NMAP

Pourquoi cartographier un réseau ?

Dans un réseau informatique il est essentiel de savoir qui est connecté et quels services sont disponibles. Effectuer la cartographie d'un réseau permet d'établir un inventaire des machines, services, ports, anomalies...

Elle est aussi utile pour les services informatiques afin de vérifier la conformité d'un réseau en l'analysant. En résumé, cartographier un réseau est un moyen de mieux maîtriser son infrastructure réseau afin de limiter les risques liés aux intrusions, piratages ou autres.

Qu'est-ce que NMAP ?

Nmap, de l'abréviation Network Mapper, est un outil libre et open source d'analyse de réseau. Il a été créé par Gordon Lyon, plus connu sous le pseudonyme de Fyodor. Distribué sous licence GPL (licence qui fixe les conditions légales de distribution d'un logiciel libre), Nmap est aujourd'hui utilisé par les administrateurs réseaux et par les experts de cybersécurité.

L'outil permet de détecter les hôtes présents sur un réseau, les ports ouverts/fermés, trouver les services ainsi que leurs versions. Il peut aussi automatiser des analyses plus avancées telle que la rechercher de vulnérabilités d'un système informatique.

Cas d'usage et exemples :

Nmap s'utilise dans de nombreux cas :

- Inventaire réseau : Lister des machines connectées à un réseau ;

- Test d'intrusion : Essayer de trouver des informations sur une cible ;

- Audit interne : Vérifier qu'il n'y est pas de faille qui représente une vulnérabilité pour le système ;

- Dépannage : Effectuer un diagnostic réseau lorsque qu'un problème intervient.

Voici quelques exemples concrets que nous avons effectué sur une machine Kali Linux afin de présenter l'outil dans les grandes lignes.

Syntaxe de base nmap

nmap [options] <cible>

[option] -sS (SYN Scan), -sV (Service Scan), -sn (Network Scan), -p (Port scan), -A (Complet scan)

<cible> `192.168.1.10`, `example.com`, `192.168.1.0/24`

Afin de mener à bien notre exemple, nous avons connectés nos PCs (et par conséquent nos VMs) sur le même réseau en partage de connexion. Notre réseau était : 172.20.10.0/24

–sn, afin de scanner complètement notre réseau et y découvrir les hôtes connectés.

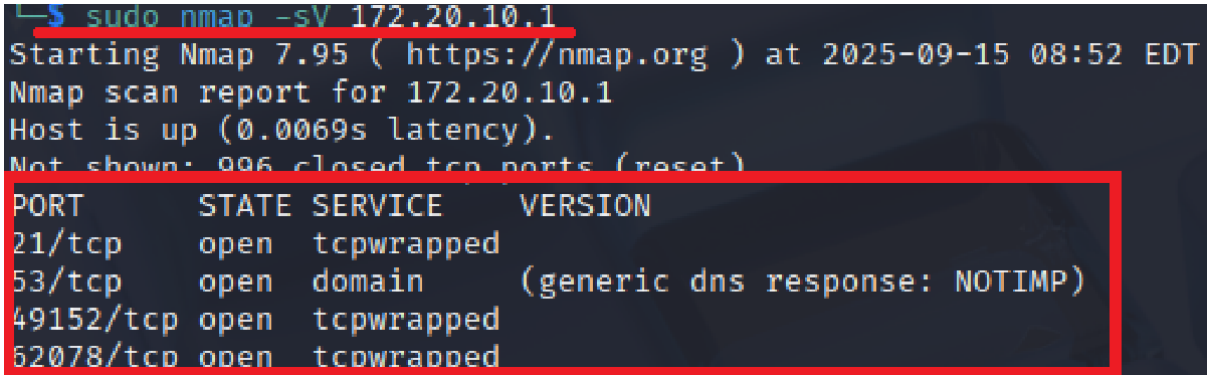
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sN 172.20.10.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 07:57 EDT
Nmap scan report for 172.20.10.1
Host is up (0.0073s latency).
All 1000 scanned ports on 172.20.10.1 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 2A:02:2E:05:3B:64 (Unknown)

Nmap scan report for 172.20.10.2
Host is up (0.00019s latency).
All 1000 scanned ports on 172.20.10.2 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 14:5A:FC:77:54:D1 (Liteon Technology)

Nmap scan report for 172.20.10.4
Host is up (0.033s latency).
All 1000 scanned ports on 172.20.10.4 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 88:F4:DA:D9:89:15 (Unknown)

Nmap scan report for 172.20.10.5
Host is up (0.011s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE         SERVICE
22/tcp open|filtered ssh
MAC Address: 88:F4:DA:D9:89:15 (Unknown)
```

–sV, afin de scanner les services utilisés sur un hôte (Port, État, Service et Version)



Sécurité & Légalité :

Il est important de parler de légalité lorsque nous utilisons des logiciels telles que Nmap. Pour rappel, scanner un réseau sans autorisation est totalement illégal. Les analyses doivent toujours être réaliser dans un cadre clair avec une autorisation. Un simple scan peut être détecter par les systèmes de sécurité et perturber ces derniers.

L'utilisation de certains scripts comme –A peut-être intrusive et doit être réservée à des environnements de test ou à des audits officiels.

En pratique, la bonne approche consiste à utiliser Nmap sur un réseau de laboratoire ou sur des systèmes dont on a la responsabilité, afin de bénéficier de ses fonctionnalités sans enfreindre la loi ni risquer d'interruption de service.