Hashcat

1. Introduction

Hashcat is one of the most powerful password recovery and hash-cracking tools available today.
It is widely used by penetration testers, cybersecurity researchers, and forensic investigators.
Hashcat supports hundreds of algorithms, including MD5, SHA family, Windows NTLM, WPA/WPA2, and more.
Its GPU acceleration makes it significantly faster than traditional CPU-only tools.

Key Features:

- Supports **300+ hash algorithms**
- Works on **CPU and GPU (NVIDIA/AMD)**
- Cross-platform (Windows, Linux, macOS)
- Open-source and actively maintained
- Multiple attack modes (Dictionary, Brute-force, Mask, Hybrid)
- Optimized for performance and flexibility

2. Installation

On Linux

```
sudo apt update
sudo apt install hashcat
```

GPU Setup

NVIDIA: install CUDA toolkit

AMD: install ROCm/OpenCL

Check supported devices:

```
hashcat -I
```

3. Attack Modes in Hashcat

- **Dictionary Attack (-a 0)**

```
hashcat -m 0 -a 0 hash.txt wordlist.txt
```

- **Brute-force Attack (-a 3)**

```
hashcat -m 1000 -a 3 hash.txt ?d?d?d?d
```

- **Mask Attack (-a 3)**

```
hashcat -m 0 -a 3 hash.txt P@ss?d?d?d?d
```

- **Hybrid Attack**

```
hashcat -m 0 -a 6 hash.txt wordlist.txt ?d?d
```

4. Supported Hash Types

Mode (-m)	Algorithm	Use Case
0	MD5	Websites, apps
100	SHA1	Old web apps
500	md5crypt	Linux systems
1000	NTLM	Windows login
1800	SHA-512	Linux shadow file
22000	WPA/WPA2 (PMKID)	Wi-Fi password cracking

Full list with:

```
hashcat -h | more
```

5. Practical Examples

Crack MD5 with rockyou.txt

```
hashcat -m 0 -a 0 hash.txt rockyou.txt
```

Crack NTLM with 8-digit brute-force

```
hashcat -m 1000 -a 3 hash.txt ?d?d?d?d?d?d?d?d
```

Crack WPA2 Wi-Fi hash

```
hashcat -m 22000 -a 3 wifi_hash.hc22000 ?d?d?d?d?d?d?d?d
```

6. Wordlists for Hashcat

- **RockYou Dictionary**

  Most famous password list (common + fast).

  Already available in Kali Linux:

  ```
  /usr/share/wordlists/rockyou.txt.gz
  gunzip /usr/share/wordlists/rockyou.txt.gz
  ```

- **SecLists Collection**

  Huge collection for security testing.

  Includes passwords, usernames, Wi-Fi keys, and fuzzing lists.

- **CrackStation Wordlist**

  Very large list (15GB+).

- **Weakpass.com**

  Huge online database of wordlists.

- **Custom Wordlists (CeWL)**

  Create your own lists from a target website:

  ```
  cewl https://example.com -w mylist.txt
  ```

7. Optimization Tips

- Use GPU for faster performance.
- Apply rules to wordlists.
- Use masks for targeted cracking.
- Pause/Resume jobs:

```
hashcat --pause
hashcat --resume
```

- Show cracked passwords:

```
hashcat --show -m 0 hash.txt
```

8. Ethical Considerations

- Hashcat is a **security research tool**, not a hacking tool.
- Use **only** with permission.
- Unauthorized cracking = **illegal**.
- Always follow **ethical hacking guidelines**.