Projet-SE :

Mise en place d'un dispositif permettant d’analyser un paquet.

Membres du groupe :

* MAIGA Abdel Nasser
* ABAYAZID Mohamed AbdoulKader

SOMMAIRE

INTRODUCTION

I. Présentation de l’environnement de travail

a) Environnement matériel

b) Environnement logiciel

II. Présentation du Projet

a) Présentation de la machine 1 : serveur

b) Présentation de la machine 2 : client

c) Présentation de la machine 3 : man of the middle

**INTRODUCTION :**

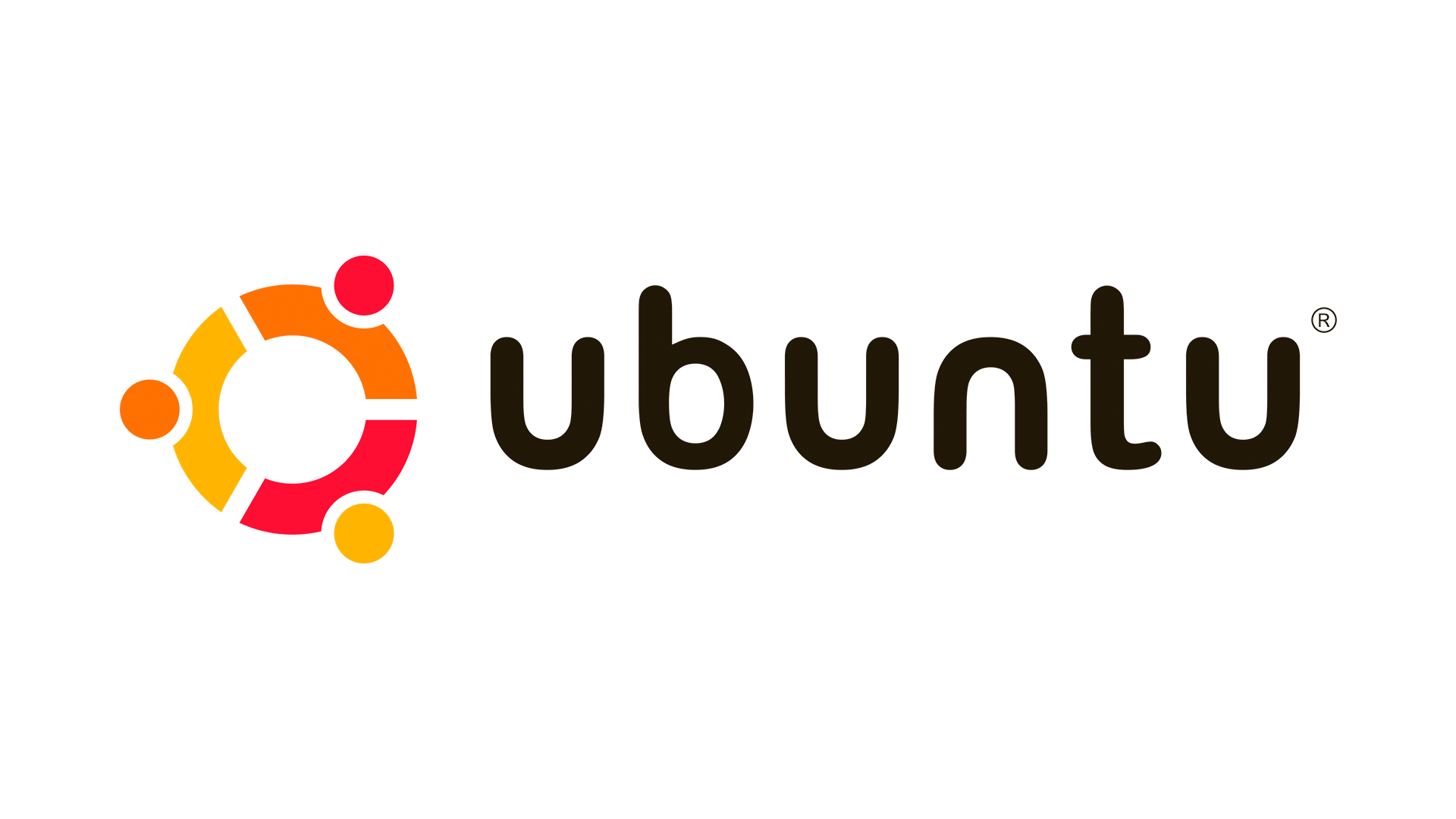
Pour comprendre les réseaux, il est important de savoir que la recherche et le développement se sont effectués en trois temps. Avant les années 1960, la question fondamentale était : << Comment est-il possible d’acheminer, de façon fiable et efficace, des débits le long d’un support de transmission ? >>. Les résultats ont inclus le développement de la théorie du signal. Aux environs des années 1965, l’intérêt s’est concentré sur la commutation de paquets et la question est devenue : << Comment est-il possible de transmettre des paquets, de façon efficace et fiable, sur un support de communication ?>>. Les résultats ont abouti au développement des techniques de communication par paquets et des réseaux locaux. Des années 1975 jusqu’à aujourd’hui, l’attention s’est portée sur les architectures de réseaux et sur la question : << Comment fournir des services de communication à travers une interconnexion de réseaux >>. Les résultats incluent les techniques d’interconnexion, les modèles de protocoles en couches, les datagrammes, les services de transport en mode connecté et le modèle client/serveur. Ce rapport se focalise sur la programmation d’applications basées sur le modèle client/serveur utilisant les protocoles TCP/IP Internet du D.A.R.P.A. (Défense Advanced Research Projets Agency). Un protocole est un ensemble de règles et de conventions nécessaires pour la communication entre ordinateurs. Comme ces protocoles sont complexes, ils sont découpés en plusieurs couches pour faciliter leurs implémentations. Chacune étant construite sur la précédente. Le nombre de couches, leur nom et leur fonction varie selon les réseaux. Cependant, dans chaque réseau, l’objet de chaque couche est d’offrir certains services aux couches plus hautes. La couche N d’une machine gère la conversation avec la couche N d’une autre machine en utilisant un protocole de niveau N. En réalité, aucune donnée n’est transférée directement de la couche N d’une machine à la couche N de l’autre machine mais chaque couche passe les données et le contrôle à la couche immédiatement inférieure, jusqu’à la plus basse. En dessous de la couche 1 se trouve le support physique qui véhicule réellement la communication. L’ensemble des couches et protocoles est appelé l’architecture du réseau.

1. **Présentation de l’environnement de travail :**
2. **Environnement matériel :**

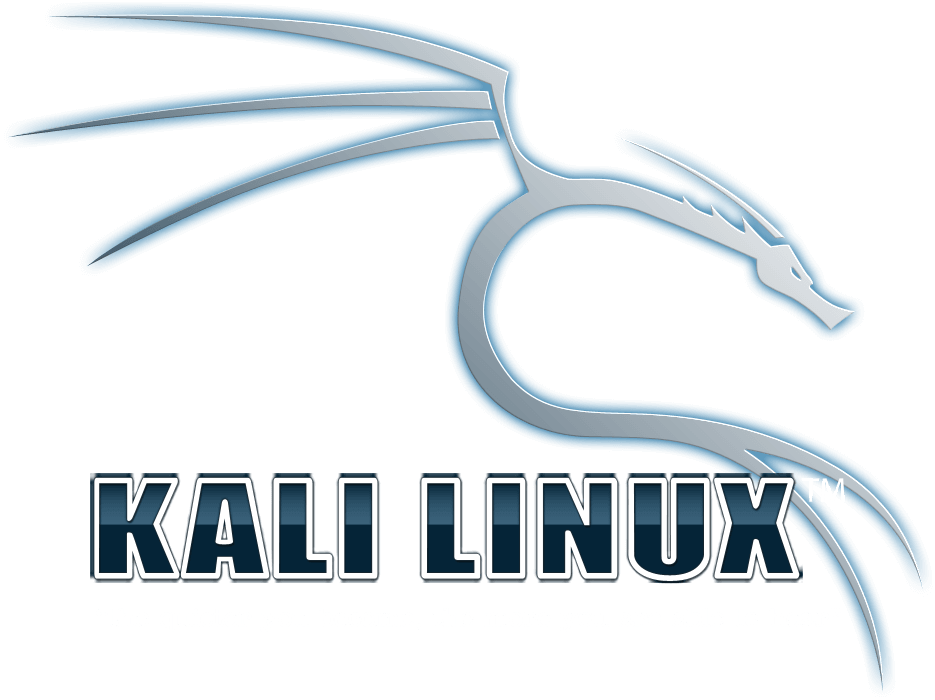
Comme station de développement, nous avons utilisé deux ordinateurs portables Lenovo. Il est équipé d’un processeur Intel Core i7 et de 16 Go de mémoire vive et d’une version 64 bits de Windows 10 Professional et trois (3) machines virtuelles avec des distributions LINUX(Ubuntu/Debian) :

* **Ubuntu** est un [système d’exploitation GNU/Linux](https://fr.wikipedia.org/wiki/Distribution_Linux) basé sur [Debian](https://fr.wikipedia.org/wiki/Debian). Il est développé, commercialisé et maintenu pour les [ordinateurs individuels (desktop)](https://fr.wikipedia.org/wiki/Ordinateur_personnel), les [serveurs (Server)](https://fr.wikipedia.org/wiki/Serveur_informatique) et les [objets connectés (Core)](https://fr.wikipedia.org/wiki/Internet_des_objets) par la société [Canonical](https://fr.wikipedia.org/wiki/Canonical).

Ubuntu est disponible en deux versions, une qui évolue tous les six mois, et une version [LTS](https://fr.wikipedia.org/wiki/Long-term_support), pour Long Term Support (« Support long terme ») qui évolue tous les deux ans. Ubuntu se définit comme « un système d'exploitation utilisé par des millions de PC à travers le monde et avec une interface « simple, intuitive, et sécurisée ». Elle est la distribution la plus utilisée pour accéder aux sites web d'après le site Alexa, et le système d'exploitation le plus utilisé pour les [serveurs informatiques](https://fr.wikipedia.org/wiki/Serveur_informatique).



* **Kali Linux** est une [distribution GNU/Linux](https://fr.wikipedia.org/wiki/Distribution_Linux) sortie le 13 mars 201[3](https://fr.wikipedia.org/wiki/Kali_Linux#cite_note-3), basée sur [Debian](https://fr.wikipedia.org/wiki/Debian). La distribution a pris la succession de [BackTrack](https://fr.wikipedia.org/wiki/BackTrack" \o "BackTrack) et est financée et maintenue à jour par [Offensive Security](https://en.wikipedia.org/wiki/Offensive_Security).



1. **Environnement logiciel :**

* Base de données **MySQL** : MySQL est un système de gestion de bases de données relationnelles. Il est distribué sous une double licence GPL et propriétaire.



* **IREDMAIL :** est une suite complète de messagerie open-source qui comprend un serveur de messagerie et un client webmail. Elle est conçue pour une utilisation en entreprise car elle prend en charge la gestion et la synchronisation des calendriers, la synchronisation des contacts ActiveSync, CalDav et CardDav, etc.



* **WIRESHARK :** est un analyseur de paquets libre et gratuit. Il est utilisé dans le dépannage et l’analyse de réseaux informatiques, le développement de protocoles, l’éducation et la rétro-ingénierie.



* **GIT :** est un logiciel de gestion de versions décentralisé. C'est un logiciel libre créé par Linus Torvalds, auteur du noyau Linux, et distribué selon les termes de la licence publique générale GNU version 2.

1. **Présentation du projet :**
2. **Présentation de la machine 1 : serveur**

Pour la première machine nous avons utilisé Ubuntu qui est un [système d’exploitation GNU/Linux](https://fr.wikipedia.org/wiki/Distribution_Linux) basé sur [Debian](https://fr.wikipedia.org/wiki/Debian)

-En premier lieu nous devons créer une machine virtuelle intitulé serveur et puis fixé l’adresse IP de la machine.

-Pour ce qui s’agit de la fixation j’ai passé par netplan et voilà le script :

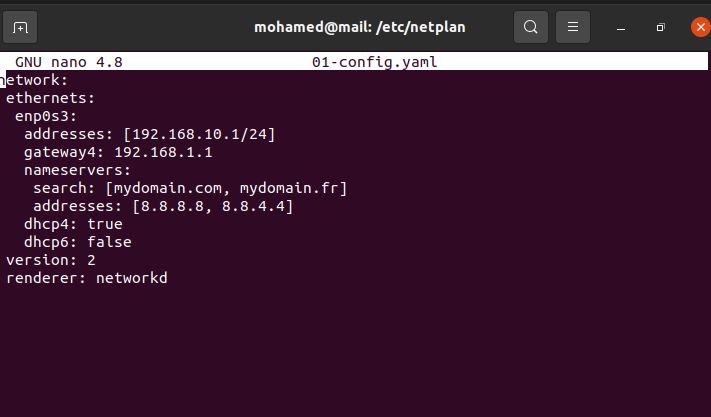
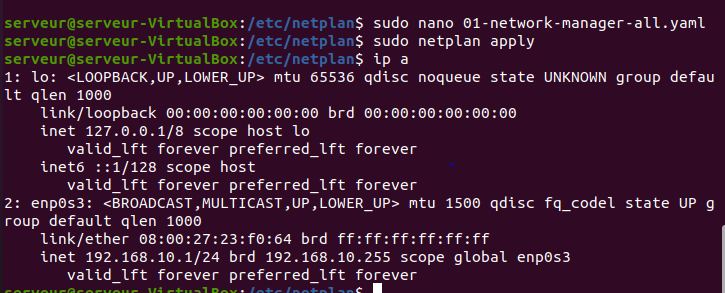


Figure 1:script pour la fixation d'adresse IP



-Configuration de DHCP

Pour la configuration de DHCP nous devons tout d’abord installer le paquet de DHCP, puis configurer le service DHCP (lui attribuer une plage d’adresse allons de 192.168.10.2 à 192.168.10.10)

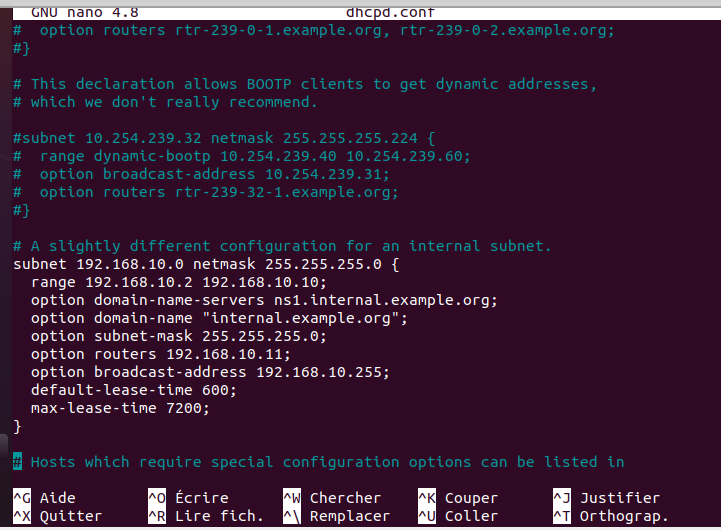


Figure 2:le fichier de configuration de DHCP

-Configuration du service DNS

Pour la mise en place du service DNS il faut tout d’abord installer le paque t de DNS, puis configurer le fichier named.conf.options et enfin configurer le fichier nommé named.conf

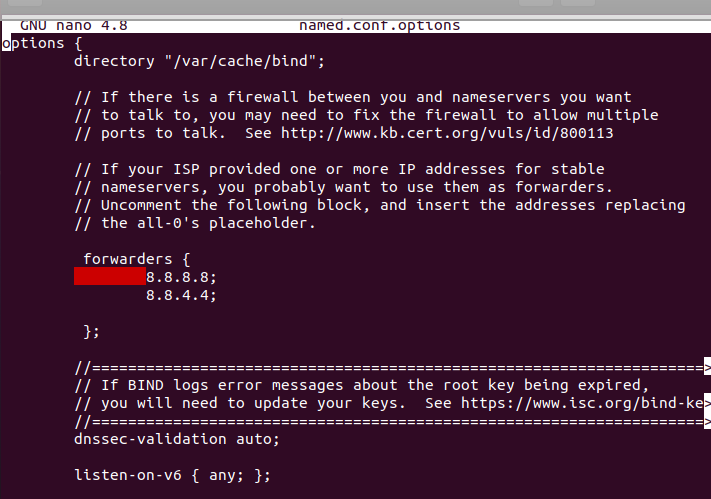


Figure 3: le fichier named.conf.options

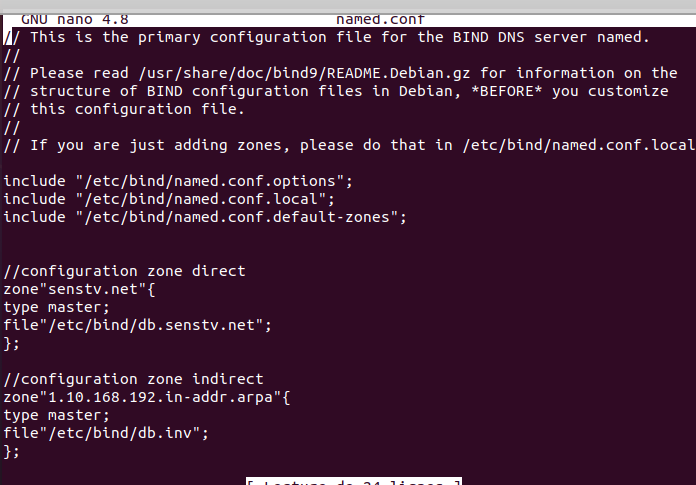
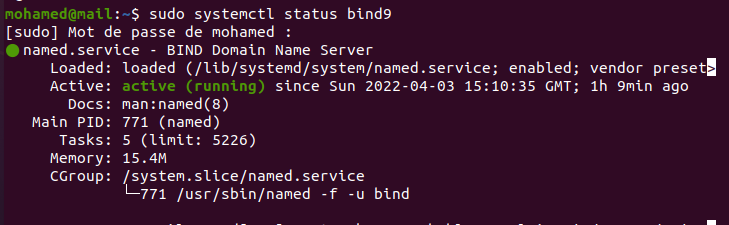


Figure 4:le fichier named.conf



-Les scripts d’installations de MYSQL et IREDMAIL

Dans cette partie nous avons mise en place deux script qui permettent d’installer et configurer les deux serveurs à savoir MYSQL et IREDMAIL (INSTALL\_MYSQL, INSTALL\_IREDMAIL\_DEPENDENCIES)

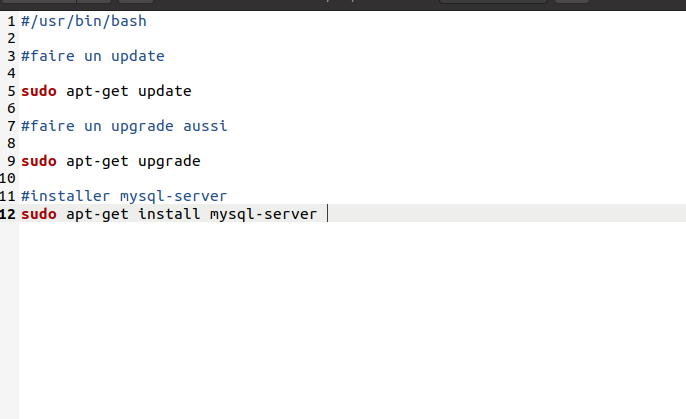


Figure 5:script d'installation de mysql

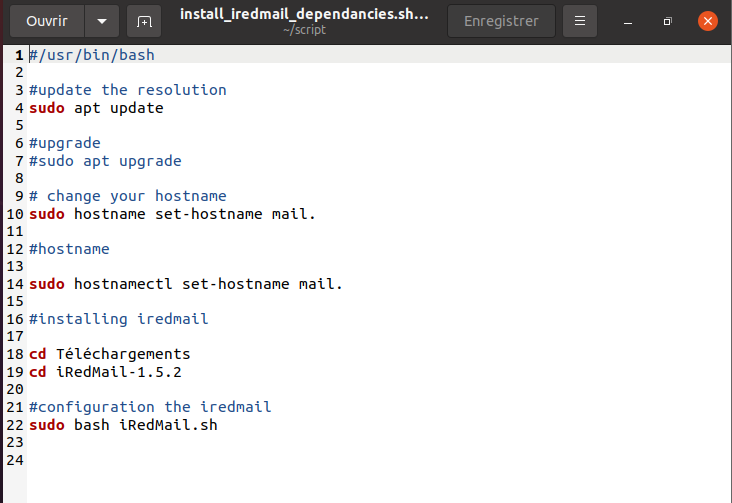
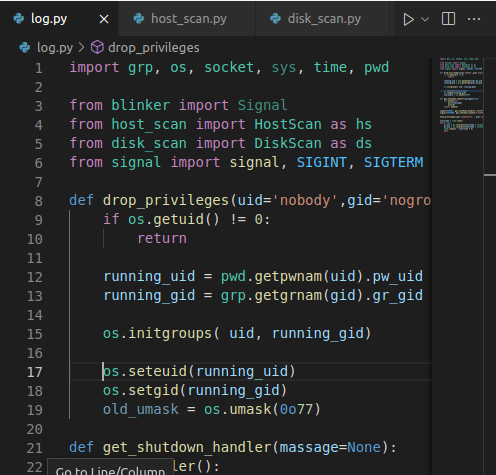


Figure 6:script d'installation iredmail

-Création d’une interface login

Dans cette partie nous allons coder (résultat sur console) une interface de login permettant à l’utilisateur de se connecter aux différents services du serveur.



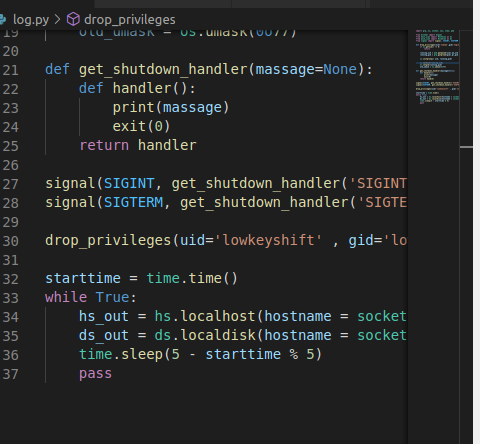
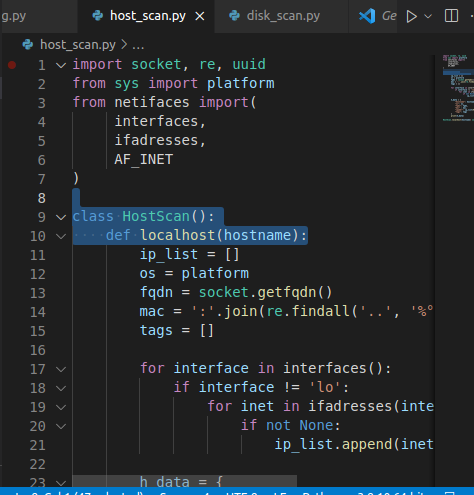


Figure 7:script de login



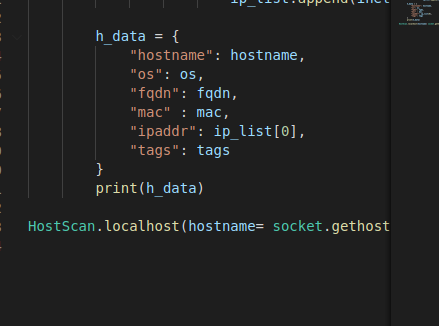
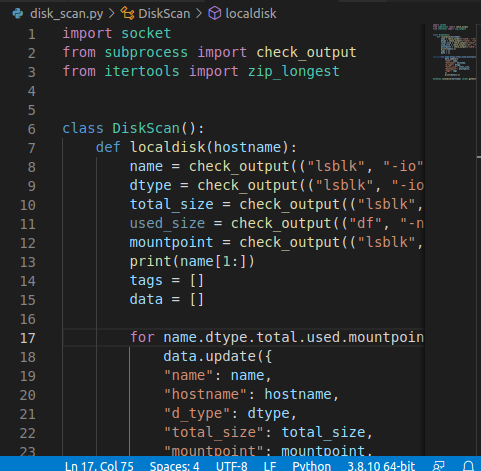


Figure 8:script de host scan



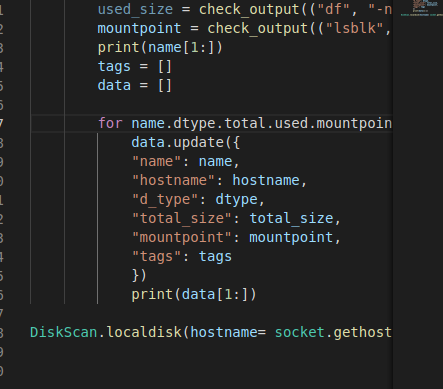


Figure 9:script de disk scan

1. **Présentation de la machine 2 : cliente**

Pour la deuxième machine nous avons utilisé Ubuntu qui est un [système d’exploitation GNU/Linux](https://fr.wikipedia.org/wiki/Distribution_Linux) basé sur [Debian](https://fr.wikipedia.org/wiki/Debian)

-En premier lieu nous devons créer une machine virtuelle intitulé cliente et puis installer python et ses différentes dépendances ainsi que sqlite3 pour la base des données.



Figure 10:commande pour installer sqlite3

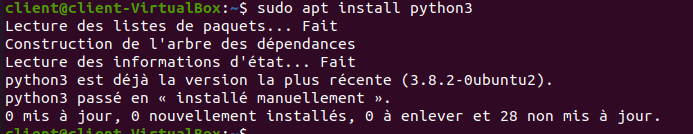
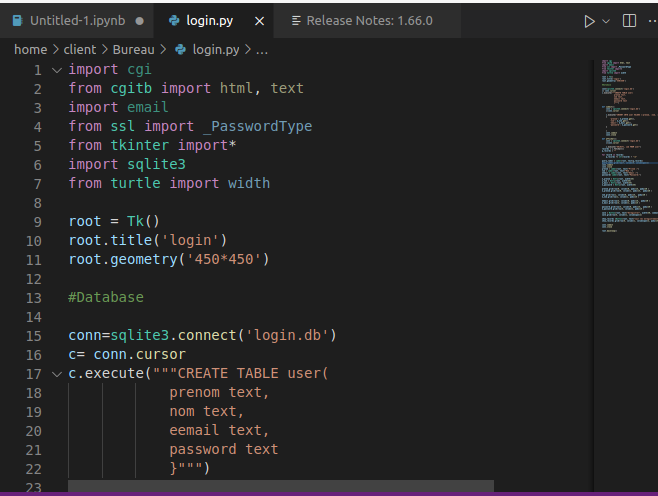
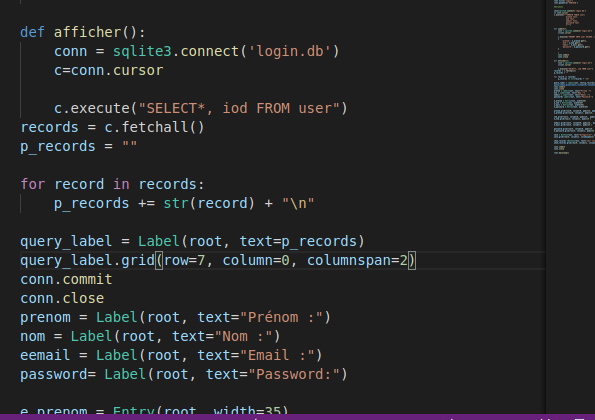
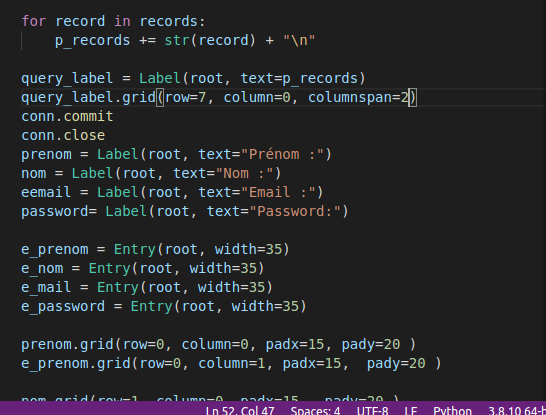
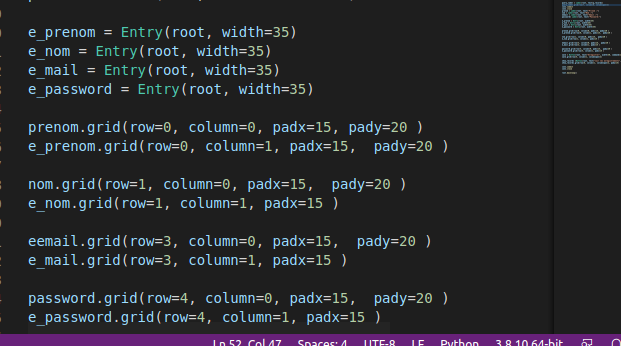
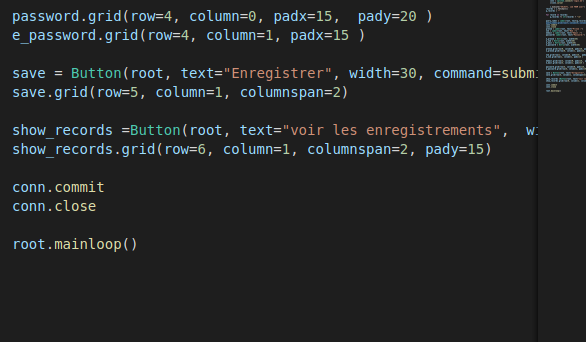


Figure 11:commande pour installer python qui est déjà installer

-Mise en place d’un script Python.

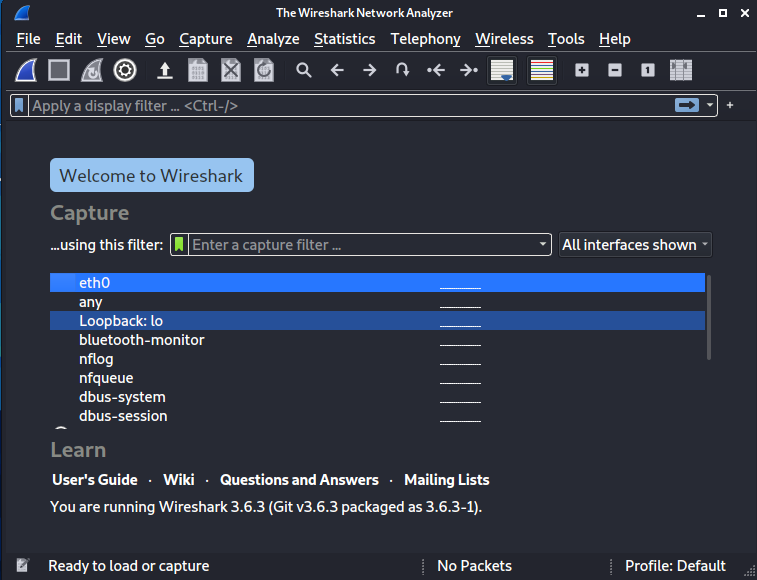
Pour cette partie nous avons mise en place un script python permettant de présenter une interface graphique qui demande les identifiants suivants : le nom complet, le mail et le mot de passe de l’utilisateur en plus d’un champ de confirmation de son mot de passe et puis donc à créer une table user dans la base de données.

1. Présentation de la machine 3 : man of the middle

Pour la troisième machine nous avons utilisé kali linux

-Installation de Wireshark



- Mise en place d’un script Python pour récupérer les paquets TCP/IP

A ce niveau avons installé **PyShark** qui est un wrapper pour l'interface CLI Wireshark, tshark, de sorte que tous les décodeurs Wireshark sont disponibles pour PyShark et nous avons mis en place un script python qui nous permettra d'analyser le trafic réseau du fichier de capture générer par Wireshark de nos échanges et aussi la sauvegarde dans un fichier csv.

