

Installation & Setup

Everything you need to get hashcat running on your system — from hardware requirements to environment configuration and your first benchmark.

Learning Objectives

- Understand the **hardware requirements** for CPU and GPU cracking
 - Install hashcat on **macOS, Linux, and Windows**
 - Configure **environment variables** for optimal operation
 - Verify your installation with **hashcat --version** and **hashcat -l**
 - Run your first **benchmark** to measure cracking speed
-

CPU Requirements

While hashcat is primarily a GPU tool, the CPU still matters for coordination, rule processing, and fallback cracking modes.

Component	Minimum	Recommended
Architecture	x86_64 with SSE2	AVX2 / AVX-512 support
Intel	Core i5 (8th gen+)	Core i7 / i9 (10th gen+)
AMD	Ryzen 5	Ryzen 7 / Ryzen 9
Cores	4 cores	8+ cores
RAM	4 GB	16 GB+

Why AVX/AVX2 Matters

Hashcat uses SIMD instructions (AVX, AVX2, AVX-512) to accelerate CPU-based operations. Without AVX support, some hash modes will be significantly slower or unavailable in CPU-only

mode.

Notes: Check AVX support with `lscpu | grep avx` on Linux or `sysctl -a | grep machdep.cpu.features` on macOS.

GPU Requirements

The GPU is the heart of hashcat's performance. A modern GPU can be **100–1000x faster** than a CPU for most hash types.

NVIDIA (CUDA / OpenCL)

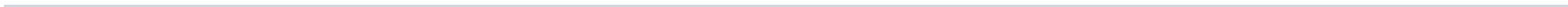
- **Minimum:** GTX 1060 6GB
- **Recommended:** RTX 3080 / RTX 3090
- **Best:** RTX 4090 / A100
- Driver: 440.0+ (CUDA 10.1+)
- VRAM: 6 GB min, 10 GB+ recommended

AMD (OpenCL / ROCm)

- **Minimum:** RX 580 8GB
- **Recommended:** RX 6800 XT / RX 6900 XT
- **Best:** RX 7900 XTX / MI250
- Driver: Adrenalin 21.5+ or ROCm 4.0+
- VRAM: 8 GB min, 16 GB+ recommended

Storage & OS

Storage: 20 GB free space minimum (SSD strongly recommended for large wordlists). **OS:** 64-bit Windows 10/11, Linux (Ubuntu 20.04+, Kali), or macOS 11+.



Installation: macOS

Two paths: Homebrew (simplest) or building from source for the latest features.

Option A: Homebrew

```
# Install via Homebrew
brew install hashcat

# Verify installation
hashcat --version
hashcat -I          # List detected compute devices
```

Option B: Build from Source

```
# Clone the repository
git clone https://github.com/hashcat/hashcat.git
cd hashcat

# Build
make -j$(sysctl -n hw.ncpu)
```

```
# Test  
./hashcat --version
```

macOS Note

Apple removed OpenCL support in macOS 12+. Hashcat on Apple Silicon uses Metal via OpenCL compatibility layer. Performance is limited compared to dedicated NVIDIA/AMD GPUs. For serious work, consider a Linux machine with a discrete GPU.

Installation: Linux & Windows

Linux (Debian/Ubuntu)

```
# Package manager
sudo apt update
sudo apt install hashcat

# Or build from source
git clone https://github.com/hashcat/hashcat.git
cd hashcat
make -j$(nproc)
sudo make install
```

On Kali Linux, hashcat is **pre-installed**.

Windows

```
# 1. Download binary from
#   https://hashcat.net/hashcat/

# 2. Extract the archive
# 3. Open CMD or PowerShell
cd C:\hashcat

# 4. Verify
.\hashcat.exe --version
.\hashcat.exe -I
```

No compilation needed — binaries are provided.

Notes: On Linux, ensure GPU drivers are installed first: `nvidia-smi` for NVIDIA or `rocm-smi` for AMD. Without proper drivers, hashcat will fall back to CPU-only mode.

Environment Variables

Hashcat can be configured via environment variables for repeatable setups and automation scripts.

Variable	Purpose	Example
<code>HASHCAT_HOME</code>	Base directory for hashcat files	<code>/opt/hashcat</code>
<code>HASHCAT_LOG</code>	Log file output path	<code>/var/log/hashcat.log</code>
<code>HASHCAT_GPU</code>	Specify GPU device(s) to use	<code>1,2</code>
<code>HASHCAT_CPU</code>	Force CPU-only mode	<code>1</code>
<code>HASHCAT_FORCE</code>	Bypass warnings (use with caution)	<code>1</code>
<code>HASHCAT_WORKLOAD_PROFILE</code>	Default workload profile (1-4)	<code>3</code>

```
# Add to ~/.bashrc or ~/.zshrc
export HASHCAT_HOME="/opt/hashcat"
```

```
export HASHCAT_LOG="$HOME/.hashcat/logs"  
export HASHCAT_WORKLOAD_PROFILE=3
```

Benchmarking

After installation, run a benchmark to confirm hashcat can use your hardware and to establish a performance baseline.

```
# Full benchmark across all hash types
hashcat -b

# Benchmark a specific hash type (e.g., MD5 = 0)
hashcat -b -m 0

# Benchmark with specific device
hashcat -b -d 1

# Show detected devices
hashcat -I
```

Sample Benchmark Output (RTX 3080)

```
Hashmode: 0 - MD5
Speed.#1.....: 52314.3 MH/s

Hashmode: 1000 - NTLM
```

```
Speed.#1.....: 93827.1 MH/s
```

```
Hashmode: 1800 - sha512crypt
```

```
Speed.#1.....: 412.8 kH/s
```

Notes: MH/s = millions of hashes per second, kH/s = thousands. The difference between MD5 and sha512crypt highlights why algorithm choice matters for password security.

Lab & Homework

Lab Exercises

1. **Install hashcat** — follow the installation steps for your OS and verify with `hashcat --version`
2. **Device detection** — run `hashcat -I` and document your available compute devices
3. **First benchmark** — run `hashcat -b -m 0` and `hashcat -b -m 1000` to compare MD5 vs NTLM speeds
4. **Environment setup** — configure environment variables and create a hashcat working directory

Homework Tasks

1. Run a full benchmark (`hashcat -b`) and identify the 3 fastest and 3 slowest hash types on your hardware.
 2. Set up all recommended environment variables and verify they persist across terminal sessions.
 3. Research why sha512crypt is orders of magnitude slower than MD5 for cracking. Write a short explanation.
-

