Partie 1 – Mise en place de l'environnement réseau

Consignes :

1. Créez **3 machines virtuelles** (VirtualBox ou VMware) sur un réseau interne :

   VM1 : Client → navigateur.

   VM2 : Serveur d'autorisation / Identity Provider → Keycloak.

   VM3 : Serveur de ressources → API REST simulée (Flask).

Remarque : VM1 et VM3 sont placées sur deux réseaux différents. VM2 dispose de deux interfaces réseau et joue le rôle de routeur entre les deux réseaux.

2. Assurez-vous que toutes les VM peuvent se **pinguer entre elles** pour vérifier la connectivité réseau.

3. Notez les **adresses IP internes** de chaque VM pour configurer vos applications.

4. Testez l'accès à la VM2 (IdP) depuis VM1 avec un navigateur pour vérifier que Keycloak/IdP est accessible.

Partie 2 – Expérimentation OAuth2

Objectifs : comprendre le flux OAuth2 en pratique et observer les échanges sur le réseau.

Consignes :

1. **Configuration du serveur d'autorisation (VM2)**
   - Créez un client OAuth2 dans Keycloak.
   - Configurez l'URL de redirection vers le client (VM1).
2. **Simulation du flux Authorization Code**
   - Depuis VM1, ouvrez le navigateur et accédez à l'application cliente.

- Cliquez sur « Se connecter via OAuth2 » pour initier le flux.
- L'utilisateur est redirigé vers le serveur d'autorisation pour s'authentifier.

3. **Observation du flux réseau**
   - Lancez **Wireshark** ou **tcpdump** sur VM1 et VM2.
   - Identifiez et notez :
     - La requête d'autorisation initiale (redirection vers IdP)
     - Le **code d'autorisation** renvoyé par le serveur d'autorisation
     - L'échange du code contre un **Access Token**
4. **Analyse pratique**
   - À partir du flux capturé, relevez les URL, headers et jetons échangés.
   - Notez les différences entre le code d'autorisation et le jeton d'accès.
5. **Interaction avec le serveur de ressources (VM3)**
   - Avec l'Access Token obtenu, effectuez une requête à l'API REST sur VM3.