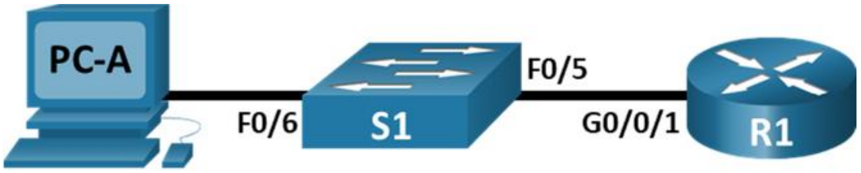
Lab 16.5.2 - Secure Network Devices

This lab has been updated for use on NETLAB+.

www.netdevgroup.com

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	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

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure Basic Security Measures on the Router

Part 3: Configure Basic Security Measures on the Switch

Background / Scenario

It is recommended that all network devices be configured with at least a minimum set of best practice security commands. This includes end user devices, servers, and network devices, such as routers and switches.

In this lab, you will configure the network devices in the topology to accept SSH sessions for remote management. You will also use the IOS CLI to configure common, basic best practice security measures. You will then test the security measures to verify that they are properly implemented and working correctly.

Note: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.2(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Instructions

Part 1: Configure Basic Device Settings

In Part 1, you will configure basic settings, such as the interface IP addresses, device access, and passwords on the devices.

Step 1: Configure the router and switch.

a. Click on each device to access the console port and enable privileged EXEC mode.

b. Assign the device name according to the Addressing Table.

c. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.

d. Assign class as the privileged EXEC encrypted password.

e. Assign cisco as the console password and enable login.

f. Assign cisco as the VTY password and enable login.

g. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

h. Configure and activate the G0/0/1 interface on the router using the information contained in the Addressing Table.

i. Configure the default SVI on the switch with the IP address information according to the Addressing Table.

j. Save the running configuration to the startup configuration file.

Step 2: Configure PC-A.

a. Configure PC-A with an IP address and subnet mask.

b. Configure a default gateway for PC-A.

Step 3: Verify network connectivity.

Ping R1 and S1 from PC-A. If any of the pings fail, troubleshoot the connection.

Part 2: Configure Basic Security Measures on the Router

Step 1: Configure security measures.

a. Encrypt all clear-text passwords.

b. Configure the system to require a minimum 12-character password.

c. Change the passwords (privileged exec, console, and vty) to meet the new length requirement.

   1) Set the privileged exec password to **$cisco!PRIV***

   2) Set the console password to **$cisco!!CON***

   3) Set the vty line password to **$cisco!!VTY***

d. Configure the router to accept only SSH connections from remote locations

   1) Configure the username **SSHadmin** with an encrypted password of **55HAdm!n2020**

   2) The router’s domain name should be set to ccna-lab.com

   3) The key modulus should be 1024 bits.

e. Set security and best-practice configurations on the console and vty lines.

   1) Users should be disconnected after 5 minutes of inactivity.

   2) The router should not allow vty logins for 2 minutes if 3 failed login attempts occur within 1 minute.

Part 3: Configure security measures.

Step 1: Verify that all unused ports are disabled.

Depending on the model of the router, ports may be disabled by default, but it is always prudent to verify that all unused ports are in an administratively down state. This can be quickly checked by issuing the **show ip interface brief** command. Any unused ports that are not in an administratively down state should be disabled using the **shutdown** command in interface configuration mode.

Step 2: Verify that your security measures have been implemented correctly.

a. Use Tera Term on PC-A to telnet to R1.

Does R1 accept the Telnet connection? Explain.

R1 does not accept the Telnet connection since it was disabled. Only SSH is allowed.

b. Use Tera Term on PC-A to SSH to R1.

Does R1 accept the SSH connection?

R1 accepts an SSH connection because SSH connections are allowed.

c. Intentionally mistype the user and password information to see if login access is blocked after two attempts.

What happened after you failed to login the second time?

The connection is disconnected, and if the users tries to connect within 30 seconds, the connection will be refused,

d. From your console session on the router, issue the **show login** command to view the login status. In the example below, the **show login** command was issued within the 120 second login blocking period and shows that the router is in Quiet-Mode. The router will not accept any login attempts for 111 more seconds.

e. After the 120 seconds has expired, SSH to R1 again and login using the **SSHadmin** username and **55HAdm!n2020** for the password.

After you successfully logged in, what was displayed?

After successfully logging in, the MOTD banner is displayed.

f. Enter privileged EXEC mode and use **$cisco!PRIV*** for the password.

If you mistype this password, are you disconnected from your SSH session after three failed attempts within 60 seconds? Explain.

No because the command that blocks login attempts only monitors the VTY lines.

g. Issue the **show running-config** command at the privileged EXEC prompt to view the security settings you have applied.

Part 4: Configure Basic Security Measures on the Switch

Step 1: Configure security measures.

a. Encrypt all clear-text passwords.

b. Configure the system to require a minimum 12 character password

c. Change the passwords (privileged exec, console, and vty) to meet the new length requirement.

   1) Set the privileged exec password to **$cisco!PRIV***

   2) Set the console password to **$cisco!!CON***

   3) Set the vty line password to **$cisco!!VTY***

d. Configure the switch to accept only SSH connections from remote locations.

   1) Configure the username **SSHadmin** with an encrypted password of **55HAdm!n2020**

   2) The switches domain name should be set to ccna-lab.com

   3) The key modulus should be 1024 bits.

e. Set security and best-practice configurations on the console and vty lines.

   1) Users should be disconnected after 5 minutes of inactivity.

   2) The switch should not allow logins for 2 minutes if 3 failed login attempts occur within 1 minute.

f. Disable all of the unused ports.

Step 2: Verify all unused ports are disabled.

Switch ports are enabled, by default. Shut down all ports that are not in use on the switch.

a. You can verify the switch port status using the **show ip interface brief** command.

b. Use the **interface range** command to shut down multiple interfaces at a time.

c. Verify that all inactive interfaces have been administratively shut down.

Step 3: Verify that your security measures have been implemented correctly.

a. Verify that Telnet has been disabled on the switch.

b. SSH to the switch and intentionally mistype the user and password information to see if login access is blocked.

c. After the 30 seconds has expired, SSH to S1 again and log in using the **SSHadmin** username and **55HAdm!n2020** for the password.

   Did the banner appear after you successfully logged in?

   Type your answers here.

   Yes

d. Enter privileged EXEC mode using **$cisco!PRIV*** as the password.

e. Issue the **show running-config** command at the privileged EXEC prompt to view the security settings you have applied.

Reflection Questions

1. The **password cisco** command was entered for the console and VTY lines in your basic configuration in Part 1. When is this password used after the best practice security measures have been applied?

The "password cisco" command won't be used to sign in, but it will still appear in the config, but it will get disabled with the "login local" command.

2. Are preconfigured passwords shorter than 10 characters affected by the **security passwords min-length 12** command?

No, the command "security passwords min-length 12" only affects passwords entered after the command was entered.

Router and Switch Interface Summary Table

Router / Switch Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2960	Fast Ethernet 0/1 (F0/1)	Fast Ethernet 0/2 (F0/2)	n/a	n/a
3560	Fast Ethernet 0/1 (F0/1)	Fast Ethernet 0/2 (F0/2)	n/a	n/a
3650	Gigabit Ethernet 1/0/1 (G1/0/1)	Gigabit Ethernet 1/0/2 (G1/0/2)	n/a	n/a
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.