Mini Project Report - Password Cracking using John the Ripper

Title

Password Cracking Using John the Ripper with RockYou Wordlist

Environment: Kali Linux

Tool Used: John the Ripper

Wordlist Used: RockYou.txt

Project Type: Cybersecurity Mini Project

1. Introduction

Password security is a critical aspect of system protection. Weak passwords are often the easiest entry points for attackers. This project demonstrates how a password hash can be cracked using a dictionary attack via John the Ripper, a widely used password-cracking tool. The RockYou wordlist, a famous password list leaked from a compromised site, is used for this dictionary attack.

2. Tools & Setup

- OS: Kali Linux (latest version)

- Tool: John the Ripper (pre-installed on Kali)

- Wordlist: /usr/share/wordlists/rockyou.txt

- Target: Sample password hash file (manually created)

3. Methodology

3.1 Create a User Password Hash File

```
$ echo "testuser:$(openssl passwd -1 password123)" > password.txt
```

3.2 Format Password File

Ensure hash is in the format username:hash.

3.3 Run John the Ripper

```
$ john --wordlist=/usr/share/wordlists/rockyou.txt password.txt
```

3.4 View Cracked Passwords

```
$ john --show password.txt
```

Output:

testuser:password123

4. Results

- Password successfully cracked: Yes

- Time taken: Depends on system resources and password strength

- Cracked password: password123

5. Security Implications

This project demonstrates how easily weak passwords can be compromised. If 'password123' is part of a known wordlist, any attacker with access to password hashes can break it within seconds.

6. Recommendations

- Avoid common passwords or dictionary words.

- Use complex passwords with special characters and length >12.

- Enable 2FA (Two Factor Authentication).

- Monitor login attempts and implement account lockout policies.

7. Conclusion

This mini project highlights the importance of strong password practices. Tools like John the Ripper show how simple it is to crack weak credentials using freely available tools and wordlists. Organizations must adopt better password hygiene and train users on the risks of poor password management.