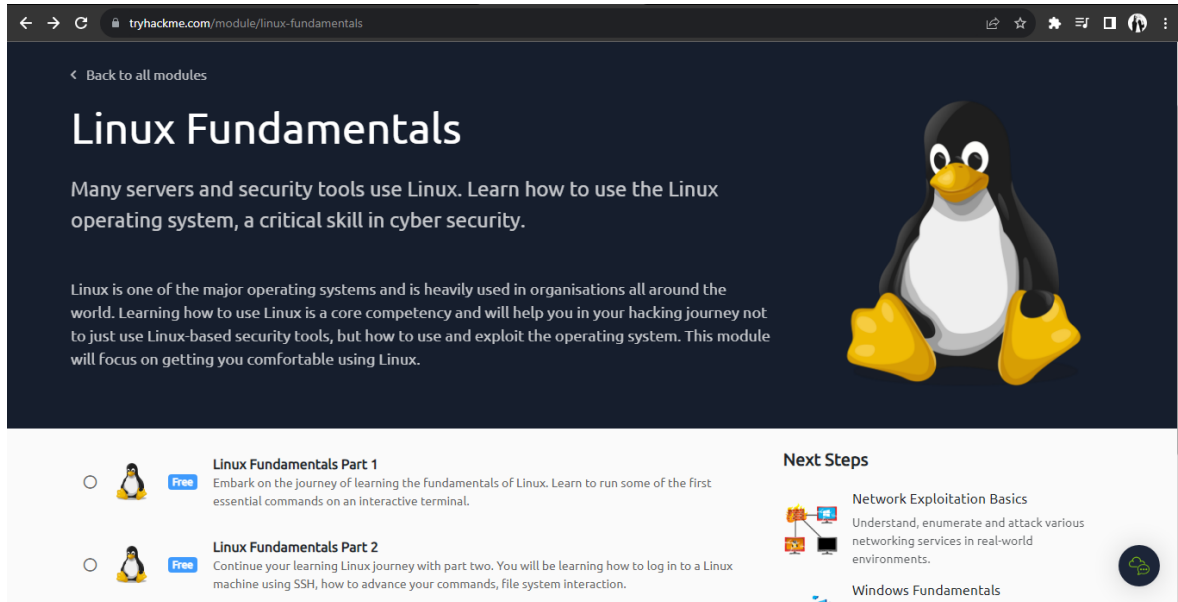


Linux Fundamentals

Part-1

1) LOGIN to try hack me.




The screenshot shows the 'Linux Fundamentals' module page on tryhackme.com. The page has a dark blue header with the title 'Linux Fundamentals' and a description: 'Many servers and security tools use Linux. Learn how to use the Linux operating system, a critical skill in cyber security.' Below this, there's a paragraph about Linux's importance. To the right is a large image of Tux the penguin. At the bottom, there are two sections: 'Linux Fundamentals Part 1' and 'Linux Fundamentals Part 2', both marked as 'Free'. To the right of these is a 'Next Steps' section with links to 'Network Exploitation Basics' and 'Windows Fundamentals'.


< Back to all modules

Linux Fundamentals


Many servers and security tools use Linux. Learn how to use the Linux operating system, a critical skill in cyber security.


Linux is one of the major operating systems and is heavily used in organisations all around the world. Learning how to use Linux is a core competency and will help you in your hacking journey not to just use Linux-based security tools, but how to use and exploit the operating system. This module will focus on getting you comfortable using Linux.

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

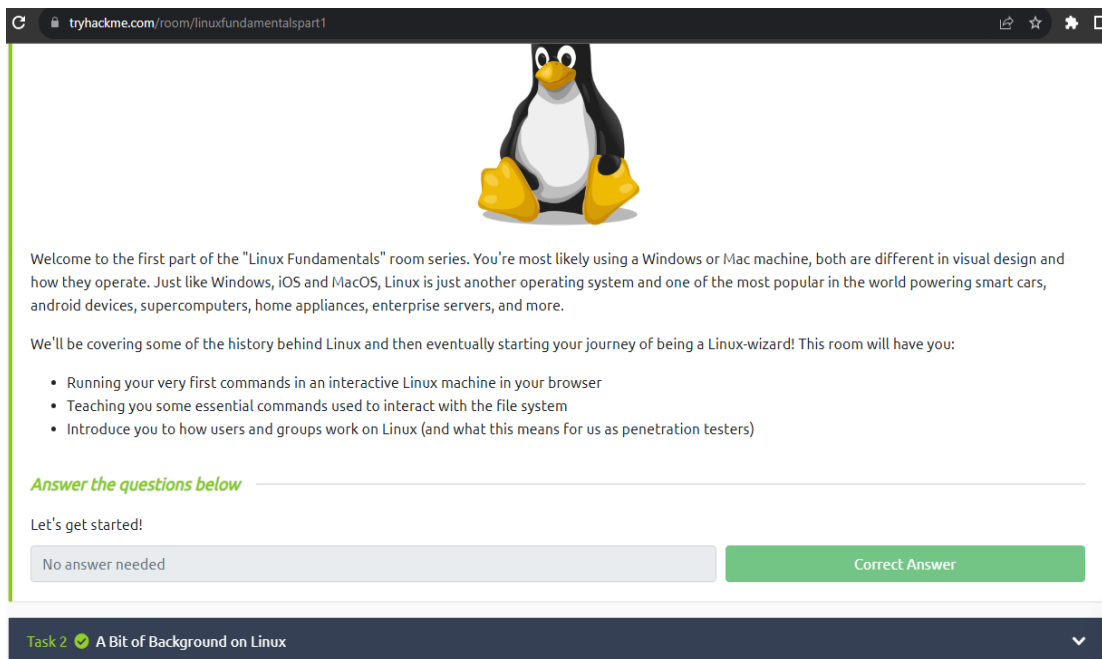
 **Linux Fundamentals Part 2** Free Continue your learning Linux journey with part two. You will be learning how to log in to a Linux machine using SSH, how to advance your commands, file system interaction.

Next Steps

 **Network Exploitation Basics**
Understand, enumerate and attack various networking services in real-world environments.

 **Windows Fundamentals**

1)



The screenshot shows the 'Linux Fundamentals Part 1' room page on tryhackme.com. It features a large image of Tux the penguin at the top. Below it, there's a welcome message and a list of topics to be covered. At the bottom, there's a 'Task 2' section titled 'A Bit of Background on Linux'.

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

2)

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

3)

tryhackme.com/room/linuxfundamentalspart1

Active Machine Information

Title	IP Address	Expires	
linuxfundpart1v1	10.10.202.237	54m 35s	<div>? Add 1 hour Terminate</div>

28%

4)

tryhackme.com/room/linuxfundamentalspart1

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

Using echo

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

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

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

Try this on your Linux machine now!

Answer the questions below

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

Answer format: *****

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

Answer format: *****

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 Tue Aug  1 11:06:05 UTC 2023

System load:  0.03          Processes:           107
Usage of /:   18.7% of 9.63GB Users logged in:        0
Memory usage: 38%          IPv4 address for ens5: 10.10.202
.237
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:~$
```

linuxfundpar... 57m 45s

tryhackme.com/room/linuxfundamentalspart1

Using echo

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

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

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

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 TryHackMe Correct Answer Hint

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

tryhackme Correct Answer Hint

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 Tue Aug  1 11:06:05 UTC 2023

System load:  0.03          Processes:           107
Usage of /:   18.7% of 9.63GB Users logged in:        0
Memory usage: 38%          IPv4 address for ens5: 10.10.202
.237
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 TryHackMe
TryHackMe
tryhackme@linux1:~$ ^C
tryhackme@linux1:~$ whoiam
whoiam: command not found
tryhackme@linux1:~$ whoami
tryhackme
tryhackme@linux1:~$

```

5)

tryhackme.com/room/linuxfundamentalspart1

"/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?

4 Correct Answer

Which directory contains a file?

folder4 Correct Answer Hint

What is the contents of this file?

Hello World! Correct Answer

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

/home/tryhackme/folder4 Correct Answer

Task 6 Searching for Files

```

tryhackme@linux1:~$ ls
access.log  folder1  folder2  folder3  folder4
tryhackme@linux1:~$ cd folder3
tryhackme@linux1:~/folder3$ cd..
cd..: command not found
tryhackme@linux1:~/folder3$ cd ..
tryhackme@linux1:~$ cd folder4
tryhackme@linux1:~/folder4$ ls
note.txt
tryhackme@linux1:~/folder4$ cat note.txt
Hello World!
tryhackme@linux1:~/folder4$

```

6)

tryhackme.com/room/linuxfundamentalspart1

```

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?

THM{ACCESS} Submit Hint

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

No answer needed Correct Answer

Task 7 An Introduction to Shell Operators

```

tryhackme@linux1:~$ grep THM access.log
13.127.130.212 - - [04/May/2021:08:35:26 +0000] "GET THM{ACCESS} l
ang=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:~$

```

7)

The screenshot shows a web browser window with the URL `tryhackme.com/room/linuxfundamentalspart1`. The page contains three questions with input fields and 'Correct Answer' buttons. The first question asks for a background command operator, with the answer being `&`. The second question asks for a command to replace file contents, with the answer being `echo password123 > passwords`. The third question asks for a command to append text, with the answer being `echo tryhackme >> passwords`. Below the questions is a terminal window showing a series of commands and their outputs, including `grep`, `touch`, `echo`, and `cat` commands. The terminal output shows the results of these commands, such as the contents of `access.log` and the creation of the `passwords` file.

8-9)

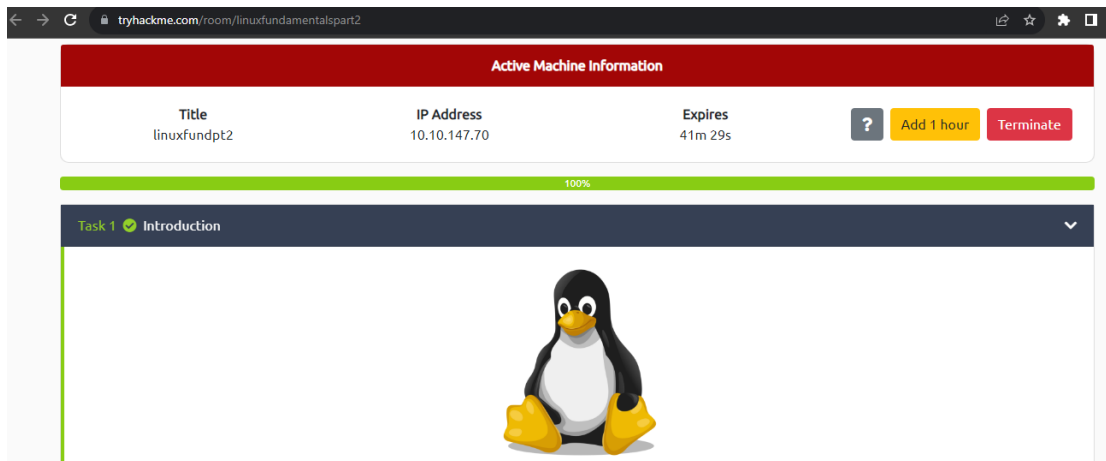
The screenshot shows a web browser window with the URL `tryhackme.com/room/linuxfundamentalspart2`. The page displays 'Task 8' and 'Task 9' summaries. Task 8 is 'Conclusions & Summaries' and Task 9 is 'Linux Fundamentals Part 2'. Below the task summaries, there is a link to 'Visit part two of the Linux fundamentals series here!' with the URL `https://tryhackme.com/room/linuxfundamentalspart2`. The page also includes a section titled 'Answer the questions below' with two questions. The first question asks to 'Terminate the machine deployed in this room from task 3.' with the answer 'No answer needed'. The second question asks to 'Join Linux Fundamentals Part 2!' with the answer 'No answer needed'.

Completed

The screenshot shows a web browser window with the URL `tryhackme.com/room/linuxfundamentalspart1`. A large green notification box with a checkmark icon and the text 'Congratulations' is centered on the screen. The notification says 'You've completed the room! Share this with your friends:' and includes buttons for 'Share Awarded Badge', 'Twitter', 'Facebook', and 'LinkedIn'. Below these buttons is a 'Leave Feedback' link. The background shows a terminal window with a 'Welcome to Ubuntu' message and system information, and a sidebar with a list of tasks.

PART-2

1)




tryhackme.com/room/linuxfundamentalspart2

Active Machine Information

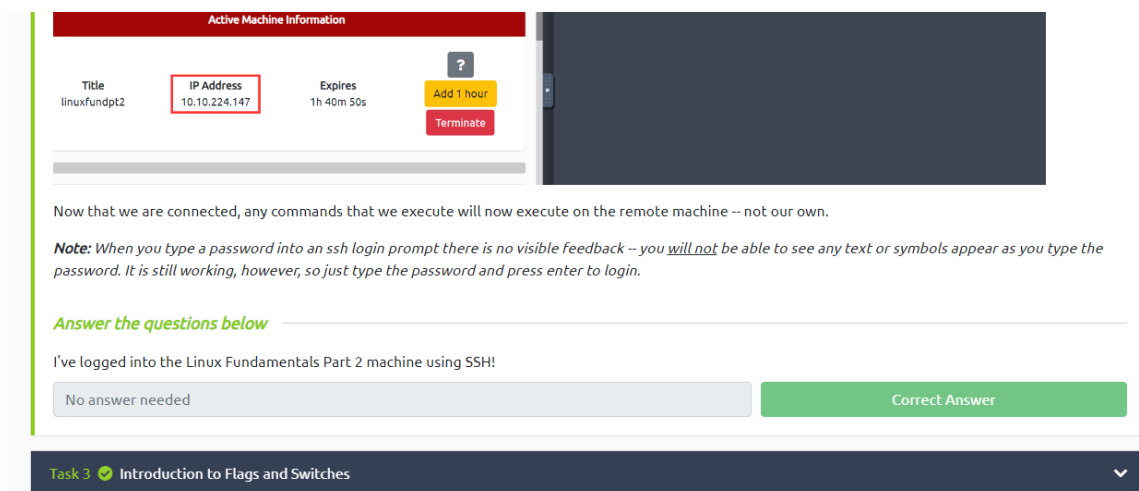
Title	IP Address	Expires	
linuxfundpt2	10.10.147.70	41m 29s	? Add 1 hour Terminate

100%

Task 1 Introduction



2)



Active Machine Information

Title	IP Address	Expires	
linuxfundpt2	10.10.224.147	1h 40m 50s	? Add 1 hour Terminate

100%

Task 3 Introduction to Flags and Switches

3)

Answer the questions below

How would you create the file named "newnote"?

Correct Answer

Hint

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

Correct Answer

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

Correct Answer

What are the contents of this file?

Correct Answer

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

Correct Answer

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

6)

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 7  Conclusions and Summaries

7)

Answer the questions below

Proceed to the next task to continue your learning

No answer needed

Correct Answer

Task 8  Linux Fundamentals Part 3

8)

Task 8  Linux Fundamentals Part 3Visit 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

PART-3

1)

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

2)

Use The Following Credentials:

IP Address: MACHINE_IP
 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

Task 3 ✓ Terminal Text Editors ▼

3)

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

Task 4 ✓ General/Useful Utilities ▼

```

^C
Keyboard interrupt received, exiting.
root@ip-10-10-42-136:~# ls -la
.                .gem              .nuget            .themes
..               .ghidra           Pictures          thinclient_drives
.bash_history    .gnupg            .pki              Tools
.bash_aliases    .gradle           Postman           .viminfo
.bashrc          .gvfs             .profile          .vnc
.burpsuite       .hashcat          .python_history   .wfsuzz
.bundle          .ICEauthority     .recon-ng         .wget-hsts
.cache           .icons            Rooms             .wpscan
.config          .install4j        .rpmbd            .Xauthority
.dbus            Instructions      Scripts           .xorgxrdp.10.log
.desktop        .java             .selected_editor  .xorgxrdp.10.log.old
.dmrc           .john             .set              .xsession-errors
.dnsmasq        .local            .ssh              .xsession-errors.old
.dotnet         .mozilla          .subversion       .ZAP
Downloads       .msf4             .terraform.d
root@ip-10-10-42-136:~#
  
```

4)

Answer the questions below

Ensure you are connected to the deployed instance (MACHINE_IP)

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://MACHINE_IP:8000/flag.txt onto the TryHackMe AttackBox

What are the contents?

THM{WGSET_WEBSERVER} 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

```

Application: Thu 3 Aug, 09:46 AttackBox IP: 10.10.42.136
root@ip-10-10-42-136:~# nano text3
root@ip-10-10-42-136:~# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
^C
Keyboard interrupt received, exiting.
root@ip-10-10-42-136:~# ls -la
.                .gem              .nuget            .themes
..               .ghidra           Pictures          thinclient_drives
.bash_history    .gnupg            .pki              Tools
.bash_aliases    .gradle           Postman           .viminfo
.bashrc          .gvfs             .profile          .vnc
.burpsuite       .hashcat          .python_history   .wfsuzz
.bundle          .ICEauthority     .recon-ng         .wget-hsts
.cache           .icons            Rooms             .wpscan
.config          .install4j        .rpmbd            .Xauthority
.dbus            Instructions      Scripts           .xorgxrdp.10.log
.desktop        .java             .selected_editor  .xorgxrdp.10.log.old
.dmrc           .john             .set              .xsession-errors
.dnsmasq        .local            .ssh              .xsession-errors.old
.dotnet         .mozilla          .subversion       .ZAP
Downloads       .msf4             .terraform.d
root@ip-10-10-42-136:~#
  
```


5)

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

```

Application  Thu 3 Aug, 09:59 AttackBox IP:10.10.42.136
root@ip-10-10-42-136: ~
File Edit View Search Terminal Help
top - 09:57:26 up 19 min, 0 users, load average: 0.08, 0.11, 0.16
Tasks: 184 total, 1 running, 139 sleeping, 0 stopped, 0 zombie
%Cpu(s): 1.9 us, 0.7 sy, 0.0 ni, 96.1 id, 0.0 wa, 0.0 hi, 0.4 si, 0
KiB Mem : 3989968 total, 1109832 free, 594380 used, 2285756 buff/cach
KiB Swap: 1048572 total, 1048572 free, 0 used, 3079252 avail Mem
Change delay from 3.0 to 1

```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+
1051	root	20	0	234896	78284	27820	S	3.3	2.0	0:37.53
2628	root	20	0	189280	29020	7652	S	1.5	0.7	0:16.47
2050	root	20	0	485084	28376	20960	S	0.6	0.7	0:08.57
1438	root	20	0	50460	3952	2892	S	0.3	0.1	0:00.19
1715	root	20	0	517440	39020	29520	S	0.3	1.0	0:02.77
2047	root	20	0	484328	31408	23808	S	0.3	0.8	0:03.84
2712	root	20	0	651800	41616	31724	S	0.3	1.0	0:00.61
4656	root	20	0	0	0	0	I	0.3	0.0	0:00.01
5047	root	20	0	44128	4044	3436	R	0.3	0.1	0:00.03
1	root	20	0	159976	9248	6688	S	0.0	0.2	0:02.75

Locate the process that is running on the deployed instance (MACHINE_IP). 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

```

Application  Thu 3 Aug, 10:00 AttackBox IP:10.10.42.136
root@ip-10-10-42-136: ~
File Edit View Search Terminal Help
top - 09:57:26 up 19 min, 0 users, load average: 0.08, 0.11, 0.16
Tasks: 184 total, 1 running, 139 sleeping, 0 stopped, 0 zombie
%Cpu(s): 1.9 us, 0.7 sy, 0.0 ni, 96.1 id, 0.0 wa, 0.0 hi, 0.4 si, 0
KiB Mem : 3989968 total, 1109832 free, 594380 used, 2285756 buff/cach
KiB Swap: 1048572 total, 1048572 free, 0 used, 3079252 avail Mem
Change delay from 3.0 to 1

```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+
1051	root	20	0	234896	78284	27820	S	3.3	2.0	0:37.53
2628	root	20	0	189280	29020	7652	S	1.5	0.7	0:16.47
2050	root	20	0	485084	28376	20960	S	0.6	0.7	0:08.57
1438	root	20	0	50460	3952	2892	S	0.3	0.1	0:00.19
1715	root	20	0	517440	39020	29520	S	0.3	1.0	0:02.77
2047	root	20	0	484328	31408	23808	S	0.3	0.8	0:03.84
2712	root	20	0	651800	41616	31724	S	0.3	1.0	0:00.61
4656	root	20	0	0	0	0	I	0.3	0.0	0:00.01
5047	root	20	0	44128	4044	3436	R	0.3	0.1	0:00.03
1	root	20	0	159976	9248	6688	S	0.0	0.2	0:02.75
2	root	20	0	0	0	0	S	0.0	0.0	0:00.00
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00
7	root	20	0	0	0	0	S	0.0	0.0	0:00.12
8	root	20	0	0	0	0	I	0.0	0.0	0:00.75
9	root	20	0	0	0	0	I	0.0	0.0	0:00.00
10	root	rt	0	0	0	0	S	0.0	0.0	0:00.00
11	root	rt	0	0	0	0	S	0.0	0.0	0:00.00
12	root	20	0	0	0	0	S	0.0	0.0	0:00.00
13	root	20	0	0	0	0	S	0.0	0.0	0:00.00
14	root	rt	0	0	0	0	S	0.0	0.0	0:00.00

6)

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 (MACHINE_IP) run?

@reboot

Correct Answer

Hint

```

Application  Thu 3 Aug, 10:02 AttackBox IP:10.10.42.136
root@ip-10-10-42-136: ~
File Edit View Search Terminal Help
@reboot vncserver :1 -depth 24 -geometry 1900x1200
@reboot python -m websocketify 80 localhost:5901 -D
@reboot vncconfig -nowin&
@reboot /bin/bash /root/Scripts/displayip.sh

```

7)

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

8)

Answer the questions below

Look for the apache2 logs on the deployable Linux machine

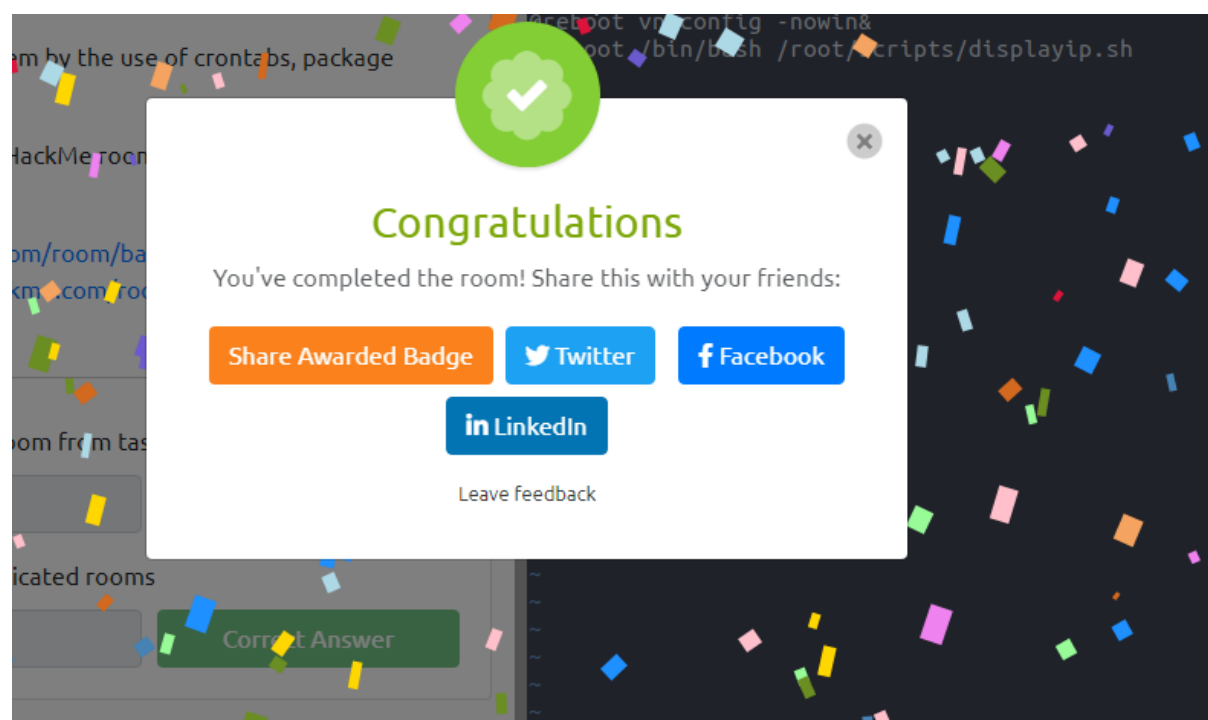
What is the IP address of the user who visited the site?


What file did they access?

Task 9 ☐ Conclusions & Summaries

9)

Continue your learning in other Linux-dedicated rooms





Congratulations

You've completed the room! Share this with your friends:

[Leave feedback](#)