UNIT: Linux fundamentals: HackTheBox

NAME: MWITHUI DANIEL MWENDWA

REG NO. CS-SA04-23080

COURSE: SECURITY ANALYST

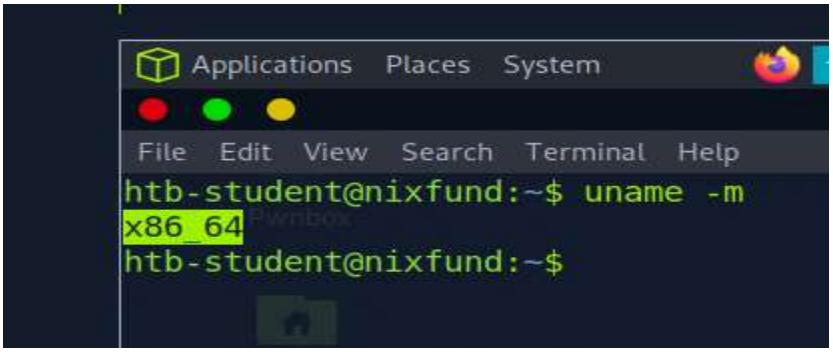
Introduction

Welcome to the world of Linux fundamentals in Hackthebox! In this report, we will embark on an exciting journey together, where we will explore the basics of Linux operating system and its fundamental concepts. Whether you are a beginner or have some experience with Linux, this guide will provide you with a solid foundation to navigate and understand the powerful world of Linux within Hackthebox. So, let's dive in and discover the key principles and tools that make Linux an essential skill for any aspiring hacker or cybersecurity enthusiast.

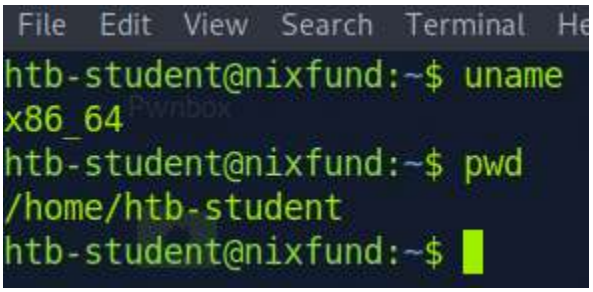
Task 1: Shell

In this task, we learn how to use shell to get information about the system we are running. Commands that we are going to learn here include whoami which displays the current username, id which returns user id and uname which prints basic information about the operating system. Below are screenshots and description of the steps used to complete the task 1. To start the task, you should ssh htb_student@ipaddress to connect to the box.

Task 1a. run uname -m to get machine hardware name. you can try uname -help to get help on the command to use. Here is the screenshot.



Task 1b. to know the name of the path to htb-student directory, do pwd to print the working directory since it is the directory, we are in.



Task 1c. To know the path to htb-student mail folder, do cd to the /var directory then cd mail. Run env to check the environment variables.

```
htb-student@nixfund:~$ cd /var
htb-student@nixfund:/var$ ls
backups  cache  crash  lib  local  lock  log  mail  opt  run  snap  spool  tmp  www
htb-student@nixfund:/var$ cd mail
htb-student@nixfund:/var/mail$ env
```

```
LC_ADDRESS=C.UTF-8
LC_NUMERIC=C.UTF-8
SSH_TTY=/dev/pts/0
MAIL=/var/mail/htb-student
TERM=xterm-256color
```

Task 1d. you can find the answer from the above shell screen by running env on /var/mail directory.

```
MAIL=/var/mail/htb-student
TERM=xterm-256color
SHELL=/bin/bash
SHLVL=1
LC_TELEPHONE=C.UTF-8
LOGNAME=htb-student
XDG_RUNTIME_DIR=/run/user/1002
PATH=/usr/local/sbin:/usr/loca
```

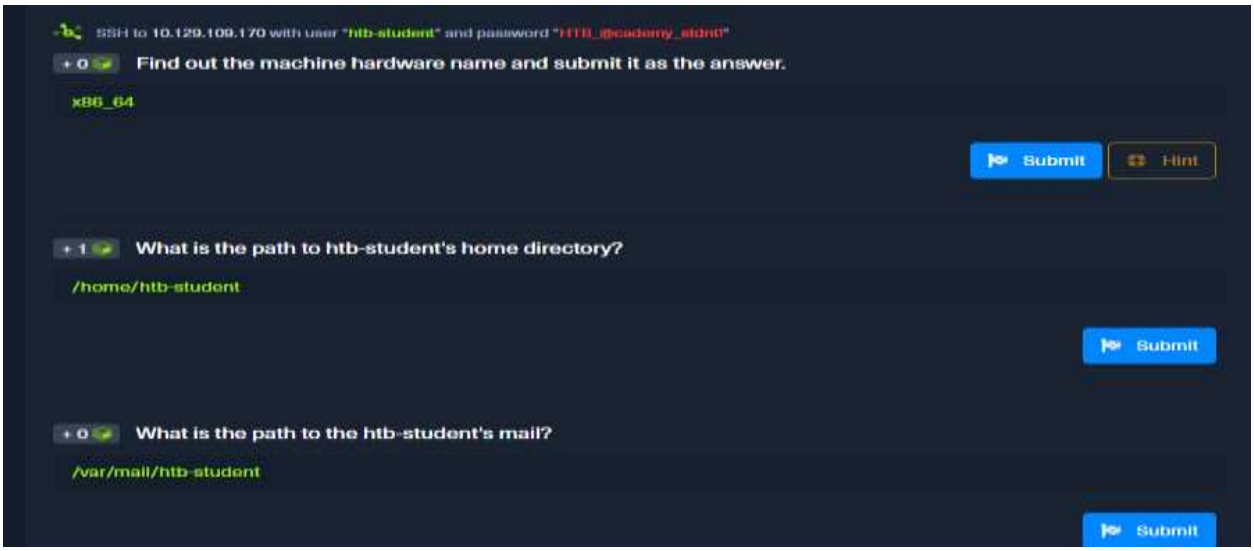
Task 1e. to get kernel version. on home directory do uname -r for kernel release. Again you can use uname -help to get the command you should use.

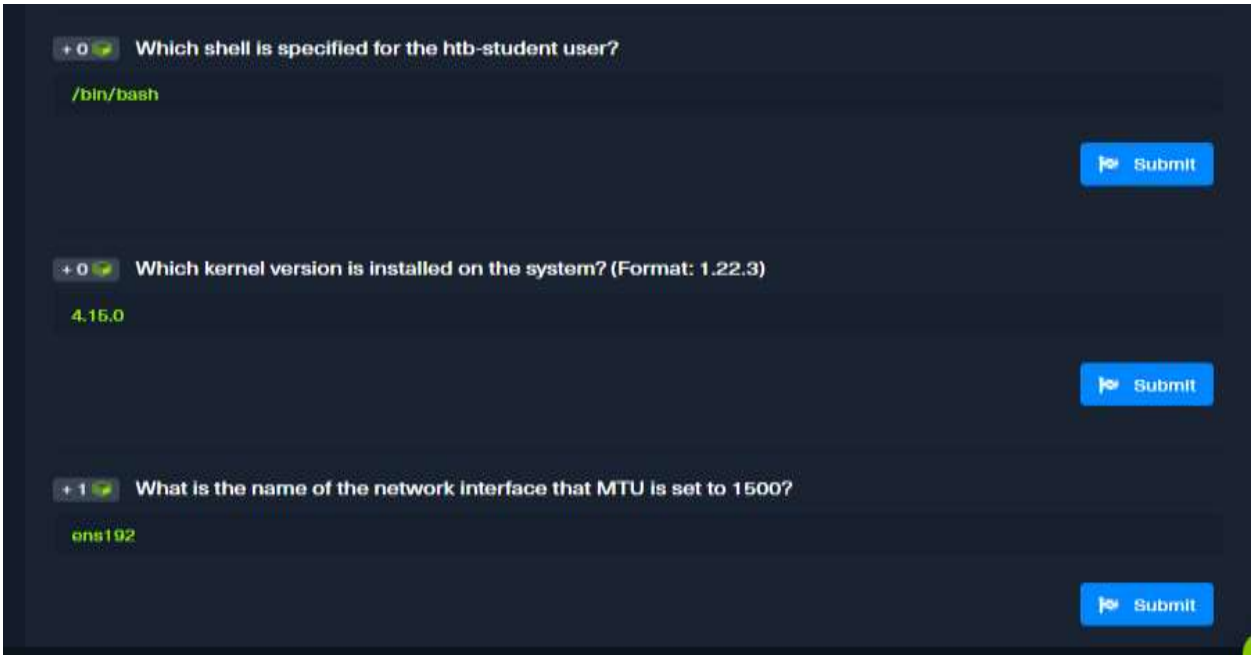
```
htb-student@nixfund:/var/mail$ cd .
htb-student@nixfund:/var$ cd ../\
>
htb-student@nixfund:/$ uname -r
4.15.0-123-generic
htb-student@nixfund:/$
```

Task 1f. to get the name of the network interface that MTU is set to 1500, do ifconfig command.

```
4.15.0-123-generic
htb-student@nixfund:/$ ifconfig
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.129.109.170  netmask 255.255.0.0  broadcast 10.129.255.255
        inet6 fe80::250:56ff:feb9:c17a  prefixlen 64  scopeid 0x20<link>
        inet6 dead:beef::250:56ff:feb9:c17a  prefixlen 64  scopeid 0x0<global>
        ether 00:50:56:b9:c1:7a  txqueuelen 1000  (Ethernet)
```

Here is the completion for task 1.





Task 2. Navigation

In this second task, we will learn about navigation in Linux. This means moving from one directory to the other and opening and viewing files as well as listing files in a given directory. Let us delve into this discussion.

Task 1a. To get the name of the hidden directory here you do ls -la. Any file with starting with a dot(.) as .name_of_the_file in Linux is a hidden file.

```
htb-student@nixfund:/$ cd home
htb-student@nixfund:/home$ ls
cry0l1t3  htb-student  mrb3n
htb-student@nixfund:/home$ cd htb-student
htb-student@nixfund:~$ ls -la
total 32
drwxr-xr-x 4 htb-student htb-student 4096 Aug  3  2021 .
drwxr-xr-x 5 root        root        4096 Aug  3  2021 ..
-rw------- 1 htb-student htb-student    5 Sep 23  2020 .bash_history
-rw-r--r-- 1 htb-student htb-student  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 htb-student htb-student 3771 Apr  4  2018 .bashrc
drwx------ 2 htb-student htb-student 4096 Aug  3  2021 .cache
drwx------ 3 htb-student htb-student 4096 Aug  3  2021 .gnupg
-rw-r--r-- 1 htb-student htb-student  807 Apr  4  2018 .profile
```

Task 2b. to get index number of the "sudoers" file in the "/etc" directory, cd to the /etc directory, the do ls -I to list index of all files there.

```
146907 init.d                    146946 ssh
146908 initramfs-tools           146947 ssl
147583 inputrc                   148802 subgid
148741 insserv.conf.d            147624 subgid-
146909 iproute2                  148699 subuid
146910 iscsi                     147626 subuid-
148324 issue                     147627 sudoers
148325 issue.net                 146948 sudoers.d
146911 kernel                    147628 sysctl.conf
148234 kernel-img.conf           146949 sysctl.d
```

Here is the completion level for the task 2.

Questions

Answer the question(s) below to complete this Section and earn cubes!

Target: **Click here to spawn the target system!**

SSH to with user "**htb-student**" and password "HTB_@cademy_stdnt!"

+ 0 **What is the name of the hidden "history" file in the htb-user's home directory?**

.bash_history

+ 1 **What is the index number of the "sudoers" file in the "/etc" directory?**

147627

Task 3. Working with files and directory

In this task we will learn on how to work with files and directory in Linux. This will help us to understand commands like mv to move or rename files, cp to copy files, mkdir for making directory, rmdir for removing directories among others.

Task 3a. to complete this task, use ls -la on the /var/backups directory. Check date to see the latest modified file.

```
htb-student@nixfund:~$ cd /var/backups
htb-student@nixfund:/var/backups$ ls -la
total 2168
drwxr-xr-x  2 root root     4096 Aug  3  2021 .
drwxr-xr-x 14 root root     4096 Sep 23  2020 ..
-rw-r--r--  1 root root    51200 Oct 29  2020 alternatives.tar.0
-rw-r--r--  1 root root     2497 Oct 16  2020 alternatives.tar.1.gz
-rw-r--r--  1 root root     2492 Sep 24  2020 alternatives.tar.2.gz
-rw-r--r--  1 root root    41872 Nov 12  2020 apt.extended_states.0
-rw-r--r--  1 root root     4437 Nov 12  2020 apt.extended_states.1.gz
```

Task 3b. to check the inode number of shadow.bak file, do ls -I on /var/backups

```
htb-student@nixfund:/var/backups$ ls -i
262248 alternatives.tar.0          262310 dpkg.statoverride.2.gz
262559 alternatives.tar.1.gz       262311 dpkg.statoverride.3.gz
262261 alternatives.tar.2.gz       262247 dpkg.statoverride.4.gz
266334 apt.extended_states.0       262250 dpkg.statoverride.5.gz
266335 apt.extended_states.1.gz    262236 dpkg.statoverride.6.gz
266430 apt.extended_states.2.gz    263999 dpkg.status.0
264827 apt.extended_states.3.gz    262179 dpkg.status.1.gz
262233 apt.extended_states.4.gz    262234 dpkg.status.2.gz
262178 dpkg.diversions.0           262241 dpkg.status.3.gz
262203 dpkg.diversions.1.gz        262243 dpkg.status.4.gz
262264 dpkg.diversions.2.gz        262220 dpkg.status.5.gz
262257 dpkg.diversions.3.gz        262230 dpkg.status.6.gz
262246 dpkg.diversions.4.gz        265226 group.bak
262249 dpkg.diversions.5.gz        265817 gshadow.bak
262235 dpkg.diversions.6.gz        264599 passwd.bak
262231 dpkg.statoverride.0         265293 shadow.bak
262205 dpkg.statoverride.1.gz
htb-student@nixfund:/var/backups$
```

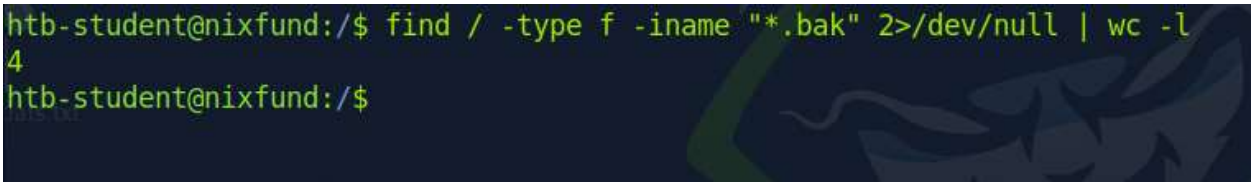
Here is the completed task

Task 4. How to find files in Linux

In this task, we will learn on how to find files on Linux. here we will learn tools such as which and find all used to find files in Linux. let us go straight to the specific tasks in this module.

Task 4a. to find the file with given description run the command as shown in the screenshot below

Task 4b. to find files with .bak extension, use the command shown below.



Task 4c. to find the path of xxd binary, do the following as shown in the screenshot below.

Task 5. File descriptions and redirections

This explains the connection by the kernel to perform an I\O operation. Here we will learn data streams for input, output and error. It is like the filehandle in windows.

Task 5a. to find files with .log extensions do

```
htb-student@nixfund:/bin$ find / -type f -iname "*.log" 2>/dev/null | wc -l
32
htb-student@nixfund:/bin$
```

Task 5b. to find the number of total installed packages do

```
htb-student@nixfund:/$ dpkg --list | grep ii |wc -l
737
htb-student@nixfund:/$
```

Here is completed answers.

SSH to 10.129.12.237 with user "htb-student" and password "HTB{_@cademy_stdnt!"

+1 How many files exist on the system that have the ".log" file extension?

32

+0 How many total packages are installed on the target system?

737

Task 6. Filter contents

Here we will learn command such as more, tail, head, and grep which are used to filter content and have only the results that you are interested in.

task 6a. To know how many services are listening to all interfaces use netstat as shown below. By counting only ipv4 and excluding local host you get 7 tcp interfaces.

```
htb-student@nixfund:/$ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:smtp          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:microsoft-ds    0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:imaps           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:pop3s           0.0.0.0:*               LISTEN
tcp        0      0 localhost:mysql         0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:netbios-ssn     0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:pop3            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:imap2           0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN
```

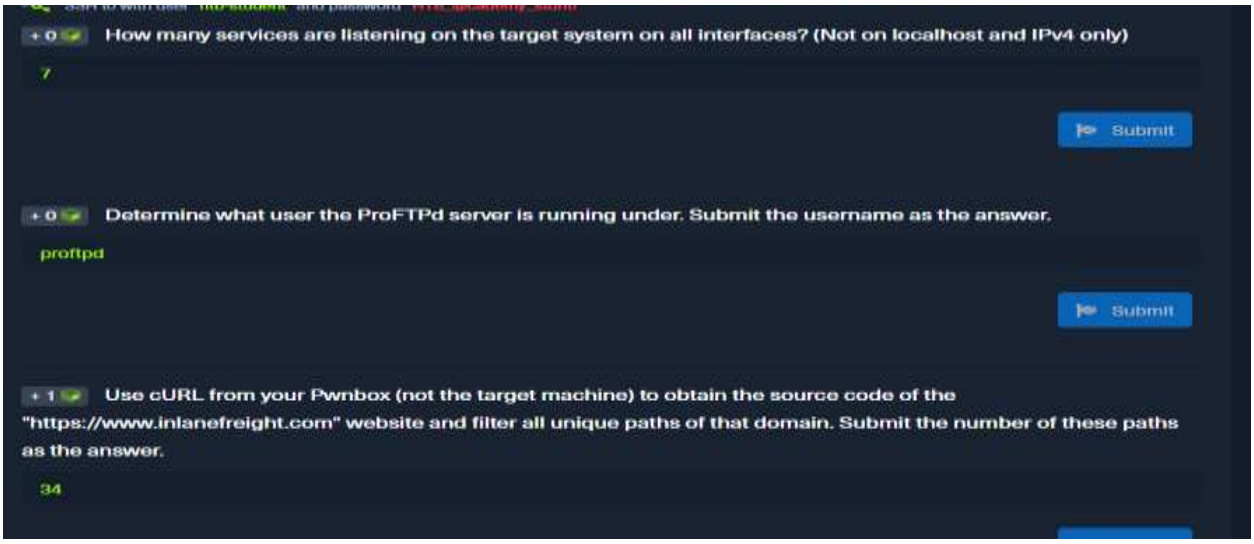
Task 6b. to determine what user the ProFTPd server is running under, scroll down to see answer.

```
htb-student@nixfund:/$ ps aux ||grep ProFTPd
USER       PID %CPU %MEM    VSZ   RSS TTY
root         1  0.0  0.4 225324  9004 ?
root         2  0.0  0.0      0     0 ?
root         3  0.0  0.0      0     0 ?
root         4  0.0  0.0      0     0 ?
```

Task 6c. To answer this task, use curl command with the http link provided to get the source code, then do grep, tr “” “\n” to remove spaces and add new line to easily count the new lines, use sort -u to remove anything that is not unique. Then do grep for src and href to only get count of the lines we are interested in. after that then do sort -u and wc -l to count line. Make sure to notice the same lines repeated.

```
$grep https://www.inlanefreight.com inlane | tr " " "\n" | sort -u | grep -E 'src|href'
href="https://www.inlanefreight.com/"
href='https://www.inlanefreight.com/'
href="https://www.inlanefreight.com/index.php/about-us/">About
href="https://www.inlanefreight.com/index.php/career/">Career</a></li>
href="https://www.inlanefreight.com/index.php/comments/feed/"
href="https://www.inlanefreight.com/index.php/contact/">Contact</a></li>
href="https://www.inlanefreight.com/index.php/feed/"
href="https://www.inlanefreight.com/index.php/news/">News</a></li>
href="https://www.inlanefreight.com/index.php/offices/">Offices</a></li>
href="https://www.inlanefreight.com/index.php/wp-json/"
href="https://www.inlanefreight.com/index.php/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fwww.inlanefreight.com%2F"
href="https://www.inlanefreight.com/index.php/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fwww.inlanefreight.com%2F&#038;format=xml"
href="https://www.inlanefreight.com/index.php/wp-json/wp/v2/pages/7"
href="https://www.inlanefreight.com/">Inlanefreight
href="https://www.inlanefreight.com/">Inlanefreight                    <br>
href="https://www.inlanefreight.com/">Services</a></li>
href='https://www.inlanefreight.com/wp-content/themes/ben_theme/css/animate.css?ver=5.6.9'
href='https://www.inlanefreight.com/wp-content/themes/ben_theme/css/bootstrap.css?ver=5.6.9'
href='https://www.inlanefreight.com/wp-content/themes/ben_theme/css/bootstrap-progressbar.min.css?ver=5.6.9'
href='https://www.inlanefreight.com/wp-content/themes/ben_theme/css/colors/default.css?ver=5.6.9'
href='https://www.inlanefreight.com/wp-content/themes/ben_theme/css/font-awesome.css?ver=5.6.9'
href='https://www.inlanefreight.com/wp-content/themes/ben_theme/css/jquery.smartmenus.bootstrap.css?ver=5.6.9'
href='https://www.inlanefreight.com/wp-content/themes/ben_theme/css/magnific-popup.css?ver=5.6.9'
href='https://www.inlanefreight.com/wp-content/themes/ben_theme/css/owl.carousel.css?ver=5.6.9'
href='https://www.inlanefreight.com/wp-content/themes/ben_theme/css/owl.transitions.css?ver=5.6.9'
href='https://www.inlanefreight.com/wp-content/themes/ben_theme/style.css?ver=5.6.9'
href='https://www.inlanefreight.com/wp-includes/css/dist/block-library/style.min.css?ver=5.6.9'
href="https://www.inlanefreight.com/wp-includes/wlwmanifest.xml"
href="https://www.inlanefreight.com/xmlrpc.php?rsd"
src='https://www.inlanefreight.com/wp-content/themes/ben_theme/js/bootstrap.min.js?ver=5.6.9'
src='https://www.inlanefreight.com/wp-content/themes/ben_theme/js/jquery.smartmenus.bootstrap.js?ver=5.6.9'
src='https://www.inlanefreight.com/wp-content/themes/ben_theme/js/jquery.smartmenus.js?ver=5.6.9'
src='https://www.inlanefreight.com/wp-content/themes/ben_theme/js/navigation.js?ver=5.6.9'
src='https://www.inlanefreight.com/wp-content/themes/ben_theme/js/owl.carousel.min.js?ver=5.6.9'
src='https://www.inlanefreight.com/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2'
src='https://www.inlanefreight.com/wp-includes/js/jquery/jquery.min.js?ver=3.5.1'
src='https://www.inlanefreight.com/wp-includes/js/wp-embed.min.js?ver=5.6.9'
```

Here is the task completion for this task.

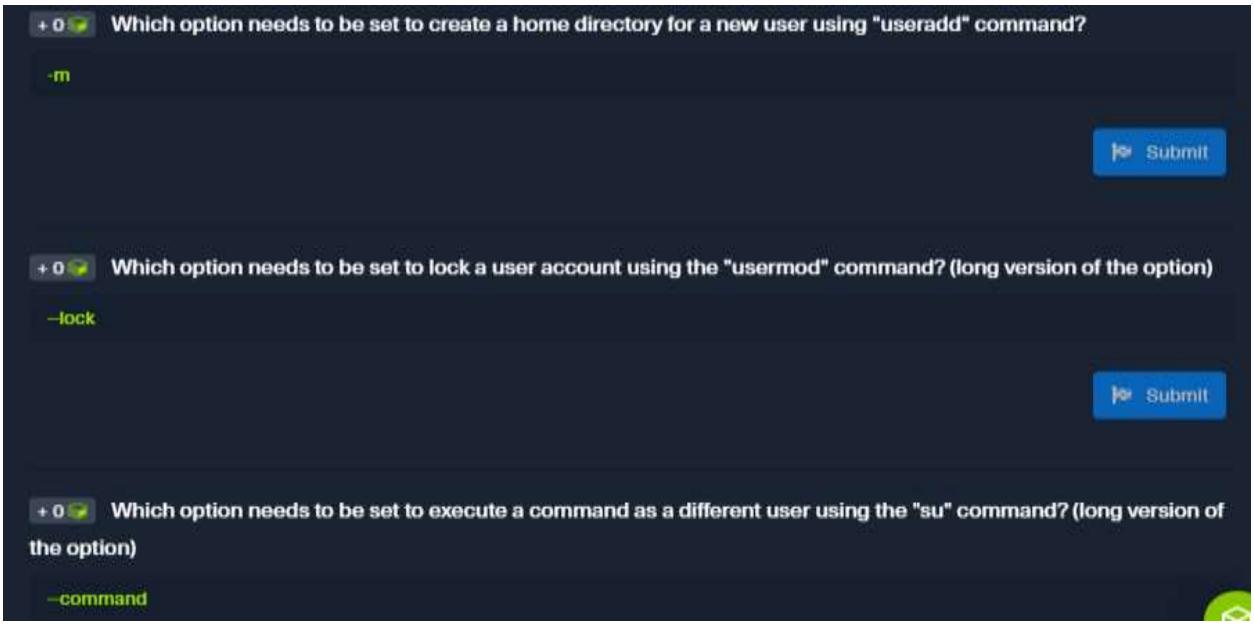


Task 7: User Management.

Just like in windows, sometimes we need to create users for our Linux devices. This task helps us to understand how to create users as well as understanding the permissions of different users to execute commands.

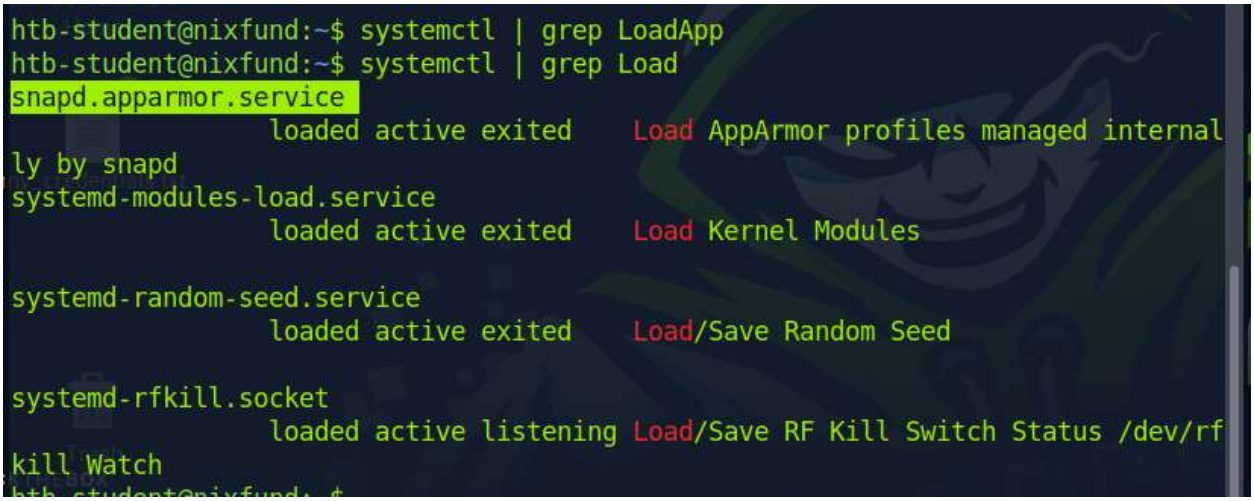
Task 7a,b,c. for a you can use man useradd to find the needed command. For b, you can use man usermod to check for the command. For c, use man su as well. You can as well as use –help for the above commands.

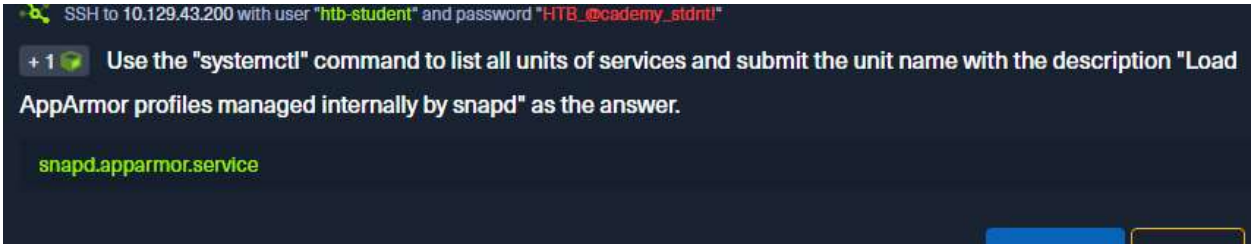
```
┌──(kali㉿kali)-[~]
└─$ su --help

Usage:
 su [options] [-] [<user> [<argument> ... ]]

Change the effective user ID and group ID to that of <user>.
A mere - implies -l.  If <user> is not given, root is assumed.

Options:
 -m, -p, --preserve-environment      do not reset environment variables
 -w, --whitelist-environment <list>  don't reset specified variables

 -g, --group <group>             specify the primary group
 -G, --supp-group <group>        specify a supplemental group

 -, -l, --login                  make the shell a login shell
 -c, --command <command>         pass a single command to the shell with -c
 --session-command <command>     pass a single command to the shell with -c
                                   and do not create a new session
 -f, --fast                      pass -f to the shell (for csh or tcsh)
 -s, --shell <shell>             run <shell> if /etc/shells allows it
 -P, --pty                       create a new pseudo-terminal

 -h, --help                      display this help
 -V, --version                   display version
```



Task 8: Services and process management

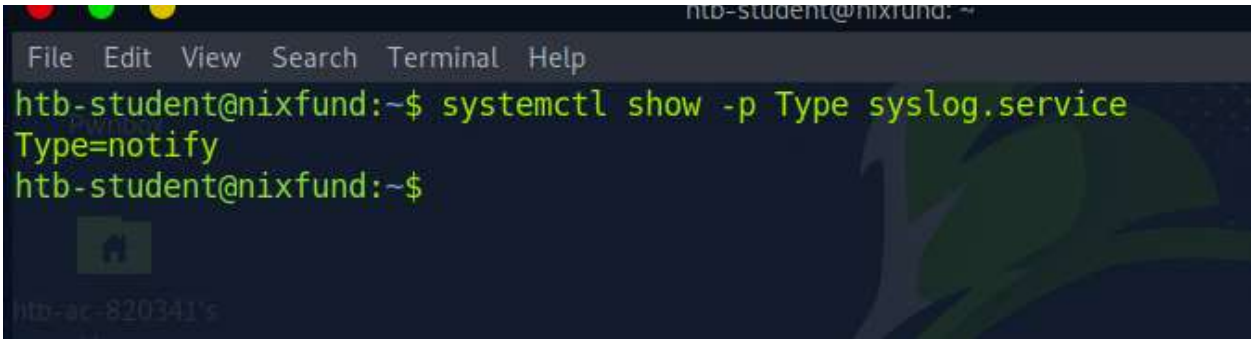
In this module, we are going to learn about Linux package managers and how to utilize them to give the install, update and delete packages. Some commands such as dpkg, apt, aptitude, ps, kill and pip are covered in this module. To solve the question on this module, do systemctl then use the command systemctl |grep Load.

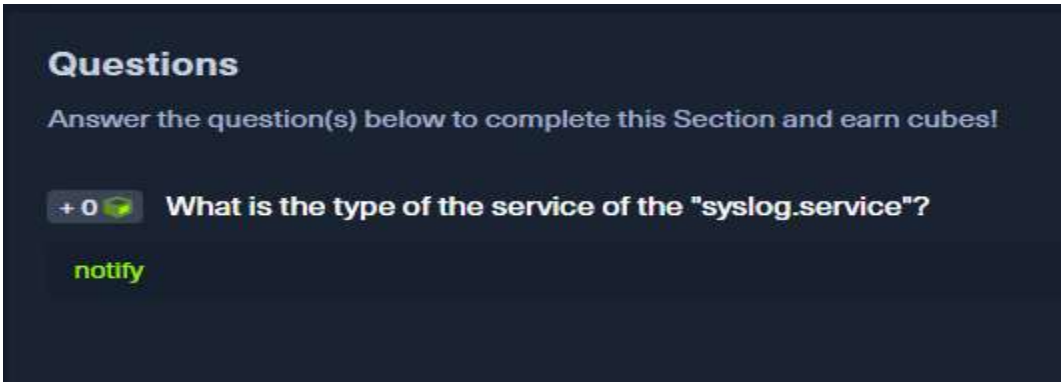




Task 9: Task scheduling

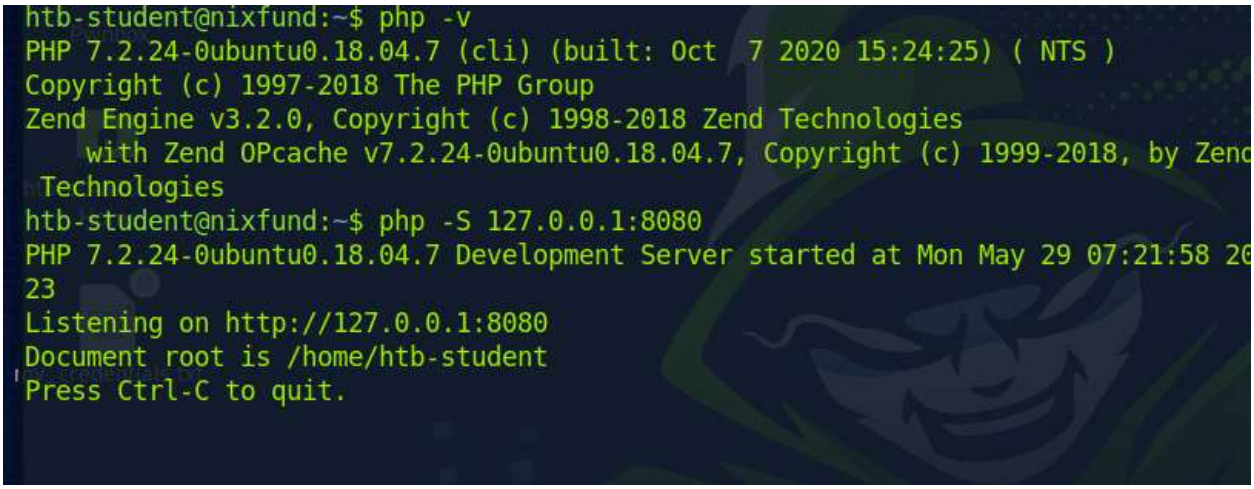
In task scheduling module, we are going to learn how an administrator or a user can automate a task to run at a specific time without having to start the without starting them manually. This can be important when we want to update software, or database cleaning among other tasks that need to be frequently done. To complete task on this module, do the following command as shown below

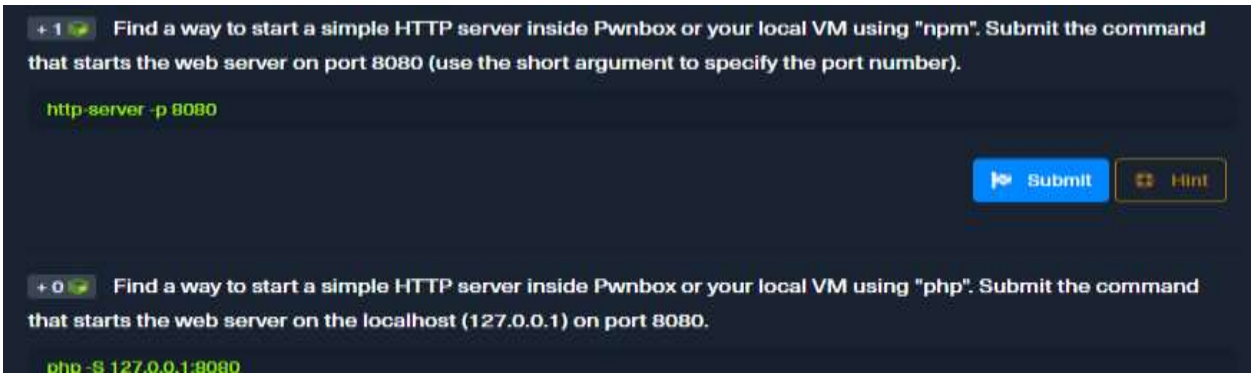




Task 10: working with webservices.

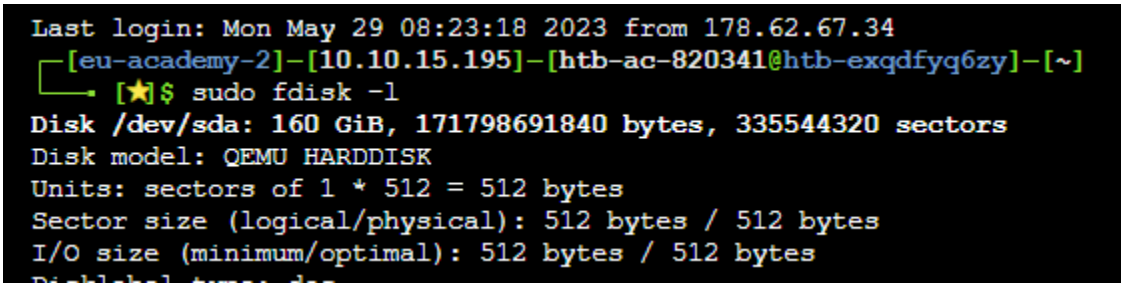
In this module, we are going to learn on different way to set up webservers, webservers include IIs, Nginx and Apache. To complete tasks on this module, lookup for npm simple server, and php simple http server to get the answers.





Task 11: File System Management

In this module, we are going to learn about organization and how to maintain data stored on a disk or any other storage devices. Linux operating system support a very wide range of file systems including the most known NTFS. To complete on the task provided here.



Here is the completion level

Sharable link https://academy.hackthebox.com/achievement/820341/path/20

Conclusion

In conclusion, we have explored the fundamental aspects of Linux within the context of Hackthebox. We started by understanding what Linux is and why it is important in the world of hacking and cybersecurity. We then delved into the key components of Linux, including the file system, processes, permissions, and user management. Additionally, we discussed essential command-line tools and techniques that allow us to interact with Linux effectively. Armed with this knowledge, we can confidently navigate and utilize Linux within the Hackthebox platform, gaining a deeper understanding of its capabilities and leveraging it to enhance our cybersecurity skills.