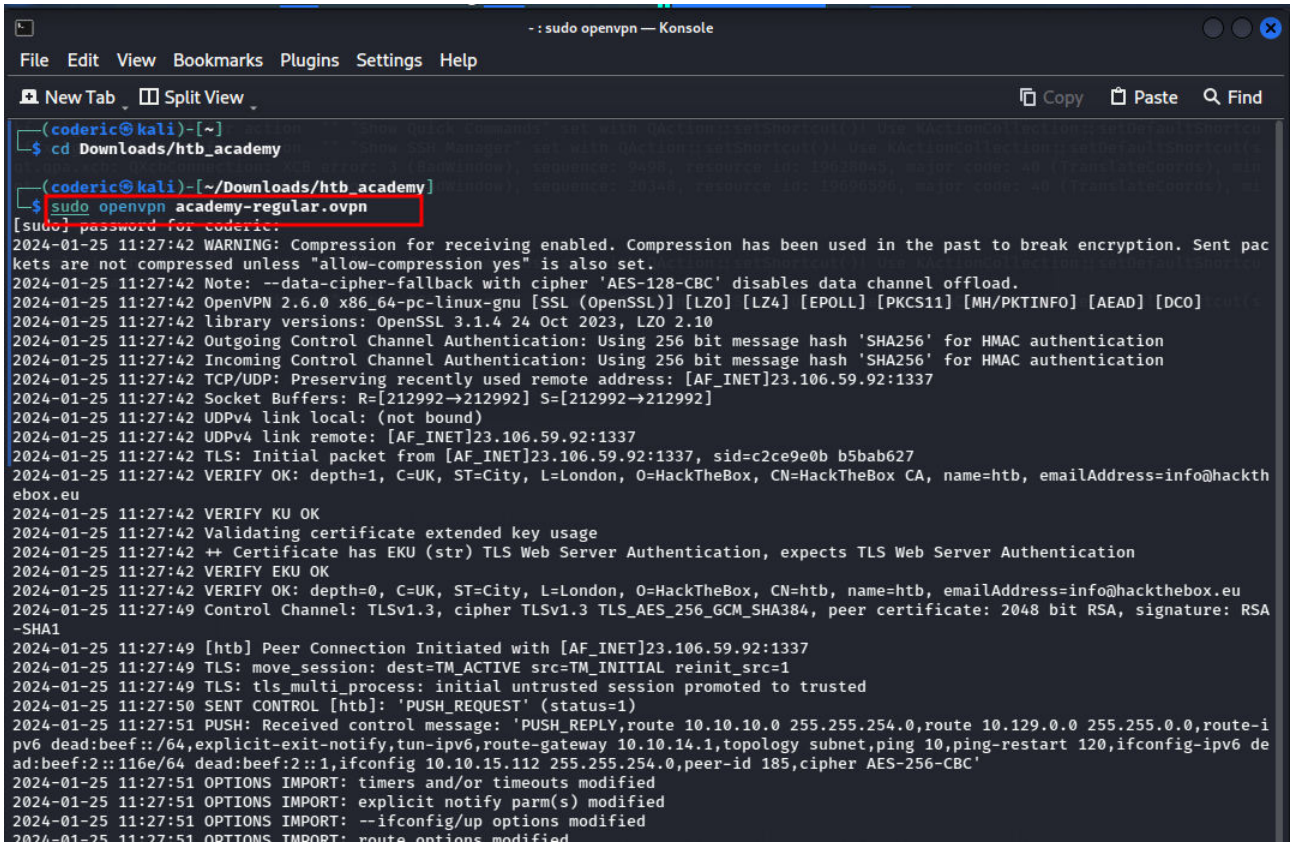
Eric Mwenda

Linux Fundamentals
https://academy.hackthebox.com/achievement/596337/18

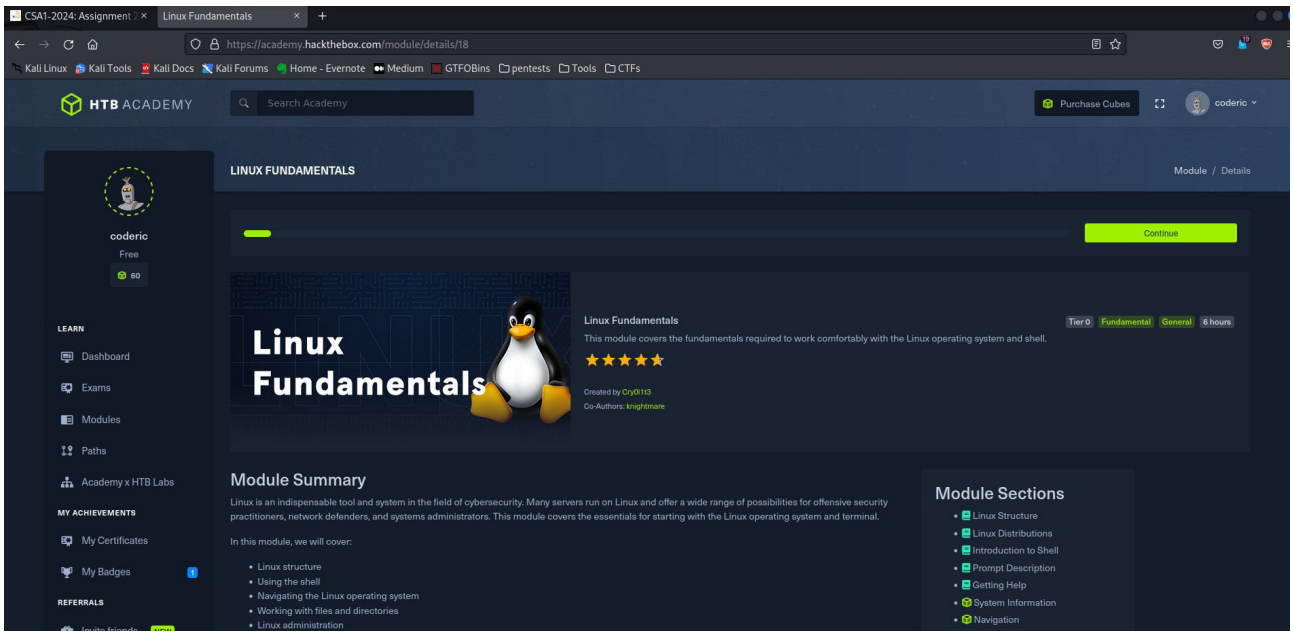
Process made to connect to my Virtual Machine:

1. I downloaded the vpn file provided in the module.
2. Opened my terminal.
3. Located to where the file was downloaded in, that is the Downloads folder.
4. Opened it with the command **sudo openvpn academy-regular.ovpn**

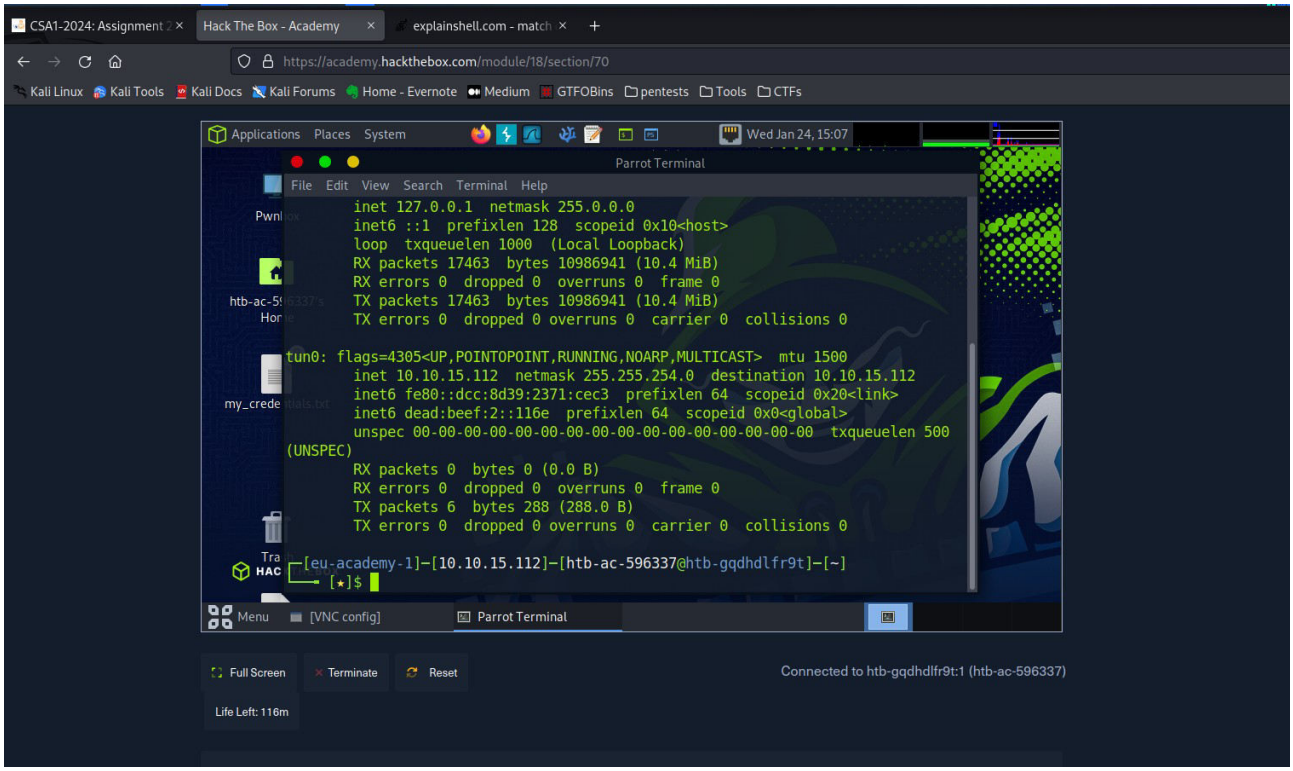


Linux Fundamentals module location:

After login into HackTheBox Academy, I searched for “Linux Fundamentals” under the search option hence landing on my assignment.



Starting to the htb virtual machine:

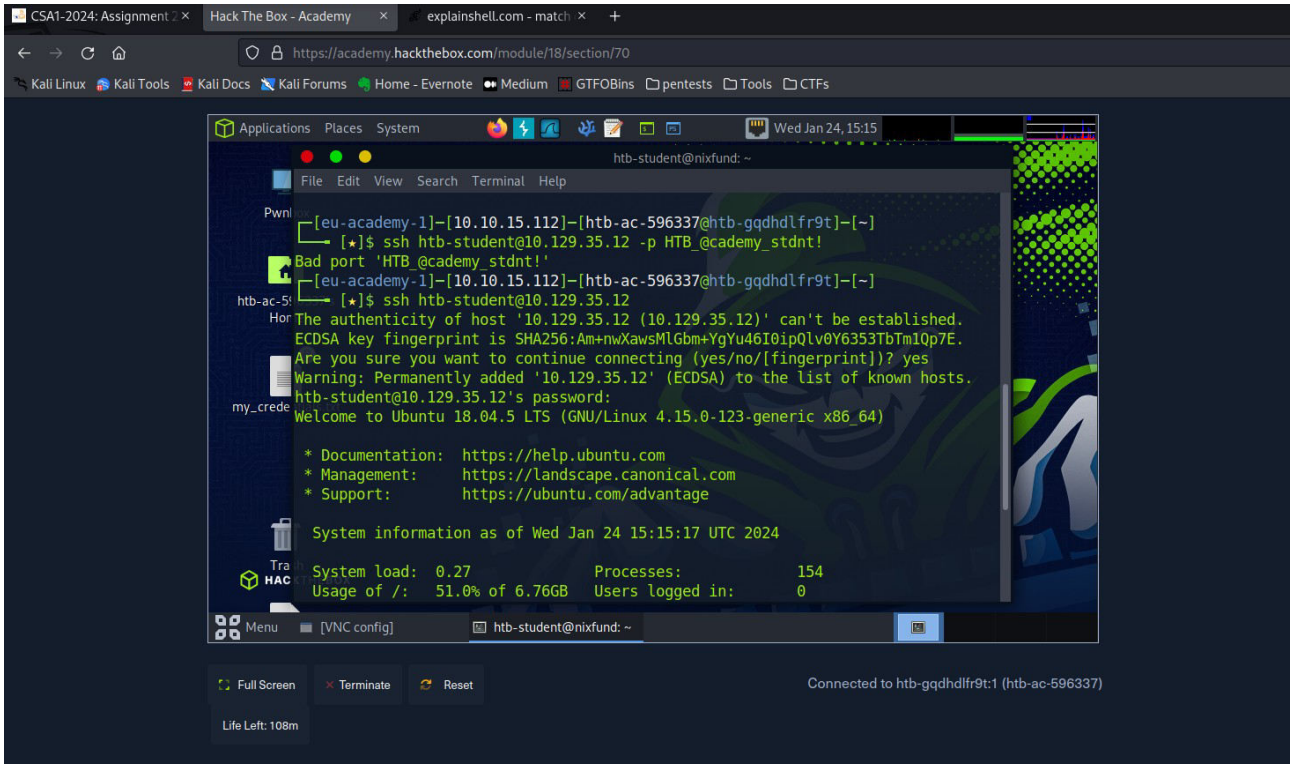


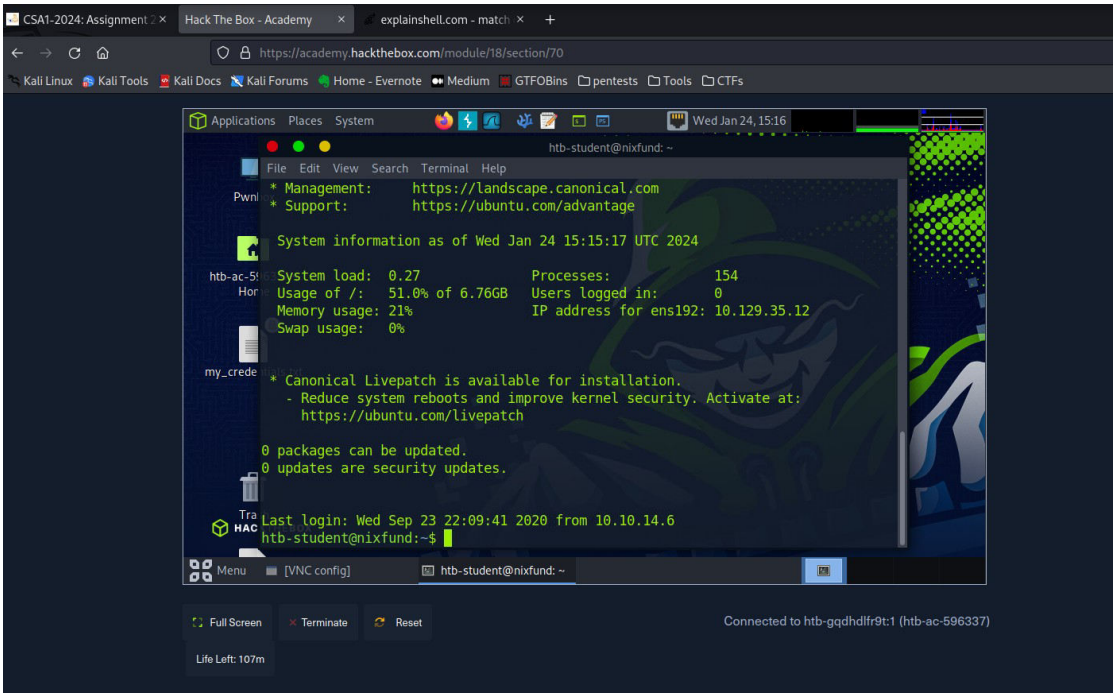
Connection to the machine using ssh protocol:

username: htb-student
Password: HTB_@cademy_stdnt!

IP: 10.129.35.12

ssh htb-student@10.129.35.12



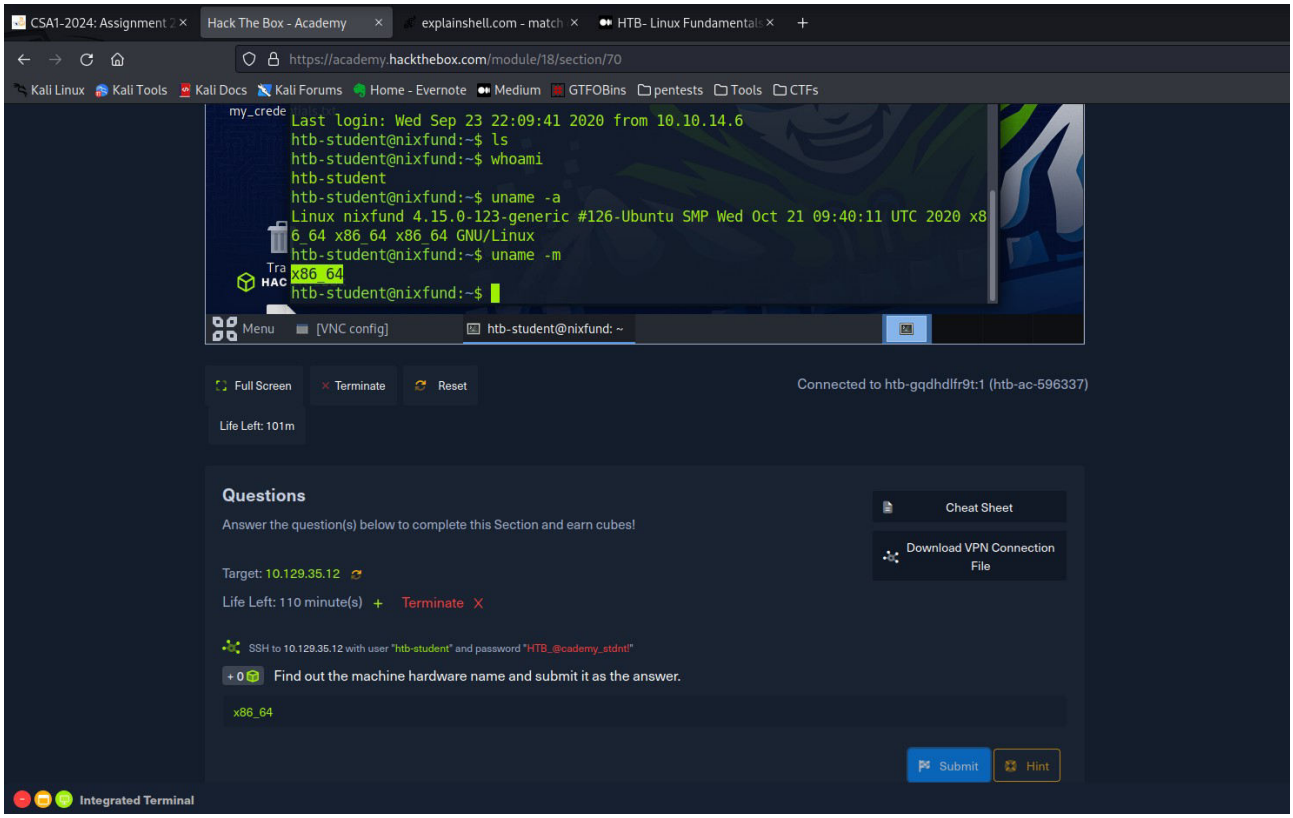


Here is the Target shell.

SYSTEM INFORMATION

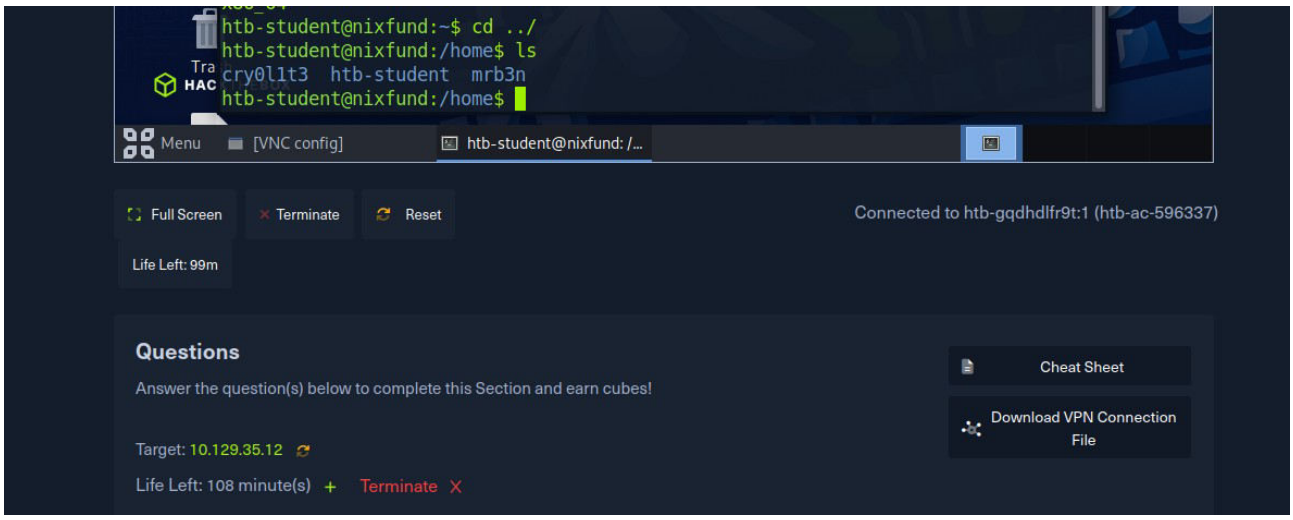
Find out the machine hardware name and submit it as the answer.
To find out the machine name I used command “uname” and attribute “-n”
Command used:- uname -n

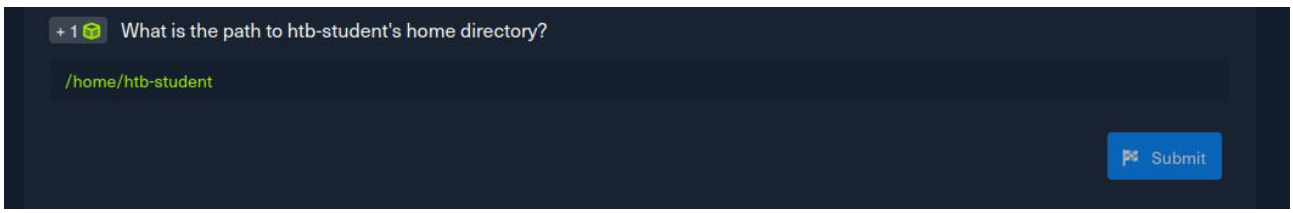
ANS: x86 64



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

To navigate in the htb-student I went back one directory, then keyed in the command “ls” to vie all files available in that directory. Here is where I found the “htb-student” directory and without much I could see the path was **ANS: /home/htb-student**





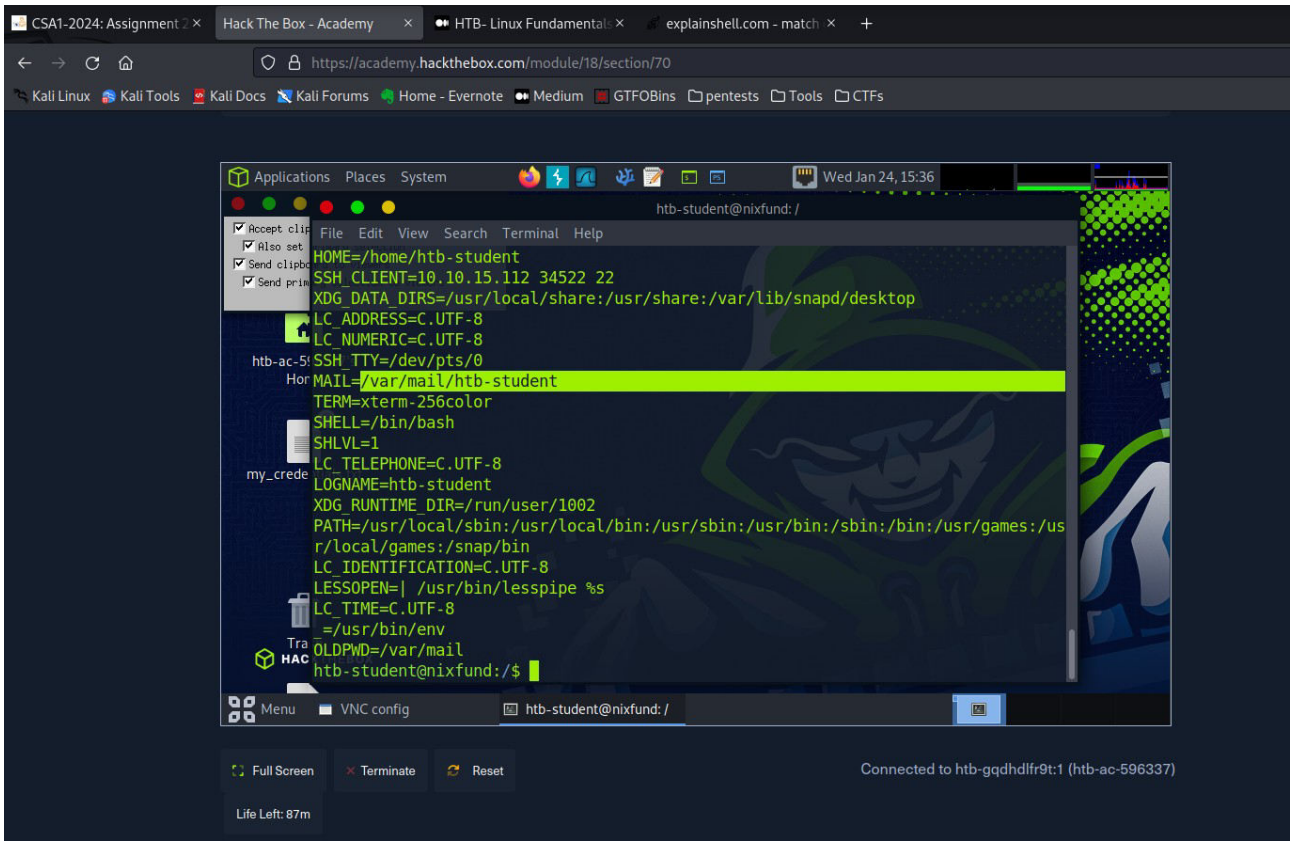
What is the path to the htb-student's mail?

To get this path I used env and grep command

- env is a shell command used to either print a list of environment variables.
- Grep command can be used to find or search a regular expression or a string in a text file.

Command used:- env | grep MAIL

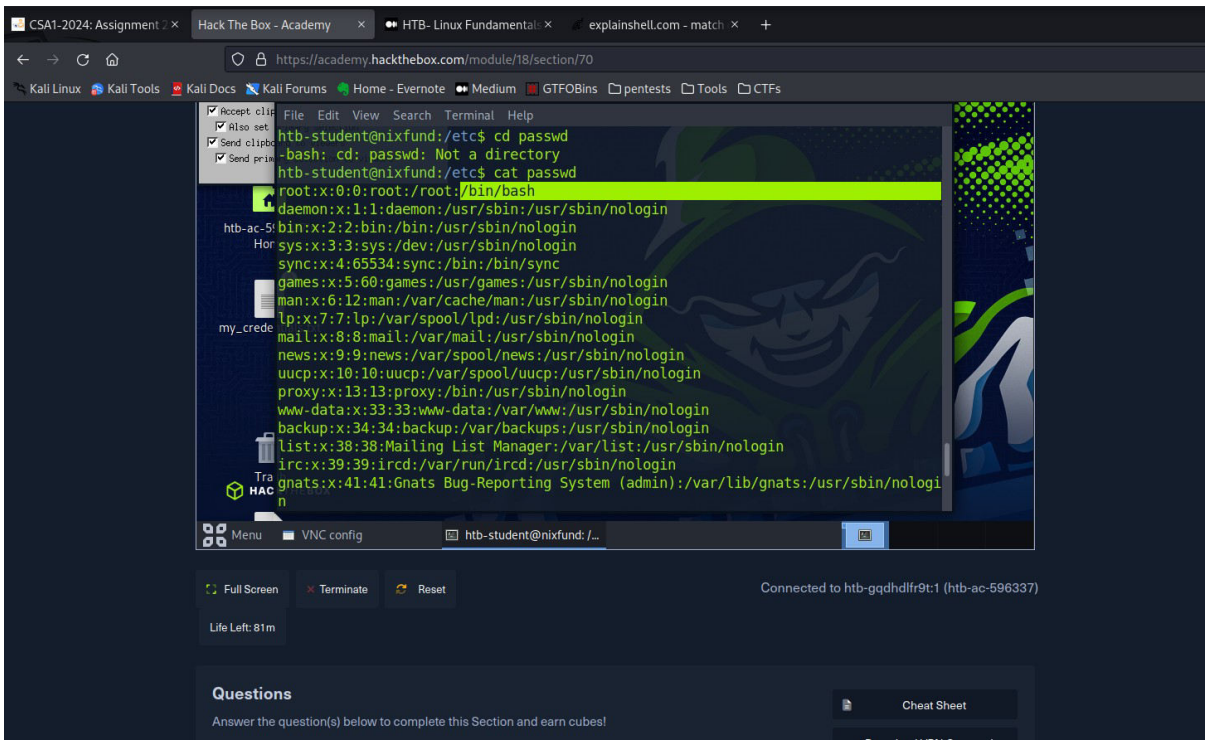
ANS: /var/mail/htb-student



Which shell is specified for the htb-student user?

The shell information is stored in the etc/passwd file we can open this file to view the information on which shell is specified to the user “htb-student”

I navigated to etc/passwd and run the file using the command “cat passwd” the file we are looking for is the one that has root permissions which is:- **ANS bin/bash**

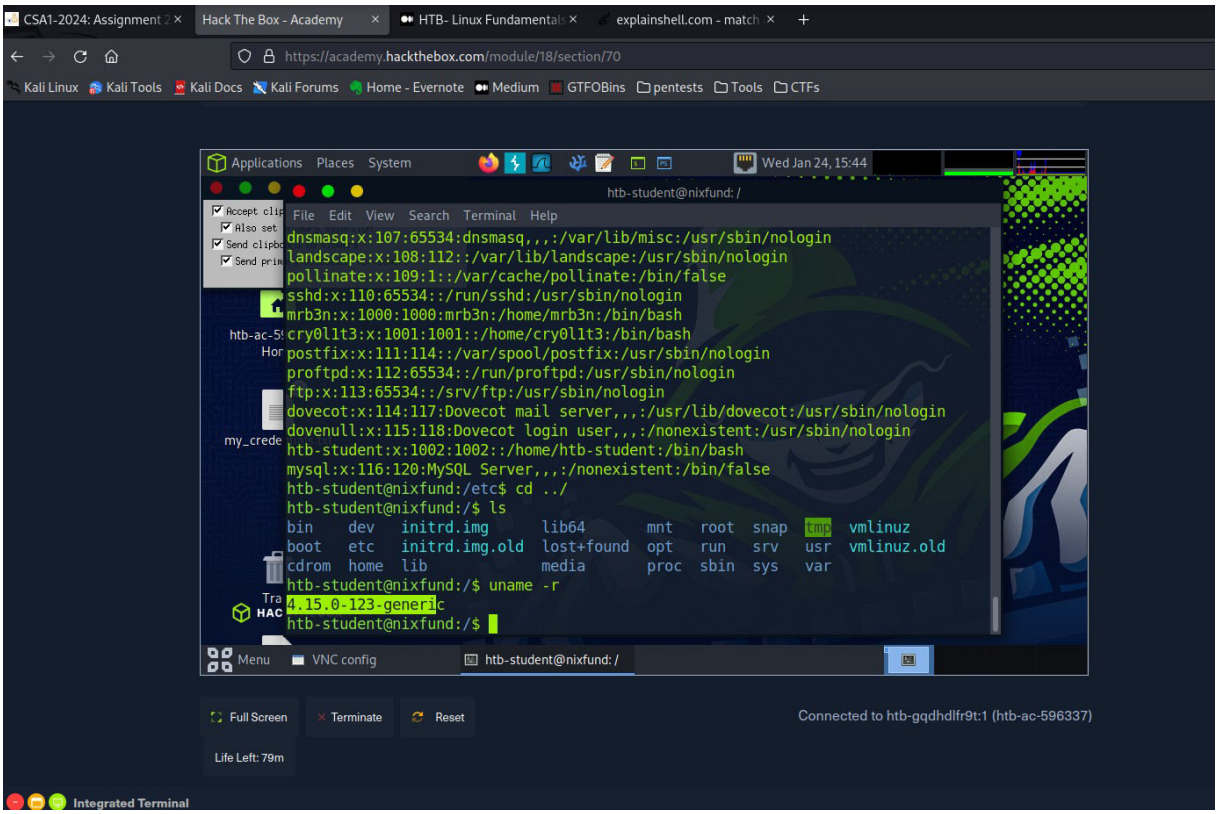


Which kernel version is installed on the system? (Format: 1.22.3)

The information of the installed kernel and OS can be seen with the 'uname' command. However, we can use additional attributes for specific information, such as '-a' for all the available information or '-r' for the release version of the installed version.

Command used:- uname -r

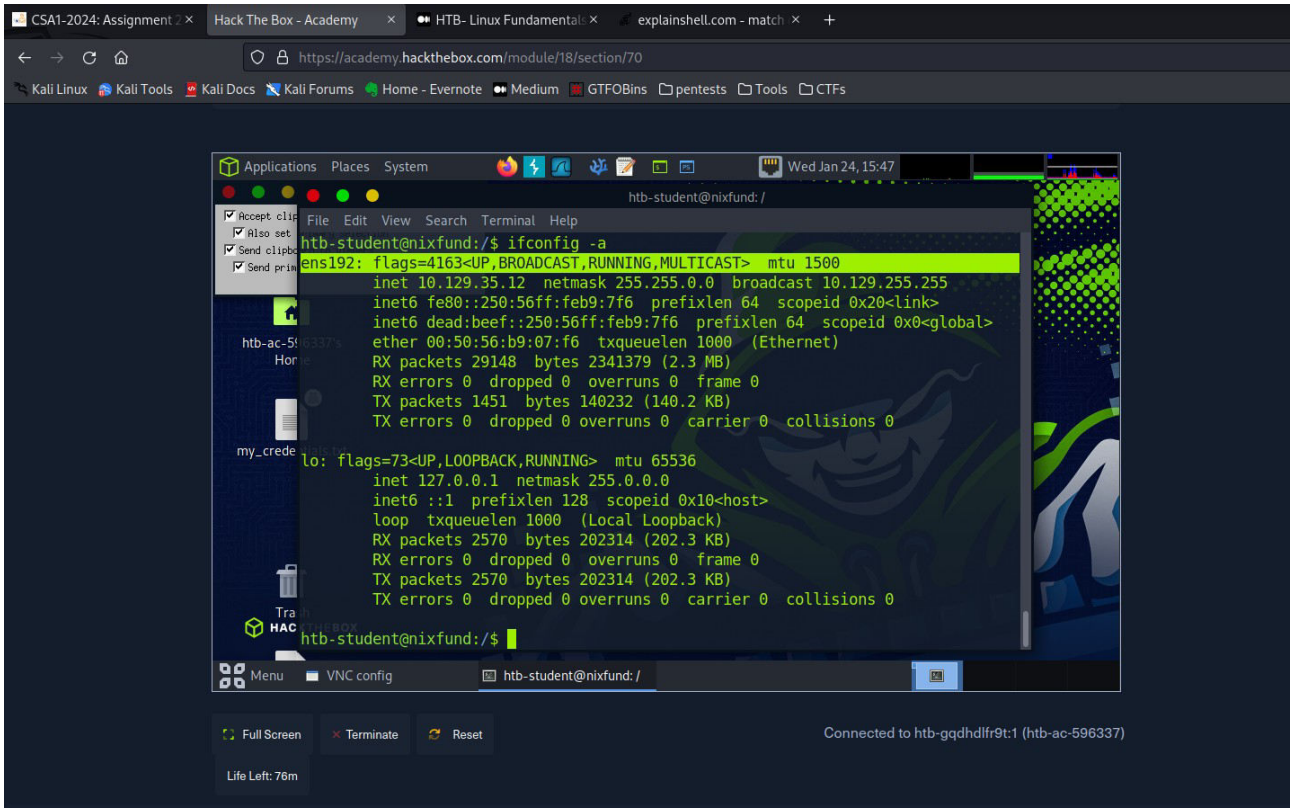
ANS: 4.15.0



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

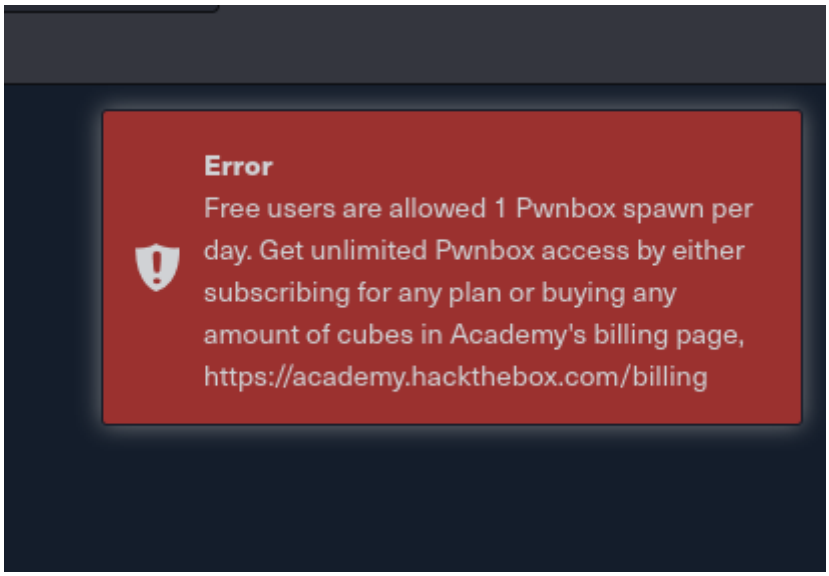
To view network interfaces in linux environments we can use “ifconfig” command. By running this command I found the MTU for interface ens192 set to 1500

ANS: ens192



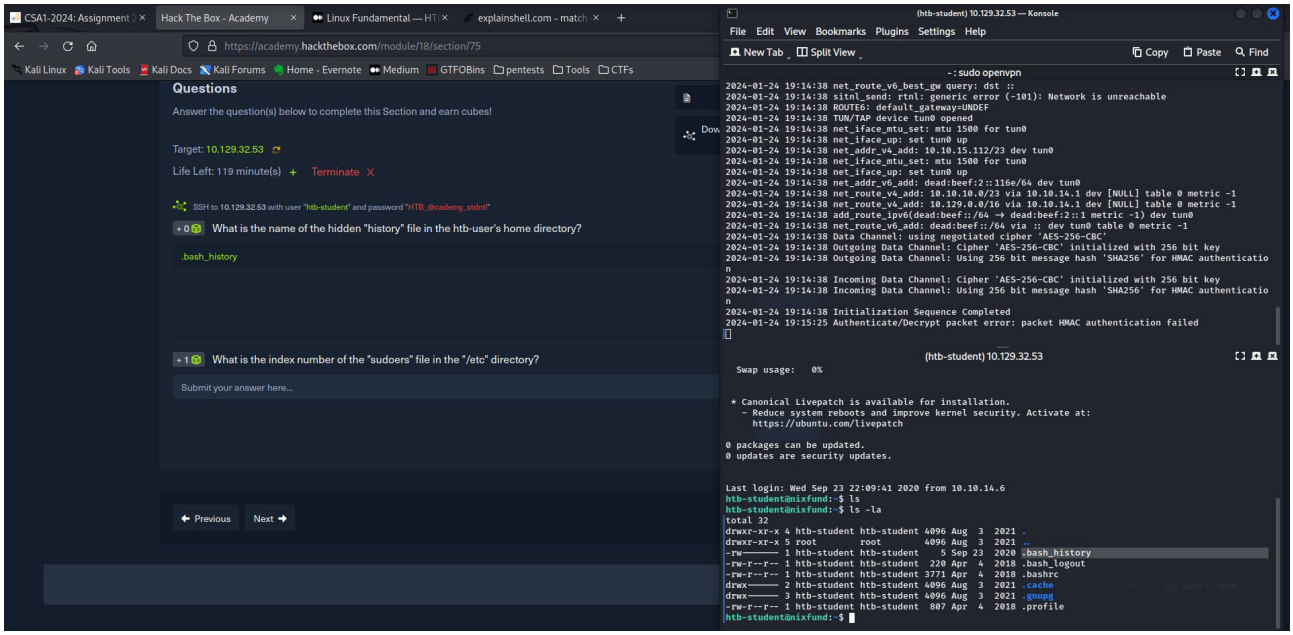
NAVIGATION

After concluding the section on System Information, I terminated the virtual machine provided in htb academy and on powering it back on I got an error only to realize I have one offer per day to use the htb virtual machine therefore I had to switch to my Local virtual machine using the VPN file provided in the module hence from here my IP address will keep changing as I did the work in different timestamps.



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

I first did an “ls” on this directory but couldn’t find any file present therefore, I used ‘ls -la’ to list all items (including hidden) briefly of the home directory and with that I was able to see the hidden file that was lacking with an history file attached on it **ANS: .bash_history**



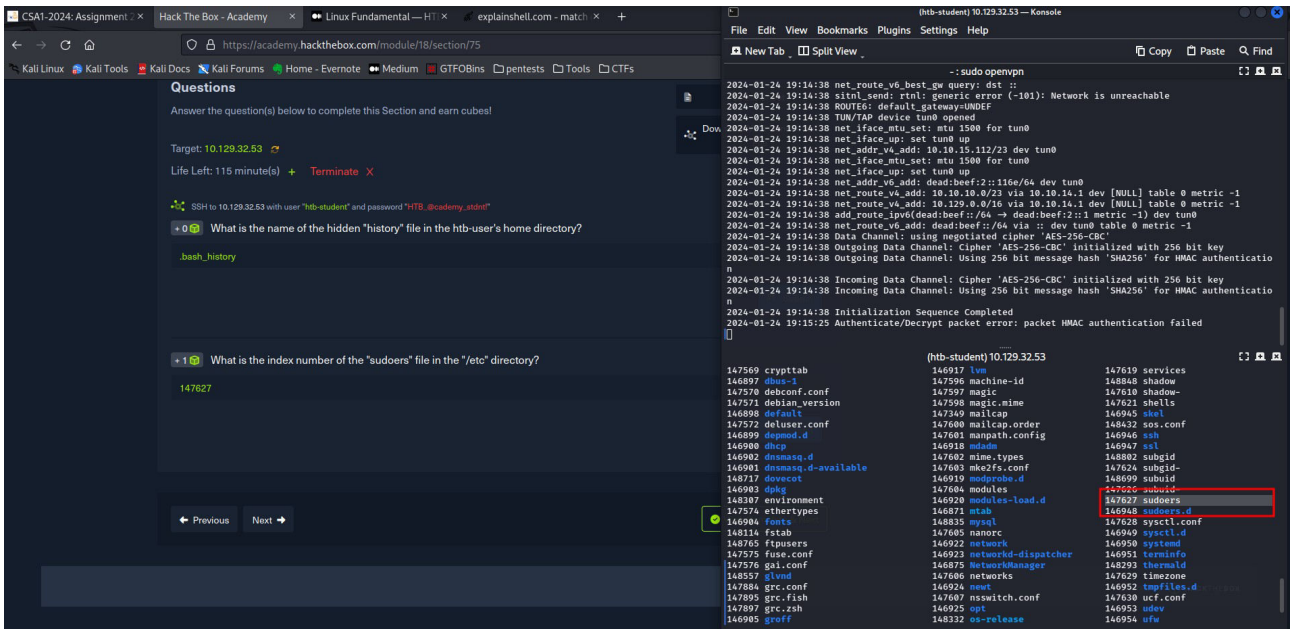
What is the index number of the "sudoers" file in the "/etc" directory?

Command used:- “ls -i”

The ls command is a command-line utility for listing the contents of a directory

-i will list the index for the files in the specified directory, with joining both “ls” and “-i” a files in the /etc directory all appear with their given indexes one of the files is sudoers appears with index no 147627

ANS: 147627

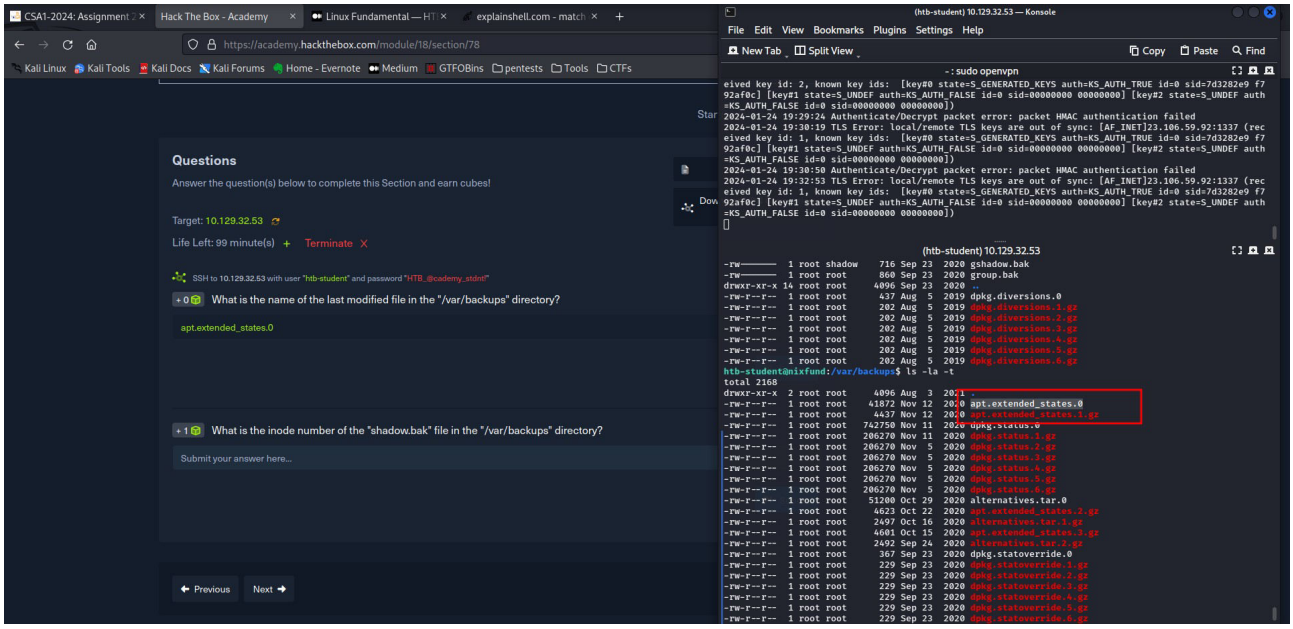


Working with Files and Directories

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

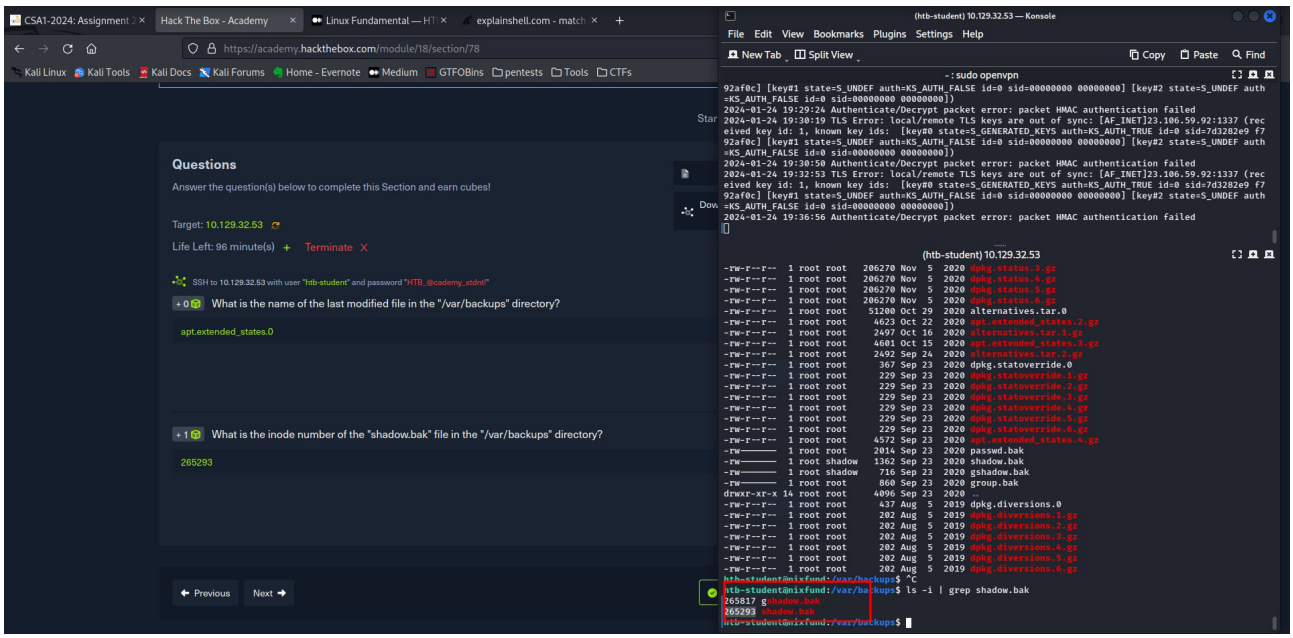
Command used:- ls -la -t

ls - lists the contents of a directory, la – lists all, -t shows the last time of modification. In our results apt.extended_states.0 appears to be last mdified on Nov 12 2020. **ANS: apt.extended_states.0**



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

First is to navigate to the file “shadow.bak” then run the command ls -i | grep shadow.bak to get the inode number. **ANS: 265293**



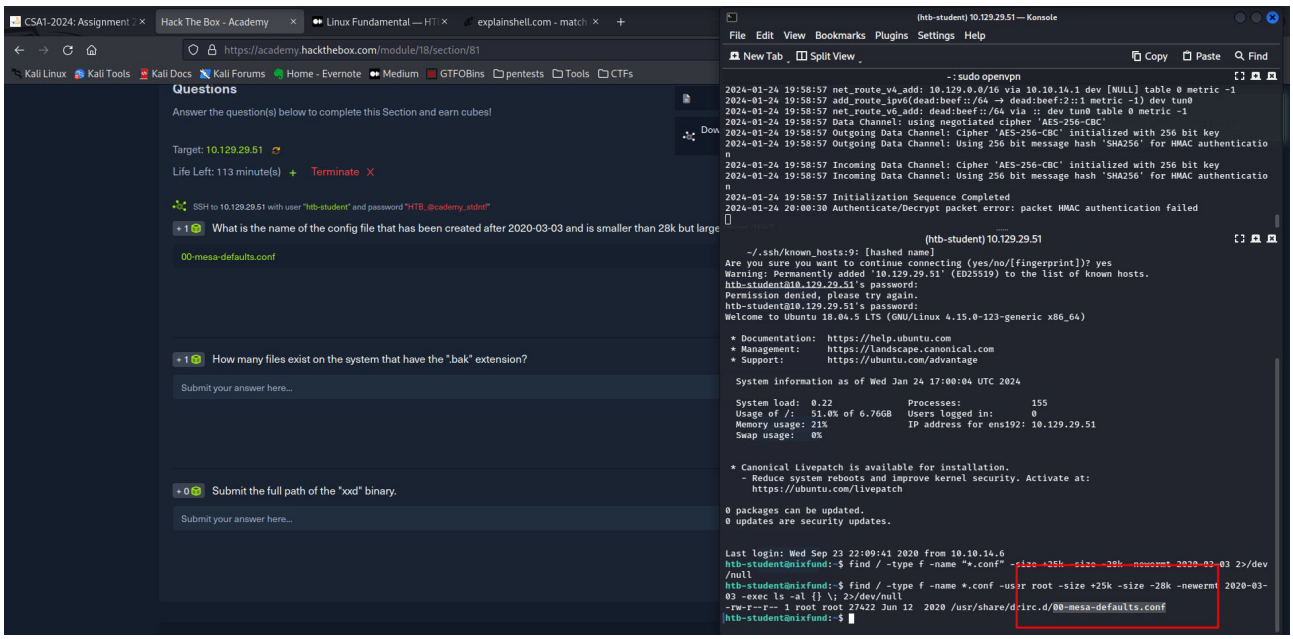
Editing files

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?

Command used is: find / -type f -name "*.conf" -size +25k -size -28k --newermt 2020–03–03 2>/dev/null

- find - The command used for searching files and directories.
- /: The starting directory for the search, in this case, the root directory.
- -type f: Specifies that the search is for files (not directories).
- -name "*.conf": Specifies that the file names should match the pattern "*.conf" (files with the ".conf" extension).
- -size +25k -size -28k: Filters files based on size. It searches for files larger than 25 kilobytes and smaller than 28 kilobytes.
- --newermt 2020-03-03: Filters files modified after the specified date (March 3, 2020).
- 2>/dev/null: Redirects error messages to /dev/null, discarding them. This is done to suppress any permission denied or other error messages that might occur during the search.

ANS: 00-mesa-defaults.conf

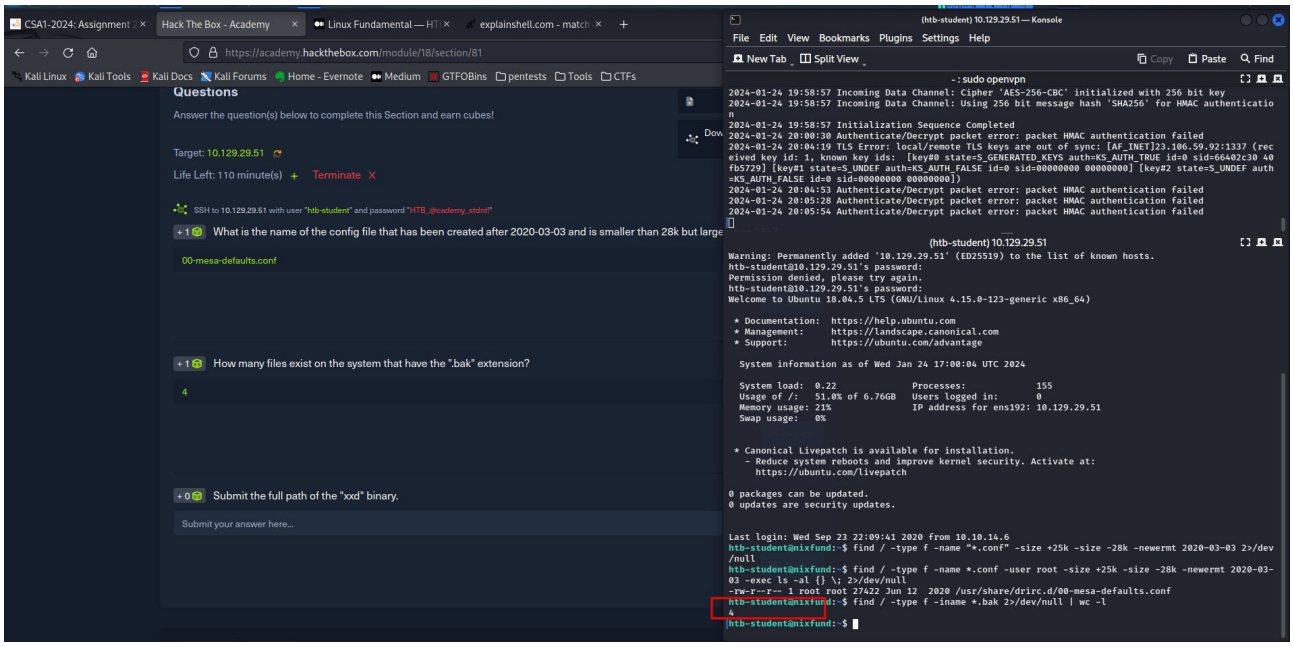


How many files exist on the system that have the ".bak" extension?

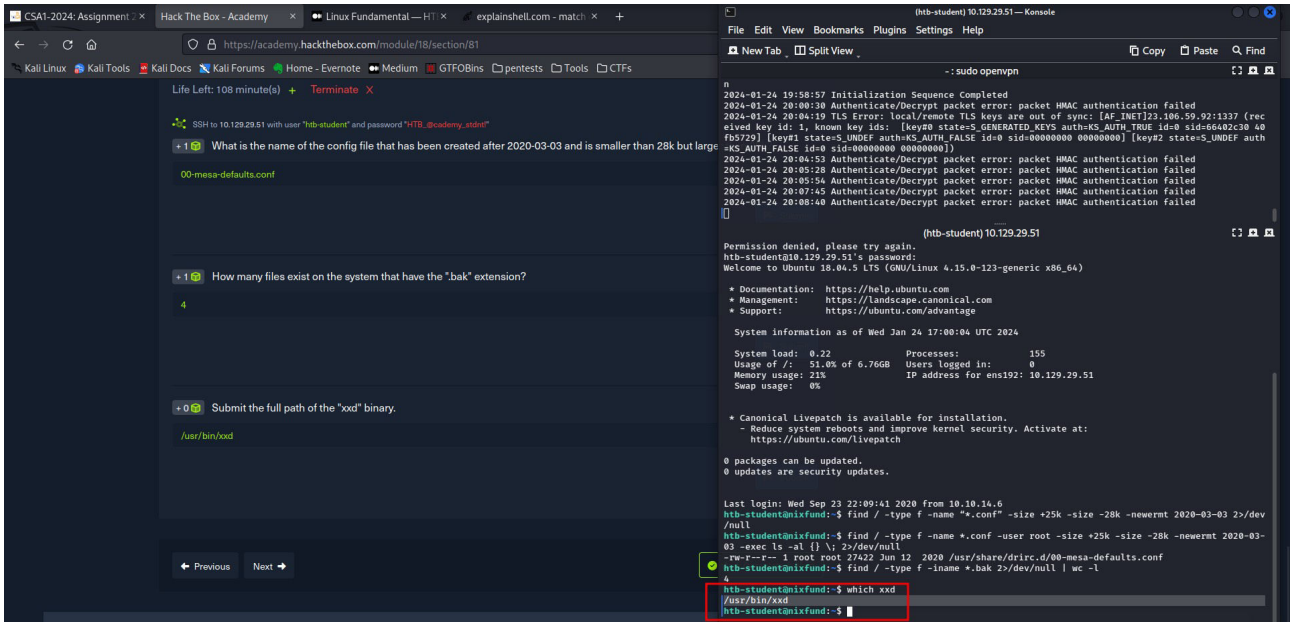
Using command :- find / -type f -iname *.*bak* 2>/dev/null | wc -l

Here “wc-l” Counts the number of lines in the input it receives. In this context, it counts the number of files found by the find command.

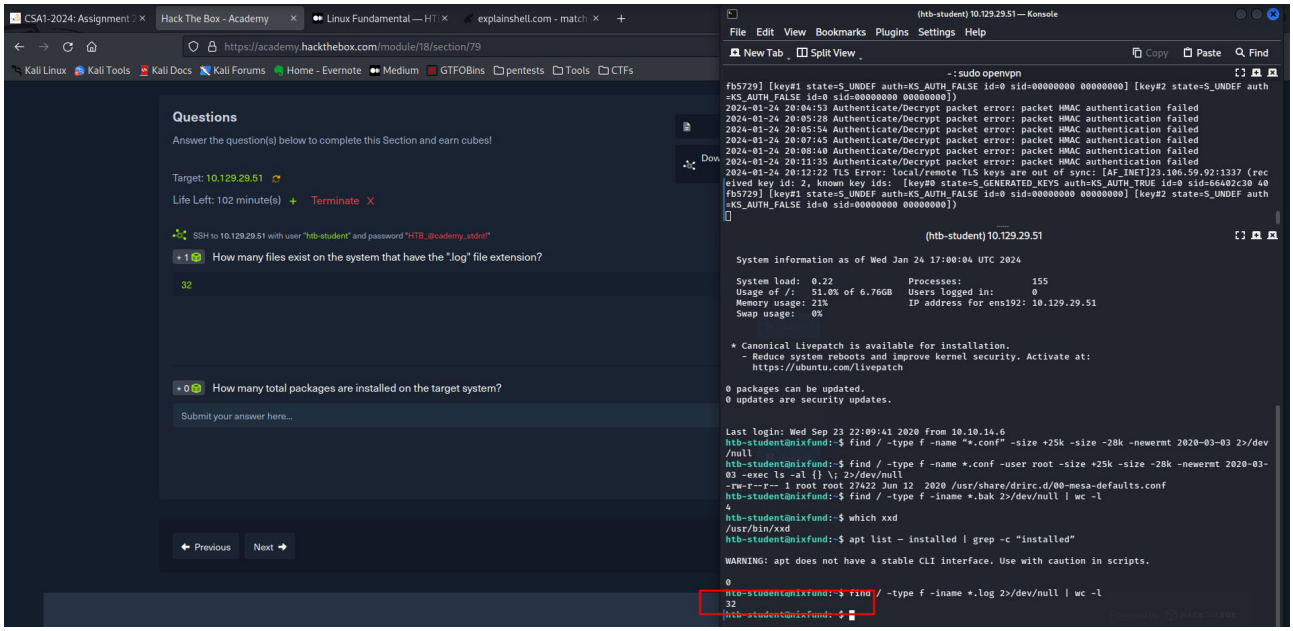
ANS: 4



Submit the full path of the "xxd" binary.
I used the “which” command that allows users to search the list of paths in the $PATH environment variable and outputs the full path of the command specified as an argument.
Command used:- which xxd
ANS: /usr/bin/xxd

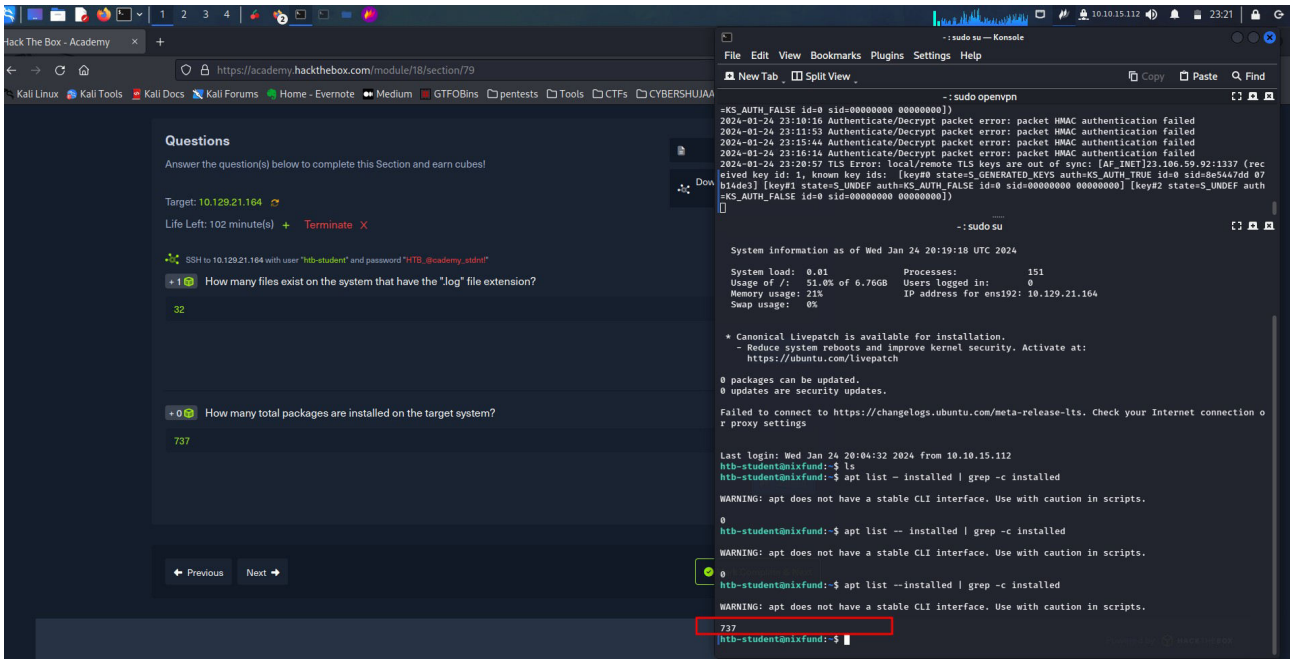


How many files exist on the system that have the ".log" file extension?
Command used: - find / -type f -iname *.log 2>/dev/null | wc -l
ANS:32



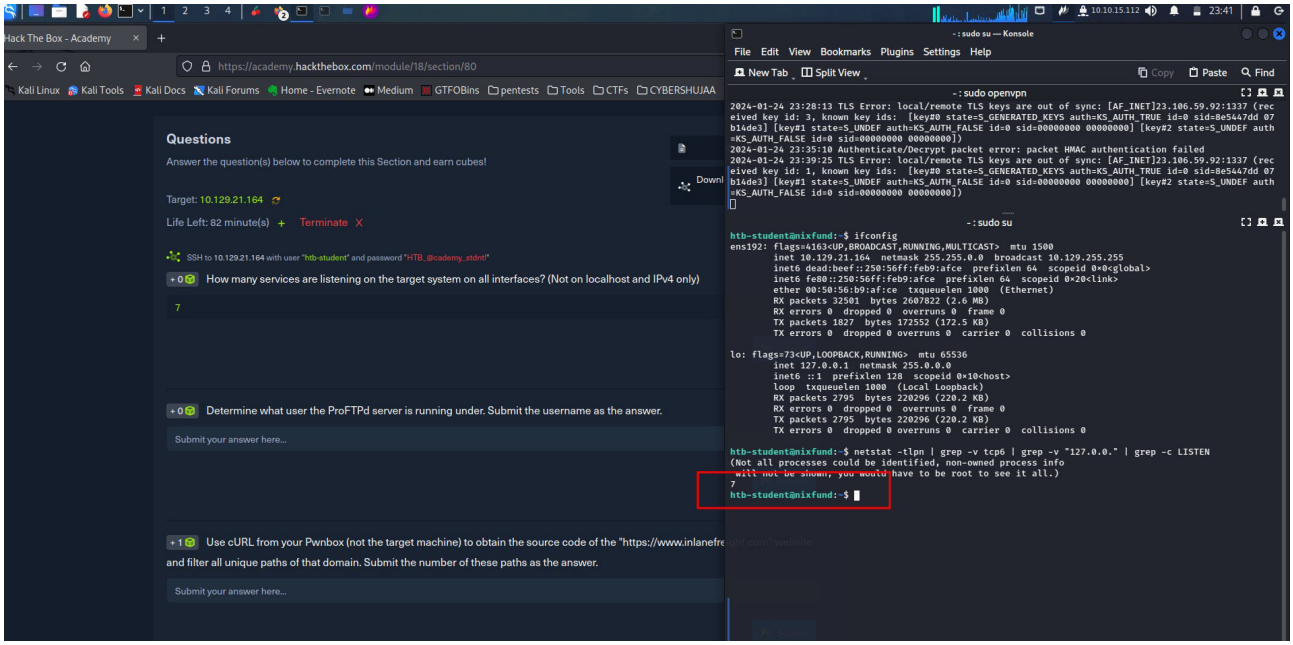
Took A break.
Lets Continue

How many total packages are installed on the target system?
Command used:- apt list -- installed | grep -c installed. This command will list all the installed packages in the target system.
ANS:737



Filter Contents.

How many services are listening on the target system on all interfaces? (Not on localhost and IPv4 only)
First I looked up at my target IPv4 address which came up as 127.0.0.1 therefore having this we can listen to all services on the target system.
Command used: netstat -tlpn | grep -v tcp6 | grep -v "127.0.0." | grep -c LISTEN
ANS: 7



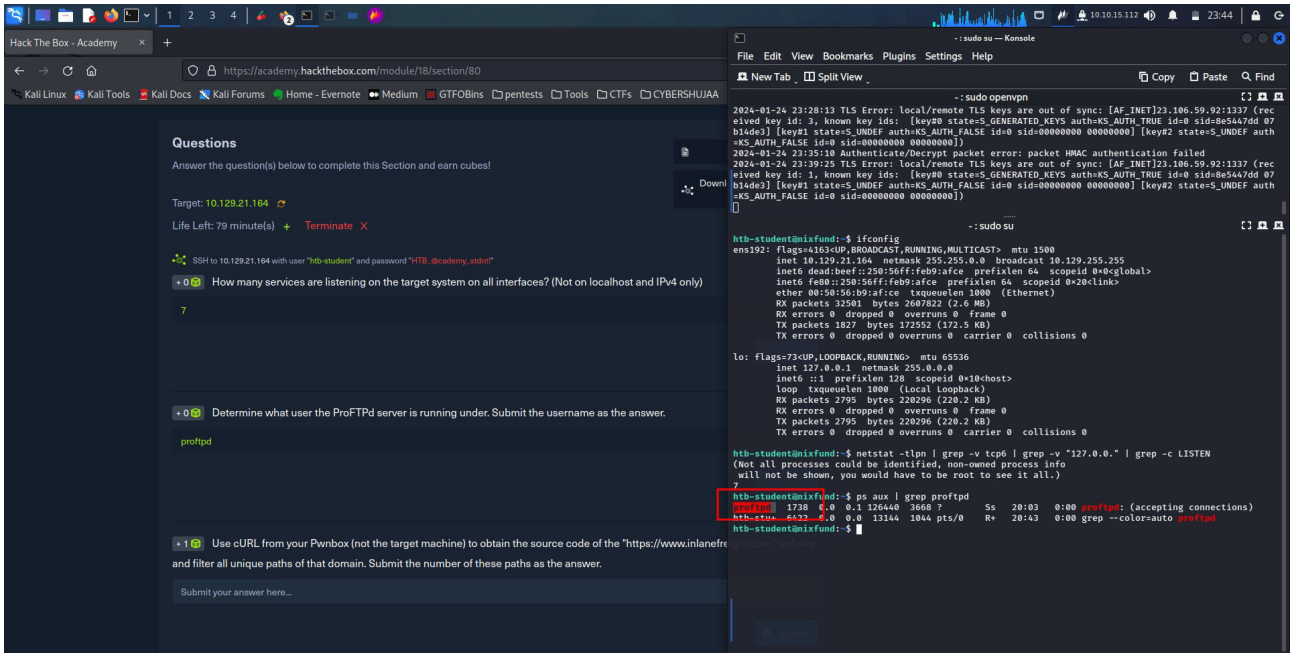
Determine what user the ProFTPd server is running under. Submit the username as the answer.

Command used:- ps aux | grep proftpd

- ps aux: Lists information about currently running processes. The aux options provide a detailed listing of all processes owned by any user.
- |: Pipes the output of the ps aux command (the list of all processes) to the next command.
- grep proftpd: will search for lines in the output that contain the string "proftpd".

grep is a command-line utility for searching plain-text data using regular expressions.

ANS: proftpd



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.

For this ill use my host machine as intructed.

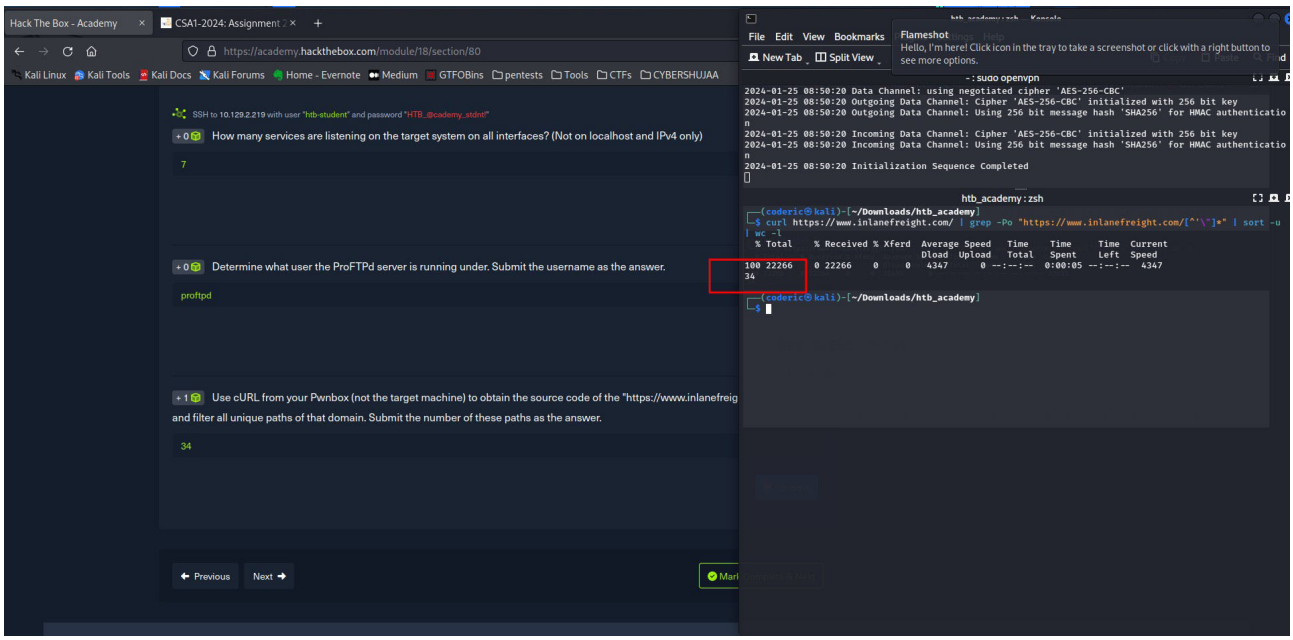
Command used:- curl https://www.inlanefreight.com/ | grep -Po “ https://www.inlanefreight.com/[^’*]*” | sort -u | wc -l

- curl command: Retrieves the HTML content of the specified website.
- grep -Po: Searches for lines in the HTML content that match the specified regular expression. This regular expression is designed to extract URLs that start with "https://www.inlanefreight.com/" and may contain characters other than single quotes or asterisks. The -P option enables Perl-compatible regular expressions, and the -o option only outputs the matched part of the line.

-sort -u: Sorts the extracted URLs in lexicographical order (sort) and removes duplicate URLs (-u option).

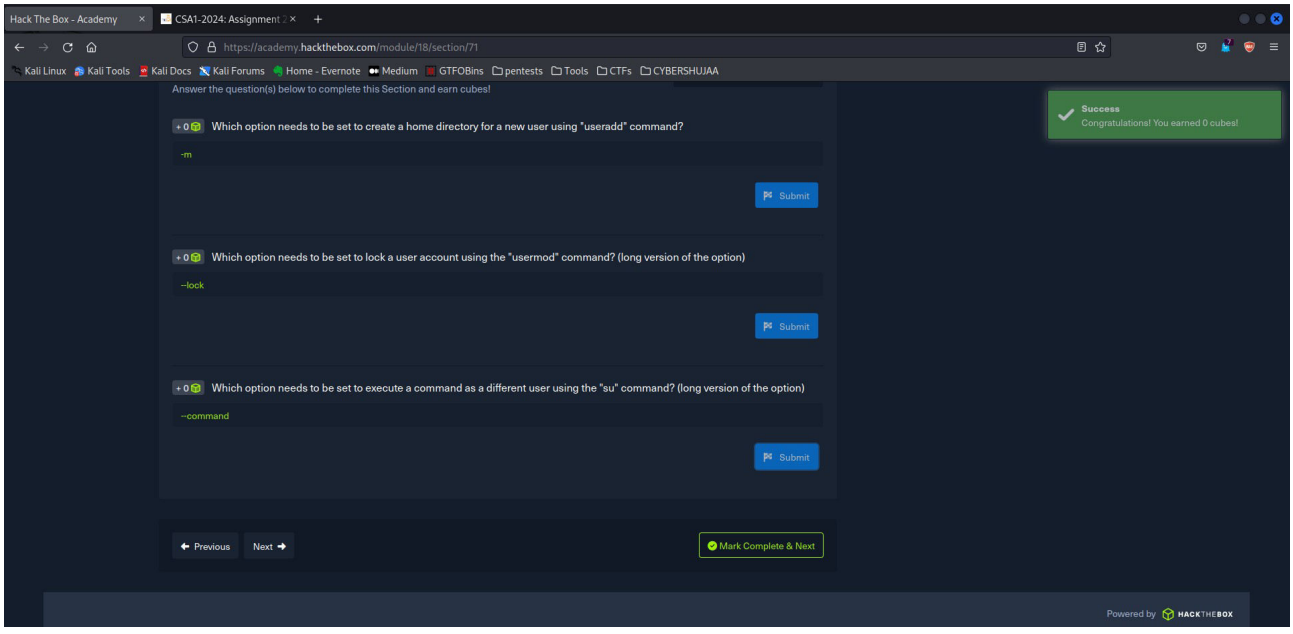
-wc -l: Counts the number of lines in the output, which corresponds to the number of unique URLs found.

ANS: 34



User Management

Which option needs to be set to create a home directory for a new user using "useradd" command? **ANS: -m**
Which option needs to be set to lock a user account using the "usermod" command? (long version of the option) **ANS: --lock**
Which option needs to be set to execute a command as a different user using the "su" command? (long version of the option) **ANS: --command**

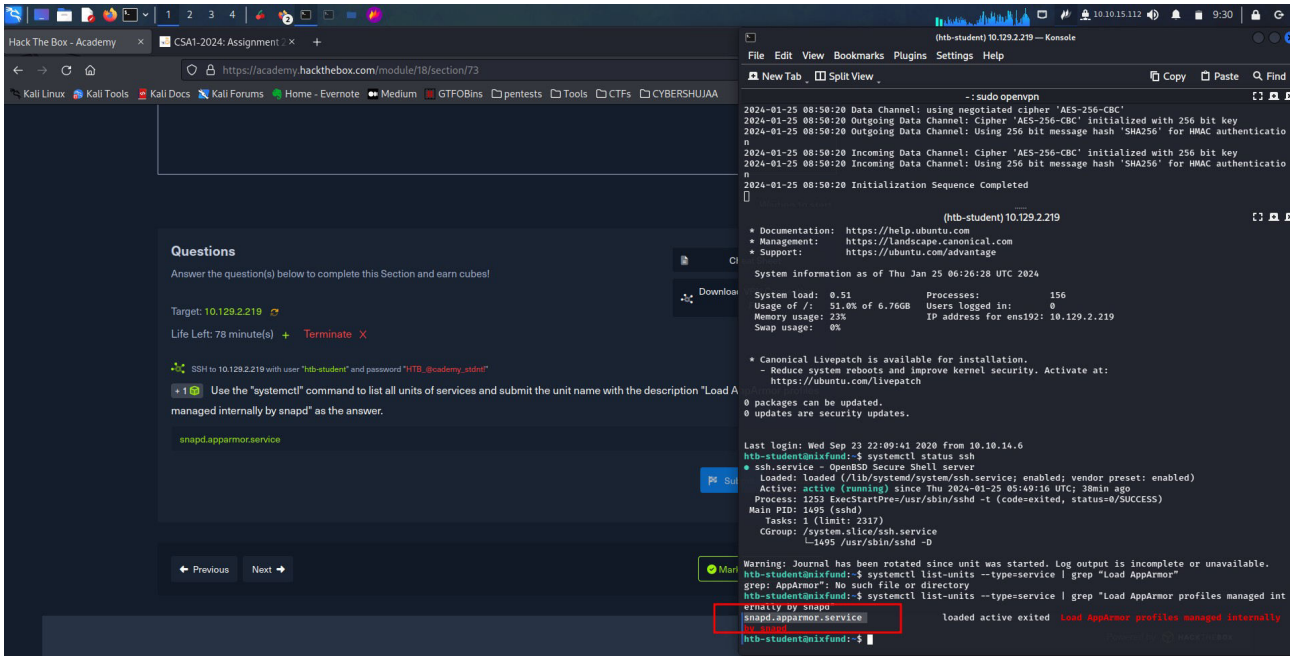


Service and Process Management

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.
Command Used:- systemctl list-units --type=service | grep Load AppArmor

- systemctl list-units --type=service: Lists all active systemd units of type "service" along with their current status and some additional information.
- grep Load AppArmor: Searches for lines in the output that contain both the words "Load" and "AppArmor". This would filter the results to only show lines related to services with "AppArmor" in their load information.

ANS: snapd.apparmor.service



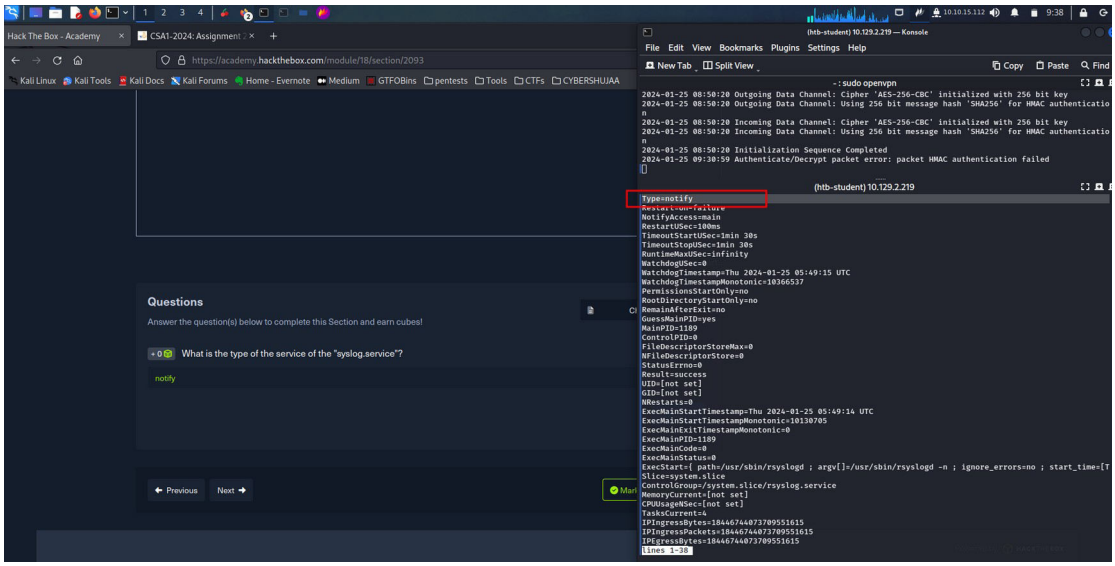
Task Scheduling

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

Command used:- systemctrl show syslog.service

This command will display detailed information about the syslog.service unit, including its configuration settings and current status. This information also incudes the type of service running. In this case Type=notify.

ANS: notify

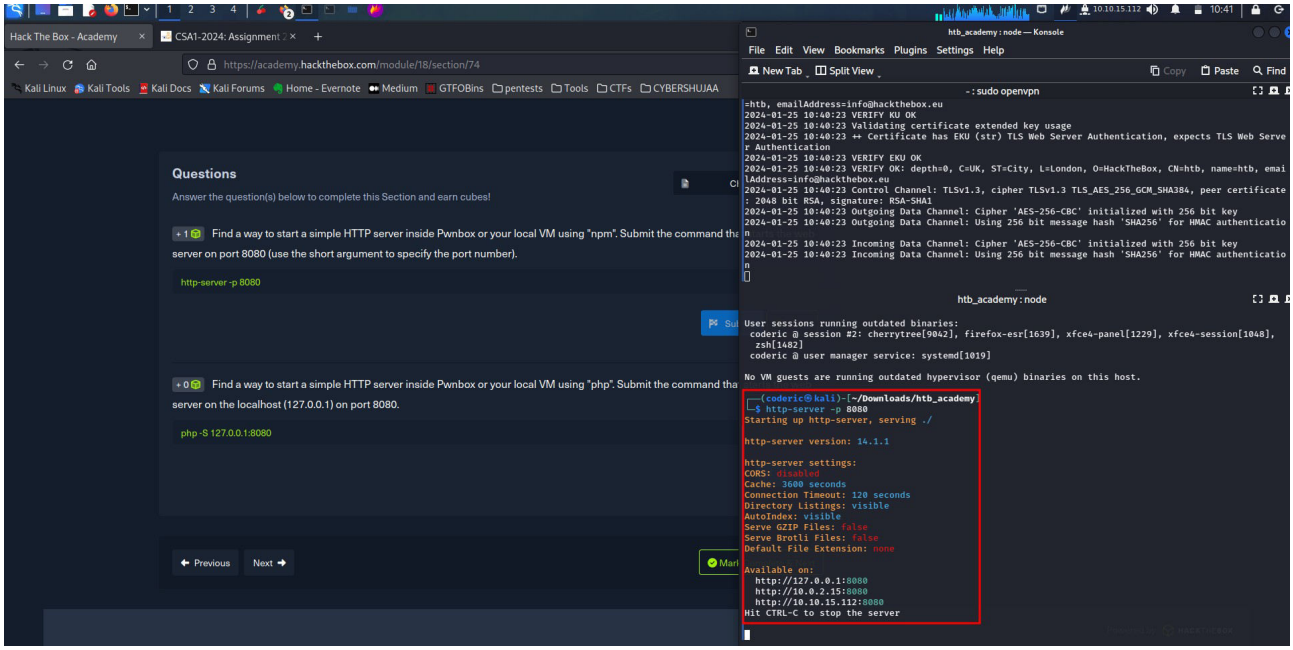


Working with Web Services

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).

Here is the command to run http-server -p 8080

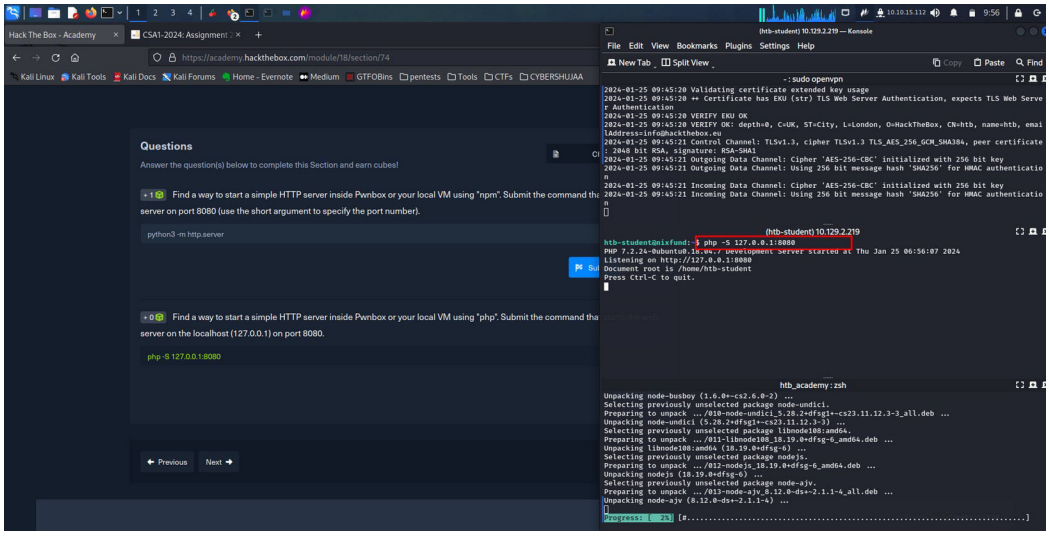
"-p" (specifying port 8080) **ANS: http-server -p 8080**



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.

Command used:- php -S 127.0.0.1:8080

ANS: php -S 127.0.0.1:8080



File System Management

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

"lsblk" command provides information like:

NAME: The name of the block device.

MAJ:MIN: The major and minor device numbers.

RM: Whether the device is removable or not (1 for removable, 0 for non-removable).

SIZE: The size of the block device.

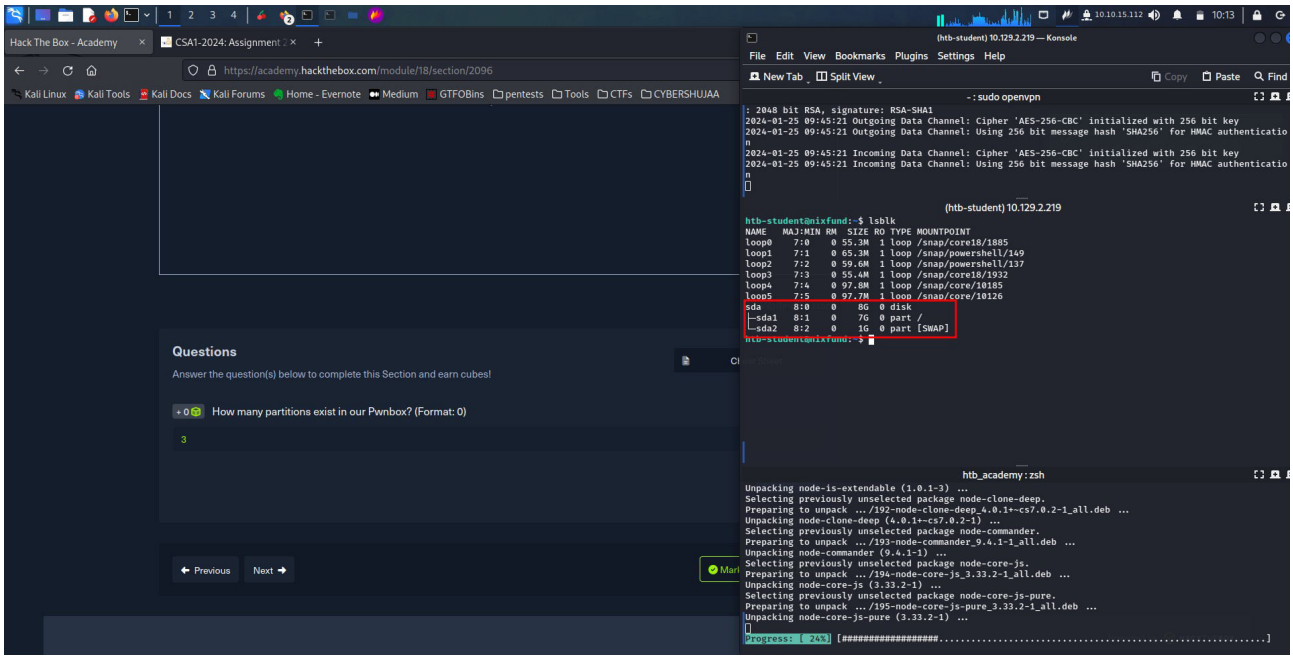
RO: Whether the device is read-only or read-write.

TYPE: The type of the block device (disk, partition, etc.).

MOUNTPOINT: The mount point of the device if it is mounted.

Therefore with this command we shall also get the number of partitions with the format of "0"

ANS: 3



Conclusion.

I have really enjoyed the course module, I have been able to lean on different ways to navigate through the directories and easier search of specific files using their extensions, name and size as well. I have also learnt on how to add users and remove users, grouping of users in Linux environments using the terminal and also to give permissions to who can read, write or execute a file.

In conclusion this module has opened up my eyes on new ways of approach on the Linux environment.

Thank you.