

UNIT: Linux fundamentals: HackTheBox
NAME: MWITHUI DANIEL MWENDWA
REG NO. CS-SA04-23080
COURSE: SECURITY ANALYST

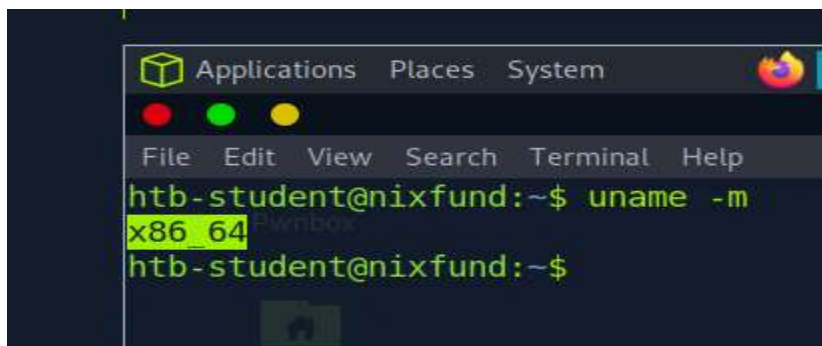
Introduction

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

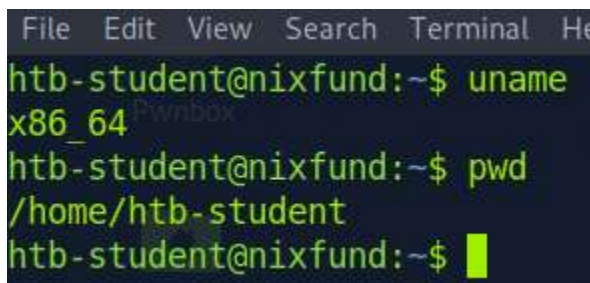
In this task, we learn how to use shell to get information about the system we are running. Commands that we are going to learn here include `whoami` which displays the current username, `id` which returns user id and `uname` which prints basic information about the operating system. Below are screenshots 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.



```
Applications Places System
File Edit View Search Terminal Help
htb-student@nixfund:~$ uname -m
x86_64
htb-student@nixfund:~$
```

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.



```
File Edit View Search Terminal He
htb-student@nixfund:~$ uname
x86_64
htb-student@nixfund:~$ pwd
/home/htb-student
htb-student@nixfund:~$
```

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.

```

/home/htb-student
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/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

```

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.

SSH to 10.129.109.170 with user "htb-student" and password "HTB_@cademry_student"

+ 0 Find out the machine hardware name and submit it as the answer.

x86_64

Submit Hint

+ 1 What is the path to htb-student's home directory?

/home/htb-student

Submit

+ 0 What is the path to the htb-student's mail?

/var/mail/htb-student

Submit

+ 0 Which shell is specified for the htb-student user?

/bin/bash

Submit

+ 0 Which kernel version is installed on the system? (Format: 1.22.3)

4.15.0

Submit

+ 1 What is the name of the network interface that MTU is set to 1500?

ens192

Submit

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
cry0llt3 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-r----- 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 -l to list index of all files there.

```

146907 init
146907 init.d
146908 initramfs-tools
147583 inputrc
148741 insserv.conf.d
146909 iproute2
146910 iscsi
148324 issue
148325 issue.net
146911 kernel
148234 kernel-img.conf
146432 sos.conf
146946 ssh
146947 ssl
148802 subgid
147624 subgid-
148699 subuid
147626 subuid-
147627 sudoers
146948 sudoers.d
147628 sysctl.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_@caderny_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 -li on /var/backups

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

Here is the completed task

+ 0 🟢

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

aptextended_states.0

Submit

+ 1 🟢

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

265293

Submit

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

```
htb-student@nixfund:/$ find / -iname "*.conf" -size +25k -size -28k -newermt 2020-03-03 2>/dev/null
/usr/share/drirc.d/00-mesa-defaults.conf
htb-student@nixfund:/$
```

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

```
htb-student@nixfund:/$ find / -type f -iname "*.bak" 2>/dev/null | wc -l
4
htb-student@nixfund:/$
```

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

```
htb-student@nixfund:/bin$ find /usr/bin -type f -name *xxd
/usr/bin/xxd
htb-student@nixfund:/bin$
```

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.

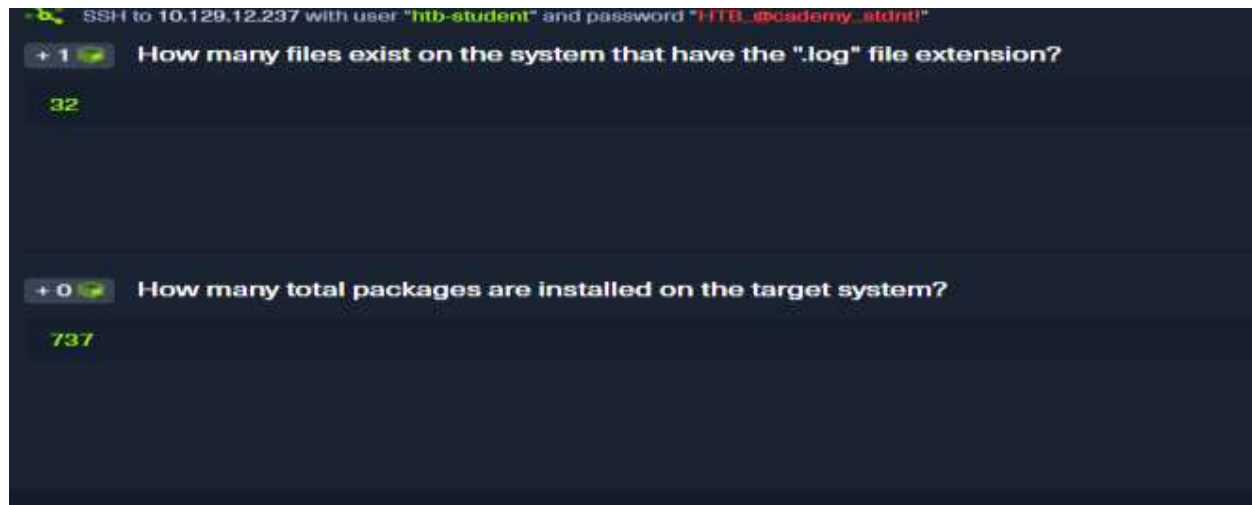
Task 5a. to find files with .log extensions do

```
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 --get-architecture | 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_student!"

+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
tcp6       0      0 ip6-localhost:smtp     ::::*
```

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.

```
htb-student@nixfund:/$ curl https://www.inlane4freight.com | tr " " "\n" | sort -u | grep -E 'src|href'
href="https://www.inlane4freight.com/"
href="https://www.inlane4freight.com/"
href="https://www.inlane4freight.com/index.php/about-us/">About
href="https://www.inlane4freight.com/index.php/career/">Career</li>
href="https://www.inlane4freight.com/index.php/comments/feed/"
href="https://www.inlane4freight.com/index.php/contact/">Contact</a></li>
href="https://www.inlane4freight.com/index.php/feed/"
href="https://www.inlane4freight.com/index.php/news/">News</a></li>
href="https://www.inlane4freight.com/index.php/offices/">Offices</a></li>
href="https://www.inlane4freight.com/index.php/wp-json/"
href="https://www.inlane4freight.com/index.php/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fwww.inlane4freight.com%2F"
href="https://www.inlane4freight.com/index.php/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fwww.inlane4freight.com%2F%2F#038;format=xml"
href="https://www.inlane4freight.com/index.php/wp-json/wp/v2/pages/7"
href="https://www.inlane4freight.com/">Inlane4freight
href="https://www.inlane4freight.com/">Inlane4freight
href="https://www.inlane4freight.com/">Services</a></li>
href="https://www.inlane4freight.com/wp-content/themes/ben_theme/css/animate.css?ver=5.6.9"
href="https://www.inlane4freight.com/wp-content/themes/ben_theme/css/bootstrap.css?ver=5.6.9"
href="https://www.inlane4freight.com/wp-content/themes/ben_theme/css/bootstrap-progressbar.min.css?ver=5.6.9"
href="https://www.inlane4freight.com/wp-content/themes/ben_theme/css/colors/default.css?ver=5.6.9"
href="https://www.inlane4freight.com/wp-content/themes/ben_theme/css/font-awesome.css?ver=5.6.9"
href="https://www.inlane4freight.com/wp-content/themes/ben_theme/css/jquery.smartmenus.bootstrap.css?ver=5.6.9"
href="https://www.inlane4freight.com/wp-content/themes/ben_theme/css/magnific-popup.css?ver=5.6.9"
href="https://www.inlane4freight.com/wp-content/themes/ben_theme/css/owl.carousel.css?ver=5.6.9"
href="https://www.inlane4freight.com/wp-content/themes/ben_theme/css/owl.transitions.css?ver=5.6.9"
href="https://www.inlane4freight.com/wp-content/themes/ben_theme/style.css?ver=5.6.9"
href="https://www.inlane4freight.com/wp-includes/css/dist/block-library/style.min.css?ver=5.6.9"
href="https://www.inlane4freight.com/wp-includes/wlwmanifest.xml"
href="https://www.inlane4freight.com/xmlrpc.php?rsd"
src="https://www.inlane4freight.com/wp-content/themes/ben_theme/js/bootstrap.min.js?ver=5.6.9"
src="https://www.inlane4freight.com/wp-content/themes/ben_theme/js/jquery.smartmenus.bootstrap.js?ver=5.6.9"
src="https://www.inlane4freight.com/wp-content/themes/ben_theme/js/jquery.smartmenus.js?ver=5.6.9"
src="https://www.inlane4freight.com/wp-content/themes/ben_theme/js/navigation.js?ver=5.6.9"
src="https://www.inlane4freight.com/wp-content/themes/ben_theme/js/owl.carousel.min.js?ver=5.6.9"
src="https://www.inlane4freight.com/wp-includes/js/jquery/jquery.migrate.min.js?ver=3.3.2"
src="https://www.inlane4freight.com/wp-includes/js/jquery/jquery.min.js?ver=3.5.1"
src="https://www.inlane4freight.com/wp-includes/js/wp-embed.min.js?ver=5.6.9"
```

Here is the task completion for this task.

0 How many services are listening on the target system on all interfaces? (Not on localhost and IPv4 only)

7

Submit

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

proftpd

Submit

1 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.

34

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
```

+ 0 🟢 Which option needs to be set to create a home directory for a new user using "useradd" command?

-m

Submit

+ 0 🟢 Which option needs to be set to lock a user account using the "usermod" command? (long version of the option)

--lock

Submit

+ 0 🟢 Which option needs to be set to execute a command as a different user using the "su" command? (long version of the option)

--command

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.

```
htb-student@nixfund:~$ systemctl | grep LoadApp
htb-student@nixfund:~$ systemctl | grep Load
snapd.apparmor.service
loaded active exited Load AppArmor profiles managed internal
ly by snapd
systemd-modules-load.service
loaded active exited Load Kernel Modules
systemd-random-seed.service
loaded active exited Load/Save Random Seed
systemd-rfkill.socket
loaded active listening Load/Save RF Kill Switch Status /dev/rf
kill Watch
htb-student@nixfund:~$
```

SSH to 10.129.43.200 with user "htb-student" and password "HTB_@cademy_stdnt"

+ 1 🟢 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.

snapd.apparmor.service

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

```
htb-student@nixfund:~$ systemctl show -p Type syslog.service
Type=notify
htb-student@nixfund:~$
```

Questions

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

+ 0

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

notify

Task 10: working with webservices.

In this module, we are going to learn on different way to set up websevers, websevers 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.

```
htb-student@nixfund:~$ php -v
PHP 7.2.24-0ubuntu0.18.04.7 (cli) (built: Oct  7 2020 15:24:25) ( NTS )
Copyright (c) 1997-2018 The PHP Group
Zend Engine v3.2.0, Copyright (c) 1998-2018 Zend Technologies
    with Zend OPcache v7.2.24-0ubuntu0.18.04.7, Copyright (c) 1999-2018, by Zend
Technologies
htb-student@nixfund:~$ php -S 127.0.0.1:8080
PHP 7.2.24-0ubuntu0.18.04.7 Development Server started at Mon May 29 07:21:58 20
23
Listening on http://127.0.0.1:8080
Document root is /home/htb-student
Press Ctrl-C to quit.
```


+1 🟢 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).

```
http-server -p 8080
```

Submit Hint

+0 🟢 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.

```
php -S 127.0.0.1:8080
```

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.

```
Last login: Mon May 29 08:23:18 2023 from 178.62.67.34
[eu-academy-2]-[10.10.15.195]-[htb-ac-820341@htb-exqdfyq6zy]-[~]
[★]$ sudo fdisk -l
Disk /dev/sda: 160 GiB, 171798691840 bytes, 335544320 sectors
Disk model: QEMU HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
```

Here is the completion level

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



Operating System Fundamentals

Congratulations **CyberDance!**
You have just completed the Operating System Fundamentals path!

Let's share your success with everyone!

in Share on LinkedIn 🐦 Share on Twitter f Share on Facebook

🌐 Get a shareable link

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.