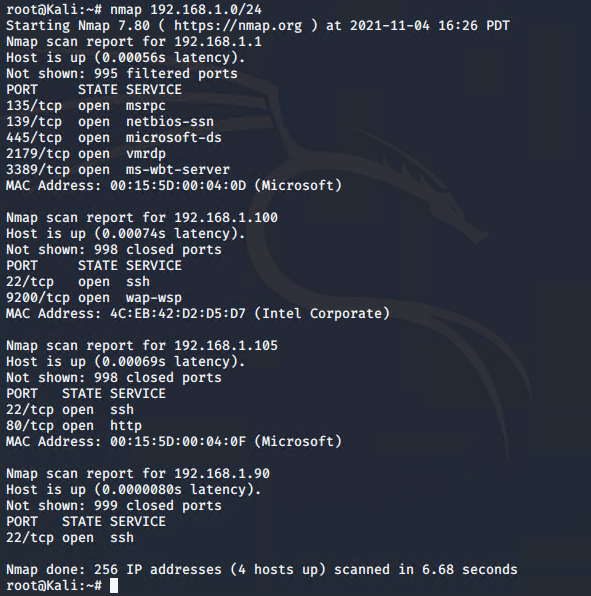
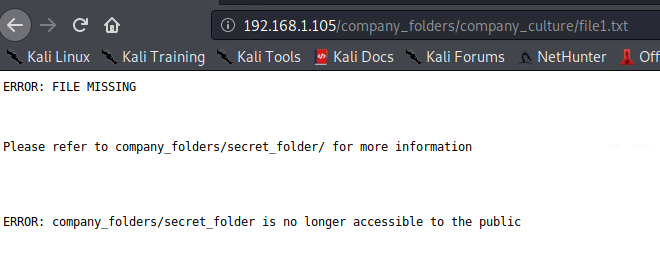
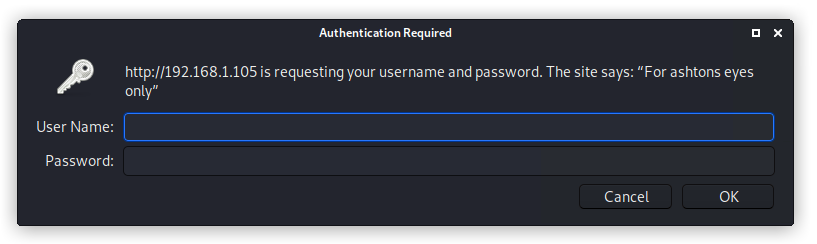
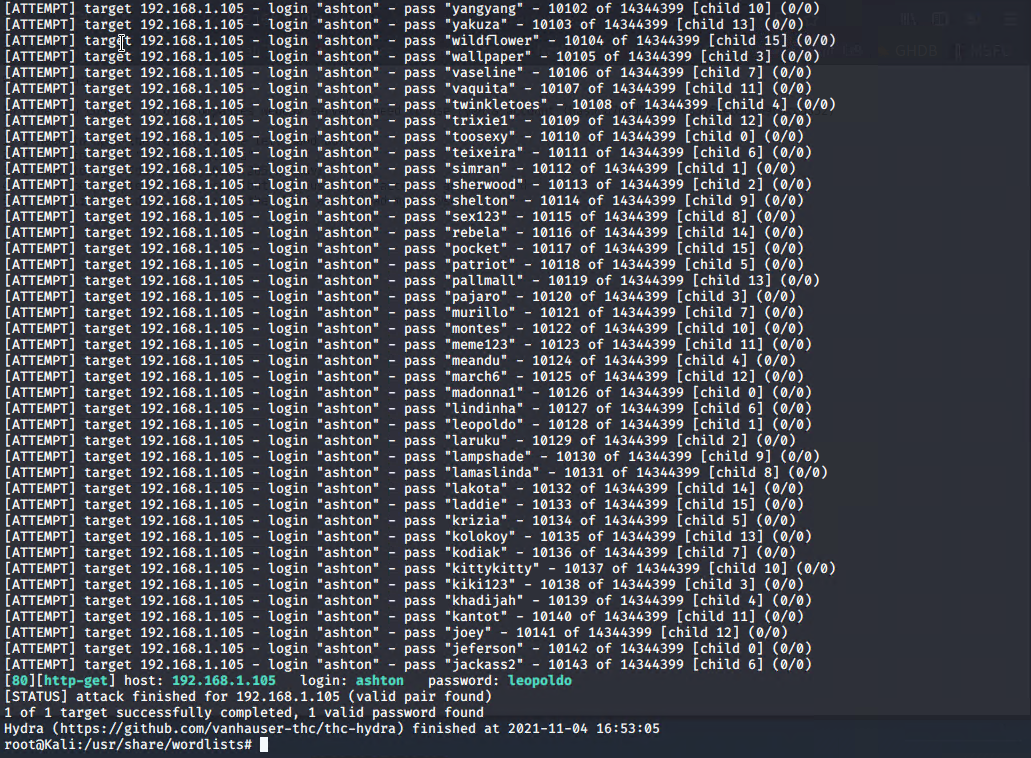
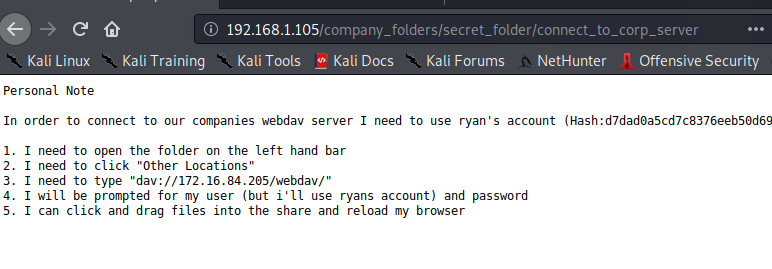
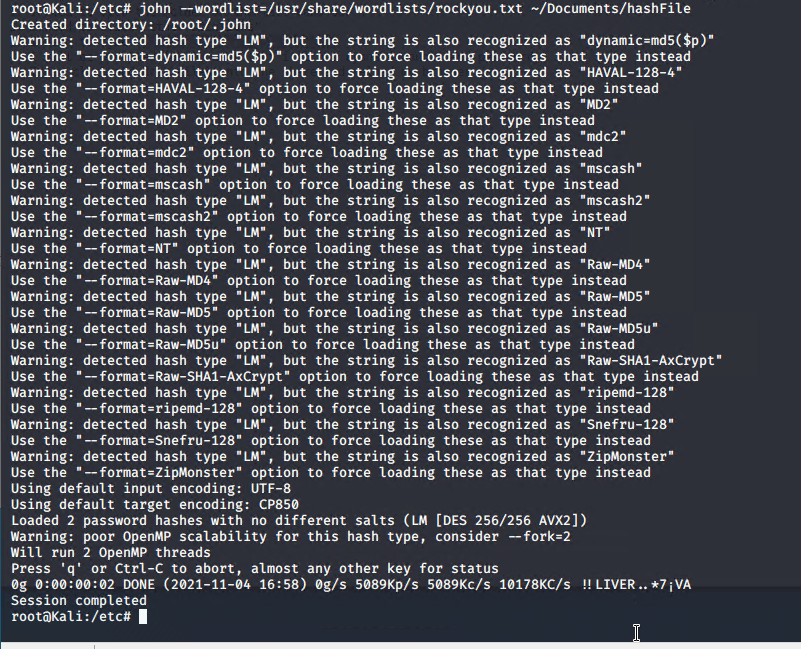
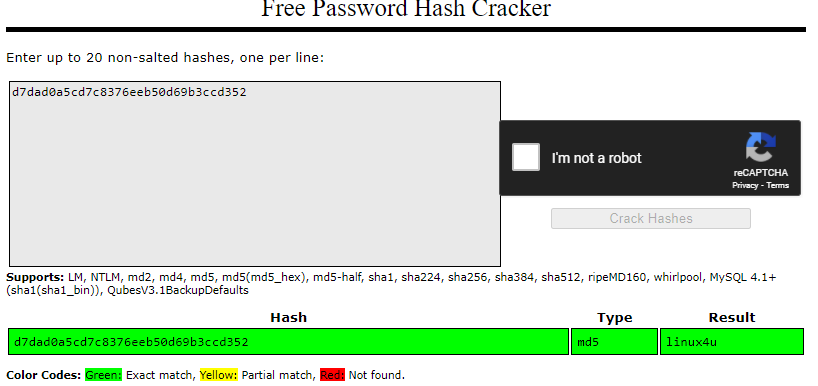
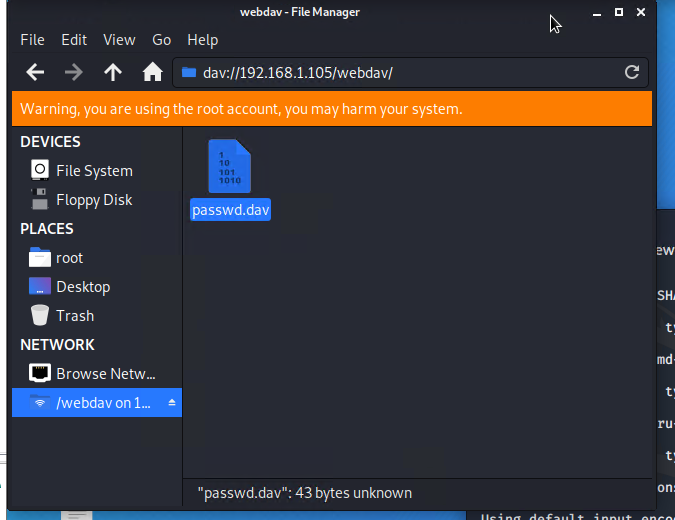
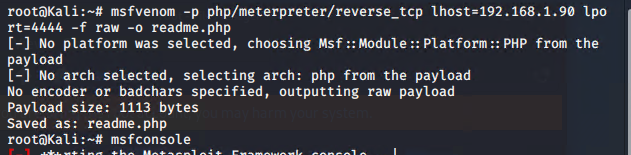
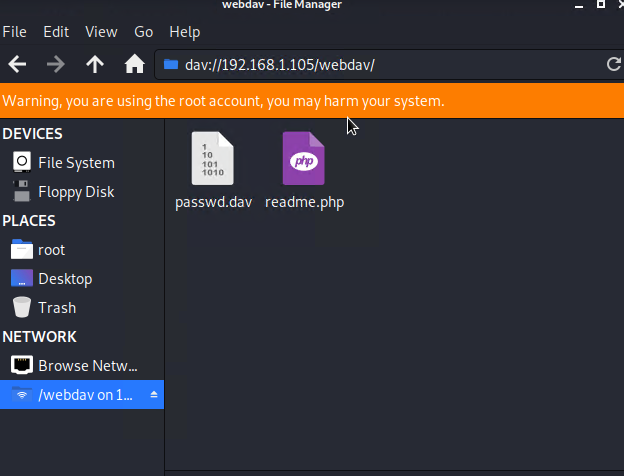
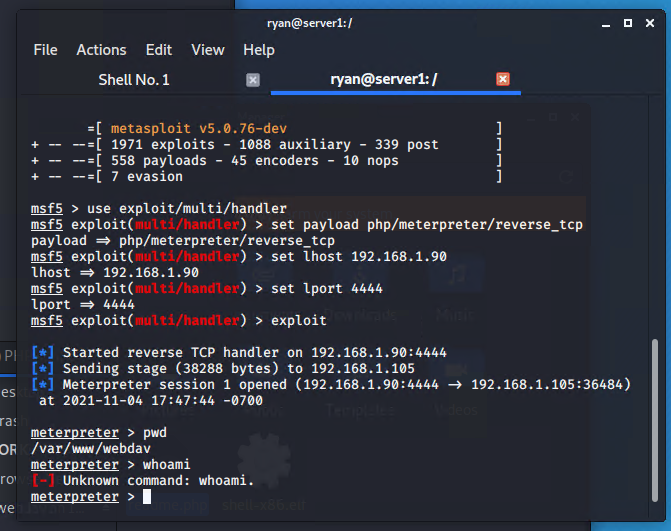
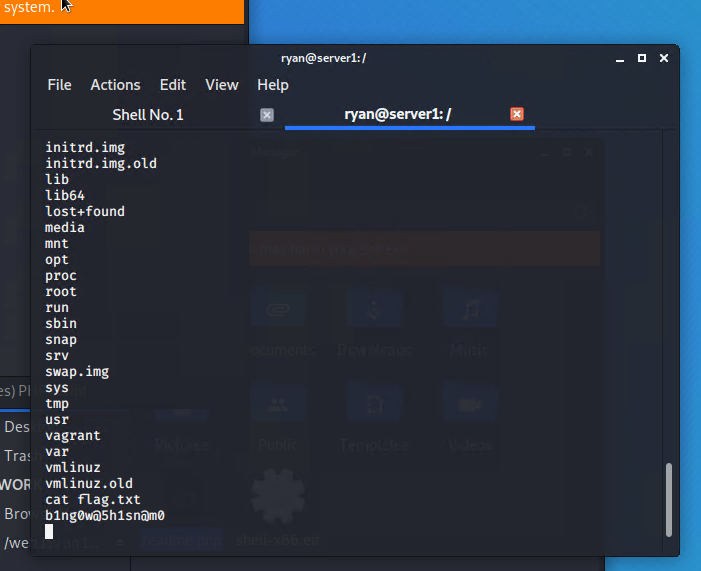
### **Instructions**

Complete the following to find the flag:

* Discover the IP address of the Linux web server.
  + Scan entire network with nmap  
    
  + Service/OS Scan with nmap  
    
* 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.  
    
  + 
* 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>  
    
  + 
* Break the hashed password with the Crack Station website or John the Ripper.  
  
* 
* 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 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.

Logging in with Ryan

