PSP0201 Pen Test 2

Room B - Iron Corp

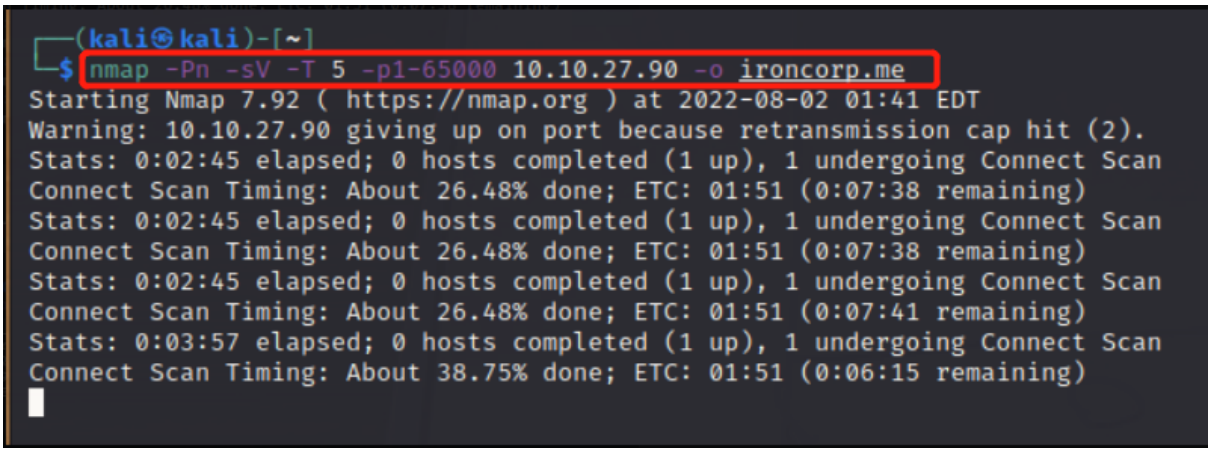
Group Name: Metamorphosis

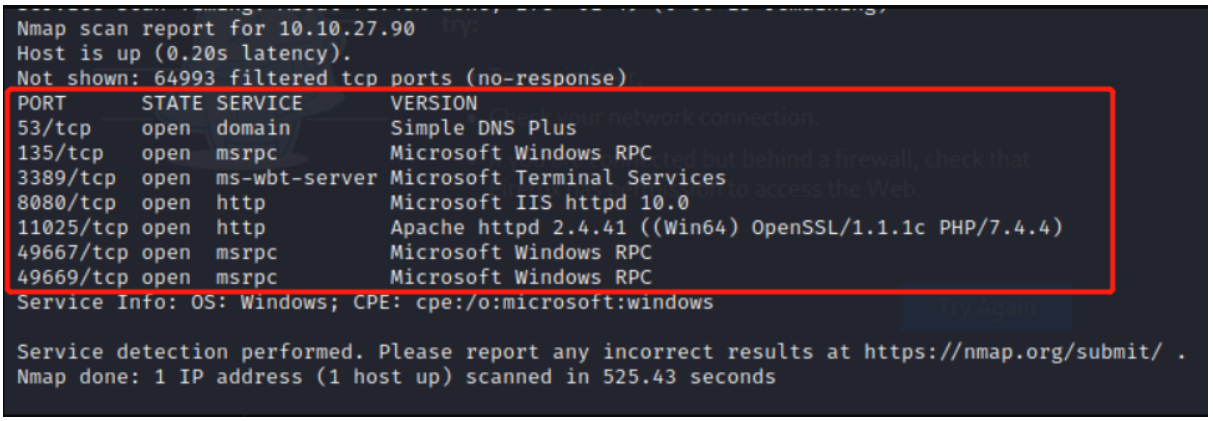
ID	Name	Role
1211101704	Aniq Danial Bin Mohd Adli	Leader
1211101790	Lee Heng Yep	Member
1211102806	Ong Kwang Zheng	Member
1211103063	Ng Weng Lam	Member

Recon & Enumeration

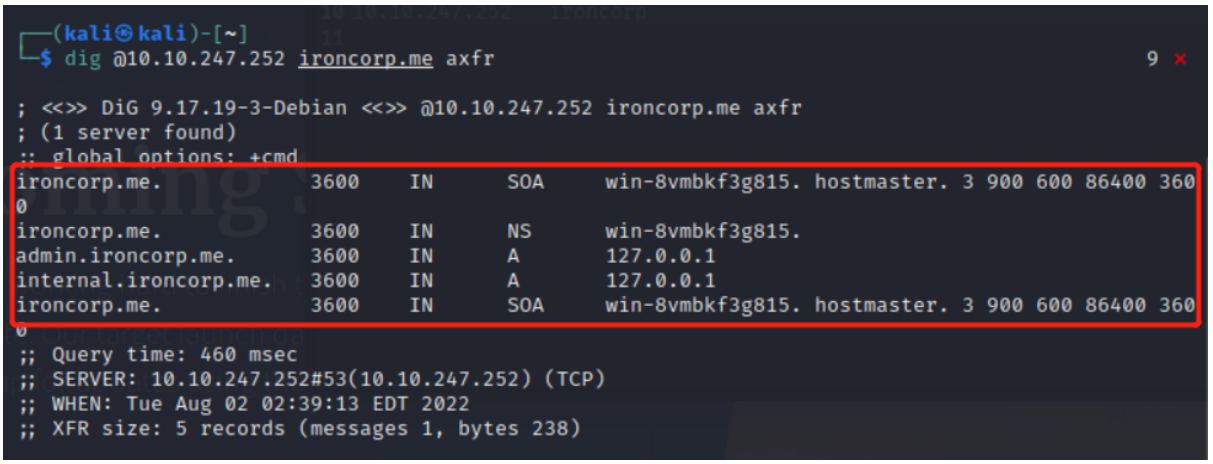
Members Involved: Lee Heng Yep
Tools used: Nmap, Dig
Thought Process/Methodology:

So, after we started the machine, the first thing we did was run the nmap command.However, we found that ping probes were being blocked.So, we used another command and we managed to find the ports there after scanning.



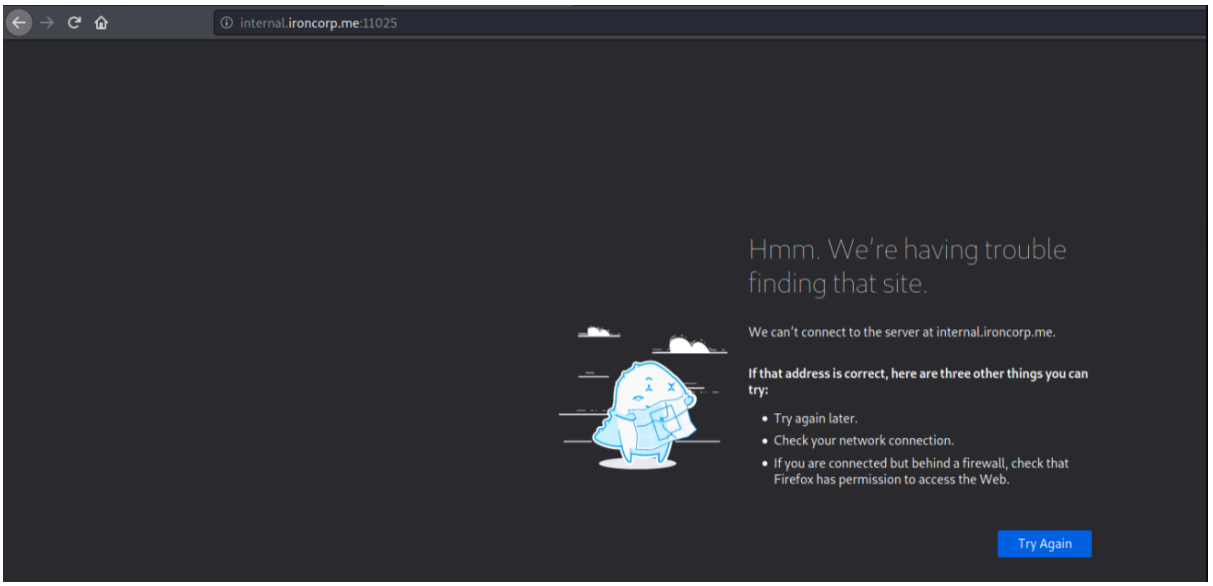


We use dig <machine_ip> to obtain some useful information. This will be useful later.

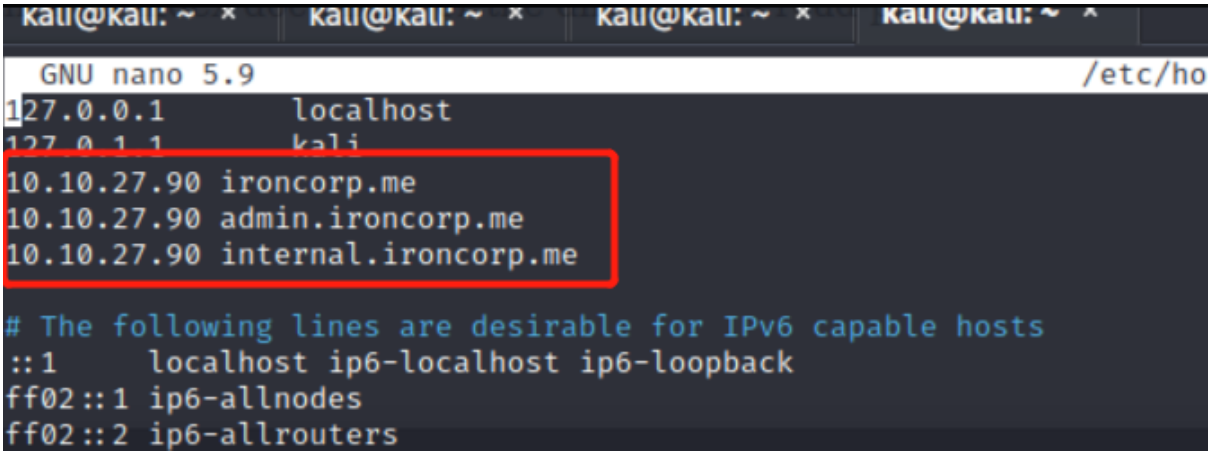


INITIAL FOOTHOLD

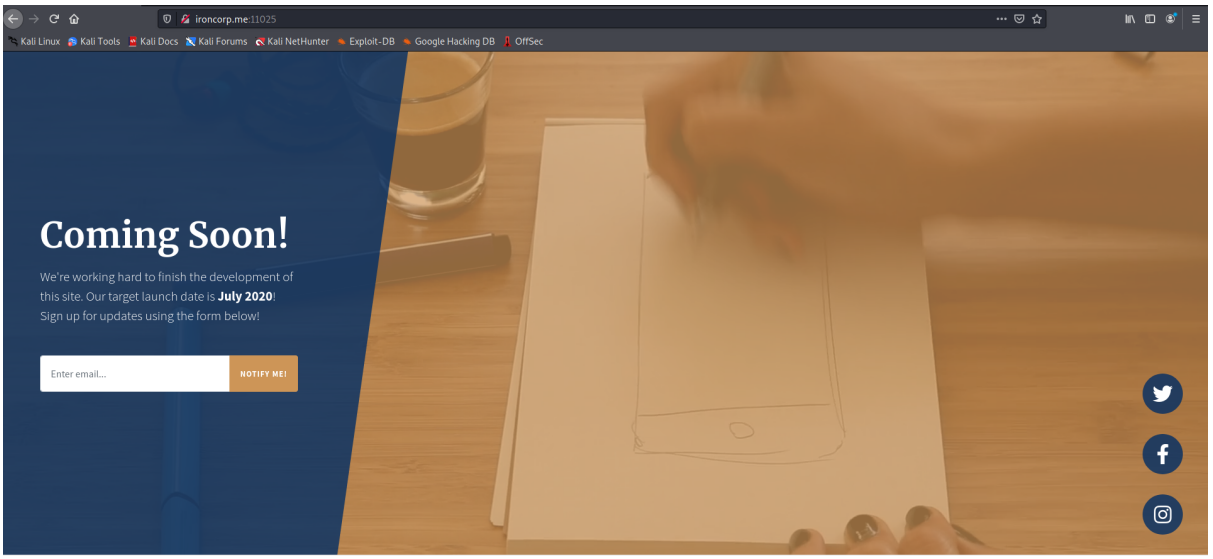
Members Involved: Ng Weng Lam
Tools used: Firefox, Kali, Hydra
Thought Process/Methodology:
So after that ,we met a problem which was that we couldn't connect to the server. After doing some research regarding this problem, we found that we forgot to edit /etc/hosts. To edit it we run sudo nano /etc/hosts.

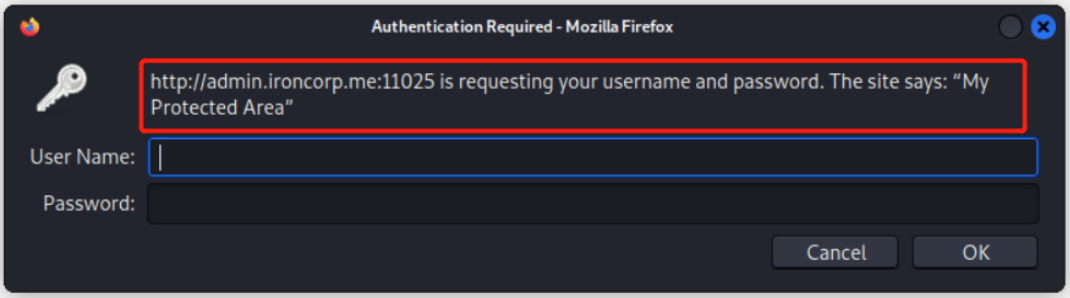


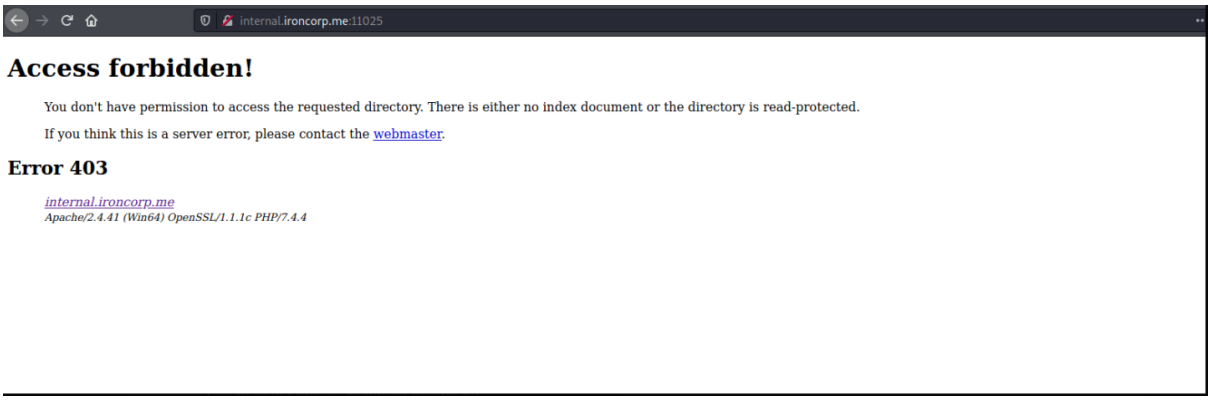
After that, we use the information that we got from digging and we edit the text file that was mentioned just now like the following screenshot.



After that we tried the ports that we scanned just now, we entered the port 1 by 1 and found the correct port which is (11025) and successfully entered the server but we found that there is only a space for us to enter our email inside the domain ironcorp.me. So we moved to the next domain admin.ironcorp.me and found that we need username and password to log in but we don't have one. We move to another domain which is internal.ironcorp.me as well and we found nothing inside there







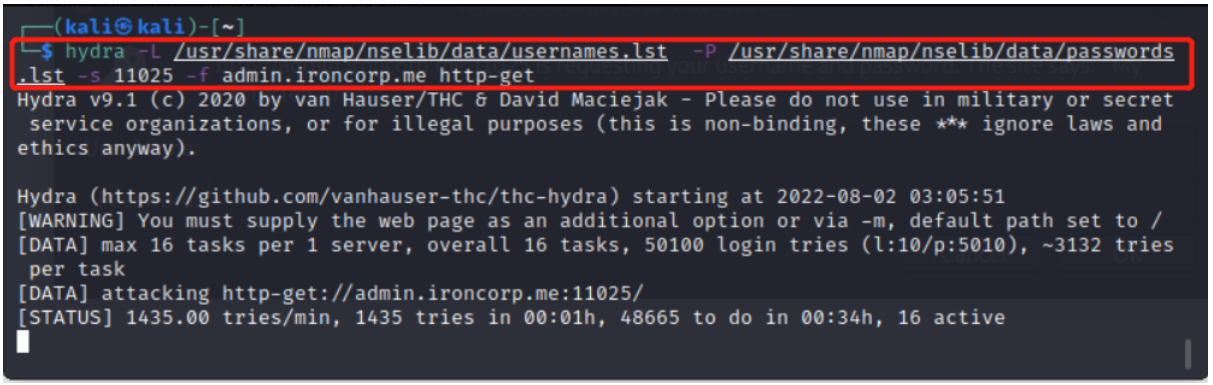
So next, we use **Hydra**

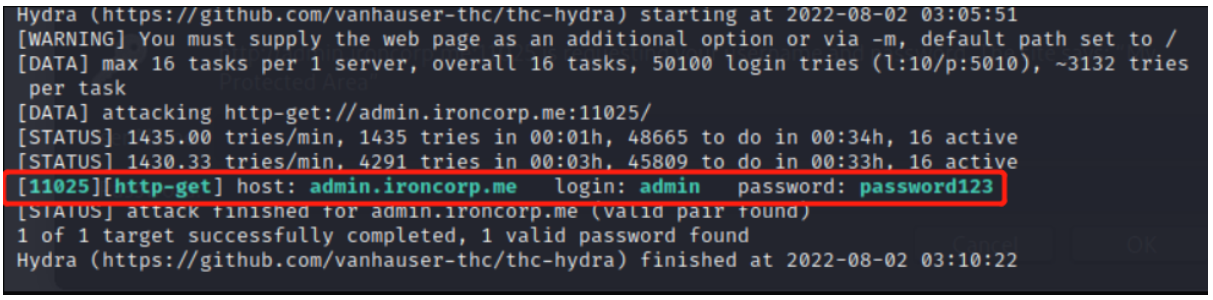
> Hydra (or THC Hydra) is **a parallelized network login cracker** built in various operating systems like Kali Linux, Parrot and other major penetration testing environments. Hydra works by using different approaches to perform brute-force attacks in order to guess the right username and password combination.

and we run command hydra -L /usr/share/nselib/data/usernames.lst -P

/usr/share/nmap/nselib/data/passwords.lst -s 11025 -f admin.ironcorp.me http-get /.

To get the file location we run locate usr.lst. While waiting for a while to let hydra do the attacking, we took a short break. After several minutes we finally got the username and password!

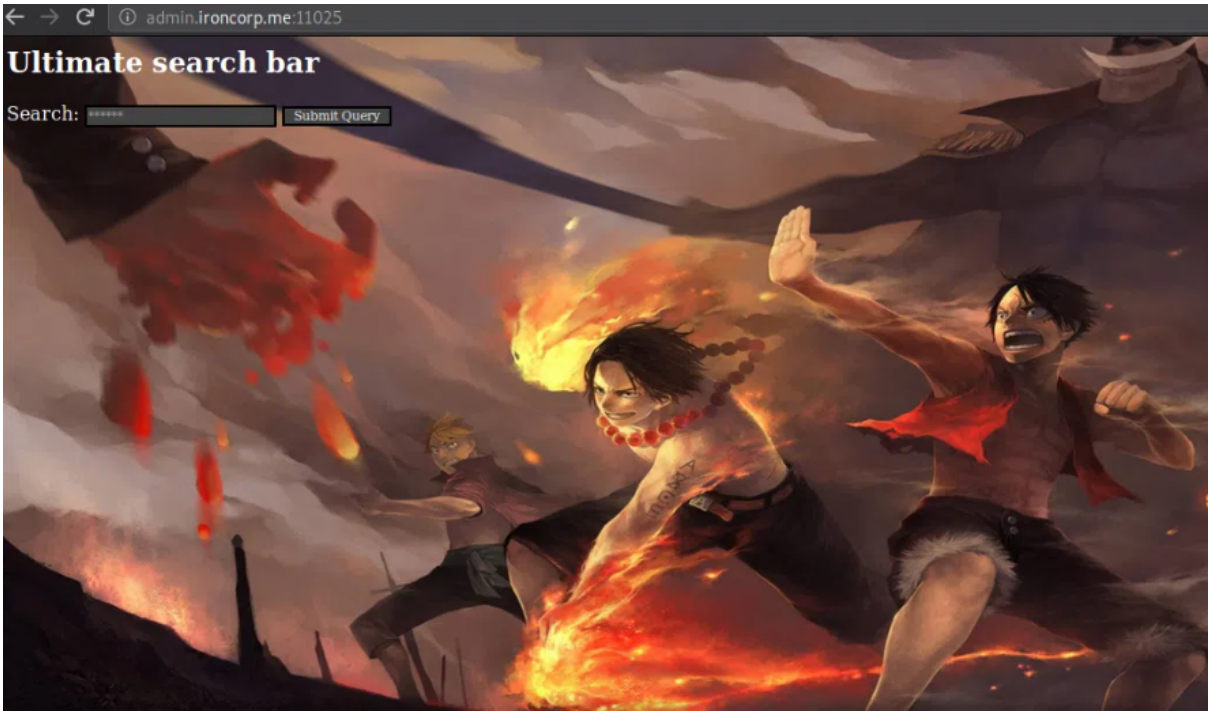




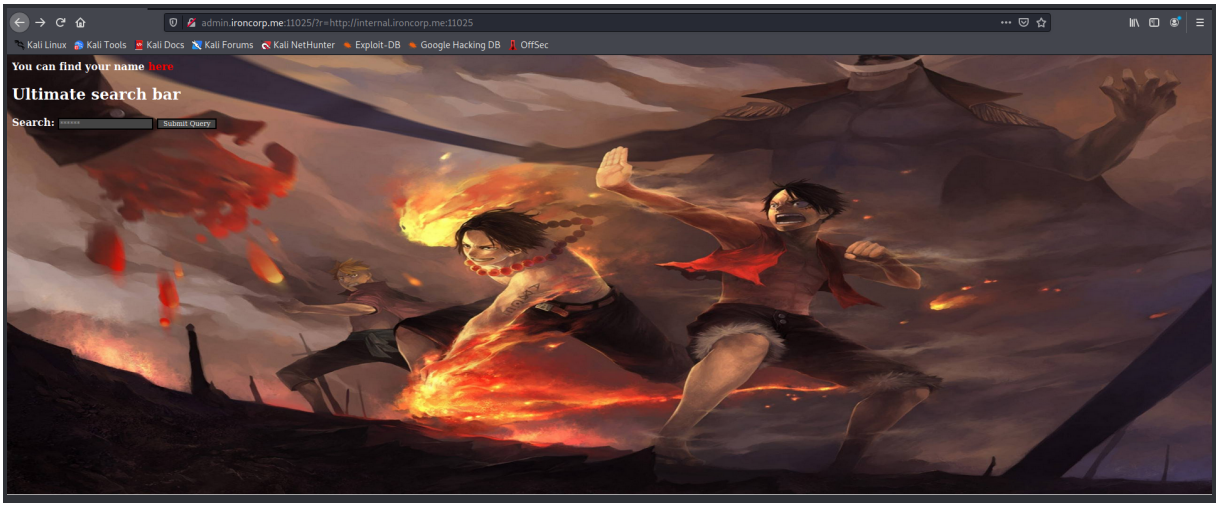
HORIZONTAL PRIVILEGE ESCALATION

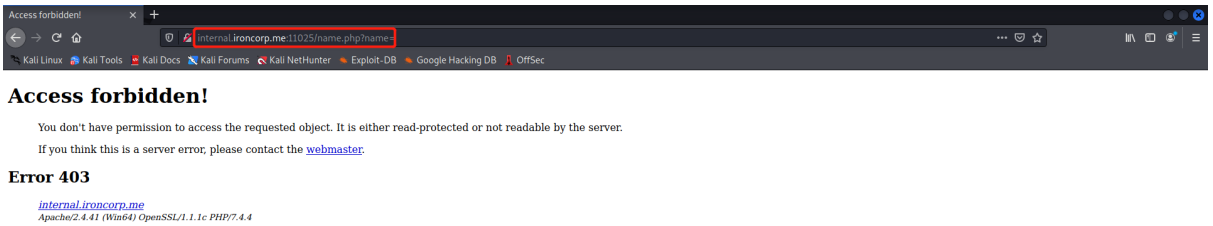
Members Involved: Aniq Danial Bin Mohd Adli
Tools used: Firefox, Powershell, Kali,
Thought Process/Methodology:

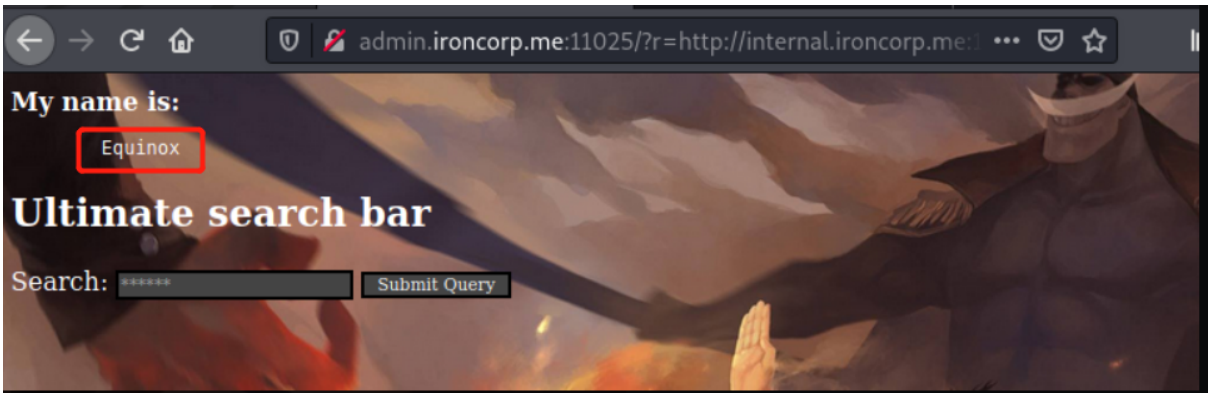
So after logging in **admin.ironcorp.me** with the username and password we got up there.we will redirect to a new page with a very cool Luffy , Ace and WhiteBeard background.

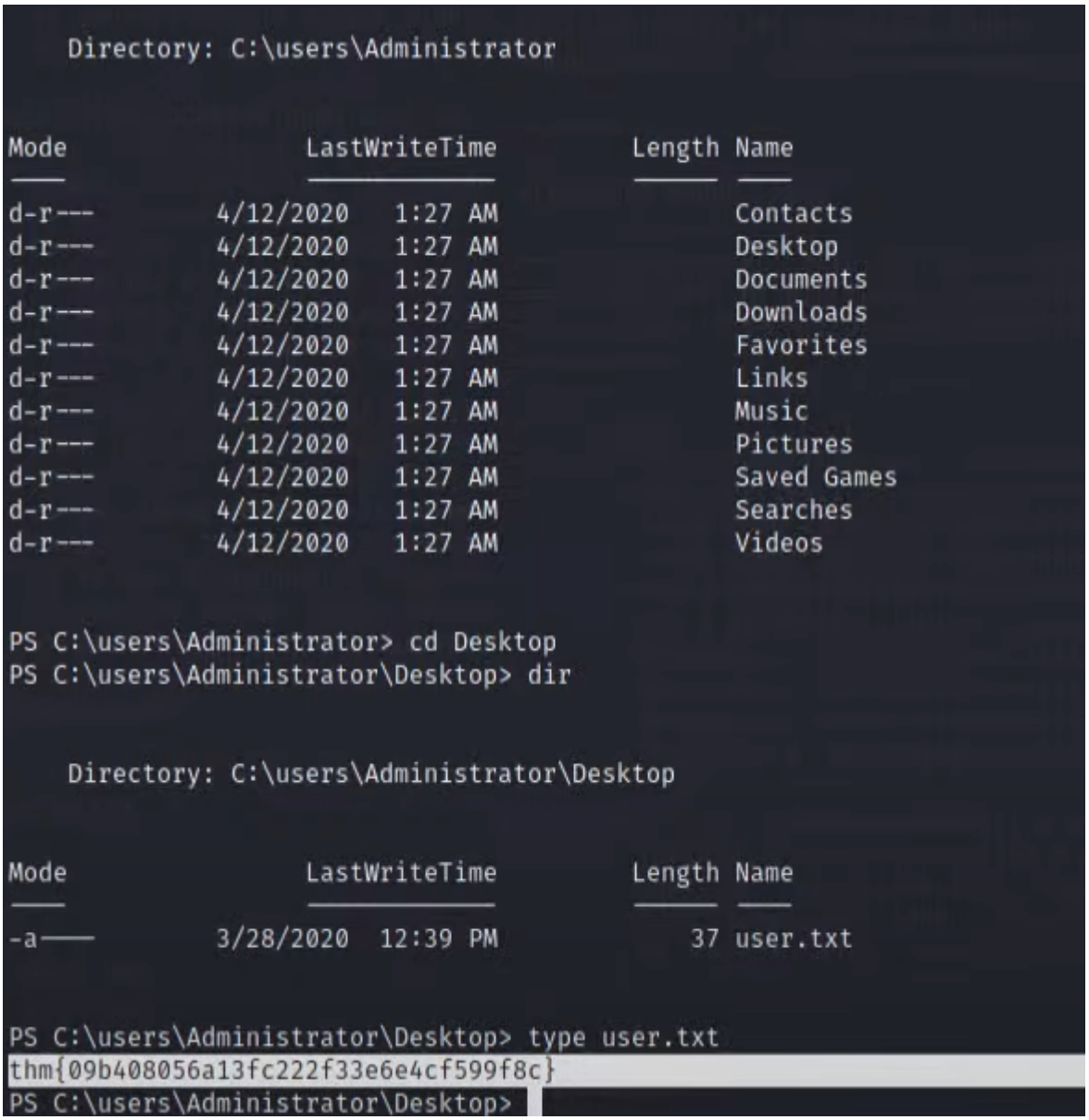


We were lost here for a few minutes since there was only a space for us to search for something.So we tried to combine the two links we got just now which are **internal.ironcorp.me** and **admin.ironcorp.me** and we redirect to a page with a button here.However, when we thought that we got to the next step after clicking the button.We were redirect to the internal.ironcorp.me but we observed that there is something different with the URL .So,we tried to add the name.php?= to the link we combined just now and we got a new thing there **Equinox.**









After a bit of trial and error, we managed to establish a reverse shell and get into the machine. We can then navigate to **C:\users\Administrator\Desktop** to find the file called **user.txt** and capture the first flag.

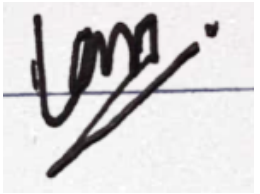
flag:thm{90b408056a13fc222f33e6e4cf599f8c}

ROOT PRIVILEGE ESCALATION

Members Involved: Ong Kwang Zheng
Tools used: Metasp
Thought Process/Methodology:

To find the final flag, some privilege escalation is needed. It is located at **C:\users\SuperAdmin\Desktop** in a file called **root.txt.**For the rooting part,we used **metasploit** to get a **meterpreter session.**After we obtaining user's tokens, we use them to get the flag for root.txt.We got too frustrated with this disaster of the room and realise that we forgot to take screenshots after all and frankly there is not much time for us to redo the whole thing again so we decided to accept the truth that we forgot the screenshots.Once again,we apologise for the amateur mistake even we know that this is not the excuses that we made such mistake.

flag:thm{a1f936a086b367761cc4e7dd6cd2e2bd}

ID	NAME	CONTRIBUTION	SIGNATURES
1211101704	**Aniq Danial Bin Mohd Adli**	- Logged into page using credentials acquired by Heng Yep - Acquired the first flag - Video Editing	
1211101790	**Lee Heng Yep**	- Reconed for open ports and subdomains - Helped to get username and password for admin. Subdomain - Video Editing - Despayourlastsito	
1211103063	**Ng Weng Lam**	- Found the correct port for the website and tried every single domain and got nothing inside :). - Run Hydra to get the username and password.	
1211102806	**Ong Kwang Zheng**	- Did the rooting part and got the flag for root.txt - Also forgot to take screenshots to add in the writeup report.	

VIDEO LINK: https://youtu.be/QNmn-HEY1ZQ