

TASK 2

Linux Fundamentals Part 1:- Embark on the journey of learning the fundamentals of Linux. Learn to run some of the first essential commands on an interactive terminal.

Task 1:- Introduction

Task 1 Introduction



Welcome to the first part of the "Linux Fundamentals" room series. You're most likely using a Windows or Mac machine, both are different in visual design and how they operate. Just like Windows, iOS and MacOS, Linux is just another operating system and one of the most popular in the world powering smart cars, android devices, supercomputers, home appliances, enterprise servers, and more.

We'll be covering some of the history behind Linux and then eventually starting your journey of being a Linux-wizard! This room will have you:

- Running your very first commands in an interactive Linux machine in your browser
- Teaching you some essential commands used to interact with the file system
- Introduce you to how users and groups work on Linux (and what this means for us as penetration testers)

Answer the questions below

Let's get started!

No answer needed

Correct Answer

Task 2:- A Bit of Background on Linux

Task 2 A Bit of Background on Linux

Where is Linux Used?

It's fair to say that Linux is a lot more intimidating to approach than Operating System's (OSs) such as Windows. Both variants have their own advantages and disadvantages. For example, Linux is considerably much more lightweight and you'd be surprised to know that there's a good chance you've used Linux in some form or another every day! Linux powers things such as:

- Websites that you visit
- Car entertainment/control panels
- Point of Sale (PoS) systems such as checkout tills and registers in shops
- Critical infrastructures such as traffic light controllers or industrial sensors

Flavours of Linux

The name "Linux" is actually an umbrella term for multiple OS's that are based on UNIX (another operating system). Thanks to UNIX being open-source, variants of Linux comes in all shapes and sizes - suited best for what the system is being used for.

For example, Ubuntu & Debian are some of the more commonplace distributions of Linux because it is so extensible. I.e. you can run Ubuntu as a server (such as websites & web applications) or as a fully-fledged desktop. For this series, we're going to be using Ubuntu.

Ubuntu Server can run on systems with only 512MB of RAM

Similar to how you have different versions Windows (7, 8 and 10), there are many different versions/distributions of Linux.

Answer the questions below

Research: What year was the first release of a Linux operating system?

1991

Correct Answer

TASK 2

Task 3:- Interacting With Your First Linux Machine (In-Browser)

Active Machine Information

| Title | IP Address | Expires | |
|--------------|---------------|------------|--|
| linuxfundpt1 | 10.10.144.238 | 1h 58m 49s | <div>? Add 1 hour</div> <div>Terminate</div> |

This contains all of the information for the machine deployed in the room including the IP address and expiry timer - along with buttons to manage the machine. Remember to **"Terminate"** a machine once you are done with the room. More information on this can be found in the [tutorial](#) room.

For now, press **"Start Machine"** where you will be able to interact with your own Linux machine within your browser whilst following along with this room:

Task 3 - Interacting With Your First Linux Machine (In-Browser)

This room has a Ubuntu Linux machine that you can interact with all within your browser while following along with this room's material.

Answers: To get started, simply press the green "Deploy" button on the top right of this task indicated by the arrow on the right.

Clear displayed, a card will appear at the top of the room:

Active Machine Information

This contains all of the information for the machine deployed in the room including the IP address and expiry timer along with buttons to manage the machine. Remember to "Terminate" a machine once you are done with the room. More information on this can be found in the tutorial room.

For now, press "Start Machine" where you will be able to interact with your own Linux machine within your browser whilst following along with this room:

Update me...

No answer needed

Task 3 - Interacting With Your First Linux Machine (In-Browser)

tryhackme@linux1:~\$

Answer the questions below

I've deployed my first Linux machine!

No answer neededCorrect Answer

```
welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.11.0-1017-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

System information as of Sat Jan 20 14:53:28 UTC 2024

System load:  0.03          Processes:           108
Usage of /:   18.7% of 9.63GB Users logged in:        0
Memory usage: 39%          IPv4 address for ens5: 10.10.38.164
Swap usage:   0%

0 updates can be applied immediately.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

tryhackme@linux1:~$
```

Task 4:- Running Your First few Commands

We need to be able to do basic functions like navigate to files, output their contents and make files! The commands to do so are self-explanatory (once you know what they are of course...)

Let's get started with two of the first commands which I have broken down in the table below:

| Command | Description |
|---------|--|
| echo | Output any text that we provide |
| whoami | Find out what user we're currently logged in as! |

See the snippets below for an example of each command being used...

Using echo

```
tryhackme@linux1:~$ echo "Hello Friend!"
Hello Friend!
```

Using whoami to find out the username of who we're logged in as

```
tryhackme@linux1:~$ whoami
tryhackme
```

Try this on your Linux machine now!

Answer the questions below

If we wanted to output the text **"TryHackMe"**, what would our command be?

echo TryHackMeCorrect AnswerHint

What is the username of who you're logged in as on your deployed Linux machine?

tryhackmeCorrect AnswerHint

Task 5 - Interacting With the Filesystem!

```
welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.11.0-1017-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

System information as of Sat Jan 20 14:53:28 UTC 2024

System load:  0.03          Processes:           108
Usage of /:   18.7% of 9.63GB Users logged in:        0
Memory usage: 39%          IPv4 address for ens5: 10.10.38.164
Swap usage:   0%

0 updates can be applied immediately.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

tryhackme@linux1:~$ echo "Hello Tushar Gitte Welcome to Linux!"
Hello Tushar Gitte Welcome to Linux!
tryhackme@linux1:~$ whoami
tryhackme
tryhackme@linux1:~$
```

TASK 2

Task 5:- Interacting With the Filesystem!

It's easy to lose track of where we are on the filesystem exactly, which is why I want to introduce **"pwd"**. This stands for **print Working directory**.

Using the example machine from before, we are currently in the "Documents" folder — but where is this exactly on the Linux machine's filesystem? We can find this out using this "pwd" command like within the screenshot below:

```
Using "pwd" to list the full path of the current directory

tryhackme@linux1:~/Documents$ pwd
/home/ubuntu/Documents
tryhackme@linux1:~/Documents$
```

Let's break this down:

1. We already know we're in "Documents" thanks to our terminal, but at this point in time, we have no idea where "Documents" is stored so that we can get back to it easily in the future.
2. I have used the **"pwd"** (print working directory) command to find the full file path of this "Documents" folder.
3. We're helpfully told by Linux that this "Documents" directory is stored at `"/home/ubuntu/Documents"` on the machine — great to know!
4. Now in the future, if we find ourselves in a different location, we can just use `cd /home/ubuntu/Documents` to change our working directory to this "Documents" directory.

Answer the questions below

On the Linux machine that you deploy, how many folders are there?

Correct Answer

Which directory contains a file?

Correct Answer

Hint

What is the contents of this file?

Correct Answer

Use the cd command to navigate to this file and find out the new current working directory. What is the path?

Correct Answer

```
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.11.0-1017-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

System information as of Sat Jan 20 14:53:28 UTC 2024

System load:  0.03          Processes:    108
Usage of /:   18.7% of 9.63GB Users logged in: 0
Memory usage: 39%          IPv4 address for ens5: 10.10.38.164
Swap usage:   0%

0 updates can be applied immediately.
```

The list of available updates is more than a week old.
To check for new updates run: `sudo apt update`

```
tryhackme@linux1:~$ echo "Hello Tushar Gitte Welcome to Linux!"
Hello Tushar Gitte Welcome to Linux!
tryhackme@linux1:~$ whoami
tryhackme
tryhackme@linux1:~$ ls
access.log  folder1  folder2  folder3  folder4
tryhackme@linux1:~$ cd folder1
tryhackme@linux1:~/folder1$ ls
tryhackme@linux1:~/folder1$ cd ..
tryhackme@linux1:~$ ls folder4
note.txt
tryhackme@linux1:~$ ls folder3
tryhackme@linux1:~$ ls folder2
tryhackme@linux1:~$ ls folder1
tryhackme@linux1:~$ cd folder4
tryhackme@linux1:~/folder4$ cat note.txt
Hello World!
tryhackme@linux1:~/folder4$ cd..
cd..: command not found
tryhackme@linux1:~/folder4$ cd ..
tryhackme@linux1:~$ cd folder4
tryhackme@linux1:~/folder4$ pwd
/home/tryhackme/folder4
tryhackme@linux1:~/folder4$ ^C
tryhackme@linux1:~/folder4$
```

Task 6:- Searching for Files

Another great utility that is a great one to learn about is the use of **grep**. The **grep** command allows us to search the contents of files for specific values that we are looking for.

Take for example, the access log of a web server. In this case, the access.log of a web server has 244 entries.

```
Using "wc" to count the number of entries in "access.log"

tryhackme@linux1:~$ wc -l access.log
244 access.log
tryhackme@linux1:~$
```

Using a command like **cat** isn't going to cut it too well here. Let's say for example if we wanted to search this log file to see the things that a certain user/IP address visited? Looking through 244 entries isn't all that efficient considering we want to find a specific value.

We can use **grep** to search the entire contents of this file for any entries of the value that we are searching for. Going with the example of a web server's access log, we want to see everything that the IP address "81.143.211.90" has visited (note that this is fictional)

```
Using "grep" to find any entries with the IP address of "81.143.211.90" in "access.log"

tryhackme@linux1:~$ grep "81.143.211.90" access.log
81.143.211.90 - - [25/Mar/2021:11:17 + 0000] "GET / HTTP/1.1" 200 417 "-" "Mozilla/5.0
(Linux; Android 7.0; Moto G(4))"
tryhackme@linux1:~$
```

"Grep" has searched through this file and has shown us any entries of what we've provided and that is contained within this log file for the IP.

Answer the questions below

Use grep on "access.log" to find the flag that has a prefix of "THM". What is the flag?

Correct Answer

Hint

And I still haven't found what I'm looking for!

Correct Answer

```
* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

System information as of Sat Jan 20 14:53:28 UTC 2024

System load:  0.03          Processes:    108
Usage of /:   18.7% of 9.63GB Users logged in: 0
Memory usage: 39%          IPv4 address for ens5: 10.10.38.164
Swap usage:   0%

0 updates can be applied immediately.
```

The list of available updates is more than a week old.
To check for new updates run: `sudo apt update`

```
tryhackme@linux1:~$ echo "Hello Tushar Gitte Welcome to Linux!"
Hello Tushar Gitte Welcome to Linux!
tryhackme@linux1:~$ whoami
tryhackme
tryhackme@linux1:~$ ls
access.log  folder1  folder2  folder3  folder4
tryhackme@linux1:~$ cd folder1
tryhackme@linux1:~/folder1$ ls
tryhackme@linux1:~/folder1$ cd ..
tryhackme@linux1:~$ ls folder4
note.txt
tryhackme@linux1:~$ ls folder3
tryhackme@linux1:~$ ls folder2
tryhackme@linux1:~$ ls folder1
tryhackme@linux1:~$ cd folder4
tryhackme@linux1:~/folder4$ cat note.txt
Hello World!
tryhackme@linux1:~/folder4$ cd..
cd..: command not found
tryhackme@linux1:~/folder4$ cd ..
tryhackme@linux1:~$ cd folder4
tryhackme@linux1:~/folder4$ pwd
/home/tryhackme/folder4
tryhackme@linux1:~/folder4$ ^C
tryhackme@linux1:~/folder4$ cd ..
tryhackme@linux1:~$ grep "THM*" access.log
13.127.130.212 - - [04/May/2021:08:35:26 +0000] "GET THM{ACCESS} lang=en HTTP/1.1" 404 360 "-"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0
.3865.120 Safari/537.36"
tryhackme@linux1:~$
```

TASK 2

Task 7:- An Introduction to Shell Operators

This operator is also an output redirector like in the previous operator we discussed. However, what makes this operator different is that rather than overwriting any contents within a file, for example, it instead just puts the output at the end.

Following on with our previous example where we have the file "welcome" that has the contents of "hey". If we were to use echo to add "hello" to the file using the `>>` operator, the file will now only have "hello" and not "hey".

The `>>` operator allows to append the output to the bottom of the file — rather than replacing the contents like so:

Using the >> Operator

```
tryhackme@linux1:~$ echo hello >> welcome
```

Using cat to output the "welcome" file

```
tryhackme@linux1:~$ cat welcome
hey
hello
```

Answer the questions below

If we wanted to run a command in the background, what operator would we want to use?

Correct Answer

If I wanted to replace the contents of a file named "passwords" with the word "password123", what would my command be?

Correct Answer Hint

Now if I wanted to add "tryhackme" to this file named "passwords" but also keep "passwords123", what would my command be

Correct Answer Hint

Now use the deployed Linux machine to put these into practice

Correct Answer

```
Memory usage: 39%      IPv4 address for ens5: 10.10.38.164
Swap usage: 0%

0 updates can be applied immediately.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

tryhackme@linux1:~$ echo "Hello Tushar Gitte Welcome to Linux!"
Hello Tushar Gitte Welcome to Linux!
tryhackme@linux1:~$ whoami
tryhackme
tryhackme@linux1:~$ ls
access.log  folder1  folder2  folder3  folder4
tryhackme@linux1:~$ cd folder1
tryhackme@linux1:~/folder1$ ls
tryhackme@linux1:~/folder1$ cd ..
tryhackme@linux1:~$ ls folder4
note.txt
tryhackme@linux1:~$ ls folder3
tryhackme@linux1:~$ ls folder2
tryhackme@linux1:~$ ls folder1
tryhackme@linux1:~$ cd folder4
tryhackme@linux1:~/folder4$ cat note.txt
Hello World!
tryhackme@linux1:~/folder4$ cd..
cd.: command not found
tryhackme@linux1:~/folder4$ cd ..
tryhackme@linux1:~$ cd folder4
tryhackme@linux1:~/folder4$ pwd
/home/tryhackme/folder4
tryhackme@linux1:~/folder4$ ^C
tryhackme@linux1:~/folder4$ cd ..
tryhackme@linux1:~$ grep "THM*" access.log
13.127.130.212 - - [04/May/2021:08:35:26 +0000] "GET THM{ACCESS} lang=en HTTP/1.1" 404 360 "-"
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 Safari/537.36"
tryhackme@linux1:~$ echo hey > welcome
tryhackme@linux1:~$ ls
access.log  folder1  folder2  folder3  folder4  welcome
tryhackme@linux1:~$ cat welcome
hey
tryhackme@linux1:~$ echo Hello All >> welcome
tryhackme@linux1:~$ cat welcome
hey
Hello All
tryhackme@linux1:~$
```

Task 8:- Conclusions & Summaries

Task 8 Conclusions & Summaries

Nice work on getting to this stage! We covered quite a bit for your first interactions with Linux. However, these are the most essential/functions you're going to be using whenever you interact with a Linux machine.

I hope this room hasn't been too daunting for you to power-on through with. It's as I previously mentioned, you're going to become familiar with these things very quickly because of how often you're going to be using them.

To quickly recap, we've covered the following:

- Understanding why Linux is so commonplace today
- Interacting with your first-ever Linux machine!
- Ran some of the most fundamental commands
- Had an introduction to navigating around the filesystem & how we can use commands like find and grep to make finding data even more efficient!
- Power up your commands by learning about some of the important shell operators.

Take some time to have a play around in this room. When you feel a little bit more comfortable, progress onto [Linux Fundamentals Part 2](#)

Answer the questions below

I'll have a play around!

Correct Answer

TASK 2


Task 9:- Linux Fundamentals Part 2

Task 9  Linux Fundamentals Part 2 

Visit part two of the Linux fundamentals series here! <https://tryhackme.com/room/linuxfundamentalspart2>

Answer the questions below

Terminate the machine deployed in this room from task 3.

No answer needed 

Correct Answer

Join [Linux Fundamentals Part 2!](#)

No answer needed

Correct Answer

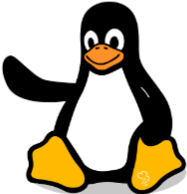
TASK 2

Linux Fundamentals Part 2:- Continue your learning Linux journey with part two. You will be learning how to log in to a Linux machine using SSH, how to advance your commands, file system interaction.

Task 1:- Introduction

Task 1

Introduction



Welcome to the second part of the reworked "Linux Fundamentals" series. We'll be applying our knowledge from the first installment in this series, so I highly recommend you [completing that room](#) **before** proceeding further.

In part 2, we'll be ditching the in-browser functionality and help you get started in what is a fundamental skill in being able to login to and control the terminals of remote machines. Not only this, but the room will also have you:

- Unlocking the potential of your first few commands by introducing you to using flags and arguments
- Advancing your knowledge of the filesystem to perform some more useful commands such as copying and moving files
- Introducing you to the access mechanisms in place to keep files and folders secure and how to identify the things that our current user has access too
- Running your first few scripts and executables!

Answer the questions below

Let's proceed!

No answer needed

Correct Answer

Task 2:- Accessing Your Linux Machine Using SSH (Deploy)

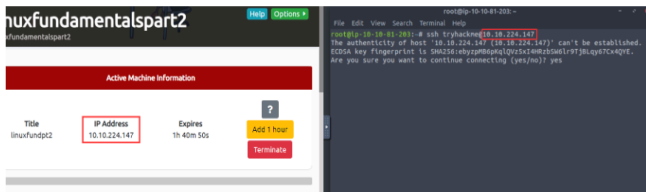
1. The IP address of the remote machine

2. Correct credentials to a valid account to login with on the remote machine

For this room, we will be logging in as "tryhackme", whose password is "tryhackme" without the quotation (") marks. Let's use the IP address of the machine displayed in the card at the top of the room as the IP address and this user, to construct a command to log in to the remote machine using SSH. The command to do so is `ssh` and then the username of the account, `g` the IP address of the machine.

But first, we need to open a terminal on the TryHackMe AttackBox. There is an icon placed on the desktop named "Terminal". And now, we can proceed to input commands.

For example: `ssh tryhackme@10.10.128.215`. Replacing the IP address with the IP address for your Linux target machine. Once executed, we will then be asked to trust the host and then provide a password for the "tryhackme" account, which is also "tryhackme".



Now that we are connected, any commands that we execute will now execute on the remote machine – not our own.

Note: When you type a password into an ssh login prompt there is no visible feedback – you will not be able to see any text or symbols appear as you type the password. It is still working, however, so just type the password and press enter to login.

Answer the questions below

I've logged into the Linux Fundamentals Part 2 machine using SSH!

No answer needed

Correct Answer

The screenshot shows a Kali Linux desktop environment. The desktop background is black with several icons: a home folder, a terminal, a folder named 'Tools', and a folder named 'Additional Tools'. The terminal window is open, showing a netcat listener on port 2441. The terminal output is as follows:

```
tryhackme@linux2: ~
File Edit View Search Terminal Help
root@ip-10-10-214-241:~# ssh tryhackme@10.10.128.215
The authenticity of host '10.10.128.215 (10.10.128.215)' can't be established.
ECDSA key fingerprint is SHA256:Q/7X8itkZJGq7nydeGSnqBrknpDImme4rY8uMXASVMA.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.128.215' (ECDSA) to the list of known hosts.
tryhackme@10.10.128.215's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-1047-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sat Jan 20 15:44:34 UTC 2024

System load:  0.59               Processes:    110
Usage of /:   26.8% of 7.69GB    Users logged in: 0
Memory usage: 46%              IPV4 address for eth0: 10.10.128.215
Swap usage:   0%

The list of available updates is more than a week old.
```

TASK 2

Task 3:- Introduction to Flags and Switches

```
List information about the FILES (the current directory by default). Sort entries
alphabetically if none of
-cftuvSUX nor --sort is specified.

Mandatory arguments to long options are mandatory for short options too.

-a, --all
    do not ignore entries starting with .

-A, --almost-all
    do not list implied . and ..

--author
    with -l, print the author of each file

-b, --escape
    print C-style escapes for nongraphic characters

--block-size=SIZE
    with -l, scale sizes by SIZE when printing them; e.g., '--block-size=M'; see
    SIZE format below

Manual page ls(1) line 1 (press h for help or q to quit)
```

Answer the questions below

Explore the manual page of the ls command

No answer needed

Correct Answer

What directional arrow key would we use to navigate down the manual page?

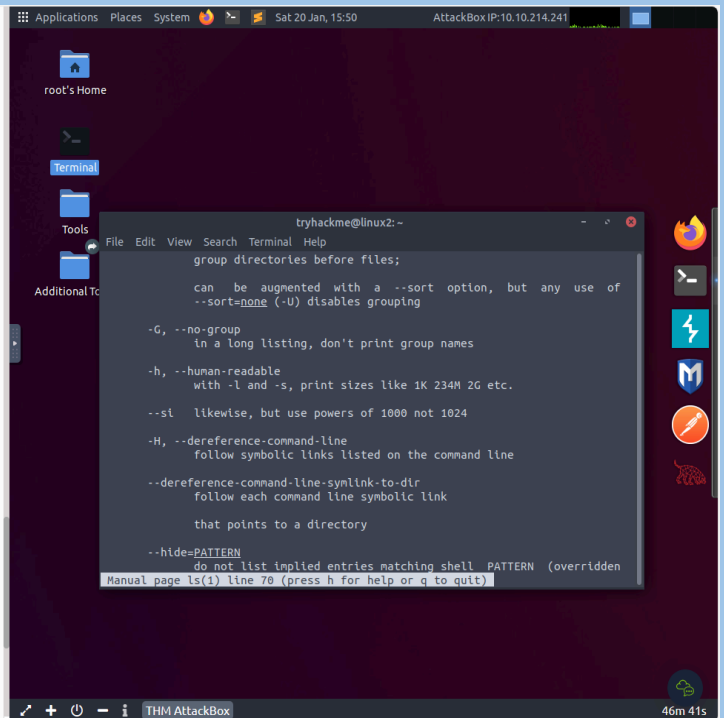
down

Correct Answer

What flag would we use to display the output in a "human-readable" way?

-h

Correct Answer



Task 4:- Filesystem Interaction Continued

Determining File Type

What is often misleading and often catches people out is making presumptions from files as to what their purpose or contents may be. Files usually have what's known as an extension to make this easier. For example, text files usually have an extension of ".txt". But this is not necessary.

So far, the files we have used in our examples haven't had an extension. Without knowing the context of why the file is there – we don't really know its purpose. Enter the `file` command. This command takes one argument. For example, we'll use `file` to confirm whether or not the "note" file in our examples is indeed a text file, like so `file note`.

```
Using file to determine the contents of a file

tryhackme@linux2:~$ file note
note: ASCII text
```

Answer the questions below

How would you create the file named "newnote"?

touch newnote

Correct Answer

Hint

On the deployable machine, what is the file type of "unknown1" in "tryhackme's" home directory?

ASCII text

Correct Answer

How would we move the file "myfile" to the directory "myfolder"?

mv myfile myfolder

Correct Answer

What are the contents of this file?

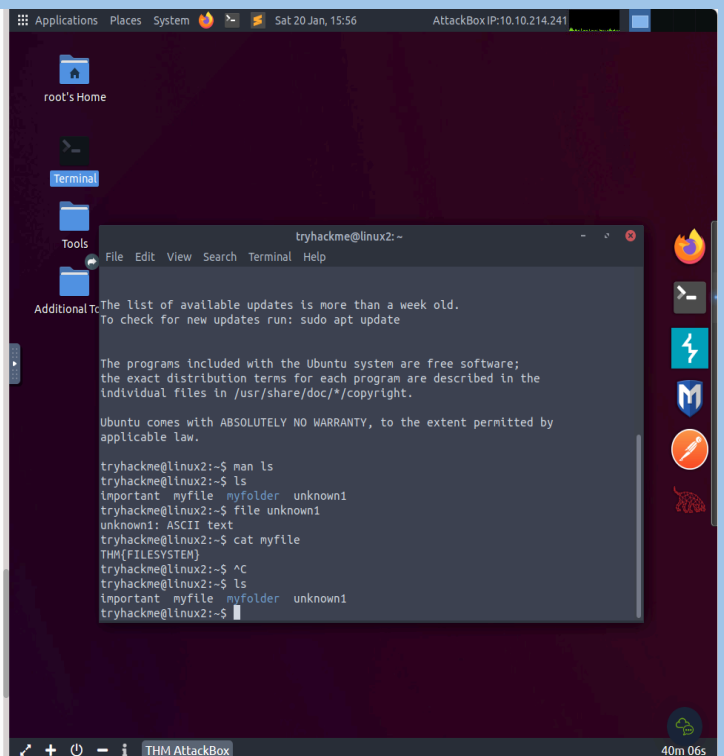
THM{FILESYSTEM}

Correct Answer

Continue to apply your knowledge and practice the commands from this task.

No answer needed

Correct Answer



TASK 2

Task 5:- Permissions 101

Simply, by providing the `-i` switch to `su`, we start a shell that is much more similar to the actual user logging into the system - we inherit a lot more properties of the new user, i.e., environment variables and the likes.

```
Using su to switch to user2 interactively

tryhackme@linux2:~$ su user2
Password:
user2@linux2: /home/tryhackme$
```

For example, when using `su` to switch to "user2", our new session drops us into our previous user's home directory.

```
Using su to switch to user2 interactively

tryhackme@linux2:~$ su -i user2
Password:
user2@linux2:~$ pwd
user2: /home/user2$
```

Where now, after using `-i`, our new session has dropped us into the home directory of "user" automatically.

Answer the questions below

On the deployable machine, who is the owner of "important"?

user2 Correct Answer

What would the command be to switch to the user "user2"?

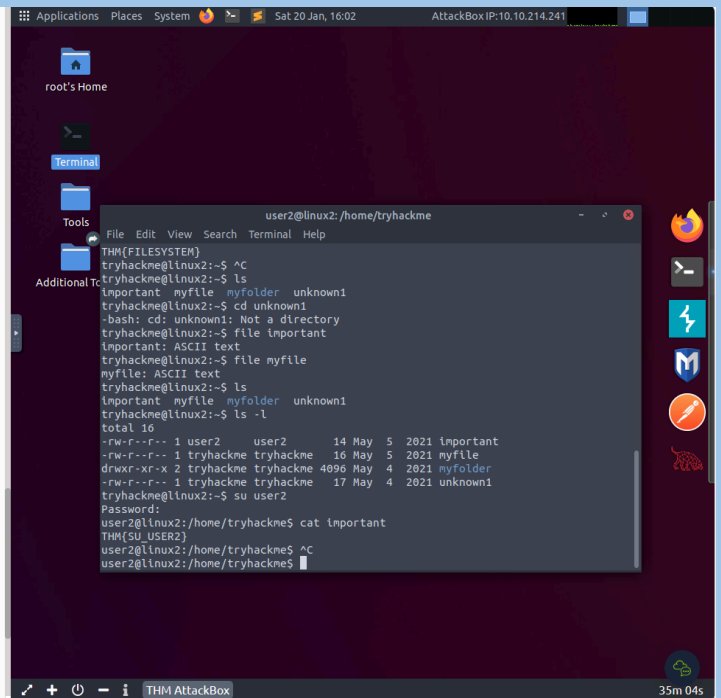
su user2 Correct Answer

Now switch to this user "user2" using the password "user2"

No answer needed Correct Answer

Output the contents of "important", what is the flag?

THM{SU_USER2} Correct Answer



Task 6:- Common Directories

```
myfile myfolder passwords.xlsx
```

/tmp

This is a unique root directory found on a Linux install. Short for "temporary", the /tmp directory is volatile and is used to store data that is only needed to be accessed once or twice. Similar to the memory on your computer, once the computer is restarted, the contents of this folder are cleared out.

What's useful for us in pentesting is that any user can write to this folder by default. Meaning once we have access to a machine, it serves as a good place to store things like our enumeration scripts.

```
Some notable contents of the /tmp directory

root@linux2: /tmp# ls
todelete trash.txt rubbish.bin
```

Answer the questions below

Read me!

No answer needed Correct Answer

What is the directory path that would we expect logs to be stored in?

/var/log Correct Answer

What root directory is similar to how RAM on a computer works?

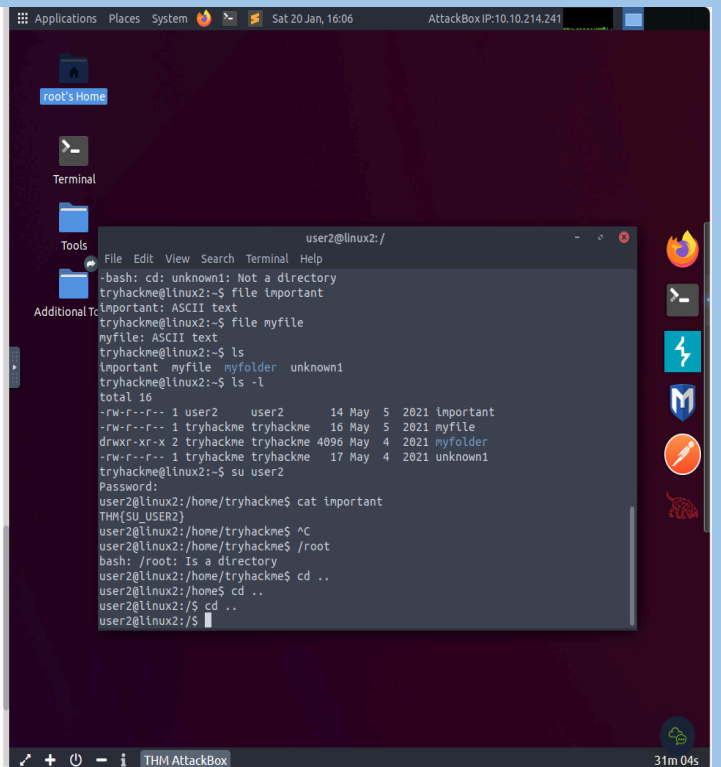
/tmp Correct Answer Hint

Name the home directory of the root user

/root Correct Answer

Now apply your learning and navigate through these directories on the deployed Linux machine.

No answer needed Correct Answer



TASK 2

Task 7:- Conclusions and Summaries

Task 7 Conclusions and Summaries

Nice work! This room was quite theory-heavy and covered quite a range of the fundamentals in getting you familiar with Linux. To quickly recap, this room taught you:

- How to connect to a Linux machine remotely using SSH
- Advancing your use of commands by providing flags, switches and where you can go to learn about these for each command (man pages)
- Some more commands that you'll frequently be using to interact with the filesystem and its contents
- A brief introduction to file permissions & switching users
- A summary paragraph of the important root directories on a Ubuntu Linux install and how we may be able to use the data stored within these.

I encourage you to go through this room again once or twice to gain some familiarity with the concepts. After all, practice makes perfect!

Answer the questions below

Proceed to the next task to continue your learning

No answer needed

Correct Answer

Task 8:- Linux Fundamentals Part 3

Task 8 Linux Fundamentals Part 3

Visit part three of the Linux fundamentals series here! <https://tryhackme.com/room/linuxfundamentalspart3>

Answer the questions below

Terminate the machine from task 2!

No answer needed

Correct Answer

Join [Linux Fundamentals Part 3!](#)

No answer needed


Correct Answer

TASK 2

Linux Fundamentals Part 3:- Power-up your Linux skills and get hands-on with some common utilities that you are likely to use day-to-day!

Task 1:- Introduction

Task 1 Introduction



Welcome to part three (and the finale) of the Linux Fundamentals module. So far, throughout the series, you have got hands-on with some fundamental concepts and used some important commands. This room is going to showcase some useful utilities and applications that you are likely to use day-to-day. You're also going to advance your Linux-fu skills by learning about automation, package management, and service/application logging.

Answer the questions below

Let's proceed!

No answer needed

Correct Answer

Task 2:- Deploy Your Linux Machine

Task 2 Deploy Your Linux Machine

Deploying Your Linux Machine


Press the green "Start Machine" button on the top-right of this task and then scroll to the top of the page to see the deployment information like so:

| Active Machine Information | | | |
|----------------------------|--------------|------------|------------|
| Title | IP Address | Expires | Add 1 hour |
| linuxfundpt3 | 10.10.139.84 | 1h 58m 58s | Terminate |

The IP address displayed is the address of your Linux machine that you will be logging into using SSH. Take note of this for now.

Deploying the TryHackMe AttackBox

Looking at the top of the page, press the "Start AttackBox" button to deploy the TryHackMe AttackBox that we will be interacting with. The TryHackMe AttackBox is a Ubuntu Linux machine that is hosted online in the cloud and can be interacted with via your browser. You will be using this to interact with the machine that you deploy in this task.

**Linux Fundamentals Part 3**
linuxfundamentalspart3

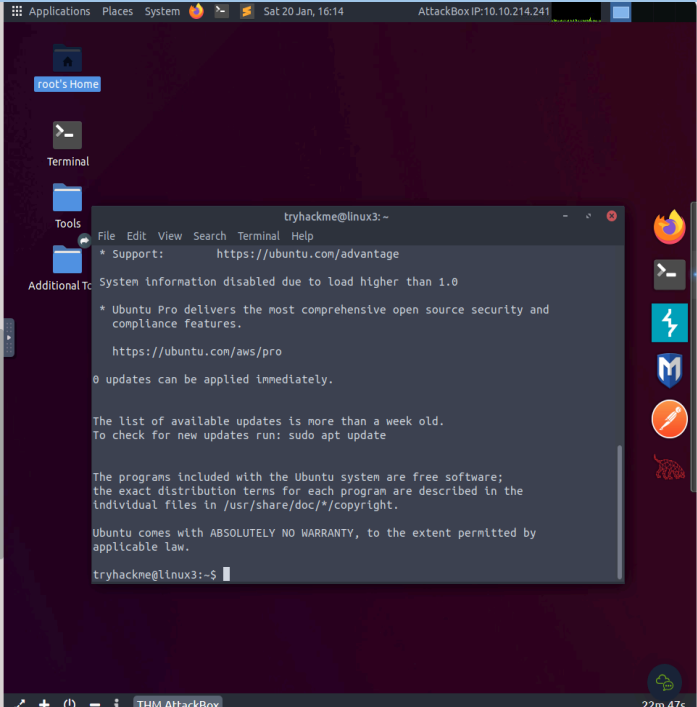
Use The Following Credentials:
IP Address: 10.10.61.141
Username: tryhackme
Password: tryhackme

Answer the questions below

I've logged into the Linux Fundamentals Part 3 machine using SSH and have deployed the AttackBox successfully!

No answer needed

Correct Answer



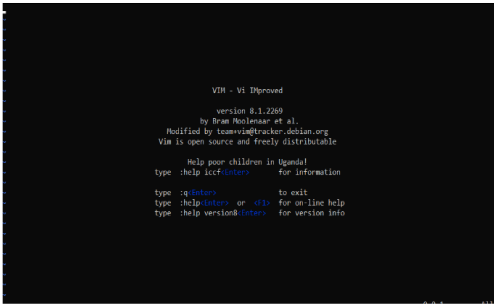
The screenshot shows a Linux desktop environment with a terminal window open. The terminal displays the following output:

```
tryhackme@linux3:~$  
* Support: https://ubuntu.com/advantage  
System Information disabled due to load higher than 1.0  
* Ubuntu Pro delivers the most comprehensive open source security and compliance features.  
https://ubuntu.com/aws/pro  
0 updates can be applied immediately.  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
tryhackme@linux3:~$
```

TASK 2

Task 3:- Terminal Text Editors

mention it for powering up your [Linux](#) skills.



Some of VIM's benefits, albeit taking a much longer time to become familiar with, includes:

- Customisable - you can modify the keyboard shortcuts to be of your choosing
- Syntax Highlighting - this is useful if you are writing or maintaining code, making it a popular choice for software developers
- VIM works on all terminals where nano may not be installed
- There are a lot of resources such as [cheatsheets](#), tutorials, and the sorts available to you use.

TryHackMe has a [room showcasing VIM](#) if you wish to learn more about this editor!

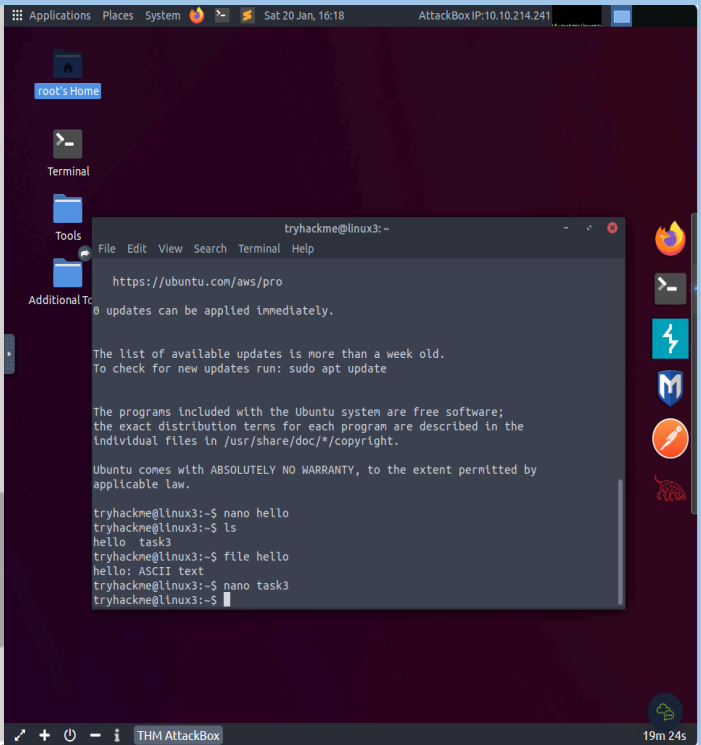
Answer the questions below

Create a file using Nano

No answer needed Correct Answer


Edit "task3" located in "tryhackme"'s home directory using Nano. What is the flag?

THM[TEXT_EDITORS] Correct Answer



tryhackme@linux3:~
https://ubuntu.com/aws/pro
updates can be applied immediately.
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
tryhackme@linux3:~\$ nano hello
tryhackme@linux3:~\$ ls
hello task3
tryhackme@linux3:~\$ file hello
hello: ASCII text
tryhackme@linux3:~\$ nano task3
tryhackme@linux3:~\$

Task 4:- General/Useful Utilities



One flaw with this module is that you have no way of indexing, so you must know the exact name and location of the file that you wish to use. This is why I prefer to use Updog. [What's Updog?](#) A more advanced yet lightweight webserver. But for now, let's stick to using Python's "HTTP Server".

Answer the questions below

Ensure you are connected to the deployed instance (10.10.61.141)

No answer needed Correct Answer

Now, use Python 3's "HTTPServer" module to start a web server in the home directory of the "tryhackme" user on the deployed instance.

No answer needed Correct Answer Hint

Download the file <http://10.10.61.141:8000/flag.txt> onto the TryHackMe AttackBox. Remember, you will need to do this in a new terminal.

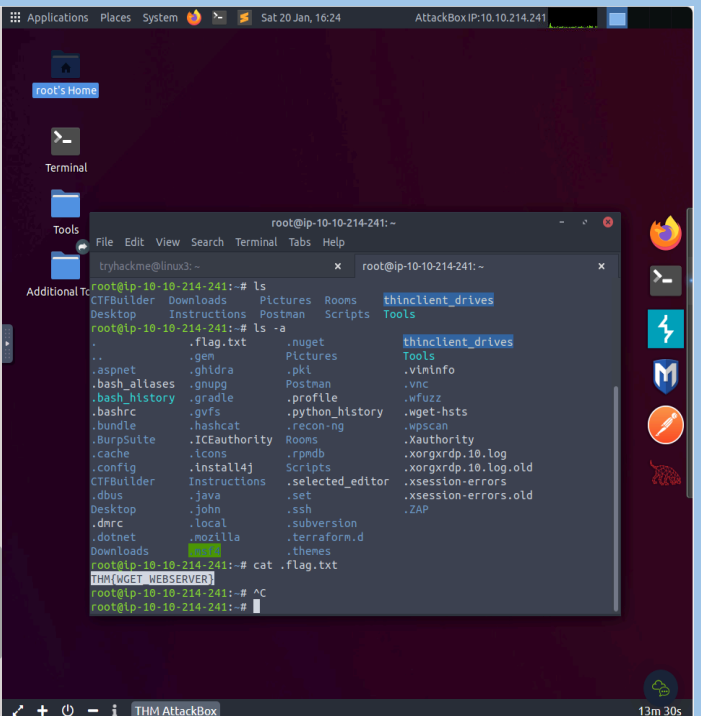
What are the contents?

THM[WGET_WEBSEVER] Correct Answer Hint

Create and download files to further apply your learning – see how you can read the documentation on Python3's "HTTPServer" module.

Use Ctrl + C to stop the Python3 HTTPServer module once you are finished.

No answer needed Correct Answer Hint



root@ip-10-10-214-241:~
tryhackme@linux3:~
root@ip-10-10-214-241:~
root@ip-10-10-214-241:~\$ ls
CTFBuilder Downloads Pictures Rooms thnclient_drives
Desktop Instructions Postman Scripts Tools
root@ip-10-10-214-241:~\$ ls -a
.
..
.aspnet .gen .nuget
.bash_aliases .ghidra .pki
.bash_history .gnupg Postman .viminfo
.bashrc .gradle .profile
.bundle .gvfs .python_history .wget-hsts
.ICEauthority .hashcat .recon-ng .wpscan
.BurpSuite .ICEDevelopment .rooms .Xauthority
.cache .icons .rpmdb .xorgxrdp-10.log
.config .install4j Scripts .xorgxrdp-10.log.old
CTFBuilder Instructions .selected_editor .xsession-errors
.dbus .java .set .xsession-errors.old
Desktop .john .ssh .ZAP
.dnrc .local .subversion
.dotnet .mozilla .terraform.d
Downloads .themes
root@ip-10-10-214-241:~\$ cat .flag.txt
THM[WGET_WEBSEVER]
root@ip-10-10-214-241:~\$ ^C
root@ip-10-10-214-241:~\$

TASK 2

Task 5:- Processes 101

```
This will keep on looping until I stop it!  
This will keep on looping until I stop it!  
This will keep on looping until I stop it!  
This will keep on looping until I stop it!  
This will keep on looping until I stop it!  
This will keep on looping until I stop it!  
This will keep on looping until I stop it!  
This will keep on looping until I stop it!
```

Answer the questions below

Read me!

No answer needed

Correct Answer

If we were to launch a process where the previous ID was "300", what would the ID of this new process be?

301

Correct Answer

If we wanted to **cleanly** kill a process, what signal would we send it?

SIGTERM

Correct Answer

Locate the process that is running on the deployed instance (10.10.61.141). What flag is given?

THM[PROCESSES]

Correct Answer

Hint

What command would we use to stop the service "myservice"?

systemctl stop myservice

Correct Answer

Hint

What command would we use to start the same service on the boot-up of the system?

systemctl enable myservice

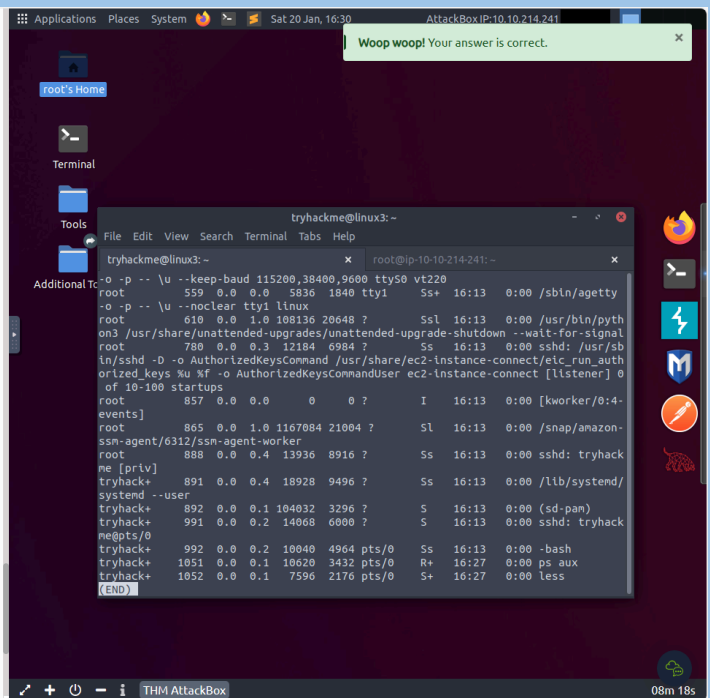
Correct Answer

Hint

What command would we use to bring a previously backgrounded process back to the foreground?

fg

Correct Answer



Task 6:- Maintaining Your System: Automation

Cron Job Generated (you may copy & paste it to your crontab):

```
0 */12 * * * cp -R /home/cmnaic/Documents /var/backups/ >/dev/null 2>&1
```

Your cron job will be run at: (5 times displayed)

- 2021-04-26 00:00:00 UTC
- 2021-04-26 12:00:00 UTC
- 2021-04-27 00:00:00 UTC
- 2021-04-27 12:00:00 UTC
- 2021-04-28 00:00:00 UTC

```
GNU nano 4.8 /tmp/crontab.0014v7/crontab
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# h m dom mon dow command
0 */12 * * * cp -R /home/cmnaic/Documents /var/backups/ >/dev/null 2>&1
```

Answer the questions below

Ensure you are connected to the deployed instance and look at the running crontabs.

No answer needed

Correct Answer

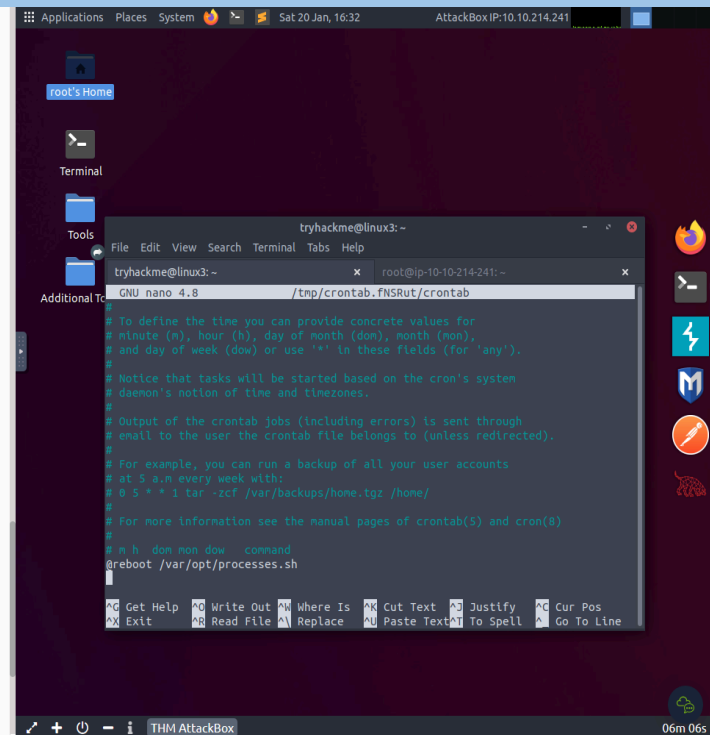
Hint

When will the crontab on the deployed instance (10.10.61.141) run?

@reboot

Correct Answer

Hint



TASK 2

Task 7:- Maintaining Your System: Package Management

So, to start, we need to add the GPG key for the developers of Sublime Text 3. (Note that TryHackMe instances do not have internet access and so we're not expecting you to add this to the machine that you deploy, as it would fail.)

1. Let's download the GPG key and use apt-key to trust it:

```
wget -qO - https://download.sublimetext.com/sublimehq-pub.gpg | sudo apt-key add -
```

2. Now that we have added this key to our trusted list, we can now add Sublime Text 3's repository to our apt sources list. A good practice is to have a separate file for every different community/3rd party repository that we add.

2.1. Let's create a file named `sublime-text.list` in `/etc/apt/sources.list.d` and enter the repository information like so:

```
root@linux3:/etc/apt/sources.list.d# touch sublime-text.list
root@linux3:/etc/apt/sources.list.d# ls
sublime-text.list
root@linux3:/etc/apt/sources.list.d#
```

2.2. And now use Nano or a text editor of your choice to add & save the Sublime Text 3 repository into this newly created file:

```
GNU nano 4.8
deb https://download.sublimetext.com/ apt/stable/
```

2.3. After we have added this entry, we need to update apt to recognise this new entry -- this is done using the `apt update` command

2.4. Once successfully updated, we can now proceed to install the software that we have trusted and added to apt using `apt install sublime-text`

Removing packages is as easy as reversing. This process is done by using the

`add-apt-repository --remove ppa:PPA_Name/ppa` command or by manually deleting the file that we previously added to.

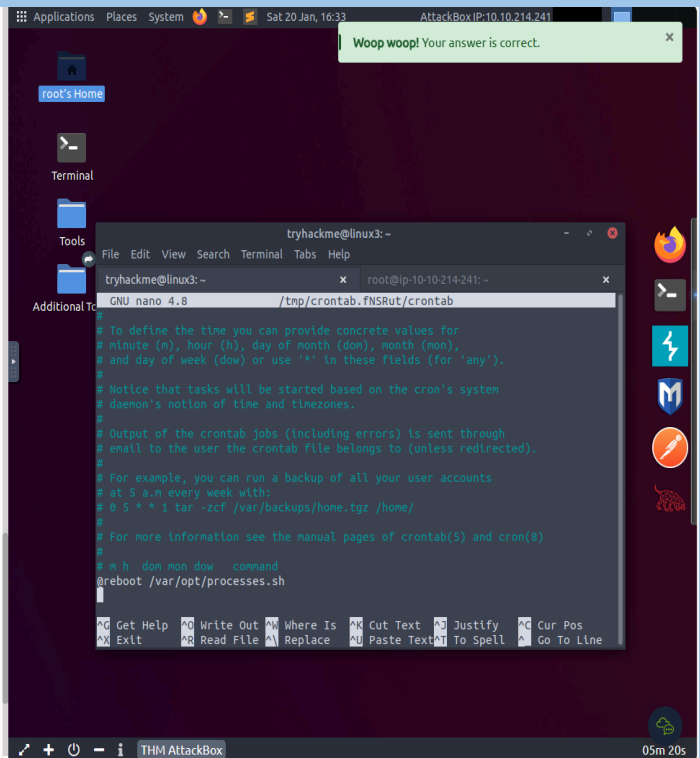
Once removed, we can just use `apt remove [software-name-here]` i.e. `apt remove sublime-text`

Answer the questions below

Since TryHackMe instances do not have an internet connection...this task only requires you to read through the material.

No answer needed

Correct Answer



Task 8:- Maintaining Your System: Logs

```
tmp.1      kern.log.2.gz  wtmp
cloud-init-output.log  kern.log.3.gz  wtmp.1
cloud-init.log         kern.log.4.gz
dist-upgrade          landscape
ubuntu@ip-172-31-23-158:/var/log$
```

These services and logs are a great way in monitoring the health of your system and protecting it. Not only that, but the logs for services such as a web server contain information about every single request - allowing developers or administrators to diagnose performance issues or investigate an intruder's activity. For example, the two types of log files below that are of interest:

- access log
- error log

```
ubuntu@ip-172-31-23-158:/var/log/apache2$ ls
access.log      access.log.3.gz  error.log.1      error.log.4.gz
access.log.1    access.log.4.gz  error.log.10.gz  error.log.5.gz
access.log.10.gz access.log.5.gz  error.log.11.gz  error.log.6.gz
access.log.11.gz access.log.6.gz  error.log.12.gz  error.log.7.gz
access.log.12.gz access.log.7.gz  error.log.13.gz  error.log.8.gz
access.log.13.gz access.log.8.gz  error.log.14.gz  error.log.9.gz
access.log.14.gz access.log.9.gz  error.log.2.gz   error.log.3.gz
access.log.2.gz error.log         error.log.3.gz   other_vhosts_access.log
ubuntu@ip-172-31-23-158:/var/log/apache2$
```

There are, of course, logs that store information about how the OS is running itself and actions that are performed by users, such as authentication attempts.

Answer the questions below

Look for the apache2 logs on the deployable Linux machine

No answer needed

Correct Answer

Hint

What is the IP address of the user who visited the site?

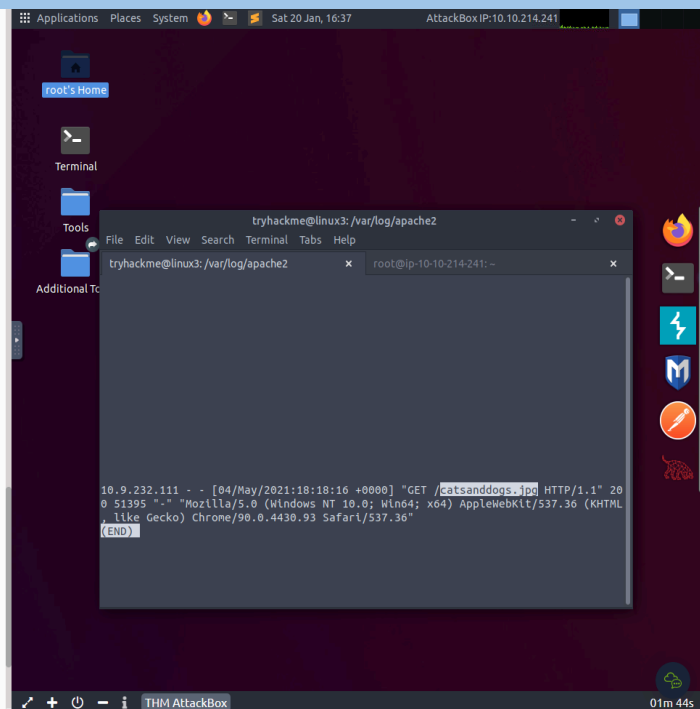
10.9.232.111

Correct Answer

What file did they access?

catsanddogs.jpg

Correct Answer



TASK 2

Task 9:- Conclusions & Summaries

Task 9 Conclusions & Summaries

Welcome to the end of the Linux Fundamentals module. Your familiarity with Linux will improve as you get to interact with it over time. Linux has the potential to do very powerful things with relative ease (as you have hopefully discovered throughout this module)

To recap, this room introduced you to the following topics:

- Using terminal text editors
- General utilities such as downloading and serving contents using a python webserver
- A look into processes
- Maintaining & automating your system by the use of crontabs, package management, and reviewing logs

Continue your learning in some other TryHackMe rooms that are dedicated to Linux tools or utilities:

- Bash Scripting - <https://tryhackme.com/room/bashscripting>
- Regular Expressions - <https://tryhackme.com/room/catregex>

Answer the questions below

Terminate the machine deployed in this room from task 2.

No answer needed

Correct Answer

Continue your learning in other Linux-dedicated rooms

No answer needed

Correct Answer