Rapport d’audit de sécurité réseau – Projet MiniAuditSec

Projet : MiniAuditSec – Audit réseau de poste local

Réalisé par : Abdoul-Rachid BAWA

Niveau : Étudiant en 2e année d’Informatique de Gestion

Durée du projet : Juin 2025

Outils utilisés : Nmap (sous Windows), terminal CMD

1. Contexte

Ce mini-projet a pour objectif de simuler un audit de sécurité sur une machine personnelle (Windows).
L'analyse est effectuée via l'outil **Nmap**, connu pour la détection des services actifs et l'identification des ports ouverts.

Cet exercice vise à :

- développer ma compréhension des risques liés à l'exposition de services réseau,
- proposer des recommandations élémentaires en matière de sécurité.

2. Objectifs de l'audit

- Identifier les **ports ouverts** sur la machine
- Déterminer les **services** qui y sont associés
- Analyser les **risques potentiels**
- Formuler des **recommandations** concrètes

3. Outils utilisés

Outil	**Rôle**
Nmap	Scanner les ports et services
Zenmap *(optionnel)*	Interface graphique de Nmap
Windows 10	Machine scannée (adresse IP locale 127.0.0.1)

4. Résultats du scan

Commande utilisée :

nmap -sV 127.0.0.1

Résultat brut :

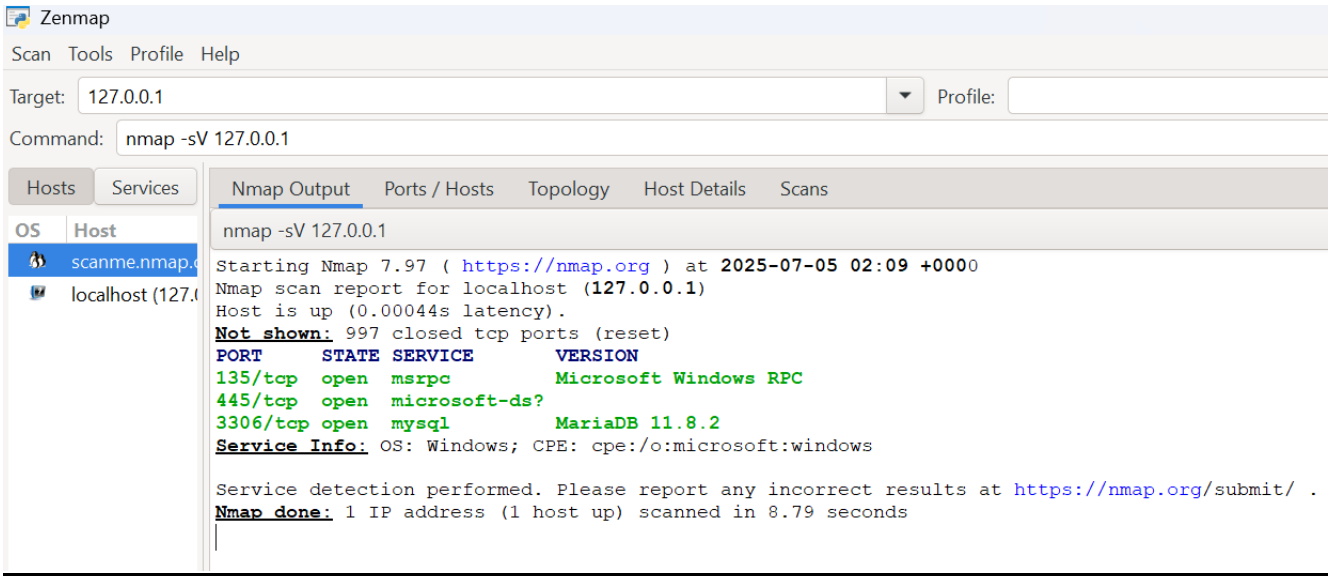
PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

445/tcp open microsoft-ds?

3306/tcp open mysql MariaDB 11.8.2

Capture d'écran du scan :



5. Analyse des services

Port	Service	Description	Risques identifiés	Recommandations
135	RPC (msrpc)	Appels de procédure à distance Windows	Ciblé par malwares (WannaCry, etc.)	Bloquer sur les interfaces publiques

Port	Service	Description	Risques identifiés	Recommandations
445	SMB (NetBIOS)	Partage de fichiers réseau Windows	Exploité par EternalBlue, failles SMBv1	Désactiver SMBv1, sécuriser ou bloquer
3306	MariaDB	Système de base de données	Accès potentiel aux données, version exposée	Limiter accès à localhost, mot de passe fort

---

6. Recommandations globales

- Désactiver les services réseau non nécessaires
- Bloquer les ports sensibles via un pare-feu local
- Mettre à jour régulièrement les services actifs (MariaDB, Windows Update)
- Utiliser un antivirus fiable et maintenir un suivi de sécurité

7. Leçons apprises

Grâce à cet exercice :

- J’ai découvert les **bases de l’audit de port**
- J’ai appris à **interpréter les résultats d’un scan**
- Je comprends mieux **les risques liés aux services exposés**

8. Conclusion

Ce mini-audit réseau montre ma capacité à utiliser des outils professionnels comme Nmap pour identifier des failles potentielles.
Ce projet reflète mon **engagement à progresser en sécurité informatique**, domaine essentiel en entreprise aujourd’hui.

Fait à Lomé, en Mars 2025
Abdoul-Rachid BAWA
Étudiant en Informatique de Gestion