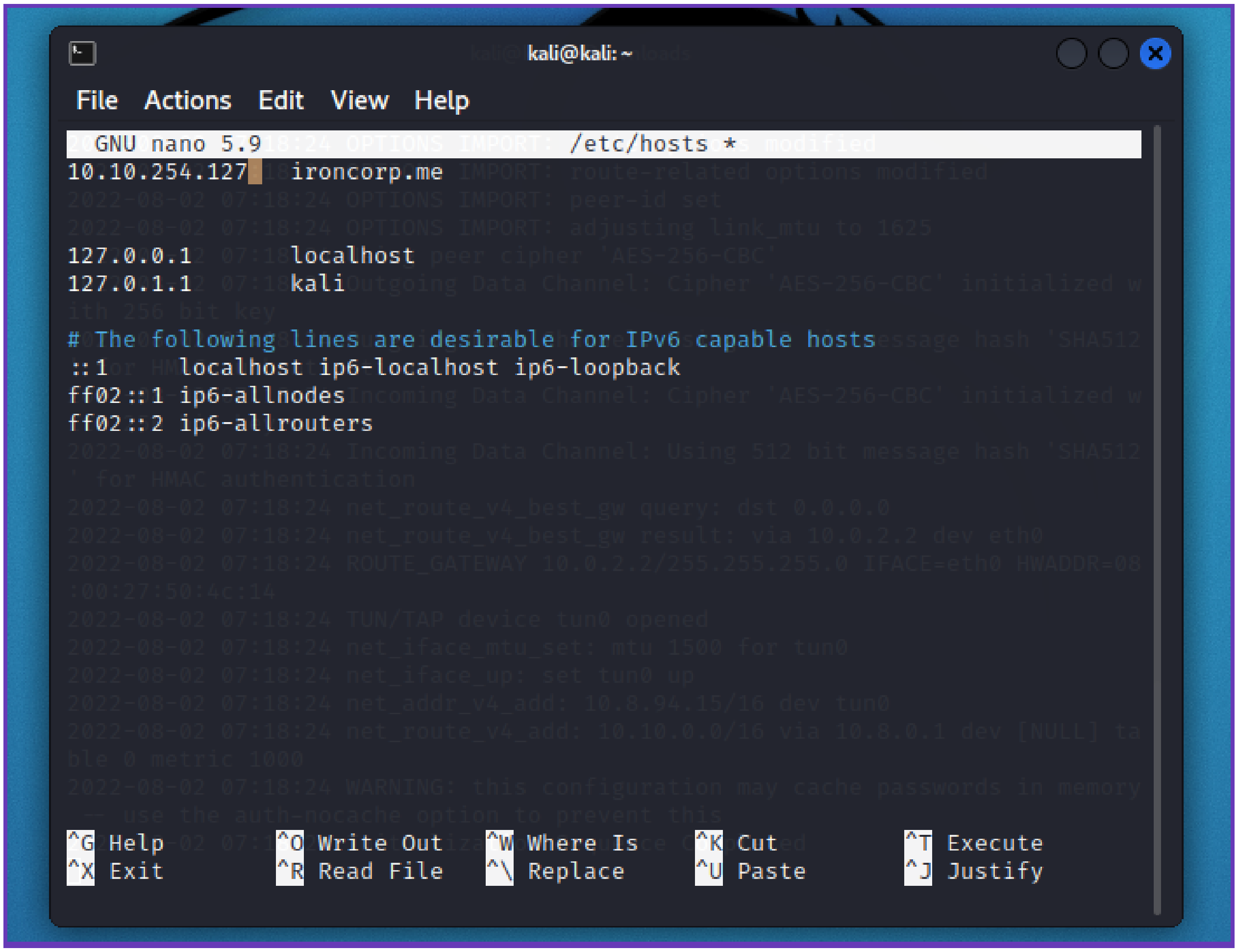
PenTest 2 Looking Glass CyberTeam

Members

ID	**Name**	**Role**
1211101864	Julian Koh Chee Yong	Leader
1211103605	Danial Ierfan Bin Hazmi	Member
1211103281	Jievenesh Arvind Naidu A/L Uma Selvam	Member
1211103785	Brijhendhra A/L Saravanaraj	Member

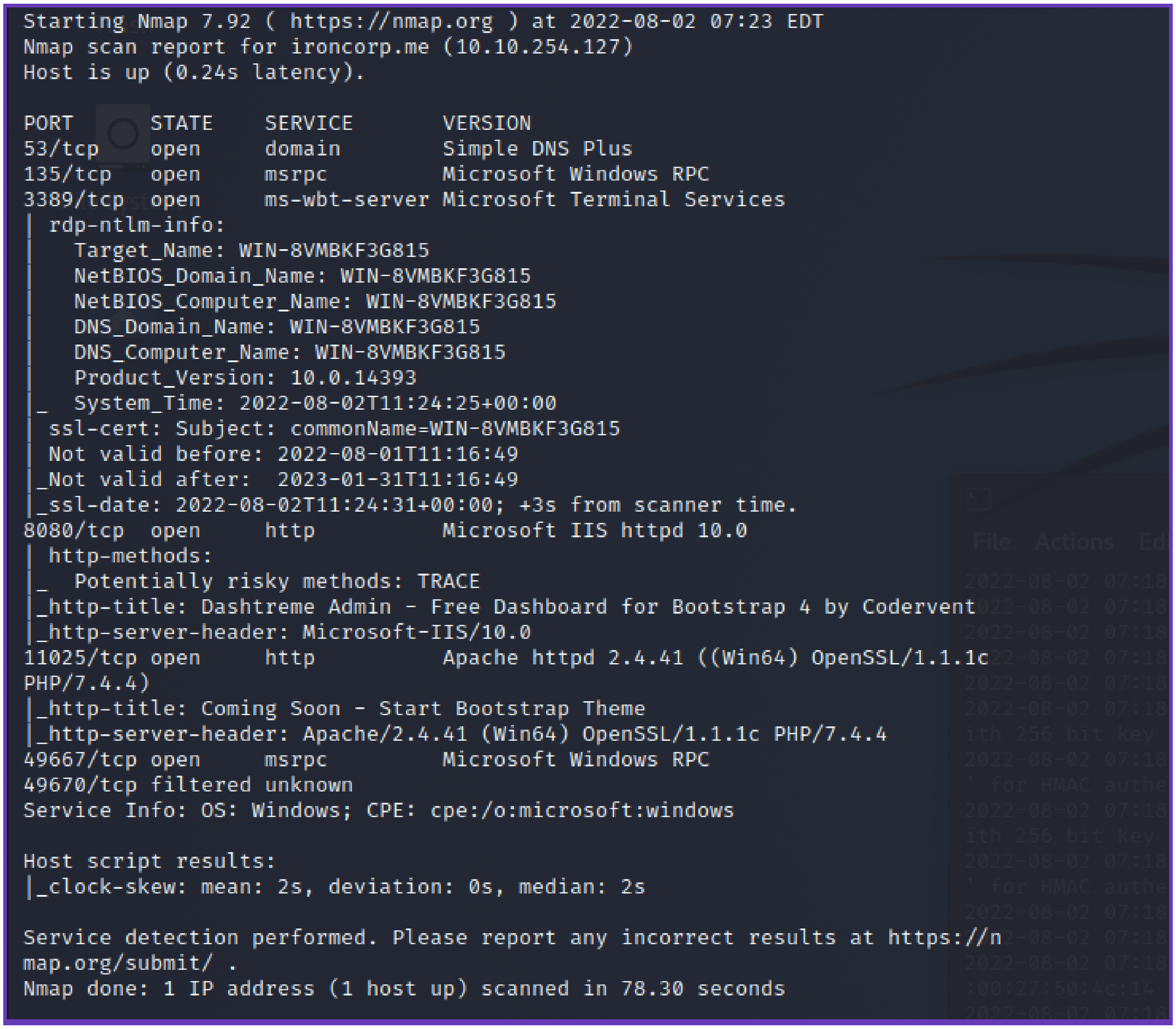
Steps: Recon and Enumeration
Members involved: Julian Koh Chee Yong
Tools used: Kali Linux, Nmap
Thought Process and Methodology and Attempts:

First, I put the IP address in “etc/hosts” file through sudo nano command



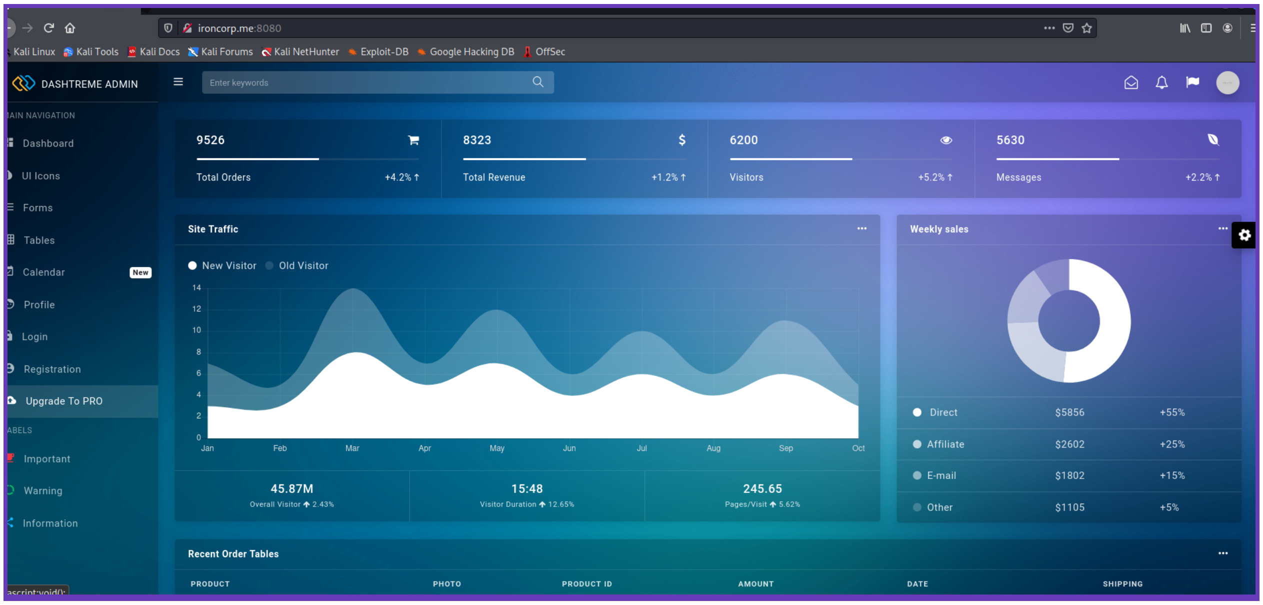
```
 GNU nano 5.9                       /etc/hosts *
10.10.254.127   ironcorp.me


127.0.0.1       localhost
127.0.1.1       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters















^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

Then execute nmap to find the open ports

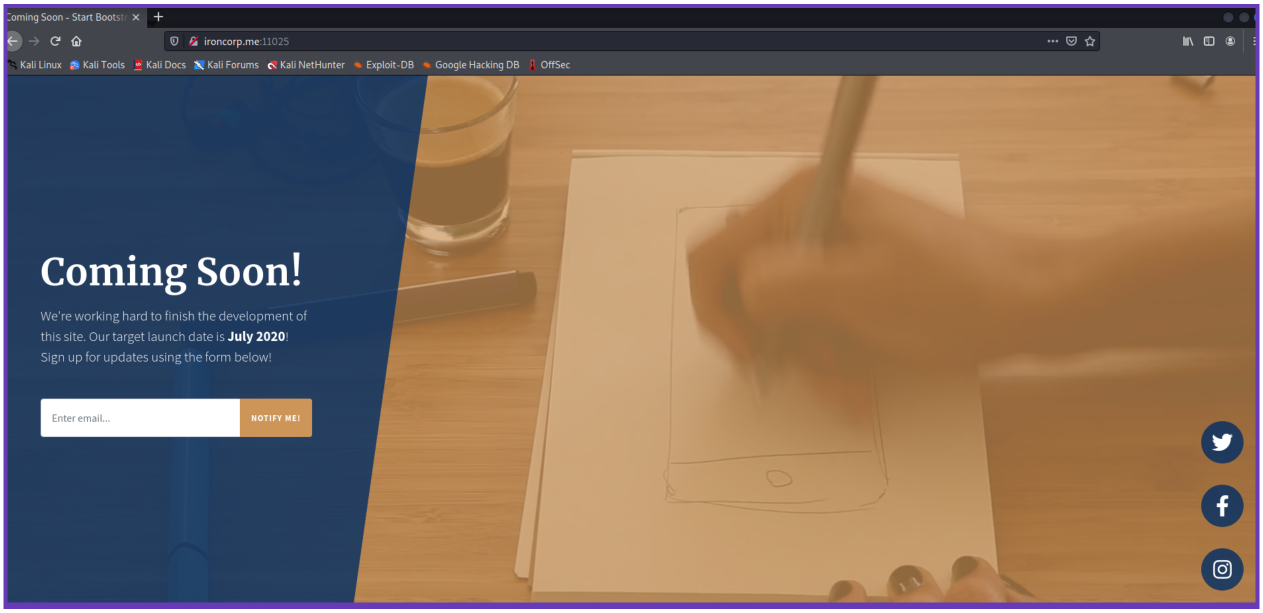


```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 07:23 EDT
Nmap scan report for ironcorp.me (10.10.254.127)
Host is up (0.24s latency).

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: 2022-08-02T11:24:25+00:00
| ssl-cert: Subject: commonName=WIN-8VMBKF3G815
| Not valid before: 2022-08-01T11:16:49
|_Not valid after:  2023-01-31T11:16:49
|_ssl-date: 2022-08-02T11:24:31+00:00; +3s 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-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

Host script results:
|_clock-skew: mean: 2s, deviation: 0s, median: 2s

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 78.30 seconds
```

Examining the website of port 8080



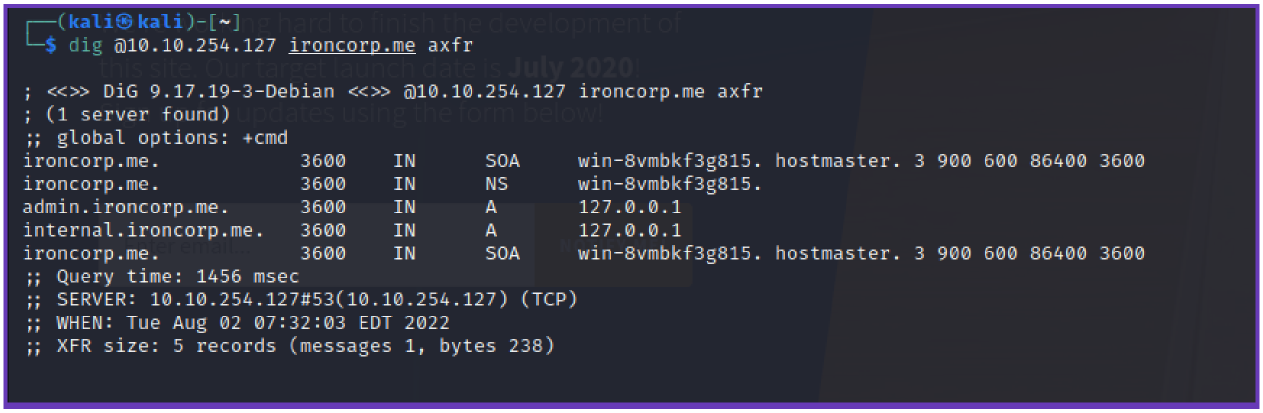
Examining port 11025



Coming Soon!

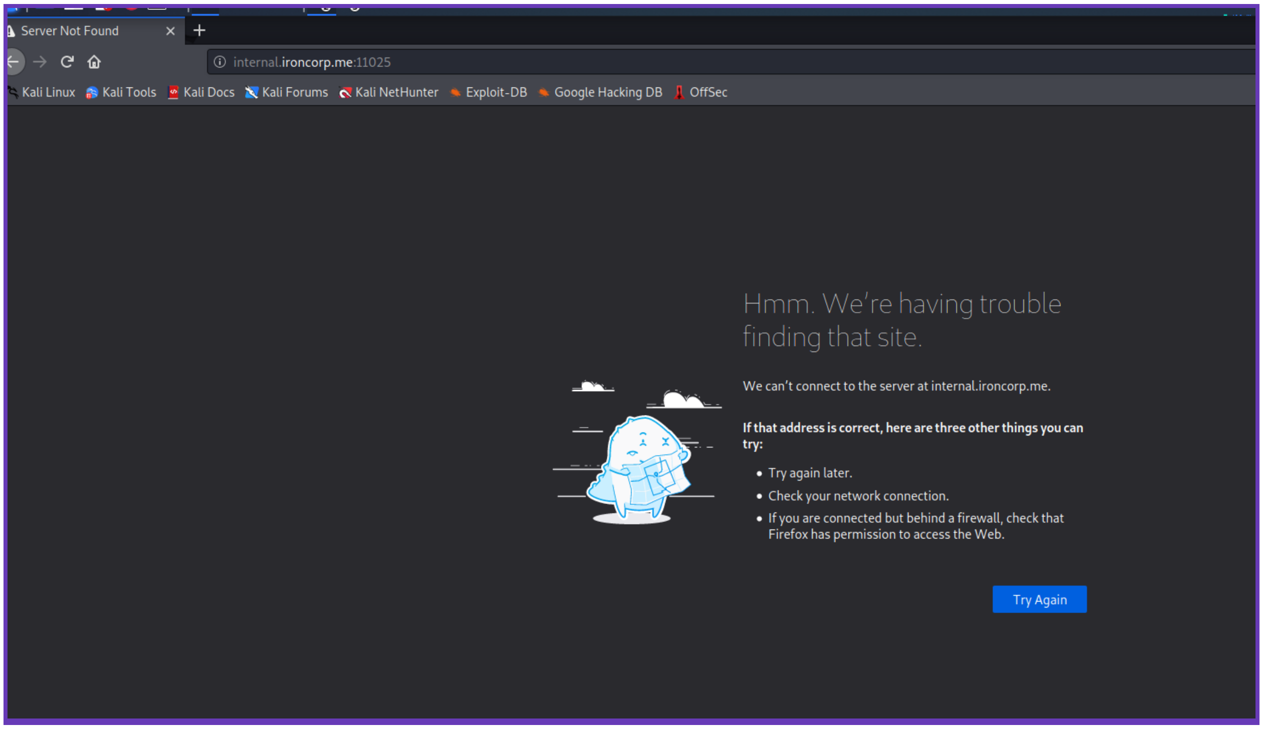
We're working hard to finish the development of this site. Our target launch date is **July 2020**! Sign up for updates using the form below!

Use dig to see if I can find any subdomain or useful information



```
┌──(kali㉿kali)-[~]
└─$ dig @10.10.254.127 ironcorp.me axfr

; <<>> DiG 9.17.19-3-Debian <<>> @10.10.254.127 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: 1456 msec
;; SERVER: 10.10.254.127#53(10.10.254.127) (TCP)
;; WHEN: Tue Aug 02 07:32:03 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

Unable to connect, maybe due to THM problems

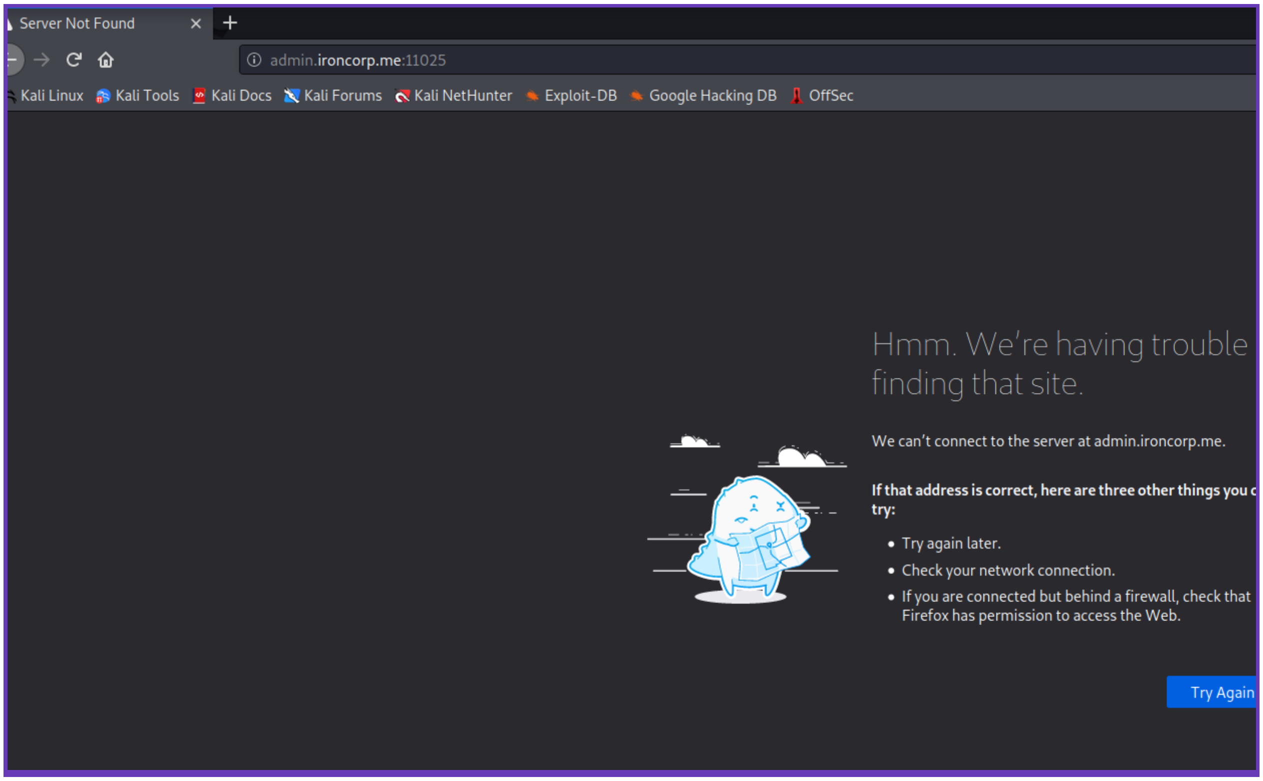


Hmm. We're having trouble finding that site.

We can't connect to the server at internal.ironcorp.me.

If that address is correct, here are three other things you can try:

- Try again later.
- Check your network connection.
- If you are connected but behind a firewall, check that Firefox has permission to access the Web.



Hmm. We're having trouble finding that site.

We can't connect to the server at admin.ironcorp.me.

If that address is correct, here are three other things you c try:

- Try again later.
- Check your network connection.
- If you are connected but behind a firewall, check that Firefox has permission to access the Web.