**Internet Security-COS80013**

**Lab – 1 Report**

|  |
| --- |
| Student ID: 104837257 |
| Student Name: Arun Ragavendhar Arunachalam Palaniyappan |
| Lab Name: Lab 1 |
| Lab Date: 07/03/2025 |
| Tutor: Yasas Akurudda Liyanage Don |

**Title:**

Basics of Cyber Security, Introduction to Linux and Practising basic commands on a Linux Virtual Machine

**Introduction:**

The overall purpose of the lab was to learn the basics of Cyber Security, getting familiar with Linux and basic bash commands on the Command Line Interface.

**Methodology:**

**System Navigation Commands:**

* **ls, ls -l** – Lists out the files in a directory.
* **pwd** -Shows current directory.
* **cd, cd /, cd ~, cd ../** -Changes directories.

**Process Management Commands:**

* **ps, ps -al** - Displays running processes.
* **history, history | more, history -c** -shows command history.
* **top** - Shows real-time system process usage.

**Networking Commands:**

* **ping <hostname>** - Testing the connectivity.
* **nslookup <domain>, dig <domain> -** Obtain DNS information.
* **netstat, netstat | grep CONNECTED, netstat | grep ESTABLISHED** -Monitoring network connections.

**File Handling Commands:**

* **cat > <filename> -** Creates a file.
* **rm -i <filename>** - Deletes a file.
* **touch <filename>** - Creates an empty file.
* **vi <filename>** - Allows to edit a file.

**System Information Commands:**

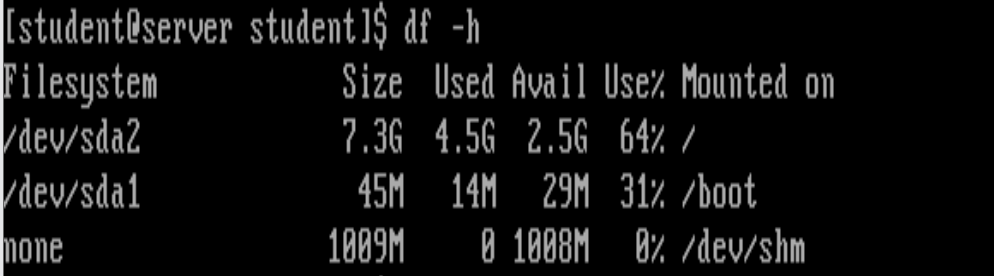
* **uname, uname -a** - Displays system details.
* **df, df -hi** - Shows disk usage.
* **echo $PATH** - Displays system paths.
* **who, whoami** - Identifies logged-in users.

**Shutdown and Access Commands:**

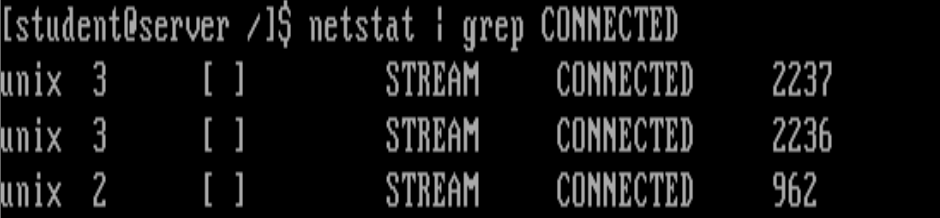
* **exit** - Logs out.
* **halt, poweroff** - Shuts down the system.

**Screenshots and Data Recording:**

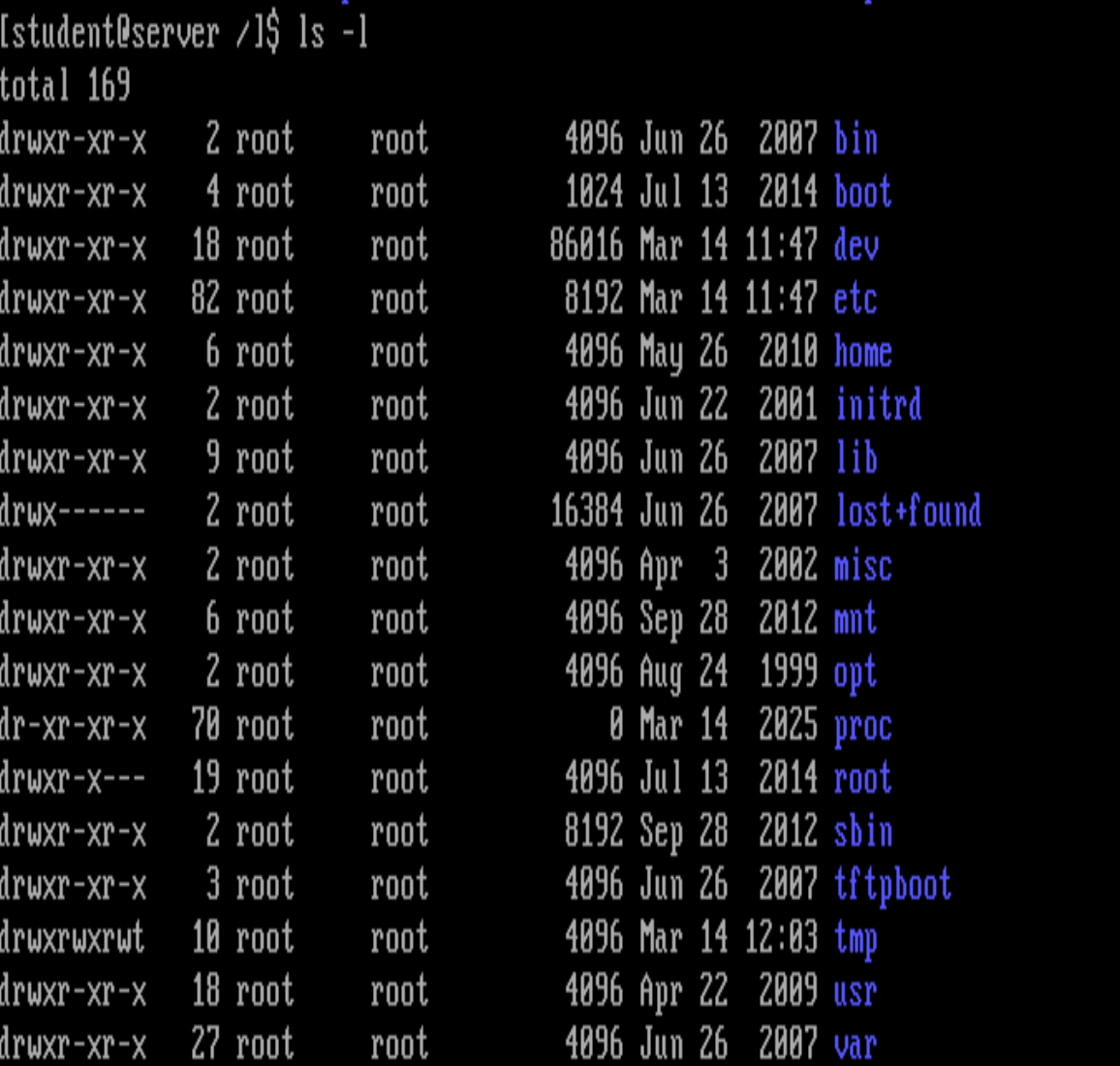
* Ran **df -h** to check the disk space usage.

****

* Ran **netstat | grep CONNECTED** to monitor network connections.

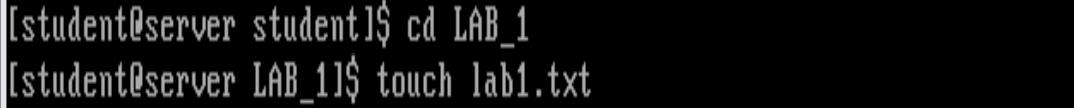
****

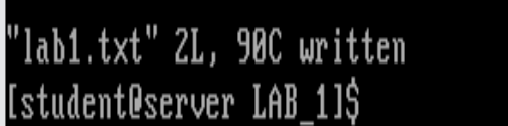
* Executed **ls -l** to check the file permissions.

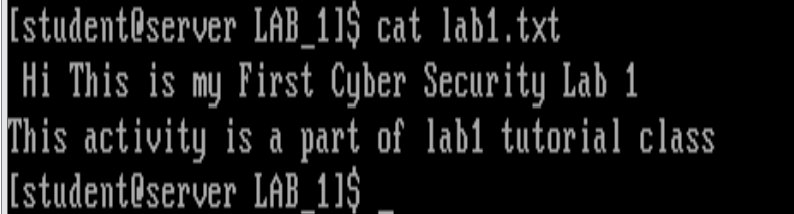
****

* Ran **mkdir LAB\_1** to create a new directory, then **touch lab1.txt** to create an empty file, **vi lab1.txt** to edit the file and then viewing the file using **cat lab1.txt.**

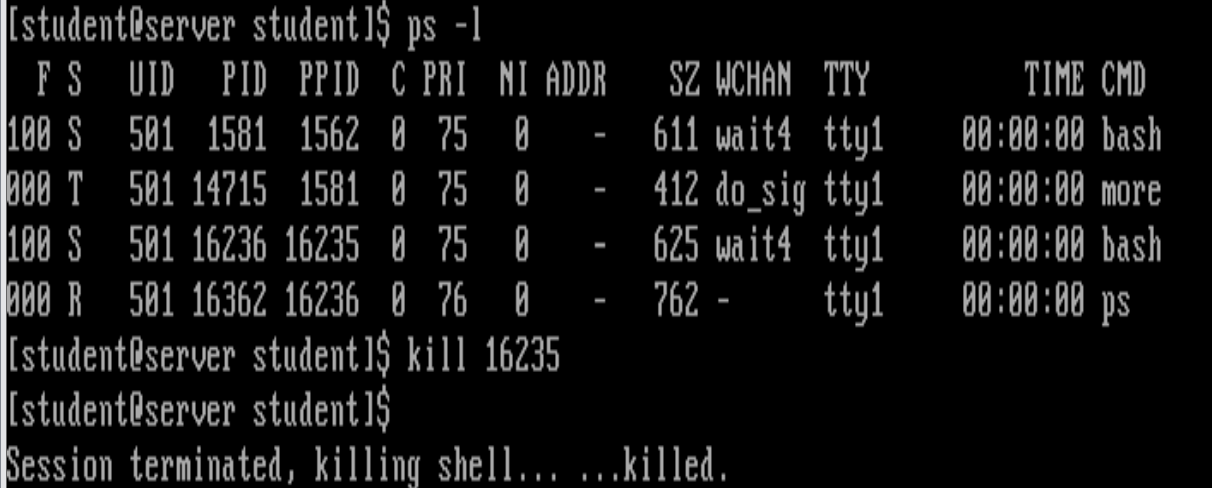
****

****

****

****

* Ran **kill 16235** to stop a process that was running.

****

**Discussion and Lessons learnt from the Lab**

This lab helped in strengthening the foundations for learning further in the cyber security and networking domain.

1. Learnt about a broad overview of the domain

* The main concept of CIA (Confidentiality, Integrity, Availability).
* Different type of cyber threats
* Impact of a specific threat, Tactics and Techniques used by Hackers and Defenders
* Was introduced to the MYTRI ATT&CK Matrix and NIST framework

1. Hands on with Linux

* Installed VMware Workstation Pro, Red Hat Linux and started a red Hat Linux VM instance
* Practised basic bash commands on the CLI.
* commands for basic navigation, creating/ deleting a directory, network diagnostics and system monitoring, etc.
* Learned about file permissions and execution rules in Linux environments.

1. Basic Networking Concepts

* SSH (encrypts data before communication, more secure)
* Telnet (sends data as plain text, more vulnerable)

1. Tried to access Swinburne’s Mercury server, but was denied access.

**Limitations:**

It was an introductory lab, hence, there were not many limitations to be observed yet. The focus was mainly on basic CLI commands and not into much deeper security or network configurations yet.

Network adapter settings were not configured yet; hence some network connection commands and configuration commands were not working as expected. A deeper analysis using security tools like Wireshark were not used in this lab 1, and no threat simulations were performed.

Log files (/var/log/auth.log, /var/log/syslog) were not analysed, limiting the ability to detect unauthorized access or security breaches.