Course Name:	**Information and Cyber Security Laboratory**	**Semester:**	**VII**
Date of Performance:	**10 / 09 / 2025**	**Batch No:**	**B - 1**
Faculty Name:	**Prof. Makrand Kulkarni**	**Roll No:**	**16014022050**
Faculty Sign & Date:		**Grade/Marks:**	**___ / 25**

Experiment No: 6

Title: To perform 'Password Cracking' using John the Ripper on Kali Linux

Aim and Objective of the Experiment:

To perform 'Password Cracking' using John the Ripper on Kali Linux.

COs to be achieved:

CO3: Comprehend concept of cyber-crime, threats, security, cyber offenses and methods used in cybercrime.

Books/Journals/Websites referred:

1. https://www.virtualbox.org/wiki/Downloads
2. https://www.kali.org/docs/introduction/download-official-kali-linux-images/
3. https://www.md5hashgenerator.com/
4. https://youtu.be/frL21o37klM?si=_Hy2QHpppOdoVIaX

Tools required:

Virtual -VM Box, Kali Linux OS and MD5 Hash Generator (online)

Theory:

'Password cracking' is the process of recovering passwords from data that has been stored or transmitted in a hashed form. It is mainly used in penetration testing, forensics, and security auditing to evaluate password strength.

John the Ripper (JtR) is one of the most widely used open-source password cracking tools included in Kali Linux. **John the Ripper** is a fast password cracker developed for Unix-like systems but now supports multiple platforms. It supports numerous password hash types, including:

- Traditional Unix (DES, MD5, SHA-256, SHA-512)
- Windows LM/NTLM hashes
- Web application hashes (MD5, SHA1, etc.)
- Encrypted files and archives.

Applications of John the Ripper

- Security Auditing: Testing organizational password strength.
- Digital Forensics: Recovering lost or forgotten passwords.
- Penetration Testing: Simulating attacker techniques to find weak credentials.

Limitations

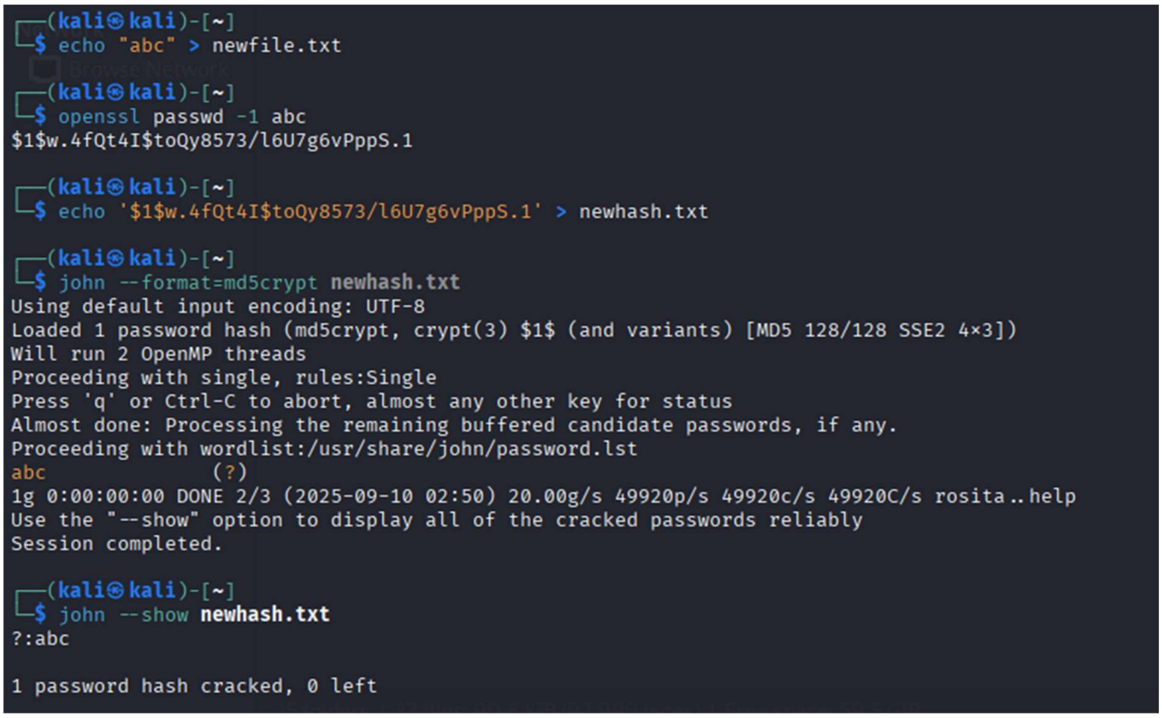
- Time-Consuming: Strong passwords take extremely long to crack.
- Resource Intensive: Brute-force attacks may require powerful hardware (GPU acceleration).
- Legal Restrictions: Unauthorized use of password cracking is illegal

MD5 Hash: Message Digest (MD) Algorithm-5, ‘Message Digest’ is a fixed-size output (hash value) produced from any length of input message and ‘5’ represents fifth version of the algorithm developed by Ronald Rivest in 1991. MD5 is a widely used hashing algorithm that takes an input (like a password, file, or text) and produces a fixed-size output of 32 hexadecimal characters. It is not designed to be reversed; you cannot get the original input directly from the hash. It is used to check data integrity (ensuring files are not altered). Used in older systems for storing passwords.

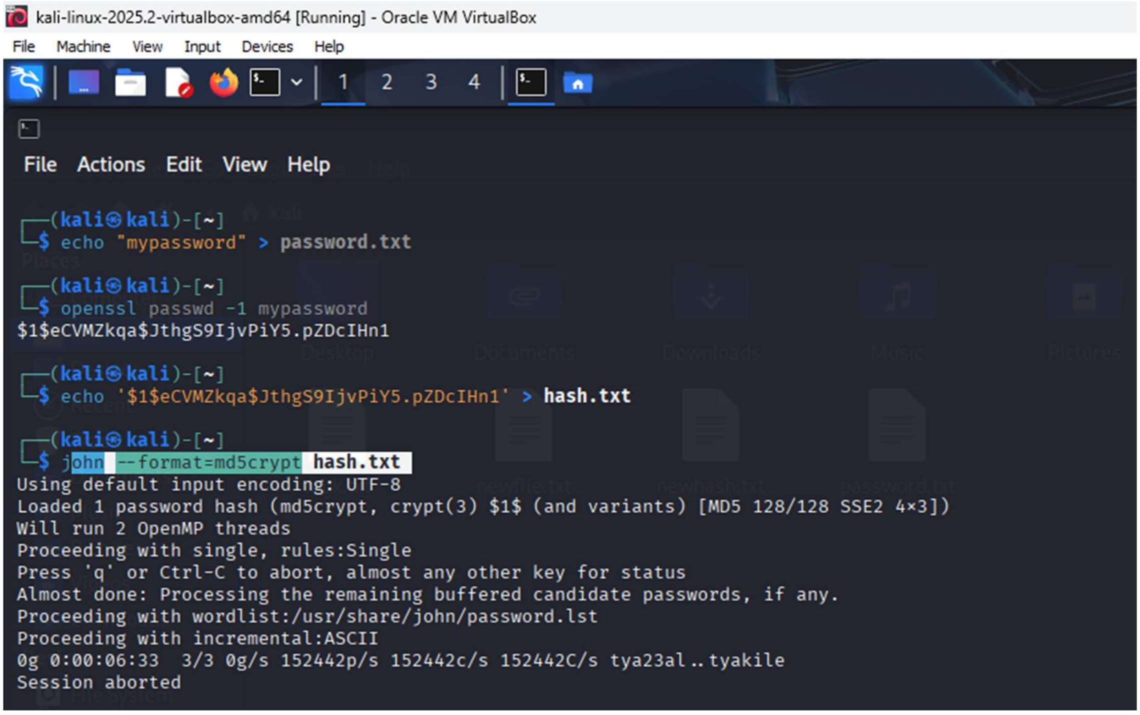
Implementation details:

1. Install the Virtual -VM Box and Kali Linux OS.
2. In Kali Linux create .txt file using ‘touch’ command on desktop.
3. Using MD5 online generator, generate hash value of the password.
4. Use ‘echo’ command to save this has in the .txt file made in step1.
5. Ensure the text written in .txt file using ‘cat’ command.
6. Use ‘John the Ripper’ to crack the password using its command.
   John --format=raw-md5   .txt
7. Take the screenshots and submit.

Output / Screenshots:



```
┌──(kali㉿kali)-[~]
└─$ echo "abc" > newfile.txt

┌──(kali㉿kali)-[~]
└─$ openssl passwd -1 abc
$1$w.4fQt4I$toQy8573/l6U7g6vPppS.1

┌──(kali㉿kali)-[~]
└─$ echo '$1$w.4fQt4I$toQy8573/l6U7g6vPppS.1' > newhash.txt

┌──(kali㉿kali)-[~]
└─$ john --format=md5crypt newhash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 SSE2 4×3])
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
abc              (?)
1g 0:00:00:00 DONE 2/3 (2025-09-10 02:50) 20.00g/s 49920p/s 49920c/s 49920C/s rosita..help
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$ john --show newhash.txt
?:abc

1 password hash cracked, 0 left
```



kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ echo "mypassword" > password.txt

┌──(kali㉿kali)-[~]
└─$ openssl passwd -1 mypassword
$1$eCVMZkqa$JthgS9IjvPiY5.pZDcIHn1

┌──(kali㉿kali)-[~]
└─$ echo '$1$eCVMZkqa$JthgS9IjvPiY5.pZDcIHn1' > hash.txt

┌──(kali㉿kali)-[~]
└─$ john --format=md5crypt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 SSE2 4×3])
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
Proceeding with incremental:ASCII
0g 0:00:06:33  3/3 0g/s 152442p/s 152442c/s 152442C/s tya23al..tyakile
Session aborted
```

Post Lab Subjective/Objective type Questions:

1. **What are the ethical and legal considerations of using John the Ripper for password cracking?**

Ethical Use

• Authorized Testing Only: Use it strictly on systems you own or have explicit permission to test.

• Responsible Disclosure: If you discover weak passwords or vulnerabilities, report them privately to the system owner rather than exploiting them.

• Professional Integrity: Ethical hackers and security professionals are expected to follow codes of conduct that prioritize user privacy and system integrity.

Legal Risks

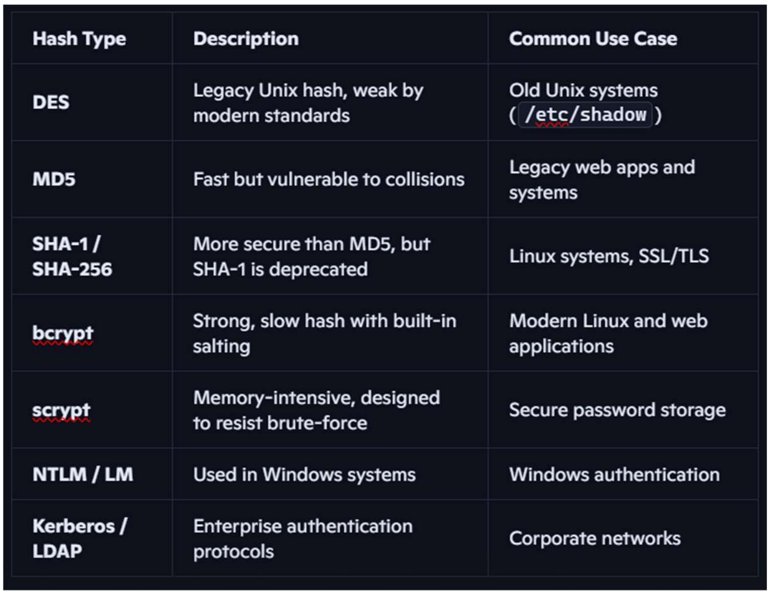
• Unauthorized Access: Cracking passwords on systems without permission is illegal under laws like the Computer Fraud and Abuse Act (CFAA) in the U.S. and similar laws worldwide.

• Privacy Violations: Even if a password is weak, exploiting it without consent breaches privacy and can result in criminal charges.

• Penalties: Misuse can lead to fines, imprisonment, and damage to your professional reputation.

In short: use John the Ripper only in ethical hacking scenarios, such as penetration testing with client consent or academic research in controlled environments.

2. **What types of password hashes can John the Ripper crack, and how are these hashes obtained in Linux systems?**
John the Ripper supports a wide range of hash algorithms, from legacy to modern:



Hash Type	Description	Common Use Case
DES	Legacy Unix hash, weak by modern standards	Old Unix systems (`/etc/shadow`)
MD5	Fast but vulnerable to collisions	Legacy web apps and systems
SHA-1 / SHA-256	More secure than MD5, but SHA-1 is deprecated	Linux systems, SSL/TLS
bcrypt	Strong, slow hash with built-in salting	Modern Linux and web applications
scrypt	Memory-intensive, designed to resist brute-force	Secure password storage
NTLM / LM	Used in Windows systems	Windows authentication
Kerberos / LDAP	Enterprise authentication protocols	Corporate networks

In Linux systems:

- Password hashes are stored in the /etc/shadow file.
- Each line corresponds to a user and includes a hashed password, typically using SHA-512 or bcrypt.
- These hashes are protected by strict permissions — only root can access them.
- Hashes are salted to prevent rainbow table attacks.
- To audit these hashes ethically:
  sudo cat /etc/shadow > hashes.txt
  john hashes.txt

Conclusion:

This experiment showcased how John the Ripper can efficiently crack password hashes in a secure Kali Linux environment. It emphasizes the importance of ethical practices and strong password protection in cybersecurity.

Signature of faculty in-charge with Date: