

# 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
```

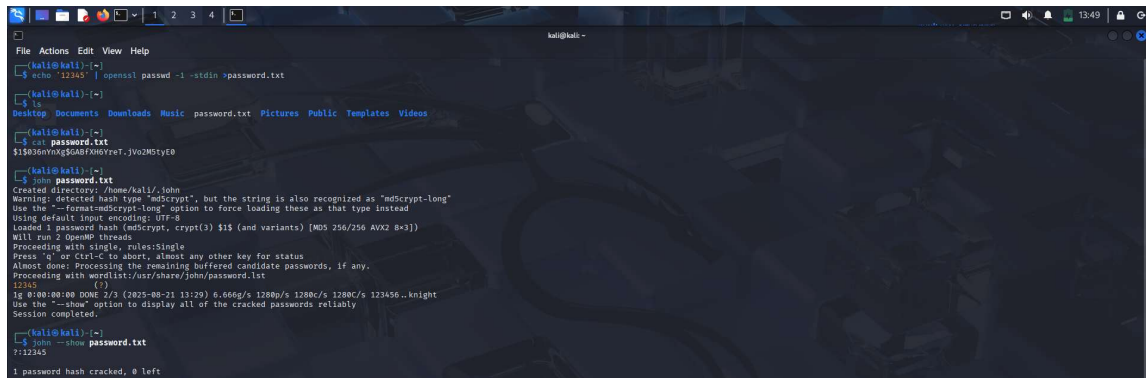
## 4. RESULTS

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



```
kali@kali:~$ echo '12345' | openssl passwd -1 -stdin >password.txt
kali@kali:~$ ls
Desktop  Documents  Downloads  Music  password.txt  Pictures  Public  Templates  Videos
kali@kali:~$ cat password.txt
$1$036nv0xg$GABF0HdyreT.jVoZM5tyE0
kali@kali:~$ john password.txt
Created directory: /home/kali/.john
Warning: detected hash type "mdcrypt", but the string is also recognized as "mdcrypt-long"
Use the --format=mdcrypt-long option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (mdcrypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8+3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
12345
(??)
ig 8:00:00:00 DONE 2/3 (2025-08-21 13:29) 6.666g/s 1280p/s 1280c/s 123456..knight
Session completed.

kali@kali:~$ john --show password.txt
12345
1 password hash cracked, 0 left
```

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