PenTest 2

Iron Corp

OraOraOra

Members

ID	Name	Role
1211103141	Muhammad Haikal Afiq Bin Rafingei	Leader
1211103148	Muhamad Izzul Iqbal Bin Ismail	Member
1211103830	Hakeem Bin Aminudin	Member

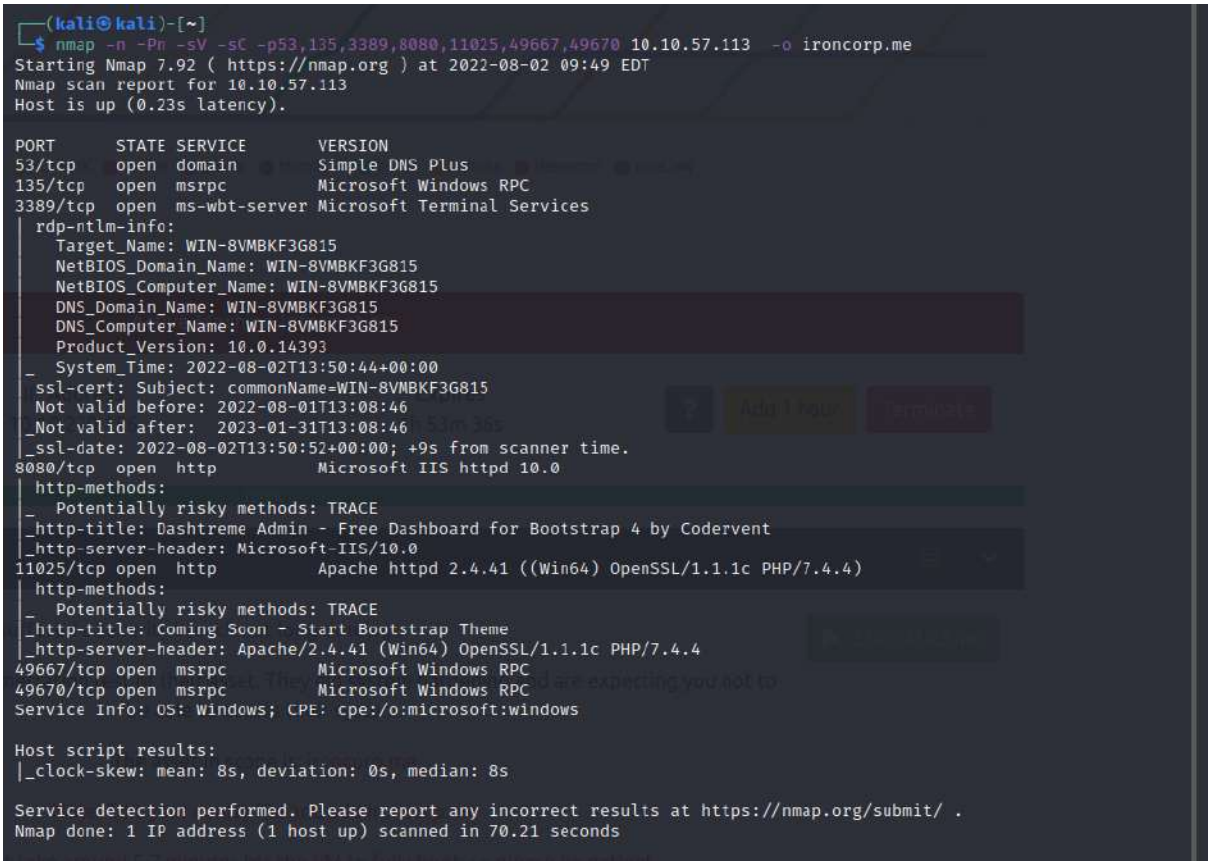
Recon and Enumeration

Members Involved: Izzul and Hakeem

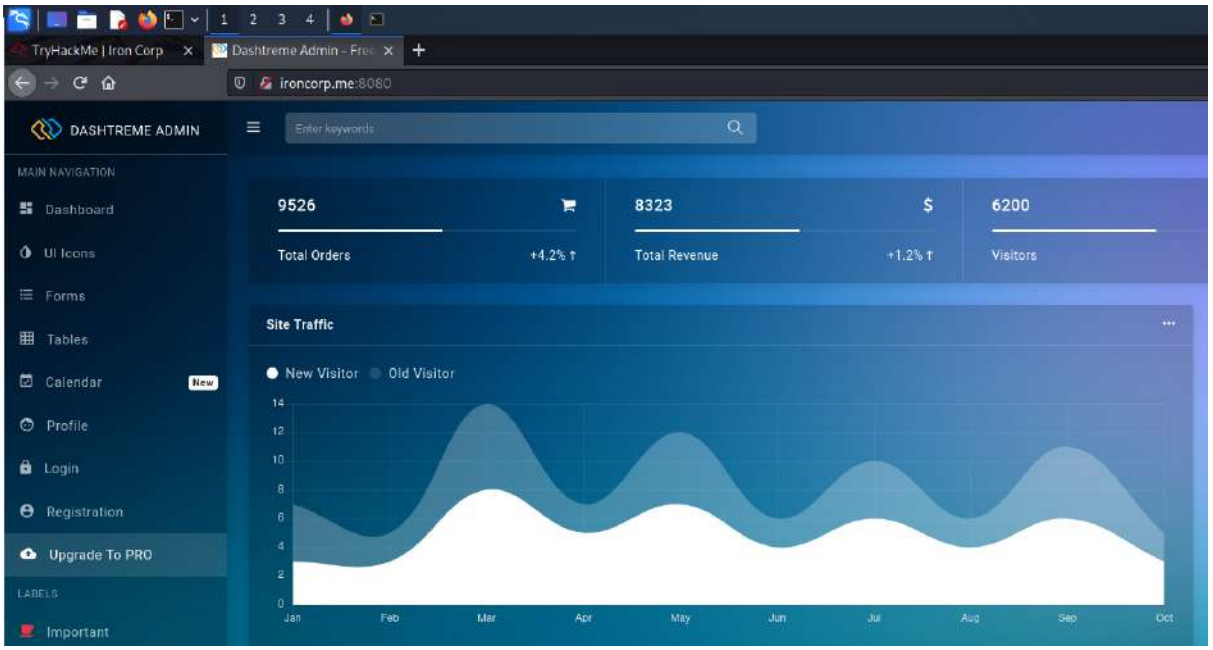
Tools used: Nmap, Dig, Hydra

Thought Process and Methodology and Attempts:

First Hakeem put IP Address to etc/hosts file and execute the file



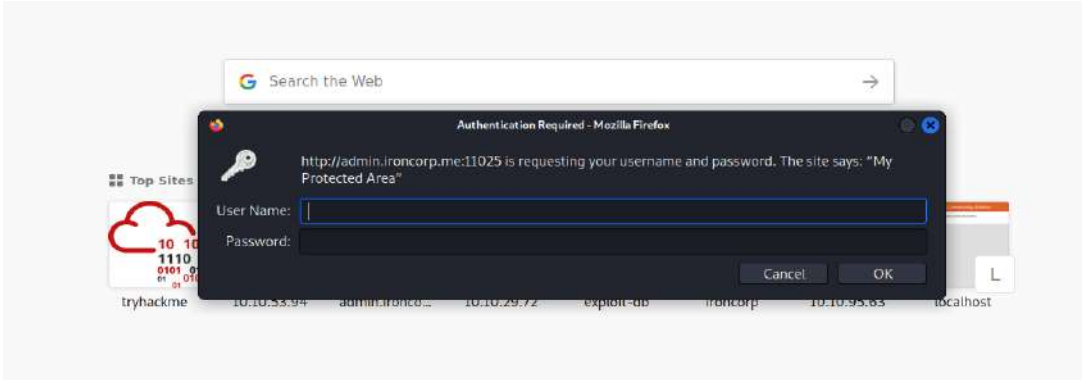
Then Hakeem tries to access the port 8080 , but there is no functionality that can serve him.



So he try open the port 53 where you can see list of sub-domain or information that relevant

After that Hakeem found two subdomains that are running internally.

He tries to access the port but none of them he can access because it is protected by basic authentication.



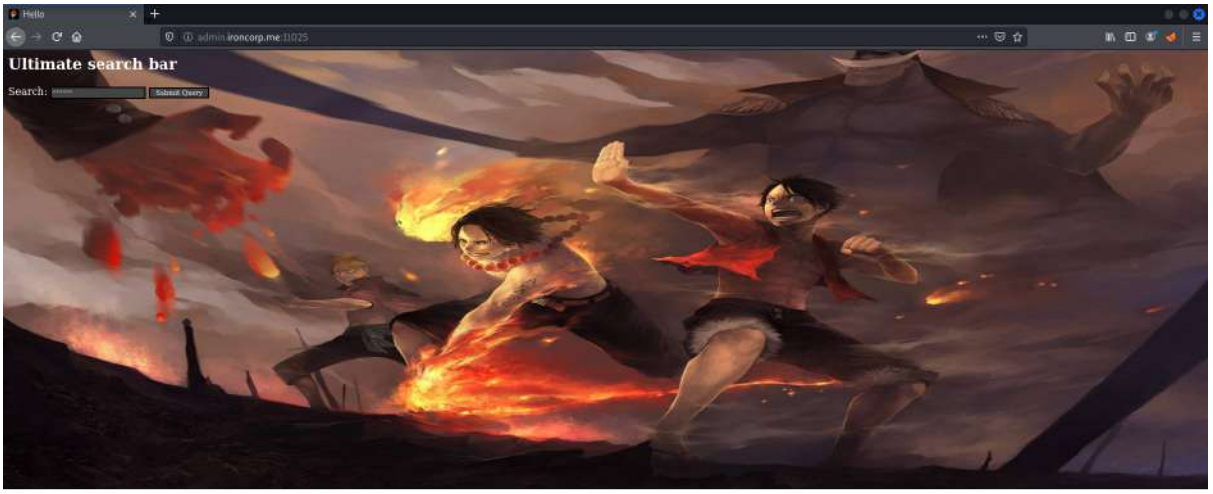
Izzul tried to open the admin.ironcorp.me but it needed a password.

To get the username and password for the web page, Izzul uses hydra to brute force the password. By using ‘rockyou.txt’ with hydra, Izzul gets the password = ‘password123’.

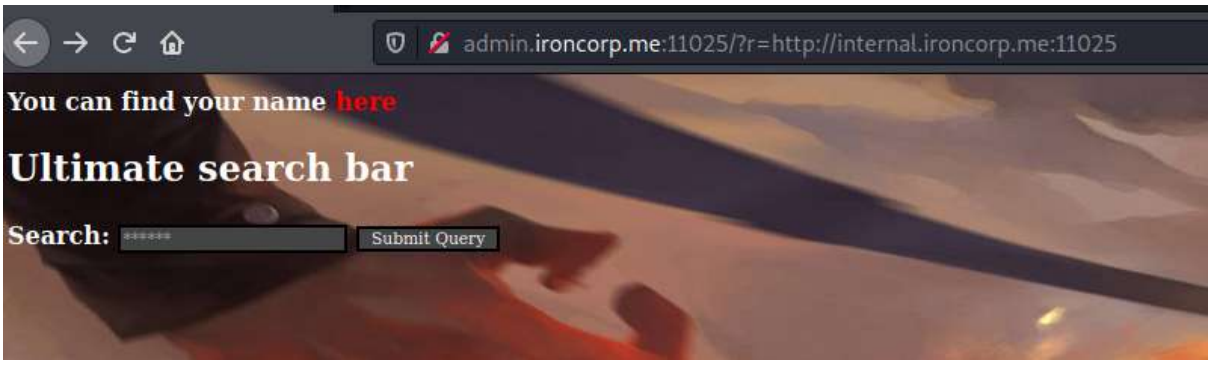
```
┌──(kali㉿kali)-[~]
└─$ hydra -l admin -P /home/kali/Desktop/rockyou.txt -s 11025 admin.ironcorp.me http-get
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret
 service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and
ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-02 09:19:42
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~8965
25 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[STATUS] 1296.00 tries/min, 1296 tries in 00:01h, 14343103 to do in 184:28h, 16 active
[11025][http-get] host: admin.ironcorp.me   login: admin   password: password123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-02 09:20:50
```

Final Result:

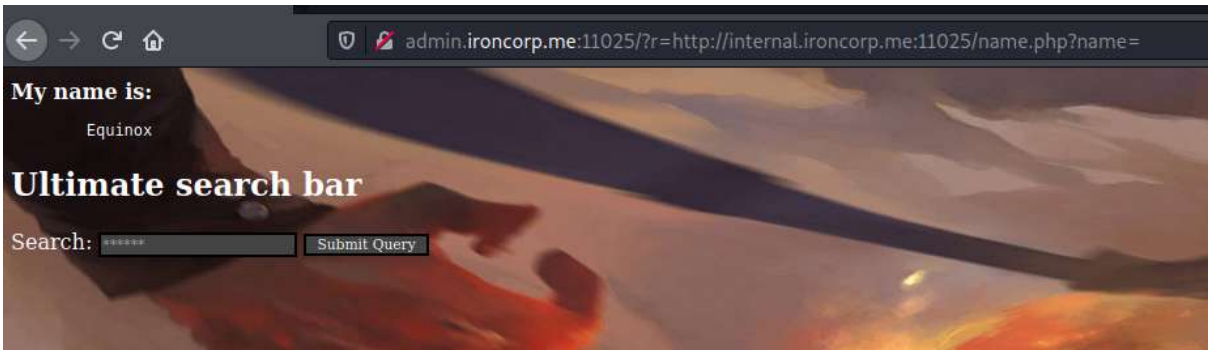
After inputting the password, Izzul can access the page with the One Piece background.



Izzul tested to see what sort of vulnerabilities the website was exposed to, and found out it was SSRF.



By abusing the vulnerability, Izzul gets the name of a user.



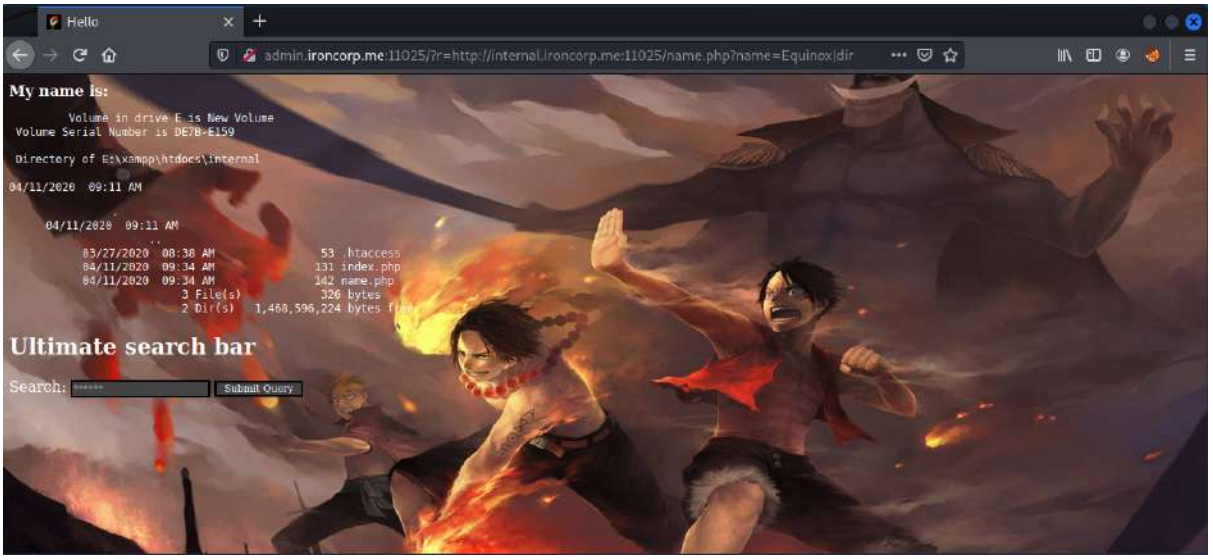
Initial Foothold

Members Involved: Haikal

Tools used: Burp suite, Mozilla Firefox, Terminal

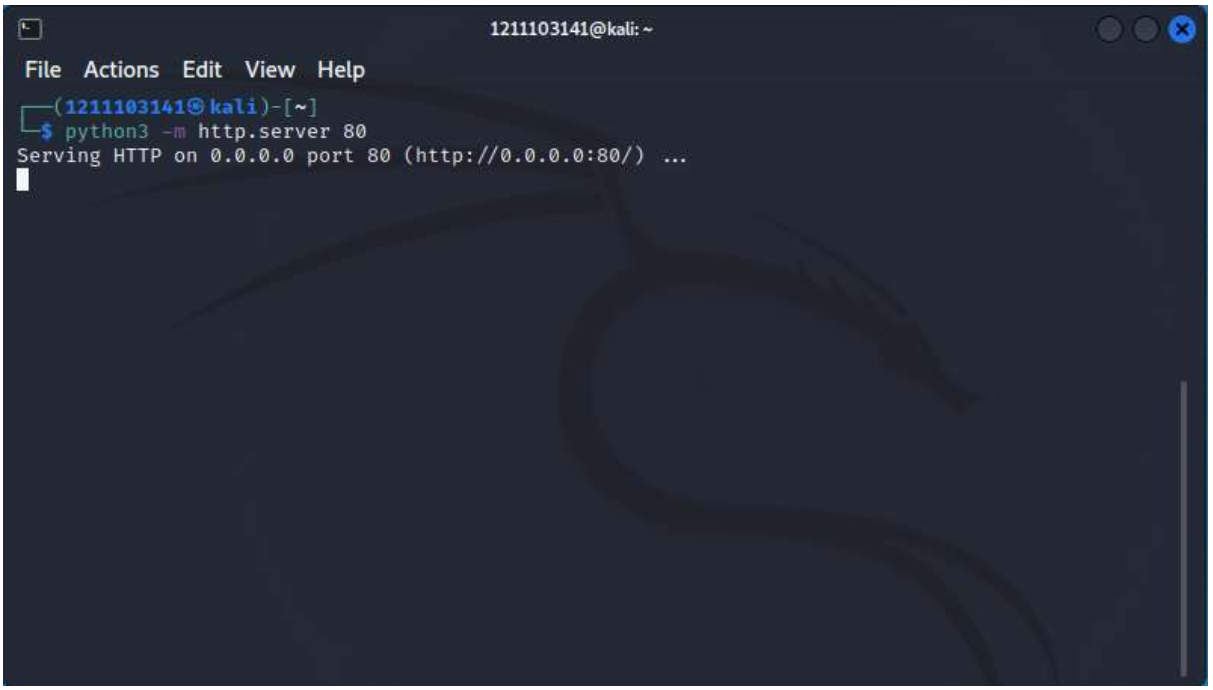
Thought Process and Methodology and Attempts:

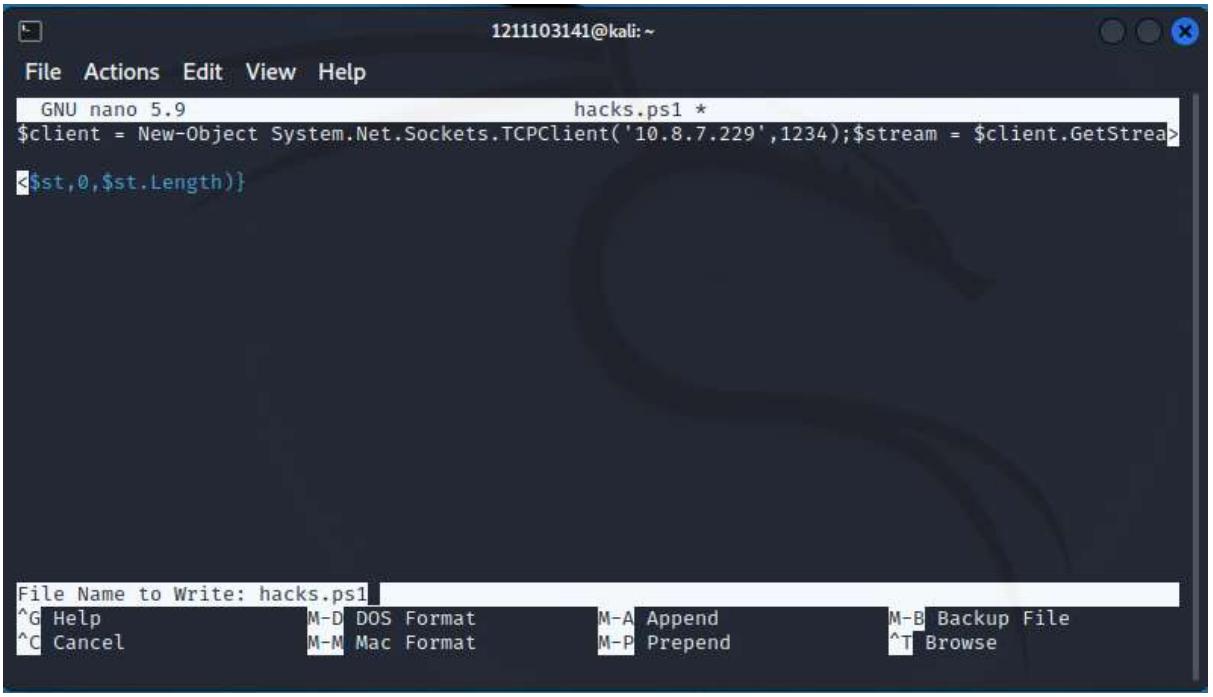
If we continue to enumerate, we can find the content of the drive E which can be a location to upload the reverse shell.



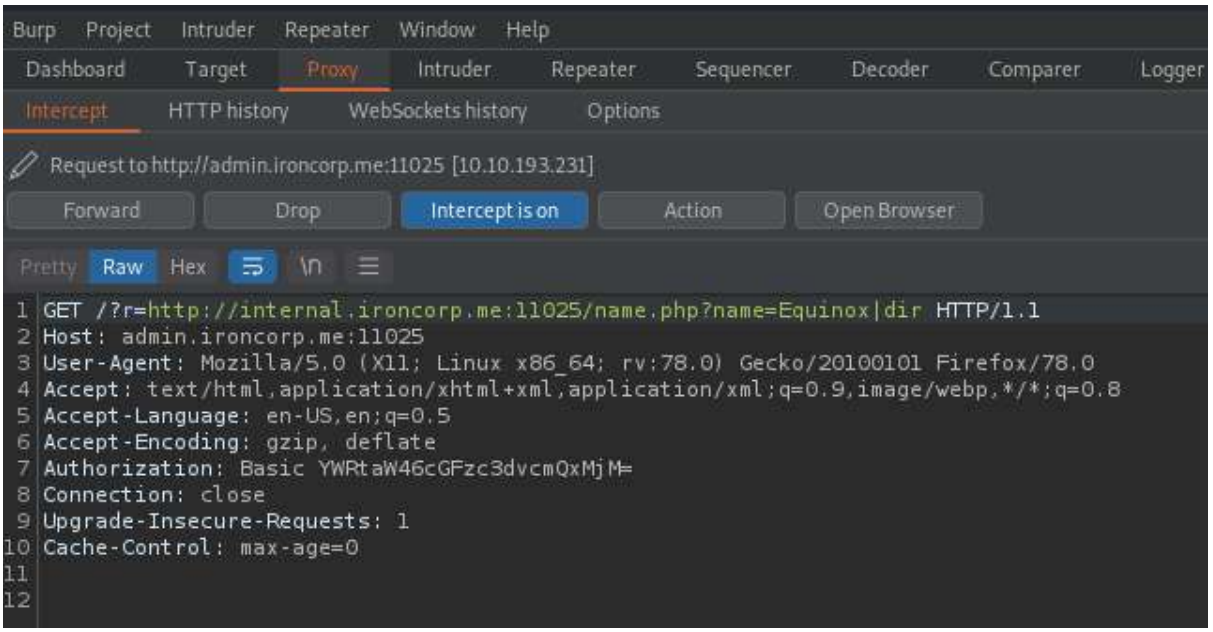
Haikal made his own http server and made a powershell reverse shell using the code made by nishan.

(https://github.com/vulware/powershell-reverse-shell-/blob/master/powershell%20tcp%20reverse%20shell.ps1)

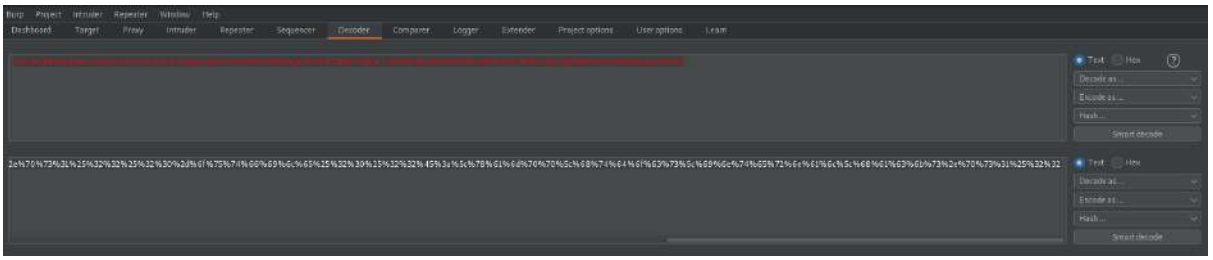


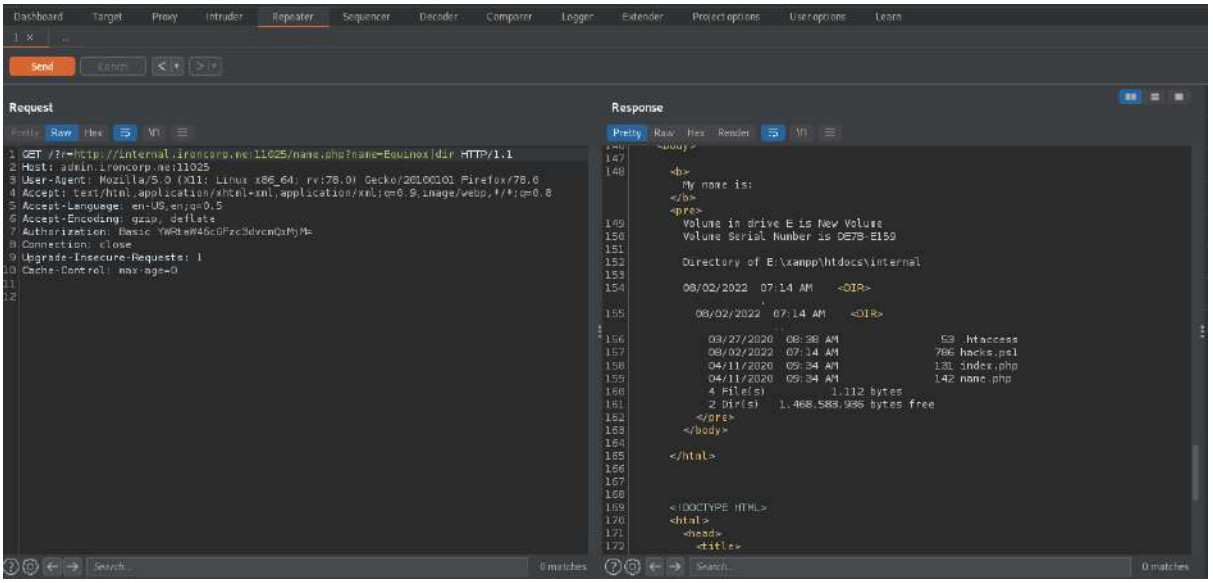


Haikal uses the repeater and decoder from Burp Suite to upload and run the powershell reverse shell into the remote device. He uses a proxy to intercept the request and send the codes to the repeater.

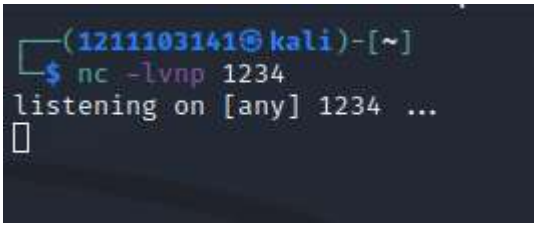


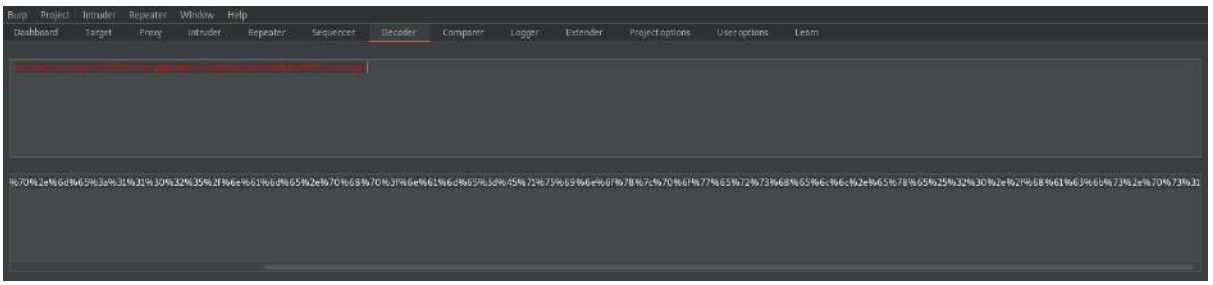
Then, he encodes the following plain text into the url and uses it to replace the url in repeater. If we check at the dir page, the shell is already in the directory.

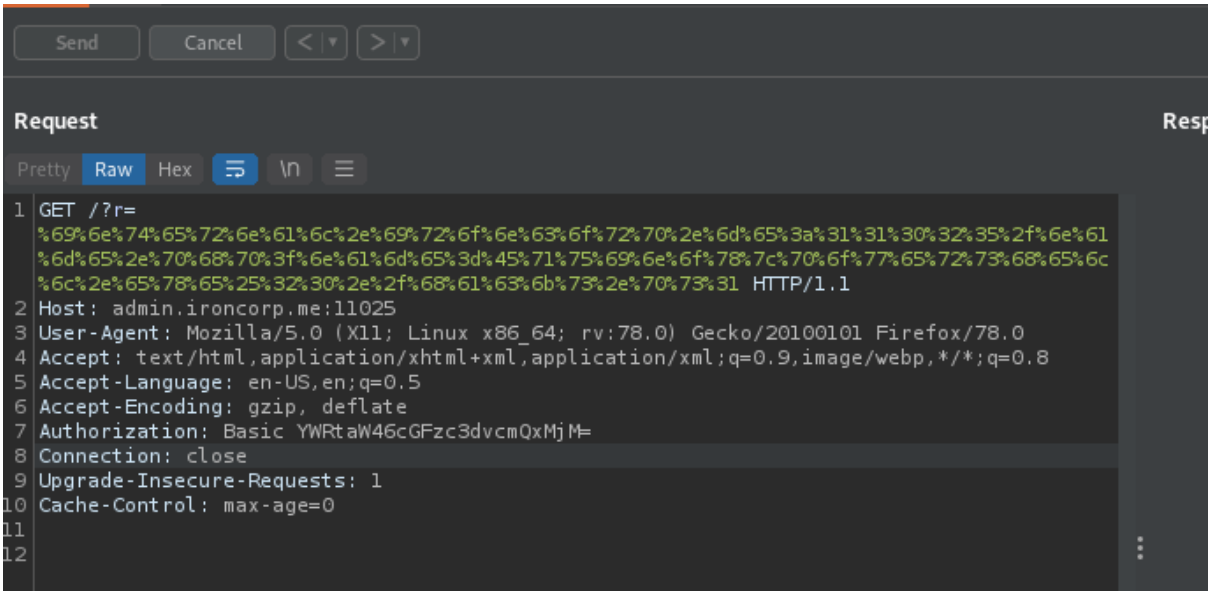




Next, Haikal encodes the following plain text into the url and uses it to replace the url in repeater to activate the powershell reverse shell. Make sure to make a listener first.

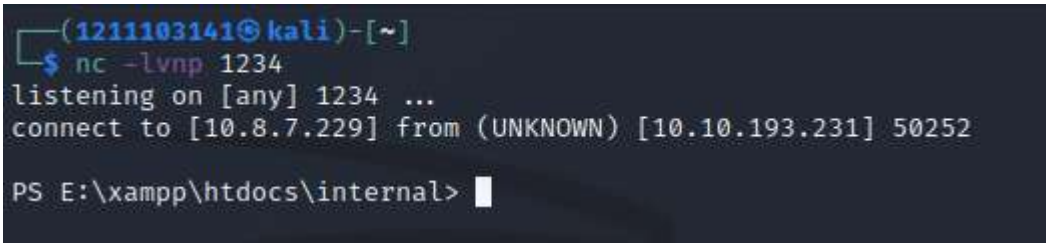


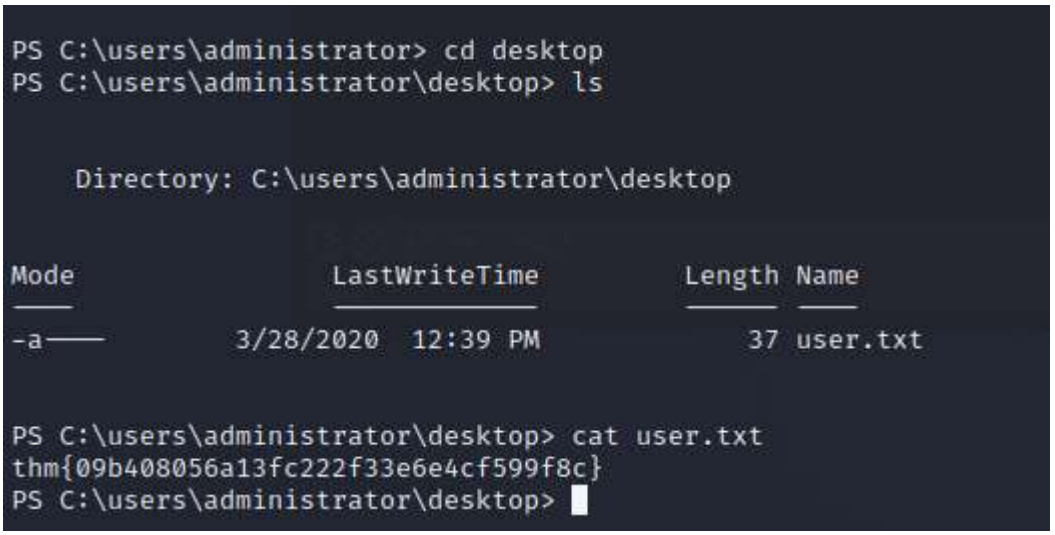




Final Result:

The netcat listener managed to catch it and Haikal managed to get into the remote machine. After changing the directory, Haikal finds the user.txt and sees its content with cat command.





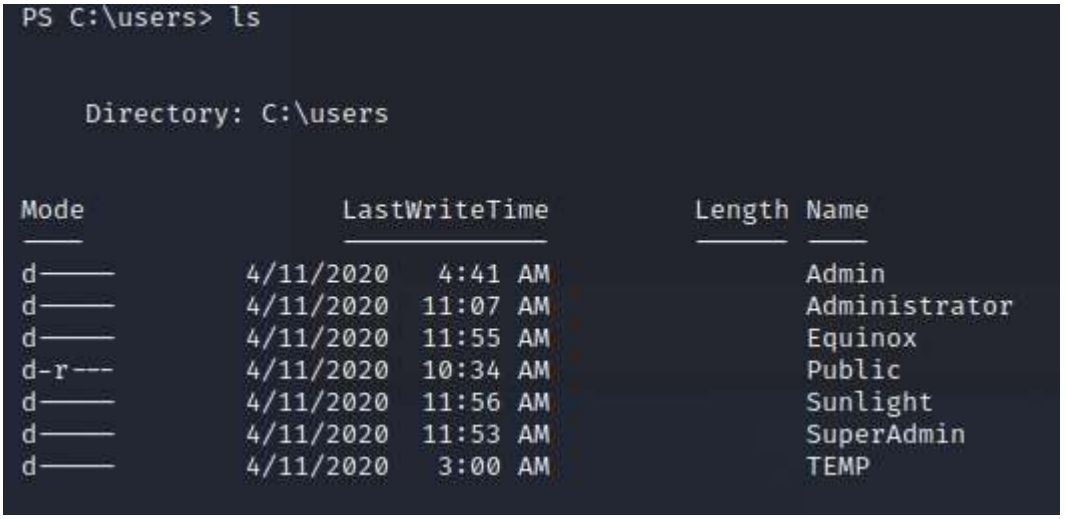
Root Privilege Escalation

Members Involved: Haikal

Tools used: Netcat, Terminal

Thought Process and Methodology and Attempts:

Haikal noticed the user superadmin, and suspects that the root.txt is in it.



Final Result:

SInce Haikal can't change his directory into the superadmin, he just uses cat command towards the directory into the root.txt.

Contributions

ID	Name	Contribution	Signatures
1211103141	Muhammad Haikal Afiq Bin Rafingei	Gain the initial foothold and manage to get both flags.	Haikal
1211103148	Muhamad Izzul Iqbal Bin Ismail	Did some recon and enumeration by using hydra. Edit the video presentation.	Izzul
1211103830	Hakeem Bin Aminudin	Did some recon and enumeration by using nmap and dig. Record the video presentation.	Hakeem

VIDEO LINK: https://youtu.be/488LxRE_-BE