Introduction à Nmap

Nmap (Network Mapper) est un outil open source d'exploration réseau et d'audit de sécurité. Il est conçu pour rapidement scanner de grands réseaux, mais fonctionne également très bien sur des hôtes uniques. Nmap utilise des paquets IP bruts pour déterminer quels hôtes sont disponibles sur le réseau, quels services (nom de l'application et version) ces hôtes offrent, quels systèmes d'exploitation (et versions d'OS) ils exécutent, quel type de filtres de paquets/pare-feu sont utilisés, et des dizaines d'autres caractéristiques. Il est largement utilisé par les administrateurs réseau pour l'audit de sécurité, la gestion des inventaires réseau, la surveillance des services, et bien plus encore.

Fonctionnement de Nmap

Nmap utilise diverses techniques d'analyse qui s'appuient sur des protocoles tels que TCP, IP, UDP ou ICMP. Il se fonde sur les réponses qu'il obtient à des requêtes particulières pour obtenir une empreinte de la pile IP, souvent propre au système qui l'utilise. C'est par cette méthode qu'il peut reconnaître la version d'un système d'exploitation ainsi que la version des services (aussi appelés démons) en écoute.

Interfaces graphiques

Bien que Nmap soit principalement un outil en ligne de commande, des interfaces graphiques existent pour faciliter son utilisation :

- **Zenmap** : L'interface graphique officielle de Nmap, basée sur UMIT. Elle offre une visualisation des résultats de scan, une gestion des profils de scan, et un constructeur de commandes.
- D'autres interfaces web et des outils tiers sont également disponibles.

Exemple d'utilisation

Un exemple simple de commande Nmap :

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

Cette commande effectue une détection du système d'exploitation (`-O`), une détection de version (`-sV`), un scan de script par défaut (`-sC`), et un traceroute (`--traceroute`) sur la cible `scanme.nmap.org` .

Formats de sortie

Nmap fournit différents formats de sortie possibles :

- **Interactif** : Les résultats d'analyse Nmap sont directement affichés sur la ligne de commande.
- **Texte** : Les résultats sont générés au format TXT, et peuvent être enregistrés dans un fichier.
- **XML** : Un format qui peut être traité ultérieurement par des outils XML, idéal pour l'intégration avec d'autres systèmes.

Commandes Nmap Essentielles

Voici une liste de commandes Nmap essentielles avec leurs descriptions et exemples d'utilisation :

1. Scan Nmap de base contre une adresse IP ou un hôte

```
nmap 1.1.1.1
```

Cette commande effectue un scan de base sur l'adresse IP spécifiée. Vous pouvez remplacer l'adresse IP par un nom d'hôte.

```
nmap recordedfuture.xyz
```

2. Scan Ping Nmap

```
nmap -sn 192.168.5.0/24
```

Cette commande effectue un scan ping pour détecter les hôtes actifs sur un réseau. `-sn` désactive le scan de ports et ne fait que la découverte d'hôtes.

3. Scanner des ports spécifiques ou des plages de ports

```
nmap -p 1-65535 localhost
```

Scanne tous les 65535 ports sur l'hôte local. Vous pouvez spécifier des ports individuels ou des plages de ports.

`nmap -p 80,443 8.8.8.8`

Scanne les ports 80 et 443 sur l'adresse IP 8.8.8.8.

4. Scanner plusieurs adresses IP

`nmap 1.1.1.1 8.8.8.8`

Scanne plusieurs adresses IP spécifiées.

`nmap 1.1.1.1,2,3,4`

Scanne les adresses IP consécutives 1.1.1.1, 1.1.1.2, 1.1.1.3 et 1.1.1.4.

5. Scanner des plages d'adresses IP (CIDR ou tiret)

`nmap 8.8.8.0/28`

Scanne une plage d'adresses IP en utilisant la notation CIDR.

`nmap 8.8.8.1-14`

Scanne une plage d'adresses IP en utilisant la notation avec tiret.

`nmap 8.8.8.*`

Scanne toutes les adresses IP dans la plage de classe C (par exemple, de 8.8.8.1 à 8.8.8.256).

6. Exclure des hôtes d'un scan

`nmap -p 8.8.8.* --exclude 8.8.8.1`

Scanne la plage 8.8.8.* en excluant l'adresse 8.8.8.1.

7. Scanner les ports les plus populaires

`nmap --top-ports 20 192.168.1.106`

Scanne les 20 ports les plus couramment utilisés sur l'hôte spécifié.

8. Scan de détection de version de service

`nmap -sV 192.168.1.1`

Cette commande tente de déterminer la version des services s'exécutant sur les ports ouverts.

9. Scan de détection de système d'exploitation (OS)

```
nmap -O 192.168.1.1
```

Cette commande tente de déterminer le système d'exploitation de la cible.

10. Scan furtif (SYN scan)

```
nmap -sS 192.168.1.1
```

Le scan SYN est le type de scan par défaut et le plus populaire. Il est rapide et discret car il ne complète pas la connexion TCP.

11. Scan UDP

```
nmap -sU 192.168.1.1
```

Scanne les ports UDP. Les scans UDP sont souvent plus lents que les scans TCP.

12. Scan complet (détection de version, OS, scripts par défaut)

```
nmap -A 192.168.1.1
```

Cette option active la détection de l'OS, la détection de version, le scan de script par défaut et le traceroute. C'est une option très complète mais aussi plus bruyante.

13. Scan de scripts Nmap (NSE - Nmap Scripting Engine)

```
nmap -sC 192.168.1.1
```

Exécute les scripts NSE par défaut. Ces scripts peuvent être utilisés pour la détection de vulnérabilités, la découverte de services plus approfondie, etc.

```
nmap --script http-enum 192.168.1.1
```

Exécute un script spécifique (ici, `http-enum` pour énumérer les répertoires web).

14. Scan avec agrégation de sorties

```
nmap -oA output_file 192.168.1.1
```

Cette commande enregistre la sortie dans trois formats différents (normal, XML, et Grepable) avec le préfixe `output_file`.

15. Scan avec un fichier d'entrée de cibles

```
nmap -iL targets.txt
```

Scanne les cibles listées dans le fichier `targets.txt`.

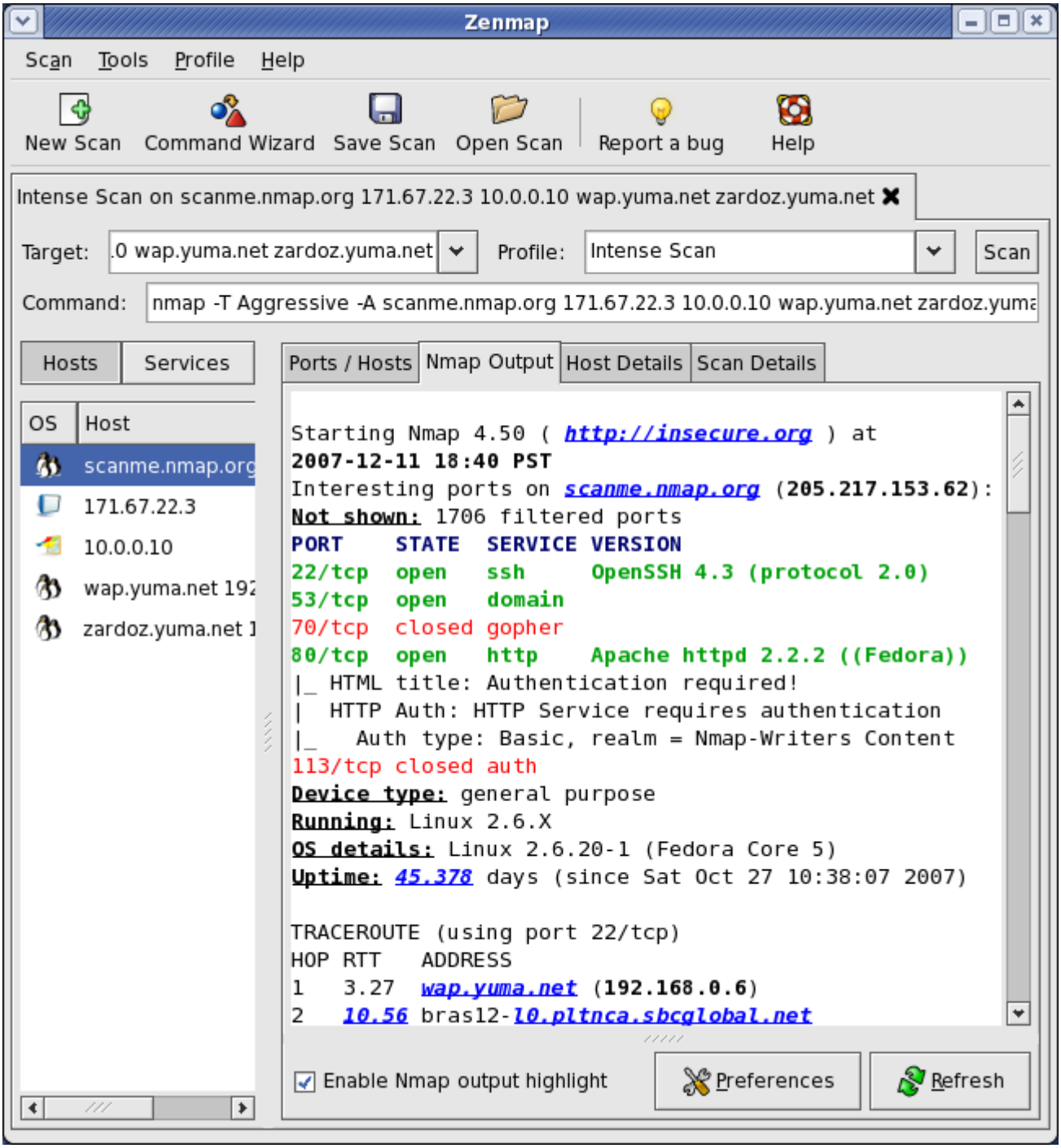
16. Scan avec une vitesse de temporisation spécifiée

```
nmap -T4 192.168.1.1
```

`T4` (Aggressive) est une option de temporisation qui accélère le scan en envoyant plus de paquets en parallèle. Les options vont de `T0` (Paranoid) à `T5` (Insane).

Zenmap : L'interface graphique de Nmap

Zenmap est l'interface graphique officielle de Nmap. Elle simplifie l'utilisation de Nmap en offrant une interface conviviale pour la construction de commandes, la visualisation des résultats de scan, et la gestion des profils. C'est un excellent outil pour les débutants comme pour les utilisateurs avancés.



Zenmap permet de :

- Construire des commandes Nmap complexes via une interface intuitive.
- Visualiser les topologies réseau découvertes.
- Comparer les résultats de scans pour identifier les changements.
- Enregistrer et charger des profils de scan pour une réutilisation facile.

Fonctionnalités Avancées de Nmap

Nmap ne se limite pas aux scans de ports basiques. Il offre une multitude de fonctionnalités avancées qui en font un outil indispensable pour les professionnels de la sécurité et les administrateurs réseau.

Détection de Vulnérabilités avec le Nmap Scripting Engine (NSE)

Le Nmap Scripting Engine (NSE) est l'une des fonctionnalités les plus puissantes de Nmap. Il permet aux utilisateurs d'écrire (ou d'utiliser des scripts existants) pour automatiser une grande variété de tâches réseau. Ces scripts peuvent être utilisés pour :

- **Détection de vulnérabilités** : Identifier les failles de sécurité connues sur les services découverts.
- **Découverte de services avancée** : Obtenir des informations plus détaillées sur les services en cours d'exécution.
- **Exploitation de vulnérabilités** : Dans certains cas, les scripts peuvent même être utilisés pour exploiter des vulnérabilités simples (bien que ce ne soit pas l'objectif principal de Nmap).
- **Backdoors et détection de malwares** : Identifier la présence de portes dérobées ou de logiciels malveillants.
- **Fuzzing** : Tester la robustesse des services en leur envoyant des données inattendues.

Pour utiliser le NSE, vous pouvez spécifier des scripts individuels ou des catégories de scripts. Par exemple :

`nmap --script vuln <cible>` : Exécute tous les scripts de la catégorie 'vuln' pour détecter les vulnérabilités.

`nmap --script http-enum <cible>` : Exécute le script `http-enum` pour énumérer les répertoires web et les fichiers sur un serveur HTTP.

Options de Temporisation et de Performance

Nmap offre des options pour contrôler la vitesse et l'agressivité des scans, ce qui est crucial pour éviter la détection par les systèmes de détection d'intrusion (IDS) ou pour accélérer les scans sur des réseaux fiables.

Les options de temporisation (`-T`) vont de `T0` (paranoid) à `T5` (insane) :

- `T0` (Paranoid) : Très lent, utilisé pour éviter la détection. Envoie les paquets très lentement.
- `T1` (Sneaky) : Similaire à T0, mais un peu plus rapide.
- `T2` (Polite) : Ralentit le scan pour utiliser moins de bande passante et de ressources CPU sur la cible.
- `T3` (Normal) : Le mode par défaut. Équilibre entre vitesse et furtivité.
- `T4` (Aggressive) : Accélère le scan en supposant que vous êtes sur un réseau rapide et que vous ne vous souciez pas d'être détecté.

- `T5` (Insane) : Le plus rapide, mais peut être très bruyant et entraîner des résultats imprécis sur des réseaux lents ou instables.

Exemple :

`nmap -T4 <cible>` : Effectue un scan agressif.

Évasion de Pare-feu et d'IDS

Nmap propose plusieurs techniques pour tenter d'éviter les pare-feu et les systèmes de détection d'intrusion :

- **Fragmentation de paquets (`-f`)** : Divise les paquets Nmap en fragments plus petits pour contourner les règles de pare-feu basées sur la taille des paquets.
- **Spécification d'un MTU (`--mtu <valeur>`)** : Définit la taille maximale de l'unité de transmission pour les paquets envoyés.
- **Utilisation de leurres (`-D <leurre1>,<leurre2>,...`)** : Envoie des paquets de scan à partir de plusieurs adresses IP factices en plus de votre propre adresse, rendant difficile l'identification de la source réelle du scan.
- **Changement d'adresse MAC (`--spoof-mac <adresse_mac>`)** : Modifie l'adresse MAC de l'interface d'envoi pour masquer votre identité.
- **Envoi de paquets avec des sommes de contrôle invalides (`--badsum`)** : Certains pare-feu peuvent ignorer les paquets avec des sommes de contrôle invalides, ce qui peut permettre à Nmap de passer inaperçu.

Exemple :

`nmap -f -D RND:10 <cible>` : Fragmente les paquets et utilise 10 leurres aléatoires.

Sortie et Rapports

Nmap offre des options de sortie flexibles pour s'adapter à différents besoins :

- **Sortie normale (`-oN <fichier>`)** : Enregistre la sortie dans un fichier texte lisible par l'homme.
- **Sortie XML (`-oX <fichier>`)** : Enregistre la sortie au format XML, ce qui est utile pour l'intégration avec d'autres outils ou pour l'analyse programmatique.
- **Sortie Grepable (`-oG <fichier>`)** : Un format simple qui facilite le traitement des résultats avec des outils comme `grep`, `awk`, ou `cut`.
- **Sortie tout-en-un (`-oA <préfixe>`)** : Enregistre la sortie dans les trois formats (normal, XML, Grepable) avec le préfixe de fichier spécifié.

Exemple :

`nmap -oA mon_scan <cible>` : Crée `mon_scan.nmap`, `mon_scan.xml`, et `mon_scan.gnmap`.

Installation de Nmap

Nmap est un outil multiplateforme, disponible sur la plupart des systèmes d'exploitation. Voici comment l'installer sur les plateformes les plus courantes :

Installation sur Linux

Sur les distributions basées sur Debian/Ubuntu, vous pouvez installer Nmap via le gestionnaire de paquets `apt` :

```
sudo apt update
sudo apt install nmap
```

Sur les distributions basées sur Red Hat/CentOS/Fedora, utilisez `dnf` ou `yum` :

```
sudo dnf install nmap
# Ou pour les anciennes versions de CentOS/RHEL :
sudo yum install nmap
```

Installation sur Windows

Pour Windows, il est recommandé de télécharger l'installeur officiel depuis le site web de Nmap. L'installeur inclut Nmap, Npcap (pour la capture de paquets) et Zenmap (l'interface graphique).

1. Rendez-vous sur le site officiel de Nmap : https://nmap.org/download.html
2. Téléchargez la dernière version de l'installeur `nmap-<version>-setup.exe`.
3. Exécutez l'installeur et suivez les instructions à l'écran. Assurez-vous de cocher les options pour installer Npcap et Zenmap si vous souhaitez les utiliser.

Installation sur macOS

Pour macOS, vous pouvez également télécharger l'installeur officiel ou utiliser un gestionnaire de paquets comme Homebrew.

Méthode 1 : Installeur officiel

1. Rendez-vous sur le site officiel de Nmap : https://nmap.org/download.html
2. Téléchargez le fichier `nmap-<version>.dmg`.

3. Ouvrez le fichier `.dmg` et faites glisser l'application Nmap dans votre dossier Applications.

Méthode 2 : Homebrew

Si vous avez Homebrew installé, vous pouvez installer Nmap avec une simple commande :

```
brew install nmap
```

Conclusion

Nmap est un outil puissant et polyvalent pour l'exploration de réseau et l'audit de sécurité. Que vous soyez un administrateur système, un professionnel de la sécurité ou simplement un passionné, la maîtrise de Nmap vous fournira des capacités inestimables pour comprendre et sécuriser les réseaux. Ce manuel a couvert les bases, les commandes essentielles, les fonctionnalités avancées et les méthodes d'installation, vous donnant une base solide pour commencer votre exploration avec Nmap. N'oubliez pas de toujours utiliser Nmap de manière éthique et légale, en respectant la vie privée et les politiques de sécurité des réseaux que vous scannez.