

~~Password Cracking on Kali Linux~~ p4s5w0rD kR4<kin 0n k4L! L!NuX

Index

1 - Terminology	2
2 - Idea	3
3 - Requirements	3
4 - Objectives	3
5 - Kali Linux	3
6 - Kali Linux Passwords	4
7 - Password Cracking	5
8 - Tools Used	5
9 - Warnings and Disclaimer	5
10 - John The Ripper	6
11 - Procedure for John the Ripper	6 - 7
12 - Results for John The Ripper	8
13 - Johnny	9
14 - Procedure for Johnny	9 - 10
15 - Results for Johnny	11
16 - Conclusion	11
17 - References	12

1 - Terminology

- > **GUI:** Stands for "Graphical User Interface". It is a user interface that includes graphical elements, such as windows, icons, and buttons.
- > **Linux:** Linux is a family of free and open-source software operating systems (examples of other operating systems include Windows and MacOS) built around the Linux kernel. Typically, Linux is packaged in a form known as a Linux distribution for both desktop and server use. The defining component of a Linux distribution is the Linux kernel, an operating system kernel was first released on September 17, 1991, by Linus Torvalds.
- > **Terminal / Command Line:** The command line is a text interface for your computer. It's a program that takes in commands, which it passes on to the computer's operating system to run. From the command line, you can navigate through files and folders on your computer, just as you would with Windows Explorer on Windows or Finder on Mac OS.
- > **Toolkit:** A single utility program, a set of software routines or a complete integrated set of software utilities that are used to develop and maintain applications and databases. There are toolkits for developing almost anything.
- > **Hash / Hashing:** A hash is a function that converts one value to another. Hashing data is a common practice in computer science and is used for several different purposes. Examples include cryptography, compression, checksum generation, and data indexing.

2 - Idea

The idea is to show beginners and people with interest in learning about password cracking how it is done with real tools like John The Ripper and its GUI, Johnny. I will show a demo on how to crack passwords of newly created users with both the command line tool and its GUI. I will also explain more about the password file, what and how data is stored there, and how the toolkit works.

3 - Requirements

If you are a beginner or are not so familiar with password cracking, you will need Kali Linux operating system in order to follow the ideas and procedures step by step. You will also need a decent understanding on how the command line works on UNIX systems and basic computer knowledge such as locating files and menus.

4 - Objectives

The main objective for this project is really to show that passwords in fact can be cracked using Kali Linux powerful tools and to raise awareness of using strong passwords instead of weak, simple ones.

5 - Kali Linux

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. Kali Linux is developed, funded and maintained by Offensive Security, a leading information security training company.

6 - Kali Linux Passwords

Kali Linux passwords are stored in the `/etc/passwd` file in cleartext in older systems and in `/etc/shadow` file in hash form on newer systems. We should expect that the passwords on anything other than old legacy systems to be stored in `/etc/shadow`.

The `/etc/shadow` file stores actual password in encrypted format for user's account with additional properties related to user password. Basically, it stores secure user account information. All fields are separated by a colon (:) symbol. It contains one entry per line for each user listed in `/etc/passwd` file. File fields are as follow:

The diagram shows a line from the `/etc/shadow` file: `vivek:1fnfffc$PgtEYHdicpGOffXX4ow#5:13064:0:99999:7::`. Below this line, six arrows point down to numbers 1 through 6, indicating the fields of the entry:

- 1: Username (vivek)
- 2: Encrypted password (\$1\$fnfffc\$PgtEYHdicpGOffXX4ow#5)
- 3: Days since last change (13064)
- 4: Minimum days between changes (0)
- 5: Maximum days password is valid (99999)
- 6: Warn days before expiration (7)

1. **Username** : It is your login name.
2. **Password** : It is your encrypted password. The password should be minimum 8-12 characters long including special characters, digits, lower case alphabetic and more. Usually password format is set to `idsalt$hashed`, The `$id` is the algorithm used On GNU/Linux as follows:
 1. `1` is MD5
 2. `$2a$` is Blowfish
 3. `$2y$` is Blowfish
 4. `5` is SHA-256
 5. `6` is SHA-512
3. **Last password change (lastchanged)** : Days since Jan 1, 1970 that password was last changed
4. **Minimum** : The minimum number of days required between password changes i.e. the number of days left before the user is allowed to change his/her password
5. **Maximum** : The maximum number of days the password is valid (after that user is forced to change his/her password)
6. **Warn** : The number of days before password is to expire that user is warned that his/her password must be changed
7. **Inactive** : The number of days after password expires that account is disabled
8. **Expire** : days since Jan 1, 1970 that account is disabled i.e. an absolute date specifying when the login may no longer be used.

7 - Password Cracking

To crack or hack a password means the use of various methods used to discover computer passwords. It is usually accomplished by recovering data or to get them through a computer system. A password cracking example can be repeatedly guessing a password with an algorithm until the password is successfully discovered.

Password cracking can be done for several reasons, but the most malicious reason is in order to gain unauthorized access to a computer without the computer owner's awareness. This results in cybercrime such as stealing passwords for the purpose of accessing banking information.

8 - Tools Used

For this project, I will be running Kali Linux as a virtual image of VirtualBox software on my MacBook Pro as the host. I will be using John the Ripper and its GUI, Johnny, on Kali Linux as password cracking toolkits.

9 - Warnings and Disclaimer

Proceed at your own risk, Kali Linux is a professional environment with industry-level tools. Do not attempt the following procedure for malicious ends, this is purely educational penetration testing. I am not responsible for any damages on your side.

10 - John The Ripper

John the Ripper is a free password cracking software tool. Initially developed for the Unix operating system, it now runs on fifteen different platforms. It is one of the most popular password testing and breaking programs as it combines a number of password crackers into one package, autodetects password hash types, and includes a customizable cracker. It can be run against various encrypted password formats including several crypt password hash types most commonly found on various Unix versions, Kerberos AFS, and Windows NT/2000/XP/2003 LM hash. Additional modules have extended its ability to include MD4-based password hashes and passwords stored in LDAP, MySQL, and others.

11 - Procedure for John The Ripper

Additionally to cracking the “root” user password (which is “toor” by default), we will be creating new usernames with new passwords to use them in this demonstration.

> Create new users:

Open the terminal, let's create two new users: “user1” with password “easy” and “user2” with password “stillVeryEasy”.

(Terminal Commands):

```
useradd user1
```

```
Passwd user1
```

(enter “flower” when prompted twice - text will not show up, but it will be recorded when the enter key is pressed)

```
useradd user2
```

```
Passwd user2
```

(enter “1234567” when prompted twice - text will not show up, but it will be recorded when the enter key is pressed)

At this point, your command prompt should look like this:

```
root@kali:~# useradd user1
root@kali:~# passwd user1
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@kali:~# useradd user2
root@kali:~# passwd user2
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

> Test John The Ripper:

By typing the command:

```
john -test
```

you will send the toolkit through a variety of benchmarks tests to estimate how long it will take to crack the passwords on your system.

> Copy the password files to a new file in the Desktop:

The system stores its passwords in /etc/shadow, so what we want to do is copy this file to our current directory along with the /etc/passwd file and store them in file we will call “passwordFile”.

(Terminal Commands):

First, we need to change directory to the Desktop, type:

```
cd Desktop
```

Next, copy the contents of both passwd and shadow files into our new “passwordFile” file, type:

```
cat /etc/passwd > passwordList && cat /etc/shadow >> passwordList
```

You now should have a new file in your desktop called “passwordList”.

> Input the file to John The Ripper:

Finally, let’s input it to John The Ripper, type:

```
john passwordList
```

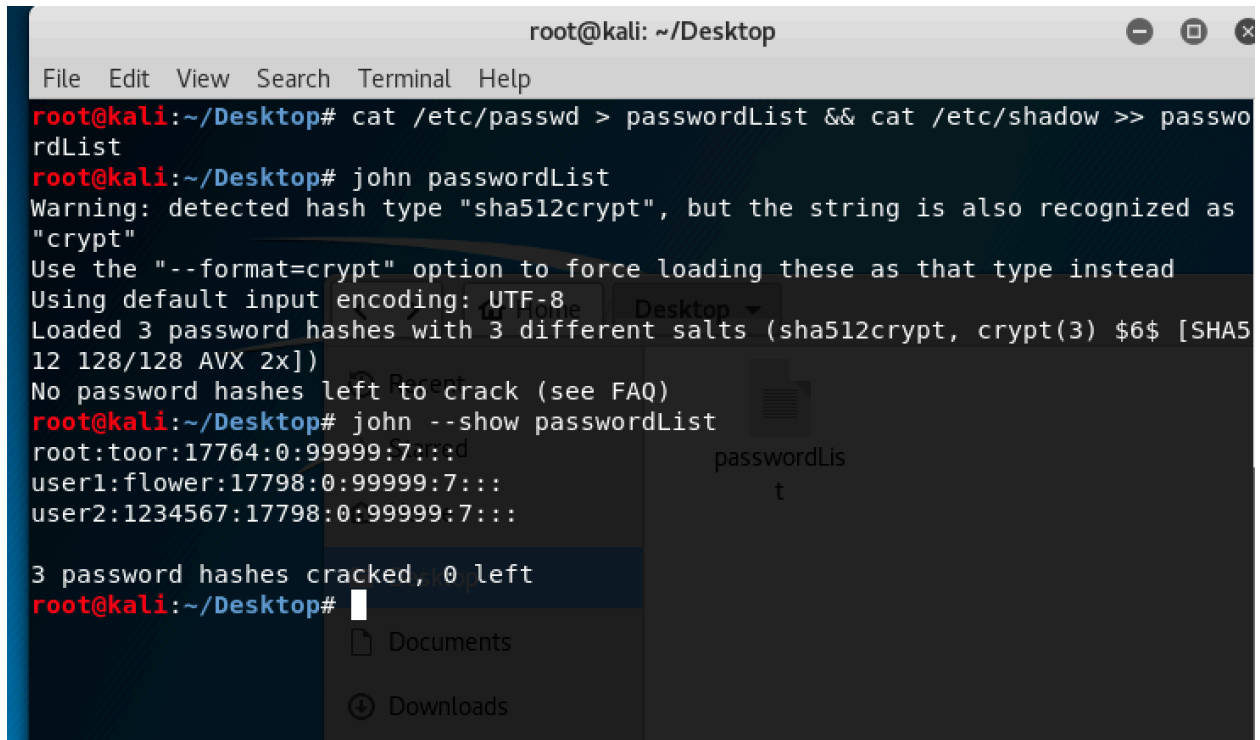
You might have to wait some time, depending on how strong the passwords are.

12 - Results for John The Ripper

Once the toolkit is done cracking the passwords, we can view the results by typing in the terminal:

```
john --show passwordList
```

At this point, our terminal should look similar to this:



```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# cat /etc/passwd > passwordList && cat /etc/shadow >> passwordList
root@kali:~/Desktop# john passwordList
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
No password hashes left to crack (see FAQ)
root@kali:~/Desktop# john --show passwordList
root:toor:17764:0:99999:7:::d
user1:flower:17798:0:99999:7:::
user2:1234567:17798:0:99999:7:::

3 password hashes cracked, 0 left
root@kali:~/Desktop#
```

We can see that John The Ripper effectively cracked our passwords, with the password for the root user being “toor”, user1 being “flower” and user2 being “1234567”.

13 - Johnny

Johnny provides a GUI for the John The Ripper toolkit.

14 - Procedure for Johnny

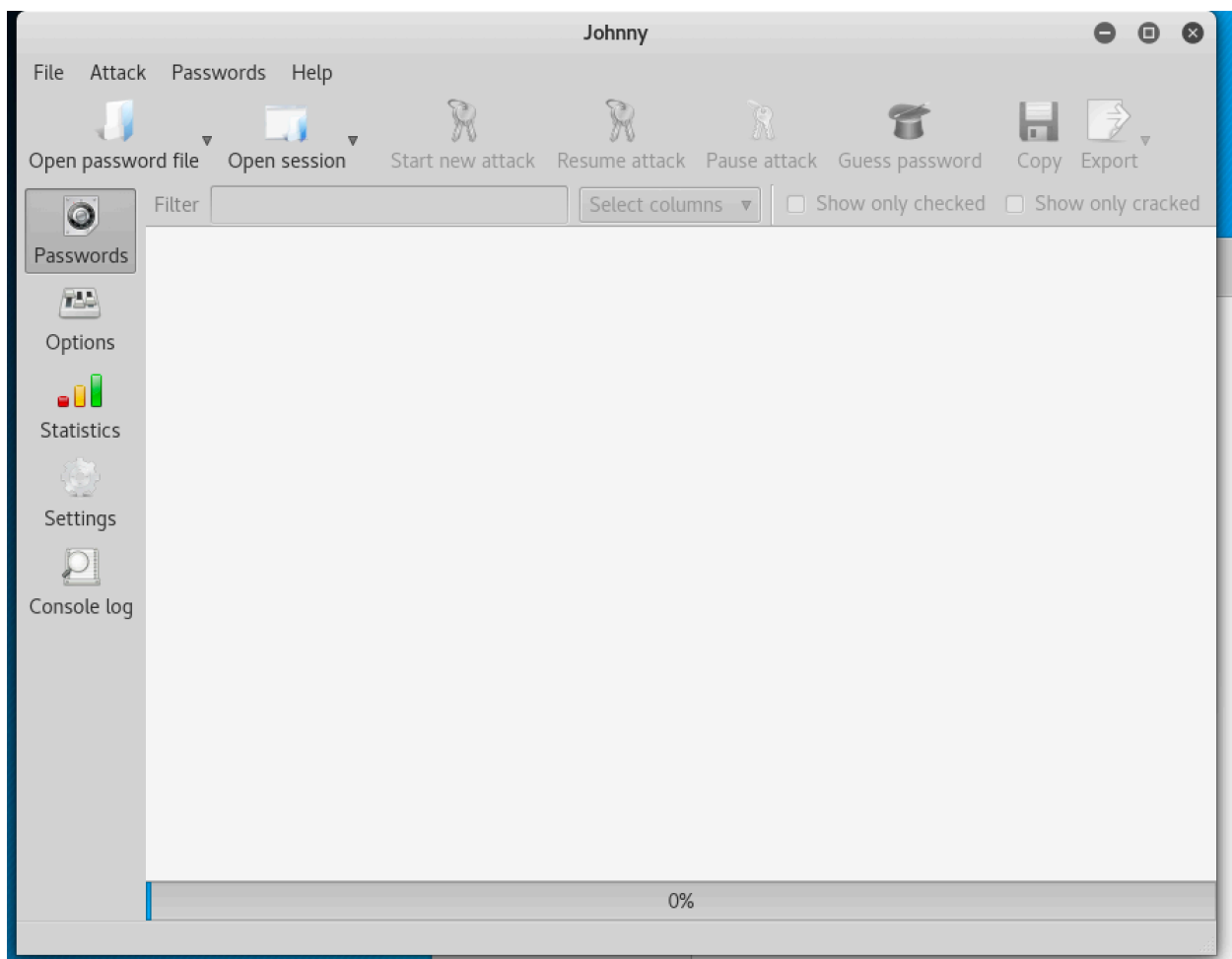
Now that we already have the password file in our desktop as “passwordList”, we just need to give it as input to Johnny.

> **Open Johnny:**

(Terminal Commands):

johnny

You should see the following:



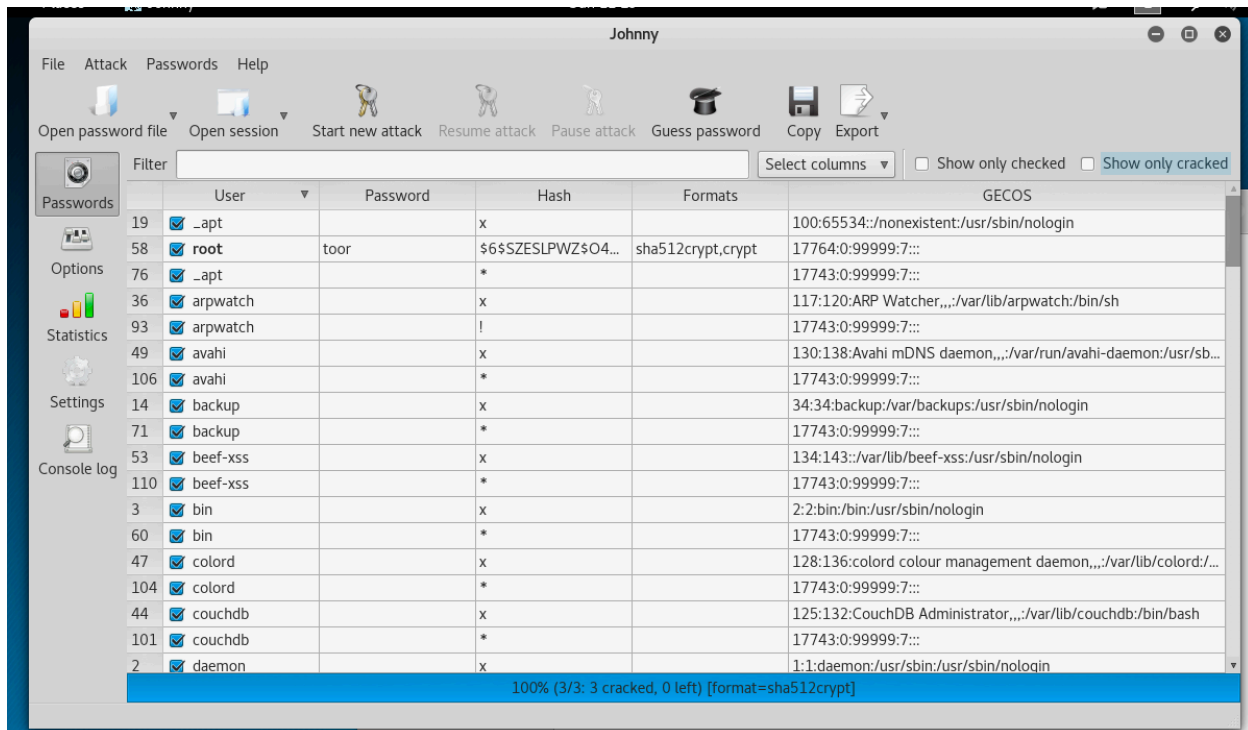
Next,

> click on “Open password file” at the top left of the menu,

> then on the (PASSWD format) option,

> and finally navigate to your Desktop folder and double click the password file that we created earlier, “passwordList”

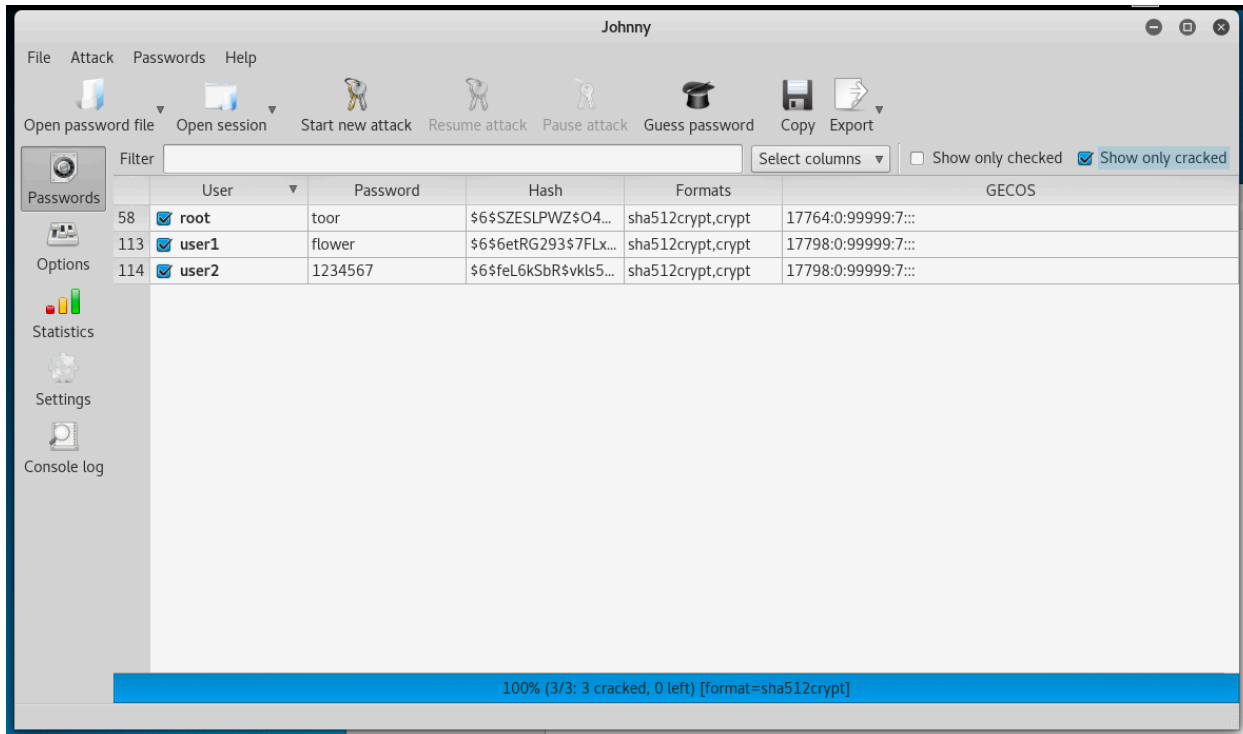
Something like this should up:



On the top right, click and check the box that says “Show only cracked”, the results will show up.

15 - Results for Johnny

Once you are done with the procedure, the following should show up:



Just as expected, Johnny has cracked the passwords for the 3 usernames in the system.

16 - Conclusion

We can conclude that cracking simple passwords is really easy for Kali Linux tools Johnny The Ripper and its GUI. If we had chosen a very strong password, such as “xX-V3rY*5tR0nG*p4sZwORd!-Xx” (ok, maybe that was a bit exaggerated), the toolkit would display a very long ETA (estimated time for cracking the password) and probably would not even be able to crack it. That is why it is important to use long passwords with special characters, alternating between uppercase and lowercase characters, and numbers included.

17 - References

Kali Linux Official Documentation:

> <https://docs.kali.org/introduction/what-is-kali-linux>

Password Cracking:

> <https://www.techopedia.com/definition/4044/password-cracking>

John the Ripper:

> https://en.wikipedia.org/wiki/John_the_Ripper

> <https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-user-passwords-linux-system-0147164/>

Kali Linux passwords:

> <https://www.cyberpratikbha.com/unshadow-the-file-and-dump-linux-password/>

> <https://www.cyberciti.biz/faq/understanding-etcshadow-file/>