**Návod na prácu s protokolmi Telnet a SSH v Cisco Packet Tracer**

**1. Úvod**

Protokoly Telnet a SSH sa používajú na vzdialený prístup k sieťovým zariadeniam, ako sú smerovače a prepínače. Telnet prenáša dáta v nešifrovanej podobe, čo z neho robí nezabezpečený protokol. Na druhej strane SSH (Secure Shell) využíva šifrovanie a je odporúčaný na používanie vo všetkých sieťach.

V tomto návode si vysvetlíme, ako nakonfigurovať Telnet a SSH v prostredí Cisco Packet Tracer, a zistíme ich funkčnosť a bezpečnostné rozdiely.

**2. Sieťová topológia a konfigurácia**

**2.1 Príprava siete v Packet Tracer**

1. **Rozvrhnutie siete:**
   * Zoberieme niekoľko počítačov/notebookov, ktoré nám budú tvoriť sieť, a ľubovoľný switch/prepínač. Potom zoberieme ešte jeden počítač, ktorý si umiestnime ďalej od našich PC v sieti, pretože to bude počítač administrátora.
2. **Prepojenie siete:**
   * Prepojíme všetky počítače k switchu káblom Copper-Straight-Through cez ľubovoľné FastEthernet porty.
3. **Konfigurácia switchu:**
   * Otvoríme switch a zvolíme CLI zadáme že nechceme initial configuration od CISCA keďže si ju spravíme samy, a zadáme príkazy:

enable

configure terminal

interface vlan 1

ip address 192.168.10.100 255.255.255.0

no shutdown

Stlačte Enter.

exit

line vty 0 15

password telnet@1234

login

exit

exit

copy running-config startup-config

//vysvetlenie príkazov:

1. **enable** - Prepneme sa do režimu, kde môžeme vykonávať dôležité zmeny na switchi.
2. **configure terminal** - Vstúpime do režimu na konfiguráciu switchu.
3. **interface vlan 1** - Zvolíme VLAN 1, čo je predvolená sieťová karta switchu.
4. **ip address 192.168.10.100 255.255.255.0** - Priradíme IP adresu switchu, aby sme ho mohli spravovať.
5. **no shutdown** - Zapneme sieťové rozhranie (inak by bolo vypnuté).
6. **exit** - Ukončíme režim rozhrania VLAN.
7. **line vty 0 15** - Prepneme sa do nastavení pre vzdialený prístup (Telnet).
8. **password telnet@1234** - Nastavíme heslo pre pripojenie cez Telnet.
9. **login** - Aktivujeme používanie hesla pri pripojení.
10. **copy running-config startup-config** - Uložíme nastavenia, aby sa nestratili po reštarte.
11. **Konfigurácia admin počítača:**
    * Nemusíme nastavovať IP adresy aj počítačom v sieti, zatiaľ nám bude stačiť ju nastaviť len na admin počítaču.
    * Otvoríme počítač a prejdeme do Desktop, kde zvolíme IP Configuration. Nastavíme IP adresu 192.168.10.2 (u vás sa to môže líšiť podľa toho, ktorú IP adresu ste si predtým vybrali) a necháme základnú Subnet masku.
    * Vrátime sa na Desktop a zvolíme Command Prompt, kde zadáme tieto príkazy:

telnet 192.168.10.100

Vypýta si to heslo, kde musíme zadať to heslo, čo sme nastavili, takže v mojom prípade:

telnet@1234

enable

Ak vám to vypíše % No password set., všetko funguje správne. Teraz sa musíme vrátiť späť do switch CLI a nastaviť heslo týmito príkazmi:

configure terminal

enable password admin@1234

exit

copy running-config startup-config

Teraz môžeme zavrieť konfiguráciu switchu a ísť späť do admin počítača, do Command Prompt, kde napíšeme toto:

enable

Zadáme naše admin heslo, čiže u mňa:

admin@1234

//vysvetlenie príkazov

1. **telnet 192.168.10.100** - Pripojíte sa na switch cez Telnet pomocou jeho IP adresy (192.168.10.100).
2. **telnet@1234** - Switch si vyžiada heslo, ktoré ste nastavili pre Telnet (v tomto prípade telnet@1234).
3. **enable password admin@1234** - Nastavte heslo (admin@1234) pre privilegovaný režim.
4. **exit** - Ukončite konfiguračný režim.
5. **password telnet@1234** - Nastavíme heslo pre pripojenie cez Telnet.
6. **login** - Aktivujeme používanie hesla pri pripojení.

Teraz už máme nastavený Telnet a sme v admin počítači, čiže môžeme príkazmi ovládať sieť, ako napríklad zrušiť prístup jednému z počítačov k switchu príkazmi:

configure terminal

interface fastethernet 0/3

shutdown

A opäť mu môžeme povoliť prístup, ak napíšeme:

no shutdown

//vysvetlenie príkazov

1. **interface fastethernet 0/3** - Vyberieme konkrétny port na switchi, v tomto prípade port **FastEthernet 0/3**. Tento port je prepojený s jedným z počítačov v sieti.
2. **shutdown** - Vypneme zvolený port, čím zablokujeme prístup zariadeniu pripojenému k tomuto portu. Počítač pripojený k tomuto portu stratí spojenie so sieťou.

Takže cez tento počítač spravujeme sieť.

**2.2 Vysvetlenie fungovania siete Telnet**

V tejto **Telnet** sieti sú počítače prepojené so switchom, pričom **admin počítač spravuje sieť** na diaľku cez Telnet. Switch má pridelenú IP adresu a nakonfigurovaný Telnet prístup s **heslom**. **Administrátor** sa cez **Telnet** pripojí k switchu a môže ovládať sieť, napríklad blokovať alebo povoliť prístup zariadeniam cez konkrétne porty. Hoci je Telnet **jednoduchý**, nie je **bezpečný**, pretože neprenáša údaje **šifrovane**.

**2.3 Dôvod konfigurácie**

Tento spôsob konfigurácie siete poskytuje **efektívny** a **bezpečný** prístup k správe zariadení v sieti pomocou **Telnetu** a jednoduchých **CLI príkazov**. Nastavením silných **hesiel** a **vzdialeného prístupu** získate flexibilitu v riadení pripojení a zabezpečení siete. Použitím príkazov na **blokovanie** alebo **povolenie** prístupu cez porty, ako aj **uložením konfigurácie**, zaistíte **stabilitu** a **spoľahlivosť** celej siete.

**2.4 Bezpečnostné riziká**

**1. Nešifrovaný Telnet:** Telnet neposkytuje šifrovanie, čo môže umožniť zachytenie citlivých údajov.

**2. Slabé heslá:** Jednoduché heslá sú náchylné na útoky hrubou silou (Brute force).

**3. Neobmedzený prístup:** Ak nie sú nastavené obmedzenia prístupu, môže to umožniť neoprávnený prístup k zariadeniam.

**4. Chýbajúca autentifikácia:** Ak nie je správne nastavená autentifikácia, môže dôjsť k neautorizovanému prístupu.

**3.1 Konfigurácia SSH**

1. **Rozvrhnutie siete:**
   * **Najprv zoberieme jeden PC/notebook, jeden switch a jeden router a prepojíme ich káblom Copper Straight-Through.**
2. **Konfigurácia PC:**
   * **Pôjdeme do nášho PC, do Desktop a IP Configuration, kde nastavíme IP adresu, ktorú chceme použiť, u mňa to je 192.168.1.3. Masku necháme tak, ako ju prednastaví Packet Tracer, a musíme ešte nastaviť Default Gateway, v mojom prípade na 192.168.1.1.**
3. **Prepojenie PC a routera:**
   * **Zoberieme prepojenie Console a prepojíme PC a router cez porty RS232 (PC) a Console (router).**
4. **Konfigurácia routera:**
   * **Pôjdeme späť do PC, do Terminal, a stlačíme OK.**
   * **Opäť, ako aj pri Telnete, nechceme initial configuration a zadáme tieto príkazy:**

**enable**

**configure terminal**

**hostname R1**

**banner motd 'Toto je CISCO router'**

**interface g0/0**

**ip address 192.168.1.1 255.255.255.0**

**no shutdown**

**exit**

**//vysvetlenie prikazov**

1. **hostname R1** - Nastaví názov routera na "R1". Názov je užitočný na identifikáciu zariadenia v sieťovej infraštruktúre.
2. **banner motd 'Toto je CISCO router'** - Nastaví správu dňa (Message of the Day), ktorá sa zobrazí používateľom pri prihlásení. Táto správa slúži hlavne na informačné alebo výstražné účely.
3. **interface g0/0** - Vyberie rozhranie GigabitEthernet 0/0, ktoré sa bude konfigurovať. Toto rozhranie je pripojené k sieti.
4. **ip address 192.168.1.1 255.255.255.0** - Priradí IP adresu (192.168.1.1) a masku podsiete (255.255.255.0) zvolenému rozhraniu. Táto IP adresa je brána (default gateway) pre zariadenia v sieti.
5. **Konfigurácia zabezpečenia routera:**
   * **Stále sme v PC v Terminal a zadáme príkazy:**

**ip domain-name admin**

**username admin secret Cisco**

**enable secret Cisco**

**line console 0**

**password class**

**login**

**exit**

**service password-encryption**

**do show run**

**Skontrolujeme, či sa heslo šifruje.**

* + **Vygenerujeme RSA kľúče a nastavíme SSH:**

**crypto key-generate rsa**

**1024**

**ip ssh version 2**

**line vty 0 15**

**transport input ssh**

**login local**

**//vysvetlenie prikazov**

1. **ip domain-name admin** - Nastaví názov domény pre router na "admin". Tento názov je potrebný na vygenerovanie RSA kľúčov pre SSH, pretože šifrované pripojenia vyžadujú názov domény na identifikáciu zariadenia.
2. **username admin secret Cisco** - Vytvára používateľský účet s menom "admin" a heslom "Cisco". Príkaz **secret** zabezpečí, že heslo bude uložené v zašifrovanej podobe v konfigurácii.
3. **enable secret Cisco** - Nastavuje heslo "Cisco" pre privilegovaný režim (**enable mode**). Tento príkaz používa silnejší šifrovací algoritmus v porovnaní s príkazom enable password.
4. **line console 0** - Prechádza do konfigurácie konzolového prístupu (fyzického portu Console, cez ktorý sa zariadenie spravuje lokálne).
5. **password class** - Nastaví heslo "class" na konzolový prístup.
6. **login** - Aktivuje povinnosť zadávať heslo pri pokuse o pripojenie cez konzolový port.
7. **service password-encryption** - Aktivuje šifrovanie všetkých hesiel uložených v konfigurácii. Bez tohto príkazu budú heslá uložené v čitateľnej podobe (plain text).
8. **do show run** - Zobrazí aktuálnu konfiguráciu zariadenia (tzv. **running configuration**) priamo z konfiguračného režimu. Používa sa na overenie, či sú heslá zašifrované.
9. **crypto key generate rsa** - Vytvorí RSA kľúče potrebné na bezpečnú komunikáciu cez SSH. Pri vytváraní sa zvyčajne určuje dĺžka kľúča (v tomto prípade 1024 bitov), čo ovplyvňuje úroveň zabezpečenia.
10. **ip ssh version 2** - Aktivuje druhú verziu SSH protokolu, ktorá je bezpečnejšia ako verzia 1.
11. **transport input ssh** - Umožňuje iba SSH pripojenia na VTY linkách. Zakazuje nešifrované protokoly, ako napríklad Telnet.
12. **login local** - Nastavuje autentifikáciu používateľov cez lokálny zoznam účtov (napr. účet "admin", ktorý bol predtým vytvorený pomocou príkazu username admin secret Cisco).
13. **Kontrola komunikácie PC a routera:**
    * **Teraz môžeme konzolové spojenie s PC a routerom vypojiť z routera a zapojiť do switchu, tak aby bolo konzolové spojenie prepojené s PC a switchom.**
    * **Pôjdeme do PC, do Command Prompt, a pingneme náš router:**

**ping 192.168.1.1**

**Prihlásime sa do "admin účtu" v našom routeri cez PC:**

**ssh -l admin 192.168.1.1**

**Zadáme heslo, v mojom prípade:**

**Cisco**

**Ak sa chceme dostať do konfigurácie routera, stačí zadať:**

**enable**

**A heslo:**

**Cisco**

**//vysvetlenie prikazov**

1. **ping 192.168.1.1** - Tento príkaz posiela ICMP pakety na IP adresu 192.168.1.1, aby sa overila dostupnosť cieľového zariadenia (v tomto prípade routera). Ak odpovede prídu (bez veľkých strát), spojenie medzi PC a routerom funguje správne.
2. **ssh -l admin 192.168.1.1** - Tento príkaz slúži na vzdialené pripojenie k zariadeniu cez protokol SSH.

**-l admin**: Špecifikuje používateľské meno, ktoré sa použije na prihlásenie (v tomto prípade "admin").

**192.168.1.1**: IP adresa routera, na ktorý sa chcete pripojiť.

Po zadaní tohto príkazu sa zariadenie opýta na heslo zodpovedajúce zadanému používateľskému menu.

1. **Cisco** - Heslo potrebné na autentifikáciu. V tomto prípade bolo heslo nastavené na "Cisco" pomocou príkazu username admin secret Cisco.
2. **Konfigurácia switchu:**
   * **Konfigurácia switchu je skoro rovnaká ako pri routeri, takže pôjdeme do PC, do Terminal, a stlačíme OK a zadáme príkazy:**

**enable**

**configure terminal**

**hostname S1**

**banner motd 'Toto je CISCO switch'**

**interface vlan 1**

**ip address 192.168.1.2 255.255.255.0**

**no shutdown**

**exit**

**enable secret Cisco**

**line console 0**

**password Cisco**

**login**

**exit**

**username admin secret Cisco**

**service password-encryption**

**ip domain-name admin**

**crypto key generate rsa**

**1024**

**ip ssh version 2**

**line vty 0 15**

**transport input ssh**

**login local**

**exit**

**ip default-gateway 192.168.1.1**

**Väčšinou nedávame viac IP adries na Layer 2 switche, jediný dôvod je práve SSH.**

**//vysvetlenie prikazov**

1. **ip default-gateway 192.168.1.1** - Nastaví predvolenú bránu na **192.168.1.1**. Switch bude vedieť komunikovať so zariadeniami mimo svojej podsiete.
2. **Kontrola komunikácie PC a switcha:**
   * **Teraz už môžeme konzolové spojenie odstrániť úplne, keďže by malo byť všetko správne nastavené a už ho nebudeme potrebovať.**
   * **Pôjdeme späť do nášho PC, do Command Prompt, a ako aj pri kontrole routera zadáme:**

**ping 192.168.1.2**

**Mal by byť jeden dropnutý packet.**

* + **Prihlásime sa na switch cez SSH:**

**ssh -l admin 192.168.1.2**

**Cisco**

**A teraz by sme mali už byť schopní dostať sa cez SSH z routera do switchu:**

**ssh -l admin 192.168.1.1**

**Cisco**

**exit**

**A mali by sme byť v routeri cez switch.**

* + **Keď chceme skúsiť, či vieme ísť naopak, z routera do switchu, zadáme:**

**ssh -l admin 192.168.1.1**

**Cisco**

**ssh -l admin 192.168.1.2**

**Cisco**

* + **Keď nám to vypíše našu predvolenú správu, u mňa 'Toto je CISCO switch', všetko funguje správne a máme nastavenú SSH komunikáciu.**

**3.2 Vysvetlenie fungovania siete** **SSH**

Konfigurácia **SSH** zabezpečuje bezpečný vzdialený prístup k zariadeniam prostredníctvom šifrovaného prenosu. Vytvorenie **RSA** kľúčov umožňuje bezpečnú komunikáciu, pričom používateľský účet "admin" so šifrovaným heslom poskytuje **autentifikáciu**. Aktivácia **SSH verzie 2** zabezpečuje, že pripojenia budú šifrované a bezpečné. Na **VTY linkách** je povolený len SSH prenos, čo zakazuje **nezabezpečený Telnet**. Šifrovanie hesiel zabezpečuje, že všetky prístupové údaje sú uložené v zašifrovanej podobe, čím sa chráni citlivá informácia pred neoprávneným prístupom. Týmto spôsobom je **zabezpečená** celková komunikácia a ochrana pred **vonkajšími hrozbami**.

**3.3 Dôvod konfigurácie**

Moja konfigurácia **SSH** je optimálna z hľadiska **bezpečnosti** a **efektívnosti**. Použitím silného šifrovania cez **RSA** kľúče a verzie **2 SSH** zabezpečujeme šifrovaný prenos dát, čo chráni pred **odpočúvaním** a **útokmi**. Nastavenie **silných hesiel** a **lokálnej autentifikácie** znižuje riziko neautorizovaného prístupu, pričom vylučuje **nešifrované pripojenie cez Telnet**. Tento prístup je stabilný, flexibilný a zabezpečuje bezpečné vzdialené riadenie siete.

**3.4 Bezpečnostné riziká**

**1. Slabé heslá:** Použitie slabších hesiel, ako "Cisco", môže byť náchylné na útoky hrubou silou (Brute force). Je potrebné používať silné, unikátne heslá.

**2. Nezabezpečený prístup cez SSH:** Ak nie je správne nastavený prístup (napr. obmedzenie prístupu podľa IP adries), môže dôjsť k neautorizovanému pripojeniu.

**3. RSA kľúče:** Neopatrné zaobchádzanie s RSA kľúčmi, ako ich nezabezpečenie alebo nesprávne generovanie, môže ohroziť šifrovaný prenos.

**4. Zanedbanie aktualizácií:** Neaktualizovanie firmvéru zariadení môže zanechať sieť zraniteľnú voči známym zraniteľnostiam.

**4. Záver a odporúčania**

**Bezpečnosť**

* Telnet by sa mal používať iba na testovacie účely alebo v uzavretých sieťach, kde nehrozí odchytávanie prenosov.
* SSH je štandardný a bezpečný protokol na vzdialený prístup a odporúča sa používať vždy, keď je to možné.