



PenTest 2

Iron Corp

Ilomilo

Members:

| STUDENT ID | NAME | ROLE |
|------------|---------------------------------|--------|
| 1211103196 | Adriana Iman binti Noor Azrai | Leader |
| 1211103282 | Aida Maisarah binti Hisam | Member |
| 1211103216 | Sofea Hazreena binti Hasdi | Member |
| 1211103227 | Wan Alia Adlina binti Wan Azman | Member |

Steps: Recon and Enumeration

Members Involved: Wan Alia Adlina

Tools used: Terminal, Kali Linux, Nmap, Hydra, Nano editor, Firefox, Dig

Thought Process and Methodology and Attempts:

First, Adlina types in [ifconfig] to define the network address of each interface present on a system.



```
root@kali: ~# ifconfig
eth0: flags=4163<UP,BROADCAST,NOARP,MULTICAST>  mtu 1500
inet 192.168.1.10 netmask 255.255.255.0 broadcast 192.168.1.255
ether 08:00:27:1b:3c:1a txqueuelen 1000 (Ethernet)
RX packets 109211 bytes 1431328 (142.1 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 42338 bytes 106336 (104.5 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128, scopeid 01<host>
loop 1000000000 (local loopback)
RX packets 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun0: flags=4096<UP,PERSISTENT,RUNNING,MAINT,MULTICAST>  mtu 1500
inet 10.11.10.10 netmask 255.255.255.0 association 10.11.10.10
ether 08:00:27:1b:3c:1a txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun1: flags=4096<UP,PERSISTENT,RUNNING,MAINT,MULTICAST>  mtu 1500
inet 10.11.10.11 netmask 255.255.255.0 association 10.11.10.11
ether 08:00:27:1b:3c:1a txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Then, she uses [nano /etc/hosts] to edit the local host as mentioned in the TryHackMe website and add the file [ironcorp.me] along with the machine IP address. After that, she uses nmap -Pn -n [ip address] to scan the network.

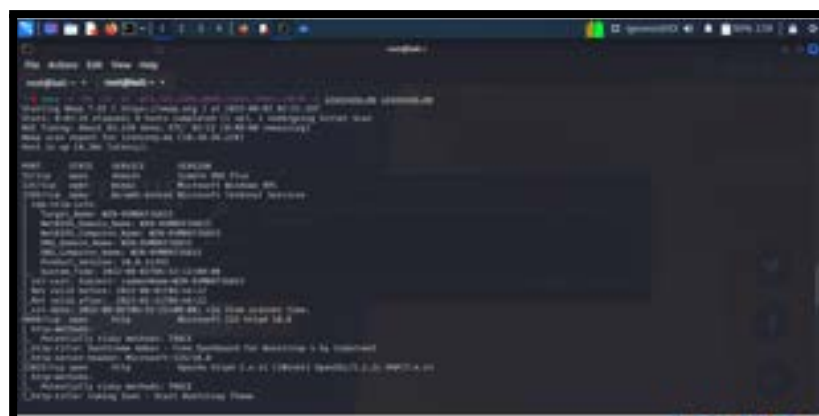


After the scanning is complete, Adlina types [ls] to check whether the ironcorp.me file is inside their local network. So she uses cat ironcorp.me to open the file.



```
ls
total 12
drwxr-xr-x 3 root root 4096 Jan 10 10:10 .
drwxr-xr-x 1 root root 4096 Jan 10 10:10 ..
-rw-r--r-- 1 root root  100 Jan 10 10:10 ironcorp.me
```

In the output, there will be a nmap command along with all 7 wanted ports so she copies and pastes it in the terminal. This will run a network scan again. The outputs will show all the ports that are open.



```
cat ironcorp.me
nmap -sS -p 22,80,443,8080,8443,9000,9001 10.10.10.10
nmap -sS -p 22,80,443,8080,8443,9000,9001 10.10.10.10
```

After doing nmap and finding the right port to the admin log in, Adlina tries to find the subdomain for the website that is running by using dig (for interrogating DNS name servers) along with axfr (a simplest mechanism to replicate DNS records across DNS servers). She managed to find the subdomain such as admin and internal for the ironcorp.me. After that, she nano the hosts file again as she need to add the admin and internal for ironcorp.me inside the local host file. She entered both subdomains however only admin can load.

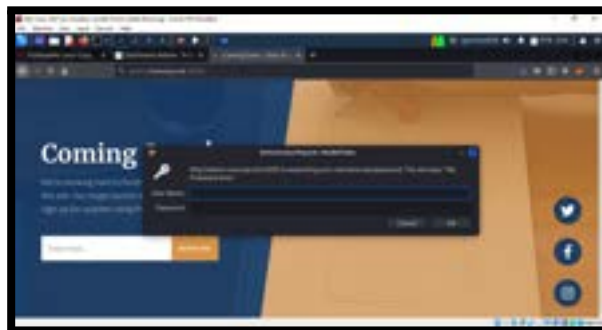


```
dig ironcorp.me
; Standard query response from 192.168.1.1
flags: qr rd ra ra-ra;
answer:
question: ironcorp.me
answer: 192.168.1.1
authority:
addition:
```

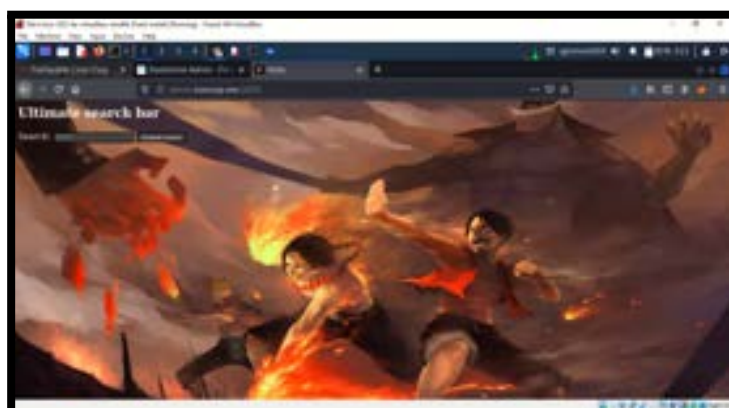
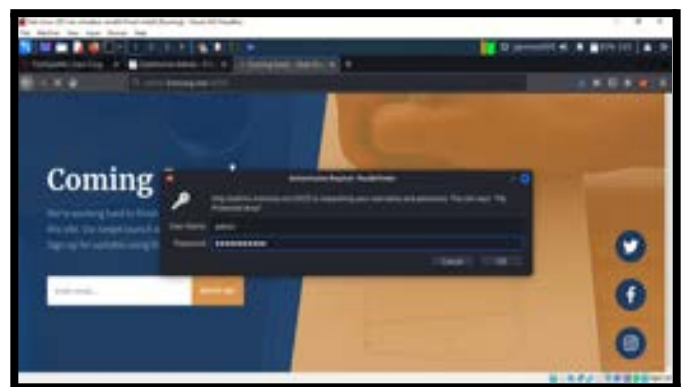


```
axfr
; Standard query response from 192.168.1.1
flags: qr rd ra ra-ra;
answer:
question: ironcorp.me
answer: 192.168.1.1
authority:
addition:
```

After Adlina successfully entered admin.ironcorp.me, Adlina was provided with a pop out for username and password to login.



By using hydra, using the command -l to load several logins from the file,-P to try the password that can pass from the username:admin, -s to connect the credential with the port and -f to exit after the first login username and password found, we run hydra and after a few minutes waiting we were provided with the credentials, username and password. Adlina guesses that we can specify the user to admin as we are in the admin website and for the password we connect with a password.lst file that she created, copy pasted the common passwords from browser [password.lst](#) as if we nano the file, we will be provided with thousands of common passwords used. In addition, as Adlina already specified the username to admin, it will print the password of admin from password.lst file that is connected to the port and lead us to get the right username and password. With the credentials provided, we logged into the admin page and we were navigated to a website named 'Hello'.



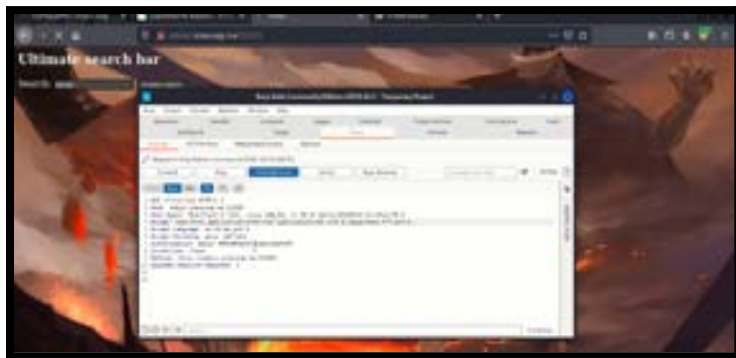
Steps: Initial Foothold

Members Involved: Aida Maisarah, Sofea Hazreena

Tools used: Reverse shell, Powershell, Burpsuite, Decoder, Repeater, Intruder, Nano, Netcat, Terminal, Python3, Proxy

Thought Process and Methodology and Attempts:

Aida then turned on the burpsuite and turned on intercept. On the search bar of the website, she typed in “dirasd” to test if the burpsuite is connected to the website. After that she pressed forward in burpsuite and refreshed the website page. There are some new additional words which say “dirasd” meaning that it is connected already. Then she right clicked and pressed “send to the repeater” and pressed forward.



She entered command `/etc/init/apache` and started. After that, she found the vpn ip address from `ifconfig tun0`.



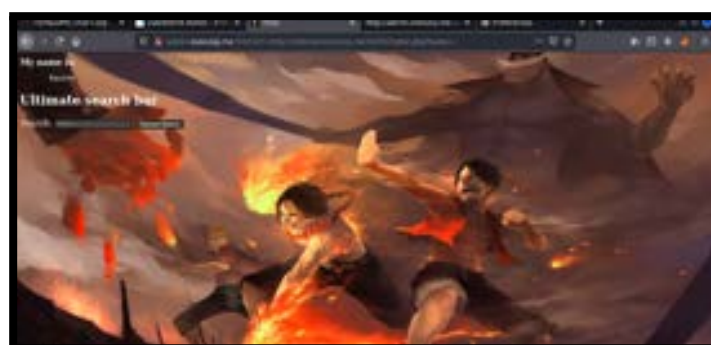
In the repeater, she changed the url to vpn ip address and sent a response to see the code that will appear.



She right clicked at the 'helo' website and clicked on the open source. In the open source, it shows the url that we are supposed to use to find the correct directory.



She copy pasted the link from open source and click enter to see what is inside the website.



She modified the end of the url and added Equinox. It does not appear like what we want. So she modified the url again.



Next, she added a dir which directed to the directory of \xampp\htdocs\internal and this the website that we want.



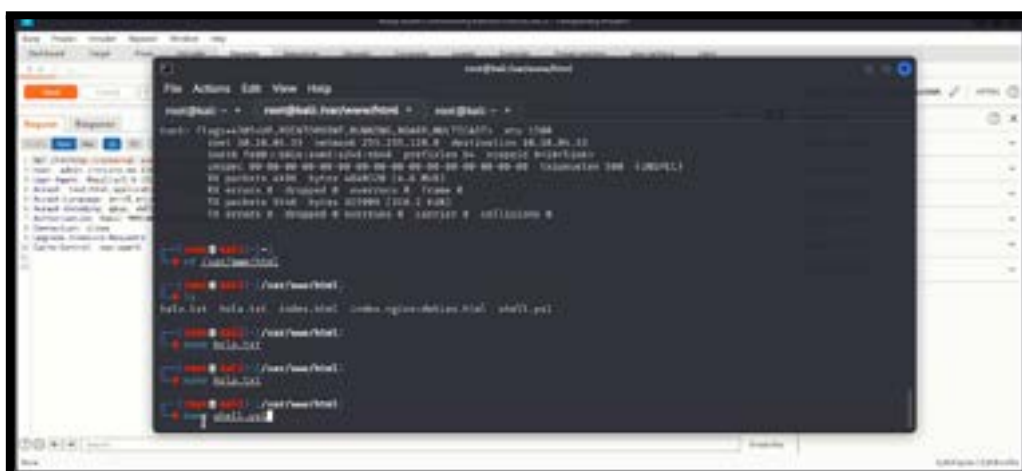
Sofea refreshes the 'Hello' website and its intercept to the proxy. She right clicks and sends the script to the repeater. After that, she clicks the send button so the data will be directed to the response.



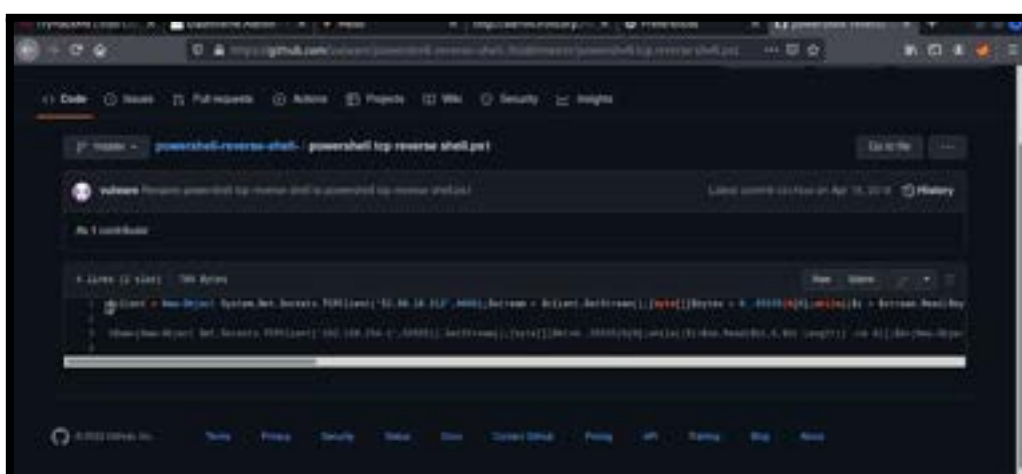
She deleted the url before <http://internal..> and sent a response to see the code that was shown. The code shown proved that we can use burp suite to upload the shell.



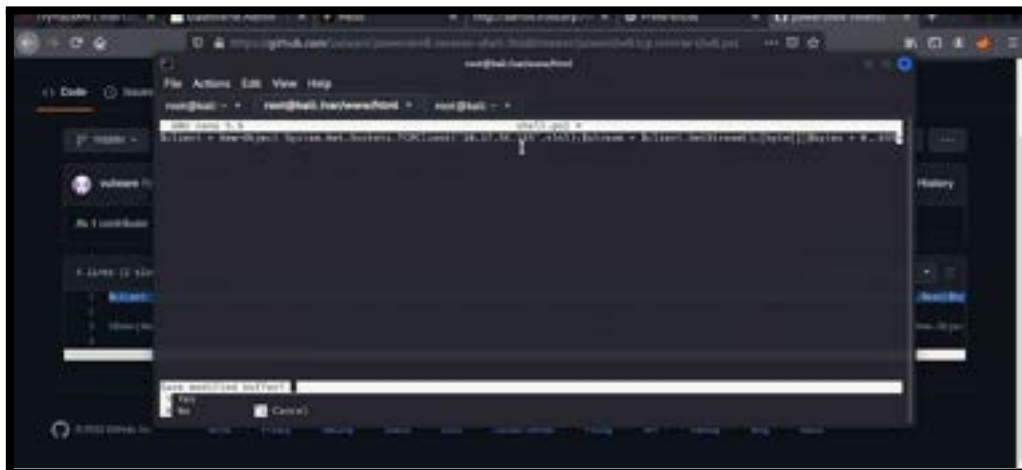
She changed the directory to /var/www/html. Typed in command ls to see the files inside the directory and before she nano shell.ps1, that file does not exist in that directory. So, she used the nano command followed by the shell.ps1 which is the file name.



In the Firefox browser, she searches for the powershell reverse shell script to be inserted in shell.ps1.



She uses nano command to open and edit shell.ps1. She copied all the script that needed to reverse shell the shell.ps1 and pasted it in the shell.ps1 file. Before she saved the shell.ps1 in /var/www/html directory, she change the ip address using the ip address that was provided in the ifconfig command, she used the one in tun0. Also, she changed the port number and saved the file.



While it is listening to the port. She opened a new Firefox browser and copy pasted the “Helo” website url to intercept it to proxy Burp Suite. The proxy can capture the url and press forward to enter the website.



She opened the decoder in the Burp suite. She typed in the url and added powershell followed by the ASCII character which are %20(space) and %22(""). She also added wget which is for non-interactive download for files from the web.in the url also, she put in the ip address of the vpn interface and the directory with shell.ps1. She encoded the text to url.



She replaces the link(red in colour) in the repeater with the encoded url then sends it to respond to see the code that will appear.



After it responds, she encoded as url the text that contains powershell.exe for execution and the shell.ps1. It proved that shell.ps1 is uploaded in the directory.



Steps: Horizontal Privilege Escalation

Members Involved: Sofea Hazreena, Adriana Iman

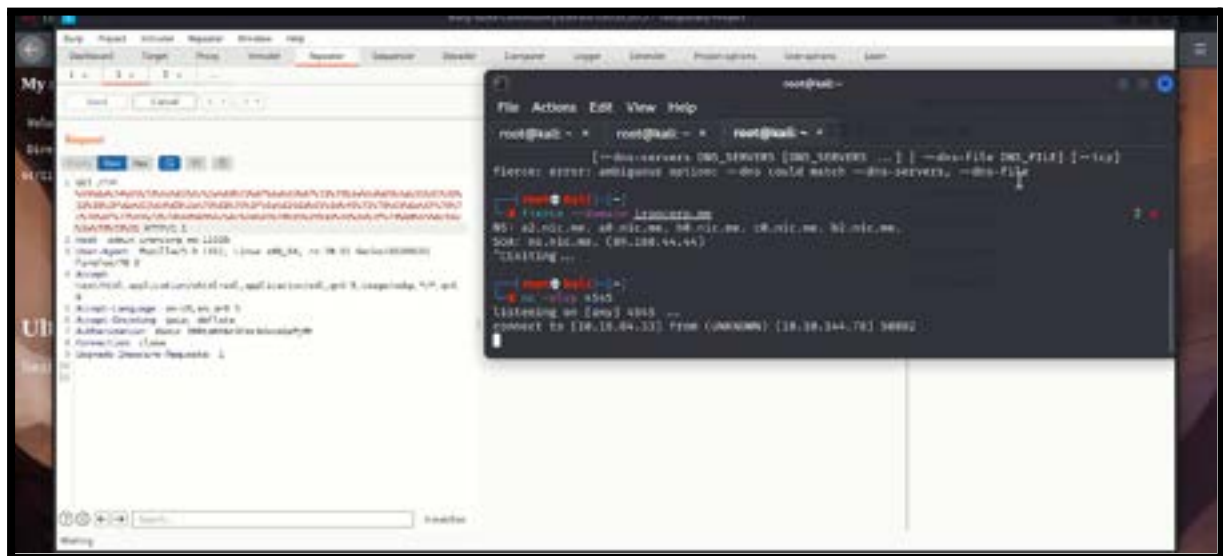
Tools used: Terminal, Dig, Netcat, Repeater

Thought Process and Methodology and Attempts:

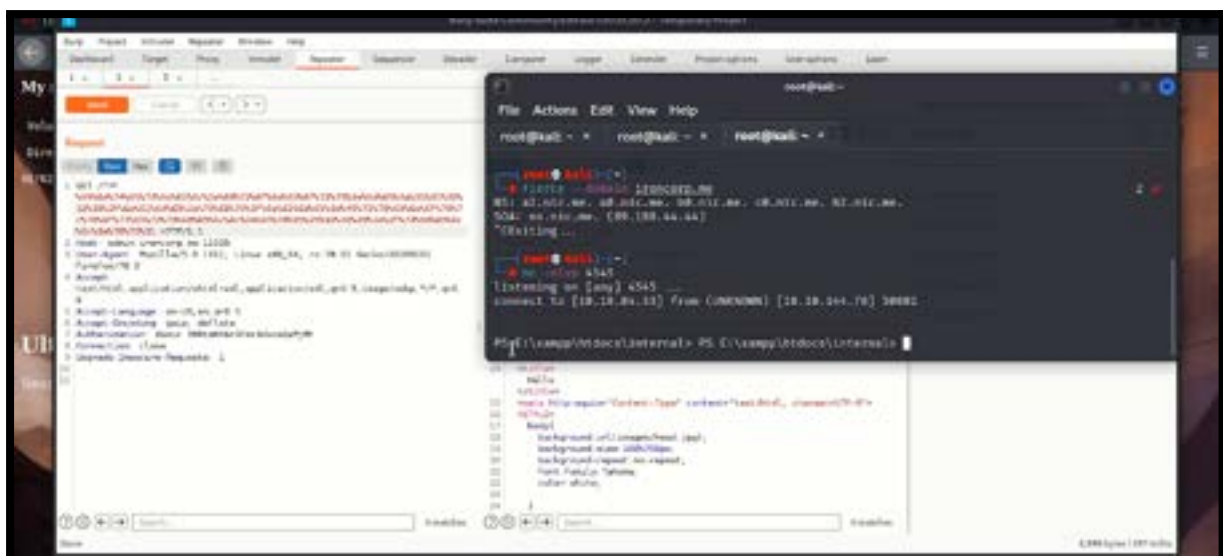
Sofea used the netcat command as the scanning tool and she added nlvp which is for to specify what nc should listen to, service lookups on any ports, have the nc give more verbose output and specify the source port.

[illegible]

Now, she sends to the respond the url that has been decoded and refreshes the 'Helo' website. It seems that it is connected to the port that we netcat before.



After it connected, she entered and it directed to the directory of \xampp\htdocs\internal.



Once the machine is successfully connected to kali, Adriana types in `[dir]` to list down all directories and files. Then, on a different terminal tab, she tries to use the `dig` command again to gather information in `ironcorp.me`.

[illegible][illegible]

After that, she went to the terminal tab that is connected and type [ls] to look at all the files again but there doesn't seem anything to be helpful there. So she tries to type in [ipconfig] to display informations about our network configuration and went into local files which is [c:].

```

File Actions Edit View Help
root@kali: ~ - root@kali: ~ - root@kali: ~ -

```

| Mode | LastModification | Length | Name |
|------------|-------------------|--------|---------------|
| -rwxr-xr-x | 3/27/2019 9:10 AM | 52 | .X11-unix |
| -rwxr-xr-x | 3/27/2019 9:10 AM | 135 | .X11-unix.php |
| -rwxr-xr-x | 3/27/2019 9:10 AM | 142 | .X11-unix.png |
| -rwxr-xr-x | 3/27/2019 9:10 AM | 142 | .X11-unix.png |

```

root@kali: /tmp/.X11-unix - ls -la

```

```

Directory: /tmp/.X11-unix

```

| Mode | LastModification | Length | Name |
|------------|-------------------|--------|---------------|
| -rwxr-xr-x | 3/27/2019 9:10 AM | 52 | .X11-unix |
| -rwxr-xr-x | 3/27/2019 9:10 AM | 135 | .X11-unix.php |
| -rwxr-xr-x | 3/27/2019 9:10 AM | 142 | .X11-unix.png |
| -rwxr-xr-x | 3/27/2019 9:10 AM | 142 | .X11-unix.png |

```

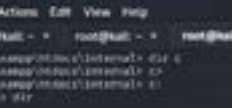
root@kali: /tmp/.X11-unix -

```

[illegible]A screenshot of a Windows Command Prompt window titled "cmd.exe". The menu bar shows "File", "Actions", "Edit", "View", and "Help". The address bar displays three instances of "msn@kali: ~". The command prompt shows the following output:

```
PS C:\Users\Andrew\Documents> ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Ethernet0:  
  
    Connection-specific DNS Suffix . : example.compute.internal  
    Link-local IPv6 Address . . . . . : fe80::9d7c:a18:ad8:faf6e%  
    IPv4 Address. . . . . : 10.10.104.78  
    Subnet Mask . . . . . : 255.255.0.0  
    Default Gateway . . . . . : 10.10.0.1  
  
Tunnel adapter {isatap.{...}}:  
  
    Media State . . . . . : Media disconnected  
    Connection-specific DNS Suffix . : example.compute.internal  
PS C:\Users\Andrew\Documents>  
PS C:\Users\Andrew\Documents>  
PS C:\Users\Andrew\Documents>  
PS C:\Users\Andrew\Documents>  
PS C:\Users\Andrew\Documents>  
PS C:\Users\Andrew\Documents>
```

Then, Adriana types in `[dir]` again and looks at the all the files and directories in there and sees a Users file. So she changed directory to users using `[cd users]` and types `[whoami]` where `[nt authority/system]` will come out.

[illegible]

```

root@kali: ~
File Actions Edit View Help

root@kali: ~ root@kali: ~ root@kali: ~
PS C:\Users\ahmed> cd /usr/share/doc/iptables
PS C:\Users\ahmed> ls
PS C:\Users\ahmed> cd /usr/share/doc/iptables
PS C:\Users\ahmed> ls
ls

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d-----         4/11/2018 11:27 AM             0 iptables
d-----         4/11/2018 11:25 AM             0 iptables.man
d-----         4/11/2018 11:25 PM             0 iptables.rules
d-----         4/11/2018 11:25 AM             0 iptables.xm
d-----         4/11/2018 11:42 AM             0 iptables.xm.gz
d-----         4/11/2018 11:41 AM             0 iptables.xm.gz.asc
d-----         4/11/2018 11:25 AM             0 iptables.xm.gz.asc

PS C:\Users\ahmed> cd /usr/share/doc/iptables
PS C:\Users\ahmed> ls
PS C:\Users\ahmed> cd /usr/share/doc/iptables
PS C:\Users\ahmed> ls

```

So then, she takes a look at directories in users with [dir] again. She tries changing the directory to Admin and looks if there are any files and there is none. So she tried again with the Administrator where she found a list of files and directories.

[illegible]

The screenshot shows a Windows command prompt window titled 'root@kali ~'. The command 'dir' has been executed, displaying the contents of the 'C:\Users\Administrator' directory. The output lists various files and folders with their attributes, including 'Contacts', 'Desktop', 'Downloads', 'Favorites', 'Links', 'Music', 'Pictures', 'Saved Games', 'Searches', and 'Videos'.

```

root@kali ~
File Actions Edit View Help

root@kali ~ - root@kali ~ -
PS C:\Users\Administrator> dir
PS C:\Users\Administrator> cd ..
PS C:\Users> cd Administrator
PS C:\Users\Administrator> dir

Directory: C:\Users\Administrator

Mode                LastWriteTime         Length Name
----                -
d-----          4/13/2019   1:12 PM             Contacts
d-----          4/13/2019   1:12 PM             Desktop
d-----          4/13/2019   1:12 PM             Downloads
d-----          4/13/2019   1:12 PM             Favorites
d-----          4/13/2019   1:12 PM             Links
d-----          4/13/2019   1:12 PM             Music
d-----          4/13/2019   1:12 PM             Pictures
d-----          4/13/2019   1:12 PM             Saved Games
d-----          4/13/2019   1:12 PM             Searches
d-----          4/13/2019   1:12 PM             Videos

PS C:\Users\Administrator>

```

From there, Adriana tries changing the directory again to Desktop and sees that there is a file named [user.txt]. So, she puts in [type user.txt] to find out information about the file and the user flag will show up.

```

root@kali: ~
File Actions Edit View Help
root@kali: ~ root@kali: ~ root@kali: ~
d-rwx 4/12/2020 1:27 AM Desktop
d-rwx 4/12/2020 1:29 AM Documents
d-rwx 4/12/2020 1:27 AM Downloads
d-rwx 4/12/2020 1:27 AM Favorites
d-rwx 4/12/2020 1:27 AM Links
d-rwx 4/12/2020 1:27 AM Music
d-rwx 4/12/2020 1:27 AM Pictures
d-rwx 4/12/2020 1:27 AM Saved Games
d-rwx 4/12/2020 1:27 AM Searches
d-rwx 4/12/2020 1:27 AM Videos

PS C:\Users\Administrator\Desktop
PS C:\Users\Administrator\Desktop> dir

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-a----- 4/26/2020 12:39 PM             37 user.txt

PS C:\Users\Administrator\Desktop>

```

[illegible]

Lastly, to go to the root file, Adriana changed directory to SuperAdmin and used the same steps as before for it to navigate us directly to root. There, we can get our final flag under root.txt



Final Result:

Upon verification of the flag, Adriana pasted the user.txt flag and root.txt flag into the TryHackMe site and got the confirmation of the flags

[thm{09b408056a13fc222f33e6e4cf599f8c}] and [thm{a1f936a086b367761cc4e7dd6cd2e2bd}]

| | | |
|----------|---------------------------------------|----------------|
| user.txt | thm{09b408056a13fc222f33e6e4cf599f8c} | Correct Answer |
|----------|---------------------------------------|----------------|

| | | |
|----------|---------------------------------------|----------------|
| root.txt | thm{a1f936a086b367761cc4e7dd6cd2e2bd} | Correct Answer |
|----------|---------------------------------------|----------------|

Contributions

| Student ID | Student Name | Contribution | Signatures |
|------------|---------------------------------|--|----------------|
| 1211103196 | Adriana Iman binti Noor Azrai | <ul style="list-style-type: none">- Finding the user.txt flag- Finding the root.txt flag- Helps Aida to compile her video presentation | <i>adriana</i> |
| 1211103282 | Aida Maisarah binti Hisam | <ul style="list-style-type: none">- Uses burpsuite to find the correct directory website | <i>aida</i> |
| 1211103216 | Sofea Hazreena binti Hasdi | <ul style="list-style-type: none">- Provides screenshots for group's walkthrough- Run the powershell- Netcat and reverse shell- Completing Aida's part for the report | <i>sofea</i> |
| 1211103227 | Wan Alia Adlina binti Wan Azman | <ul style="list-style-type: none">- Recon and enumerate by nmap, hydra, nano and dig- Video editor | <i>adlina</i> |

Youtube video link: [TT6L P2 Ilomilo Presentation Video](#)