**Lab Report: Linux Servers**

**Objectives**

* Use the Linux command line to identify servers running on a computer.
* Explore server and client interactions.
* Use the **telnet** command to test TCP services .

**Theory**

* **Servers** are programs that provide specific information or services upon request.
* **Clients** are programs that request information from servers.
* In Linux, running programs are called **processes**. Some processes are background services started at boot time.
* Common tools:
  + **ps** → displays running processes.
  + **netstat** → shows active network connections and listening servers.
  + **telnet** → used to test TCP services (default port 23, but you can specify others like 80 for HTTP or 22 for SSH) .

**Steps & Commands**

**Part 1: Servers**

1. **Access Command Line**
   * Log in to the VM as analyst (password: cyberops).
   * Open terminal .
2. **Display Services Running**
3. sudo ps -elf

Shows all background processes .

1. **View Process Hierarchy**
2. sudo /usr/sbin/nginx
3. sudo ps -ejH

Displays running process tree, highlighting nginx service .

1. **List Active Network Connections**
2. netstat

Shows active internet connections .

1. **Detailed Network Servers**
2. sudo netstat -tunap

Displays TCP/UDP connections with process info .

**Part 2: Using Telnet to Test TCP Services**

* **Telnet** is an insecure remote shell (no encryption).
* Still useful for testing TCP services by connecting directly to a port.
* Example commands:
* telnet 127.0.0.1 80
* telnet 127.0.0.1 22
* On port **80** (HTTP): server responds with HTTP messages (e.g., 400 Bad Request if invalid input).
* On port **22** (SSH): server responds with SSH version, rejects invalid input .

**Questions (from lab document)**

1. What command shows all processes running on the system?
   * ps -elf
2. Which command shows the process hierarchy?
   * ps -ejH
3. How can you list active TCP/UDP connections with process info?
   * netstat -tunap
4. Why is Telnet not recommended for remote access?
   * Because it sends data in **clear text**, no encryption.
5. How can Telnet still be useful?
   * For **testing TCP services** quickly.
6. How is the process hierarchy represented by **ps**?

through indentation.

1. Why was it necessary to run **ps** as root (prefacing the command with **sudo**)?

**Some processes do not belong to the analyst user and may not be displayed if ps was executed as analyst, which is a regular user account.**

1. What is the meaning of the **–t**, **-u**, **–n**, **–a** and **–p** options in **netstat**?

-a: shows both listen and non-listening sockets. -n: use numeric output (no DNS, service port or username resolution), -p: show the PID of the connection owner process. -t: shows TCP connections. –u: shows UDP connections

9. What is **nginx**? What is its function?

nginx is a lightweight webserver. A quick google search is extremely helpful on finding information about unidentified processes.

10. Why was the error sent as a web page?

Nginx is a web server and as such, only speaks the HTTP protocol.

1. Use Telnet to connect to port 68. What happens? Explain.

Unable to connect because the connection is refused. Telnet is a TCP-based protocol and will not be able to connect to UDP ports.

1. What are the advantages of using netstat?

Netstat allows for an analyst to display all the connections currently present on a computer. Source and destination addresses, ports, and process IDs can also be displayed, providing a quick overview of all connections present on a computer.

1. What are the advantages of using Telnet? Is it safe?

Yes, as long it is not used as a remote shell. It is perfectly safe to quickly test or gather information about a given network service.

**Learning Outcomes**

* Gained experience using **ps** to explore processes.
* Learned how to use **netstat** to identify servers and network connections.
* Understood the role of **nginx** as a web server.
* Practiced using **telnet** to connect to specific TCP ports and interpret responses.
* Recognized why **SSH is preferred over Telnet** for secure remote access.

**Summary**

In this lab, we used the Linux command line to identify and analyze running servers. Using ps and netstat, we viewed processes and active connections. We tested services with telnet on different ports (HTTP and SSH), observing how each responded to input. This demonstrated the differences in protocol behavior and highlighted why Telnet is insecure but useful for quick TCP service testing.

**Outputs**









