Projet Professionnel — Sécurité Réseau

Analyse de réseau locale avec Nmap et Zenmap

Auteur :
Yacine Sehli

Étudiant passionné en cybersécurité et réseaux

Date : Octobre 2025

Durée du projet : 2 jours

Résumé

Ce projet présente une analyse complète du réseau local réalisée à l'aide des outils **Nmap** et **Zenmap**. L'objectif était de découvrir les hôtes actifs, d'identifier les ports ouverts et de reconnaître les systèmes d'exploitation afin d'évaluer la sécurité du réseau. Le projet a été mené sur une période de deux jours, en utilisant un environnement **Kali Linux** configuré sur une machine virtuelle.

Table des matières

1. Introduction

La sécurité des réseaux est un enjeu majeur dans le domaine de la cybersécurité. Pour tout administrateur ou analyste SOC, la connaissance des outils de scan réseau est essentielle pour détecter les vulnérabilités potentielles. **Nmap** (Network Mapper) est un des outils les plus puissants pour cette tâche, et **Zenmap** constitue son interface graphique conviviale.

Ce rapport documente les différentes étapes de la mise en œuvre d'un scan réseau local, effectué sur l'adresse **192.168.1.1**, ainsi que l'analyse et l'interprétation des résultats obtenus.

2. Présentation de Nmap et Zenmap

2.1 Nmap

Nmap est un outil open source utilisé pour l'exploration réseau et l'audit de sécurité. Il permet de découvrir les hôtes présents sur un réseau, les ports ouverts, les services disponibles et les systèmes d'exploitation associés.

2.2 Zenmap

Zenmap est l'interface graphique officielle de Nmap. Elle facilite la création, la sauvegarde et la visualisation des scans, notamment à travers des profils prédéfinis comme le « *Intense Scan* ».

3. Objectifs du projet

Les objectifs principaux de ce projet étaient :

— Comprendre le fonctionnement des commandes Nmap et Zenmap ;

— Effectuer un scan complet d'un hôte local (**192.168.1.1**) ;

— Identifier les ports et services ouverts ;

— Analyser le type de système détecté ;

— Présenter les résultats dans un rapport professionnel.

4. Environnement et configuration

4.1 Matériel et logiciel utilisés

— Système d'exploitation : **Kali Linux 2025**
— Outils : **Nmap 7.95** et **Zenmap GUI**
— Machine virtuelle : Oracle VirtualBox
— Cible : **192.168.1.1** (routeur / passerelle locale)

4.2 Préparation du scan

Le scan a été réalisé dans un environnement isolé, sans impact sur le réseau de production. Les permissions administrateur ont été utilisées pour garantir un scan complet et précis.

5. Méthodologie et commandes utilisées

Deux types de scans ont été réalisés :

5.1 Scan Nmap en ligne de commande

Listing 5.1 – Scan complet de tous les ports TCP

```
nmap -p0-65535 192.168.1.1
```

5.2 Scan approfondi avec détection d'OS et de services

Listing 5.2 – Scan avancé avec détection complète

```
nmap -p1-65535 -T4 -A -v 192.168.1.1
```

Les options utilisées :

- `-p1-65535` : scan de tous les ports TCP.
- `-T4` : vitesse du scan augmentée.
- `-A` : détection de l'OS et des services.
- `-v` : mode verbeux.

6. Résultats et interprétation

6.1 Extrait des résultats obtenus

Les ports suivants ont été détectés ouverts sur l'hôte :

— **53/tcp** — service DNS
— **80/tcp** — service HTTP (serveur web)
— **139/tcp** — NetBIOS Session Service
— **445/tcp** — Microsoft-DS (partage de fichiers)
— **2000/tcp** — Cisco SCCP
— **5060/tcp** — SIP (Session Initiation Protocol)

6.2 Analyse

Les services détectés indiquent que la machine cible agit comme un routeur ou un équipement de communication (ex. passerelle VoIP ou VirtualBox NAT). Les ports 2000 et 5060 révèlent des protocoles de communication VoIP, tandis que 80 et 53 indiquent des services web et DNS.

```
┌──(yacine㉿kali)-[~]
└─$ nmap -p0-65535 192.168.1.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-19 11:58 +01
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 14.41% done; ETC: 12:03 (0:04:27 remaining)
Stats: 0:02:55 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 61.36% done; ETC: 12:03 (0:01:50 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.12s latency).
Not shown: 65531 filtered tcp ports (no-response), 1 filtered tcp ports (net-unreach)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 284.51 seconds
```

FIGURE 6.1 – Résultat du scan Nmap en ligne de commande

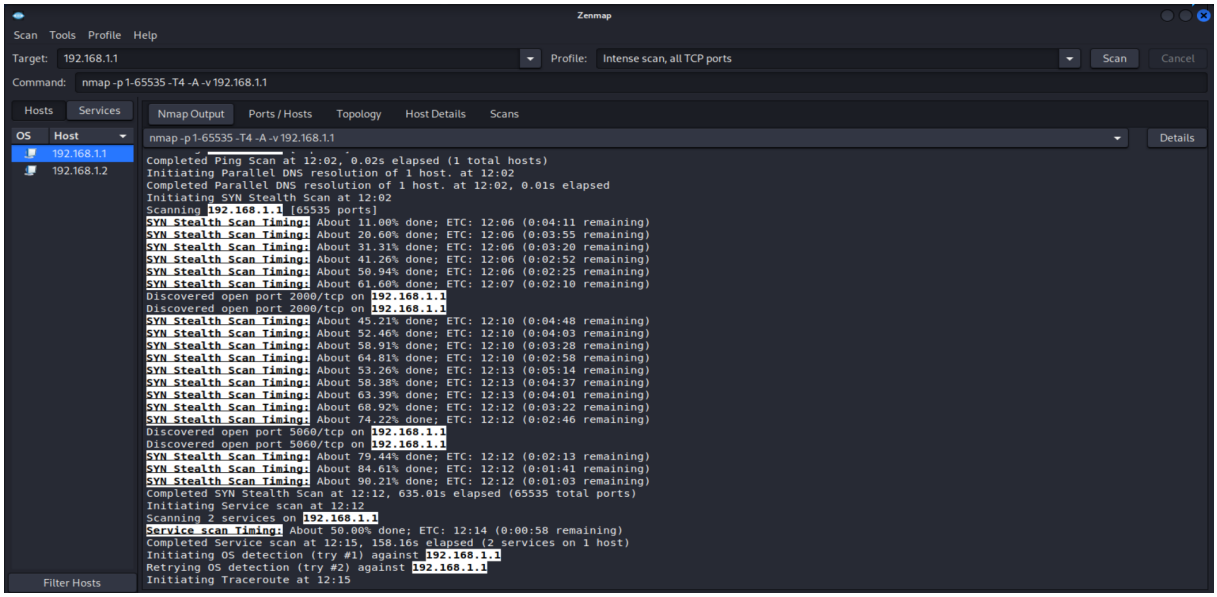

FIGURE 6.2 – Résultat du scan Zenmap (Intense Scan)

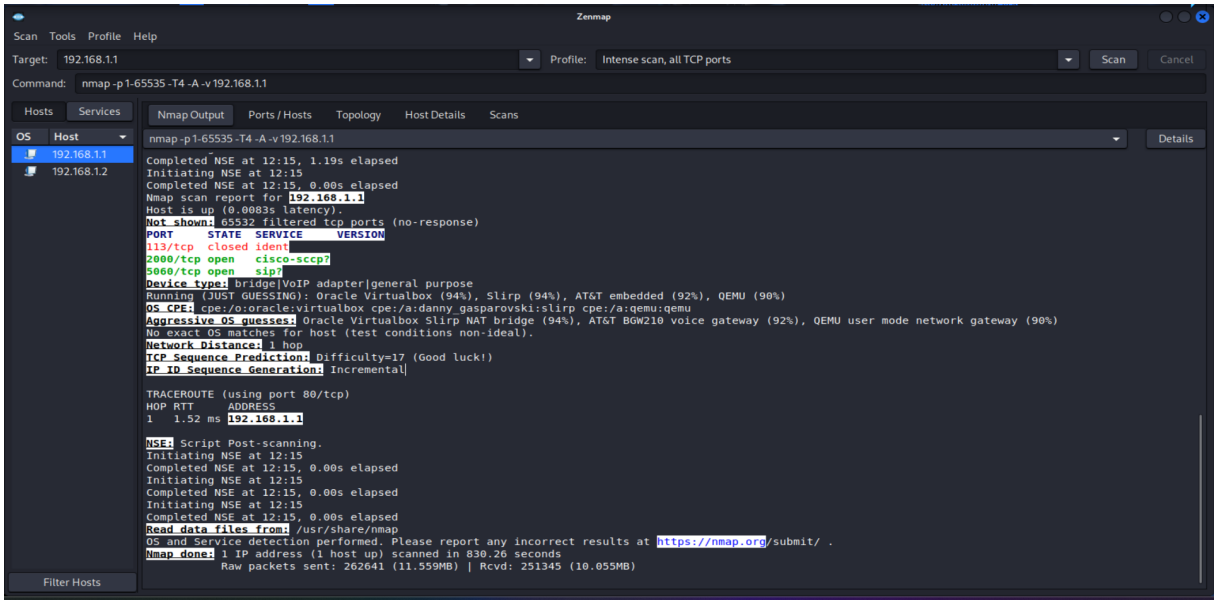

FIGURE 6.3 – Résultat du scan Zenmap (Intense Scan)

7. Analyse critique et bonnes pratiques

— Vérifier les permissions et la portée du scan avant exécution.
— Utiliser les options Nmap de façon responsable et légale.
— Documenter chaque commande pour assurer la traçabilité.
— Compléter l'analyse avec d'autres outils (Wireshark, Nikto, etc.).

8. Conclusion et perspectives

Ce projet m'a permis de maîtriser les fonctionnalités essentielles de Nmap et Zenmap en seulement deux jours. L'analyse m'a offert une meilleure compréhension de la topologie réseau, de l'identification des ports et des services, ainsi que de la détection d'OS. À l'avenir, je compte approfondir mes connaissances en automatisant les scans via des scripts Nmap et en couplant les résultats à des outils d'analyse avancée.

À propos de l'auteur

Yacine Sehli est un étudiant passionné par la cybersécurité, les systèmes et réseaux, et les outils d'analyse de vulnérabilités. Il s'intéresse particulièrement à la défense des infrastructures et à la sécurisation des environnements Linux.