Lab 02 – Securing Network Device Protocols

In this lab, you will begin to bring multiple security technologies together to harden the network devices. After all, these are the devices that allow the network to function and pass packets so the business can run efficiently. You will begin to limit administrative access to key networking devices, restricting access with ACLs, add authentication to NTP, log critical alerts and messages via Syslog, enable and limit access to SSH, and add authentication to routing updates to limit rogue routers from obtaining and participating in routing updates.

You will begin with a guided network design, move into basic network connectivity, then begin to secure the networking environment. Once you have everything configured correctly, you will then verify everything works as intended. If it doesn't, then you may need to circle back to revisit and reconfigure a technology or two. This should be a cyclic process until everything is working as intended and specified. The goal of this lab is to bring together multiple protocols into one secure network design and implementation.

Complete the following tasks:

TASK ONE: Develop the Network Topology

1. Open Cisco Packet Tracer. You will use this application to design, implement and troubleshoot your network.

    a) Create a network topology using the following criteria:

    - ✓ ISP is a Cisco 1941 router
    - ✓ ISP-Sw is a Cisco 2960 switch
    - ✓ Corp is a Cisco 1941 router
    - ✓ Corp-Sw is a Cisco 2960 switch
    - ✓ RemoteA is a Cisco 1941 router
    - ✓ RemoteA-Sw is a Cisco 2960 switch
    - ✓ RemoteB is a Cisco 1941 router
    - ✓ RemoteB-Sw is a Cisco 2960 switch
    - ✓ Internet-PC is a Generic PC
    - ✓ Internet-Server is a Generic Server
    - ✓ Corp-PC is a Generic PC
    - ✓ Corp-Mgmt is a Generic PC
    - ✓ Corp-Server is a Generic Server
    - ✓ RemoteA-PC is a Generic PC
    - ✓ RemoteB-PC is a Generic PC

    - ✓ Internet-PC's FastEthernet connection is connected to ISP-Sw's interface F0/5
    - ✓ Internet-Server's FastEthernet connection is connected to ISP-Sw's interface F0/10
    - ✓ ISP-Sw's interface G0/1 is connected to ISP's interface G0/1

- ✓ ISP’s interface S0/0/0 (DCE) is connected to Corp’s interface S0/0/0
- ✓ Corp’s interface S0/1/0 (DCE) is connected to RemoteA’s interface S0/1/0
- ✓ Corp’s interface S0/1/1 (DCE) is connected to RemoteB’s interface S0/1/1
- ✓ Corp’s interface G0/1 is connected to Corp-Sw’s interface G0/1
- ✓ Corp-PC’s FastEthernet connection is connected to Corp-Sw’s interface F0/5
- ✓ Corp-Mgmt’s FastEthernet connection is connected to Corp-Sw’s interface F0/6
- ✓ Corp-Server’s FastEthernet connection is connected to Corp-Sw’s interface F0/10
- ✓ RemoteA’s interface G0/1 is connected to RemoteA-Sw’s interface G0/1
- ✓ RemoteB’s interface G0/1 is connected to RemoteB-Sw’s interface G0/1
- ✓ RemoteA-PC’s FastEthernet connection is connected to RemoteA-Sw’s interface F0/5
- ✓ RemoteB-PC’s FastEthernet connection is connected to RemoteB-Sw’s interface F0/5
- ✓ Internet-PC's RS232 connection is connected to the console line on ISP
- ✓ Corp-PC's RS232 connection is connected to the console line on Corp
- ✓ RemoteA-PC's RS232 connection is connected to the console line on RemoteA
- ✓ RemoteB-PC's RS232 connection is connected to the console line on RemoteB

- ✓ Internet-PC's IP Address is 192.168.168.5/24
- ✓ Internet-Server’s IP Address is 192.168.168.10/24
- ✓ Corp-PC’s IP Address is 172.16.32.5/24
- ✓ Corp-Mgmt’s IP Address is 172.16.32.6/24
- ✓ Corp-Server’s IP Address is 172.16.32.10/24
- ✓ RemoteA-PC's IP Address is 172.16.41.5/24
- ✓ RemoteB-PC's IP Address is 172.16.42.5/24
- ✓ ISP's interface G0/1 IP Address is 192.168.168.1/24
- ✓ ISP’s interface S0/0/0 IP Address is 192.168.169.1/24
- ✓ Corp's interface G0/1 IP Address is 172.16.32.1/24
- ✓ Corp's interface S0/0/0 IP Address is 192.168.169.2/24
- ✓ Corp's interface S0/1/0 IP Address is 172.16.33.1/24
- ✓ Corp's interface S0/1/1 IP Address is 172.16.34.1/24
- ✓ RemoteA's interface G0/1 IP Address is 172.16.41.1/24
- ✓ RemoteA's interface S0/1/0 IP Address is 172.16.33.2/24
- ✓ RemoteB's interface G0/1 IP Address is 172.16.42.1/24
- ✓ RemoteB's interface S0/1/1 IP Address is 172.16.34.2/24

You should specify all of your IP Addresses and subnet masks (in bit notation) within individual text boxes on your topology diagram for each interface or device that has one assigned.

Please NOTE: The router model you will be using in Cisco Packet Tracer is the 1941 Router. You will need to power down the router and add the two WIC-2T modules in the HWIC slots. The switch model you will be using is the 2960 Layer 2 Switch.

Make sure you save your packet tracer file frequently (and make a backup copy) so you do not lose your work in case the application crashes. It is always nice to revert back to a previous backup in case the file is corrupt.

TASK TWO: Understanding Types of Network Traffic and Protocols

1. Research two different protocols from the following list:
   - ✓ OSPF
   - ✓ SYSLOG
   - ✓ SSH
   - ✓ NTP
2. For each protocol, provide the following:
   - ✓ A conceptual protocol flow diagram consisting of a source and a destination
   - ✓ The ports used in the network communication
   - ✓ The types of authentication available

TASK THREE: Configuration

1. On each router, configure the following:
   a) hostname
   b) an encrypted privileged mode password of 'cisco'
   c) the IP Address and Subnet Mask of the interfaces in use
   d) enable the interfaces in use
   e) configure the clock rate of 2000K on the DCE interfaces
   f) enable 'logging synchronous' on the console line
   g) password of 'cisco' on the console line
   h) enable a login prompt to appear when consoling into the router from the PC
   i) enable 'logging synchronous' on the first five virtual terminal lines
   j) password of 'cisco' on the first five virtual terminal lines
   k) enable a login prompt to appear when using the first five virtual terminal lines (ie: when you telnet or SSH into the router from the PC you should receive a login prompt)
   l) save your current configuration file to nvram (ie: the filename should be 'startup-config)

2. Verify each PC is able to ping its default gateway. Please keep in mind that a default gateway is the router interface IP Address that is closest to the host (ie: PC).

3. Verify connectivity from each router to each router. For instance, you should be able to ping from the ISP Router to the Corp Router; however you should not be able to ping from the ISP Router to the RemoteA Router (yet).

4. On each router, display the routing table by issuing the “show ip route” command in the CLI.

5. Configure the dynamic routing protocol of OSPF between Corp, RemoteA and RemoteB using MD5 Authentication. Display your dynamic routing protocol properties with issuing a “show ip protocol” in the CLI.
6. Configure a default static route using the upstream router’s IP Address as the next hop address on Corp. And, then configure a default static route on ISP pointing back down to Corp. Display the IPv4 routing table again. Do you notice a difference from earlier?

7. Test connectivity from one PC to another PC in the topology. Are you able to successfully ping from each PC within the topology to every other PC in the topology? You should be able to at this point.

8. Make sure you have clicked on “Options” -> “Preferences” and the “Always Show Port Labels in Logical Workspace” check box is checked. This will display all of the interfaces on all of the devices within the topology.

9. Now that you have basic connectivity in place, let’s secure the network. Configure secure administrative access.

   a) On every router:
      - ✓ Create a username of “cisco” with a password of “cisco”.
      - ✓ Create a username of “yourfirstname.yourlastname” with another password.
      - ✓ Setup local authentication for the first five virtual terminal lines (ie: line vty 0 4).
      - ✓ SSH version 2.
      - ✓ Restrict virtual terminal access to only allow SSH (ie: transport input ssh).

   b) On Corp:
      - ✓ Construct an access list only allowing Corp-Mgmt to SSH into Corp.
      - ✓ Apply this to the virtual terminal lines you configured above.

10. Configure NTP and Syslog:

   a) On Corp-Server:
      - ✓ Enable the NTP Server so that this is the NTP Master.
      - ✓ Specify an MD5 authentication key of your choosing.
      - ✓ Enable the Syslog Server.

   b) On Corp, RemoteA and RemoteB:
      - ✓ Setup NTP so these routers are NTP clients.
      - ✓ Make sure you are using an MD5 authentication key.
      - ✓ Enable logging so that all log messages are sent to the Syslog server.

11. Ensure that your topology diagram is aesthetically pleasing. Think like a consultant. Would you submit this to a customer or your manager?

12. Save your .pkt file as YOURFIRSTNAME.YOURLASTNAME-Lab02.pkt

13. Create a document for your lab report that will be saved and submitted as a .pdf. You will use this to formally document and capture your lab results as you continue through the lab.

DELIVERABLE:

1. Complete a professional write-up and include the following information:

a. **Description:** Brief description, such as an executive summary, depicting an overall view of what topic or technology you are concentrating on within this lab. Keep this short and to the point. Think like a consultant and be mindful that what you are providing should represent you as a professional in the industry.

b. **Task Two Flow Diagrams and Answers:** Be thorough, provide the necessary topologies, illustrations, and answer all questions.

c. **Topology/Diagram:** Take a screenshot of your topology from your Packet Tracer file (do not include the menu bars or tools in your screenshot). Paste this screenshot below your executive summary with the heading of "Topology".

d. **Key Syntax:** Sometimes it's nice to include key syntax used. Include a table of CLI syntax used to complete this lab. Remember to list the command used in the first column and a description of what the command does in your own words in the second column.

e. **Verification:** Provide key screenshots that display verification that all tasks and all steps of the lab have been completed. For instance, if you have an FTP server in the topology, capture the screen after you've transferred a file from the host to the server. Make sure you provide a description of what the screenshot is showing. Do not simply add the screenshot and state, "here is the screenshot". These descriptions and screenshots should paint a story of the work you put into this lab and verify you have successfully completed each lab step. Be thorough and professional!

f. **Conclusion:** Wrap up your lab report with a short conclusion. If something did not work, state it. If everything did work successfully, state that as well.

g. **References:** Make sure you include any works cited here as well as throughout your lab report. If you looked something up, include it.

2. Submit your .pkt and .pdf files to the appropriate assignment within iLearn.

(Please do not zip these files nor should you submit multiple .pngs, .gifs, .jpgs, etc…)

Good Luck with your lab!