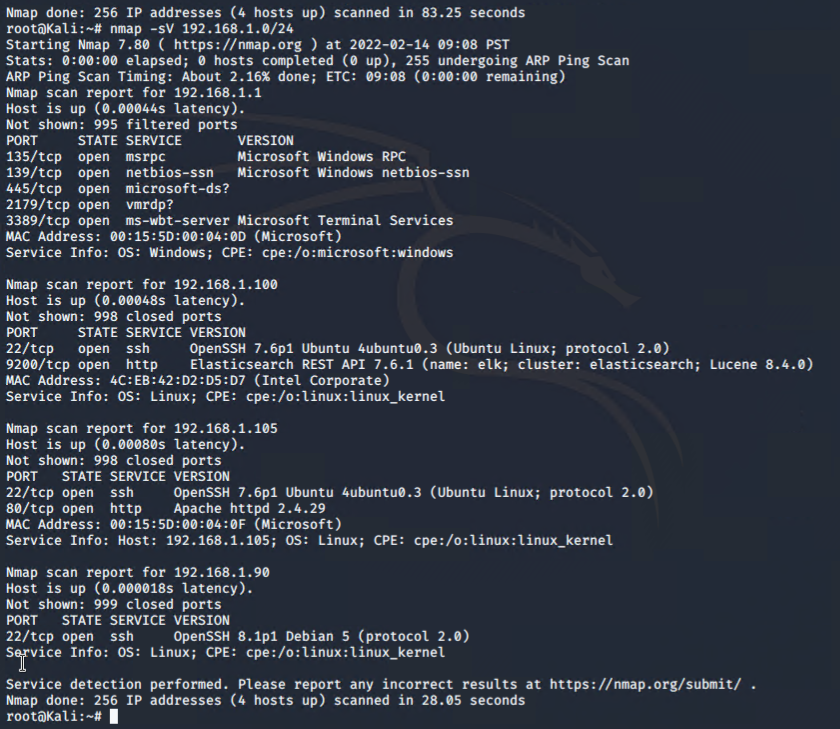
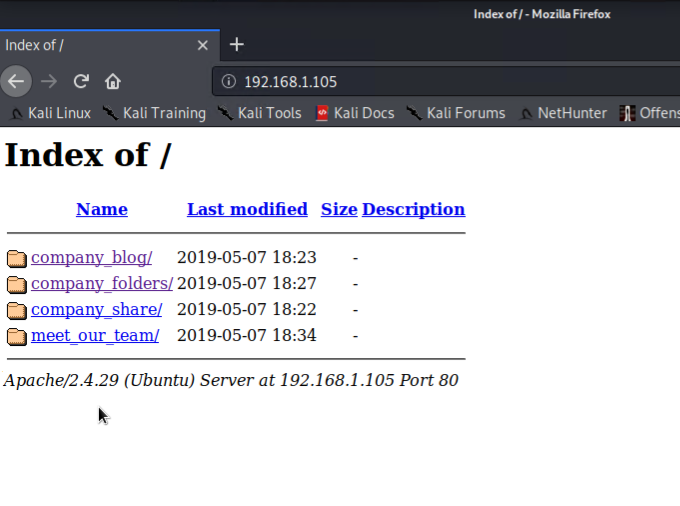
Complete the following to find the flag:

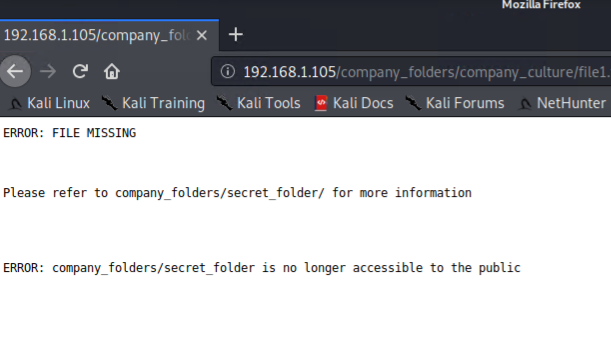
* Discover the IP address of the Linux web server.
  + Linux Web Server: 192.168.1.105



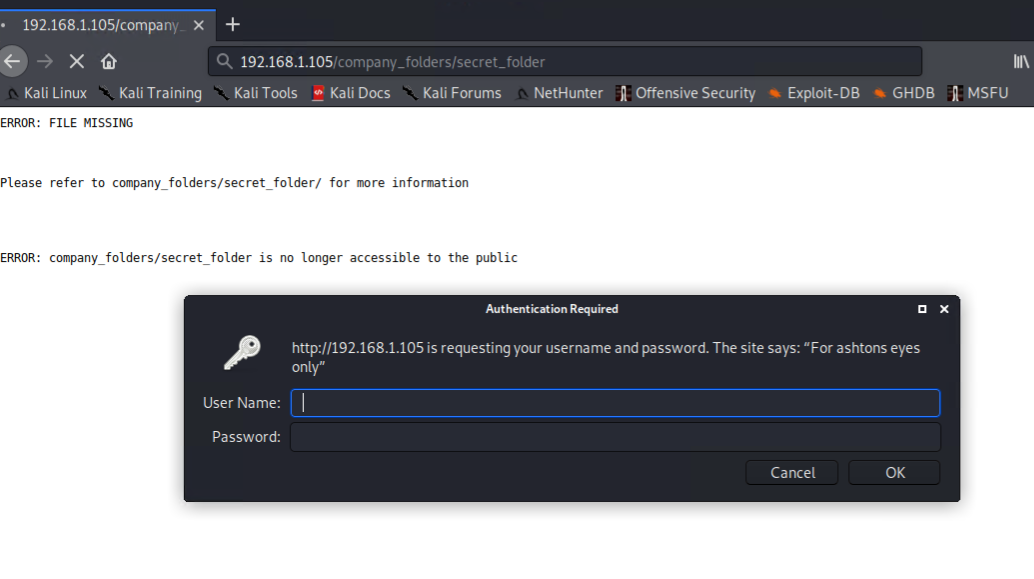
* Entering 192,168.1.105 into a browser comes up with Webdav Page



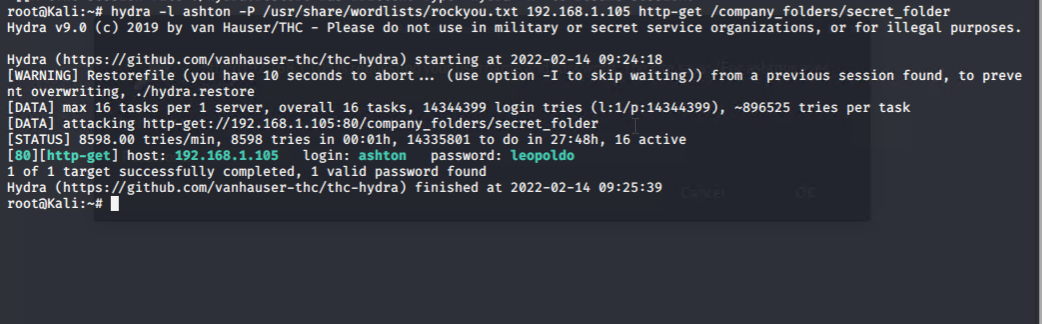
* Locate the hidden directory on the web server.
  + Searching the webdav page you come across a mention of a secret folder page.



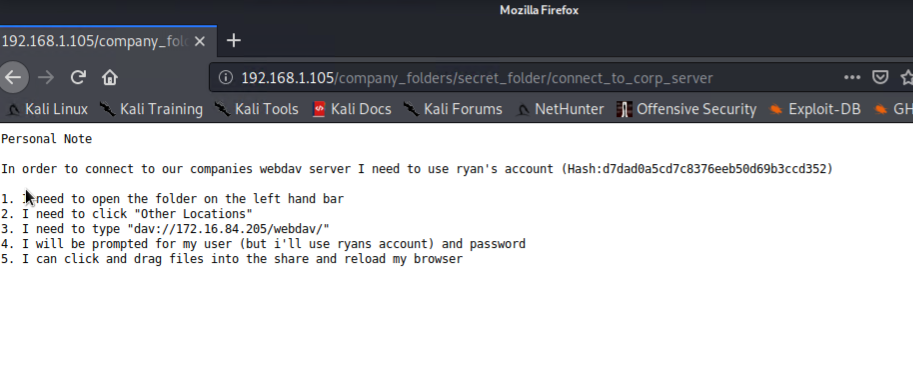
* The secret folder directory requires a prompt



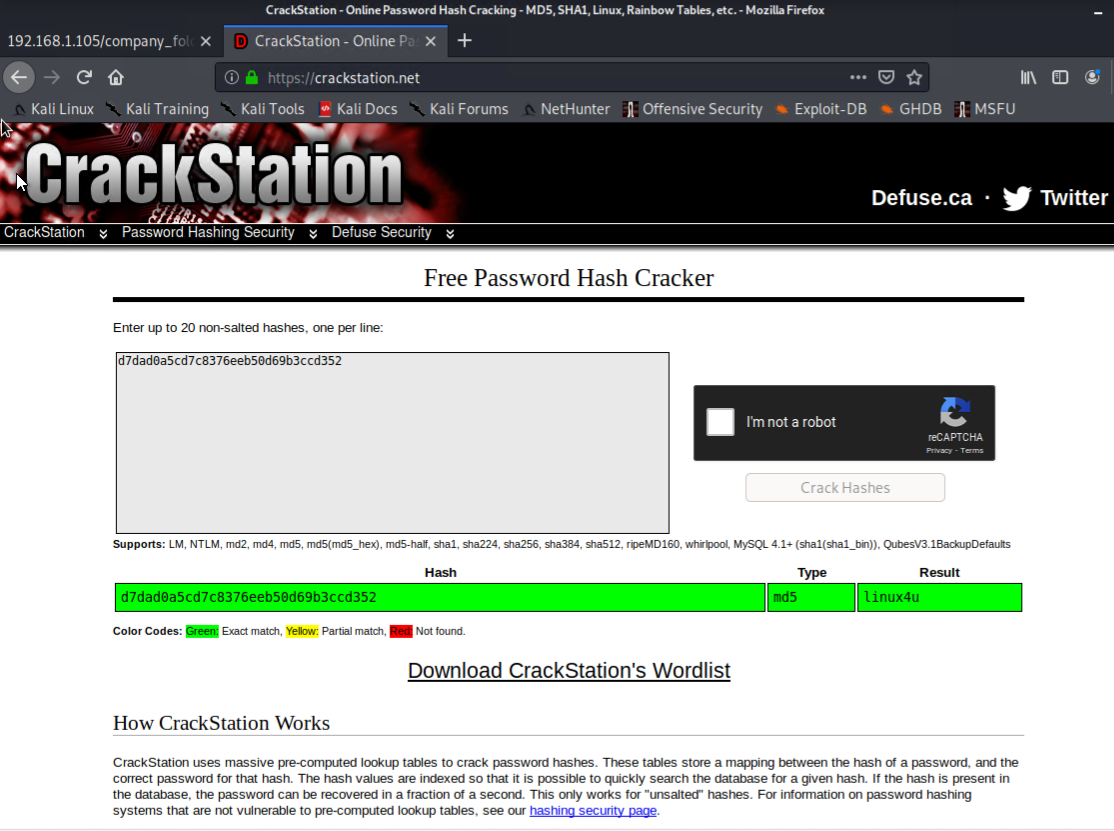
* Using hydra to brute force my way into the directory using ashtons name and the rockyou wordlist to speed up the search.

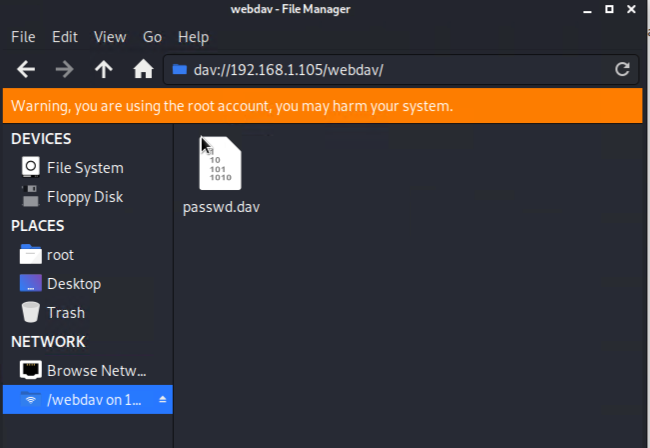


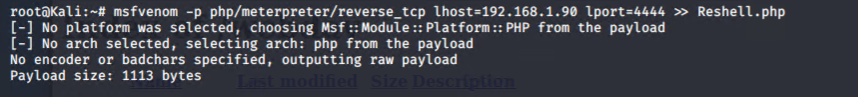
* Connecting to the secret folder webdav directory led me to instructions on how to connect to the webdav server as well as the hash for ryans account.

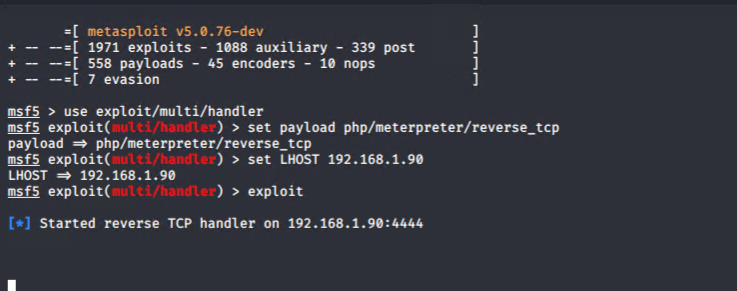


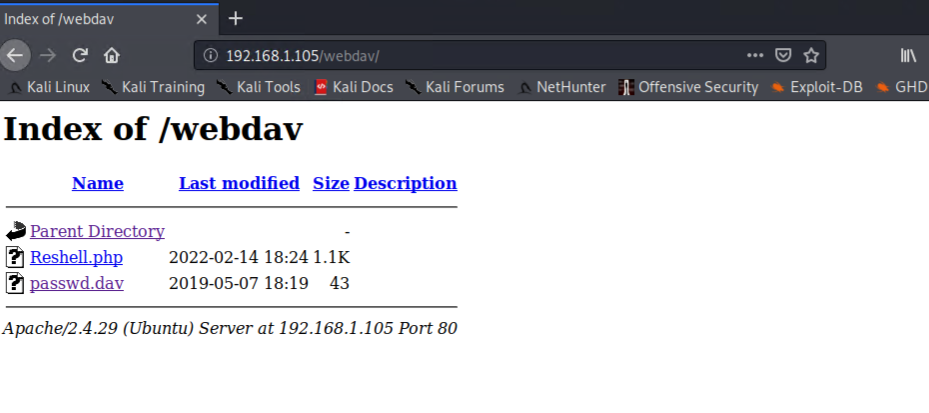
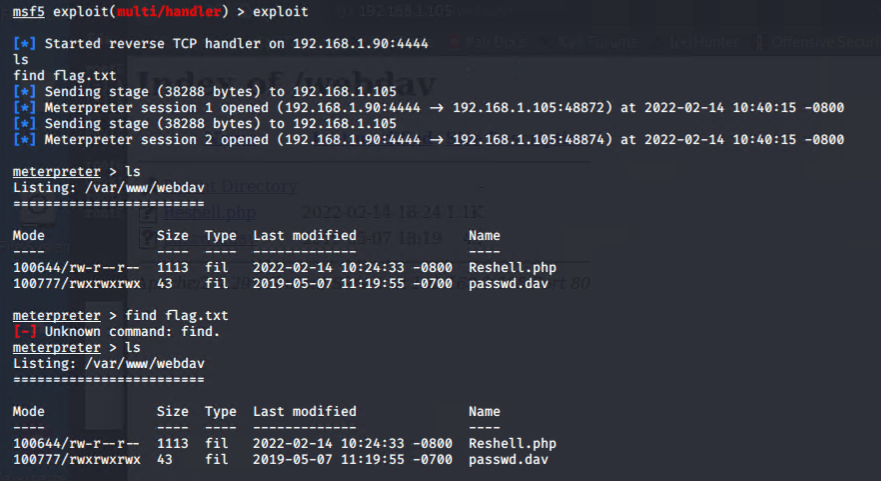
* Using a website called crackstation which contains a free password hash cracker I was able to crack the md5 hash password linux4u.



* Using the Browse Network in my file manager on my vm I typed in webdav address and found the password file.
* I created a reverse shell exploit using msfvenom and ran a listener using meterpreter and the exploit inside the webdav directory.







* After the reverse shell had been put inside the webdav directory I ran the exploit and gained access to the server via the listener.
* The flag was found on the server under flag.txt after dropping into a shell using the shell command and searching the directory for phrase containing “flag”.

