

# Projet :Pentest Toolbox

## Projet de fin de M1 Cybersécurité

### *Informations sur la Toolbox :*

Toolbox de Maxime Gaucher nommée «Cyber Tools»

Lien vers le GitHub : <https://github.com/Jhakatos/TheCTBprojet>

### *Rappel résumé du projet :*

Le projet concerne le développement d'une boîte à outils automatisée pour les tests d'intrusion, visant à simplifier et accélérer ce processus tout en améliorant la qualité des résultats.

Les points clés du projet sont les suivants :

#### 1. Objectif du projet :

- Concevoir et développer une boîte à outils (toolbox) automatisée pour la réalisation de tests d'intrusion.
- Simplifier le processus en automatisant de nombreuses tâches.
- Utiliser des techniques avancées d'analyse de vulnérabilités pour améliorer l'efficacité des tests.

#### 2. Fonctionnalités principales :

- Découverte de ports et services** : Identifier les ports et services en cours d'exécution sur le système cible.
- Détection de vulnérabilités** : Rechercher et identifier les vulnérabilités dans les ports et services détectés.
- Analyse de la sécurité des mots de passe** : Évaluer la sécurité des mots de passe utilisés.
- Tests d'authentification** : Vérifier la validité des identifiants et mots de passe.
- Exploitation de vulnérabilités** : Exploiter les vulnérabilités identifiées pour obtenir un accès non autorisé.
- Post-exploitation** : Analyser le système cible pour identifier les données sensibles et les mesures de sécurité.
- Reporting** : Générer des rapports détaillés et des visualisations graphiques des résultats des tests d'intrusion.

Le projet utilise des technologies modernes telles que Python et des bibliothèques orientées cybersécurité, permettant à l'utilisateur d'en faire usage sans une connaissance approfondie des tests d'intrusion ou des outils de cybersécurité.

L'objectif final étant de fournir à l'entreprise une solution efficace et automatisée pour réaliser des tests d'intrusion dans des délais plus courts, améliorant ainsi la satisfaction du client.