LINUX FUNDAMENTALS

ASSIGNMENT REPORT

Peter Kinyumu,
cs-sa07-24067,
May 9th, 2024.

1. INTRODUCTION

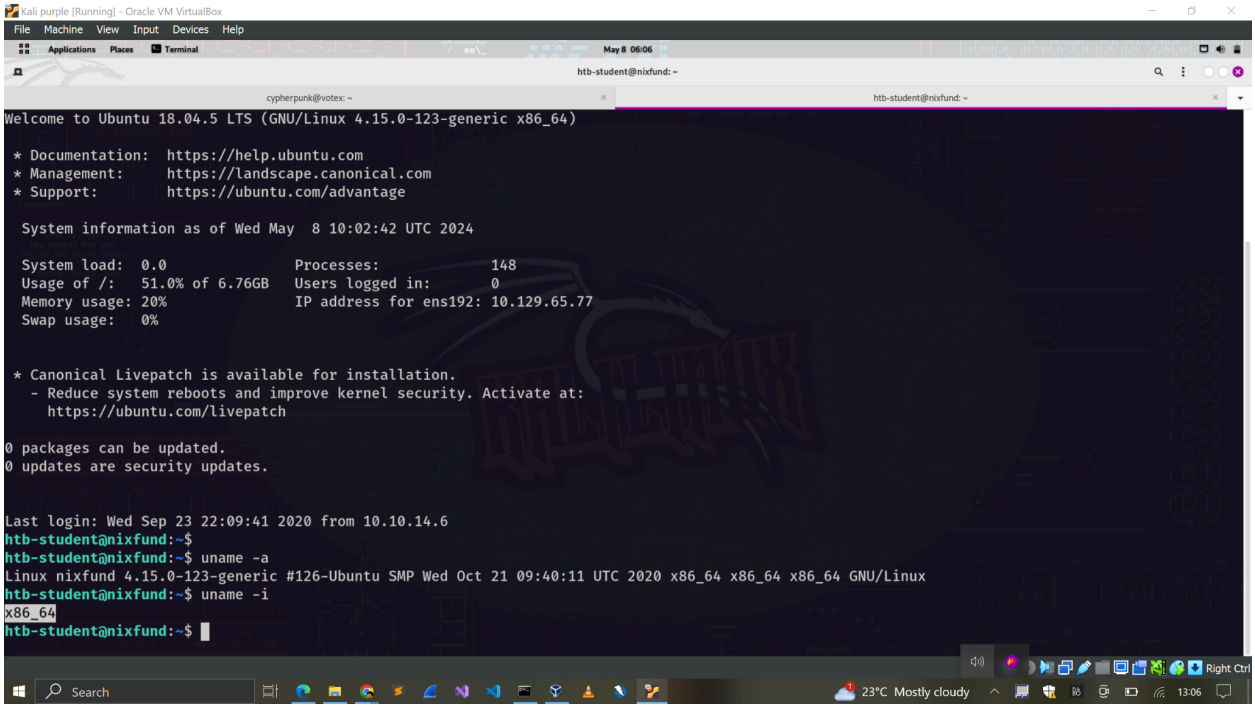
This report documents my completion of the **Linux Fundamentals** Module on the HacktheBox platform. The module covered the fundamentals required to work comfortably with the Linux operating system and shell. Linux is an open-source operating system that is essential for cybersecurity analysts because it contains tools that can help automate tasks and manipulate files easily.

The module covered various topics, from Linux structure, an introduction to the shell, text manipulation, user management, and network management.

2. ANSWERS TO QUESTIONS

System Information

a. Find out the machine hardware name and submit it as the answer.

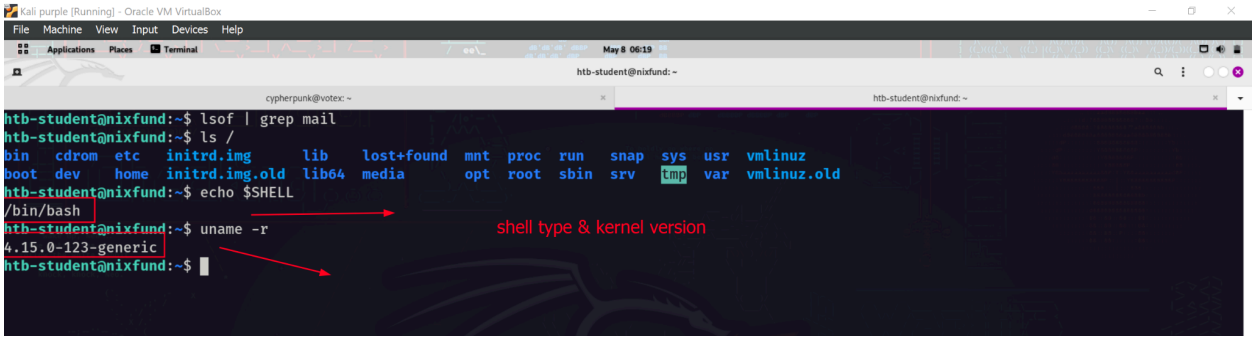


b. What is the path to htb-student's home directory?

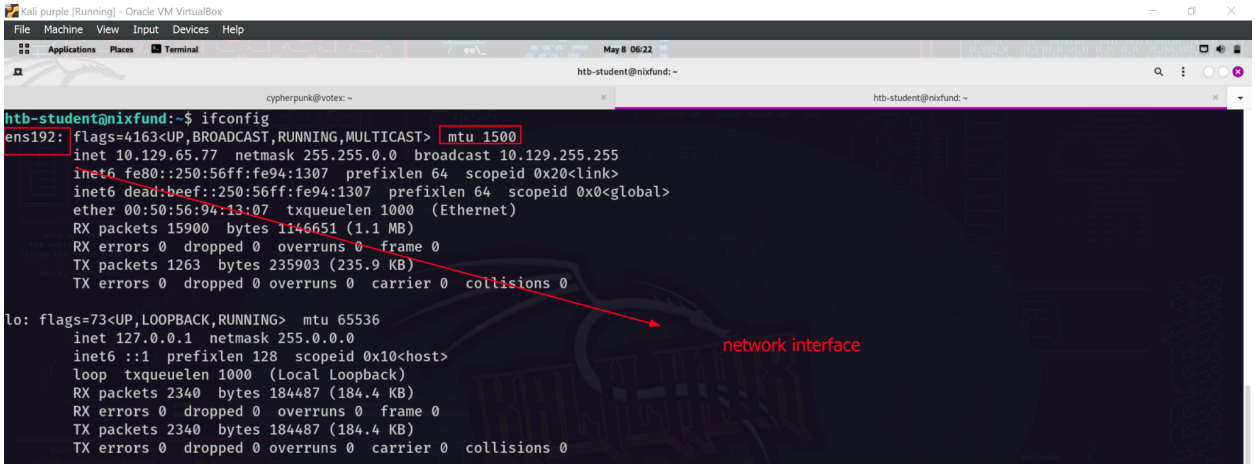
Running the command **pwd** at the home directory displays **/home/htb-student** as the path.

c. Which shell is specified for the htb-student user?

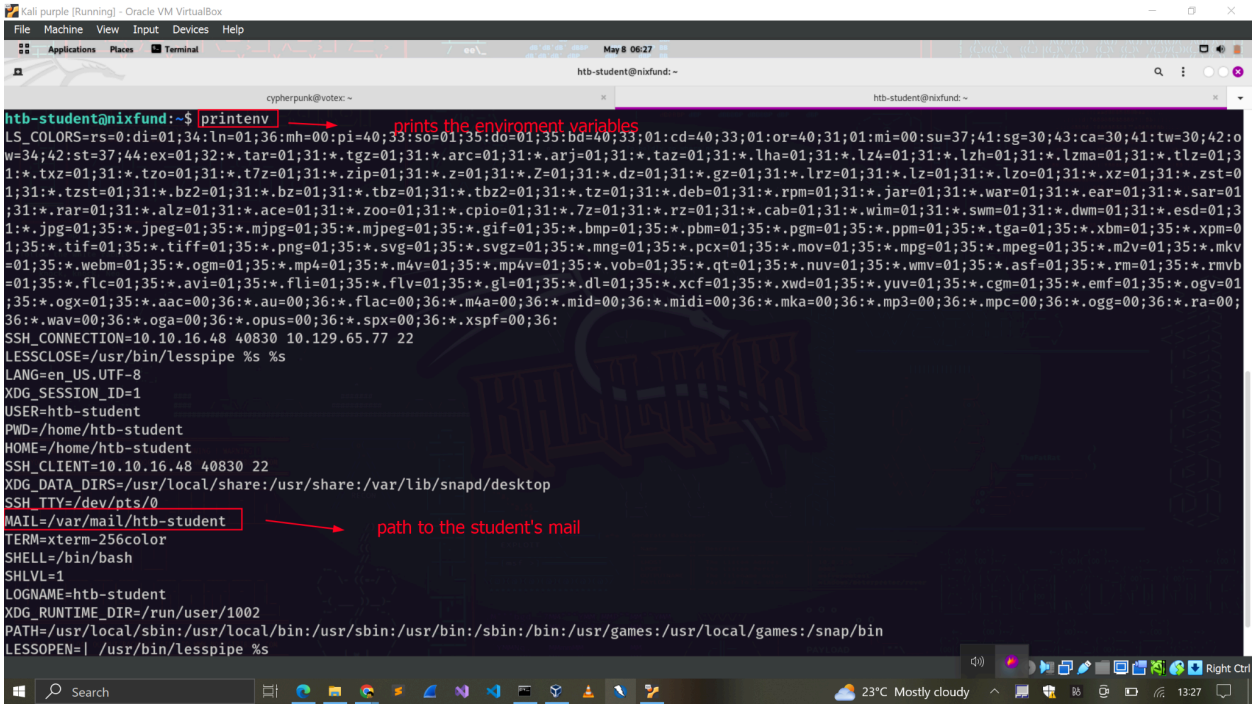
d. Which kernel version is installed on the system? (Format: 1.22.3)



e. What is the name of the network interface that MTU is set to 1500?

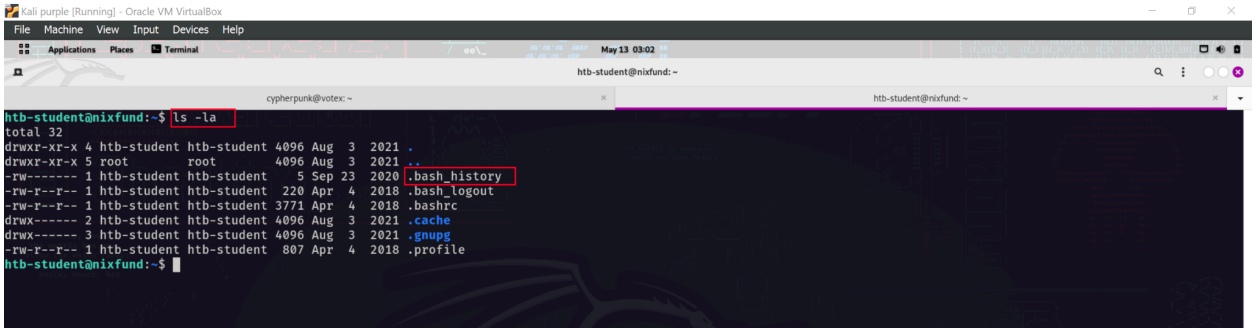


f. What is the path to the htb-student's mail?

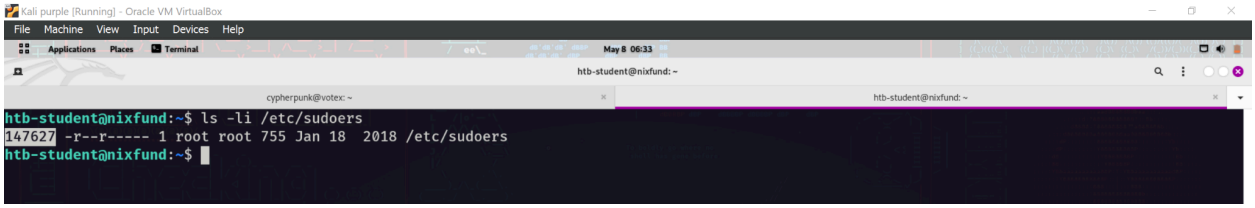


Navigation - Your way around Linux

a. **What is the name of the hidden "history" file in the htb-user's home directory?**

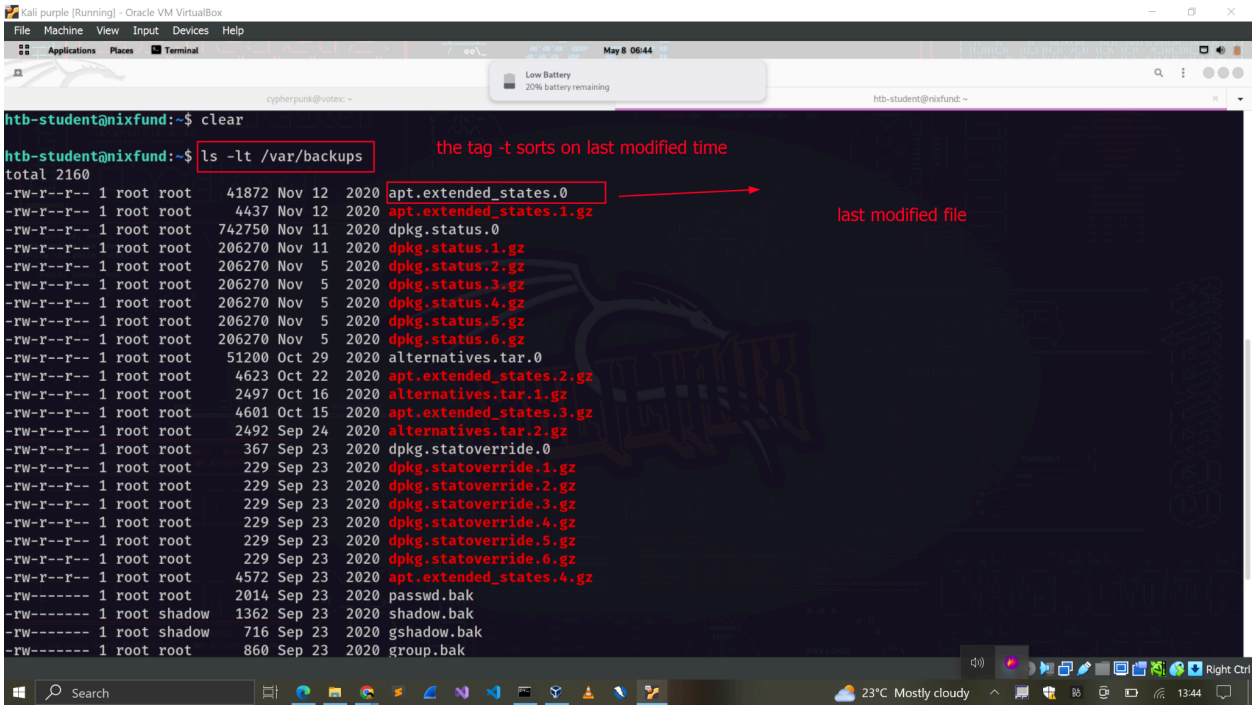


b. **What is the index number of the "sudoers" file in the "/etc" directory?**

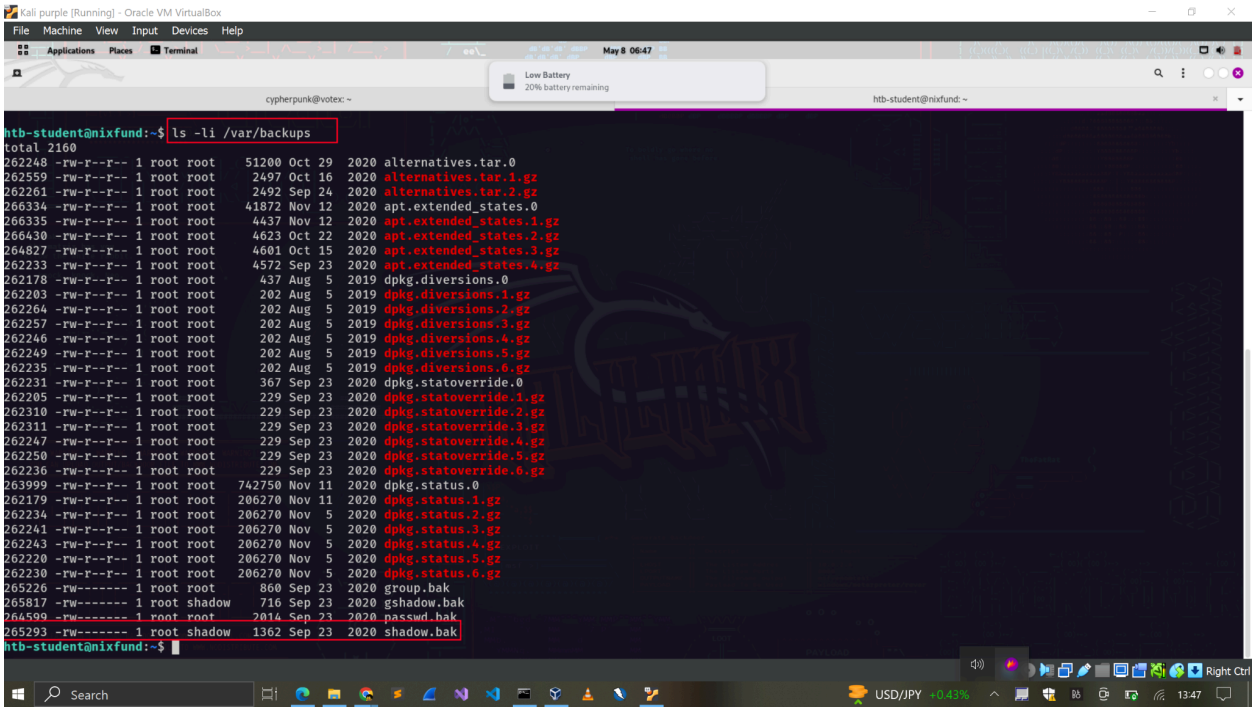


Working with files

a. **What is the name of the last modified file in the "/var/backups" directory?**

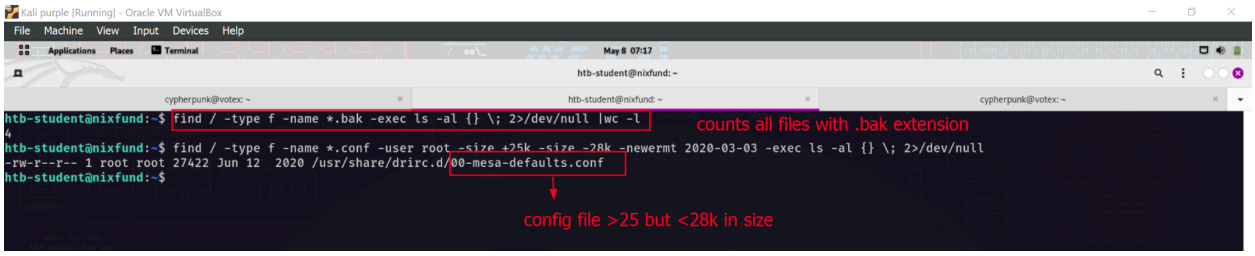


b. **What is the inode number of the "shadow.bak" file in the "/var/backups" directory?**



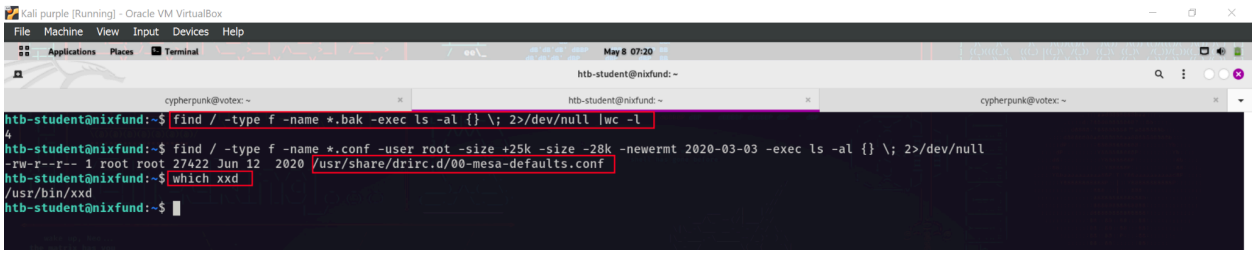
Finding files

a. **What is the name of the config file that has been created after 2020-03-03 and is smaller than 28k but larger than 25k?**



b. **How many files exist on the system that have the ".bak" extension?**

c. **Submit the full path of the "xxd" binary.**

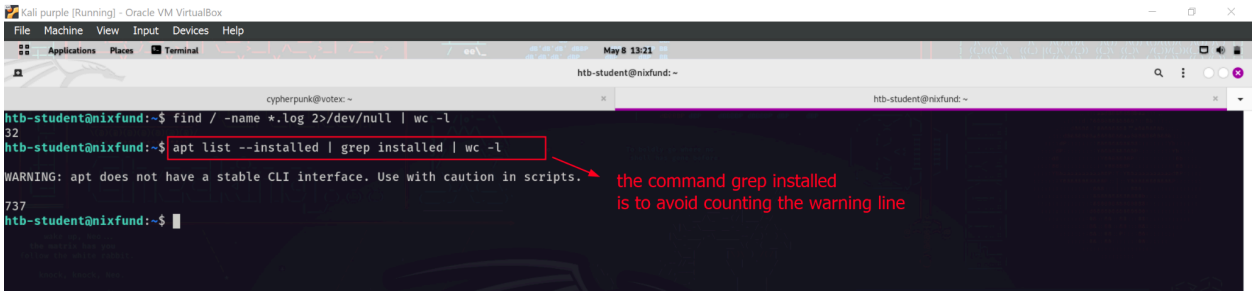


File descriptors

This section focused on using pipes to redirect STDOUT from one program to be processed by another.

a. **How many files exist on the system that have the ".log" file extension?**
   The command *find / -name *.log 2>/dev/null | wc -l* displays the count all all log files within the system. The first part of the command before the pipe will display all files with a **.log** extension and the rest part of the command counts the lines.

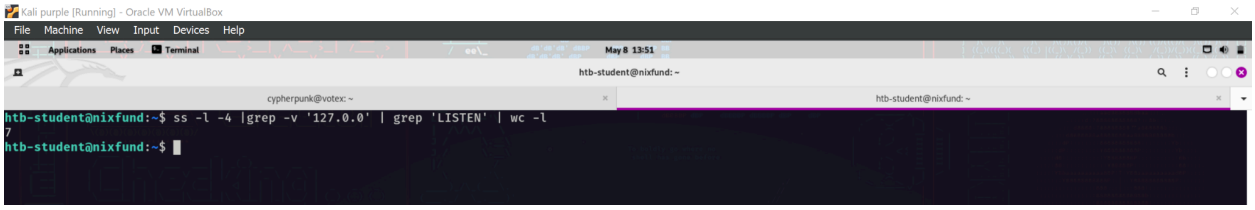
b. **How many total packages are installed on the target system?**



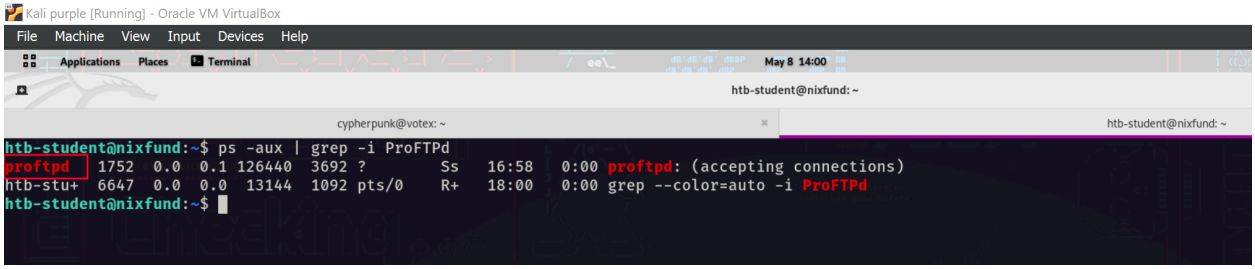
Filter contents

This section aimed to teach how to use pagers like **less** and **more** to read files interactively and to filter specific contents from files using **grep**.

a. **How many services are listening on the target system on all interfaces? (Not on localhost and IPv4 only)**
   The command ss is used to investigate sockets, which are bound connections of IP addresses with their port number. The option - 4 displays only IPv4 addresses. grep -v then performs an invert match of localhost addresses. grep 'LISTEN' finally matches all listening services.



b. **Determine what user the ProFTPd server is running under. Submit the username as the answer.**



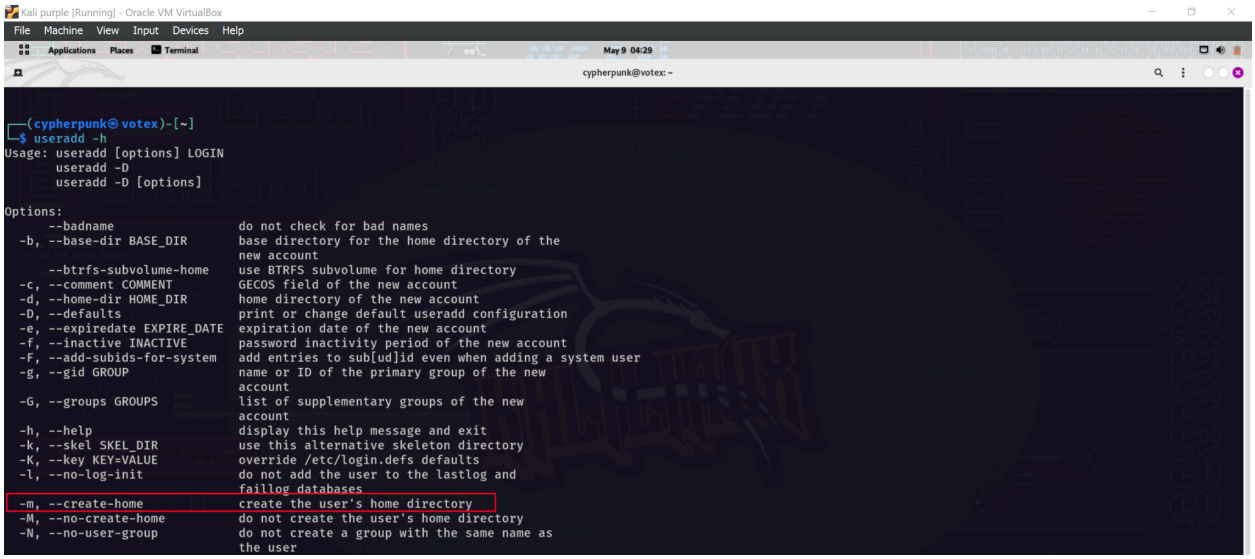
c. **Use cURL from your Pwnbox (not the target machine) to obtain the source code of the "https://www.inlanefreight.com" website and filter all unique paths of that domain. Submit the number of these paths as the answer.**

With the command curl https://www.inlanefreight.com/ | grep Eo "https:\/\/.{0,3}\.inlanefreight\.com[^\"\']*"| sort -u | wc -l I retrieved the count for all unique paths of that domain to be 34.

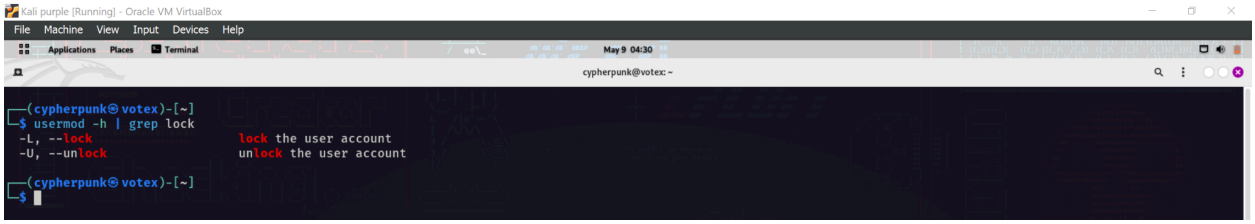
User Management

User management is essential for Linux administration. Creating new users and adding users to specific groups are important for access control.

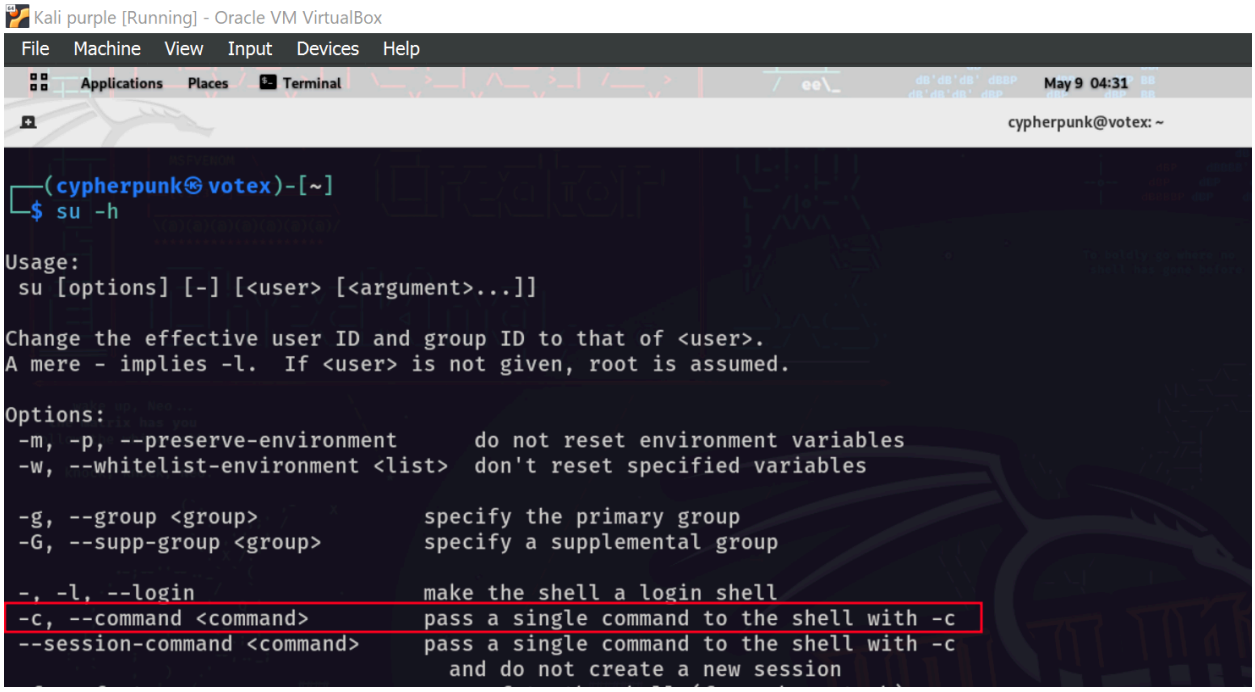
a. **Which option needs to be set to create a home directory for a new user using "useradd" command?**



b. **Which option needs to be set to lock a user account using the "usermod" command? (long version of the option)**

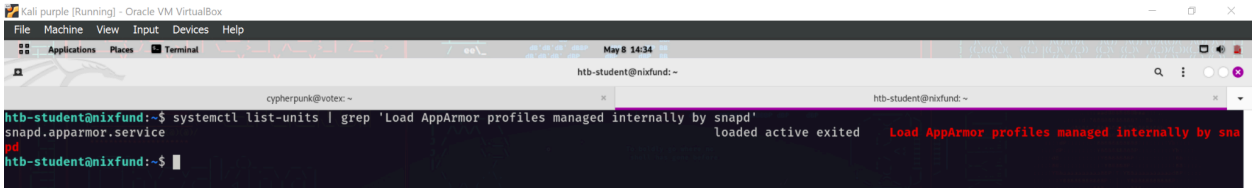


c. **Which option needs to be set to execute a command as a different user using the "su" command? (long version of the option)**



Service, Process Management and Task scheduling

a. **Use the "systemctl" command to list all units of services and submit the unit name with the description "Load AppArmor profiles managed internally by snapd" as the answer.**

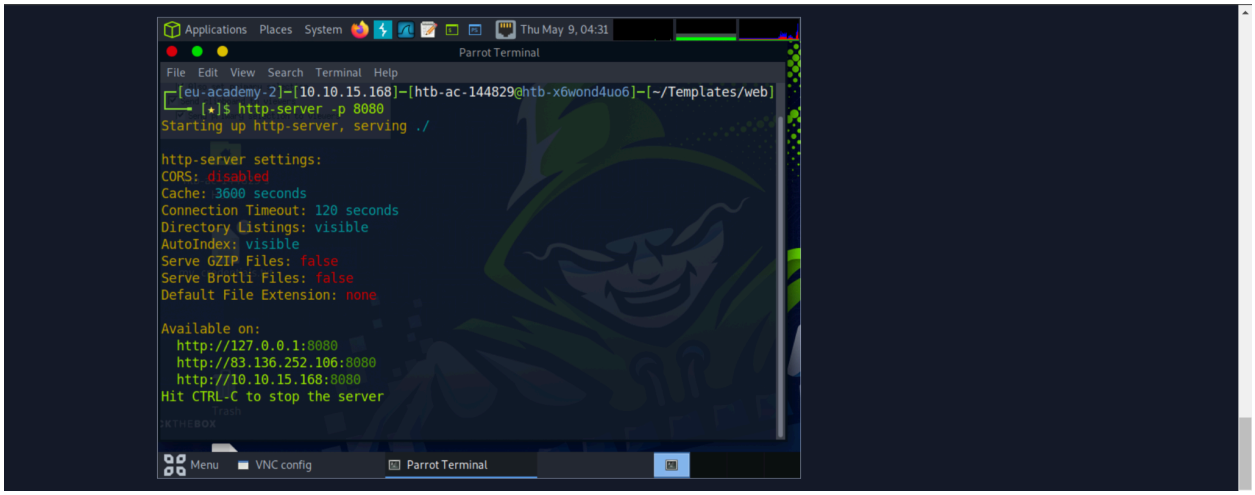


b. **What is the type of the service of the "syslog.service"?**

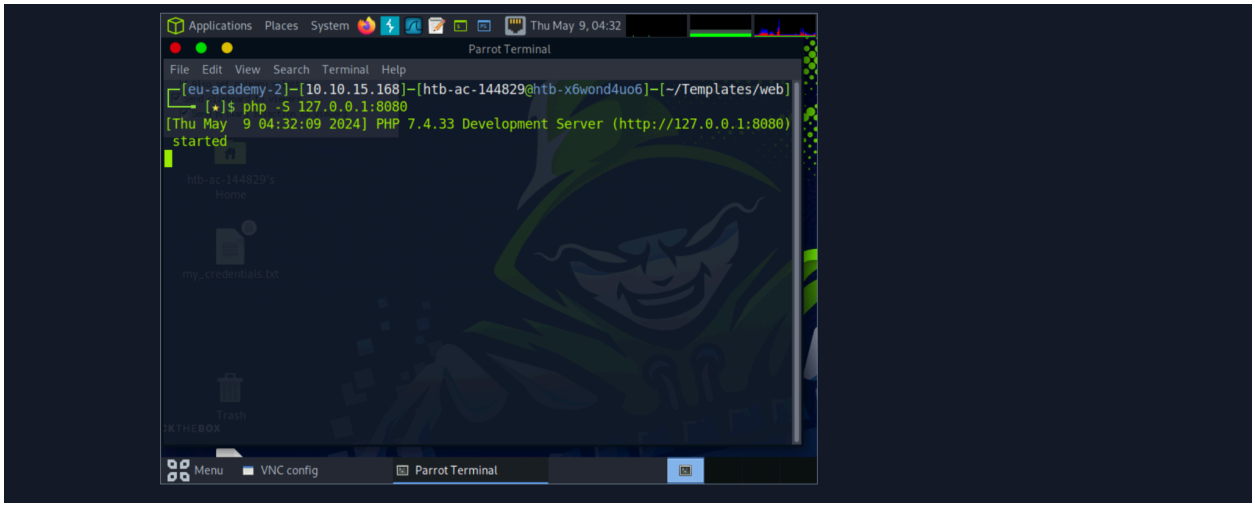
Web services

a. **Find a way to start a simple HTTP server inside Pwnbox or your local VM using "npm". Submit the command that starts the web server on port 8080 (use the short**

argument to specify the port number).



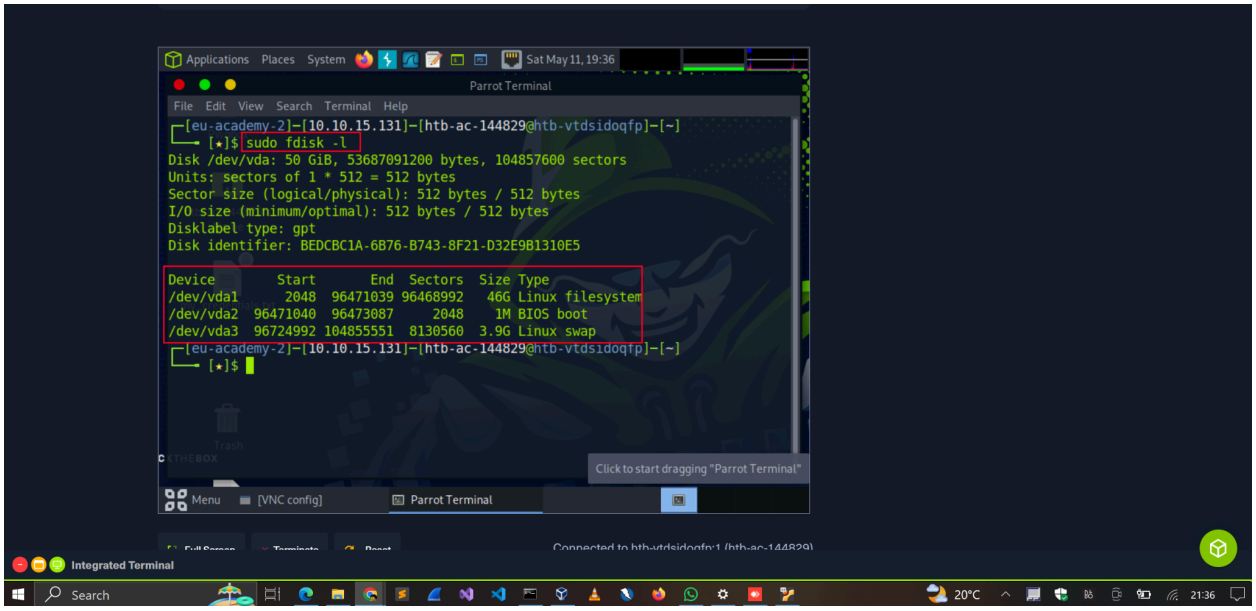
b. Find a way to start a simple HTTP server inside Pwnbox or your local VM using "php". Submit the command that starts the web server on the localhost (127.0.0.1) on port 8080.



File system Management

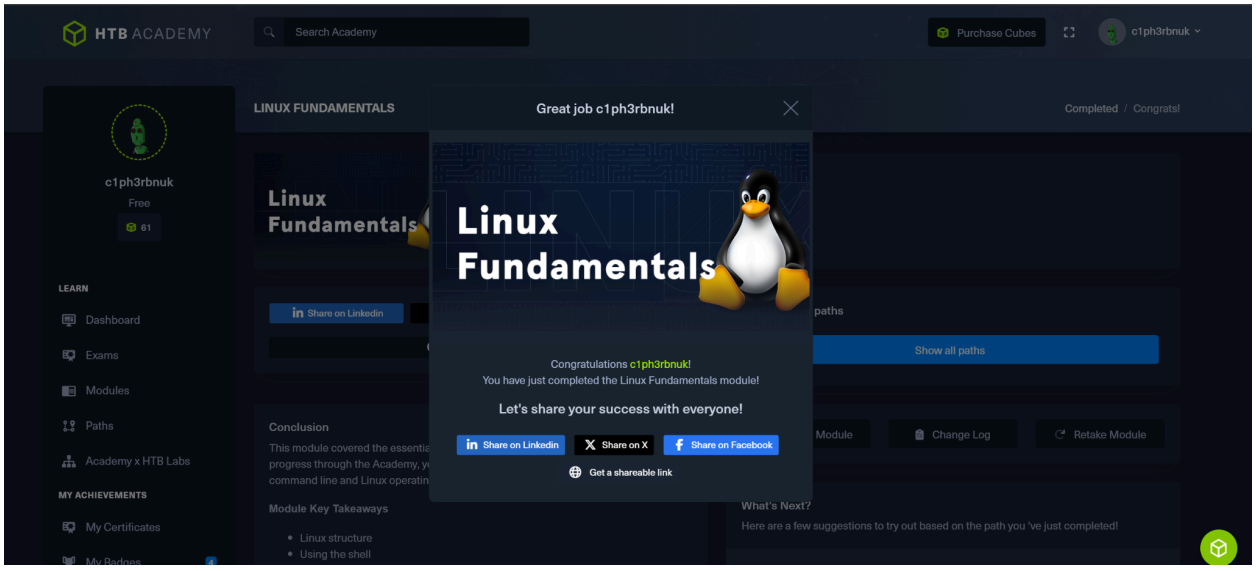
a. How many partitions exist in our Pwnbox? (Format: 0)

There are only 3 partitions, /dev/vda1, /dev/vda2, /dev/vda3 as shown below.



3. MODULE COMPLETION

The following is a sharable link to the badge I earned after completing the module.
https://academy.hackthebox.com/achievement/144829/18



4. CONCLUSION

To summarise, this module provided great insights and an overview of the Linux system. I have learned how to navigate around Linux with commands like **cd**, find and locate files using **find locate** commands, manipulate texts with **sed, cut and awk,** manage users, packages, and disks, backup files, schedule tasks, harden the security of the system and many more.
It was fun and enjoyable to explore Linux. I look forward to practising more and hopefully using the techniques that I have learned during the later chapters of the course.