PENTEST 2
ROOM A
CYBORGS

MEMBERS

ID NUMBER	NAME	ROLE
1211102066	Hemma Ravindran	Leader
1211100614	Tivaasheny Ananthan	Member
1211102168	Nicholas Cheok Jia Jie	Member
1211100986	Sarvesh Munusamy	Member

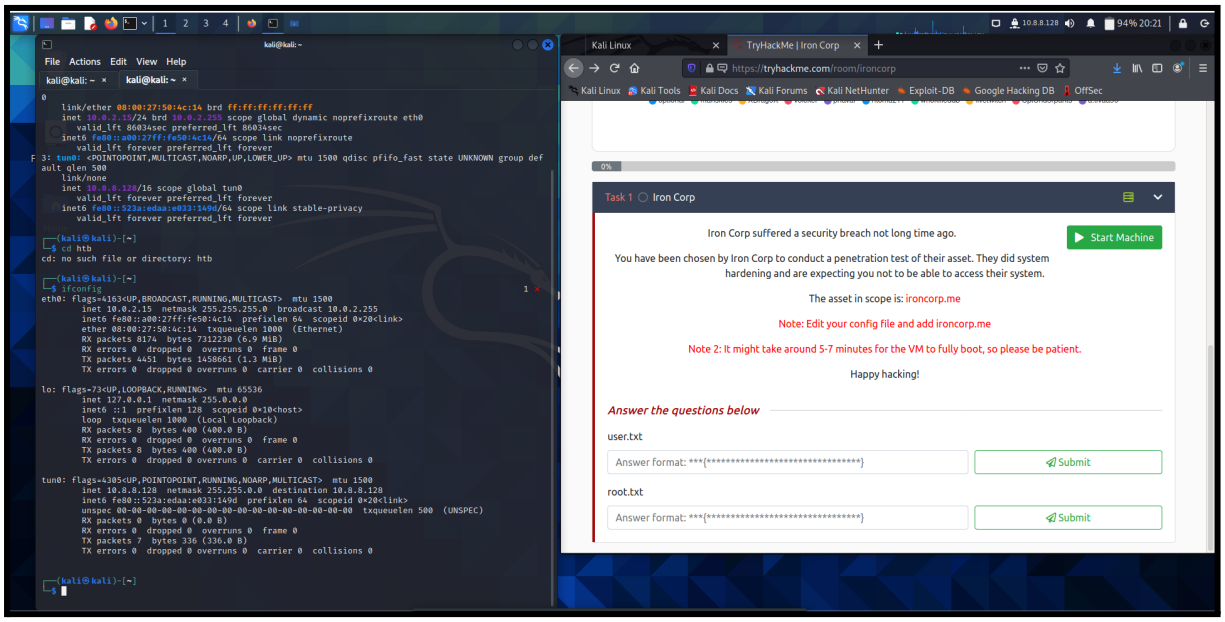
Steps: Recon and Enumeration

1) Reconnaissance

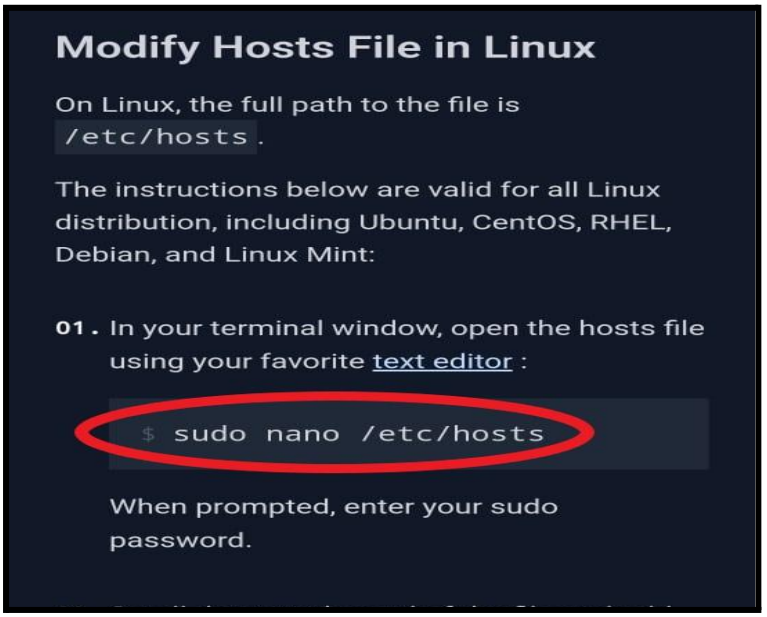
Members Involved: Tivaasheny Ananthan

Tools used: Nmap, firefox and kali terminal

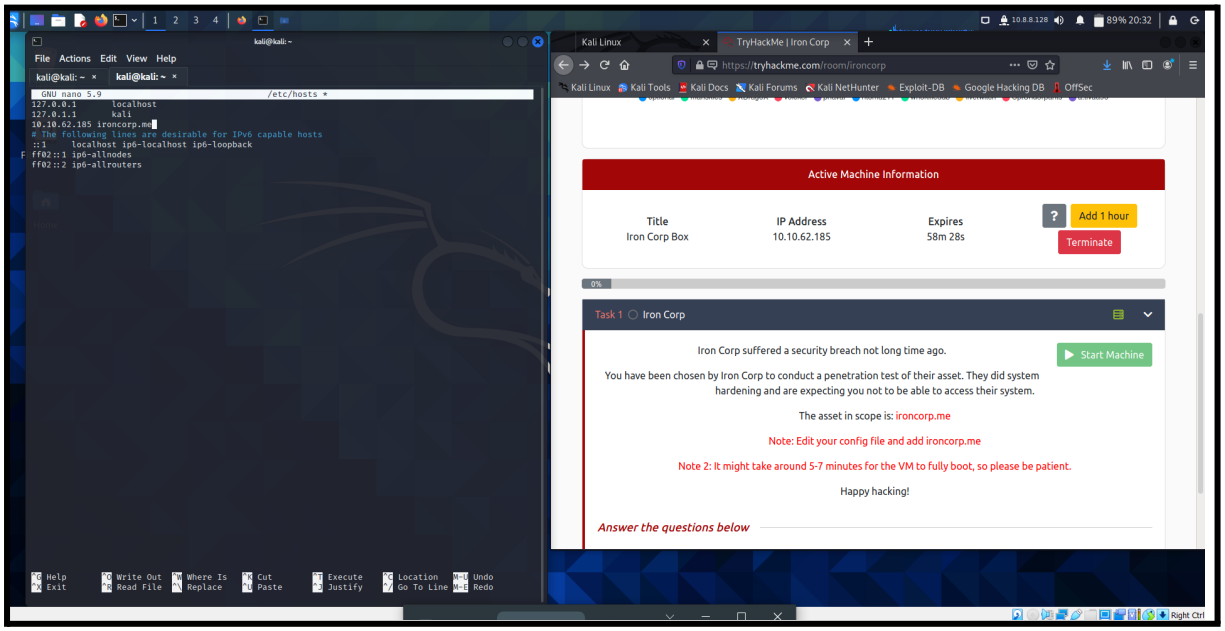
Firstly, i checked whether did we already connect with the access machine by using openvpn. I typed ifconfig in terminal.



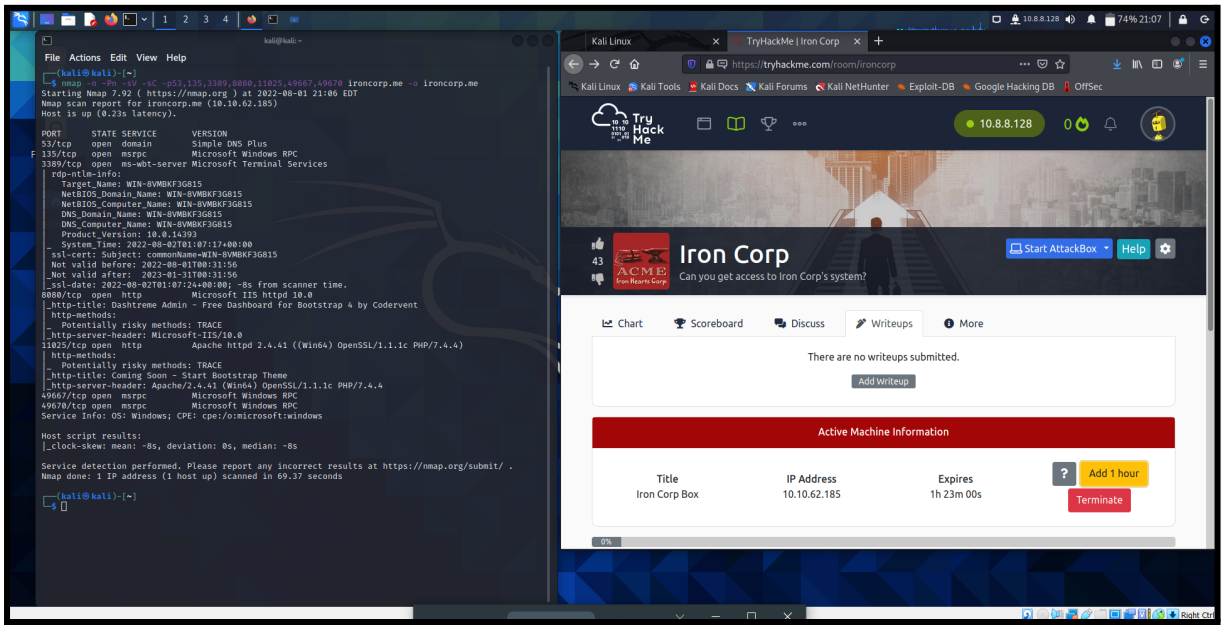
Then when I tried to type nano /etc/hosts by referring to the youtube I couldn't manage to save the host file. Thus, I googled and finally managed to get the proper command.



Then I typed sudo nano /etc/hosts and inside the host file I entered my IP address ironcorp.me. Then press ctrl X to exit followed by ctrl Y to to save and ctrl MD.



Next, we need to execute the nmap so i typed(nmap -n -Pn -sV -sC -p53,135,3389,8080,11025,49667,49670 ironcorp.me -o ironcorp.me) command to scan the nmap.



Thought Process and Methodology and Attempts:

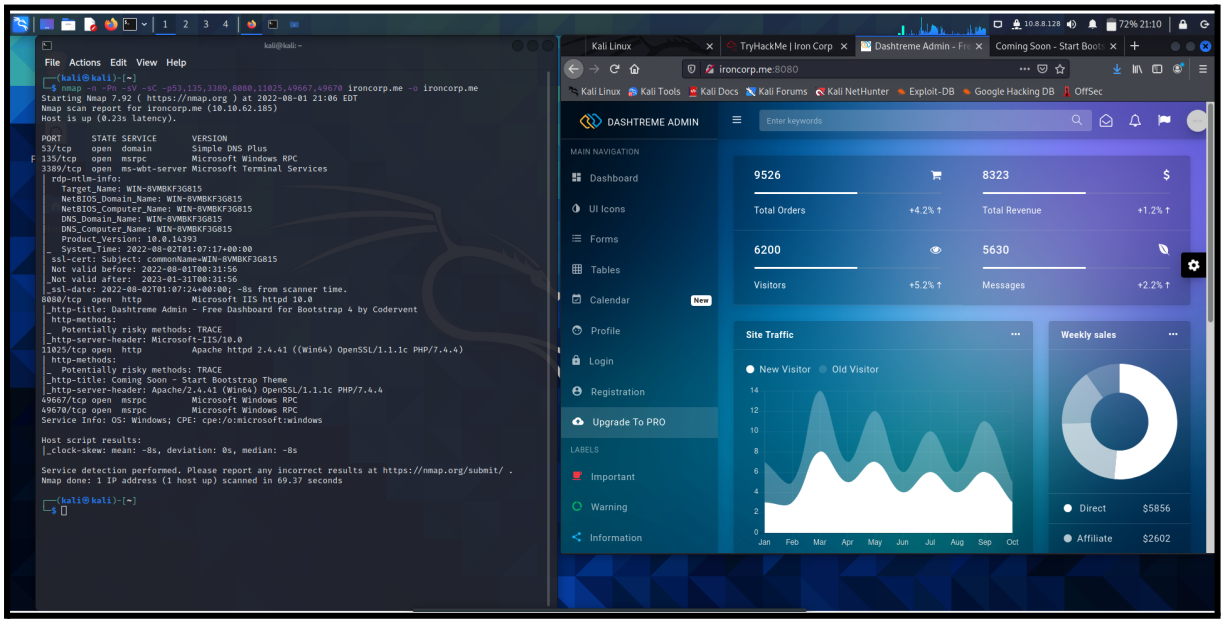
We have to save ip address ironcorp.me in hosts file. Then execute nmap to scan it.

2)Enumeration

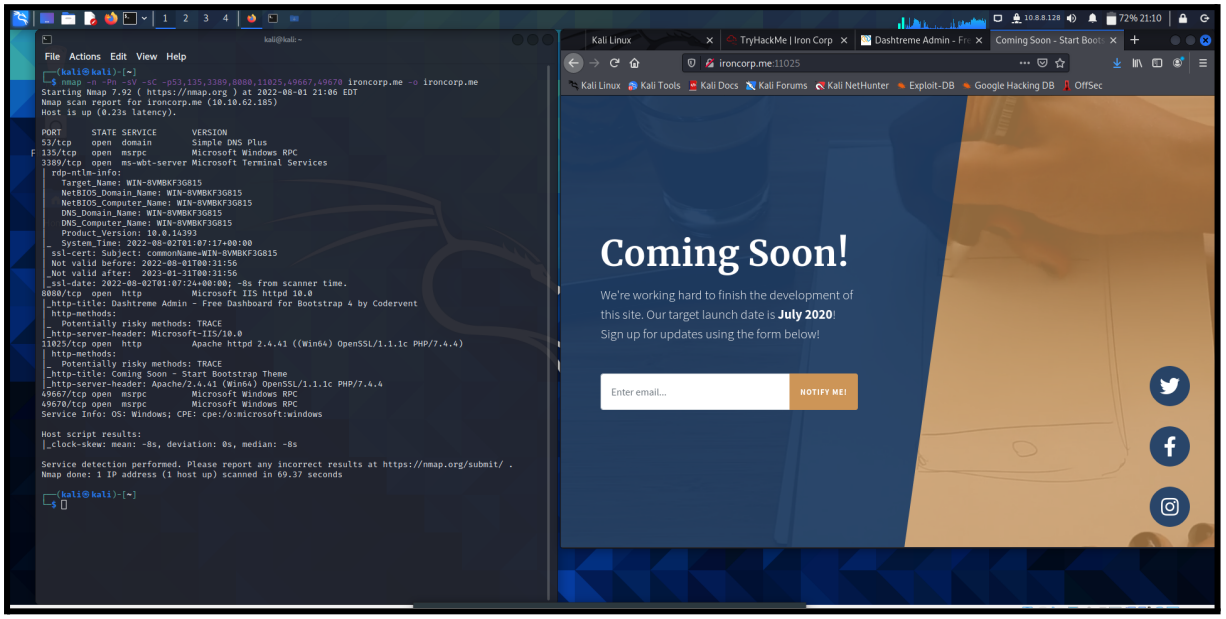
Members Involved: Tivaasheny Ananthan

Tools used: Nmap, wordlists, firefox, and kali terminal

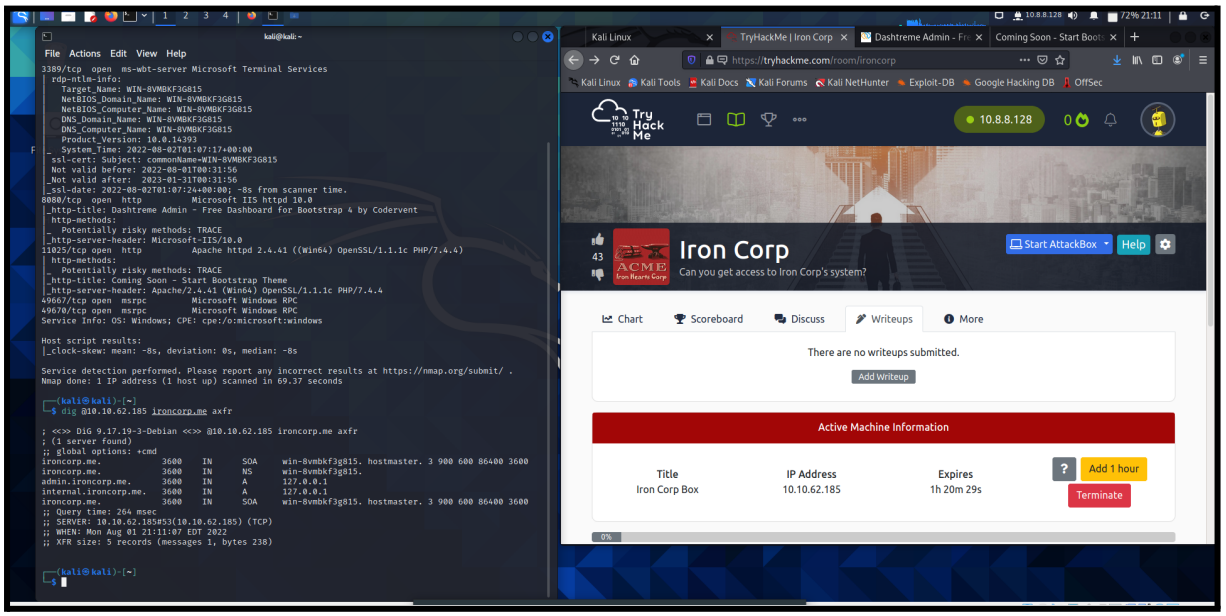
We have to access webservice of port 8080. So type ironcorp.me:8080 in firefox.



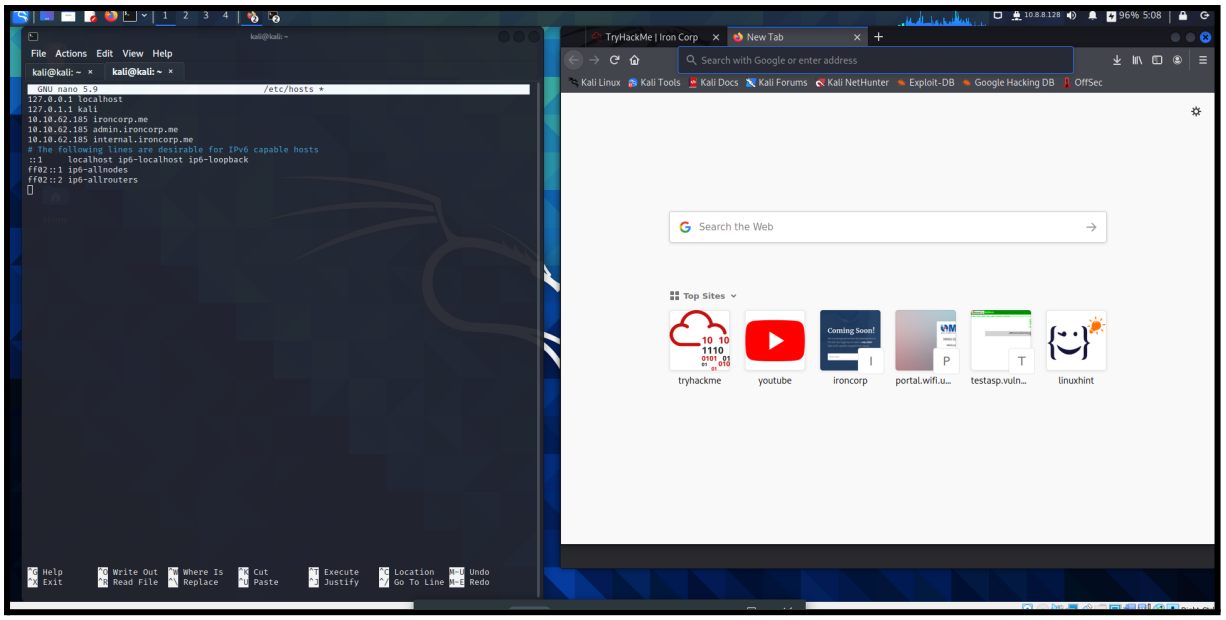
Then we have to access the wes server at port 11025 by typing ironcorp.me:11025 in firefox.



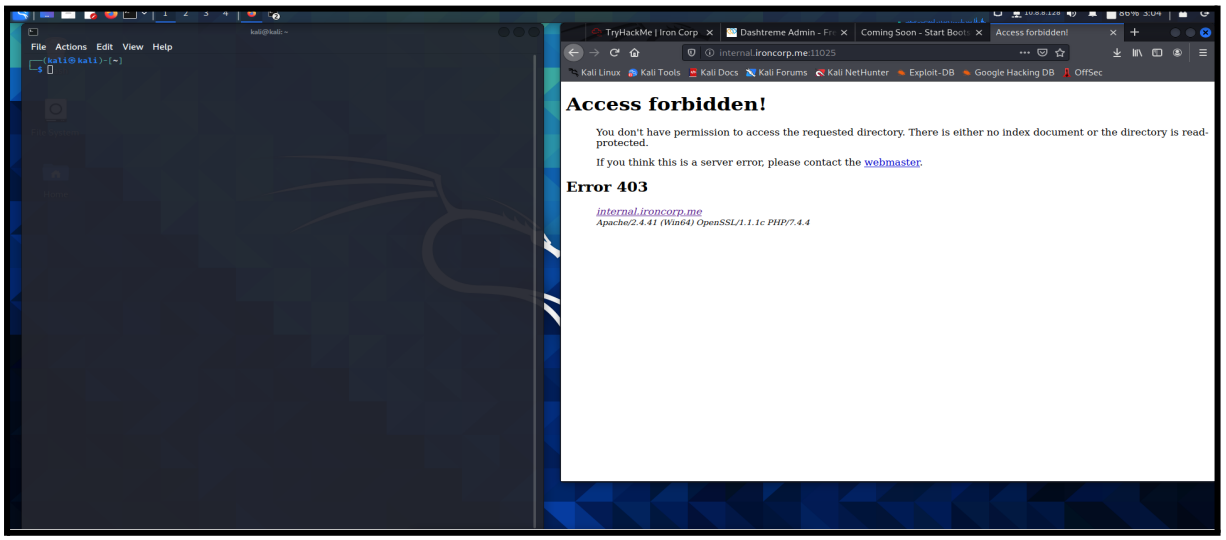
Type dig@IP address ironcorp.me axfr to get the subdomain. There will be 2 subdomain which is admin.ironcorp.me and internal.ironcop.me.



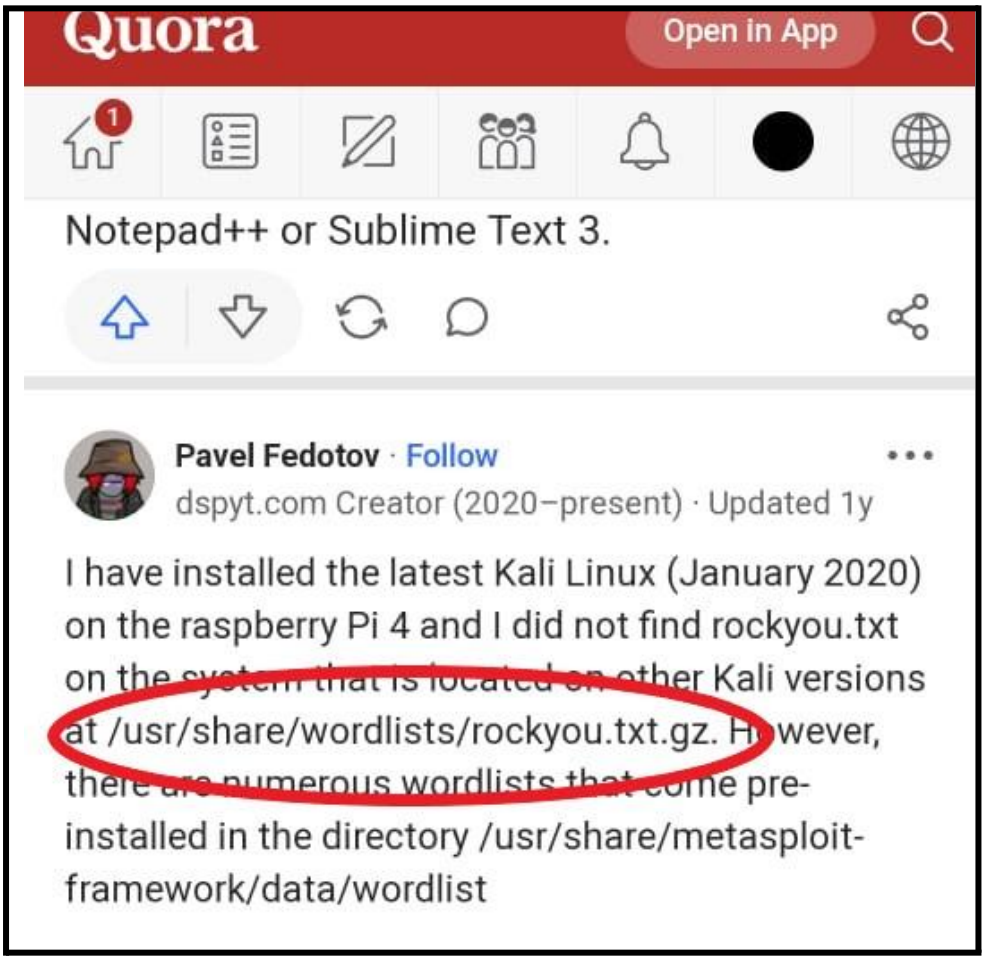
Then i saved both subdomain in host file in sudo nano /etc/hosts and type both subdomain below my ironcorp.me n begin with IP address as shown in below.



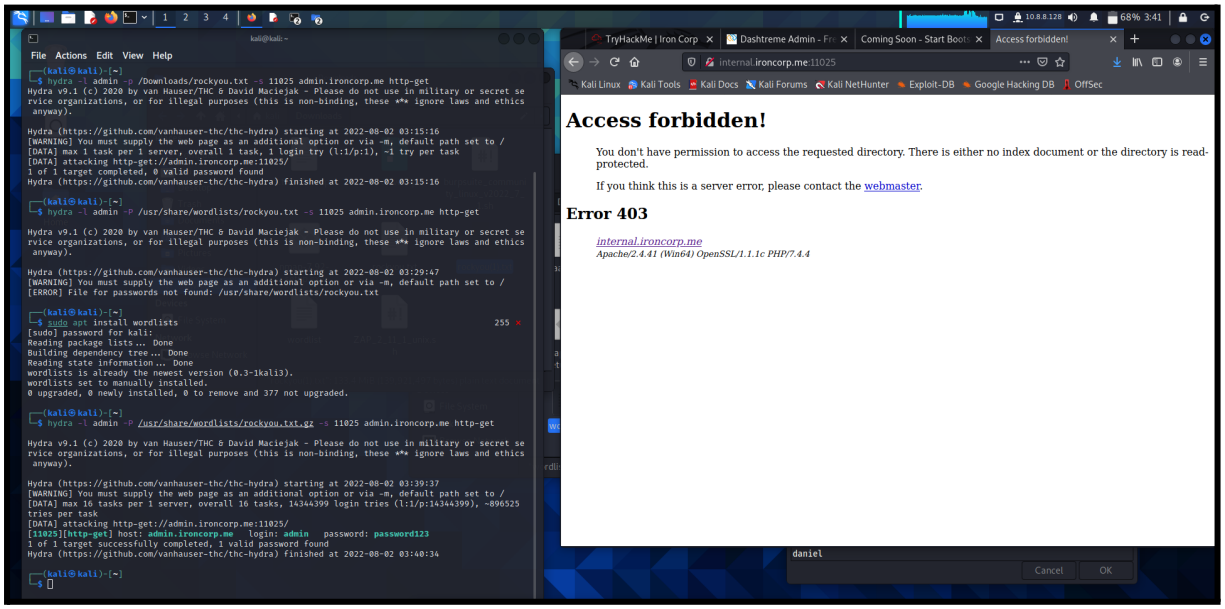
Then I searched for internal.ironcorp.me:11025 and access forbidden and error 403 appeared.



Then i face a problem to get login and password so i tried to google it and managed to get a proper command.

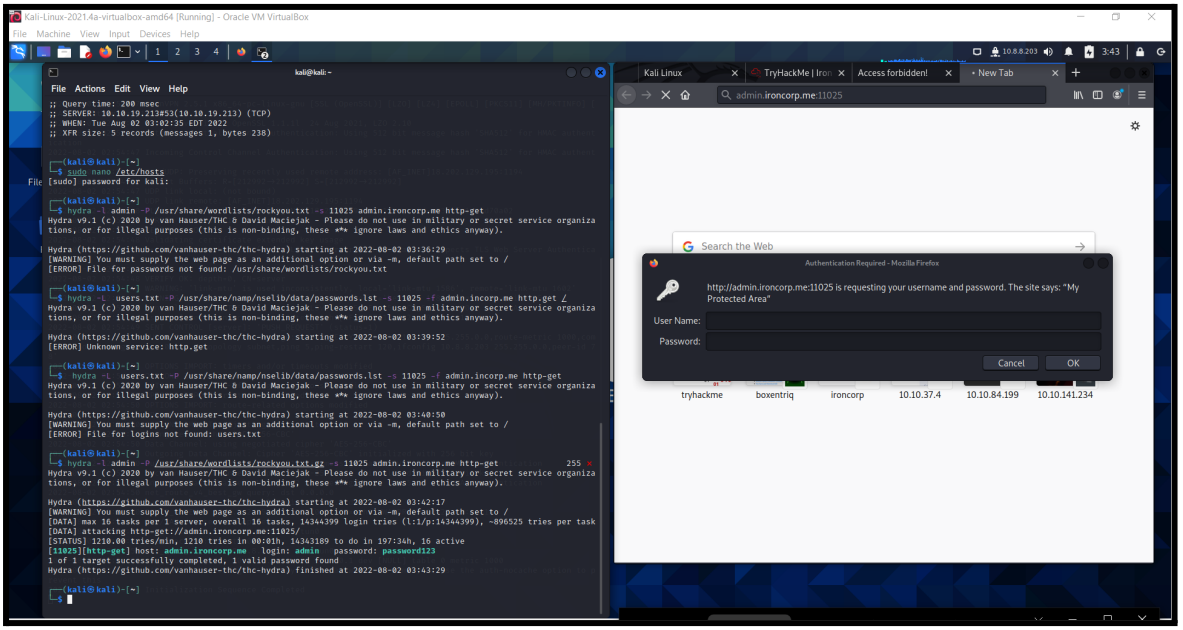


Finally, i managed to get login and password with using hydra.

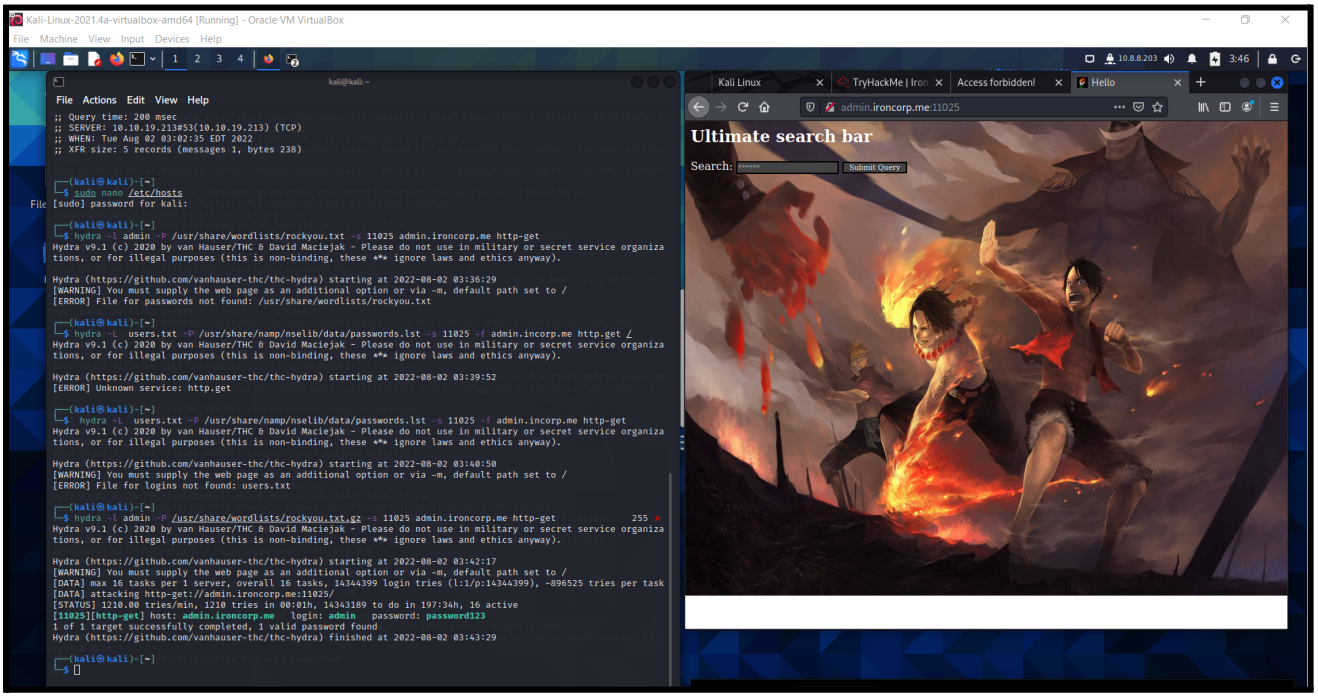


Members Involved: Hemma Ravindran
Tools used: hydra, firefox and kali terminal

Hydra is employed to assist us, the user is "guessed" at, and a dictionary of the 10,000 most popular passwords is used.



We've added a new location where you may submit a form to request information.



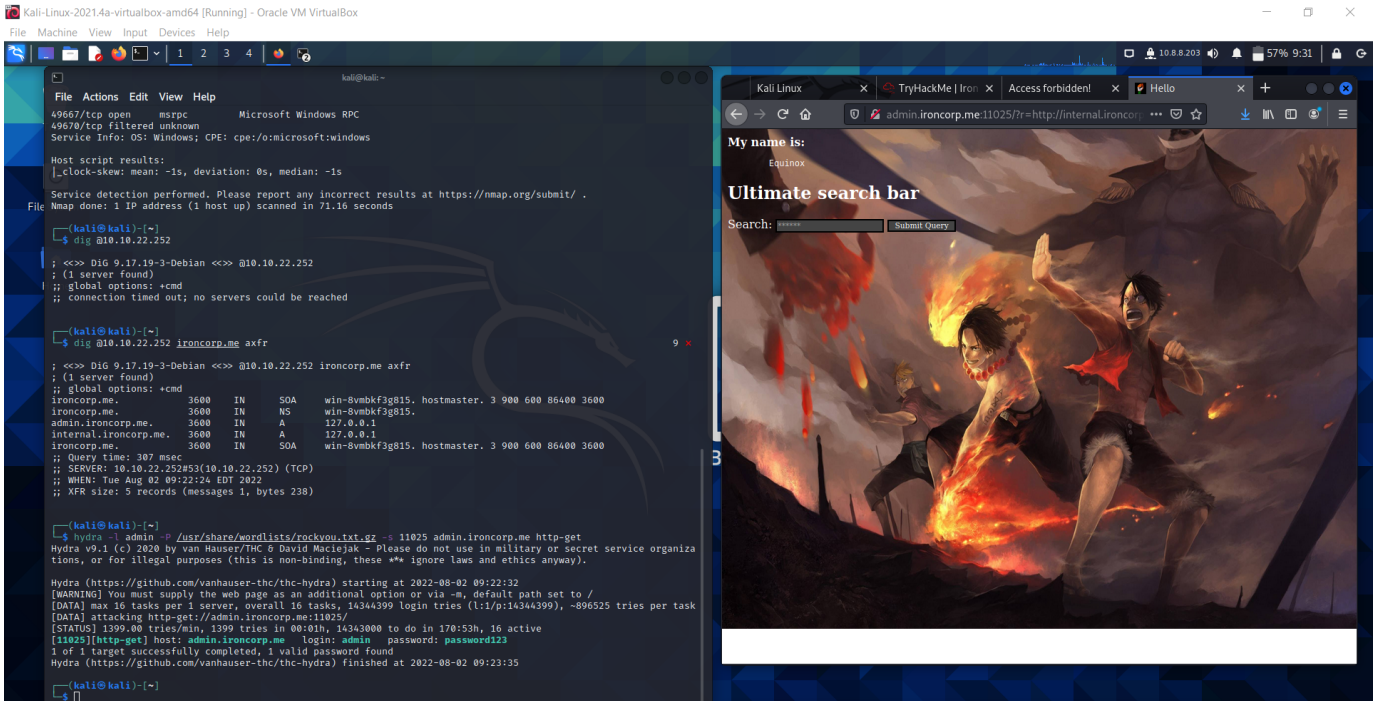
Thought Process and Methodology and Attempts:

We have to access web service of port 8080 and 11025. Type dig@IP address ironcorp.me axfr to get the subdomain. Save both subdomain in host file in sudo nano /etc/hosts and type both subdomain below my ironcorp.me n begin with IP address. Search for internal.ironcorp.me:11025. Managed to get login and password with using hydra.Put the username and password in the admin page and got the form to request information.

3) Exploiting

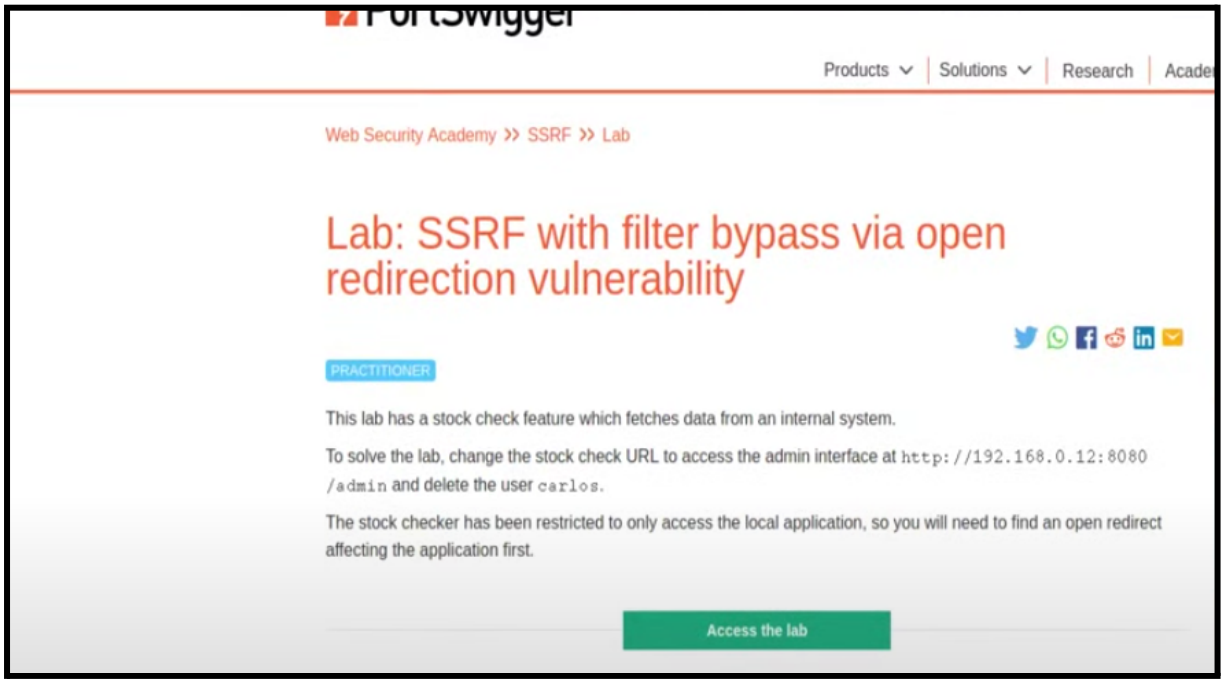
Members Involved: Hemma Ravindran & Sarvesh Munusamy & Nicholas
Tools used: Nmap, wordlists, firefox, kali terminal, burpsuite

After running a number of tests to determine the type of vulnerability we are dealing with, we discovered that the site is open to SSRF assaults.As a result, we can utilise it to do an internal port search and find new services that are only accessible internally. An attacker may use this to find internally exposed services and get around their firewall.

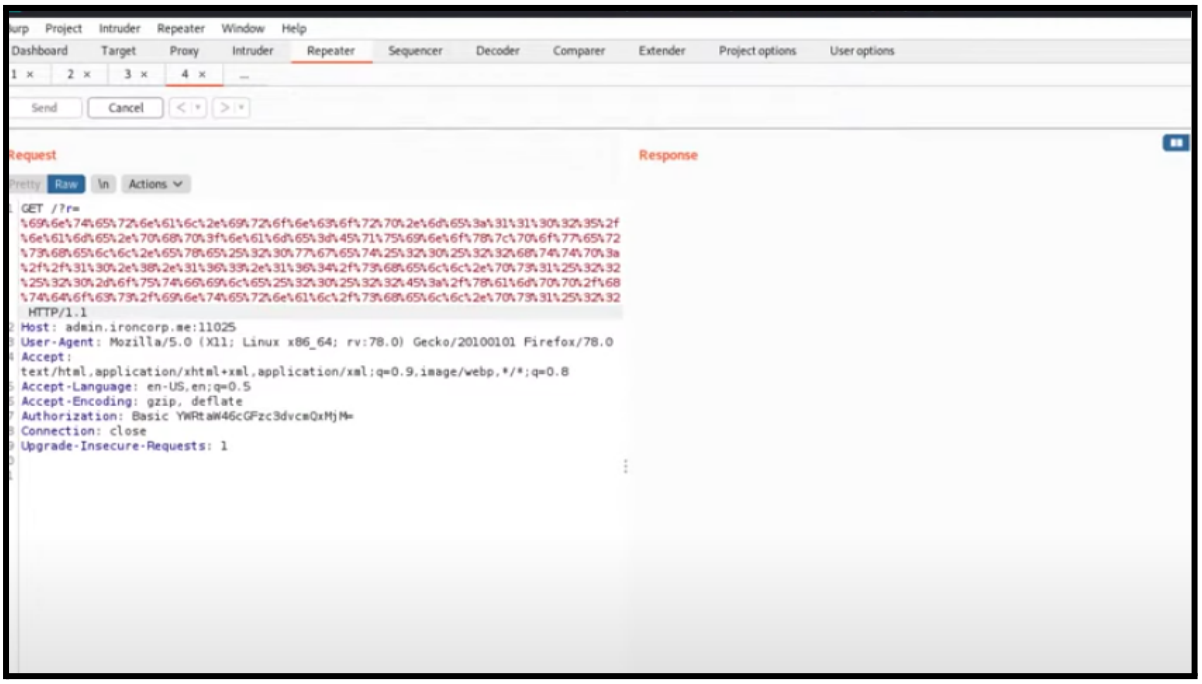


A variable that prints a user's name is visible when we look at the code. (Equinox)

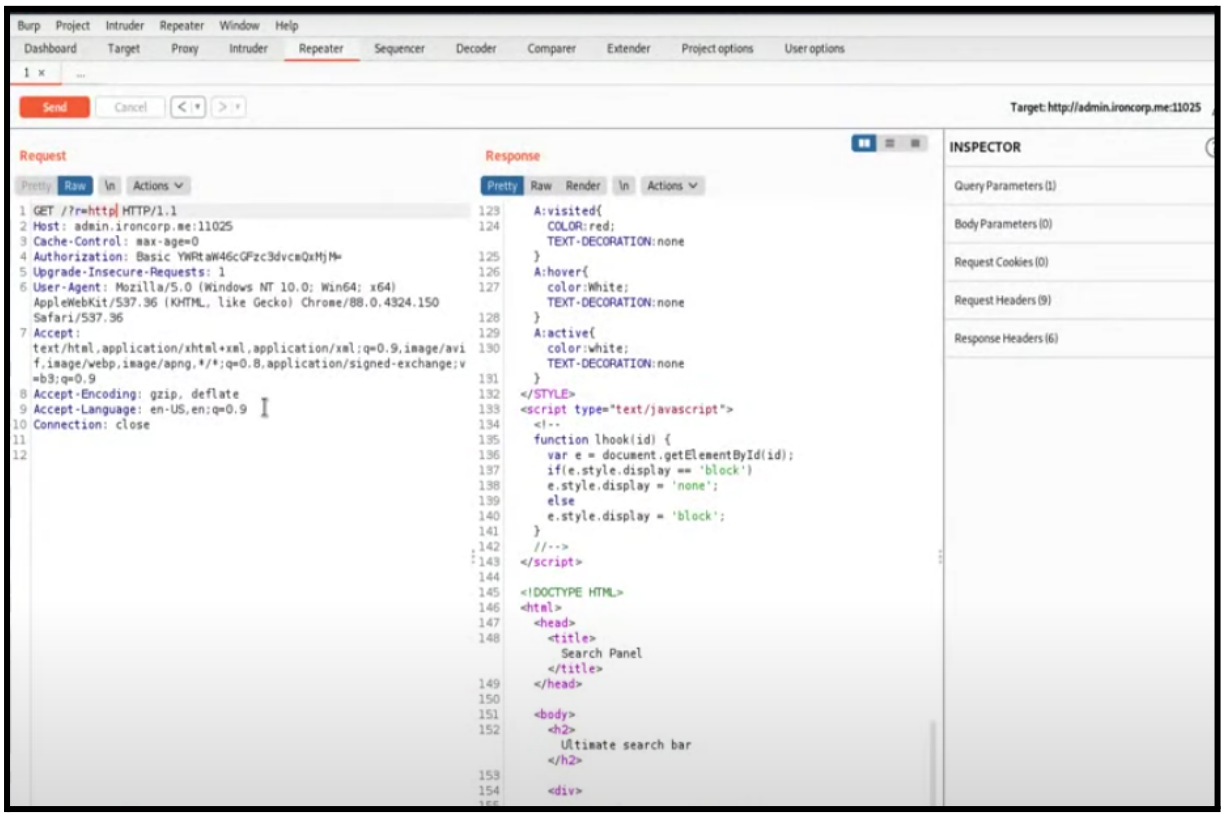
We could also search the ssrf vulnerability and how to use it.



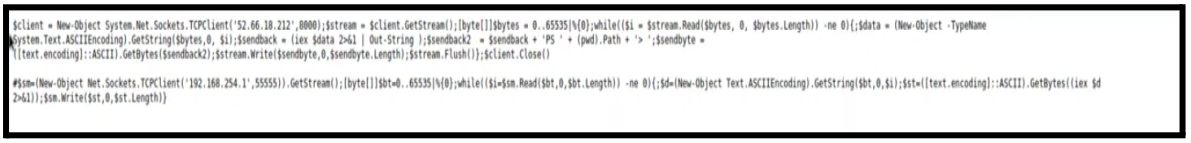
Following a number of code injection experiments, it became evident that the encoded url allowed system instructions to be executed. We should use burpsuite in order to get the encoded urls.

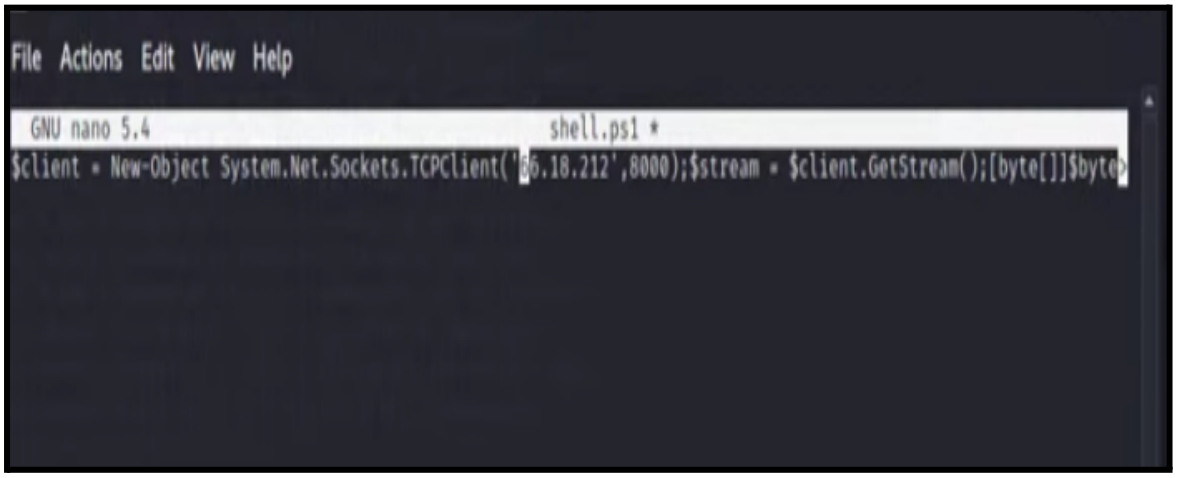


Copy the url link from the admin.incorp.me:11025 and paste it in burpsuite

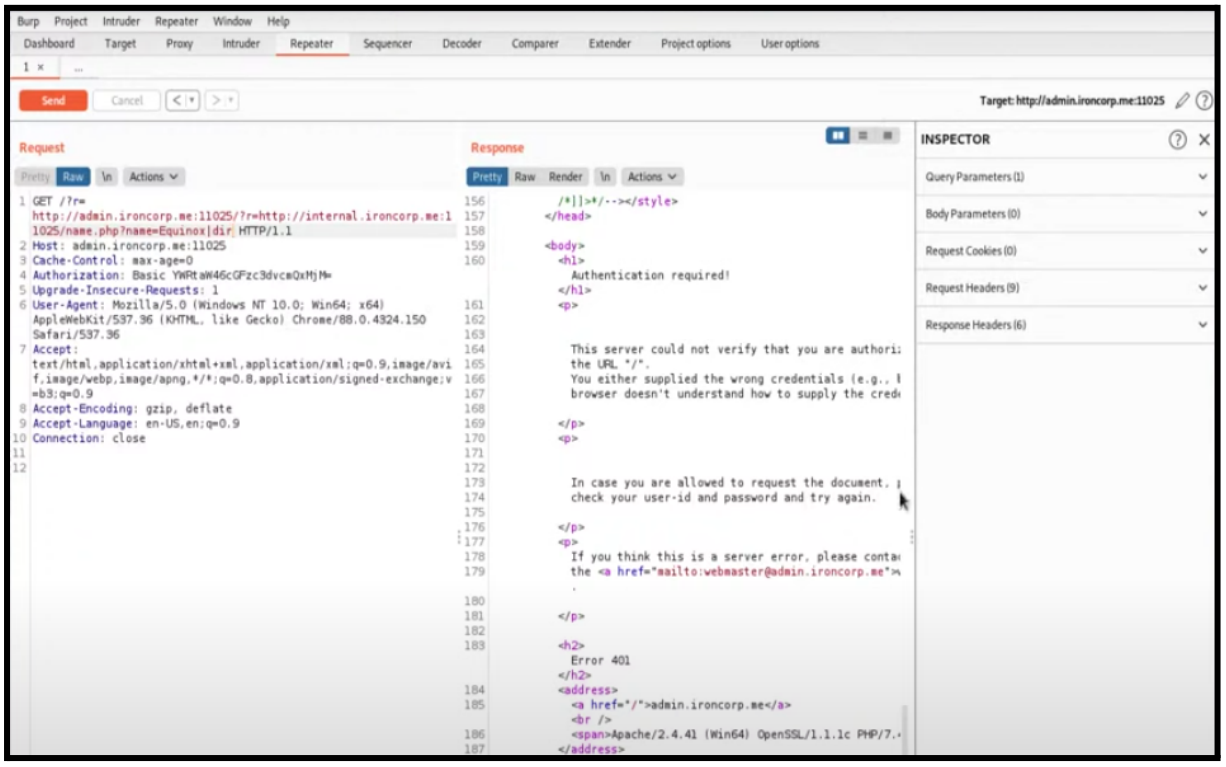


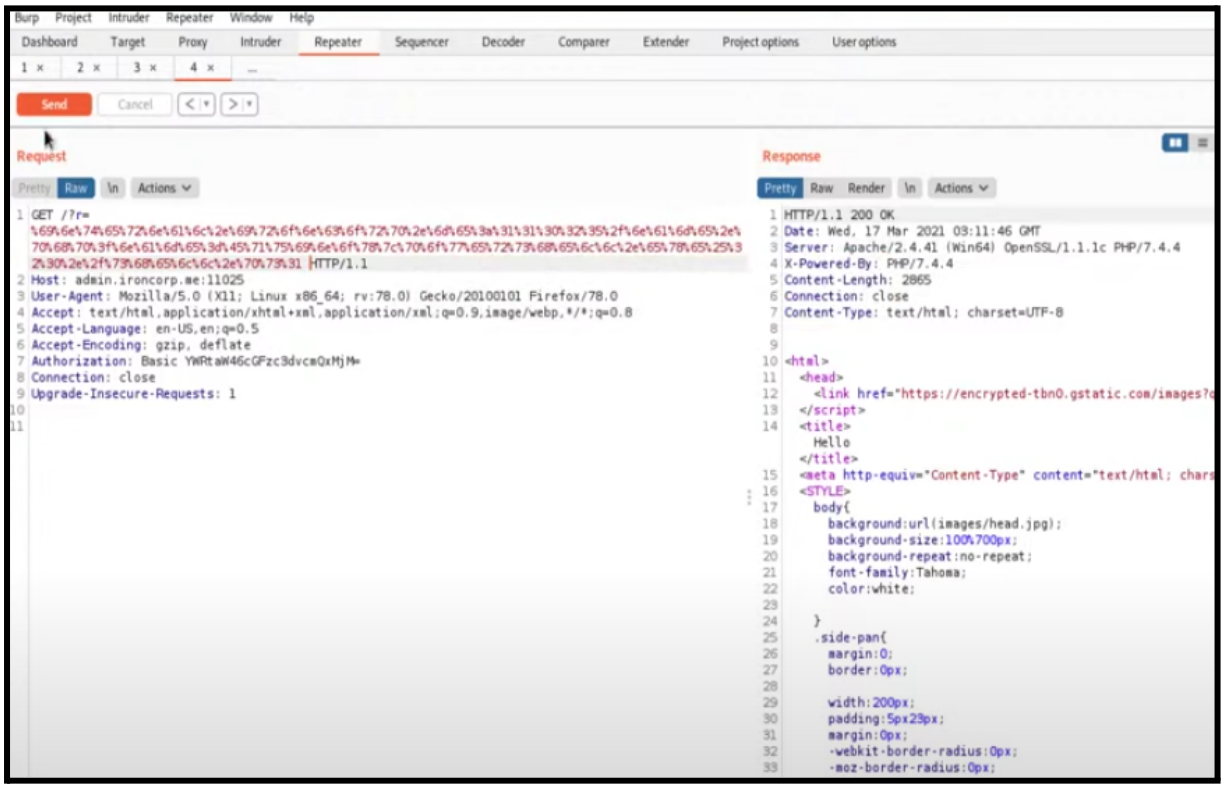
Later on, we should find the poweshell script from github and paste it in our script



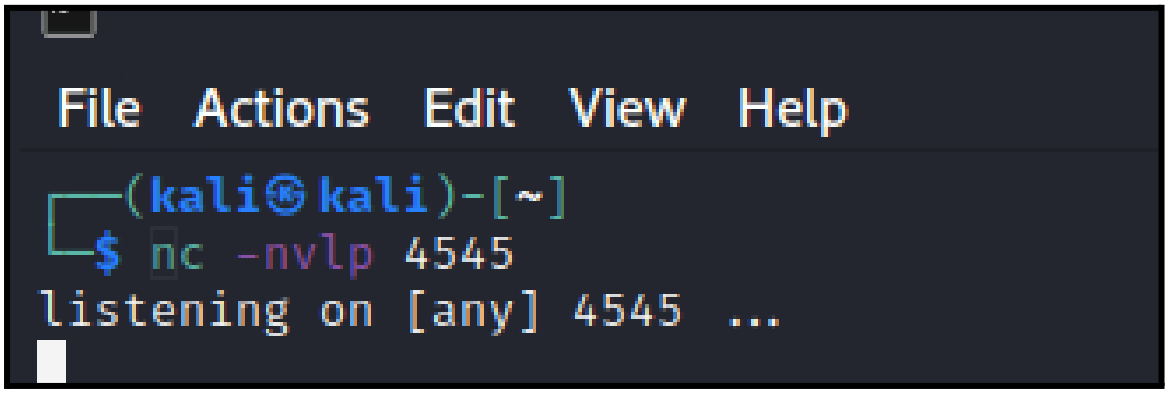


After including the poweshell in burpsuite nd try to decode it using the repeater and decoder , we might get access to the machine .





The connection from the machine to our Kali will have "nt authority / system" permissions if everything has gone according to plan.



Thought Process and Methodology and Attempts:

We found that the site is vulnerable to SSRF attacks after doing a series of tests to identify the kind of vulnerability we are dealing with. We may use it to do an internal port search and discover new services that are only available internally. This might be used by an attacker to identify internally exposed services and bypass their firewall. When we examine the code, we can see a variable that outputs a user's name. (Equinox). Additionally, we might research the ssrf vulnerability and its use. It was discovered after a number of code injection studies that the encoded url enabled the execution of system commands. Burpsuite should be used to obtain the encoded urls. Take note of the URL address at admin.incorp.me:11025 and paste it in burpsuite. Later on, we should find the poweshell script from github and paste it in our script.After including the poweshell in burpsuite nd try to decode it using the repeater and decoder , we might get access to the machine .The connection from the machine to our Kali will have "nt authority / system" permissions if everything has gone according to plan.

4) Escalation

Members involved: Nicholas Cheok

Tools Used: Kali terminal, firefox, BurpSuite, Nmap.

Get the terminal to listen by the code set in the firefox browser. Once it starts to listen, direct the documents in the terminal. Cd on the users, administrator and desktop. Then, get the flag of user.txt by using the command “more user.txt”.

Direct the SuperAdmin and modify it in the file. Then, Get-ChildItem at Force and direct it into the file. After that, use “type c:\users\SuperAdmin\Desktop\root.txt” to get the root flag.

Thought Process/Methodology:

We used “nc -nlvp 4545” to get it to listen by sending the url of the decoded code in BurpSuite and by sending it to the repeater to respond. After that, we direct the documents in the terminal and the documents are displayed. Then, type in “whoami” to get the name “nt authority\system”. Use cd on the user, administrator together with the desktop. And to get the flag of user.txt, we typed in the command “more user.txt” and we got the user flag. Secondly, we configured the IP and the Ethernet adapter was displayed. Then we sent it to the directory and use cd on users. Change the directory to SuperAdmin and type again “whoami” and got the name “nt authority\system” again. We then direct the SuperAdmin and modify it in the file. We used the Get-ChildItem at Force and direct it into the file. Last but not least we then used the command “type c:\users\SuperAdmin\Desktop\root.txt” to get the root flag. Finally we terminated the machine as we have done getting the user and root flags.

Contributions

ID	Name	Contributions	Signatures
1211102066	Hemma Ravindran	Entering the password and getting the enquiry form.Did half of the exploiting and burpsuite.Contributed in the writeup	R.hemma
1211100614	Tivaasheny Ananthan	Scanned nmap after save ip address in host file. Did dig and found 2 subdomain(admin and internal ironcorp.me). Did hydra. Get login and password. Did writeup untill hydra.	A.tivaa
1211102168	Nicholas Cheok Jia Jie	Capturing the user and root flags. Did writeup	Nich
1211100986	Sarvesh Munusamy	Did a half of Exploiting. Found the ssrf vulnerability attack Used burpsuite to encode the urls Contributed in the writeup	M.vesh

VIDEO LINK: https://youtu.be/DAxQQolTfc0