PenTest 2

ROOM A

Potatoes & Tomatoes

Members

ID	Name	Role
1211101125	Sayid Abdur-Rahman Al-Aidarus Bin Syed Abu Bakar Mashor Al-Idrus	Leader
1211103699	Choo Qing Lam	Member
1211101237	Mohammad Zulhilman Bin Mohd Hisham	Member
1211101234	Muhammad Zahin Adri Bin Mohd Nawawi	Member

Recon and Enumeration

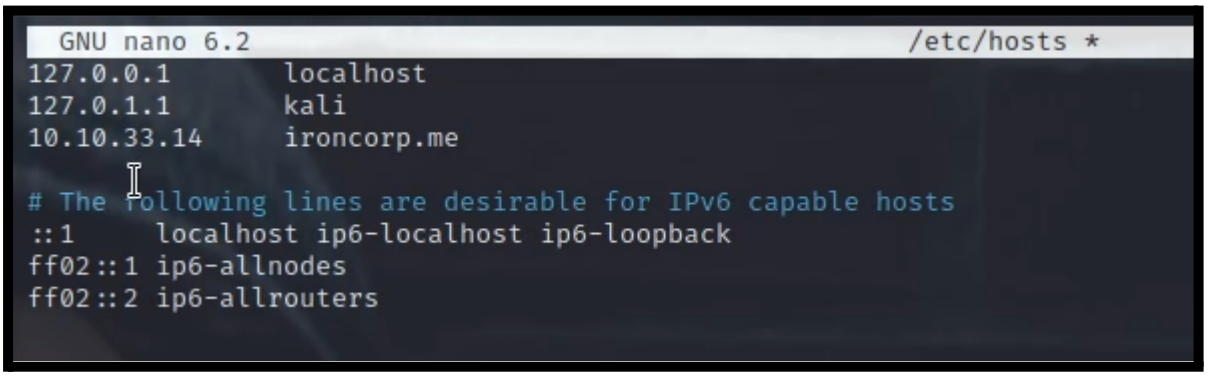
Members Involved: Sayid

Tools used: Nmap, Google, Searchsploit, Firefox, Scattered Secrets, Wireshark, FreeRDP(xfreerdp), OWASP ZAP, Ncrack, SecLists, Cyberchef, Python3

Thought Process and Methodology and Attempts:

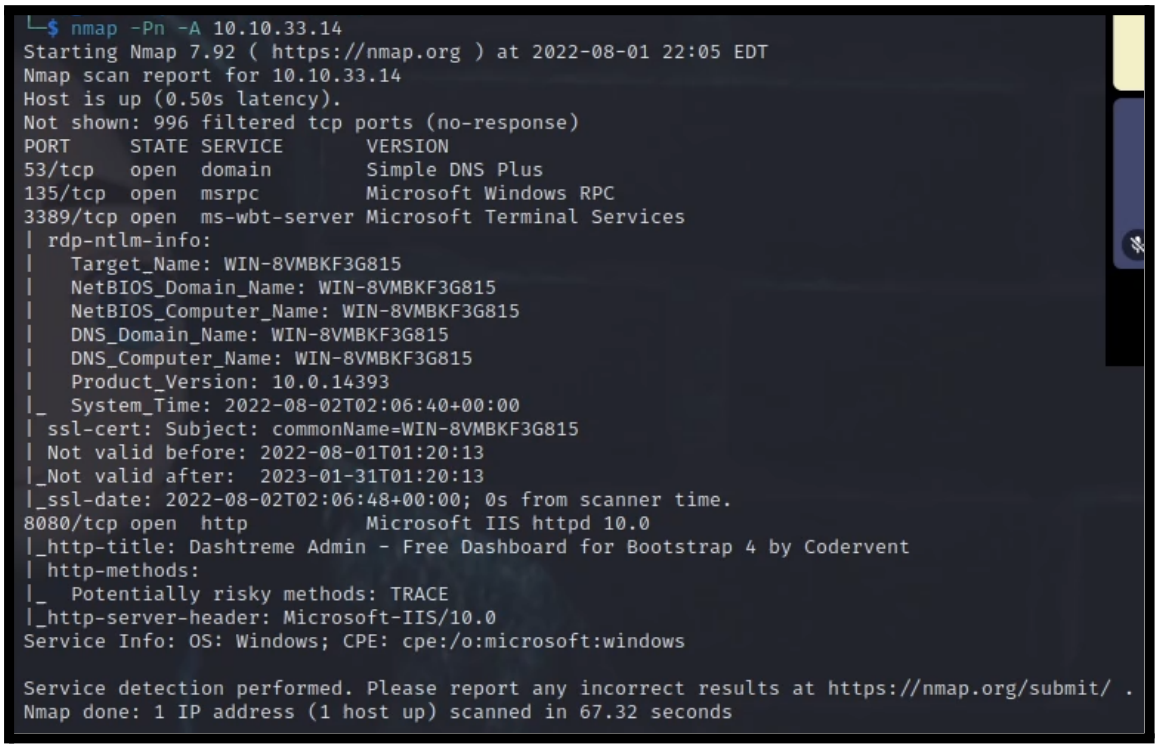
Configure /etc/hosts File

I first started by configuring my **`/etc/hosts`** file by adding the domain ironcorp.me



Initial Nmap Scan

I also did an Nmap scan. The flags used and the results are shown below.



From the scan we know that there are 4 ports open.

1. **Port 53**

This port seems to be a DNS server. We may be able to query it for domains and addresses.

```
53/tcp   open  domain        Simple DNS Plus
```

Searchsploit

I did a search using searchsploit for potentially useful exploits.

```
┌──(goldensquirrel㉿kali)-[~]
└─$ searchsploit simple dns plus
------------------------------------------------------------ ---------------------
 Exploit Title                                              |  Path
------------------------------------------------------------ ---------------------
Simple DNS Plus 5.0/4.1 - Remote Denial of Service          | windows/dos/6059.pl
------------------------------------------------------------ ---------------------
Shellcodes: No Results
Papers: No Results
```

I only found a remote DoS attack exploit which is not likely to be useful for gaining a foothold.

2. **Port 135**

After doing some googling, this port seems to belong to a service called Microsoft Remote Procedure Call which is used in client/server applications.

```
135/tcp  open  msrpc         Microsoft Windows RPC
```

Searchsploit

I also looked for exploits using searchsploit. I briefly looked through the list but was unsure if any of these exploits would be of use to me at this moment.

```
┌──(goldensquirrel㉿kali)-[~]
└─$ searchsploit msrpc
Exploits: No Results
Shellcodes: No Results
Papers: No Results
```

```
┌──(goldensquirrel㉿kali)-[~]
└─$ searchsploit microsoft windows rpc
```

Exploit Title	Path
Microsoft DNS RPC Service - 'extractQuotedChar()' Remote Overflow 'SMB' (MS07-029	windows/remote/16366.rb
Microsoft DNS RPC Service - 'extractQuotedChar()' TCP Overflow (MS07-029) (Metasp	windows/remote/16748.rb
Microsoft RPC DCOM Interface - Remote Overflow (MS03-026) (Metasploit)	windows/remote/16749.rb
Microsoft Windows - 'Lsasrv.dll' RPC Remote Buffer Overflow (MS04-011)	windows/remote/293.c
Microsoft Windows - 'RPC DCOM' Long Filename Overflow (MS03-026)	windows/remote/100.c
Microsoft Windows - 'RPC DCOM' Remote (1)	windows/remote/69.c
Microsoft Windows - 'RPC DCOM' Remote (2)	windows/remote/70.c
Microsoft Windows - 'RPC DCOM' Remote (Universal)	windows/remote/76.c
Microsoft Windows - 'RPC DCOM' Remote Buffer Overflow	windows/remote/64.c
Microsoft Windows - 'RPC DCOM' Scanner (MS03-039)	windows/remote/97.c
Microsoft Windows - 'RPC DCOM2' Remote (MS03-039)	windows/remote/103.c
Microsoft Windows - 'RPC2' Universal / Denial of Service (RPC3) (MS03-039)	windows/remote/109.c
Microsoft Windows - DCE-RPC svcctl ChangeServiceConfig2A() Memory Corruption	windows/dos/3453.py
Microsoft Windows - DCOM RPC Interface Buffer Overrun	windows/remote/22917.txt
Microsoft Windows - DNS RPC Remote Buffer Overflow (2)	windows/remote/3746.txt
Microsoft Windows - Net-NTLMv2 Reflection DCOM/RPC (Metasploit)	windows/local/45562.rb
Microsoft Windows 10 1903/1809 - RPCSS Activation Kernel Security Callback Privil	windows/local/47135.txt
Microsoft Windows 2000/NT 4 - RPC Locator Service Remote Overflow	windows/remote/5.c
Microsoft Windows 8.1 - DCOM DCE/RPC Local NTLM Reflection Privilege Escalation (	windows/local/37768.txt
Microsoft Windows Message Queuing Service - RPC Buffer Overflow (MS07-065) (1)	windows/remote/4745.cpp
Microsoft Windows Message Queuing Service - RPC Buffer Overflow (MS07-065) (2)	windows/remote/4934.c
Microsoft Windows Server 2000 - RPC DCOM Interface Denial of Service	windows/dos/61.c
Microsoft Windows Server 2000 SP4 - DNS RPC Remote Buffer Overflow	windows/remote/3737.py
Microsoft Windows XP/2000 - 'RPC DCOM' Remote (MS03-026)	windows/remote/66.c
Microsoft Windows XP/2000 - RPC Remote Non Exec Memory	windows/remote/117.c
Microsoft Windows XP/2000/NT 4.0 - RPC Service Denial of Service (1)	windows/dos/21951.c
Microsoft Windows XP/2000/NT 4.0 - RPC Service Denial of Service (2)	windows/dos/21952.c
Microsoft Windows XP/2000/NT 4.0 - RPC Service Denial of Service (3)	windows/dos/21953.txt
Microsoft Windows XP/2000/NT 4.0 - RPC Service Denial of Service (4)	windows/dos/21954.txt
Microsoft Windows XP/2003 - RPCSS Service Isolation Privilege Escalation	windows/local/32892.txt

```
Shellcodes: No Results
Papers: No Results
```

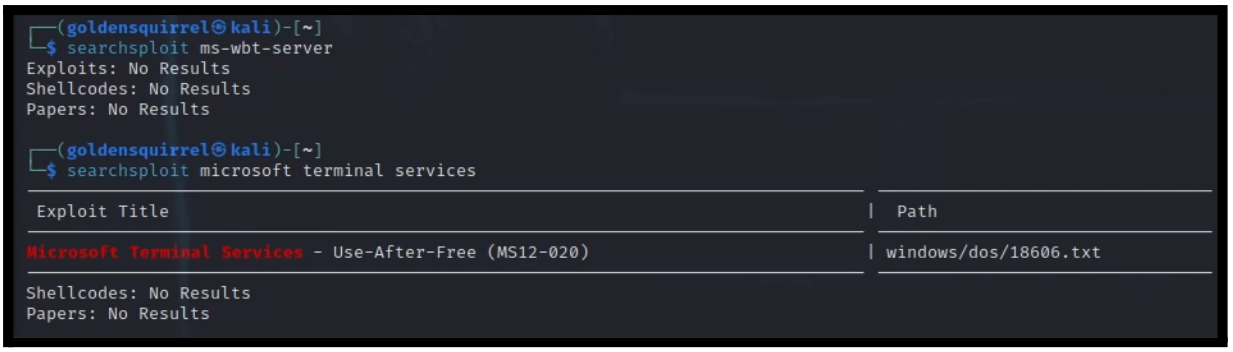
3. Port 3389

After googling Microsoft Terminal Services, it appears to be an RDP service by Microsoft. We are also able to see some of the computer's information from the nmap scan.

```
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: 2022-08-02T02:06:40+00:00
| ssl-cert: Subject: commonName=WIN-8VMBKF3G815
| Not valid before: 2022-08-01T01:20:13
|_Not valid after:  2023-01-31T01:20:13
|_ssl-date: 2022-08-02T02:06:48+00:00; 0s from scanner time.
```

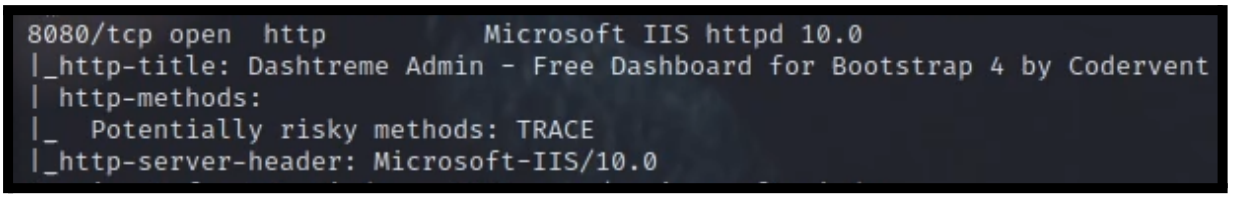
Searchsploit

I then did a search on searchsploit but did not really find anything of use here.



4. **Port 8080**

This port has a http service running. Based on the http title it seems it is an admin console.

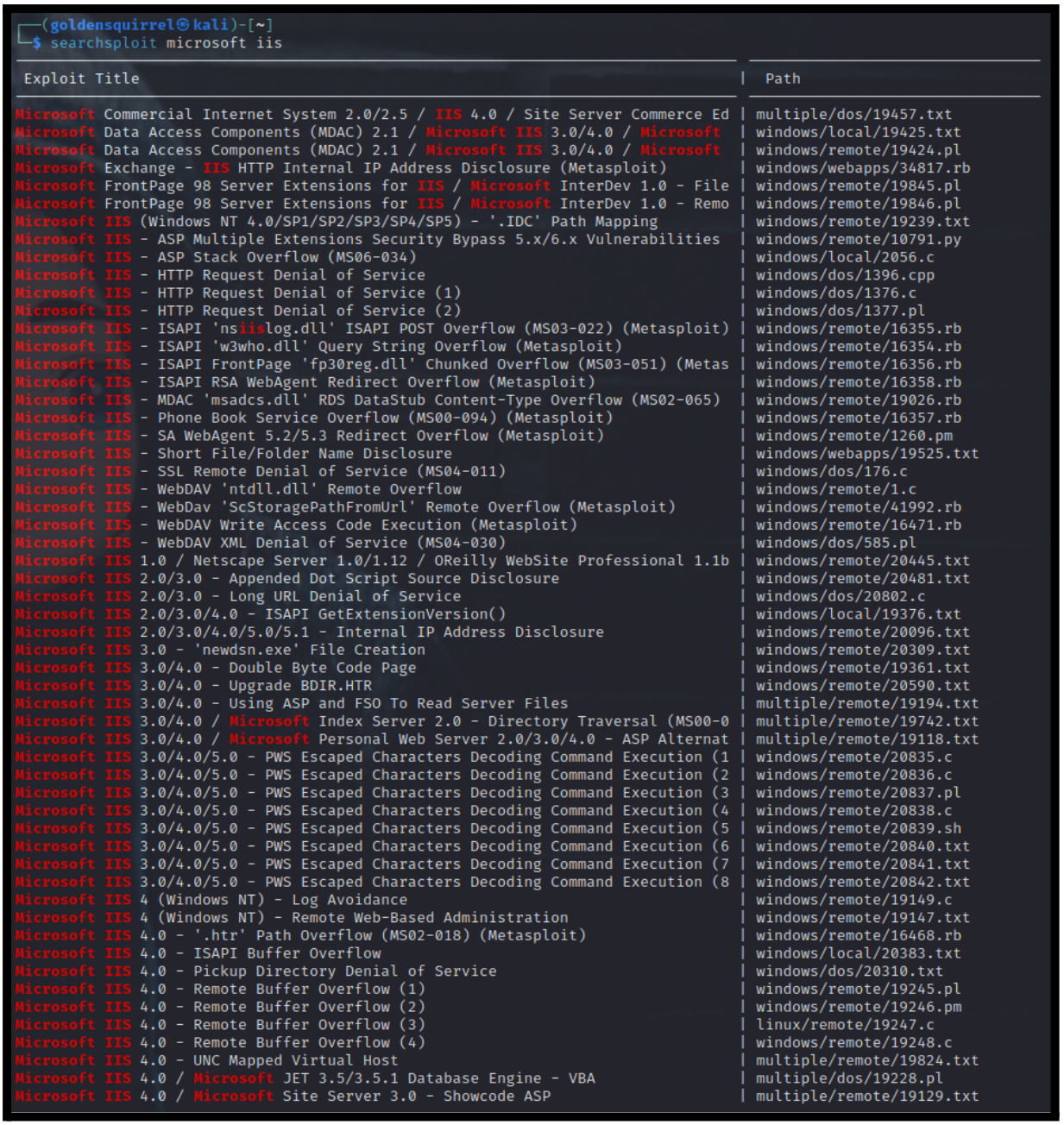


After opening the website, I confirmed that it was an admin page but it seemed like it was only a template as shown below. After looking around the page and trying some of the functions, it turns out that this website is completely a template as the buttons and interactables on the page do not do anything.

After googling the http title I found the link to the original template. When I compared the original template with this website, they seem to be carbon copies of each other.

Searchsploit

After searching on searchsploit I was unsure if any of these exploits could be used. I read through the code of some of the entries below but either did not understand it or it did not seem suited for gaining a foothold on the machine.



```
┌──(goldensquirrel㉿kali)-[~]
└─$ searchsploit microsoft iis
```

Exploit Title	Path
Microsoft Commercial Internet System 2.0/2.5 / IIS 4.0 / Site Server Commerce Ed	multiple/dos/19457.txt
Microsoft Data Access Components (MDAC) 2.1 / Microsoft IIS 3.0/4.0 / Microsoft	windows/local/19425.txt
Microsoft Data Access Components (MDAC) 2.1 / Microsoft IIS 3.0/4.0 / Microsoft	windows/remote/19424.pl
Microsoft Exchange - IIS HTTP Internal IP Address Disclosure (Metasploit)	windows/webapps/34817.rb
Microsoft FrontPage 98 Server Extensions for IIS / Microsoft InterDev 1.0 - File	windows/remote/19845.pl
Microsoft FrontPage 98 Server Extensions for IIS / Microsoft InterDev 1.0 - Remo	windows/remote/19846.pl
Microsoft IIS (Windows NT 4.0/SP1/SP2/SP3/SP4/SP5) - '.IDC' Path Mapping	windows/remote/19239.txt
Microsoft IIS - ASP Multiple Extensions Security Bypass 5.x/6.x Vulnerabilities	windows/remote/10791.py
Microsoft IIS - ASP Stack Overflow (MS06-034)	windows/local/2056.c
Microsoft IIS - HTTP Request Denial of Service	windows/dos/1396.cpp
Microsoft IIS - HTTP Request Denial of Service (1)	windows/dos/1376.c
Microsoft IIS - HTTP Request Denial of Service (2)	windows/dos/1377.pl
Microsoft IIS - ISAPI 'nsiislog.dll' ISAPI POST Overflow (MS03-022) (Metasploit)	windows/remote/16355.rb
Microsoft IIS - ISAPI 'w3who.dll' Query String Overflow (Metasploit)	windows/remote/16354.rb
Microsoft IIS - ISAPI FrontPage 'fp30reg.dll' Chunked Overflow (MS03-051) (Metas	windows/remote/16356.rb
Microsoft IIS - ISAPI RSA WebAgent Redirect Overflow (Metasploit)	windows/remote/16358.rb
Microsoft IIS - MDAC 'msadcs.dll' RDS DataStub Content-Type Overflow (MS02-065)	windows/remote/19026.rb
Microsoft IIS - Phone Book Service Overflow (MS00-094) (Metasploit)	windows/remote/16357.rb
Microsoft IIS - SA WebAgent 5.2/5.3 Redirect Overflow (Metasploit)	windows/remote/1260.pm
Microsoft IIS - Short File/Folder Name Disclosure	windows/webapps/19525.txt
Microsoft IIS - SSL Remote Denial of Service (MS04-011)	windows/dos/176.c
Microsoft IIS - WebDAV 'ntdll.dll' Remote Overflow	windows/remote/1.c
Microsoft IIS - WebDav 'ScStoragePathFromUrl' Remote Overflow (Metasploit)	windows/remote/41992.rb
Microsoft IIS - WebDAV Write Access Code Execution (Metasploit)	windows/remote/16471.rb
Microsoft IIS - WebDAV XML Denial of Service (MS04-030)	windows/dos/585.pl
Microsoft IIS 1.0 / Netscape Server 1.0/1.12 / OReilly WebSite Professional 1.1b	windows/remote/20445.txt
Microsoft IIS 2.0/3.0 - Appended Dot Script Source Disclosure	windows/remote/20481.txt
Microsoft IIS 2.0/3.0 - Long URL Denial of Service	windows/dos/20802.c
Microsoft IIS 2.0/3.0/4.0 - ISAPI GetExtensionVersion()	windows/local/19376.txt
Microsoft IIS 2.0/3.0/4.0/5.0/5.1 - Internal IP Address Disclosure	windows/remote/20096.txt
Microsoft IIS 3.0 - 'newdsn.exe' File Creation	windows/remote/20309.txt
Microsoft IIS 3.0/4.0 - Double Byte Code Page	windows/remote/19361.txt
Microsoft IIS 3.0/4.0 - Upgrade BDIR.HTR	windows/remote/20590.txt
Microsoft IIS 3.0/4.0 - Using ASP and FSO To Read Server Files	multiple/remote/19194.txt
Microsoft IIS 3.0/4.0 / Microsoft Index Server 2.0 - Directory Traversal (MS00-0	multiple/remote/19742.txt
Microsoft IIS 3.0/4.0 / Microsoft Personal Web Server 2.0/3.0/4.0 - ASP Alternat	multiple/remote/19118.txt
Microsoft IIS 3.0/4.0/5.0 - PWS Escaped Characters Decoding Command Execution (1	windows/remote/20835.c
Microsoft IIS 3.0/4.0/5.0 - PWS Escaped Characters Decoding Command Execution (2	windows/remote/20836.c
Microsoft IIS 3.0/4.0/5.0 - PWS Escaped Characters Decoding Command Execution (3	windows/remote/20837.pl
Microsoft IIS 3.0/4.0/5.0 - PWS Escaped Characters Decoding Command Execution (4	windows/remote/20838.c
Microsoft IIS 3.0/4.0/5.0 - PWS Escaped Characters Decoding Command Execution (5	windows/remote/20839.sh
Microsoft IIS 3.0/4.0/5.0 - PWS Escaped Characters Decoding Command Execution (6	windows/remote/20840.txt
Microsoft IIS 3.0/4.0/5.0 - PWS Escaped Characters Decoding Command Execution (7	windows/remote/20841.txt
Microsoft IIS 3.0/4.0/5.0 - PWS Escaped Characters Decoding Command Execution (8	windows/remote/20842.txt
Microsoft IIS 4 (Windows NT) - Log Avoidance	windows/remote/19149.c
Microsoft IIS 4 (Windows NT) - Remote Web-Based Administration	windows/remote/19147.txt
Microsoft IIS 4.0 - '.htr' Path Overflow (MS02-018) (Metasploit)	windows/remote/16468.rb
Microsoft IIS 4.0 - ISAPI Buffer Overflow	windows/local/20383.txt
Microsoft IIS 4.0 - Pickup Directory Denial of Service	windows/dos/20310.txt
Microsoft IIS 4.0 - Remote Buffer Overflow (1)	windows/remote/19245.pl
Microsoft IIS 4.0 - Remote Buffer Overflow (2)	windows/remote/19246.pm
Microsoft IIS 4.0 - Remote Buffer Overflow (3)	linux/remote/19247.c
Microsoft IIS 4.0 - Remote Buffer Overflow (4)	windows/remote/19248.c
Microsoft IIS 4.0 - UNC Mapped Virtual Host	multiple/remote/19824.txt
Microsoft IIS 4.0 / Microsoft JET 3.5/3.5.1 Database Engine - VBA	multiple/dos/19228.pl
Microsoft IIS 4.0 / Microsoft Site Server 3.0 - Showcode ASP	multiple/remote/19129.txt

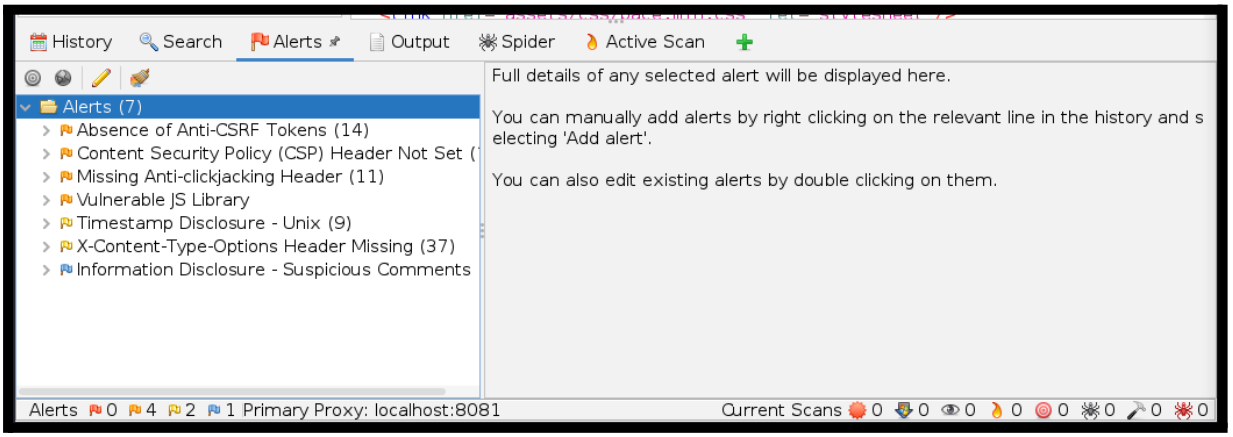
```
Microsoft IIS 4.0/5.0 - Chunked Encoding Transfer Heap Overflow (1)              | windows/remote/21368.c
Microsoft IIS 4.0/5.0 - Chunked Encoding Transfer Heap Overflow (2)              | windows/remote/21369.c
Microsoft IIS 4.0/5.0 - Chunked Encoding Transfer Heap Overflow (3)              | windows/remote/21370.c
Microsoft IIS 4.0/5.0 - Chunked Encoding Transfer Heap Overflow (4)              | windows/remote/21371.c
Microsoft IIS 4.0/5.0 - Device File Local Denial of Service                      | windows/dos/20989.txt
Microsoft IIS 4.0/5.0 - Device File Remote Denial of Service                     | windows/dos/20991.txt
Microsoft IIS 4.0/5.0 - Executable File Parsing                                  | windows/remote/20384.txt
Microsoft IIS 4.0/5.0 - FTP Denial of Service (MS01-026)                         | windows/dos/20846.pl
Microsoft IIS 4.0/5.0 - HTTP Error Page Cross-Site Scripting                     | windows/remote/21372.txt
Microsoft IIS 4.0/5.0 - Malformed File Extension Denial of Service               | windows/dos/19907.txt
Microsoft IIS 4.0/5.0 - Malformed Filename Request                               | windows/remote/19908.txt
Microsoft IIS 4.0/5.0 - SMTP Service Encapsulated SMTP Address (MS99-027)        | windows/remote/21613.txt
Microsoft IIS 4.0/5.0 - Source Fragment Disclosure                               | windows/remote/20089.txt
Microsoft IIS 4.0/5.0 - SSI Buffer Overrun Privilege Escalation                  | windows/local/21071.c
Microsoft IIS 4.0/5.0 and PWS - Extended Unicode Directory Traversal (1)         | windows/remote/20298.c
Microsoft IIS 4.0/5.0 and PWS - Extended Unicode Directory Traversal (2)         | windows/remote/20299.pl
Microsoft IIS 4.0/5.0 and PWS - Extended Unicode Directory Traversal (3)         | windows/remote/20300.c
Microsoft IIS 4.0/5.0 and PWS - Extended Unicode Directory Traversal (4)         | windows/remote/20301.php
Microsoft IIS 4.0/5.0 and PWS - Extended Unicode Directory Traversal (5)         | windows/remote/20302.pl
Microsoft IIS 4.0/5.0 and PWS - Extended Unicode Directory Traversal (6)         | windows/remote/189.c
Microsoft IIS 4.0/5.0 and PWS - Extended Unicode Directory Traversal (7)         | windows/remote/191.pl
Microsoft IIS 4.0/5.0 and PWS - Extended Unicode Directory Traversal (8)         | windows/remote/192.pl
Microsoft IIS 4.0/5.0 and PWS - Extended Unicode Directory Traversal (9)         | windows/remote/190.c
Microsoft IIS 4.0/5.0/5.1 - Authentication Method Disclosure                     | windows/remote/21313.txt
Microsoft IIS 4.0/5.0/6.0 - Internal IP Address/Internal Network Name Disclosure | windows/remote/21057.txt
Microsoft IIS 5.0 (Windows XP/2000/NT 4.0) - WebDAV 'ntdll.dll' Remote Buffer Ov | windows/remote/22365.pl
Microsoft IIS 5.0 (Windows XP/2000/NT 4.0) - WebDAV 'ntdll.dll' Remote Buffer Ov | windows/remote/22366.c
Microsoft IIS 5.0 (Windows XP/2000/NT 4.0) - WebDAV 'ntdll.dll' Remote Buffer Ov | windows/remote/22367.txt
Microsoft IIS 5.0 (Windows XP/2000/NT 4.0) - WebDAV 'ntdll.dll' Remote Buffer Ov | windows/remote/22368.txt
Microsoft IIS 5.0 - '.printer' ISAPI Extension Buffer Overflow (1)               | windows/remote/20815.pl
Microsoft IIS 5.0 - '.printer' ISAPI Extension Buffer Overflow (2)               | windows/remote/20816.c
Microsoft IIS 5.0 - '.printer' ISAPI Extension Buffer Overflow (3)               | windows/remote/20817.c
Microsoft IIS 5.0 - '.printer' ISAPI Extension Buffer Overflow (4)               | windows/remote/20818.txt
Microsoft IIS 5.0 - '500-100.asp' Server Name Spoof                              | windows/remote/1178.c
Microsoft IIS 5.0 - 'CodeBrws.asp' Source Code Disclosure                        | windows/remote/21385.txt
Microsoft IIS 5.0 - 'Translate: f' Source Disclosure (1)                         | windows/remote/20151.pl
Microsoft IIS 5.0 - 'Translate: f' Source Disclosure (2)                         | windows/remote/20152.pl
Microsoft IIS 5.0 - Authentication Bypass (MS10-065)                             | windows/remote/14179.txt
Microsoft IIS 5.0 - Failure To Log Undocumented TRACK Requests                   | windows/remote/23490.txt
Microsoft IIS 5.0 - False Content-Length Field Denial of Service                 | windows/dos/21177.txt
Microsoft IIS 5.0 - IDC Extension Cross-Site Scripting                           | windows/remote/21910.txt
Microsoft IIS 5.0 - IDQ Path Overflow (MS01-033) (Metasploit)                    | windows/remote/16472.rb
Microsoft IIS 5.0 - IISAPI Extension Enumerate Root Web Server Directory         | windows/remote/19152.txt
Microsoft IIS 5.0 - In-Process Table Privilege Escalation                        | windows/local/21072.txt
Microsoft IIS 5.0 - Indexed Directory Disclosure                                 | windows/remote/20269.txt
Microsoft IIS 5.0 - Printer Host Header Overflow (MS01-023) (Metasploit)         | windows/remote/16469.rb
Microsoft IIS 5.0 - SSL Remote Buffer Overflow (MS04-011)                        | windows/remote/275.c
Microsoft IIS 5.0 - User Existence Disclosure (1)                                | windows/remote/22562.pl
Microsoft IIS 5.0 - User Existence Disclosure (2)                                | windows/remote/22563.pl
Microsoft IIS 5.0 - WebDAV 'ntdll.dll' Path Overflow (MS03-007) (Metasploit)     | windows/remote/16470.rb
Microsoft IIS 5.0 - WebDAV Denial of Service                                     | windows/dos/20664.pl
Microsoft IIS 5.0 - WebDAV Lock Method Memory Leak Denial of Service             | windows/dos/20854.txt
Microsoft IIS 5.0 - WebDAV PROPFIND / SEARCH Method Denial of Service            | windows/dos/22670.c
Microsoft IIS 5.0 - WebDAV Remote                                                | windows/remote/2.c
Microsoft IIS 5.0 - WebDAV Remote Code Execution (3) (xwdav)                     | windows/remote/51.c
Microsoft IIS 5.0 < 5.1 - Remote Denial of Service                               | windows/dos/35.c
Microsoft IIS 5.0 FTP Server (Windows 2000 SP4) - Remote Stack Overflow          | windows/remote/9559.pl
Microsoft IIS 5.0/6.0 FTP Server (Windows 2000) - Remote Stack Overflow          | windows/remote/9541.pl
Microsoft IIS 5.0/6.0 FTP Server - Stack Exhaustion Denial of Service            | windows/dos/9587.txt
Microsoft IIS 5.1 - Hit Highlighting Authentication Bypass                       | windows/remote/4016.sh
Microsoft IIS 5.1 - WebDAV HTTP Request Source Code Disclosure                   | windows/remote/26230.txt
```

```
Microsoft IIS 6.0 - '/AUX / '.aspx' Remote Denial of Service                    | windows/dos/3965.pl
Microsoft IIS 6.0 - ASP Stack Overflow Stack Exhaustion (Denial of Service) (MS1 | windows/dos/15167.txt
Microsoft IIS 6.0 - WebDAV 'ScStoragePathFromUrl' Remote Buffer Overflow        | windows/remote/41738.py
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass                         | windows/remote/8765.php
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (1)                     | windows/remote/8704.txt
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (2)                     | windows/remote/8806.pl
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (Patch)                 | windows/remote/8754.patch
Microsoft IIS 6.0/7.5 (+ PHP) - Multiple Vulnerabilities                        | windows/remote/19033.txt
Microsoft IIS 7.0 FTP Server - Stack Exhaustion Denial of Service (MS09-053) (Me | windows/dos/17476.rb
Microsoft IIS 7.5 (Windows 7) - FTPSVC Unauthorized Remote Denial of Service (Po | windows/dos/15803.py
Microsoft IIS FTP Server - NLST Response Overflow (MS09-053) (Metasploit)       | windows/remote/16740.rb
Microsoft IIS/PWS - CGI Filename Double Decode Command Execution (MS01-026) (Met | windows/remote/16467.rb
Microsoft Internet Explorer 8/9/10/11 / IIS / CScript.exe/WScript.exe VBScript - | windows/remote/40721.html
Microsoft Site Server 2.0 with IIS 4.0 - Arbitrary File Upload                  | windows/remote/20305.txt
Microsoft Windows Media Services - 'nsiislog.dll' Remote Overflow               | windows/remote/56.c
Microsoft Windows NT 4.0/2000 - Media Services 'nsiislog.dll' Remote Buffer Over | windows/remote/22837.c
---------------------------------------------------------------------------------- ----------------------------------------
Shellcodes: No Results
---------------------------------------------------------------------------------- ----------------------------------------
 Paper Title                                                                     |  Path
---------------------------------------------------------------------------------- ----------------------------------------
Microsoft IIS self decoding behavior leads to WAF Bypass/information disclosure  | english/13620-microsoft-iis-self
Microsoft IIS Tilde Character Short File/Folder Name Disclosure                  | docs/english/19527-microsoft-iis
---------------------------------------------------------------------------------- ----------------------------------------
```

Looking at the titles of the exploits, they did not seem particularly useful to me and most exploits are version numbered and did not have an exploit for version 10(the version of the Microsoft IIS running on the machine.

OWASP ZAP Automated Scan

I tried running an OWASP ZAP automated scan on the website running on port 8080 to see if there were any possible security vulnerabilities that I might have missed.



There were no high priority alerts (red flags) which typically indicate an immediate vulnerability that can be exploited. After looking through the other alerts, no exploitable items were found.

Google Dorking

Creator of the Original Website Template

I then did some google searching on the company that originally created the website template. After some googling, I found out the template was made under the company

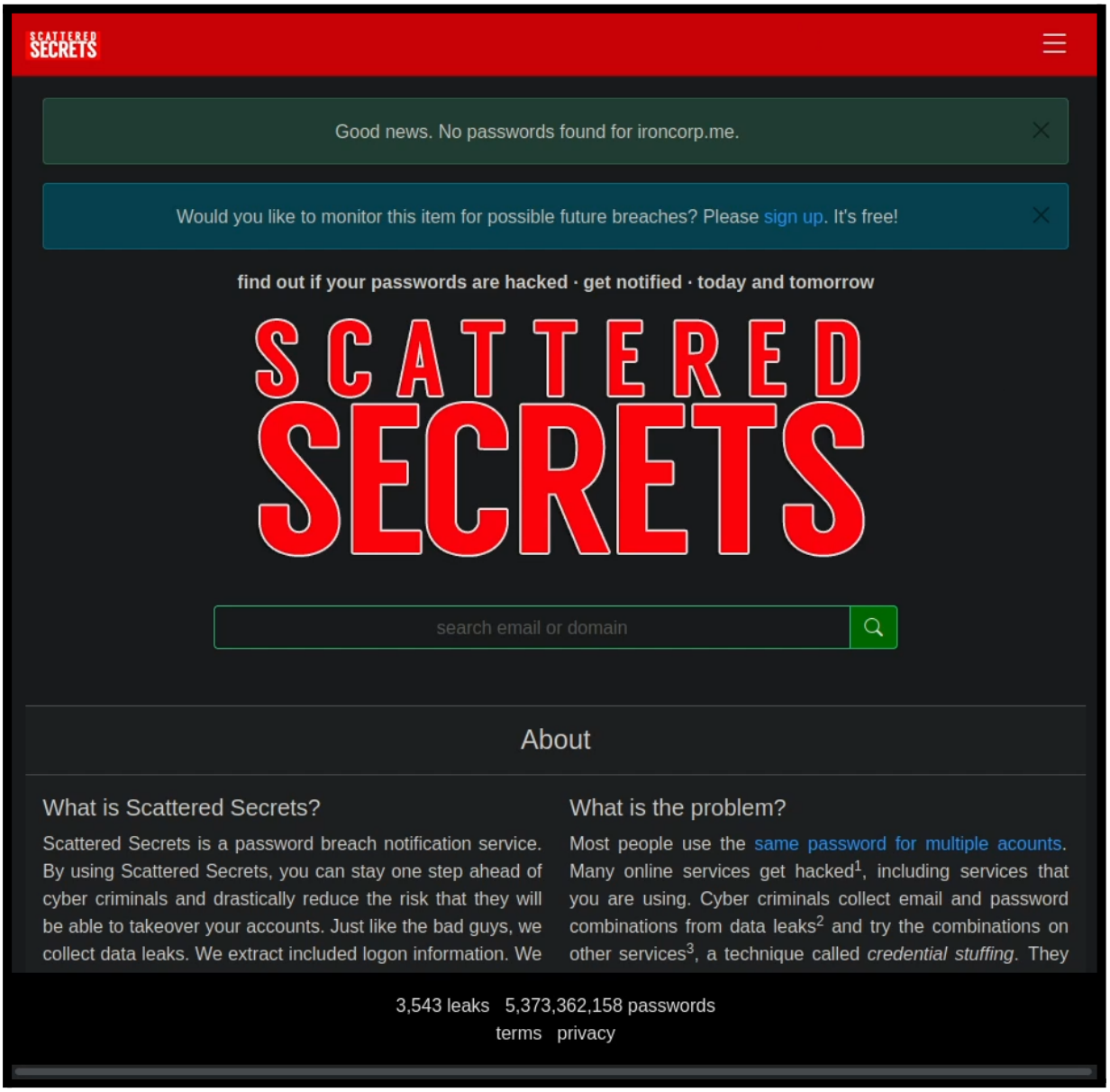
called Technext. After more googling I deduced that it is a legitimate company so I figured that the company would not likely be directly involved with this TryHackMe room.

Ironcorp

I also tried to google information about any company related to ironcorp.me to see if there is any useful information but only found TryHackMe write ups and other companies that have the words “iron” and “corp” in their names but did not seem to be related to this room.

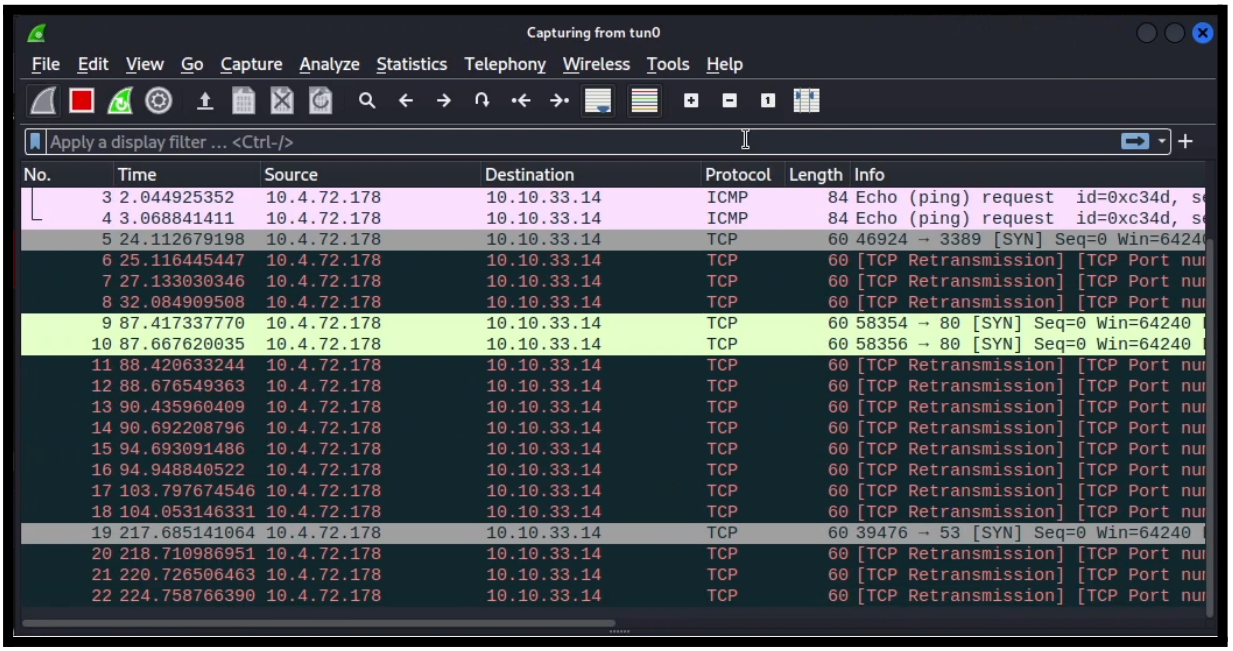
Searching Data Breaches for Passwords

I tried querying the domain name “ironcorp.me” on scatteredsecrets.com to see if there were any leaked passwords but no leaked passwords were found.



Wireshark

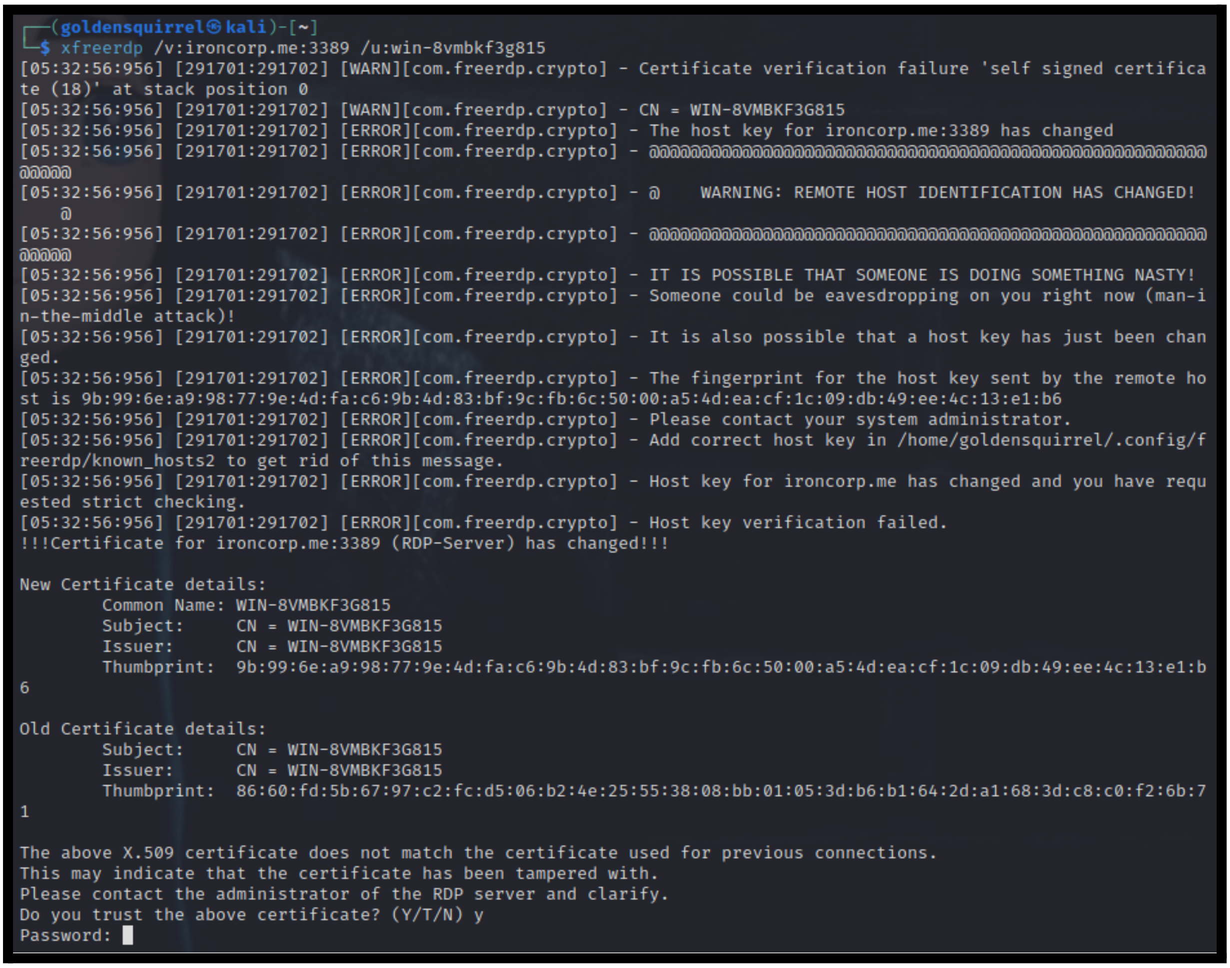
I had also ran wireshark for a couple of minutes just to see if there were any interesting packets being sent around but did not really find anything useful.



All the packets seen above were initiated by my machine.

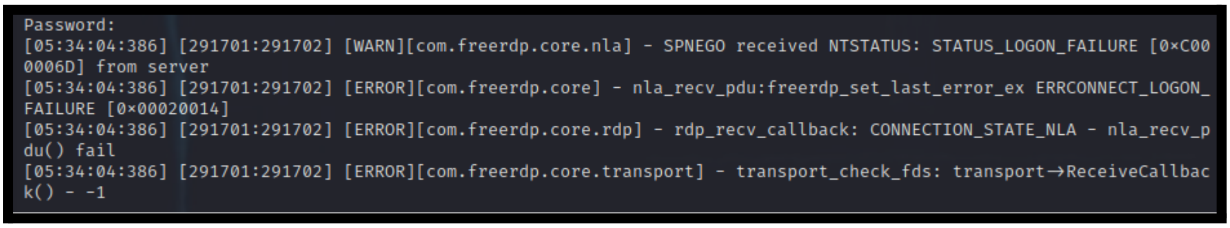
Brute Forcing RDP

I tried to connect to the machine using RDP on port 3389 but I did not have proper credentials so I just used the machine name(win-8vmbkf3g815) as the username.



```
┌──(goldensquirrel㉿kali)-[~]
└─$ xfreerdp /v:ironcorp.me:3389 /u:win-8vmbkf3g815
[05:32:56:956] [291701:291702] [WARN][com.freerdp.crypto] - Certificate verification failure 'self signed certificate (18)' at stack position 0
[05:32:56:956] [291701:291702] [WARN][com.freerdp.crypto] - CN = WIN-8VMBKF3G815
[05:32:56:956] [291701:291702] [ERROR][com.freerdp.crypto] - The host key for ironcorp.me:3389 has changed
[05:32:56:956] [291701:291702] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[05:32:56:956] [291701:291702] [ERROR][com.freerdp.crypto] - @    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
[05:32:56:956] [291701:291702] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[05:32:56:956] [291701:291702] [ERROR][com.freerdp.crypto] - IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
[05:32:56:956] [291701:291702] [ERROR][com.freerdp.crypto] - Someone could be eavesdropping on you right now (man-in-the-middle attack)!
[05:32:56:956] [291701:291702] [ERROR][com.freerdp.crypto] - It is also possible that a host key has just been changed.
[05:32:56:956] [291701:291702] [ERROR][com.freerdp.crypto] - The fingerprint for the host key sent by the remote host is 9b:99:6e:a9:98:77:9e:4d:fa:c6:9b:4d:83:bf:9c:fb:6c:50:00:a5:4d:ea:cf:1c:09:db:49:ee:4c:13:e1:b6
[05:32:56:956] [291701:291702] [ERROR][com.freerdp.crypto] - Please contact your system administrator.
[05:32:56:956] [291701:291702] [ERROR][com.freerdp.crypto] - Add correct host key in /home/goldensquirrel/.config/freerdp/known_hosts2 to get rid of this message.
[05:32:56:956] [291701:291702] [ERROR][com.freerdp.crypto] - Host key for ironcorp.me has changed and you have requested strict checking.
[05:32:56:956] [291701:291702] [ERROR][com.freerdp.crypto] - Host key verification failed.
!!!Certificate for ironcorp.me:3389 (RDP-Server) has changed!!!

New Certificate details:
        Common Name: WIN-8VMBKF3G815
        Subject:     CN = WIN-8VMBKF3G815
        Issuer:      CN = WIN-8VMBKF3G815
        Thumbprint:  9b:99:6e:a9:98:77:9e:4d:fa:c6:9b:4d:83:bf:9c:fb:6c:50:00:a5:4d:ea:cf:1c:09:db:49:ee:4c:13:e1:b6

Old Certificate details:
        Subject:     CN = WIN-8VMBKF3G815
        Issuer:      CN = WIN-8VMBKF3G815
        Thumbprint:  86:60:fd:5b:67:97:c2:fc:d5:06:b2:4e:25:55:38:08:bb:01:05:3d:b6:b1:64:2d:a1:68:3d:c8:c0:f2:6b:71

The above X.509 certificate does not match the certificate used for previous connections.
This may indicate that the certificate has been tampered with.
Please contact the administrator of the RDP server and clarify.
Do you trust the above certificate? (Y/T/N) y
Password:
```

After that I was prompted to enter a password but I did not have one so I left that blank which then led to my RDP attempt failing.



```
Password:
[05:34:04:386] [291701:291702] [WARN][com.freerdp.core.nla] - SPNEGO received NTSTATUS: STATUS_LOGON_FAILURE [0xC000006D] from server
[05:34:04:386] [291701:291702] [ERROR][com.freerdp.core] - nla_recv_pdu:freerdp_set_last_error_ex ERRCONNECT_LOGON_FAILURE [0x00020014]
[05:34:04:386] [291701:291702] [ERROR][com.freerdp.core.rdp] - rdp_recv_callback: CONNECTION_STATE_NLA - nla_recv_pdu() fail
[05:34:04:386] [291701:291702] [ERROR][com.freerdp.core.transport] - transport_check_fds: transport->ReceiveCallback() - -1
```

After that I tried to bruteforce the username & password using Ncrack. I tried using the username "administrator" and a password wordlist but it failed. I am not too familiar with Ncrack but my assumption of why it failed was because the machine had locked me out after failing too many times. Due to this issue I concluded that brute forcing RDP was not viable.

```
┌──(goldensquirrel㉿kali)-[~]
└─$ ncrack -vv --user administrator -P /usr/share/seclists/Passwords/2020-200_most_used_passwords.txt rdp://10.10.50
.241:3389

Starting Ncrack 0.7 ( http://ncrack.org ) at 2022-08-01 23:38 EDT

rdp://10.10.50.241:3389 finished. Too many failed attempts.


Ncrack done: 1 service scanned in 141.12 seconds.
Probes sent: 86 | timed-out: 31 | prematurely-closed: 0

Ncrack finished.
```

Querying DNS Server

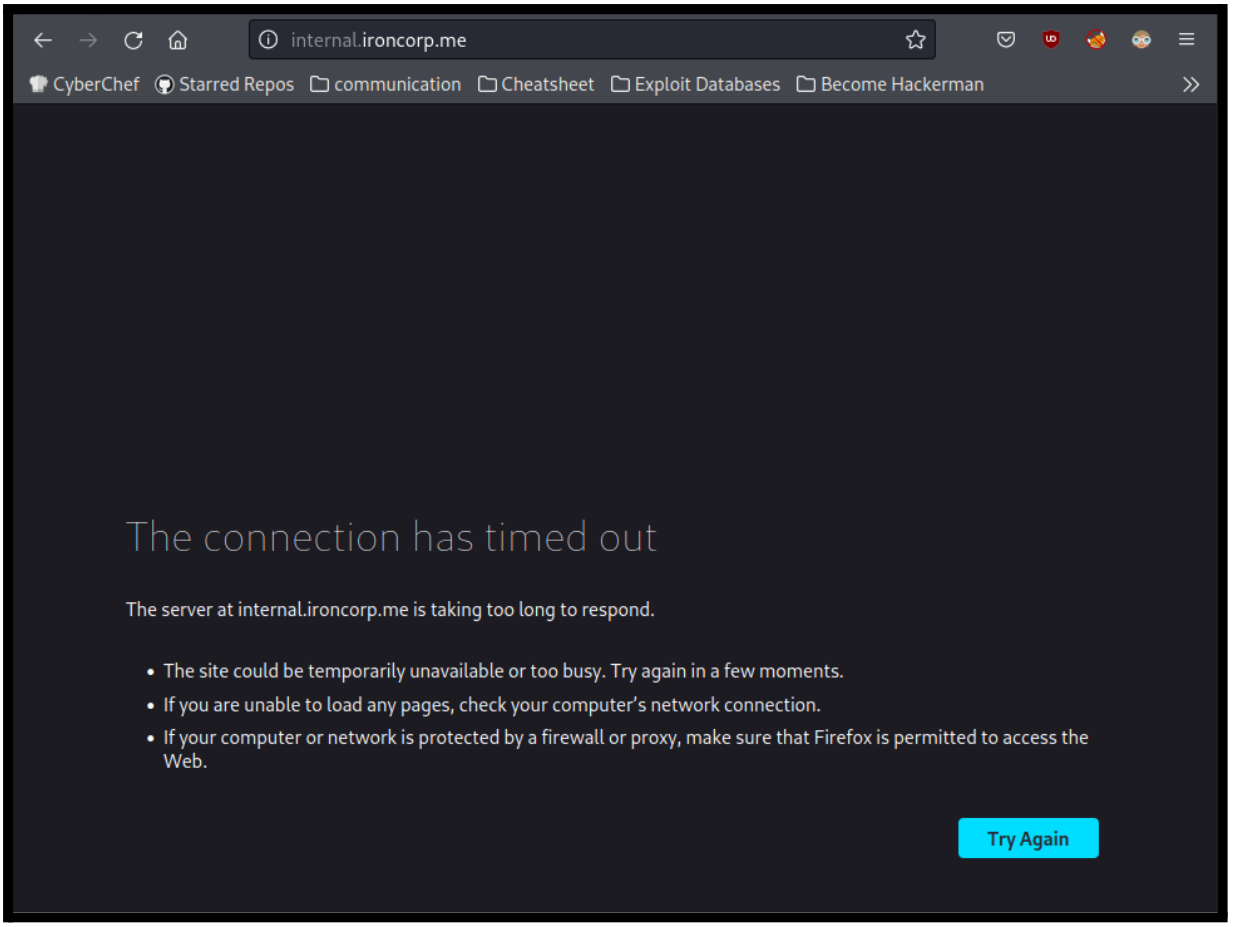
Next, I proceeded to query the DNS server using the axfr protocol. From the query, we obtain two subdomains of ironcorp.me

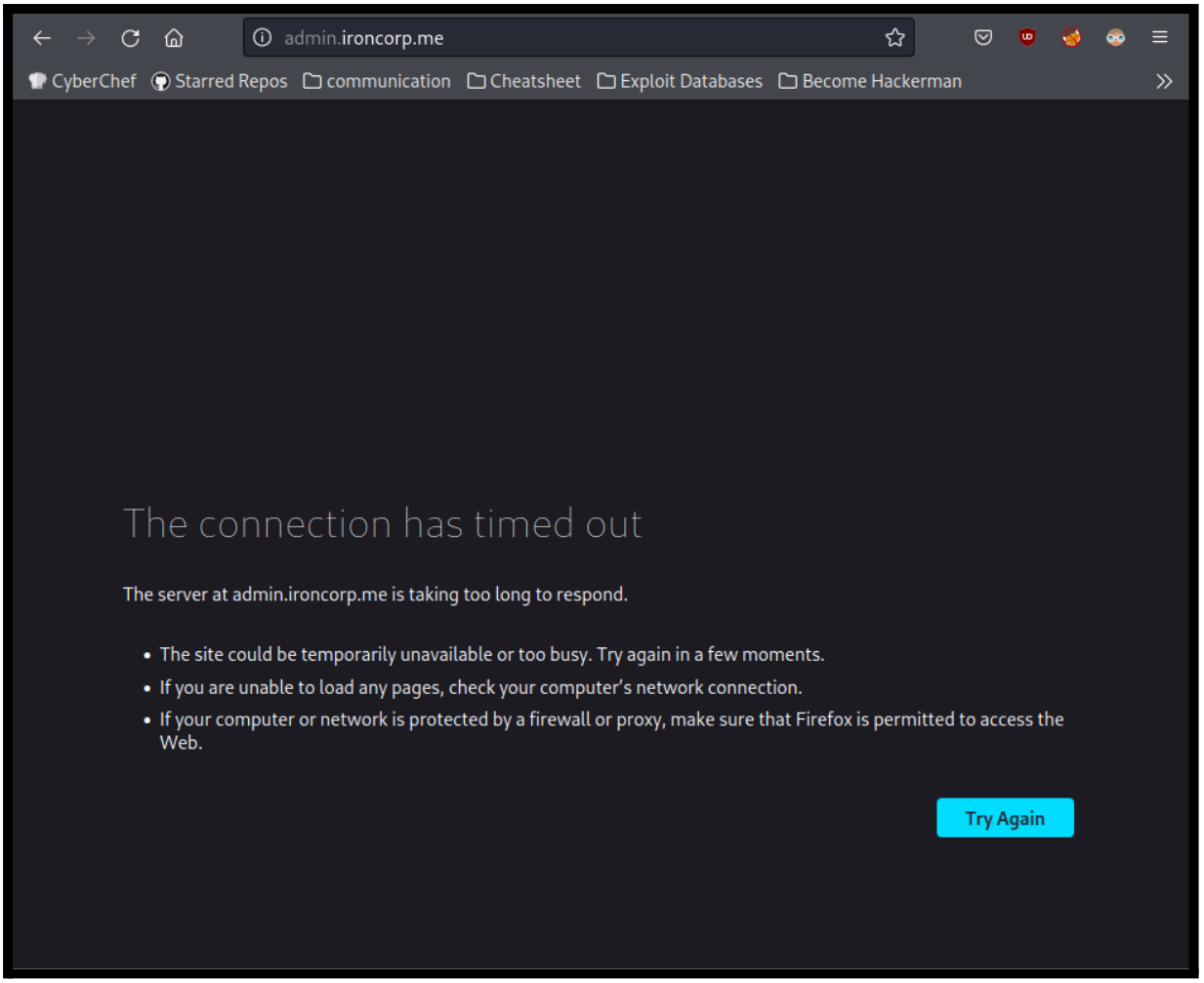
```
┌──(goldensquirrel㉿kali)-[~]
└─$ dig axfr @ironcorp.me ironcorp.me

; <<>> DiG 9.18.1-1-Debian <<>> axfr @ironcorp.me ironcorp.me
; (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: 403 msec
;; SERVER: 10.10.112.244#53(ironcorp.me) (TCP)
;; WHEN: Wed Aug 03 04:37:51 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

Then I added these subdomains to my **`/etc/hosts`** file.

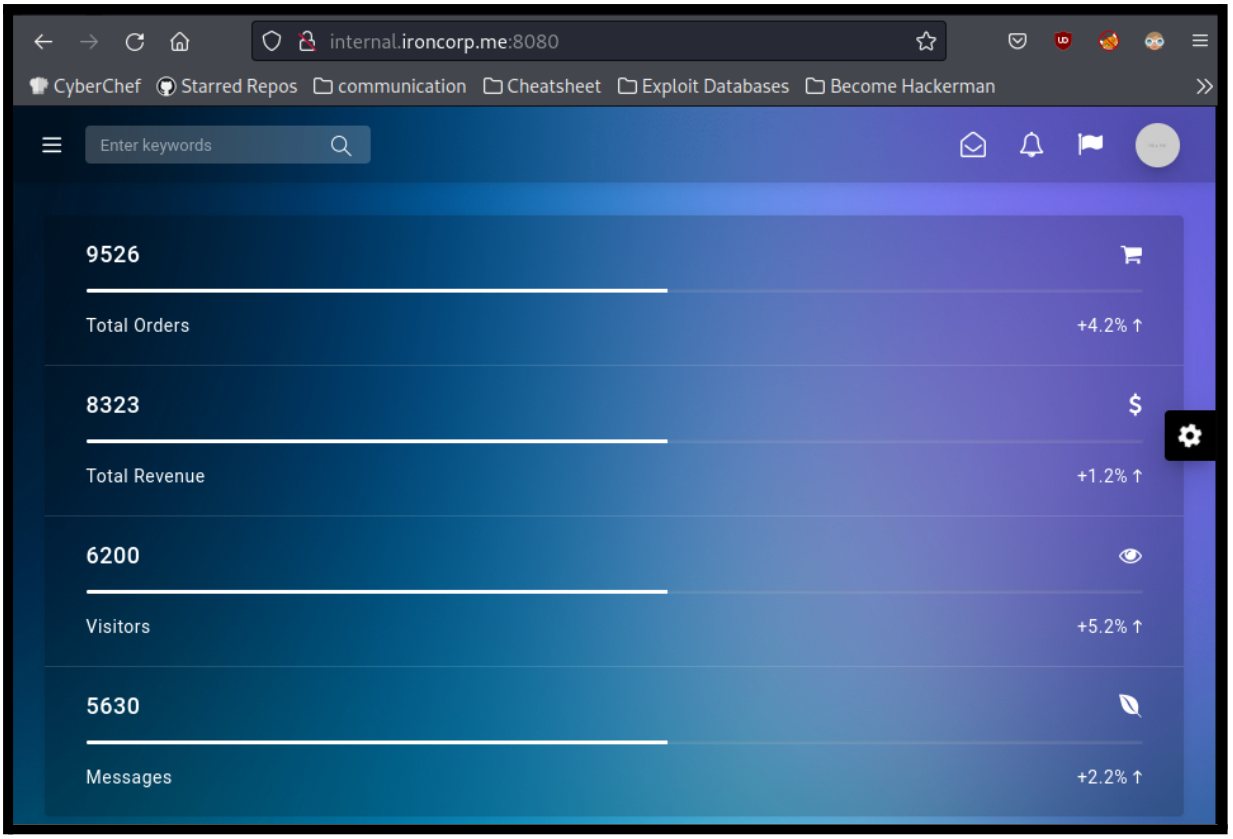
```
  GNU nano 6.2                                        /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
10.10.113.20    ironcorp.me
10.10.113.20    admin.ironcorp.me
10.10.113.20    internal.ironcorp.me

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

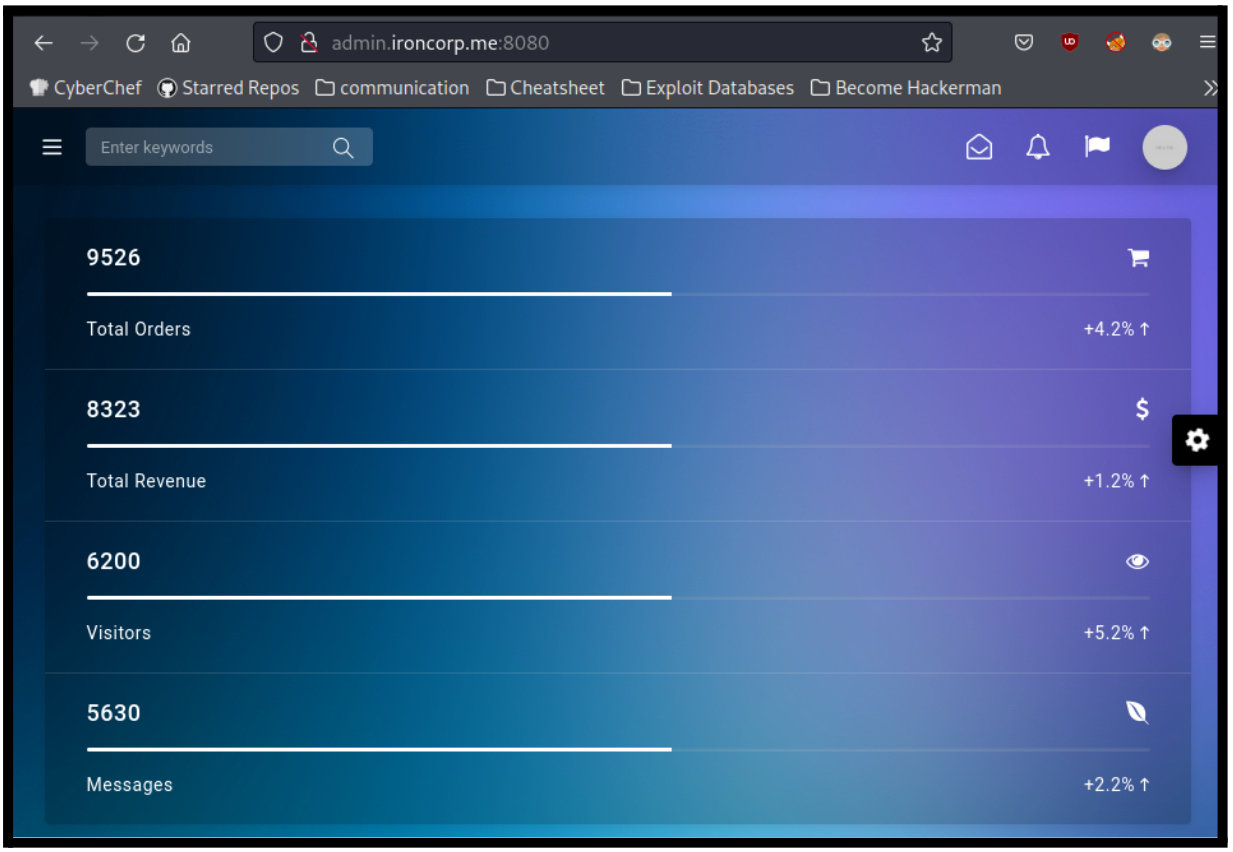
After that, I tried accessing the subdomains in firefox but was unable to connect.


internal.ironcorp.me
CyberChef
Starred Repos
communication
Cheatsheet
Exploit Databases
Become Hackerman
The connection has timed out
The server at internal.ironcorp.me is taking too long to respond.
• The site could be temporarily unavailable or too busy. Try again in a few moments.
• If you are unable to load any pages, check your computer's network connection.
• If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.
Try Again



Next I tried to access the subdomain pages under port 8080 but it just brought me back to the admin template page from earlier.

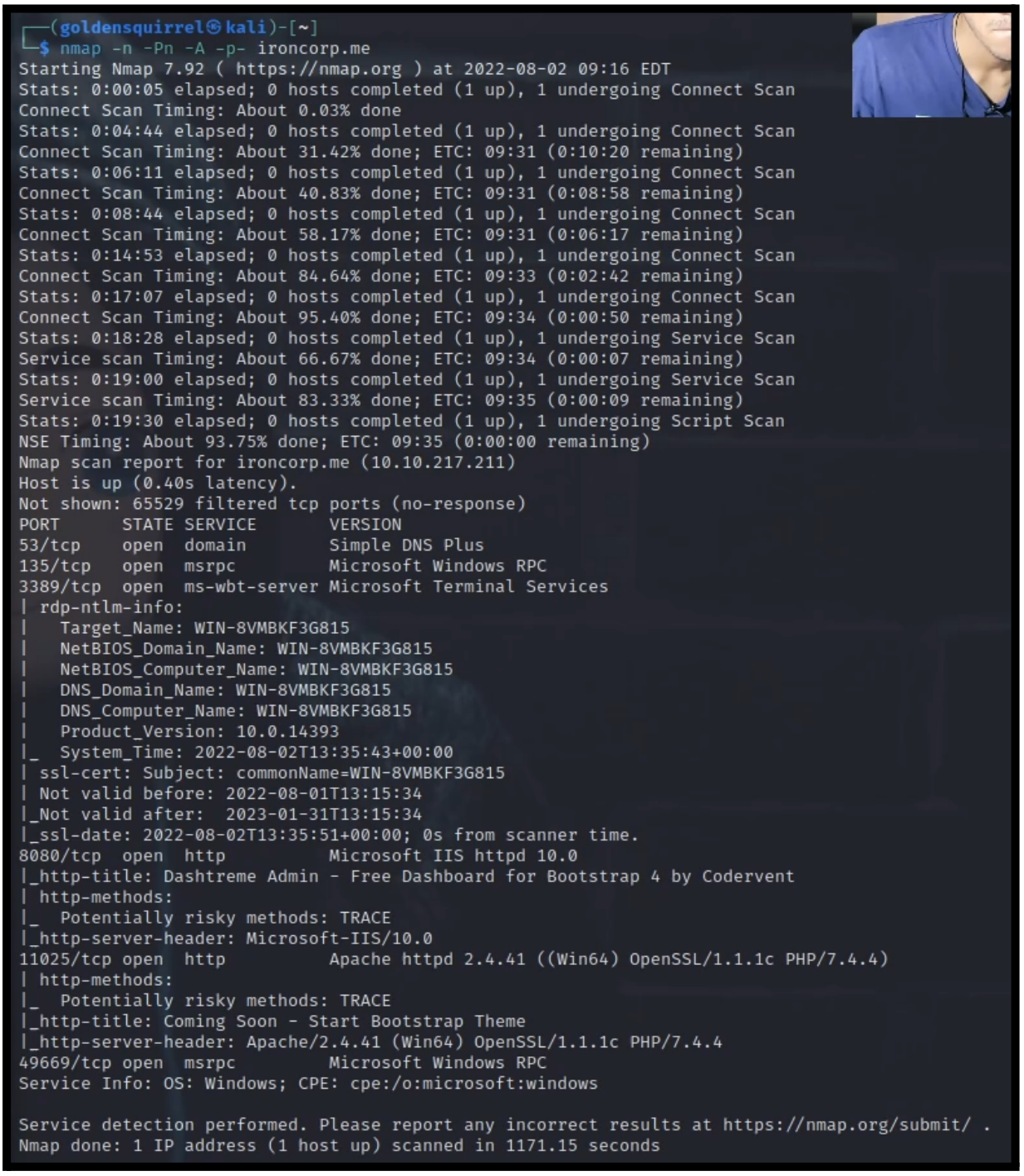

internal.ironcorp.me:8080
CyberChef
Starred Repos
communication
Cheatsheet
Exploit Databases
Become Hackerman
Enter keywords
9526
Total Orders
+4.2% ↑
8323
Total Revenue
+1.2% ↑
6200
Visitors
+5.2% ↑
5630
Messages
+2.2% ↑


admin.ironcorp.me:8080
CyberChef
Starred Repos
communication
Cheatsheet
Exploit Databases
Become Hackerman
Enter keywords
9526
Total Orders
+4.2% ↑
8323
Total Revenue
+1.2% ↑
6200
Visitors
+5.2% ↑
5630
Messages
+2.2% ↑

At this point I was stuck unsure on what else I could try to do. I ended up trying to read up more online about DNS servers in hopes of finding inspiration. After many hours, I thought of the idea of doing a full port scan using Nmap.

Full Port Scan

So I conducted a full port scan using the flags shown below.



There are 2 new ports that appear in the scan, port 11025 and port 49669.

1. **Port 49669**

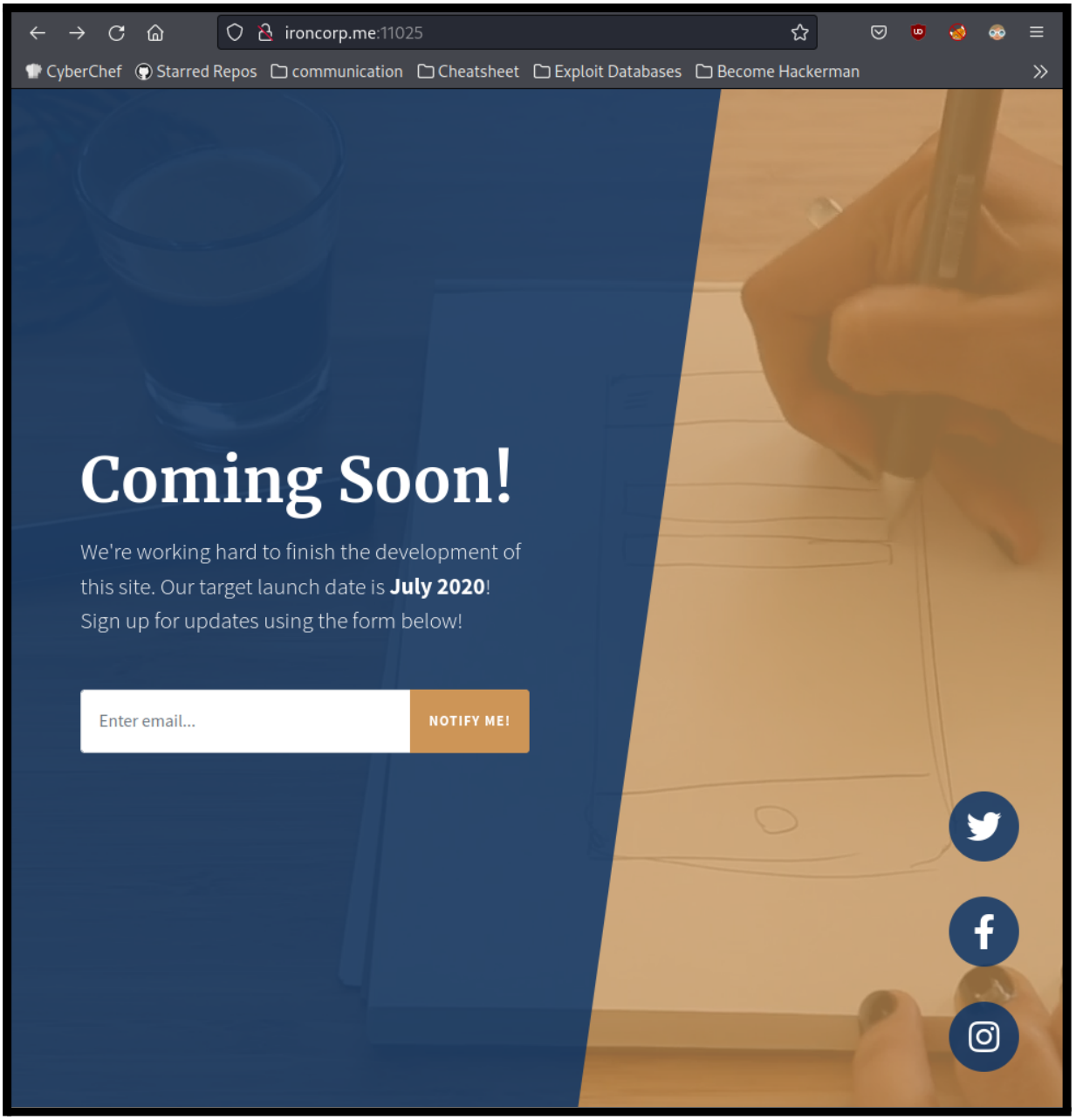
   This port seems to be another port for Microsoft Windows RPC so it might not be very helpful right now.

2. **Port 11025**

   This port seems to be another http service running on the port so I tried to open it using my browser and trying on the subdomains I've found.

   ironcorp.me

   Opening this domain on port 11025 reveals a coming soon page. After snooping around on this website, I find that all the interactables on the website do not do anything.

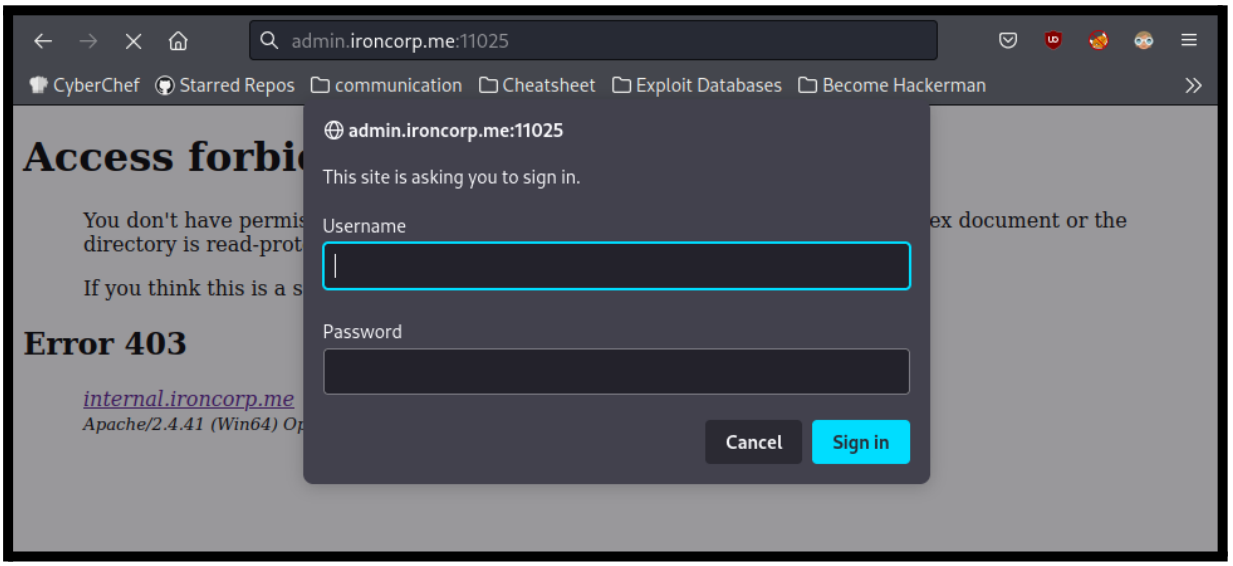

ironcorp.me:11025
CyberChef
Starred Repos
communication
Cheatsheet
Exploit Databases
Become Hackerman
Coming Soon!
We're working hard to finish the development of this site. Our target launch date is July 2020!
Sign up for updates using the form below!
Enter email...
NOTIFY ME!

internal.ironcorp.me

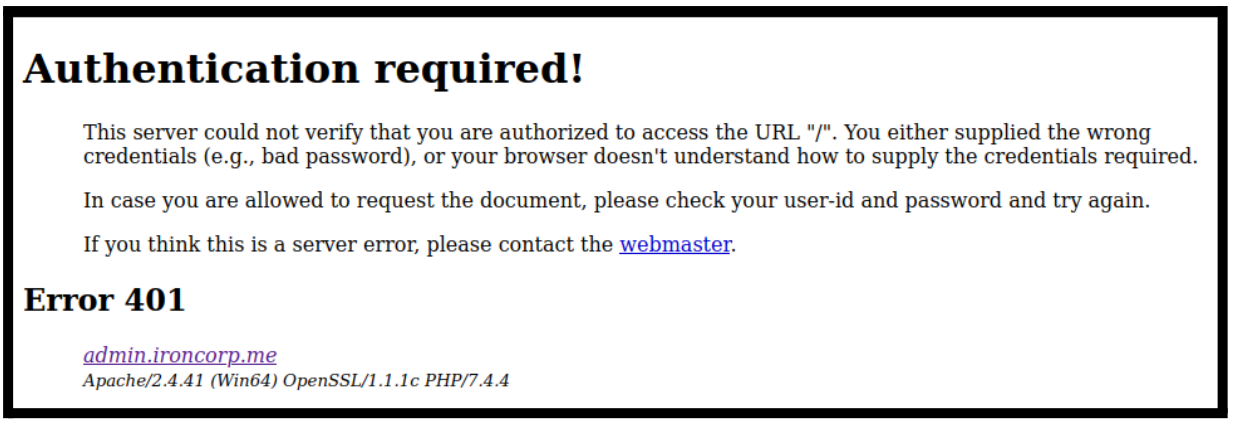
When I try accessing this subdomain on port 11025 I get an Access forbidden error most likely because I currently do not have the permissions to access the site.

admin.ironcorp.me:11025

When I try to access this subdomain on port 11025 I am prompted to enter a username and password. Whenever I enter the wrong credentials, I am prompted to enter my credentials again.



When I leave the fields empty and click on the Sign in button, I'm prompted with an error message.

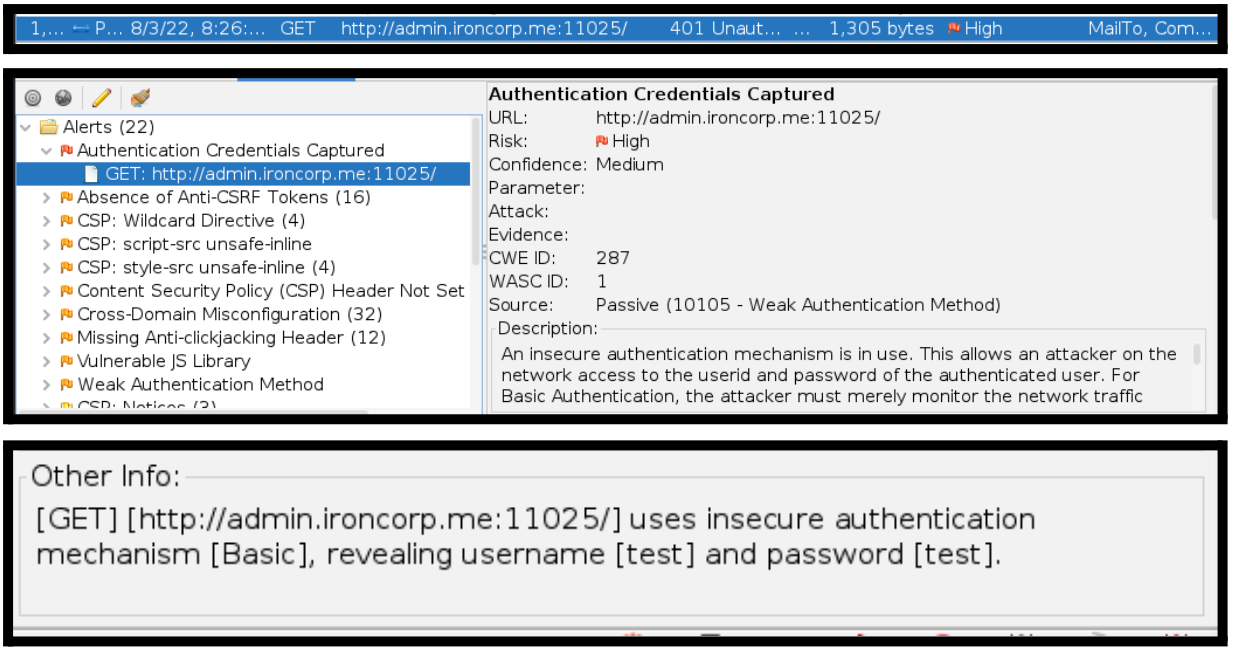


Brute Forcing Admin Login

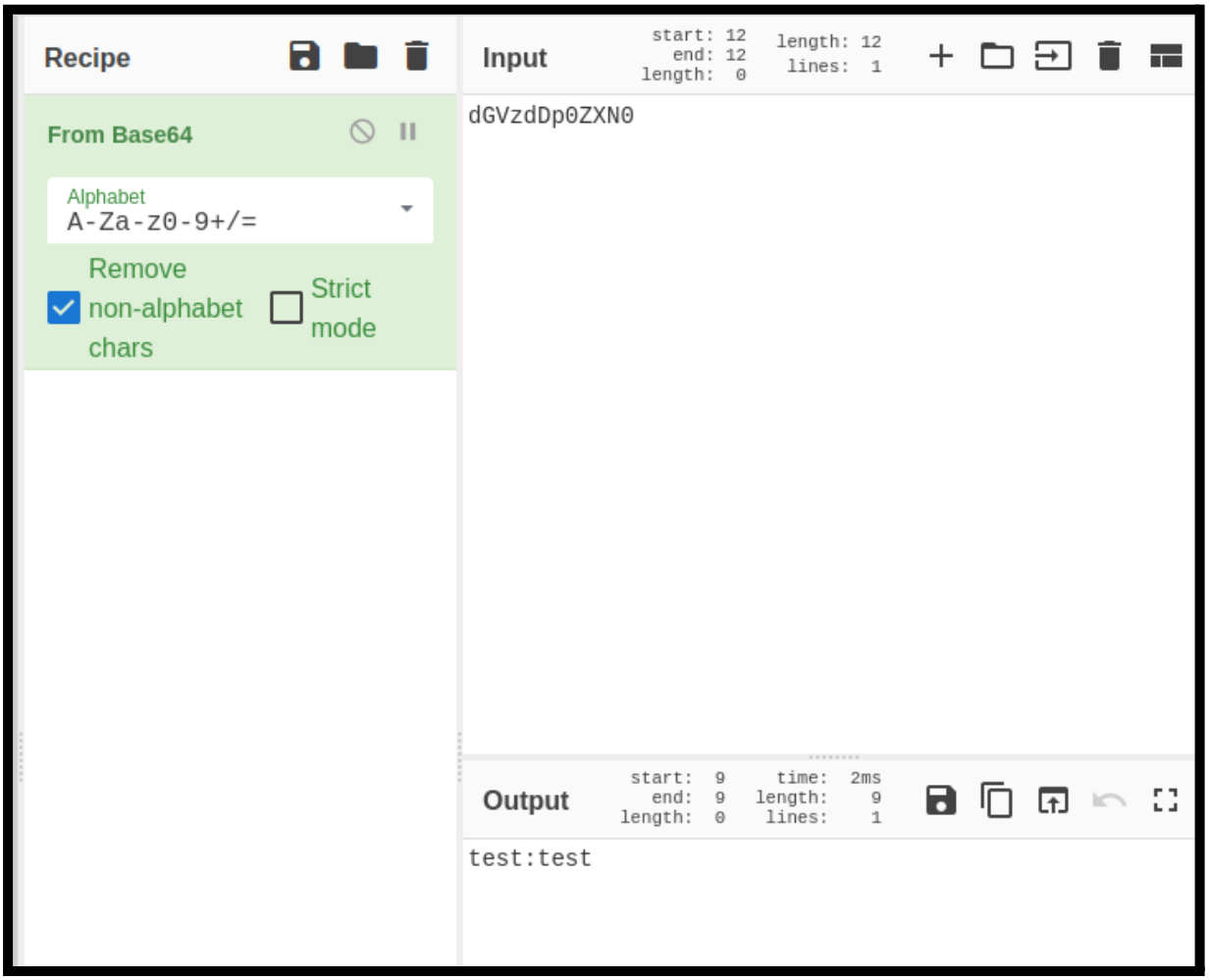
I proceeded to try to brute force the admin login using OWASP ZAP. I started by capturing a request that was using the username “test” and the password “test”.

```
GET http://admin.ironcorp.me:11025/ HTTP/1.1
Host: admin.ironcorp.me:11025
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Authorization: Basic dGVzdDp0ZXN0
```

The request was also flagged by OWASP because authentication credentials were captured.



This seems to be from the Authorization request header. Under this header there is some sort of encoded text so I put it inside Cyberchef to decode it. Using the magic wand tool on cyberchef, it automatically detected the encoding to be Base64.

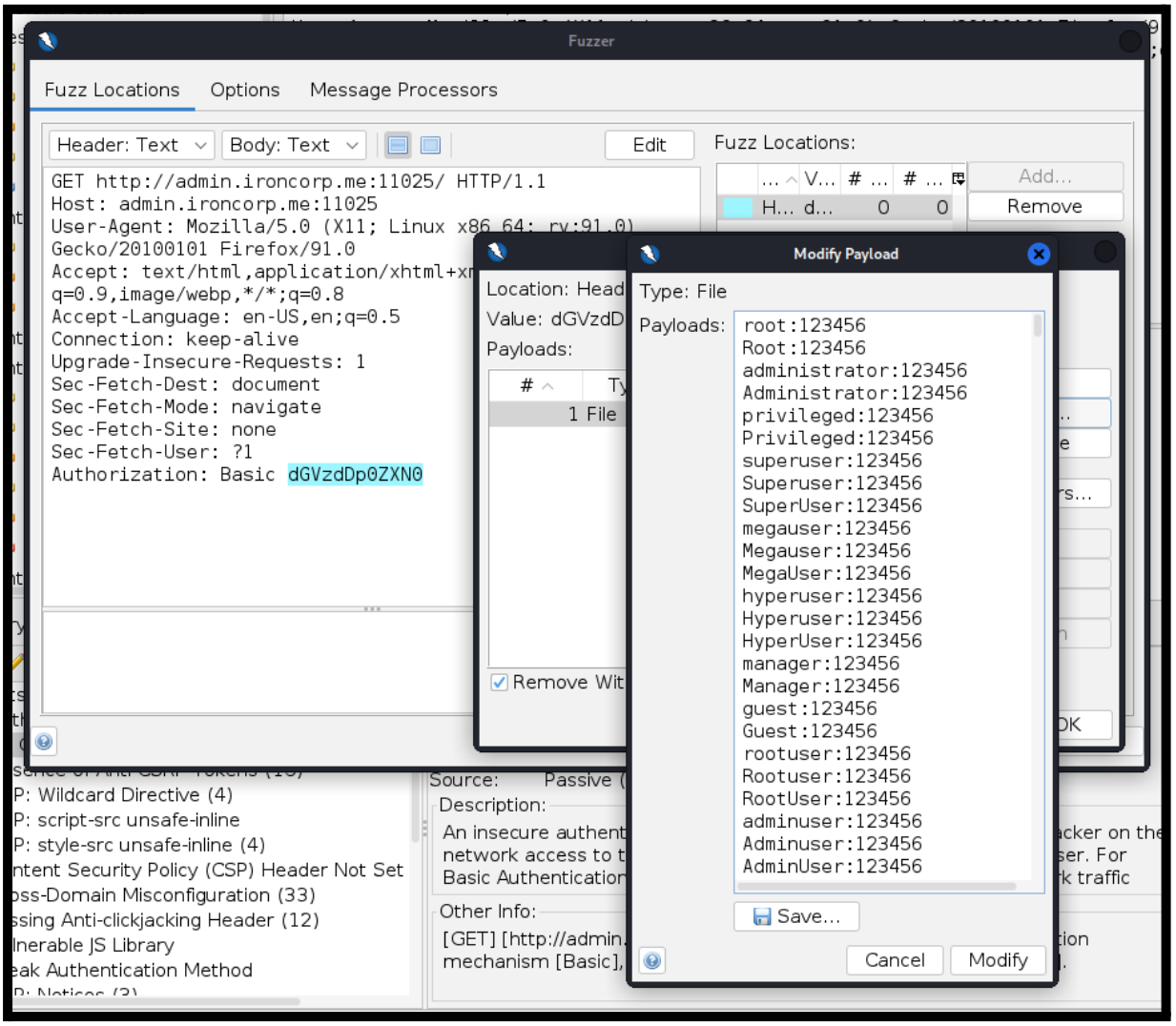


Crafting a suitable wordlist

I then proceeded to craft a username & password wordlist that follows the format username:password. To make it easier, I created a [python script] that takes input from a username wordlist and a password wordlist and outputs a new wordlist file that follows the format.

```python
password = open("2020-200_most_used_passwords.txt", "r")
username = open("ModifiedCommonAdminBase64.txt", "r").read().splitlines()
payload = open("payload.txt", "w")

for p in password:
    for u in username:
        payload.write(f"{u.rstrip()}:{p.rstrip()}\n")

```

Now I can use the request from before inside the OWASP Fuzzer. I just add the payload.txt file as the payload for the fuzzer.

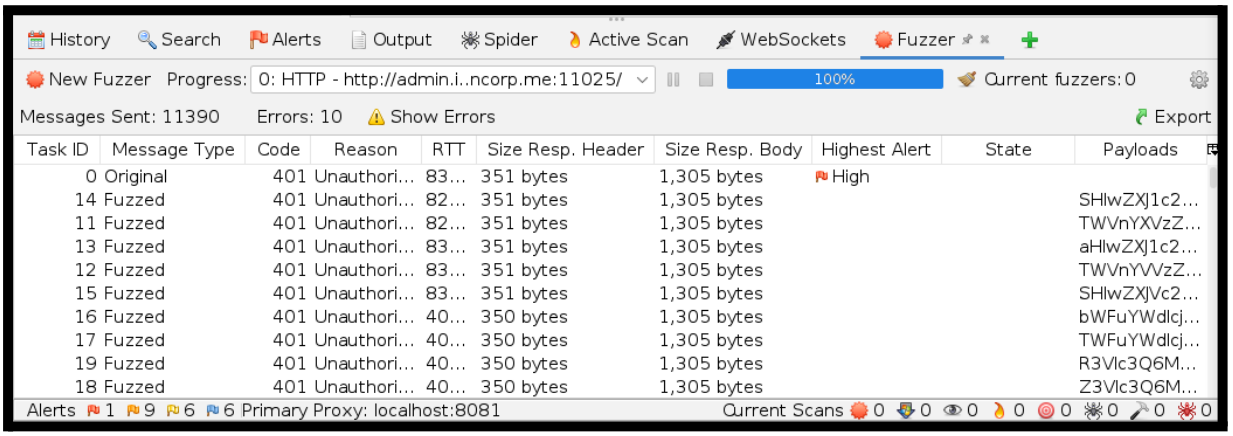


Then I add a Base64 Encode processor on the payload and start fuzzing.


Add Processor
Type: Base64 Encode
Character Encoding: UTF-8
Break Lines:
Generate Preview
Current Payloads:
Processed Payloads:
root:123456
Root:123456
administrator:123456
Administrator:123456
privileged:123456
Privileged:123456
superuser:123456
Superuser:123456
SuperUser:123456
megauser:123456
Megauser:123456
MegaUser:123456
hyperuser:123456
Hyperuser:123456
HyperUser:123456
manager:123456
Manager:123456
guest:123456
Guest:123456
rootuser:123456
cm9vdDoxMjM0NTY=
Um9vdDoxMjM0NTY=
YWRtaW5pc3RyYXRvcjoxMjM
QWRtaW5pc3RyYXRvcjoxMjM
cHJpdmlsZWdlZDoxMjM0NTY
UHJpdmlsZWdlZDoxMjM0NTY
c3VwZXJ1c2VyOjEyMzQ1Ng=
U3VwZXJ1c2VyOjEyMzQ1Ng=
U3VwZXJVc2VyOjEyMzQ1Ng=
bWVnYXVzZXI6MTIzNDU2
TWVnYXVzZXI6MTIzNDU2
TWVnYVVzZXI6MTIzNDU2
aHlwZXJ1c2VyOjEyMzQ1Ng=
SHlwZXJ1c2VyOjEyMzQ1Ng=
SHlwZXJVc2VyOjEyMzQ1Ng=
bWFuYWdlcjoxMjM0NTY=
TWFuYWdlcjoxMjM0NTY=
Z3Vlc3Q6MTIzNDU2
R3Vlc3Q6MTIzNDU2
cm9vdHVzZXI6MTIzNDU2
Lock Scroll
Cancel
Add

Fuzzing Results

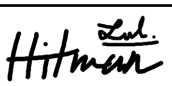
After the fuzzing was completed, I analysed the Size of the response bodies and also the status code but they were all the same in every request sent.



Out of Time

At this point I have already run out of time to crack the machine and failed to even get a foothold. If I had more time to continue my efforts, I would have tried to brute force the admin login more using other wordlists.

Contributions

ID	Name	Contribution	Signatures
1211101125	Sayid Abdur-Rahman Al-Aidarus Bin Syed Abu Bakar Mashor Al-Idrus	Wrote the write up, attempted to crack the machine (attempts explained in the write up)	
1211103699	Choo Qing Lam	-	
1211101237	Mohammad Zulhilman Bin Mohd Hisham	Cracked the machine (attempts are not in the write-up)	
1211101234	Muhammad Zahin Adri Bin Mohd Nawawi	Attempted to crack the machine.	

Due to a couple of communication errors we decided to do an individual pentest. Every member did it individually.

Video presentation:

VIDEO LINK: https://youtu.be/di-mzAko1Oc