SCAN DE PORT

Pourquoi Effectuer un Scan de Ports ?

- **Sécurité** : Identifier les **ports** ouverts susceptibles d'être exploités par des attaquants.
- **Dépannage** : Vérifier les **services actifs** sur une machine pour diagnostiquer des problèmes de connexion.
- **Cartographie réseau** : Obtenir une vue d'ensemble des **services disponibles** sur un réseau.

Scan Actif

- **Description** : Envoie des **requêtes directes** aux ports d'une machine cible pour voir lesquels sont **ouverts**.
- **Utilisations** : Tests de sécurité, audits de réseau, **identification des services actifs**.

Outil : Nmap

Commande : `nmap -p 1-65535 -A <Adresse IP>`

`-p 1-65535` : Scanne tous les ports (1 à 65535).

`-A` : Active des fonctionnalités avancées comme la détection de services, de versions et d'OS.

Type de scans actifs :

Scan TCP Connect `-sT` Établit une connexion complète (**3-way handshake**). Facilement détectable.

Scan SYN `-sS` N'achève pas le **handshake** complet, donc plus discret. Connu comme "half-open scan".

Scan UDP `-sU` **Scanne les ports UDP**. Plus lent car UDP n'a pas d'accusé de réception.

Scan Passif

- **Description** : Analyse le trafic réseau existant **sans envoyer de requêtes** supplémentaires.
- **Utilisations** : Surveillance **discrète** des réseaux pour identifier les services actifs **sans se faire détecter.**
- **Exemple d'outils** : Wireshark, Zeek (anciennement Bro).
- **Méthode** : Observe les **échanges de données** en cours pour identifier les **ports** et **services** utilisés.

Résumé des États

Netstat n'est pas du scan de port,il fournit des détails sur les connexions réseau actuelles **sur votre propre machine**

Etat (Nmap)	Signification
Open	Port ouvert, une application écoute
Closed	Port fermé mais accessible
Filtered	Port filtré par un pare-feu
Unfiltered	Port accessible, mais état indéterminé

Etat (netstat)	Signification
LISTENING	En écoute pour des connexions entrantes
ESTABLISHED	Connexion TCP active
TIME_WAIT	Connexion récemment fermée, attente
CLOSE_WAIT	Connexion fermée par le client distant
SYN_SENT	Demande de connexion envoyée
SYN_RECEIVED	Demande de connexion reçue, en attente d'accusé de réception

Options sur nmap

Option	Description
-sS	Scan SYN furtif, rapide et discret pour détecter les ports ouverts.
-p	Spécifier les ports à scanner (ex: -p 80,443)
-A	Scan avancé : détection d'OS, versions, traceroute, scripts.
-sV	Identifier la version des services actifs.
-T<0-5>	Intensité du scan : 0 (lent) à 5 (agressif).
-sU	Scanner les ports UDP (plus lent que TCP).
-sC	Exécuter les scripts NSE par défaut pour vulnérabilités communes.
-F	Scan rapide des ports les plus fréquents.
--top-ports <num>	Scanner seulement les <num> ports les plus utilisés.

Option	Description
-n	Désactive la résolution DNS, affiche les adresses IP directement.
-Pn	Pas de ping initial, utile si la cible bloque ICMP.
-sT	Scan TCP complet, établit une connexion (moins furtif que -sS).
-O	Détection d'OS en analysant les réponses.
-D <IP1,IP2...>	Utiliser des adresses IP factices pour masquer l'origine.
-D RND:<num>	Utiliser <num> adresses IP aléatoires pour dissimuler le scan.
--script=<nom>	Exécuter des scripts NSE spécifiques (ex: vulnérabilités).
-sP / -sn	Ping scan : détecte les hôtes actifs sans scanner les ports.
-g <num>	Spécifier un port source (ex: -g 53) pour contourner les pare-feu.

Option	Description
-v / -vv	Mode verbeux pour plus de détails (-vv encore plus).
-f	Fragmentation des paquets pour contourner les IDS/pare-feu.
--open	Afficher uniquement les ports ouverts.
--reason	Afficher la raison pour chaque état de port (ouvert/fermé/filtré).
--traceroute	Exécuter un traceroute après le scan pour voir le chemin vers la cible.
--max-retries <num>	Limiter les tentatives de scan par port.
--max-rate <num>	Limiter le taux de scan (paquets par seconde) pour éviter la détection.