# Lab 1 : Préparation de l’environnement de travail et analyse des vulnérabilités

**4ERP-Bi 7**

**Ahmed Abidhiaf**

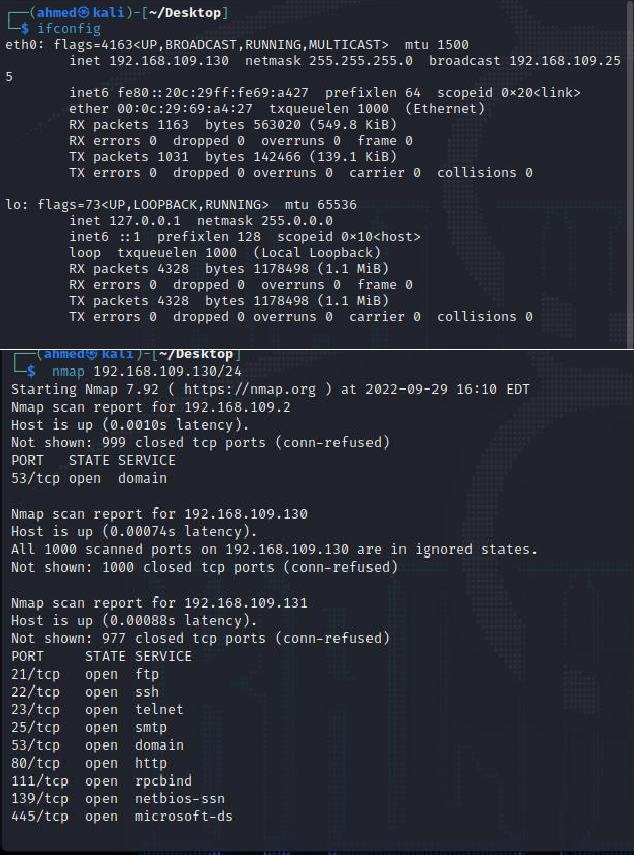
**Fares Bkklouti**

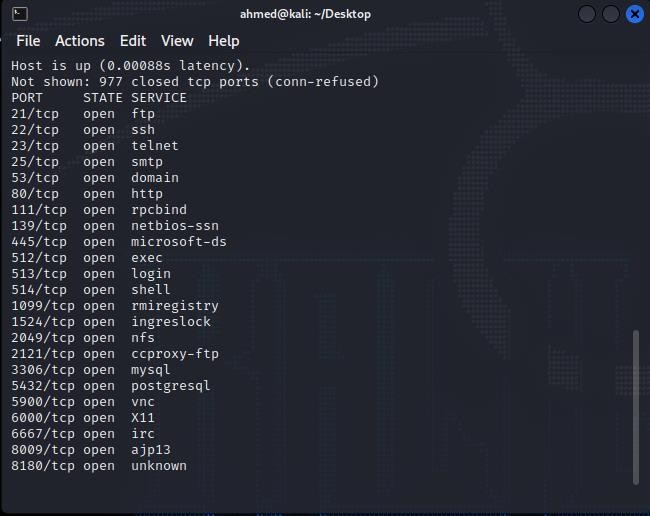
**Sinda chamakh**

**Yassine Barkallah**

# Partie 1 : Scan Nmap:

1. Exécuter une analyse rapide des machines. Utiliser la commande « Ifconfig » pour avoir l’adresse IP et la masque du réseau.

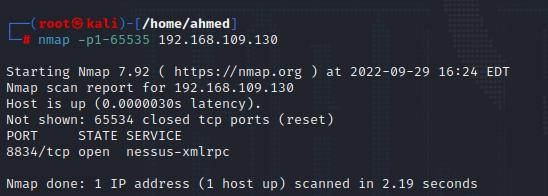




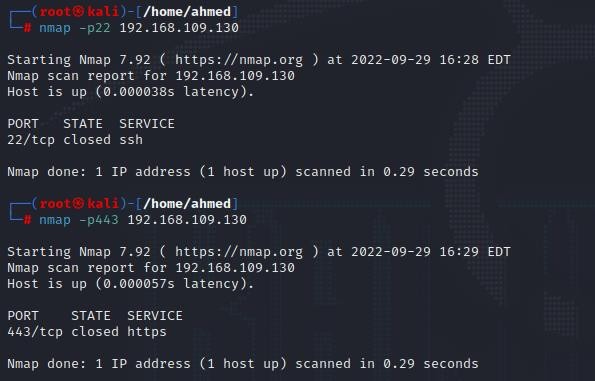
1. Identifier les systèmes d’exploitation d’une machine cible.



1. Scan tous les ports d’une machine cible.



1. Vérifier l’état des ports 22 et 443 sur les machines du réseau.

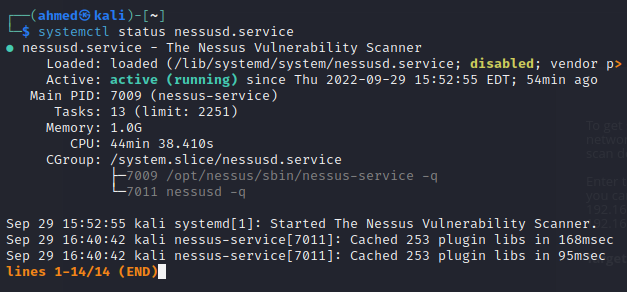


# Partie 2 : Nessus Vulnerability Scanner sur Kali Linux

1. Démarrer le service requis pour faire fonctionner Nessus vulnerability scanner

C:\Users\R I B\Downloads\309892797_465875062143662_2692226354734626796_n.png

1. Confirmer que nessusd est démarré et en cours dexécution



1. Visitez votre interface Web Nessus sur l&#39;adresse IP de votre serveur, le port de nom D hôte 8834 pour terminer l installation et lactivation de Nessus.

C:\Users\R I B\Downloads\309429198_671378864042793_7137138089542498344_n.png

1. faire un login sur Nessus.
2. La page par défaut de Nessus lors de la connexion devrait ressembler à celle ci-

dessous :

