Getting someone's password

How to get a password in clear?

- Social engineering - Phishing
- Data mining (emails, logs)
- Keyloggers (keystroke logging)

How to get an encrypted or hashed password?

- Know where it is stored

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, …)

Tools : John the Ripper, HashCat