المدرسة العليا للتكنولوجيا - الداخلة
ⵜⵉⵙⵙⵏ ⵜⴰⵏⴰⵡⴰⵢⵜ ⵏ ⵜⵙⵔⵉⵜⵜ - ⴰⴷⴰⵅⵓ
ÉCOLE SUPÉRIEURE DE TECHNOLOGIE - DAKHLA

Rapport du TP

Sécurité Informatique

Installation et exploration de Kali Linux.

YAOGO Lucien | CIA : sécurité Informatique | 09/03/2026

Pr : Samya BOUHADDOUR

Table des matières

Important :

Les commandes et outils mentionnés dans ce document (Nmap, Metasploit, SET Toolkit, arpspoof) sont extrêmement puissants et ne doivent être utilisés que dans un cadre éducatif, sur des environnements de test isolés ou avec l'autorisation explicite du propriétaire du système cible. L'utilisation de ces techniques sur des réseaux tiers sans autorisation est illégale et passible de poursuites judiciaires.

Objectif

L'objectif principal de ce laboratoire est de se familiariser avec l'environnement Kali Linux et de comprendre les phases d'un test d'intrusion. Plus spécifiquement, le TP vise à :

- Installer et configurer un environnement de virtualisation (VirtualBox) pour exécuter Kali Linux.
- Analyser un réseau à l'aide de l'outil **Nmap** pour identifier les hôtes, les ports et les services ouverts.
- Simuler des attaques d'ingénierie sociale (phishing) avec **SET Toolkit**.
- Tester la robustesse des authentifications (SSH, FTP) via des attaques par dictionnaire ou force brute.
- Comprendre et réaliser une attaque **Man in the Middle (MiTM)** par empoisonnement ARP pour intercepter du trafic en clair.

Introduction

Ce rapport présente la mise en place d'un laboratoire de cybersécurité utilisant la distribution **Kali Linux**. L'étude commence par la configuration technique de l'environnement virtuel avant d'explorer les outils de référence pré-intégrés pour l'audit de sécurité. À travers différents scénarios (scan réseau, ingénierie sociale, brute force et interception de trafic), le document expose les méthodologies employées par les professionnels du pentesting pour identifier et exploiter des vulnérabilités système et réseau.

LAB1

1. Installation et exploration de Kali Linux

1.1 Installation de l'hyperviseur

Pour réaliser ce laboratoire, nous avons installé un environnement de virtualisation afin d'exécuter Kali Linux.

Deux solutions sont possibles :

- **VirtualBox**
- **VMware Workstation Player**

Dans ce TP, **VirtualBox** a été utilisé.

Étapes réalisées

1. Télécharger VirtualBox depuis le site officiel.
2. Installer le logiciel sur la machine hôte.
3. Créer une nouvelle machine virtuelle.

Configuration de la VM :

- RAM : 4 GB
- CPU : 2
- Stockage : 40 GB
- Mode réseau : **NAT**

1.2 Installation de Kali Linux

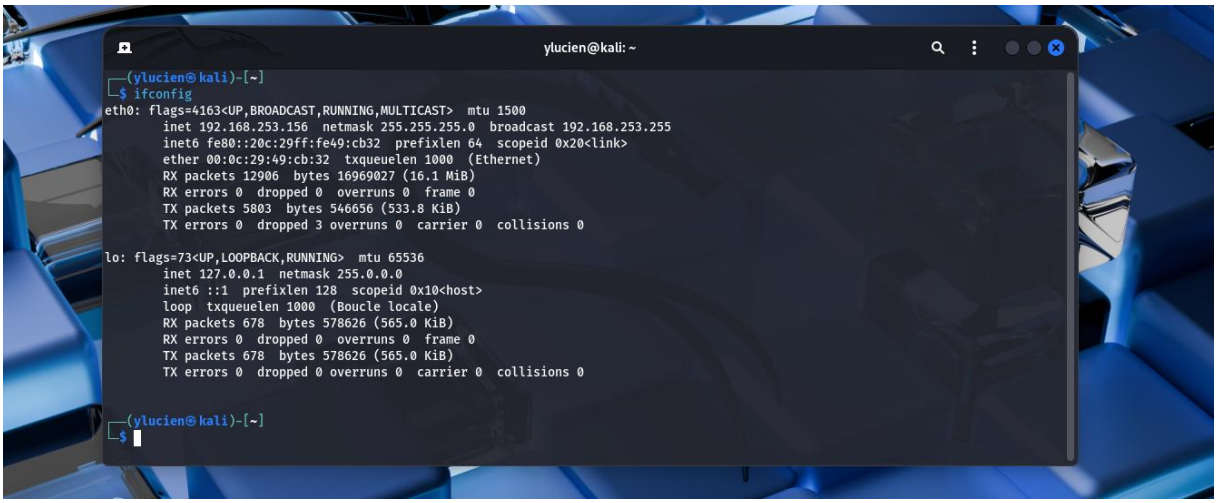
L'installation de Kali Linux a été réalisée à partir d'une **image ISO** téléchargée sur le site officiel :

https://www.kali.org/downloads/

Étapes

1. Création d'une nouvelle machine virtuelle.
2. Sélection de l'image ISO de Kali Linux.
3. Installation du système.
4. Configuration du compte utilisateur.

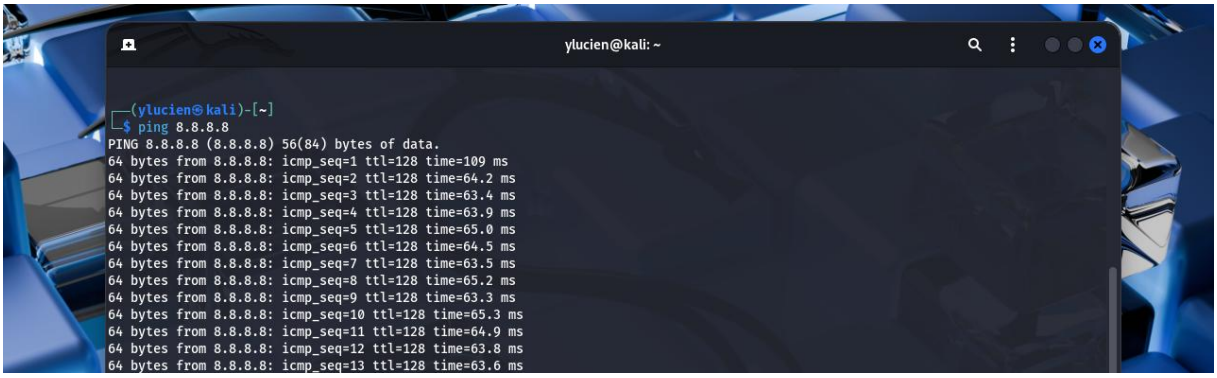
Après installation, la machine Kali Linux a été démarrée avec succès.



1.3 Vérification de la connexion Internet

La connectivité réseau a été testée à l'aide de la commande suivante :

ping 8.8.8.8



Résultat :
La machine virtuelle a reçu des réponses, ce qui confirme que la connexion Internet fonctionne correctement.

1.4 Exploration des outils de Kali Linux

Kali Linux contient de nombreux outils utilisés dans les tests de sécurité.

Analyse et Scan (Réseau Web)

- Nmap (Scan réseau) : C'est l'outil de référence pour la découverte d'hôtes et l'énumération de services sur un réseau

Ces outils permettent de réaliser différentes phases d'un **test d'intrusion**.

- Niko (Web Scan) : Un scanner spécialisé pour la détection de vulnérabilités web
- Wireshark (Analyse réseau) : Un analyseur de protocole utilisé pour **l'inspection détaillée du trafic** de paquets en temps réel, permettant de comprendre ce qui circule sur le réseau.

Attaque et exploitation Web

- Burp Suite (Web Sécurity) : Une plateforme intégrée pour l'analyse et l'interception du trafic HHTP.
- SQLMap (Web Attack) : Un outil automatisé dédié à la détection et à l'exploitation d'injection SQL.

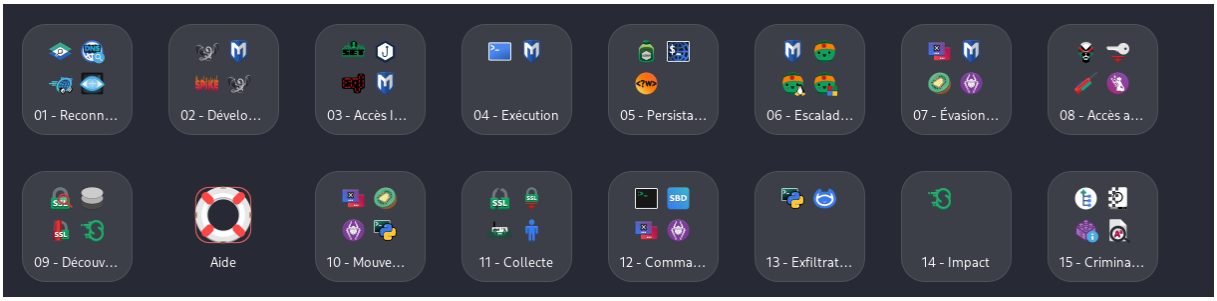
Exploitation de Système et Ingénierie Sociale

- Metasploit (Exploitation) : Un framework puissant utilisé pour l'exploitation de vulnérabilités.
- SET Toolkit (Sociale Engineering) : Un framework conçu pour mener des attaques contre le facteur humain.

Gestion de mot de passe

- Hydra (Bruteforce) : Un outil spécialisé dans les attaques par dictionnaire ou force brute contre divers protocoles de connexion pour tester la robustesse des mots de passe.
- Join the Ripper (Password Cracking) : Un utilitaire de cassage de hash utilisé pour retrouver des mots de passe à partir de fichiers de hachage récupérés lors d'une intrusion.
- Aircrack-ng (Wifi Securitty) : Une suite complete d'outils pour l'audit des réseaux Wifi, permettant de tester la sécurité des clés de chifrement (WEP, WPA/WPA2).

Ces outils sont souvent pé-intégrés dans des distributions comme Kali Linux pour faciliter les tests de pénétration et les audits de sécurité avancés.



2. Analyse du réseau avec Nmap

2.1 Présentation de Nmap

Nmap (Network Mapper) est un outil utilisé pour :

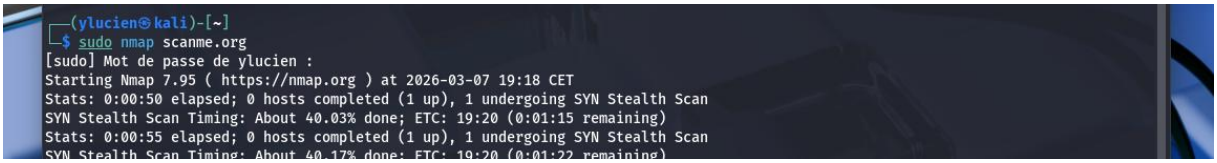
- Découvrir les hôtes sur un réseau
- Scanner les ports ouverts
- Identifier les services
- Détecter le système d'exploitation

Il est largement utilisé en **cybersécurité et pentesting**.

2.2 Scan de base

Commande utilisée :

nmap scanme.nmap.org



Cette commande permet de scanner l'hôte cible afin d'identifier les ports ouverts.

Exemple de résultats

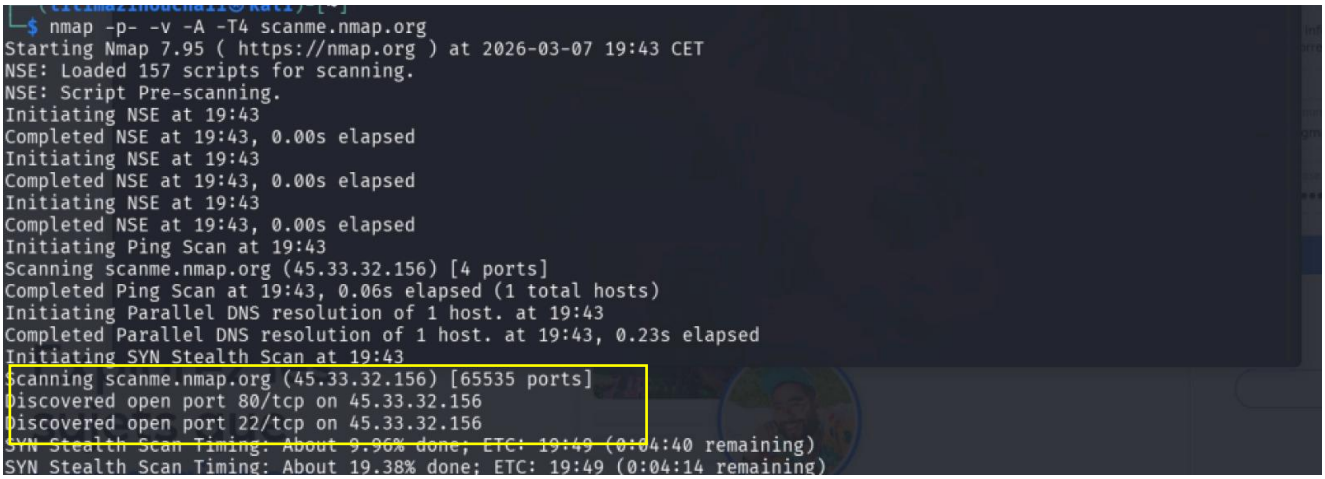
Port	Service
22	SSH
80	HTTP
9929	nping-echo

Ces ports indiquent que certains services sont accessibles sur la machine cible.

2.3 Scan avancé

Commande utilisée :

nmap -p0- -v -A -T4 scanme.nmap.org



Explication des paramètres

-p0- : Scanner **tous les ports (1 à 65535)**.

-v : Mode **verbose** qui affiche plus d'informations pendant le scan.

-A : Active plusieurs fonctionnalités avancées :

- Détection du système d'exploitation
- Détection de version des services
- Scripts NSE
- Traceroute

-T4 : Augmente la **vitesse du scan** tout en gardant une bonne fiabilité.

2.4 Résultat du scan

À partir des résultats obtenus, Nmap peut également suggérer le **système d'exploitation probable** de la machine cible.

Exemple :

Linux / Unix based system

Cela permet aux pentesters de comprendre la configuration du système afin d'identifier d'éventuelles vulnérabilités.

3. Attaque d'ingénierie sociale avec SET Toolkit

3.1 Présentation de SET

Le **Social Engineer Toolkit (SET)** est un framework utilisé pour simuler des attaques d'ingénierie sociale.

Il permet de tester la sensibilisation des utilisateurs face aux attaques de phishing.

Fonctionnalités principales :

Module	Description
Spear Phishing	Email ciblé
Website Attack	Création de faux site
Mass Mailer	Envoi massif d'emails
Wireless AP	Faux point d'accès WiFi
QR Code Attack	Phishing via QR code

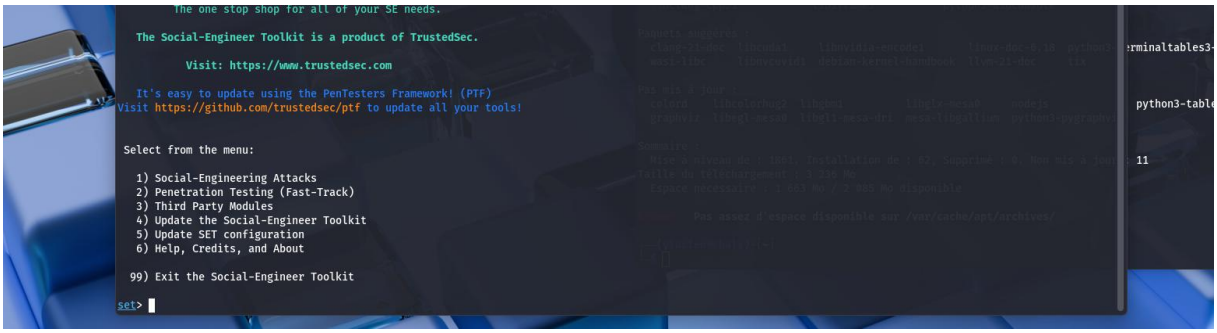
3.2 Clonage d'un site web

SET permet de cloner un site web pour simuler une attaque de phishing.

Étapes

1. *Lancer l'outil :*

Setoolkit



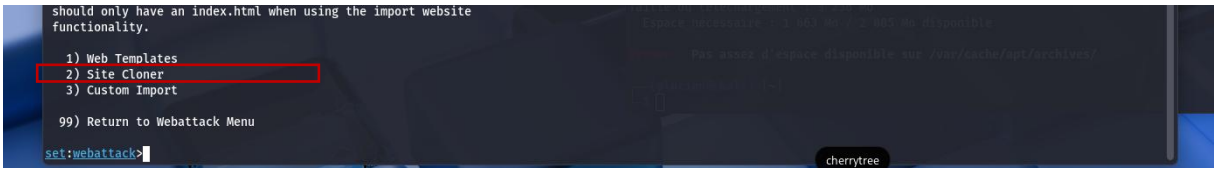
2. *Choisir les options :*

1) Social Engineering Attack (+ la touche entre)

2) Website Attack Vectors (+ la touche entre)

3) Credential Harvester Attack Method (+ la touche entre)

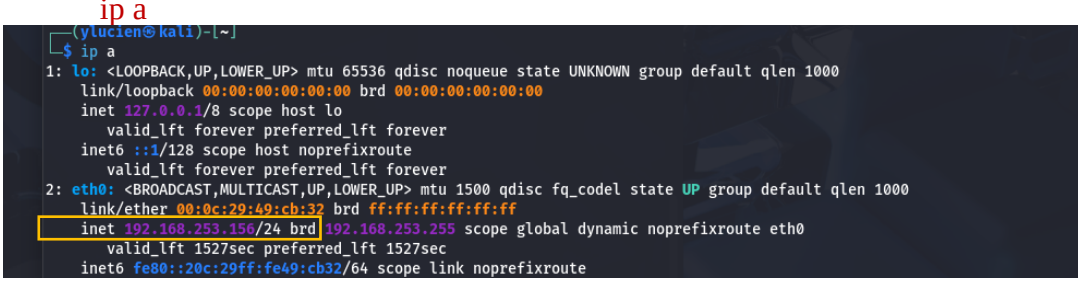
2) Site Cloner



3. Entrer :

- L'adresse IP de la machine Kali

  ifconfig
  ip a

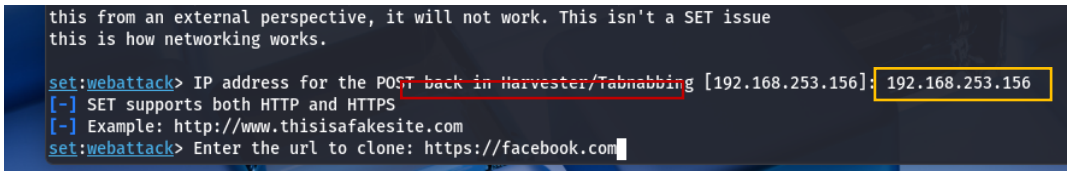


- L'URL du site à cloner

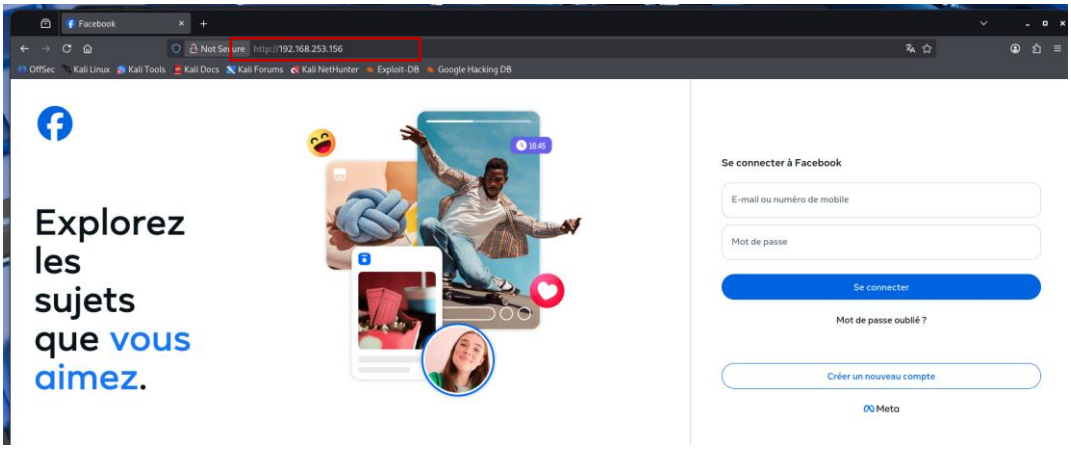
Ici :

IP Kali : 192.168.253.156

URL : https://facebook.com



SET crée alors une **copie du site web**.



Lorsque la victime entre ses identifiants, ceux-ci sont affichés dans le terminal.

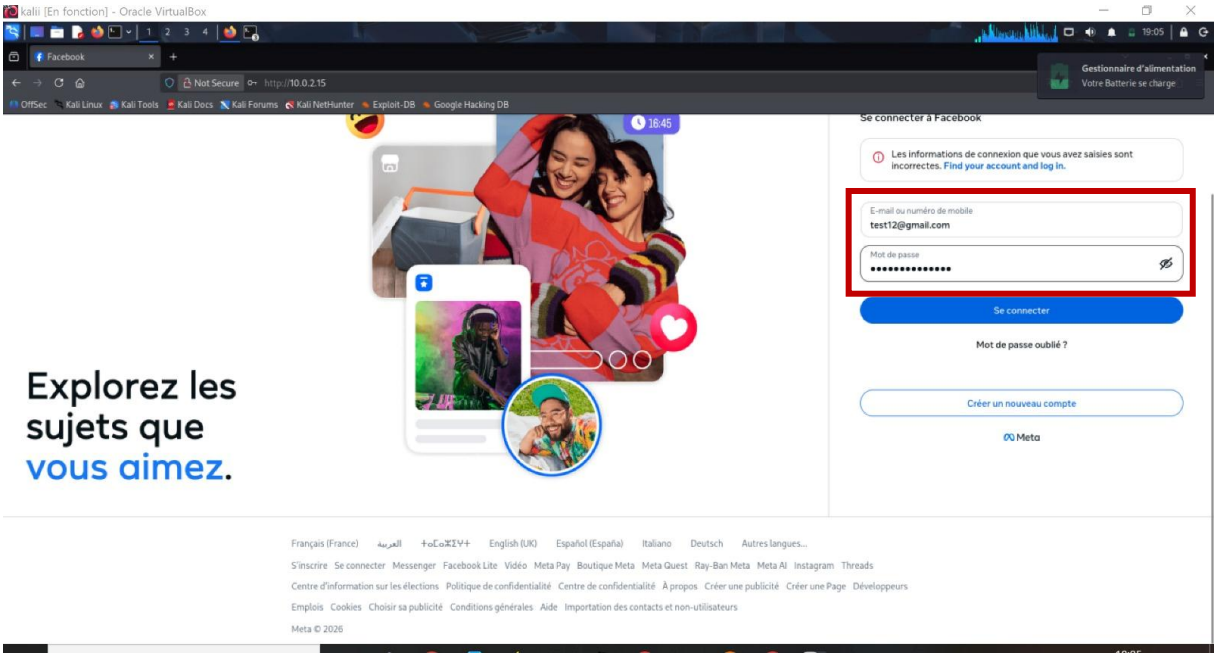
3.3 Information Gathering via moteurs de recherche et réseaux sociaux

L'ingénierie sociale commence souvent par une phase appelée **OSINT (Open Source Intelligence)**.

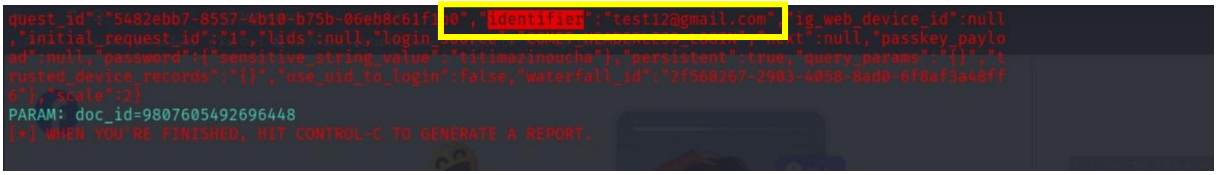
Elle consiste à collecter des informations publiques sur une cible.

Sources possibles :

- LinkedIn
- Facebook



Récupération des identifiant avec Kali



- Site web de l’entreprise
- Google

Exemples d’informations collectées :

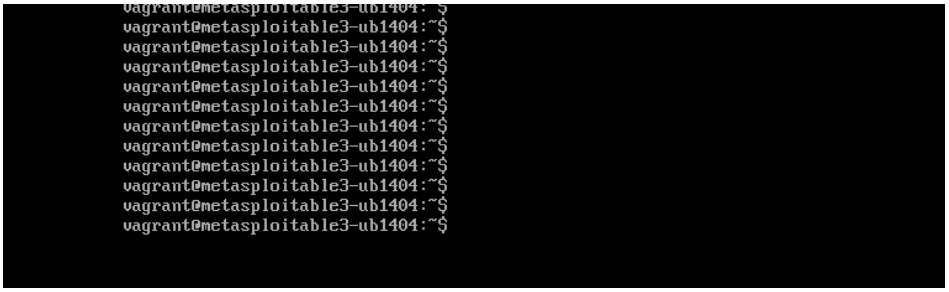
- Nom
- Poste
- Adresse email professionnelle
- Département
- Technologies utilisées par l’entreprise

Ces informations peuvent ensuite être utilisées pour simuler une attaque de **spear-phishing**.

Dans le cadre de ce TP, un **profil fictif d’employé** peut être utilisé afin de démontrer la méthode de collecte d’informations.

Lab 2

Network Scanning & SSH Brute Force



1. Objectif du laboratoire

L'objectif de ce laboratoire est de :

- Analyser un réseau à l'aide de **Nmap**
- Identifier les ports et services ouverts
- tester l'authentification SSH avec **Metasploit**
- comprendre le fonctionnement d'une **attaque par dictionnaire (Brute Force)**

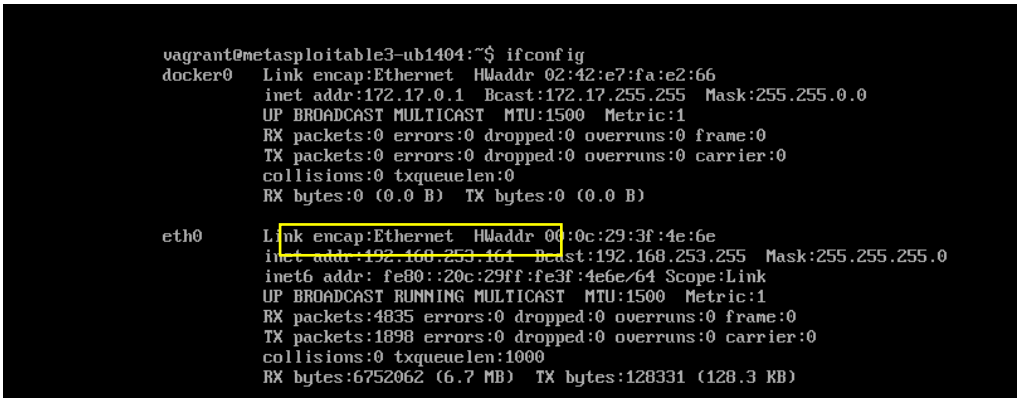
La machine cible utilisée dans ce laboratoire est **Metasploitable 3**, une machine volontairement vulnérable utilisée pour l'apprentissage du pentesting.

2. Scan du réseau avec Nmap

2.1 Identification de la machine cible

La première étape consiste à identifier l'adresse IP de la machine Metasploitable.

Dans notre laboratoire, l'adresse IP détectée est :



2.2 Scan des ports ouverts

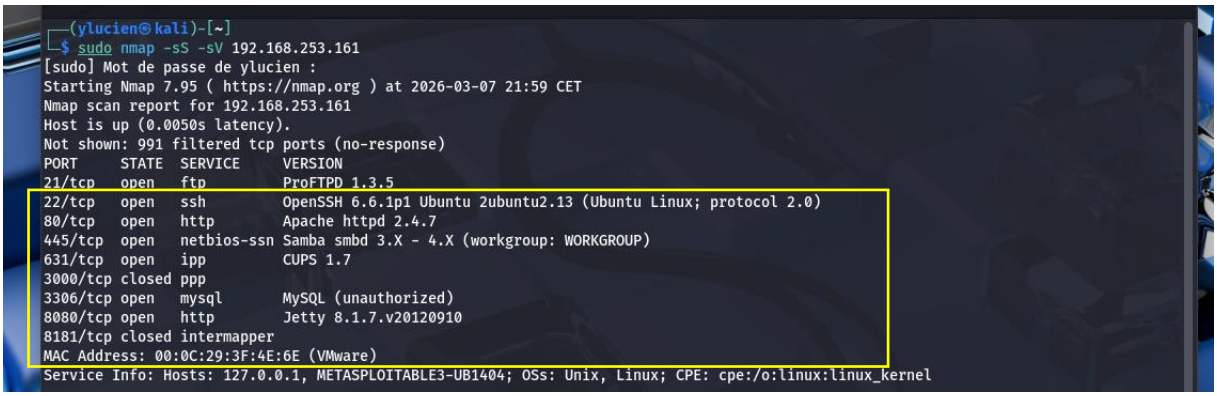
Nous utilisons l'outil **Nmap** afin d'identifier les ports ouverts et les services actifs sur la machine cible.

Commande utilisée :

nmap -sS -sV 192.168.253.161

Explication des paramètres

Option	Description
-sS	Scan TCP SYN (stealth scan)
-sV	Détection de la version des services
IP	Adresse de la machine cible



2.3 Résultats obtenus

Le scan révèle plusieurs ports ouverts, par exemple :

Port	Service
22	SSH
80	HTTP
445	SMB
3306	MySQL

Le port **22 (SSH)** est particulièrement intéressant car il permet une connexion distante au système.

3. Attaque SSH avec Metasploit

3.1 Lancement de Metasploit

Metasploit est un framework utilisé pour tester la sécurité des systèmes et exploiter des vulnérabilités.

Commande pour démarrer Metasploit :

msfconsole

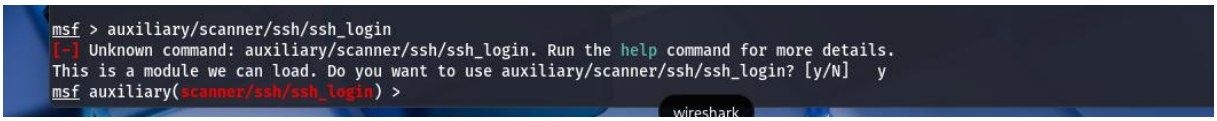
3.2 Sélection du module SSH

Nous utilisons le module suivant :

auxiliary/scanner/ssh/ssh_login

Commande :

use auxiliary/scanner/ssh/ssh_login



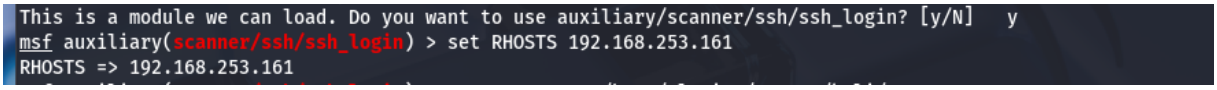
Ce module permet de tester plusieurs combinaisons **username / password** afin d'accéder au service SSH.

3.3 Configuration du module

Nous configurons les paramètres suivants :

Définir la cible

set RHOSTS 192.168.253.161

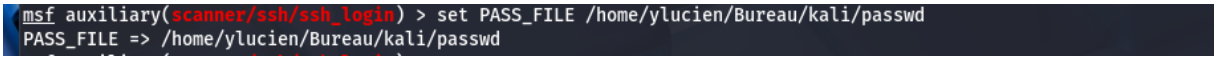


Définir le fichier contenant les usernames

set USER_FILE /home/ylucien/Bureau/kali/username

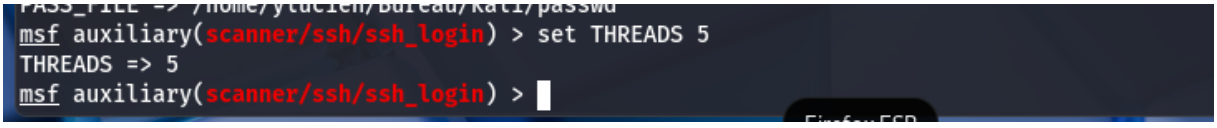
Définir le fichier contenant les mots de passe

set PASS_FILE /home/ylucien/Bureau/kali/passwd



Définir le nombre de threads

set THREADS 5

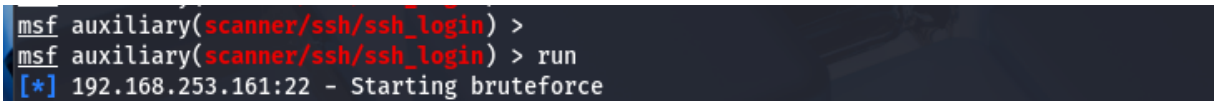


Les **threads** permettent d'accélérer l'attaque en testant plusieurs combinaisons en parallèle.

3.4 Lancement de l'attaque

Commande :

run



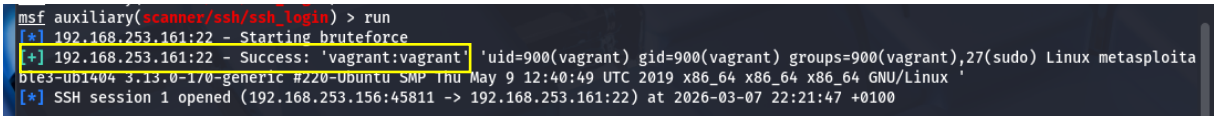
Metasploit va tester les combinaisons contenues dans les fichiers :

username : Pour stocker les noms d'utilisateur

passwd : Pour stocker les mots de passe

3.5 Résultat possible

Si une combinaison valide est trouvée, Metasploit affiche :



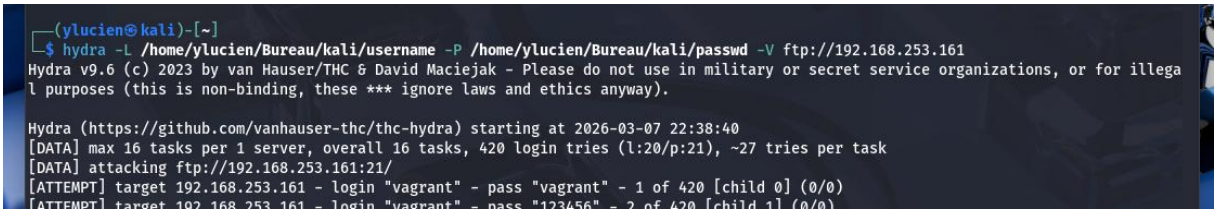
[+] 192.168.253.161:22 - Success: username 'vagrant' password 'vagrant'

Cela signifie que l'authentification SSH a réussi.

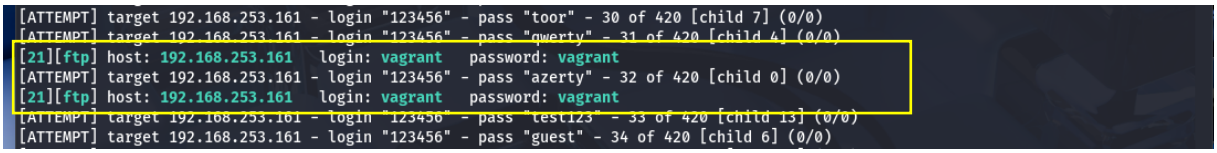
3.6 Sélection du module FTP

Nous utilisons le module suivant :

Hydra pour le test avec ftp pour retrouver les identifiant de la machine cible.



Résultat possible :



4. Analyse de l'attaque

L'attaque utilisée dans ce laboratoire est une **attaque par dictionnaire**.

Principe :

1. L'attaquant possède une liste de **noms d'utilisateurs (username)**.
2. Il possède une liste de **mots de passe (passwd)**.
3. L'outil teste toutes les combinaisons possibles.

Si le mot de passe est faible, l'accès peut être obtenu rapidement.

5. Mesures de sécurité

Pour se protéger contre ce type d’attaque, plusieurs mesures peuvent être mises en place :

- utiliser des **mots de passe forts**
- limiter le nombre de tentatives de connexion
- utiliser **Fail2Ban**
- désactiver l’authentification par mot de passe
- utiliser **authentification par clé SSH**

Réalisation d’une attaque Man in the Middle (MiTM) et interception d’une session FTP

Dans cette partie du laboratoire, nous exploitons la vulnérabilité du protocole **ARP** afin de réaliser une attaque **Man in the Middle (MiTM)**.

L’objectif est de se positionner entre le **client FTP** et le **serveur FTP** afin d’intercepter les informations échangées, notamment les **identifiants transmis en clair**.

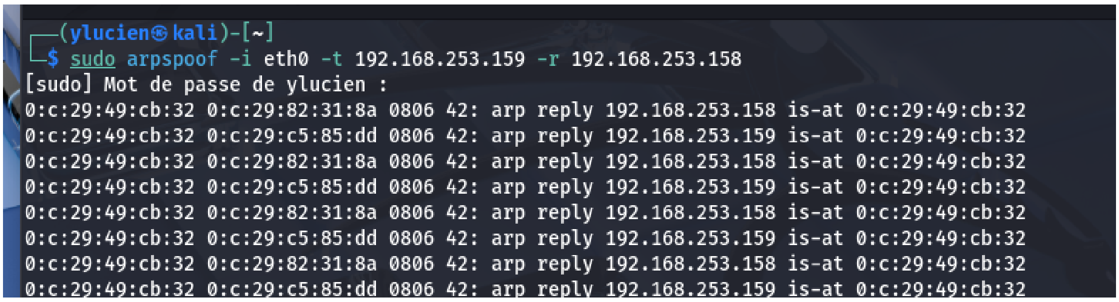
L’attaque se déroule en plusieurs étapes.

1. Mise en place de l’attaque ARP Poisoning

Sur la machine **Kali Linux (attaquant)**, nous utilisons l’outil **arpspoof** afin d’envoyer de fausses réponses ARP au client et au serveur.

Commande utilisée :

sudo arpspoof -i eth0 -t 192.168.253.159 -r 192.168.253.158



Cette commande permet à Kali d’envoyer des **réponses ARP falsifiées** afin de faire croire :

- au **client** que Kali est le **serveur FTP**
- au **serveur** que Kali est le **client FTP**

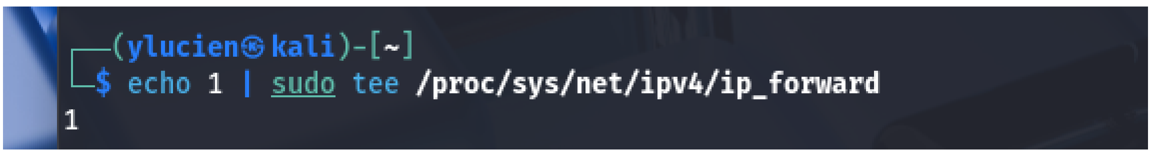
Ainsi, tout le trafic entre les deux machines passe par la machine attaquante.

2. Activation du forwarding des paquets

Pour que la communication entre le client et le serveur continue de fonctionner, nous devons activer le **IP forwarding** sur Kali.

Commande utilisée :

echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward



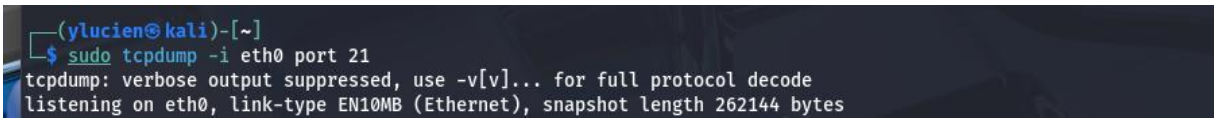
Cette commande permet à Kali de **transmettre les paquets interceptés** entre les deux machines.

3. Capture du trafic réseau

Pour analyser les communications interceptées, nous utilisons un outil d'analyse réseau comme **Wireshark** ou **tcpdump**.

Avec tcpdump :

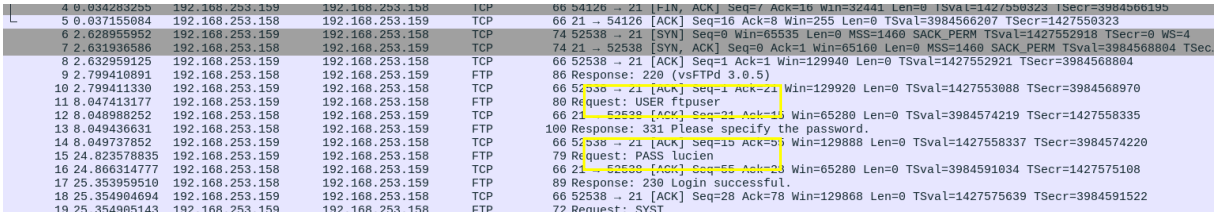
sudo tcpdump -i eth0 port 21



Cette commande permet de capturer uniquement le **trafic FTP**.

Avec Wireshark, nous pouvons appliquer le filtre :

ftp>192.168.253.158



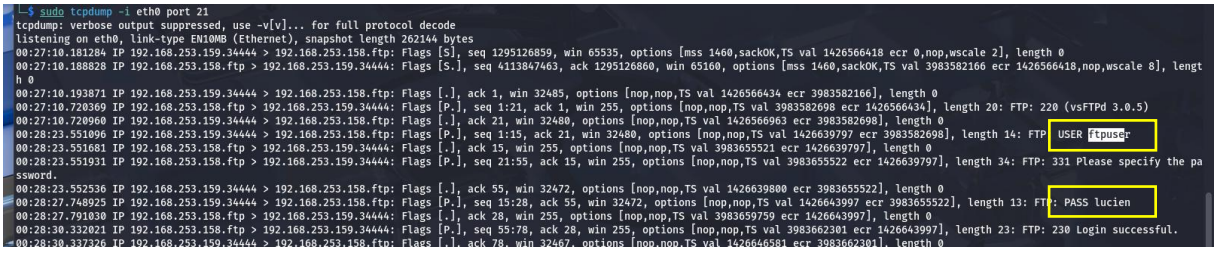
Lors de la connexion avec Wireshark, l'utilisateur saisit :

- son **nom d'utilisateur (ftpuser)**
- son **mot de passe (lucien)**

4. Interception de la session FTP

Depuis la machine **Ubuntu Client**, nous lançons une connexion FTP vers le serveur :

ftp>192.168.253.158



Lors de la connexion, l'utilisateur saisit :

- son **nom d'utilisateur (ftpuser)**
- son **mot de passe (lucien)**

Ces informations sont envoyées **en clair** dans le protocole FTP.

Dans Wireshark ou tcpdump, nous pouvons observer les paquets suivants :

Le nom d’utilisateur : ftpuser

Le mot de passe : lucien

Cela montre que les identifiants FTP peut être **facilement interceptés** par un attaquant positionné au milieu de la communication.

Conclusion

Le laboratoire démontre que l'utilisation d'outils automatisés permet d'identifier rapidement des faiblesses critiques, telles que des ports inutilement ouverts ou des services utilisant des protocoles non sécurisés (comme le FTP transmettant des identifiants en clair). Les tests d'attaques par dictionnaire soulignent l'importance vitale de politiques de mots de passe robustes. Pour contrer ces menaces, le rapport préconise la mise en œuvre de mesures de défense telles que l'utilisation de clés SSH, l'activation de Fail2Ban et la limitation des tentatives de connexion.