	TP1 : Nmap AU 2022 /2023	Enseignante : Dr. Ing. Ghofrane Fersi

ATTENTION : Le balayage d'un réseau sans l'accord de l'administrateur réseau est strictement interdit et répréhensible par la loi.

Pour notre TP, il est strictement **interdit** d'utiliser n'importe quel réseau à votre portée. Les tests ne sont effectués que sur **votre propre réseau** crée par vous-même. Chaque trinôme créera son propre réseau et fera les tests sur celui-ci.

Pour faire des tests sur une machine distante, veuillez utiliser scanme.nmap.org

Notez bien : les TPs sont réalisés par trinôme. Vous pouvez tout de même créer un réseau plus large comportant cinq ou six machines de vos collègues dans la même salle pour une étude plus approfondie.

Nmap permet de faire le scan des machines d'un sous-réseau, d'en connaître les ports ouverts, et donc probablement de connaître les services lancés sur chaque machine, de connaître leurs versions et potentiellement les vulnérabilités.

En interrogeant la pile Tcp /IP (Transmission Control Protocol/Internet Protocol) d'un serveur, on peut en effet apprendre de nombreuses informations utiles lors d'une attaque.

Tout d'abord, la connaissance du système d'exploitation d'un serveur est évidemment cruciale pour un attaquant. Beaucoup de failles sont spécifiques aux systèmes d'exploitation, et les façons d'y pénétrer sont également différentes.

Si un exploit existe concernant un service de Solaris par exemple, une prise d'empreinte peut nous indiquer quelles sont les machines utilisant Solaris, et si le service concerné est lancé, l'attaque est imminente.

Le fait de balayer un réseau, de le scanner, permet de connaître sa topologie. Le scanneur de ports va détecter les IP actives sur le réseau, détecter les ports ouverts et les services potentiels qui tournent derrière chaque port ouvert.

En cela, nmap est un outil pratique et indispensable pour tout administrateur, dans le sens où il est capable de retirer beaucoup d'informations par prise d'empreinte TCP/IP sur les réseaux complets avec une adresse de sous-réseau et son masque. Il permet de trouver par exemple le système d'exploitation en analysant la réponse donnée d'abord à la connexion TCP à un port ouvert, puis à un port fermé. Cette technique n'est pas fiable à 100% mais reste très efficace.

Selon nmap un port d'une machine peut être dans un des états suivants :

| open (ouvert) : port associé à un service actif.

| closed (fermé) : port associé à un service inactif.

| filtered (filtré) : Port inaccessible à cause d'un pare-feu par exemple.

| unfiltered (non filtré) : port accessible mais nmap n'arrive pas à déterminer s'il est ouvert ou fermé.

Dans la pratique, pour découvrir par exemple la topologie d'un réseau 192.168.0.0/24, dont l'adresse réseau est 192.168.0 et pouvant contenir jusqu'à 254 machines, nous utiliserons la commande:

nmap - sS - su -0 -oN nmap.log 192.168.0.1-254

Installation nmap

Installation sous Ubuntu

sudo apt-get update
sudo apt-get install nmap

Vérification de la version installée : nmap –version

Utilisation nmap

1. Tapez dans l'invite de commande nmap –help pour voir les options de nmap
2. Tapez la commande qui permet de faire une découverte générale des hôtes connectées sur le réseau crée
3. Tapez la commande qui permet de scanner des ports spécifiques d'un ensemble d'hôtes du réseau
4. Tapez la commande qui permet de scanner tous les ports d'une plage d'adresses du réseau

5. Tapez la commande qui permet de savoir le système d'exploitation d'un ensemble d'hôtes de votre réseau

6. Tapez la commande permettant de connaître la/les machines ayant le port 80 ouvert
7. Scannez les vulnérabilités d'un hôte de votre réseau
8. Scannez les vulnérabilités de service d'un hôte
9. Scannez les ports utilisant la connexion TCP