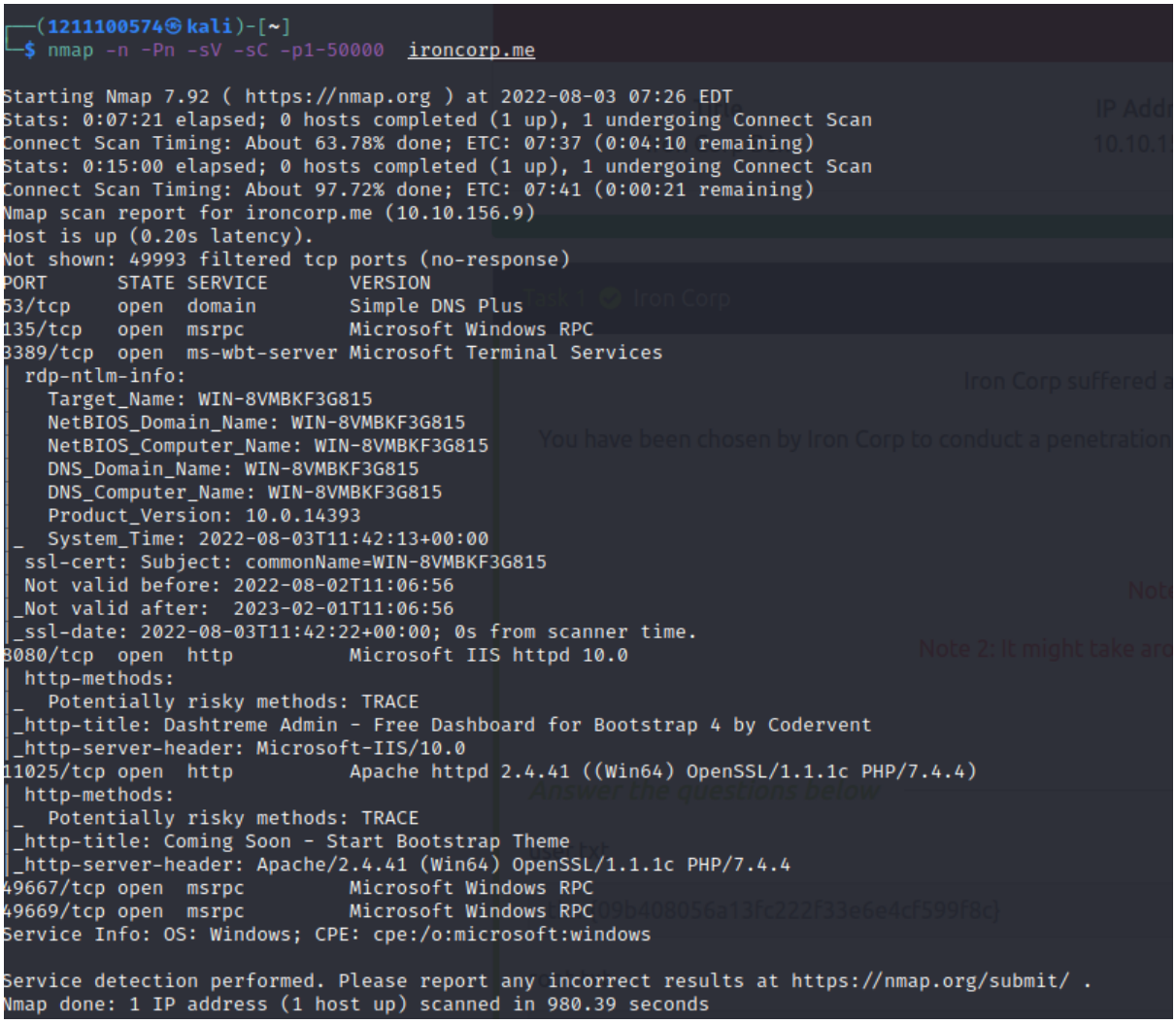
PenTest 2
Iron corp
SOLO

ID	Name	Role
1211100574	Ivan Liew Qi Hong	Leader

Tools used: Kali Linux, Firefox, Burpsuite

Thought process/methodology/attempts:

I began by running nmap to identify open ports.

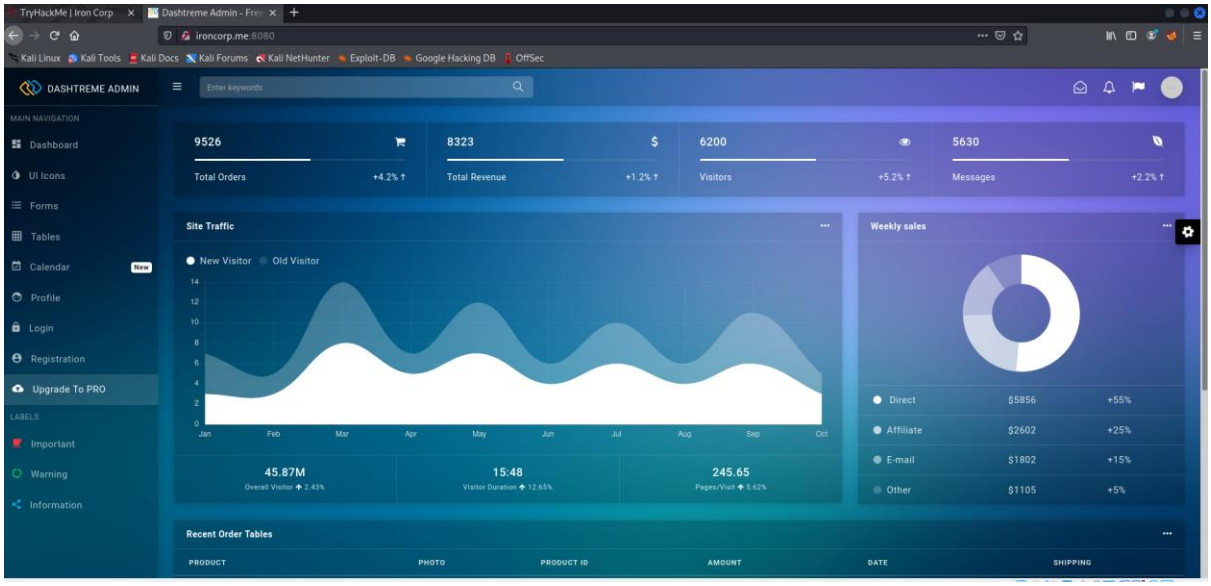


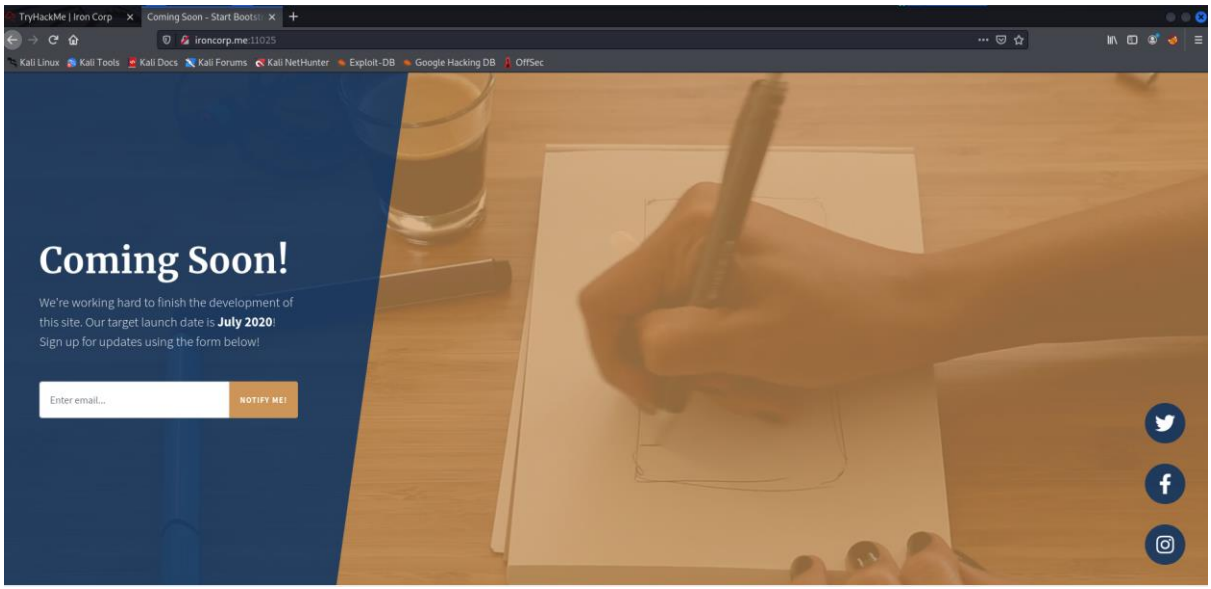
```
┌──(1211100574㉿kali)-[~]
└─$ nmap -n -Pn -sV -sC -p1-50000  ironcorp.me

Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 07:26 EDT
Stats: 0:07:21 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 63.78% done; ETC: 07:37 (0:04:10 remaining)
Stats: 0:15:00 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 97.72% done; ETC: 07:41 (0:00:21 remaining)
Nmap scan report for ironcorp.me (10.10.156.9)
Host is up (0.20s latency).
Not shown: 49993 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: 2022-08-03T11:42:13+00:00
| ssl-cert: Subject: commonName=WIN-8VMBKF3G815
| Not valid before: 2022-08-02T11:06:56
|_Not valid after:  2023-02-01T11:06:56
|_ssl-date: 2022-08-03T11:42:22+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
49669/tcp open  msrpc         Microsoft Windows RPC
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 980.39 seconds
```

I then began checking out the open ports with the ironcorp.me domain to see if anything interesting pops out.



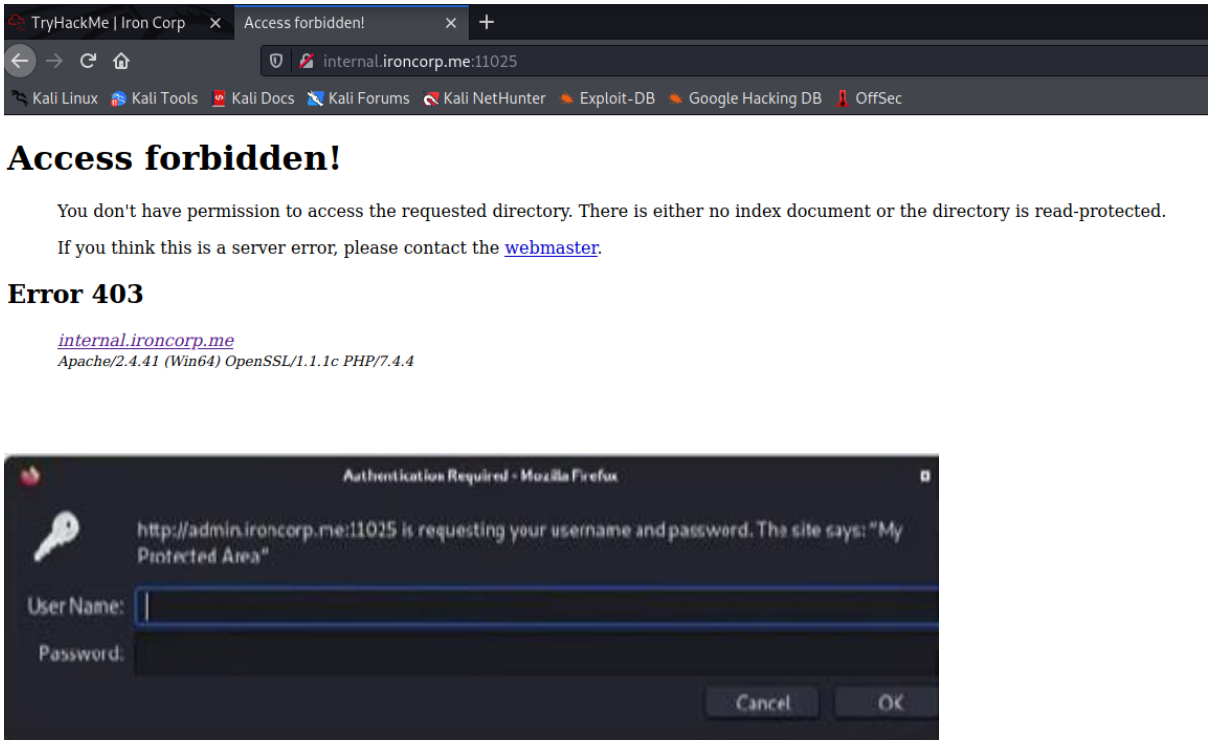


I found nothing of interest so I used the dig command to see if there are any subdomains.

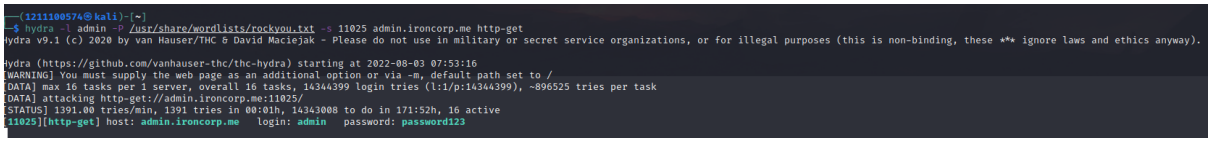
```
┌──(1211100574㉿kali)-[~]
└─$ dig @10.10.156.9 ironcorp.me axfr

; <<>> DiG 9.17.19-3-Debian <<>> @10.10.156.9 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: 216 msec
;; SERVER: 10.10.156.9#53(10.10.156.9) (TCP)
;; WHEN: Wed Aug 03 07:45:52 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

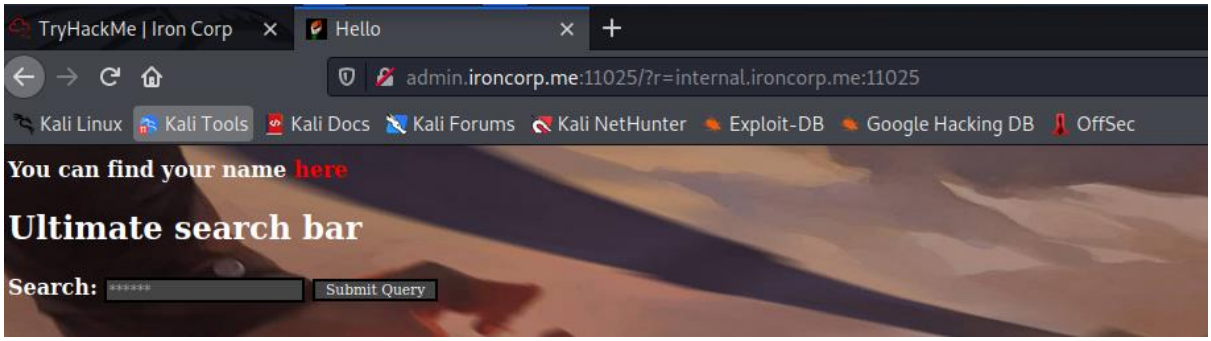
Checking out internal.ironcorp.me shows a website I can't access while checking out admin.ironcorp.me shows a username and password that is needed to enter the website.



I then decided to use hydra with a wordlist of the most common passwords to find the username and password.



I then abused the SSRF vulnerability in order to access to subdomain that I was unable to access earlier.



I then intercepted the webpage using BurpSuite and forwarded it the repeater. I then url encoded a reverse shell and injected it into the directory.I then ran powershell and listened using netcat which connected me to the directory where I navigated to the desktop directory to access

the user flag and since I’m unable to access superadmin, I just read the flag directly.

ID	Name	Contribution	Signature
1211100574	Ivan Liew Qi Hong	Recon and enumerating, establish foothold and escalated privileges to the root.	

VIDEO LINK: -