



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: ~
File Actions Edit View Help

root@kali: ~ * root@kali: ~ *

root@kali: ~ *
# ifconfig
eth0: flags=4163<UP, BROADCAST, RUNNING, MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27fff:fe50:4c14 prefixlen 64 scopeid 0<20<link>
    ether 08:00:27:50:4c:14 txqueuelen 1000 (Ethernet)
    RX packets 329631 bytes 149415226 (142.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 415330 bytes 84094509 (80.1 MiB)
    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 0<1chost>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 12 bytes 600 (600.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 600 (600.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun0: flags=4305<UP, POINTOPOINT, RUNNING, NOARP, MULTICAST> mtu 1500
    inet 10.17.56.195 netmask 255.255.128.0 destination 10.17.56.195
    inet6 fe80::886d:2123:c17e:5475 prefixlen 64 scopeid 0<20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
    RX packets 2 bytes 96 (96.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 576 (576.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun1: flags=4305<UP, POINTOPOINT, RUNNING, NOARP, MULTICAST> mtu 1500
    inet 10.18.84.33 netmask 255.255.128.0 destination 10.18.84.33
    inet6 fe80::e081:fc0b:bf2d:c80b prefixlen 64 scopeid 0<20<link>

```

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.

A screenshot of a Kali Linux terminal window. The title bar shows various application icons and system status indicators like battery level at 87% and time at 3:02. The terminal prompt is root@kali: ~. The user has entered the command cat /etc/hosts, which displays the contents of the hosts file. Below this, there are several commented-out lines related to IPv6 configuration, such as # The following lines are desirable for IPv6 capable hosts and # Uncommenting this line will allow you to disable the need for DNS. At the bottom of the terminal, there is a toolbar with icons for Help, Write Out, Read File, Where Is, Replace, Cut, Paste, Execute, Justify, Location, Go To Line, Undo, Redo, Set Mark, Copy, To Bracket, Where Was, Previous, Next, and a search icon.

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~ root@kali: ~  
[+] root@kali:~(-)  
[+] root@kali:~(-)  
[+] root@kali:~(-)  
root@kali: ~ - 10.10.16.228  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 02:16 EDT  
Host: 0x00132 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 15.56s done; ETC: 02:18 (0:02:34 remaining)  
Stats: 0:01:00 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 29.56s done; ETC: 02:19 (0:02:23 remaining)  
Stats: 0:01:28 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 43.56s done; ETC: 02:19 (0:01:54 remaining)  
Stats: 0:01:58 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 63.56s done; ETC: 02:19 (0:01:34 remaining)  
Stats: 0:02:28 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 79.56s done; ETC: 02:19 (0:01:58 remaining)  
Stats: 0:02:52 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 85.56s done; ETC: 02:19 (0:01:29 remaining)  
Nmap scan report for 10.10.16.228  
Host is up.  
All 1000 scanned ports on 10.10.16.228 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
  
Nmap done: 1 IP address (1 host up) scanned in 201.57 seconds  
  
[+] root@kali:~(-)  
[*] name rockyvue.txt  
  
[+] root@kali:~(-)  
[*] name etc/hosts  
  
[+] root@kali:~(-)
```

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.

[illegible]

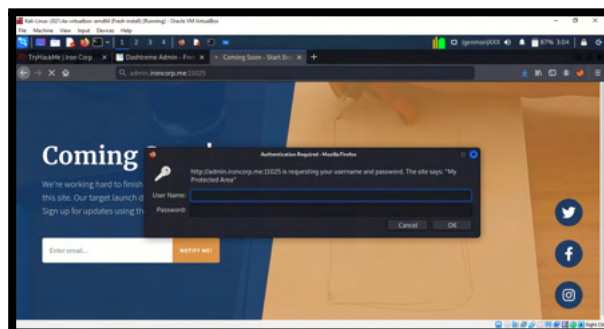
In the output, there will be a nmap command along with all 7 wanted ports so she copies and pastes it in the terminal. This will run a network scan again. The outputs will show all the ports that are open.

```
root@kali: ~  
File Actions Edit View Help  
  
root@kali: ~ root@kali: ~ *  
+ ssh -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no -o ConnectTimeout=5 root@10.10.16.228:22  
Starting Nmap 7.92 (https://nmap.org) at 2022-08-02 02:51 EDT  
Stats: 0%[1] elapsed; 0 hosts completed (1 up); 1 undergoing Script Scan  
NUT Training: About 5%-25% done; ETX: 02:55 (about 28 remaining).  
Nmap scan report for ironcorp.me (10.10.16.228)  
Host is up (0.39s latency).  
  
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  
  
|_ Host OS info:  
Target_Name: WIN-BVMKFXJG815  
Netbios_Name: WIN-BVMKFXJG815  
Netbios_ComputerName: WIN-BVMKFXJG815  
DNS_Name: WIN-BVMKFXJG815  
OS_Compiler_Java: WIN-BVMKFXJG815  
Product_Version: 10.0.17139  
System_Time: 2022-08-02T04:52:17-08:00  
ssl-cert: Subject: commonname=WIN-BVMKFXJG815  
not valid before: 2022-08-01T00:16:22Z  
Not Valid After: 2022-05-31T00:16:22Z  
ssl-data: 2022-08-02T06:52:22+08:00; +3s from scanner time.  
msh/cip    http       Microsoft IIS httpd 10.0  
  
|_ http-methods:  
Potentially risky methods: TRACE  
|_ http-title: Backstage Admin - Free Dashboard for Bootstrap 4 by Codevrent  
|_ http-server-header: Microsoft-IIS/10.0  
|_ https/cip open  https     Apache httpd 2.4.41 ((Ubuntu)) OpenSSL/1.1.1c PHP/7.4.4  
|_ http-methods:  
Potentially risky methods: TRACE  
|_ http-title: Coming Soon - Start Bootstrap Theme
```

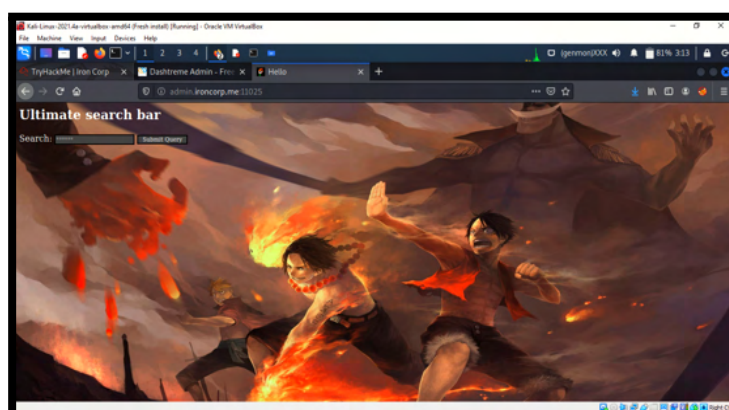
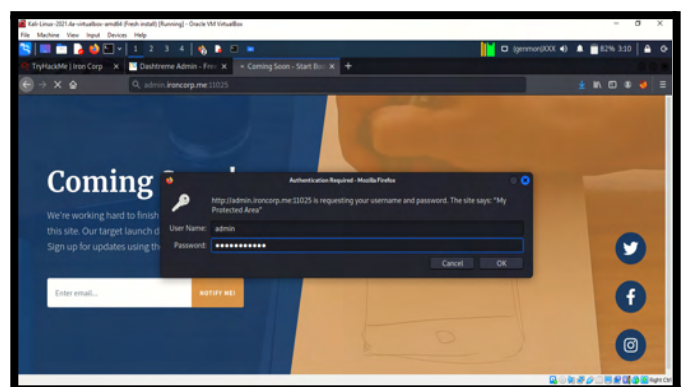
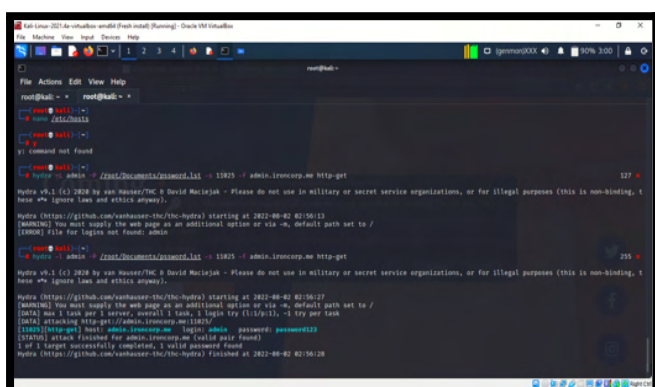
After doing nmap and finding the right port to the admin log in, Adlina tries to find the subdomain for the website that is running by using dig (for interrogating DNS name servers) along with axfr (a simplest mechanism to replicate DNS records across DNS servers). She managed to find the subdomain such 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.

[illegible][illegible]

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'.



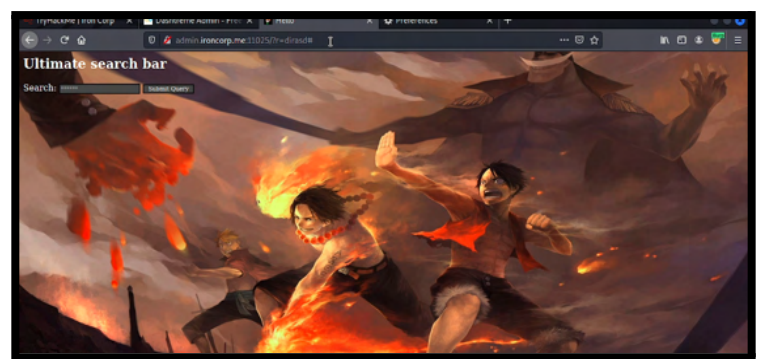
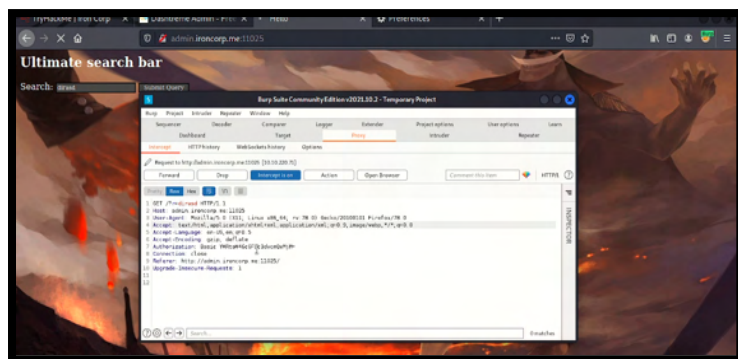
Steps: Initial Foothold

Members Involved: Aida Maisarah, Sofea Hazreena

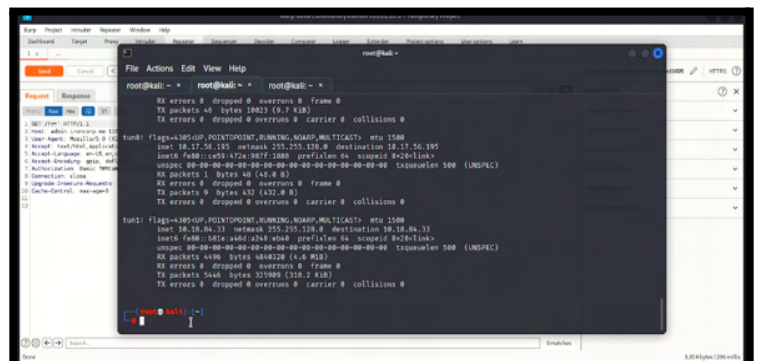
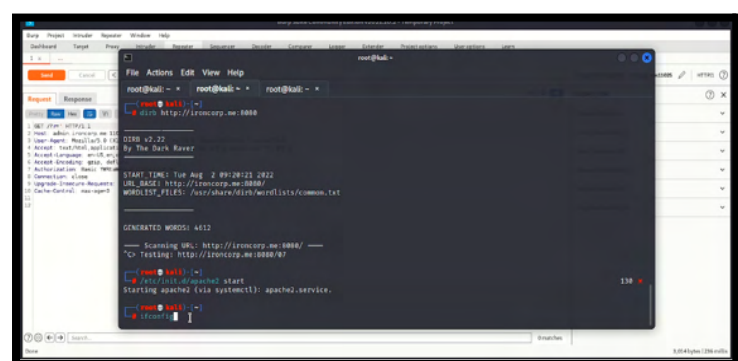
Tools used: Reverse shell, Powershell, Burpsuite, Decoder, Repeater, Intruder, Nano, Netcat, Terminal, Python3, Proxy

Thought Process and Methodology and Attempts:

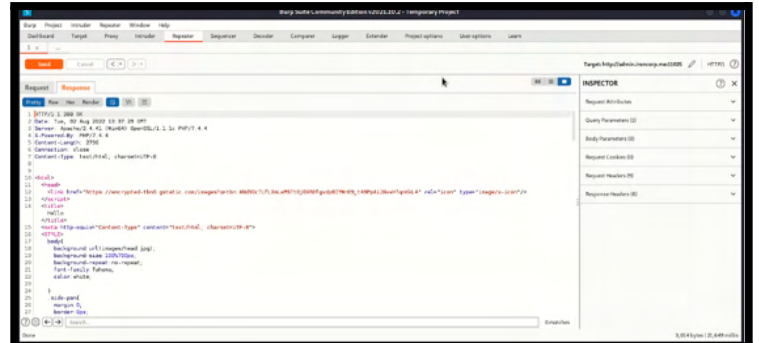
Aida then turned on the burpsuite and turned on intercept. On the search bar of the website, she typed in “dirasd” to test if the burpsuite is connected to the website. After that she pressed forward in burpsuite and refreshed the website page. There are some new additional words which say “dirasd” meaning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



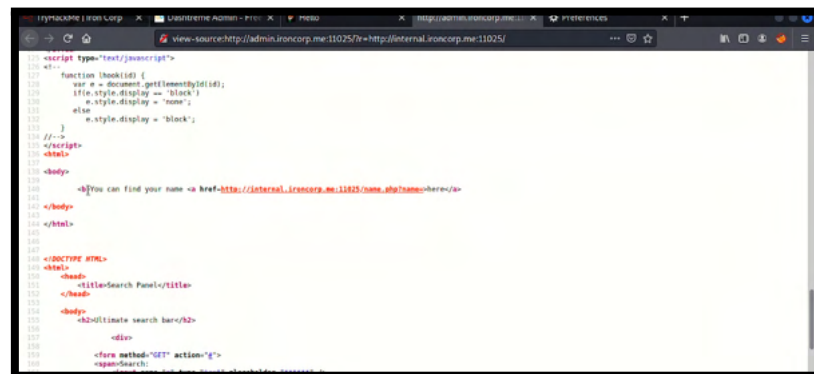
She entered command `/etc/init/apache` and started. After that, she found the vpn ip address from `ifconfig tun0`.



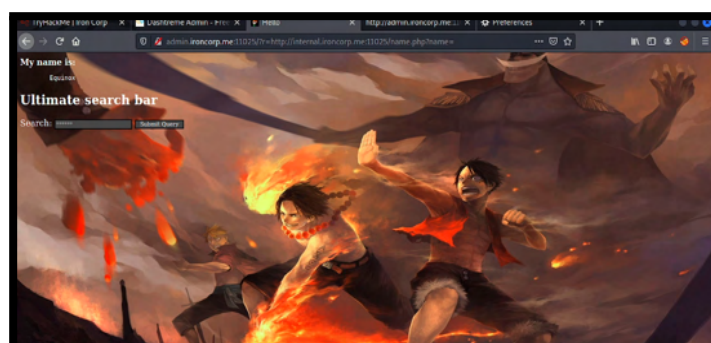
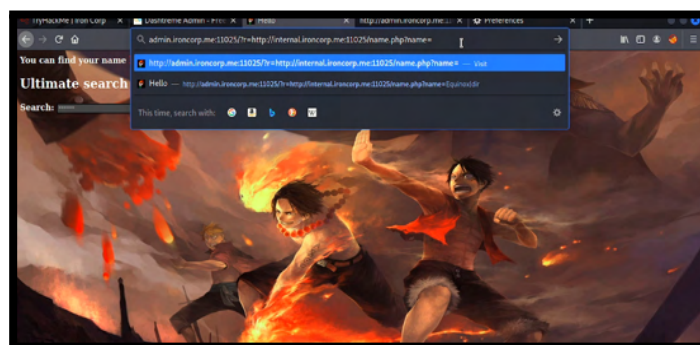
In the repeater, she changed the url to vpn ip address and sent a response to see the code that will appear.



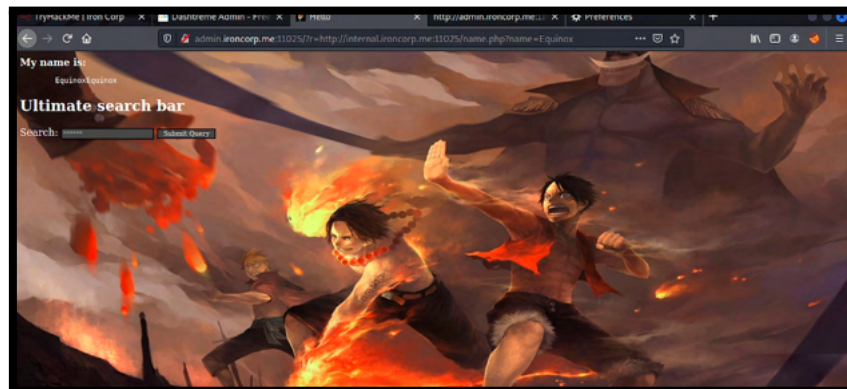
She right clicked at the 'helo' website and clicked on the open source. In the open source, it shows the url that we are supposed to use to find the correct directory.



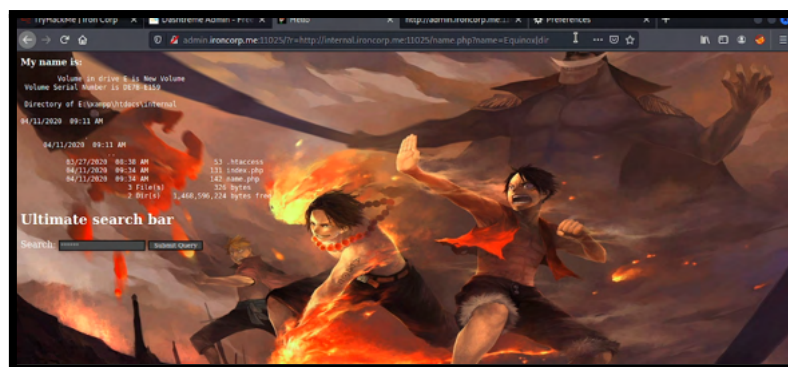
She copy pasted the link from open source and click enter to see what is inside the website.



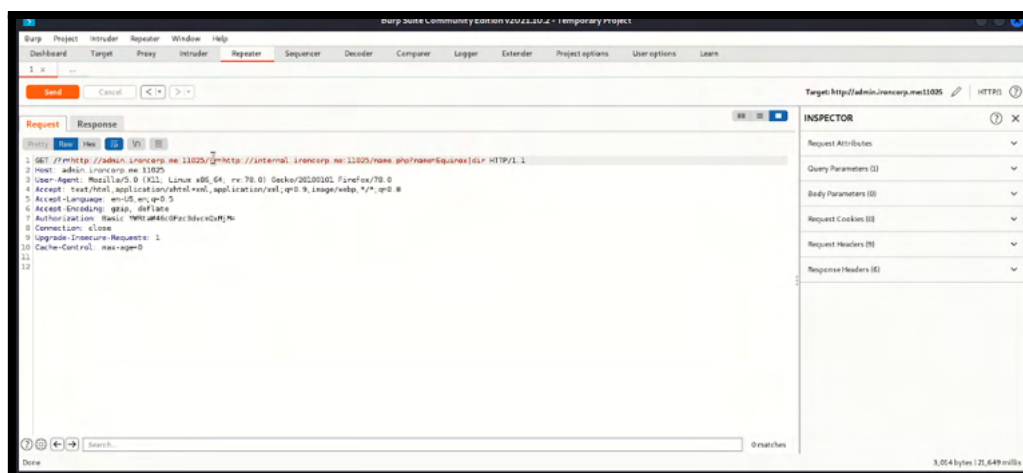
She modified the end of the url and added Equinox. It does not appear like what we want. So she modified the url again.



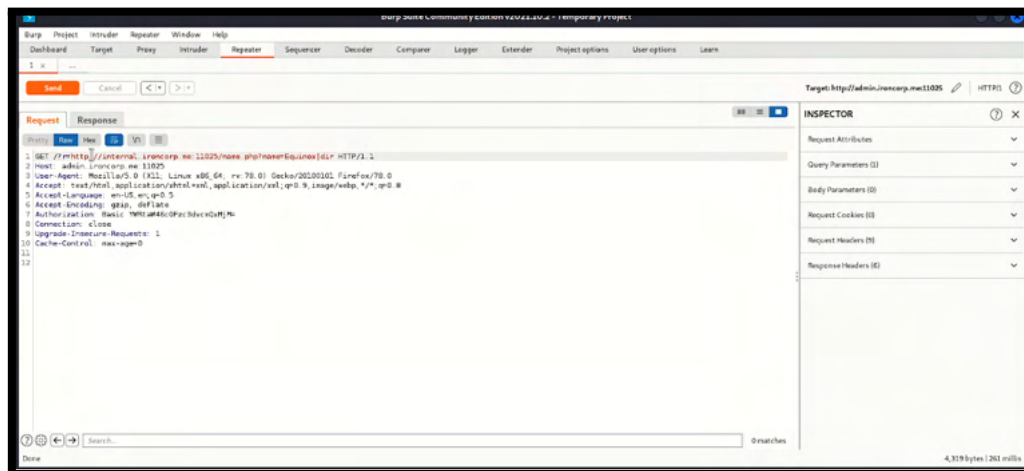
Next, she added a dir which directed to the directory of \xampp\htdocs\internal and this the website that we want.



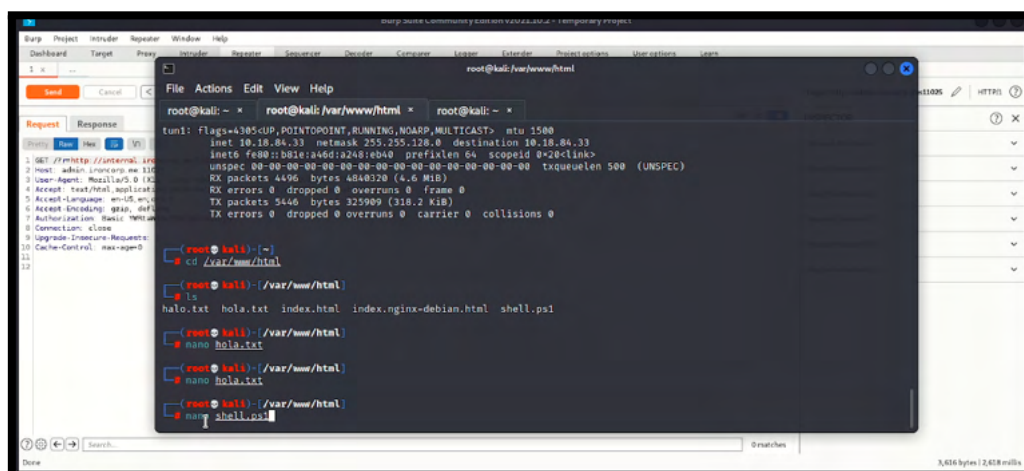
Sofea refreshes the 'Hello' website and its intercept to the proxy. She right clicks and sends the script to the repeater. After that, she clicks the send button so the data will be directed to the response.



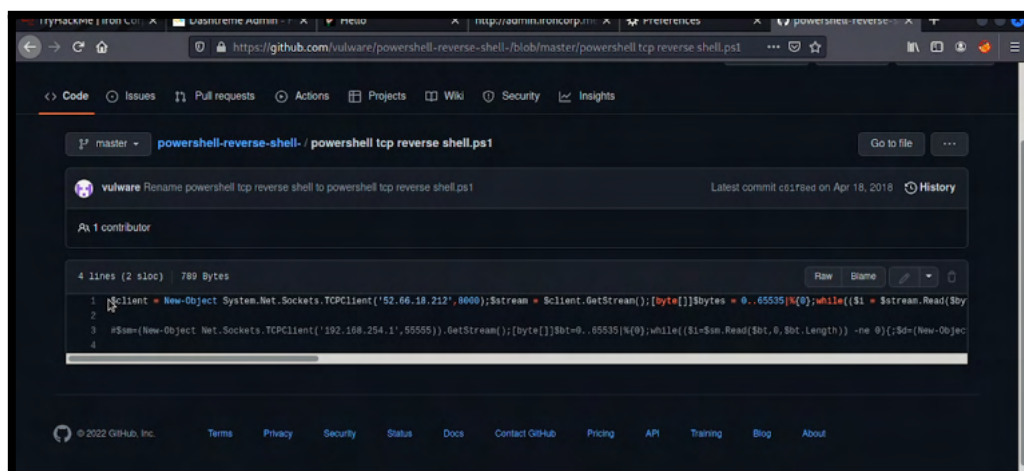
She deleted the url before <http://internal..> and sent a response to see the code that was shown. The code shown proved that we can use burp suite to upload the shell.



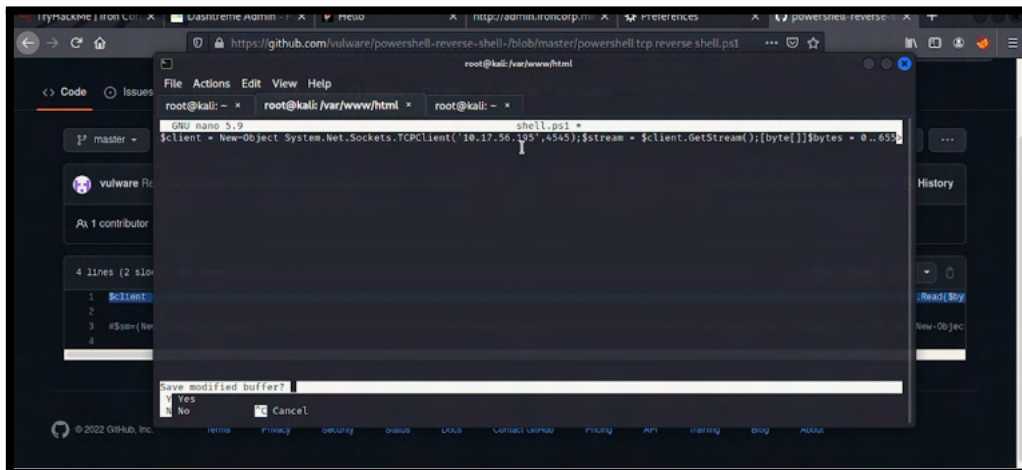
She changed the directory to /var/www/html. Typed in command ls to see the files inside the directory and before she nano shell.ps1, that file does not exist in that directory. So, she used the nano command followed by the shell.ps1 which is the file name.



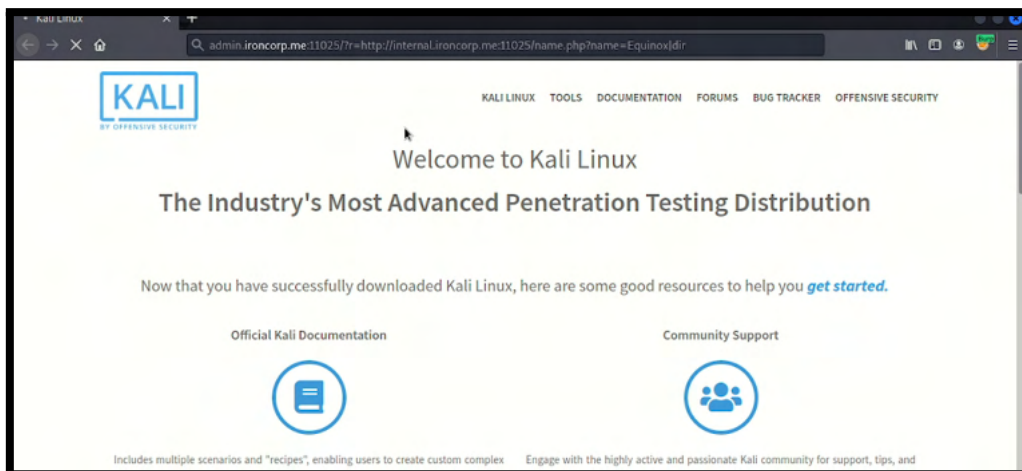
In the Firefox browser, she searches for the powershell reverse shell script to be inserted in shell.ps1.



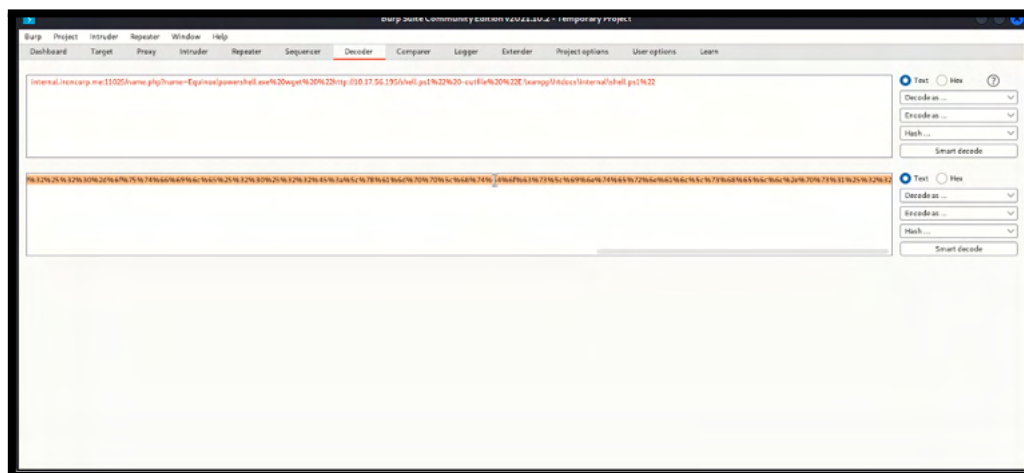
She uses nano command to open and edit shell.ps1. She copied all the script that needed to reverse shell the shell.ps1 and pasted it in the shell.ps1 file. Before she saved the shell.ps1 in /var/www/html directory, she change the ip address using the ip address that was provided in the ifconfig command,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



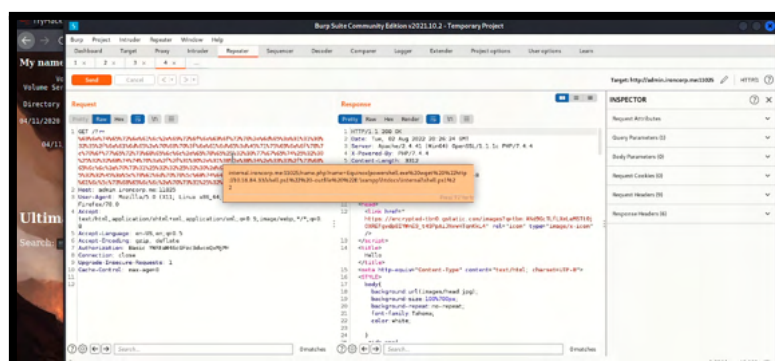
While it is listening to the port. She opened a new Firefox browser and copy pasted the “Helo” website url to intercept it to proxy Burp Suite. The proxy can capture the url and press forward to enter the website.



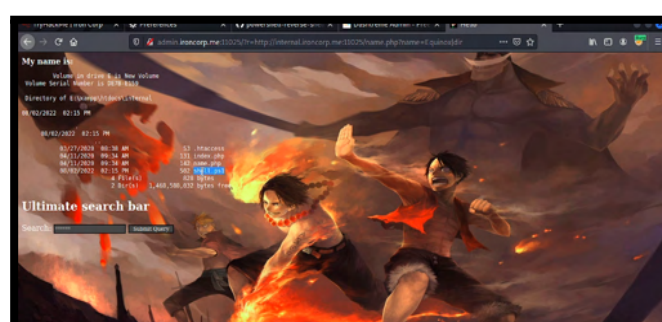
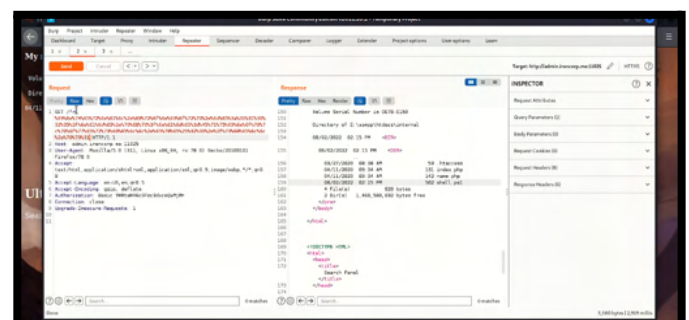
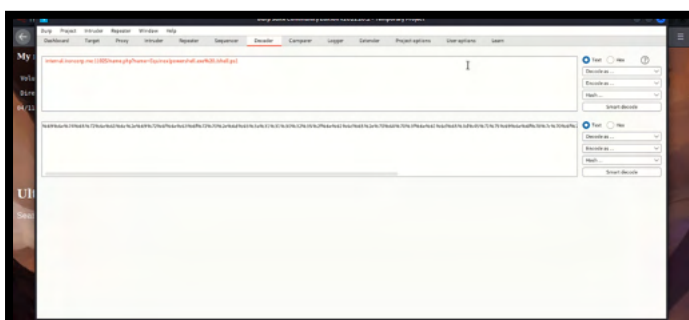
She opened the decoder in the Burp suite. She typed in the url and added powershell followed by the ASCII character which are %20(space) and %22(""). She also added wget which is for non-interactive download for files from the web.in the url also, she put in the ip address of the vpn interface and the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



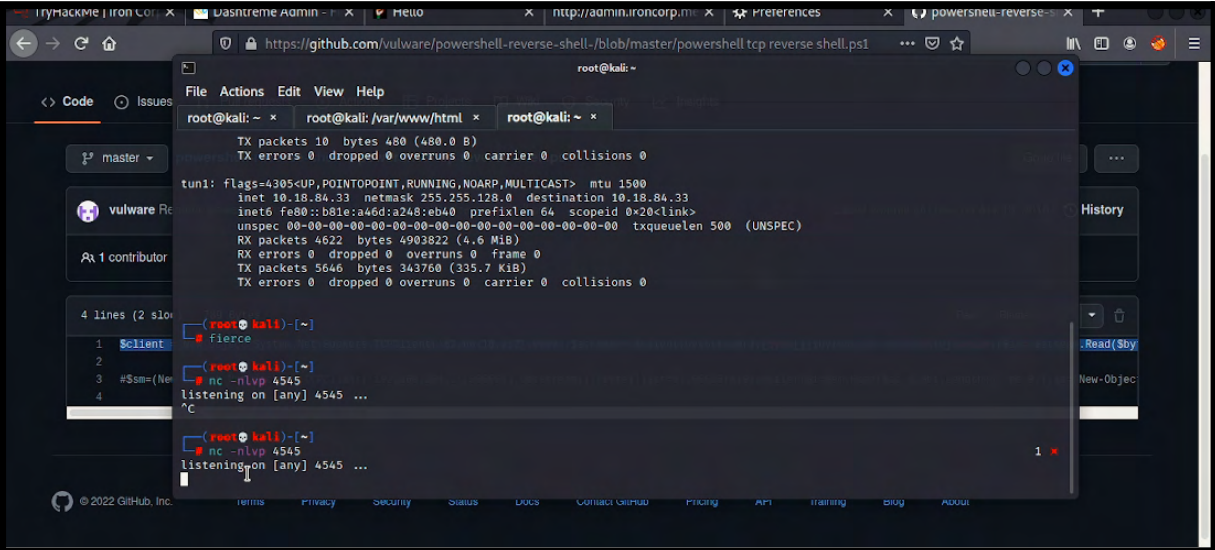
Steps: Horizontal Privilege Escalation

Members Involved: Sofea Hazreena, Adriana Iman

Tools used: Terminal, Dig, Netcat, Repeater

Thought Process and Methodology and Attempts:

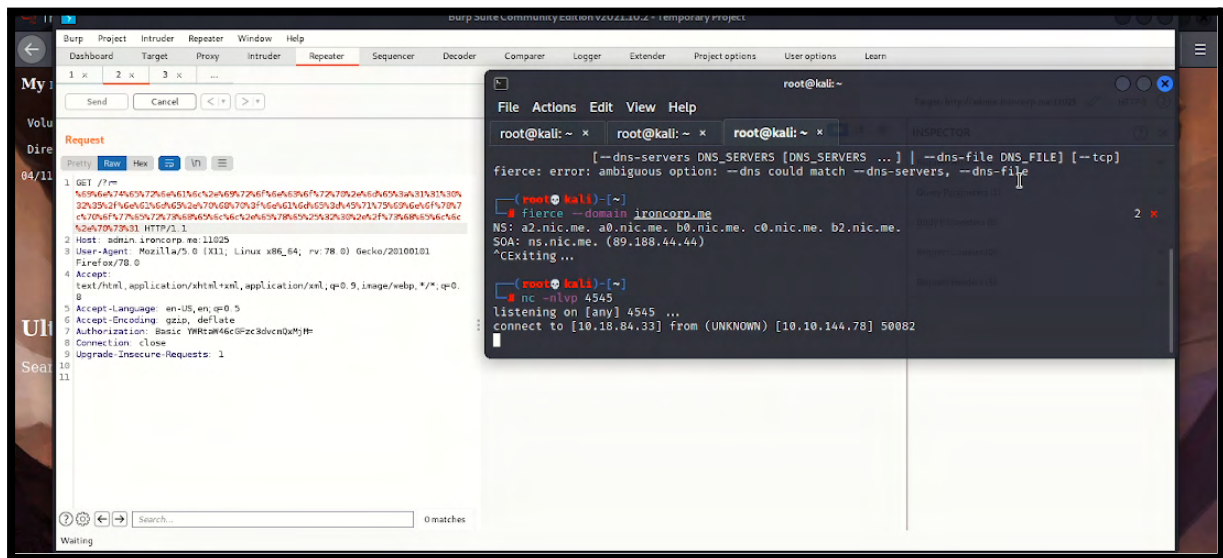
Sofea used the netcat command as the scanning tool and she added nlvp which is for to specify what nc should listen to, service lookups on any ports, have the nc give more verbose output and specify the source port.



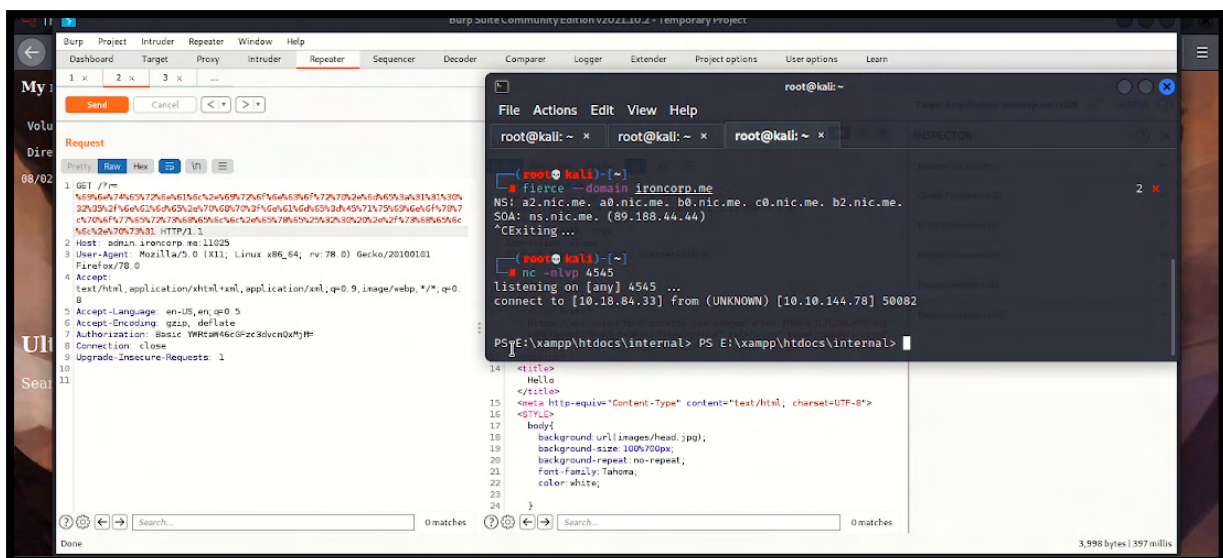
The screenshot shows a Kali Linux terminal window with the following content:

```
root@kali: ~  
TX packets 10 bytes 480 (480.0 B)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
tun1: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500  
inet 10.18.84.33 netmask 255.255.128.0 destination 10.18.84.33  
inet6 fe80::b81e:a46d:a248:eb40 prefixlen 64 scopeid 0x20<link>  
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)  
RX packets 4622 bytes 4903822 (4.6 MiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 5646 bytes 343760 (335.7 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(root@kali)~  
# nc -nlvp 4545  
listening on [any] 4545 ...  
  
(root@kali)~  
# nc -nlvp 4545  
listening on [any] 4545 ...
```

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`.

```

root@kali: ~
File Actions Edit View Help

root@kali: ~ x root@kali: ~ x
NS: a2.nic.me. a8.nic.me. b8.nic.me. c0.nic.me. b2.nic.me.
SOA: ns.nic.me. (89.18.44.44)
^CExiting ...

root@kali: ~ x [-]
# nc -l -p 4545
listening on [any] 4545 ...
connect to [10.18.84.33] from (UNKNOWN) [10.10.146.79] 50082

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

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   2:23 PM             582 shell.ps1

PS E:\xampp\htdocs\internal>

```

The screenshot shows a terminal window titled "root@kali: ~". The user has executed the command `dig @10.10.144.78 ironcorp.me axfr`. The output displays several DNS records:

```
;; WHEN: Tue Aug 02 17:32:47 EDT 2022
;; MSG SIZE rcvd: 101

<> DIG 9.17.19-3-Debian <> 10.10.144.78 ironcorp.me axfr
(1 server found)
;; global options: +cmd
ironcorp.me.          3600    IN      SOA     win=8vnbkf3g815.hostmaster. 3 900 600 86400 3600
ironcorp.me.          3600    IN      NS      win=8vnbkf3g815.
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=8vnbkf3g815.hostmaster. 3 900 600 86400 3600

;; Query time: 335 msec
;; SERVER: 10.10.144.78#53(10.10.144.78) (TCP)
;; WHEN: Tue Aug 02 17:33:41 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

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:].

The screenshot shows a Kali Linux terminal window with the following content:

```

root@kali: ~
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x root@kali: ~ x
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 2:23 PM 502 shell.ps1

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
-a 8/2/2022 2:23 PM 502 shell.ps1

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

The screenshot shows a Kali Linux terminal window with the following content:

```

root@kali: ~ - root@kali: ~ - root@kali: ~
-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 2:23 PM 582 shell.ps1

PS E:\xampp\htdocs\internal> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : eu-west-1.compute.internal
Link-local IPv6 Address . . . . . : fe80::5926:4c1b:4040:f6b64
IPv4 Address. . . . . : 10.10.164.78
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 10.10.0.1

Tunnel adapter Isatap.eu-west-1.compute.internal:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : eu-west-1.compute.internal

PS E:\xampp\htdocs\internal>

```

A screenshot of a Kali Linux terminal window titled "root@kali: ~". The terminal shows the following commands and output:

1. Command: `PS E:\xampp\htdocs\internal> ipconfig`
Output:
Windows IP Configuration

Ethernet adapter Ethernet:

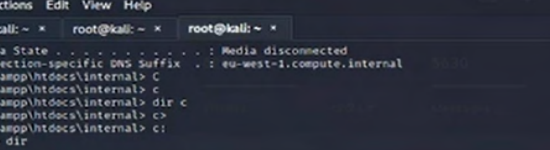
 Connection-specific DNS Suffix . : eu-west-1.compute.internal
 Link-local IPv6 Address : fe80::5926:ac18:404e:f4ba%
 IPv4 Address. : 10.10.144.78
 Subnet Mask : 255.255.0.0
 Default Gateway : 10.10.0.1

Tunnel adapter isatap.eu-west-1.compute.internal:

 Media State : Media disconnected
 Connection-specific DNS Suffix . : eu-west-1.compute.internal

2. Command: `PS E:\xampp\htdocs\internal> C`
3. Command: `PS E:\xampp\htdocs\internal>`
4. Command: `PS E:\xampp\htdocs\internal> dir c`
5. Command: `PS E:\xampp\htdocs\internal> c>`
6. Command: `PS E:\xampp\htdocs\internal> c:`
7. Command: `PS C:>`

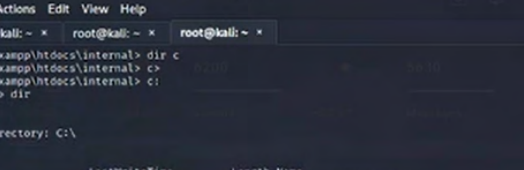
Then, Adriana types in `[dir]` again and looks at the all the files and directories in there and sees a Users file. So she changed directory to users using `[cd users]` and types `[whoami]` where `[nt authority/system]` will come out.



The screenshot shows a Kali Linux terminal window with a dark background. At the top, the title bar reads "root@kali: ~". The terminal prompt is "root@kali: ~". The user has entered the command "PS E:\xampp\htdocs\internal> c", which has been executed. The output shows the directory "C:\\" and its contents. The directory listing is as follows:

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-----	4/11/2020 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-----	4/11/2020 11:28 AM		Windows

The terminal window also shows the command "PS C:\> dir" and the output "Directory: C:\\". The terminal window has a menu bar with "File", "Actions", "Edit", "View", and "Help". The terminal window also has a status bar at the bottom showing "PS C:\>".



The screenshot shows a Kali Linux terminal window with the title bar "root@kali: -". The terminal content is as follows:

```

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

root@kali: ~ - x root@kali: ~ - x root@kali: ~ - x

PS E:\xampp\htdocs\internal> dir c
PS E:\xampp\htdocs\internal> c>
PS E:\xampp\htdocs\internal> c:
PS C:\> dir

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 10:45 PM             PerfLogs
d-----         4/13/2020 11:19 AM             Program Files
d-----         4/11/2020 10:42 AM             Program Files (x86)
d-----         4/11/2020  4:41 AM             Users
d-----         4/11/2020 11:26 AM             Windows

PS C:\> cd users
PS C:\users> whoami
PS C:\users> whoami
nt authority\system
PS C:\users>
  
```

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.

The screenshot shows a Kali Linux terminal window with the title bar 'root@kali: ~'. The terminal content is as follows:

```

root@kali: ~ ~ root@kali: ~ ~ root@kali: ~ ~
d----- 4/13/2020 11:28 AM
PS C:\> cd users
PS C:\users> whoami
PS C:\users> whoami
nt authority\system
PS C:\users> dir

        Directory: C:\users

Mode                LastWriteTime         Length Name
----                -
d----- 4/11/2020 4:43 AM             Admin
d----- 4/11/2020 11:07 AM           Administrator
d----- 4/11/2020 11:55 AM           Equinox
d-r----- 4/11/2020 10:36 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>

```

The screenshot shows a Windows command prompt window with the title bar 'root@kali -'. The command history and current session are as follows:

```

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

The screenshot shows a Kali Linux terminal window with the title 'root@kali:~'. The terminal displays the following commands and output:

```

root@kali:~# ls -l
total 12
drwxr-xr-x 3 root root 4096 Apr 12 2020 .
drwxr-xr-x 3 root root 4096 Apr 12 2020 ..
drwxr-xr-x 2 root root 4096 Apr 12 2020 Desktop
drwxr-xr-x 2 root root 4096 Apr 12 2020 Documents
drwxr-xr-x 2 root root 4096 Apr 12 2020 Downloads
drwxr-xr-x 2 root root 4096 Apr 12 2020 Favorites
drwxr-xr-x 2 root root 4096 Apr 12 2020 Links
drwxr-xr-x 2 root root 4096 Apr 12 2020 Music
drwxr-xr-x 2 root root 4096 Apr 12 2020 Pictures
drwxr-xr-x 2 root root 4096 Apr 12 2020 Saved Games
drwxr-xr-x 2 root root 4096 Apr 12 2020 Searches
drwxr-xr-x 2 root root 4096 Apr 12 2020 Videos

root@kali:~# cd Desktop
root@kali:~/Desktop# touch user.txt
root@kali:~/Desktop# ls -l
total 4
-rw-rw-r-- 1 root root 0 Apr 28 2020 user.txt

root@kali:~/Desktop#

```

The terminal window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The title bar shows 'root@kali:~' and standard window controls. The background of the terminal is dark with a large, faint Kali Linux logo watermark.

The screenshot shows a Kali Linux terminal window with the title bar "Kali Linux" and standard window controls. The terminal prompt is "1211103282@kali: ~". The user has entered the command "ls -la /Desktop", which has produced a long listing of files in the Desktop directory. The output shows files like "Contacts", "Desktop", "Documents", "Downloads", "Favorites", "Links", "Music", "Pictures", "Saved Games", "Searches", and "Videos", all with permissions of "d-r--r--r--". Below this, the user has entered "cd Desktop" and "dir", which has produced a directory listing of the Desktop directory, showing a file named "user.txt" with permissions "37 user.txt".

```

1211103282@kali: ~
File Actions Edit View Help
1211103282@kali: ~ x 1211103282@kali: ~ x 1211103282@kali: ~ x 1211103282@kali: ~ x

Mode                LastWriteTime         Length Name
----                -
d-r--r--r--       4/12/2020   1:27 AM             Contacts
d-r--r--r--       4/12/2020   1:27 AM             Desktop
d-r--r--r--       4/12/2020   1:27 AM             Documents
d-r--r--r--       4/12/2020   1:27 AM             Downloads
d-r--r--r--       4/12/2020   1:27 AM             Favorites
d-r--r--r--       4/12/2020   1:27 AM             Links
d-r--r--r--       4/12/2020   1:27 AM             Music
d-r--r--r--       4/12/2020   1:27 AM             Pictures
d-r--r--r--       4/12/2020   1:27 AM             Saved Games
d-r--r--r--       4/12/2020   1:27 AM             Searches
d-r--r--r--       4/12/2020   1:27 AM             Videos

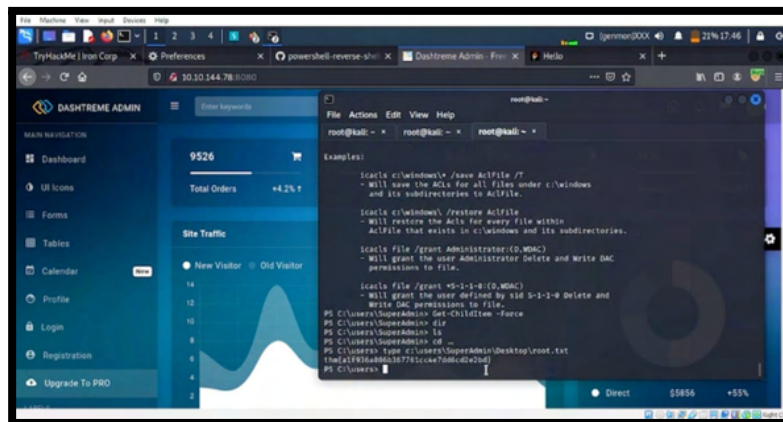
PS C:\Users\Administrator> cd Desktop
PS C:\Users\Administrator\Desktop> dir

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-----       3/28/2020   12:39 PM             37 user.txt

PS C:\Users\Administrator\Desktop> type user.txt
tmi[09b480856a13fc222f3be64cf599f8c]
PS C:\Users\Administrator\Desktop>
  
```

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](#)