

Hashcat example output

Output 1

Identifying the Hashing type for the password:

[illegible]

Output 2

Configuring the Hashcat tool with the attack and hash mode parameters:

```
(sly@sly)-[~/Cybersec/Pwd_cracking]
$ hashcat -a 0 -m 0 0c352d5b2f45217c57bef9f8452ce376 /usr/share/wordlists/rockyou.txt.gz
```

Output 3

Cracked password:

```
0c352d5b2f45217c57bef9f8452ce376:cricket1
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 0 (MD5)
Hash.Target.....: 0c352d5b2f45217c57bef9f8452ce376
Time.Started.....: Tue Feb 10 11:35:30 2026 (0 secs)
Time.Estimated...: Tue Feb 10 11:35:30 2026 (0 secs)
Kernel.Feature...: Pure Kernel (password length 0-256 bytes)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt.gz)
Guess.Queue.....: 1/1 (100.00%)
Speed.#01.....: 25043 H/s (0.39ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 8192/14344385 (0.06%)
Rejected.....: 0/8192 (0.00%)
Restore.Point....: 4096/14344385 (0.03%)
Restore.Sub.#01..: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#01...: newzealand -> whitetiger
```