov. Pomocou nástroja **hping3** je možné vytvárať vlastné pakety s upraveným IP záhlavím a sledovať, ako cieľové systémy reagujú na neštandardné sieťové pakety (napríklad či odpovedajú na požiadavky, blokujú komunikáciu alebo generujú chyby apod.).

Pri práci s nástrojom **hping3** je možné využiť „pomocníka“ k zobrazeniu dostupných príkazov podporujúcich rozličné funkcie tohto nástroja, a to pomocou príkazu:

```
hping3 --help
```

Nástroj **hping3** poskytuje tiež možnosť pre overenie dostupnosti cieľovej služby (napr. webového servera). Pomocou nižšie uvedeného príkazu je možné overiť, či je testovaná služba aktuálne dostupná a či firewall umožňuje, resp. neblokuje prístup k uvedenému portu:

```
sudo hping3 -S 192.168.126.130 -p 80 -c 3
```

kde prepínač **-S** zaistí odoslanie postupne **troch** TCP/IP paketov s nastaveným príznakom **SYN = 1** na **port 80** cieľového zariadenia s uvedenou **IP adresou**.

Pre účely simulácie IP *spoofingu* je možné **hping3** použiť nasledovne:

```
sudo hping3 -a 192.168.126.129 -S 192.168.126.130 -p 80 -c 5
```

Uvedený príkaz vygeneruje celkom **päť** TCP SYN paketov smerovaných na **port 80** cieľovej IP adresy **192.168.126.130**, pričom do záhlavia týchto paketov bude vložená (pomocou prepínača **-a**) falošná zdrojová IP adresa s hodnotou **192.168.126.129**.

Vysvetlenie použitých prepínačov príkazu a ich parametrov:

- **sudo** spustenie nástroja s oprávneniami správcu,
- **hping3** spustenie príslušného nástroja,
- **-a 192.168.126.129** nastavenie falošnej (*spoofovanej*) zdrojovej IP adresy,
- **-S** nastavenie TCP príznaku SYN⁴ na hodnotu 1,
- **-p 80** cieľový port, typicky používaný pre HTTP,
- **-c 5** počet odoslaných paketov (v tomto prípade 5).

Wireshark

Wireshark je pokročilý sieťový analyzátor, ktorý umožňuje zachytávať, vizualizovať a analyzovať sieťovú prevádzku v reálnom čase. Je vhodný pre analýzu komunikačných protokolov a obsahu prenášaných dátových jednotiek, detekciu podozrivých paketov a identifikáciu sieťových problémov. Tento nástroj ponúka možnosť filtrovať zachytenú komunikáciu na základe rôznych kritérií (napr. zdrojová/destinovaná IP, protokol, port).

S nástrojom Wireshark ste sa oboznámili už v predošlom cvičení, v rámci ktorého ste si tiež vyskúšali aj jeho praktické použitie. Pre potreby praktickej časti tejto úlohy je nižšie v tabuľke 1.1 uvedený prehľad niekoľkých možných filtrov pre selektívne zobrazenie vhodných paketov zo zaznamenatej komunikácie.

Tabuľka 1.1 Wireshark: príklady použitých filtrov komunikácie.

účel	filter
zobrazenie všetkých paketov ICMP protokolu:	icmp
sledovanie dátovej komunikácie medzi dvoma IP adresami:	ip.src == 192.168.126.129 && ip.dst == 192.168.126.130
zobrazenie všetkých ESP⁵ paketov:	esp

⁴ Príznakový bit SYN = 1 v záhlaví TCP protokolu indikuje zahájenie, resp. vytvorenie TCP spojenia medzi koncovými bodmi komunikácie.

⁵ ESP = *Encapsulating Security Payload* – súčasť rozšírenia IPsec, protokol pre šifrovanie komunikácie.

Strongswan

strongSwan je *open-source* implementácia protokolov IPsec a IKE (*Internet Key Exchange*)⁶, ktorá umožňuje vytvoriť bezpečné prepojenie dvoch alebo viacerých uzlov, resp. zariadení, na sieťovej vrstve. Podporuje IPv4 aj IPv6, transportný aj tunelový režim IPsec, a v rámci protokolu IKE podporuje statickú i dynamickú výmenu kľúčov.

Pre konfiguráciu bezpečnostného rozšírenia IPsec k zabezpečeniu sieťovej komunikácie je kľúčová práca s nižšie uvedenými konfiguračnými súborami:

- **etc/ipsec.conf** – hlavný konfiguračný súbor pre definíciu spojení, (nastavenie napr. IP adries, režimu prenosu, spôsobu autentifikácie)
- **etc/ipsec.secrets** – konfiguračný súbor obsahujúci zdieľané tajomstvá alebo kľúče potrebné pre autentifikáciu komunikujúcich strán.

Pre prácu s knižnicou strongSwan je nutné spustiť samotnú službu pomocou príkazu:

```
sudo systemctl start strongswan
```

Knižnica strongSwan umožňuje vytváranie IPsec spojení, resp. tunelov medzi dvoma koncovými bodmi komunikácie. Spustenie, resp. manuálne vytvorenie zabezpečeného spojenia je možné príkazom:

```
sudo ipsec up <názov_spojenia>
```

Taktiež je možné zobrazit' stav implementovaných IPsec tunelov vytvorených medzi zariadeniami:

```
sudo ipsec statusall
```

⁶ IKE (*Internet Key Exchange*) je protokol používaný v rámci IPsec spojenia pre bezpečnú výmenu kryptografických kľúčov a vyjednanie bezpečnostných parametrov medzi dvoma komunikujúcimi stranami. Jeho cieľom je vytvoriť a spravovať tzv. Security Associations (SA), ktoré definujú, aké kryptografické mechanizmy budú použité k zaisteniu dôvernosti a integrity prenášaných dát. V rámci knižnice strongSwan predstavuje IKE nevyhnutnú súčasť, ktorá zaisťuje bezpečné nadviazanie IPsec spojenia a následné obnovenie a/alebo ukončenie vytvoreného tunela.

2. Praktická časť

V rámci praktickej časti počítačového cvičenia bude vytvorená **simulácia útoku IP Spoofing** pomocou nástroja **hping3** s následnou analýzou komunikácie cez **Wireshark**. Simulovaný útok bude prebiehať vo virtuálnej sieti pozostávajúcej z troch virtuálnych strojov s Kali Linux (klient, server a útočník), ktorej topológia je schematicky znázornená nižšie na obr. 2.1. Komunikácia medzi uvedenými virtuálnymi strojmi prebieha skrz virtuálny prepínač VMware virtual switch, ako je znázornené na uvedenom obrázku.

Cieľom IP *spoofingu* môže byť v dôsledku generovania IP paketov s podvrhnutou zdrojovou IP adresou vyvolanie nadväzujúceho DDoS útoku s cieľom zapríčiniť nemožnosť plnohodnotného fungovania zariadenia, ktoré je cieľom (tzv. obeťou) zamýšľaného útoku. Následne si v nadväzujúcej ďalšej časti za účelom zabezpečenia prebiehajúcich dátových prenosov na úrovni sieťovej vrstvy vyskúšate **konfiguráciu bezpečnostného rozšírenia IPsec**, ktoré zaistuje v rámci komunikácie medzi dvoma zariadeniami dôvernosť prenášaných IP paketov prostredníctvom šifrovania a tiež ich autentickosť a odolnosť voči narušeniu integrity.

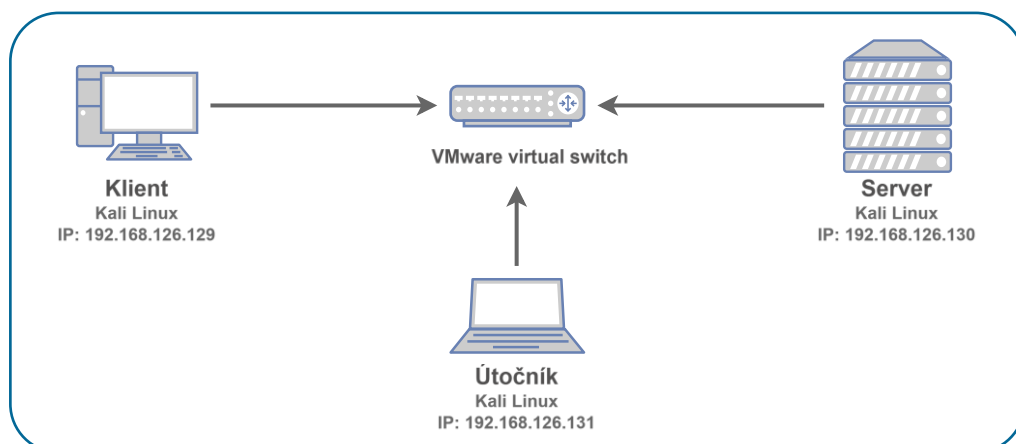
2.1. Topológia virtuálnej siete a nastavenie virtuálnych strojov

Použité virtuálne stroje:

- **obet' (klient):** bežný počítač v sieti, cieľ útoku.
- **server:** poskytovateľ sieťovej služby (napr. webserver, gateway).
- **útočník:** vykonáva IP *spoofing*, generuje IP pakety s falošnou zdrojovou IP adresou.

Sieťová konfigurácia:

- obet': 192.168.126.129
- server: 192.168.126.130
- útočník: 192.168.126.131



Obrázok 2.1 Topológia siete laboratórnej úlohy.

Všetky virtuálne stroje musia byť prepojené v rovnakej virtuálnej podsieti pomocou sieťového režimu **Host-only** alebo **NAT**, aby mohlo byť na VM predstavujúcim „útočníka“ realizované zachytávanie dátových prenosov (komunikácie) medzi klientom a serverom.

2.2. Zoznámenie sa s použitými nástrojmi

Prehľad základných príkazov pre jednotlivé používané nástroje

- **hping3**: spustenie simulácie IP spoofingu:

```
sudo hping3 -a <zdroj_IP> -S <ciel_IP> -p <port> -c <pakety>
```

- **Wireshark**: za účelom prehľadnejšej analýzy zachytenej dátovej komunikácie je doporučené využívanie vhodných filtrov pre zobrazenie vybraných paketov, napr. na základe konkrétnej zdrojovej a/alebo cieľovej IP adresy:

```
ip.src == 192.168.126.129 && ip.dst == 192.168.126.130
```

- **strongSwan**: pre konfiguráciu zabezpečeného IPsec pripojenia medzi klientom a serverom pomocou knižnice Strongswan bude nutná vhodná modifikácia základných konfiguračných súborov, a to konkrétne:
 - **/etc/ipsec.conf** (hlavný konfiguračný súbor IPsec)
 - **/etc/ipsec.secrets** (súbor obsahujúci autentifikačné kľúče)

2.3. Postup pre vypracovanie laboratórnej úlohy


A) Príprava prostredia

Spustenie virtuálnych strojov:

- Otvorte VMware Workstation Pro (umiestnený na ploche).
- Spustite postupne všetky tri virtuálne stroje (klient, server, útočník).
- Uistite sa v správnosti konfigurácie sieťových parametrov, overte priradenie IP adries zariadeniam.
- Prihláste sa do prostredia Kali Linux na VM útočníka.

VM „útočník“	– prihlasovacie údaje: Username: kali, Password: kali
VM „klient“	– prihlasovacie údaje: Username: klient, Password: kali
VM „server“	– prihlasovacie údaje: Username: server, Password: kali

Overenie sieťovej konektivity:

- Otvorte **terminál** (kliknite na ikonu terminálu  v záhlaví horného pracovného panelu alebo stlačte Ctrl + Alt + T).
- Na jednotlivých VMs si zobrazte priradené IP adresy (na rozhraní **eth0**):

```
ip a
```

- Z klienta odošlite testovaciu požiadavku (ping) a vyskúšajte pripojenie na server pomocou príkazu:


```
ping <ip_adresa_servera>
```

- Ak klientovi prichádza odpoveď **ping echo reply** zo strany servera, sieťová komunikácia medzi zariadeniami funguje.
- Obdobným spôsobom overte možnosť spojenia v opačnom smere komunikácie.

B) IP spoofing útok pomocou hping3

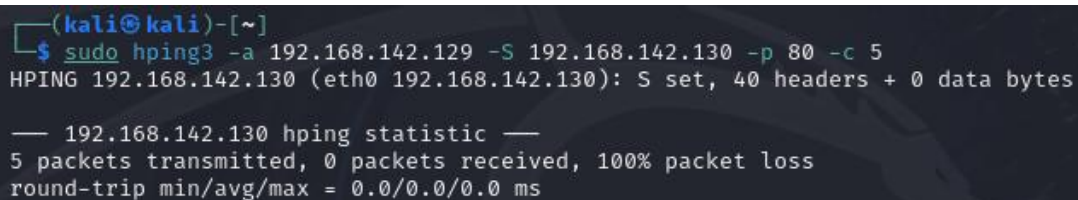
Pomocou nástroja hping3 na VM útočníka je možné simulovať IP *spoofing* útok generovaním IP paketov s podvrhnutou zdrojovou IP adresou. Cieľom je odosielať pakety vzbudzujúce dojem, akoby boli odoslané samotným klientom. Týmto útokom je možné overiť, že cieľové zariadenie (v tomto prípade server) nedokáže rozpoznať skutočného odosielateľa (= útočníka). Prebiehajúca komunikácia vo vytvorenej sieti bude monitorovaná pomocou nástroja Wireshark.

Použitie nástroja hping3

- Na stroji útočníka otvorte terminál kliknutím na ikonu  umiestnenú v záhlaví hlavného pracovného okna alebo v menu zvolíte **Applications > System Tools > Terminal**. Otvorí sa okno s príkazovým riadkom.
- Pre spustenie IP *spoofingu* zadajte príkaz:

```
sudo hping3 -a 192.168.126.129 -S 192.168.126.130 -p 80 -c 5
```

Po zadaní príkazu bude zahájená simulácia útoku, resp. generovanie dátových paketov, ktoré sa budú javiť, ako keby boli odosielané zo zariadenia klienta.



```
(kali@kali)-[~]
$ sudo hping3 -a 192.168.142.129 -S 192.168.142.130 -p 80 -c 5
HPING 192.168.142.130 (eth0 192.168.142.130): S set, 40 headers + 0 data bytes

— 192.168.142.130 hping statistic —
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Obrázok 2.2 Spustenie IP spoofing útoku v termináli Kali Linux.

Sledovanie prichádzajúcej komunikácie (server) vo Wiresharku

- Na serveri spustíte **Wireshark** pomocou príkazu:

```
sudo wireshark &
```

Prepínač '**sudo**' spustí nástroj Wireshark s oprávneniami administrátora, čo je nevyhnutné pre zachytávanie sieťovej prevádzky v Kali Linux.

- V hlavnom okne vyberte sieťové rozhranie **eth0** – dvojité kliknutím spustíte zachytávanie (alebo kliknite na **Start Capturing Packets** v záhlaví panelu s nástrojmi).
- Do okna pre filtrovanie komunikácie zadajte:

```
ip.src == 192.168.126.129 && ip.dst == 192.168.126.130
```

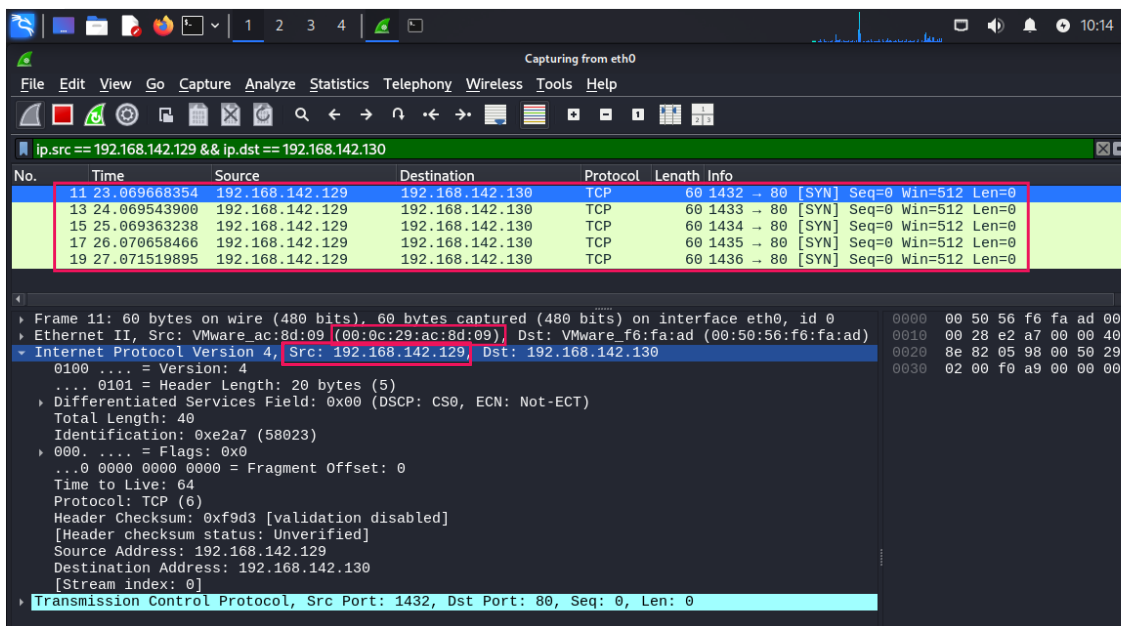
túto voľbu potvrdíte stlačením **Enter**.

Použitie uvedeného filtra zaistí, že spomedzi všetkých zachytených dátových jednotiek prenesených v rámci komunikácie cez zvolené rozhranie budú zobrazené len pakety údajne „pochádzajúce od klienta“, t. j. pakety vyhovujúce filtru **ip.src == 192.168.126.129** a ďalej tiež pakety, ktoré majú byť doručené na server t. j. pakety vyhovujúce druhému zo zadanych filtrov **ip.dst == 192.168.126.130**. V skutočnosti sa však jedná o pakety generované na strane útočníka nástrojom **hping3**.

- Kliknutím pravým tlačidlom myši na niektorý zo zobrazených paketov a následným výberom možnosti „**Follow > TCP Stream**“ je možné zobrazit' celkový prehľadný priebeh spojenia medzi komunikujúcimi zariadeniami.
- Pre podrobnejšiu analýzu komunikácie kliknite na vybraný paket a v dolnej časti sledovaného okna Wiresharku si zobrazte sekciu **Internet Protocol Version 4**, kde si môžete bližšie zobrazit' konkrétne hodnoty *Source IP* (zdrojová) a *Destination IP* (cieľová adresa).

Zdrojová IP adresa by mala mať hodnotu 192.168.126.129 odpovedajúcu VM klienta, hoci bol príslušný paket v skutočnosti odoslaný zo stanice útočníka (viď zachytená komunikácia na obr. 2.3).

- Pre overenie úspešnosti IP spoofingu ďalej analyzujte fyzické MAC adresy zariadení, z ktorých boli jednotlivé pakety odoslané (zobrazenie v sekcii **Ethernet II**).



Obrázok 2.3 Ukážka zachytenej komunikácie po spustení útoku IP spoofing (server).

C) Zabezpečenie komunikácie s využitím IPsec

V nasledujúcej časti laboratórnej úlohy si vyskúšate prácu s knižnicou **strongSwan** podporujúcu implementáciu IPsec-u.

Konfigurácia IPsec v transportnom režime

- Na zariadení klienta a na serveri spustíte inštaláciu knižnice **strongSwan**:

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

Použitie uvedeného príkazu zabezpečí inštaláciu balíka **strongSwan**, ktorý obsahuje potrebné komponenty pre vytvorenie zabezpečeného IPsec spojenia. Aktualizácia balíčkov v Kali Linux (príkaz: **apt update**) zabezpečí, že sa použijú aktuálne dostupné verzie.

- Na oboch zariadeniach (klient a server) upravte konfiguračný súbor **/etc/ipsec.conf** – pre editáciu súborov v textovom režime môžete využiť napr. editor **nano**, a to nasledovne:

- pre presun do adresára, kde sa príslušný konfiguračný súbor nachádza, môžete v otvorenom terminálovom okne použiť príkaz:

```
cd /etc
```

- následne otvorte súbor na úpravu:

```
sudo nano ipsec.conf
```

- do súboru vložte nasledujúcu konfiguráciu:

```
conn test
    left=192.168.126.129          # klient (aktuálny VM)
    right=192.168.126.130        # server (protistrana)
    authby=secret
    auto=start
    ike=aes256-sha1-modp1024
    esp=aes256-sha1
    keyexchange=ikev2
```

!! Uvedená konfigurácia sa týka nastavení IPsec na strane klienta.

Týmto nastavením sa definujú parametre zabezpečeného spojenia medzi vašim klientom (**left**) a serverom (**right**). Parameter **authby=secret** určuje, že sa bude pre autentizáciu komunikujúcich strán používať zdieľané tajomstvo PSK (*pre-shared key*). Ďalej nastavujeme výmenu kľúčov pomocou IKEv2, a špecifikujeme šifrovacie a autentifikačné algoritmy pre fázu IKE (**ike**) aj samotné dáta (**esp**). Parameter **auto=start** zabezpečí automatické nadviazanie definovaného IPsec spojenia pri štarte služby.

- Po úprave konfigurácie stlačte kombináciu kláves **Ctrl + O** (uloženie), potvrdíte názov súboru klávesou **Enter** a následne ukončíte textový editor **nano** pomocou kombinácie **Ctrl + X**.
- Alternatívne môžete úpravu konfigurácie ukončiť stlačením **Ctrl + X**, následne pre potvrdenie uloženia vykonaných zmien stlačte **Y** (ako Yes/áno), a nakoniec potvrdíte stlačením **Enter**. Týmto spôsobom sa zmeny uložia a editor sa zároveň zatvorí.
- Ďalej upravte konfiguračný súbor **/etc/ipsec.secrets**:

```
sudo nano ipsec.secrets
```

- do ktorého vložíte nasledovné:

```
192.168.126.129 192.168.126.130 : PSK "tajneheslo"
```

Tento riadok definuje spoločný zdieľaný kľúč (PSK), ktorý bude použitý na autentizáciu medzi dvoma zariadeniami s uvedenými IP adresami (medzi klientom a serverom). **Je dôležité zadať na oboch stranách komunikácie identický kľúč**, inak proces autentizácie neprebehne úspešne a zabezpečené

spojenie nebude možné nadviazať. PSK predstavuje jednoduchý spôsob autentifikácie, ktorý je vhodný pre menšie a testovacie prostredia, no menej bezpečný pre rozsiahle produkčné nasadenie.

- Po úprave súboru opäť použite kombináciu **Ctrl + O** → **Enter** → **Ctrl + X** alebo alternatívne **Ctrl + X** → **Y** → **Enter** pre potvrdenie a uloženie vykonaných zmien.
- Po zmene v konfigurácii je potrebné službu reštartovať, príp. môžete overiť, či je služba po spustení aktívna:

```
sudo systemctl restart strongswan-starter  
sudo systemctl status strongswan-starter
```

- Obdobne postupujte pri inštalácii strongSwan a konfigurácii zabezpečeného IPsec spojenia aj na strane serveru, pričom dbajte na správne definovanie jednotlivých parametrov (IP adries) pri úprave konfigurácie.

Pripojenie a overenie konfigurácie IPsec

- Na oboch zariadeniach (klient i server) spustite IPsec a následne vytvorte medzi nimi zabezpečené spojenie na základe predchádzajúcej konfigurácie:

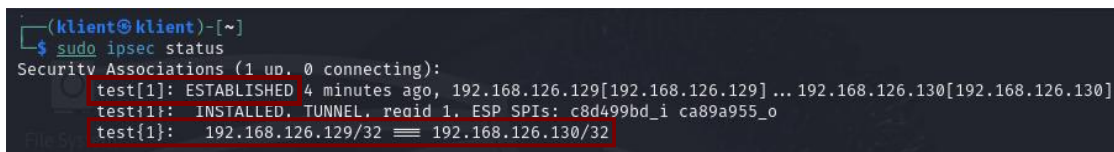
```
sudo ipsec start
```

```
sudo ipsec up test
```

- Zobrazte si stav vytvoreného spojenia pomocou príkazu:

```
sudo ipsec status
```

V prípade správnej konfigurácie, by malo byť spojenie v stave **ESTABLISHED** (viď obr. 2.4). Pre zobrazenie podrobnejších informácií o spojení je možné alternatívne použiť príkaz `ipsec statusall`.



```
(klient@klient)-[~]  
$ sudo ipsec status  
Security Associations (1 up, 0 connecting):  
test[1]: ESTABLISHED 4 minutes ago, 192.168.126.129[192.168.126.129] ... 192.168.126.130[192.168.126.130]  
test[1]: INSTALLED, TUNNEL, reqid 1, ESP SPIs: c8d499bd_i ca89a955_o  
test{1}: 192.168.126.129/32 == 192.168.126.130/32
```

Obrázok 2.4 Overenie vytvorenia IPsec spojenia (klient).

- Dôležité je overiť tiež to, či komunikácia medzi zariadeniami klient ↔ server skutočne prebieha cez vytvorený IPsec tunel.
- Na serveri opäť otvorte nástroj Wireshark a spustite zachytávanie sieťovej prevádzky na rozhraní `eth0`.

- V termináli (server) s pomocou nástroja `tcpdump` sledujte komunikáciu na strane serveru, ktorá bude vykazovať známky používania IPsec tunela:

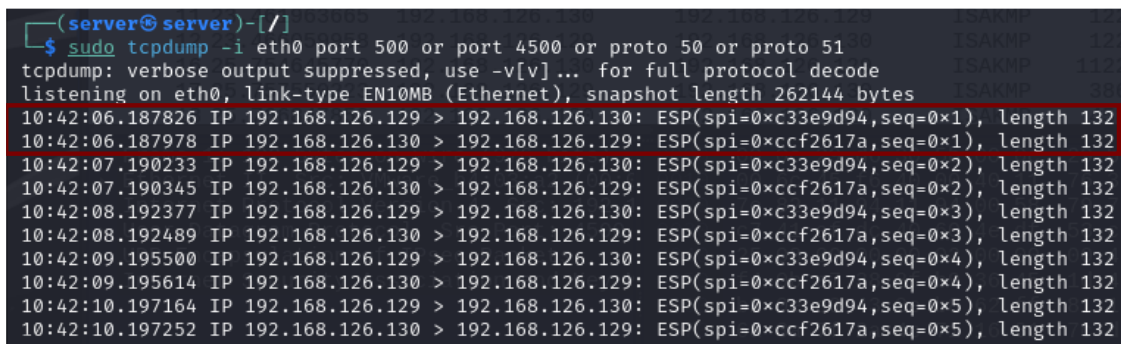
```
sudo tcpdump -i eth0 port 500 or port 4500 or proto 50 or proto 51
```

Použitie `tcpdump` s uvedenými parametrami zaistí sledovanie prevádzky súvisiacej s IPsec: **UDP port 500 (IKE), protokol 50 (ESP), protokol 51 (AH)**. Pre prípad použitia prekladu adres je vhodné overiť aj komunikáciu cez UDP port 4500 (NAT-T).

- Z klientskeho VM odošlite `ping` na server:

```
ping 192.168.126.130
```

- Na serveri sledujte jednak výstup nástroja `tcpdump` v otvorenom okne terminálu, a súčasne i záznam komunikácie vo Wiresharku.
- Nižšie uvedený výpis dokazuje, že vytvorený **šifrovaný IPsec tunel funguje** a teda že medzi klientom a serverom prebieha **výmena šifrovaných ESP paketov** (protokol 50) práve cez tento tunel – podrobnejšie viď obr. 2.5.



Obrázok 2.5 Výpis nástroja `tcpdump`: sledovanie komunikácie prostredníctvom vytvoreného IPsec tunela (server).

- Pre zobrazenie šifrovanej komunikácie vo Wiresharku je vhodné použiť filter:

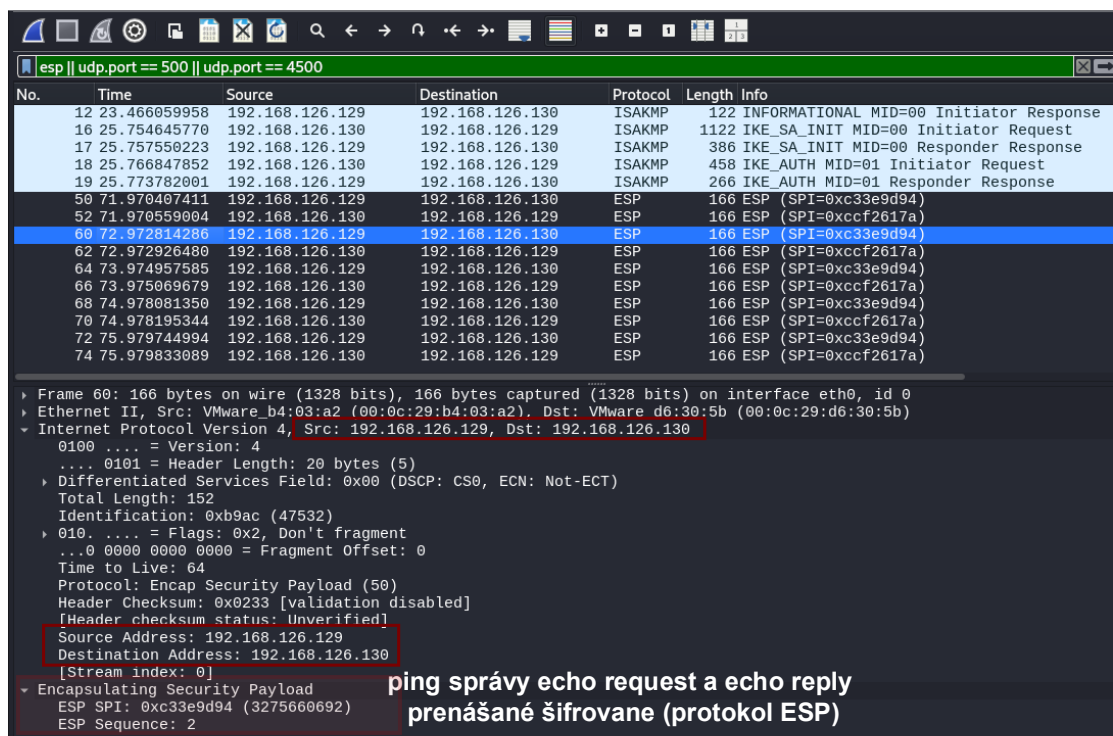
```
esp || udp.port == 500 || udp.port == 4500
```

Použitie uvedeného filtra zobrazí:

- **ESP pakety** (protokol 50),
- **IKE komunikáciu** (na porte UDP 500 – vytvorenie IPsec tunela),
- **IKE cez NAT-T** (UDP port 4500 – ak sa IPsec prispôsobuje NAT-u).

- **Ďalšia možnosť overenia:**

Pomocou nástroja hping3 opäť spustíte na VM útočníka simuláciu útoku IP Spoofing a sledujte, či sú odosielané pakety od útočníka na strane serveru odmietnuté. Správne nakonfigurované spojenie by malo zabrániť prijatiu neautentifikovanej komunikácie. Pribeh komunikácie sledujte tiež pomocou nástroja Wireshark.



Obrázok 2.6 Ukážka zachytenej komunikácie – prenos cez šifrovaný IPsec tunel (server).

2.4. Samostatná úloha

A) Implementácia IPsec v tunelovom režime

V poslednej časti úlohy si samostatne vyskúšate praktické nasadenie bezpečnostného rozšírenia **IPsec v tunelovom režime** pre zabezpečenie komunikácie odosielanej cez simulovanú „verejnú sieť“.

Cieľom vašej samostatnej práce bude najskôr simulovať vlastnú verejnú sieť a následne správnym spôsobom nakonfigurovať IPsec rozšírenie v tunelovom režime pre zabezpečenie komunikácie medzi klientom a serverom.

Po implementácii otestujete a porovnáte výkon siete pri použití transportného a tunelového IPsec režimu, a to najmä z pohľadu latencie komunikácie, spoľahlivosti prenosu a stability vytvoreného spojenia.

Zachytenú komunikáciu analyzujte vo Wiresharku a porovnajte rozdiely medzi oboma režimami. Pri analýze venujte pozornosť aj štruktúre paketov (napr. viditeľnosť vnútorných záhlaví, šifrovanie obsahu a použité protokoly).

3. Záver

V tejto laboratórnej úlohe ste sa zoznámili s problematikou bezpečnosti sieťovej vrstvy počítačových sietí a v tejto súvislosti tiež s rizikami spojenými s podvrhnutím IP adresy (tzv. IP spoofing), čo predstavuje častý spôsob narušenia integrity alebo dôvernosti komunikácie na sieťovej vrstve.

V praktickej časti ste **pomocou nástroja hping3** realizovali simuláciu útoku, ktorý ilustruje, akým spôsobom je možné oklamať cieľové zariadenie použitím falošnej zdrojovej IP adresy uvedenej v záhlaví odosielaných dátových jednotiek. Následne ste si vyskúšali **praktickú implementáciu rozšírenia IPsec**, ktorý umožňuje komplexné zabezpečenie IP komunikácie, a to vrátane šifrovania dát, autentizácie a zaistenia integrity prenosu. Porovnaním transportného a tunelového IPsec režimu ste získali prehľad o rôznych spôsoboch ochrany dátovej prevádzky a taktiež o ich vplyve na výslednú podobu paketov či celkový výkon počítačovej siete.

3.1. Kontrolné otázky

1. Čo je cieľom IP *spoofing* útoku?

- A) Zmeniť MAC adresu útočníka
- B) Získať neautorizovaný prístup predstieraním cudzej IP adresy
- C) Presmerovať legítimnú 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

4. Literatúra

- [1] CLOUDFARE. *IP Spoofing Explained*. Cloudflare.com [online]. [cit. 2024-11-26]
Dostupné z: <https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/>
- [2] CLOUDFARE. *SYN flood attack*. [online]. 2023. [cit. 2024-11-26]. Dostupné z:
<https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/>
- [3] KAVISANKAR, L. and CHELLAPPAN, C. *A mitigation model for TCP SYN flooding with IP spoofing*. In: 2011 International Conference on Recent Trends in Information Technology (ICRTIT). 2011. s. 251–256. [online]. Dostupné z:
<https://ieeexplore.ieee.org/document/5972435> [cit. 2024-11-26].
- [4] CISCO. IPsec Overview. [online]. 2023 [cit. 2025-04-13]. Dostupné z:
https://www.cisco.com/c/en/us/td/docs/net_mgmt/vpn_solutions_center/2-0/ip_security/provisioning/guide/IPsecPG1.html
- [5] FERGUSON, P. *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*. [Internet Requests for Comments]. RFC Editor, 2000. [cit. 2024-11-26]. Dostupné z:
<https://datatracker.ietf.org/doc/html/rfc2827>
- [6] STRONGSWAN. *strongSwan – the OpenSource IPsec-based VPN Solution*. [online]. 2024 [cit. 2025-04-20]. Dostupné z: <https://www.strongswan.org/>