Práca s protokolmi SSH a Telnet

## 1. Úvod

Telnet a SSH sú protokoly na vzdialenú správu sieťových zariadení, ako sú smerovače a prepínače. Telnet prenáša údaje bez šifrovania, čo znamená nižšiu úroveň zabezpečenia. Naopak, SSH (Secure Shell) používa šifrovanie, čím zabezpečuje bezpečný prenos dát. Tento návod ukáže, ako nastaviť Telnet a SSH v Cisco Packet Tracer a porovnať ich vlastnosti a úroveň zabezpečenia.

## 2. Sieťová topológia a konfigurácia

### 2.1 Telnet

Telnet je protokol, ktorý umožňuje pripojenie k zariadeniam v sieti cez príkazový riadok. Je to nešifrovaný protokol, čo znamená, že všetky dáta vrátane prihlasovacích údajov sú prenášané v textovej podobe a môžu byť zachytené.

**Konfigurácia Telnet na Cisco zariadení:**

1. **Povolenie Telnet pripojenia:**
   * Zadajte príkazy na povolenie Telnet pripojení a konfiguráciu vzdialeného prístupu.

Switch(config)# line vty 0 4

Switch(config-line)# password yourpassword # Nastavte heslo pre Telnet pripojenie

Switch(config-line)# login

Switch(config-line)# transport input telnet # Povolenie Telnet pripojenia

Switch(config-line)# exit

1. **Testovanie Telnet pripojenia:**
   * Na počítači sa pripojte k zariadeniu pomocou Telnet klienta:

telnet 192.168.1.1 # Pripojte sa na IP adresu zariadenia

### 2.2 SSH

SSH (Secure Shell) je bezpečnejší protokol ako Telnet, pretože všetky dáta sú šifrované. Používa sa na vzdialené pripojenie k zariadeniam a spravovanie ich konfigurácie.

**Konfigurácia SSH na Cisco zariadení:**

1. **Povolenie SSH:**
   * Pre používanie SSH je potrebné nastaviť doménové meno, generovať RSA kľúče a povoliť SSH.Switch(config)# ip domain-name example.com # Nastavte doménové meno

Switch(config)# crypto key generate rsa general-keys modulus 2048 # Generovanie RSA kľúčov

Switch(config)# ip ssh version 2 # Povolenie SSH verzie 2

1. **Konfigurácia prihlasovacích údajov:**
   * Nastavte prihlasovacie údaje pre SSH pripojenie.

Switch(config)# username admin privilege 15 secret yourpassword # Nastavte používateľské meno a heslo

Switch(config)# line vty 0 4

Switch(config-line)# login local # Použitie miestneho prihlasovania (používatelia nastavení na zariadení)

Switch(config-line)# transport input ssh # Povolenie SSH pripojení

Switch(config-line)# exit

1. **Testovanie SSH pripojenia:**
   * Na počítači použite SSH klienta na pripojenie k zariadeniu:

ssh admin@192.168.1.1 # Pripojte sa na zariadenie pomocou SSH

## 3. Porovnanie Telnet a SSH:

**SSH**

Závislosť na slabých heslách: Ak sú použité jednoduché heslá, môže dôjsť k prelomeniu hesla brute-force útokmi.

Zraniteľné konfigurácie: Nesprávne nastavenie môže umožniť prístup útočníkom (napr. povolený root login).

Zraniteľnosti starších verzií: Nepoužívanie aktuálnej verzie SSH môže obsahovať známe bezpečnostné chyby.

Man-in-the-Middle (MITM) útoky: Pri nesprávnom overovaní verejných kľúčov.

**Telnet**

Nešifrovaná komunikácia: Všetky údaje (vrátane hesiel) sú posielané v plaintext forme, ľahko zachytiteľné pomocou sniffingu.

Zraniteľné voči odpočúvaniu: Dáta môžu byť zachytené útočníkom na akomkoľvek mieste siete.

Autentifikácia bez šifrovania: Útočník môže ľahko ukradnúť prihlasovacie údaje.

Man-in-the-Middle (MITM) útoky: Neexistuje ochrana pred manipuláciou s prenášanými dátami.

Zastaraný protokol: Telnet je považovaný za nevhodný pre moderné siete kvôli nízkej bezpečnosti.

**Zhrnutie:**SSH je odporúčané pre bezpečné pripojenie, zatiaľ čo Telnet by mal byť používaný iba v uzavretých a zabezpečených sieťach.