**TRAVAUX PRATIQUES: METASPLOIT**

Prérequis :
- Machine Kali Linux fonctionnelle.
- Machine Metasploitable 2 déployée.
- Les deux machines doivent être sur le même réseau.
- Créez un réseau local sur votre machine (préférence pour VirtualBox/VMware), et attribuez des adresses IP statiques aux deux machines pour vous faciliter les tests.

-

**TP 1 : Découverte de Metasploitable 2 et exploitation basique avec Metasploit**

Objectifs pédagogiques :
- Apprendre à lancer Metasploit Framework.
- Effectuer un scan de base avec des outils comme Nmap.
- Identifier des services vulnérables.
- Exploiter une vulnérabilité présente sur VSFTPd.

Exercices :

1.Découverte de la cible :
- Trouvez l'adresse IP de Metasploitable 2 sur votre réseau local.
- Réalisez un scan Nmap pour identifier les ports ouverts sur cette machine.
- Comparez les résultats avec ceux d'un scan réalisé avec Metasploit (utilisez le module `auxiliary/scanner/portscan/tcp`).

2.Utilisation de Metasploit :
- Lancez la console Metasploit Framework (`msfconsole`).
- Recherchez les exploits disponibles pour le service VSFTPd.
- Configurez et lancez l'exploit pour obtenir un accès à la cible.

3. Exploration approfondie :
- Une fois connecté, explorez le système compromis :
  - Listez les utilisateurs et les processus actifs.
  - Recherchez des fichiers sensibles sur la machine cible.
  - Identifiez s'il existe des informations permettant une élévation de privilèges.

4.Questions :
- Quels sont les ports principaux ouverts sur Metasploitable 2 ?
- Quelle version de VSFTPd est vulnérable ?
- Quel type de shell obtenez-vous après exploitation ?

- Quels sont les risques associés à une vulnérabilité comme celle de VSFTPd ?

5. Challenge bonus :
- Modifiez le payload utilisé dans l'exploit pour tester d'autres options (par exemple, un payload encodé pour éviter la détection).

**TP 2 : Exploitation d'une vulnérabilité Samba avec Metasploit**

Objectifs pédagogiques :
- Identifier et exploiter des vulnérabilités liées à Samba.
- Utiliser des payloads Metasploit pour obtenir un accès distant.
- Comprendre les mécanismes d'élévation de privilèges.

Exercices :

1.Reconnaissance :
- Effectuez un scan ciblé des ports Samba (139, 445) à l'aide de Nmap et identifiez les services.
- Utilisez Nmap avec des scripts comme `nmap --script smb*` pour obtenir davantage d'informations.
- Listez les partages Samba disponibles avec Metasploit.

2. Recherche de vulnérabilités :
- Recherchez les exploits Samba disponibles dans Metasploit.
- Identifiez l'exploit "username map script" et analysez ses options requises.
- Recherchez d'autres exploits Samba et documentez leurs fonctionnalités.

3. Exploitation :
- Configurez et exécutez l'exploit "username map script".
- Utilisez un payload adapté pour établir une session.
- Une fois connecté, tentez une élévation de privilèges pour obtenir un accès administrateur.

4. Défis supplémentaires :
- Essayez d'exploiter Samba avec un autre outil que Metasploit (comme `smbclient` ou `rpcclient`).
- Identifiez les fichiers sensibles accessibles via les partages réseau.

5. Questions :
- Pourquoi Samba est-il une cible fréquente ?
- Quelle est la différence entre les ports 139 et 445 ?
- Quel est l'impact potentiel de cette vulnérabilité ?
- Quels mécanismes Samba pourrait-on mettre en place pour réduire ces risques ?

6. Challenge bonus :

- Configurez un exploit personnalisé pour tester des payloads encodés.
- Automatisez l'exploitation avec un script Metasploit (`resource script`).

**TP 3 : Exploitation de Apache Tomcat Manager avec Metasploit**

Objectifs pédagogiques :
- Comprendre la gestion des serveurs d'applications Java.
- Pratiquer l'énumération des services web.
- Exploiter les identifiants par défaut pour compromettre une cible.
- Déployer un payload via une interface d'administration.

Exercices :

1. Reconnaissance Web :
- Identifiez le port sur lequel Tomcat est actif (par exemple, via un scan Nmap).
- Accédez à l'interface de gestion Tomcat Manager via un navigateur.
- Énumérez les pages web disponibles ainsi que les répertoires accessibles.

2. Recherche d'accès :
- Créez un dictionnaire d'identifiants faibles (ou utilisez un existant).
- Testez ces identifiants avec des outils comme Hydra ou Metasploit.
- Identifiez la version de Tomcat en cours d'exécution.

3.Exploitation Metasploit :
- Recherchez les exploits disponibles pour Tomcat Manager dans Metasploit.
- Configurez les identifiants découverts pour accéder à l'interface de gestion.
- Déployez un shell distant en utilisant un payload adapté.
- Établissez une session stable et explorez le système compromis.

4. Défis supplémentaires :
- Testez une élévation de privilèges après avoir compromis la machine.
- Essayez des méthodes manuelles (hors Metasploit) pour exploiter l'interface Tomcat.
- Trouvez des fichiers sensibles ou des configurations mal sécurisées sur le serveur.

5. Questions :
- Pourquoi Tomcat est-il une cible attractive pour les attaquants ?
- Quels sont les risques d'utiliser des identifiants par défaut ?
- Comment sécuriser un serveur Tomcat efficacement ?
- Quels mécanismes peuvent empêcher ce type d'attaque à l'avenir ?

6. Challenge bonus :
- Exploitez une autre vulnérabilité présente sur Tomcat (par exemple, via des fichiers de configuration mal configurés ou des vulnérabilités spécifiques à une version).

- Automatisez l'exploitation et la post-exploitation avec un script Metasploit.

**TP 4 : Exploitation avancée et persistance sur Metasploitable 2**

Objectifs pédagogiques :
- Tester des vulnérabilités multiples sur une même machine.
- Configurer des backdoors pour maintenir un accès persistant.
- Étudier des outils de post-exploitation.

Exercices :

1. Exploitation multiple :
- Identifiez au moins trois services vulnérables différents sur Metasploitable 2.
- Exploitez-les successivement avec Metasploit ou d'autres outils.
- Comparez les résultats des différentes sessions obtenues.

2. Persistance :
- Configurez un backdoor pour maintenir un accès à la machine (ex. : via Metasploit ou Netcat).
- Testez si le backdoor persiste après un redémarrage de la machine cible.

3. Post-Exploitation avancée :
- Explorez les fichiers système, les configurations réseau, et les logs.
- Exfiltrez des données critiques (ex. : mots de passe, fichiers sensibles).
- Identifiez des vecteurs pour attaquer d'autres machines sur le réseau.

4. Challenge bonus :
- Automatisez tout le processus (scanning, exploitation, persistance et post-exploitation) via un script Metasploit ou Python.