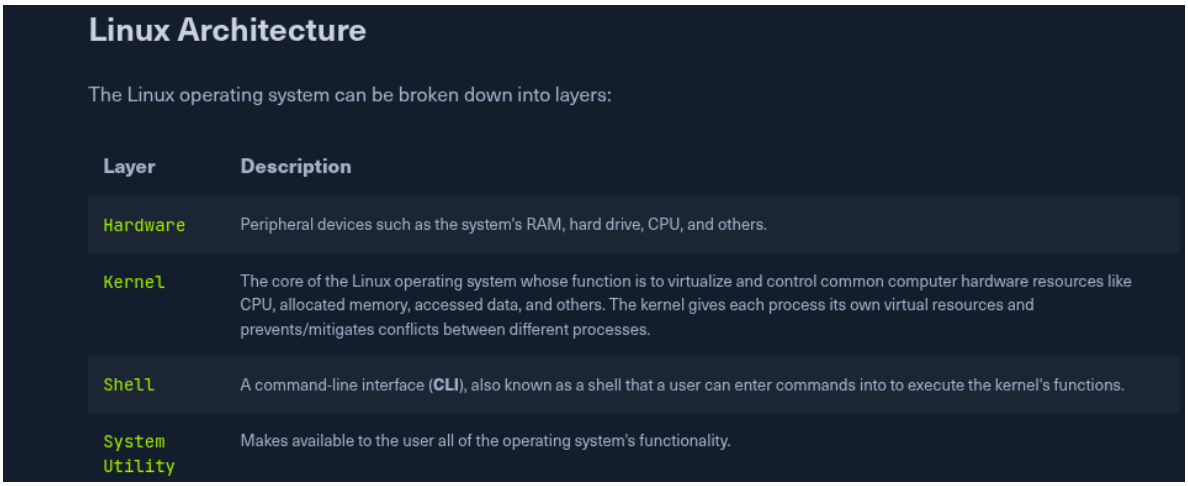
LINUX FUNDAMENTAL

Overview

Linux is an OS known for its robustness,flexibility and its open source nature.

Linux at first was a personal project started in 1991 by a Finnish student named Linux Trovalds whose goal was to create a new free OS kernel.

Linux has over many distribution but the most known ones are Ubuntu,Debian,Fedora,RedHat, OpenSuse and is generally considered more secure compared to other OS because its frequently updated.



Linux Architecture

The Linux operating system can be broken down into layers:

Layer	Description
Hardware	Peripheral devices such as the system's RAM, hard drive, CPU, and others.
Kernel	The core of the Linux operating system whose function is to virtualize and control common computer hardware resources like CPU, allocated memory, accessed data, and others. The kernel gives each process its own virtual resources and prevents/mitigates conflicts between different processes.
Shell	A command-line interface (**CLI**), also known as a shell that a user can enter commands into to execute the kernel's functions.
System Utility	Makes available to the user all of the operating system's functionality.

The Linux operating system is structured in a tree-like hierarchy and is documented in file system hierarchy standard and the top common file directories are:

(i) /bin which contains essential command binaries.

(ii) /boot consists of static boot loader,kernel executable and file required to boot the Linux OS.

(iii) /dev – contains device files to facilitate access to every hardware device attached to the sytsem.

(iv) /etc – local system configuration files also for installed applications.

(v) /lib – shared libraries files that are required for system boot.

(vi) /var – contains variable data files such as log files,emails in-boxes,web application related files,cron files and more.

(vii) /usr – contains executable,libraries,man files and more.

This module will help get familiar with all skills required when dealing with Linux OS and also foundational knowledge on Linux. The aim is to provide hands-on experience with real Linux environment such as pwnbox and virtual machine.

Introduction to shell

Shell in simple terms is a command line or a Linux terminal which provides a text based I/O interface between users and kernel for a computer system.
The most commonly used shell is bourne-again shell(bash).
Terminal emulators are software that emulates the function of a terminal allowing use of text-based programs within a GUI.
Terminal emulators and multiplexers are beneficial extensions for the terminal as they provide different methods and functions to work with terminal such as splitting the terminal into one window, working in multiple directories,creating different workspaces and much more. An example of the use of multiplexer is tmux.

Prompt Description

Here will be talking about PS1(Prompt customization) which is the environment variable in Linux/Unix system that controls how your command prompts looks.
The importance of customizing is because when doing penetration testing it helps to have more info visible directly in the terminal such as username(/u),hostname(/H),current working directories(/w),time(A).
This helps track what you are doing more clearly and avoid confusions.
To make your custom prompt(PS1) permanent you need to add export command to your shell configuration file(~/.bashrc).
To do this open the file in text editor and scroll to the bottom of the file.

```
$nano ~/.bashrc
```

Next add this :

```
export PS1='[\u@\h \W \A $(if [ $? = 0 ]; then echo ":)"; else echo ":("; fi)]\$ '
```

To apply this change run : `$source ~/.bashrc`

Some of this sysmbols are explained above but the if part will show if last command was successful or : it failed and every time your shell will be showing this and if you want to stop it you can delete it or put # to comment it out.

Getting Help

In Linux to get more info about the tool use the command (man or help)

Logging in via SSH

Secure Shell(ssh) is a protocol that allows client to access and execute commands or actions on remote computers.

To login to the target machine will do the following:

```
$ ssh htb-student@10.129.2.219
```

Questions:

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

In here the command *uname* will be used with an option -m to display the machine hardware name.

Answer x86_64

```
htb-student@nixfund:~$ uname -m
x86_64
```

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

Pwd command is used to print the current working directory.

Answer :/home/htb-student

```
htb-student@nixfund:~$ pwd
/home/htb-student
```

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

echo command can be used here to display the path of student mail.

Answer /var/mail/htb-student

```
htb-student@nixfund:~$ echo $MAIL
/var/mail/htb-student
```

Which shell is specified for the htb-student user?

Answer /bin/bash

```
htb-student@nixfund:~$ echo $SHELL
/bin/bash
```

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

answer 4.15.0

```
htb-student@nixfund:~$ uname -r
4.15.0-123-generic
```

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

answer ens192

```
htb-student@nixfund:~$ ifconfig
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.129.2.219  netmask 255.255.0.0  broadcast 10.129.255.255
        inet6 dead:beef::250:56ff:fe94:2147  prefixlen 64  scopeid 0x0<global
```

Navigation

This is essential as it allow ones to move across the system and work in directories and with the files one need and want by using different commands and tools to print out information about a directory or file.

Examples of commands include ls,ls -al,ls -l which are used to list out directories and files.

Questions:

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

Answer .bash_history

```
htb-student@nixfund:~$ ls -al
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  151 May 18 08:21 .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
```

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

Answer 147627

```
htb-student@nixfund:~$ ls -i /etc/sudoers
147627 /etc/sudoers
```

Working with files and directories

This part involves creating using touch for text file and mkdir command for directories/folders, moving using mv command and copying file or directories using cp command.

For example creating a file within a specific directories can be done by specifying the path where the file should be stored by using a single dot to indicate you want to start from the current working directories. *touch ./storage/local/user/userinfo.txt*

The mv command sysntax is :

mv <file/directory> <renamed file/directory>

This command (mv) can be used also to rename a file.

To mv a file into a specific directory do *mv file/directory* folder/

Questions

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

Answer apt.extended_states.0

```
htb-student@nixfund:~$ ls -lat /var/backups
total 2168
drwxr-xr-x  2 root root     4096 Aug  3  2021 .
-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
-rw-r--r--  1 root root   742750 Nov 11  2020 dpkg.status.0
-rw-r--r--  1 root root   206270 Nov 11  2020 dpkg.status.1.gz
-rw-r--r--  1 root root   206270 Nov  5  2020 dpkg.status.2.gz
```

used ls -lat command to list out files with the time each was modified by using option -t

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

Answer 265293

used ls with an option i to list files with their inode number

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

Finding files and directories

The most crucial tools/commands here are which, find, locate.

Questions

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? 00-mesa-defaults.conf

the command find will be used with various options.

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

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

4

```
htb-student@nixfund:~$ locate .bak
/var/backups/group.bak
/var/backups/gshadow.bak
/var/backups/passwd.bak
/var/backups/shadow.bak
```

Submit the full path of the "xxd" binary.

/usr/bin/xxd

```
htb-student@nixfund:~$ which xxd
/usr/bin/xxd
```

Files Descriptors and Redirections

Questions

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

32

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

How many total packages are installed on the target system?

737

```
htb-student@nixfund:~$ dpkg -l | grep ^ii | wc -l
737
```

the command grep ^ii filter lines for packages that are fully installed

Filter content

The command less or more will be helpful in this section. Also head command if one want to get the first lines of the file. tail command would be opposite of what the head command does(last lines of the file).

Grep command is used to search for specific results that match patterns we define.

wc command is used to avoid counting the lines or characters manually and if its line it is used with an option -l.

Questions:

How many services are listening on the target system on all interfaces? (Not on localhost and IPv4 only) 8

```
htb-student@nixfund:~$ ss -tuln4 | grep 'LISTEN' | grep -v '127.0.0.1' | wc -l
8
```

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

Proftpd

```
htb-student@nixfund:~$ ps aux | grep proftpd
proftpd     1904  0.0  0.1 126440  3672 ?        Ss   07:00   0:00 proftpd: (accepting connections)
htb-stu+    5995  0.0  0.0  13144  1112 pts/0    S+   07:03   0:00 grep --color=auto 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 (https://www.inlanefreight.com/directory" or "/another/directory") of that domain. Submit the number of these paths as the answer.

34

Regular expressions

Regular expressions (RegEx) are like the art of crafting precise blueprints for searching patterns in text or fileswhich allow you to find, replace and manipulate data with incredible precision.

Regular expression is a sequence of characters and symbols that together form a search pattern. These patterns often involve special symbols called metacharacters, which define the structure of the search rather than representing literal text.

Basically, regex follows three different concepts, which are distinguished by the three different brackets:

Grouping Operators

	Operators	Description
1	(a)	The round brackets are used to group parts of a regex. Within the brackets, you can define further patterns which should be processed together.
2	[a-z]	The square brackets are used to define character classes. Inside the brackets, you can specify a list of characters to search for.
3	{1,10}	The curly brackets are used to define quantifiers. Inside the brackets, you can specify a number or a range that indicates how often a previous pattern should be repeated.
4	|	Also called the OR operator and shows results when one of the two expressions matches
5	.*	Operates similarly to an AND operator by displaying results only when both expressions are present and match in the specified order

User Management

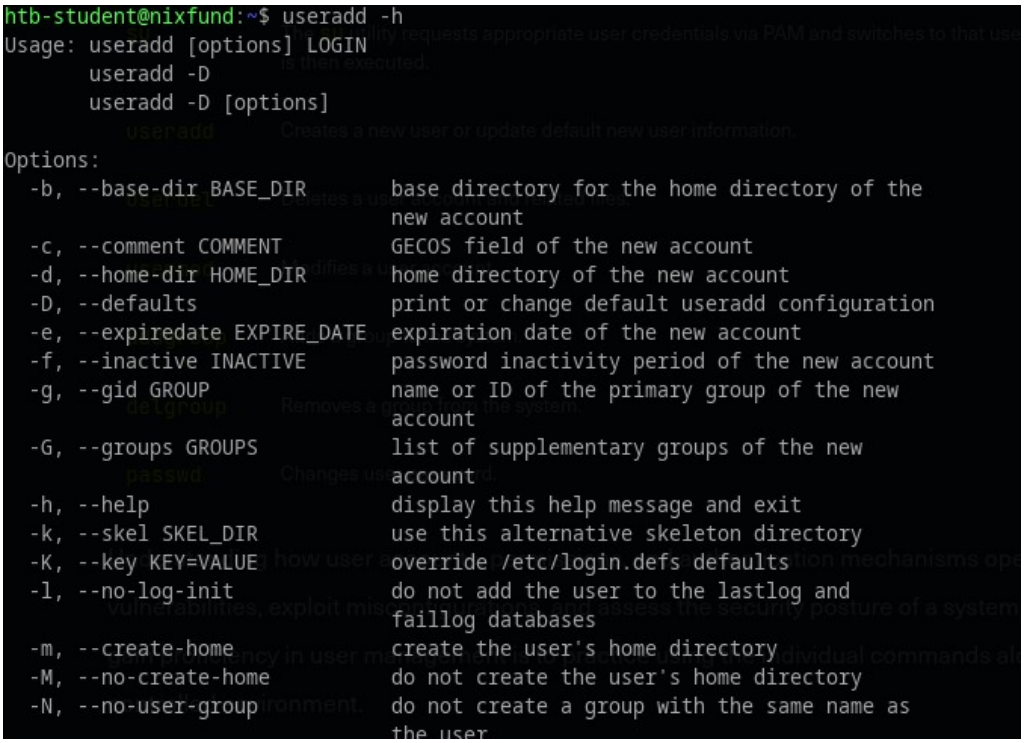
Administrators frequently need to create new user accounts or assign existing users to specific groups to enforce appropriate access controls.

Additionally, executing commands as a different user is often necessary for tasks that require different privileges. For example, certain groups may have exclusive permissions to view or modify specific files or directories, which is essential for maintaining system security and integrity.

The /etc/shadow file is a critical system file that stores encrypted password information for all user accounts. For security reasons, it is readable and writable only by the root user to prevent unauthorized access to sensitive authentication data.

Questions:

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



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

```
htb-student@nixfund:~$ usermod -h
Usage: usermod [options] LOGIN

Options:
  -c, --comment COMMENT         new value of the GECOS field
  -d, --home HOME_DIR           new home directory for the user account
  -e, --expiredate EXPIRE_DATE  set account expiration date to EXPIRE_DATE
  -f, --inactive INACTIVE       set password inactive after expiration
                                to INACTIVE
  -g, --gid GROUP               force use GROUP as new primary group
  -G, --groups GROUPS           new list of supplementary GROUPS
  -a, --append                  append the user to the supplemental GROUPS
                                mentioned by the -G option without removing
                                him/her from other groups
  -h, --help                    display this help message and exit
  -l, --login NEW_LOGIN         new value of the login name
  -L, --lock                    lock the user account
  -m, --move-home               move contents of the home directory to the
                                new location (use only with -d)
```

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

```
htb-student@nixfund:~$ su --help
Usage: su [options] [LOGIN]

Options:
  -c, --command COMMAND         pass COMMAND to the invoked shell
  -h, --help                    display this help message and exit
  -, -l, --login                make the shell a login shell
  -m, -p,
  --preserve-environment        do not reset environment variables, and
                                keep the same shell
  -s, --shell SHELL             use SHELL instead of the default in passwd
```

Package management

The package management requirement is that the software to be installed is available as a corresponding package.

The package management software retrieves the necessary changes for system installation from the package itself and then implements these changes to install the package successfully. If the package management software recognizes that additional packages are required for the proper functioning of the package that has not yet been installed, a dependency is included and either warns the

administrator or tries to reload the missing software from a repository, for example, and install it in advance.

If an installed software has been deleted, the package management system then retakes the package's information, modifies it based on its configuration, and deletes files.

Examples of this programs are:

Command	Description
`dpkg`	The `dpkg` is a tool to install, build, remove, and manage Debian packages. The primary and more user-friendly front-end for `dpkg` is aptitude.
`apt`	Apt provides a high-level command-line interface for the package management system.
`aptitude`	Aptitude is an alternative to apt and is a high-level interface to the package manager.
`snap`	Install, configure, refresh, and remove snap packages. Snaps enable the secure distribution of the latest apps and utilities for the cloud, servers, desktops, and the internet of things.
`gem`	Gem is the front-end to RubyGems, the standard package manager for Ruby.
`pip`	Pip is a Python package installer recommended for installing Python packages that are not available in the Debian archive. It can work with version control repositories (currently only Git, Mercurial, and Bazaar repositories), logs output extensively, and prevents partial installs by downloading all requirements before starting installation.
`git`	Git is a fast, scalable, distributed revision control system with an unusually rich command set that provides both high-level operations and full access to internals.

Services and Process management

Services, also known as daemons, run silently in the background "without direct user interaction" and perform crucial tasks that keep the system operational and provide additional functionalities.

A process can be in running,waiting,stopped and zombie state and can be controlled using kill, pkill, pgrep, and killall. To interact with a process we must send signals to it and common used signals are:

Signal	Description
1	`SIGHUP` - This is sent to a process when the terminal that controls it is closed.
2	`SIGINT` - Sent when a user presses `[Ctrl] + C` in the controlling terminal to interrupt a process.
3	`SIGQUIT` - Sent when a user presses `[Ctrl] + D` to quit.
9	`SIGKILL` - Immediately kill a process with no clean-up operations.
15	`SIGTERM` - Program termination.
19	`SIGSTOP` - Stop the program. It cannot be handled anymore.
20	`SIGTSTP` - Sent when a user presses `[Ctrl] + Z` to request for a service to suspend. The user can handle it afterward.

Questions:

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.

Answer snapd.apparmor.service

```
htb-student@nixfund:~$ systemctl -l | grep "Load AppArmor profiles managed internally by snapd"
snapd.apparmor.service
 snapd
htb-student@nixfund:~$
```

Task Scheduling

This allows users and administrators to automate tasks by running them at specific times or regular intervals, eliminating the need for manual initiation.

Tools or commands to use are systemd and cron

Questions:

What is the Type of the service of the "dconf.service"? Dbus

```
htb-student@nixfund:~$ find /usr/share/dbus-1/ -name "*dconf*"
/usr/share/dbus-1/services/ca.desrt.dconf.service
htb-student@nixfund:~$ cat /usr/share/dbus-1/services/ca.desrt.dconf.service
[D-BUS Service]
Name=ca.desrt.dconf
Exec=/usr/lib/dconf/dconf-service
```

Network Services

SSH and NFS are two protocols that will concentrate on.

SSH is used because it provides secure way of transmission of data and command over network ;the most commonly server is OpenSSH server which is free.

NFS is a network protocol that allows us to store and manage files on remote systems as if they were stored on local system. It also provides same features as FTP like sharing and managing resources .

Working with web services

Apache is mostly used web server due to its modularity, it can be customized and extended with various modules to perform specific tasks.

For example, mod_ssl acts like a lockbox, securing the communication between the browser and the web server by encrypting the data. The mod_proxy module is like a traffic controller, directing requests to the correct destination, especially useful when setting up proxy servers.

Other modules such as mod_headers and mod_rewrite give you fine control over the data traveling between browser and server, allowing you to modify HTTP headers and URLs on the fly, like adjusting the course of a stream.

Curl and wget tools are useful in communicating with the web server when one want to systematically analyze the content of a webpage hosted on a web server.

Questions:

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).

Answer 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.

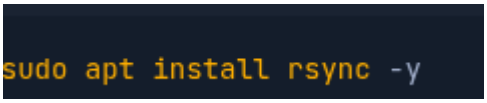
answer php -S 127.0.0.1:8080

Backup and restore

When backing up data on ubuntu system various options are available Rsync,Deja Dup and Duplicity. Rsync is an open-source tool that allows for fast and secure backups, whether locally or to a remote location. One of its key advantages is that it only transfers the portions of files that have changed, making it highly efficient when dealing with large amounts of data.

Duplicity is another powerful tool that builds on Rsync, but adds encryption features to protect the backups. It allows you to encrypt your backup copies, ensuring that sensitive data remains secure even if stored on remote servers, FTP sites, or cloud services like Amazon S3.

To install rysnc do the following:



To backup an entire directory using rysnc use following commands

```
rsync -av /path/to/mydirectory user@backup_server:/path/to/backup/directory
```

This command will copy the entire directory (/path/to/mydirectory) to a remote host (backup_server), to the directory /path/to/backup/directory. The option archive (-a) is used to preserve the original file attributes, such as permissions, timestamps, etc., and using the verbose (-v) option provides a detailed output of the progress of the rsync operation.

It can be further customized by adding the backup process such as compression and incremental backups .

```
rsync -avz --backup --backup-dir=/path/to/backup/folder --delete /path/to/mydirectory user@backup_server:/path/to/backup/directory
```

With this, we back up the mydirectory to the remote backup_server, preserving the original file attributes, timestamps, and permissions, and enabled compression (-z) for faster transfers. The --backup option creates incremental backups in the directory /path/to/backup/folder, and the --delete option removes files from the remote host that is no longer present in the source directory.

To restore the backup

```
rsync -av user@remote_host:/path/to/backup/directory /path/to/mydirectory
```

To ensure security of rysnc file transfer between our local host and backup server a combination of the use of ssh and other security measures are used as ssh encrypts data as it is being transferred.

```
rsync -avz -e ssh /path/to/mydirectory user@backup_server:/path/to/backup/directory
```

File system management

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

```
htb-student@nixfund:~$ lsblk -o NAME,TYPE | grep part | wc -l
2
```

Conclusion

Through this Linux Fundamentals assignment, I have gained a deeper understanding of how to interact with and manage a Linux-based system. I learned how to navigate the file system, use essential commands, manage files and directories, check system status, and work with users and permissions. I also explored basic networking commands and understood how services run in the background. This hands-on experience improved my confidence in using the command line and taught me how to approach real-world Linux tasks more efficiently. Overall, the assignment strengthened my problem-solving skills and gave me a solid foundation for further studies in cybersecurity and system administration. Also it improved my searching skills that would be essential in future when dealing and solving related problems.

https://academy.hackthebox.com/achievement/1917469/18