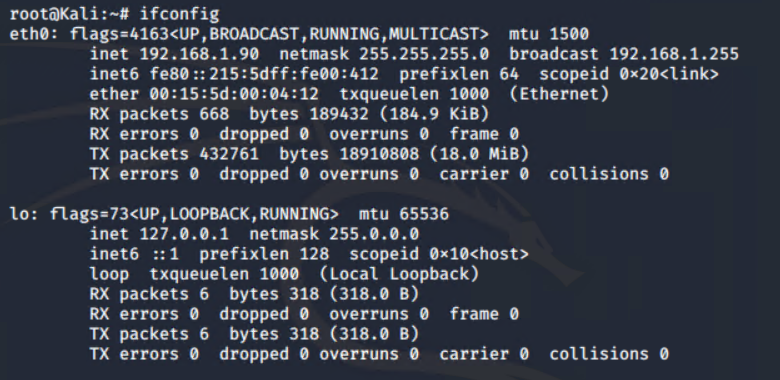
### **Red Vs. Blue Project**

### **Instructions**

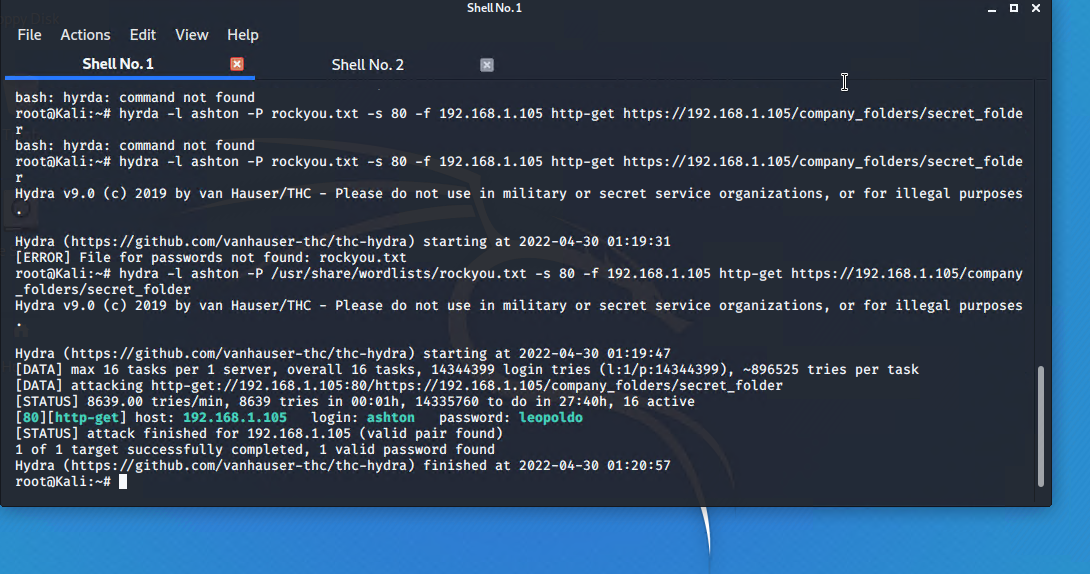
Complete the following to find the flag:

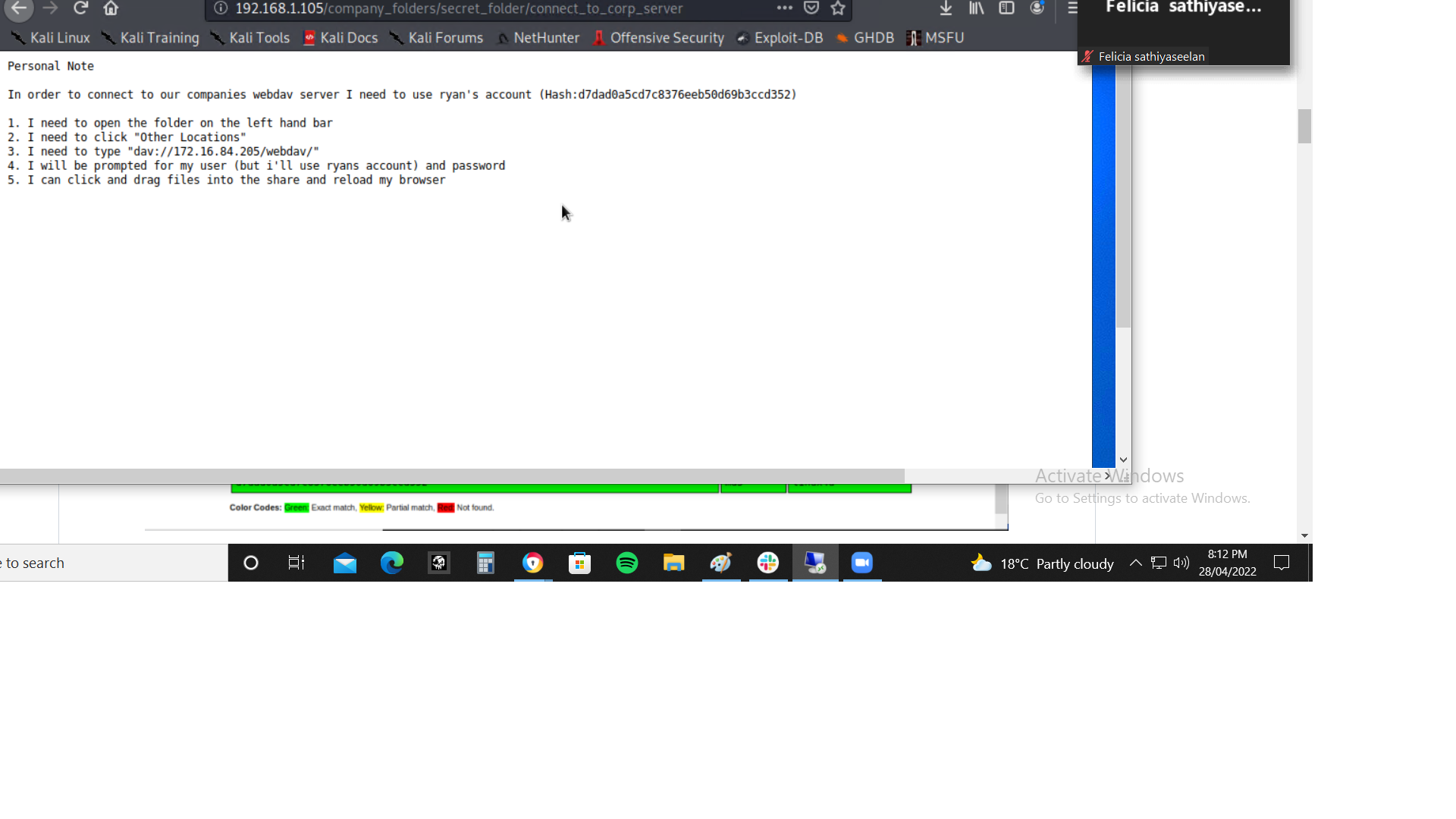
* Discover the IP address of the Linux web server.  
  - **192.168.1.90**

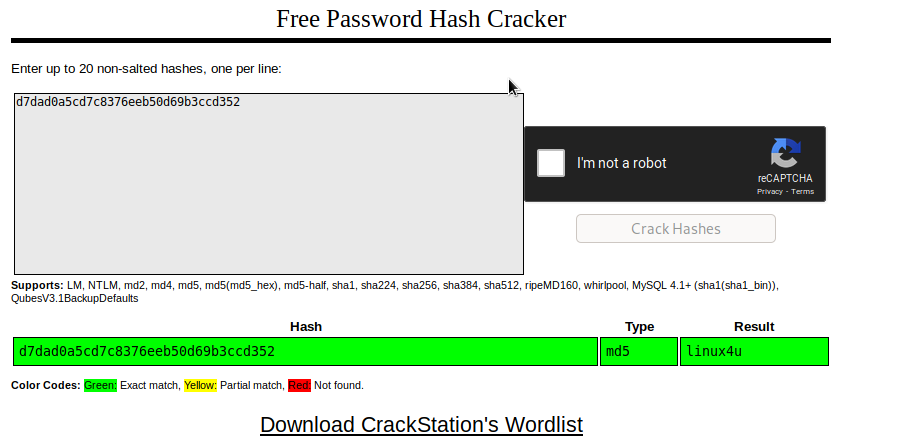


* Locate the hidden directory on the web server.
  + **Hint**: Use a browser to see which web pages will load, and/or use a tool like dirb to find URLs on the target site.

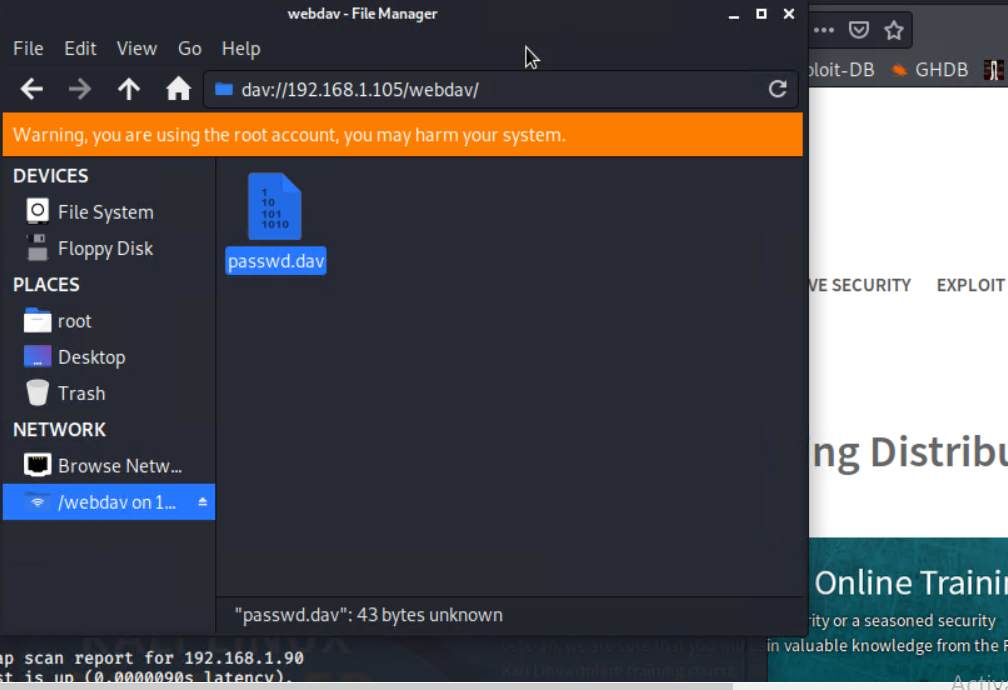
**-**[**https://192.168.1.105/company\_folders/secret\_folder/**](https://192.168.1.105/company_folders/secret_folder/)

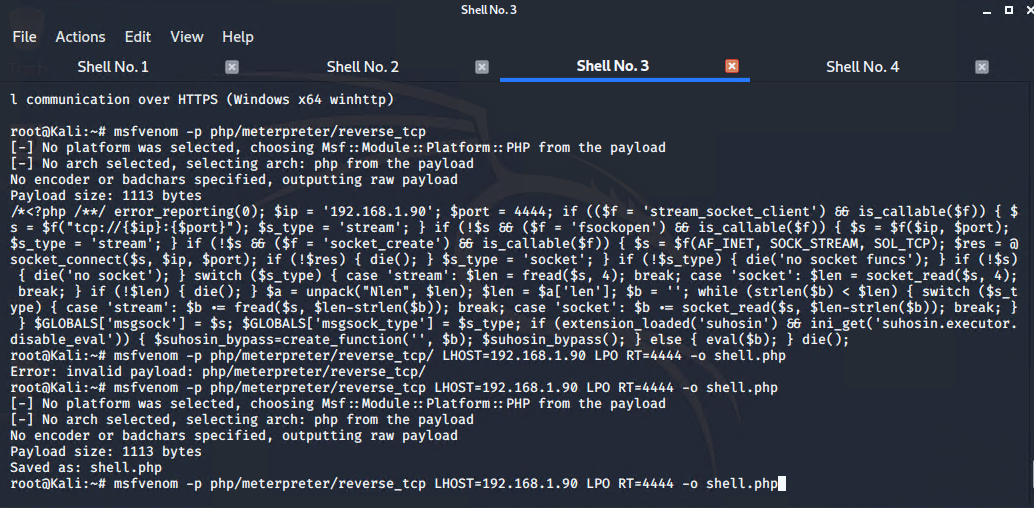
* Brute force the password for the hidden directory using the hydra command:
  + **Hint**: You may need to use gunzip to unzip rockyou.txt.gz before running Hydra.
  + **Hint**: hydra -l <username> -P <wordlist> -s <port> -f -vV <victim.server.ip.address> http-get <path/to/secret/directory>
  + **Hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f 192.168.1.105 http-get** [**https://192.168.1.105/company\_folders/secret\_folder**](https://192.168.1.105/company_folders/secret_folder)
* Break the hashed password with the Crack Station website or John the Ripper.

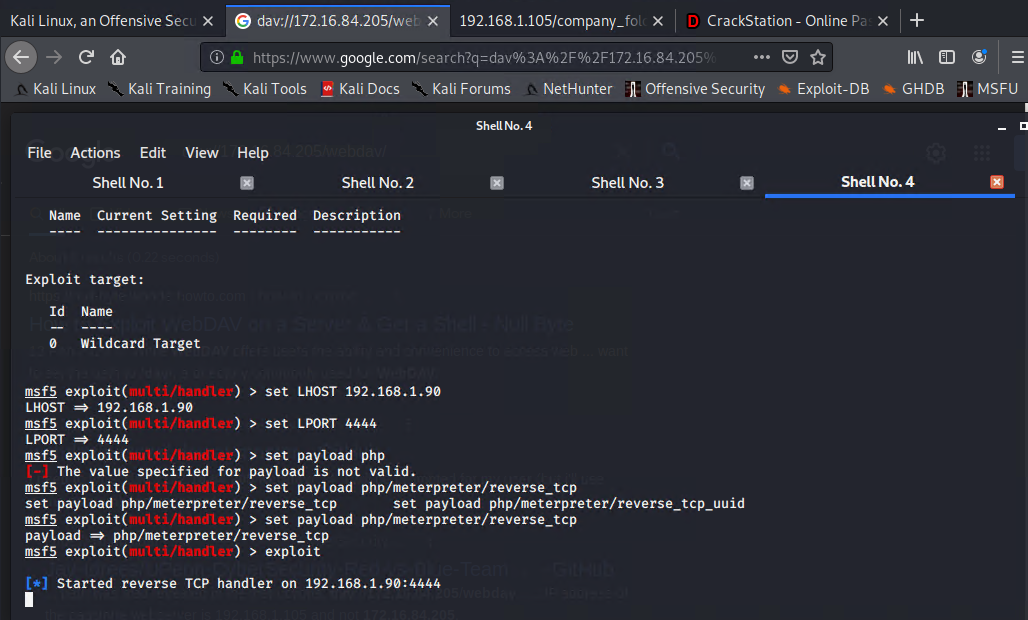
Hash md5, password= **linux4u** via CrackStation



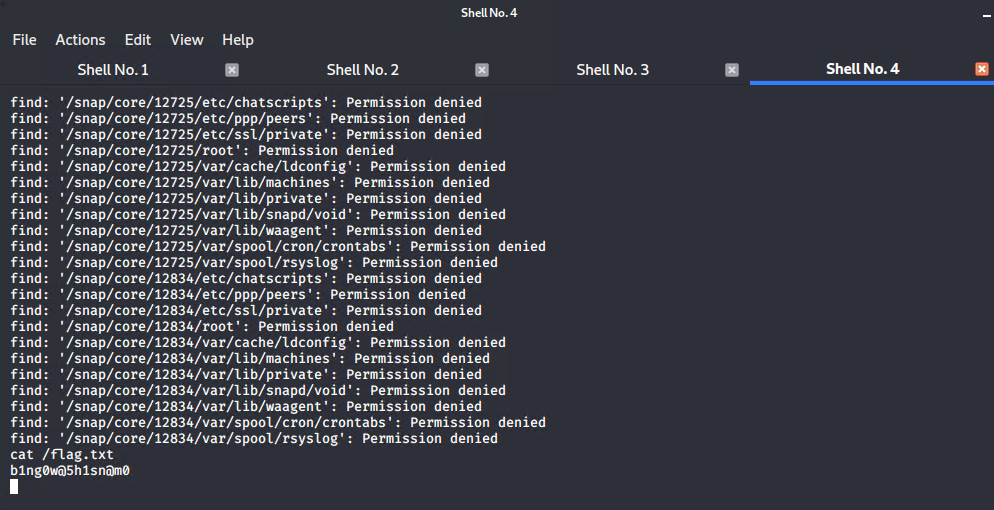
* Connect to the server via WebDav.
  + **Hint**: Look for WebDAV connection instructions in the file located in the secret directory. Note that these instructions may have an old IP Address in them, so you will need to use the IP address you have discovered.



* Upload a PHP reverse shell payload.
  + **Hint**: Try using your scripting skills! MSVenom may also be helpful.
* Execute the payload that you uploaded to the site to open up a meterpreter session.



* Find and capture the flag.



After you have captured the flag, show it to your instructor.

Be sure to save important files (e.g., scan results) and take screenshots as you work through the assessment. You'll use them again when creating your presentation.   
  
BLUE TEAM:

After creating your dashboard and becoming familiar with the search syntax, use these tools to answer the questions below:

1. Identify the offensive traffic.  
   * Identify the traffic between your machine and the web machine:
     + When did the interaction occur? April 28th 2022, at 04:25 AM
     + What responses did the victim send back? 401, 301, 200 ,204
     + What data is concerning from the Blue Team perspective?
2. Find the request for the hidden directory.  
   * In your attack, you found a secret folder. Let's look at that interaction between these two machines.
     + How many requests were made to this directory? At what time and from which IP address(es)?  
       192.168.1.90 -> 192.168.1.105
     + Which files were requested? What information did they contain?  
       /company\_folders/secret\_folder/
     + What kind of alarm would you set to detect this behavior in the future?  
       An alarm that alerts to the use of GET requests from hidden folders.
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack.  
       Remove the directory from this server, ‘rmdir -r’
3. Identify the brute force attack.  
   * After identifying the hidden directory, you used Hydra to brute-force the target server. Answer the following questions:
     + Can you identify packets specifically from Hydra?
     + How many requests were made in the brute-force attack?  
       16772 requests to the ‘secret\_folder’
     + How many requests had the attacker made before discovering the correct password in this one?
     + What kind of alarm would you set to detect this behavior in the future and at what threshold(s)?
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack.
4. Find the WebDav connection.  
   * Use your dashboard to answer the following questions:
     + How many requests were made to this directory?
     + Which file(s) were requested?
     + What kind of alarm would you set to detect such access in the future?
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack.
5. Identify the reverse shell and meterpreter traffic.  
   * To finish off the attack, you uploaded a PHP reverse shell and started a meterpreter shell session. Answer the following questions:
     + Can you identify traffic from the meterpreter session?
     + What kinds of alarms would you set to detect this behavior in the future?
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack.