PASSWORD CRACKING USING JOHN THE RIPPER ON ENCRYPTED HASHES

1. OBJECTIVE

The objective of this project is to demonstrate how encrypted password hashes can be cracked using John the Ripper in Kali Linux. This highlights the security risks of weak passwords and the importance of strong password policies.

2. TOOLS USED

- Kali Linux

- OpenSSL (for generating password hashes)

- John the Ripper (for password cracking)

3. METHODOLOGY

The following steps were followed in the project:

- Step 1: Generate MD5 Hash

```
echo '12345' | openssl passwd -1 -stdin > password.txt
```

- Step 2: View Generated Hash

```
cat password.txt

Example output:
$1$036nYnXg$GABfXH6YreT.jVo2M5tyE0
```

- Step 3: Run John the Ripper

```
john password.txt

John identifies the hash type (md5crypt) and attempts to crack it.
```

- Step 4: Show Cracked Password

```
john --show password.txt

Output:
?:12345
```

4. RESULTS

The password '12345' was successfully cracked using John the Ripper. This demonstrates that weak passwords can be broken in seconds, even when hashed.

5. CONCLUSION

This project highlights the importance of using strong passwords and secure hashing algorithms. Weak passwords such as '12345' can be easily cracked with tools like John the Ripper. For better security, organizations should enforce password complexity rules and use modern hashing algorithms like bcrypt, scrypt, or Argon2.

6. PROJECT SCREENSHOT

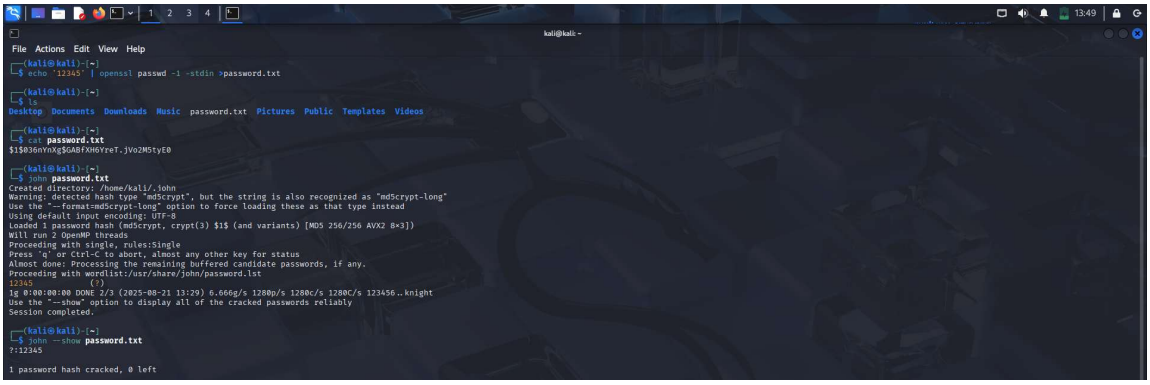

Figure 1: Password cracking demonstration using John the Ripper in Kali Linux.