[Exploitation/Réseau] Pwncat

Introduction

Cet outil vise à fournir la même fonction que netcat avec des fonctions supplémentaires très pratiques lors de vos tests d'intrusion.

Installation

Voici la commande pour installer **pwncat** dans un environnement virtuel :

```
python3 -m venv /opt/pwncat && /opt/pwncat/bin/pip install pwncat-cs && ln -s /opt/pwncat/bin/pwncat-cs /usr/local/bin
```

Manuel

Documentation officielle

- Pwncat documentation

Lancer un listener

- Voici la première méthode pour le faire

```
pwncat-cs -lp <PORT>
```

- Ou la deuxième (depuis le mode interractif) :

```
pwncat-cs
```

```
listen -m linux <PORT>
```

Sélection d'une session

Depuis le mode interractif :

```
sessions <NUMBER>
```

Passer du mode local à remote

Une fois votre connexion établie, vous pourrez basculer du mode **local** (shell local de votre machine) au mode **remote** (shell distant de la machine compromise).

Pour basculer d'un mode à l'autre il vous suffit d'utiliser la combinaison **CTRL+D**.

Upload

Plus besoin de bricoler pour transférer des fichiers de votre machine vers la machine distante, vous pouvez utiliser la commande upload **depuis le mode local** pour téléverser un fichier dans le répertoire courant de la session distante:

```
upload <FILE>
```

Download

De la même manière vous pouvez récupérer des fichiers distants sur votre machine locale (cela peut être utile pour les analyser) :

```
download <FILE>
```

Revision #5
Created 11 December 2023 16:29:38 by Elieroc

Updated 3 May 2024 13:14:39 by Elieroc