Lab - Secure Network Devices

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

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.

Instructions

Part 1: Configure Basic Device Settings

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

Step 1: Cable the network as shown in the topology.

Attach the devices shown in the topology and cable as necessary.

Step 2: Initialize and reload the router and switch.

Step 3: Configure the router and switch.

a. Console into the device 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 4: Configure PC-A.

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

b. Configure a default gateway for PC-A.

Step 5: 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.

```
security passwords min-length 12
```

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.

```
line vty 0 4
 exec-timeout 5 0
```

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

```
login block-for 120 attempts 3 within 60
```

Part 3: Configure security measures.

Step 1: Verify that all unused ports are disabled.

Router ports are 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.

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0/0   unassigned      YES unset  administratively down down
GigabitEthernet0/0/1   192.168.1.1     YES manual up                    up
Serial0/1/0            unassigned      YES unset  administratively down down
Serial0/1/1            unassigned      YES unset  administratively down down
```

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.

No, the connection is refused. Telnet was disabled with the transport input ssh **command.**

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

Does R1 accept the SSH connection?

Yes

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 to R1 was disconnected. If you attempt to reconnect 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.

```
R1# show login
     A default login delay of 1 seconds is applied.
     No Quiet-Mode access list has been configured.
     All successful login is logged.

     Router enabled to watch for login Attacks.
     If more than 3 login failures occur in 60 seconds or less,
     logins will be disabled for 120 seconds.

     Router presently in Quiet-Mode.
     Will remain in Quiet-Mode for 111 seconds.
     Denying logins from all sources.
```

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?

The R1 –MOTD banner.

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. The login block-for 120 attempts 3 within 60 **command only monitors session login attempts on 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.

```
S1# show ip interface brief
```

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

```
S1(config)# interface range f0/1-4 , f0/7-24 , g0/1-2
S1(config-if-range)# shutdown
S1(config-if-range)# end
```

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

```
S1# show ip interface brief
```

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?

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.