

Lab 03

Utilisation de Hack The Box (HTB)

Objectif :

Apprendre à utiliser la plateforme Hack The Box pour pratiquer le hacking éthique et comprendre les bases du pentesting, y compris la reconnaissance, l'exploitation des vulnérabilités et l'acquisition d'accès à une machine vulnérable.

Pré-requis

- Avoir un compte sur **Hack The Box** (HTB). Si vous n'en avez pas, vous devrez créer un compte en vous inscrivant sur <https://www.hackthebox.eu/>.
- Avoir un environnement de pentesting configuré, comme une machine virtuelle avec Kali Linux ou un autre système adapté.

Étape 1 : Connexion à Hack The Box

1. **Créer un compte HTB** : Si ce n'est pas déjà fait, inscrivez-vous sur la plateforme Hack The Box. Vous devrez résoudre un petit défi pour obtenir votre invitation.
2. **Accéder à l'interface** : Une fois votre compte validé, connectez-vous et familiarisez-vous avec l'interface utilisateur de HTB. Vous y trouverez des machines de différents niveaux de difficulté (comme "Beginner", "Medium", "Advanced").
3. Utiliser le VPN OpenVPN pour se connecter à l'infrastructure.
4. **Choisir une machine** : Choisissez une machine de niveau "**Easy**" ou "**Beginner**", par exemple "**Starting Point**" qui est une bonne machine d'introduction.

Étape 2 : Rapport et conclusion

1. **Rédaction d'un rapport** :
 - Une fois que vous avez réussi à obtenir un accès root ou que vous avez découvert des vulnérabilités intéressantes, rédigez un petit rapport sur votre expérience.
 - Votre rapport doit inclure :
 - Une brève description de la machine ciblée.
 - Les informations de reconnaissance collectées (ports ouverts, services, versions, etc.).

- Les vulnérabilités exploitées.
- Les étapes pour l'escalade de privilèges et l'obtention de l'accès complet.
- Les recommandations de sécurité pour la machine cible (même si c'est une machine d'entraînement, cela permet de pratiquer la rédaction de rapports).

2. Soumettre l'"I'm Root" Flag :

- Lorsque vous avez pris le contrôle de la machine, vous trouverez un fichier **"user.txt"** ou **"root.txt"** qui contiendra le flag. Ce flag est la preuve que vous avez bien réussi à exploiter la machine.
- Soumettez le flag pour valider la mission sur HTB.

Livrable

- Fourniture d'un document PDF qui reprends un guide explicatif des actions effectué dans les Labs avec également des captures d'écran.