**John the Ripper: Password Cracking Tool 1**

John the Ripper is a powerful tool in the cyber world that is used mainly for password cracking. It is a primary tool for any security professional who needs to test the strength and weakness of passwords in various systems. The name, similar to the famous Jack the Ripper, refers to the tool's function-to rip through password encryption to expose vulnerabilities within.

**Purpose and Use:**

**Password Strength Assessment**: John the Ripper provides capabilities for assessing password strength, which will indicate weak passwords that could be vulnerable to attack.

**Security auditing:** helps an organization understand its vulnerability to password-related attacks through the simulation of actions that a potential intruder might undertake.

**Password Cracking:** John the Ripper is employed in ethical hacking to simulate password attacks so that security teams can strengthen their defences before actual attackers take advantage of any weakness.

**Working:**  
John the Ripper works by using various methods to crack passwords, from using lists of commonly used words, known as dictionary attacks, to testing all possible character combinations, also called brute-force attacks.

**Steps:**  
  
**1) Installation:**

Download and install John the Ripper from the official site at, or from a trusted repository. Extract the files and open terminal in the installation directory.

**2)Prepare the Hashes**:

Acquire the password hashes to be cracked. These can be lifted directly from a password file (for example, /etc/shadow in Unix-derived operating systems).

Save the hashes in a text file.

**3)Run John the Ripper:**

Open the terminal and change directory to John the Ripper directory.

Use the following command to start cracking:

john [options] [path\_to\_hash\_file]

Example:

john password\_hashes.txt

John the Ripper will start to attempt the breaking of the passwords with its default approach.

**4)You can monitor the progress using:**

John --state

It gives information on the number of passwords cracked so far and how much time has expired.

**5)When John the Ripper has completed, to view results:**

John --show