CERT Lab 5 – Password Cracking

Educational Objectives

1. Learn how to crack simple passwords from a zip file and a Linux user account

Tools

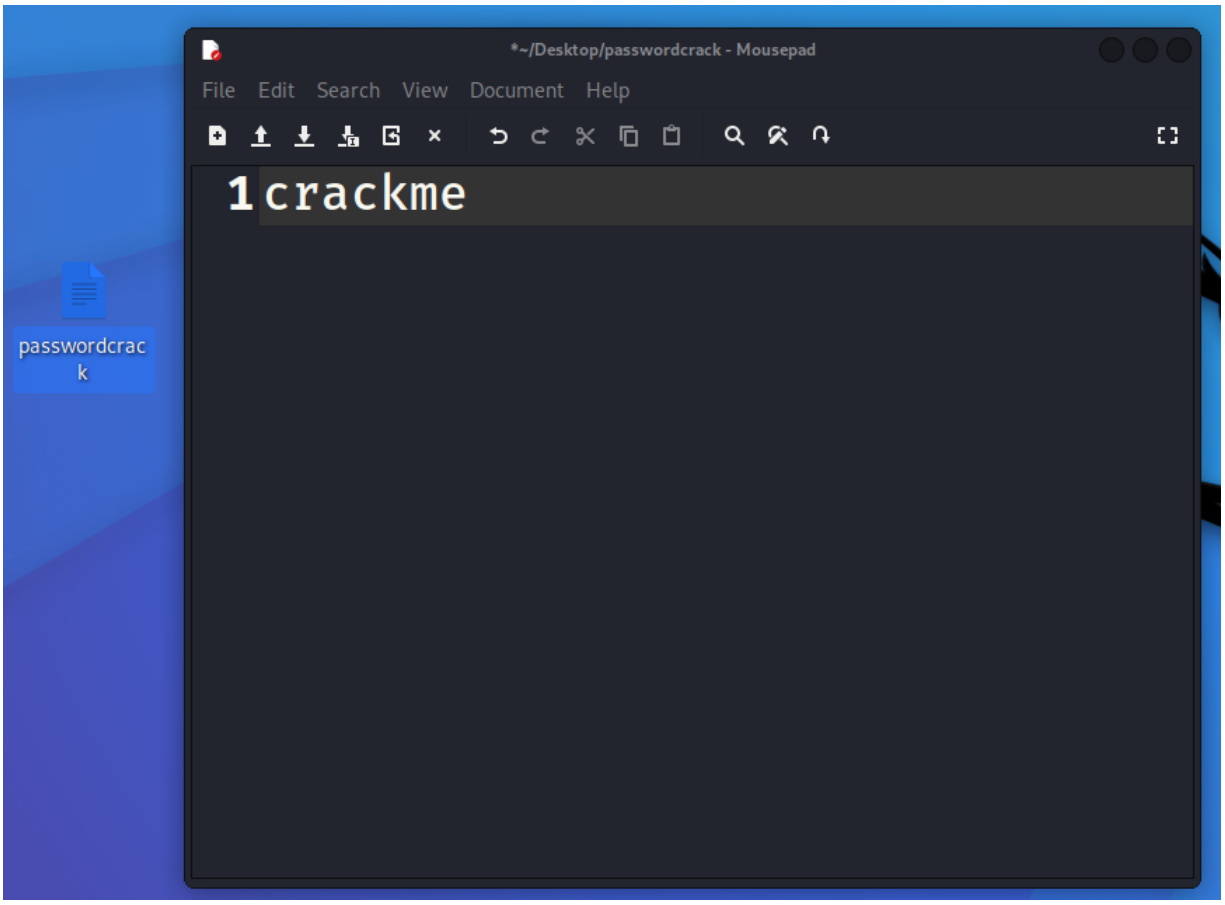
1. Kali Linux VM
    a. John the Ripper

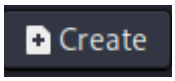
Lab Task 5.1 – Cracking a simple password from a zip file

1. Login to the Kali Linux machine

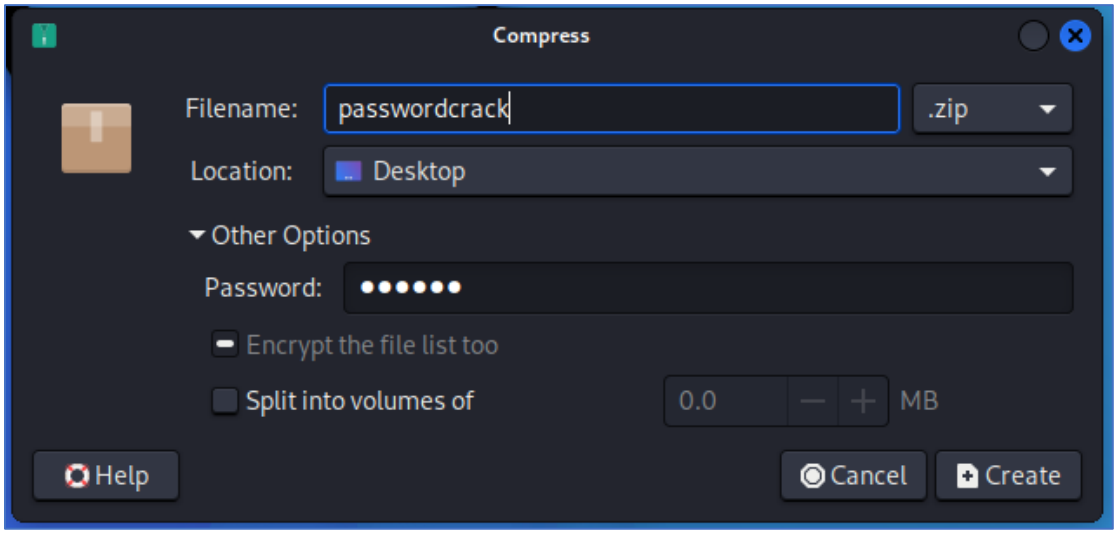
Step 1 – Create dummy file with password

1. Right click on an empty space on desktop and select Create Document > Empty file
    a. Rename the file as "**passwordcrack**"
    b. Double click on the passwordcrack file and type in anything inside this file



2. Zipping the file and insert password
    a. Right click on passwordcrack file and select “Create Archive”
    b. Set the compression type to “.zip”
    c. Click on Other Options
    d. In the Password bar, set the password to “123456”
    e. Once set, click on 

button

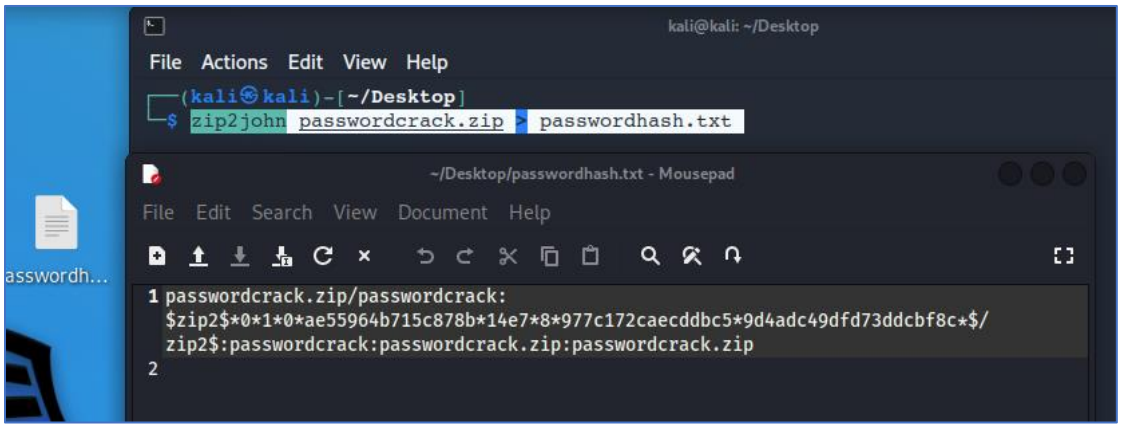


Step 2 – Generate Hash file

1. Open terminal in Desktop
    a. In the terminal type the following command:

```
zip2john passwordcrack.zip > passwordhash.txt
```

    b. This command will generate the hash for the zip file using john the ripper and outputs it as “passwordhash.txt”

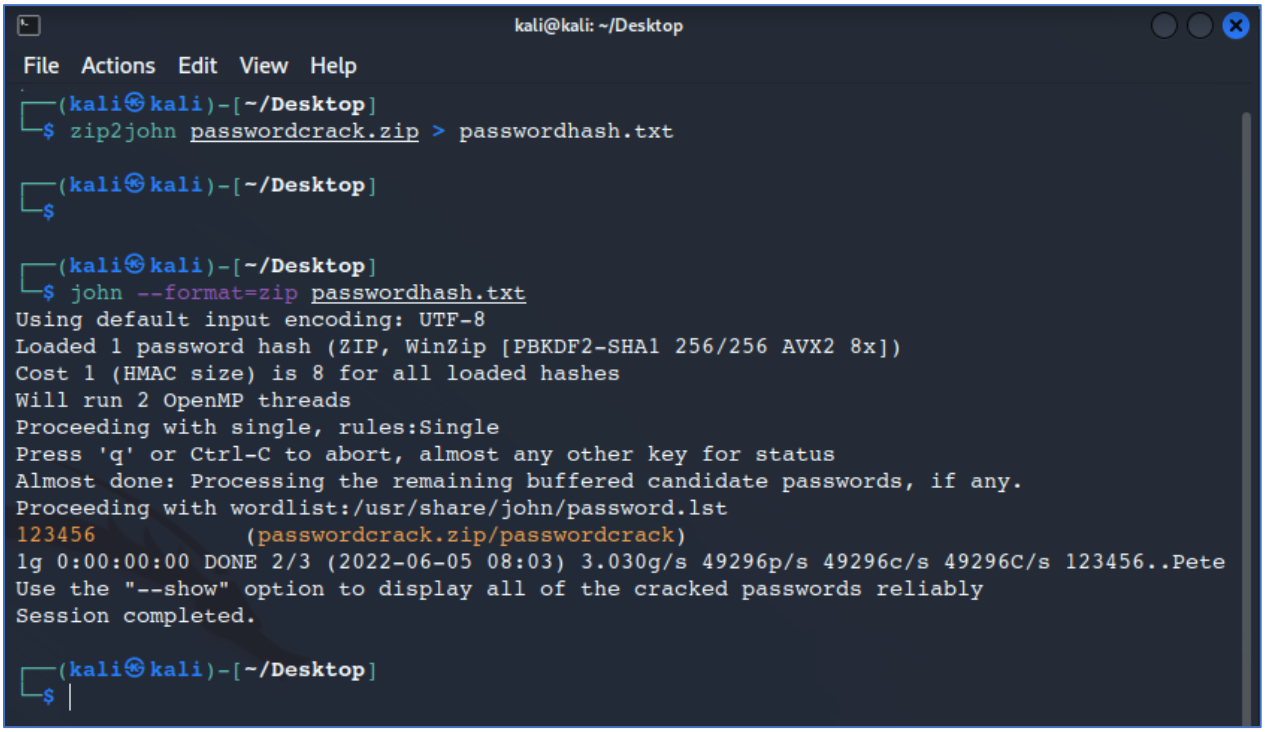


Step 3 – Cracking the password from the hashfile

1. In the terminal, type the following command:

```
john --format=zip passwordhash.txt
```

   a. We can see that the tool has successfully cracked the password in seconds, because the password is simple



Lab Task 5.2 – Cracking a Linux user's password using John

Step 1 – Create a new user account

1. Open terminal and type in **"`sudo su`"** for accessing the root (admin) privileges
2. Enter password
3. Type in the following commands:

```
useradd -r newuser
passwd newuser
```

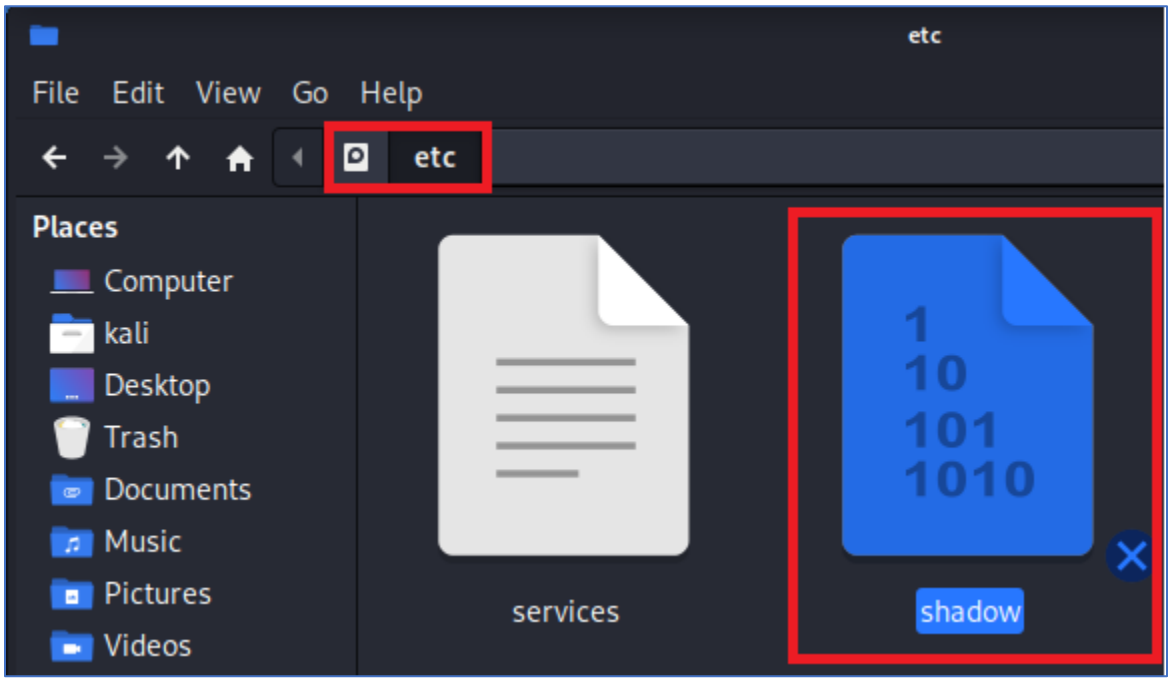
New password : **1234567**

Retype password : **12345467**

Note: If you want to know more about **`useradd`** command, type in **"`useradd -h`"** for help

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo passwd newuser
New password:
Retype new password:
passwd: password updated successfully
```

- The above commands create a new system account (denoted by -r) called 'newuser' with the password '1234567'
- The passwords for Linux users are stored in file called 'shadow' located in the /etc/ directory. This file is encrypted.



Step 2 – Cracking the password from the shadow file

We need to get both /etc/passwd and the shadow file (typically /etc/shadow or /etc/master.passwd), and combine them into one file using "unshadow" (which is supplied with John)

1. Open terminal in Desktop and type the following commands

```
unshadow /etc/passwd /etc/shadow > johninput
```

   i. The unshadow command combines the /etc/passwd and /etc/shadow files into a new file called johninput so John can use this new input to crack the password

2. Type in the next command to crack the password:

```
john --format=crypt johninput
```

Result:

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# john --format=crypt johninput

Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) i
s 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
kali             (kali)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
1234567          (newuser)
2g 0:00:00:06 DONE 2/3 (2022-06-05 10:04) 0.2881g/s 208.2p/s 208.3c/s 208.3C/s leslie..bos
ton
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

- John successfully detected that the password for newuser is 1234567 relatively quickly because the password is simple
- In case John needs a little help with detecting the hash format, we can use a wordlist called rockyou.txt (rockyou.txt contains the most frequently used passwords sorted by frequency. It is not effective against targets with good password policies) and therefore the command to use rockyou wordlist into the above usage is:

```
john --format=crypt --wordlist=/usr/share/wordlists/rockyou.txt
johninput
```

Step 3 – Delete the newly created user account

1. Open terminal as root (**sudo su**)
2. Type the following command

```
userdel -r newuser
```