Experiment No. 4

Title: Password Cracking Tools

Roll No.: 16010423076 **Experiments No.:4**

Aim : To learn about password cracking tools

Resources : Internet access, web-browser, password cracking tools

Theory:

Introduction to Password Cracking

Password cracking is the process of recovering passwords from stored data. It is used in cybersecurity to test the strength of passwords and improve security. When a user sets a password, it is not stored in its original form. Instead, it is converted into a scrambled version using a mathematical process called hashing. This scrambled version is called a hash. The main idea behind password cracking is to take a hash and find the original password that created it.

Types of Password Attacks

There are different ways to crack passwords. One of the most common methods is the dictionary attack. In this method, a tool checks a long list of commonly used passwords one by one to see if any of them match the hash. If a weak password is used, this method can crack it in seconds. Another method is the brute-force attack, where every possible combination of letters, numbers, and symbols is tried until the correct password is found. This method is slow, but it works if enough time is given. A more advanced method is the rainbow table attack. This method uses precomputed tables of hashes and their matching passwords. Instead of calculating a hash for every possible password, the tool simply looks it up in the table, which makes the process much faster.

Common Password Cracking Tools

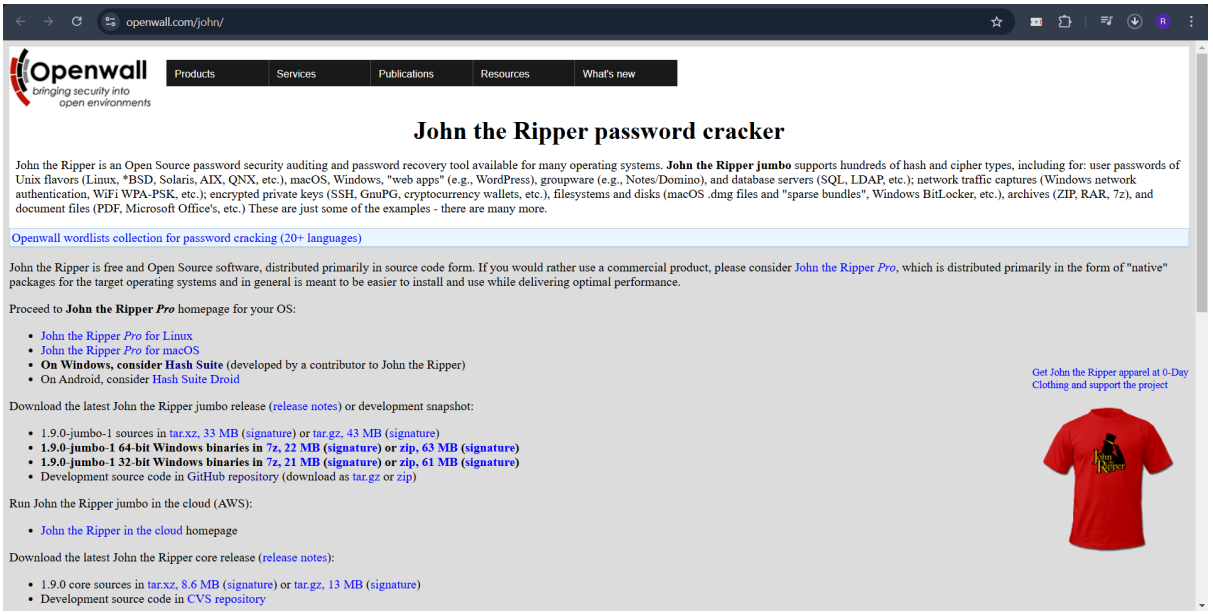
Password cracking tools are designed to automate these processes. John the Ripper is one of the most popular tools for this task. It works by taking a hash and testing passwords against it using different attack methods. It has a built-in list of common passwords, but users can also provide custom wordlists. Hashcat is another powerful tool. It can use the computer's processor and graphics card to speed up the cracking process. Hashcat supports many types of attacks, including dictionary and brute-force attacks. Another tool that was commonly used in the past is Cain and Abel, which could recover passwords stored on a Windows system. However, it is now outdated and not widely used.

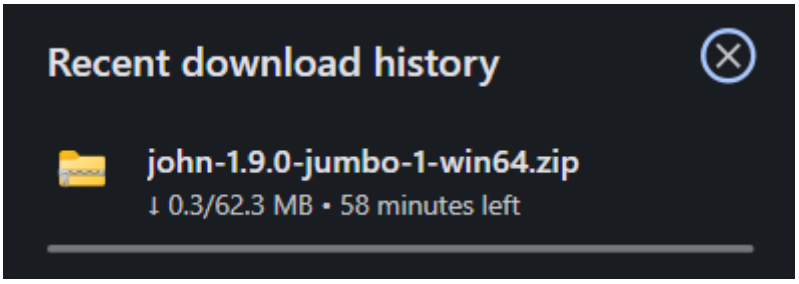
Importance of Strong Passwords

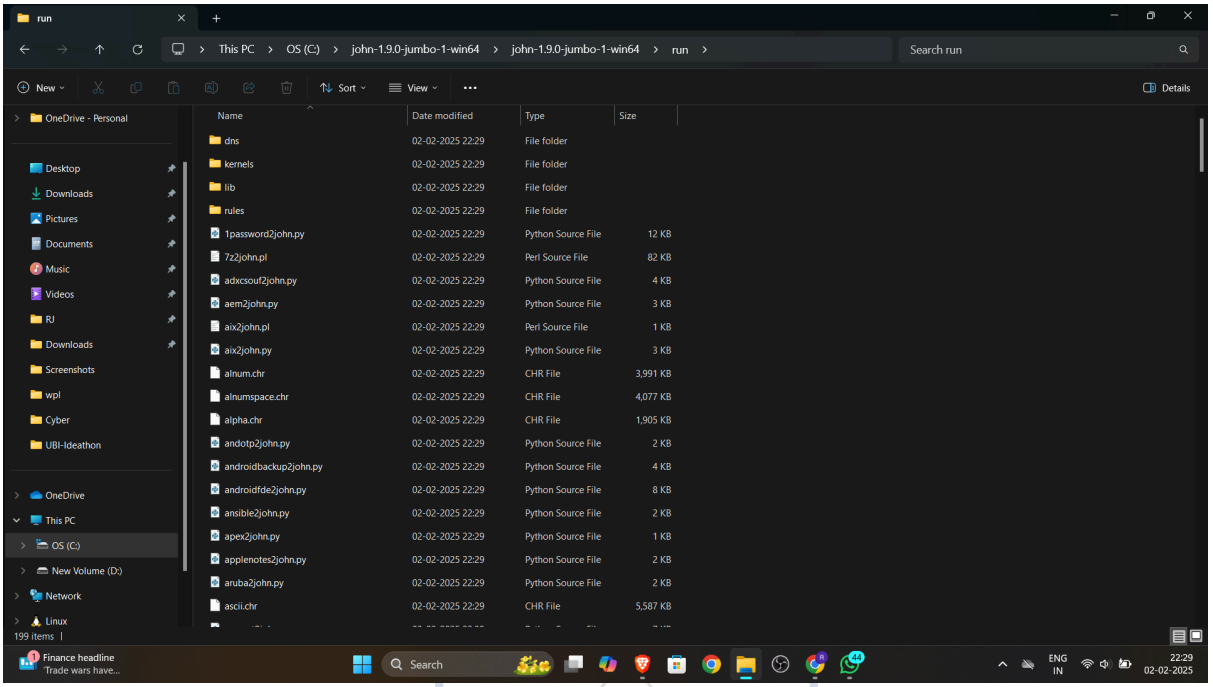
Strong passwords are difficult to crack. A password that is long and includes a mix of uppercase letters, lowercase letters, numbers, and symbols is much harder to break. Using unique passwords for different accounts also improves security. Many websites use salting to make password cracking harder. Salting means adding a random value to a password before hashing it. This prevents attackers from using precomputed tables like rainbow tables to find passwords easily.

IMPLEMENTATION AND RESULTS:

Step 1 : Download and Install the Tool - John The Ripper





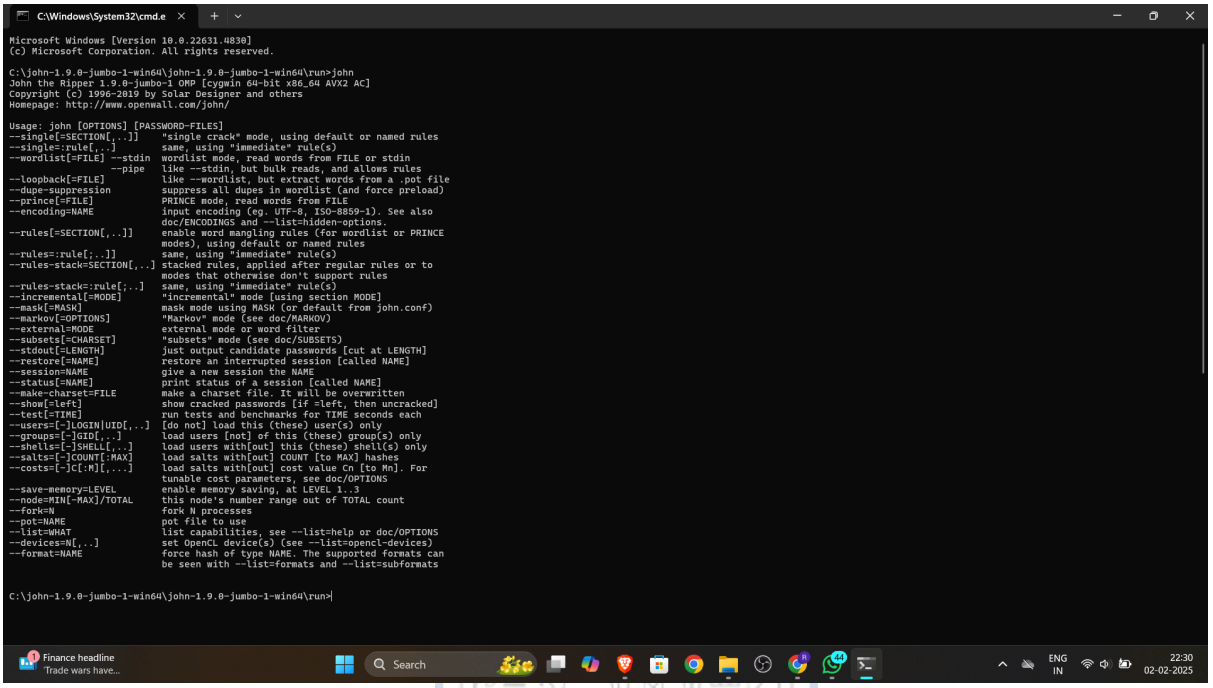


Step 2 : Prepare a Sample Hash File:

md5 hash for the word ‘hello’

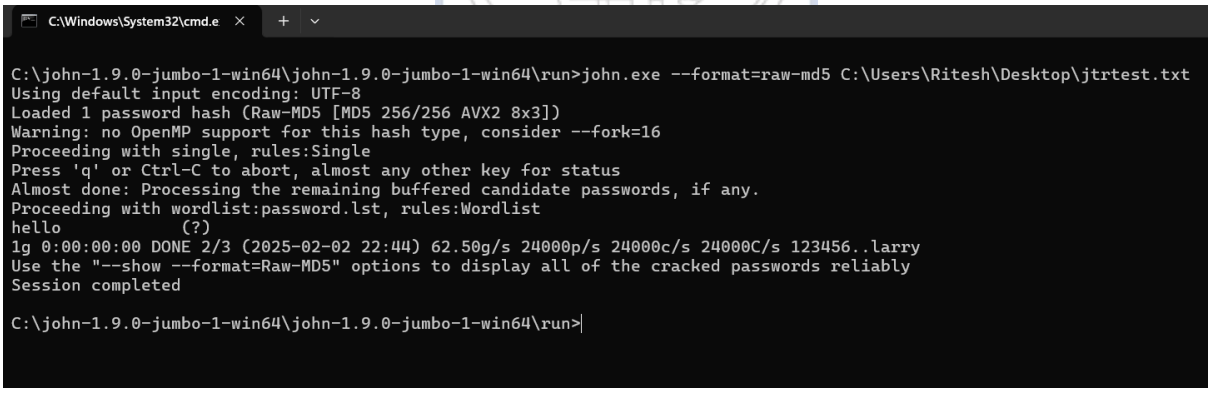
Step 3 : Run John the Ripper

Command : john



Step 4 : Crack the md5 hash

command : john.exe --format=raw-md5 C:\Users\Ritesh\Desktop\jtrtest.txt



It has successfully cracked the password ‘hello’.

Outcomes: CO3: Understand Attack Methodology

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

From this experiment I learned that password cracking tools such as John the Ripper and Hashcat are powerful resources for assessing the strength of password storage mechanisms. The experiment highlighted the importance of using strong, complex passwords and secure hashing algorithms, as even well-known and publicly available tools can successfully crack weak passwords. It also underscored the ethical responsibilities and limitations inherent in such tools, emphasizing that they should only be used in authorized environments for security testing purposes.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

REFERENCES:

https://www.openwall.com/john/

John the Ripper in Action: Practical Steps to Crack Passwords

Cain & Abel Overview