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. **Choisir une machine** : Choisissez une machine de niveau **"Easy"** ou **"Beginner"**, par exemple **"Starting Point"** qui est une bonne machine d'introduction.

Étape 2 : Reconnaissance de la cible

1. **Scan avec Nmap** :
    - Ouvrez votre terminal (Kali ou autre) et utilisez Nmap pour scanner les ports et services de la machine cible de HTB.
    - Exemple de commande :

```
nmap -sV -p- [IP_de_la_machine_HTB]
```

    - Cela effectuera un scan complet des ports (de 1 à 65535) et affichera les services ouverts et leurs versions.
2. **Collecter les informations de base** :

- Prenez des notes sur les ports ouverts, les services, les versions, et d'autres informations pertinentes. Recherchez des failles potentielles en fonction des versions des services identifiés.

Étape 3 : Exploitation des vulnérabilités

1. **Utilisation de Gobuster** :
    - Effectuez un scan des répertoires web pour découvrir des fichiers ou des applications cachées sur le serveur web (si la machine a un serveur web actif).
    - Exemple de commande pour utiliser **Gobuster** :

ruby

gobuster dir -u http://[IP_de_la_machine_HTB] -w /usr/share/wordlists/dirb/common.txt

    - Cela va essayer de trouver des répertoires et des fichiers potentiellement vulnérables sur le serveur web.
2. **Exploitation d'une vulnérabilité** :
    - Si vous trouvez une vulnérabilité, utilisez un exploit approprié (par exemple, une injection SQL, un accès FTP avec un mot de passe faible, une vulnérabilité dans un service web, etc.).
    - Si la machine cible est vulnérable à un exploit connu (par exemple **CVE-2021-34527** pour Windows Print Spooler), tentez de l'exploiter pour obtenir un accès à la machine.
3. **Utilisation de Metasploit (optionnel)** :
    - Si vous trouvez une vulnérabilité que vous pouvez exploiter à l'aide de Metasploit, utilisez la commande suivante pour rechercher des exploits correspondants :

search [vuln_name]

    - Choisissez un exploit et suivez les instructions pour l'exécuter. Si l'exploit fonctionne, vous obtiendrez un **shell** ou un accès à la machine cible.

Étape 4 : Escalade de privilèges

1. **Vérification des privilèges** :
    - Une fois que vous avez obtenu un shell, vérifiez les privilèges dont vous disposez :
        - Si vous êtes un utilisateur normal, vous devrez peut-être rechercher des moyens d'**escalader les privilèges** et obtenir un accès root.
        - Commandes utiles : whoami, id, sudo -l.
2. **Exploitation d'une faille d'escalade de privilèges** :

- Si vous êtes limité à un compte utilisateur, recherchez des **failles locales** d'escalade de privilèges (par exemple, des fichiers SUID mal configurés, des commandes avec des permissions de sudo incorrectes, etc.).
- Utilisez des outils comme **LinPEAS** (sur la machine Kali) pour rechercher des vulnérabilités locales d'escalade de privilèges :

wget https://github.com/carlospolop/PEASS-ng/releases/download/20210529/linpeas.sh

chmod +x linpeas.sh

./linpeas.sh

Étape 5 : 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.