Lab – Securing Network Devices

Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	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 1941 ISRs with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(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 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.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS software, release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

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 G0/1 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.

Part 2: Configure Basic Security Measures on the Router

Step 1: Encrypt the clear text passwords.

```
R1(config)# service password-encryption
```

Step 2: Strengthen passwords.

An administrator should ensure that passwords meet the standard guidelines for strong passwords. These guidelines could include combining letters, numbers and special characters in the password and setting a minimum length.

Note: Best practice guidelines require the use of strong passwords, such as those shown here, in a production environment. However, the other labs in this course use the cisco and class passwords for ease in performing the labs.

a. Change the privileged EXEC encrypted password to meet guidelines.

```
R1(config)# enable secret Enablep@55
```

b. Require that a minimum of 10 characters be used for all passwords.

```
R1(config)# security passwords min-length 10
```

Step 3: Enable SSH connections.

a. Assign the domain name as **CCNA-lab.com**.

```
R1(config)# ip domain-name CCNA-lab.com
```

b. Create a local user database entry to use when connecting to the router via SSH. The password should meet strong password standards, and the user should have user EXEC access. If privilege level is not specified in the command, the user will have privileged EXEC (level 15) access by default.

```
R1(config)# username SSHadmin privilege 1 secret Admin1p@55
```

c. Configure the transport input for the VTY lines so that they accept SSH connections, but do not allow Telnet connections.

```
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
```

d. The VTY lines should use the local user database for authentication.

```
R1(config-line)# login local
R1(config-line)# exit
```

e. Generate a RSA crypto key using a modulus of 1024 bits.

```
R1(config)# crypto key generate rsa modulus 1024
```

Step 4: Secure the console and VTY lines.

a. You can set the router to log out of a connection that has been idle for a specified time. If a network administrator was logged into a networking device and was suddenly called away, this command automatically logs the user out after the specified time. The following commands cause the line to log out after five minutes of inactivity.

```
R1(config)# line console 0
R1(config-line)# exec-timeout 5 0
R1(config-line)# line vty 0 4
R1(config-line)# exec-timeout 5 0
R1(config-line)# exit
R1(config)#
```

b. The following command impedes brute force login attempts. The router blocks login attempts for 30 seconds if someone fails two attempts within 120 seconds. This timer is set especially low for the purpose of this lab.

```
R1(config)# login block-for 30 attempts 2 within 120
```

What does the **2 within 120** mean in the above command?

2 attempts inside 2 mins

What does the **block-for 30** mean in the above command?

Block for 30 seconds

Step 5: 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
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet0/1         192.168.1.1     YES manual up                    up
Serial0/0/0                unassigned      YES NVRAM  administratively down down
Serial0/0/1                unassigned      YES NVRAM  administratively down down
R1#
```

Step 6: Verify that your security measures have been implemented correctly.

a. Use Tera Term to telnet to R1.

Does R1 accept the Telnet connection? Explain.

No, because we disabled it

b. Use Tera Term 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?

closed by foreign host

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 30 second login blocking period and shows that the router is in Quiet-Mode. The router will not accept any login attempts for 14 more seconds.

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

    Router enabled to watch for login Attacks.
    If more than 2 login failures occur in 120 seconds or less,
    logins will be disabled for 30 seconds.

    Router presently in Quiet-Mode.
    Will remain in Quiet-Mode for 14 seconds.
    Denying logins from all sources.
R1#
```

e. After the 30 seconds has expired, SSH to R1 again and login using the **SSHadmin** username and **Admin1p@55** for the password.

After you successfully logged in, what was displayed? The banner

f. Enter privileged EXEC mode and use **Enablep@55** for the password.

If you mistype this password, are you disconnected from your SSH session after two failed attempts within 120 seconds? Explain.

No, because it was not enabled/configured that way

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

Part 3: Configure Basic Security Measures on the Switch

Step 1: Encrypt the clear text passwords.

```
S1(config)# service password-encryption
```

Step 2: Strengthen Passwords on the switch.

Change the privileged EXEC encrypted password to meet strong password guidelines.

```
S1(config)# enable secret Enablep@55
```

Note: The security **password min-length** command is not available on the 2960 switch.

Step 3: Enable SSH Connections.

a. Assign the domain-name as **CCNA-lab.com**

```
S1(config)# ip domain-name CCNA-lab.com
```

b. Create a local user database entry for use when connecting to the switch via SSH. The password should meet strong password standards, and the user should have user EXEC access. If privilege level is not specified in the command, the user will have user EXEC (level 1) access by default.

```
S1(config)# username SSHadmin privilege 1 secret Admin1p@55
```

c. Configure the transport input for the VTY lines to allow SSH connections but not allow Telnet connections.

```
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
```

d. The VTY lines should use the local user database for authentication.

```
S1(config-line)# login local
S1(config-line)# exit
```

e. Generate an RSA crypto key using a modulus of 1024 bits.

```
S1(config)# crypto key generate rsa modulus 1024
```

Step 4: Secure the console and VTY lines.

a. Configure the switch to log out a line that has been idle for 10 minutes.

```
S1(config)# line console 0
S1(config-line)# exec-timeout 10 0
S1(config-line)# line vty 0 15
S1(config-line)# exec-timeout 10 0
S1(config-line)# exit
S1(config)#
```

b. To impede brute force login attempts, configure the switch to block login access for 30 seconds if there are 2 failed attempts within 120 seconds. This timer is set especially low for the purpose of this lab.

```
S1(config)# login block-for 30 attempts 2 within 120
S1(config)# end
```

Step 5: 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
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.11    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  down                  down
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  down                  down
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down
FastEthernet0/20       unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  down                  down
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
S1#
```

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
S1#
```

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

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.11    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
FastEthernet0/2        unassigned      YES unset  administratively down down
FastEthernet0/3        unassigned      YES unset  administratively down down
FastEthernet0/4        unassigned      YES unset  administratively down down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  administratively down down
FastEthernet0/8        unassigned      YES unset  administratively down down
FastEthernet0/9        unassigned      YES unset  administratively down down
FastEthernet0/10       unassigned      YES unset  administratively down down
FastEthernet0/11       unassigned      YES unset  administratively down down
FastEthernet0/12       unassigned      YES unset  administratively down down
FastEthernet0/13       unassigned      YES unset  administratively down down
FastEthernet0/14       unassigned      YES unset  administratively down down
FastEthernet0/15       unassigned      YES unset  administratively down down
FastEthernet0/16       unassigned      YES unset  administratively down down
FastEthernet0/17       unassigned      YES unset  administratively down down
FastEthernet0/18       unassigned      YES unset  administratively down down
FastEthernet0/19       unassigned      YES unset  administratively down down
FastEthernet0/20       unassigned      YES unset  administratively down down
FastEthernet0/21       unassigned      YES unset  administratively down down
FastEthernet0/22       unassigned      YES unset  administratively down down
FastEthernet0/23       unassigned      YES unset  administratively down down
FastEthernet0/24       unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
S1#
```

Step 6: 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 **Admin1p@55** for the password.

Did the banner appear after you successfully logged in? yes

d. Enter privileged EXEC mode using **Enablep@55** as the password.

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

Reflection

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 will not be used any longer

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

No, only passwords the command was issued

Router Interface Summary Table

Router Interface Summary				
Router 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 (S0/0/0)	Serial 0/1/1 (S0/0/1)
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)

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.