Password Cracking Technique Report

This project aims to assess the effectiveness of different password cracking techniques while underscoring the critical need for strong password policies. Weak passwords present serious security vulnerabilities within systems. Through simulated attacks using widely recognized tools like John the Ripper and Hashcat, the study reveals how effortlessly weak passwords can be exploited**.**

Tools& Environment

Operating system: Kali Linux 2023.2

Tools Used

- John the Ripper
- Hashca

Wordlist: passwords.txt

Hash collection: Password hashes were extracted from simulated Linux system files (/etc/shadow) and database dumps

Cracking Techniques Used

- **Dictionary Attack** – Attempted passwords from precompiled wordlists.
- **Brute Force Attack** – Tried all combinations of characters within a defined length.
- **Hybrid Attack**– Combined dictionary with mutation rules.

Tool Execution:

Result and Analysis

John the Ripper – Dictionary – 2 minutes

Hashcat - Brute force – 15 minutes

conclusion

The findings of this project highlight the vulnerability of weak passwords to modern cracking techniques. The use of tools such as John the Ripper and Hashcat provided a practical demonstration and includes a detailed analysis of recovered passwords by correlating them with their associated usernames. These results emphasize the critical importance of enforcing comprehensive password policies, promoting user awareness, and adopting multi-layered security practices to protect sensitive information in today's threat landscape.