MANUEL D'OUTIL DE SCAN DE PORT

Nmap5

Nmap est un scanner de ports open source. Il est conçu pour détecter les ports ouverts, les services hébergés et les informations sur le système d'exploitation d'un ordinateur distant. Ce logiciel est devenu une référence pour les administrateurs réseaux car l'audit des résultats de nmap fournit des indications sur la sécurité d'un réseau. Ce guide décrit comment installer et utiliser nmap sous le système debian.

Agence Nationale de la Sécurité Informatique

Gestion des versions du document

Version	Date	Modification apportée
1.0	23/02/2010	Première version

PLAN

1. FONCTIONNEMENT

Pour scanner les ports d'un ordinateur distant, Nmap utilise diverses techniques d'analyse basées sur des protocoles tels que TCP, IP, UDP ou ICMP. De même, il se base sur les réponses particulières qu'il obtient à des requêtes particulières pour obtenir une empreinte de la pile IP, souvent spécifique du système qui l'utilise. C'est par cette méthode que l'outil permet de reconnaitre la version d'un système d'exploitation et aussi la version des services en écoute.

2. INSTALLATION

- Téléchargez la dernière version de Nmap depuis http://nmap.org/download.html
- Décompressez l'archive téléchargée puis installez-le comme suit :

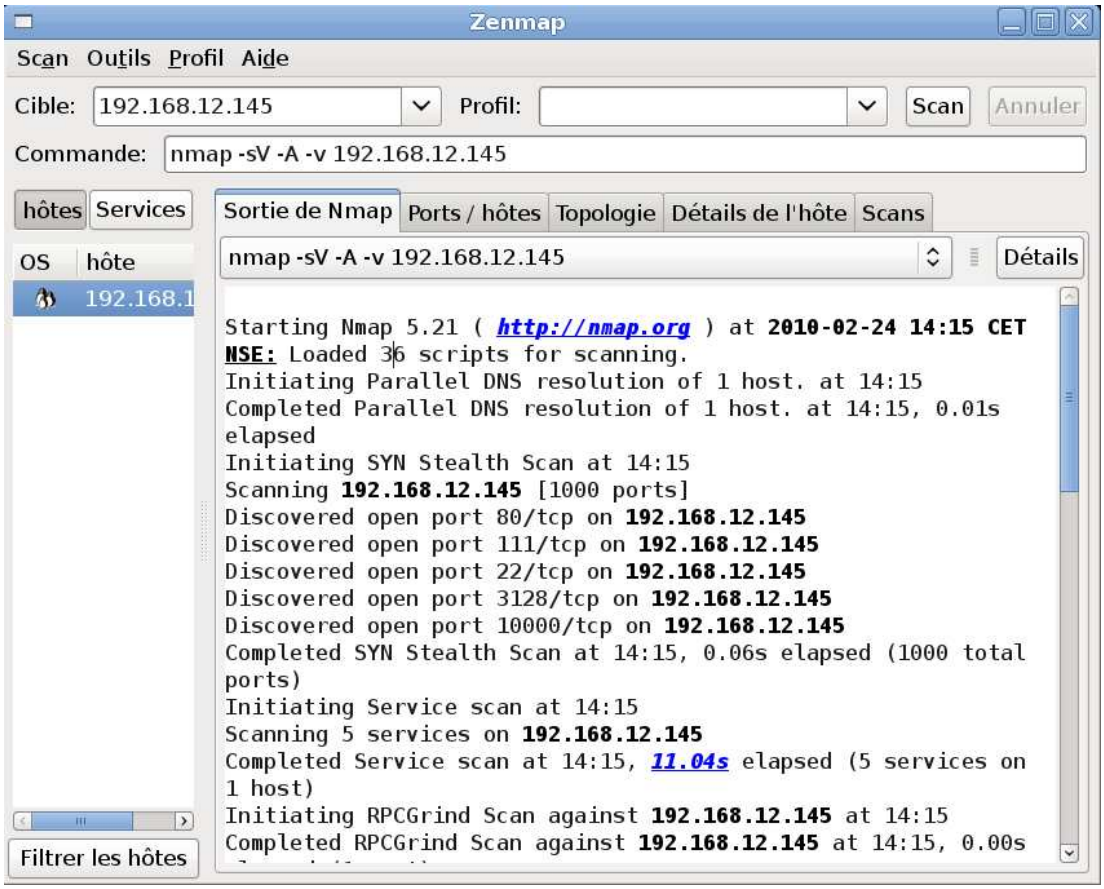
```
Tar xjvf nmap-5.21.tar.bz2

Cd nmap-5.21

./configure

Make

Make install
```

3. INTERFACE GRAPHIQUE

NmapFE, écrite au départ par Zach Smith, était l'interface graphique officielle de Nmap pour les versions 2.2 à 4.22. À partir de la version 4.23 de Nmap, NmapFE a été remplacé par Zenmap, une nouvelle interface graphique basée sur UMIT et développée par Adriano Monteiro Marques.

De nombreuses interfaces web sont également disponibles pour utiliser Nmap à partir d'un navigateur web. On peut citer LOCALSCAN, nmap-web et Nmap-CGI.
Enfin, il existe des interfaces graphiques disponibles sous Microsoft Windows.

On peut citer NMapWin, qui n'est pas mis à jour depuis la version v1.4.0, et NMapW développé par Syhunt.



4. OPTIONS DISPONIBLES

Les options utilisables pour Nmap 5.21 sont les suivantes :

- Spécifications des cibles :

Les cibles peuvent être spécifiées par des noms d'hôtes, des adresses IP (v4 ou v6), des adresses de réseaux…
Exemples : scanme.nmap.org, microsoft.com/24, 192.168.0.1, 10.0-255.0-255.1-254

-iL <inputfilename>: Lit la liste des hôtes/réseaux cibles à partir du fichier -iR <num hosts>: Choisit les cibles au hasard

--exclude <host1[, host2][, host3], ...>: Exclut des hôtes/réseaux du scan

--excludefile <exclude_file>: Exclut des hôtes/réseaux des cibles à partir du fichier

- Découverte des hôtes :

-sL: List Scan - Liste simplement les cibles à scanner

-sP: Ping Scan - Ne fait que déterminer si les hôtes sont en ligne

-PN : Considérer tous les hôtes comme étant connectés -- saute l'étape de découverte des hôtes

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

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

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

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

--dns-servers <serv1 [, serv2], ...>: Spécifier des serveurs DNS particuliers

--system-dns: Utilise le résolveur DNS du système d'exploitation

--tracereoute: Détermine une route vers chaque hôte

- Techniques de scan :

-sS/sT/sA/sW/sM: Scans TCP SYN/Connect ()/ACK/Window/Maimon

-sN/sF/sX: Scans TCP Null, FIN et Xmas

-sU: Scan UDP (Cette option ne fonctionne pas en IPv6)

-sY : sctp (Stream Control Transmission Protocol) init scan

-sZ : sctp (Stream Control Transmission Protocol) cookie echo

-sO : Scan des protocoles supportés par la couche IP

-sI <zombie host [: probeport]>: Idlescan (scan passif)

-b <ftp relay host>: Scan par rebond FTP

- Spécifications des ports et ordre de scan :

-p <plage de ports>: Ne scanne que les ports spécifiés

Exemple: -p22; -p1-65535; -pU:53,111,137,T:21-25,80,139,8080

-F: Fast - Ne scanne que les ports listés dans le fichier nmap-services

-r: Scan séquentiel des ports, ne mélange pas leur ordre

--top-ports <nombre>: Scan <nombre> de ports parmi les plus courants

--port-ratio <ratio>: Scan <ratio> pour cent des ports les plus courants

- Détection de service/version :

-sV: Teste les ports ouverts pour déterminer le service en écoute et sa version

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

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

--version-all: Tente un à un tous les tests possibles pour la détection des versions

--version-trace: Affiche des informations détaillées du scan de versions (pour débogage)

- Script scan :

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

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

--script-args=<n1=v1,[n2=v2,...]>: passer des arguments aux scripts

--script-trace: Montre toutes les données envoyées ou reçues

--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 :

-O: Active la détection d'OS

--osscan-limit: Limite la détection aux cibles prometteuses

--osscan-guess: Devine l'OS de façon plus agressive

- Temporisation et performance :

Les options qui intègrent un argument de temps sont basées sur une unité de temps exprimée en millisecondes à moins que soit spécifié 's' (secondes), 'm' (minutes), ou 'h' (heures) à la valeur (par exemple : 30m).

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

--min-hostgroup/max-hostgroup <msec>: Tailles des groupes d'hôtes à scanner en parallèle

--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

--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Précise le round

trip time des paquets de tests.

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

--host-timeout <msec>: Délai d'expiration du scan d'un hôte

--scan-delay/--max-scan-delay <time>: Ajuste le délai entre les paquets de tests.

- Évasion pare-feu/ids et usurpation d'identité :

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

-D <decoy1, decoy2 [, ME], ...>: Obscurcit le scan avec des leurres

-S <IP_Address>: Usurpe l'adresse source

-e <iface>: Utilise l'interface réseau spécifiée

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

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

--ip-options <options>: Envoie des paquets avec les options IP spécifiées.

--ttl <val>: Spécifie le champ time-to-live IP

--spoof-mac <adresse MAC, préfixe ou nom du fabriquant>: Usurpe une adresse MAC

--badsum: Envoie des paquets TCP/UDP avec une somme de contrôle erronée.

--adler32: Utilise Adler32 obsolète au lieu de CRC32C pour checksums SCTP

- Sortie :

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

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

-v: Rend Nmap plus verbeux (-vv pour plus d'effet)

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

--packet-trace: Affiche tous les paquets émis et reçus

--iflist: Affiche les interfaces et les routes de l'hôte (pour débogage)

--log-errors: Consigne les erreurs/alertes dans un fichier-journal au format normal

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

--resume <filename>: Reprend un scan interrompu

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

--webxml: Feuille de styles de références d'Insecure.Org pour un XML plus portable

--no_stylesheet: Nmap n'associe pas la feuille de styles XSL à la sortie XML

- Options diverses:

-6: Active le scan IPv6

-A: Active la détection du système d'exploitation et des versions

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

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

--privileged: Suppose que l'utilisateur est entièrement privilégié

--unprivileged: Suppose que l'utilisateur n'a pas les privilèges d'usage des raw

socket

-V: Affiche le numéro de version

-h: Affiche ce résumé de l'aide

- Exemples :

- Analyse de l'hôte de nom symbolique (résolvable) scanme.nmap.org pour identifier le système d'exploitation sous-jacent :

```
nmap  -v -A scanme.nmap.org
```

- Analyse de deux réseaux privées de classes respectives C et A pour une découverte des hôtes en ligne :

```
nmap -v -sP 192.168.0.0/16 10.0.0.0/8
```

- Analyse du port 80 de 10 000 hôtes sélectionnés de manière aléatoire et sans découverte préalable des hôtes :

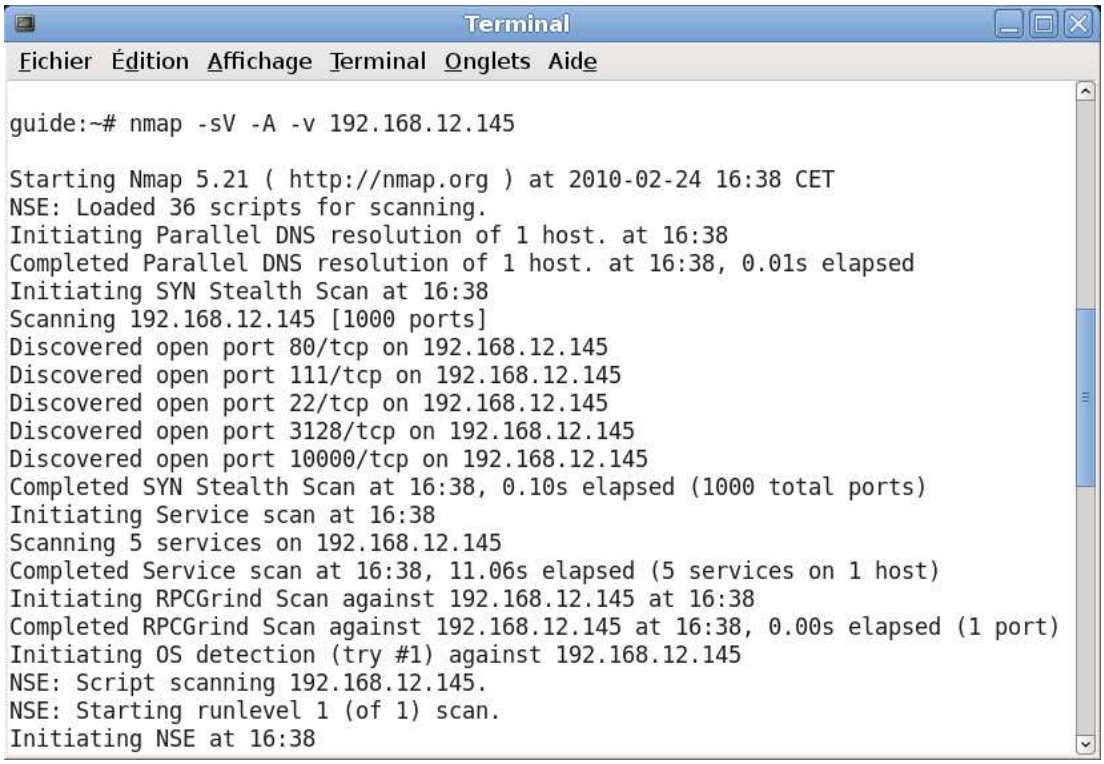
```
nmap -v -iR 10000 -P0 -p 80
```

- Analyse de l'hôte courant par son adresse locale de bouclage IPv6 :

```
nmap -6   0 ::1
```

- Exemple de sortie

Exemple d'un scan nmap 5.21 sur linux debian avec les options d'identification des services et de reconnaissance du système d'exploitation.


Terminal
Fichier Édition Affichage Terminal Onglets Aide
guide:~# nmap -sV -A -v 192.168.12.145
Starting Nmap 5.21 (http://nmap.org) at 2010-02-24 16:38 CET
NSE: Loaded 36 scripts for scanning.
Initiating Parallel DNS resolution of 1 host. at 16:38
Completed Parallel DNS resolution of 1 host. at 16:38, 0.01s elapsed
Initiating SYN Stealth Scan at 16:38
Scanning 192.168.12.145 [1000 ports]
Discovered open port 80/tcp on 192.168.12.145
Discovered open port 111/tcp on 192.168.12.145
Discovered open port 22/tcp on 192.168.12.145
Discovered open port 3128/tcp on 192.168.12.145
Discovered open port 10000/tcp on 192.168.12.145
Completed SYN Stealth Scan at 16:38, 0.10s elapsed (1000 total ports)
Initiating Service scan at 16:38
Scanning 5 services on 192.168.12.145
Completed Service scan at 16:38, 11.06s elapsed (5 services on 1 host)
Initiating RPCGrind Scan against 192.168.12.145 at 16:38
Completed RPCGrind Scan against 192.168.12.145 at 16:38, 0.00s elapsed (1 port)
Initiating OS detection (try #1) against 192.168.12.145
NSE: Script scanning 192.168.12.145.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 16:38