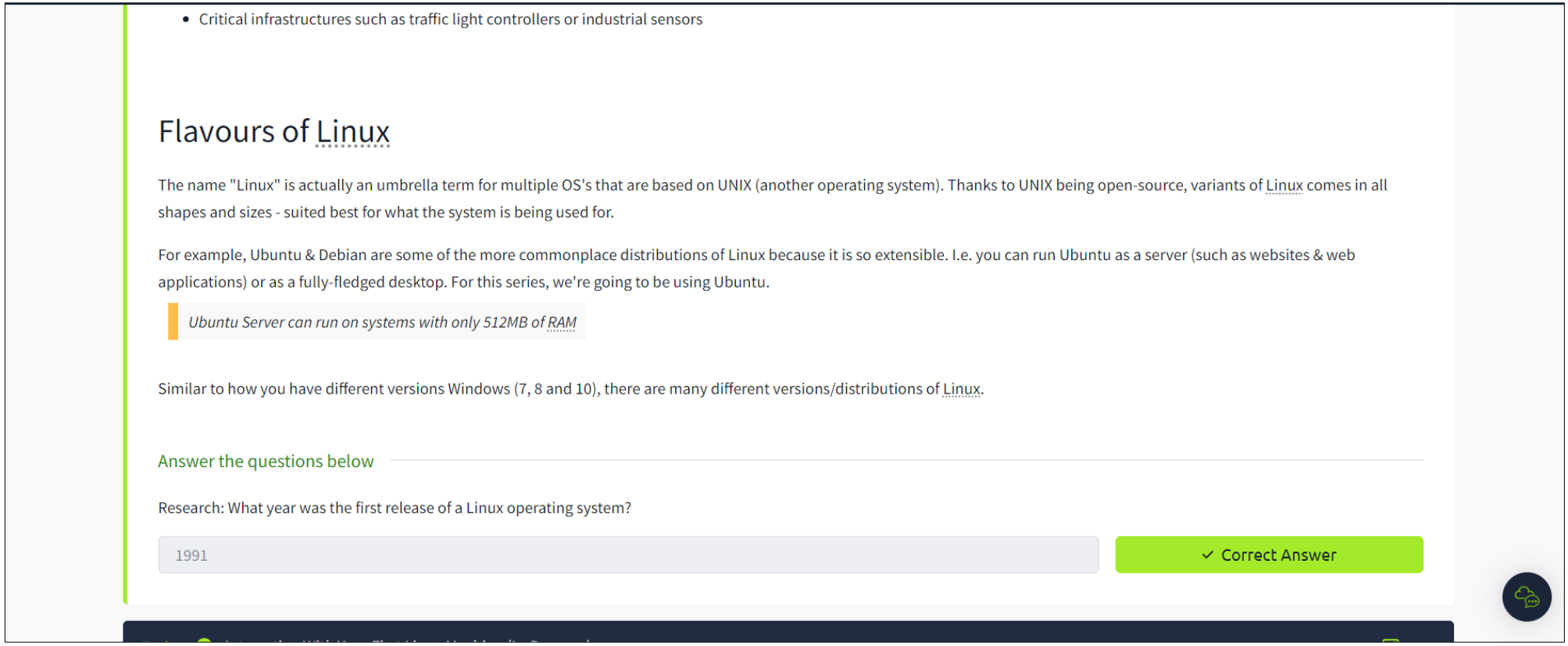
# Linux Fundamentals – Yasas Priyamantha

## Part 01

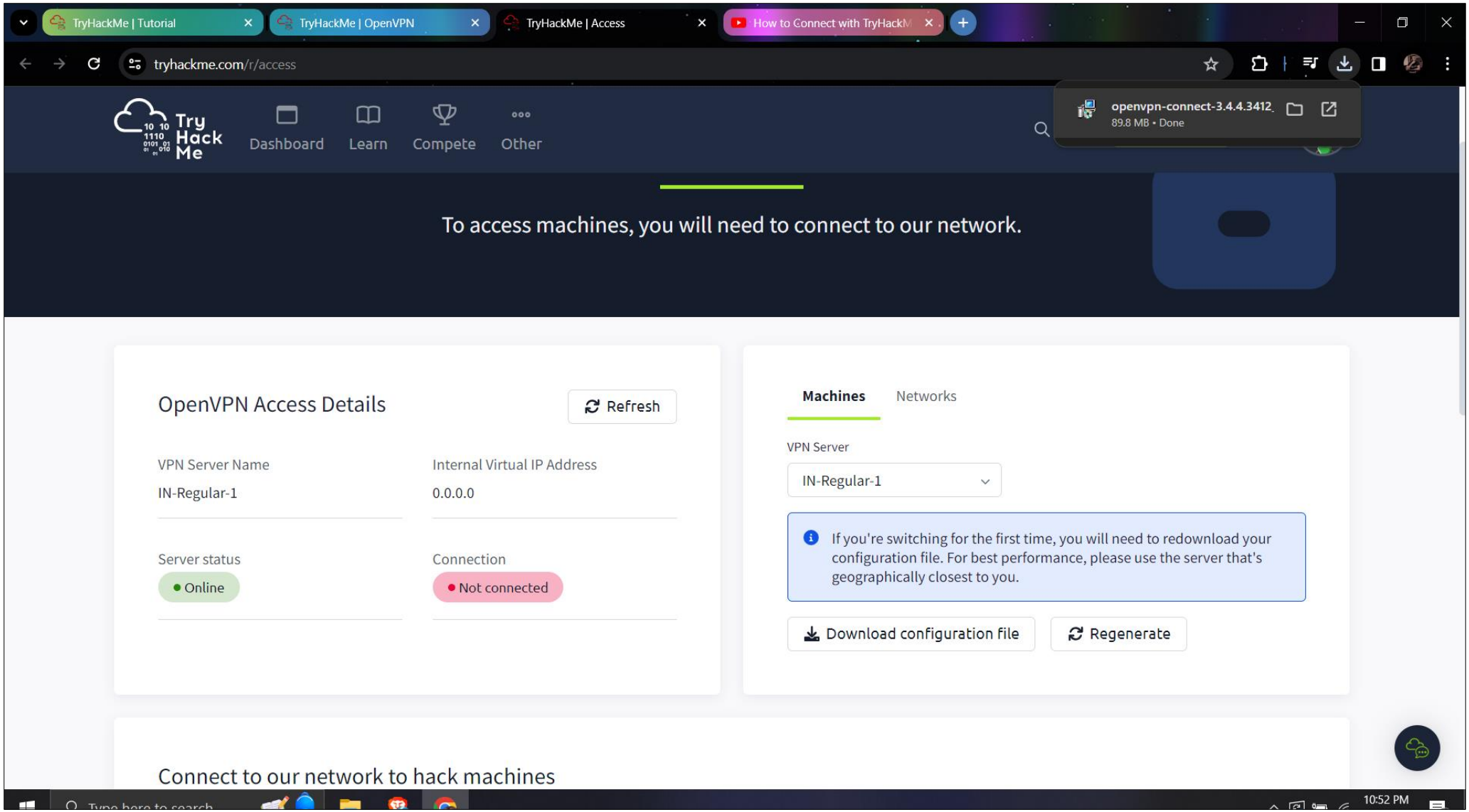
### Task 1. Introduction

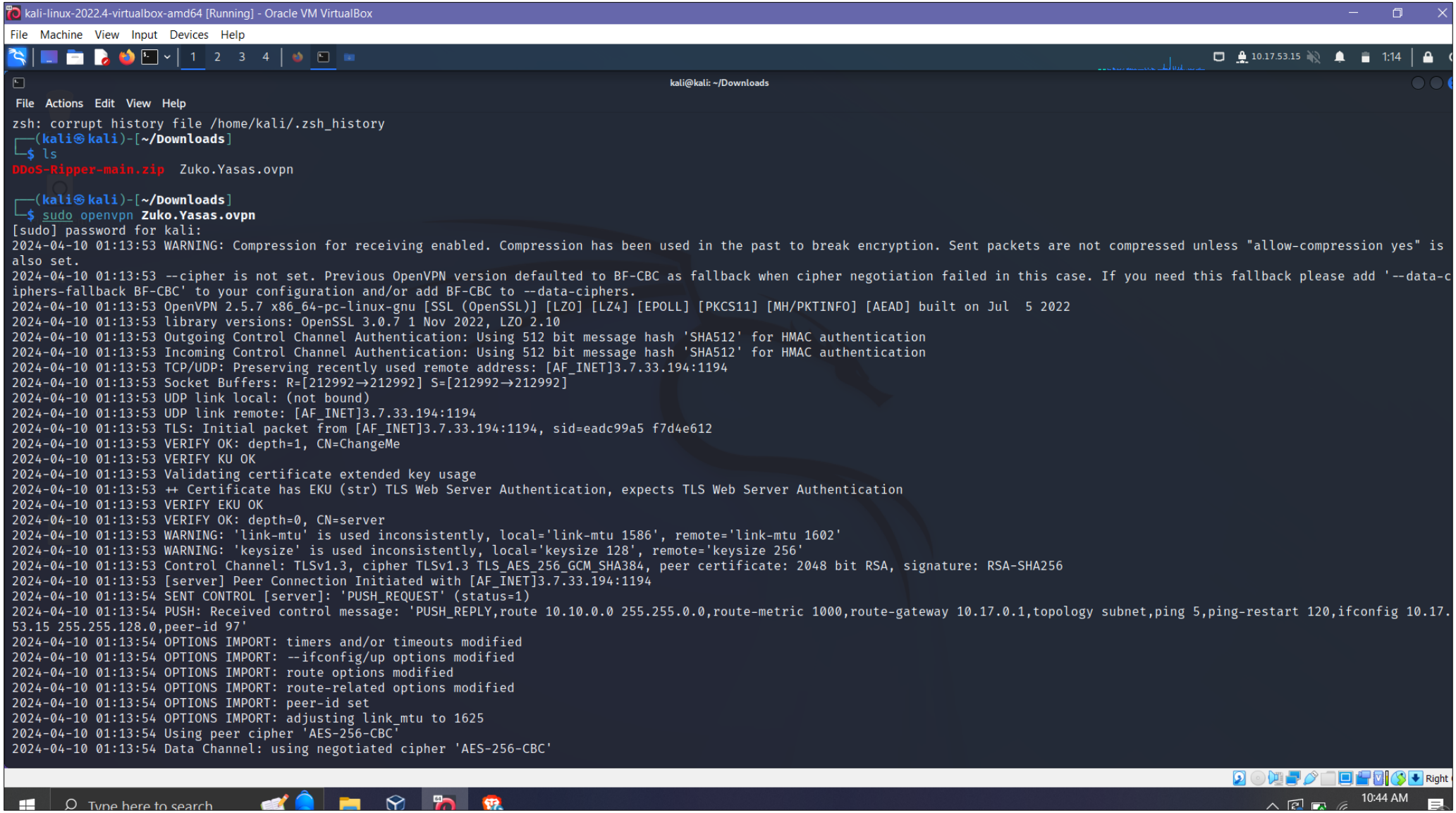
- No exercises.

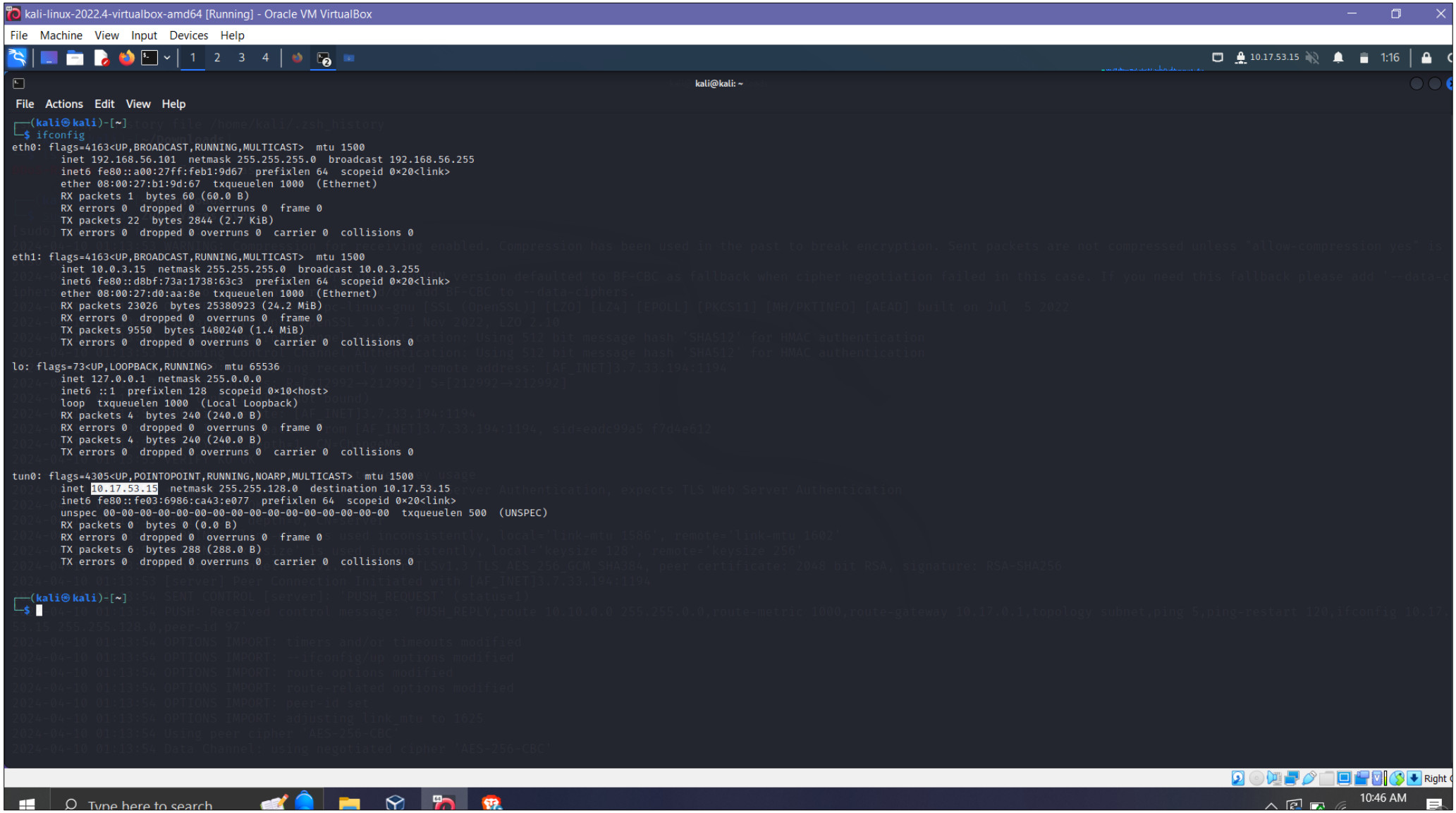
### Task 2. A Bit of Background on Linux

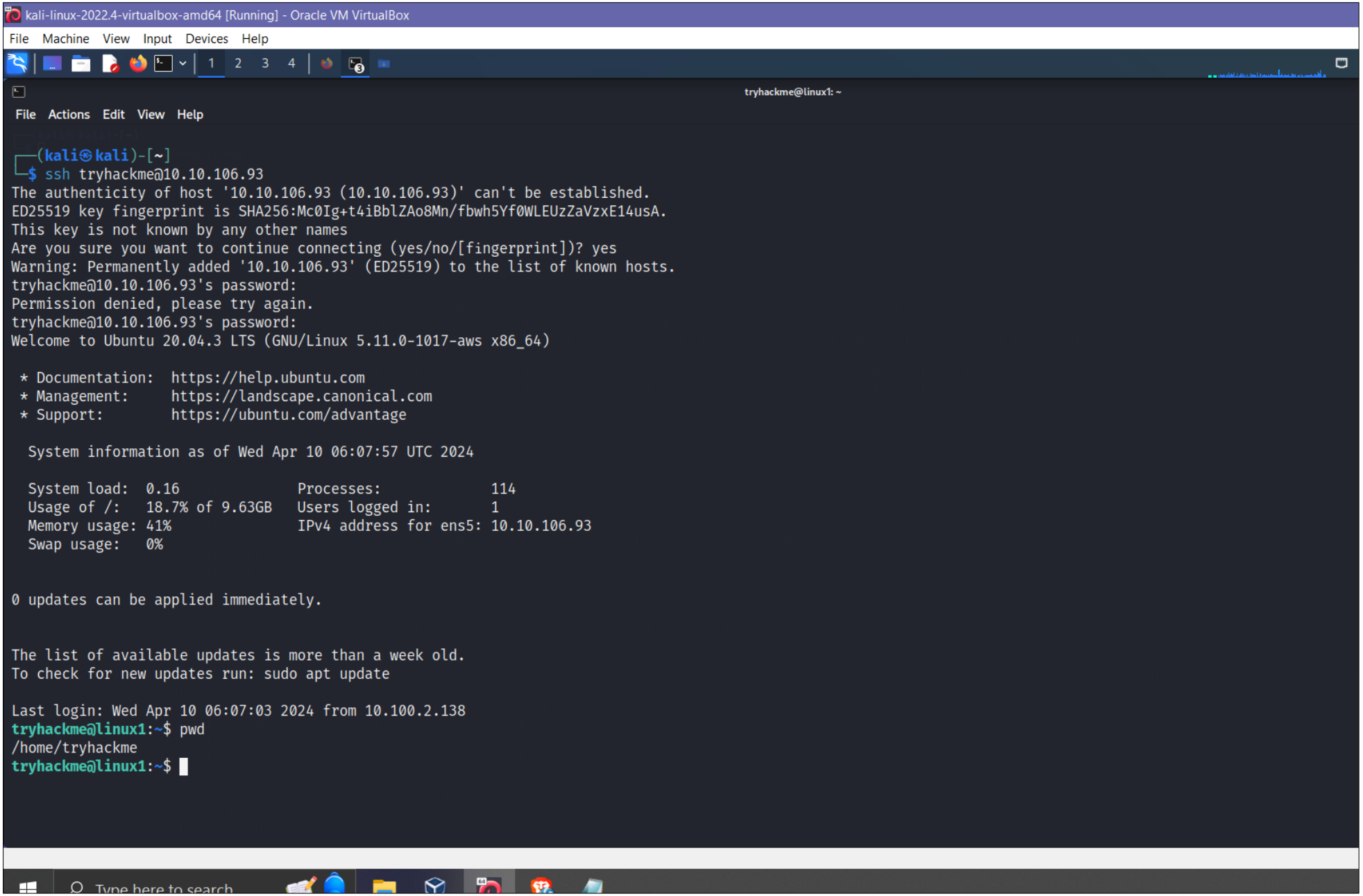


## Task 3. Interacting With Your First Linux Machine

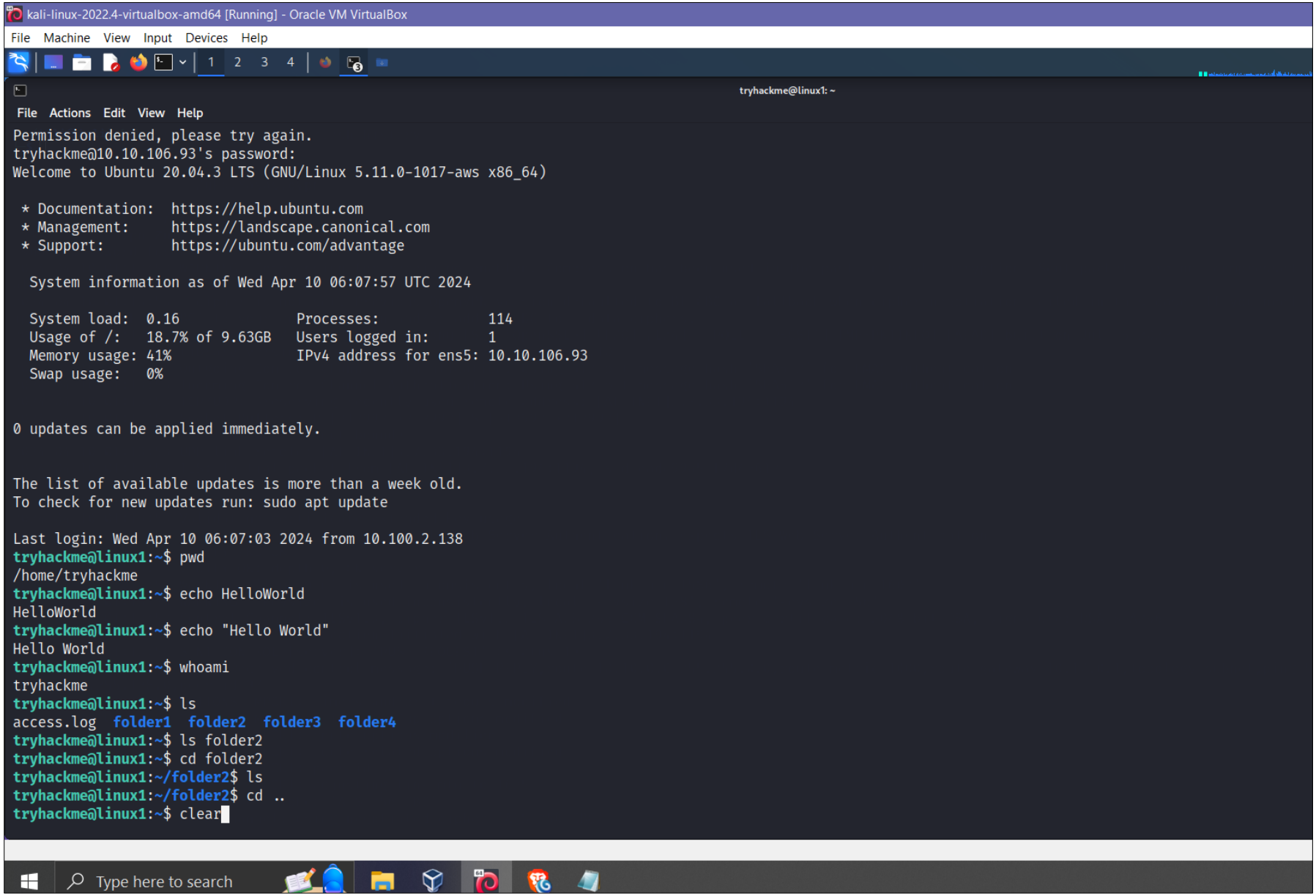



kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Downloads
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali)-[~/Downloads]
$ ls
DDoS-Ripper-main.zip Zuko.Yasas.ovpn
(kali㉿kali)-[~/Downloads]
$ 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

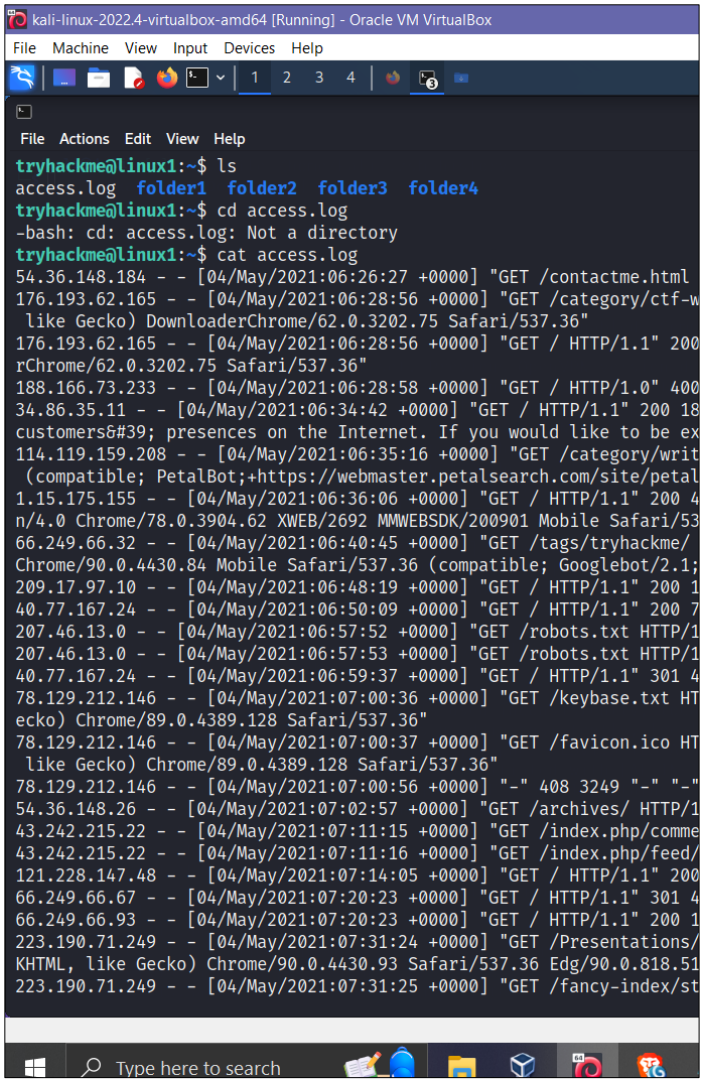

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.56.101 netmask 255.255.255.0 broadcast 192.168.56.255
inet6 fe80::a00:27ff:feb1:9d67 prefixlen 64 scopeid 0×20<link>
ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
RX packets 1 bytes 60 (60.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 22 bytes 2844 (2.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.3.15 netmask 255.255.255.0 broadcast 10.0.3.255
inet6 fe80::d8bf:73a:1738:63c3 prefixlen 64 scopeid 0×20<link>
ether 08:00:27:d0:aa:8e txqueuelen 1000 (Ethernet)
RX packets 23026 bytes 25380923 (24.2 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 9550 bytes 1480240 (1.4 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 4 bytes 240 (240.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4 bytes 240 (240.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
inet 10.17.53.15 netmask 255.255.128.0 destination 10.17.53.15
inet6 fe80::fe03:6986:ca43:e077 prefixlen 64 scopeid 0×20<link>
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 6 bytes 288 (288.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(kali㉿kali)-[~]
$
Type here to search
10:46 AM

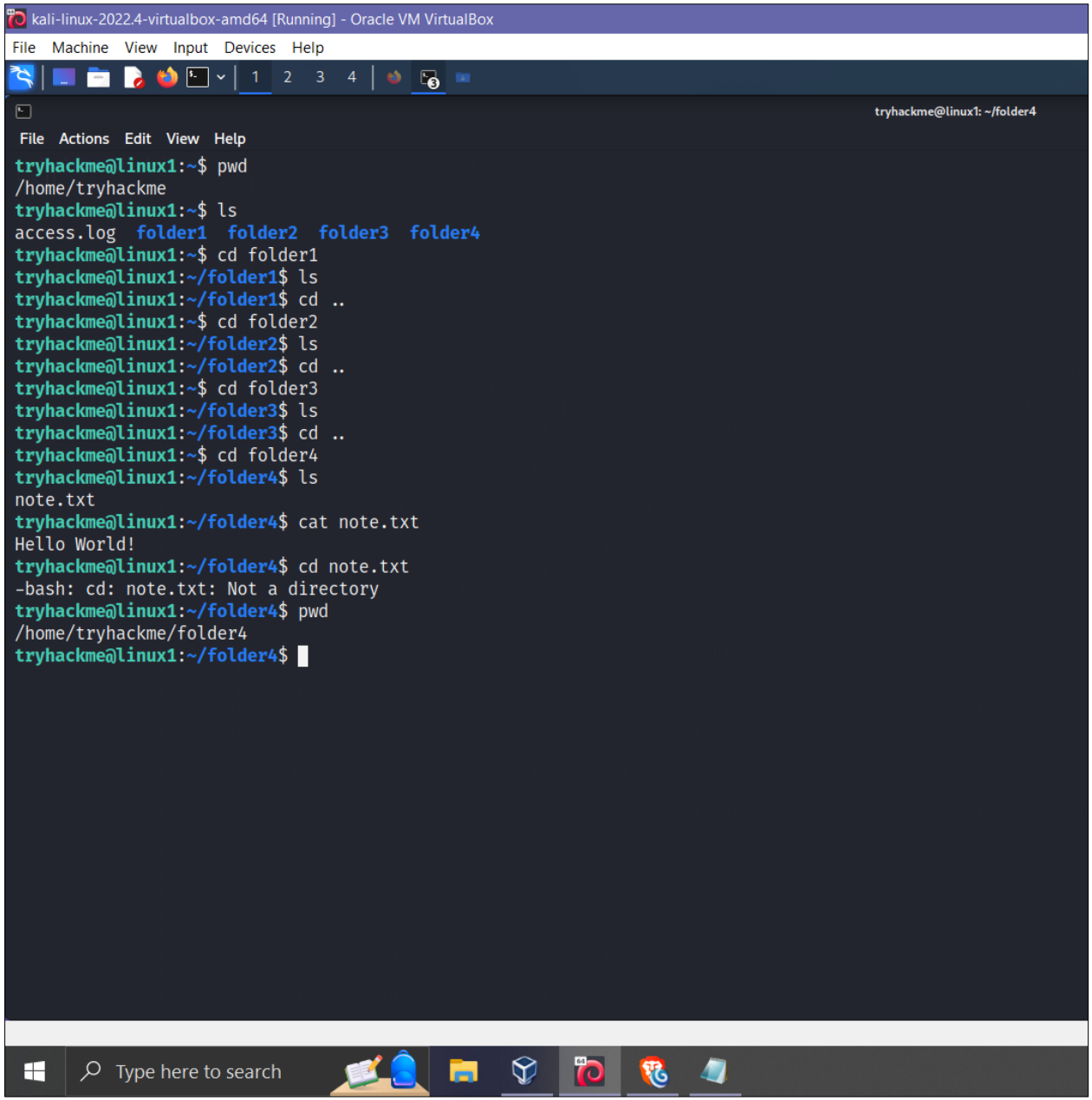

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
tryhackme@linux1: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ ssh tryhackme@10.10.106.93
The authenticity of host '10.10.106.93 (10.10.106.93)' can't be established.
ED25519 key fingerprint is SHA256:Mc0Ig+t4iBblZAo8Mn/fbwh5Yf0WLEUzZaVzxE14usA.
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:~$
Type here to search

## Task 4. Running Your First few Commands

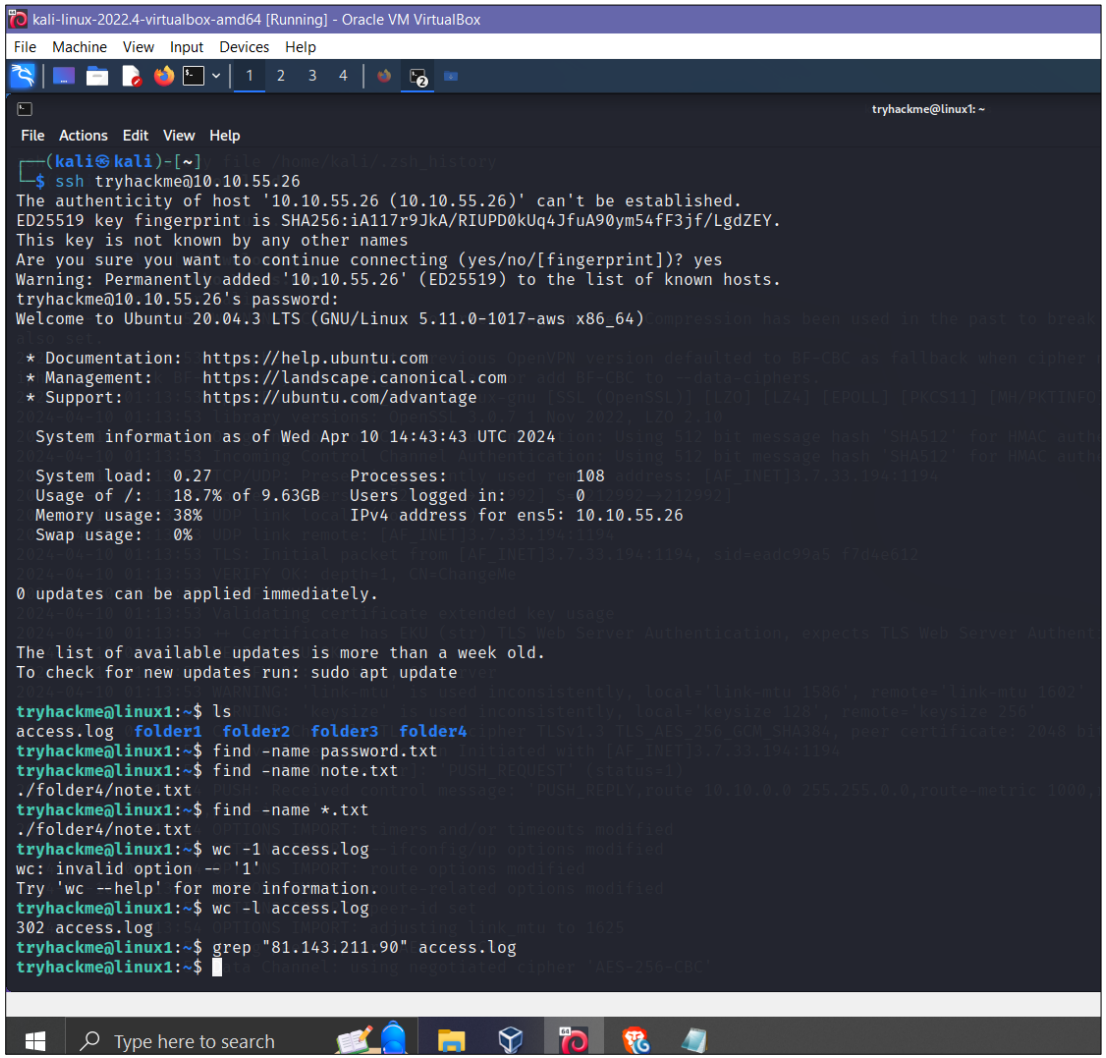


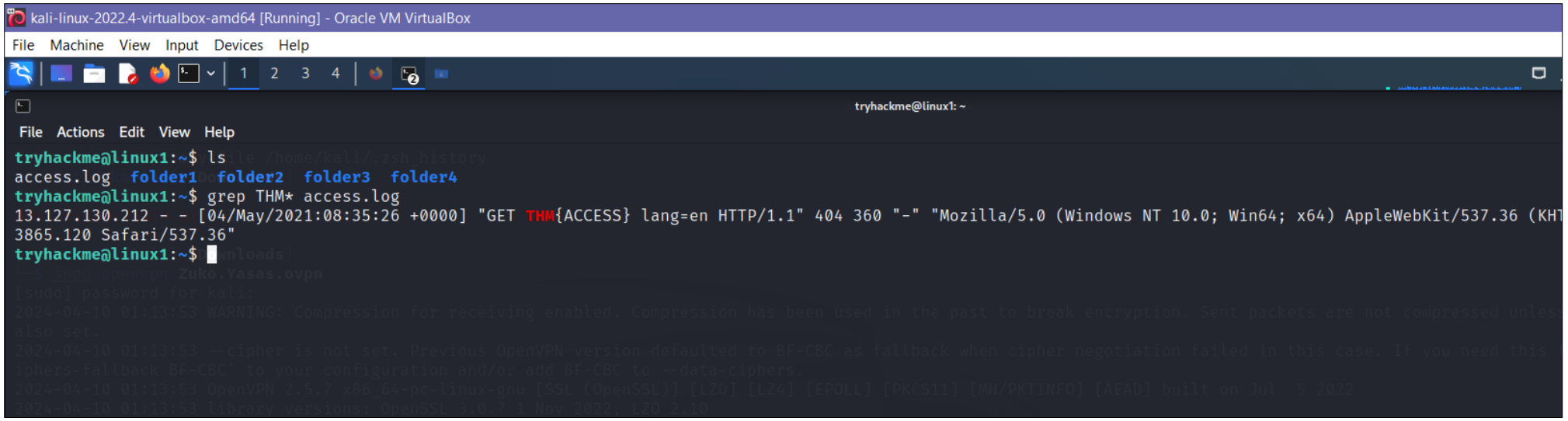
# Task 5. Interacting With the Filesystem!



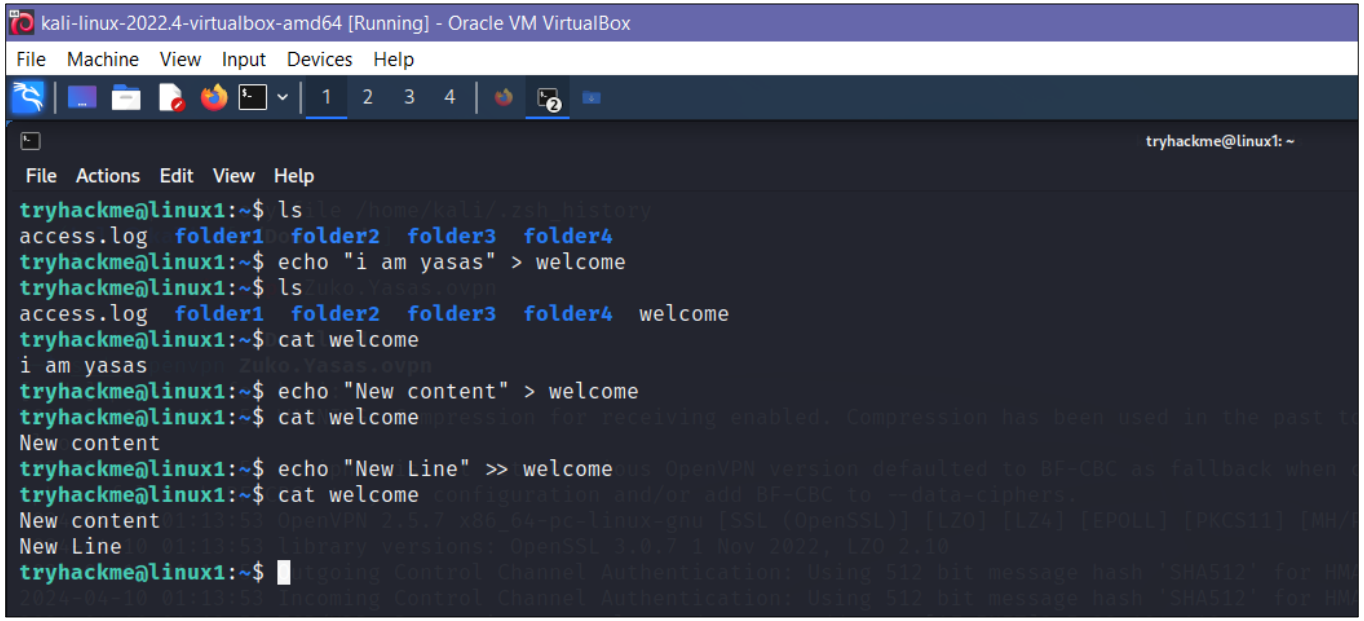

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
tryhackme@linux1: ~/folder4
File Actions Edit View Help
tryhackme@linux1:~$ pwd
/home/tryhackme
tryhackme@linux1:~$ ls
access.log folder1 folder2 folder3 folder4
tryhackme@linux1:~$ cd folder1
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$
Type here to search

# Task 6. Searching for Files

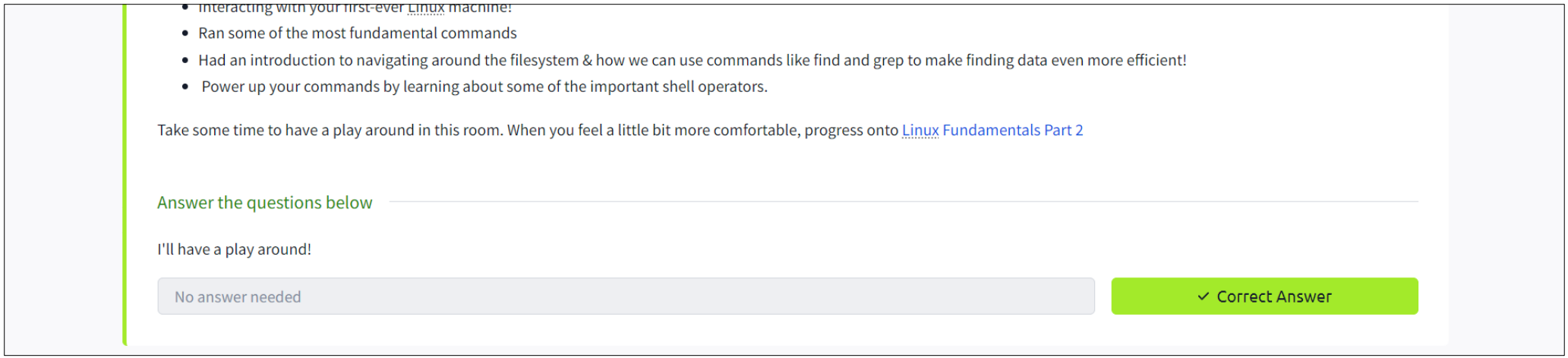




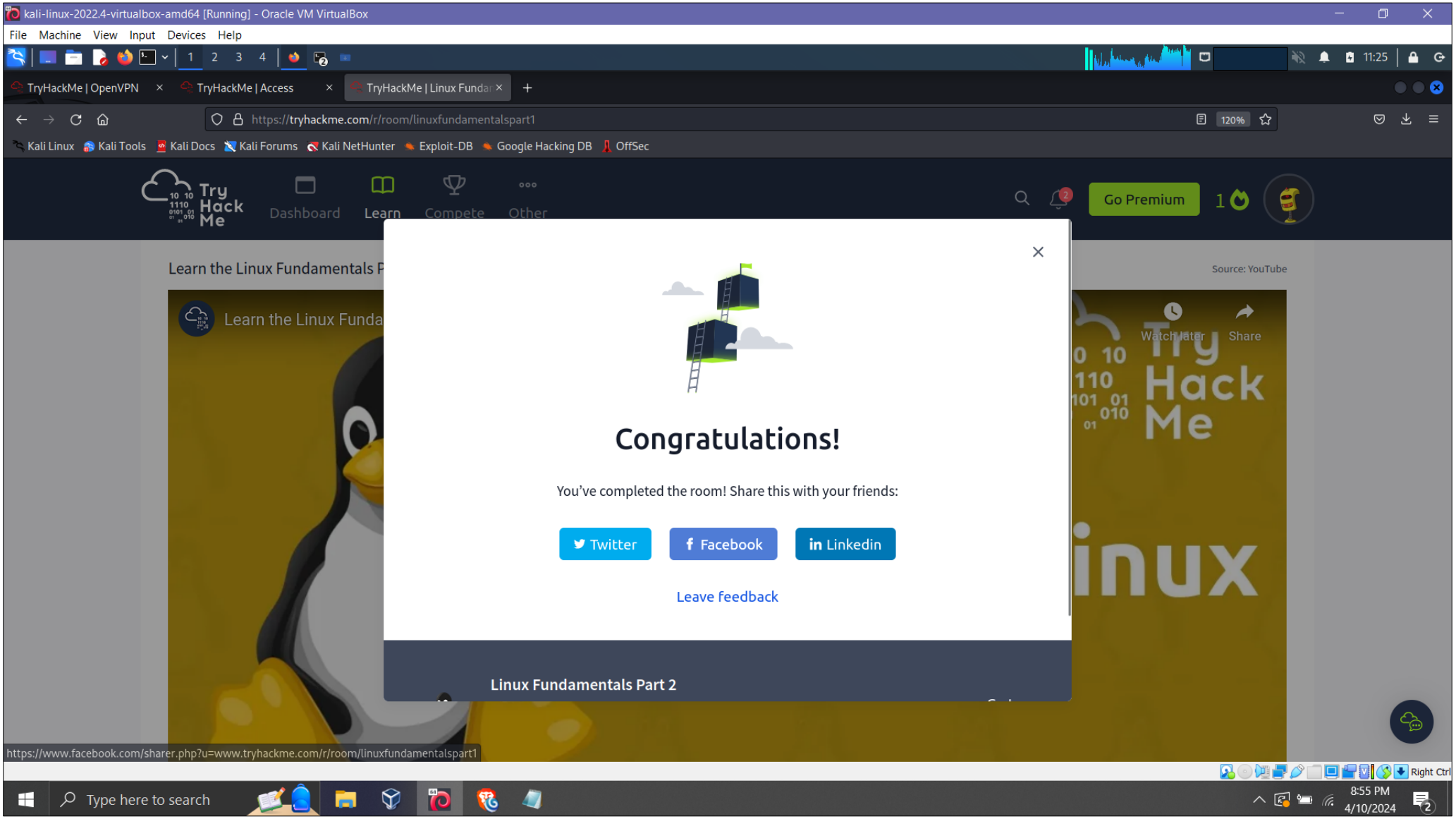

## Task 7. An Introduction to Shell Operators



## Task 8. Conclusions & Summaries

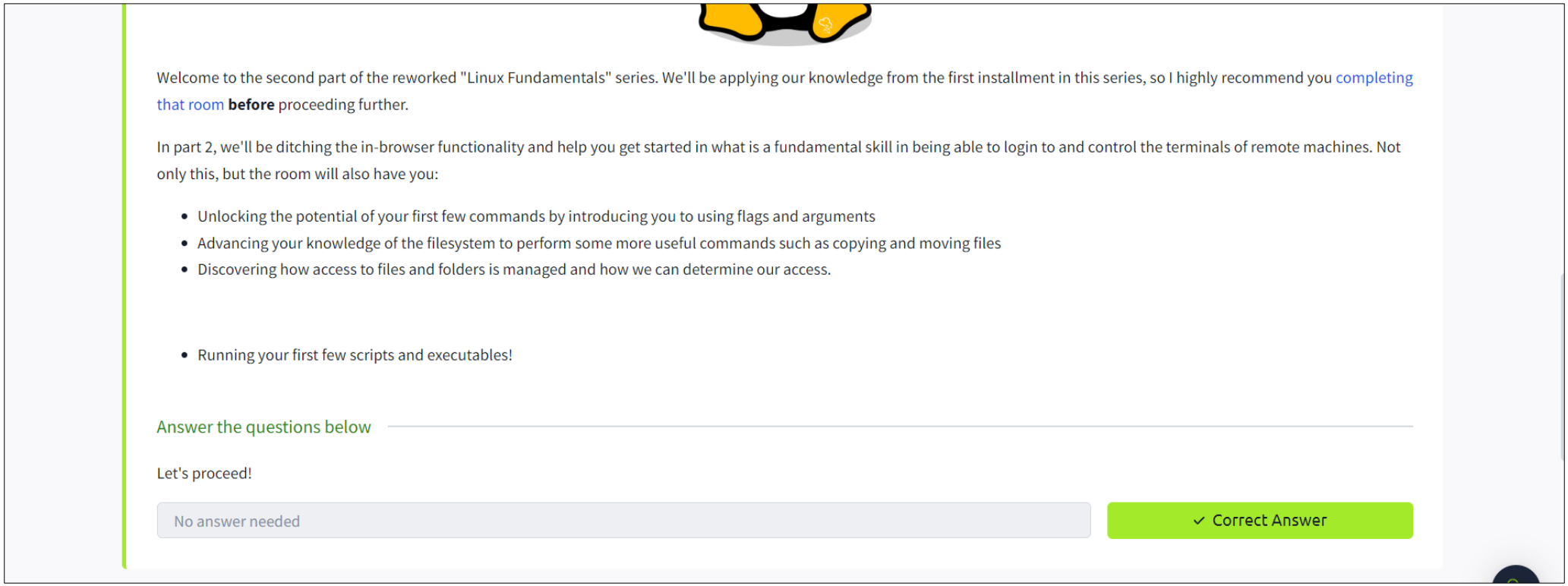



## Task 9. Linux Fundamentals Part 2


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
TryHackMe | OpenVPN
TryHackMe | Access
TryHackMe | Linux Fundar
https://tryhackme.com/r/room/linuxfundamentalspart1
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
Learn the Linux Fundamentals P
Source: YouTube
Learn the Linux Funda
Watch later
Share
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

# 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!

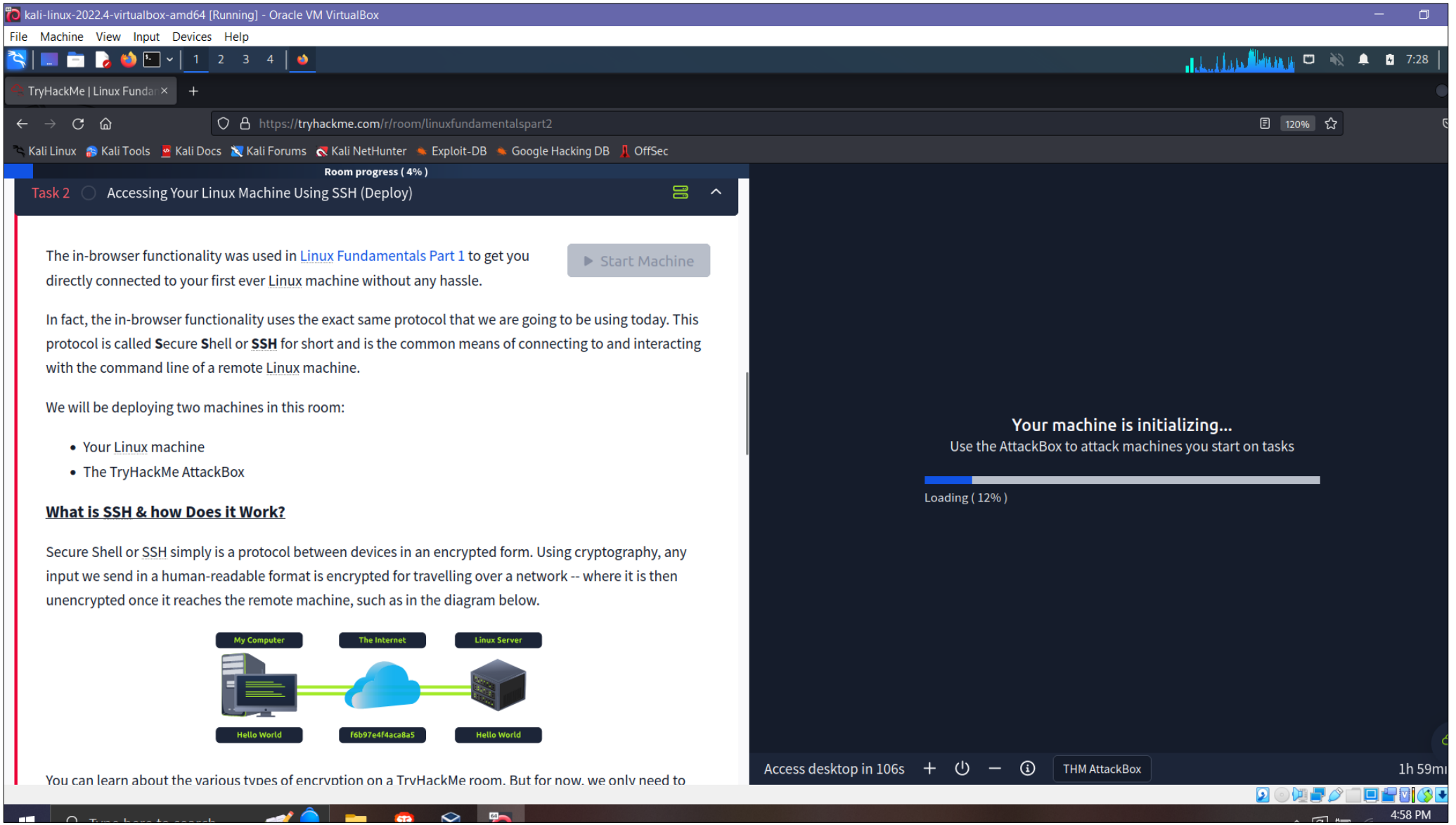
Answer the questions below

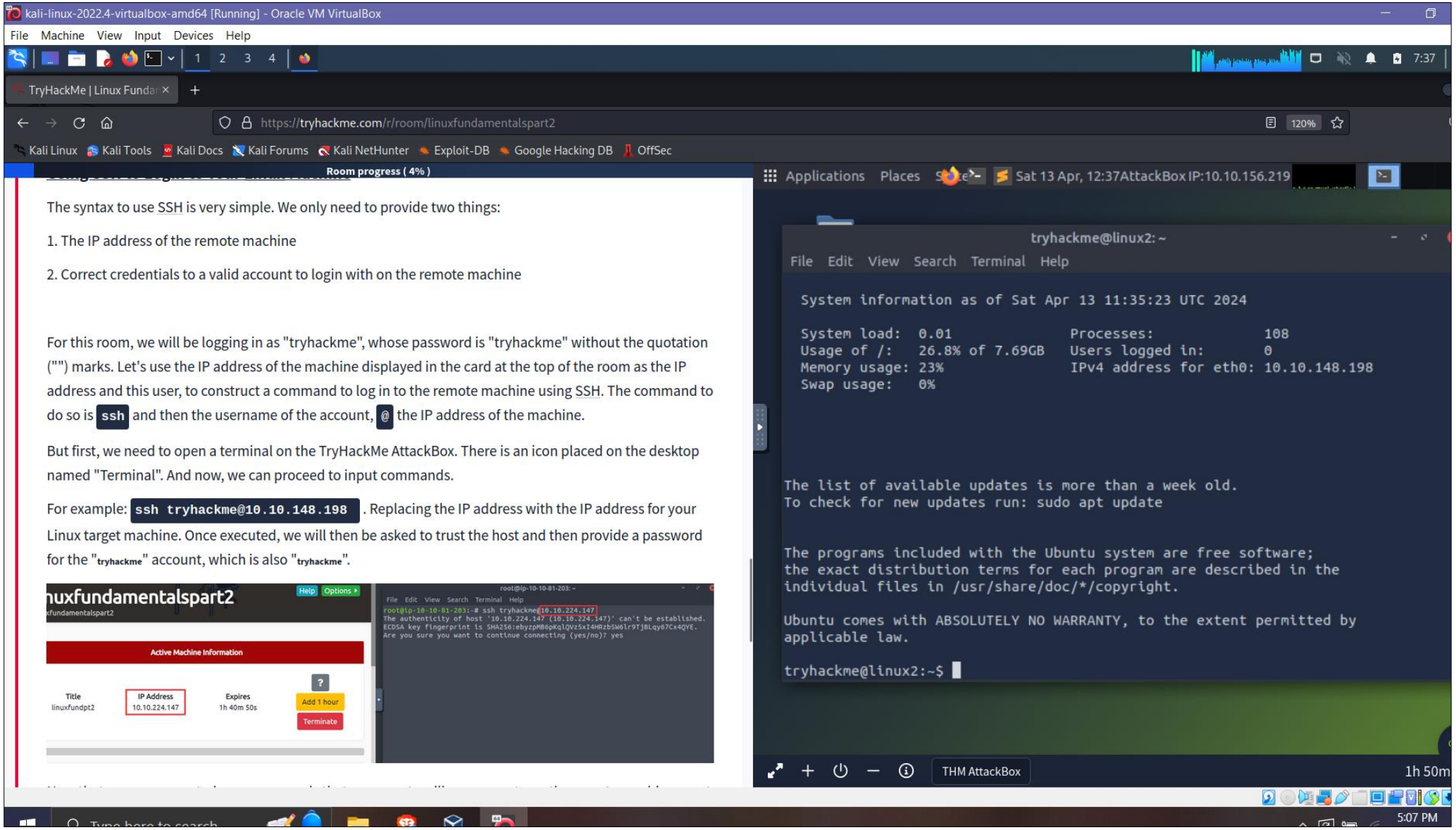
Let's proceed!

No answer needed

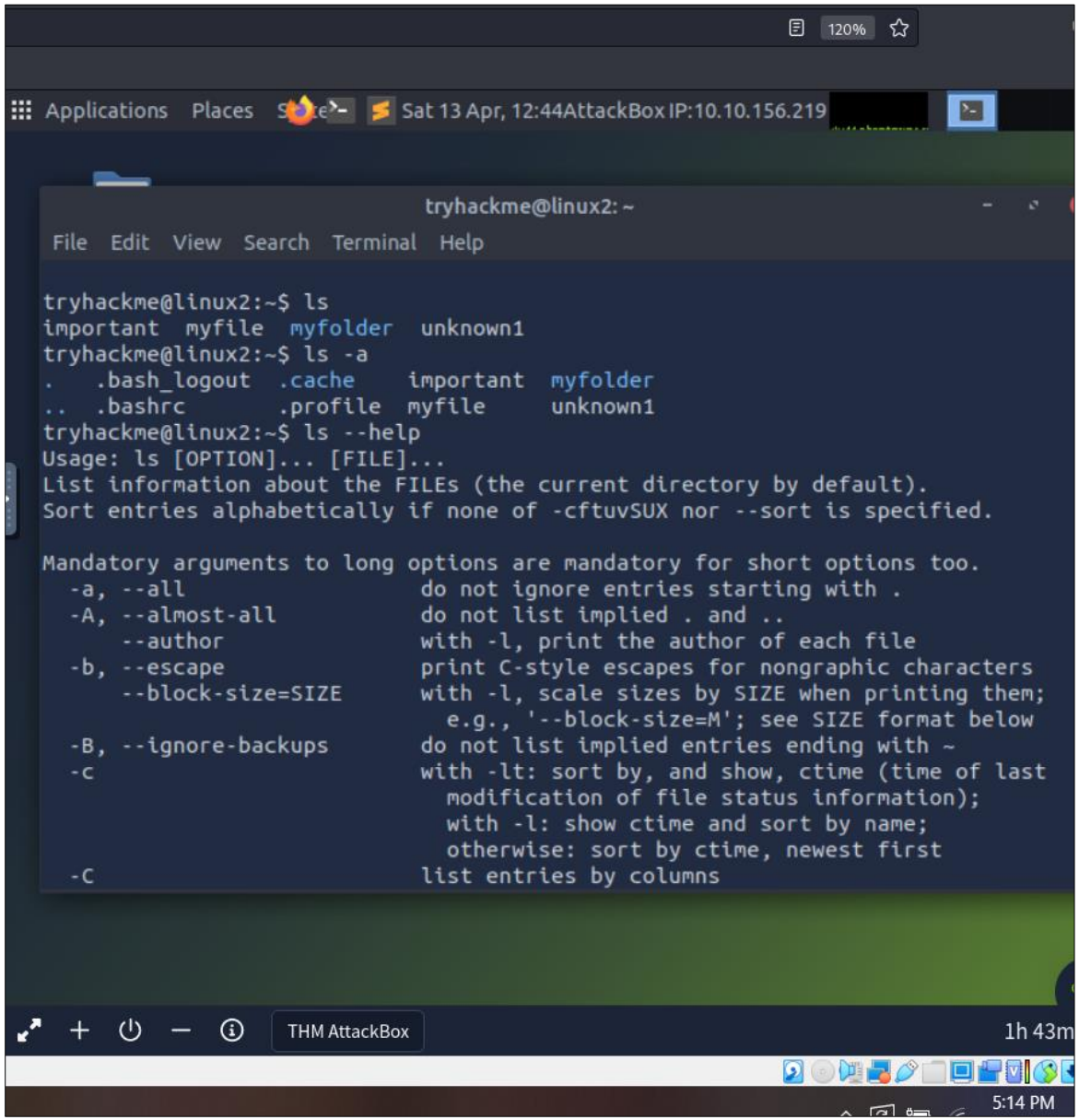
✓ Correct Answer

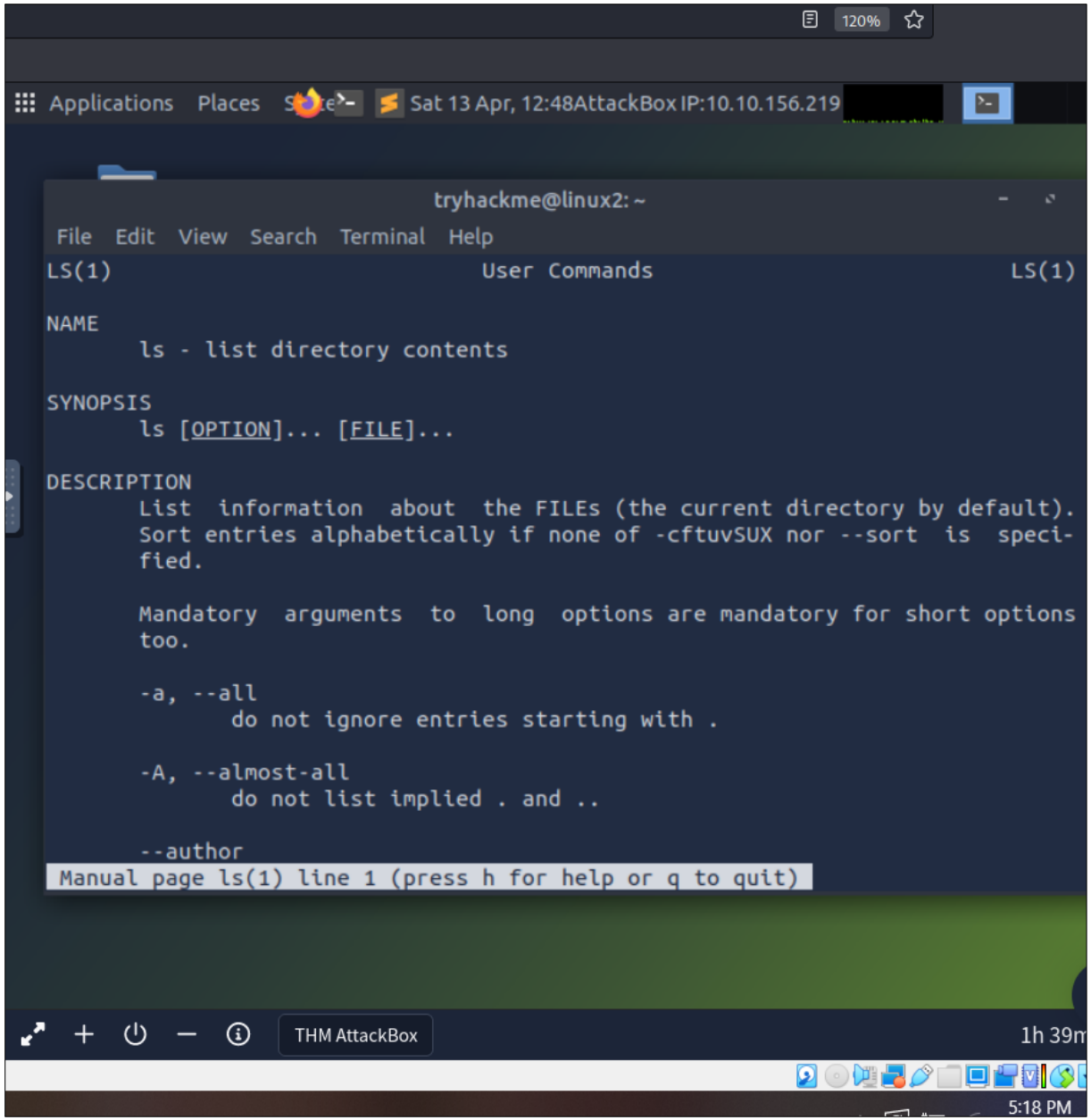
# Task 2. Accessing Your Linux Machine Using SSH (Deploy)



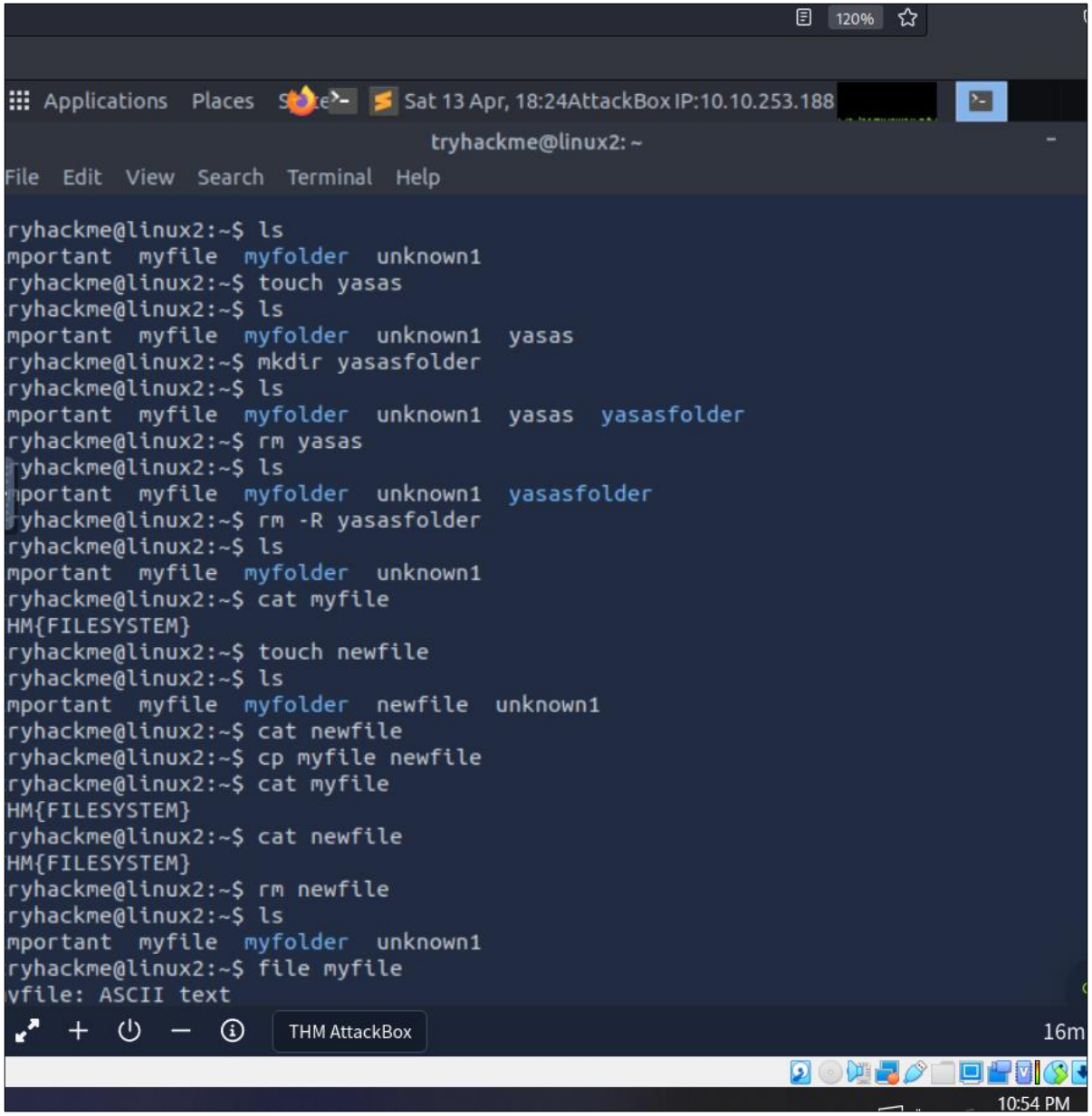

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
TryHackMe | Linux Fundar
https://tryhackme.com/r/room/linuxfundamentalspart2
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Room progress ( 4% )
The 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".
Active Machine Information
Title
linuxfundpt2
IP Address
10.10.224.147
Expires
1h 40m 50s
Add 1 hour
Terminate
The authenticity of host '10.10.224.147 (10.10.224.147)' can't be established.
ECDSA key fingerprint is SHA256:ebyzpMB6pKqlQVz5xI4HRzbSW6lr9TjBLqy67Cx4QYE.
Are you sure you want to continue connecting (yes/no)? yes
Applications Places Sat 13 Apr, 12:37 AttackBox IP:10.10.156.219
tryhackme@linux2: ~
File Edit View Search Terminal Help
System information as of Sat Apr 13 11:35:23 UTC 2024
System load: 0.01 Processes: 108
Usage of /: 26.8% of 7.69GB Users logged in: 0
Memory usage: 23% IPv4 address for eth0: 10.10.148.198
Swap usage: 0%
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:~$
THM AttackBox
1h 50m
5:07 PM

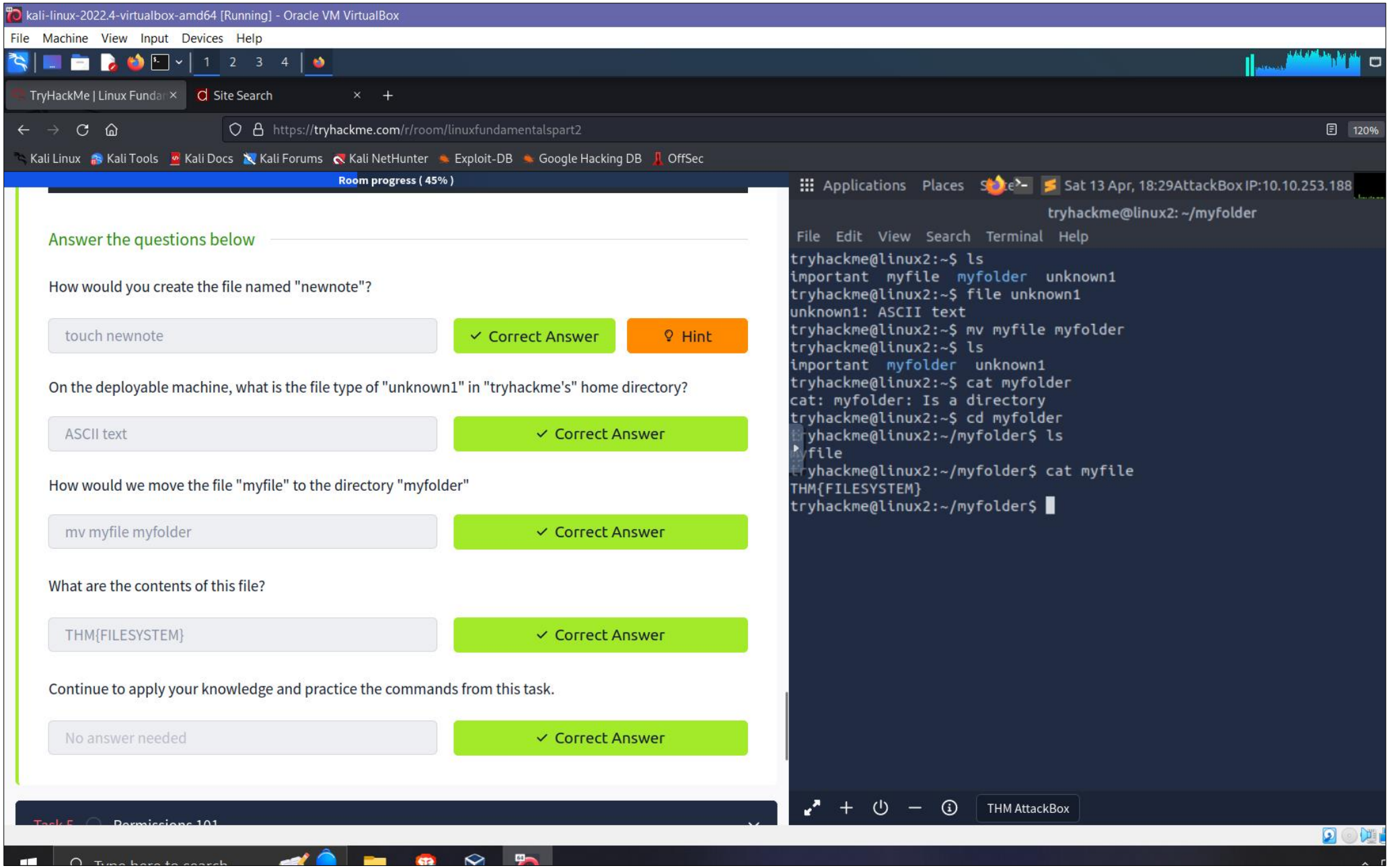
## Task 3. Introduction to Flags and Switches



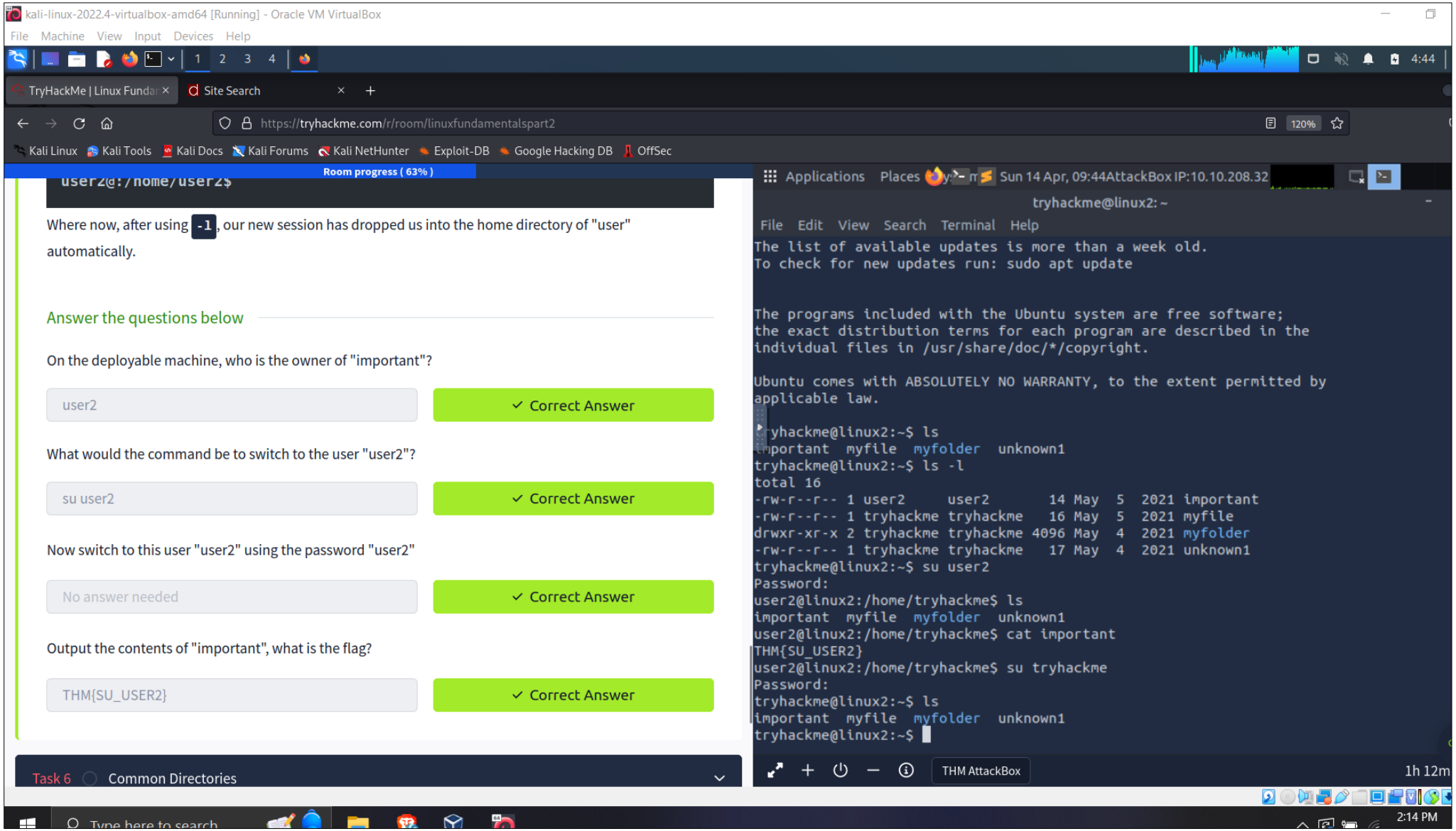

120%
Applications
Places
Sat 13 Apr, 12:48
AttackBox IP:10.10.156.219
tryhackme@linux2: ~
File Edit View Search Terminal Help
LS(1) User Commands LS(1)
NAME
ls - list directory contents
SYNOPSIS
ls [OPTION]... [FILE]...
DESCRIPTION
List information about the FILEs (the current directory by default).
Sort entries alphabetically if none of -cftuvSUX nor --sort is speci-
fied.
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

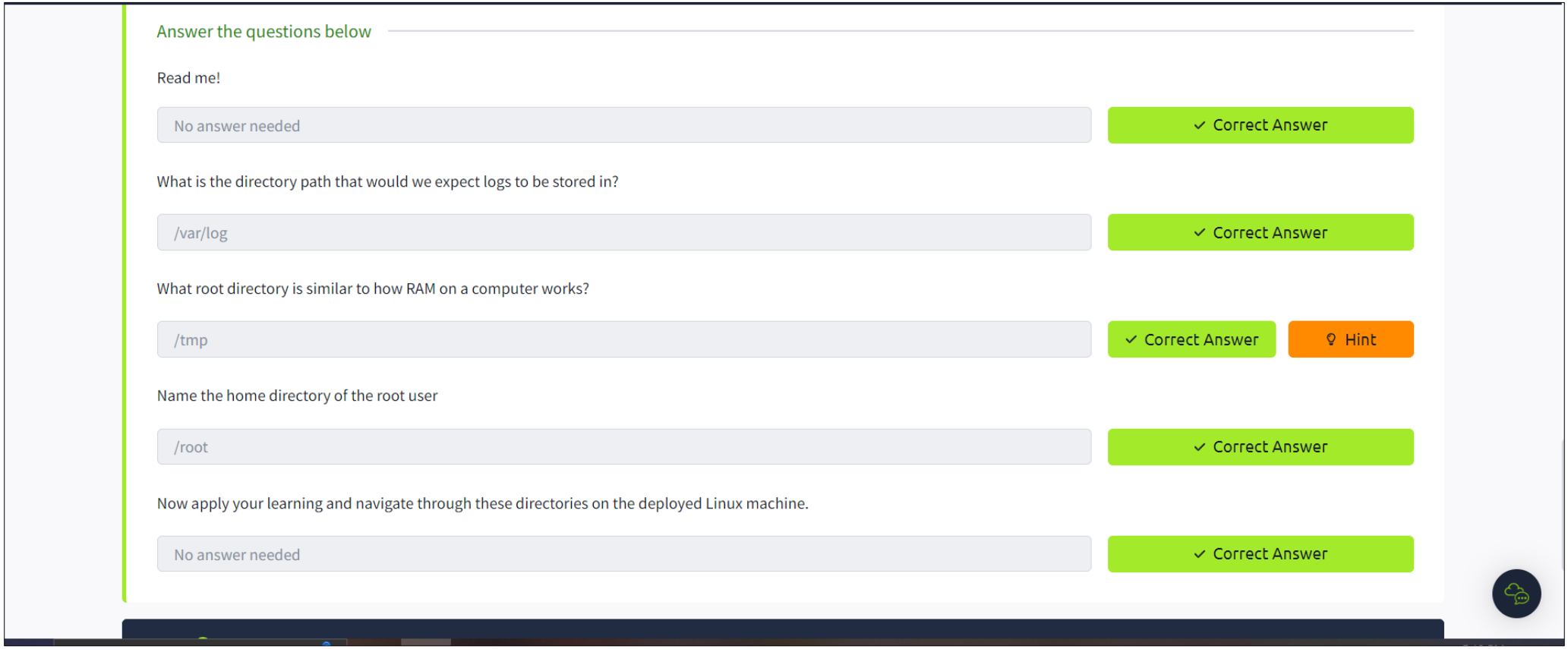



kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
TryHackMe | Linux Fundar
Site Search
https://tryhackme.com/r/room/linuxfundamentalspart2
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Room progress ( 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
Applications Places
Sat 13 Apr, 18:29
AttackBox IP:10.10.253.188
tryhackme@linux2: ~/myfolder
File Edit View Search Terminal Help
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$
THM AttackBox

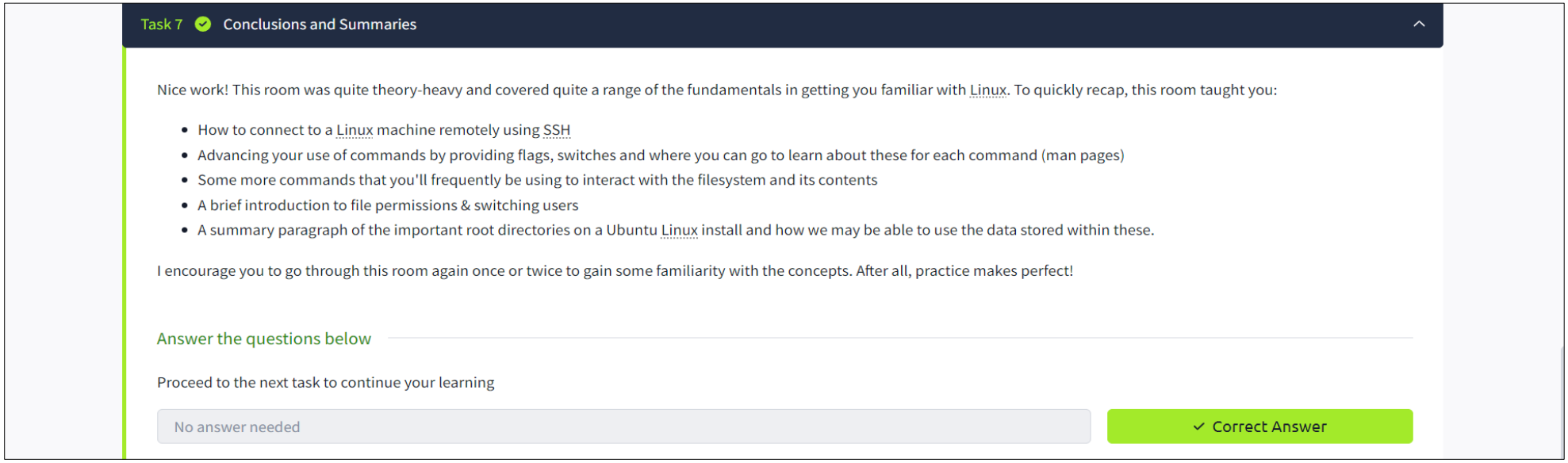
# Task 5. Permissions 101



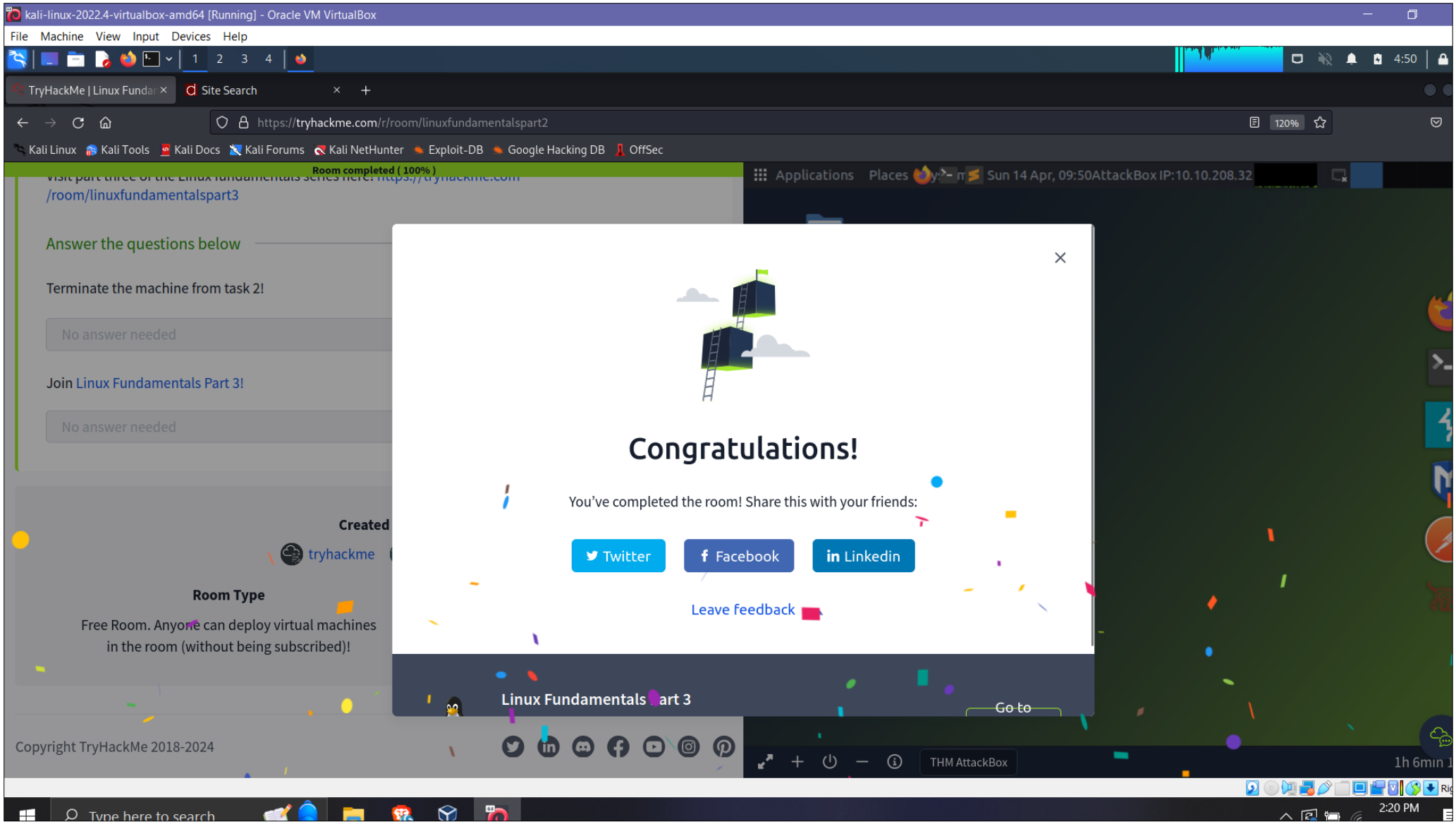
## Task 6. Common Directories



## Task 7. Conclusions and Summaries

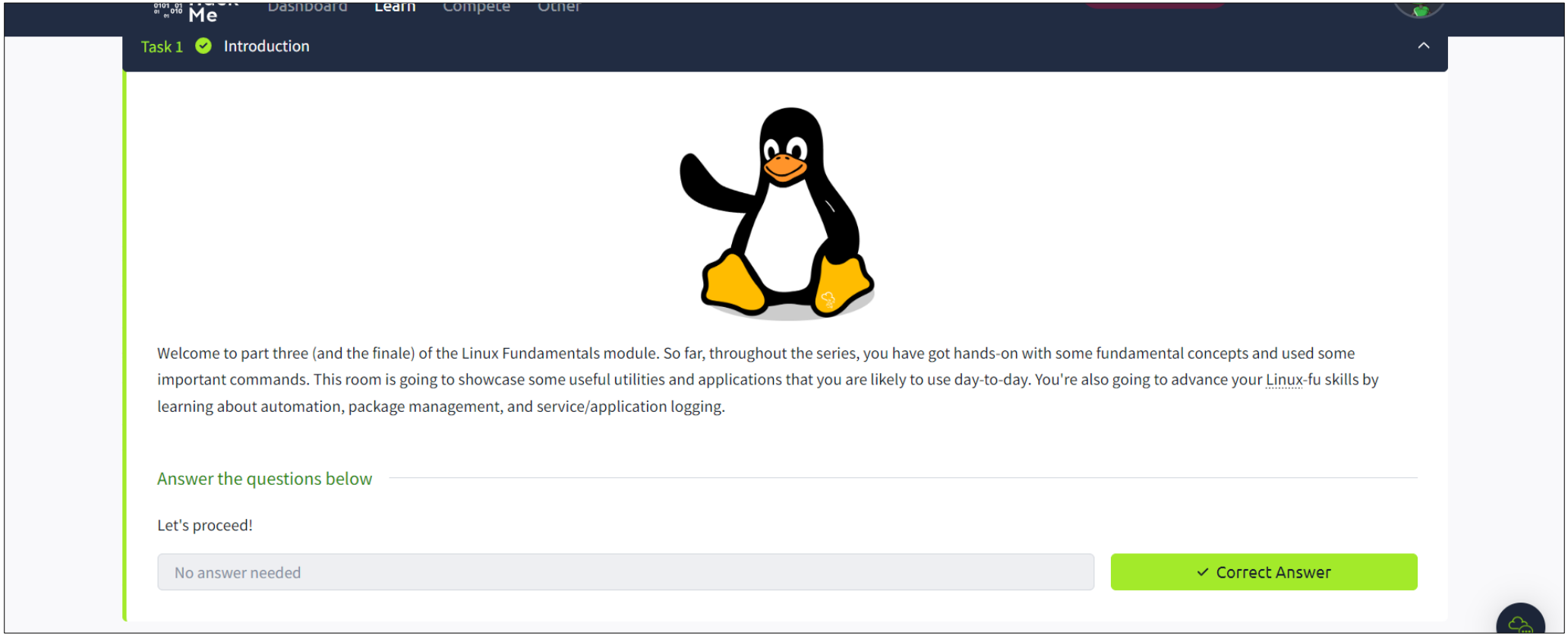



## Task 8. Linux Fundamentals Part 3

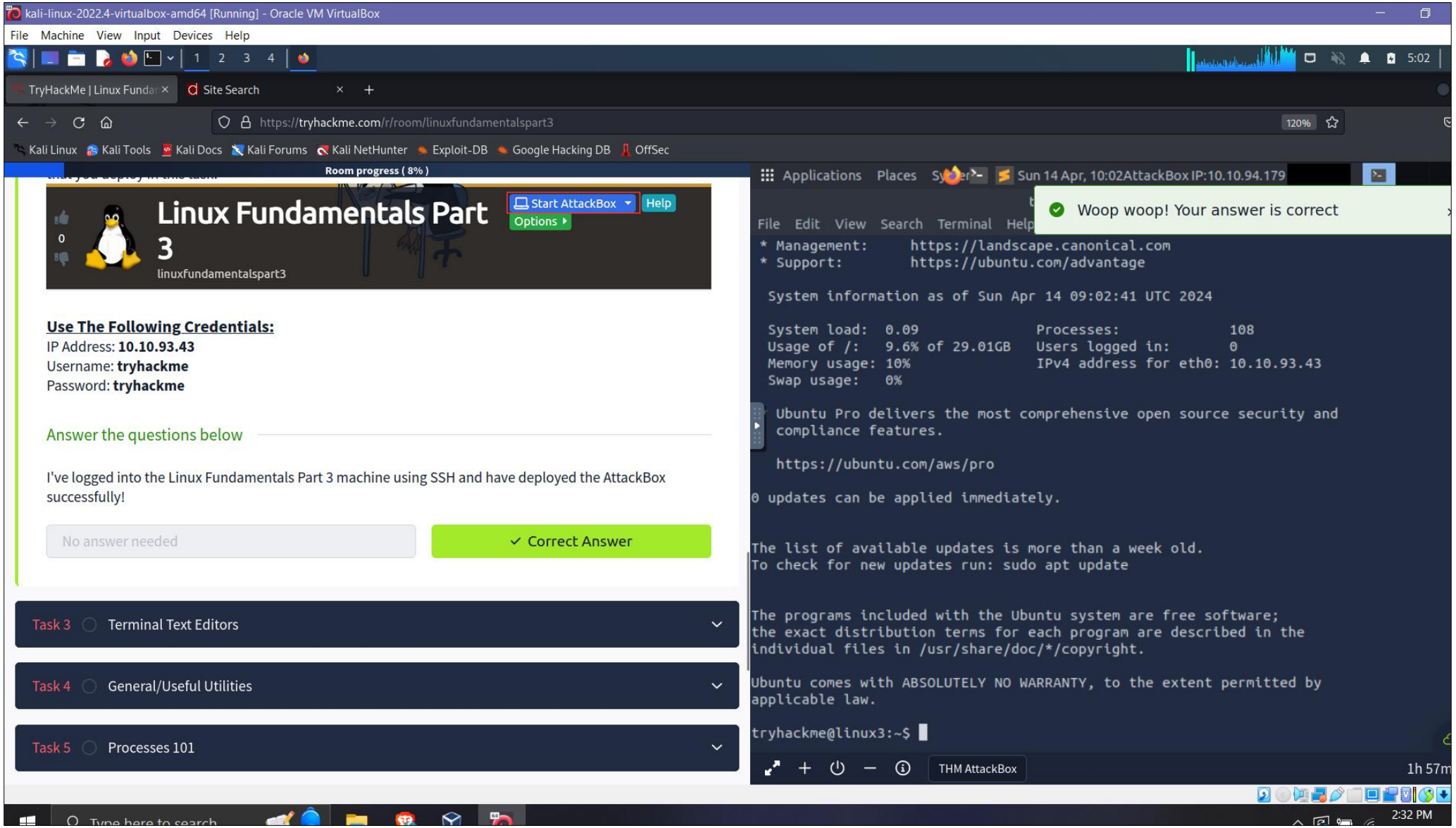

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
TryHackMe | Linux Fundar
Site Search
https://tryhackme.com/r/room/linuxfundamentalspart2
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Room completed ( 100% )
/room/linuxfundamentalspart3
Answer the questions below
Terminate the machine from task 2!
No answer needed
Join Linux Fundamentals Part 3!
No answer needed
Created
tryhackme
Room Type
Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!
Copyright TryHackMe 2018-2024
Congratulations!
You've completed the room! Share this with your friends:
Twitter
Facebook
Linkedin
Leave feedback
Linux Fundamentals Part 3
Go to
Applications Places Sun 14 Apr, 09:50AttackBox IP:10.10.208.32
THM AttackBox
1h 6min
Type here to search
2:20 PM

# Part 03

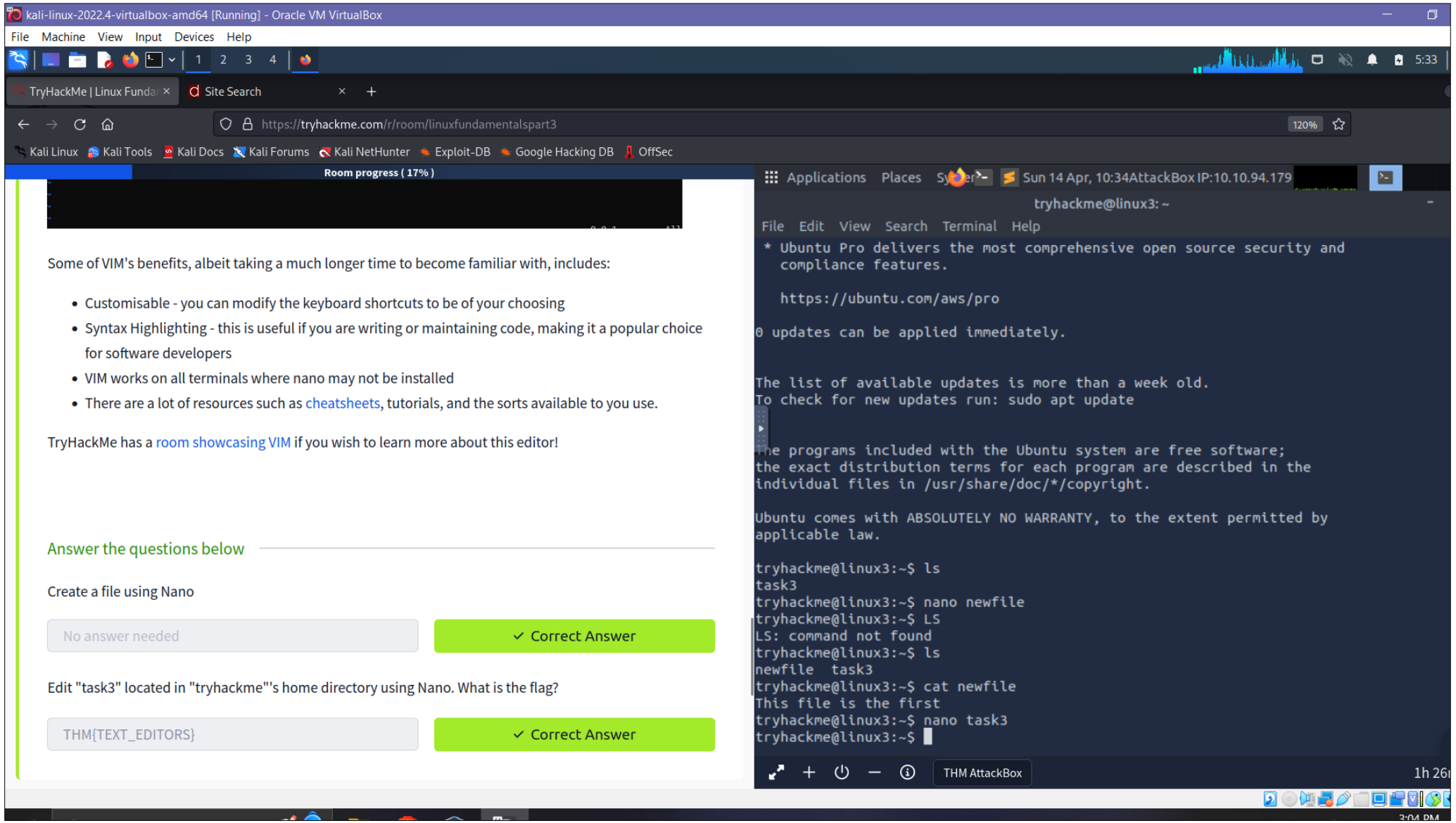
## Task 1. Introduction



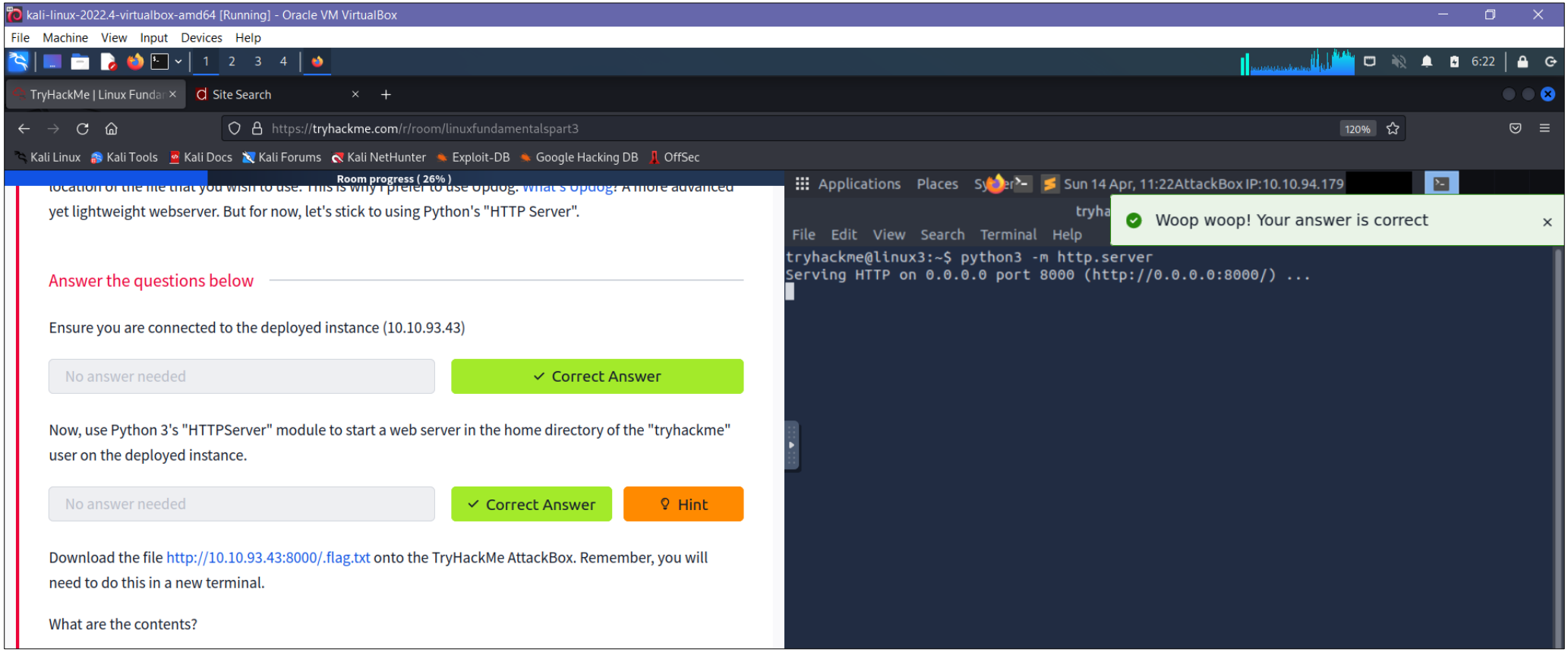
## Task 2. Deploy Your Linux Machine

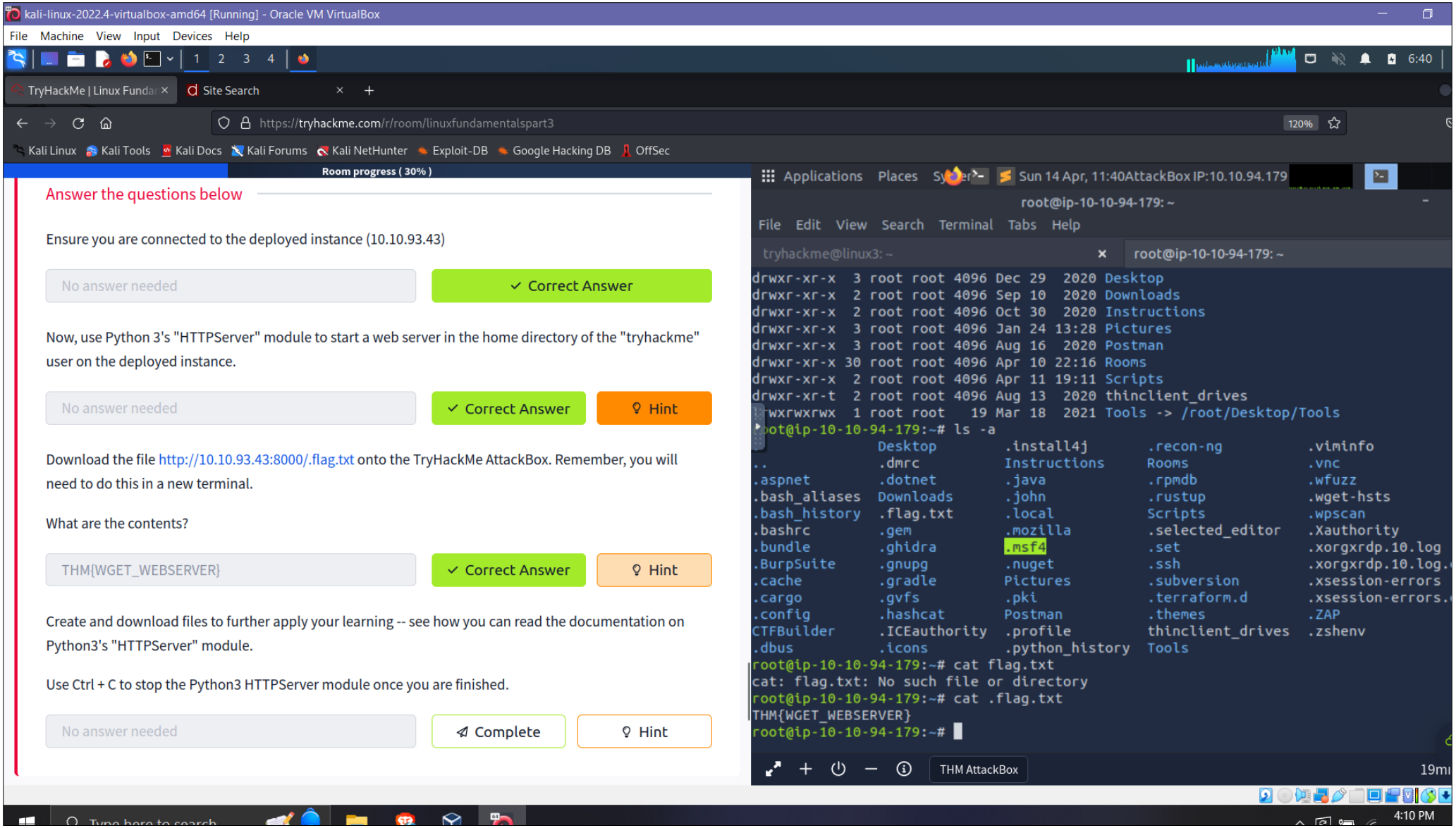


# Task 3. Terminal Text Editors

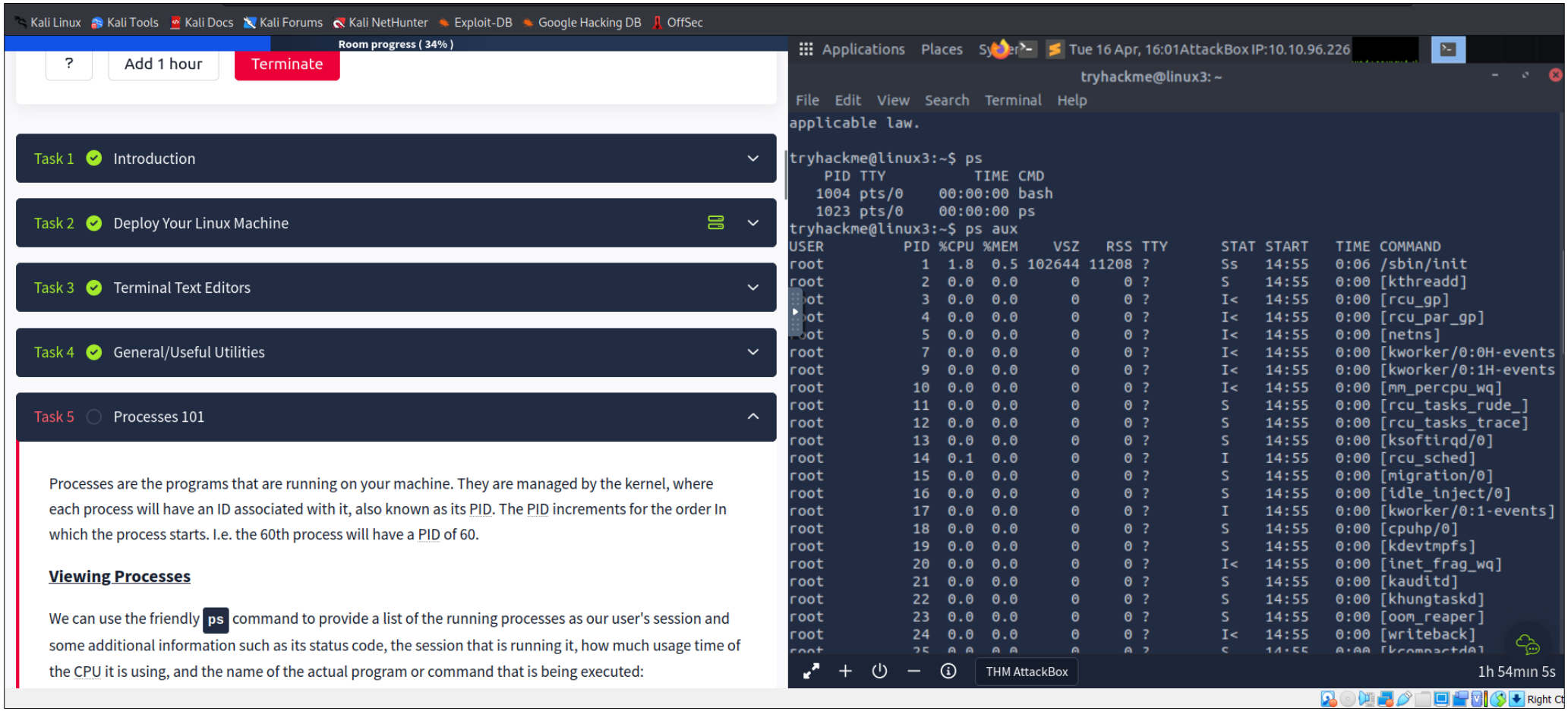


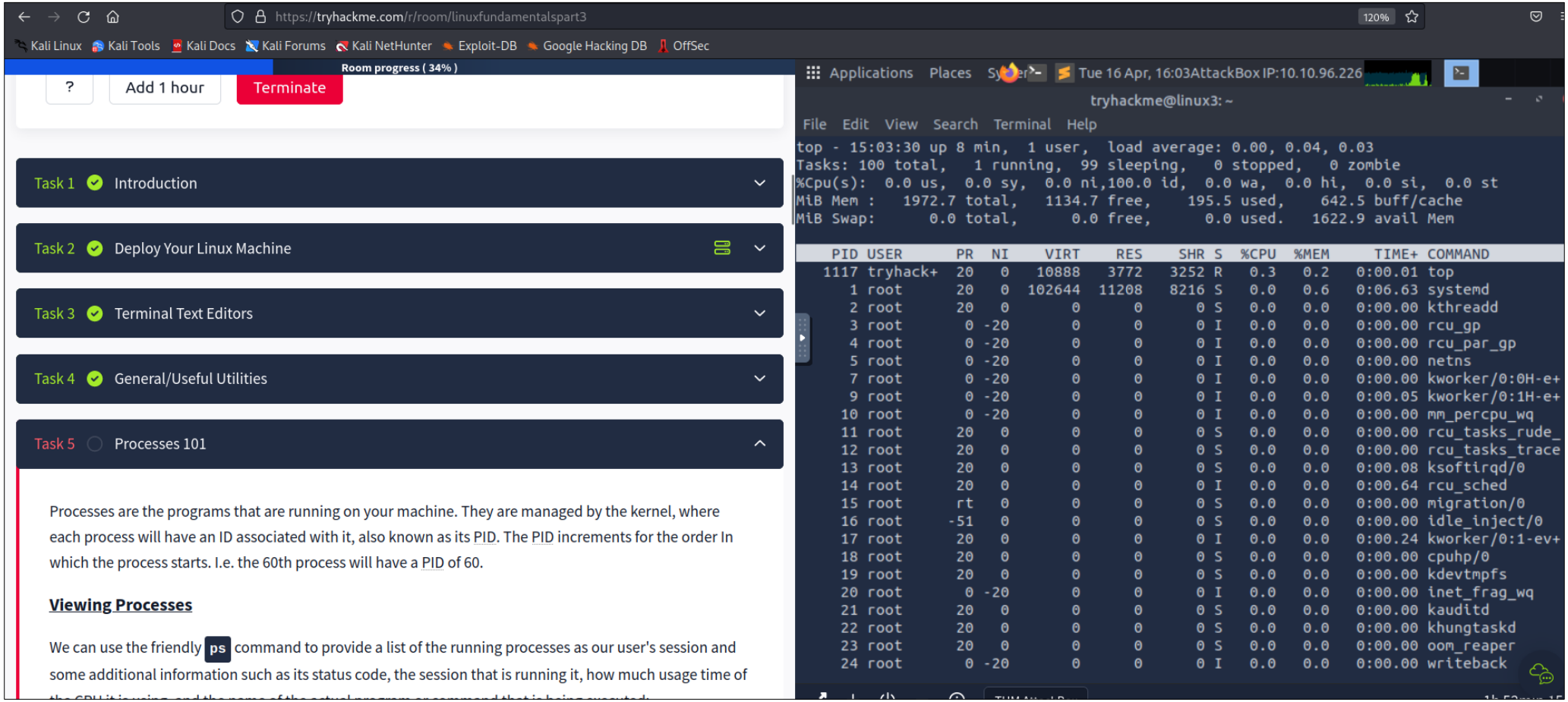
# Task 4. General/Useful Utilities

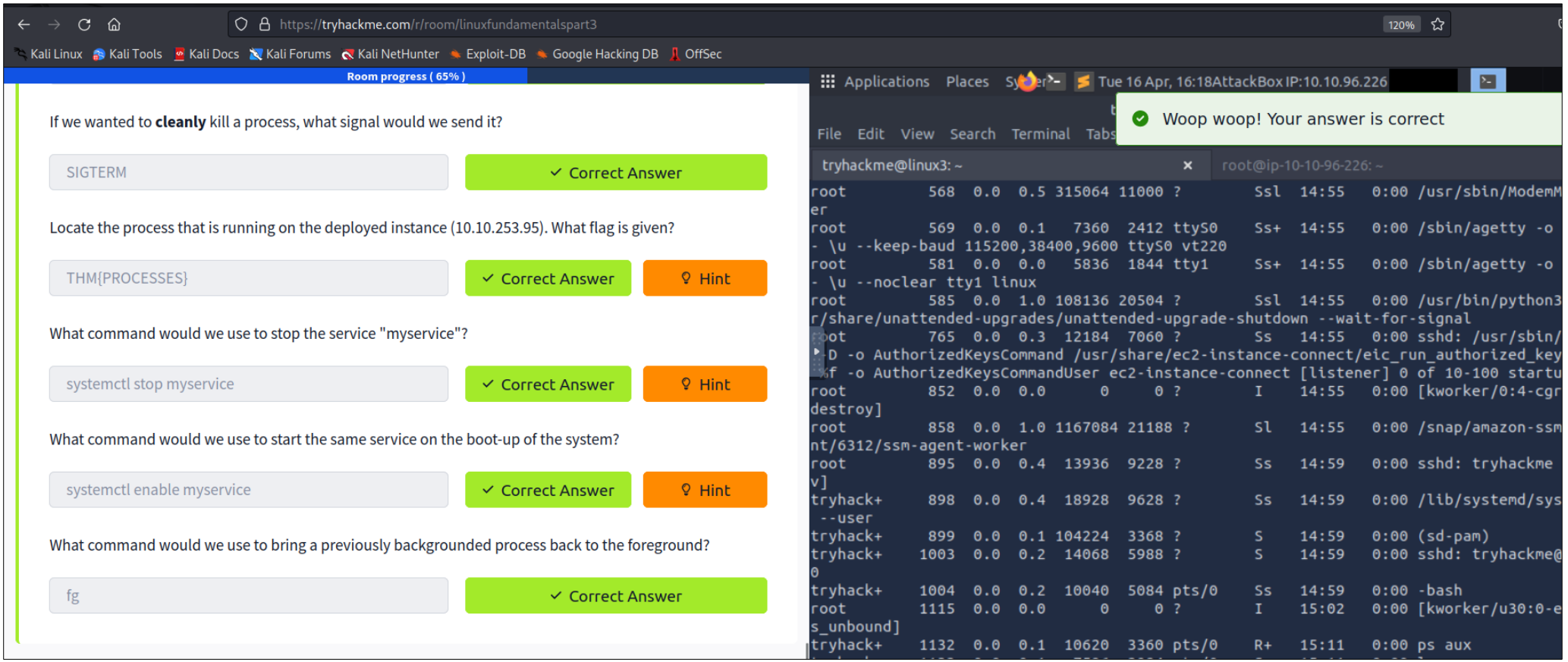



kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
TryHackMe | Linux Fundar
Site Search
https://tryhackme.com/r/room/linuxfundamentalspart3
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Room progress ( 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 Sun 14 Apr, 11:40 AttackBox IP:10.10.94.179
root@ip-10-10-94-179: ~
File Edit View Search Terminal Tabs Help
tryhackme@linux3: ~
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
rwxrwxrwx 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 .rpmdb .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 .xsession-errors
.cargo .gvfs .pki .terraform.d .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
4:10 PM

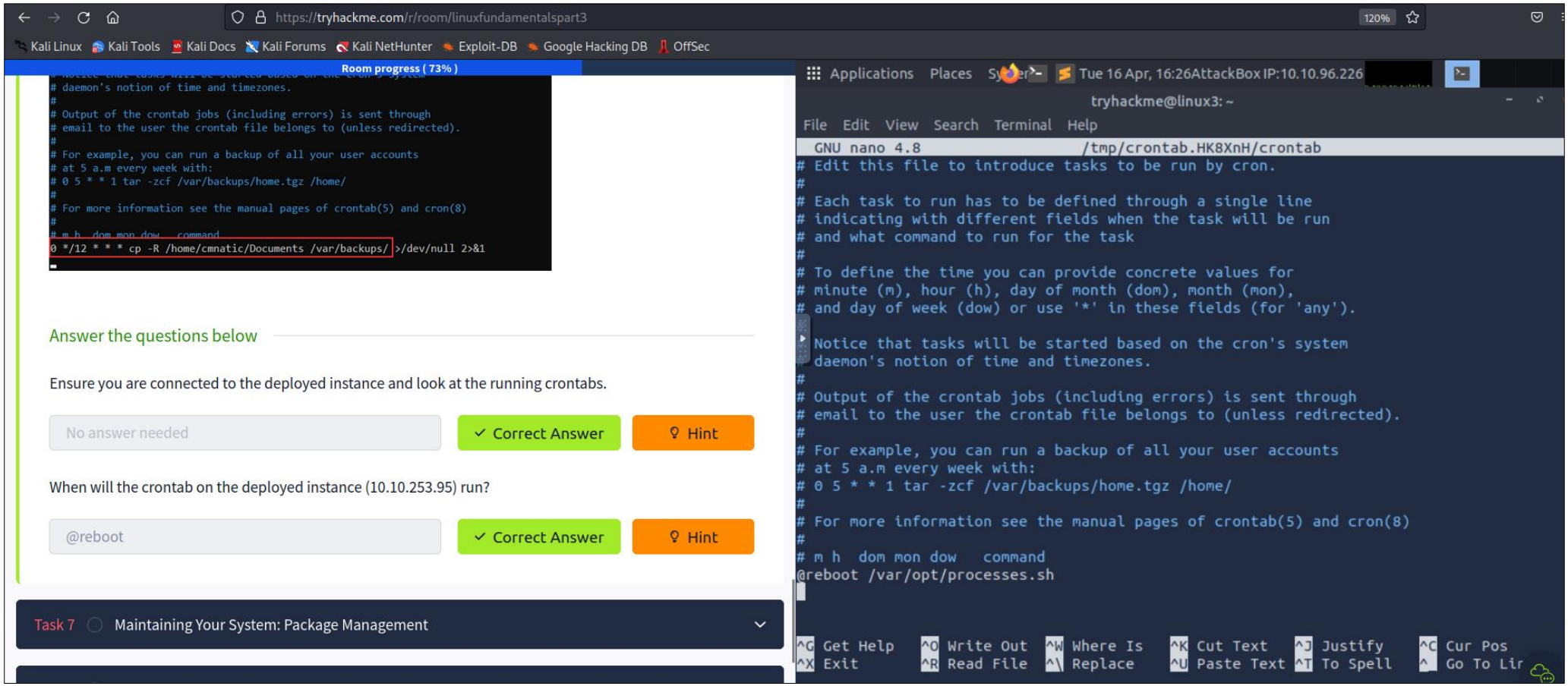
# Task 5. Processes 101



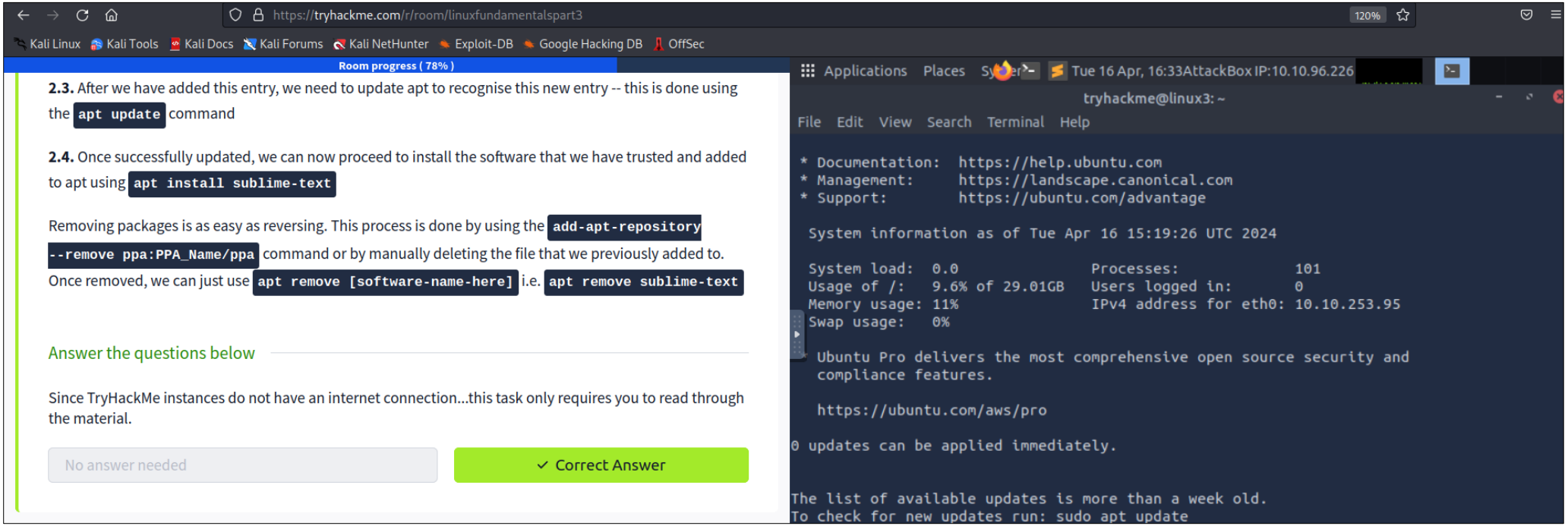

https://tryhackme.com/r/room/linuxfundamentalspart3
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Room progress ( 34% )
?
Add 1 hour
Terminate
Task 1 Introduction
Task 2 Deploy Your Linux Machine
Task 3 Terminal Text Editors
Task 4 General/Useful Utilities
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 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


https://tryhackme.com/r/room/linuxfundamentalspart3
120%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Room progress ( 65% )
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
Applications
Places
Tue 16 Apr, 16:18
AttackBox IP:10.10.96.226
Woop woop! Your answer is correct
File
Edit
View
Search
Terminal
tryhackme@linux3: ~
root@ip-10-10-96-226: ~
root 568 0.0 0.5 315064 11000 ? Ssl 14:55 0:00 /usr/sbin/ModemM
er
root 569 0.0 0.1 7360 2412 ttyS0 Ss+ 14:55 0:00 /sbin/agetty -o
- \u --keep-baud 115200,38400,9600 ttyS0 vt220
root 581 0.0 0.0 5836 1844 tty1 Ss+ 14:55 0:00 /sbin/agetty -o
- \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/
D -o AuthorizedKeysCommand /usr/share/ec2-instance-connect/eic_run_authorized_key
f -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

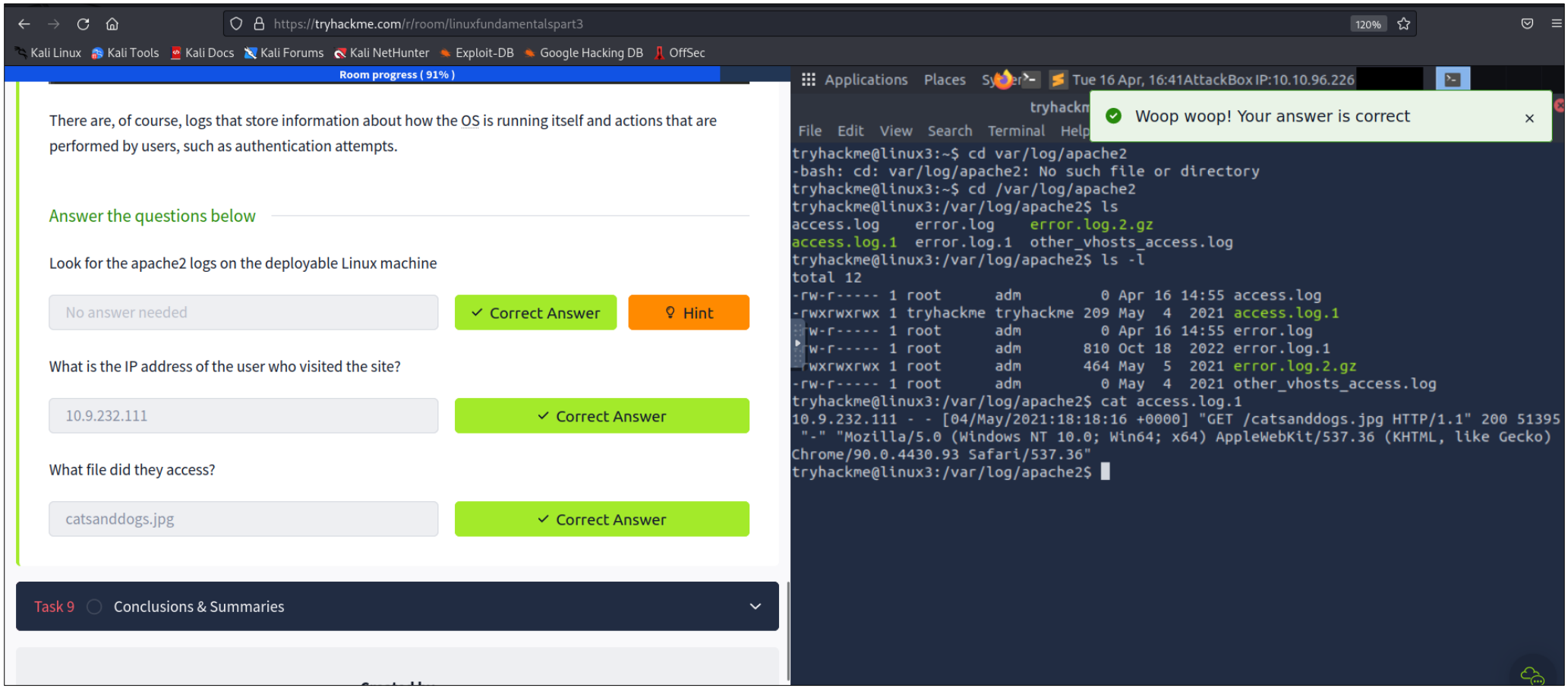
# Task 6. Maintaining Your System: Automation



# Task 7. Maintaining Your System: Package Management



# Task 8. Maintaining Your System: Logs



## Task 9. Conclusions & Summaries