

Text laboratorní úlohy

Laboratorní úloha č. 4

BEZPEČNOST SÍŤOVÉ VRSTVY

Úvod k laboratorní úloze

Cílem laboratorní úlohy je seznámit se s možnými hrozbami a analyzovat zranitelnosti ohrožující síťovou vrstvu počítačových sítí, zejména s útokem IP *spoofing*, a také demonstrovat způsoby kryptografického zabezpečení datových přenosů využitím technologie IPsec.

V první části laboratorní úlohy pomocí vhodných nástrojů ve virtuálním stroji Kali Linux nejprve provedete simulaci síťového útoku IP spoofing za účelem demonstrace manipulace s řídicími informacemi obsaženými v IP záhlaví přenášeného datového paketu, konkrétně generováním paketů s podvrženou zdrojovou IP adresou zařízení, které má být cílem tohoto útoku. Kromě samotného provedení útoku budete sledovat a následně analyzovat jeho průběh v prostředí síťového analyzátoru Wireshark. Nakonec se zaměříte na implementaci bezpečnostního rozšíření IPsec za účelem zabezpečení datových přenosů na úrovni síťové vrstvy, a to nejprve v transportním a později i v tunelovém režimu.

Požadavky pro vypracování úlohy:

- software: VMware Workstation Player pro virtualizaci stanic,
- virtuální stroje: tři virtuální stroje s Kali Linux.

1. Teoretický úvod

V této laboratorní úloze budete seznámeni s problematikou možných bezpečnostních hrozeb na úrovni síťové vrstvy referenčního modelu ISO/OSI. Seznámíte se se základním principem **útoku IP spoofing**, jehož simulaci si také prakticky vyzkoušíte. Ve druhé části cvičení se pokusíte za účelem ochrany probíhajících datových přenosů na úrovni síťové vrstvy implementovat **bezpečnostní rozšíření IPsec**, které pomocí kryptografických mechanismů zajišťuje důvěrnost a také autentizaci IP paketů.

1.1. Hrozby na síťové vrstvě: IP spoofing

IP spoofing je typ síťového útoku spočívající ve falšování (podvržení) zdrojové IP adresy v IP záhlaví odesílaných paketů s cílem vyvolat dojem, že pakety pocházejí z jiného zařízení než z útočnickova. Tato technika umožňuje útočnickovi obejít určitá bezpečnostní opatření, jako jsou pravidla firewallu pro filtrování komunikace nebo autentifikační mechanismy, které používají jako identifikátor při ověřování identity právě IP adresu. IP spoofing může útočník využít například při realizaci DDoS útoků, kdy je cílem útočníka zpravidla zahlcení cílové stanice (oběti) generováním a odesíláním falešných požadavků s podvrženými IP adresami. [1]

Základní mechanismus IP *spoofing* útoku spočívá v odesílání IP paketů, ve kterých útočník manuálně a cíleně upraví informace přenášené v poli zdrojové IP adresy na IP adresu oběti (konkrétního zařízení v síti) nebo legitimního serveru. [1].

Vhodnou ochranou proti popsanému typu útoku může být použití technik jako např. *ingress filtering*¹, které blokují příjem příchozích paketů se zdrojovou IP adresou, která neodpovídá očekávané adrese pro dané rozhraní, nebo **použití bezpečnostního rozšíření IPsec (*Internet Protocol Security*)** pro zabezpečení komunikace pomocí autentizace a šifrování přenášených dat. Zabezpečení datových přenosů pomocí IPsec bude podrobněji rozebráno v další části úlohy.

1.2. Technologie IPsec

IPsec (*Internet Protocol Security*) představuje bezpečnostní rozšíření síťového IP protokolu. Jedná se o sadu protokolů, které společně poskytují kombinaci bezpečnostních mechanismů pro komplexní zabezpečení datových přenosů probíhajících na úrovni síťové vrstvy počítačových sítí využívajících IP protokol. IPsec je používán v různých prostředích, zpravidla se s jeho implementací setkáme například při zabezpečení virtuálních privátních sítí VPN.

IPsec zajišťuje **integritu, autentizaci a šifrování** přenášených IP paketů, čímž chrání datové přenosy před neoprávněným přístupem a manipulací.

Protokol IPsec může být implementován ve dvou základních režimech:

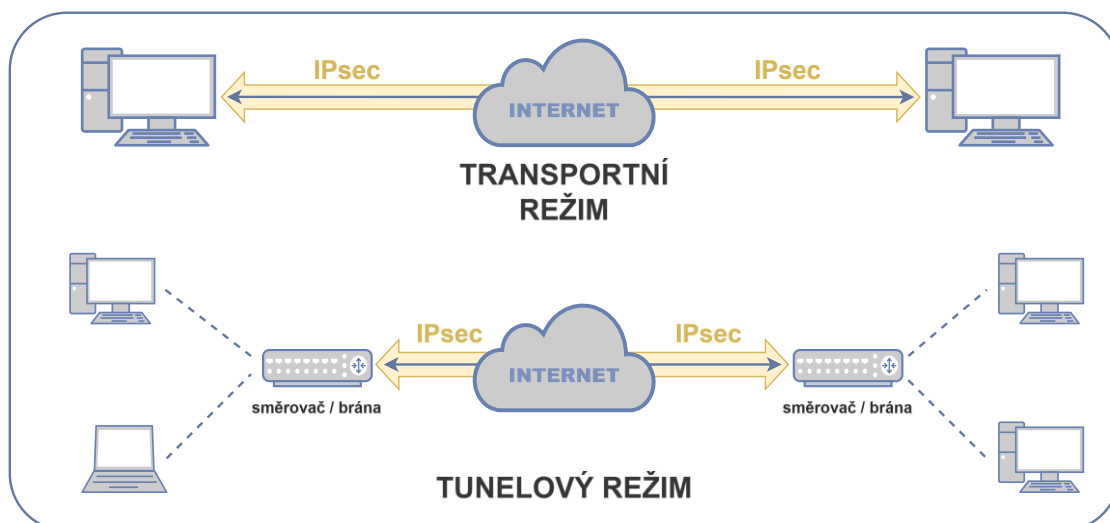
- **transportní mód:** šifruje se pouze obsah přenášeného IP paketu, přičemž IP záhlaví zůstává nezměněné. Transportní mód se zpravidla používá pro zabezpečení komunikace mezi koncovými zařízeními v síti.
- **tunelový mód:** šifruje se celý původní IP paket včetně jeho záhlaví, který je posléze vložen do nového IP paketu s novým IP záhlavím. Tento režim se využívá při vytváření tunelů mezi sítěmi, např. mezi dvěma bránami.

Součásti protokolu IPsec

Bezpečnostní rozšíření IPsec poskytuje možnosti komplexního zabezpečení přenášených datových jednotek prostřednictvím dvou hlavních protokolů:

- **Authentication Header (AH):** používá se k ověření autenticity IP paketů. Zajišťuje ochranu proti neoprávněné změně dat, nešifruje však obsah paketů, a tedy nechrání obsah dat před neoprávněným odposlechem.
- **Encapsulating Security Payload (ESP):** zajišťuje šifrování přenášeného datového obsahu (resp. celého IP paketu v tunelovém režimu) a současně i ověření autenticity obsahu IP paketu. Pro zajištění autentičnosti IP záhlaví je potřeba používat ESP současně s AH protokolem.

¹ Pro více informací o technice *Network Ingress Filtering* viz [5]20.



Obrázek 1.1 IPsec: transportní a tunelový režim ².

Zapouzdření přenášeného IP paketu, které spočívá v přidání odpovídajících záhlaví a zápatí nosoucích řídicí informace, při použití AH a/nebo ESP protokolu pro zabezpečení přenášeného datového obsahu, je znázorněno pro oba režimy IPsec (transportní i tunelový) na obr. 1.2.

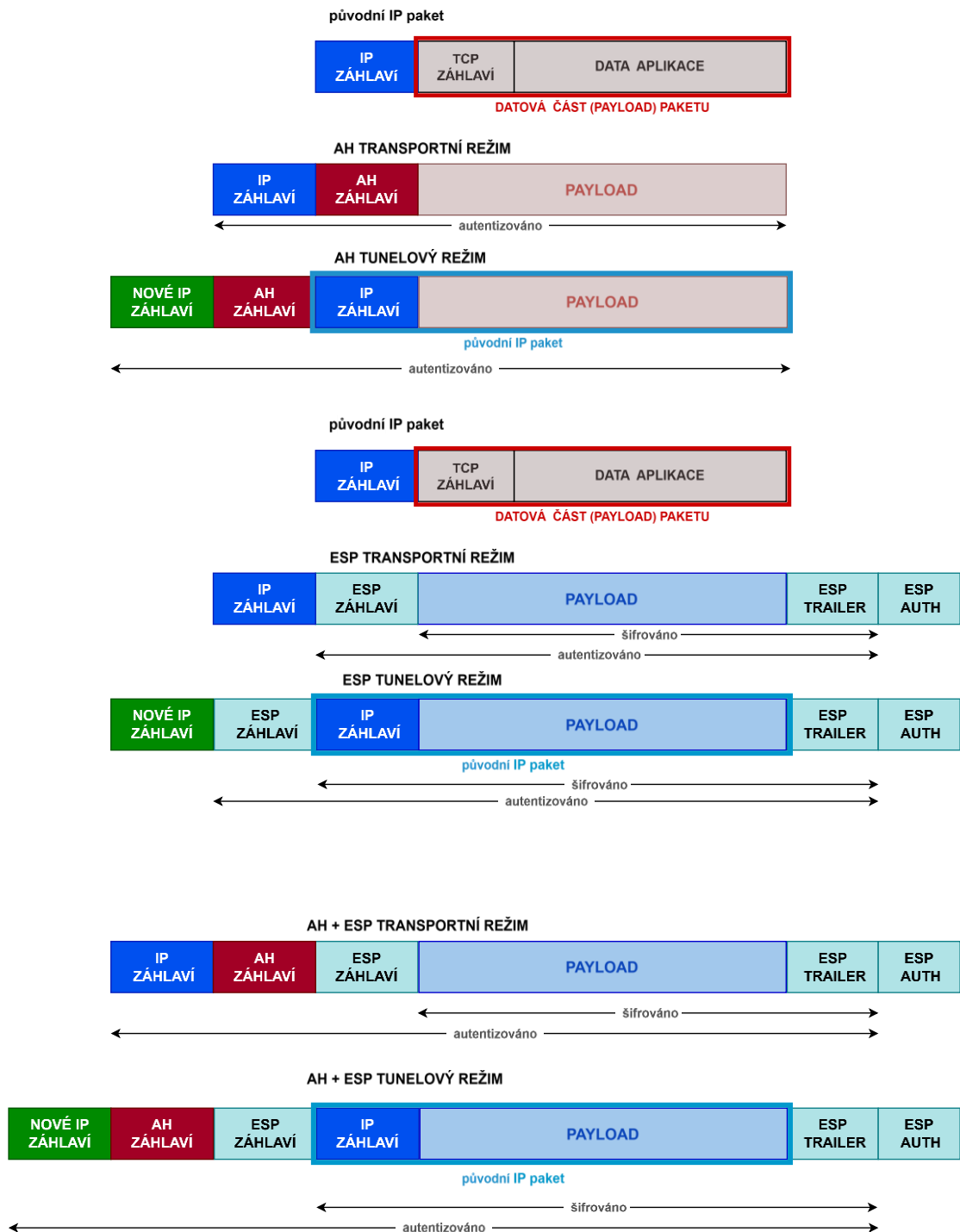
Podrobnější popis technologie IPsec lze nalézt v literatuře [4].

1.3. Kali Linux a použité nástroje

V rámci této laboratorní úlohy budou pro útok IP *spoofing*, záznam a analýzu probíhající datové komunikace a později pro implementaci bezpečnostního rozšíření IPsec postupně využity níže uvedené nástroje:

- **hping3**: pokročilý nástroj pro generování a odesílání vlastních IP paketů, vhodný pro simulaci IP spoofing útoků.
- **Wireshark**: síťový analyzátor pro sledování a záznam probíhající síťové komunikace (resp. jednotlivých paketů) s možností následné analýzy zachycených paketů.
- **strongSwan**: *open-source* knihovna pro implementaci bezpečnostního rozšíření IPsec, používaná k nastavení zabezpečených VPN spojení.

² Převzato z [3].



Obrázek 1.2 Schematické znázornění zapouzdření IPsec paketu.

Nástroj hping3

hping3 je flexibilní nástroj umožňující generovat TCP/IP pakety, simulovat různé typy útoků, jako jsou IP spoofing, *port scanning* nebo různé typy DoS útoků, a může být použit také k testování firewallů. Pomocí **hping3** je možné vytvářet vlastní pakety s upraveným IP záhlavím, což umožňuje analyzovat reakce cílových systémů (jestli reagují na požadavky, blokují komunikaci anebo generují chyby apod.).

Při práci s nástrojem **hping3** lze využít „pomocníka“ k zobrazení dostupných příkazů podporujících různé funkce nástroje pomocí příkazu:

```
hping3 --help
```

Nástroj **hping3** umožňuje také ověřit i dostupnost cílové služby (např. webového serveru). Pomocí níže uvedeného příkazu lze zjistit, zda je služba dostupná a zda firewall neblokuje přístup k příslušnému portu:

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

kde přepínač **-S** zajistí odeslání postupně **tří** TCP/IP paketů s nastaveným příznakem **SYN = 1** na **port 80** cílového zařízení s uvedenou **IP adresou**.

Pro účely simulace IP *spoofingu* je možné **hping3** použít následovně:

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

Uvedený příkaz vygeneruje celkem **pět** TCP SYN paketů směřovaných na **port 80** cílové IP adresy **192.168.126.130**, přičemž do hlavičky těchto paketů bude vložena (pomocí přepínače **-a**) falešná zdrojová IP adresa s hodnotou **192.168.126.129**.

Vysvětlení použitých přepínačů a parametrů příkazu:

- **sudo** spuštění nástroje s oprávněním správce,
- **hping3** spuštění nástroje,
- **-a 192.168.126.129** nastavení falešné (*spofovanéj*) zdrojové IP adresy,
- **-S** nastavení TCP příznaku SYN³ na hodnotu 1,
- **-p 80** cílový port, typicky používaný pro HTTP,
- **-c 5** počet odeslaných paketů (v tomto případě 5).

³ Příznakový bit SYN = 1 v záhlaví TCP protokolu indikuje zahájení, resp. vytvoření TCP spojení mezi koncovými body komunikace.

Wireshark

Wireshark je pokročilý síťový analyzátor umožňující zachytávat, vizualizovat a analyzovat síťový provoz v reálném čase. Je vhodný pro analýzu komunikačních protokolů a obsahu přenášených datových jednotek, detekci podezřelých paketů a identifikaci síťových problémů. Nástroj nabízí možnost filtrování zachycené komunikace podle různých kritérií (např. zdrojová/cílová IP adresa, protokol, port).

S nástrojem Wireshark jste se již seznámili v předchozím cvičení, kdy jste si rovněž vyzkoušeli jeho praktické použití. Pro účely praktické části tohoto počítačového cvičení je v tabulce 1.1 uveden přehled několika základních filtrů pro selektivní zobrazení paketů.

Tabulka 1.1 Wireshark: příklady použitých filtrů komunikace.

účel	filtr
zobrazení všech paketů ICMP protokolu:	<code>icmp</code>
sledování datové komunikace mezi dvěma IP adresami:	<code>ip.src == 192.168.126.129 && ip.dst == 192.168.126.130</code>
zobrazení všech ESP⁴ paketů:	<code>esp</code>

Strongswan

strongSwan je *open-source* implementace protokolů IPsec a IKE (*Internet Key Exchange*)⁵, která umožňuje vytvoření bezpečného propojení mezi dvěma nebo více uzly (zařízeními) na síťové vrstvě. Podporuje jak IPv4, tak IPv6, a umožňuje provoz v transportním i tunelovém režimu IPsec. V rámci IKE protokolu podporuje statickou i dynamickou výměnu klíčů.

Pro konfiguraci bezpečnostního rozšíření IPsec k zabezpečení síťové komunikace jsou klíčové následující konfigurační soubory:

- **etc/ipsec.conf** – hlavní konfigurační soubor pro definici spojení, (např. nastavení IP adres, přenosového režimu, způsobu autentizace)
- **etc/ipsec.secrets** – konfigurační soubor obsahující sdílená tajemství nebo klíče potřebné pro autentizaci komunikujících stran.

⁴ ESP = *Encapsulating Security Payload* – součást rozšíření IPsec, protokol pro šifrování komunikace.

⁵ IKE (*Internet Key Exchange*) je protokol používaný v rámci IPsec spojení pro bezpečnou výměnu kryptografických klíčů a vyjednání bezpečnostních parametrů mezi dvěma komunikujícími stranami. Jeho cílem je vytvořit a spravovat tzv. **Security Associations (SA)**, které definují, jaké kryptografické mechanismy budou použity k zajištění důvěrnosti a integrity přenášených dat. V rámci knihovny **strongSwan** představuje IKE nezbytnou součást, která zajišťuje bezpečné navázání IPsec spojení a následné obnovení a/nebo ukončení vytvořeného tunelu.

Pro práci s knihovnou strongSwan je nutné spustit odpovídající službu příkazem:

```
sudo systemctl start strongswan
```

Knihovna strongSwan umožňuje navázání IPsec spojení, resp. tunelu mezi dvěma koncovými body komunikace. Manuální navázání zabezpečeného spojení lze provést příkazem:

```
sudo ipsec up <název_spojení>
```

Aktuální stav aktivních IPsec tunelů lze zobrazit pomocí příkazu:

```
sudo ipsec statusall
```


2. Praktická část

V rámci praktické části počítačového cvičení bude **simulován útok IP spoofing** pomocí nástroje **hping3**, následovaný analýzou síťové komunikace prostřednictvím nástroje **Wireshark**. Simulovaný útok bude probíhat ve virtuální síti složené ze tří virtuálních strojů s OS Kali Linux (klient, server a útočník), jejíž topologie je schematicky znázorněna na obr. 2.1. Komunikace mezi těmito virtuálními stroji bude probíhá prostřednictvím virtuálního přepínače VMware Virtual Switch, jak je znázorněno v uvedeném schématu.

Cílem útoku IP *spoofing*, který spočívá v generování IP paketů s podvrženou zdrojovou IP adresou, může být vyvolání následného DDoS útoku, jehož účelem je způsobit nefunkčnost nebo nedostupnost cílového zařízení (tzv. oběti útoku). V navazující části se dále za účelem zabezpečení přenášených dat na síťové vrstvě zaměříte na **konfiguraci bezpečnostního rozšíření IPsec**, které zajišťuje důvěrnost přenášených IP paketů pomocí šifrování, dále jejich autentizaci a odolnost proti narušení integrity.

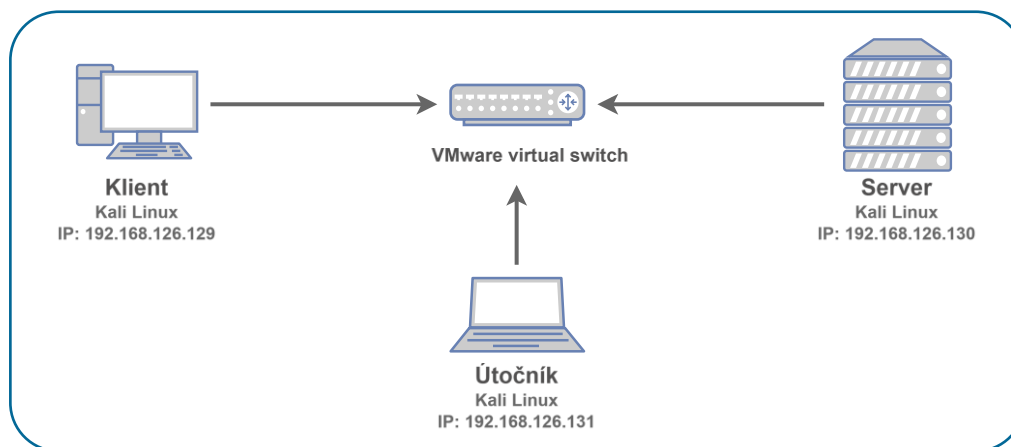
2.1. Topologie virtuální sítě a konfigurace virtuálních strojů

Použité virtuální stroje:

- **oběť (klient):** běžný počítač v síti, cíl útoku,
- **server:** poskytovatel síťové služby (např. webový server, brána),
- **útočník:** provádí IP *spoofing*, generuje IP pakety s falešnou zdrojovou IP adresou.

Síťová konfigurace:

- oběť: 192.168.126.129
- server: 192.168.126.130
- útočník: 192.168.126.131



Obrázek 2.1 Topologie sítě laboratorní úlohy.

Všechny virtuální stroje musí být připojeny ve stejné virtuální podsíti pomocí síťového režimu **Host-only** nebo **NAT**, aby bylo možné na VM „útočník“ zachytávat komunikaci mezi klientem a serverem.

2.2. Seznámení s použitými nástroji

Přehled základních příkazů pro jednotlivé používané nástroje

- **hping3**: spuštění simulace IP spoofingu:

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

- **Wireshark**: pro přehlednější analýzu zachycené komunikace ve Wiresharku je doporučeno využívat vhodné filtry pro zobrazení konkrétních paketů, např. na základě konkrétní zdrojové a/nebo cílové IP adresy:

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

- **strongSwan**: pro konfiguraci zabezpečeného IPsec spojení mezi klientem a serverem pomocí knihovny strongSwan je nutné upravit následující konfigurační soubory:
 - **/etc/ipsec.conf** (hlavní konfigurační soubor IPsec)
 - **/etc/ipsec.secrets** (soubor s autentizačními klíči)

2.3. Postup pro vypracování laboratorní úlohy


A) Příprava prostředí

Spuštění virtuálních strojů:

- Otevřete VMware Workstation Pro (ikona na ploše).
- Postupně spusťte všechny tři virtuální stroje (klient, server, útočník).
- Zkontrolujte správnost síťové konfigurace, ověřte přiřazení IP adres.
- Přihlaste se do systému Kali Linux na VM útočníka.

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

Ověření síťové konektivity:

- Otevřete **terminál** (kliknutím na ikonu terminálu  v horní liště nebo pomocí klávesové zkratky Ctrl + Alt + T).

- Na každém VM zobrazte přidělené IP adresy (na rozhraní **eth0**):

```
ip a
```

- Z klienta odešlete testovací požadavek (ping) a vyzkoušejte připojení na server pomocí příkazu:


```
ping <ip_adresa_serveru>
```

- Pokud se vrací odpovědi **ping echo reply** ze strany serveru, komunikace mezi zařízeními funguje. Stejným způsobem ověřte spojení i v opačném směru.

B) IP spoofing útok pomocí hping3

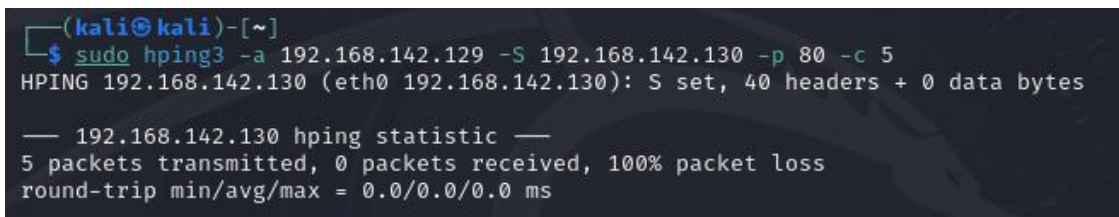
Pomocí nástroje **hping3** lze na VM útočníka simulovat IP *spoofing* útok generováním IP paketů s podvrženou zdrojovou IP adresou. Cílem je odesílat pakety, které se jeví, jako by byly odeslány klientem. Tento útok umožňuje ověřit, že cílové zařízení (server) nedokáže odhalit skutečného odesílatele – tedy útočníka. Probíhající komunikace bude monitorována pomocí nástroje Wireshark.

Použití nástroje hping3

- Na stroji útočníka otevřete terminál kliknutím na ikonu  v horní liště nebo v menu zvolte **Applications > System Tools > Terminal**. Otevře se okno s příkazovou řádkou.
- Spustěte útok příkazem:

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

Po zadání příkazu bude zahájena simulace útoku, tedy generování datových paketů, které budou působit dojemem, že pocházejí od 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
```

Obrázek 2.2 Spuštění IP *spoofing* útoku v terminálu Kali Linux.

Sledování příchozí komunikace (server) ve Wiresharku

- Na serveru spustěte **Wireshark** pomocí příkazu:

```
sudo wireshark &
```

Přepínač '**sudo**' spustí nástroj Wireshark s oprávněními administrátora, což je nezbytné pro zachytávání síťového provozu v Kali Linuxu.

- V hlavním okně vyberte síťové rozhraní **eth0** – dvojitým kliknutím spustíte zachytávání (nebo klikněte na **Start Capturing Packets** v záhlaví panelu nástrojů).
- Do okna pro filtrování komunikace zadejte:

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

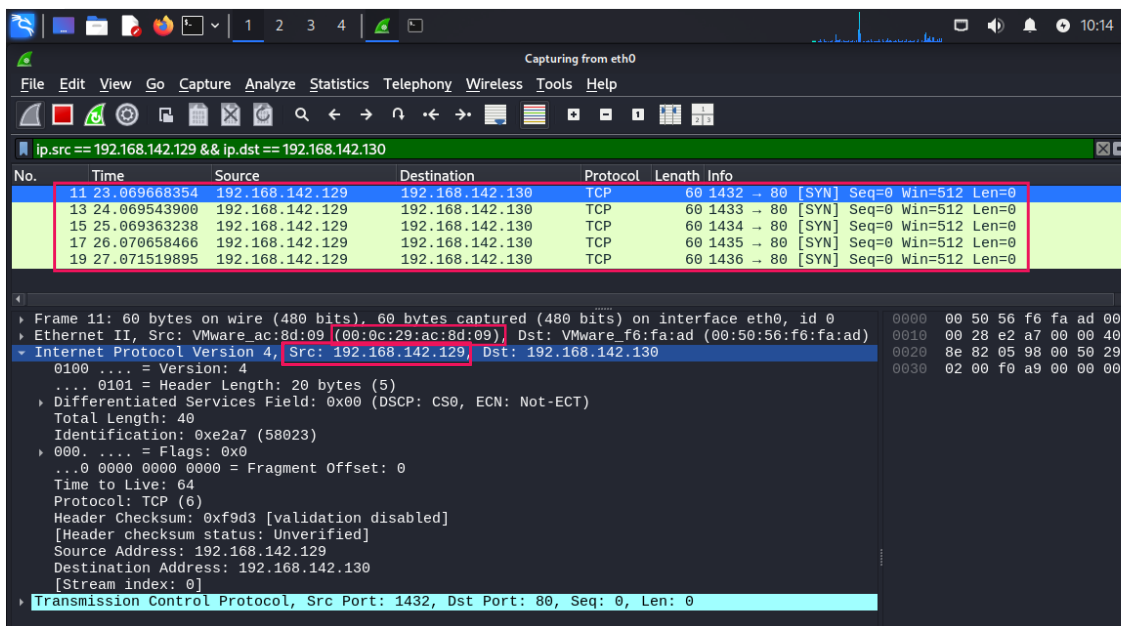
tuto volbu potvrďte stlačením **Enter**.

Použití uvedeného filtru zajistí, že z veškerých zachycených datových jednotek přenesených v rámci komunikace přes zvolené rozhraní budou zobrazeny pouze pakety údajně „pocházející od klienta“, tedy pakety odpovídající filtru **ip.src == 192.168.126.129**, a dále také pakety, které mají být doručeny na server, tedy pakety odpovídající druhému ze zadaných filtrů **ip.dst == 192.168.126.130**. Ve skutečnosti se však jedná o pakety generované na straně útočníka nástrojem **hping3**.

- Kliknutím pravým tlačítkem myši na některý ze zachycených paketů a následným výběrem možnosti „**Follow > TCP Stream**“ lze zobrazit celkový přehledný průběh spojení mezi komunikujícími zařízeními.
- Pro podrobnější analýzu komunikace klikněte na vybraný paket a v dolní části sledovaného okna Wiresharku si zobrazte sekci **Internet Protocol Version 4**, kde si můžete detailně prohlédnout konkrétní hodnoty *Source IP* (zdrojová) a *Destination IP* (cílová adresa).

Zdrojová IP adresa by měla mít hodnotu 192.168.126.129 odpovídající VM klienta, ačkoli byl příslušný paket ve skutečnosti odeslán ze stanice útočníka (viz zachycená komunikace na obr. 2.3).

- Pro ověření úspěšnosti IP *spoofingu* dále analyzujte fyzické MAC adresy zařízení, ze kterých byly jednotlivé pakety odeslány (zobrazení v sekci **Ethernet II**).



Obrázek 2.3 Ukázka zachycené komunikace po spuštění útoku IP *Spoofing* (server).

C) Zabezpečení komunikace s využitím IPsec

V následující části laboratorního úkolu si vyzkoušíte práci s knihovnou **strongSwan**, která podporuje implementaci IPsec.

Konfigurace IPsec v transportním režimu

- Na zařízení klienta i serveru spusťte instalaci knihovny **strongSwan**:

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

Použití uvedeného příkazu zajistí **inštaláci balíka strongSwan**, který obsahuje potřebné komponenty pro vytvoření zabezpečeného IPsec spojení. Aktualizace balíčků v Kali Linuxu (příkaz: **apt update**) zajistí, že budou použity aktuálně dostupné verze.

- Na obou zařízeních (klient i server) upravte konfigurační soubor **/etc/ipsec.conf** – pro editaci souboru v textovém režimu můžete využít např. editor **nano**, a to následovně:

- pro přesun do adresáře, kde se příslušný konfigurační soubor nachází, použijte v otevřeném terminálu příkaz:

```
cd /etc
```

- následně otevřete soubor pro úpravu:

```
sudo nano ipsec.conf
```

- do souboru vložte následující konfiguraci (pro klienta):

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

!! Uvedená konfigurace se týká nastavení IPsec na straně klienta.

Tímto nastavením jsou definovány parametry zabezpečeného spojení mezi klientem (**left**) a serverem (**right**). Parametr **authby=secret** určuje, že pro autentizaci komunikujících stran bude použito sdílené tajemství PSK (*pre-shared key*). Dále je nastavena výměna klíčů pomocí IKEv2 a specifikovány šifrovací a autentizační algoritmy pro fázi IKE (**ike**) i pro samotná data (**esp**). Parametr **auto=start** zajistí automatické navázání definovaného IPsec spojení při startu služby.

- Po úpravě konfigurace stiskněte kombinaci kláves **Ctrl + O** (uložení), potvrďte název souboru klávesou **Enter** a následně ukončete textový editor **nano** pomocí **Ctrl + X**.
- Alternativně můžete úpravu ukončit stisknutím **Ctrl + X**, následným potvrzením uložení stisknutím **Y** (Yes/ano) a finálním potvrzením **Enter** – změny se tím uloží a editor se zavře.
- Dále upravte konfigurační soubor **/etc/ipsec.secrets**:

```
sudo nano ipsec.secrets
```

- Do souboru vložte následující řádek:

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

Tento řádek definuje sdílený klíč (**PSK**), který bude použit pro autentizaci mezi dvěma zařízeními s uvedenými IP adresami (klient a server). **Je nezbytné, aby byl na obou stranách komunikace zadán stejný klíč** – v opačném případě nebude proces autentizace úspěšný a nebude možné navázat zabezpečené spojení.

PSK představuje jednoduchý způsob autentizace vhodný pro menší a testovací prostředí, méně však pro rozsáhlé produkční nasazení.

- Po úpravě souboru opět použijte kombinaci **Ctrl + O** → **Enter** → **Ctrl + X** nebo alternativně **Ctrl + X** → **Y** → **Enter** pro potvrzení a uložení provedených změn.
- Po změnách v konfiguraci je třeba službu restartovat, případně ověřit, zda je po spuštění aktivní:

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

- Stejným způsobem postupujte při instalaci **strongSwan** a konfiguraci IPsec i na straně serveru, přičemž dbejte na správné definování parametrů (IP adresy) v konfiguraci.

Připojení a ověření konfigurace IPsec

- Na obou zařízeních (klient i server) spusťte službu IPsec a vytvořte mezi nimi zabezpečené spojení na základě předchozí konfigurace:

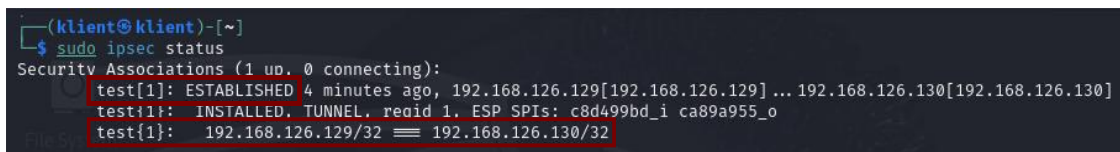
```
sudo ipsec start
```

```
sudo ipsec up test
```

- Zobrazte si stav vytvořeného spojení pomocí příkazu:

```
sudo ipsec status
```

V případě správné konfigurace by mělo být spojení ve stavu **ESTABLISHED** (viz obr. 2.4). *Pro zobrazení podrobnějších informací o spojení můžete alternativně použít příkaz `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
```

Obrázek 2.4 Ověření vytvoření IPsec spojení (klient).

- Důležité je také ověřit, zda komunikace mezi zařízeními **klient** ↔ **server** skutečně probíhá přes vytvořený IPsec tunel.
- Na serveru opět otevřete nástroj **Wireshark** a spusťte zachytávání síťového provozu na rozhraní **eth0**.

- V terminálu (server) pomocí nástroje **tcpdump** sledujte komunikaci, která bude vykazovat známky použití IPsec tunelu:

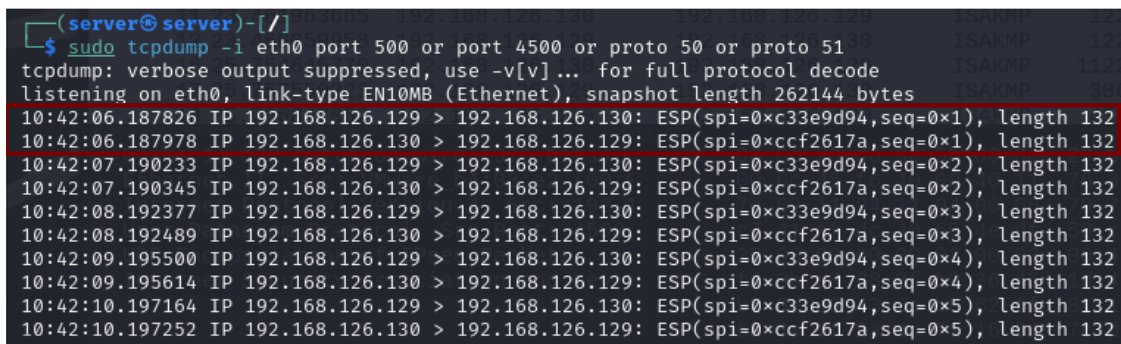
```
sudo tcpdump -i eth0 port 500 or port 4500 or proto 50 or proto 51
```

Použití nástroje **tcpdump** s uvedenými parametry zajistí sledování provozu souvisejícího s IPsec: **UDP port 500 (IKE)**, **protokol 50 (ESP)**, **protokol 51 (AH)**. Pro případ použití překladu adres je vhodné sledovat také komunikaci na portu UDP 4500 (NAT-T).

- Z klientského VM odešlete ping na server:

```
ping 192.168.126.130
```

- Na serveru sledujte výstup nástroje **tcpdump** v otevřeném terminálu a zároveň záznam komunikace ve Wiresharku.
- Níže uvedený výpis dokazuje, že vytvořený **šifrovaný IPsec tunel funguje** – mezi klientem a serverem probíhá **výměna šifrovaných ESP paketů** (protokol 50) právě skrze tento tunel – podrobněji viz obr. 2.5.



```
(server@server)-[//]
$ sudo tcpdump -i eth0 port 500 or port 4500 or proto 50 or proto 51
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10:42:06.187826 IP 192.168.126.129 > 192.168.126.130: ESP(spi=0xc33e9d94,seq=0x1), length 132
10:42:06.187978 IP 192.168.126.130 > 192.168.126.129: ESP(spi=0xccf2617a,seq=0x1), length 132
10:42:07.190233 IP 192.168.126.129 > 192.168.126.130: ESP(spi=0xc33e9d94,seq=0x2), length 132
10:42:07.190345 IP 192.168.126.130 > 192.168.126.129: ESP(spi=0xccf2617a,seq=0x2), length 132
10:42:08.192377 IP 192.168.126.129 > 192.168.126.130: ESP(spi=0xc33e9d94,seq=0x3), length 132
10:42:08.192489 IP 192.168.126.130 > 192.168.126.129: ESP(spi=0xccf2617a,seq=0x3), length 132
10:42:09.195500 IP 192.168.126.129 > 192.168.126.130: ESP(spi=0xc33e9d94,seq=0x4), length 132
10:42:09.195614 IP 192.168.126.130 > 192.168.126.129: ESP(spi=0xccf2617a,seq=0x4), length 132
10:42:10.197164 IP 192.168.126.129 > 192.168.126.130: ESP(spi=0xc33e9d94,seq=0x5), length 132
10:42:10.197252 IP 192.168.126.130 > 192.168.126.129: ESP(spi=0xccf2617a,seq=0x5), length 132
```

Obrázek 2.5 Výpis nástroje **tcpdump**: sledování komunikace prostřednictvím vytvořeného IPsec tunelu (server).

- Pro zobrazení šifrované komunikace ve Wiresharku je vhodné použít filtr:

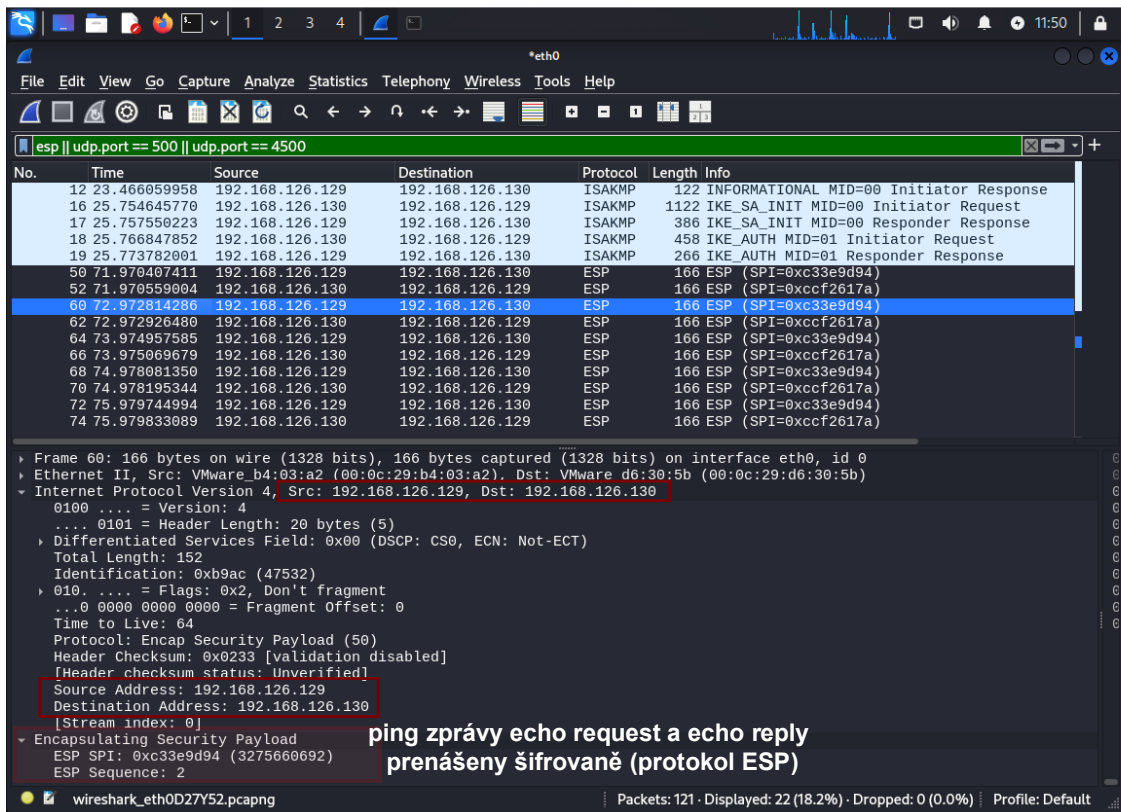
```
esp || udp.port == 500 || udp.port == 4500
```

Použití uvedeného filtru zobrazí:

- **ESP pakety** (protokol 50),
- **IKE komunikaci** (na portu UDP 500 – vytvoření IPsec tunelu),
- **IKE přes NAT-T** (UDP port 4500 – pokud se IPsec přizpůsobuje NAT-u).

- **Další možnost ověření:**

Pomocí nástroje **hping3** opět spusťte na VM útočníka simulaci útoku **IP spoofing** a sledujte, zda jsou odeslané pakety ze strany útočníka na serveru odmítnuty. Správně nakonfigurované spojení by mělo zabránit přijetí neautentizované komunikace. Průběh komunikace sledujte rovněž pomocí nástroje **Wireshark**.



Obrázek 2.6 Ukázka zachycené komunikace – přenos přes šifrovaný IPsec tunel (server).

2.4. Samostatný úkol

D) Implementace IPsec v tunelovém režimu

V poslední části úkolu si samostatně vyzkoušíte praktické nasazení bezpečnostního rozšíření **IPsec v tunelovém režimu** pro zabezpečení komunikace odesílané přes simulovanou „veřejnou síť“.

Cílem vaší samostatné práce bude nejprve simulovat vlastní veřejnou síť a následně správným způsobem nakonfigurovat IPsec rozšíření v tunelovém režimu pro zabezpečení komunikace mezi klientem a serverem.

Po implementaci otestujete a porovnáte výkonnost sítě při použití transportního a tunelového režimu IPsec, zejména z pohledu latence komunikace, spolehlivosti přenosu a stability vytvořeného spojení.

Zachycenou komunikaci analyzujte ve Wiresharku a porovnejte rozdíly mezi oběma režimy. Při analýze věnujte pozornost také struktuře paketů (např. viditelnost vnitřních hlaviček, šifrování obsahu a použité protokoly).

3. Závěr

V tomto laboratorním úkolu jste se seznámili s problematikou bezpečnosti síťové vrstvy počítačových sítí a v této souvislosti také s riziky spojenými s podvržením IP adresy (tzv. *IP spoofing*), což představuje častý způsob narušení integrity nebo důvěrnosti komunikace na síťové vrstvě.

V praktické části jste **pomocí nástroje hping3** realizovali simulaci útoku, který ilustruje, jakým způsobem lze oklamat cílové zařízení pomocí falešné zdrojové IP adresy uvedené v hlavičce odesílaných datových jednotek. Následně jste si vyzkoušeli **praktickou implementaci rozšíření IPsec**, které umožňuje komplexní zabezpečení IP komunikace, a to včetně šifrování dat, autentizace a zajištění integrity přenosu. Porovnáním transportního a tunelového režimu IPsec jste získali přehled o různých způsobech ochrany datového provozu a rovněž o jejich vlivu na výslednou podobu paketů či celkový výkon počítačové sítě.

3.1. 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

4. Literatura

- [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/>