Nmap Analyse de Commandes Avancées

29.01.2025

Bodnar Georges

nmap -sS -p- -T4 -v -sC -sV -oA scan

1. Introduction à NMAP

NMAP (Network Mapper) est un outil open-source utilisé pour la découverte de réseau et l'audit de sécurité. Il permet d'identifier les hôtes actifs, les ports ouverts et les services en cours d'exécution.

2. Commandes de Base

Scan basique d'une cible

nmap <IP_cible>

Scanne les 1000 ports les plus courants de la cible.

Scan de ports spécifiques

nmap -p 22,80,443 <IP_cible>

Scanne uniquement les ports 22, 80 et 443.

Scan complet de tous les ports

nmap -p-

Scanne les 65535 ports disponibles.

Détection des services et versions

nmap -sV <IP_cible>

Identifie les services et leurs versions.

Scan furtif SYN (Stealth Scan)

nmap -sS <IP_cible>

Permet d'éviter d'être facilement détecté par les IDS/IPS.

IDS : mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée

Détection du système d'exploitation

nmap -O <IP_cible>

Identifie le système d'exploitation de la cible.

Scan avec script de détection de vulnérabilités

nmap --script=vuln <IP_cible>

Utilise des scripts pour détecter les vulnérabilités connues.

`-T4` (Optimisation de la vitesse)

Définit une vitesse de scan agressive (valeur de 4 sur une échelle de 0 à 5).

Accélère le scan mais peut être plus bruyant sur le réseau.

`-v` (Mode verbeux)

Affiche des informations détaillées en temps réel sur l'exécution du scan

`-sC` (Exécution des scripts par défaut de Nmap)
Utilise des scripts de la bibliothèque NSE (Nmap Scripting Engine) pour collecter plus d'informations sur la cible.

`-oA scan` (Sortie du rapport sous plusieurs formats)

Enregistre les résultats du scan dans trois formats : .nmap (lisible), .xml (traitable) et .gnmap (pour d'autres outils).

Tous les fichiers générés auront le préfixe scan (ex. scan.nmap, scan.xml).

4. Stratégies de Cartographie et Sécurité

- Cartographie du réseau : Utiliser nmap -sn 192.168.1.0/24 pour identifier les hôtes actifs.
- Filtrage de pare-feu : Analyser avec nmap -sA <IP_cible> pour voir si des pare-feux bloquent des ports.
- Test d'intrusion complémentaire : Utilisation de Metasploit ou Nessus pour approfondir l'analyse.

Conclusion

Maîtriser NMAP permet une analyse efficace des réseaux et une meilleure anticipation des vulnérabilités. Ce guide couvre les bases essentielles pour l'examen et la pratique en cybersécurité.