

# Netcat



## 1) Introduction

Netcat (souvent abrégé en nc) est un outil en ligne de commande utilisé pour lire et écrire des données sur des connexions réseau en utilisant les protocoles TCP ou UDP. Netcat est utilisé pour le diagnostic réseau, le transfert de fichiers, l'écoute de ports et les tests de sécurité.

## 2) Fonctionnalités principales

- Connexion et écoute de ports TCP/UDP
- Scan de ports
- Transfert de fichiers
- Création de shell distant
- Test et débogage des connexions réseau
- Serveur HTTP basique

## 3) Installation de Netcat

Netcat est préinstallé sur de nombreuses distributions Linux :

```
sudo apt update  
sudo apt install netcat
```

## 4) Utilisation de Netcat

### Ecouter un port (mode serveur)

Netcat peut être utilisé pour écouter un port sur une machine et attendre des connexions entrantes avec la commande `nc -lvp 1234`

- `-l` : Mode écoute (serveur).
- `-v` : Mode verbeux (affiche les détails de la connexion).

- -p : Spécifie le port.

## Se connecter à un serveur (mode client)

Depuis une autre machine ou terminal, connectez-vous au serveur Netcat avec `nc IP_du_serveur 1234`

Une fois connecté, tout ce que vous tapez sera envoyé à l'autre machine.

## Scanner des ports ouverts

Netcat peut être utilisé comme un scanner de ports de base avec `nc -zv IP_du_serveur 20-100`

- -z : Mode scan (sans envoyer de données).
- -v : Mode verbeux
- 20-100 : Plage de ports à tester.

Transfert de fichiers

- Envoyer un fichier

Sur la machine qui envoie : `cat fichier.txt | nc IP_du_serveur 1234`

- Recevoir un fichier

Sur la machine qui reçoit : `nc -lvp 1234 > fichier_recu.txt`

## 5) Exercice

Je veux tester la communication réseau entre une machine virtuelle Kali Linux et Windows avec Netcat.

D'abord, je vérifie l'adresse IP de chaque machine :

- ifconfig sur Kali
- ipconfig sur Windows

```
(lea@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 172.20.5.109  netmask 255.255.252.0  broadcast 172.20.7.255
    inet6 fe80::a00:27ff:feb9:2523  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:b9:25:23  txqueuelen 1000  (Ethernet)
    RX packets 2136  bytes 600739 (586.6 KiB)
    RX errors 0  dropped 1  overruns 0  frame 0
    TX packets 276  bytes 35218 (34.3 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 4  bytes 240 (240.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 4  bytes 240 (240.0 B)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

```
C:\Windows\system32>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::8db4:5dd1:8249:9d84%8
    Adresse IPv4. . . . . : 172.20.5.111
    Masque de sous-réseau. . . . . : 255.255.252.0
    Passerelle par défaut. . . . . : 172.20.7.254

C:\Windows\system32>
```

J'utilise Netcat pour établir une communication entre les machines.

Sur Kali, j'exécute cette commande : netcat -nvlp 5000.

➔ Kali attend une connexion entrante sur le port 5000.

```
(lea@kali)-[~]
$ sudo su
[sudo] password for lea:
(root@kali)-[/home/lea]
# netcat -nvlp 5000
listening on [any] 5000 ...
ncat connect to [172.20.5.109] from (UNKNOWN) [172.20.5.111] 3478
allo
█
```

Sur Windows, j'exécute cette commande : ncat 172.20.5.109 5000.

➔ Windows se connecte à Kali, je peux prendre le contrôle de Windows depuis Kali.

```
C:\Windows\System32\netcat-1.11>ncat 172.20.5.109 5000
allo
```

Ensuite, j'envoie un fichier texte.

Avec la commande suivante, je met Kali en écoute sur le port 5000 puis je sauvegarde la sortie reçue dans le fichier output.txt.

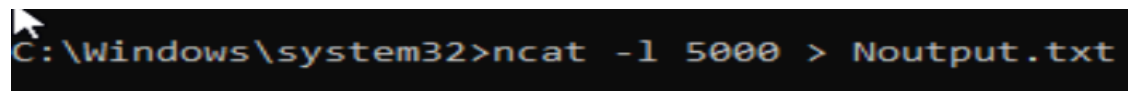
```
(root@kali)-[/home/lea]
# netcat -nvlp 5000 -oNoutput.txt
listening on [any] 5000 ...
connect to [172.20.5.109] from (UNKNOWN) [172.20.5.111] 3673
bonjour
je suis connecté
ok
█
```

Sur Windows, j'exécute une commande pour me connecter à Kali sur le port 5000 puis j'envoie le contenu de fichier.txt à Kali.

```
C:\Windows\System32\netcat-1.11>ncat 172.20.5.109 5000
bonjour
je suis connecté-
ok
```

```
~\Noutput.txt [Read Only] - Mousepad
File Edit Search View Document Help
1 | 00000000 62 6f 6e 6a 6f 75 72 0a # bonjour.
2 > 00000000 6a 65 20 73 75 69 73 20 63 6f 6e 6e 65 63 74 c3 # je suis connect.
3 > 00000010 a9 0a # ..
4 < 00000008 6f 6b 0a # ok.
5
```

J'envoie le fichier texte à l'autre machine.

A screenshot of a Windows command prompt window. The text displayed is 'C:\Windows\system32>ncat -l 5000 > Noutput.txt'. A mouse cursor is visible at the beginning of the command line.

```
C:\Windows\system32>ncat -l 5000 > Noutput.txt
```