PenTest 2
TT7L
GROUPNAME: GGez

Members

ID	NAME	ROLE
1211101951	Muhammad Zaieff Danial Bin Mohd Suhaimi	Leader
1211100528	Muhammad Arief Fahmi Bin Syahril Anuar	Member
1211101643	Sivaharriharann A/L Ramanathan	Member
1211101120	Adam Uzair Bin Mohd Sori	Member

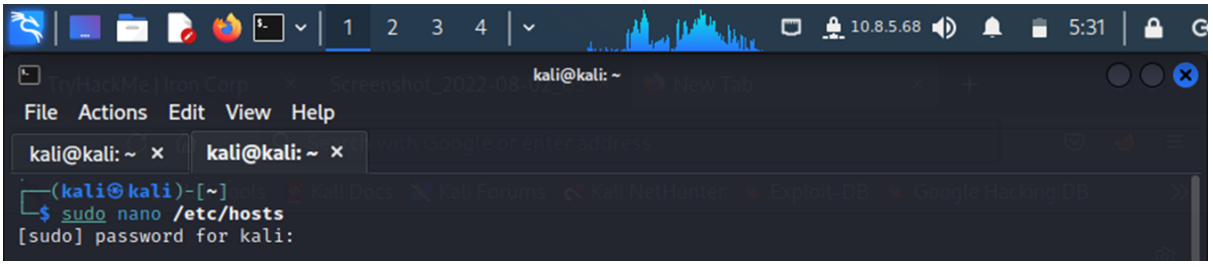
Steps: (example) Recon and Enumeration
You should divide your report into 4 sections in general:

1) Recon and Enumeration (Where you gather data)
2) Initial Foothold (where you gain the first reverse shell)
3) Horizontal Privilege Escalation (If any, if you pivot to other users)
4) Root Privilege Escalation (final step, rooting)

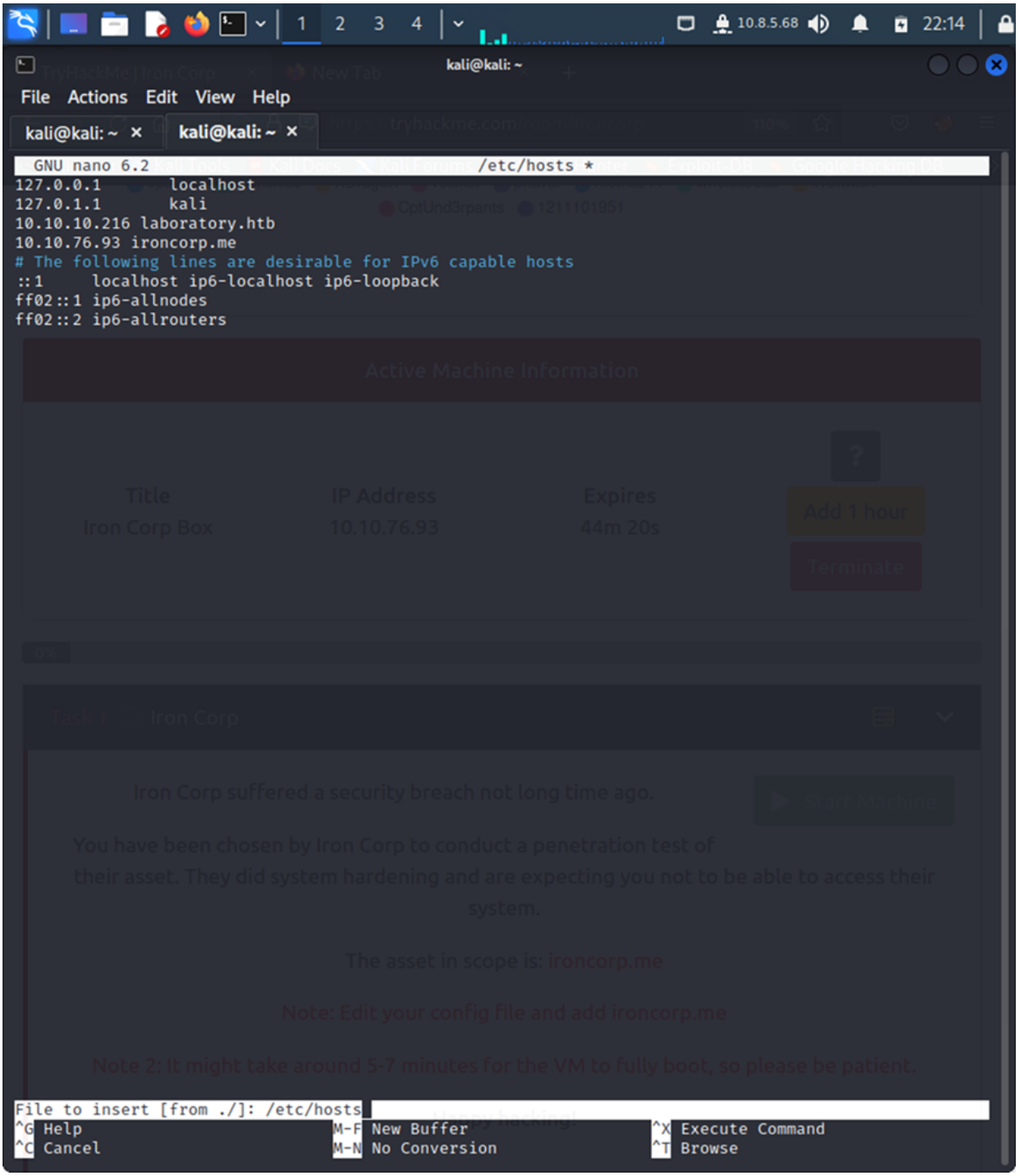
Recon and Enumaration

Members involved : Muhammad Zaieff Danial Bin Mohd Suhaimi
Tools used :Terminal,Mozilla Firefox,Hydra,Nano,Digmentation

Thought Process , Methodology and Attempt



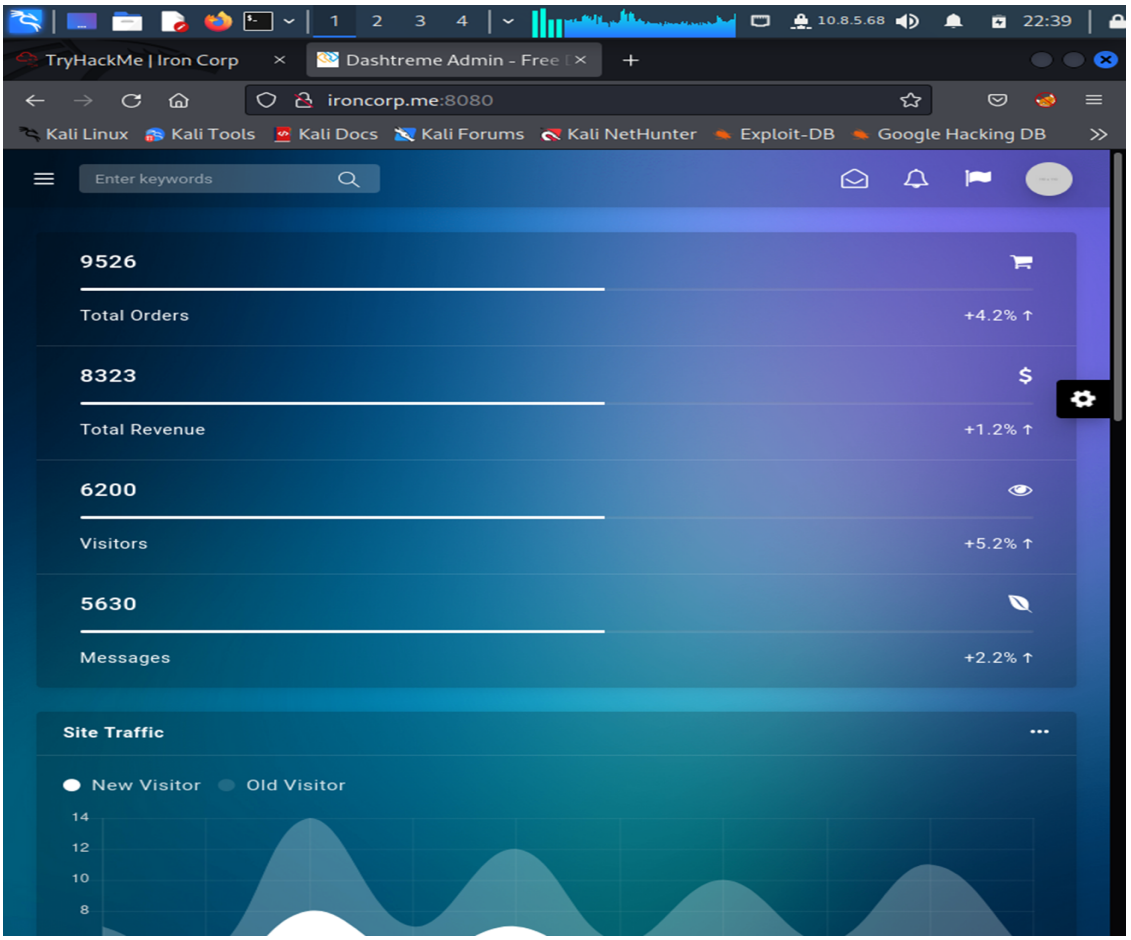
Open terminal and enter nano hosts.



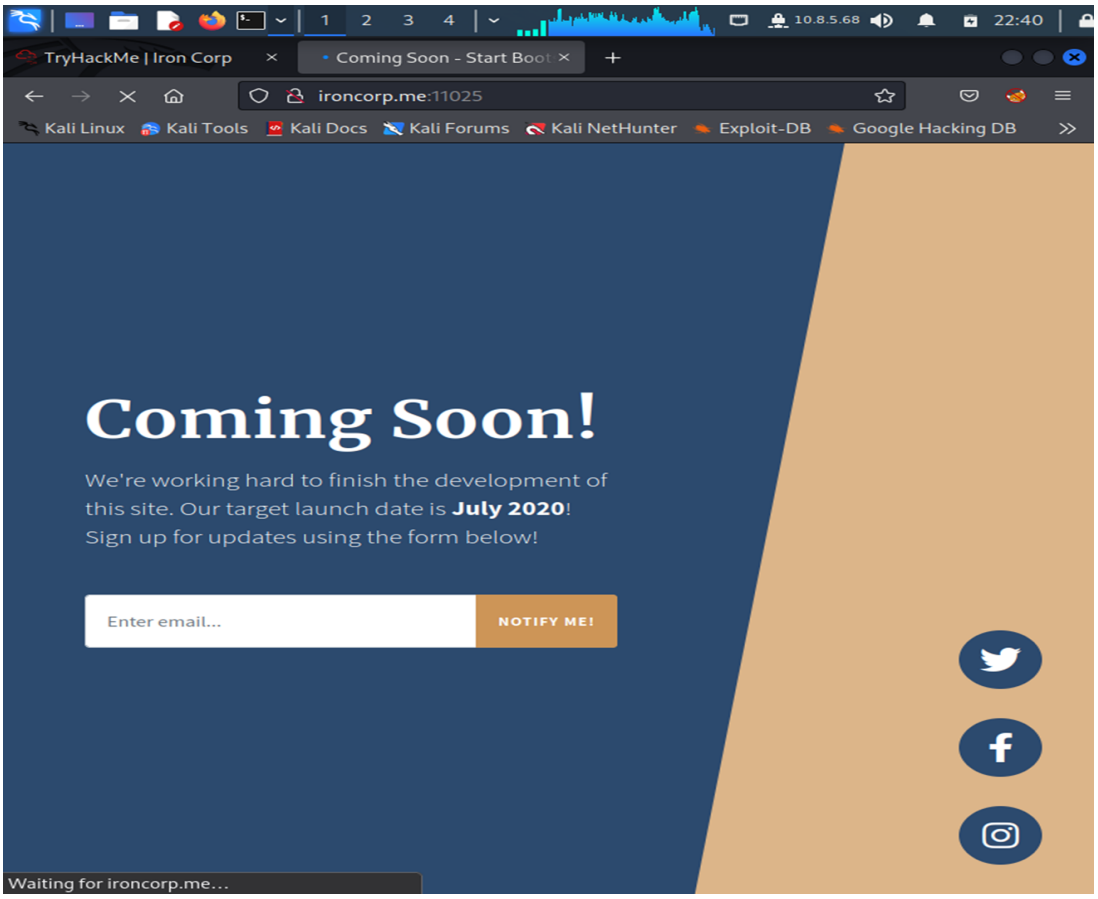
Insert MACHINE_IP address and the assets to allocate the connection.

```
┌──(kali㉿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 04:44 EDT
Nmap scan report for ironcorp.me (10.10.119.59)
Host is up (0.24s 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: 2022-08-02T08:46:02+00:00
| ssl-cert: Subject: commonName=WIN-8VMBKF3G815
| Not valid before: 2022-08-01T08:36:51
|_Not valid after:  2023-01-31T08:36:51
|_ssl-date: 2022-08-02T08:46:10+00:00; +1s 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-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
```

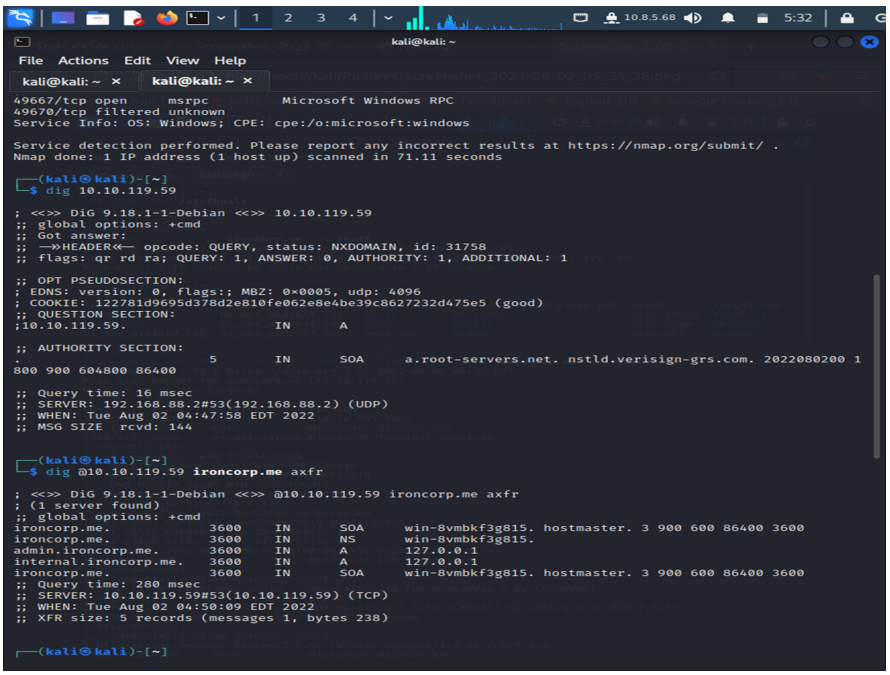
Kick start with insert IP Address in ‘etc/hosts’ and execute nmap



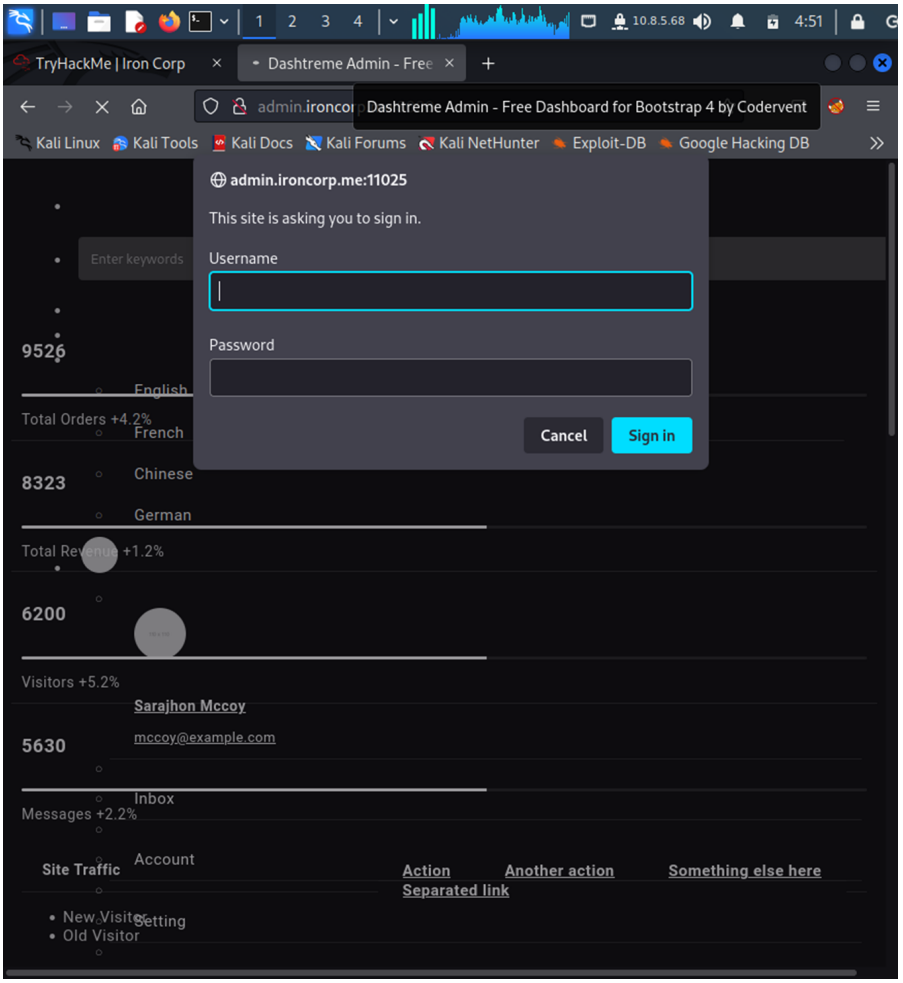
We access the web service of port 8080 and have a control panel, we examine but there is no functionality that can serve us.



Next we access the web service of port 11025 and have the control panel but it shows an entered email address but another reason that does not contain information or any functionality.



Nmap took out only 53 ports so we should command dig so we can list any sub-domain or information that is relevant to us. It has useful content to search on to continue the mission.



For example , if we copy admin.ironcorp.me:11025 which is allocated in the dig information the site will ask you to sign-in.

```
┌──(kali㉿kali)-[~]
└─$ hydra -l admin -p password123 -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 04:56:48
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[11025][http-get] host: admin.ironcorp.me   login: admin   password: password123
```

Enter Hydra for admin and password for attacking http-get website. It provides login and password information.

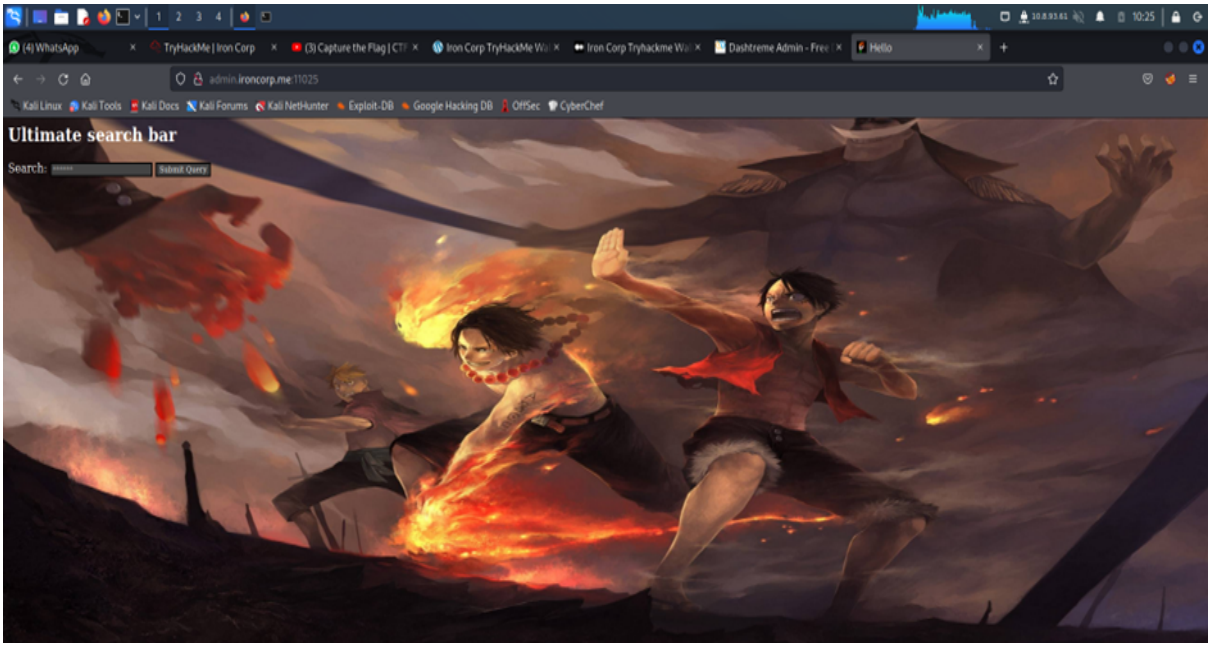
Initial Foothold

Members involved : Muhammad Arief Fahmi Bin Syahril Anuar
Tools used :Terminal , Mozilla Firefox , Nano , Shell , Hydra , Burp Suite

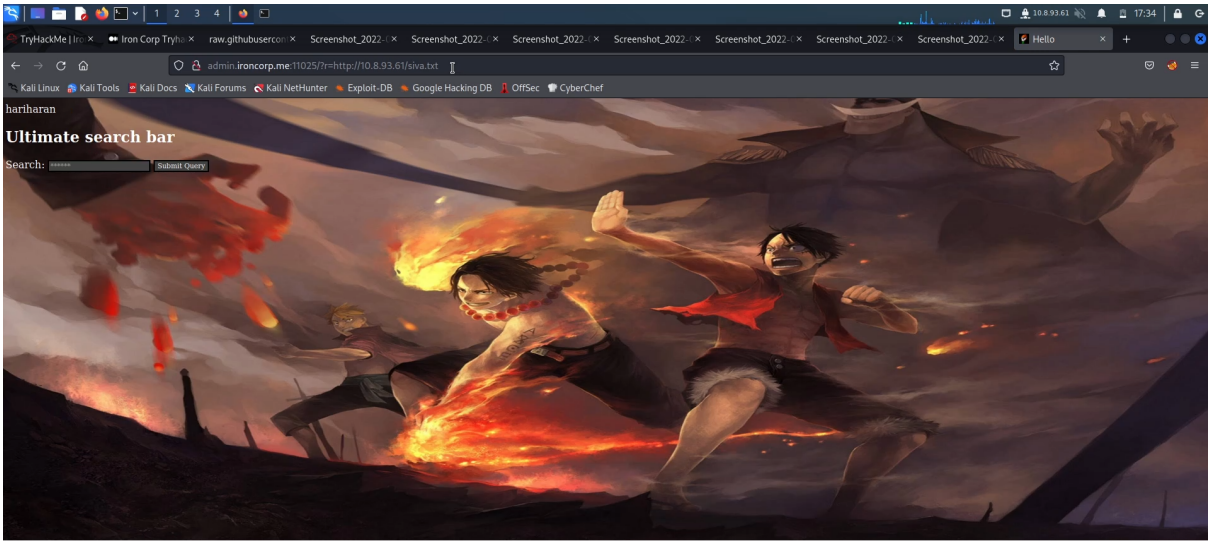
Thought Process , Methodology and Attempt

```
┌──(kali㉿kali)-[~]
└─$ hydra -l admin -p password123 -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 04:56:48
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[11025][http-get] host: admin.ironcorp.me   login: admin   password: password123
```

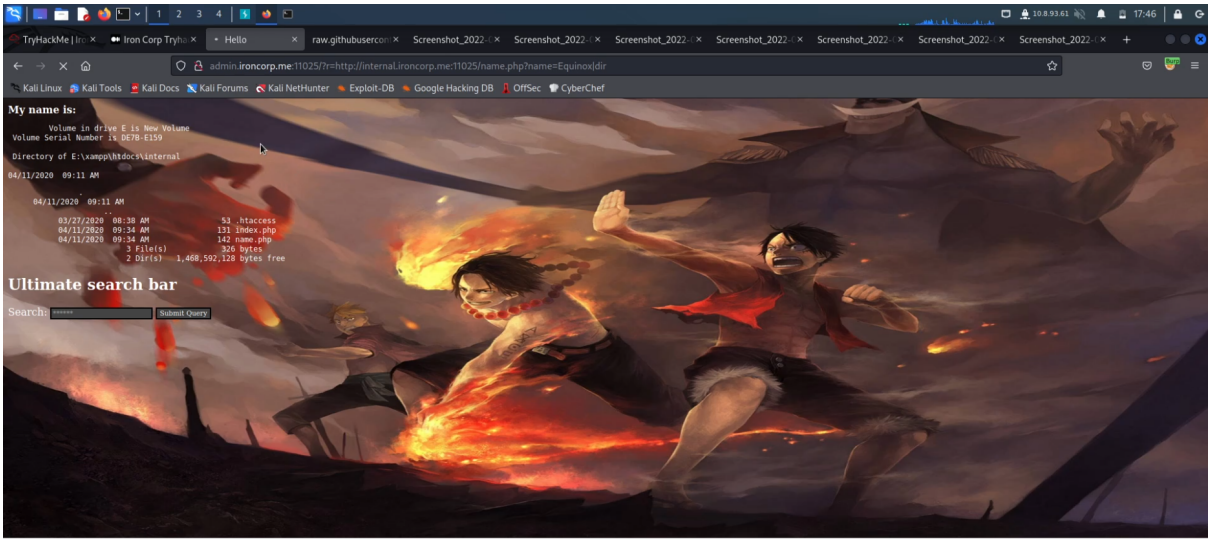
To get the user and password , we can use multiple ways to brute force and we choose to use Hydra by running a few commands and we will get it.



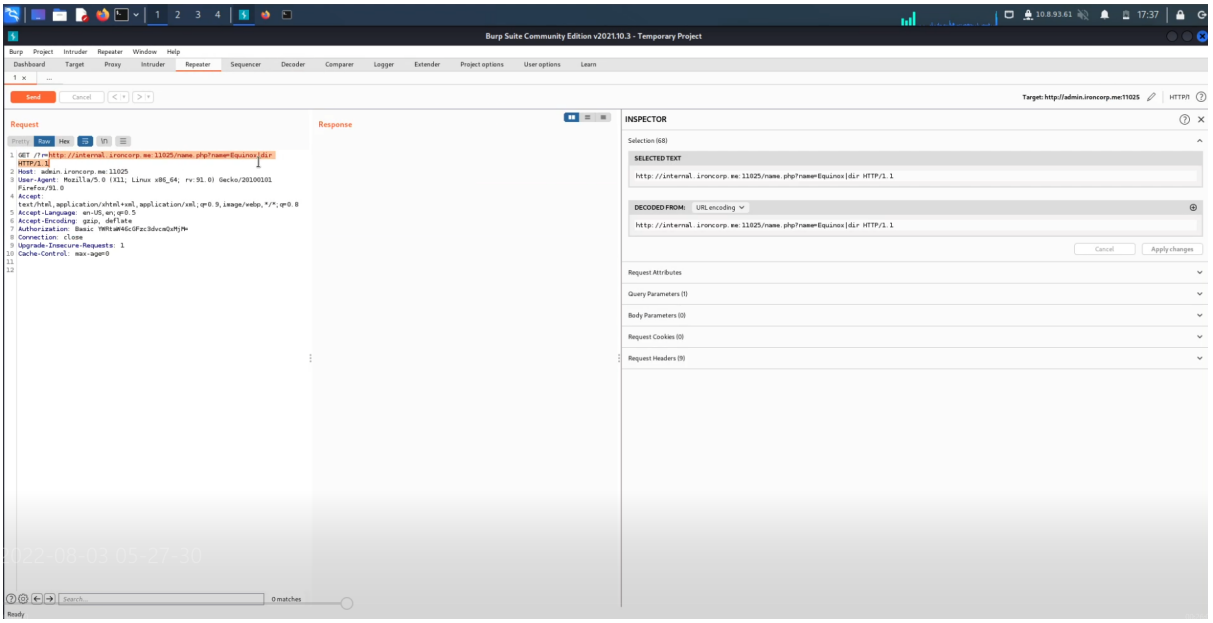
After we got in , we will see a web where we can check to see any vulnerabilities within the web .



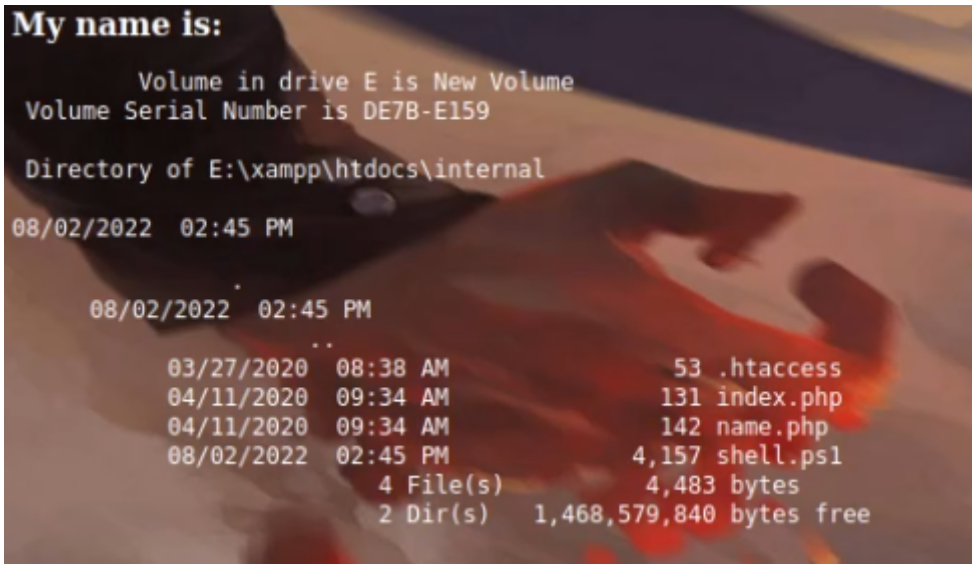
We later found out that we can change the text on the top of the search bar by just using nano and just upload the things that u wrote on the nano using the name of the text saved on the ip address .



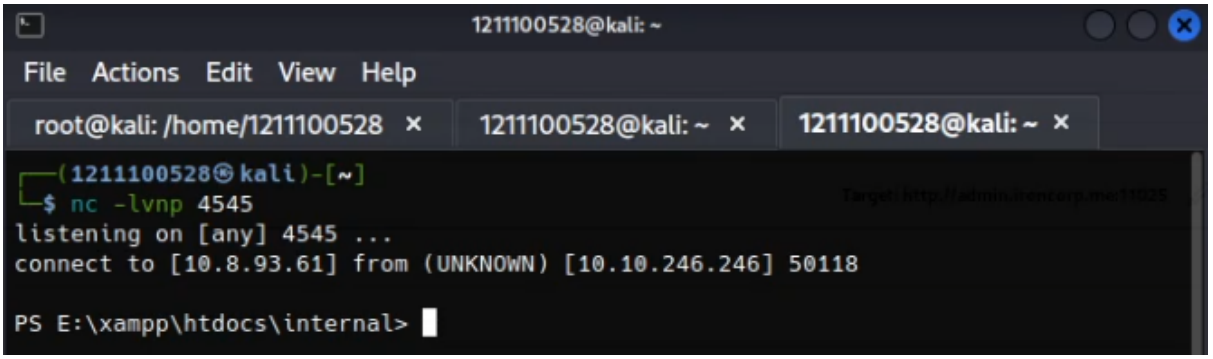
By putting in the internal Ip that we created on the web admin Ip address , we can see the hidden directory that existed on the web itself .



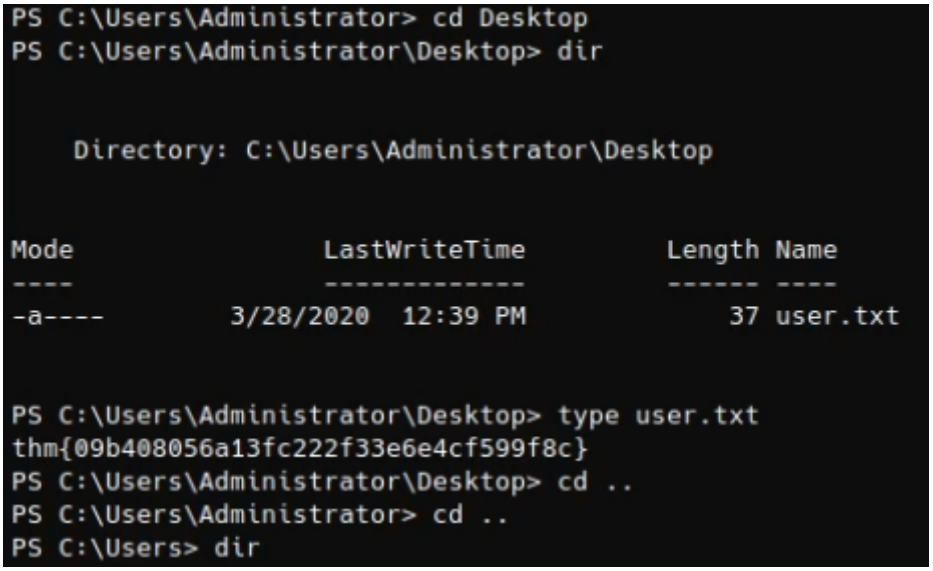
Then we just have to use Burp suite to intercept and to add on a reverse shell text that we created to put up on the web so that we can access the terminal later .



After we successfully uploaded the text , we can use the terminal to connect the web to the terminal itself so that we can access the admin directory page.



After we tried multiple times we finally managed to get the terminal to connect to the web so we can go on further solving the task .

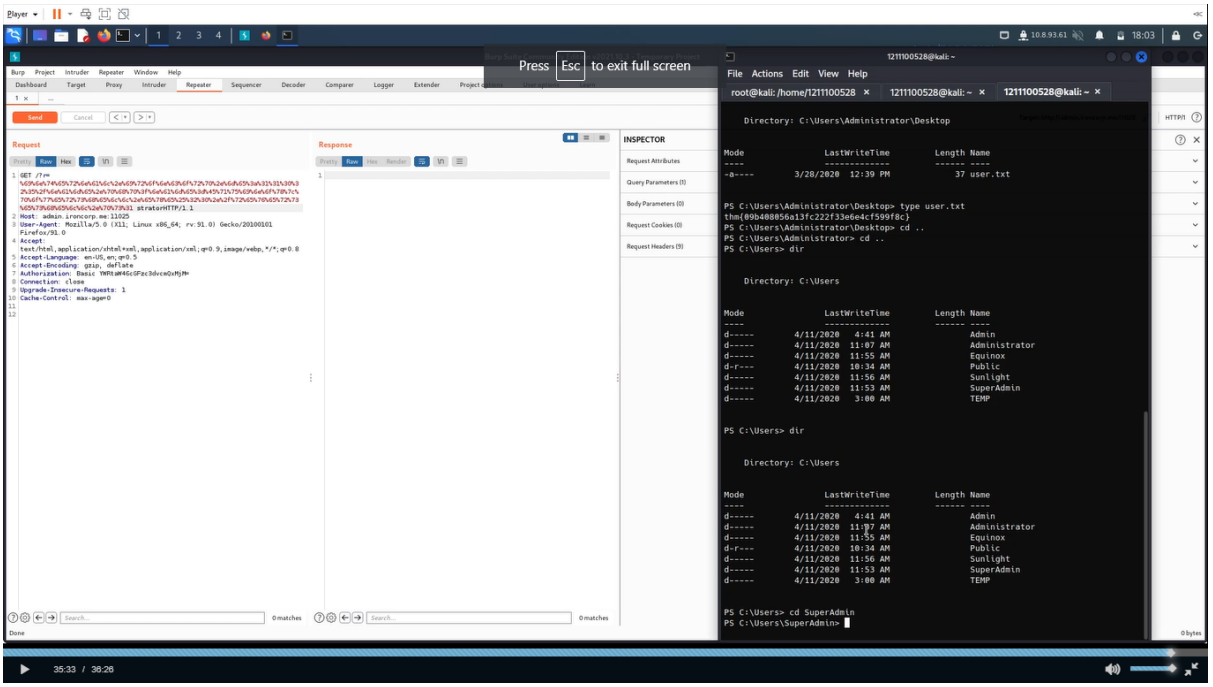


By just accessing the admin page we will get the first flag.

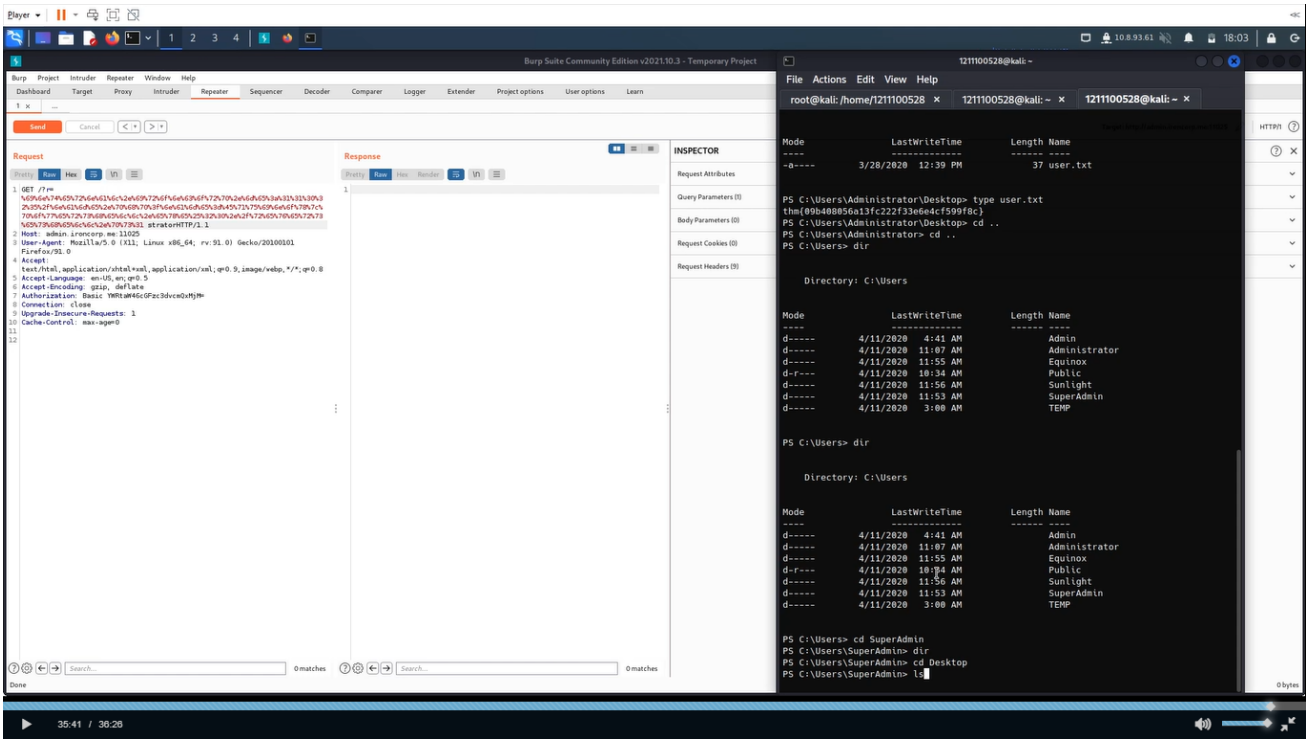
Root Privilege Escalation

Members involved : Sivaharriharann and Adam uzair
Tools used :Terminal , Mozilla Firefox

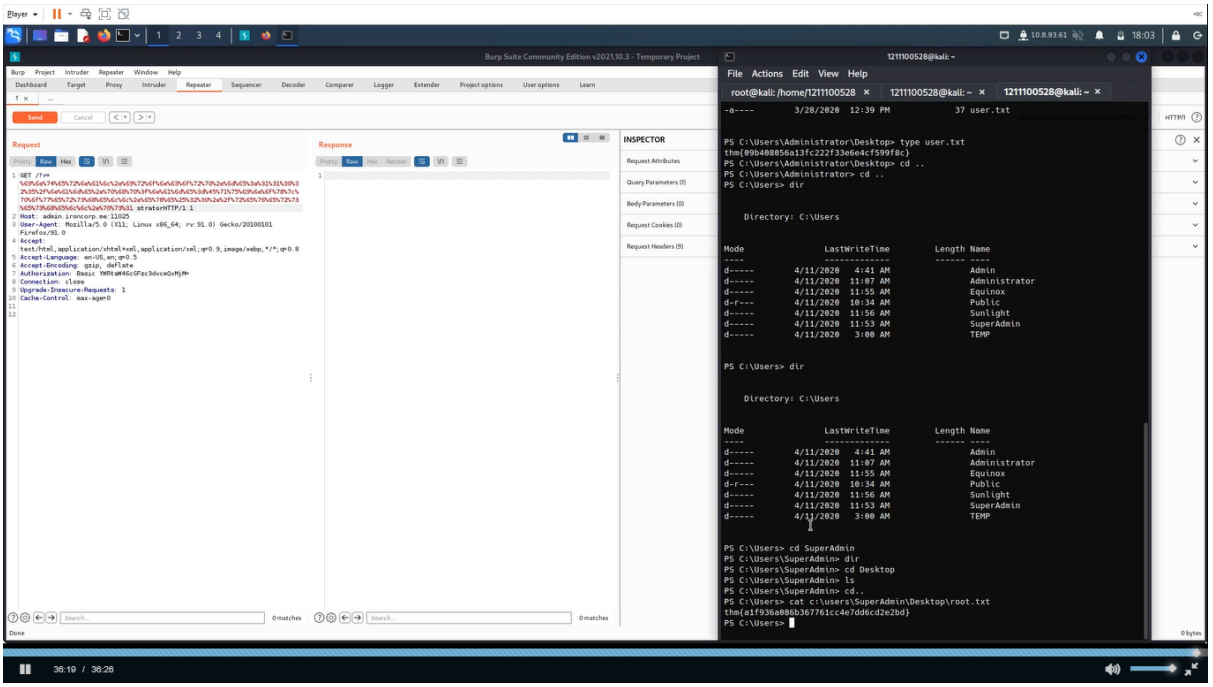
Thought Process , Methodology and Attempt



We execute the command “cd SuperAdmin” to find the root flag and also we cannot access the user”s directory.

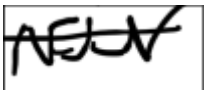


Then we command “cat :\users\SuperAdmin\Desktop\root.txt” to get the second flag of the pentest.



Finally we get the second flag which is the root flag.

Contribution

ID	Name	Contribution	Signature
1211101951	Zaieff	Did the Initial Foothold part , found the first flag , moral support giver	
1211100528	Arief	Did the recon and enumeration , food supplier	
1211101643 and 1211101120	Siva and Adam Uzair	Did the root privilege escalation part , found the second flag