~~Password Cracking on Kali Linux~~

p4s5w0rD kr4<kin 0n k4L! L!NuX

CS 486 - Cryptography

Angel Rodriguez

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.

Requirements

> Kali Linux

> Decent understanding on the command line.

Objective

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.

Kali Linux Passwords

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:

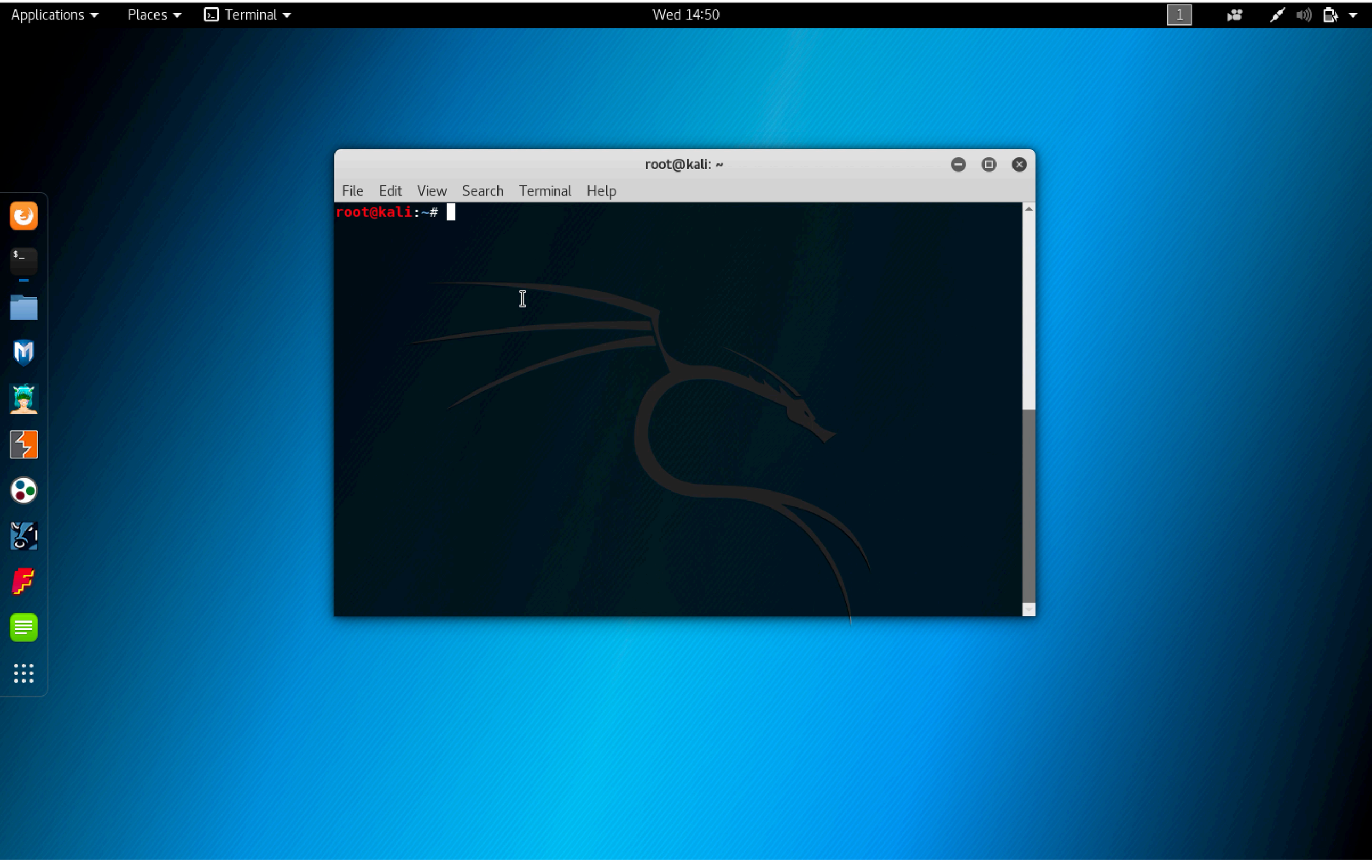
Kali Linux Passwords

1. **Username**
2. **Password** (encrypted)
3. **Last change:** Days since January 1st, 1970 that password was last changed.
4. **Minimum:** The minimum number of days required between password changes.
5. **Maximum:** The maximum number of days the password is valid.
6. **Warn:** Number of days before password is to expire that user is warned that the password must be changed.

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 operating systems. Additional modules have extended its ability to include MD4-based password hashes and passwords stored in LDAP, MySQL, and others.

Demonstration



Conclusion

We can conclude that **cracking simple passwords is really easy for Kali Linux tools** John The Ripper. 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 complex, long passwords** with special characters, alternating between uppercase and lowercase characters, and numbers included.