[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@4edc1edcf4084a5bad4c8a63d48226cf?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

**CrackThe Hash With HashCat**

Hashcat is a password-cracking tool used for licit and illicit purposes.

Hashat is a particularly fast, efficient, and versatile hacking tool that assists brute-force attacks by conducting them with hash values of passwords that the tool is guessing or applying. When used for benign purposes, such as in penetration testing one’s own infrastructure, it can reveal compromised or easy-to-guess credentials.

Hashcat is, however, better known for being used for nefarious purposes. Hackers use Hashcat, readily available for download on all major operating systems, to automate attacks against passwords and other shared secrets. It gives the user the ability to brute-force credential stores using known hashes, to conduct dictionary attacks and rainbow tables, and to reverse engineer readable information on user behavior into hashed-password combination attacks.

**Example:**

“Breaches of complex passwords are on the rise as hackers use Hashcat as a means of cracking passwords using known hashes. This is next-level hacking that goes beyond the simple stuffing of credentials into username/password fields on web applications.”