TP 1

Objectif

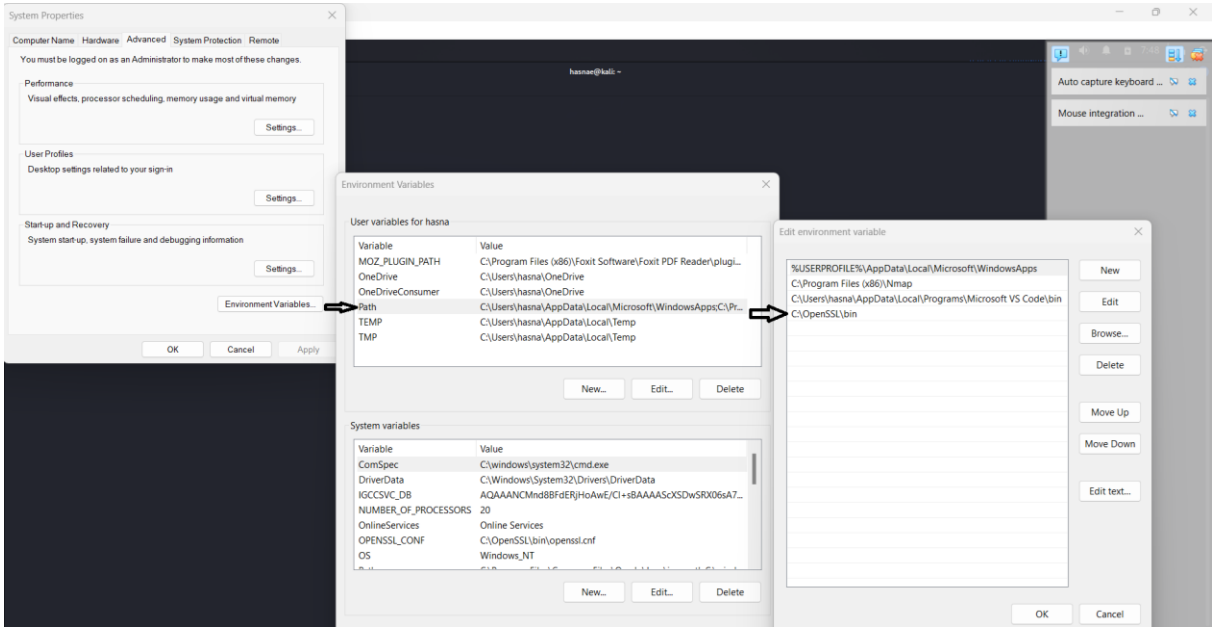
- Se familiariser avec les fonctionnalités et la bibliothèque openSSL
- Génération et utilisation des Clés secrètes
- Chiffrement de données via les commandes de la bibliothèque openSSL

Outils

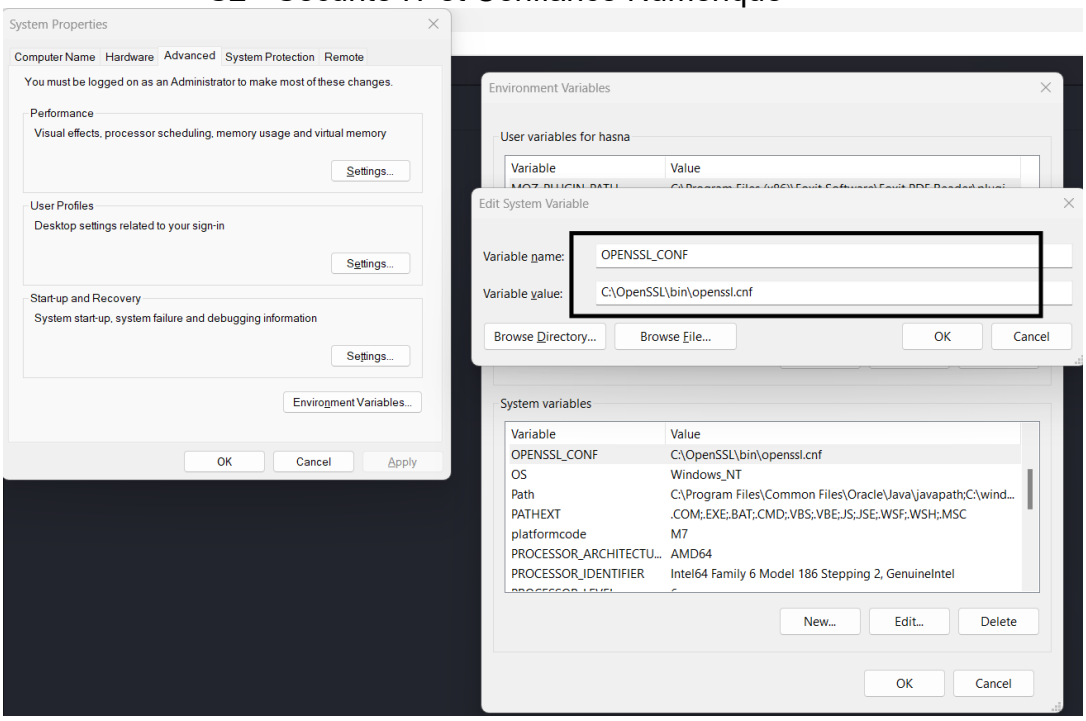
- Système Windows ou Linux
- Bibliothèque openSSL

Préparation de l'environnement de travail

- **Kali Linux**
  - Sur Kali linux bibliothèque openSSL existe déjà, vous pouvez vérifier son existence et sa version par la commande : openssl version
- **Windows**
  - Sur la machine Windows du lab de test (virtual box) ou sur votre machine : Telecharger la bibliothèque openSSL .
  - Une fois téléchargé, décompressé le dossier et placer le sur le disque C:\
  - Ajouter le chemin : C:\OpenSSL\bin au variable utilisateur path



  - Création d'une nouvelle variable système : OPENSSL_CONF, cette variable devrait pointer sur le fichier : C:\OpenSSL\bin\openssl.cnf



- Un redémarrage du système est nécessaire
- Vous pouvez vérifier son existence et sa version par la commande : openssl version

Fonctionnalités OpenSSL

La bibliothèque OpenSSL est une implémentation libre des protocoles SSL et TLS qui offre un ensemble d'outils en ligne de commande permettant, le chiffrement et le déchiffrement (RSA, DES, IDEA, RC2, RC4, Blowfish, etc.)…La syntaxe générale pour utiliser les fonctionnalités d'OpenSSL en mode shell est la suivante : **openssl <commande> <options>**

Chiffrement d'un fichier

openssl enc -aes-256-cbc -in fichier.txt -out fichier_chiffre_aes.enc -k motdepasse
openssl enc -des-ede3-cbc -in fichier.txt -out fichier_chiffre_3des.enc -k password

Déchiffrement du fichier

openssl enc -aes-256-cbc -d -in fichier_chiffre_aes.enc -out fichier_dechiffre_aes.txt
openssl enc -aes-256-cbc -d -in fichier_chiffre_aes.enc -out fichier_dechiffre_aes.txt -k motdepasse
openssl enc -des-ede3-cbc -d -in fichier_chiffre_3des.enc -out fichier_dechiffre_3des.txt -k password

Questions :

- Expliquez les options utilisées sur les commandes de chiffrement et de déchiffrement
- Comparez les commandes et notez leurs différences.
- Quelle est la différence entre AES-256 et 3DES en termes de sécurité et de performances ?
- Ajoutez l'option **-salt** aux commandes de chiffrement avec **AES-256-CBC** et **3DES**, puis chiffrez. Comparez les fichiers chiffrés obtenus. Quelle différence observez-vous ?