nmap – Résumé des principaux commutateurs

Spécifications des cibles  
Les cibles peuvent être spécifiées par:

* des noms d'hôtes (*scanme.nmap.org*);
* des adresses IP (*192.168.10.100*)
* des adresses de réseaux (*cmaisonneuve.qc.ca/24*, *192.168.10.0/24*);
* dés étendues spécifiques (*10.0-255.0-255.1-254*);
* etc.

**nmap -iL <inputfilename>**Lecture de la liste des hôtes/réseaux cibles à partir du fichier

**nmap -iR <num hosts>**Choix des cibles au hasard

**nmap --exclude <host1[,host2][,host3],...>**Exclusion des hôtes/réseaux du scan

**namp --excludefile <exclude\_file>**Exclusion des hôtes/réseaux des cibles à partir du fichier

Découverte des hôtes:

**nmap -sL**Liste des hôtes – Liste simplement les cibles à balayer

**nmap -sP**Balayage de ping – Détermination des hôtes en ligne

**nmap -P0  
nmap -PN**Considère que tous les hôtes sont en ligne -- évite la découverte des hôtes

**nmap -PS/PA/PU [portlist]**Découverte TCP SYN/ACK ou UDP des ports en paramètre

**nmap -PE/PP/PM**Découverte de type requête ICMP echo, timestamp ou netmask

**namp -PO [num de protocole]**Ping IP (par type)

**nmap -n/-R**Ne jamais résoudre les noms DNS/Toujours résoudre [résout les cibles actives par défaut]

**namp --dns-servers <serv1[,serv2],...>**Spécifie des serveurs DNS particuliers

Techniques de balayage

**nmap -sS/sT/sA/sW/sM**Balaye TCP SYN/Connect()/ACK/Window/Maimon

**nmap -sN/sF/sX**Balaye TCP Null, FIN et Xmas

**nmap -sU**Balaye UDP

**nmap --scanflags <flags>**Personnalise les flags des balayages TCP

**nmap -sI <zombie host[:probeport]>**Idlescan (Balayage passif)

**nmap -sO**Balaye des protocoles supportés par la couche IP

**nmap -b <ftp relay host>**Balaye par rebond FTP

**nmap --traceroute**Détermine une route vers chaque hôte

**nmap --reason**Donne la raison pour laquelle tel port apparait à tel état

Spécifications des ports et ordre de balayage

**namp -p <étendue de ports>**Ne balaye que les ports spécifiés  
Exemple:  
namp -p22; -p1-65535; -pU:53,111,137,T:21-25,80,139,8080

**namp –F**Fast - Ne balaye que les ports listés dans le fichier nmap-services

**namp –r**Balayage séquentiel des ports en ne mélangeant pas leur ordre

**namp --top-ports <nombre>**Balaye <nombre> de ports parmi les plus courants

**namp --port-ratio <ratio>**Balay <ratio> pourcent des ports les plus courants

Détection de service/version

**namp –sV**Teste les ports ouverts pour déterminer le service en écoute et sa version

**namp --version-light:**Limite les tests aux plus probables pour une identification plus rapide

**namp --version-intensity <niveau>**De 0 (léger) à 9 (tout essayer)

**namp --version-all**Essaie un à un tous les tests possibles pour la détection des versions

**namp 1/**Affiche des informations détaillées du balayage de versions (pour débogage)

Script da balayage

**namp -sC:**équivalent de --script=safe,intrusive

**namp --script=<lua scripts>**<lua scripts> est une liste de répertoires ou de scripts séparés par des virgules

**namp --script-args=<n1=v1,[n2=v2,...]>**Passer des arguments aux scripts

**namp --script-trace**Montre toutes les données envoyées ou recues

**namp --script-updatedb**Met à jour la base de données des scripts. Seulement fait si -sC ou --script a été aussi donné.

Détection de système d'exploitation:

**namp –O**Active la détection d'OS

**namp --osscan-limit**Limite la détection aux cibles prometteuses --osscan-guess: Détecte l'OS de façon plus agressive

**namp --osscan-guess**Devine l'OS de façon plus agressive

Temporisation et performance

Les options qui prennent un argument de temps sont en milisecondes a moins que vous ne spécifiiez 's' (secondes), 'm' (minutes), ou 'h' (heures) à la valeur (e.g. 30m).

**namp -T[0-5]**Choisit une politique de temporisation (plus élevée, plus rapide)

**namp --min-hostgroup/max-hostgroup <msec>**Tailles des groupes d'hôtes à balayer en parallèle

**namp --min-parallelism/max-parallelism <msec>***Parallélisation* des paquets de tests (probes) --min\_rtt\_timeout/max-rtt-timeout/initial-rtt-timeout <msec>: Spécifie le temps d'aller-retour des paquets de tests

**namp --min\_rtt\_timeout/max-rtt-timeout/initial-rtt-timeout <msec>**Spécifie le temps d'aller-retour des paquets de tests

**namp --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>**Précise le *round trip time* des paquets de tests.

**namp --max-retries <tries>**Nombre de retransmissions des paquets de tests des scans de ports.

**namp --host-timeout <msec> délai d'expiration du scan d'un hôte --scan-delay/--max\_scan-delay <msec>**Ajuste le délai de retransmission entre deux paquets de tests

**namp --scan-delay/--max-scan-delay <time>**Ajuste le delais entre les paquets de tests.

Évasion pare-Feu/IDS et usurpation d'identité

**namp -f; --mtu <val>**Fragmente les paquets (en spécifiant éventuellement la MTU)

**namp -D <decoy1,decoy2[,ME],...>**Obscurci le balayage avec des leurres

**namp -S <IP\_Address>**Usurpe l'adresse source

**namp -e <iface>**Utilise l'interface réseau spécifiée

**namp -g/--source-port <portnum>**Utilise le numéro de port comme source

**namp --data-length <num>**Ajoute des données au hasard aux paquets émis

**namp --ip-options <options>**Envoi des paquets avec les options IP spécifiées.

**namp --ttl <val>**Spécifie le champ durée de vie (*time-to-live*) IP

**namp --spoof-mac <adresse MAC, préfixe ou nom du fabriquant>**Usurpe une adresse physique (MAC)

**namp –badsum**Envoi des paquets TCP/UDP avec une somme de contrôle erronée.

Sortie

**namp -oN/-oX/-oS/-oG <file>**Sortie dans le fichier en paramètre des résultats du balayage au format normal, XML, s|<rIpt kIddi3 et Grepable, respectivement

**namp -oA <basename>**Sortie dans les trois formats majeurs en même temps

**namp –v**Rend Nmap plus verbeux (-vv pour plus d'effet)

**namp -d[level**Sélectionne ou augmente le niveau de débogage (significatif jusqu'à 9)

**namp --packet-trace**Affiche tous les paquets émis et reçus

**namp –iflist**Affiche les interfaces et les routes de l'hôte (pour débogage)

**namp --log-errors**Journalise les erreurs/alertes dans un fichier au format normal

namp --append-output  
Ajoute la sortie au fichier plutôt que de l'écraser

**namp --resume <filename>**Reprend un scan interrompu

**namp --stylesheet <path/URL>**Feuille de styles XSL pour transformer la sortie XML en HTML

**namp –webxml**Feuille de styles de références de Insecure.Org pour un XML plus portable

**namp --no\_stylesheet**Nmap n'associe pas la feuille de styles XSL à la sortie XML

Divers

**namp -6**Active le scan IPv6

**namp –A**Active la détection du système d'exploitation et des versions

**namp --datadir <dirname>**Spécifie un dossier pour les fichiers de données de Nmap

**namp --send-eth/--send-ip**Envoie des paquets en utilisant des trames Ethernet ou des paquets IP bruts

**namp –privileged**Suppose que l'utilisateur est entièrement privilégié -V: Affiche le numéro de version

**namp –unprivileged**Suppose que l'utilisateur n'a pas les privilèges d'usage des raw socket

**namp –h**Affiche ce résumé de l'aide

Exemples

**nmap -v -A scanme.nmap.org  
nmap -v -sP 192.168.0.0/16 10.0.0.0/8  
nmap -v -iR 10000 -P0 -p 80**