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.

SYN
SYN/ACK
ACK
DATA
DATA
ACK
FIN
ACK
FIN
ACK
Window
Process replicated regarding
the amount of data to be sent
Establishing connection
Transmitting data
Terminating connection

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

Nmap Cheat Sheet

comparitech

Different usage options

Port discovery and specification
Host discovery and specification
Vulnerability scanning
Application and service version detection
Software version detection against the ports
Firewall / IDS Spoofing

Port Specification Options

Syntax	Example	Description
-P	nmap -p 23 172.16.1.1	Port scanning port specific port
-P	nmap -p 23-100 172.16.1.1	Port scanning port specific port range
-p	nmap -pU:110,T:23-25,443 172.16.1.1	U-UDP,T-TCP different port types scan
-p-	nmap -p- 172.16.1.1	Port scan for all ports
-p	nmap -smtp,https 172.16.1.1	Port scan from specified protocols
-F	nmap -F 172.16.1.1	Fast port scan for speed up
-p "*"	namp -p "*" ftp 172.16.1.1	Port scan using name
-r	nmap -r 172.16.1.1	Sequential port scan

Scanning Types

Switch/Syntax	Example	Description
-sS	nmap 172.16.1.1 -sS	TCP SYN port scan
-sT	nmap 172.16.1.1 -sT	TCP connect port scan
-sA	nmap 172.16.1.1 -sA	TCP ACK port scan
-sU	nmap 172.16.1.1 -sU	UDP port scan
-Sf	nmap -Sf 172.16.1.1	TCP FIN scan
-sX	nmap -SX 172.16.1.1	XMAS scan
-Sp	nmap -Sp 172.16.1.1	Ping scan
-sU	nmap -Su 172.16.1.1	UDP scan
-sA	nmap -Sa 172.16.1.1	TCP ACK scan
-SL	nmap -Sl 172.16.1.1	list scan

Host /172.16.1.1 Discovery

Switch/Syntax	Example	Description
-sL	nmap 172.16.1.1-5 -sL	List 172.16.1.1 without scanning
-sn	nmap 172.16.1.1/8 -sn	Disable port scanning
-Pn	nmap 172.16.1.1-8 -Pn	Port scans only and no host discovery
-PS	nmap 172.16.1.185 -PS22-25,80	TCP SYN discovery on specified port
-PA	nmap 172.16.1.185 -PA22-25,80	TCP ACK discovery on specified port
-PU	nmap 172.16.1.1-8 -PU53	UDP discovery on specified port
-PR	nmap 172.16.1.1-1/8 -PR	ARP discovery within local network
-n	nmap 172.16.1.1 -n	no DNS resolution

Scanning Command Syntax

nmap [scan types] [options] {172.16.1.1 specification}

Use of Nmap Scripts NSE

nmap --script= test script 172.16.1.0/24	execute thee listed script against target IP address
nmap --script-update-db	adding new scripts
nmap -sV -sC	use of safe default scripts for scan
nmap --script-help="Test Script"	get help for script

Version Detection

Switch/Syntax	Example	Description
-sV	nmap 172.16.1.1 -sV	Try to find the version of the service running on port
-sV --version-intensity	nmap 172.16.1.1 -sV --version-intensity 6	Intensity level range 0 to 9.
-sV --version-all	nmap 172.16.1.1 -sV --version-all	Set intensity level to 9
-sV --version-light	nmap 172.16.1.1 -sV --version-light	Enable light mode
-A	nmap 172.16.1.1 -A	Enables OS detection, version detection, script scanning, and traceroute
-O	nmap 172.16.1.1 -O	Remote OS detection

Nmap output Formats

Default/normal output	nmap -oN scan.txt 172.16.1.1
XML	nmap -oX scanr.xml 172.16.1.1
Grepable format	nmap -oG grep.txt 172.16.1.1
All formats	nmap -oA 172.16.1.1

172.16.1.1 Specification

nmap 172.16.1.1	single IP scan
nmap 172.16.1.1 172.16.100.1	scan specific IPs
nmap 172.16.1.1-254	scan a range of IPs
nmap xyz.org	scan a domain
nmap 10.1.1.0/8	scan using CIDR notation
nmap -iL scan.txt	scan 172.16.1.1s from a file
nmap --exclude 172.16.1.1	specified IP s exclude from scan

Firewall Proofing

nmap -f [172.16.1.1]	scan fragment packets
nmap -mtu [MTU] [172.16.1.1]	specify MTU
nmap -sI [zombie] [172.16.1.1]	scan idle zoombie
nmap -source-port [port] [172.16.1.1]	manual source port - specify
nmap -data-length [size] [172.16.1.1]	randomly append data
nmap -randomize-hosts [172.16.1.1]	172.16.1.1 scan order randomization
nmap -badsum [172.16.1.1]	bad checksum

Miscellaneous Commands

nmap -6	scan IPV6 targets
nmap -proxies proxy 1 URL, proxy 2 URL	Run in targets with proxies
nmap -open	Show open ports only

Nmap Timing Options

Syntax	Description
nmap -T0 172.16.1.1	Slowest scan
nmap -T1 172.16.1.1	Tricky scan to avoid IDS
nmap -T2 172.16.1.1	Timely scan
nmap -T3 172.16.1.1	Default scan timer
nmap -T4 172.16.1.1	Aggressive scan
nmap -T5 172.16.1.1	Very aggressive scan

Scan Options

Syntax	Description
nmap -sP 172.16.1.1	Ping scan only
nmap -PU 172.16.1.1	UDP ping scan
nmap -PE 172.16.1.1	ICMP echo ping
nmap -PO 172.16.1.1	IP protocol ping
nmap -PR 172.16.1.1	ARP ping
nmap -Pn 172.16.1.1	Scan without pinging
nmap -traceroute 172.16.1.1	Traceroute

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