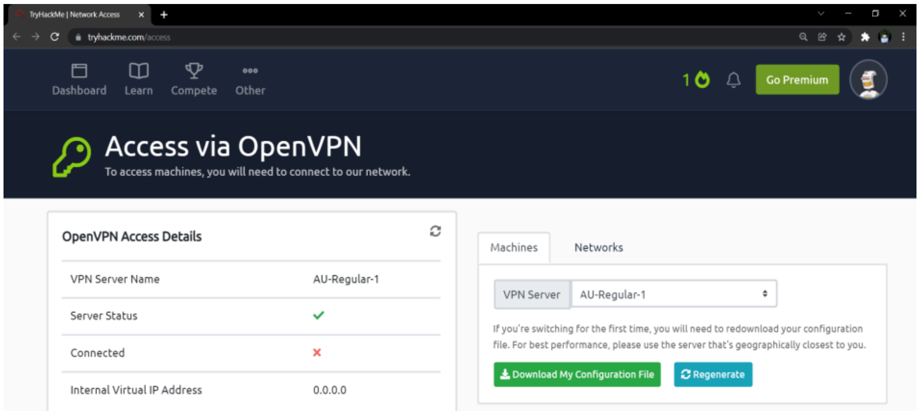
Penetration of Headless

Step 1 : Connect to open vpn using configuration file

- Download configuration file."https://tryhackme.com/access”



Access via OpenVPN

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

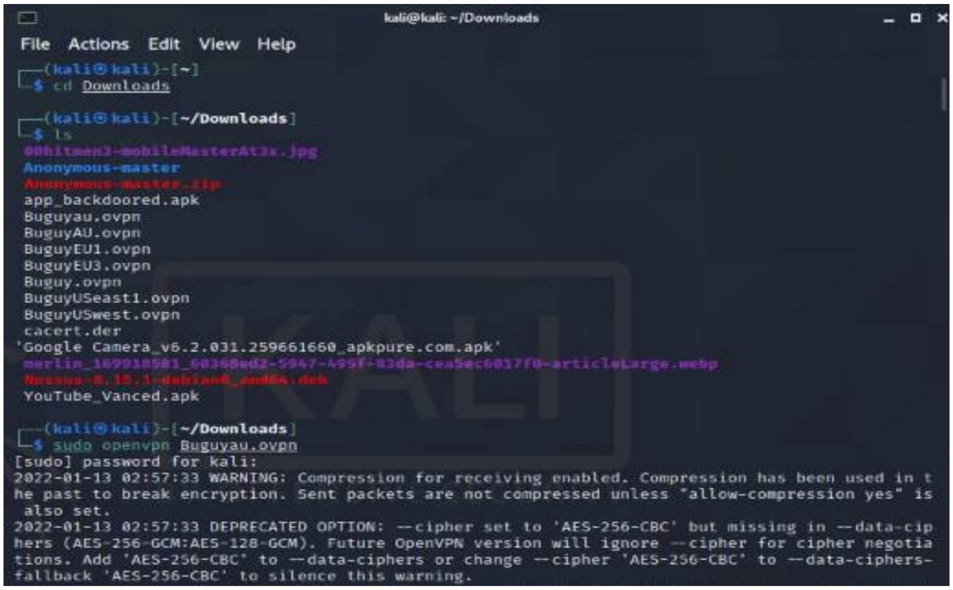
OpenVPN Access Details

VPN Server Name	AU-Regular-1
Server Status	✓
Connected	✗
Internal Virtual IP Address	0.0.0.0

VPN Server: AU-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.

- Fire up Kali Terminal.
- Move to the directory in which {filename}.ovpn is Downloaded.
- Use cmd ~ sudo openvpn Filename.ovpn

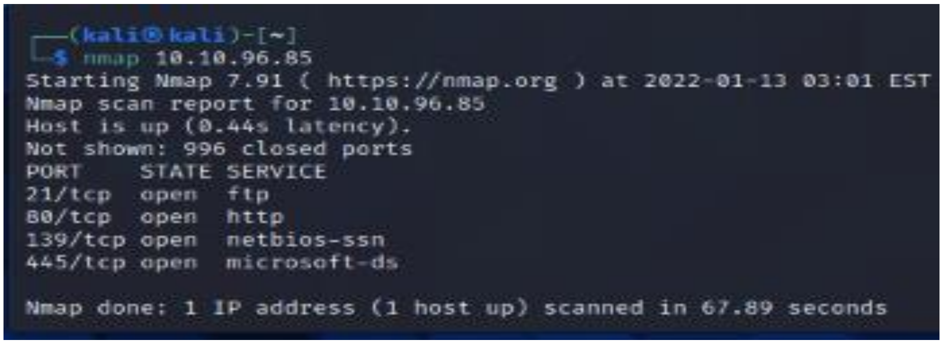


```
┌──(kali㉿kali)-[~]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
00hitmen3-mobileMasterAt3x.jpg
Anonymous-master
Anonymous-master.zip
app_backdoored.apk
Buguyau.ovpn
BuguyAU.ovpn
BuguyEU1.ovpn
BuguyEU3.ovpn
Buguy.ovpn
BuguyUSeast1.ovpn
BuguyUSwest.ovpn
cacert.der
'Google Camera_v6.2.031.259661660_apkpure.com.apk'
merlin_169918581_60368ed2-5947-495f-83da-cea5ec6017f0-articleLarge.webp
Nessus-8.15.1-debian6_amd64.deb
YouTube_Vanced.apk

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo openvpn Buguyau.ovpn
[sudo] password for kali:
2022-01-13 02:57:33 WARNING: Compression for receiving enabled. Compression has been used in t
he past to break encryption. Sent packets are not compressed unless "allow-compression yes" is
 also set.
2022-01-13 02:57:33 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' but missing in --data-cip
hers (AES-256-GCM:AES-128-GCM). Future OpenVPN version will ignore --cipher for cipher negotia
tions. Add 'AES-256-CBC' to --data-ciphers or change --cipher 'AES-256-CBC' to --data-ciphers-
fallback 'AES-256-CBC' to silence this warning.
```

- The Openvpn is connected successfully.

Step 2 : Start enumerating machines by simple nmap scan considering all Ports.

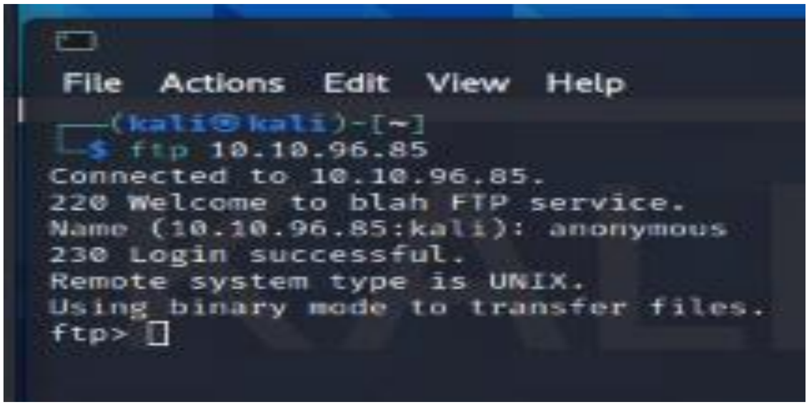
- Use cmd ~ nmap{ip address}



```
┌──(kali㉿kali)-[~]
└─$ nmap 10.10.96.85
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-13 03:01 EST
Nmap scan report for 10.10.96.85
Host is up (0.44s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 67.89 seconds
```

Step 3 : Since we can see from the nmap scan that the Ftp server allows anonymous login we can try to search for some files.

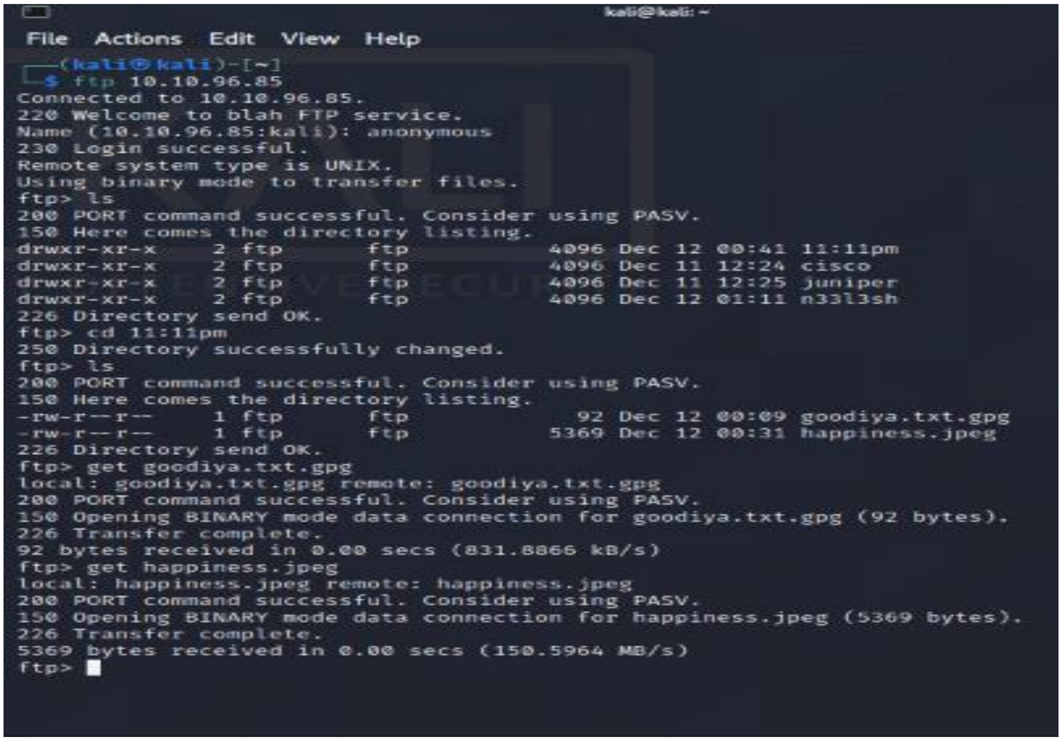
- Use cmd ~ ftp{ipaddress}



```
┌──(kali㉿kali)-[~]
└─$ ftp 10.10.96.85
Connected to 10.10.96.85.
220 Welcome to blah FTP service.
Name (10.10.96.85:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

Step 4 : Remote login successful

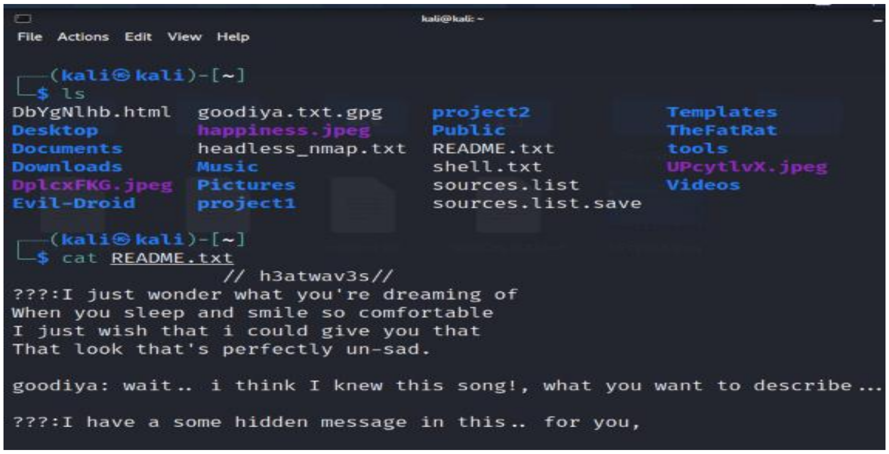
- Use cmd ~ ls to print current working directory
- Use cmd ~ ls -la to print hidden directory
- Use cmd ~ get{filename.extension} to download files
- Use cmd ~ bye to end session



```
┌──(kali㉿kali)-[~]
└─$ ftp 10.10.96.85
Connected to 10.10.96.85.
220 Welcome to blah FTP service.
Name (10.10.96.85:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Dec 12 00:41 11:11pm
drwxr-xr-x    2 ftp      ftp          4096 Dec 11 12:24 cisco
drwxr-xr-x    2 ftp      ftp          4096 Dec 11 12:25 juniper
drwxr-xr-x    2 ftp      ftp          4096 Dec 12 01:11 n3313sh
226 Directory send OK.
ftp> cd 11:11pm
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp            92 Dec 12 00:09 goodiya.txt.gpg
-rw-r--r--    1 ftp      ftp          5369 Dec 12 00:31 happiness.jpeg
226 Directory send OK.
ftp> get goodiya.txt.gpg
local: goodiya.txt.gpg remote: goodiya.txt.gpg
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for goodiya.txt.gpg (92 bytes).
226 Transfer complete.
92 bytes received in 0.00 secs (831.8866 kB/s)
ftp> get happiness.jpeg
local: happiness.jpeg remote: happiness.jpeg
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for happiness.jpeg (5369 bytes).
226 Transfer complete.
5369 bytes received in 0.00 secs (150.5964 MB/s)
ftp> 
```

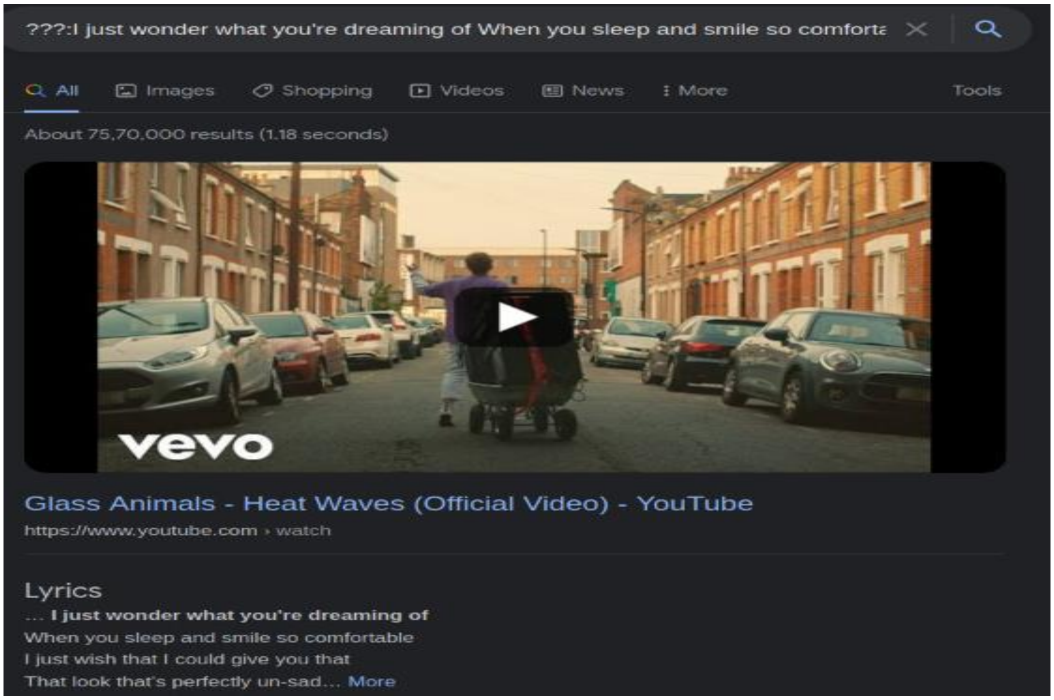
Step 5 : Exploring the hidden files.

- Readme.txt



```
┌──(kali㉿kali)-[~]
└─$ ls
DbYgNlhb.html   goodiya.txt.gpg     project2           Templates
Desktop         happiness.jpeg      Public             TheFatRat
Documents       headless_nmap.txt   README.txt         tools
Downloads       Music               shell.txt          UPcytlvX.jpeg
DplcxFKG.jpeg   Pictures            sources.list       Videos
Evil-Droid      project1            sources.list.save

┌──(kali㉿kali)-[~]
└─$ cat README.txt
                        // h3atwav3s//
???:I just wonder what you're dreaming of
When you sleep and smile so comfortable
I just wish that i could give you that
That look that's perfectly un-sad.

goodiya: wait.. i think I knew this song!, what you want to describe...

???:I have a some hidden message in this.. for you,
```

- Searched for the text on Google


???:I just wonder what you're dreaming of When you sleep and smile so comforta
All
Images
Shopping
Videos
News
More
Tools
vevo

About 75,70,000 results (1.18 seconds)

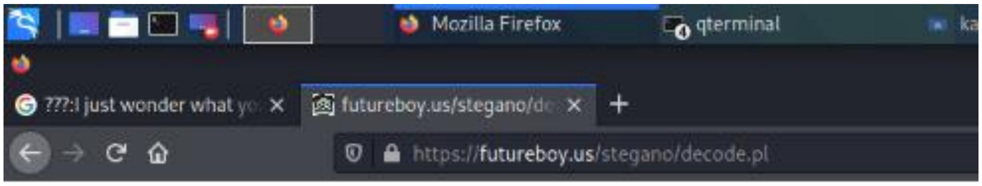
Glass Animals - Heat Waves (Official Video) - YouTube

https://www.youtube.com › watch

Lyrics

... **I just wonder what you're dreaming of**
When you sleep and smile so comfortable
I just wish that I could give you that
That look that's perfectly un-sad... More

- Uploaded Happiness.jpeg steganography tool-https://futureboy.us/stegano/decinput.html
- Passphrase tried glass animals / heatwaves/ h3at wav3s = h3at wav3s

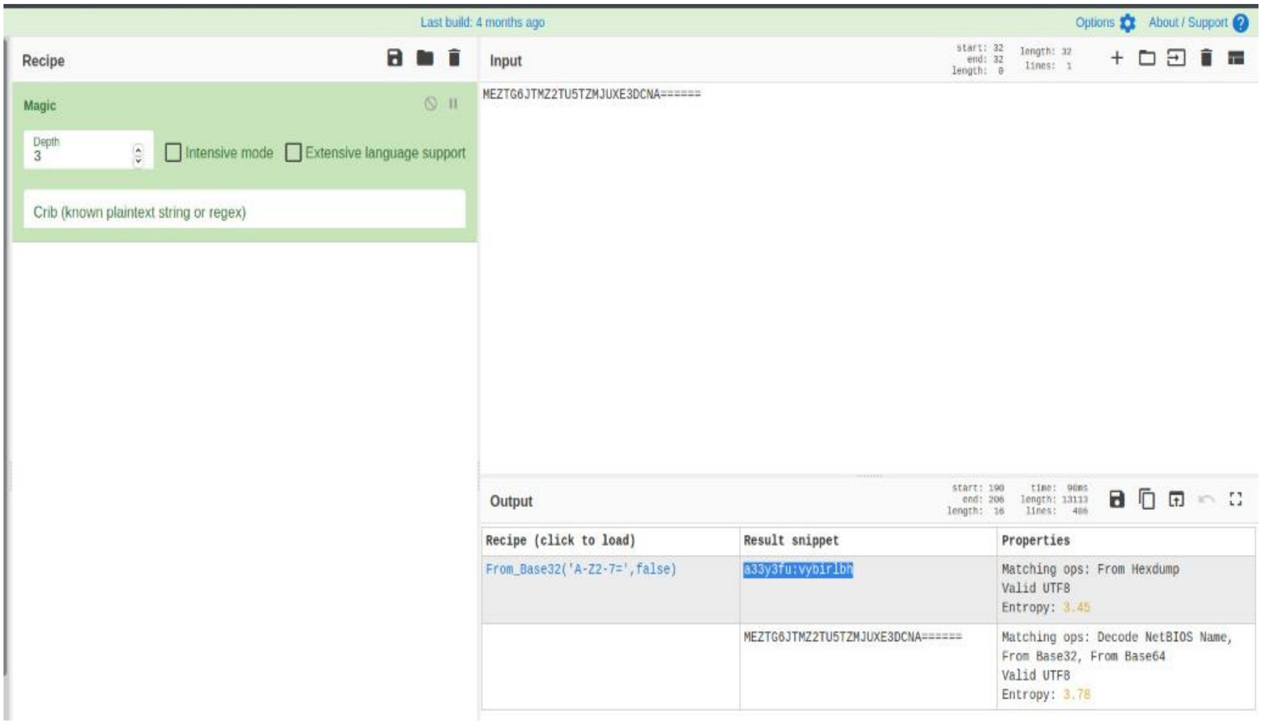

Mozilla Firefox
qterminal
???:I just wonder what yo
futureboy.us/stegano/de
https://futureboy.us/stegano/decode.pl

MEZTG6JTMZ2TU5TZMJUXE3DCNA======

- Got the String

Step 6 : check it on cyberchef

- A function called "Magic" - "The Magic operation attempts to detect various properties of the input data and suggests which operations could help to make more sense of it.



Recipe: Magic

Depth: 3 □ Intensive mode □ Extensive language support

Crib (known plaintext string or regex)

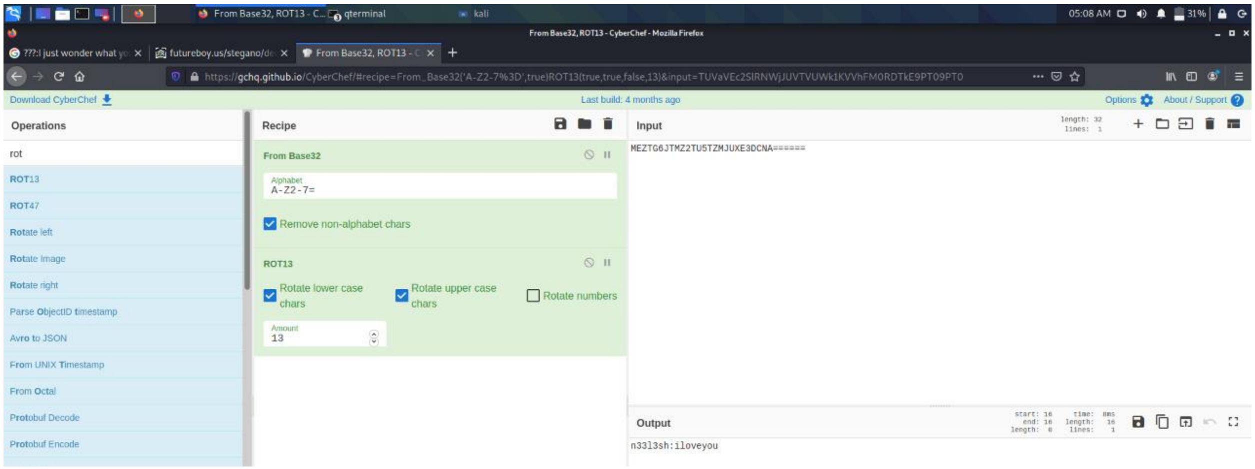
Input:

```
MEZTG6JTMZ2TU5TZMJUXE3DCNA======
```

Output:

Recipe (click to load)	Result snippet	Properties
From_Base32('A-Z2-7=',false)	a33y3fu:vybirlbh	Matching ops: From Hexdump Valid UTF8 Entropy: 3.45
	MEZTG6JTMZ2TU5TZMJUXE3DCNA======	Matching ops: Decode NetBIOS Name, From Base32, From Base64 Valid UTF8 Entropy: 3.78

- The Base32 string looked like a rot algorithm(Rotation cipher) because I had come across a directory called : "n33l3sh" - "a33y3fu"
- Rot13 Decoding - n33l3sh:{PASSWORD} .



https://gchq.github.io/CyberChef/#recipe=From_Base32('A-Z2-7%3D',true)ROT13(true,true,false,13)&input=TUVaVEc2SlRNWjJUVTVUWk1KVVhFM0RDTkE9PT09PT0

Operations: rot

Recipe:

From Base32 — Alphabet: A-Z2-7= ☑ Remove non-alphabet chars

ROT13 — ☑ Rotate lower case chars ☑ Rotate upper case chars □ Rotate numbers — Amount: 13

Input:

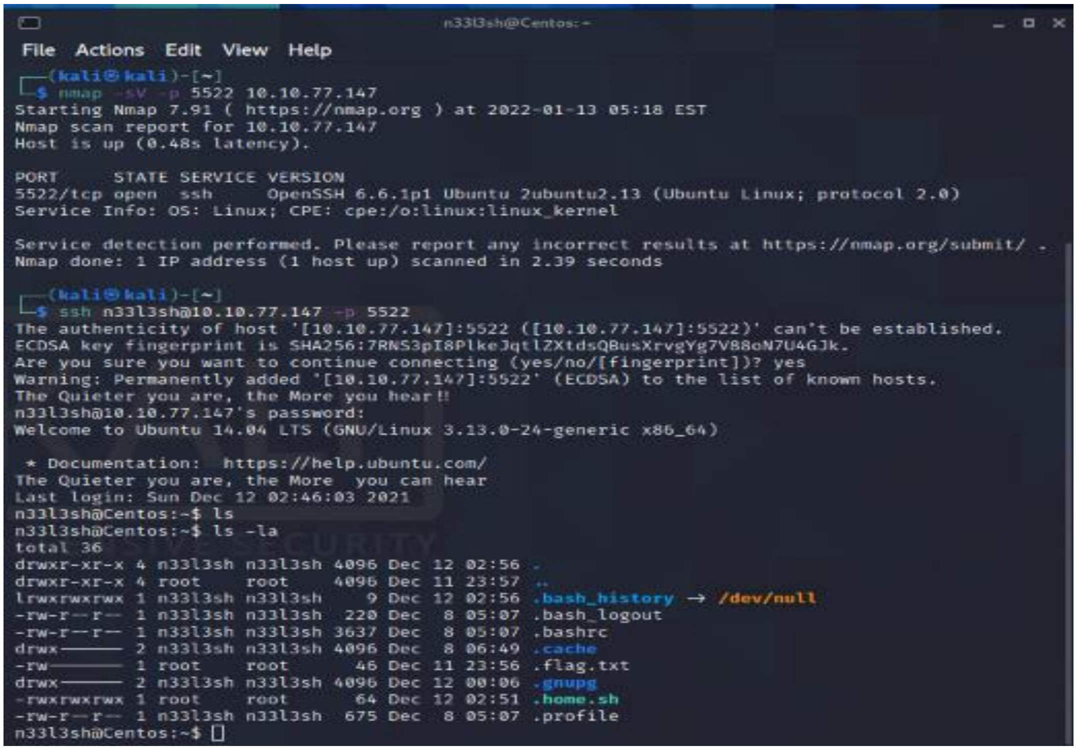
```
MEZTG6JTMZ2TU5TZMJUXE3DCNA======
```

Output:

```
n33l3sh:iloveyou
```

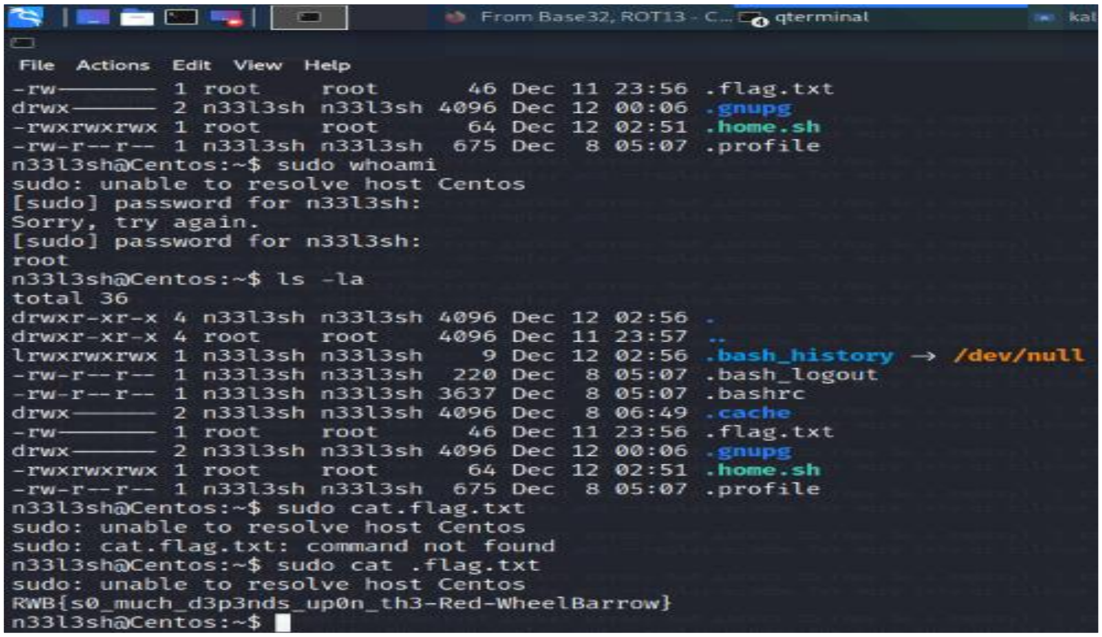
Step 7 : Trying to Login in via SSH using the port 5522.

- ssh n33l3sh@{ipaddress} -p 5522



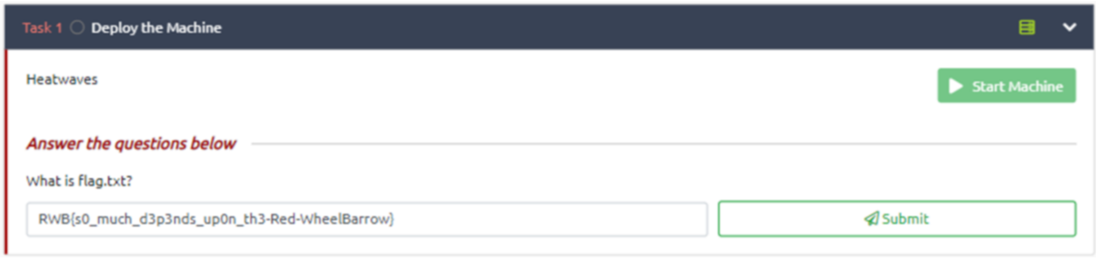
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 5522 10.10.77.147
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-13 05:18 EST
Nmap scan report for 10.10.77.147
Host is up (0.48s latency).

PORT     STATE SERVICE VERSION
5522/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.39 seconds

┌──(kali㉿kali)-[~]
└─$ ssh n33l3sh@10.10.77.147 -p 5522
The authenticity of host '[10.10.77.147]:5522 ([10.10.77.147]:5522)' can't be established.
ECDSA key fingerprint is SHA256:7RNS3pI8PlkeJqtlZXtdsQBusXrvgYg7V88oN7U4GJk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.77.147]:5522' (ECDSA) to the list of known hosts.
The Quieter you are, the More you hear!!
n33l3sh@10.10.77.147's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
The Quieter you are, the More  you can hear
Last login: Sun Dec 12 02:46:03 2021
n33l3sh@Centos:~$ ls
n33l3sh@Centos:~$ ls -la
total 36
drwxr-xr-x 4 n33l3sh n33l3sh 4096 Dec 12 02:56 .
drwxr-xr-x 4 root    root    4096 Dec 11 23:57 ..
lrwxrwxrwx 1 n33l3sh n33l3sh    9 Dec 12 02:56 .bash_history → /dev/null
-rw-r--r-- 1 n33l3sh n33l3sh  220 Dec  8 05:07 .bash_logout
-rw-r--r-- 1 n33l3sh n33l3sh 3637 Dec  8 05:07 .bashrc
drwx------ 2 n33l3sh n33l3sh 4096 Dec  8 06:49 .cache
-rw------- 1 root    root      46 Dec 11 23:56 .flag.txt
drwx------ 2 n33l3sh n33l3sh 4096 Dec 12 00:06 .gnupg
-rwxrwxrwx 1 root    root      64 Dec 12 02:51 .home.sh
-rw-r--r-- 1 n33l3sh n33l3sh  675 Dec  8 05:07 .profile
n33l3sh@Centos:~$ 
```

- Finally got the Flag file - '.flag.txt'
- After trying to cat.flag.txt



```
-rw------- 1 root    root      46 Dec 11 23:56 .flag.txt
drwx------ 2 n33l3sh n33l3sh 4096 Dec 12 00:06 .gnupg
-rwxrwxrwx 1 root    root      64 Dec 12 02:51 .home.sh
-rw-r--r-- 1 n33l3sh n33l3sh  675 Dec  8 05:07 .profile
n33l3sh@Centos:~$ sudo whoami
sudo: unable to resolve host Centos
[sudo] password for n33l3sh:
Sorry, try again.
[sudo] password for n33l3sh:
root
n33l3sh@Centos:~$ ls -la
total 36
drwxr-xr-x 4 n33l3sh n33l3sh 4096 Dec 12 02:56 .
drwxr-xr-x 4 root    root    4096 Dec 11 23:57 ..
lrwxrwxrwx 1 n33l3sh n33l3sh    9 Dec 12 02:56 .bash_history → /dev/null
-rw-r--r-- 1 n33l3sh n33l3sh  220 Dec  8 05:07 .bash_logout
-rw-r--r-- 1 n33l3sh n33l3sh 3637 Dec  8 05:07 .bashrc
drwx------ 2 n33l3sh n33l3sh 4096 Dec  8 06:49 .cache
-rw------- 1 root    root      46 Dec 11 23:56 .flag.txt
drwx------ 2 n33l3sh n33l3sh 4096 Dec 12 00:06 .gnupg
-rwxrwxrwx 1 root    root      64 Dec 12 02:51 .home.sh
-rw-r--r-- 1 n33l3sh n33l3sh  675 Dec  8 05:07 .profile
n33l3sh@Centos:~$ sudo cat.flag.txt
sudo: unable to resolve host Centos
sudo: cat.flag.txt: command not found
n33l3sh@Centos:~$ sudo cat .flag.txt
sudo: unable to resolve host Centos
RWB{s0_much_d3p3nds_up0n_th3-Red-WheelBarrow}
n33l3sh@Centos:~$ 
```

- Got the flag.



Task 1 ○ Deploy the Machine

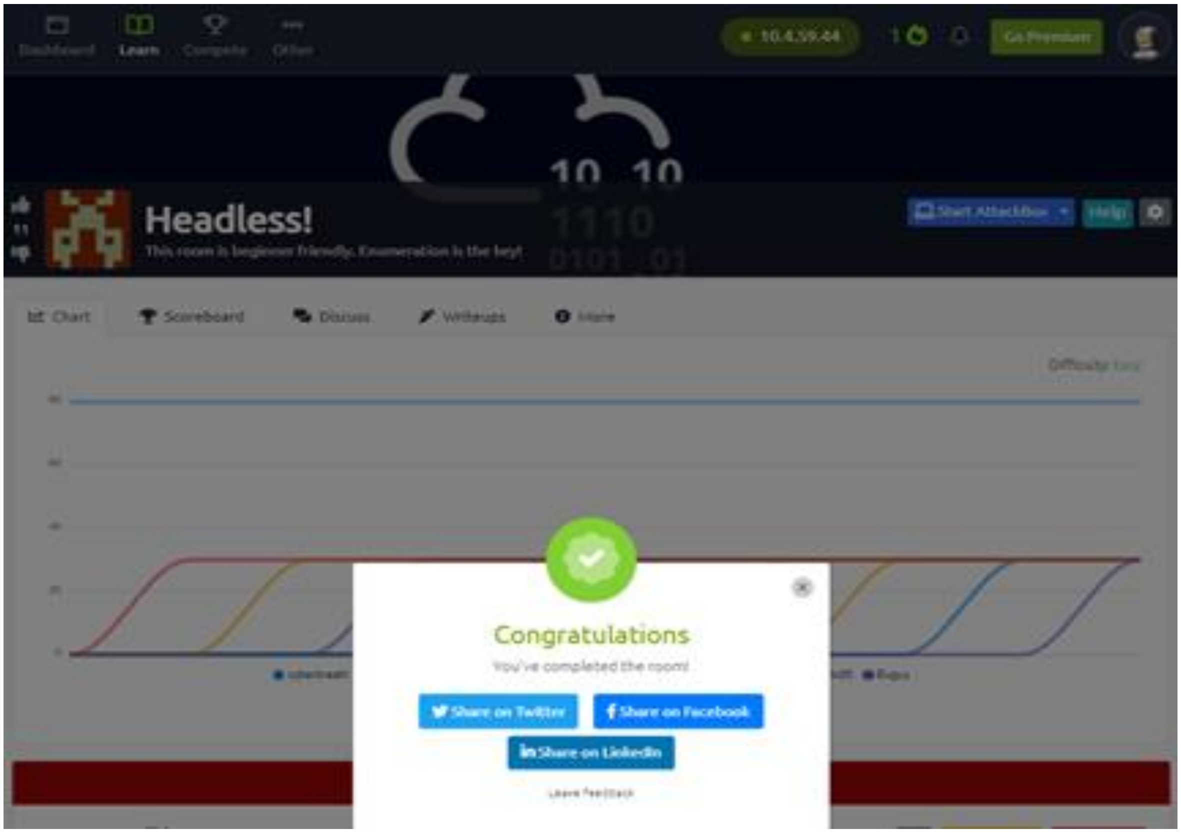
Heatwaves

Answer the questions below

What is flag.txt?

RWB{s0_much_d3p3nds_up0n_th3-Red-WheelBarrow}

- Submit the flag.



Congratulations

You've completed the room!