TP 2: Partage Sécurisé de Fichiers entre une Machine Windows et une Machine Virtuelle Linux avec SSL/TLS

Dans ce TP, nous allons configurer un partage de fichiers sécurisé entre une machine hôte et une machine virtuelle. L'objectif est de mettre en pratique les concepts de **cryptographie**, de **certificats** et de **signatures électroniques** pour sécuriser les communications sur un réseau.

I. Configuration de la Machine Virtuelle Linux

1. Installation de la VM (VMWare ou VirtualBox)
2. Téléchargez une distribution Linux (ISO)
3. Mise à jour du système avec :
    a. sudo apt-get update
    b. sudo apt-get upgrade
4. Installation d'OpenSSL :
    a. sudo apt-get install openssl

II. Configuration du Réseau entre Windows et Linux

1. Configurer le réseau de la VM :
    a. Accédez aux paramètres réseau de la VM dans VirtualBox.
    b. Activez une carte réseau en mode **"Host-Only Adapter"**.
2. Vérification des adresses IP sur Windows/MacOs :
    a. Ouvrez l'invite de commandes (cmd).
    b. Exécutez la commande : ipconfig/ifconfig
    c. Recherchez l'adaptateur Host-Only et notez son adresse IP. 172.16.47.1, 192.168.113.1
3. Vérification des adresses IP sur Linux:
    a. Ouvrez terminal.
    b. Exécutez la commande : ip addr
    c. Recherchez l'interface réseau correspondante et notez son adresse IP. 172.16.47.128
4. Tester la Connectivité :
    a. Depuis Windows : ping *'ip de vm'*

b. Depuis Linux : ping *'ip de Windows/MacOs'*

III. Mise en Place du Partage de Fichiers Sécurisé

Nous allons utiliser SFTP (SSH File Transfer Protocol) pour le partage sécurisé des fichiers.

1. Installation du Serveur SFTP sur Linux
    a. Installation du Serveur SSH : sudo apt-get install openssh-server
    b. Vérification du Service SSH : sudo systemctl status ssh
    c. Création d'un Utilisateur pour le SFTP : sudo adduser sftpuser
2. Génération des Clés et Certificats
    a. Création d'une Autorité de Certification Locale :
        i. Générer la Clé Privée de la CA : openssl genrsa -out ca.key 4096
        ii. Générer le Certificat de la CA : openssl req -x509 -new -nodes -key ca.key -sha256 -days 1024 -out ca.pem
        (Remplissez les informations demandées)
    b. Génération de la Clé du Serveur SSH et de la CSR
        i. Générer une Clé Privée pour le Serveur SSH : openssl genrsa -out ssh_server.key 4096
        ii. Générer une Demande de Signature de Certificat (CSR) : openssl req -new -key ssh_server.key -out ssh_server.csr
        (Remplissez les informations demandées)
    c. Signature du Certificat du Serveur par la CA
        i. Signer le Certificat : openssl x509 -req -in ssh_server.csr -CA ca.pem -CAkey ca.key -CAcreateserial -out ssh_server.crt -days 500 -sha256
3. Configuration du Serveur SSH pour Utiliser les Certificats
    a. Copier les Fichiers de Clé et de Certificat :
        i. Placez ***ssh_server.key*** et ***ssh_server.crt*** dans ***/etc/ssh/***.
    b. Modifier la Configuration SSH :
        i. Éditez le fichier : sudo nano /etc/ssh/sshd_config
        ii. Ajoutez ou modifiez les lignes suivantes :
            - HostCertificate /etc/ssh/ssh_server.crt
            - PasswordAuthentication yes
        iii. Redémarrer le Service SSH : sudo systemctl restart ssh

4. Configuration du Client SFTP sur Windows
    a. Installation des Outils Nécessaires
        i. Installer PuTTY (client SSH) :
            - Téléchargez et installez PuTTY (https://www.putty.org/).
    b. Installer WinSCP (client SFTP) :
        i. Téléchargez et installez WinSCP (https://winscp.net/).
    c. Importer le Certificat de la CA sur Windows
        i. Depuis Linux, copiez ca.pem vers Windows
    d. Importer le Certificat dans le Magasin de Certificats Windows :
        i. Double-cliquez sur ca.pem sur Windows.
        ii. Cliquez sur "Installer le certificat".
        iii. Choisissez "Ordinateur local" comme emplacement de stockage.
        iv. Sélectionnez "Placer tous les certificats dans le magasin suivant" et choisissez "Autorités de certification racines de confiance".
        v. Terminez l'installation.
    e. Configuration de WinSCP pour Utiliser le Certificat
        i. Lancer WinSCP.
        ii. Créer une Nouvelle Session :
            - Hôte : <ip-de-la-vm-linux>
            - Nom d'utilisateur : sftpuser
            - Mot de passe : celui défini lors de la création de l'utilisateur.
        iii. Configurer les Paramètres Avancés :
            - Allez dans "Paramètres" > "Avancé".
            - Sous "SSH", assurez-vous que "Authentification" est configuré pour accepter les certificats.
    f. Connexion au Serveur SFTP :
        i. Cliquez sur "Connexion".
        ii. Si une alerte de clé SSH s'affiche, vérifiez l'empreinte et acceptez-la.
5. Configurer macOS en tant que Client SFTP

a. **Installer Homebrew** : macOS n'a pas de client SFTP préinstallé. Utilisez Homebrew pour installer un client SFTP (comme *scp* ou *rsync*) si nécessaire :

   brew install openssh

b. **Terminal** : Utilisez directement la commande sftp depuis le Terminal de macOS au lieu de *PuTTY* et *WinSCP*.

IV. Utilisation des Signatures Électroniques pour les Fichiers

Pour assurer l'intégrité et l'authenticité des fichiers échangés, nous allons utiliser des signatures électroniques.

1. Signature d'un Fichier sur Linux
   a. Créer ou Choisir un Fichier à Partager (document.txt).
   b. Générer une Paire de Clés pour l'Utilisateur : openssl genrsa -out user.key 2048
   c. Générer un Certificat pour l'Utilisateur :
      i. openssl req -new -key user.key -out user.csr
      ii. openssl x509 -req -in user.csr -CA ca.pem -CAkey ca.key -CAcreateserial -out user.crt -days 365 -sha256
   d. Signer le Fichier : openssl smime -sign -in document.txt -signer user.crt -inkey user.key -out document_signed.p7s -outform DER
2. Vérification de la Signature sur Windows
   a. Transférer les Fichiers vers Windows
      i. Utilisez WinSCP pour télécharger les fichiers suivants depuis le serveur Linux vers Windows :
         - document.txt
         - document_signed.p7s
         - user.crt
         - ca.pem
   b. Importer les Certificats dans Windows
      i. Importer le Certificat de la CA :
         - Voir la section III.4 pour l'importation de ca.pem.
      ii. Importer le Certificat de l'Utilisateur :

- Double-cliquez sur user.crt.
- Suivez le même processus d'importation, mais placez-le dans le magasin "Personnes de confiance" ou "Autres personnes".

c. Installer OpenSSL sur Windows

i. Télécharger OpenSSL pour Windows :

- Téléchargez une version binaire d'OpenSSL pour Windows (https://slproweb.com/products/Win32OpenSSL.html).

ii. Installer OpenSSL

d. Vérifier la signature du fichier

i. Ouvrir CMD.

ii. Naviguer vers le Répertoire Contenant les Fichiers : cd C:\..\..\..\..

iii. Vérifier la Signature : openssl smime -verify -in document_signed.p7s -inform DER -content document.txt -CAfile ca.pem

Si la vérification est réussie, le contenu du document sera affiché. Sinon, une erreur sera signalée.

V. Tests et Validation

1. Vérification de la Sécurité de la Connexion SFTP
   a. Analyse du Trafic Réseau :
      i. Utilisez un outil comme **Wireshark** pour capturer le trafic réseau lors de la connexion SFTP.
      ii. Vérifiez que les données sont chiffrées et qu'il n'y a pas de texte en clair.
2. Test de l'Authentification Mutuelle
   a. Connexion sans le Certificat de la CA :
      i. Supprimez le certificat de la CA du magasin de certificats Windows et essayez de vous reconnecter en SFTP.
      ii. Vous devriez recevoir un avertissement ou une erreur indiquant que le certificat du serveur n'est pas reconnu.
3. Validation des Signatures Électroniques
   a. Modification du Fichier Signé :

i. Modifiez légèrement document.txt sur Windows.

ii. Réessayez de vérifier la signature. La vérification devrait échouer, indiquant que l'intégrité du fichier a été compromise.