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.

```
[student@server student]$ df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda2             7.3G  4.5G  2.5G  64% /
/dev/sda1              45M   14M   29M  31% /boot
none                 1009M     0 1008M   0% /dev/shm
```

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

```
[student@server /]$ netstat | grep CONNECTED
unix  3      [ ]         STREAM     CONNECTED     2237
unix  3      [ ]         STREAM     CONNECTED     2236
unix  2      [ ]         STREAM     CONNECTED     962
```

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

```
[student@server /]$ ls -l
total 169
drwxr-xr-x    2 root     root         4096 Jun 26  2007 bin
drwxr-xr-x    4 root     root         1024 Jul 13  2014 boot
drwxr-xr-x   18 root     root        86016 Mar 14 11:47 dev
drwxr-xr-x   82 root     root         8192 Mar 14 11:47 etc
drwxr-xr-x    6 root     root         4096 May 26  2010 home
drwxr-xr-x    2 root     root         4096 Jun 22  2001 initrd
drwxr-xr-x    9 root     root         4096 Jun 26  2007 lib
drwx------    2 root     root        16384 Jun 26  2007 lost+found
drwxr-xr-x    2 root     root         4096 Apr  3  2002 misc
drwxr-xr-x    6 root     root         4096 Sep 28  2012 mnt
drwxr-xr-x    2 root     root         4096 Aug 24  1999 opt
dr-xr-xr-x   70 root     root            0 Mar 14  2025 proc
drwxr-x---   19 root     root         4096 Jul 13  2014 root
drwxr-xr-x    2 root     root         8192 Sep 28  2012 sbin
drwxr-xr-x    3 root     root         4096 Jun 26  2007 tftpboot
drwxrwxrwt   10 root     root         4096 Mar 14 12:03 tmp
drwxr-xr-x   18 root     root         4096 Apr 22  2009 usr
drwxr-xr-x   27 root     root         4096 Jun 26  2007 var
```

- 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.**

```
[student@server student]$ mkdir LAB_1
[student@server student]$ ls
fix      hello1.asm  LAB_1        shell2      socket.asm  sproc
fixasm   iptalk      mytelnet.asm  shell2.asm  socket.s
hello1   iptalk.c    nsmail        socket      socket.txt
```

```
[student@server student]$ cd LAB_1
[student@server LAB_1]$ touch lab1.txt
```

```
"lab1.txt" 2L, 90C written
[student@server LAB_1]$
```

```
[student@server LAB_1]$ cat lab1.txt
 Hi This is my First Cyber Security Lab 1
This activity is a part of lab1 tutorial class
[student@server LAB_1]$ _
```

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

```
[student@server student]$ ps -l
  F S   UID   PID  PPID  C PRI  NI ADDR    SZ WCHAN  TTY          TIME CMD
100 S   501  1581  1562  0  75   0    -   611 wait4  tty1     00:00:00 bash
000 T   501 14715  1581  0  75   0    -   412 do_sig tty1     00:00:00 more
100 S   501 16236 16235  0  75   0    -   625 wait4  tty1     00:00:00 bash
000 R   501 16362 16236  0  76   0    -   762 -      tty1     00:00:00 ps
[student@server student]$ kill 16235
[student@server student]$
Session terminated, killing shell... ...killed.
```

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

2. 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.

3. Basic Networking Concepts
   - SSH (encrypts data before communication, more secure)
   - Telnet (sends data as plain text, more vulnerable)

4. 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.