Nmap - Zmap et Nmap viewer

https://www.it-connect.fr/cours/nmap-cartographie-reseau-scan-de-vulnerabilites/

Quelques commandes de base :

nmap -A
Ou comment te griller et être détecté sur le réseau. Avec ça, tu seras blacklisté directement par n'importe quel firewall ou WAF, oublie.

nmap -PS
Ça fait un ping et ça scanne les ports 80 et 443, soit, les ports HTTP et HTTPS. C'est un peu plus discret, mais ça reste un scan.

nmap -sS
On oublie.
Pourquoi on oublie ? Si tu ne sais pas comment fonctionne TCP, petit rappel :
Quand tu fais une requête HTTP ou HTTPS, ça passe par le port 80 ou 443, c'est le port de destination.
HTTP est un protocole encapsulé dans TCP, donc il faut d'abord établir une connexion TCP avant de pouvoir envoyer une requête HTTP.

En vert, c'est la négociation pour commencer la communication, et c'est que du TCP
En bleu, c'est la communication de donné, tous les paquets HTTP seront dans les requêtes DATA encapsulés dans des paquets TCP.
En rouge, c'est la négociation pour stopper proprement la communication, c'est comme ça que fonctionne un navigateur pour parler avec un serveur web, ils restent polis.

image-1726232340841.png

Donc, nmap -sS, tu fais uniquement la requête SYN, ce qui est peu habituel, donc tu risques d'être grillé.
nmap -sT
Ça, c'est déjà mieux ; tu utilises la librairie de ton système pour faire des scans, ce qui rend Nmap moins détectable.

nmap -sV
Pour tenter de récupérer les versions des services exposés, c'est un peu plus discret, mais ça reste un scan. Avec ça, si les versions sont obsolètes, tu peux aller chercher des CVE pour les outils et versions correspondantes, et si tu as de la chance, une payload sera prête à l'emploi. Sinon, il faudra lire le rapport de la vulnérabilité et construire l'exploit toi-même.

nmap -O
Pour la détection des OS, ce n’est pas très précis, autant éviter et utiliser d’autres options.

nmap -p-
Ça scanne tous les ports, il y en a 65536. Et si tu le fais sans option de temps ou dans l’ordre, autant envoyer un mail pour dire que tu fais un scan.

nmap -T0
Paranoïde - Très lent et discret. Utilisé pour éviter la détection par les systèmes de détection d'intrusion (IDS). Peut-être très lent et générer beaucoup de bruit réseau.

nmap -T1
Sneaky - Lent. Plus discret mais toujours relativement lent. Adapté pour des scans dans des environnements où la discrétion est cruciale.

nmap -T2
Gentil - Modérément lent. Réduis la vitesse du scan pour minimiser l'impact sur le réseau cible.

nmap -T3
Normal - Vitesse normale. C’est le réglage par défaut si aucune option de timing n’est spécifiée.

nmap -T4
Agressive - Plus rapide. Utilise une approche plus agressive qui peut contourner les pare-feu et les IDS, mais est plus susceptible d’attirer l’attention.

nmap -T5
Insane - Très rapide et très agressif. Les réseaux et les cibles peuvent être surchargés par cette action, qui est généralement repérée rapidement par les systèmes de sécurité.

nmap -sU
Scan UDP – Lent mais nécessaire, il explore les profondeurs des services UDP comme DNS et DHCP.
Et le meilleur pour la fin, la commande à ne SURTOUT pas lancer.

Zmap :

https://open.substack.com/pub/naimaouaichia/p/zmap-loutil-de-scan-ultra-rapide?r=t9zmv&utm_medium=ios

Nmap fait son boulot, mais il a un petit défaut : il est un peu lent quand on lui demande de faire un gros scan.

zmap, lui, utilise des groupes multiplicatifs cycliques pour scanner l'espace d’adresses IP de manière pseudorandomisée, rendant le processus environ 1 300 fois plus rapide que Nmap.

Avec une simple commande apt install, je peux scanner des millions d’IP dans un temps relativement réduit.

Zmap est un outil accessible à tous... mais pas forcément fait pour tout le monde.

- La meilleure commande de Zmap, pour voir toutes les options disponibles:

> man zmap

- Pour scanner un réseau sur le port 80 et ranger tout le rapport dans un fichier:

> sudo zmap -p 80 X.X.X.X/24 -o resultat.csv

- Pour envoyer 1000 paquets par seconde

> sudo zmap -p 80 X.X.X.X/24 -r 1000 -o resultat.csv

- Pour blacklister certaines IP :

> sudo zmap -p 80 X.X.X.X/0 -b blacklist.txt -o resultat.csv

- Cette commande scanne tout l'espace IPv4 pour le port 80 en envoyant des paquets TCP SYN avec un payload personnalisé, et enregistre les résultats dans un fichier CSV.

> sudo zmap -p 80 X.X.X.X/0 -M tcp_synscan --probe-args="payload=sample_payload.bin" -o results.csv

---

Attention, les scans intensifs peuvent surcharger les réseaux et être considérés comme des attaques par déni de service.

Nmap Viewer : (visualisez vos résultats de scans réseau)

https://korben.info/nmap-viewer-visualisation-scans-reseau.html

---

Revision #5
Created 2024-09-13 10:56:44 UTC by Admin
Updated 2024-11-11 09:28:14 UTC by Admin