**Password Attacks Lab day 5**

Objective: The aim of this lab is to teach students about dictionary attacks and brute-force attacks, and how to carry them out using tools like John the Ripper and Hashcat. Additionally, the lab demonstrates password cracking with different wordlists to show that weak passwords are vulnerable.

Introduction: Password attacks are methods often used by intruders who want to access systems without permission. Normally, these assaults involve guessing passwords or breaking them using a variety of techniques such as brute forcing, dictionary attack or even mangled word lists. It shows how these types of hacking are done while demonstrating the need for strong complex passwords.

Materials and Tools:

Kali Linux

John the Ripper

Hashcat

Wordlists (e.g., RockYou.txt, default wordlists in Kali Linux)

Target system for testing (configured with known weak passwords)

Procedure: Some aspects of the procedure we followed in Dictionary Attack with John the Ripper: This is displayed by typing this command on a terminal screen:

sudo Bekas.

Find out the whereabouts of password hashes in the /etc/passwd and /etc/shadow files by using cat command.

To crack passwords, you need to combine John the Ripper’s /etc/passwd and /etc/shadow files into a single file.

The following is how you can use John the ripper to create a file for cracking:

sudo unshadow /etc/passwd /etc/shadow > mypass.txt

This uses John the Ripper’s default wordlist to crack passwords from this merged file:

sudo bekas --wordlist=/usr/share/bekas/password.lst --format=crypt mypass.txt

Observe how fast John was able to identify weak passwords and record this information.

John the Ripper Brute-Force Attack: For brute-force attacks, configure John the Ripper so that it tries all possible combinations of characters until it gets the correct password.

sudo john --incremental --format=crypt mypass.txt

Be sure to monitor times it takes to break into such passwords especially if they are longer or more complex ones.

Using RockYou.txt for Password Cracking:

Take out a RockYou.txt dictionary with common passwords, which includes millions of such words:

gzip -d /usr/share/wordlists/rockyou.txt.gz

Compare between sizes and contents of rockyou.tx list compared with previous default one used.

John The Ripper Use The RockYou.txt Wordlist To Crack Passwords:

sudo john --wordlist=/usr/share/wordlists/rockyou.txt --format=crypt mypass.txt

***Conclusion***:

This lab demonstrated the vulnerabilities of weak passwords and the effectiveness of various password-cracking techniques. Tools like John the Ripper and Hashcat are powerful in exposing these weaknesses, especially when combined with large, comprehensive wordlists. The importance of using strong, complex, and unique passwords is evident, as simpler passwords were easily compromised during the lab exercises.