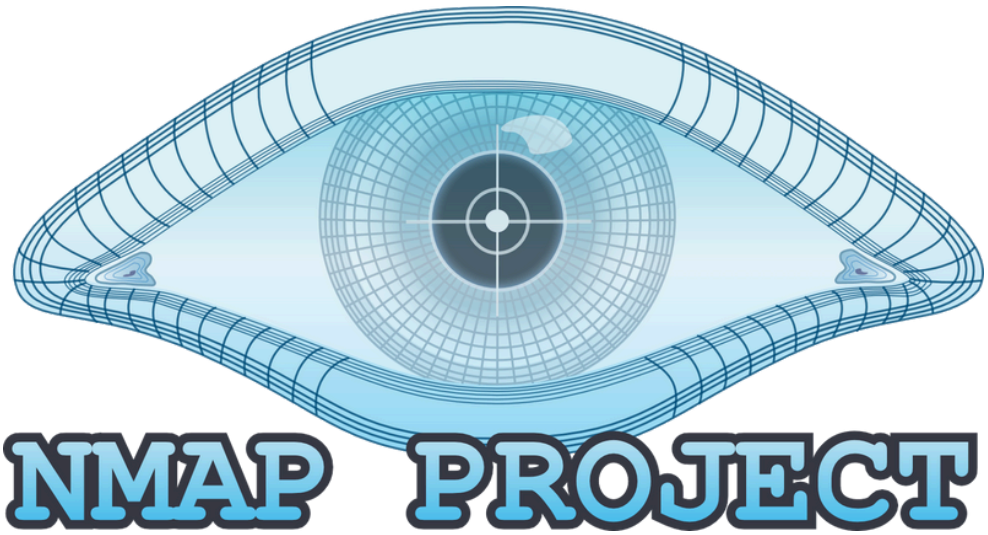
2025

DOCUMENTATION TECHNIQUE - NMAP



Présenté par :

ZOUAOUI Mehdi

2024

SOMMAIRE

2024

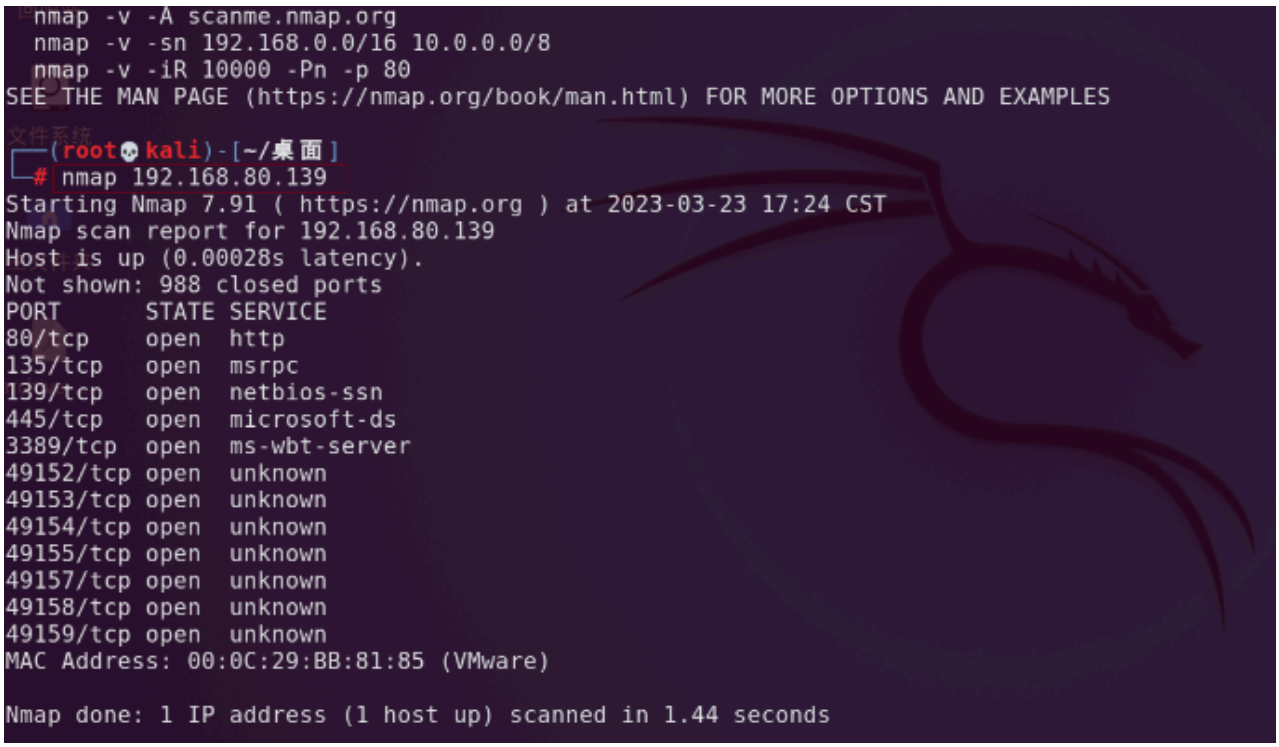
DOCUMENTATION TECHNIQUE NMAP

1. Introduction à Nmap

Nmap c'est quoi ?

Nmap (Network Mapper) est un outil open-source puissant pour la cartographie réseau, la découverte d'hôtes et l'audit de sécurité. Il permet :

- **L'identification des hôtes actifs.**
- **La détection des ports ouverts.**
- **L'analyse des services en cours d'exécution.**
- **L'évaluation des vulnérabilités réseau.**



DOCUMENTATION TECHNIQUE NMAP

2. Commandes Essentielles

Commande	Description
nmap <IP>	Scan des 1000 ports les plus courants.
nmap -p 22,80,443 <IP>	Scan ciblé des ports 22, 80 et 443.
nmap -p- <IP>	Scan de tous les 65535 ports TCP.
nmap -sS <IP>	Scan SYN furtif (stealth), discret face aux IDS/IPS.
nmap -sV <IP>	Identification des services et de leurs versions.
nmap -O <IP>	Détection du système d'exploitation.
nmap --script=vuln <IP>	Utilisation de scripts NSE pour identifier des vulnérabilités.
nmap -sC <IP>	Lancement des scripts par défaut (détection générale).
nmap -oA scan <IP>	Export des résultats en .nmap, .xml et .gnmap.

3. Options de Performance et de Détail

Option	Description
-T0 à -T5	Définit l'agressivité du scan (0 = très lent, 5 = très rapide).
-v	Mode verbeux (plus de détails pendant le scan).
-Pn	Ignore le ping préalable (utile si l'hôte ne répond pas à ICMP).
-n	Désactive la résolution DNS.
--disable-arp-ping	Ne pas envoyer de requêtes ARP (réseaux locaux).
--packet-trace	Affiche tous les paquets envoyés/reçus.

Exemple complet :

nmap -sS -p- -T4 -v -sC -sV -oA scan <IP>

Scan complet et rapide, avec scripts, détection de version, enregistrement des résultats.

DOCUMENTATION TECHNIQUE NMAP

4. Analyse Stratégique et Sécurité

Cartographie réseau

nmap -sn <IP>/24

- *Découverte des hôtes actifs sur un sous-réseau.*
- *Pare-feu et Filtrage*

nmap -sA <IP>

- *Vérifie la présence de filtrage par pare-feu (ACK scan).*
- *Audit de vulnérabilités*

nmap --script=vuln <IP>

- *Identification automatique des vulnérabilités connues.*

5. Exemples Avancés

Objectif	Commande
Scan avec OS, traceroute, scripts et versions	nmap -A <IP>
Désactiver le ping et DNS	nmap -Pn -n <IP>
Export dans 3 formats	nmap -oA resultat <IP>
Suivi complet des paquets	nmap --packet-trace <IP>

DOCUMENTATION TECHNIQUE NMAP

6. Conclusion

La maîtrise de Nmap est un atout essentiel en cybersécurité. Ce guide couvre les bases pratiques et avancées pour :

- **Cartographier un réseau.**
- **Identifier des services.**
- **Détecter des vulnérabilités.**
- **S'adapter aux contextes réseau réels.**

Exemple :

```
~/StationX  nmap -iL ip-addresses.txt -sV -oN common_services.txt

Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-29 11:39 EDT
Nmap scan report for 192.168.52.2
Host is up (0.00088s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
53/tcp open  domain  ISC BIND

Nmap scan report for 192.168.52.131
Host is up (0.0028s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 3.9p1 (protocol 1.99)
80/tcp   open  http     Apache httpd 2.0.52 ((CentOS))
111/tcp  open  rpcbind  2 (RPC #100000)
443/tcp  open  ssl/http Apache httpd 2.0.52 ((CentOS))
631/tcp  open  ipp      CUPS 1.1
3306/tcp open  mysql    MySQL (unauthorized)

Nmap scan report for 192.168.52.132
Host is up (0.00094s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
25/tcp  open  smtp        Postfix smtpd
80/tcp  open  http        Apache httpd 2.4.25 ((Debian))
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: Hosts:  symfonos.localdomain, SYMFONOS; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.52.129
```