MATHÉO GENSSE

BLOG.MATHEOGENSSE.FR

COMMANDES

Nmap

DERNIÈRE MODIFICATION LE

3 mai 2026

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

-

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

MATHÉO GENSSE
blog.matheogensse.fr

SOMMAIRE

TYPES DE SCAN (TCP)

Commande	Description
nmap -sS <cible>	Scan SYN furtif (TCP half-open)
nmap -sT <cible>	Scan TCP Connect complet (moins furtif)
nmap -sA <cible>	Scan ACK (détecte les règles de pare-feu)
nmap -sW <cible>	Scan Window (détecte les ports ouverts/filtrés)
nmap -sM <cible>	Scan Maimon (FIN/ACK)
nmap -sN <cible>	Scan Null (aucun flag TCP)
nmap -sF <cible>	Scan FIN (flag FIN)
nmap -sX <cible>	Scan Xmas (FIN + PSH + URG)
nmap --scanflags <flags> <cible>	Scan personnalisé avec flags TCP spécifiques

COMMANDES DE NMAP

TYPES DE SCAN (UDP & AUTRES)

Commande	Description
nmap -sU <cible>	Scan UDP
nmap -sY <cible>	Scan SCTP INIT
nmap -sZ <cible>	Scan SCTP COOKIE ECHO
nmap -sO <cible>	Scan de protocoles IP
nmap -b <relais>	Scan par rebond FTP

COMMANDES DE NMAP

DÉTECTION & IDENTIFICATION

Commande	Description
nmap -sV <cible>	Détection des versions des services
nmap -sV --version-intensity <0-9> <cible>	Niveau d'intensité pour la détection de version
nmap -sV --version-light <cible>	Détection rapide (intensité 2)
nmap -sV --version-all <cible>	Détection complète (intensité 9)
nmap -O <cible>	Détection du système d'exploitation
nmap -O --osscan-guess <cible>	Détection OS plus agressive
nmap -A <cible>	Scan agressif (OS + versions + scripts + traceroute)

SPÉCIFICATION DES PORTS

Commande	Description
nmap -p <port(s)> <cible>	Scanner des ports spécifiques
nmap -p <début-fin> <cible>	Scanner une plage de ports
nmap -p- <cible>	Scanner tous les ports (1-65535)
nmap -p http,https,ssh <cible>	Scanner par noms de services
nmap --top-ports <n> <cible>	Scanner les n ports les plus courants
nmap -p- --min-rate 10000 <cible>	Scan rapide de tous les ports (10k paquets/seconde)

DÉCOUVERTE D'HÔTES

Commande	Description
nmap -sn <cible>	Ping scan (découverte d'hôtes, pas de scan de port)
nmap -Pn <cible>	Scan sans ping (considère tous hôtes actifs)
nmap -PS <port> <cible>	Ping SYN sur un port spécifique
nmap -PA <port> <cible>	Ping ACK sur un port spécifique
nmap -PU <port> <cible>	Ping UDP sur un port spécifique
nmap -PE <cible>	Ping ICMP Echo Request
nmap -PP <cible>	Ping ICMP Timestamp
nmap -PM <cible>	Ping ICMP Netmask
nmap -PR <cible>	Ping ARP (sur réseau local, très efficace)
nmap -n <cible>	Pas de résolution DNS
nmap -R <cible>	Résolution DNS pour tous les hôtes
nmap --dns-servers <serveurs> <cible>	Utiliser des DNS spécifiques

SCRIPTS NSE

Commande	Description
nmap -sC <cible>	Exécuter les scripts Nmap par défaut
nmap --script <script> <cible>	Exécuter un script spécifique
nmap --script <catégorie> <cible>	Exécuter tous les scripts d'une catégorie
nmap --script-help <script> <cible>	Afficher l'aide d'un script
nmap --script-args <args> <cible>	Passer des arguments aux scripts
nmap --script-trace <cible>	Tracer l'exécution des scripts
nmap --script-updatedb	Mettre à jour la base de données des scripts

COMMANDES DE NMAP

TIMING & PERFORMANCE

Commande	Description
nmap -T0 <cible>	Très lent (paranoïde, contourne IDS)
nmap -T1 <cible>	Lent (discret)
nmap -T2 <cible>	Modéré (comportement par défaut)
nmap -T3 <cible>	Normal (par défaut)
nmap -T4 <cible>	Rapide (réseau fiable)
nmap -T5 <cible>	Très rapide (peut manquer des ports)
nmap --min-hostgroup <n> <cible>	Nombre minimum d'hôtes à scanner
nmap --max-hostgroup <n> <cible>	Nombre maximum d'hôtes à scanner
nmap --min-parallelism <n> <cible>	Nombre minimum de probes en parallèle
nmap --max-retries <n> <cible>	Nombre maximum de retransmissions
nmap --host-timeout <temps> <cible>	Timeout par hôte
nmap --scan-delay <temps> <cible>	Délai entre chaque probe
nmap --min-rate <n> <cible>	Envoi minimum de n paquets/seconde
nmap --max-rate <n> <cible>	Envoi maximum de n paquets/seconde

COMMANDES DE NMAP

FICHIERS (ENTRÉE/SORTIE)

Commande	Description
nmap -oN <fichier> <cible>	Sortie normale dans un fichier
nmap -oX <fichier> <cible>	Sortie XML dans un fichier
nmap -oS <fichier> <cible>	Sortie script kiddie (format bâclé)
nmap -oG <fichier> <cible>	Sortie grepable (fichier texte)
nmap -oA <basename> <cible>	Sortie sous les 3 formats (normal, XML, grepable)
nmap --append-output <cible>	Ajouter la sortie à un fichier existant
nmap -iL <fichier> <cible>	Scanner depuis une liste d'hôtes (un par ligne)
nmap -iR <n> <cible>	Générer n adresses aléatoires
nmap --exclude <cibles> <cible>	Exclure certaines cibles
nmap --excludefile <fichier> <cible>	Exclure les cibles d'un fichier

COMMANDES DE NMAP

ÉVASION & FURTIVITÉ

Commande	Description
nmap -D <IPs> <cible>	Scan avec décoys (usurpation d'IPs)
nmap -S <IP> <cible>	Usurper l'adresse IP source
nmap -e <interface> <cible>	Utiliser une interface spécifique
nmap --source-port <port> <cible>	Utiliser un port source spécifique
nmap --data-length <n> <cible>	Ajouter n octets aléatoires aux paquets
nmap --ttl <n> <cible>	Définir le TTL (Time To Live)
nmap --randomize-hosts <cible>	Randomiser l'ordre des hôtes
nmap --spoof-mac <MAC> <cible>	Usurper l'adresse MAC
nmap --spoof-mac 0 <cible>	Générer une MAC aléatoire
nmap --badsum <cible>	Envoyer des paquets avec checksum invalide

FIREWALL & IDS

Commande	Description
nmap -sA <cible>	Scan ACK (détecte les règles de pare-feu)
nmap -sW <cible>	Scan Window avancé pour pare-feu
nmap -f <cible>	Fragmenter les paquets (petits fragments)
nmap -ff <cible>	Fragmenter en très petits paquets (8 bytes)
nmap --mtu <n> <cible>	Fragmenter avec taille MTU spécifique

IPV6

Commande	Description
nmap -6 <cible>	Scanner en IPv6
nmap -6 -sS <cible>	Scan SYN en IPv6

FIREWALL NSE

Commande	Description
nmap --script firewall-bypass <cible>	Détection de contournement de pare-feu

MISC & UTILITAIRES

Commande	Description
nmap --iflist	Lister les interfaces réseau
nmap --stats-every <temps> <cible>	Afficher les stats toutes les n secondes
nmap -v <cible>	Mode verbeux
nmap -vv <cible>	Mode très verbeux
nmap -d <cible>	Mode debug
nmap -dd <cible>	Mode debug intense
nmap --reason <cible>	Afficher la raison de l'état des ports
nmap --open <cible>	Afficher uniquement les ports ouverts
nmap --packet-trace <cible>	Tracer tous les paquets envoyés/reçus
nmap --webxml <cible>	Utiliser la DTD XML de nmap.org
nmap --resume <fichier> <cible>	Reprendre un scan interrompu
nmap -h	Afficher l'aide
nmap -h <catégorie>	Afficher l'aide pour une catégorie