

# PenTest 2

## Iron Corp

## Cyberteam

### Members

ID	Name	Role
121110186 4	Julian Koh Chee Yong	Leader
121110360 5	Danial Ierfan Bin Hazmi	Member
121110328 1	Jievenesh Arvind Naidu A/L Uma Selvam	Member
121110378 5	Brijhendra A/L Saravanaraj	Member

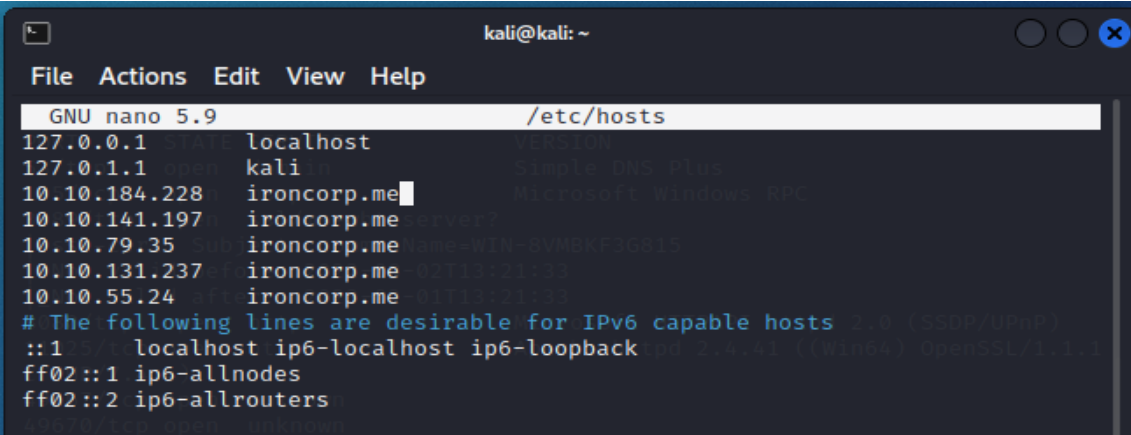
## Steps: Recon and Enumeration

**Members Involved:** Jievenesh Arvind Naidu A/L Uma Selvam

**Tools used:** Kali Linux, Nmap

## Thought Process and Methodology and Attempts:

I (Jievenesh) put in the IP address together with the website in /etc/hosts and write out to save it.

A screenshot of a terminal window on a Kali Linux system. The window title is 'kali@kali: ~'. The terminal shows the nano text editor editing the file '/etc/hosts'. The editor's menu bar includes 'File', 'Actions', 'Edit', 'View', and 'Help'. The file content lists several IP addresses mapped to 'localhost' and 'kali', followed by several IP addresses mapped to 'ironcorp.me'. The last line of the file is a comment about IPv6. The cursor is positioned at the end of the line '10.10.184.228 ironcorp.me'.

```
kali@kali: ~
File Actions Edit View Help
GNU nano 5.9 /etc/hosts
127.0.0.1 localhost
127.0.1.1 kali
10.10.184.228 ironcorp.me
10.10.141.197 ironcorp.me
10.10.79.35 ironcorp.me
10.10.131.237 ironcorp.me
10.10.55.24 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
```

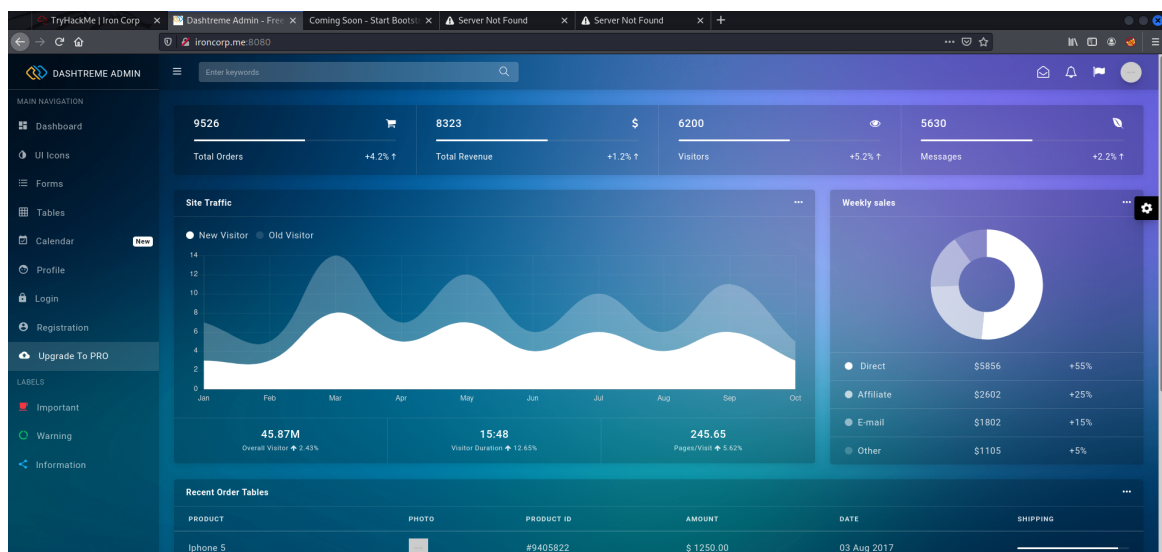
After exiting, run the nmap scan to look for open ports.

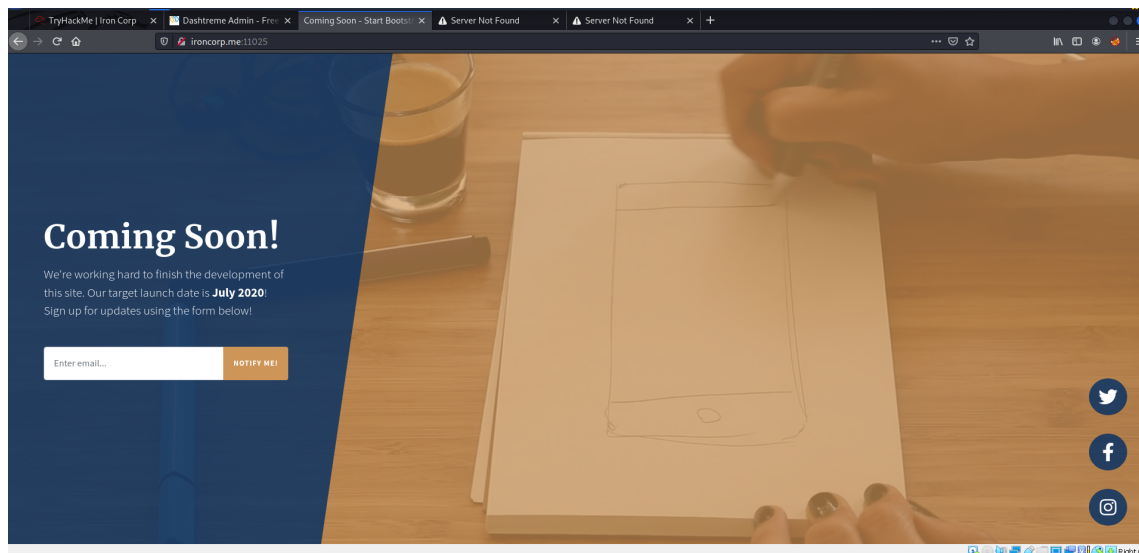
```
(kali㉿kali)-[~]
$ nmap -n -Pn -sV -sC -p53,135,3389,8080,11025,49667,49670 ironcorp.me -o ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 09:22 EDT
Nmap scan report for ironcorp.me (10.10.184.228)
Host is up (0.22s latency).
Other addresses for ironcorp.me (not scanned): 10.10.141.197 10.10.79.35 10.10.131.237 10.10.55.24

PORT      STATE SERVICE                VERSION
53/tcp    open  domain                 Simple DNS Plus
135/tcp    open  msrpc                  Microsoft Windows RPC
3389/tcp   open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=WIN-8VMBKF3G815
| Not valid before: 2022-08-02T13:21:33
|_ Not valid after: 2023-02-01T13:21:33
8080/tcp   open  http                   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
11025/tcp  open  http                   Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1c PHP/7.4.4)
49667/tcp  open  unknown
49670/tcp  open  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 182.42 seconds
```

I seen 2 open http ports which is 8080 and 11025. I took both ports and incorporated them into the website.



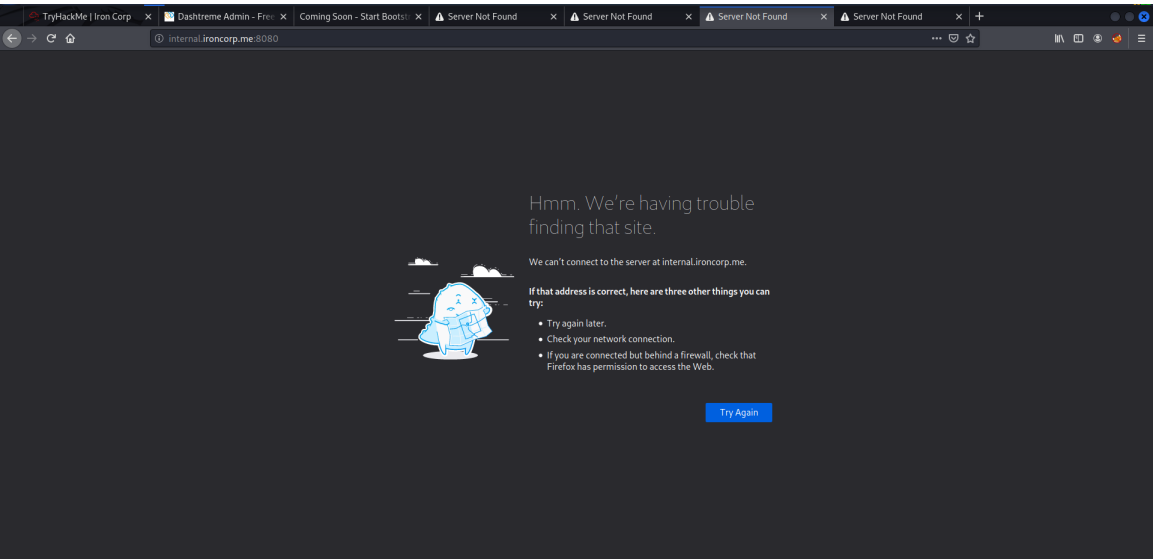
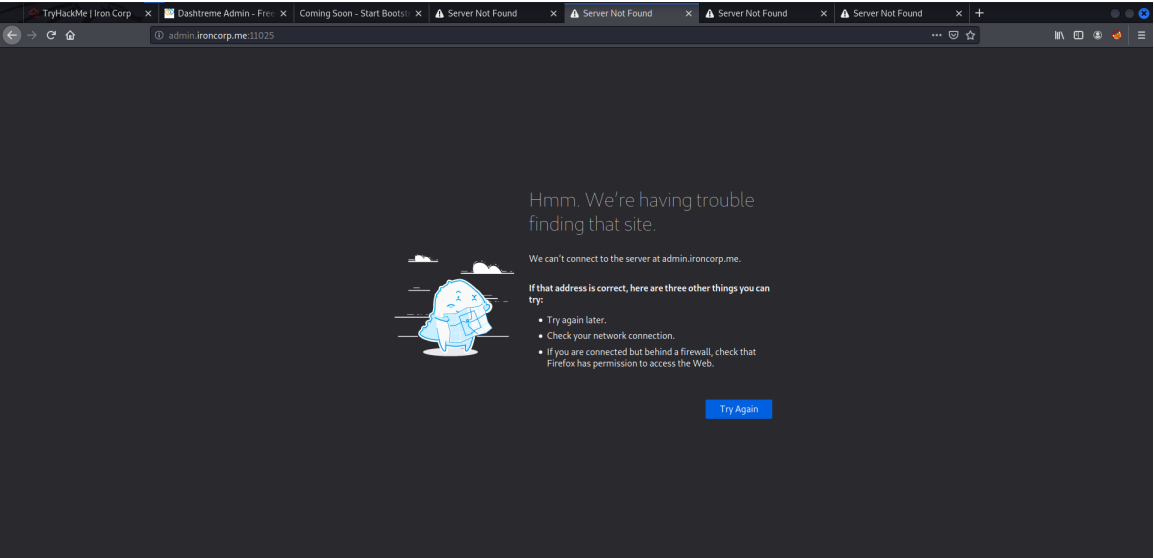
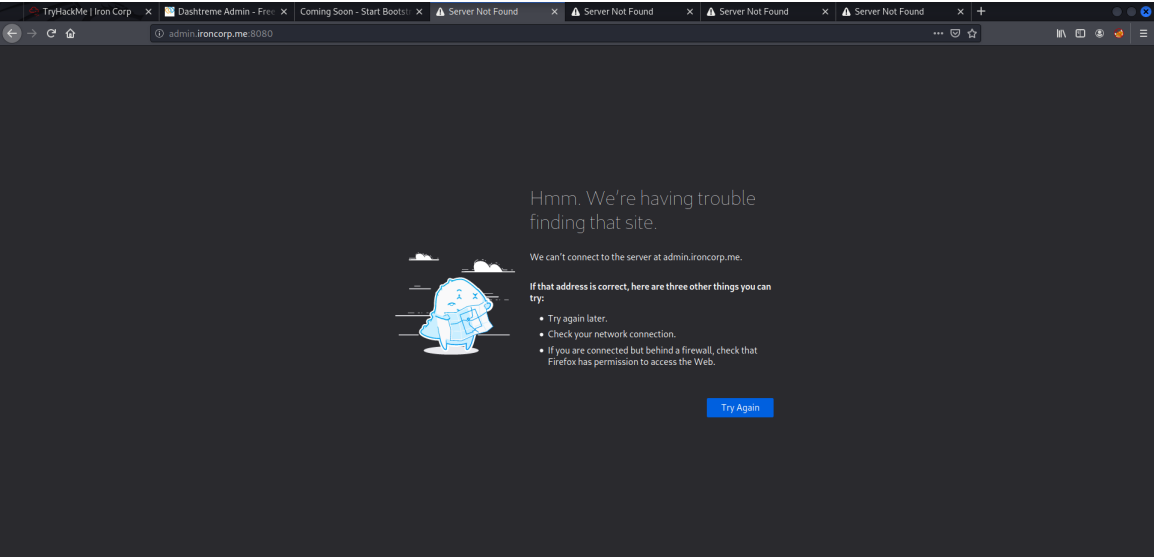


There isn't any useful information found in these 2 websites. So, I used (dig) to collect more information.

```
(kali@kali)-[~]
$ dig @10.10.184.228 ironcorp.me axfr

; <<>> DiG 9.17.19-3-Debian <<>> @10.10.184.228 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: 816 msec
;; SERVER: 10.10.184.228#53(10.10.184.228) (TCP)
;; WHEN: Wed Aug 03 09:29:47 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```


We found 2 websites running and tried opening it with both ports 8080 and 11025 but didn't load to my expectation. All websites showed "Server Not Found".



I was supposed to use only the 11025 port but tried incase it works but it still didnt. I had tried multiple times but it showed the same result. I couldnt enter the admin/internal site.

So, I did not manage to go any further and no flag was obtained.

#### Contributions

ID	Name	Contribution	Signatures
121110328 1	Jievenesh Arvind Naidu A/L Uma Selvam	Did the recon to find the ports. Did enumeration to find the accessible website.	

VIDEO LINK: <https://youtu.be/X-DHC7mPnVU>