PENTEST –
TEST AUDIT DE SECURITE’

BTS S.I.O. option S.I.S.R. 2025 – 2026

MR Michele Mastrogiacomo

Introduction

Contexte BTS SIO SISR

Dans le cadre du BTS S.I.O. , option S.I.S.R. , ce TP s'inscrit dans une démarche d'initiation à la sécurité des systèmes d'information.

TP de format réduit, l'objectif n'est pas de présenter une méthodologie d'attaque ni de fournir un guide d'intrusion, mais de comprendre le principe d'un **audit de sécurité** dans un environnement contrôlé et isolé.

Ce travail permet d'identifier, analyser et comprendre d'éventuelles vulnérabilités présentes dans un système d'information afin d'en améliorer la sécurité.

L'ensemble des manipulations est réalisé dans un environnement de laboratoire virtualisé afin de garantir un cadre sécurisé, isolé et strictement pédagogique.

Objectif du TP

Ce TP a pour objectif de mettre en place un environnement de test permettant de réaliser un audit de sécurité basique.

Les travaux réalisés permettent notamment de :

- comprendre la notion de surface d'attaque dans un réseau,
- identifier les services exposés sur une machine cible,
- analyser les résultats d'un scan dans une logique de diagnostic et non d'exploitation malveillante.

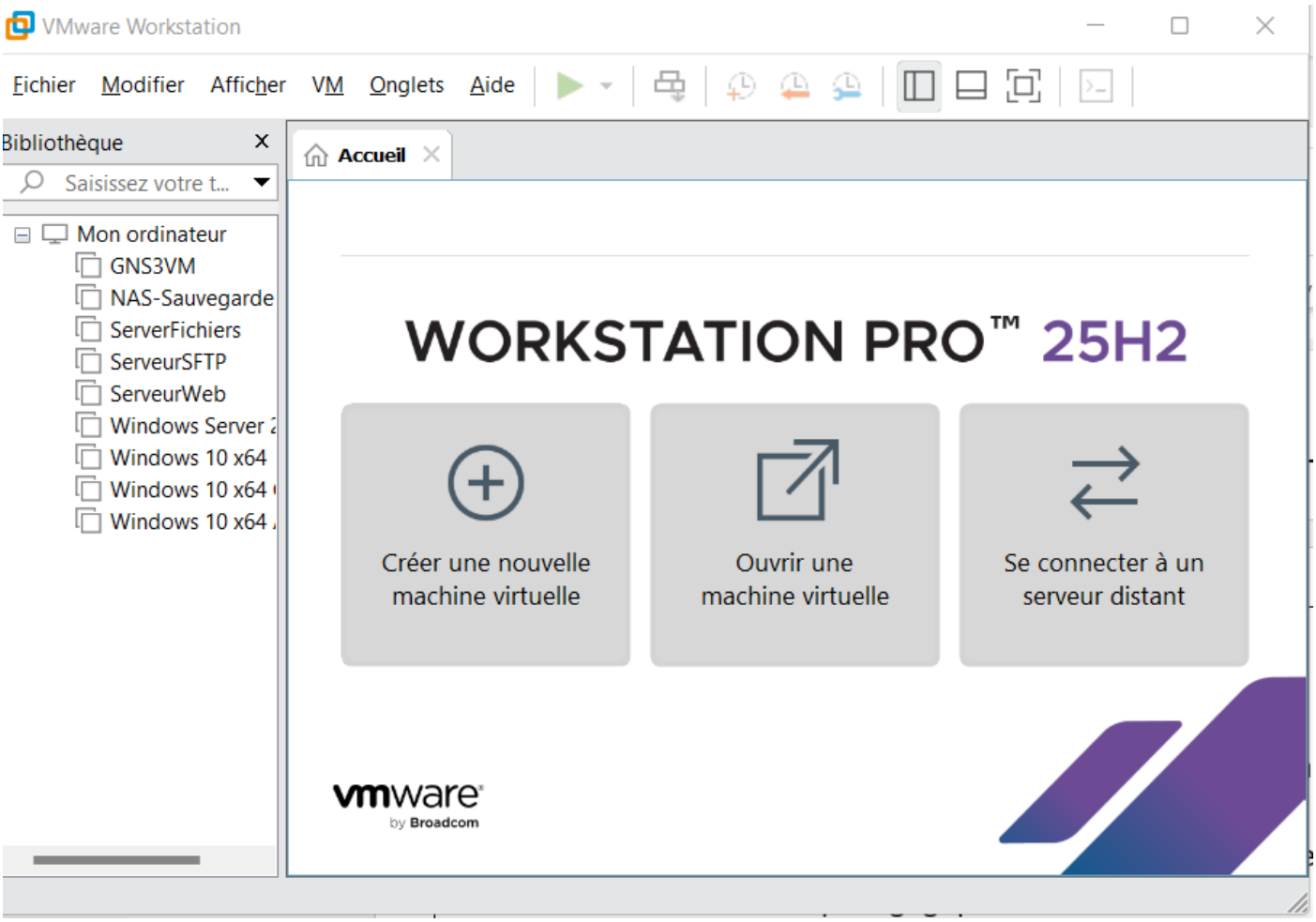
Mise en place de l'environnement virtuel

Présentation de VMware

VMware Workstation est un logiciel de virtualisation permettant de créer plusieurs machines virtuelles sur un même poste physique.

Dans ce TP, il est utilisé afin de simuler un environnement réseau isolé pour réaliser un audit de sécurité dans un cadre pédagogique.

Image 1 : VMware Workstation Pro 25h2

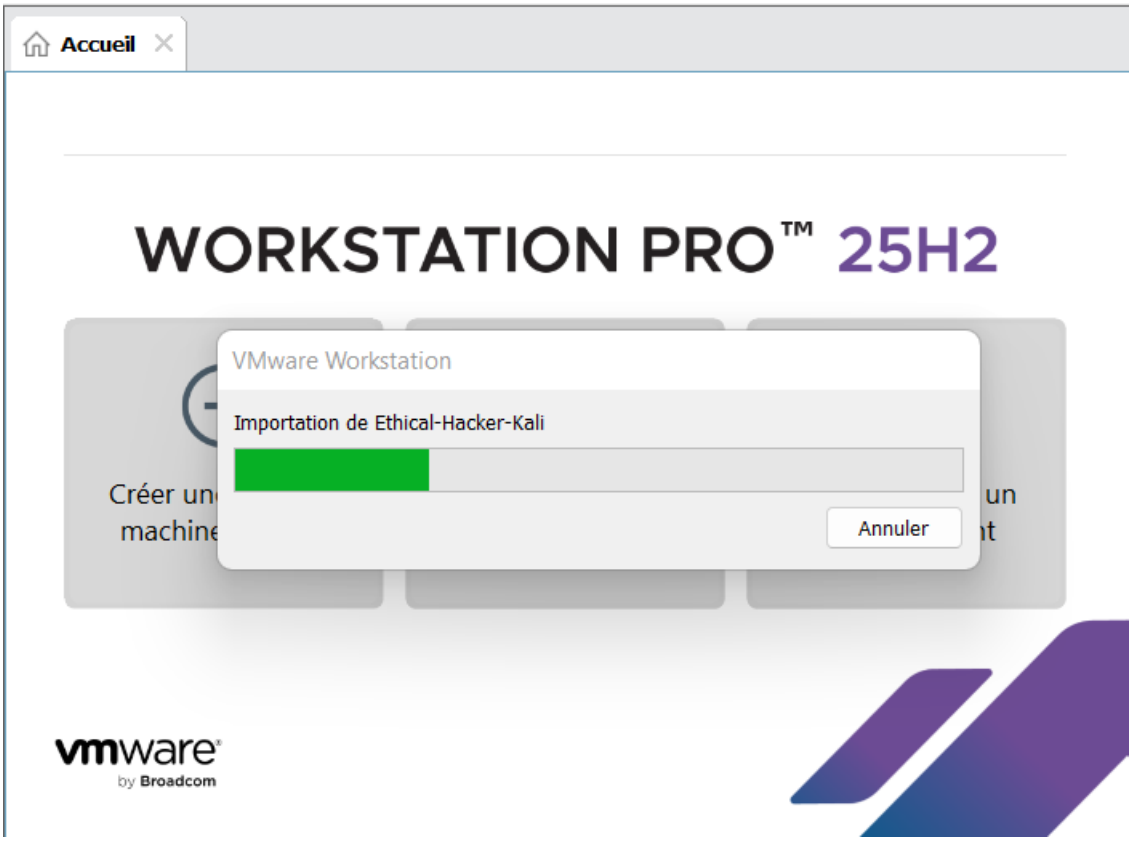


Création de la machine virtuelle Kali Linux

Une machine virtuelle a été importé afin de servir de poste d'audit et d'analyse de sécurité. Cette machine utilise Kali Linux, une distribution spécialisée dans les outils de cybersécurité.

Un 'image VMWare était déjà prêt j'ai effectué l'importation avec les outils nécessaire aux études. Toutes le machine sont configure Host-only c'est-à-dire un réseau privé pas connecté sur internet.

Image 2 : Importation de la machine virtuelle Kali Linux



Création de la machine cible (Metasploitable 2)

Afin de simuler un système volontairement vulnérable, la machine virtuelle Metasploitable 2 a été utilisée.

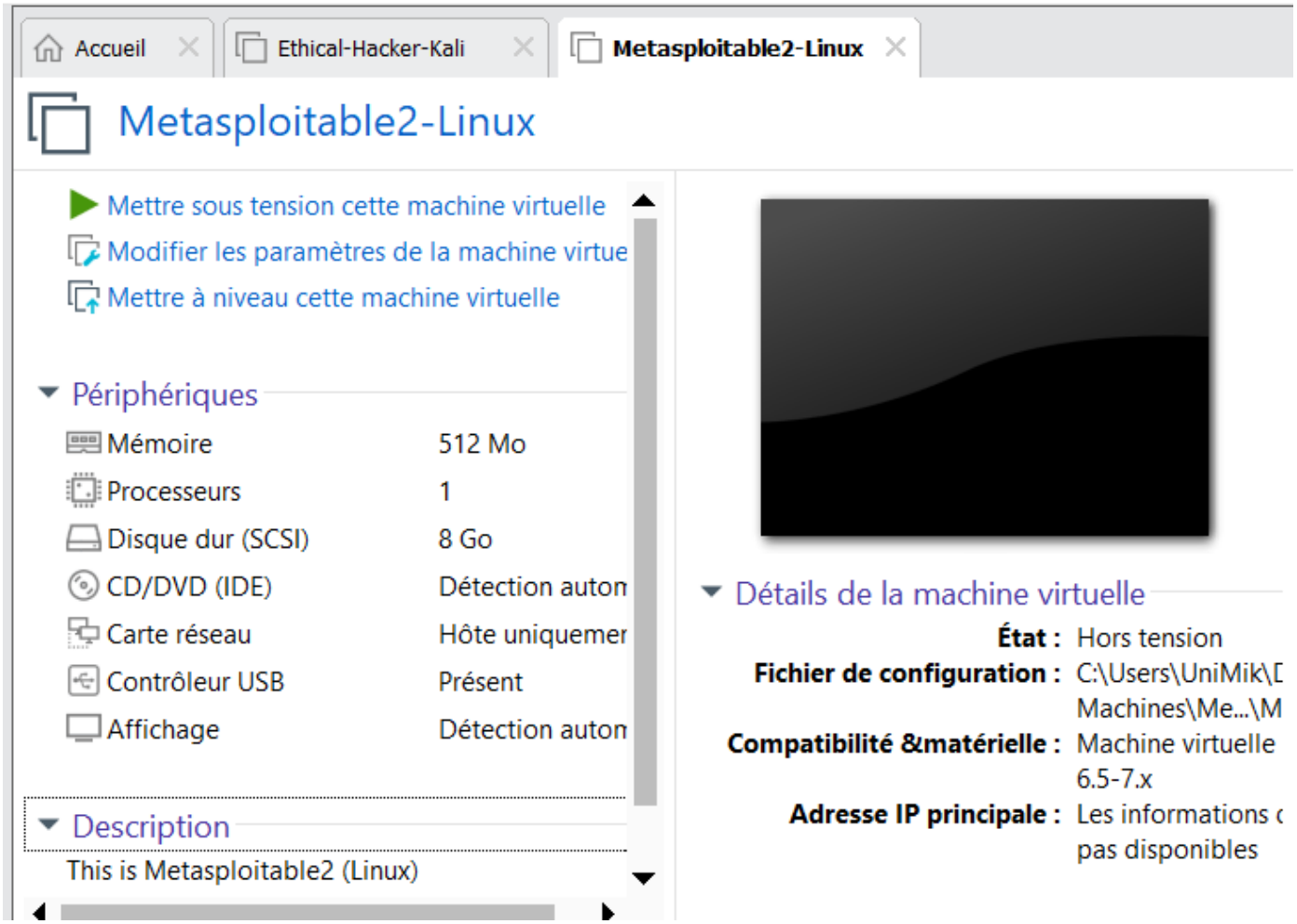
Metasploitable 2 est un système d'exploitation conçu spécifiquement pour l'apprentissage de l'audit de sécurité et des tests d'intrusion en environnement contrôlé.

Cette machine contient volontairement de nombreuses vulnérabilités au niveau des services réseau, ce qui en fait une cible idéale pour un TP d'analyse de sécurité. Toutes le machine sont configure Host-only c'est-à-dire un réseau privé pas connecté sur internet.

Remarque importante

Cette machine ne doit jamais être exposée sur un réseau public ou en dehors d'un environnement isolé, car elle contient des failles critiques intentionnelles.

Image 3 : Importation Machine virtuelle Metasploitable 2 dans VMware



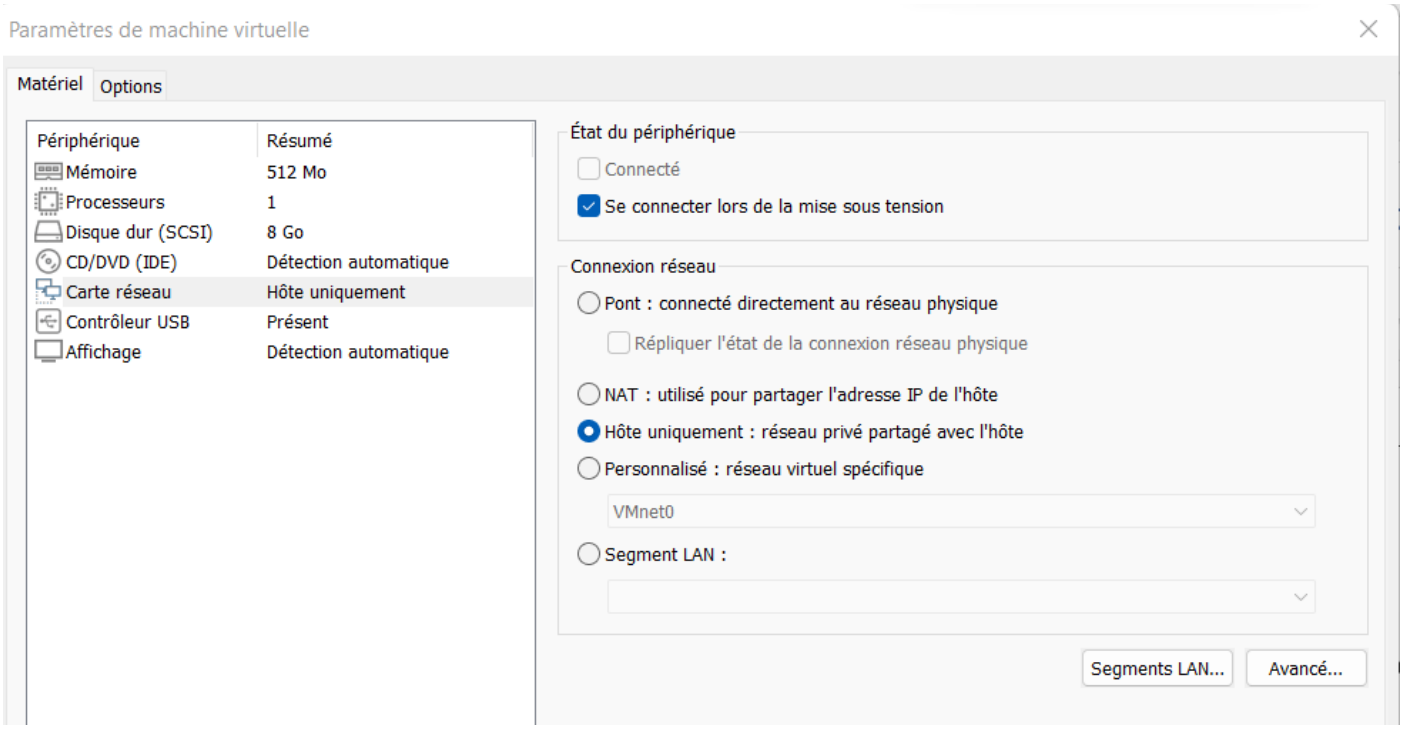
Configuration du réseau virtuel

Un réseau isolé a été configuré afin de permettre uniquement la communication entre les machines virtuelles du laboratoire.

Le mode **Host-Only** a été utilisé afin de garantir que les machines ne soient pas accessibles depuis Internet.

Cet environnement constitue la base nécessaire pour la réalisation des tests d'audit

Image 4 : Paramètres réseau des machines virtuelles



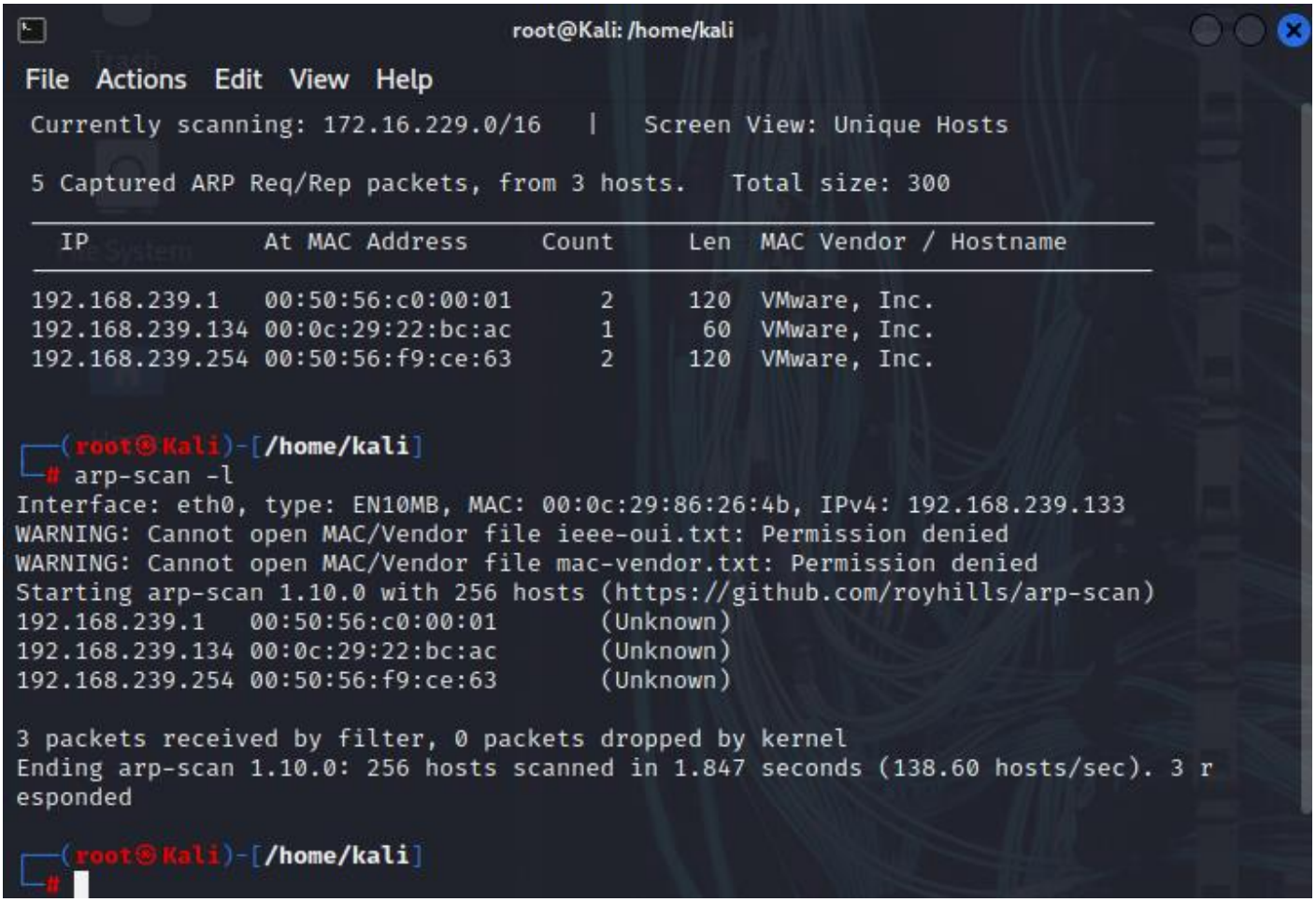
Réalisation de l'audit de sécurité

Découverte du réseau (reconnaissance)

L'étape de découverte du réseau permet d'identifier les machines présentes dans l'environnement virtuel ainsi que leurs adresses IP.

Cette phase est essentielle dans un audit de sécurité, car elle permet de cartographier le réseau avant toute analyse plus approfondie.

Image 5 : Résultat de la découverte réseau (IP des machines)



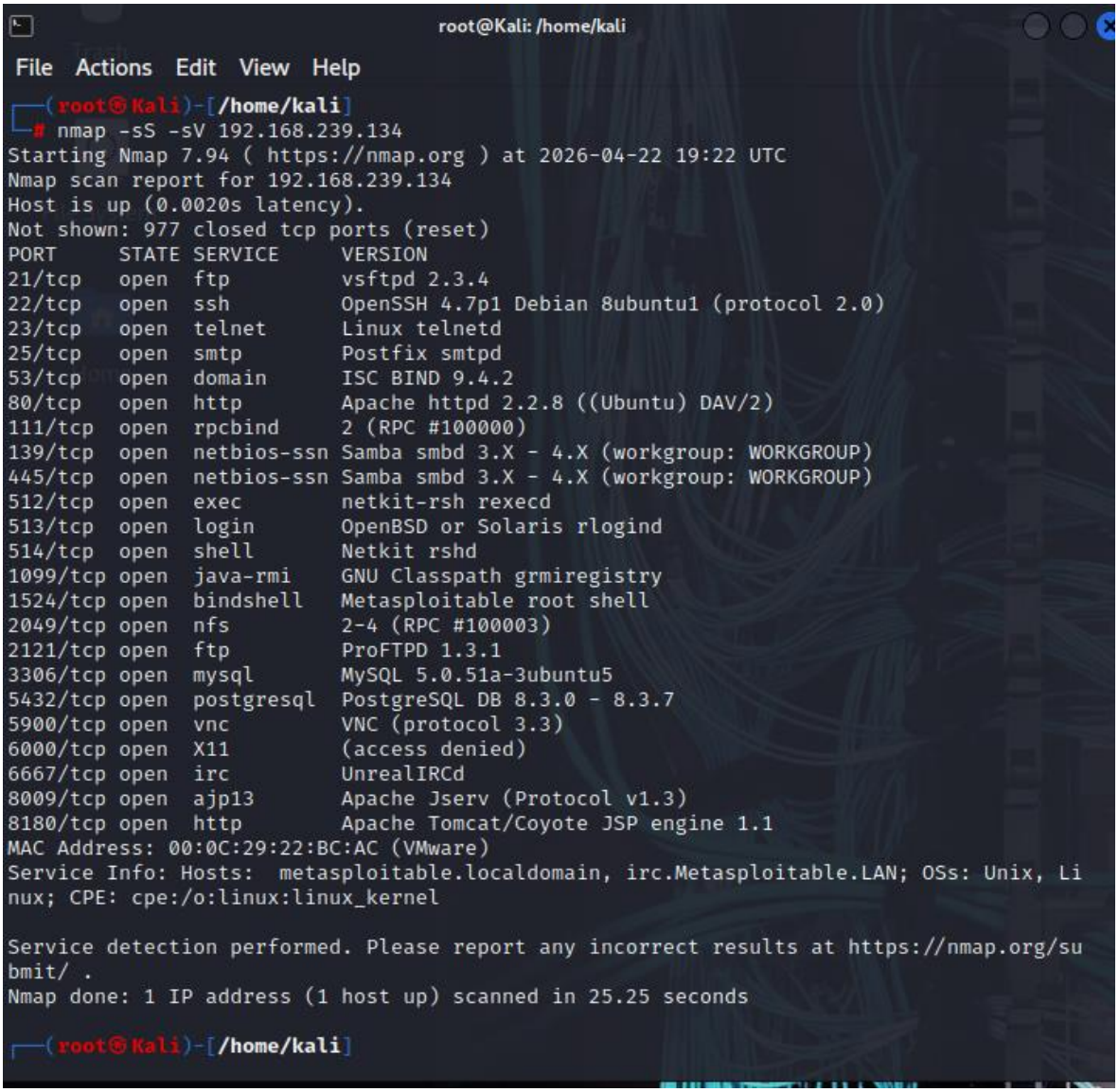
Scan des ports avec Nmap (ligne de commande)

Une analyse des services actifs sur la machine cible a été réalisée à l'aide de l'outil Nmap.

Nmap est un outil permettant d'identifier les ports ouverts, les services actifs et les versions logicielles associées.

Utilisé depuis le terminal sans interface GUI. Un scan TCP SYN (rapide et discret) avec enumeration des version des services

Image 6 : Scan réseau ciblé depuis nmap



Analyse des résultats

Le scan a permis de détecter plusieurs services actifs sur la machine cible, notamment :

- FTP (port 21)
- SSH (port 22)
- HTTP (port 80)
- MySQL (port 3306)
- Services RPC et autres services vulnérables

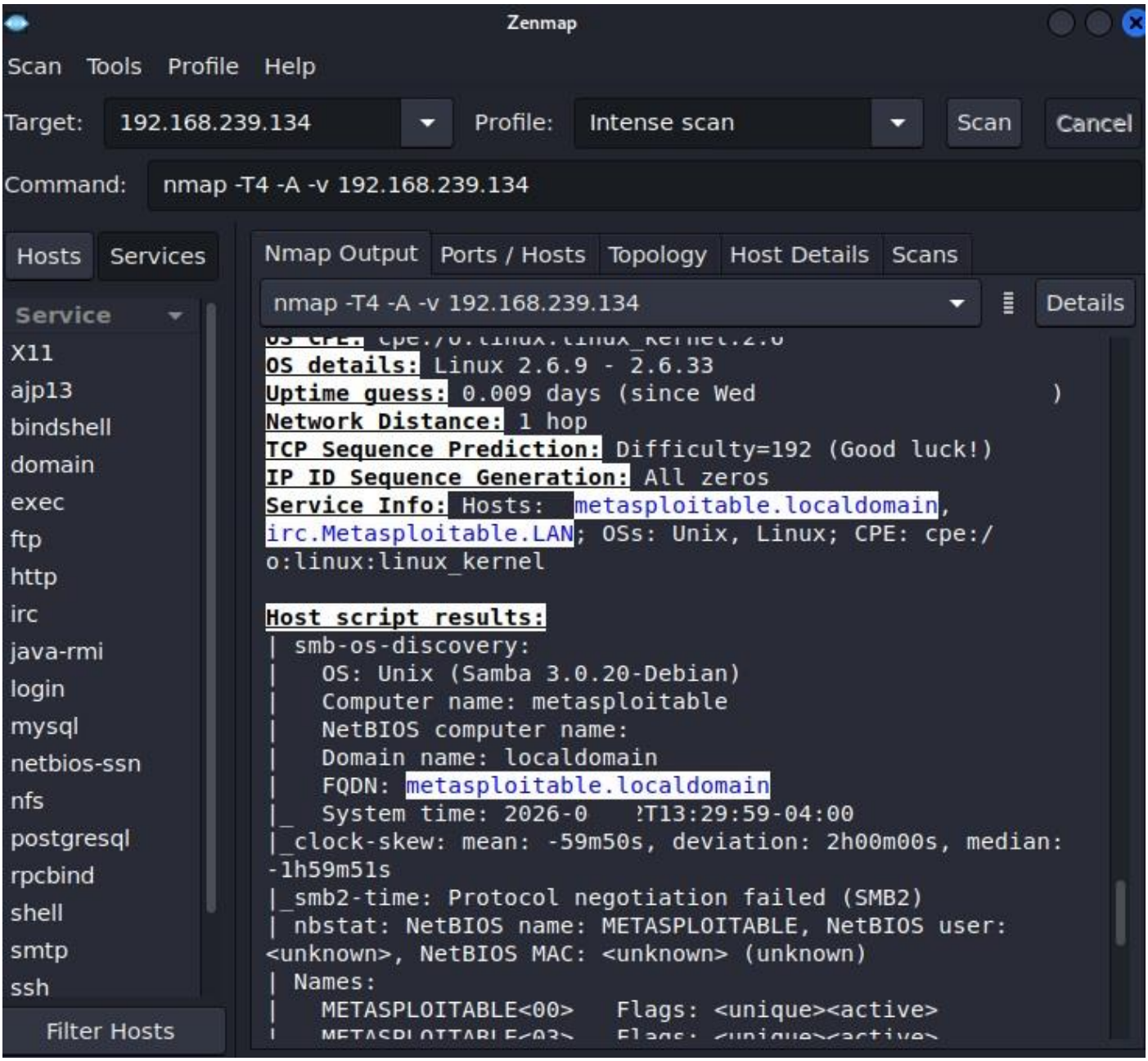
Ces services représentent des points d'entrée potentiels dans un contexte de sécurité.

Scan avec Zenmap (interface graphique)

En complément de la ligne de commande, l'outil Zenmap a été utilisé.

Zenmap est l'interface graphique officielle de Nmap, permettant de visualiser les résultats de scan de manière plus lisible.

Image 7 : Résultat graphique du scan Zenmap



Analyse des résultats

L'analyse des résultats obtenus avec Nmap et Zenmap montre que la machine Metasploitable 2 expose de nombreux services réseau.

Dans un contexte réel, cette configuration représenterait une surface d'attaque importante.

Points de vulnérabilité observés

- Multiples services ouverts inutilement
- Absence de filtrage réseau
- Services anciens et potentiellement vulnérables

Cette étape permet de comprendre l'importance de : la réduction des services exposés, la sécurisation des ports réseau, la mise en place de pare-feu et de filtrage.

Cette phase d'audit a permis de :
identifier les machines du réseau, analyser les ports ouverts sur la machine cible, utiliser des outils professionnels d'audit (Nmap et Zenmap), comprendre les risques liés à une mauvaise configuration système.

Conclusion

Ce TP avait pour objectif de mettre en place un environnement de test permettant de réaliser un audit de sécurité dans un cadre totalement isolé et contrôlé.

Grâce à l'utilisation de VMware Workstation, il a été possible de simuler un réseau composé de deux machines virtuelles :

- une machine d'audit (Kali Linux),
- une machine cible volontairement vulnérable (Metasploitable 2).

L'analyse du réseau a permis d'identifier les machines actives ainsi que les services exposés. L'utilisation des outils Nmap et Zenmap a mis en évidence plusieurs ports ouverts et services potentiellement sensibles.

Résultats obtenus

L'audit a permis de constater que la machine cible présente : de nombreux services réseau actifs, une surface d'attaque importante, une absence de filtrage des ports.

Ces résultats illustrent l'importance d'une bonne configuration des systèmes et de la réduction des services exposés.

Ce TP permet de comprendre l'intérêt d'un audit de sécurité dans un environnement informatique.

Il met en évidence que même dans un environnement contrôlé, une mauvaise configuration peut exposer un système à de nombreux risques.

Cette approche permet de développer une démarche professionnelle orientée sécurité, essentielle dans le domaine des infrastructures systèmes et réseaux.

ANNEXES

Commandes utilisées

Découverte réseau

- netdiscover
- arp-scan -l

Scan Nmap

- nmap -sS -sV 192.168.xxx.xxx