

Gagner l'accès





Gagner l'**accès** ?

- ◉ **Étape clé** du test d'intrusion
- ◉ Accès concret au système visé
- ◉ Utilisation d'une ou plusieurs vulnérabilités (humaines ou logicielles)
- ◉ Basée sur les informations trouvées dans les étapes précédentes



Diverses façons de gagner l'accès

- ◉ **Exploitation directe** d'une vulnérabilité logicielle (*Metasploit*)
- ◉ **Exploitation d'une faiblesse quelconque** (cracking de mdp, élévation de privilèges)
- ◉ **Utilisation de logiciels espions** (keyloggers)
- ◉ **Exploitation de la faille humaine** (ingénierie sociale)



Maintenir l'accès et se cacher

- ◉ Utilisation de programmes sur le système attaqué (Post-exploitation)
- ◉ Utilisation de portes dérobées pour se faciliter l'accès
- ◉ Suppression de fichiers logs/sauvegardes pour couvrir les traces



Éléments de prévention

- ◉ Utiliser une **politique de mot de passe** stricte
- ◉ Installer des **outils de sécurité** (antivirus, IDS...etc) et les **mettre à jour**
- ◉ Faire une veille constante (vérifier les modifications sur le système)
- ◉ Faire des **sauvegardes** régulières
- ◉ Rester **vigilant**