WEEK-2

Asad Muhammd Channar

DHC-56

Task-3:

Introduction to Password Cracking

Required:

- Install and explore a simple tool like John the Ripper (JTR).
- Perform a basic passwordcracking exercise on weak passwords.
- Write a brief report on the experience and discuss the importance of strong password policies

Introduction to Password Cracking

Password cracking is the process of recovering passwords from data stored in or transmitted by a computer system. It involves using different techniques to exploit weak passwords and gain unauthorized access to systems or sensitive information. Password cracking highlights the importance of implementing strong password policies and security measures, as weak passwords are one of the most common vulnerabilities in systems.

John the Ripper (JTR) is a popular open-source password cracking tool that helps security professionals and ethical hackers test the strength of passwords. It uses different techniques, such as dictionary attacks, brute-force attacks, and rainbow tables, to crack weak passwords.

Steps for the Password Cracking Exercise

- **Installation of John the Ripper (JTR)**:
  - On Kali Linux, John the Ripper comes pre-installed. If it's not installed, you can install it using the following command:

sudo apt-get install john

```
┌──(root㉿kali)-[/home/kali]
└─# sudo apt-get install john

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
john is already the newest version (1.9.0-Jumbo-1+git20211102-0kali7+b1).
john set to manually installed.
The following packages were automatically installed and are no longer required:
  libgphoto2-l10n rwho rwhod
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 675 not upgraded.
```

- **Creating a Simple Password Hash File**:
  - For this exercise, we will create a file with some weak passwords to test how quickly JTR can crack them. First, I generated password hashes using a Linux command:

echo "password123" | openssl passwd -6 > passwords.txt

  - This created a hashed version of the weak password `password123`, which will be used as the target for cracking.

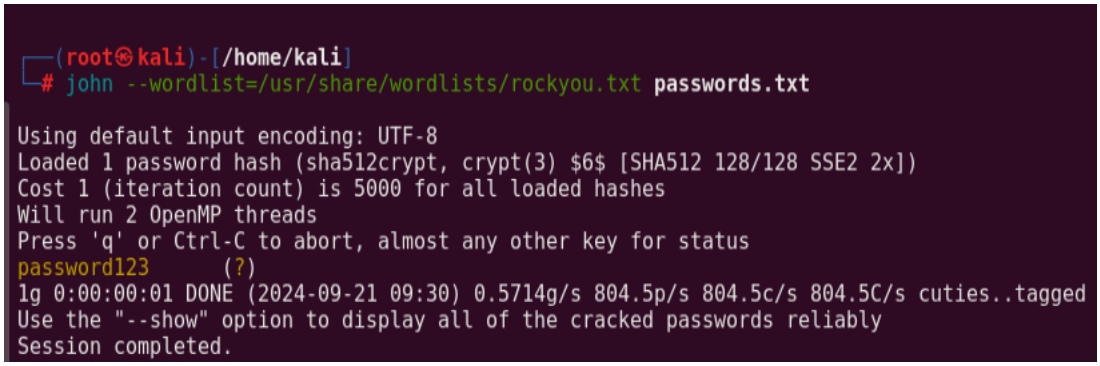
```
┌──(root㉿kali)-[/home/kali]
└─# openssl passwd -6 password123 > passwords.txt


┌──(root㉿kali)-[/home/kali]
└─# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  bash.sh  creating-file.sh  for-loop.sh  logfiles  logs.sh  passwords.txt  table.sh  test.sh  update.sh
```

Running John the Ripper:

- Once the hash file is ready, I ran John the Ripper to attempt cracking the password:

  john --wordlist=/usr/share/wordlists/rockyou.txt passwords.txt

  The wordlist used, `rockyou.txt`, is a commonly used list of weak passwords available on Kali Linux.



Result:

- Within seconds, John the Ripper was able to crack the password `password123` because it was found in the dictionary wordlist. This showed how easily weak passwords can be Report on the Experience

The exercise with **John the Ripper** demonstrated how quickly and easily weak passwords can be cracked. Even passwords that users might consider "strong enough" (like simple combinations of words and numbers) can be compromised in seconds with the right tools and techniques. This highlights the critical importance of using strong, complex passwords that are not easily guessable or found in common wordlists.

Report on the Experience

The exercise with **John the Ripper** demonstrated how quickly and easily weak passwords can be cracked. Even passwords that users might consider "strong enough" (like simple combinations of words and numbers) can be compromised in seconds with the right tools and techniques. This highlights the critical importance of using strong, complex passwords that are not easily guessable or found in common wordlists.