PenTest 2

Iron Corp

CyberTeam

Members

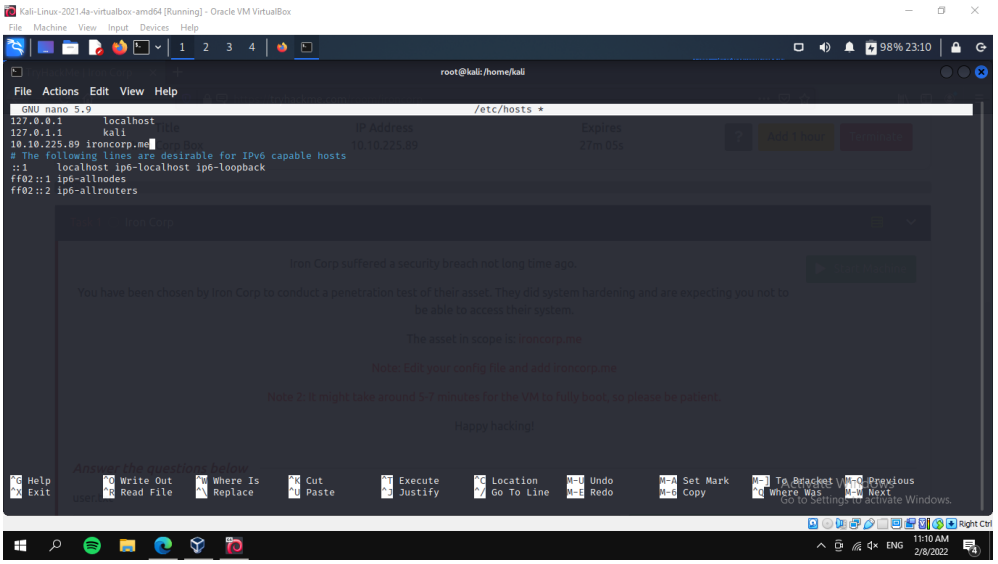
ID	NAME
1211103785	BRIJHENDHRA A/L SARAVANARAJ

Steps: Recon and Enumeration

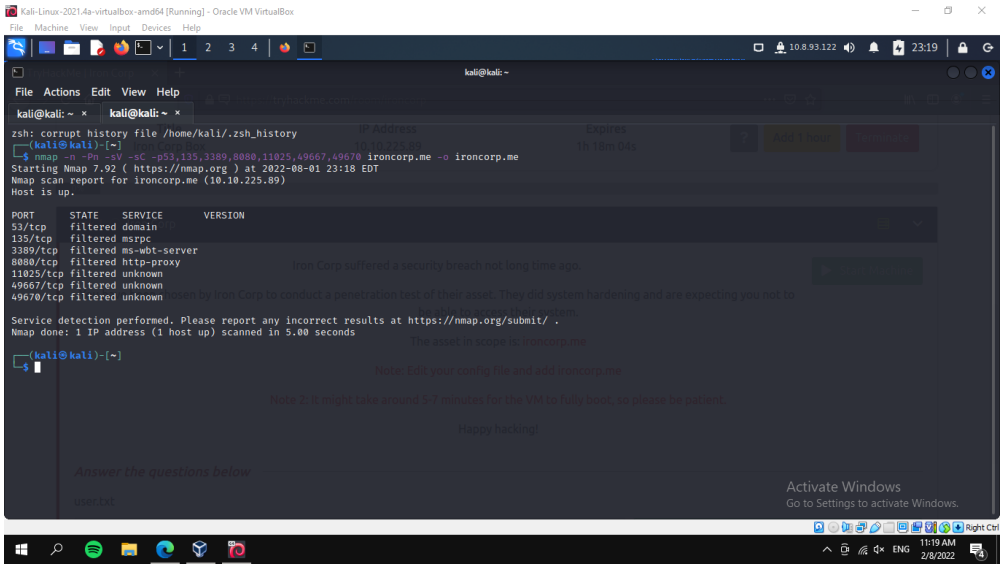
Members involved: Brijhendhra A/L Saravanaraj

Tools used: Kali Linux, Nmap

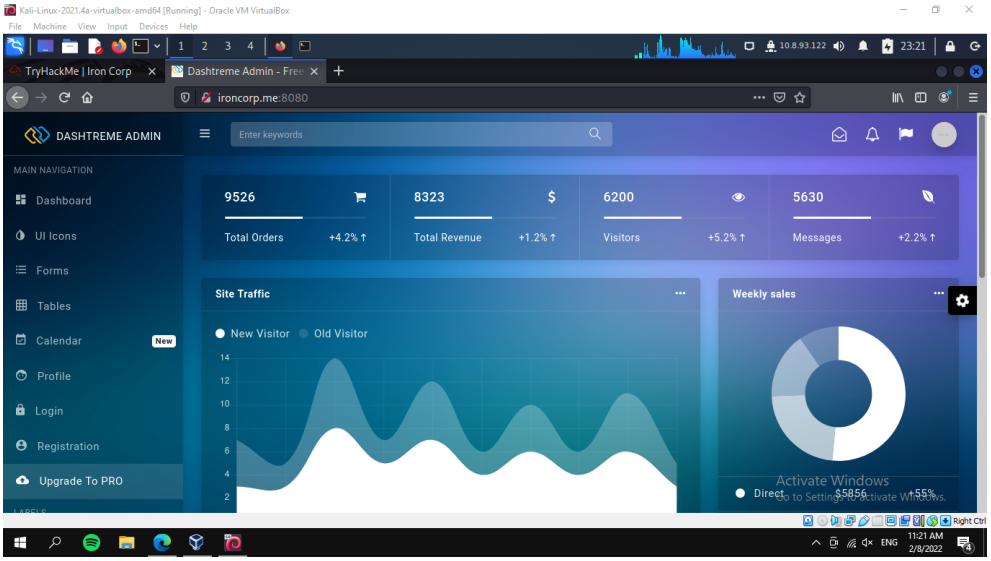
Thought Process and Methodology and Attempts:



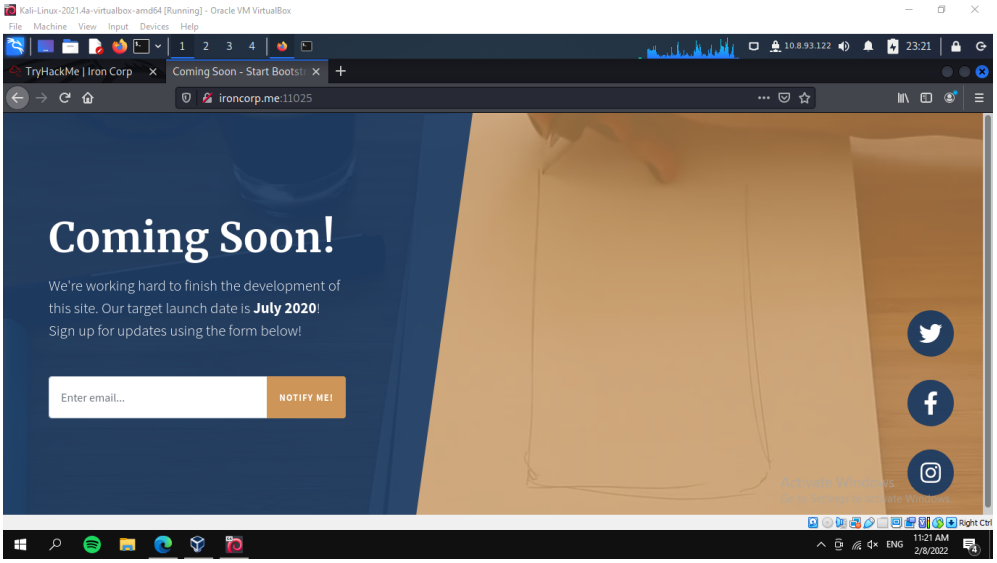
We first input IP address into “/etc/hosts” file



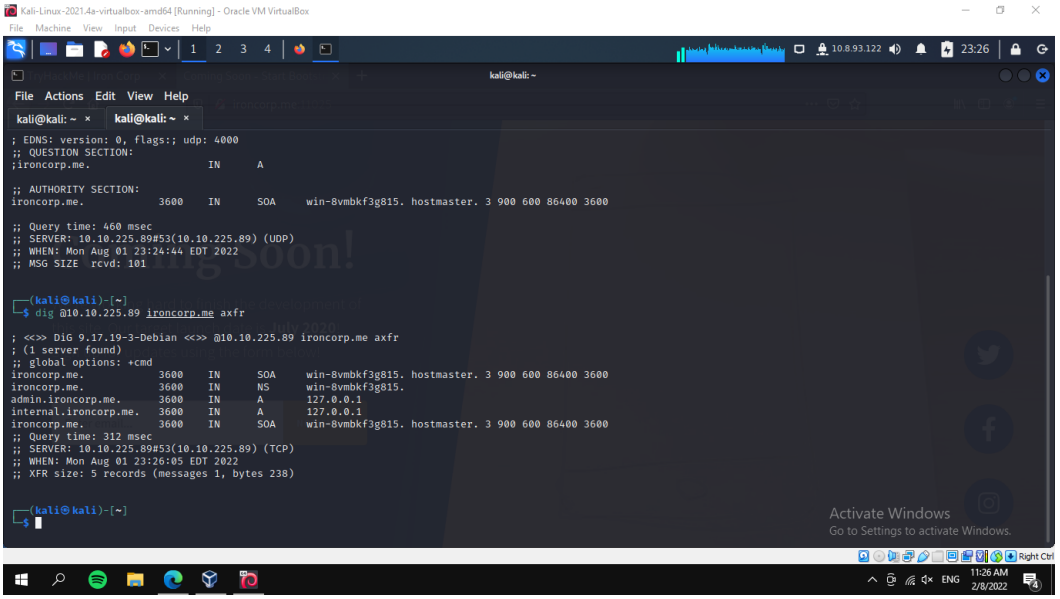
We execute nmap scan with ironcorp.me as reference to the IP address that was input into the file



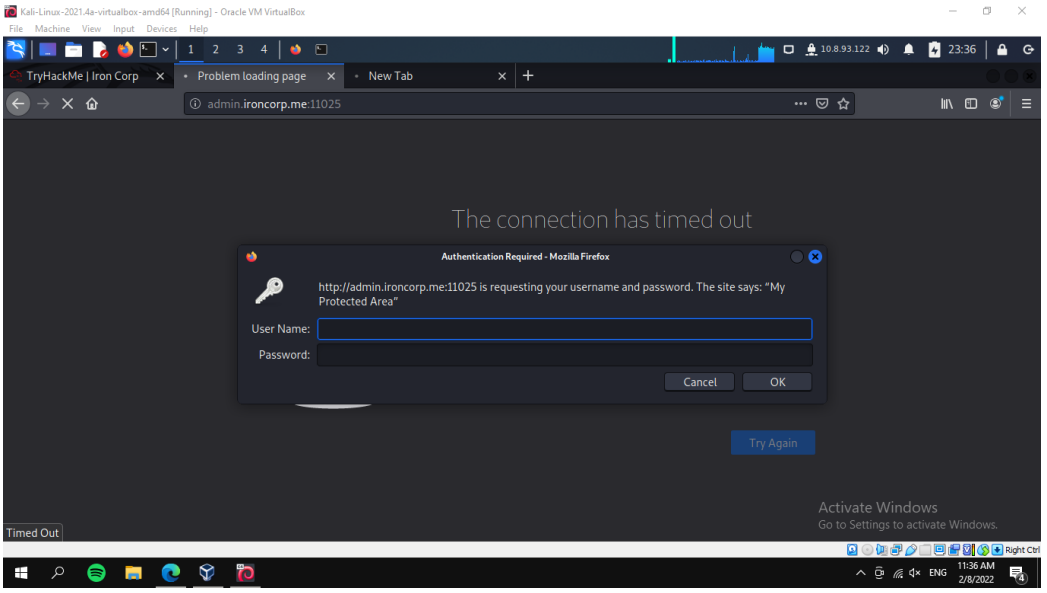
We could access into web service port 8080 but there was no functionality in there



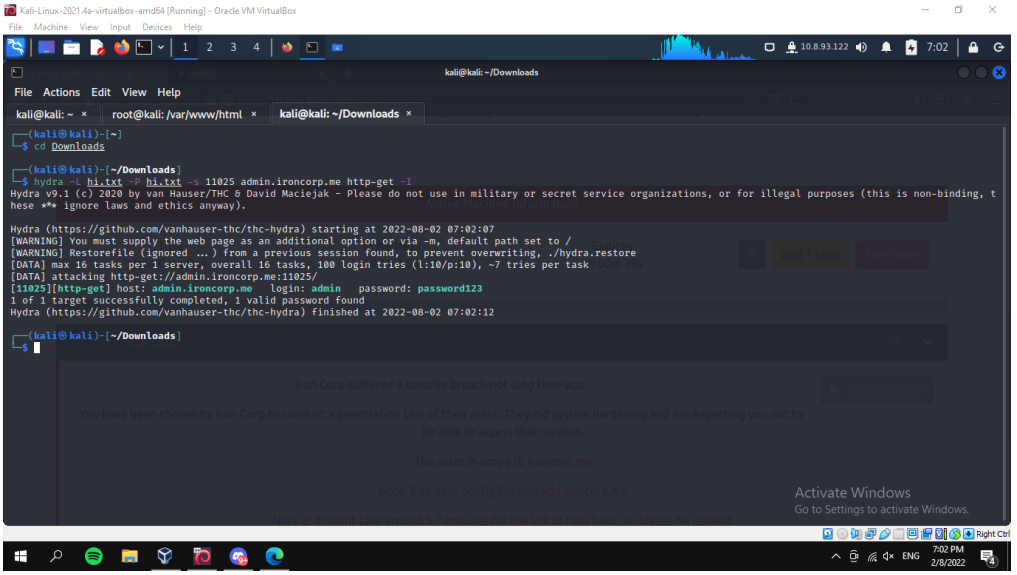
We could also access into web service 11025 but also no functionality



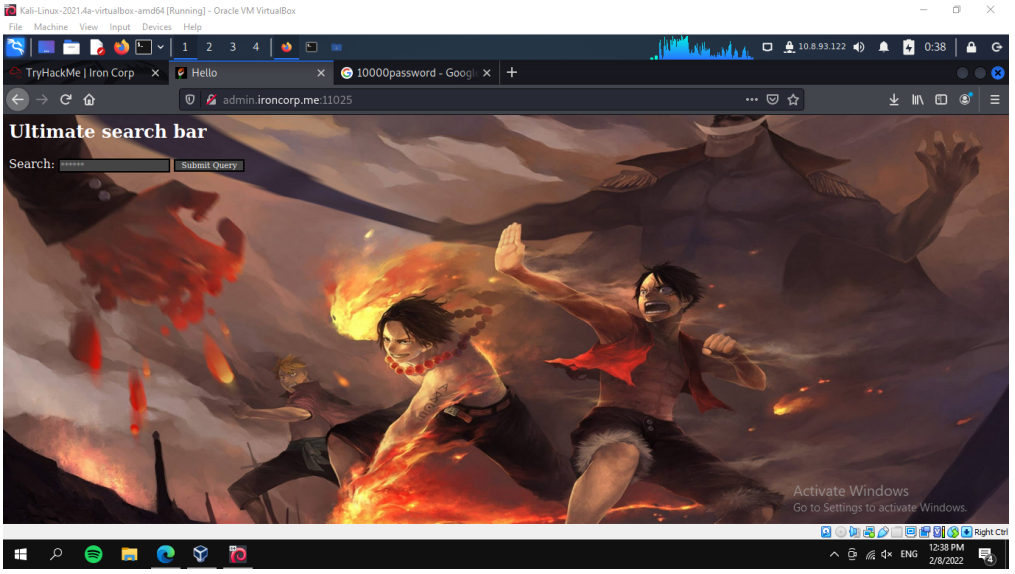
With dig, we tried to list down any other sub domain or information and found 2 subdomains running



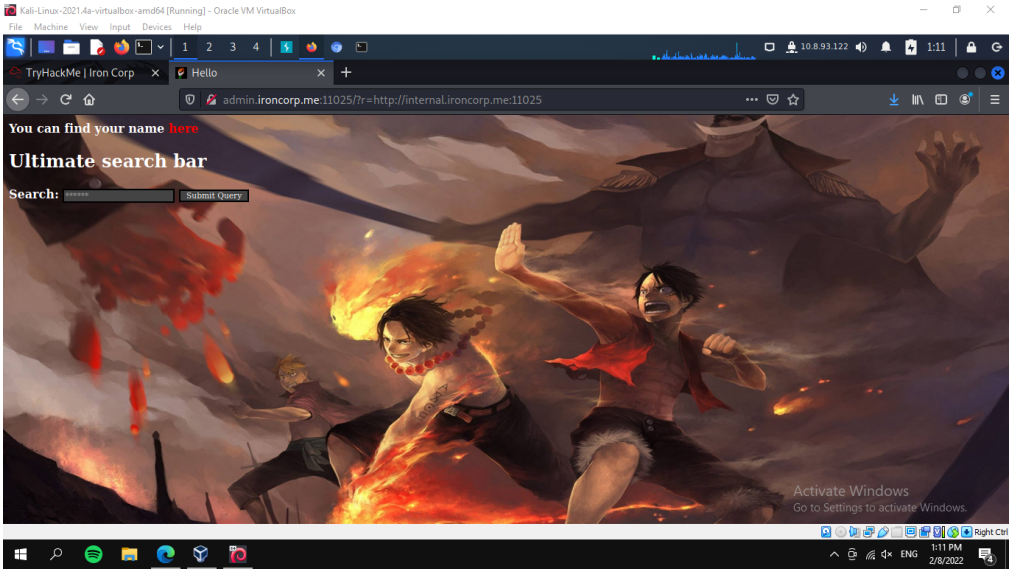
Upon input “admin.ironcorp.me:11025”, it requires a username and password



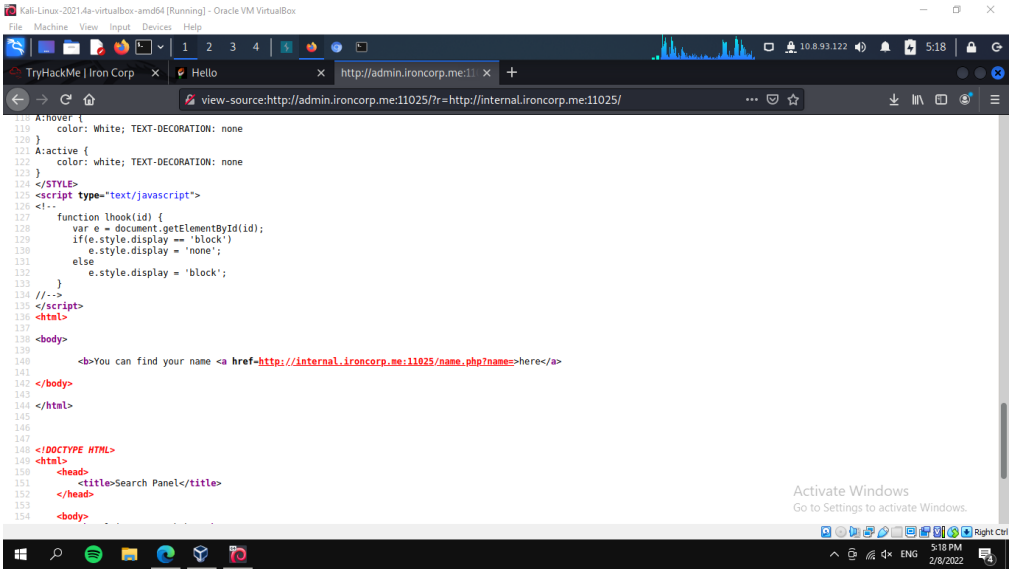
We then use hydra to guess the username and password with a set of words in a text file which is a representation of the most commonly used username and passwords



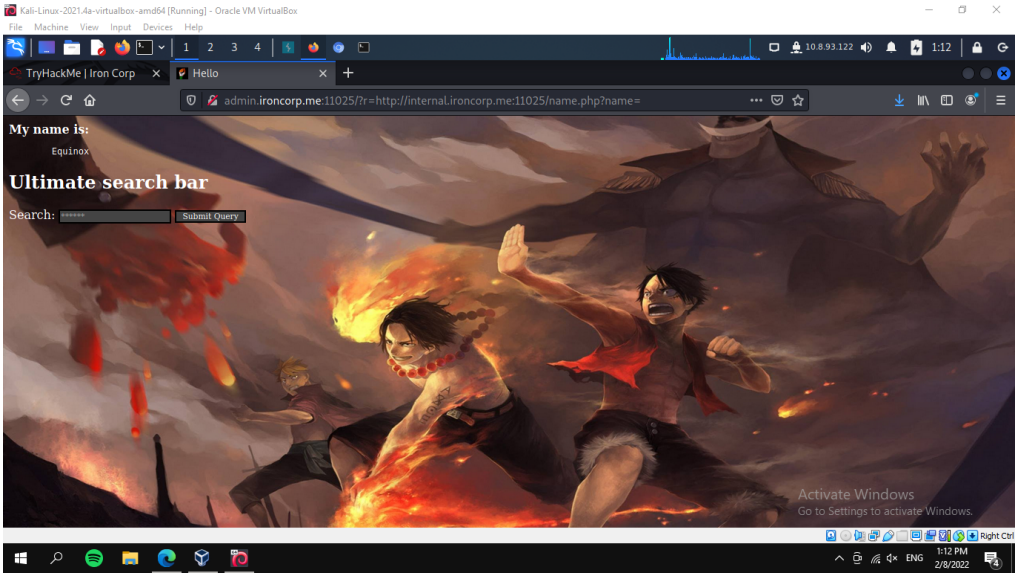
When login with the username and password, we can see the page.



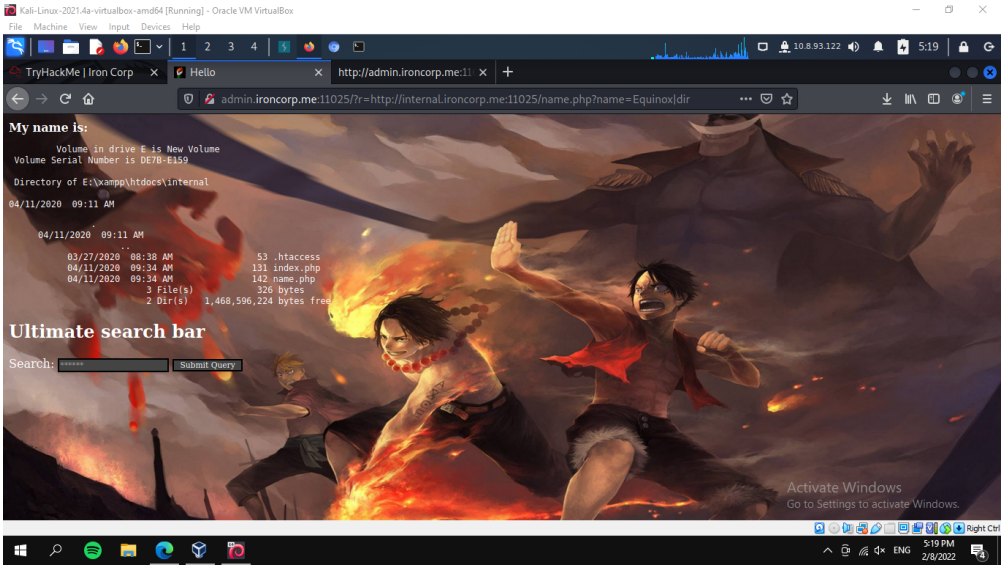
When we add on "/?r=http://internal.ironcorp.me:11025" into the current url, we can see a new message prompted saying "you can find your name here".



When we view source for "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 whats 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

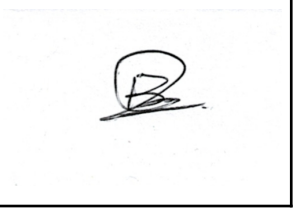
Members Involved:

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