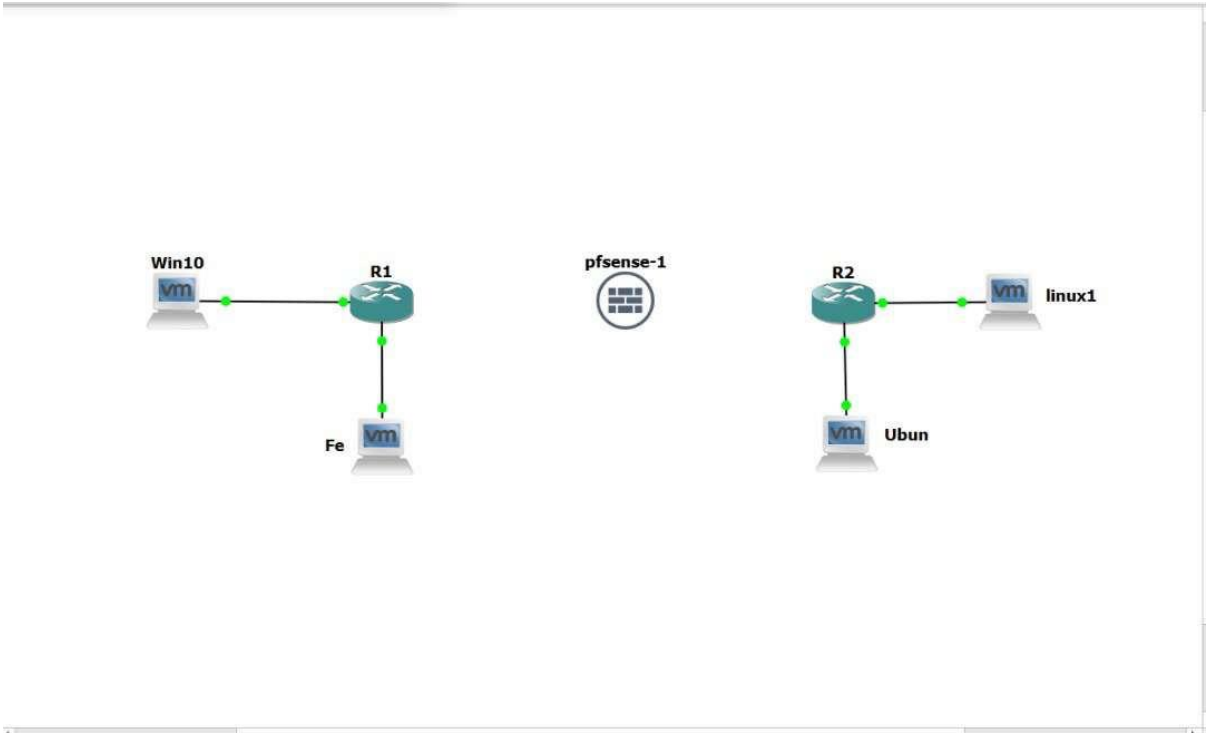
TP : Audit de Sécurité d'un Réseau Local

INTRODUCTION

Objectif : Tester la sécurité d'un réseau interne fictif pour identifier les vulnérabilités et proposer des mesures correctives.

TOPOLOGIE DU TP



Voici le graphique que j'ai pu faire pour avoir un aperçu pour pouvoir continuer le travail

1)MÉTHODOLOGIE

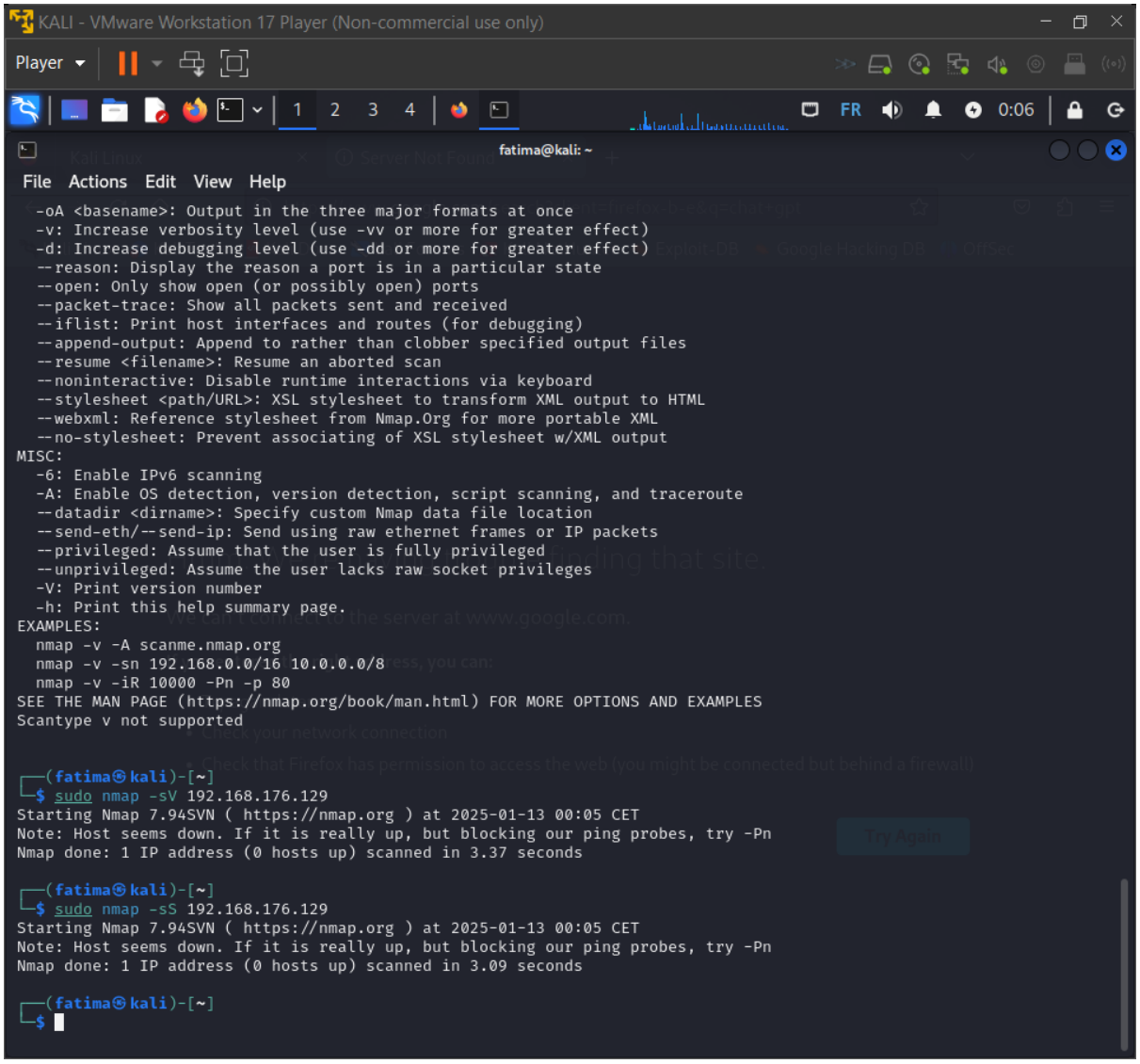
D'abord nous allons installer nos machine virtuelle pour pouvoir faire le travail

- Ensuite je vais mettre tout les machine en mm reseau pour permettre la connectivité entre eux et facilité le travail
- Nous allons utilisé kali comme systeme d'exploitation ,Ubuntu comme server ,Pfsense,win 10 et fedora et linux mint comme des clients

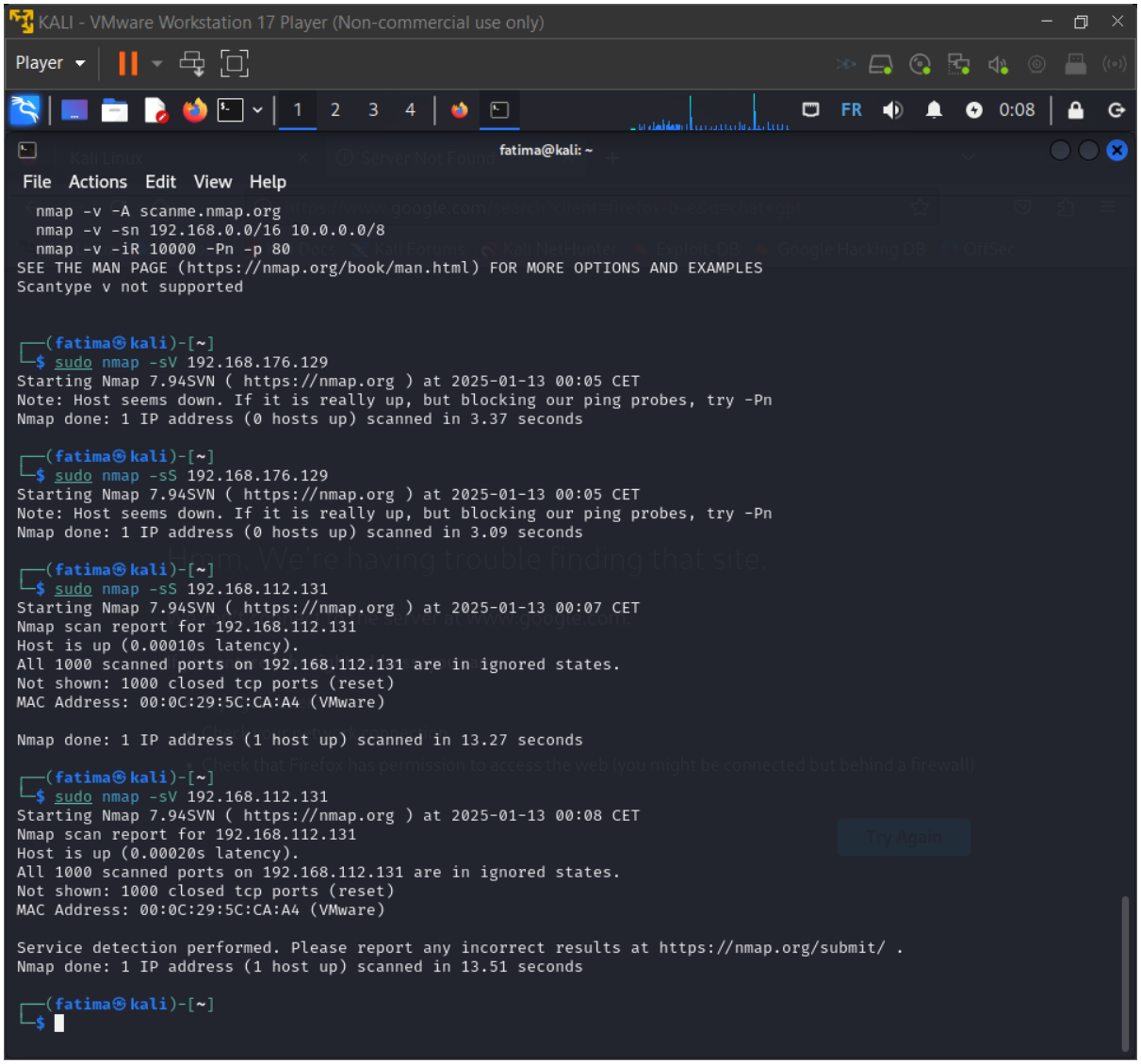
Nmap : Pour la découverte de réseau et le scan des ports.

A) KALI

Elle va nous permet faire le scanne de réseau et le scan des ports

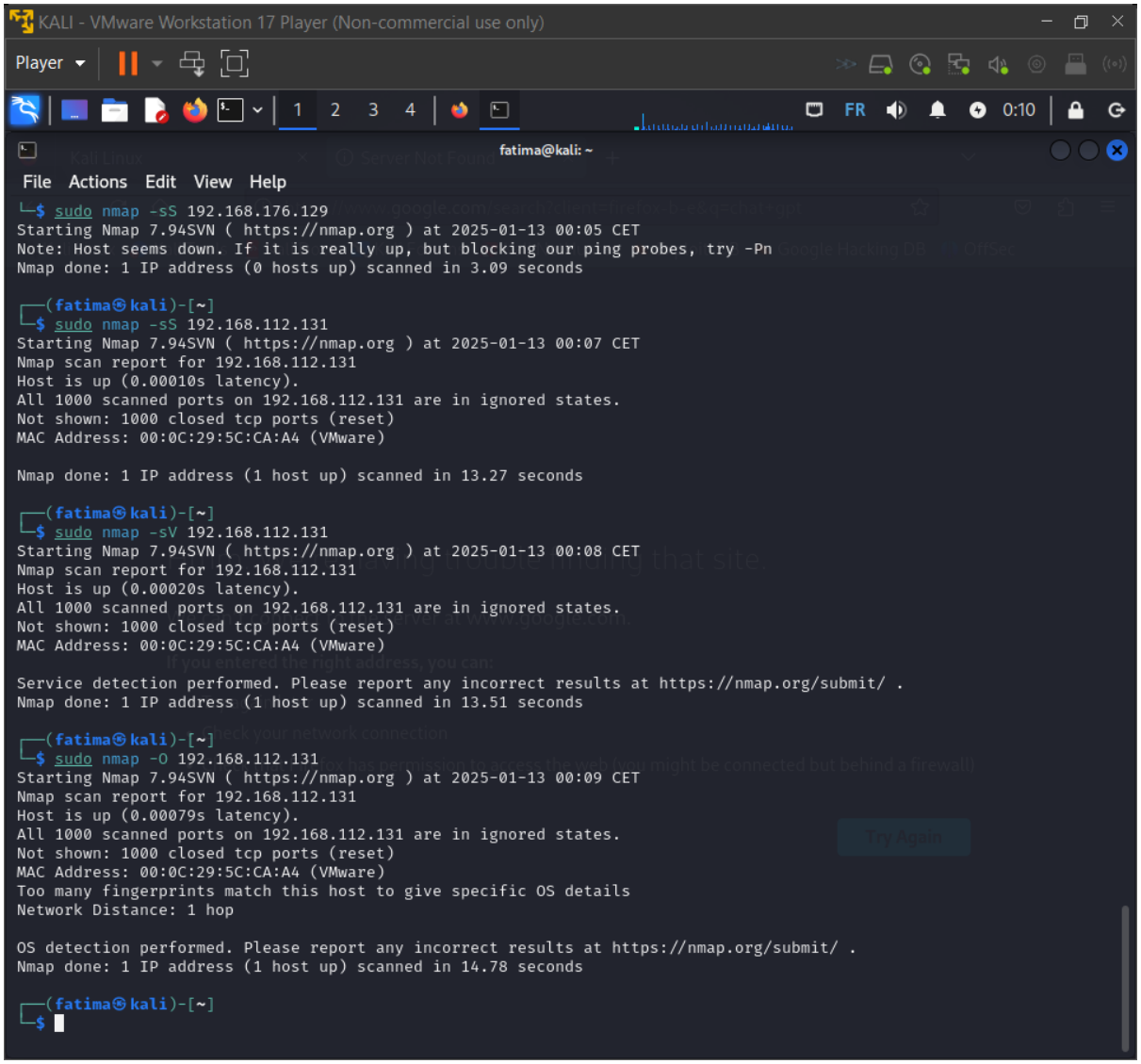


On utilise nmap sS La commande `nmap -sS` est utilisée pour effectuer un "SYN scan" (scan SYN), également appelé "scan furtif" ou "half-open scan". Ce type de scan est populaire en raison de sa rapidité et de sa capacité à éviter la détection par certaines configurations de pare-feu ou de systèmes de détection d'intrusion (IDS).

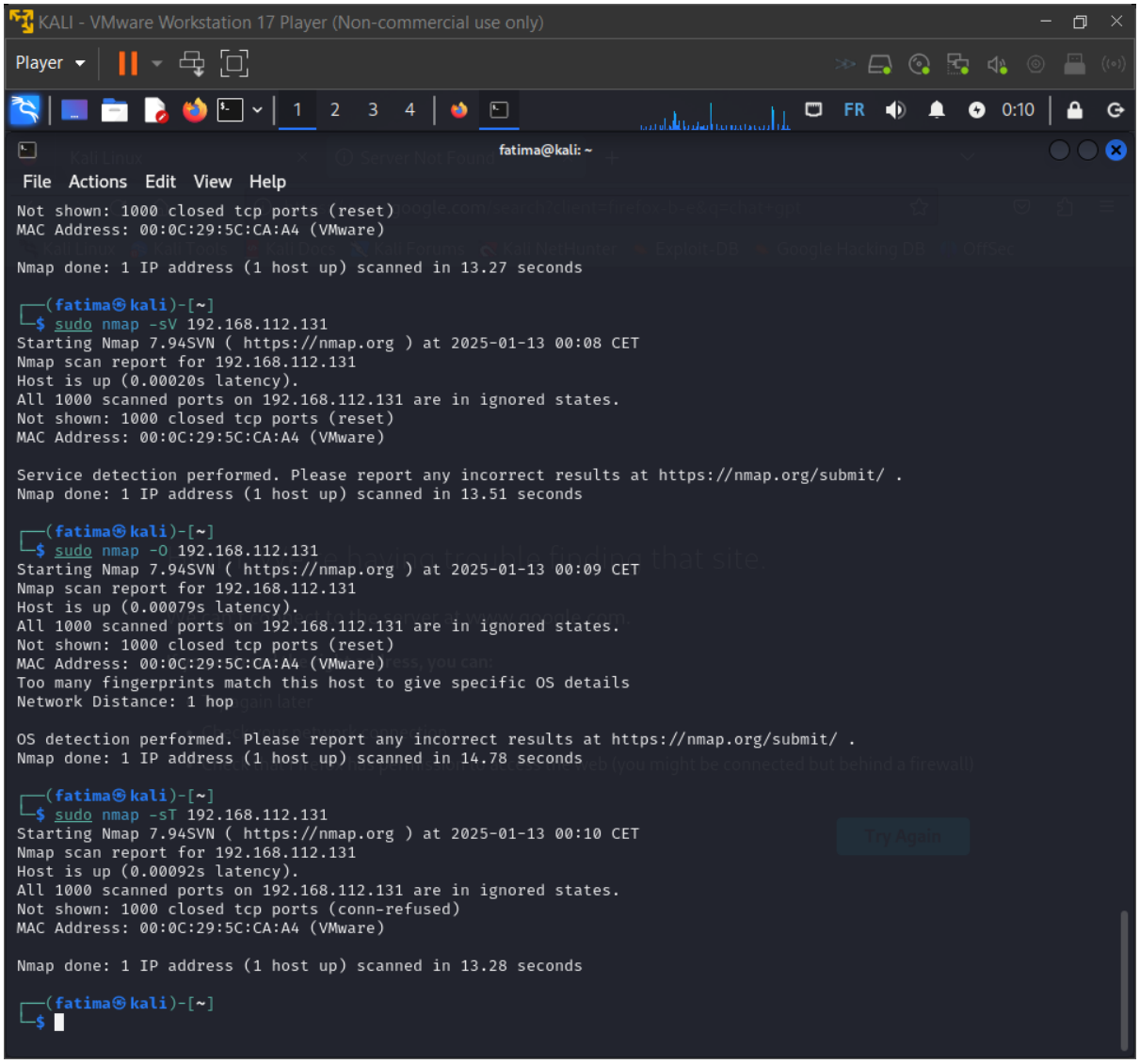


a commande `nmap -sV` est utilisée pour effectuer un scan de **détection de version des services** sur les ports ouverts d'un hôte cible. Ce scan permet à Nmap de déterminer quel logiciel (et sa version) est en cours d'exécution sur un port spécifique.

Voici le fonctionnement de `nmap -sV` :



La commande `nmap -O` est utilisée pour activer la détection du **système d'exploitation** (OS detection) d'un hôte cible. Lorsque vous utilisez l'option `-O`, Nmap tente d'identifier le système d'exploitation qui tourne sur la machine cible en analysant les réponses aux paquets envoyés pendant le scan.



La commande `nmap -sT` est utilisée pour effectuer un **scan de connexion complète** (ou "TCP connect scan"). Contrairement au scan **SYN** (`-sS`), qui n'achève pas la connexion TCP, le scan `-sT` tente d'établir une connexion complète avec chaque port ouvert sur la cible.

On a utiliser sa pour chaque machine client client pour verifier le reseau et les porsts ouverts avec Kali vu qu'il a deja nmap dedans

Nmap est un outil puissant pour l'exploration et l'analyse de réseaux. Il est essentiel pour les administrateurs réseau, les experts en sécurité et les tests de pénétration afin de surveiller, sécuriser et analyser les réseaux.

NB: J'ai pas pu utiliser NESSUS et wirshark parce que j'avais des probleme avec machine