

Cracking an encrypted or hashed password

How to crack a password knowing its stored form?

- Guessing attack (default and common passwords)
- Brute force attack
- Dictionary attack
- Rainbow tables

What are the counter-measures?

- Protect it well at the OS or application level
- Store it somewhere else (portable device, kerberos, ...)

Tool : John the Ripper

Password Strength

How strong is your password?

<http://howsecureismypassword.net/>

How long does it take to crack a password?

<http://www.lockdown.co.uk/?pg=combi>