PenTest 2

TL6L

CIPHER

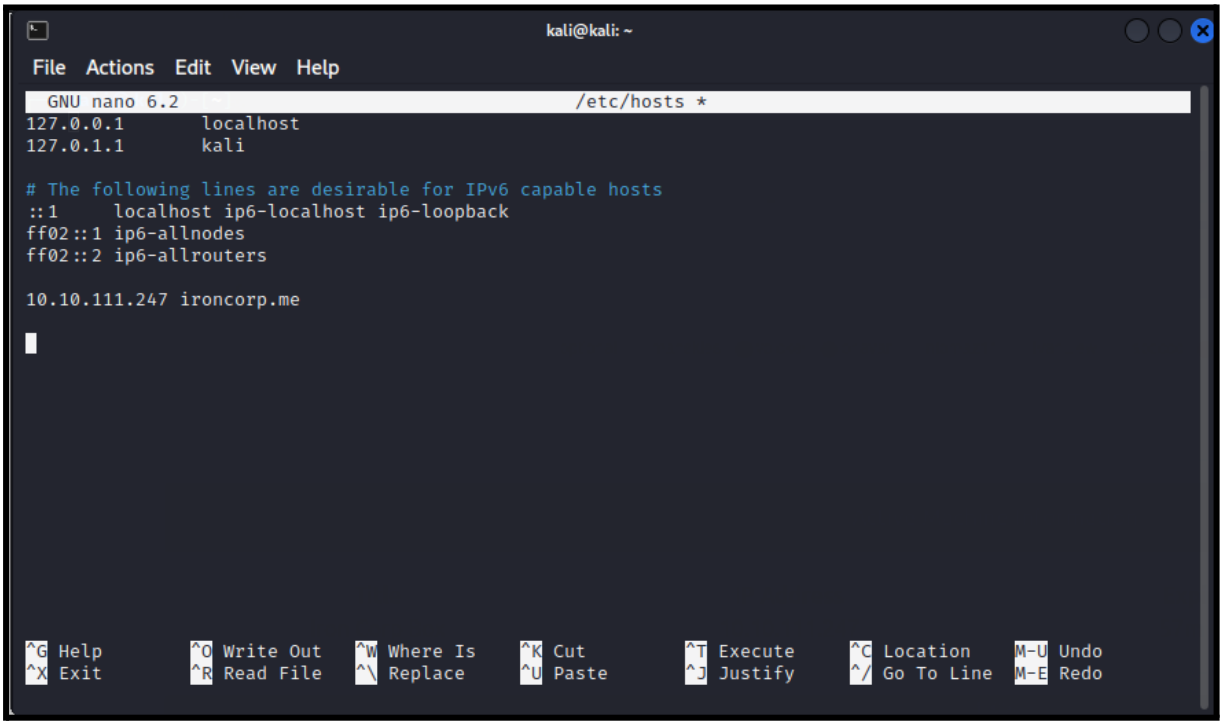
Members

ID	Name	Role
1211103064	Muhamad Aiman bin Mohd Ehwal	Leader
1211103373	Muhammad Alif bIn Khabali	Member
1211103085	Muhammad Farid bin Jayatan	Member
1211103451	Arif Muhriz bin Syamsul Fozy	Member

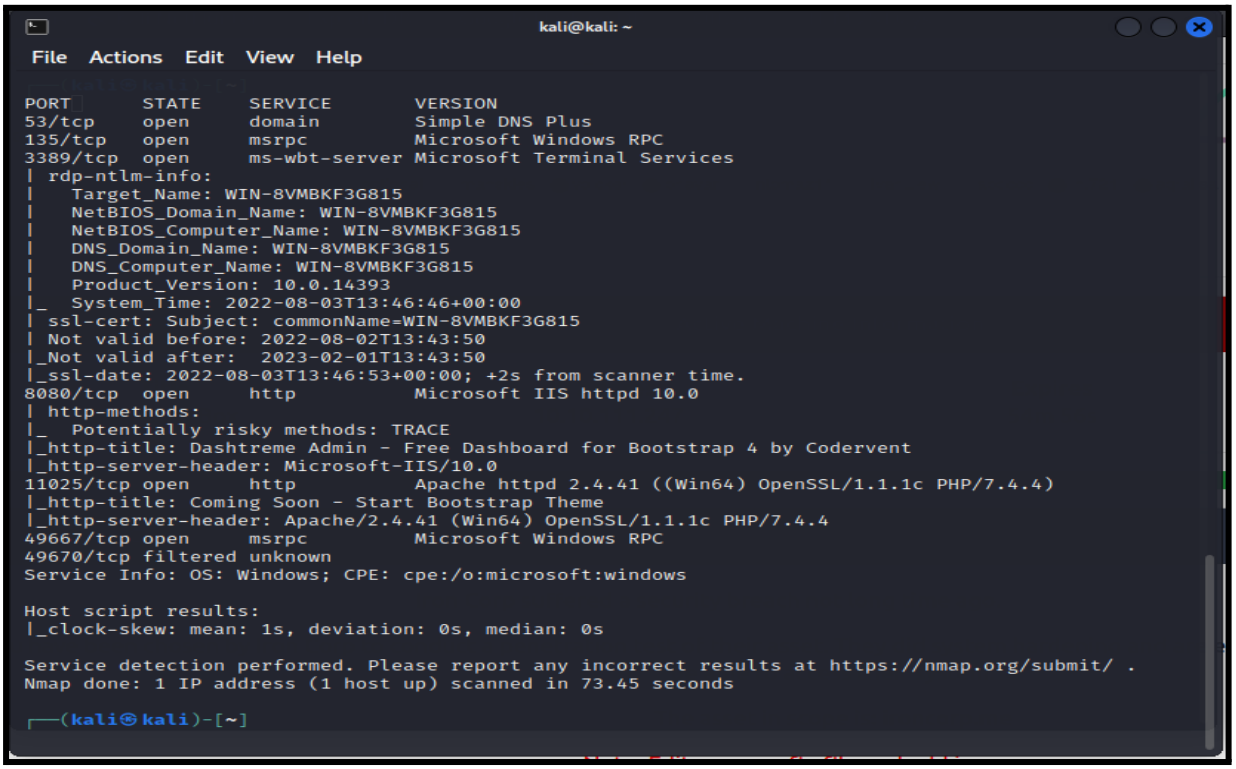
Members Involved: Aiman, Alif, Farid

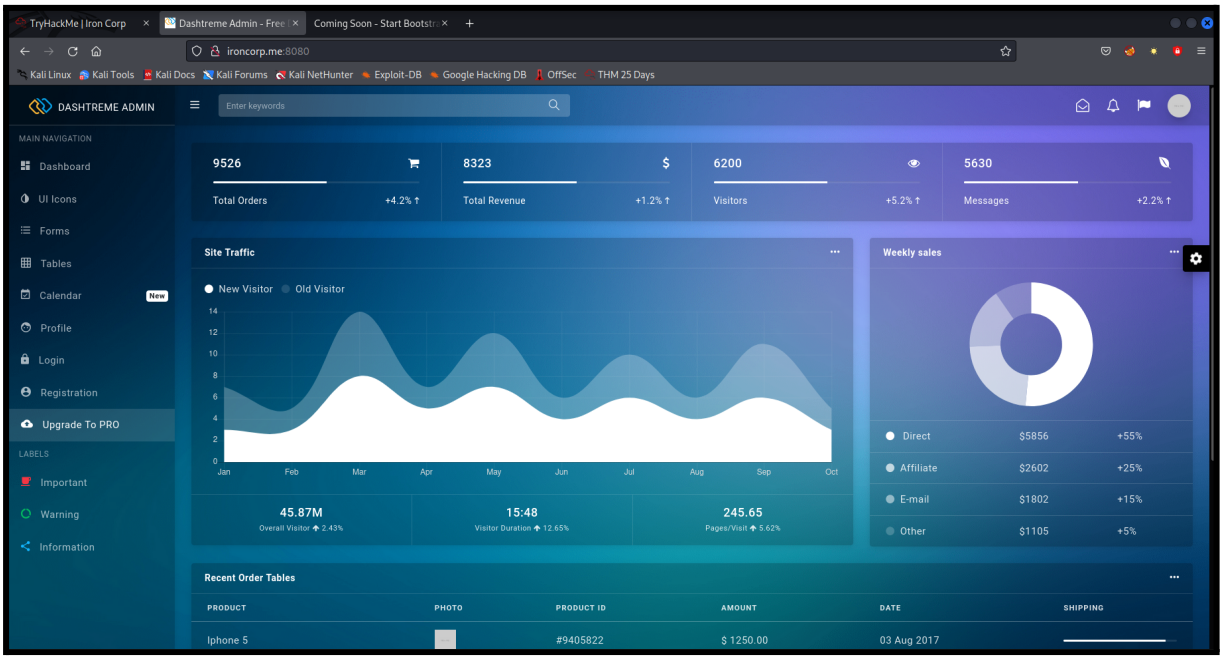
Tools used: **Nmap ,Hydra ,BurpSuite ,FoxyProxy ,Firefox**

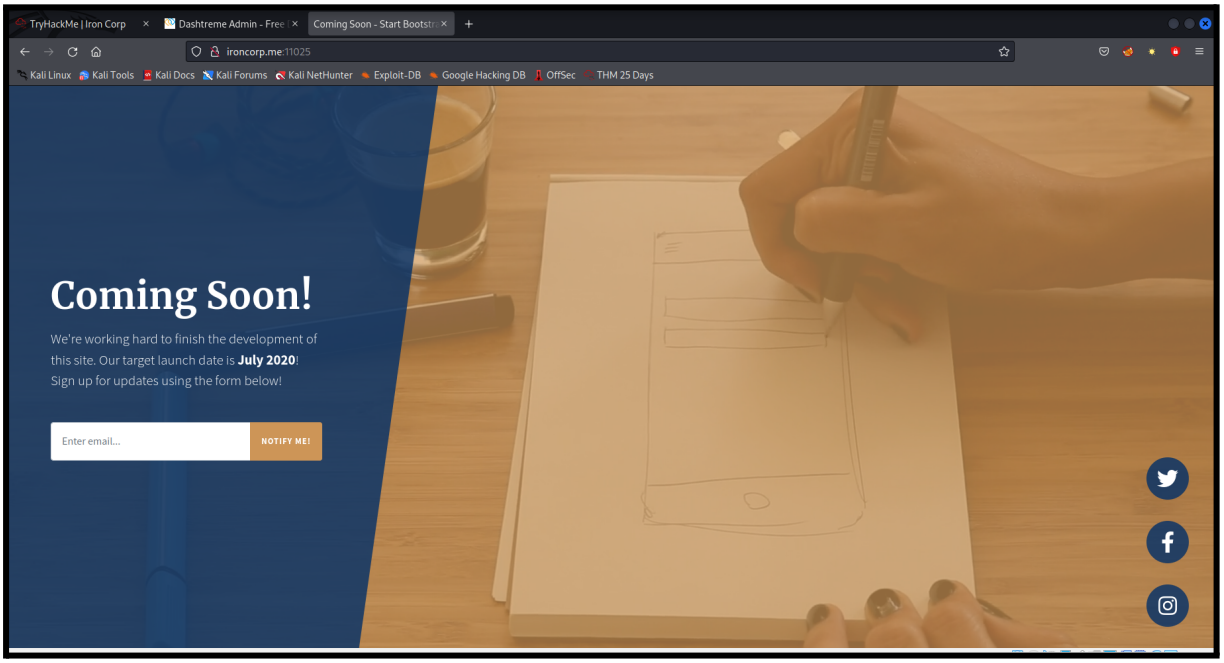
Thought Process and Methodology and Attempts:



We put the TARGET_IP_Address in the **/etc/hosts** file and use **nmap.** After getting the ports

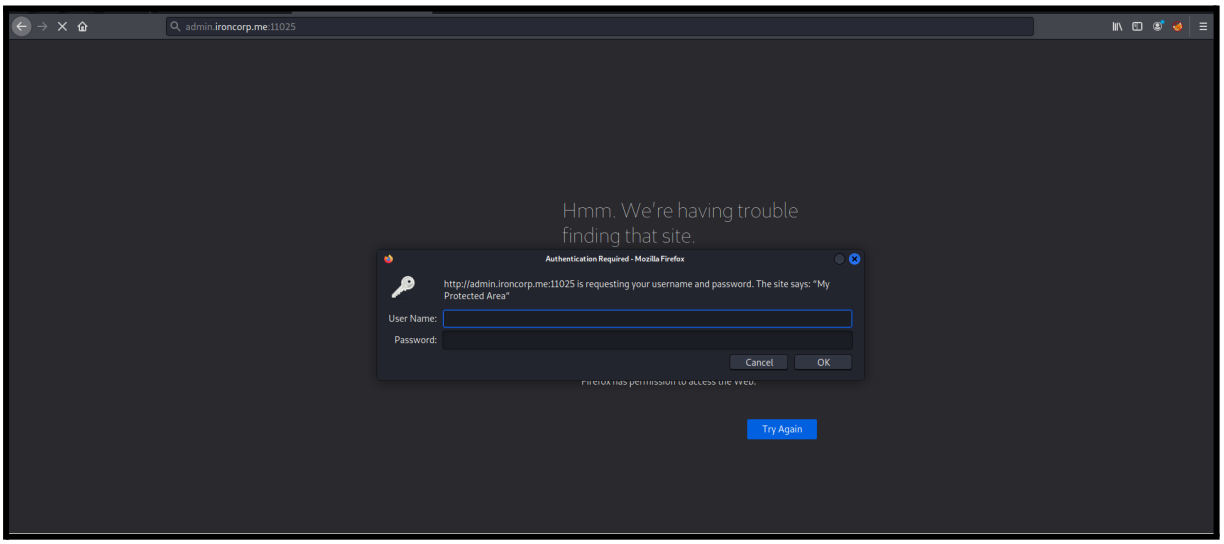


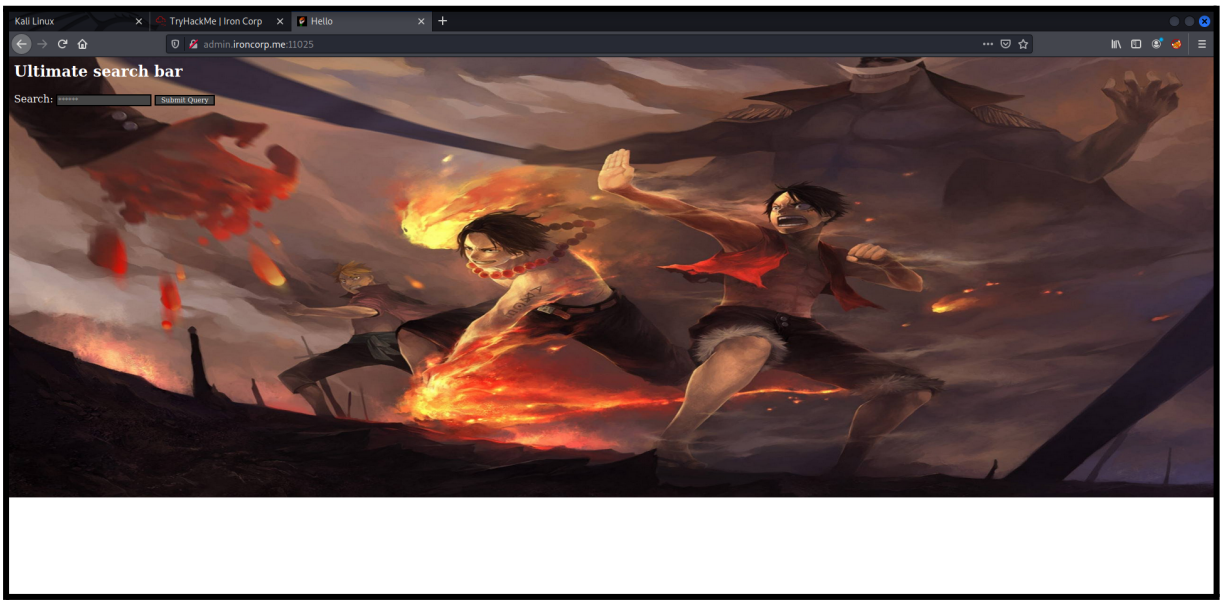




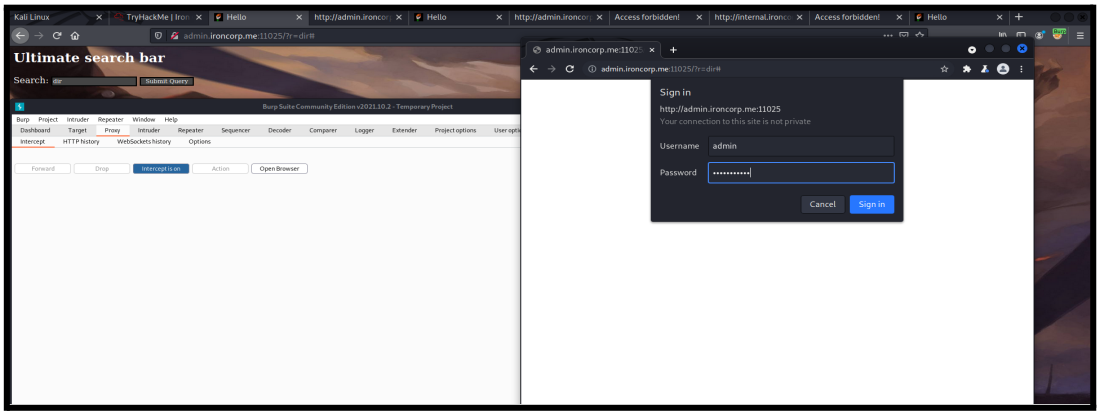
We access the web server by using 2 ports which are 8080 and 11025. We examined both websites but found no interesting information that we can use.

```
┌──(kali㉿kali)-[~]
└─$ dig @10.10.111.247 ironcorp.me axfr

; <<>> DiG 9.18.1-1-Debian <<>> @10.10.111.247 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: 220 msec
;; SERVER: 10.10.111.247#53(10.10.111.247) (TCP)
;; WHEN: Wed Aug 03 09:48:34 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)

┌──(kali㉿kali)-[~]
└─$
```

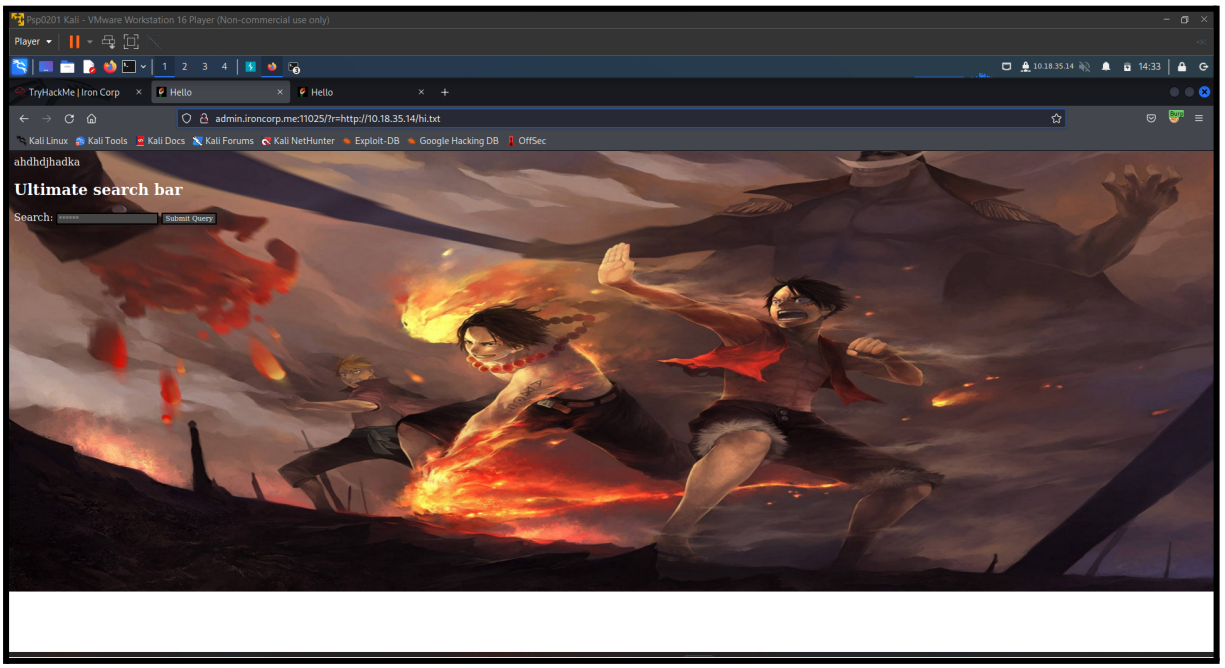




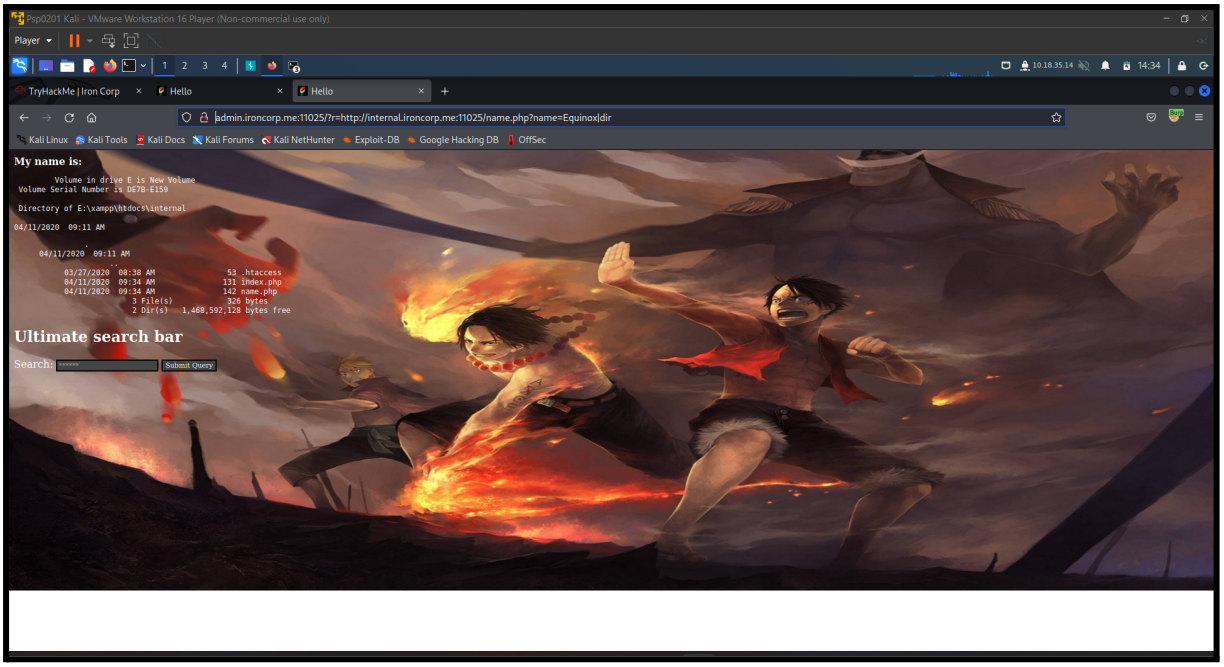
Later on we used the command dig@TARGET_IP_Address to try to search for more valuable information and then we found subdomains that run internally. After that, We tried to access the subdomains but we couldn't access one of them so we tried the other subdomain and saw that it loads a website authentication that allows users to verify their identities in order to gain access to the website. We used Hydra to acquire the username and password to access the page.



We did a test to see what we can do to the website and found that it can print our txt file.

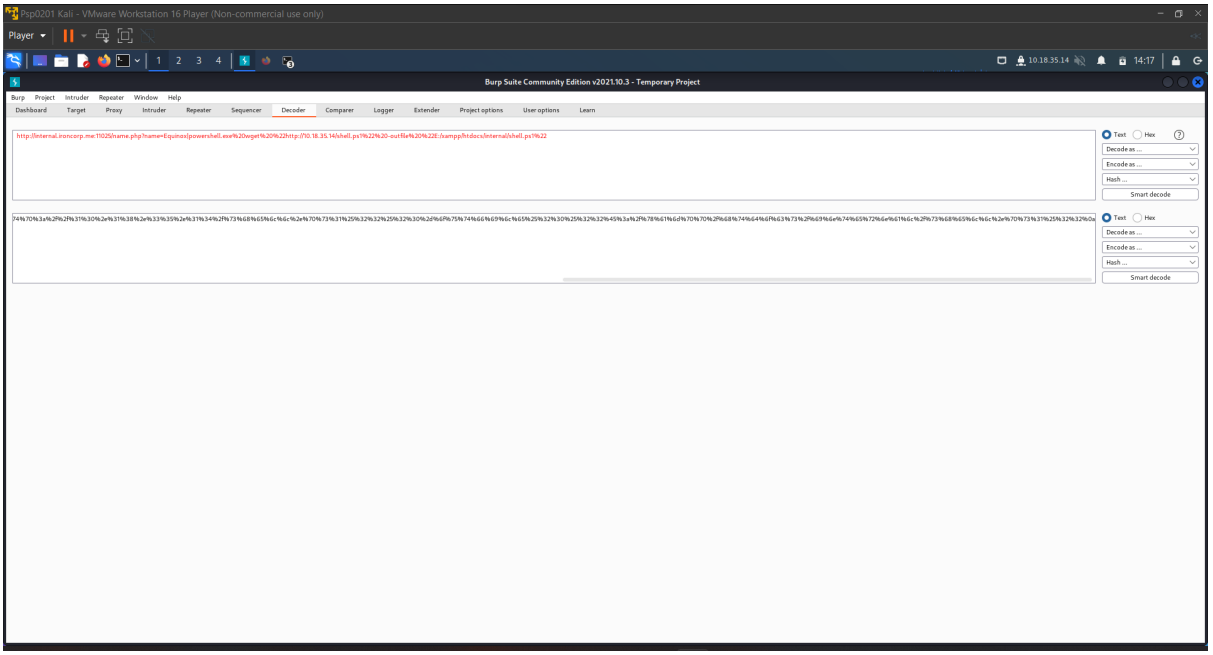


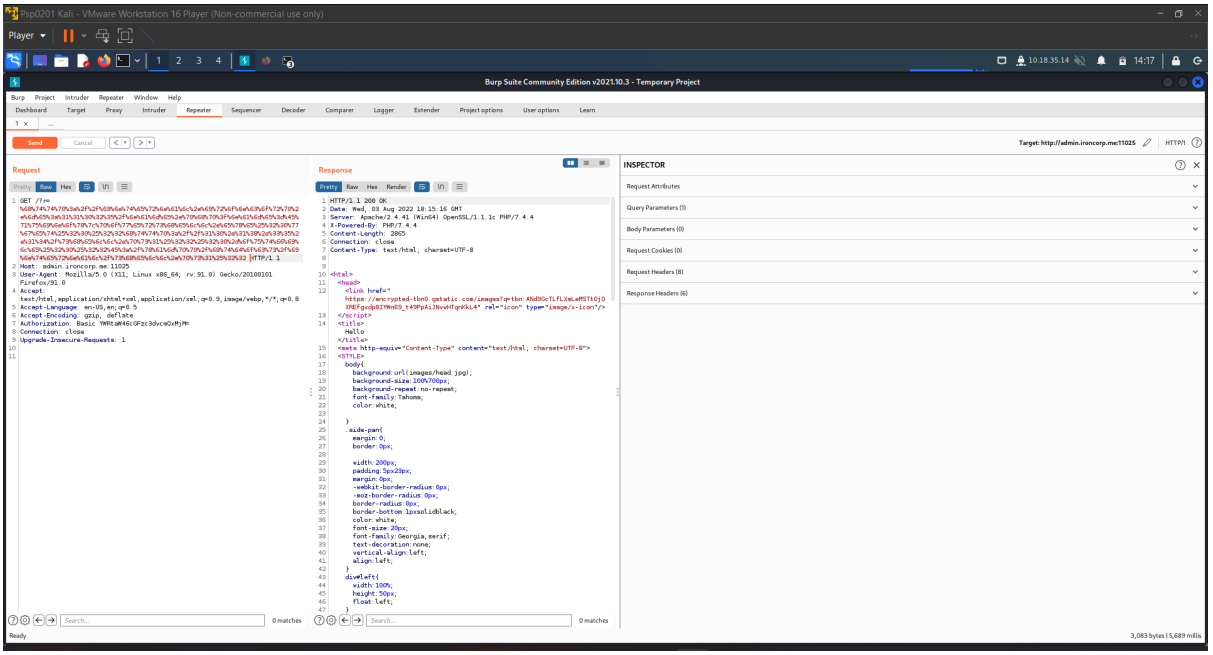
After that, we check what is inside of the website by doing | dir.



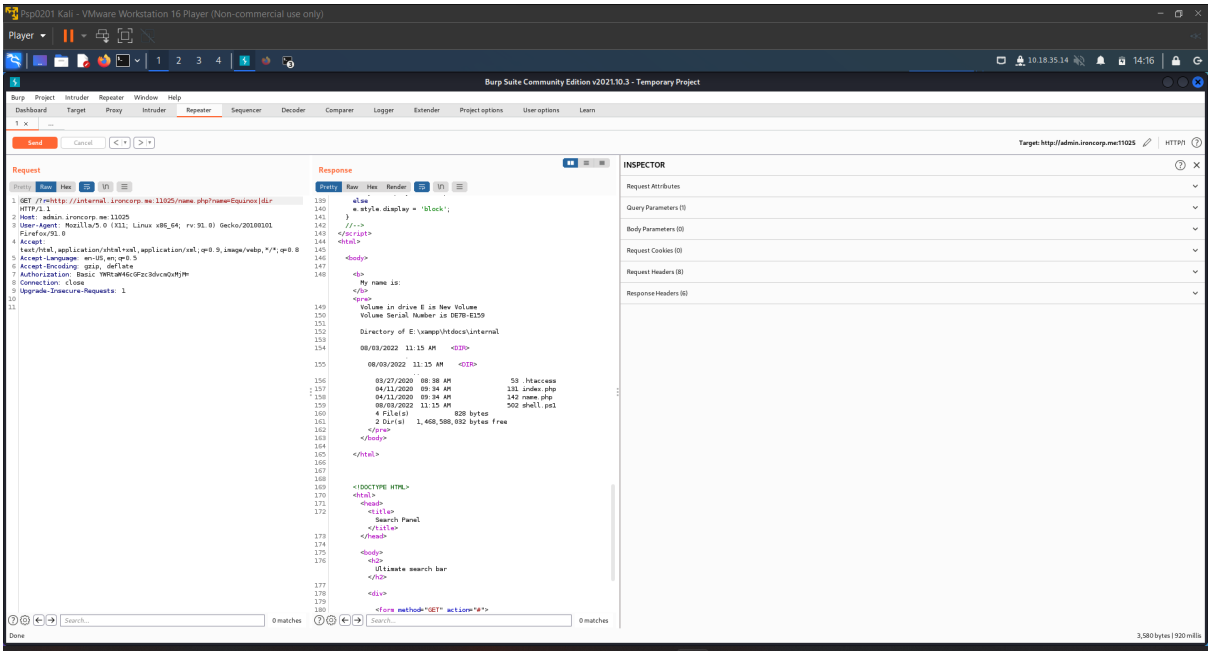
Next, we opened BurpSuite and activated our Foxyproxy in the browser. Configuring and try and error using BurpSuite, we forward some of the things shown to us and then refresh the page once again. This will display another thing in BurpSuite. We then try to click on it and send it to the repeater while turning the intercept off. From the repeater we must send it to the decoder to decode the information to the url format.

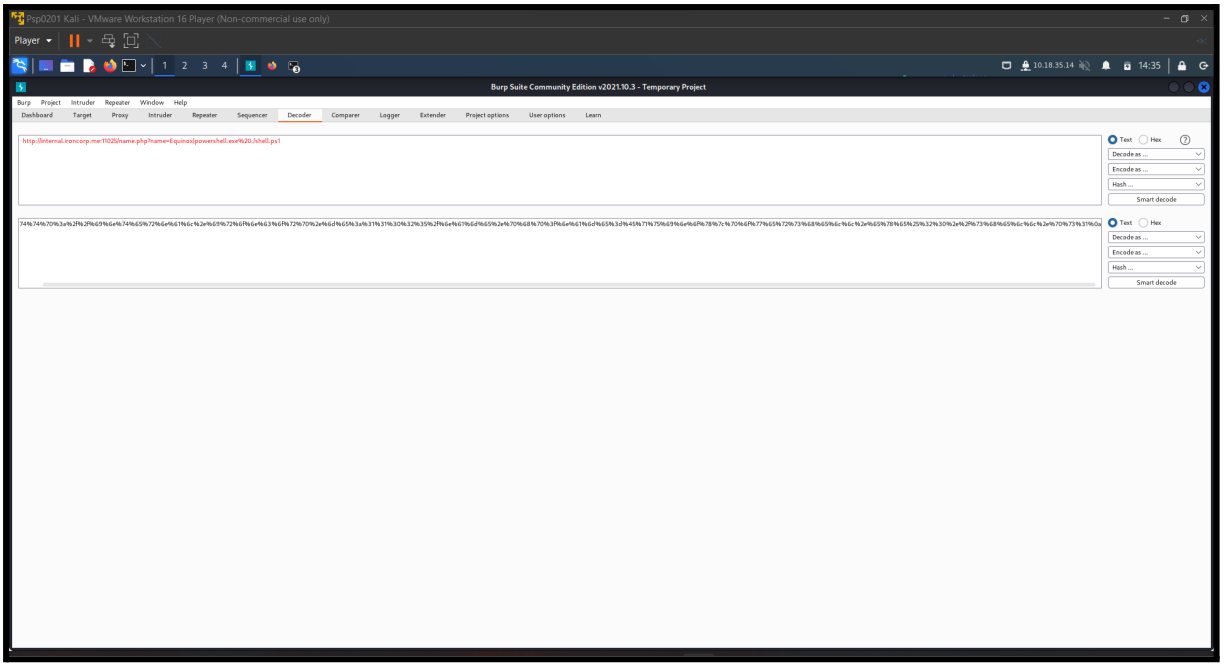
We copy and paste the url encode into the repeater and then we send it and wait for the response.

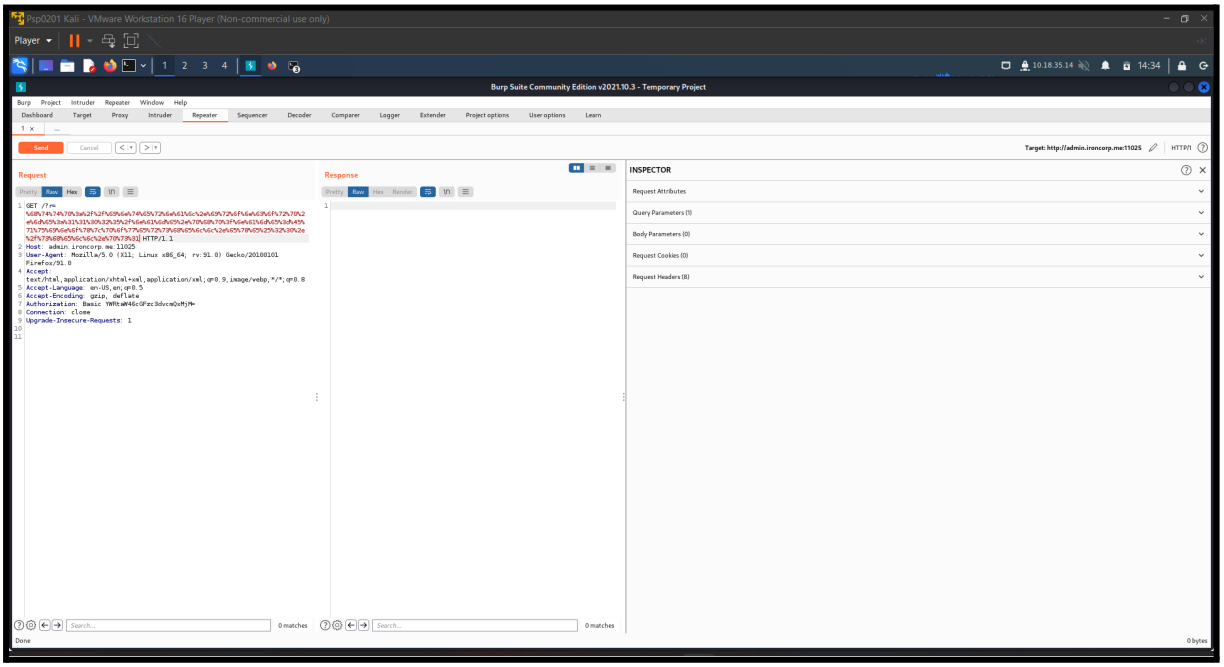




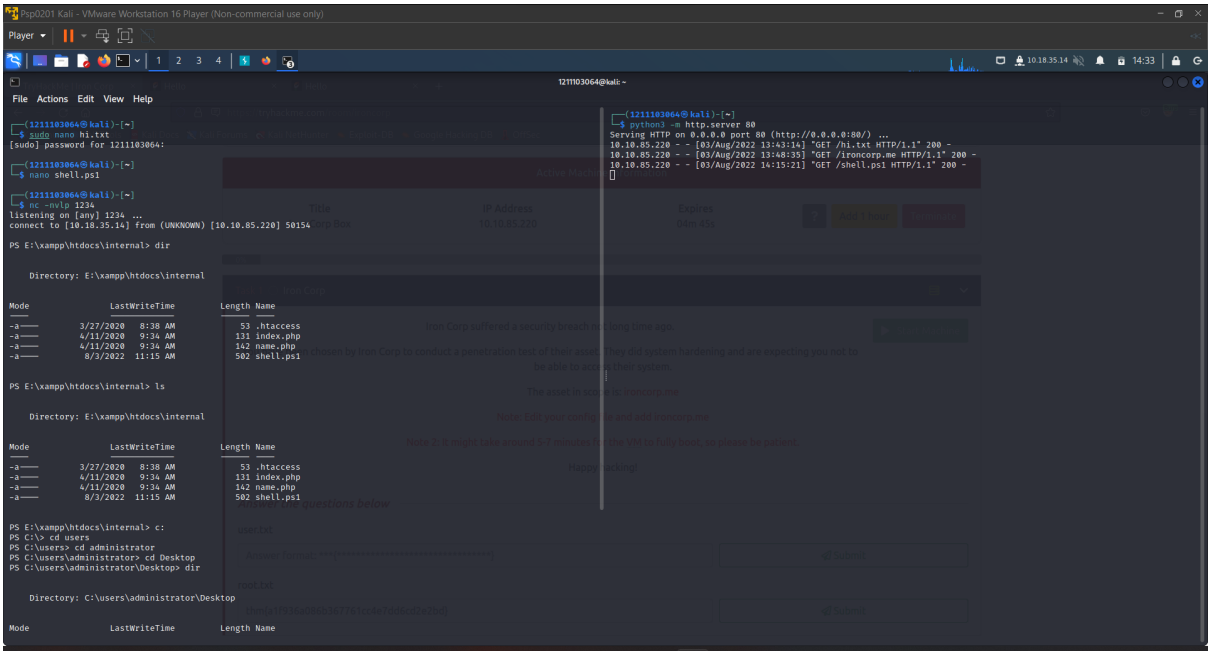
After getting the response, we proceed to the next step, which is to check if the shell is there or not.



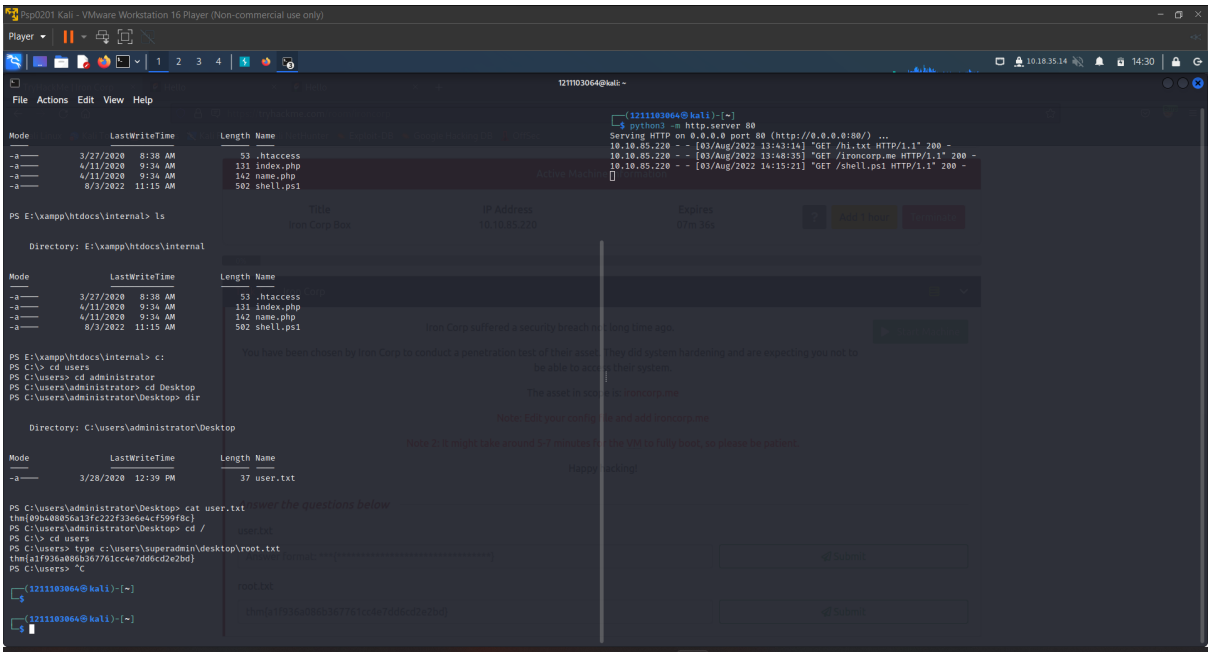




After that, we are finally connected to it.



After netcat successfully connected us, we then can find both of the flags. We first navigate through the directory from users to administrators and finally to Desktop. We then use the '**dir**' command to list everything there is. The **user.txt** file will be displayed. We then typed in '**cat users.txt**' in order to print out the information inside of it. That will display the user flag.

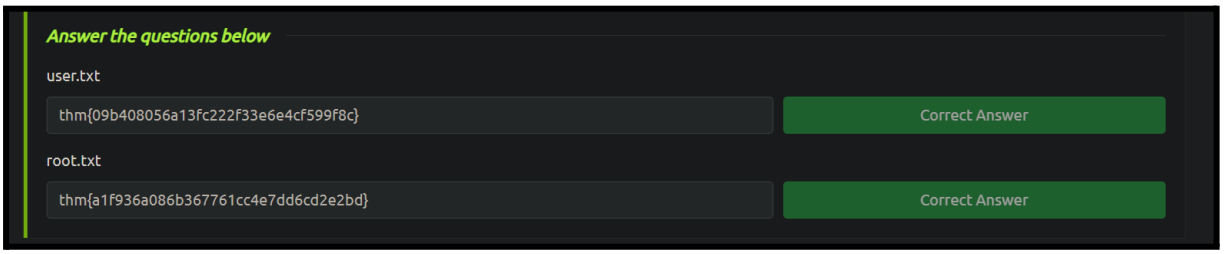


To find the root flag we must navigate through users, then superadmin, and finally Desktop. We then can find the root flag by typed in the command :

'**type c: \users\superadmin\dekstop\root.txt**'

This will display the root flag for us.

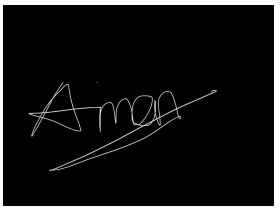
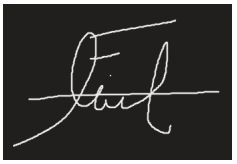
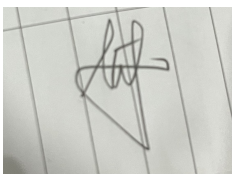
Final Result: (if you did not manage to solve, just mention you moved on to other questions)



Upon verification of the flag, we placed the flag 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
1211103064	Muhamad Aiman bin Mohd Ehwal	Intercept and acquire information using BurpSuite and Foxyproxy, decode url and sent our shell to the Equinox directory, did the Netcat listening and successfully connected to it.Did some part of the writeup and compile some of the pictures.	
1211103373	Muhammad Alif bin Khabali	Conducted Nmap scans, successfully obtained the username and password using Hydra to access the page, creating a foothold for first breach, edited our video and posted on Youtube.	
1211103085	Muhammad Farid bin Jayatan	Successfully entered as the authority, navigated through all the directories to acquire the flag, managed to locate both the user flag and root flag, did a good sum of the writeup, did a good few of the research to aid the team solve this Pentest.	
1211103451	Arif Muhriz bin Syamsul Fozy	Help aid to gather information, helped us solve certain problems, contributed to some of the writeup.	

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://youtu.be/xST2KUifioI