**Hashcat**

Prepared by: SUBHAN AHMED  
Tool: Hashcat  
Platform: Kali Linux

# 1. Introduction

Hashcat is one of the world’s fastest and most advanced password recovery tools. It is widely used in cybersecurity, penetration testing, and digital forensics. With GPU acceleration, Hashcat can crack hashed passwords using various attack modes efficiently.

## 2. Key Features

✔ Supports 300+ hashing algorithms

✔ GPU acceleration for high-speed cracking

✔ Multiple attack modes: dictionary, brute-force, hybrid, etc.

✔ Handles large wordlists and custom rules

## 3. Installation on Kali Linux

Verify installation:

hashcat --version

If not installed:

sudo apt update

sudo apt install hashcat -y

## 4. Basic Syntax

General syntax:

hashcat [options] -m <hash-type> -a <attack-mode> <hashfile> <wordlist>

## 5. Common Hash Types

• MD5 (-m 0)

• SHA1 (-m 100)

• SHA256 (-m 1400)

• NTLM (-m 1000)

• WPA2 (-m 22000)

## 6. Attack Modes

• Dictionary (-a 0)

• Combination (-a 1)

• Brute-force (-a 3)

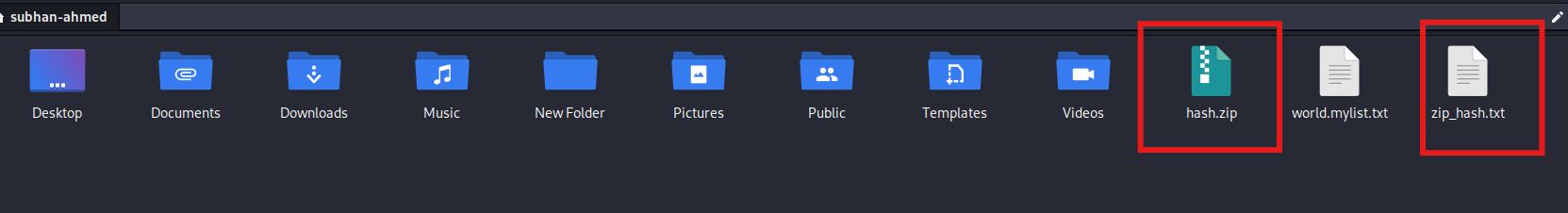
• Hybrid (-a 6 or 7)

• Rule-based

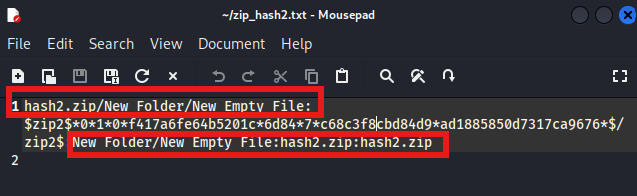
## 7. Usage Examples

I extract hash from a zip file





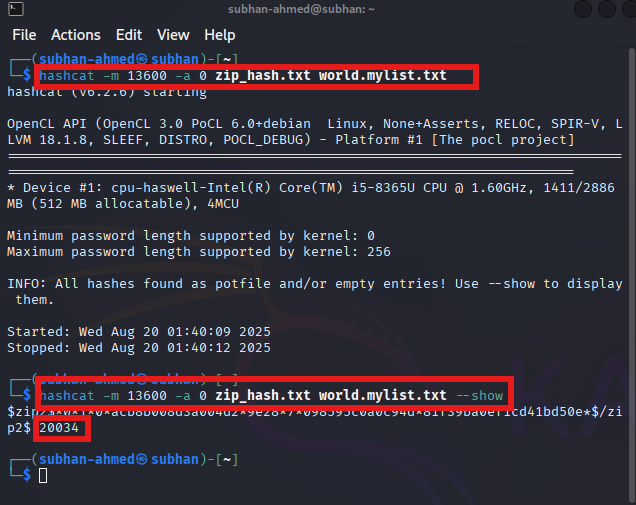
When you the hash file is create make show to remove which is show in below

Between this red box this is a hash  


* **Dictionary Attack:**

To crack zip file hash we use –m 13600

hashcat -m 0 -a 0 hash.txt /usr/share/wordlists/rockyou.txt



* **Brute-force Attack (NTLM, 6 lowercase):**

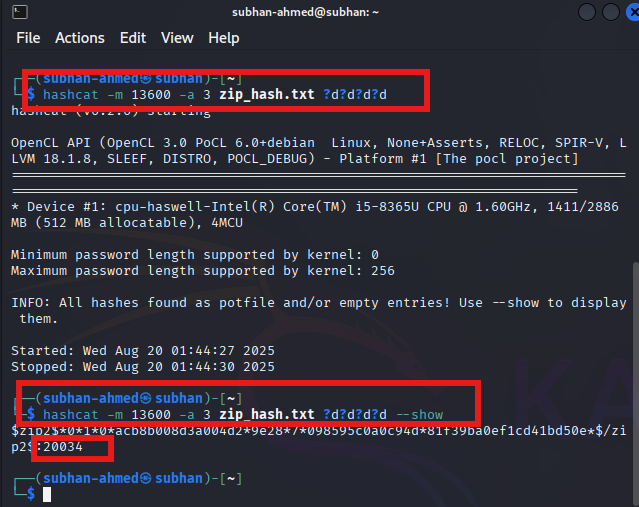
hashcat -m 1000 -a 3 hash.txt ?l?l?l?l?l?l

?l = lowercase letter

?d = digit

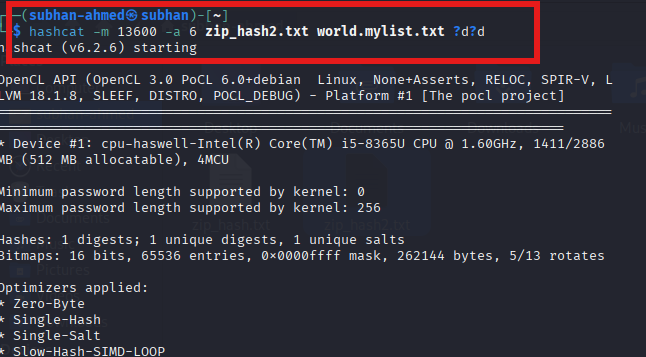
?u = uppercase

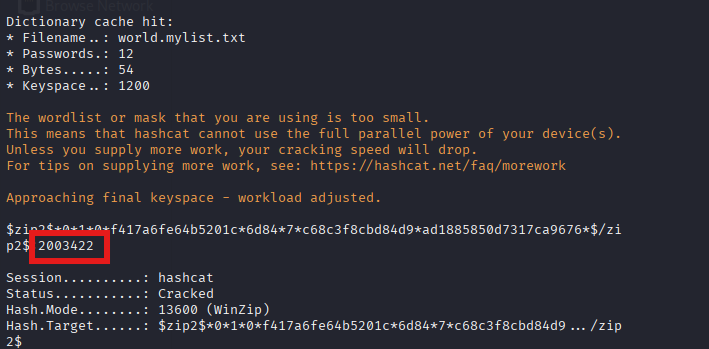
?s = symbol



* **Hybrid Attack (append 2 digits):**

hashcat -m 0 -a 6 hash.txt /usr/share/wordlists/rockyou.txt ?d?d





In wordlist only 20034 was present and other two find by bruteforce

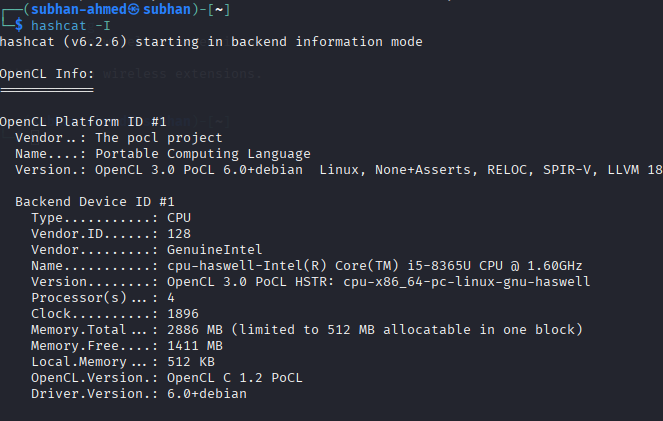
* **WPA2 Cracking:**

hashcat -m 22000 -a 0 handshake.hc22000 /usr/share/wordlists/rockyou.txt

## 8. Performance Tuning

List devices:

hashcat -I



Benchmark:

hashcat -b

Restore the last session:

hashcat --restore

Use a specific device (GPU index 1 example):

hashcat -d 1 -m 0 -a 0 hash.txt wordlist.txt

## 9. Output & Results

Cracked passwords are stored in the potfile:

cat ~/.hashcat/hashcat.potfile

## 10. Security & Legal Notice

Hashcat must be used only for authorized security testing or password recovery. Unauthorized use is illegal and punishable under cybercrime laws.

## 11. Conclusion

Hashcat is a powerful password-cracking utility for security auditing. With multiple attack modes and GPU acceleration, it provides unmatched speed and flexibility.

# 12. Extracting Hashes

Before using Hashcat, you need to extract password hashes from systems, networks, databases, or documents.

## 12.1 Linux Hashes

Use unshadow to combine /etc/passwd and /etc/shadow:

sudo unshadow /etc/passwd /etc/shadow > linux\_hashes.txt

## 12.2 Windows Hashes

Extract SAM and SYSTEM, then dump NTLM hashes with samdump2:

samdump2 SYSTEM SAM > windows\_hashes.txt

Crack with Hashcat:

hashcat -m 1000 -a 0 windows\_hashes.txt /usr/share/wordlists/rockyou.txt

## 12.3 Network Traffic (Wi‑Fi)

Capture WPA2 handshake and convert for Hashcat:

airodump-ng wlan0

aireplay-ng --deauth 5 -a <AP\_MAC> wlan0

hcxpcapngtool capture.cap -o handshake.hc22000

Crack with Hashcat:

hashcat -m 22000 -a 0 handshake.hc22000 /usr/share/wordlists/rockyou.txt

## 12.4 Databases

Export password hashes from user tables (SQL dump) and save them to a text file (e.g., db\_hashes.txt) for cracking with Hashcat.

## 12.5 Documents

Extract document password hashes:

office2john protected.docx > office\_hash.txt

pdf2john protected.pdf > pdf\_hash.txt

Crack with Hashcat:

hashcat -m 9600 office\_hash.txt /usr/share/wordlists/rockyou.txt

hashcat -m 10500 pdf\_hash.txt /usr/share/wordlists/rockyou.txt

## 12.6 Ethical Considerations

Only extract and crack hashes with explicit authorization. Unauthorized access is illegal and unethical.