PenTest 2

ROOM A

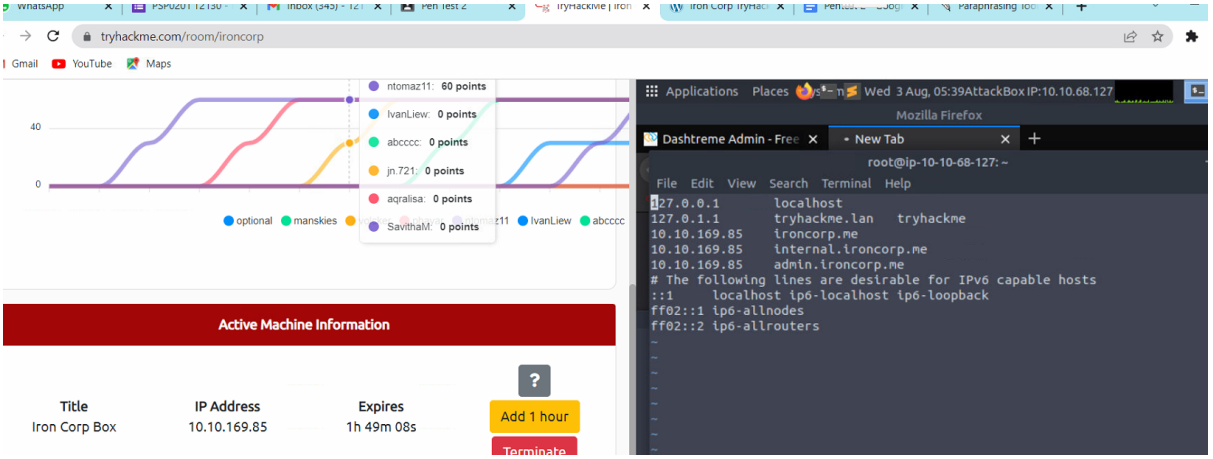
SANG HAEKEO

ID	NAME	ROLE
1211101693	Savitha Murugumunisegaran	Member

TOOLS USED: NMAP, Dig, Hydra, SSRF vulnerability attack,Burp suite, Abuse of privileges on the system and Capture the flag.

Reconnaissance

`I run nmap after adding the IP address to the "etc/hosts" file.`

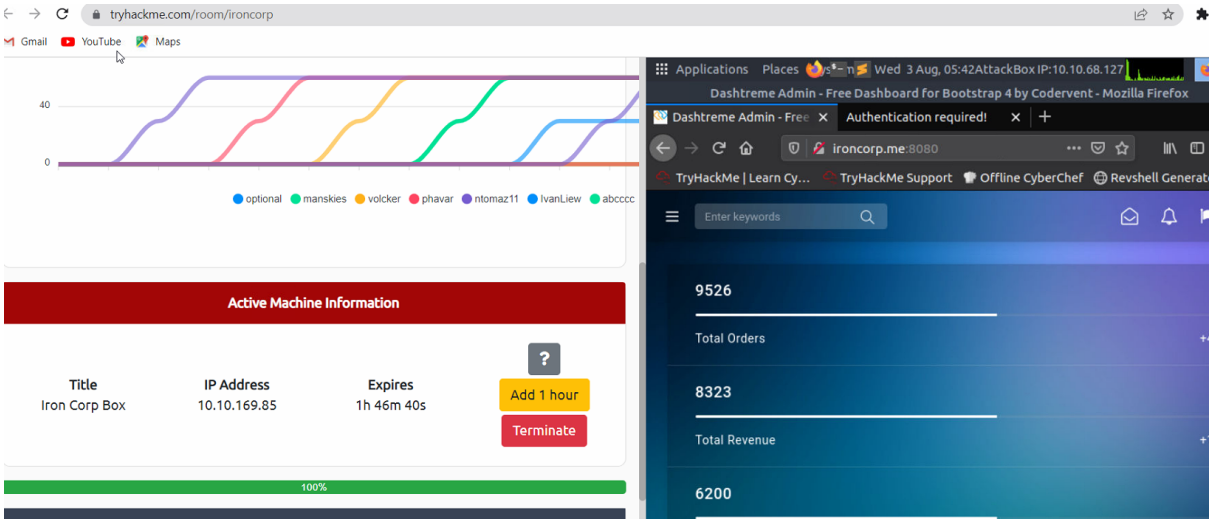


Running Nmap now

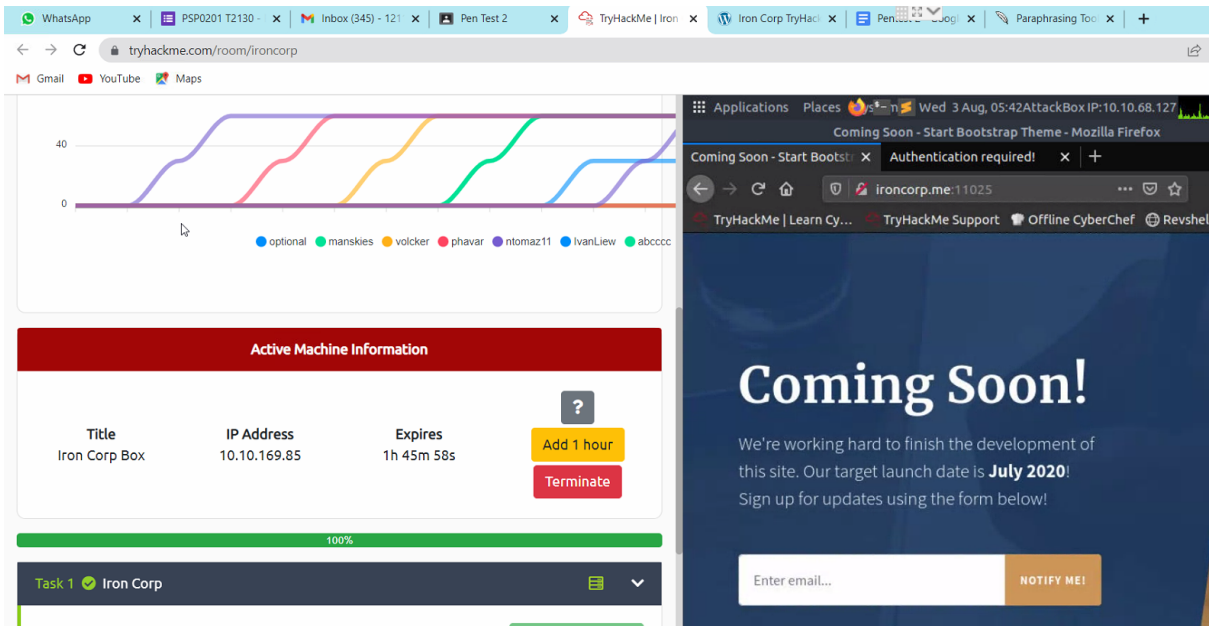
```
Service scan Timing: About 75.00% done; ETC: 02:11 (0:00:13 remaining)
Nmap scan report for ironcorp.me (10.10.118.76)
Host is up (0.024s latency).
Not shown: 64992 filtered ports
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS
135/tcp   open  msrpc         Microsoft Windows RPC
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=WIN-8VMBKF3G815
| Not valid before: 2022-08-01T00:18:57
| Not valid after:  2023-01-31T00:18:57
|_ssl-date: 2022-08-02T01:11:35+00:00; 0s from scanner time.
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
8080/tcp  open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Dashtreme Admin - Free Dashboard for Bootstrap 4 by Codervent
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-server-header: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4
|_http-title: Coming Soon - Start Bootstrap Theme
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 02:24:74:C8:64:8F (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 1323.40 seconds
root@ip-10-10-101-69:~# ~~~~~~~~~~~~~~~~~~~~
```

Enumeration

I found out that port 8080 and 11025 are running http services. So I figured out its application server and tried open it via browser.



I opened the browser on port 11025 and the page is coming soon. I suspect, usually new pages like this need to be set up and have an admin panel. So i dig more

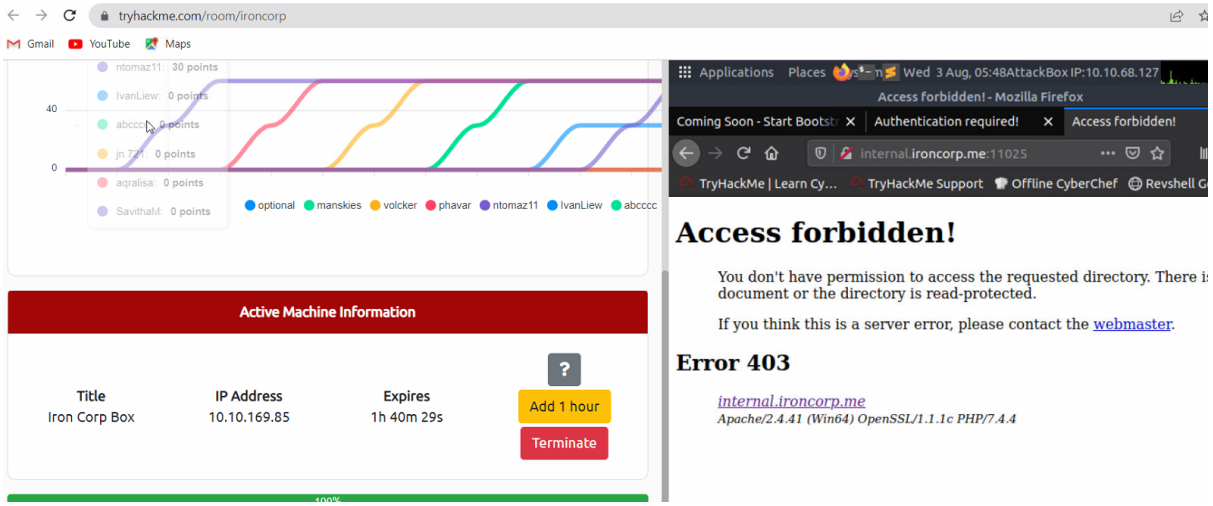


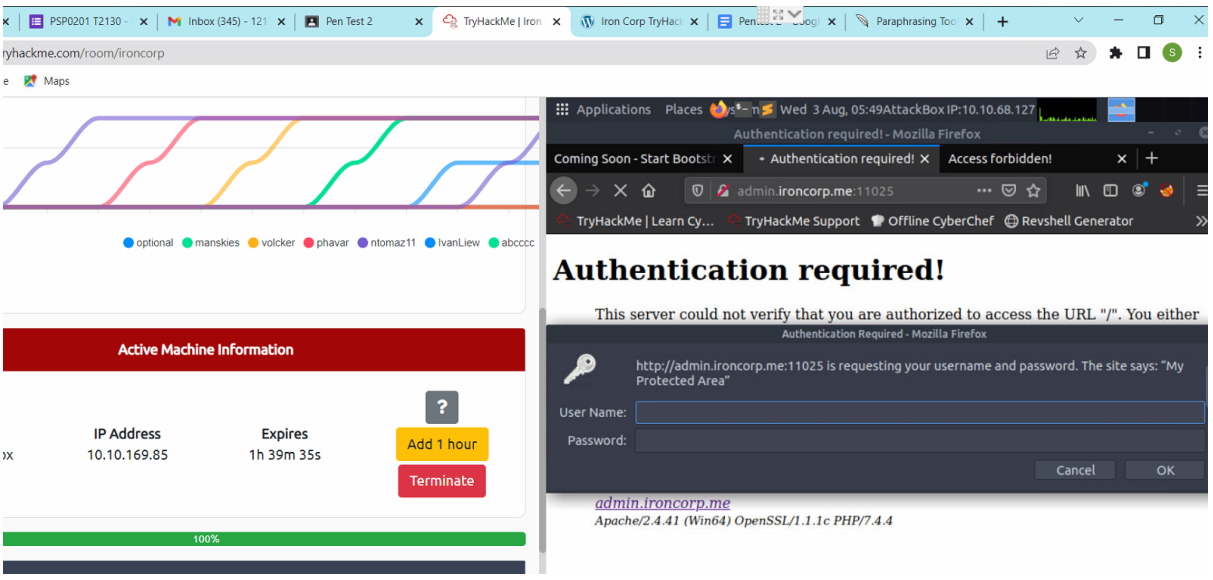
I suspect, usually new pages like this need to be set up and have an admin panel. So I dig more by putting the dig command. That's because there is DNS service up and running and we can identify the subdomains. .

Bingo! We have 2 subdomains.

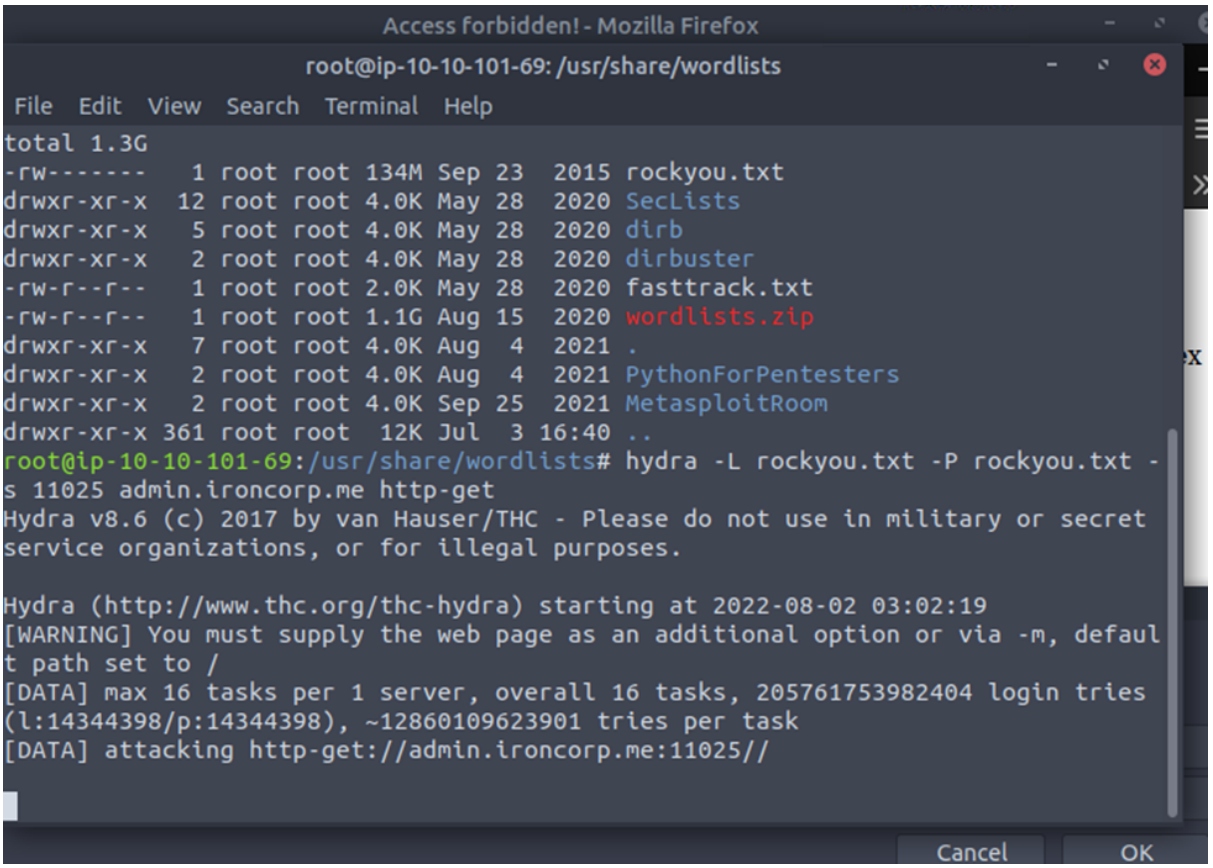
```
root@ip-10-10-101-69:~# dig @10.10.227.48 ironcorp.me  axfr

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> @10.10.227.48 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: 6 msec
;; SERVER: 10.10.227.48#53(10.10.227.48)
;; WHEN: Tue Aug 02 02:47:31 BST 2022
;; XFR size: 5 records (messages 1, bytes 238)

root@ip-10-10-101-69:~#
```

I tried to access both subdomains after adding the entry on the /etc/hosts file. Picture shown in the first picture.

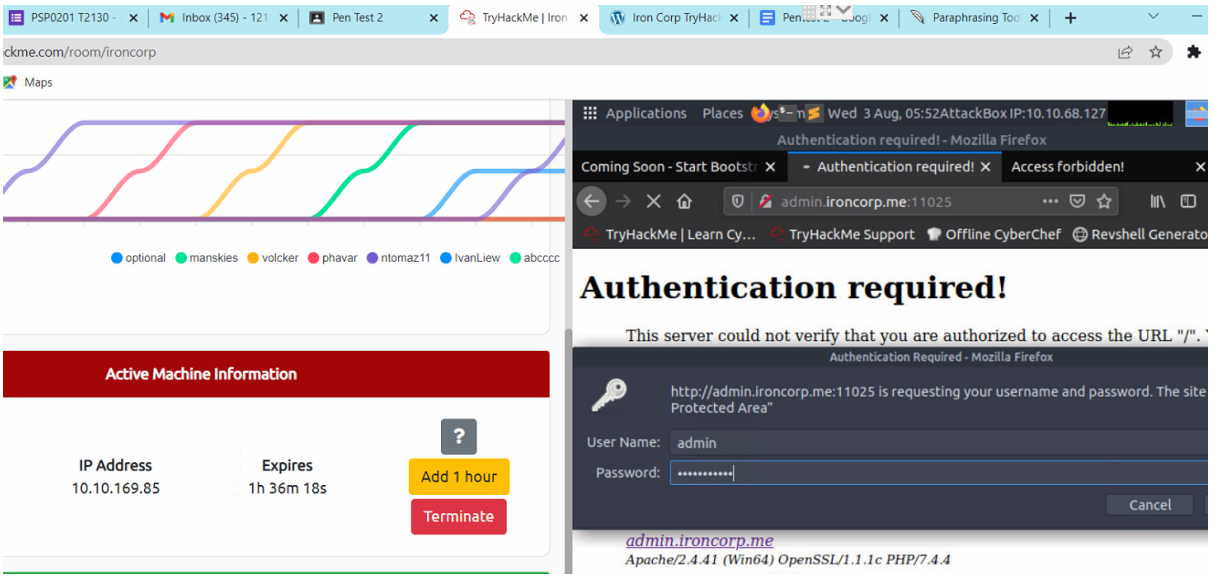




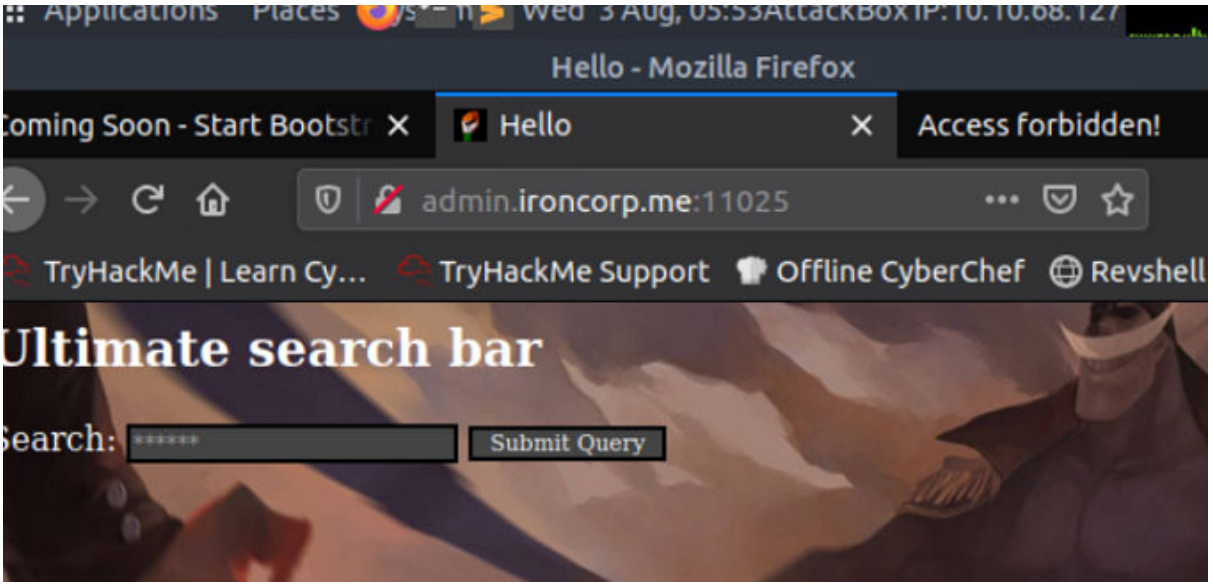
On the admin page, it requires username and password to login. So i have to use hydra to guess the password for known password list



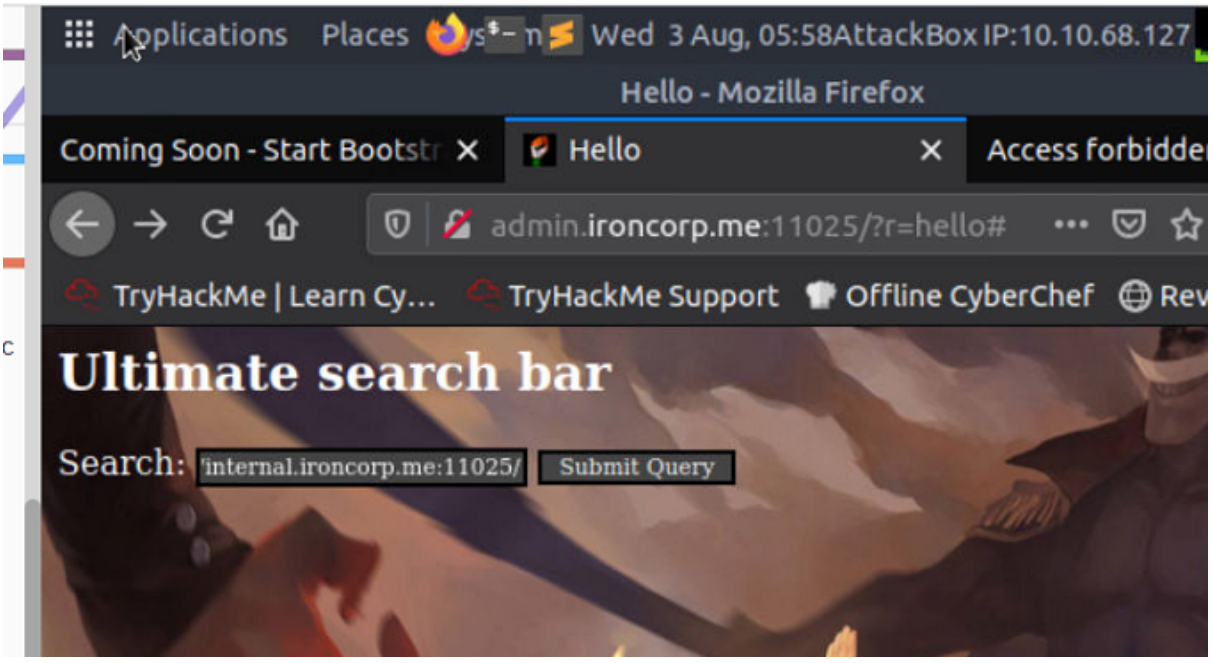
We manage to crack the password with admin and password is password 123.



Whoa! It's able to login into the server. But its just giving an empty search button.

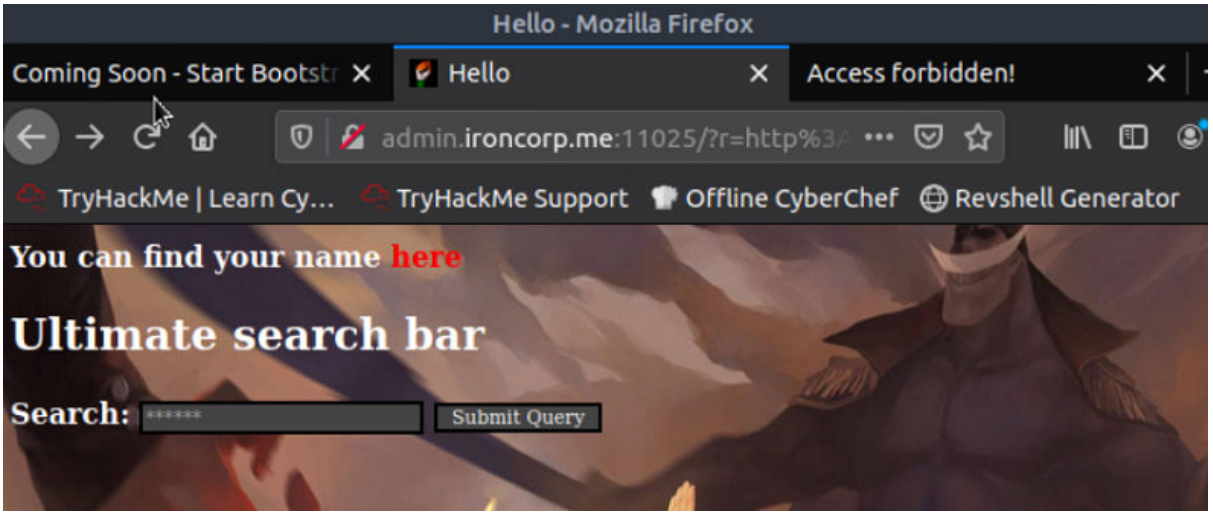


When i do search on the query, its actually redirect the query to another place.

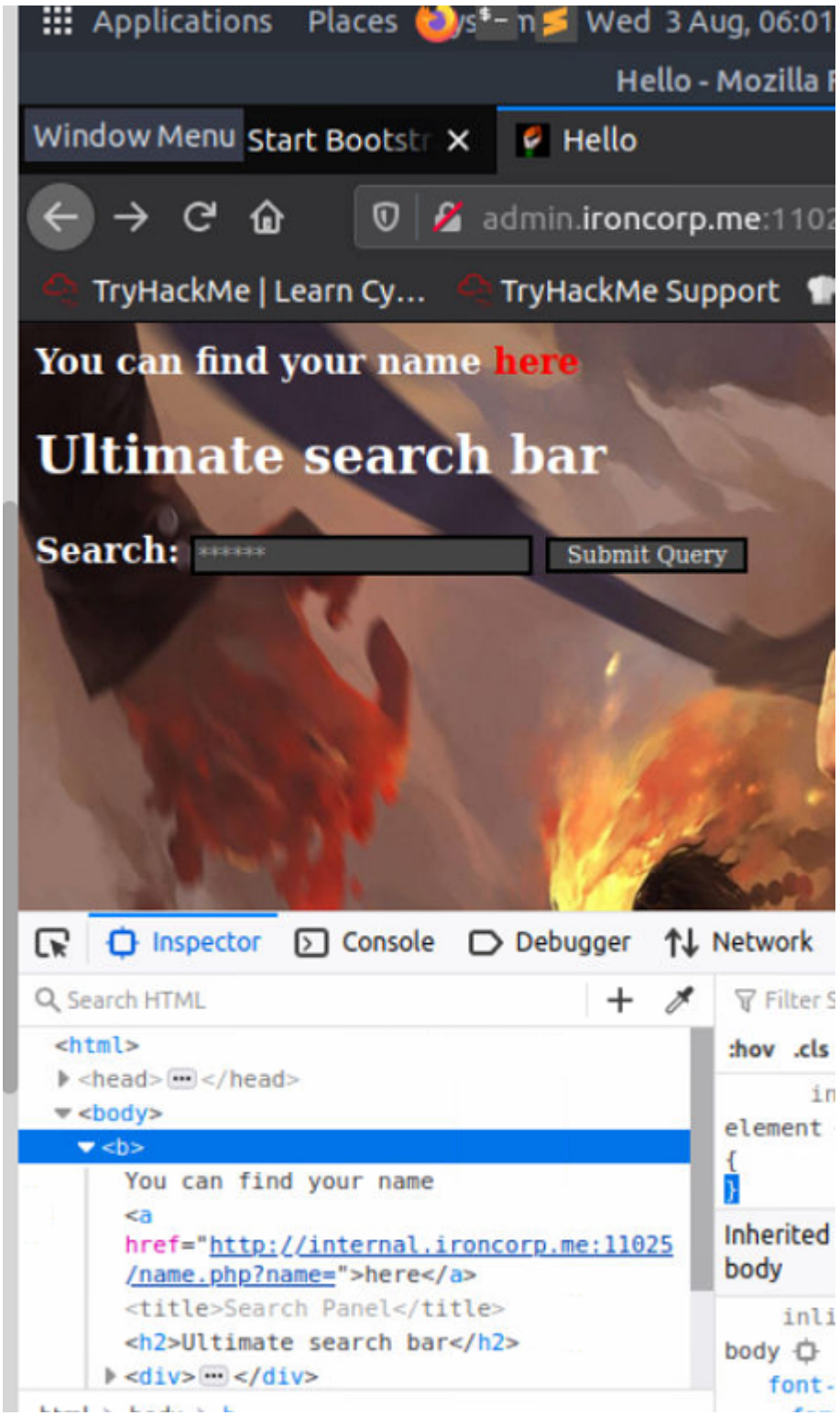


Since it redirects or calls the function on query, I decided to put the internal domain on the search button. Results as below.

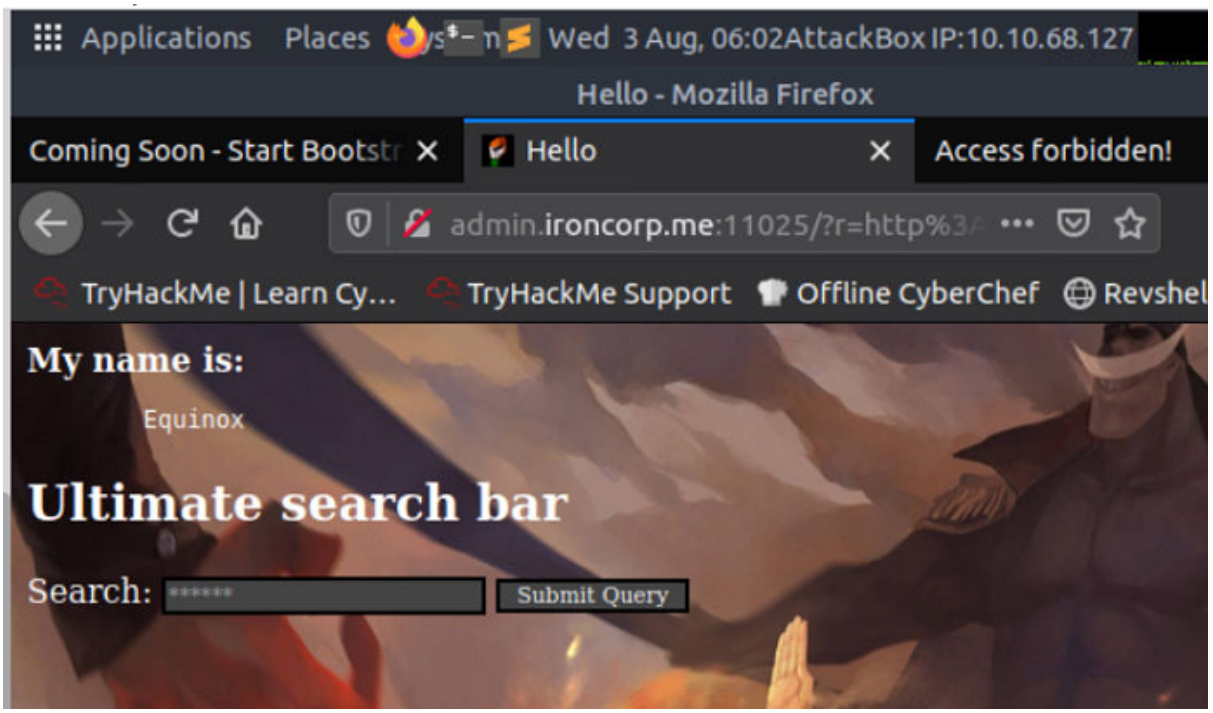
Exploiting



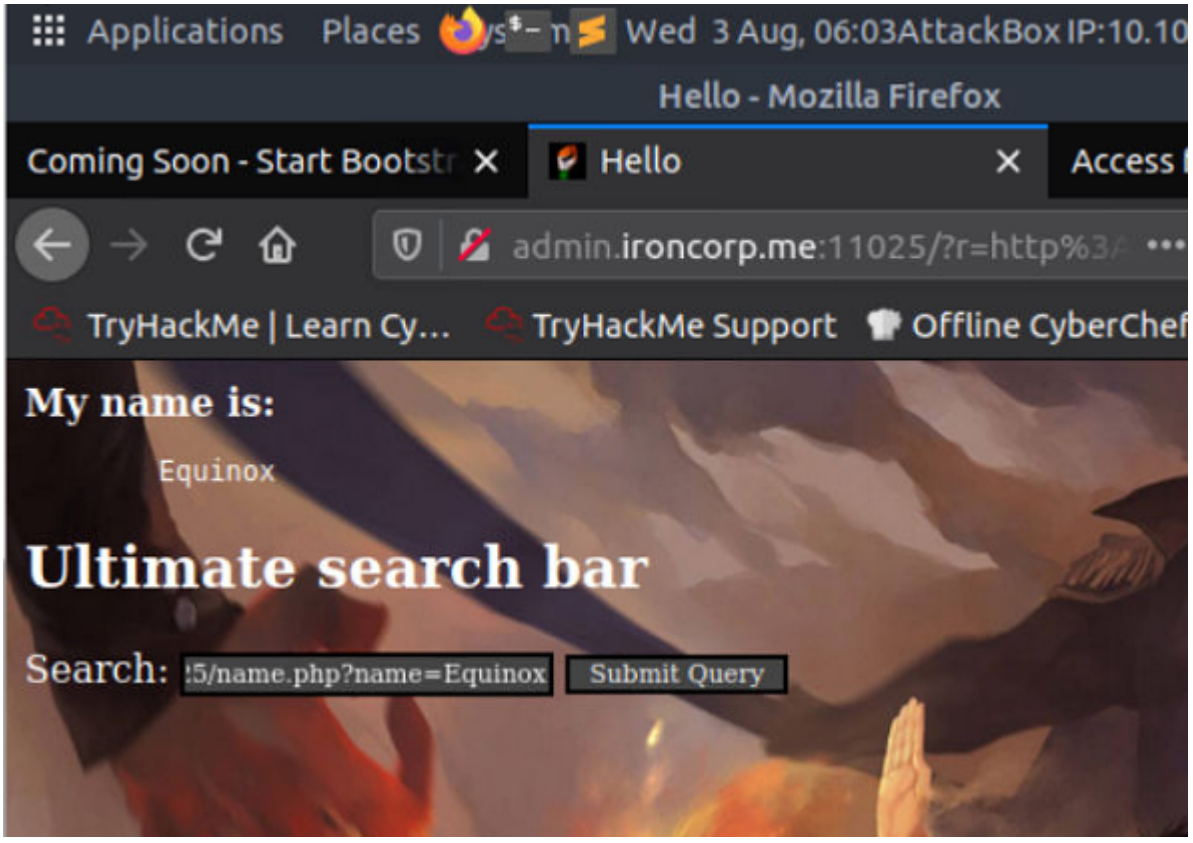
I saw here wording tight with some hyperlink. So I decided to check the link on webpage developer tools and found out the url.



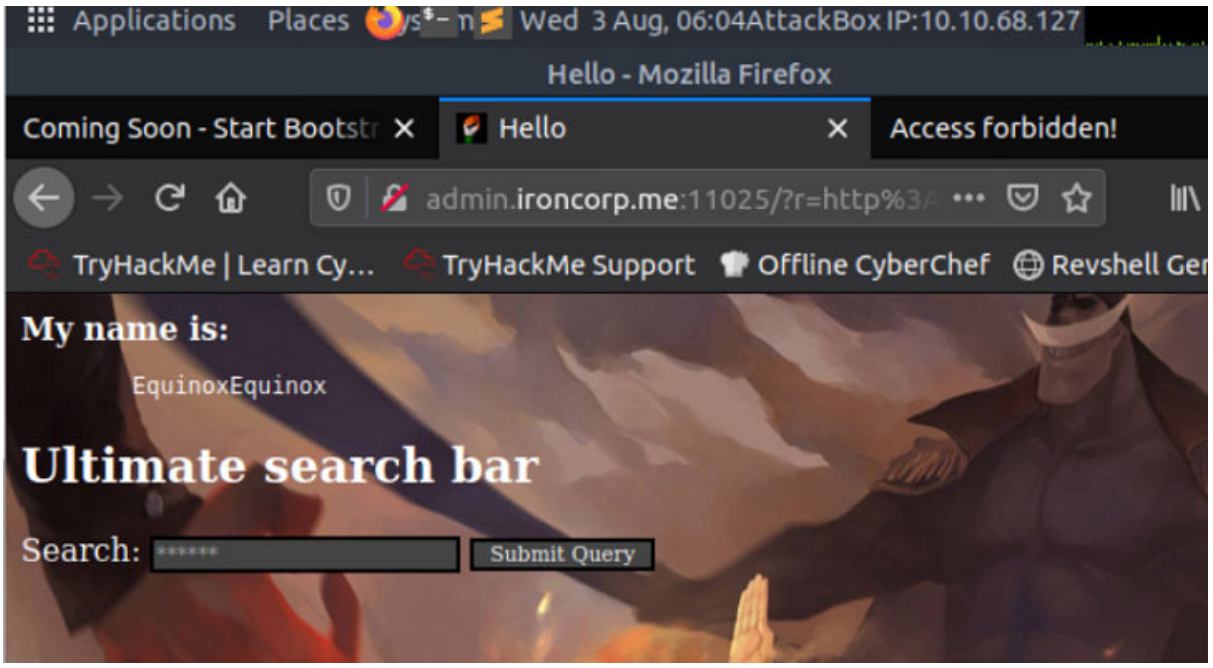
Then I put the link on the search button again.
Then its give username



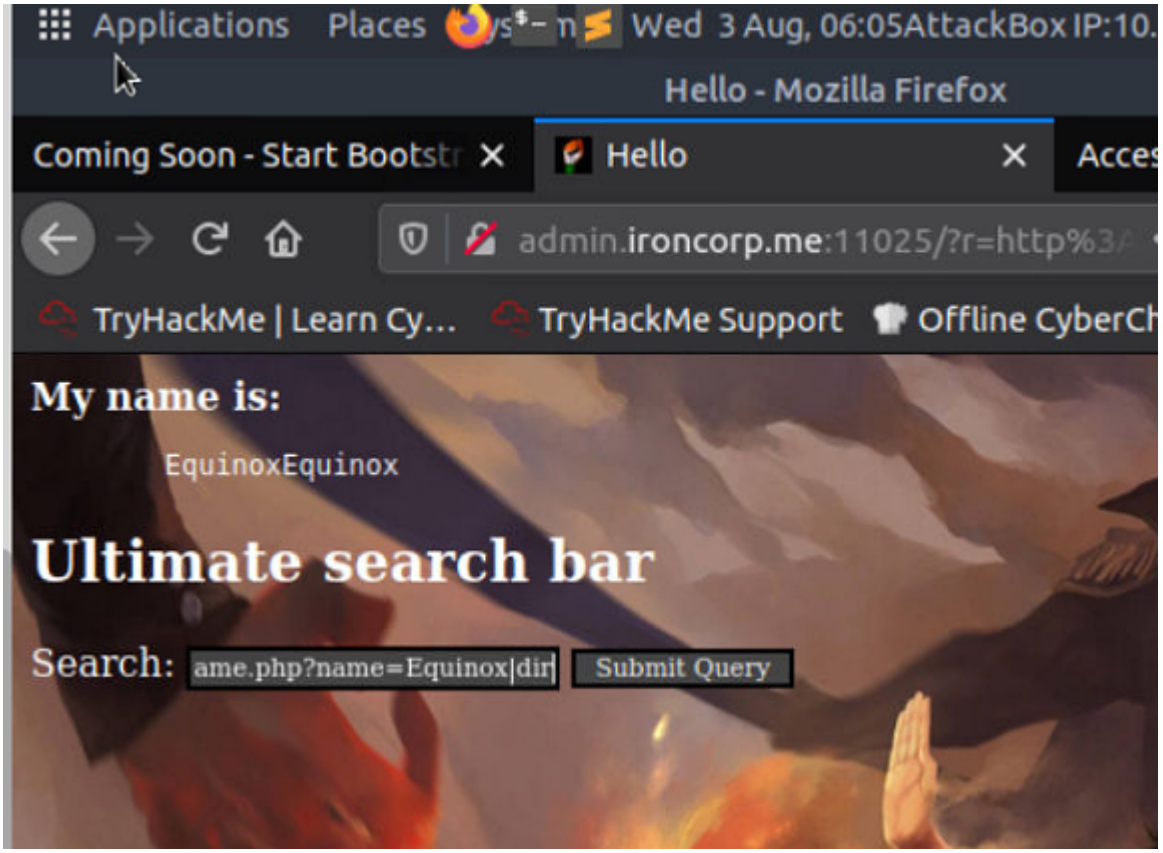
So I tried with that username and put some commands.



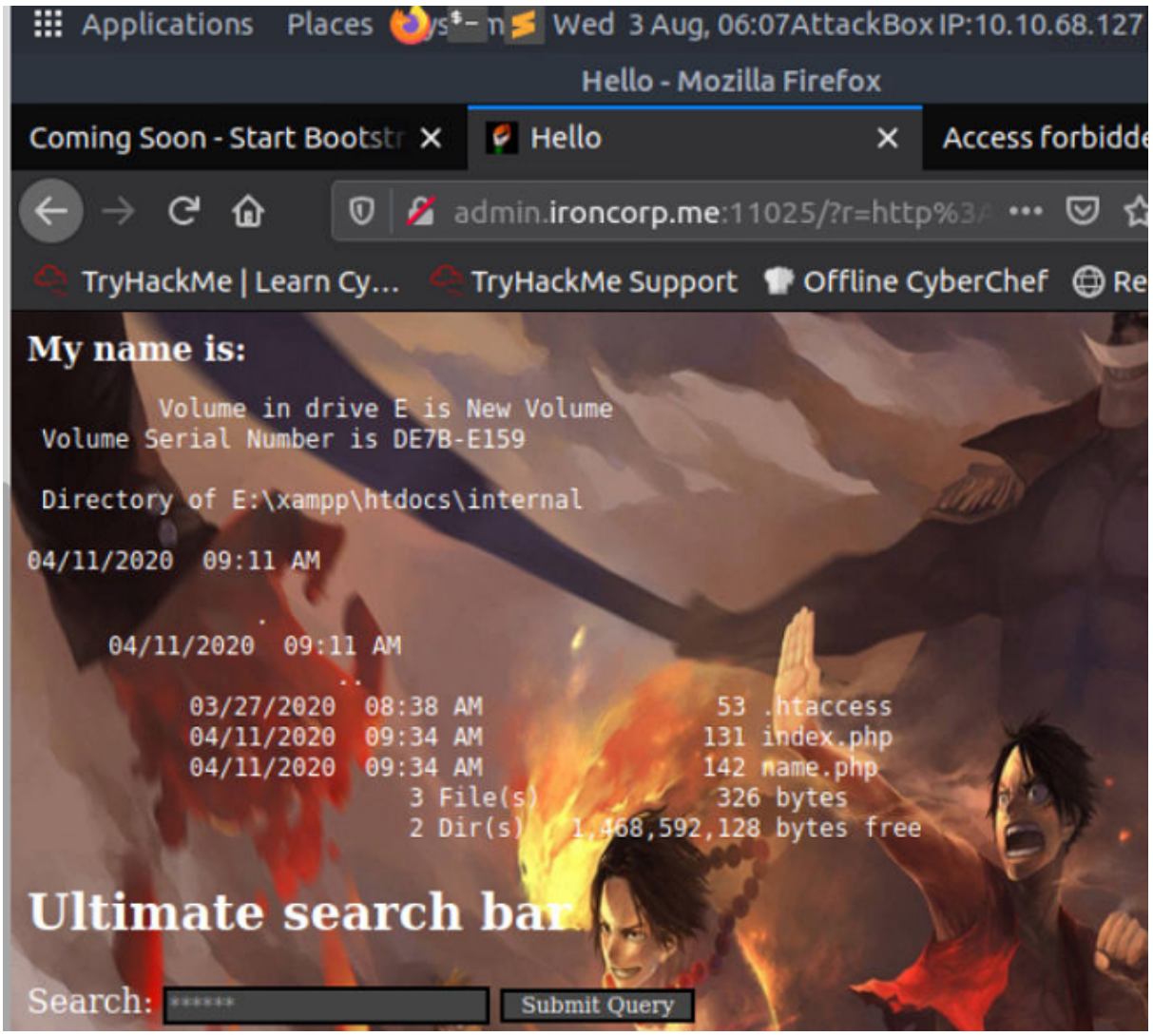
Then it gives me the username again.



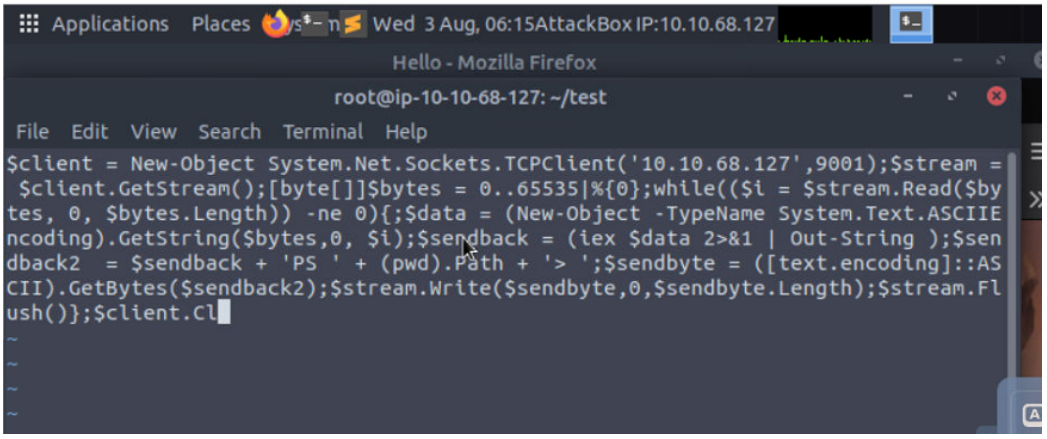
This time, I will try with the window command since its window servers. This was done during NMAP services.



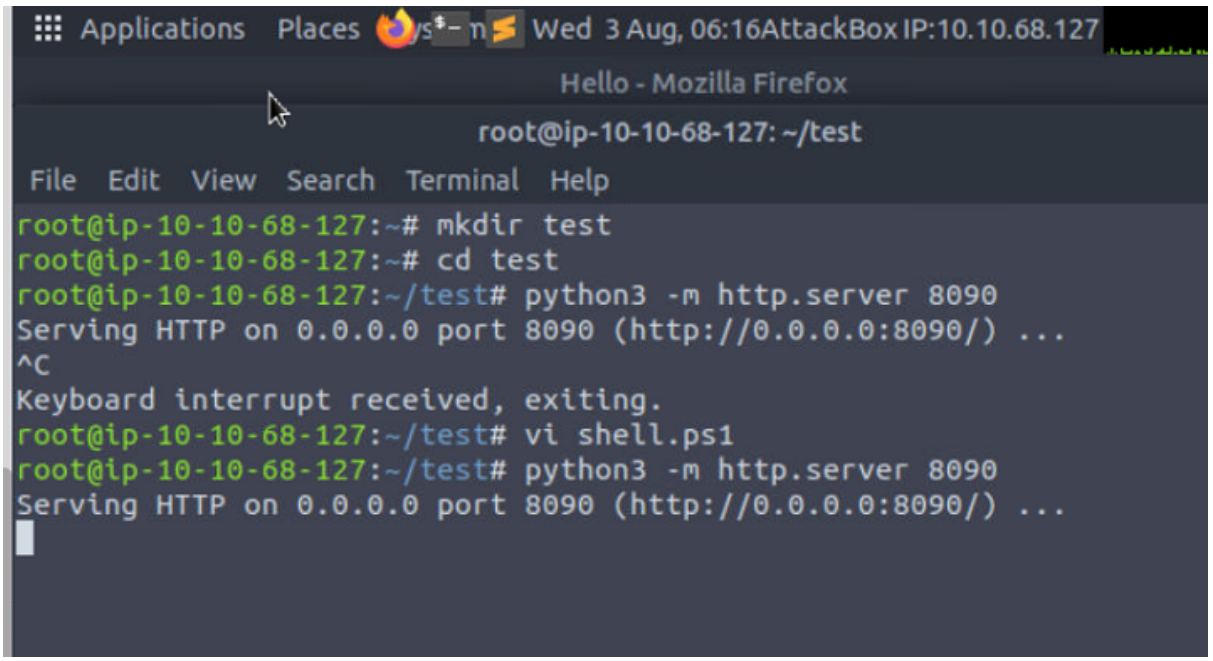
Then I can view the response for the command. So i understand with that URL search button, i can do some command



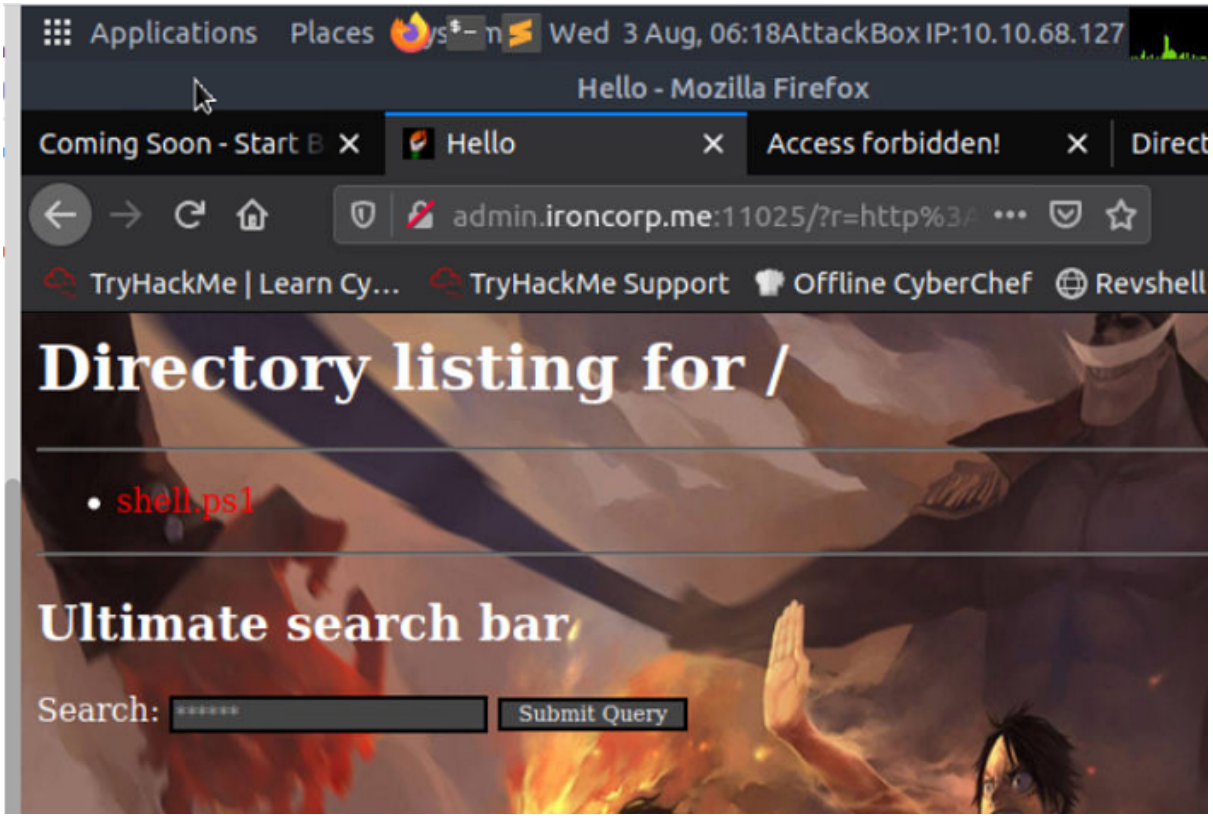
In the usual process to gain access to the server, I try inserting the reverse shell script. But since this is a windows machine, I googled for powershell script.
I managed to find the script but I need to find a way to push this script from my machine to the ironcorp machine. So I use an SSRF attack to redirect the page to my attackbox and write the file into the ironcorp machine.



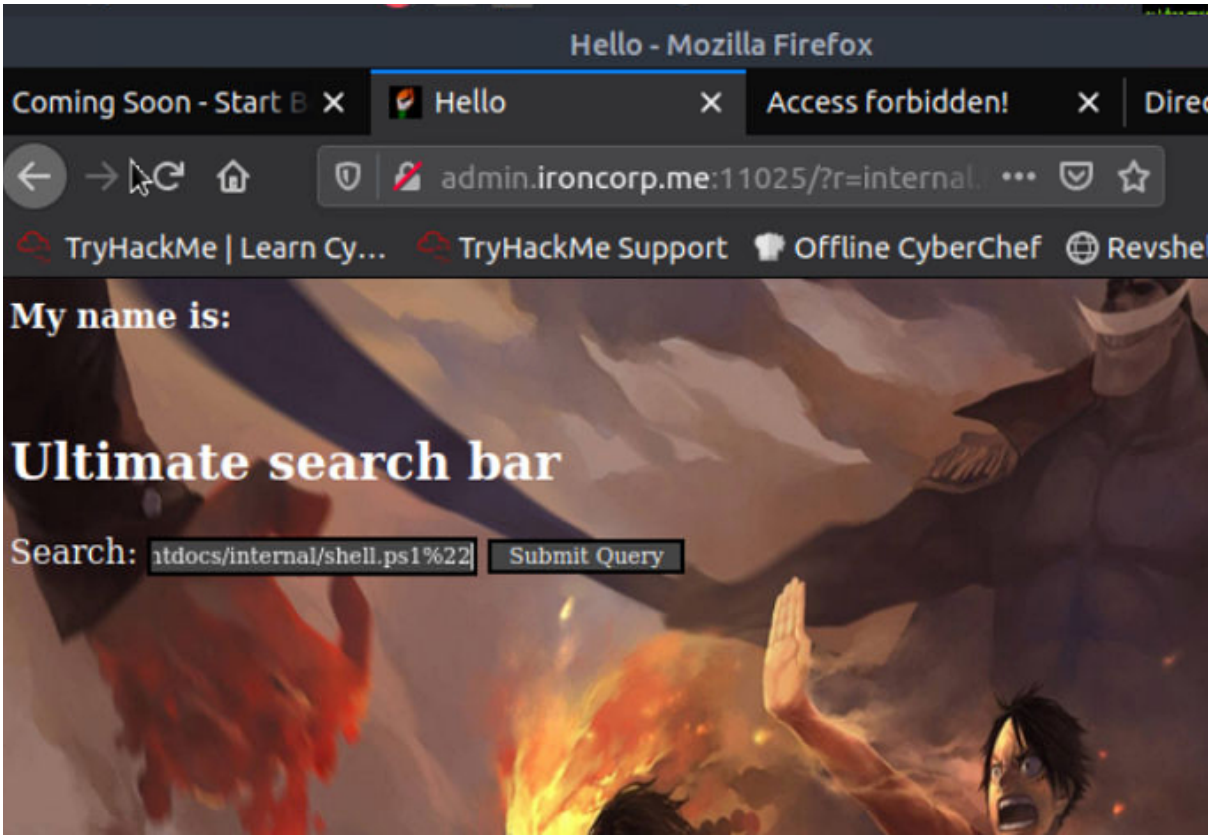
For that, I need to bring up the web server into my machine. I create a folder test and start my webservice from there.



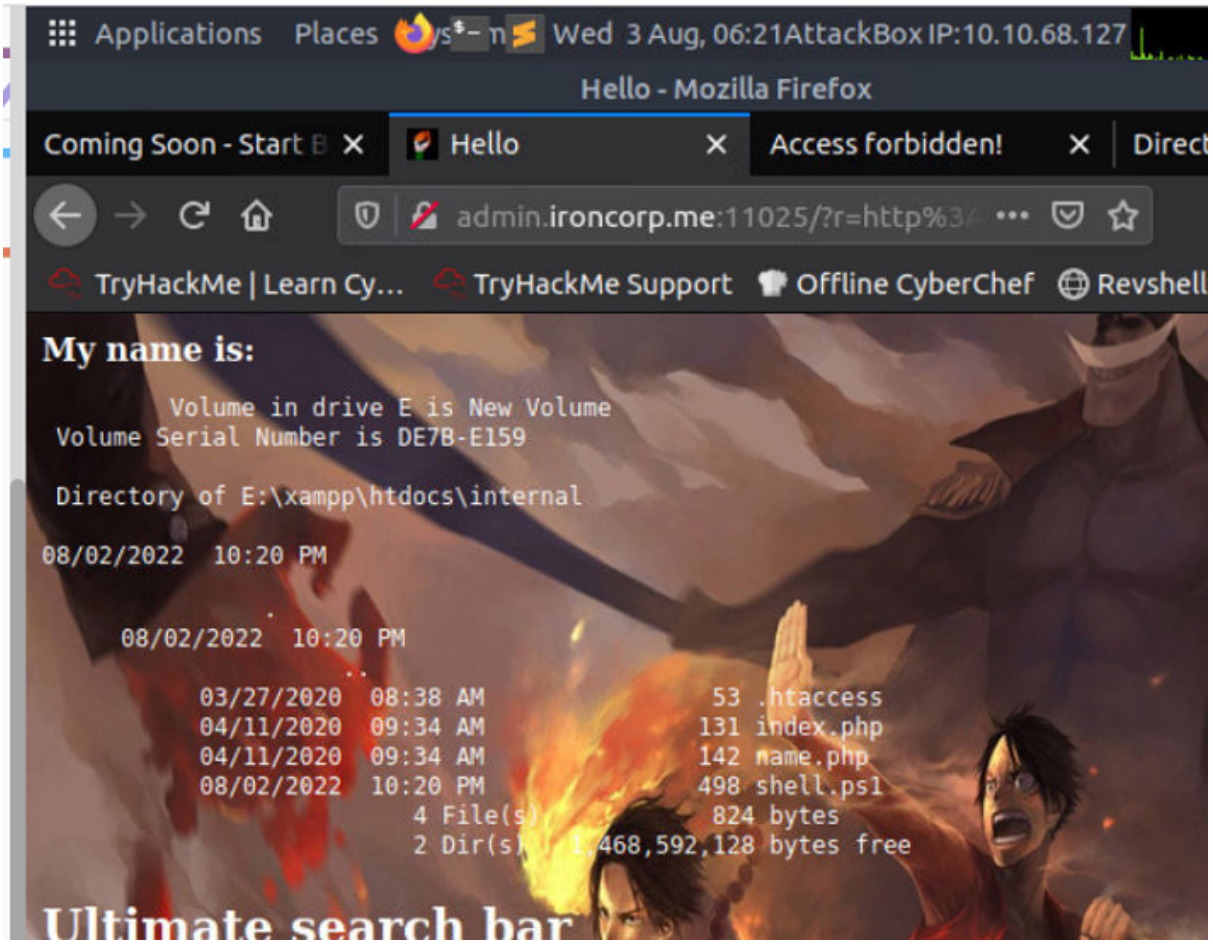
Then I make the service to the admin page redirect to my page.



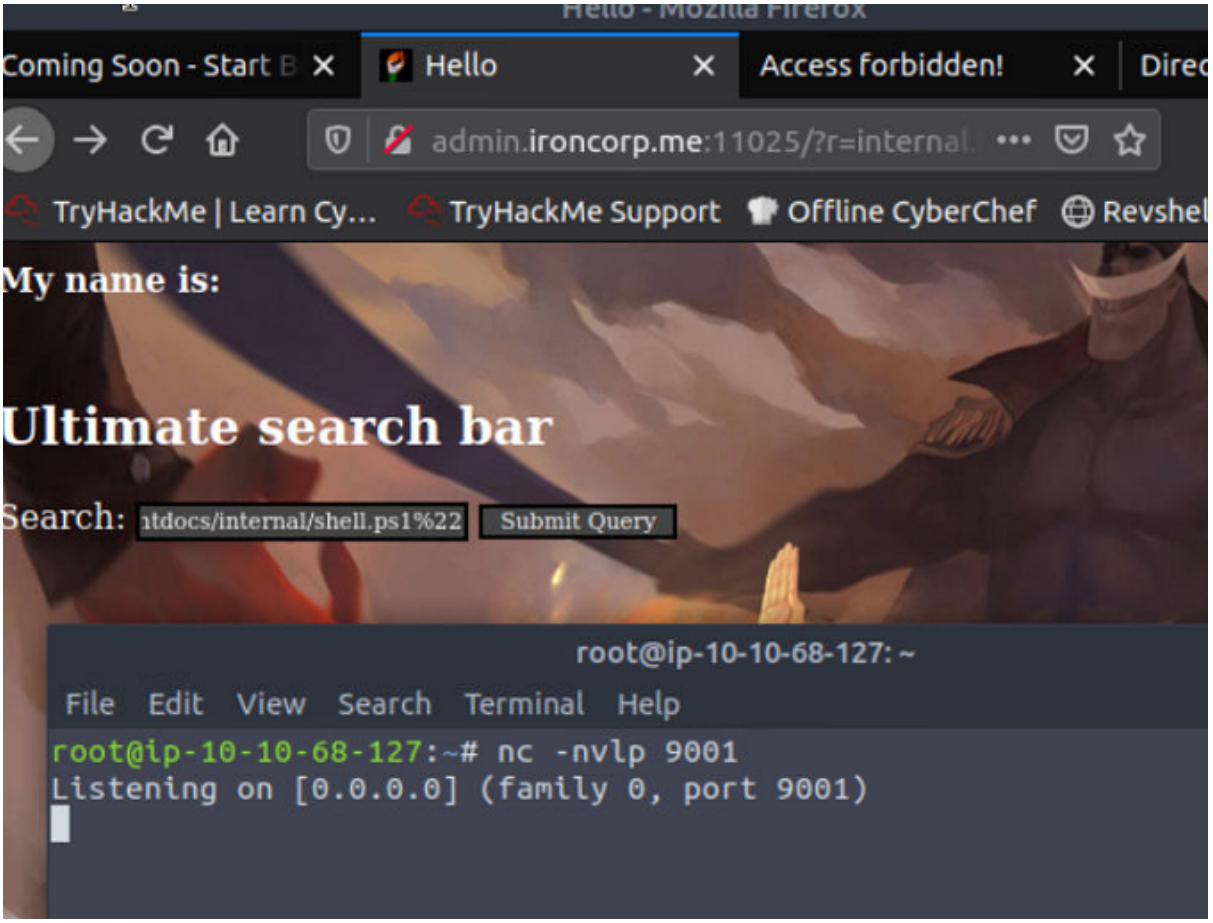
Next i need to upload this link to server



Bingo!
I was able to upload the file to the server!

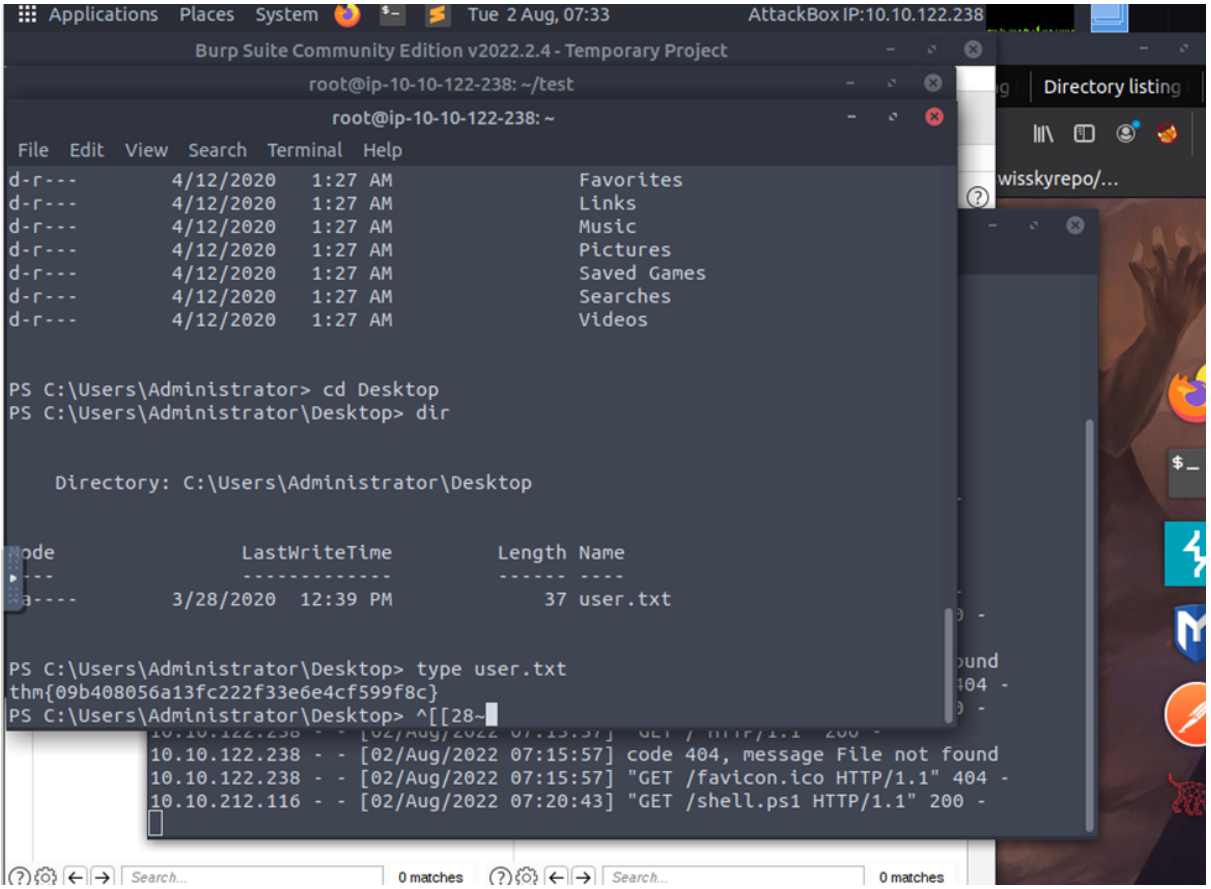


Next i need to invoke this file and i need to nc command to login to server on reverse shell.

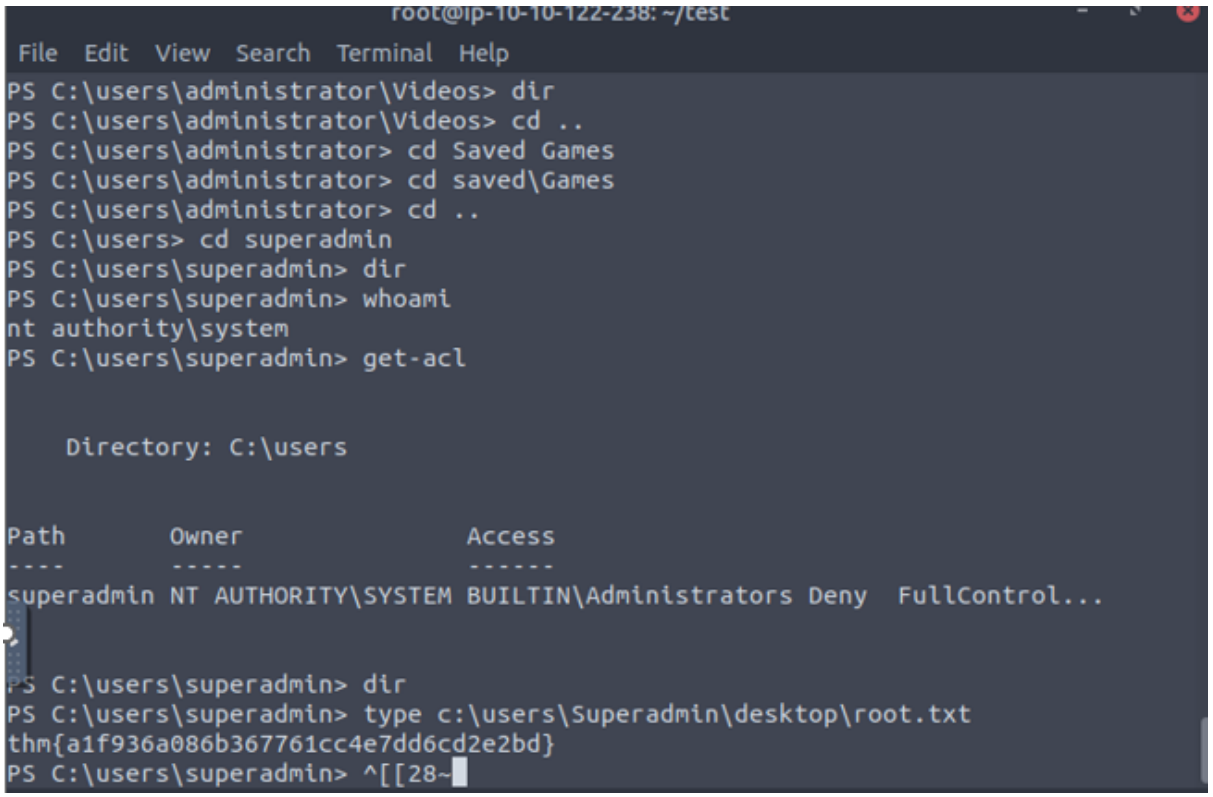


I manage to access the server and get first flag under user Administrator and its on desktop

Privilege Escalation



Then i need to check for root.txt and its hidden. After a few hours of struggle, i manage to find out the root flag as below.



CONTRIBUTION

ID	NAME	CONTRIBUTION	SIGNATURES
1211101693	Savitha Murugumunisegaran	• Launch a TCP Nmap scan • Look for the subdomain and check for username using hydra • Login and do the SSRF attack • Simulate the attack from burp suite to upload reverse shell script. • Access the server and get the flag.	*Savitha*

VIDEO LINK:
Apologies , due to time constraints and some personal issues, i am not able to do video today. The very detailed screenshot provided.