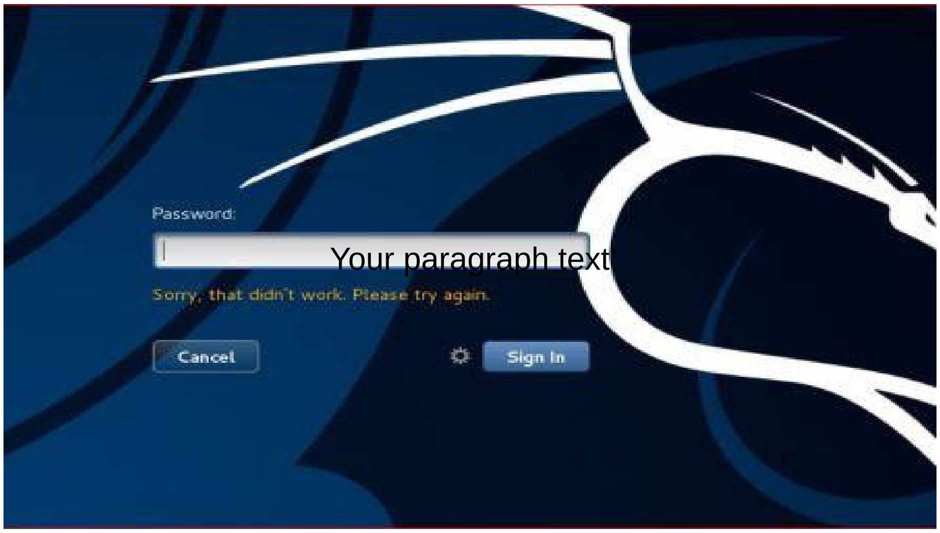
Name- Harshil Amit Buch
Class- TY CSF-1
Roll No. 14

LAB MANUAL
ON
PASSWORD CRACKING OF KALI LINUX OPERATING SYSTEM



Sorry, that didn't work. Please try again.

ESTABLISHMENT OF ADVANCED LABORATORY FOR CYBER SECURITY TRAINING TO TECHNICAL TEACHERS

DEPARTMENT OF INFORMATION MANAGEMENT AND EMERGING ENGINEERING

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

GOVERNMENT OF INDIA

Principal Investigator: Prof. Maitreyee Dutta

Co Investigator: Prof. Shyam Sundar Pattnaik

PREPARED BY:

Prof. Maitreyee Dutta and Ms. Shweta Sharma (Technical Assistant)

Table of Contents

MANUAL-5: PASSWORD CRACKING OF KALI LINUX OPERATING SYSTEM

INTRODUCTION TO KALI LINUX OPERATING SYSTEM

□ KaliLinuxis a Debian-derived Linuxdistributionoperating system which is designed for digital forensics and penetration testing. Kali Linux operating system is
□ maintained and funded by Offensive Security. The first version (1.0) of Kali Linux operating system was released in
□ March 2013 [1]. This operating system has over 600 pre-installed penetration testing and security tools such as
□ Nmap, John the Ripper, Aircrack-ng, Hashcat, Metasploit framework, and so on.

PASSWORD STORAGE IN KALI LINUX OPERATING SYSTEM

□ Passwords areused toprotectthesystemfroman unauthorized access.

□ Computers with Kali Linux operating system stores password in /etc/shadow file in the form of Message Digest 5

(MD5)/ Blowfish/ Secure Hash Algorithm (SHA-256/ SHA-512) hash.

- Passwords are stored in the form of hash due to its irreversible property. This means that password in plaintext can be converted to hash but a hash can’t be converted back to plaintext.

PASSWORD CRACKING

- Password cracking in Kali Linux operating system is a process to recover passwords from a shadow file.
- The purpose of password cracking is to recover forgotten password. The forensic team can perform password cracking on a computer system to recover the data after getting the password.
- This is usually accomplished by recovering the passwords from data stored in the shadow file in the form of a hash value.

PASSWORD CRACKING TECHNIQUES

The password cracking techniques are discussed as follows:

- BRUTE FORCE: A brute force technique is an attempt to crack passwords using permutation and combination approach. This method takes a lot of time and memory consumption depending on the length and complexity of password.

- DICTIONARY: A dictionary technique is an attempt to store in-build passwords in a file known as dictionary. Instead of trying all combination of passwords, it creates a word-list of most common passwords and calculates the hash values while cracking the passwords. It will only able to crack the password if it is stored in dictionary file. This technique takes less time as compared to brute-force technique to crack the password.

- RAINBOW TABLES: This technique is same as dictionary, but instead of calculating hash vales during password cracking; it stores the in-built hash values of password in the tables. Thus, this technique takes less time as compared to brute-force and dictionary technique to crack the password.

JOHN-THE-RIPPER TOOL

- The John-the-ripper tool [2] is an open-source application and post-exploitation Kali Linux operating system tool that allows users to view authentication credentials.

- This tool provides hashes from shadow file of Kali Linux operating system to users.

- Kali Linux store password data in a shadow file in the form of a hash. The forensics team can use John-the-ripper tool to get the password in plain text and pass it to the target computer to login.

PASSWORD CRACKING WITH JOHN-THE-RIPPER TOOL

The password in plaintext from hash can be recoveredwith John-the-ripper tool with the following steps:

Step 1: Open Kali Linux operating system as shown in Figure 1.

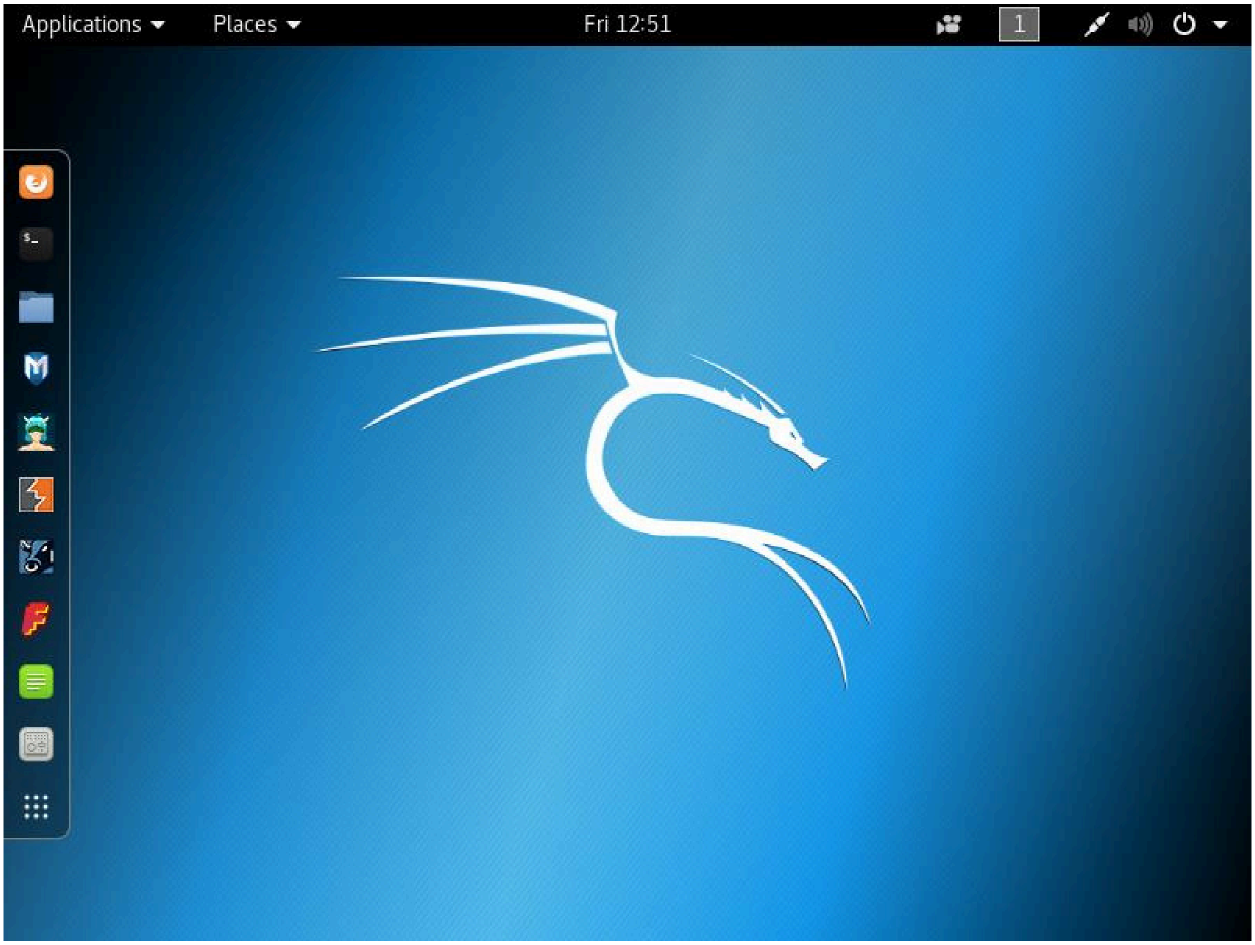


Figure 1: Kali Linux operating system

Step 2: In Kali Linux operating system, open John-the-ripper tool. Go to Applications-> Password attacks-> john as shown in Figure 2.

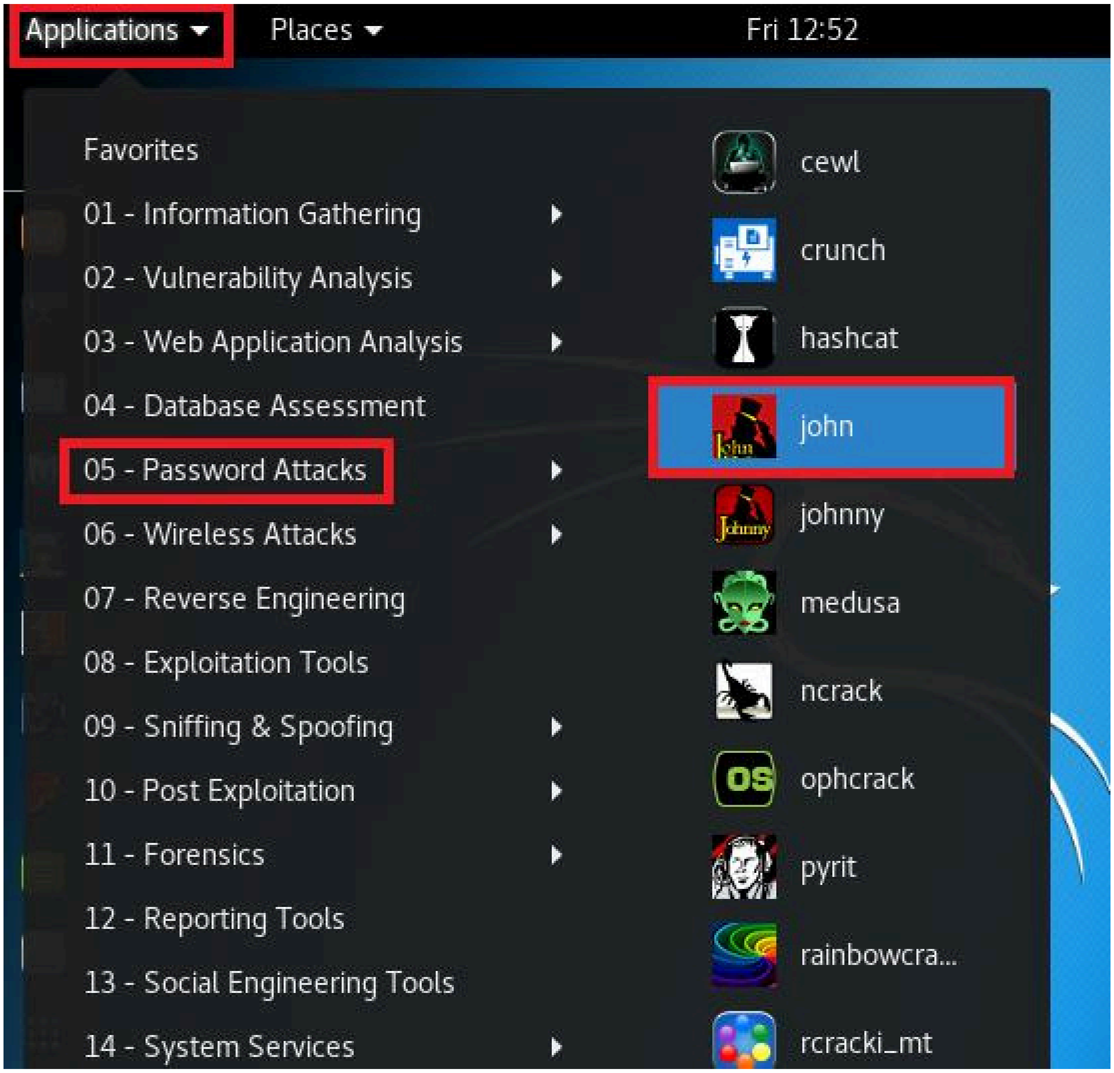
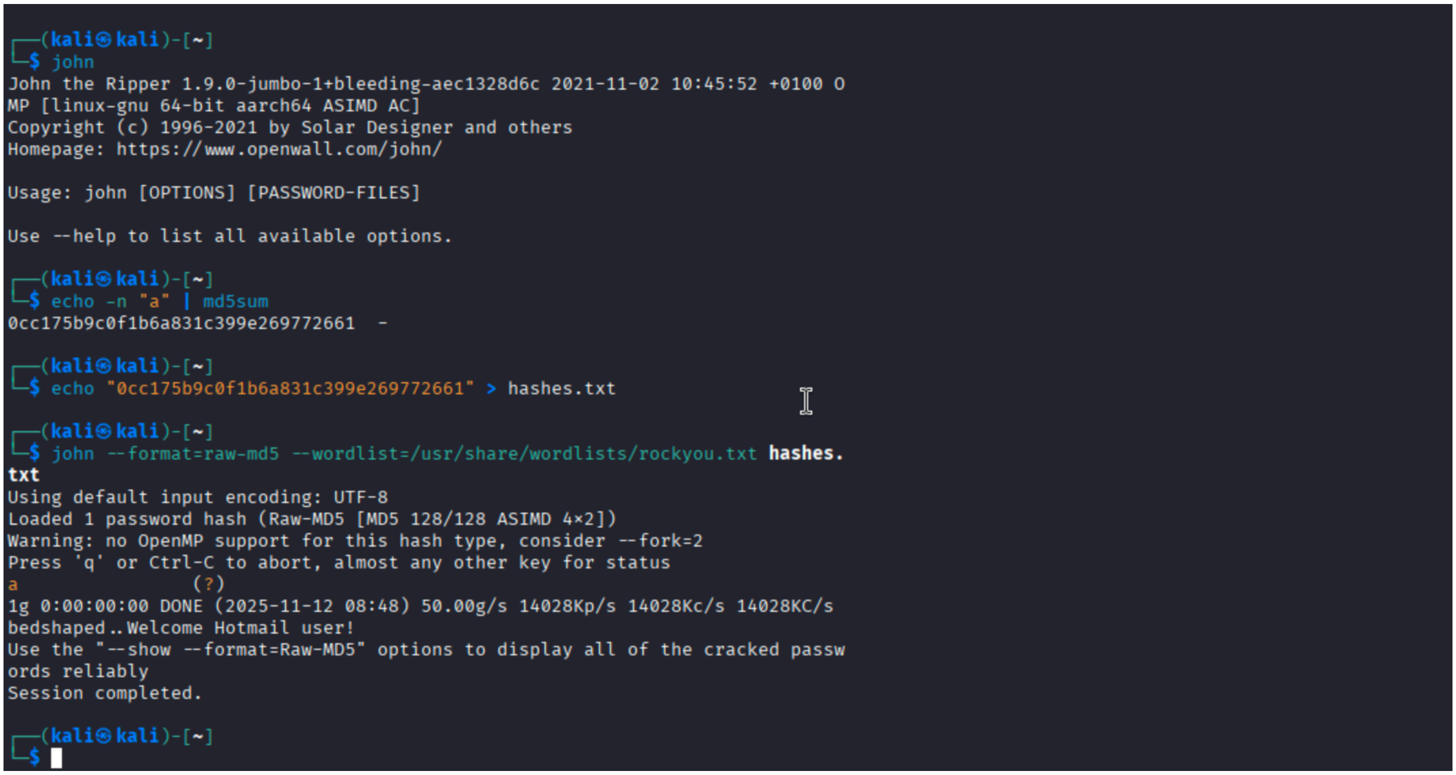


Figure 2: Opening John-the-Ripper tool

<u>Step 3:</u> A terminal with usage of John-the-ripper tool will open as shown in Figure 3 and Figure 4.



```
┌──(kali㉿kali)-[~]
└─$ john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 O
MP [linux-gnu 64-bit aarch64 ASIMD AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

Use --help to list all available options.

┌──(kali㉿kali)-[~]
└─$ echo -n "a" | md5sum
0cc175b9c0f1b6a831c399e269772661  -

┌──(kali㉿kali)-[~]
└─$ echo "0cc175b9c0f1b6a831c399e269772661" > hashes.txt

┌──(kali㉿kali)-[~]
└─$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hashes.
txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 ASIMD 4×2])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
a                (?)
1g 0:00:00:00 DONE (2025-11-12 08:48) 50.00g/s 14028Kp/s 14028Kc/s 14028KC/s
bedshaped..Welcome Hotmail user!
Use the "--show --format=Raw-MD5" options to display all of the cracked passw
ords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$ 
```