nmap

La commande nmap est un outil en ligne de commande utilisé pour scanner les réseaux et les hôtes pour découvrir des informations sur les ports ouverts, les services en cours d'exécution, les systèmes d'exploitation et les vulnérabilités potentielles. C'est un outil très populaire pour les administrateurs système, les professionnels de la sécurité et les hackers éthiques pour explorer et auditer les réseaux.

La commande nmap est très flexible et peut être utilisée pour scanner des plages d'adresses IP, des hôtes individuels ou des noms de domaine. Elle peut également être utilisée pour effectuer des scans de port simples ou avancés, des scans de vulnérabilités et des scans de scripts personnalisés.

Installation

Vous pouvez installer nmap à l'aide de votre gestionnaire de paquets système. Voici comment installer Nmap sur les distributions Linux les plus courantes :

– Ubuntu et Debian :

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

– Fedora :

```
sudo dnf install nmap
```

– CentOS et RHEL :

```
sudo yum install nmap
```

– Arch Linux :

```
sudo pacman -S nmap
```

Une fois que vous avez installé Nmap, vous pouvez l'utiliser en exécutant la commande nmap dans un terminal.

Exemples

Voici quelques exemples de commandes nmap sous Linux :

– Scanner les ports ouverts d'un hôte :

```
nmap <ip-address>
```

Cela va scanner tous les ports ouverts de l'hôte spécifié.

– Scanner les ports ouverts d'une plage d'adresses IP :

```
nmap <ip-address-range>
```

Cela va scanner tous les ports ouverts de la plage d'adresses IP spécifiée.

Plus d'infos sur la plage d'adresses IP

Il existe plusieurs façons de spécifier une **plage d'adresses IP** en utilisant nmap. Voici quelques exemples :

– Spécifier **une plage d'adresses IP** en utilisant une **notation CIDR** (Classless Inter-Domain Routing) :

```
nmap 192.168.0.0/24
```

Cela va scanner tous les hôtes de la plage d'adresses IP 192.168.0.0 à 192.168.0.255.

– **Spécifier une plage d'adresses IP** en utilisant une **notation hybride** :

```
nmap 192.168.0-255.1-254
```

Cela va scanner tous les hôtes de la plage d'adresses IP 192.168.0.1 à 192.168.0.254 et de 192.168.1.1 à 192.168.1.254.

– **Spécifier plusieurs plages d'adresses IP** en utilisant une **virgule** pour séparer les plages :

```
nmap 192.168.0.0/24,10.0.0.0/8
```

Cela va scanner tous les hôtes des plages d'adresses IP 192.168.0.0 à 192.168.0.255 et de 10.0.0.0 à 10.255.255.255.

Il existe d'autres façons de spécifier des plages d'adresses IP avec Nmap, telles que l'utilisation de fichiers de listes d'adresses IP ou l'utilisation d'expressions régulières.

– Scanner les ports ouverts d'un hôte et afficher les informations sur les services en cours d'exécution :

```
nmap -sV <ip-address>
```

Cela va scanner tous les ports ouverts de l'hôte spécifié et afficher les informations sur les services en cours d'exécution.

– Scanner les ports ouverts d'un hôte et afficher les informations sur le système d'exploitation :

```
nmap -O <ip-address>
```

Cela va scanner tous les ports ouverts de l'hôte spécifié et tenter de déterminer le système d'exploitation en cours d'exécution.

– Scanner les ports ouverts d'un hôte en utilisant un script personnalisé :

```
nmap --script=<script-name> <ip-address>
```

Cela va scanner tous les ports ouverts de l'hôte spécifié en utilisant le script personnalisé spécifié.

Il existe de nombreuses autres options et paramètres que vous pouvez utiliser avec la commande nmap, vous pouvez consulter la page de manuel en tapant man nmap dans votre terminal pour plus d'informations.