3.03 - Certificats, chiffrement, hashing

Durée approximative : ***8h***

Éléments du référentiel adressé :

U6 - Cybersécurité des services informatiques

- **B3.2 : Protéger l'identité de l'organisation et déployer les moyens appropriés de preuves électroniques**
- **B3.2 Appréhender les principes de la sécurité : Disponibilité, intégrité, confidentialité**

I. Notions sur le chiffrement

Introduire la notion de chiffrement (avec des parallèles avec des chiffrements physiques si nécessaire, comme CESAR, Enigma, etc...).

Expliquer son utilité et le lien avec les cyber-menaces.

Expliquer les algorithmes de chiffrement symétrique, asymétrique.

Expliquer les clé de chiffrement simples, donner des exemples d’algorithmes.

Introduire la notion de clé privée / publique.

II. Notions sur le Hashing

Introduire les notions de hashage.

Expliquer la différence avec le chiffrement.

Expliquer l'utilité concrète, vérification de la conformité d'une donnée d'entrée, vérification d'intégrité.

> **TP** : Faire vérifier des hash de sources, des hash de mots de passe.

III. Introduction aux certificats

Introduire les notions de certificats, les types et usages de ceux-ci.

Introduire les notions liées à la PKI.

Expliquer la portée des CA, le système de trust, Root CA, intermediate CA, etc...

> **TP** : Démontrer l'utilisation des certificats en faisant installer / utiliser une CA aux étudiants. Pour passer un site en HTTPS par exemple.

Ressources associées :

Sécurité - PKI et Certificats

Sécurité - Hash et chiffrement

Fiche TP - Hash, chiffrement, utilisation et limitations.

Apache2 - Configuration HTTPS

Revision #1
Created 2026-07-17 13:33:59 UTC by Olivier
Updated 2026-07-17 13:33:59 UTC by Olivier