Võrguseadmete turvalisusseaded

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

Taust ja eesmärgid

Varemalt oli Telnet kõige enam kasutatud protokoll võrguseadmete kaughalduse teostamiseks. Telnet ei sisalda krüpteerimist, mistõttu on ta kaitsetu pealtkuulamise suhtes, mille käigus võivad lekkida ka paroolid ja seadistusinfo. Tänapäeval kasutatakse eelkõige SSH (Secure Shell) protokolli, mis võimaldab luua krüptograafiliselt turvatud ühendust otspunktide vahel. Samuti on võimalik transportida faile üle SFTP (Secure File Transfer Protocol) või SCP (Secure Copy) protokollide.

Järgnevalt seadistame marsruuteris SSH-serveri ning teeme arvutist ühenduse marsruuterisse üle SSH-protokolli.

Sammud:

1. Tee marsruuteris põhiline seadistus
    1. Ühenda kaablid nagu topoloogiajoonisel ja lülita seadmed sisse
    2. Määra marsruuteri nimi, kasutades oma eesnime „<eesnimi>” asemel (ainult ladinatähed ja numbrid).
       Router(config)# hostname R1_<eesnimi>
    3. Lülita välja DNS lookup, mis väldib näiteks trükiveaga sisestatud käskude üritamist lahendada kui domeeninime.
       R1_erkki(config)# no ip domain lookup
    4. Priviligeeritud parooliks seadke „class” (pärisjuhtumi korral määrake ikka turvaline parool).
       R1_erkki(config)# enable secret class
    5. Pane parool „cisco” console ja VTY liinidele (pärisjuhtumi korral määrake ikka turvaline parool).
       R1_erkki(config)# line console 0
       R1_erkki(config-line)# password cisco
       R1_erkki(config)# line vty 0 4
       R1_erkki(config-line)# password cisco
    6. Krüpteeri avatud tekstina näha olevad paroolid:
       R1_erkki(config)# service password-encryption
    7. Seadistage teavitustekst, mil ühendutakse marsruuteriga
       R1_erkki(config)# banner motd $ Volitatud kasutajatele ainult! $
    8. Seadista marsruuteri ja arvuti liidesed vastavalt tabelile.
    9. Pingi PC-A'st marsruuterit. Kui pole edukas, lahenda probleemid.
2. Seadistame autentimise

1. Seadistame domeeninime seadmele
   R1_erkki(config)# ip domain-name ccna-lab.com
2. Seadistame krüpteerimisvõtme meetodi (oleneb versioonist üks neist käskudest)
   R1_erkki(config)# crypto key generate rsa modulus 1024
   R1_erkki(config)# crypto key generate rsa general-keys modulus 1024
3. Seadistame lokaalse andmebaasi kasutaja (kasutajanimeks „admin" ja parooliks „Adm1nP@55"
   R1_erkki(config)# username admin secret Adm1nP@55
4. Lülitame sisse SSH kasutamise VTY liinidel
   R1_erkki(config)# line vty 0 4
   R1_erkki(config-line)# transport input telnet ssh
5. Muudame sisse logimise autentimist kasutama lokaalset andmebaasi
   R1_erkki(config-line)# login local

3. Teeme arvutist ühenduse marsruuterisse üle SSH:
   1. Ava Putty, vali „Connection type" = „SSH", IP-aadressiks pane marsruuteri IP, vajuta „Open" nuppu
   2. Kasuta „username" on ülal seatud „admin" ja parooliks „Adm1nP@55"
   3. Nüüd peaksid olema edukalt marsruuteris sees üle SSH ehk siis üle krüpteeritud ühenduse
4. Seadistame ka kommutaatoris ligipääsetavaks üle SSH.
   1. Ühenda marsruuteri Console pordist juhe ümber kommutaatori Console porti
   2. Tee kommutaatorile põhiline seadistus, analoogselt marsruuterile
   3. IP-aadress pane liidesele „VLAN 1"
      S1_erkki(config)# interface vlan 1
      S1_erkki(config-if)# ip address 192.168.1.11 255.255.255.0
      S1_erkki(config-if)# no shutdown
5. Teeme SSH-ühenduse kommutaatorist marsruuterisse
   1. Kasutame käsku „ssh" ja vaatame, mida teha saame
      S1# ssh ?
      -c Select encryption algorithm
      -l Log in using this user name
      -m Select HMAC algorithm
      -o Specify options
      -p Connect to this port
      -v Specify SSH Protocol Version
      -vrf Specify vrf name
      WORD IP address or hostname of a remote system
   2. Vaja on kasutada valikut „-l admin", et logida sisse kasutajaga „admin"
      S1_erkki# ssh -l admin 192.168.1.1
   3. Sa saad seanssi sulgemata minna tagasi kommutaatorisse vajutades CTRL+SHIFT+6 ja kajutades „x". Nüüd peaksite nägema, et käsureaviip muutub „R1_erkki" asemel tagasi „S1_erkki" peale (vastavalt oma eesnimele).

Nüüd on üle SSH ligipääsud seadistatud ja saame ühenduda turvaliselt seadmetega üle krüpteeritud kanali. Järgnevalt seadistame veel mõned turvaseaded ja testime nende töötamist.

1. Me oleme juba seadistanud, et kõik paroolid oleksid krüpteeritud kujul
   R1_erkki(config)# service password-encryption
2. Seadistame, et nõutakse paroolide seadistamisel minimaalselt 12 märki
   R1_erkki(config)# security passwords min-length 12
3. Muudame nüüd paroolid, mis vastaksid nõutud parooli pikkusele
   1. Muudame priviligeeritud laadi parooliks „$cisco!PRIV*"

2. Muudame console liini parooliks „$cisco!!CON*”
3. Muudame vty liini parooliks „$cisco!!VTY*”

4. Varasemalt oleme seadistanud juba SSH kasutamise vty liinil, kus võtme pikkus 1024 bitti ja domeeninimi „ccna-lab.com”.
   1. Seadistame SSH jaoks kasutaja „SSHadmin” parooliga „55HAdm!n2020”
      R1_erkki(config)# username SSHadmin secret 55HAdm!n2020
   2. Varemalt oli kasutaja „admin”, mille võiks likvideerida turvalisuse kaalutlustel, kui seda pole vaja
      R1_erkki(config)# no username admin
5. Seadistame console ja vty liinide jaoks automaatse välja logimise, kui pole 5 minuti jooksul mitte midagi tehtud
   R1_erkki(config)# line console 0
   R1_erkki(config-line)# exec-timeout 5 0
   R1_erkki(config)# line vty 0 4
   R1_erkki(config-line)# exec-timeout 5 0
6. Seadistame, et kui marsruuterisse on üritatud 1 minuti jooksul üritatud 3 korda valesti sisse logida, siis uuesti ei saa proovida enne 2 minuti möödumist
   R1_erkki(config-line)# login block-for 120 attempts 3 within 60
7. Oluline on, et kõik pordid, mis ei ole kasutusel, oleksid kinni keeratud. Vaikimisi marsruuterites on liidesed kinni keeratud, aga kommutaatorites vaikimisi lubatud. Kontrollime liideseid, mis peaks olema lubatud (kui väljundis „status” veerus on „administratively down”, siis liides kinni keeratud ja nii on turvalisem, kui liides pole kasutusel).
   R1_erkki# show ip interface brief
   1. Kui mingi liidese puhul vaja kinni keerata, siis mine vastava liidese laadi ja pane kinni
      R1_erkki(config-if)# shutdown
8. Kontrollime rakendatud turvameetmete töötamist
   1. Ava Putty ja ürita teha marsruuterisse ühendus üle Telnet'i. See ei tohiks õnnestuda. Miks?
   2. Ürita uuesti teha SSH-ühendus uue kasutajaga marsruuterisse. See peaks õnnestuma
   3. Pane valmis Console liinil ühendus marsruuterisse, et saaksid seda ruttu kasutada. Ürita uuesti teha SSH-ühendus, aga pane parool mitu korda valesti. Kas toimub blokeerimine?
   4. Ava Console liinil ühendus marsruuterisse ja vaatame logimiste staatuseid. Mida näed?
      R1_erkki# show login
   5. Kui on möödunud vähemalt 2 minutit vigasest sisselogimiskatsest, üritame uuesti teha SSH-ühendus õige parooliga marsruuterisse. Kas said edukalt nüüd sisse? Peaks saama.
   6. Mine nüüd priviligeeritud laadi ja parooli küsimisel sisesta parooli 3 või enam korda valesti. Mis juhtub? Midagi ei peaks juhtuma, sest eelnev seadistus käis marsruuteriga ühendumise kohta. Sisesta nüüd õige parool ja saad priviligeeritud laadi.
9. Vaata nii marsruuteris ja kommutaatoris üle oma seadistus igaks juhuks, et midagi üleliigset või puudu poleks
   R1_erkki# show running-config
10. Praegu muutsime ja vaatasime turvaseadistused üle marsruuteris. Samad asjad käivad ka kommutaatorite kohta.
    1. Kommutaatoris võid ükshaaval porte kinni keerata, aga kui porte palju, siis saab ka hulgi kinni panna (tühikud koma ees ja taga võivad olla olulised). Paneme kinni kõik pordid, välja arvatud 5 ja 6 (need ju ühenduvad arvutiga ja marsruuteriga).
       S1_erkki(config)# interface range f0/1–4 , f0/7-24 , g0/1-2
       S1_erkki(config-if-range)# shutdown
    2. Kui aega on, siis tee kommutaatoris ka muud seadistused, mida tegime marsruuteris