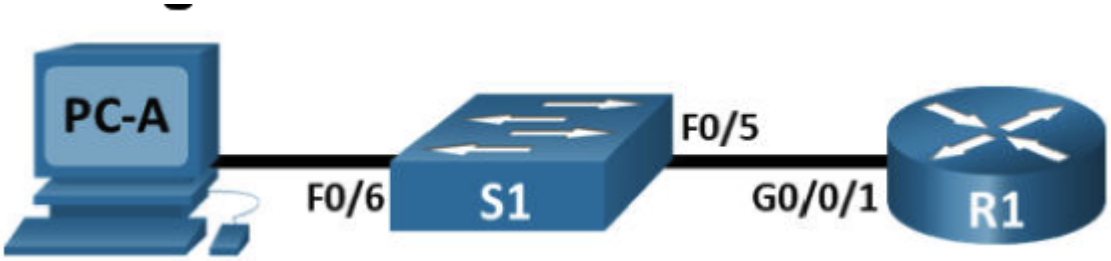
Lab 7: SSH-turvalisus võrguseadmetel

Taust: Telnet oli kunagi populaarne võrguseadmete haldamise viis, kuid see ei ole turvaline, kuna andmeid, sealhulgas paroole, edastatakse krüpteerimata kujul. SSH (Secure Shell) on nüüd eelistatud protokoll, kuna see krüpteerib andmed, muutes ühenduse turvaliseks.



Seadmete konfiguratsioon:

Seade	Liides	IP-aadress	Võrgumask	Vaikelüüs
R1	G0/0/1	192.168.1.1	255.255.255.0	-
S1	VLAN1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Samm 1: Marsruuteri (R1) põhikonfiguratsioon

1. **Lülita seadmed sisse ja ühenda kaablid vastavalt topoloogiale.**
2. **Seadista marsruuteri nimi (kasuta oma eesnime)**:

```
Router(config)# hostname R1_<eesnimi>
```

Selgitus: See määrab marsruuterile nime, näiteks: R1_Maria.

3. **Keela DNS-otsing, et vältida viivitusi, kui sisestatud käsk ei ole korrektne:**

```
R1_Maria(config)# no ip domain lookup
```

Selgitus: See aitab vältida pikki viivitusi, kui kirjutad käsu valesti.

4. **Määra salajane parool ("class") pääsemiseks "privilegeeritud režiimi":**

```
R1_Maria(config)# enable secret class
```

Selgitus: See parool kaitseb kõrgetasemeliste käskude kasutamist.

5. **Seadista konsooli ja VTY (virtuaalse terminali) liinide parool ("cisco"):**

```
R1_Maria(config)# line console 0
R1_Maria(config-line)# password cisco
R1_Maria(config)# line vty 0 4
R1_Maria(config-line)# password cisco
```

Selgitus: Need on ajutised paroolid. Päris elus kasuta kindlasti tugevamat parooli.

6. **Krüpteeri kõik paroolid, mis on avatud tekstina nähtavad:**

```
R1_Maria(config)# service password-encryption
```

Selgitus: See tagab, et kõik paroolid on varjatud ja mitte lihtsalt loetavad.

7. **Loo ühendustel teavitustekst (banner):**

```
R1_Maria(config)# banner motd $ Volitatud kasutajatele ainult! $
```

Selgitus: See kuvatakse iga kord, kui keegi ühendub seadmega.

8. **Seadista IP-aadressid vastavalt seadmete tabelile ja testi ühendust pingi abil:**

```
PC-A> ping 192.168.1.1
```

Selgitus: Kui pingi vastus puudub, siis lahenda võrguühenduse probleemid.

Samm 2: SSH serveri seadistamine

1. **Määra marsruuterile domeeninimi:**

```
R1_Maria(config)# ip domain-name ccna-lab.com
```

Selgitus: Domeeninimi on vajalik krüpteerimisvõtmete genereerimiseks.

2. **Genereeri krüpteerimisvõti (RSA):**

```
R1_Maria(config)# crypto key generate rsa modulus 1024
```

Selgitus: See loob SSH jaoks vajaliku krüpteerimisvõtme.

3. **Lisa kasutaja (kasutajanimi "admin" ja parool "Adm1nP@55"):**

```
R1_Maria(config)# username admin secret Adm1nP@55
```

Selgitus: See kasutaja saab SSH kaudu sisse logida.

4. **Luba SSH ja Telnet VTY liinidel:**

```
R1_Maria(config)# line vty 0 4
R1_Maria(config-line)# transport input telnet ssh
```

Selgitus: See võimaldab kasutada nii Telnetit kui ka SSH-d (soovituslikult kasuta ainult SSH-d).

5. **Kasuta lokaalset andmebaasi autentimiseks:**

```
    R1_Maria(config-line)# login local
```

Samm 3: Testi SSH-ühendust

1. **Ava PuTTY programm arvutis ja loo SSH-ühendus:**

- IP-aadress: 192.168.1.1
- Connection Type: SSH
- Kasutajanimi: admin
- Parool: Adm1nP@55

2. **Kontrolli, kas SSH töötab. Kui ühendus on edukas, oled turvaliselt sisse logitud.**

Samm 4: Kommutaatori seadistamine

1. **Ühenda kommutaatori konsoolipordi kaabel ümber ja seadista kommutaator (S1):**

```
S1_Maria(config)# interface vlan 1
S1_Maria(config-if)# ip address 192.168.1.11 255.255.255.0
S1_Maria(config-if)# no shutdown
```

Selgitus: Kommutaatori haldamiseks tuleb määrata IP-aadress ja aktiveerida liides.

2. **Loo SSH-ühendus kommutaatorist marsruuterisse:**

```
  S1_Maria# ssh -l admin 192.168.1.1
```

Selgitus: Kasutades käsku ssh, saad turvalise ühenduse luua marsruuterisse kommutaatorist.

Samm 5: Turvameetmete täiustamine

1. Kehtesta minimaalne parooli pikkus (12 märki):

```
R1_Maria(config)# security passwords min-length 12
```

2. Muuda paroolid tugevamaks:

- Priviligeeritud režiimi parool:

```
R1_Maria(config)# enable secret $cisco!PRIV*
```

- Console parool:

```
R1_Maria(config-line)# password $cisco!!CON*
```

- VTY liinide parool:

```
R1_Maria(config-line)# password $cisco!!VTY*
```

3. Keela kasutaja "admin" turvakaalutlustel:

```
R1_Maria(config)# no username admin
```

4. Seadista automaatne väljalogimine, kui 5 minuti jooksul tegevust ei toimu:

```
R1_Maria(config)# line console 0
R1_Maria(config-line)# exec-timeout 5 0
R1_Maria(config)# line vty 0 4
R1_Maria(config-line)# exec-timeout 5 0
```

5. Piira ebaõnnestunud sisselogimiskatsete arvu (3 katset 1 minuti jooksul, blokeeritakse 2 minutiks):

```
 R1_Maria(config)# login block-for 120 attempts 3 within 60
```

Lõpetuseks:

Peale nende sammude läbimist peaks sul olema turvaline SSH-ühendus marsruuteri ja kommutaatoriga. Kontrolli seadistusi käsuga:

```
R1_Maria# show running-config
```