**Password Cracking**

Password cracking is the process of attempting to discover or recover a password from stored data, typically by exploiting weaknesses in the way passwords are stored or by leveraging human behavior patterns. The goal is to gain unauthorized access to a system, application, or encrypted data by deciphering the password.

**Types of Password Cracking Techniques**

* **Brute Force Attack:**

This involves systematically attempting every possible combination of characters until the correct password is found. While effective, it is time-consuming, especially for complex passwords.

* **Dictionary Attack:**

This method uses a precompiled list of commonly used passwords (a "dictionary") and tries each one against the stored password hash. It’s faster than brute force but less effective for complex or unique passwords.

* **Hybrid Attack:**

A combination of dictionary and brute force attacks, where slight modifications are made to common passwords (e.g., adding numbers or symbols to the end of dictionary words).

* **Rainbow Table Attack:**

Rainbow tables are precomputed tables of password hashes that help crack passwords more efficiently. Instead of computing the hash for every guess, the attacker checks the hash against the rainbow table.

* **Social Engineering:**

This is a non-technical approach where attackers manipulate people into revealing their passwords, often through phishing emails, phone calls, or other psychological tricks.

* **Keylogging and Malware:**

Keylogging software captures keystrokes to record passwords as they are typed. Malware can also extract passwords stored on the device or intercept them during communication.

**Using John the Ripper to crack password hash**

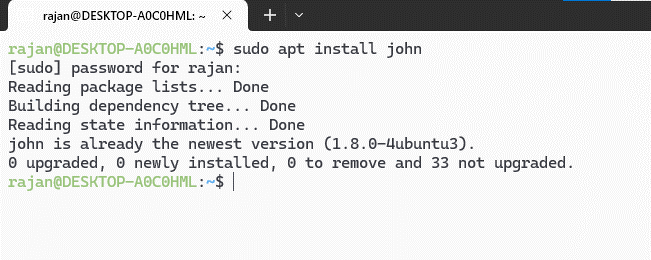
John the Ripper (often referred to as "John") is an open-source password cracking tool available on Linux, as well as other operating systems. It's primarily used for security testing and for recovering passwords from hashed data.

**Key Features:**

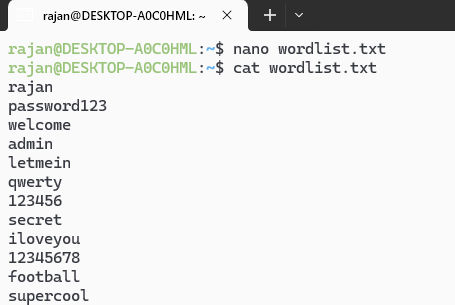
1. **Password Cracking:** John the Ripper can crack passwords using various methods such as brute force, dictionary attacks, and hybrid attacks.
2. **Supported Hash Types:** It supports a wide range of password hash types, including Unix-based password hashes (like DES, MD5, and Blowfish), Windows LM hashes, and many others.
3. **Customizable:** You can customize your attacks by modifying the wordlists, applying different rules, or combining attacks.
4. **Multi-Platform:** Although popular on Linux, it is available for other operating systems like macOS and Windows.
5. **Community and Pro Version:** There's a community-supported version that is free, and a more feature-rich pro version that includes additional functionalities.

**Using Dictionary Attack**

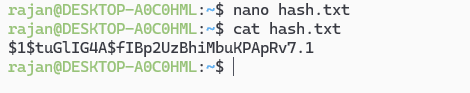
1. Install John the Ripper



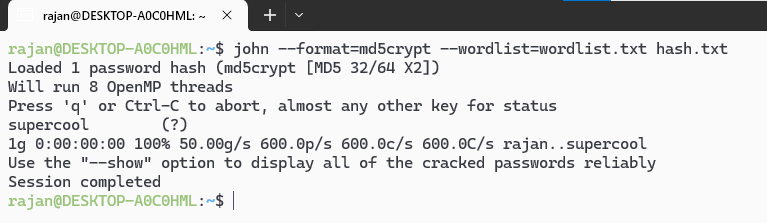
1. Create a dictionary of possible passwords in a text file



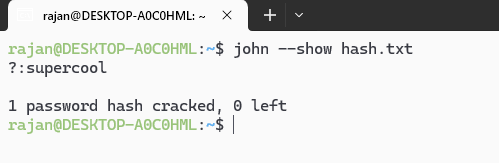
1. Store the hash you want to crack in a text file (the hash is of the word “supercool”)



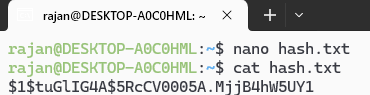
1. Use john to try the hash against each stored password

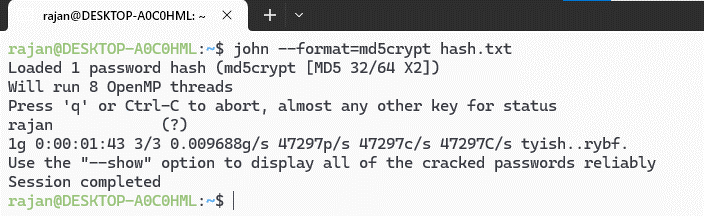


1. Use show command to view the cracked hash

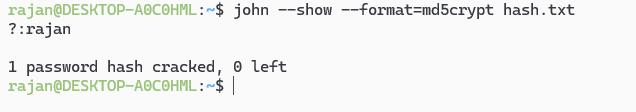


**Using Brute Force Attack**

1. Store the hash you want to crack in a text file (the hash is of the word “rajan”)
2. Use john to systematically attempt every possible combination of characters until the correct password is found



1. Once the operation is complete use the show command to view the cracked hash



**Conclusion**

In this lab, we successfully used John the Ripper to perform brute force and dictionary attacks to crack password hashes. The brute force method, while effective for short passwords, was time-consuming for more complex ones. The dictionary attack, using a list of common passwords, was faster but less effective for unique passwords.

This exercise emphasized the importance of using strong, complex passwords and highlighted the need for additional security measures like salting to defend against password cracking attacks.