

# Fonctions de hachage

## Exemples de hash de mots de passe

- SHA-256 simple:

5994471abb01112afcc18159f6cc74b4f511b99806da59b3caf5a9c173cacfc5

- Bcrypt (comme pour /etc/shadow) sous format \$<id>\$<cost>\$<salt><hash>:

\$2a\$12\$R9h/cIPz0gi.URNNX3kh20PST9/PgBkqquzi.Ss7KIUg02t0jWMUW

- PBKDF2 (technique standardisée) sous format <id>\$<cost>\$<salt><hash>:

pbkdf2-sha256\$216000\$3fIfQIweKGJy\$xHY3JKtPDdn/AktNbAwFKMQnBlrXnJyU04GElJKxEo=

- Argon2id (memory hard against GPU) sous format \$argon2id\$v=19\$m=65536,t=3,p=4\$<salt><hash>:

\$argon2id\$v=19\$m=65536,t=3,p=4\$G8NYSxrA+UMGHJbZVIXXXQ\$UrHyBcYfCEms+92QVzGmfYqrWtH54WJY9FuROBQi/X8

# Accélération par GPU

Certaines fonctions se prêtent bien au calcul parallèle

## Elcomsoft Distributed Password Recovery SHA-256

