

Linux Fundamentals – Yasas Priyamantha

Part 01

Task 1. Introduction

- No exercises.

Task 2. A Bit of Background on Linux

- 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 3. Interacting With Your First Linux Machine

To access machines, you will need to connect to our network.

OpenVPN Access Details

VPN Server Name: IN-Regular-1

Internal Virtual IP Address: 0.0.0.0

Server status: Online

Connection: Not connected

Machines

VPN Server: IN-Regular-1

If you're switching for the first time, you will need to redownload your configuration file. For best performance, please use the server that's geographically closest to you.

Download configuration file

Regenerate

Connect to our network to hack machines

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 |

kali@kali: ~/Downloads

```
zsh: corrupt history file /home/kali/.zsh_history
[(kali㉿kali)-[~/Downloads]]
$ ls
DDoS-Ripper-main.zip Zuko.Yasas.ovpn

[(kali㉿kali)-[~/Downloads]]
$ sudo openvpn Zuko.Yasas.ovpn
[sudo] password for kali:
2024-04-10 01:13:53 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2024-04-10 01:13:53 --cipher is not set. Previous OpenVPN version defaulted to BF-CBC as fallback when cipher negotiation failed in this case. If you need this fallback please add '--data-ciphers-fallback BF-CBC' to your configuration and/or add BF-CBC to --data-ciphers.
2024-04-10 01:13:53 OpenVPN 2.5.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Jul 5 2022
2024-04-10 01:13:53 library versions: OpenSSL 3.0.7 1 Nov 2022, LZO 2.10
2024-04-10 01:13:53 Outgoing Control Channel Authentication: Using 512 bit message hash 'SHA512' for HMAC authentication
2024-04-10 01:13:53 Incoming Control Channel Authentication: Using 512 bit message hash 'SHA512' for HMAC authentication
2024-04-10 01:13:53 TCP/UDP: Preserving recently used remote address: [AF_INET]3.7.33.194:1194
2024-04-10 01:13:53 Socket Buffers: R=[212992->212992] S=[212992->212992]
2024-04-10 01:13:53 UDP link local: (not bound)
2024-04-10 01:13:53 UDP link remote: [AF_INET]3.7.33.194:1194
2024-04-10 01:13:53 TLS: Initial packet from [AF_INET]3.7.33.194:1194, sid=eadc99a5 f7d4e612
2024-04-10 01:13:53 VERIFY OK: depth=1, CN=ChangeMe
2024-04-10 01:13:53 VERIFY KU OK
2024-04-10 01:13:53 Validating certificate extended key usage
2024-04-10 01:13:53 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2024-04-10 01:13:53 VERIFY EKU OK
2024-04-10 01:13:53 VERIFY OK: depth=0, CN=server
2024-04-10 01:13:53 WARNING: 'link-mtu' is used inconsistently, local='link-mtu 1586', remote='link-mtu 1602'
2024-04-10 01:13:53 WARNING: 'keysize' is used inconsistently, local='keysize 128', remote='keysize 256'
2024-04-10 01:13:53 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bit RSA, signature: RSA-SHA256
2024-04-10 01:13:53 [server] Peer Connection Initiated with [AF_INET]3.7.33.194:1194
2024-04-10 01:13:54 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2024-04-10 01:13:54 PUSH: Received control message: 'PUSH_REPLY,route 10.10.0.0 255.255.0.0,route-metric 1000,route-gateway 10.17.0.1,topology subnet,ping 5,ping-restart 120,ifconfig 10.17.53.15 255.255.128.0,peer-id 97'
2024-04-10 01:13:54 OPTIONS IMPORT: timers and/or timeouts modified
2024-04-10 01:13:54 OPTIONS IMPORT: --ifconfig/up options modified
2024-04-10 01:13:54 OPTIONS IMPORT: route options modified
2024-04-10 01:13:54 OPTIONS IMPORT: route-related options modified
2024-04-10 01:13:54 OPTIONS IMPORT: peer-id set
2024-04-10 01:13:54 OPTIONS IMPORT: adjusting link_mtu to 1625
2024-04-10 01:13:54 Using peer cipher 'AES-256-CBC'
2024-04-10 01:13:54 Data Channel: using negotiated cipher 'AES-256-CBC'
```

Type here to search

10:44 AM

A screenshot of a Kali Linux terminal window titled "kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal shows the output of the "ifconfig" command, which displays detailed information about network interfaces (eth0, eth1, lo, tun0) including flags, MTU, broadcast address, and packet statistics. The terminal also shows a series of log messages from the kernel, indicating various network events such as "PUSH_REQUEST", "PUSH_REPLY", and cipher negotiations. The desktop environment at the bottom includes icons for file explorer, terminal, browser, and system settings.

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

(kali㉿kali)-[~]

```
$ ssh tryhackme@10.10.106.93
The authenticity of host '10.10.106.93 (10.10.106.93)' can't be established.
ED25519 key fingerprint is SHA256:Mc0Ig+t4iBblZAo8Mn/fbwh5Yf0WLEUzZaVxE14usA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.106.93' (ED25519) to the list of known hosts.
tryhackme@10.10.106.93's password:
Permission denied, please try again.
tryhackme@10.10.106.93's password:
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 Wed Apr 10 06:07:57 UTC 2024

System load:  0.16          Processes:      114
Usage of /:   18.7% of 9.63GB  Users logged in:   1
Memory usage: 41%           IPv4 address for ens5: 10.10.106.93
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

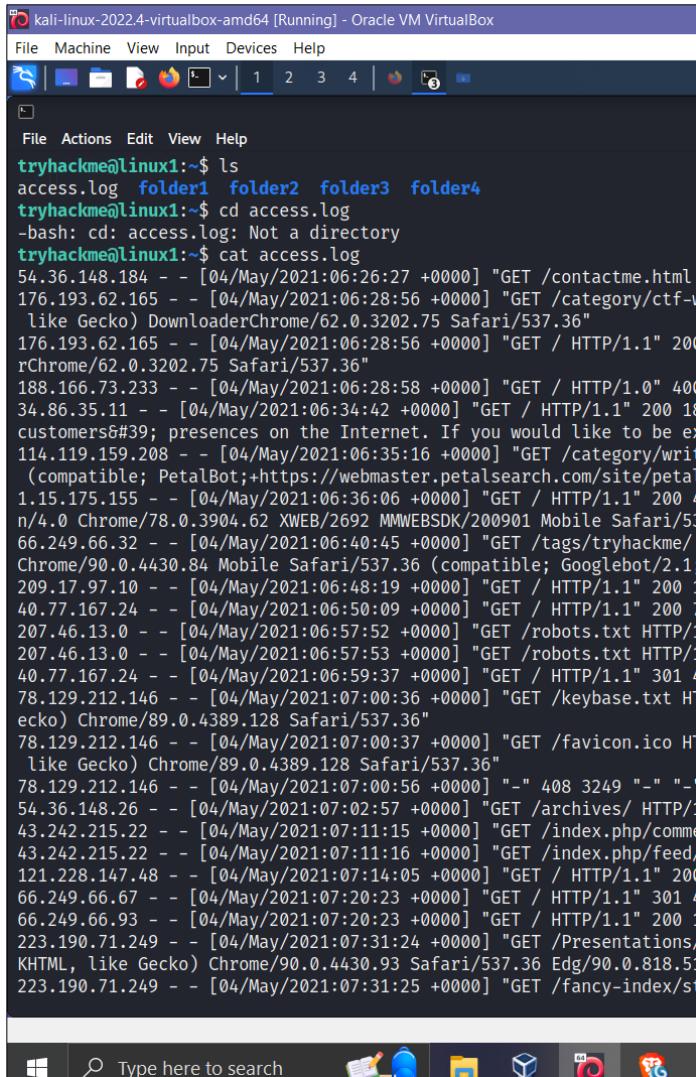
Last login: Wed Apr 10 06:07:03 2024 from 10.100.2.138

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

Task 4. Running Your First few Commands

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Permission denied, please try again.
tryhackme@10.10.106.93's password:
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 Wed Apr 10 06:07:57 UTC 2024
System load: 0.16 Processes: 114
Usage of /: 18.7% of 9.63GB Users logged in: 1
Memory usage: 41% IPv4 address for ens5: 10.10.106.93
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
Last login: Wed Apr 10 06:07:03 2024 from 10.100.2.138
tryhackme@linux1:~\$ pwd
/home/tryhackme
tryhackme@linux1:~\$ echo HelloWorld
HelloWorld
tryhackme@linux1:~\$ echo "Hello World"
Hello World
tryhackme@linux1:~\$ whoami
tryhackme
tryhackme@linux1:~\$ ls
access.log folder1 folder2 folder3 folder4
tryhackme@linux1:~\$ ls folder2
tryhackme@linux1:~\$ cd folder2
tryhackme@linux1:~/folder2\$ ls
tryhackme@linux1:~/folder2\$ cd ..
tryhackme@linux1:~\$ clear

Task 5. Interacting With the Filesystem!



The screenshot shows a terminal window titled "kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal is running on a Kali Linux system. The user has run several commands to analyze a log file:

```
tryhackme@linux1:~$ ls
access.log  folder1  folder2  folder3  folder4
tryhackme@linux1:~$ cd access.log
-bash: cd: access.log: Not a directory
tryhackme@linux1:~$ cat access.log
54.36.148.184 - - [04/May/2021:06:26:27 +0000] "GET /contactme.html
176.193.62.165 - - [04/May/2021:06:28:56 +0000] "GET /category/ctf-w
like Gecko) DownloaderChrome/62.0.3202.75 Safari/537.36"
176.193.62.165 - - [04/May/2021:06:28:56 +0000] "GET / HTTP/1.1" 200
rChrome/62.0.3202.75 Safari/537.36"
188.166.73.233 - - [04/May/2021:06:28:58 +0000] "GET / HTTP/1.0" 400
34.86.35.11 - - [04/May/2021:06:34:42 +0000] "GET / HTTP/1.1" 200 18
customers#39; presences on the Internet. If you would like to be ex
114.119.159.208 - - [04/May/2021:06:35:16 +0000] "GET /category/writ
(compatible; PetalBot;+https://webmaster.petalsearch.com/site/petal
1.15.175.155 - - [04/May/2021:06:36:06 +0000] "GET / HTTP/1.1" 200 4
n/4.0 Chrome/78.0.3904.62 XWEB/2692 MMWEBSDK/200901 Mobile Safari/53
66.249.66.32 - - [04/May/2021:06:40:45 +0000] "GET /tags/tryhackme/
Chrome/90.0.4430.84 Mobile Safari/537.36 (compatible; Googlebot/2.1;
209.17.97.10 - - [04/May/2021:06:48:19 +0000] "GET / HTTP/1.1" 200 1
40.77.167.24 - - [04/May/2021:06:50:09 +0000] "GET / HTTP/1.1" 200 7
207.46.13.0 - - [04/May/2021:06:57:52 +0000] "GET /robots.txt HTTP/1
207.46.13.0 - - [04/May/2021:06:57:53 +0000] "GET /robots.txt HTTP/1
40.77.167.24 - - [04/May/2021:06:59:37 +0000] "GET / HTTP/1.1" 301 4
78.129.212.146 - - [04/May/2021:07:00:36 +0000] "GET /keybase.txt HT
ecko) Chrome/89.0.4389.128 Safari/537.36"
78.129.212.146 - - [04/May/2021:07:00:37 +0000] "GET /favicon.ico HT
like Gecko) Chrome/89.0.4389.128 Safari/537.36"
78.129.212.146 - - [04/May/2021:07:00:56 +0000] "-" 408 3249 "-" "-"
54.36.148.26 - - [04/May/2021:07:02:57 +0000] "GET /archives/ HTTP/1
43.242.215.22 - - [04/May/2021:07:11:15 +0000] "GET /index.php/comme
43.242.215.22 - - [04/May/2021:07:11:16 +0000] "GET /index.php/feed/
121.228.147.48 - - [04/May/2021:07:14:05 +0000] "GET / HTTP/1.1" 200
66.249.66.67 - - [04/May/2021:07:20:23 +0000] "GET / HTTP/1.1" 301 4
66.249.66.93 - - [04/May/2021:07:20:23 +0000] "GET / HTTP/1.1" 200 1
223.190.71.249 - - [04/May/2021:07:31:24 +0000] "GET /Presentations/
KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36 Edg/90.0.818.51
223.190.71.249 - - [04/May/2021:07:31:25 +0000] "GET /fancy-index/st
```

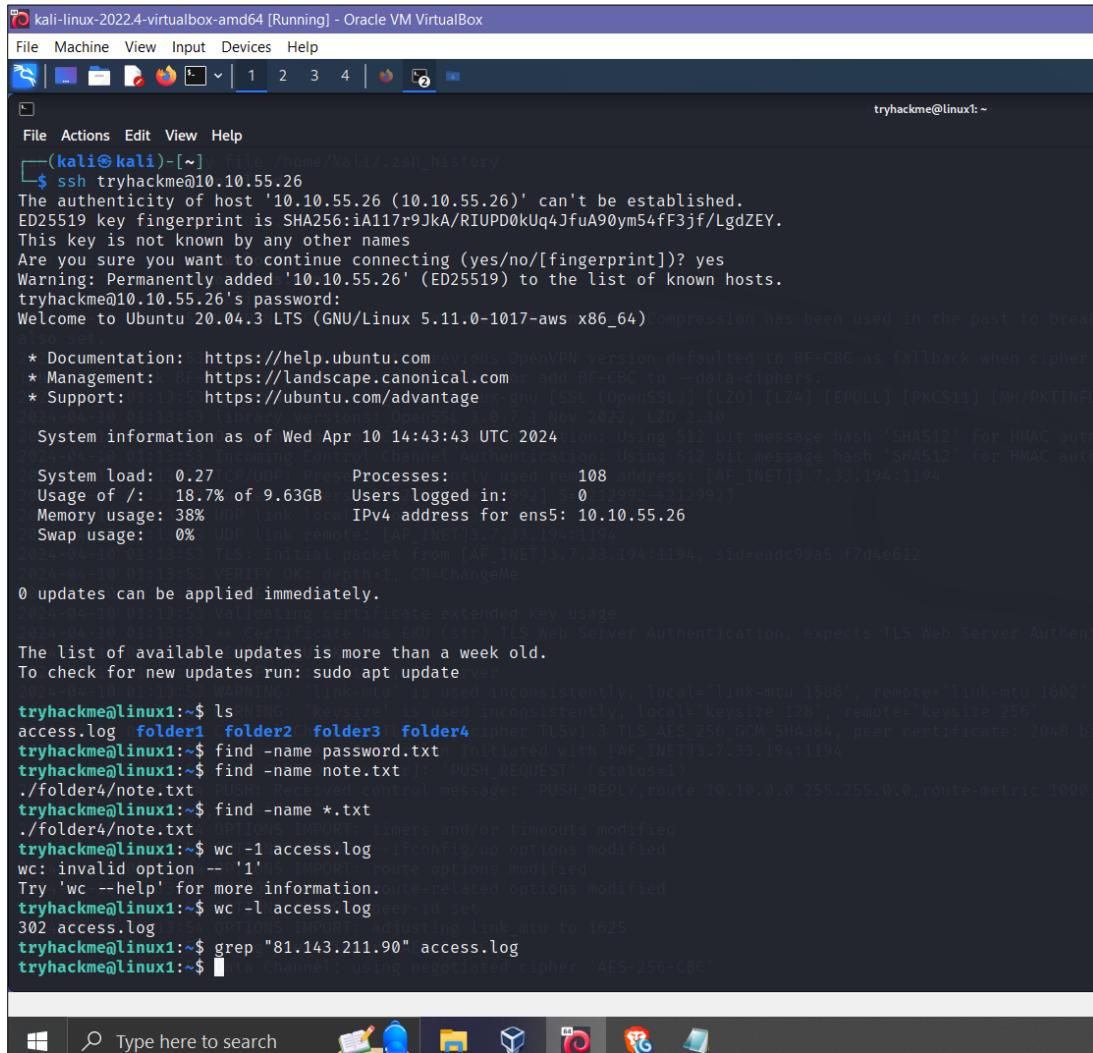
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

```
tryhackme@linux1:~$ pwd
/home/tryhackme
tryhackme@linux1:~$ ls
access.log folder1 folder2 folder3 folder4
tryhackme@linux1:~$ cd folder1
tryhackme@linux1:~/folder1$ ls
tryhackme@linux1:~/folder1$ cd ..
tryhackme@linux1:~$ cd folder2
tryhackme@linux1:~/folder2$ ls
tryhackme@linux1:~/folder2$ cd ..
tryhackme@linux1:~$ cd folder3
tryhackme@linux1:~/folder3$ ls
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$ cd note.txt
-bash: cd: note.txt: Not a directory
tryhackme@linux1:~/folder4$ pwd
/home/tryhackme/folder4
tryhackme@linux1:~/folder4$
```

Task 6. Searching for Files



The screenshot shows a terminal window titled "kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal is running on a Kali Linux system. The user has run several commands to search for files containing specific strings:

- \$ ssh tryhackme@10.10.55.26
- The authenticity of host '10.10.55.26' (10.10.55.26) can't be established.
ED25519 key fingerprint is SHA256:1A117r9JkA/RUUPD0kUq4JfuA90ym54fF3jf/LgdZEY.
- This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
- Warning: Permanently added '10.10.55.26' (ED25519) to the list of known hosts.
- tryhackme@10.10.55.26's password:
- Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.11.0-1017-aws x86_64)
- compression has been used in the past to break also set
- * Documentation: <https://help.ubuntu.com> previous OpenVPN version defaulted to BF-CBC as fallback when cipher
- * Management: BF-<https://landscape.canonical.com> add BF-CBC to --data-ciphers
- * Support: 11:37:53 https://ubuntu.com/advantage
- System information as of Wed Apr 10 14:43:43 UTC 2024: on: Using 512 bit message hash 'SHA512' for HMAC auth
- System load: 0.27
- System load: 0.27 TCP/IP: Ports Processes: only used port 108 address: [AF_INET]3.7.33.194:1194
- Usage of /: 18.7% of 9.63GB
- Users logged in: 0921 S 0 12992→212992
- Memory usage: 38%
- IPv4 address for ens5: 10.10.55.26
- Swap usage: 0%
- Swap usage: 0%
- 2024-04-10 01:13:53 TLS: Initial packet from [AF_INET]3.7.33.194:1194, sid=eadc99a5 f7d4e612
- 2024-04-10 01:13:53 VERIFY OK: depth=1, CN=ChangeMe
- 0 updates can be applied immediately.
- 2024-04-10 01:13:53 Validating certificate extended key usage
- 2024-04-10 01:13:53 + Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authent
- The list of available updates is more than a week old.
- To check for new updates run: sudo apt update
- 2024-04-10 01:13:53 WARNING: 'link-mtu' is used inconsistently, local='link-mtu 1586', remote='link-mtu 1602'
- tryhackme@linux1:\$ ls -NTNG: 'keysize' is used inconsistently, local='keysize 128', remote='keysize 256'
- access.log folder1 folder2 folder3 TL folder4 cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bi
- tryhackme@linux1:\$ find -name password.txt initiated with [AF_INET]3.7.33.194:1194
- tryhackme@linux1:\$ find -name note.txt: 'PUSH_REQUEST' (status=1)
- ./folder4/note.txt PUSH Received control message: 'PUSH_REPLY', route 10.10.0.0 255.255.0.0, route-metric 1000,
- tryhackme@linux1:\$ find -name *.txt
- ./folder4/note.txt OPTIONS IMPORT: timers and/or timeouts modified
- tryhackme@linux1:\$ wc -l access.log--ifconfig/up options modified
- wc: invalid option -- '1' is unknown route options modified
- Try 'wc --help' for more information.
- route-related options modified
- tryhackme@linux1:\$ wc -l access.log-peer-id set
- 302 access.log OPTIONS IMPORT: adjusting link_mtu to 1625
- tryhackme@linux1:\$ grep "81.143.211.90" access.log
- tryhackme@linux1:\$ [redacted] Channel: using negotiated cipher 'AES-256-CBC'

```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
tryhackme@linux1:~$ ls -le /home/kali/.zsh_history
access.log folder1 folder2 folder3 folder4
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/91.0.4453.114 Safari/537.36"
tryhackme@linux1:~$ ./unloads
$ sudo openvpn Zukö.Yasas.ovpn
[sudo] password for kali:
2024-04-10 01:13:53 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless also set.
2024-04-10 01:13:53 --cipher is not set. Previous OpenVPN version defaulted to BF-CBC as fallback when cipher negotiation failed in this case. If you need this
ciphers-fallback BF-CBC' to your configuration and/or add BF-CBC to --data-ciphers.
2024-04-10 01:13:53 OpenVPN 2.5.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Jul  5 2022
2024-04-10 01:13:53 library versions: OpenSSL 3.0.7 1 Nov 2022, LZO 2.10
```

Task 7. An Introduction to Shell Operators

```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
tryhackme@linux1:~$ ls -le /home/kali/.zsh_history
access.log folder1 folder2 folder3 folder4
tryhackme@linux1:~$ echo "i am yasas" > welcome
tryhackme@linux1:~$ ls Zukö.Yasas.ovpn
access.log folder1 folder2 folder3 folder4 welcome
tryhackme@linux1:~$ cat welcome
i am yasas
tryhackme@linux1:~$ echo "New content" > welcome
tryhackme@linux1:~$ cat welcome
New content
tryhackme@linux1:~$ echo "New Line" >> welcome
tryhackme@linux1:~$ cat welcome
New content
New Line
tryhackme@linux1:~$ ./unloads
[tryhackme@linux1 ~]$
```

Task 8. Conclusions & Summaries

- 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!

No answer needed

✓ Correct Answer

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

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

TryHackMe | OpenVPN TryHackMe | Access TryHackMe | Linux Funda +

11:25 120% ⚡

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Try Hack Me Dashboard Learn Compete Other

Go Premium 1 🔥

Source: YouTube Watch later Share

Learn the Linux Fundamentals Part 1

Learn the Linux Fundamentals Part 1

Congratulations!

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

Twitter Facebook LinkedIn

Leave feedback

Linux Fundamentals Part 2

https://www.facebook.com/sharer.php?u=www.tryhackme.com/r/room/linuxfundamentalspart1

Type here to search

8:55 PM 4/10/2024

A screenshot of a Kali Linux desktop environment within Oracle VM VirtualBox. The main window is a TryHackMe completion modal titled 'Congratulations!' with the message 'You've completed the room! Share this with your friends:' and social sharing buttons for Twitter, Facebook, and LinkedIn. Below the modal is a banner for 'Linux Fundamentals Part 2'. The background shows a large penguin icon and a video player interface for a 'Try Hack Me' video. The taskbar at the bottom includes icons for file explorer, terminal, and various applications.

Part 02

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
- Discovering how access to files and folders is managed and how we can determine our access.

- 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)

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

TryHackMe | Linux Fundamentals

https://tryhackme.com/r/room/linuxfundamentalspart2

120% 7:28

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Room progress (4%)

Task 2 Accessing Your Linux Machine Using SSH (Deploy)

The in-browser functionality was used in [Linux Fundamentals Part 1](#) to get you directly connected to your first ever Linux machine without any hassle.

Start Machine

In fact, the in-browser functionality uses the exact same protocol that we are going to be using today. This protocol is called **Secure Shell** or **SSH** for short and is the common means of connecting to and interacting with the command line of a remote **Linux** machine.

We will be deploying two machines in this room:

- Your **Linux** machine
- The TryHackMe AttackBox

What is SSH & how Does it Work?

Secure Shell or **SSH** simply is a protocol between devices in an encrypted form. Using cryptography, any input we send in a human-readable format is encrypted for travelling over a network -- where it is then unencrypted once it reaches the remote machine, such as in the diagram below.

You can learn about the various types of encryption on a TryHackMe room. But for now, we only need to

Your machine is initializing...
Use the AttackBox to attack machines you start on tasks
Loading (12%)

Access desktop in 106s + ⌂ - ⓘ THM AttackBox 1h 59m 4:58 PM

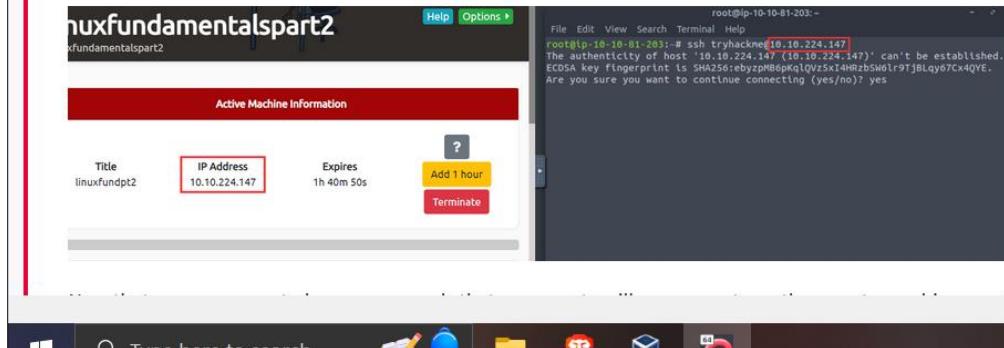
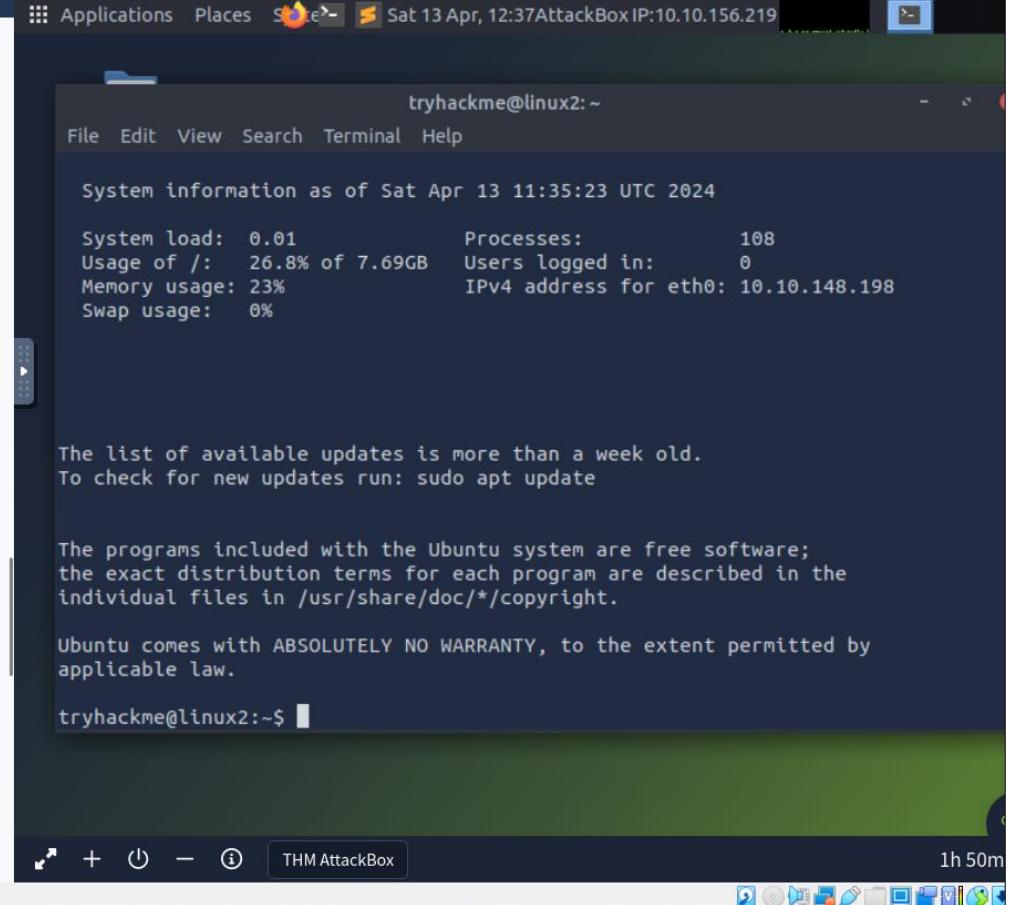
The syntax to use SSH is very simple. We only need to provide two things:

1. The IP address of the remote machine
2. Correct credentials to a valid account to login with on the remote machine

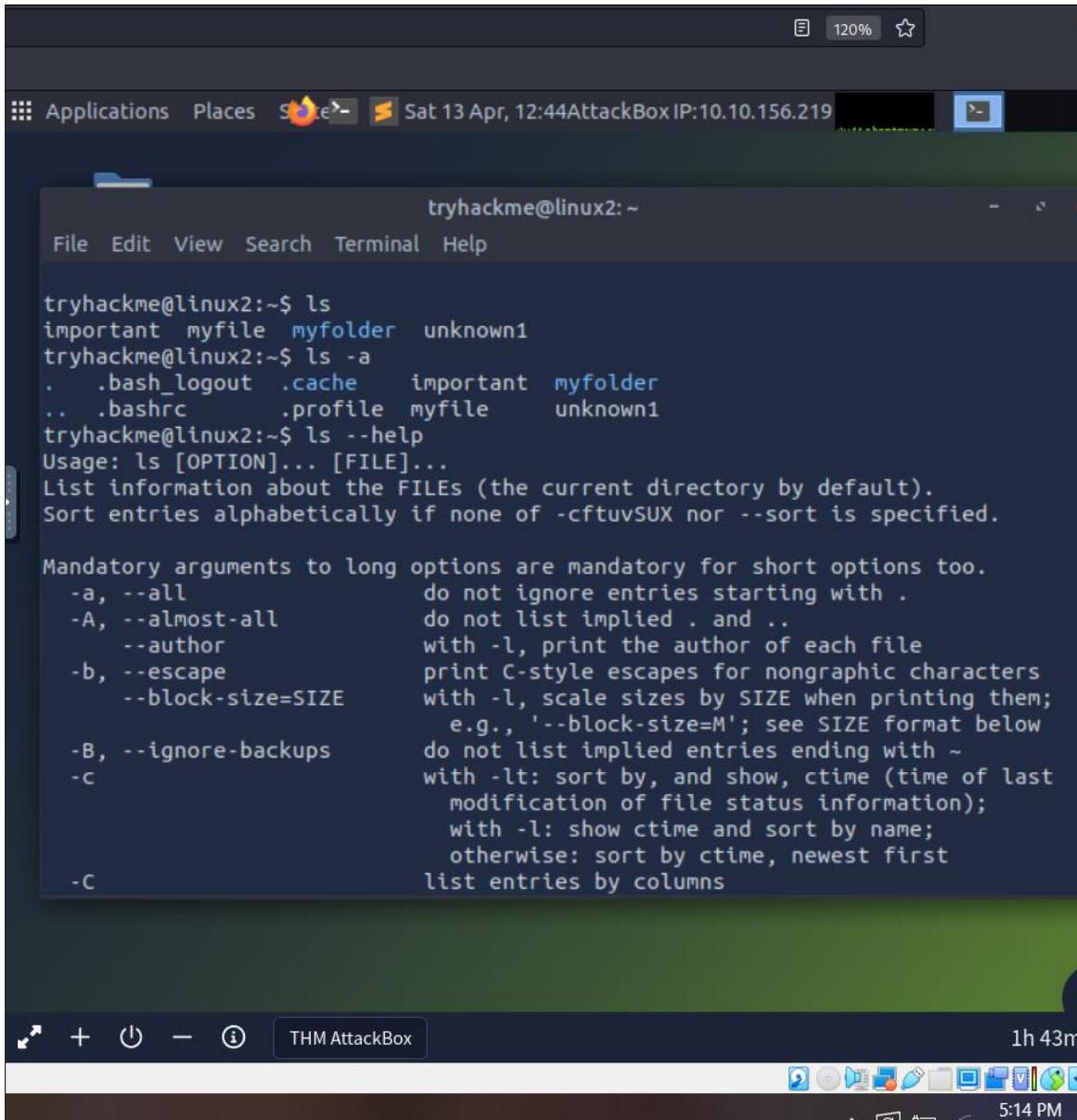
For this room, we will be logging in as "tryhackme", whose password is "tryhackme" without the quotation ("") marks. Let's use the IP address of the machine displayed in the card at the top of the room as the IP address and this user, to construct a command to log in to the remote machine using SSH. The command to do so is `ssh` and then the username of the account, @ 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@10.10.148.198`. 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".

Task 3. Introduction to Flags and Switches



The screenshot shows a terminal window titled "tryhackme@linux2:~". The terminal displays the following session:

```
tryhackme@linux2:~$ ls
important myfile myfolder unknown1
tryhackme@linux2:~$ ls -a
. .bash_logout .cache important myfolder
.. .bashrc .profile myfile unknown1
tryhackme@linux2:~$ ls --help
Usage: ls [OPTION]... [FILE]...
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
-B, --ignore-backups   do not list implied entries ending with ~
-c                      with -lt: sort by, and show, ctime (time of last
                        modification of file status information);
                        with -l: show ctime and sort by name;
                        otherwise: sort by ctime, newest first
-C                      list entries by columns
```

The terminal is running on an "AttackBox" system, as indicated by the window title and the desktop bar.

```
tryhackme@linux2:~
```

```
File Edit View Search Terminal Help
```

```
LS(1) User Commands LS(1)
```

```
NAME
ls - list directory contents
```

```
SYNOPSIS
ls [OPTION]... [FILE]...
```

```
DESCRIPTION
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 ..
```

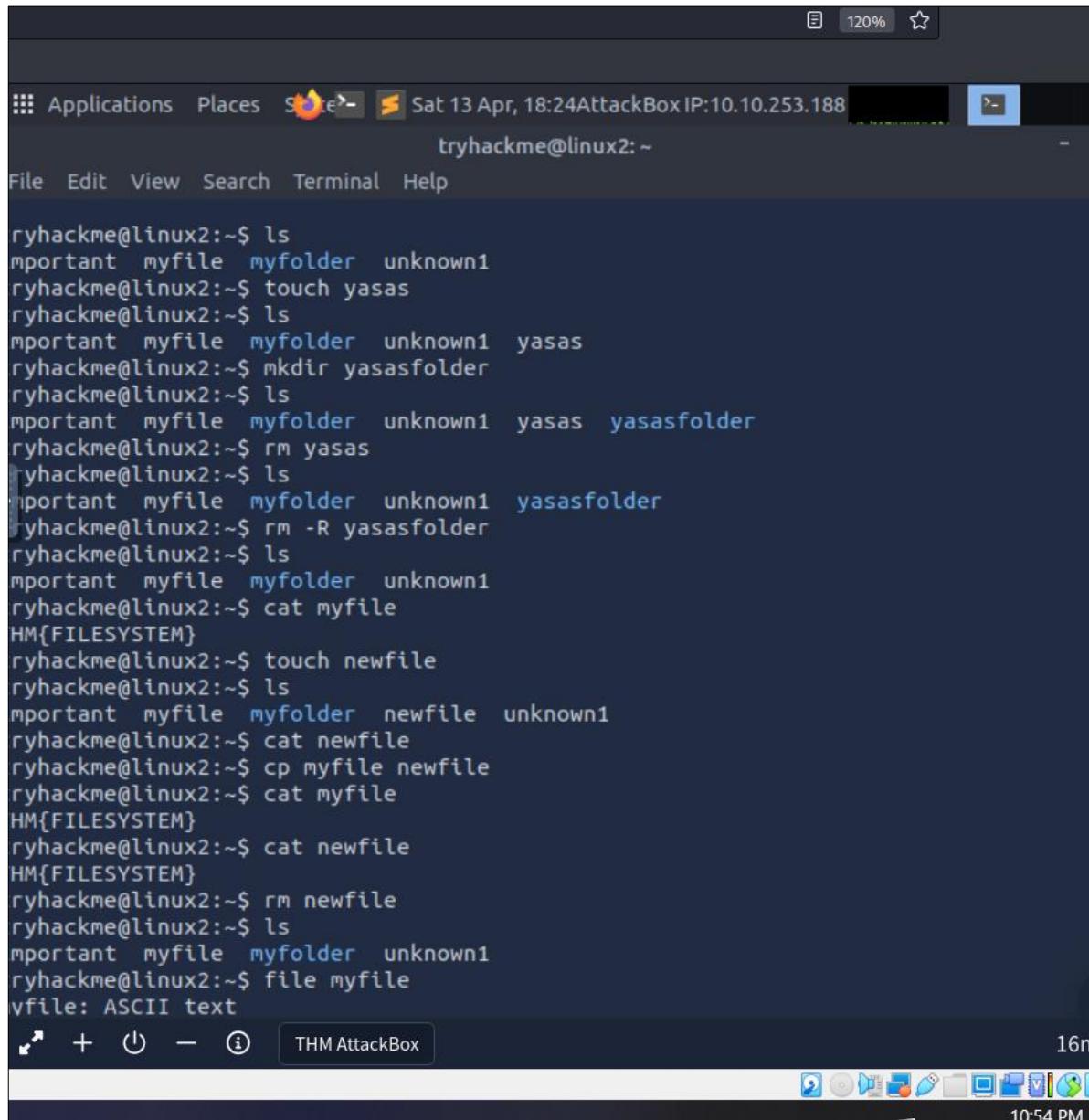
```
--author
```

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

```
THM AttackBox 1h 39m
```

```
5:18 PM
```

Task 4. Filesystem Interaction Continued



The screenshot shows a terminal window titled "tryhackme@linux2: ~". The terminal displays a series of Linux command-line interactions:

```
tryhackme@linux2:~$ ls
important myfile myfolder unknown1
tryhackme@linux2:~$ touch yasas
tryhackme@linux2:~$ ls
important myfile myfolder unknown1 yasas
tryhackme@linux2:~$ mkdir yasasfolder
tryhackme@linux2:~$ ls
important myfile myfolder unknown1 yasas yasasfolder
tryhackme@linux2:~$ rm yasas
tryhackme@linux2:~$ ls
important myfile myfolder unknown1 yasasfolder
tryhackme@linux2:~$ rm -R yasasfolder
tryhackme@linux2:~$ ls
important myfile myfolder unknown1
tryhackme@linux2:~$ cat myfile
HM{FILESYSTEM}
tryhackme@linux2:~$ touch newfile
tryhackme@linux2:~$ ls
important myfile myfolder newfile unknown1
tryhackme@linux2:~$ cat newfile
tryhackme@linux2:~$ cp myfile newfile
tryhackme@linux2:~$ cat myfile
HM{FILESYSTEM}
tryhackme@linux2:~$ cat newfile
HM{FILESYSTEM}
tryhackme@linux2:~$ rm newfile
tryhackme@linux2:~$ ls
important myfile myfolder unknown1
tryhackme@linux2:~$ file myfile
myfile: ASCII text
```

The terminal also shows a status bar at the bottom with icons for file operations, a progress bar indicating "16m", and the current time "10:54 PM".

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

TryHackMe | Linux Fundamentals

Site Search

https://tryhackme.com/r/room/linuxfundamentalspart2

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Room progress (45%)

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 5 Permissions 101

THM AttackBox

```
tryhackme@linux2:~$ ls
important myfile myfolder unknown1
tryhackme@linux2:~$ file unknown1
unknown1: ASCII text
tryhackme@linux2:~$ mv myfile myfolder
tryhackme@linux2:~$ ls
important myfolder unknown1
tryhackme@linux2:~$ cat myfolder
cat: myfolder: Is a directory
tryhackme@linux2:~$ cd myfolder
tryhackme@linux2:~/myfolder$ ls
myfile
tryhackme@linux2:~/myfolder$ cat myfile
THM{FILESYSTEM}
tryhackme@linux2:~/myfolder$
```

Task 5. Permissions 101

The screenshot shows a Kali Linux virtual machine running in Oracle VM VirtualBox. The desktop environment is Unity, with a terminal window open in the background.

Terminal Session (tryhackme@linux2:~)

```
File Edit View Search Terminal Help
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@linux2:~$ ls
important myfile myfolder unknown1
tryhackme@linux2:~$ ls -l
total 16
-rw-r--r-- 1 user2 user2 14 May 5 2021 important
-rw-r--r-- 1 tryhackme tryhackme 16 May 5 2021 myfile
drwxr-xr-x 2 tryhackme tryhackme 4096 May 4 2021 myfolder
-rw-r--r-- 1 tryhackme tryhackme 17 May 4 2021 unknown1
tryhackme@linux2:~$ su user2
Password:
user2@linux2:/home/tryhackme$ ls
important myfile myfolder unknown1
user2@linux2:/home/tryhackme$ cat important
THM{SU_USER2}
user2@linux2:/home/tryhackme$ su tryhackme
Password:
tryhackme@linux2:~$ ls
important myfile myfolder unknown1
tryhackme@linux2:~$
```

Task Progress (63%)

Where now, after using `-1`, 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

Type here to search

Task 6. Common Directories

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

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>

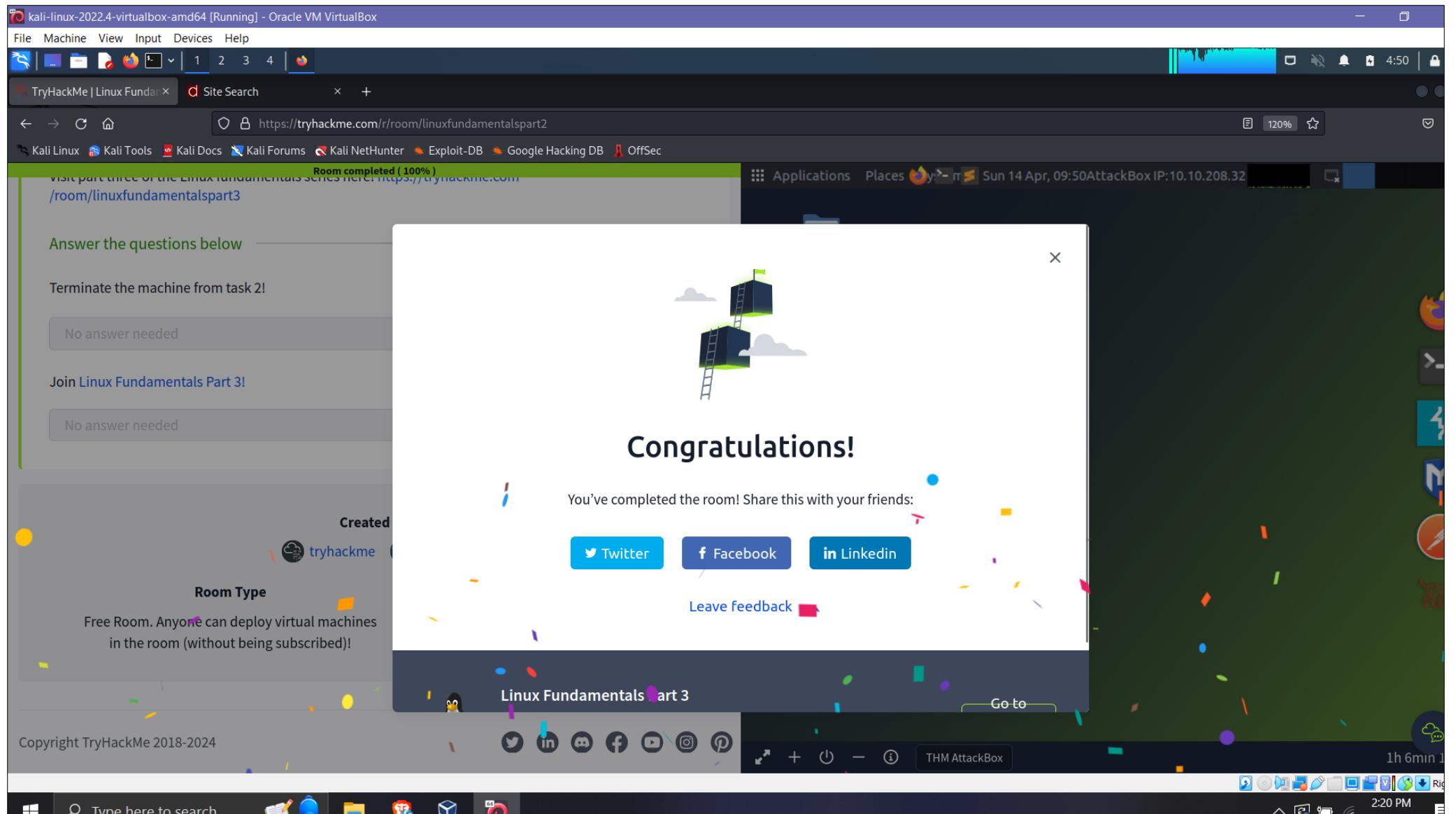
Answer the questions below

Terminate the machine from task 2!

No answer needed ✓ Correct Answer

Join [Linux Fundamentals Part 3!](#)

No answer needed ✓ Correct Answer

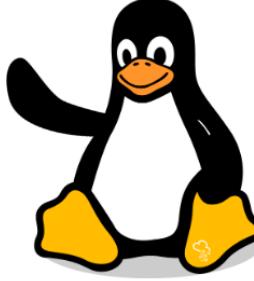


Part 03

Task 1. Introduction

Me Dashboard Learn Compete Other

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

The screenshot shows a Kali Linux 2022.4 virtual machine running in Oracle VM VirtualBox. The desktop environment is Xfce.

Left Panel (TryHackMe Challenge):

- Title:** Linux Fundamentals Part 3
- Room progress:** 8%
- Credentials:**
 - IP Address: **10.10.93.43**
 - Username: **tryhackme**
 - Password: **tryhackme**
- Message:** Answer the questions below
- Feedback:** No answer needed (grey button) or ✓ Correct Answer (green button)
- Tasks:**
 - Task 3: Terminal Text Editors
 - Task 4: General/Useful Utilities
 - Task 5: Processes 101

Right Panel (Terminal Session):

- Terminal Title:** Sun 14 Apr, 10:02 AttackBox IP:10.10.94.179
- Feedback:** Woop woop! Your answer is correct
- System Information:**

| Management: | https://landscape.canonical.com |
|-------------|---|
| Support: | https://ubuntu.com/advantage |

System information as of Sun Apr 14 09:02:41 UTC 2024

| System load: | 0.09 | Processes: | 108 |
|---------------|-----------------|------------------------|-------------|
| Usage of /: | 9.6% of 29.01GB | Users logged in: | 0 |
| Memory usage: | 10% | IPv4 address for eth0: | 10.10.93.43 |
| Swap usage: | 0% | | |
- Text:** Ubuntu Pro delivers the most comprehensive open source security and compliance features.
<https://ubuntu.com/aws/pro>
- Text:** 0 updates can be applied immediately.
- Text:** The list of available updates is more than a week old.
To check for new updates run: sudo apt update
- Text:** 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.
- Text:** Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
- Terminal Prompt:** tryhackme@linux3:~\$
- Bottom Bar:** Includes a search bar, file manager, terminal, and system icons.

Task 3. Terminal Text Editors

The screenshot shows a Kali Linux desktop environment running in Oracle VM VirtualBox. The desktop has a dark blue header bar with icons for File, Machine, View, Input, Devices, Help, and a system status bar showing 5:33. Below the header is a dock with icons for terminal, file manager, browser, and other utilities. A browser window is open at <https://tryhackme.com/r/room/linuxfundamentalspart3>, displaying a TryHackMe challenge room. The terminal window on the right shows a user session on an Ubuntu system with IP 10.10.94.179, running Sun 14 Apr, 10:34. The terminal output includes information about Ubuntu Pro, available updates, and a note about warranty. The bottom of the screen shows a dock with various application icons.

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

Task 4. General/Useful Utilities

The screenshot shows a Kali Linux VM running in Oracle VM VirtualBox. On the left, a Firefox browser window displays a TryHackMe challenge titled "Linux Fundamentals Part 3". The challenge asks to start an HTTP server using Python's "HTTPServer" module. A terminal window on the right shows the command `python3 -m http.server` being run, and the output indicates the server is listening on port 8000. A message box in the terminal says "Woop woop! Your answer is correct".

TryHackMe | Linux Fundamentals Part 3

https://tryhackme.com/r/room/linuxfundamentalspart3

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Room progress (26%)

location for the me 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 (10.10.93.43)

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://10.10.93.43:8000/.flag.txt> onto the TryHackMe AttackBox. Remember, you will need to do this in a new terminal.

What are the contents?

tryha Sun 14 Apr, 11:22 AttackBox IP:10.10.94.179

tryhackme@linux3:~\$ python3 -m http.server

Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...

✓ Woop woop! Your answer is correct

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

TryHackMe | Linux Fundamentals part 3 Site Search 120% 6:40

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Room progress (30%)

Answer the questions below

Ensure you are connected to the deployed instance (10.10.93.43)

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://10.10.93.43:8000/.flag.txt> onto the TryHackMe AttackBox. Remember, you will need to do this in a new terminal.

What are the contents?

THM[WGET_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 ⏪ Complete Hint

Applications Places System Sun 14 Apr, 11:40 AttackBox IP:10.10.94.179 root@ip-10-10-94-179:~

tryhackme@linux3:~ x root@ip-10-10-94-179:~

```
drwxr-xr-x 3 root root 4096 Dec 29 2020 Desktop
drwxr-xr-x 2 root root 4096 Sep 10 2020 Downloads
drwxr-xr-x 2 root root 4096 Oct 30 2020 Instructions
drwxr-xr-x 3 root root 4096 Jan 24 13:28 Pictures
drwxr-xr-x 3 root root 4096 Aug 16 2020 Postman
drwxr-xr-x 30 root root 4096 Apr 10 22:16 Rooms
drwxr-xr-x 2 root root 4096 Apr 11 19:11 Scripts
drwxr-xr-t 2 root root 4096 Aug 13 2020 thinclient_drives
drwxrwxrwx 1 root root 19 Mar 18 2021 Tools -> /root/Desktop/Tools
root@ip-10-10-94-179:~# ls -a
Desktop .install4j .recon-ng .viminfo
.. .dmrc Instructions Rooms .vnc
.aspnet .dotnet .java .rpmbdb .wfuzz
.bash_aliases Downloads .john .rustup .wget-hsts
.bash_history .flag.txt .local Scripts .wpscan
.bashrc .gem .mozilla .selected_editor .xauthority
.bundle .ghidra .msf4 .set .xorgxrdp.10.log
.BurpSuite .gnupg .nuget .ssh .xorgxrdp.10.log..
.cache .gradle Pictures .subversion .xsessions-errors
.cargo .gvfs .pki .terraform .xsession-errors
.config .hashcat Postman .themes .ZAP
CTFBuilder .ICEAuthority .profile thinclient_drives .zshenv
.dbus .icons .python_history Tools
root@ip-10-10-94-179:~# cat flag.txt
cat: flag.txt: No such file or directory
root@ip-10-10-94-179:~# cat .flag.txt
THM{WGET_WEBSERVER}
root@ip-10-10-94-179:~#
```

THM AttackBox 19mi 4:10 PM

Task 5. Processes 101

The screenshot shows the TryHackMe interface with the following details:

- Top Bar:** Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec.
- Room Progress:** 34% (Terminate button)
- Task List:** Task 1 (Introduction), Task 2 (Deploy Your Linux Machine), Task 3 (Terminal Text Editors), Task 4 (General/Useful Utilities), Task 5 (Processes 101) - currently selected.
- Terminal Output:**

```
tryhackme@linux3:~$ ps
  PID TTY      TIME CMD
 1004 pts/0    00:00:00 bash
 1023 pts/0    00:00:00 ps
tryhackme@linux3:~$ ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  1.8  0.5 102644 11208 ?        Ss 14:55  0:06 /sbin/init
root         2  0.0  0.0      0     0 ?        S 14:55  0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        I< 14:55  0:00 [rcu_gp]
root         4  0.0  0.0      0     0 ?        I< 14:55  0:00 [rcu_par_gp]
root         5  0.0  0.0      0     0 ?        I< 14:55  0:00 [netns]
root         7  0.0  0.0      0     0 ?        I< 14:55  0:00 [kworker/0:0H-events]
root         9  0.0  0.0      0     0 ?        I< 14:55  0:00 [kworker/0:1H-events]
root        10  0.0  0.0      0     0 ?        I< 14:55  0:00 [mm_percpu_wq]
root        11  0.0  0.0      0     0 ?        S 14:55  0:00 [rcu_tasks_rude_]
root        12  0.0  0.0      0     0 ?        S 14:55  0:00 [rcu_tasks_trace]
root        13  0.0  0.0      0     0 ?        S 14:55  0:00 [ksoftirqd/0]
root        14  0.1  0.0      0     0 ?        I 14:55  0:00 [rcu_sched]
root        15  0.0  0.0      0     0 ?        S 14:55  0:00 [migration/0]
root        16  0.0  0.0      0     0 ?        S 14:55  0:00 [idle_inject/0]
root        17  0.0  0.0      0     0 ?        I 14:55  0:00 [kworker/0:1-events]
root        18  0.0  0.0      0     0 ?        S 14:55  0:00 [cpuhp/0]
root        19  0.0  0.0      0     0 ?        S 14:55  0:00 [kdevtmpfs]
root        20  0.0  0.0      0     0 ?        I< 14:55  0:00 [inet_frag_wq]
root        21  0.0  0.0      0     0 ?        S 14:55  0:00 [kauditfd]
root        22  0.0  0.0      0     0 ?        S 14:55  0:00 [khungtaskd]
root        23  0.0  0.0      0     0 ?        S 14:55  0:00 [oom_reaper]
root        24  0.0  0.0      0     0 ?        I< 14:55  0:00 [writeback]
root        25  0.0  0.0      0     0 ?        S 14:55  0:00 [kcompactd_a]
```
- Description of Processes:** Processes are the programs that are running on your machine. They are managed by the kernel, where each process will have an ID associated with it, also known as its PID. The PID increments for the order in which the process starts. I.e. the 60th process will have a PID of 60.
- Section Header:** **Viewing Processes**
- Text:** We can use the friendly `ps` command to provide a list of the running processes as our user's session and some additional information such as its status code, the session that is running it, how much usage time of the CPU it is using, and the name of the actual program or command that is being executed:

https://tryhackme.com/r/room/linuxfundamentalspart3

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Room progress (34%)

?

Add 1 hour

Terminate

Task 1 ✓ Introduction

Task 2 ✓ Deploy Your Linux Machine

Task 3 ✓ Terminal Text Editors

Task 4 ✓ General/Useful Utilities

Task 5 ○ Processes 101

Processes are the programs that are running on your machine. They are managed by the kernel, where each process will have an ID associated with it, also known as its PID. The PID increments for the order in which the process starts. I.e. the 60th process will have a PID of 60.

[Viewing Processes](#)

We can use the friendly `ps` command to provide a list of the running processes as our user's session and some additional information such as its status code, the session that is running it, how much usage time of

Applications Places Synergy Tue 16 Apr, 16:03 AttackBox IP:10.10.96.226 tryhackme@linux3:~

File Edit View Search Terminal Help

```
top - 15:03:30 up 8 min, 1 user, load average: 0.00, 0.04, 0.03
Tasks: 100 total, 1 running, 99 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.0 us, 0.0 sy, 0.0 ni, 100.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 1972.7 total, 1134.7 free, 195.5 used, 642.5 buff/cache
MiB Swap: 0.0 total, 0.0 free, 0.0 used. 1622.9 avail Mem
```

| PID | USER | PR | NI | VIRT | RES | SHR | S | %CPU | %MEM | TIME+ | COMMAND |
|------|----------|-----|-----|--------|-------|------|---|------|------|---------|-----------------|
| 1117 | tryhack+ | 20 | 0 | 10888 | 3772 | 3252 | R | 0.3 | 0.2 | 0:00.01 | top |
| 1 | root | 20 | 0 | 102644 | 11208 | 8216 | S | 0.0 | 0.6 | 0:06.63 | systemd |
| 2 | root | 20 | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.00 | kthreadd |
| 3 | root | 0 | -20 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.00 | rcu_gp |
| 4 | root | 0 | -20 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.00 | rcu_par_gp |
| 5 | root | 0 | -20 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.00 | netns |
| 7 | root | 0 | -20 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.00 | kworker/0:0H-e+ |
| 9 | root | 0 | -20 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.05 | kworker/0:1H-e+ |
| 10 | root | 0 | -20 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.00 | mm_percpu_wq |
| 11 | root | 20 | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.00 | rcu_tasks_rude_ |
| 12 | root | 20 | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.00 | rcu_tasks_trace |
| 13 | root | 20 | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.08 | ksoftirqd/0 |
| 14 | root | 20 | 0 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.64 | rcu_sched |
| 15 | root | rt | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.00 | migration/0 |
| 16 | root | -51 | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.00 | idle_inject/0 |
| 17 | root | 20 | 0 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.24 | kworker/0:1-ev+ |
| 18 | root | 20 | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.00 | cpuhp/0 |
| 19 | root | 20 | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.00 | kdevtmpfs |
| 20 | root | 0 | -20 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.00 | inet_frag_wq |
| 21 | root | 20 | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.00 | kauditd |
| 22 | root | 20 | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.00 | khungtaskd |
| 23 | root | 20 | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.00 | oom_reaper |
| 24 | root | 0 | -20 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.00 | writeback |

Page | 30

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 (10.10.253.95). 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

tryhackme@linux3: ~ root@ip-10-10-96-226: ~

```

root      568  0.0  0.5 315064 11000 ?      Ssl  14:55  0:00 /usr/sbin/ModemManager
root      569  0.0  0.1 7360  2412  ttyS0 - \u --keep-baud 115200,38400,9600  ttyS0 vt220
root      581  0.0  0.0 5836  1844  tty1 - \u --noclear tty1 linux
root      585  0.0  1.0 108136 20504 ?      Ssl  14:55  0:00 /usr/bin/python3
r/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
root      765  0.0  0.3 12184  7060 ?      Ss  14:55  0:00 sshd: /usr/sbin/sshd -o
AuthorizedKeysCommand /usr/share/ec2-instance-connect/eic_run_authorized_key
if -o AuthorizedKeysCommandUser ec2-instance-connect [listener] 0 of 10-100 startu
root      852  0.0  0.0      0  0 ?      I   14:55  0:00 [kworker/0:4-cgr
destroy]
root      858  0.0  1.0 1167084 21188 ?      Sl  14:55  0:00 /snap/amazon-ssm
nt/6312/ssm-agent-worker
root      895  0.0  0.4 13936  9228 ?      Ss  14:59  0:00 sshd: tryhackme@v]
tryhack+  898  0.0  0.4 18928  9628 ?      Ss  14:59  0:00 /lib/systemd/sys
--user
tryhack+  899  0.0  0.1 104224  3368 ?      S  14:59  0:00 (sd-pam)
tryhack+  1003  0.0  0.2 14068  5988 ?      S  14:59  0:00 sshd: tryhackme@0
tryhack+  1004  0.0  0.2 10040  5084 pts/0  Ss  14:59  0:00 -bash
root     1115  0.0  0.0      0  0 ?      I   15:02  0:00 [kworker/u30:0-e
s_unbound]
tryhack+  1132  0.0  0.1 10620  3360 pts/0  R+  15:11  0:00 ps aux

```

Task 6. Maintaining Your System: Automation

The screenshot shows a web browser window for tryhackme.com/r/room/linuxfundamentalspart3. The terminal window displays a crontab configuration:

```
# 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)
#
# m h dom mon dow   command
0 */12 * * * cp -R /home/cmnatic/Documents /var/backups/ >/dev/null 2>&1
```

Below the terminal, there is a question: "Answer the questions below". A note says: "Ensure you are connected to the deployed instance and look at the running crontabs." There are three buttons: "No answer needed" (grey), "Correct Answer" (green with a checkmark), and "Hint" (orange). Another note asks: "When will the crontab on the deployed instance (10.10.253.95) run?". Below this is another set of buttons: "@reboot" (grey), "Correct Answer" (green with a checkmark), and "Hint" (orange). At the bottom, a navigation bar shows "Task 7" and "Maintaining Your System: Package Management".

Terminal content (continued from above):

```
tryhackme@linux3:~
```

The terminal shows the contents of /tmp/crontab.HK8XnH/crontab:

```
File Edit View Search Terminal Help
GNU nano 4.8 /tmp/crontab.HK8XnH/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)
#
# m h dom mon dow   command
@reboot /var/opt/processes.sh
```

Terminal status bar:

```
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^L Replace ^U Paste Text ^T To Spell ^_ Go To Lir
```

Task 7. Maintaining Your System: Package Management

The screenshot shows a web browser window with a Kali Linux theme. The address bar shows the URL <https://tryhackme.com/r/room/linuxfundamentalspart3>. The page content is a guide on package management:

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

The terminal window shows the following output:

```
tryhackme@linux3:~$ sudo apt update
[...]
tryhackme@linux3:~$ apt update
[...]
tryhackme@linux3:~$ apt install sublime-text
[...]
tryhackme@linux3:~$ apt remove sublime-text
[...]
tryhackme@linux3:~$
```

System information as of Tue Apr 16 15:19:26 UTC 2024

| System load | Processes |
|-------------|-----------|
| 0.0 | 101 |

Usage of /: 9.6% of 29.01GB
Memory usage: 11%
Swap usage: 0%

IPv4 address for eth0: 10.10.253.95

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`

Task 8. Maintaining Your System: Logs

https://tryhackme.com/r/room/linuxfundamentalspart3

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Room progress (91%)

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 9 Conclusions & Summaries

Applications Places Systray Tue 16 Apr, 16:41 AttackBox IP:10.10.96.226

tryhackme@linux3:~\$ cd var/log/apache2
-bash: cd: var/log/apache2: No such file or directory
tryhackme@linux3:~\$ cd /var/log/apache2
tryhackme@linux3:/var/log/apache2\$ ls
access.log error.log error.log.2.gz
access.log.1 error.log.1 other_vhosts_access.log
tryhackme@linux3:/var/log/apache2\$ ls -l
total 12
-rw-r----- 1 root adm 0 Apr 16 14:55 access.log
-rwxrwxrwx 1 tryhackme tryhackme 209 May 4 2021 **access.log.1**
-w-r----- 1 root adm 0 Apr 16 14:55 error.log
-rw-r----- 1 root adm 810 Oct 18 2022 error.log.1
-rwxrwxrwx 1 root adm 464 May 5 2021 **error.log.2.gz**
-rw-r----- 1 root adm 0 May 4 2021 other_vhosts_access.log
tryhackme@linux3:/var/log/apache2\$ cat access.log.1
10.9.232.111 - [04/May/2021:18:18:16 +0000] "GET /catsanddogs.jpg HTTP/1.1" 200 51395
"- Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/90.0.4430.93 Safari/537.36"
tryhackme@linux3:/var/log/apache2\$

Woop woop! Your answer is correct

Task 9. Conclusions & Summaries

← → ⌂ ⌂ https://tryhackme.com/r/room/linuxfundamentalspart3 120% ⌂ ⌂

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Room completed (100%) Applications Places System Tue 16 Apr, 16:42 AttackBox IP:10.10.96.226

tryhackme@linux3:/var/www/html

Woop woop! Your answer is correct

Answer the questions below

Terminate the machine deployed in this room from task:

No answer needed

Continue your learning in other Linux-dedicated rooms

No answer needed

Created by tryhackme

Room Type

Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!

Congratulations!

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

Twitter Facebook LinkedIn

Leave feedback

Windows Fundamentals 1

The screenshot shows a completed room summary on the left and a central congratulatory message. The congratulatory message includes social sharing options for Twitter, Facebook, and LinkedIn, and a 'Leave feedback' link. A terminal window on the right shows a directory listing with files like access.log, error.log, and other_vhosts_access.log.