**Hashcat: Password Cracking Tool 2**

Hashcat is a password cracking tool and it is used for its rapidity and effectiveness. In contrast to John the Ripper, which operates on CPUs, Hashcat is specifically engineered to utilize the capabilities of GPUs to facilitate quicker and more effective password cracking.

**Step-by-Step Implementation of Hashcat:**

**Installation:**

Download and install Hashcat from the official website or from a trusted repository.

**Prepare the Hashes:**

Obtain the password hashes you want to crack. Hashcat supports a vast number of hash types.

Create a text file containing the hash values, for example, hashes.txt.

**Identify the Hash Type:**

Determine the type of hash you're dealing with. For eg MD5, SHA-1, bcrypt.

**Select the Hash Mode:**

Hashcat requires to specify a mode depending on the hash type. For example:

MD5: Mode 0

SHA-1: Mode 100

bcrypt: Configuration 3200

**Run Hashcat:**

Open a terminal and change directory into the Hashcat directory.

Use the following syntax to start cracking:

hashcat -m [mode] -a [attack\_mode] [path\_to\_hash\_file] [wordlist]

e.g.: hashcat -m 0 -a 0 hashes.txt wordlist.txt

Here:

-m 0 specifies MD5 hash.

-a 0 specifies a dictionary attack.

The file containing the hashes is named hashes.txt.

The file containing potential passwords: wordlist.txt.

**Monitor the Cracking Process:**

Hashcat will display ongoing progress in real-time, the percentage of completion, the attack speed, and any passwords that have successfully been decrypted.

**View Cracked Passwords**:

Once Hashcat completes the process or when you want to check results,  
 use: hashcat -m [mode] --display hashes.txt   
This will show all the cracked passwords.