PenTest 2

Iron Corp

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

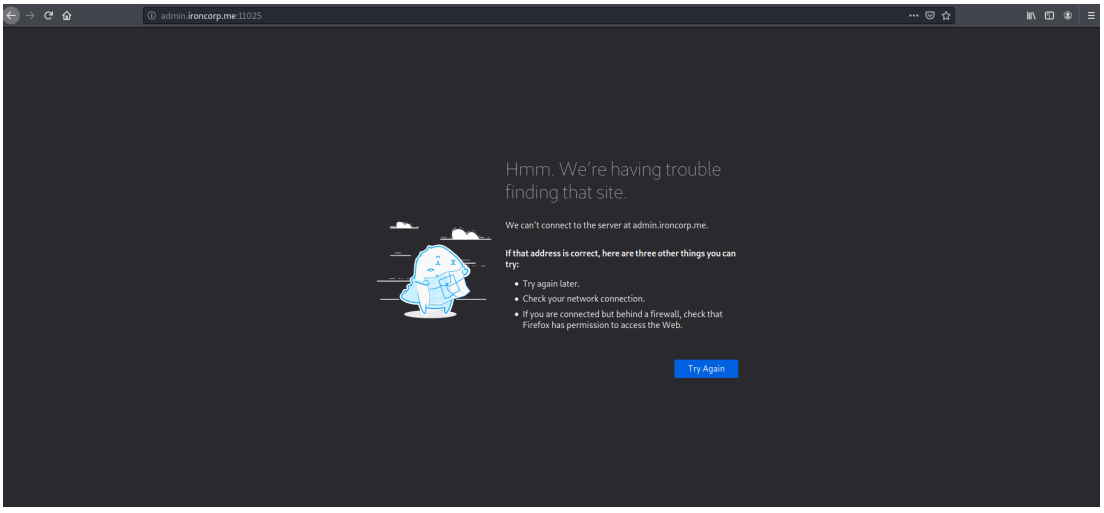
Members involved: Danial Ierfan Bin Hazmi
Tools used: Kali Linux, Nmap
Thought Process and Methodology and Attempts:

```
┌──(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 04:42 EDT
Nmap scan report for ironcorp.me (10.10.46.173)
Host is up.

PORT      STATE    SERVICE       VERSION
53/tcp    filtered domain
135/tcp   filtered msrpc
3389/tcp  filtered ms-wbt-server
8080/tcp  filtered http-proxy
11025/tcp filtered unknown
49667/tcp filtered unknown
49670/tcp filtered unknown

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.79 seconds
```

I execute Nmap scan with ironcorp.me as a reference to the IP address that was added into the file.

```
┌──(kali㉿kali)-[~]
└─$ dig ironcorp.me @10.10.7.119 axfr

; <<>> DiG 9.17.19-3-Debian <<>> ironcorp.me @10.10.7.119 axfr
;; 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: 320 msec
;; SERVER: 10.10.7.119#53(10.10.7.119) (TCP)
;; WHEN: Tue Aug 02 04:50:55 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

Then, I use DIG to obtain information from the DNS and do a zone transfer and find two new subdomains.



I try to use the subdomain but seems like the server is not working.

Contributions

ID	**Name**	Contribution	Signatures
12111 03605	Danial Ierfa Bin Hazmi	Did the recon but got stuck after trying to use the subdomain. Did the write-up.