nmap : scanner de ports

- Objet : Utiliser nmap pour découvrir les ports ouverts sur un réseau
- Niveau requis :
  débutant, avisé
- Commentaires : *Un outil pratique pour vérifier le bon fonctionnement d'un pare-feu.*
- Débutant, à savoir : Utiliser GNU/Linux en ligne de commande, tout commence là !.
- Suivi :
  doublon
  - Création par MaTTuX_ le 17/06/2007
  - Testé et augmenté par <lagrenouille...> le <14/05/2023...>
- Commentaires sur le forum : ici[1)]

Introduction

Le logiciel nmap permet de scanner une IP, il vous permettra de savoir quels sont les ports ouverts de votre réseaux afin de le sécuriser avec un firewall.

J'ajouterais que le scan de ports autre que son réseau ou sa machine et totalement interdit ! Sachez que l'ordinateur que vous scannez garde votre ip dans ces logs. Ce soft est donc réservé pour les administrateurs de réseaux ou des personnes ayant un réseaux privé à sécuriser. J'insiste sur son utilité de sécuriser votre propre réseau, pas de hacker celui des autres. En aucun cas je suis le responsable des manipulations que vous allez entreprendre avec se logiciel.

Pour installer nmap faite un petit :

```
apt-get update && apt-get install nmap
```

^^.

Ouvrez maintenant une console en root et faites :

```
nmap -v 192.168.x.x
```

retour de la commande

```
Starting Nmap 4.20 ( http://insecure.org ) at 2007-05-20 19:26 CLT
Interesting ports on 192.168.x.x:
Not shown: 1695 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
3306/tcp open  mysql
MAC Address: 00:C0:9F:46:B1:E6 (Quanta Computer)
Nmap finished: 1 IP address (1 host up) scanned in 0.461 seconds
```

Voilà dans se résultat on voit que j'ai le port 22 et le port 3306 ouvert, grâce à ce résultat je vais pouvoir établir les règles de mon firewall.

nmap est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant.

Le scan se fait à l'aide de requêtes ARP sur toutes les IP possibles, à condition qu'elles soient dans notre sous-réseau.

Si les IP de destination sont dans un autre sous réseau, des requêtes de Ping sont utilisées

Des requêtes DNS inverses sont ensuite lancées pour les IP des machines qui ont répondu.

Vous pouvez afficher toutes les machines connectées à votre Lan avec la commande :

```
nmap -T4 -sP 192.168.1.0/24
```

avec l'option -sL, regardez les informations que cette commande est allé chercher

```
nmap -sL 192.168.1.0/24
```

Sur une machine, les ports peuvent avoir 3 états :Ouverts,Fermés, Filtrés

Si le port est ouvert, c'est qu'une application écoute sur ce port.

si le port 80 est ouvert, c'est qu'il y a probablement un serveur Web qui est hébergé sur la machine.

L'option sU permet de scanner les ports en UDP, un scan UDP, ça peut aider à dénicher les planqués :

```
nmap -sU  192.168.0.0/24
```

Pour générer un rapport.

```
 nmap 192.168.1.0/24 -oX rapport.xml
```

```
cat rapport.xml
```

Encore une chose importante: Le scan de port est puni par la loi ! Vous ne devez pas scanner une machine sans l'accord du propriétaire !! C'est du piratage… 😉

[1)]
N'hésitez pas à y faire part de vos remarques, succès, améliorations ou échecs !