Lab 01

Kali Linux

Objectif de l'exercice :

1. Installer une VM avec Kali Linux

Pré-requis :

Avant de commencer, assurez-vous d'avoir les éléments suivants :

- **Téléchargement de Kali Linux** : Allez sur le site officiel de Kali Linux (https://www.kali.org/downloads/) et téléchargez l'image ISO de la dernière version stable. Vous pouvez choisir entre une version 32 bits ou 64 bits en fonction de votre machine.
- **Téléchargement de Metaplsoitable** : Sur le site officiel (https://sourceforge.net/projects/metasploitable/files/latest/download) télécharger l'iso afin de pouvoir monter ensuite une machine virtuelle.
- **Virtualisation** : Pour une installation dans une machine virtuelle, utilisez un logiciel comme **VirtualBox** ou **VMware**. Téléchargez et installez l'une de ces plateformes avant de commencer.

Étape 1 : Sur une machine virtuelle (VM)

1. **Créer une nouvelle machine virtuelle** :
    - Ouvrez **VirtualBox** ou **VMware**, puis créez une nouvelle machine virtuelle avec les paramètres suivants :
        - **Nom** : Kali Linux
        - **Type** : Linux
        - **Version** : Debian (64-bit)
        - **Mémoire** : Attribuez 2 Go de RAM ou plus.
        - **Disque dur** : Créez un disque dur virtuel avec au moins 20 Go d'espace.
2. **Monter l'image ISO** :
    - Dans la configuration de la VM, montez l'image ISO de Kali Linux comme lecteur de CD/DVD.
3. **Démarrer la machine virtuelle** :

- Lancez la machine virtuelle. Le processus d'installation est similaire à celui d'une installation physique.

Étape 2 : Sur une machine virtuelle (VM)

1. **Créer une nouvelle machine virtuelle** :
    - Ouvrez **VirtualBox** ou **VMware**, puis créez une nouvelle machine virtuelle avec les paramètres suivants :
        - **Nom** : Metasploitable
        - **Type** : Linux
        - **Version** : Debian (64-bit)
        - **Mémoire** : Attribuez 2 Go de RAM ou plus.
        - **Disque dur** : Créez un disque dur virtuel avec au moins 20 Go d'espace.
2. **Monter l'image ISO** :
    - Dans la configuration de la VM, montez l'image ISO de Metaslpoitable comme lecteur de CD/DVD.
3. **Démarrer la machine virtuelle** :
    - Lancez la machine virtuelle. Le processus d'installation est similaire à celui d'une installation physique.

Étape 3 : Prise en main de Kali Linux

Une fois Kali Linux installé et démarré, vous serez accueilli par un écran de connexion.

1. Se connecter au système

- **Utilisateur par défaut** :
    - **Nom d'utilisateur** : kali
    - **Mot de passe** : kali (c'est un mot de passe par défaut, à changer après l'installation).
    - **Super utilisateur (root)** : Si vous avez configuré un compte root pendant l'installation, vous pouvez vous connecter directement avec ces identifiants. Cependant, sur les versions récentes de Kali, il est recommandé de se connecter avec un compte utilisateur normal et de privilégier sudo pour les droits administratifs.

2. Mettre à jour Kali Linux

Une fois que vous êtes connecté, il est essentiel de mettre à jour Kali pour obtenir les derniers correctifs et mises à jour de sécurité.

sudo apt update && sudo apt upgrade

- **Explication** :

- apt update : Met à jour la liste des paquets disponibles.
- apt upgrade : Met à jour les paquets installés.

3. Interface graphique et outils

Kali Linux propose plusieurs environnements de bureau. Par défaut, il utilise **Xfce**, un environnement léger et performant. Cependant, vous pouvez installer d'autres environnements graphiques comme GNOME ou KDE si vous le souhaitez.

Vous trouverez une variété d'outils dans les menus de Kali Linux :

- **Applications > Kali Linux** : La section contenant tous les outils de sécurité.
  - **Information Gathering** : Outils pour l'information sur les réseaux (par exemple, **Nmap**, **Whois**).
  - **Vulnerability Analysis** : Outils pour l'analyse de vulnérabilités (par exemple, **Nessus**, **OpenVAS**).
  - **Exploitation Tools** : Outils pour exploiter des vulnérabilités (par exemple, **Metasploit**).
  - **Forensics** : Outils de forensic pour analyser les systèmes compromis.
  - **Sniffing & Spoofing** : Outils pour l'analyse des réseaux et les attaques par injection (par exemple, **Wireshark**, **Ettercap**).

4. Utiliser le terminal

Le terminal est l'outil principal de Kali pour interagir avec le système. Vous pouvez l'ouvrir en cliquant sur l'icône du terminal dans le menu ou en utilisant le raccourci Ctrl + Alt + T.

Quelques commandes de base :

- **ls** : Liste les fichiers dans le répertoire courant.
- **cd [répertoire]** : Change de répertoire.
- **mkdir [nom du répertoire]** : Crée un répertoire.
- **rm [fichier]** : Supprime un fichier.
- **man [commande]** : Affiche le manuel d'une commande.
- **sudo [commande]** : Exécute une commande avec des privilèges root.

5. Configurer le réseau

Assurez-vous que Kali Linux est bien connecté à votre réseau local ou à Internet :

- Si vous êtes dans une VM, vérifiez les paramètres de votre carte réseau dans **VirtualBox** ou **VMware** pour vous assurer que la machine virtuelle dispose d'une interface réseau valide (NAT ou pont).
- Si vous êtes sur une machine physique, vous pouvez configurer votre réseau en utilisant NetworkManager ou directement en modifiant les fichiers de configuration réseau.

Étape 4 : Utilisation de quelques outils de Kali Linux

Metasploit Framework

Metasploit est un framework puissant pour l'exploitation de vulnérabilités. Voici comment le lancer :

msfconsole

Une fois dans Metasploit, vous pouvez rechercher des exploits disponibles :

search [nom de l'exploit]

Pour lancer un exploit, il suffit de le configurer et de l'exécuter :

use [exploit]

set RHOST [cible]

run

Nmap

Nmap est l'outil de scanner de réseau. Pour scanner un réseau, utilisez la commande suivante :

nmap -sP 192.168.1.0/24

Cette commande scanne tous les hôtes actifs sur le réseau 192.168.1.0.

Wireshark

Wireshark est un outil de capture de paquets. Pour l'utiliser, lancez-le avec les privilèges root :

sudo wireshark

Sélectionnez l'interface réseau à surveiller, puis commencez la capture pour analyser les paquets en temps réel.

Etape 5 : Sécurisation de Kali Linux

Une fois que Kali est installé, il est important de le sécuriser avant de commencer les tests de pénétration. Quelques étapes clés :

1. **Modifier le mot de passe root** : Changez immédiatement le mot de passe par défaut.
2. **Configurer un pare-feu** : Activez ufw (Uncomplicated Firewall) pour protéger votre machine.

sudo ufw enable

3. **Mettre en place une sauvegarde régulière** : Enregistrez les configurations et les données importantes régulièrement.

Livrable

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