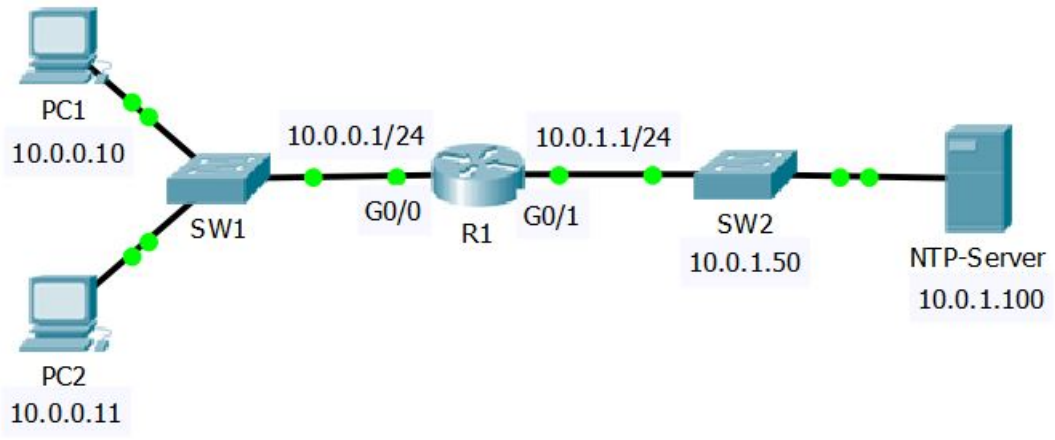
35-1 Cisco Device Security Configuration – Lab Exercise

In this lab you will secure administrative access to the Cisco router in a small campus network.

Lab Topology



Load the Startup Configurations

Open the ' 35-1 Cisco Device Security Configuration.pkt' file in Packet Tracer to load the lab.

Secure Privileged Exec Mode

1) Set the enable password **Flackbox2** on R1 to secure access to Privileged Exec (Enable) mode.

2) Exit to User Exec mode.

3) Enter Privileged Exec mode.

4) Set the enable secret **Flackbox1**.

5) Exit to User Exec mode.

6) Do you expect to be able to enter Privileged Exec mode using the password **Flackbox2**? Why or why not? Verify this.

7) Show the running configuration on R1. Can you read the enable password and secret in plain text?

8) Ensure that passwords will not show in plain text in the output of 'show' commands.

9) Verify the enable password is now encrypted when you show the running configuration.

Secure Remote Telnet and SSH Access

10) Enable synchronous logging on R1 and ensure administrators are logged out after 15 minutes of activity on the console and virtual terminal lines 0-15.

11) Allow the administrator workstation at 10.0.0.10 to Telnet into R1 using the password **Flackbox3**. Ensure no other host has Telnet access to the router.

12) Ensure that users attempting to Telnet into the router see the message "Authorised users only"

13) Verify you can Telnet into R1 from PC1 and enter Privileged Exec mode. Close the Telnet session when done.

14) Verify Telnet access fails from PC2.

15) Configure R1 so that administrators will be prompted to enter a username and password when they attempt to Telnet into the router. Use username **admin** and password **Flackbox4**.

16) Verify you are prompted for a username and password when you attempt to Telnet to the router.

17) Allow the administrator workstation at 10.0.0.10 to SSH into R1. Use the domain name **flackbox.com** and a 768 bit key.

18) Verify you can SSH into R1 from PC1. Close the session when done.

19) Do you expect to be able to SSH to R1 from PC2? Why or why not? Verify this.

20) You can currently access R1 using either Telnet or SSH. Telnet is an insecure protocol as all communication is sent in plain text. Configure R1 so that only SSHv2 remote access is allowed.

21) Verify you cannot Telnet into R1 from PC1 but can SSH. Exit when done.

22) What username and password do you need to use to login when you connect directly to R1 with a console cable?

23) Configure R1 to require no username but a password of **Flackbox5** to login over the console connection.

24) Verify you can access R1 over the console connection and enter Privileged Exec mode.

NTP Network Time Protocol

25) Configure R1 to synchronise its time with the NTP server at 10.0.1.100. Set the timezone as Pacific Standard Time which is 8 hours before UTC.

26) Check the current time on the router and verify it is synchronised with the NTP server.

Switch Management

27) Configure SW2 with IP address 10.0.1.50 for management on VLAN 1. Ensure the switch has connectivity to other IP subnets.

    (Note that it is best practice to NOT use VLAN 1 for any production traffic in a real world network and we would normally have a separate dedicated IP subnet for management traffic. We are using VLAN 1 in our lab environment to simplify the topology)