Fonctions de hachage

Exemples de hash de mots de passe

- md5("12345") = `827ccb0eea8a706c4c34a16891f84e7b`
- md5(“12346”) = `a3590023df66ac92ae35e3316026d17d`
- Une petite modification dans l’entrée produit un hash complètement différent
- MD5 est insécure car trop rapide à calculer
- Un outil comme John the Ripper casse ces hash en quelques secondes sur un laptop
- Encore plus rapidement avec une carte graphique (GPU) et un outil comme Hashcat

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.URNNX3kh2OPST9/PgBkqquzi.Ss7KIUgO2t0jWMUW
```

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

```
pbkdf2-sha256$216000$3fIfQIweKGJy$xFHY3JKtPDdn/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
```