Hashcat 使用手册：从入门到高级密码恢复指南

引言：为什么需要 Hashcat

在网络安全领域，密码是系统防护的第一道屏障，但也常常成为弱点。Hashcat 作为全球最快、最先进的密码恢复工具，能帮助安全专业人士评估密码强度、恢复遗忘凭证或进行渗透测试。它支持超过 300 种哈希算法，利用 GPU 等硬件加速，实现高效离线破解。

注意：Hashcat 仅用于合法目的，如授权渗透测试或个人密码恢复。非法使用可能违反法律。请确保遵守道德规范和当地法规。截至 2025 年 10 月，Hashcat 最新稳定版为 v7.1.2，支持更多加密货币钱包和现代哈希类型。 本手册结构清晰，从基础安装到高级技巧，适合初学者和专家。

第一章：Hashcat 基础知识

1.1 Hashcat 是什么？

Hashcat 是一个开源的命令行密码破解工具，使用 C 语言编写，支持 CPU、GPU（NVIDIA/AMD/Intel）和 DSP 等硬件。它专注于离线哈希破解，无法用于在线攻击（如网站登录）。核心优势包括：

- **高性能**：GPU 加速下，可达数亿哈希/秒。
- **多算法支持**：覆盖 MD5、SHA 系列、bcrypt、NTLM、WPA2 等 300+ 类型。
- **攻击模式多样**：字典、暴力、混合等 5 种主要模式。

与 John the Ripper 相比，Hashcat 在 GPU 优化上更强。 它不是黑客工具，而是安全审计利器。

1.2 哈希基础回顾

哈希是将明文（如密码）转换为固定长度字符串的单向函数（如 MD5：`password` → `5f4dcc3b5aa765d61d8327deb882cf99`）。破解即逆向恢复明文。常见类型：

- **无盐哈希**：MD5 (模式 0)、SHA1 (100)。
- **有盐哈希**：bcrypt (3200)、PBKDF2 (10000)。
- **文件/协议哈希**：ZIP (17220)、WPA2 (22000)。

使用 `hash-identifier` 工具预识别哈希类型。

1.3 合法应用场景

- **渗透测试**：评估企业密码策略。
- **数字取证**：恢复加密文件密码。
- **教育研究**：分析常见密码习惯。

第二章：安装与配置

2.1 系统要求

- **OS**：Linux (推荐 Kali/Ubuntu)、Windows、macOS。
- **硬件**：GPU 优先（NVIDIA RTX 系列最佳），至少 4GB VRAM。
- **依赖**：OpenCL/CUDA 驱动，7-Zip（解压）。

2.2 安装步骤

2.2.1 Linux (Debian/Ubuntu/Kali)

Kali 默认预装；否则：

```
sudo apt update
sudo apt install hashcat
hashcat --version  # 检查版本，应为 v7.1.2+
```

若需最新版，从 GitHub 编译（见 BUILD.md）。

2.2.2 RHEL/CentOS

```
wget https://hashcat.net/files/hashcat-7.1.2.7z
sudo yum install epel-release p7zip
7za x hashcat-7.1.2.7z
cd hashcat-7.1.2/
./hashcat --version
```

更换国内镜像加速下载。

2.2.3 Windows

下载预编译版（.7z），解压后运行 `hashcat.exe`。安装 NVIDIA/AMD 驱动。

2.3 驱动安装

使用 `hashcat --backend-info` 检查后端。未安装驱动时，仅 CPU 可用。

- **NVIDIA**：安装 CUDA Toolkit (v12.9+)。Linux：`sudo apt install nvidia-cuda-toolkit`；Windows：GeForce Experience。
- **AMD**：ROCm (v5.0+)，参考官方文档。
- **Intel**：OpenCL 运行时，从官网下载。

常见错误：驱动不兼容导致 “No devices found”。解决方案：重启或 `--force` 强制运行。

2.4 基准测试

安装后运行基准评估硬件：
`hashcat -b`

输出显示每算法速度（如 MD5：10 GH/s）。

第三章：基本用法与命令语法

3.1 通用语法
`hashcat [选项]... <哈希文件> [字典/掩码/目录]...`

- **核心选项**：
    - `-m <num>`：哈希类型（0=MD5，1000=NTLM）。
    - `-a <num>`：攻击模式（0=字典）。
    - `-o <file>`：输出破解结果。
    - `--show`：显示已破解哈希。
    - `-V`：版本；`-h`：帮助。

完整帮助：`hashcat -h | grep <关键词>`。

3.2 哈希类型查询

常见模式表（基于 2025 版）：

模式	名称	示例
0	MD5	8743b52063cd84097a65d1633f5c74f5
100	SHA1	da39a3ee5e6b4b0d3255bfef95601890afd80709

模式	名称	示例
1000	NTLM	b4b9b02e6f09a9bd760f388b67351e2b
3200	bcrypt	$2y 12 12 12KixfckDjul0d7/9F1Q2e4u…
17220	ZIP	$pkzip2$3*110*…
22000	WPA2	WPA*02*…

查询：`hashcat -h | grep ZIP`。

3.3 词典与规则

- **词典文件**：如 rockyou.txt（14M 常见密码）。下载自 GitHub SecLists。
- **规则**：修改词典词，如 best64.rule（添加数字/符号）。路径：`/usr/share/hashcat/rules/`。

第四章：攻击模式详解

Hashcat 支持 5 种主要模式，覆盖不同场景。

4.1 直攻/字典攻击 (-a 0)

使用词典逐词尝试。适合弱密码。

- 命令：`hashcat -m 0 -a 0 hashes.txt rockyou.txt`
- 带规则：`hashcat -m 0 -a 0 hashes.txt rockyou.txt -r rules/best64.rule`
- 示例：破解 MD5 哈希 `e99a18c428cb38d5f260853678922e03`（密码：password）。

4.2 组合攻击 (-a 1)

合并两个词典生成多词密码（如 “admin” + “123” = “admin123”）。

- 命令：`hashcat -m 0 -a 1 hashes.txt dict1.txt dict2.txt`

4.3 暴力/掩码攻击 (-a 3)

尝试所有组合。使用占位符：

占位符	字符集
?l	a-z
?u	A-Z
?d	0-9
?s	符号
?a	全 ASCII
?h	十六进制小写

- 示例：6 位数字：`hashcat -m 0 -a 3 hashes.txt ?d?d?d?d?d?d`
- 自定义：定义 ?1=?l?d，然后 `?1?1?1?1`。
- 增量：`-i --increment-min=4 --increment-max=8`（长度 4-8）。

4.4 混合攻击 (-a 6/7)

- **字典 + 掩码 (-a 6)**：词典后缀掩码。如：`hashcat -m 0 -a 6 hashes.txt rockyou.txt ?d?d`
- **掩码 + 字典 (-a 7)**：前缀词典。

4.5 关联攻击 (-a 9)

针对特定哈希，使用用户名/提示生成候选。适用于个性化密码。

第五章：高级技巧与优化

5.1 性能优化

- `-O`：启用优化内核（限 32 字符）。
- `--force`：忽略警告。
- `--self-test-disable`：跳过自检。
- 多设备：`-d 1,2` 指定 GPU。
- 分布式：使用 Hashtopolis 管理多机。

2025 提示：RTX 4090 下，MD5 达 100+ GH/s。过钟 GPU 提升 20%。

5.2 恢复与暂停

- 会话：`--session=session1`；恢复：`hashcat --session=session1 --restore`。
- Potfile：存储结果（`~/.local/share/hashcat/hashcat.potfile`）。禁用：`--potfile-disable`。

5.3 与其他工具集成

- **John the Ripper**：混合攻击。
- **Hash-Identifier**：自动检测类型。
- **脚本自动化**：Python 调用 `subprocess` 运行命令。

第六章：实际案例

6.1 破解 ZIP 文件密码

哈希：`$pkzip2$...` (模式 17220)。

```
hashcat -m 17220 zip.hash rockyou.txt -r rules/best64.rule -o cracked.txt
```

结果：显示明文。

6.2 WPA2 Wi-Fi 破解

捕获握手（aircrack-ng），转换为 hccapx。

```
hashcat -m 22000 wpa.hccapx rockyou.txt
```

常见密码如 “password123”。

6.3 NTLM 域密码

哈希：`user:b4b9b02e6f09a9bd760f388b67351e2b` (模式 1000)。

```
hashcat -m 1000 ntlm.hash ?a?a?a?a?a?a?a?a -i
```

暴力 8 字符。

第七章：最佳实践、提示与常见错误

7.1 最佳实践

- **从小到大**：先字典，后混合，再暴力。避免盲目全暴力。
- **规则优先**：用 best64.rule 扩展词典 10 倍。
- **监控温度**：GPU 过热用 `--hwmon-temp-abort=80`。
- **伦理**：仅授权使用；报告弱密码。
- **2025 更新**：集成 AI 生成词典，提升 30% 成功率。

7.2 提示

- 自定义掩码文件：存储多掩码，`-a 3 hashes.txt masks.txt`。
- 键盘布局：`--keyboard-layout-mapping` 处理区域密码。
- 云破解：AWS/GCP GPU 实例加速。

7.3 常见错误与解决方案

错误	原因	解决方案
No devices found	驱动缺失	安装 CUDA/OpenCL，重启。
Invalid attack mode	-a 值错	检查 -h 输出。
Mask too short	增量无效	确保掩码长度 >= --increment-max。
Slow speed	未优化	加 -O，检查 GPU 负载。
Hash not recognized	格式错	用 hash-identifier 验证。

结论：掌握 Hashcat，提升安全意识

Hashcat 是网络安全从业者的必备工具，通过本手册，可以从安装到高级应用全面掌握。记住：强大工具的双刃剑——用它强化防御，而非破坏。建议定期基准测试硬件，并探索 GitHub 更新。

参考资源：