

Référence rapide nmap

Analyse de ports, découverte d'hôtes, détection de services et scripts NSE

Analyses de base

Cibles d'analyse

```
nmap 192.168.1.1 # hôte unique
nmap 192.168.1.0/24 # sous-réseau complet
nmap 192.168.1.1-50 # plage d'IP
nmap -iL targets.txt # hôtes depuis un fichier
```

Spécification des cibles

```
192.168.1.1 Adresse IP unique
192.168.1.0/24 Notation CIDR (256 hôtes)
192.168.1.1-254 Plage d'IP
example.com Nom d'hôte (résolu en IP)
-iL file.txt Lire les cibles depuis un fichier
--exclude 192.168.1.1 Exclure des hôtes spécifiques
--excludefile skip.txt Exclure des hôtes depuis un fichier
```

Analyse de ports

Types d'analyse

```
-sS Analyse TCP SYN (défaut, furtive, nécessite root)
-sT Analyse TCP connect (handshake complet, sans root)
-sU Analyse UDP (lente, souvent filtrée)
-sA Analyse TCP ACK (détecter les pare-feux)
-sN Analyse TCP NULL (aucun flag)
-sF Analyse TCP FIN (flag FIN uniquement)
-sX Analyse Xmas (flags FIN+PSH+URG)
```

Sélection de ports

```
nmap -p 80,443 target # ports spécifiques
nmap -p 1-1000 target # plage de ports
nmap -p- target # les 65535 ports
nmap --top-ports 100 target # les 100 ports les plus courants
```

États des ports

```
open Une application accepte les connexions
closed Port accessible mais aucun service en écoute
filtered Pare-feu bloquant, état indéterminable
unfiltered Port accessible, état ouvert/fermé inconnu
open|filtered Impossible de déterminer si ouvert ou filtré
```

Découverte d'hôtes

Méthodes de découverte

```
-sn Analyse ping uniquement (sans analyse de ports)
-Pn Ignorer la découverte (traiter tous comme actifs)
-PS 80,443 Découverte TCP SYN sur ports
-PA 80 Découverte TCP ACK
-PU 53 Découverte UDP
-PE Requête echo ICMP
-PR Découverte ARP (réseau local)
```

Balayage réseau

```
nmap -sn 192.168.1.0/24 # balayage ping du sous-réseau
nmap -sn -n 10.0.0.0/24 # balayage, sans DNS
nmap -sn -PR 192.168.1.0/24 # analyse ARP (la plus rapide)
```

Détection de services

Détection de versions

```
nmap -sV target # détecter les versions de service
nmap -sV --version-intensity 5 target # sondage plus profond
nmap -sV --version-all target # essayer toutes les sondes (lent)
nmap -A target # OS + version + scripts + traceroute
```

Options de détection

```
-sV Sonder les ports ouverts pour service/
version
--version-intensity 0-9 Intensité du sondage (défaut 7)
--version-light Sondage léger (intensité 2)
--version-all Essayer toutes les sondes (intensité 9)
-A Agressif: -sV -O --script=default -traceroute
-sC Exécuter les scripts NSE par défaut
```

Détection de système d'exploitation

Empreinte OS

```
nmap -O target # détection OS (nécessite root)
nmap -O --osscan-limit target # analyser uniquement les hôtes
prometteurs
nmap -O --osscan-guess target # estimation agressive de l'OS
nmap -A target # inclut la détection OS
```

Options de détection OS

```
-O Activer la détection OS
--osscan-limit Ignorer les hôtes sans ports TCP ouverts+fermés
--osscan-guess Deviner l'OS plus agressivement
--max-os-tries N Nombre maximal de tentatives de détection par hôte
```

Scripts (NSE)

Utilisation des scripts

```
nmap --script=default target # catégorie par défaut
nmap --script=vuln target # scripts de vulnérabilités
nmap --script=http-headers target
nmap --script="http-*" target # correspondance générique
```

Catégories de scripts

```
default Scripts sûrs et utiles (raccourci -sC)
vuln Vérifier les vulnérabilités connues
safe Scripts non intrusifs
intrusive Peut planter les cibles ou déclencher les IDS
discovery Découverte réseau et de services
auth Vérifications liées à l'authentification
brute Test de credentials par force brute
exploit Tentatives d'exploitation active
```

Scripts utiles

```
http-title Récupérer les titres des pages web
ssl-cert Afficher les détails du certificat SSL
ssh-hostkey Afficher les empreintes des clés SSH
dns-brute Énumérer les sous-domaines DNS
smb-os-discovery Détecter l'OS Windows via SMB
vuln Exécuter toutes les vérifications de vulnérabilités
```

Formats de sortie

Options de sortie

```
nmap -oN scan.txt target # sortie texte normale
nmap -oX scan.xml target # sortie XML
nmap -oG scan.gnmap target # sortie greppable
nmap -oA scan_all target # tous les formats à la fois
```

Options de sortie

```
-oN file Sortie normale vers fichier
-oX file Sortie XML (pour outils/analyse)
-oG file Sortie greppable (un hôte par ligne)
-oA basename Trois formats (basename.nmap/xml/gnmap)
-v Augmenter la verbosité (-vv pour plus)
-d Sortie de débogage (-dd pour plus)
--open Afficher uniquement les ports ouverts
--reason Afficher la raison de l'état du port
```

Timing et performances

Gabarits de timing

```
-T0 (paranoïaque) Très lent, évasion IDS (5 min entre sondes)
-T1 (furtif) Lent, évasion IDS (15 sec entre sondes)
-T2 (poli) Vitesse réduite, moins de bande passante
-T3 (normal) Timing par défaut
-T4 (agressif) Rapide, suppose un réseau fiable
-T5 (insensé) Le plus rapide, peut manquer des résultats
```

Réglage fin

```
--min-rate 1000 Envoyer au moins 1000 paquets/sec
--max-rate 500 Limiter à 500 paquets/sec
--max-retries 2 Retransmissions maximales de sondes
--host-timeout 30m Ignorer l'hôte si l'analyse dépasse 30 min
--scan-delay 1s Délai entre les sondes
--min-parallelism 10 Groupes de sondes parallèles minimaux
```

Contournement de pare-feu

Techniques d'évasion

```
-f Fragmenter les paquets (morceaux de 8 octets)
-D RND:5 Analyse leurre avec 5 IPs aléatoires
-S spoof_ip Usurper l'IP source (nécessite paquets bruts)
-e eth0 Utiliser une interface réseau spécifique
--source-port 53 Utiliser un port source spécifique (ex. DNS)
--data-length 25 Ajouter des données aléatoires aux paquets
--spoof-mac 0 Randomiser l'adresse MAC
```

Exemples d'évasion

```
nmap -f -D RND:3 target # fragments + leurres
nmap --source-port 53 target # port DNS (souvent autorisé)
nmap -T1 --scan-delay 5s target # lent pour éviter les IDS
```

Motifs courants

Reconnaissance rapide

```
nmap -T4 -F target # ports courants rapides
nmap -T4 -A -v target # OS + détection de services
nmap -sV --top-ports 1000 target # top 1000 + versions
```

Analyse complète

```
# TCP complet + service + OS + scripts
nmap -sS -sV -O -sC -p- -T4 -oA full target
# Analyse UDP sur ports courants
nmap -sU --top-ports 50 target
```

Audit de serveur web

```
nmap -p 80,443 --script=http-title,http-headers,\
ssl-cert,http-methods target
# Vérifier les proxys ouverts et vulnérabilités
nmap -p 80,443,8080 --script=http-open-proxy,vuln target
```

Référence rapide nmap

Inventaire réseau

```
# Découvrir tous les hôtes actifs avec infos OS
nmap -sn 192.168.1.0/24 -oG - | grep "Up"
# Inventaire de services pour sous-réseau
nmap -sV -T4 192.168.1.0/24 -oX inventory.xml
```