CM1 - Introduction et Fondamentaux

Introduction à la sécurité informatique

Mohamed Said M'Bareck

SUPNUM
ms.mbareck@supnum.mr

2025-2026

Plan

1. Introduction Générale au Module
   - Contenu du Module
   - Objectifs d'Apprentissage
   - Organisation et Évaluation
2. Introduction et Définitions
   - Définitions Fondamentales
   - Les Piliers de la Sécurité (CIA+)
   - Cadre Légal et Éthique
3. Le Risque Informatique
   - Le Facteur Humain
   - Analyse et Quantification du Risque
4. Le Point de Vue de l'Attaquant
   - Vecteurs d'Attaque Communs
   - Cycle de Vie d'une Attaque

- **CM 1** : Introduction et Fondamentaux
- **CM 2** : Cryptographie Appliquée
- **CM 3** : Sécurité Réseau : Attaques et Défenses
- **CM 4** : Sécurité des Systèmes et Applications Web

Introduction Générale au Module

Objectifs d'Apprentissage

1. Expliquer les principes de sécurité fondamentaux (CID).
2. Identifier et classifier les menaces et vulnérabilités courantes.
3. Appliquer les concepts de base de la cryptographie.
4. Utiliser des outils de sécurité standards (Nmap, Wireshark, etc.).
5. Démontrer des vulnérabilités web communes (SQLi, XSS, etc.).
6. Mettre en œuvre des mesures de défense et de durcissement de base.

- Le module est conçu pour un volume total de **24 heures**.
- **Cours Magistraux (CM) :** 4 sessions de 1h30 (Total : 6 heures)
- **Travaux Dirigés (TD) :** 4 sessions de 1h30 (Total : 6 heures)
- **Travaux Pratiques (TP) :** 8 sessions de 1h30 (Total : 12 heures)

- **Évaluation Continue :** Des exercices pratiques seront à rendre après chaque séance de TD et/ou TP pour valider les acquis.
- **Projet de Module :** Un projet d'audit de sécurité sera réalisé en binôme.
  - Il suivra un fil rouge ("Golden Thread") sous la forme d'une étude de cas continue, appliquant les concepts de chaque module à un scénario pratique.

La Sécurité Informatique

L'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles.

Objectif Principal

Assurer que les ressources (matérielles/logicielles) sont uniquement utilisées dans le cadre prévu et par les personnes autorisées.

- **Confidentialité** : Seules les personnes autorisées peuvent accéder aux informations.
- **Intégrité** : Les informations ne peuvent être modifiées que par des personnes autorisées et de manière contrôlée.
- **Disponibilité** : Les systèmes et les données doivent être accessibles lorsque cela est nécessaire.
- **Authentification** : Prouver l'identité d'une entité (utilisateur, machine).
- **Non-répudiation** : Empêcher une entité de nier avoir effectué une action.

La technique ne suffit pas

Un professionnel de la sécurité doit opérer dans un cadre strict.

- **Éthique du Hacker (Ethical Hacking) :** Utiliser les compétences offensives pour un objectif défensif, avec une autorisation explicite.
- **Divulgation Responsable (Responsible Disclosure) :** Processus permettant de signaler une vulnérabilité au propriétaire du système pour qu'il la corrige avant de la rendre publique.
- **Cadre Légal :** Les actions non autorisées sont des crimes. Il est impératif de connaître les lois sur la cybercriminalité et la protection des données (ex : GDPR en Europe).

Le Maillon le Plus Faible

Un système peut être techniquement robuste, mais une erreur humaine, une négligence ou une manipulation peut anéantir toutes les mesures de sécurité.

- **L'Ingénierie Sociale** : L'art de manipuler les gens pour obtenir des informations confidentielles (mots de passe, accès, etc.).
- Exemples de risques humains :
  - Maladresse (suppression de données).
  - Ignorance (cliquer sur un lien de phishing).
  - Malveillance (employé mécontent).

- La sécurité est un compromis entre les coûts, les contraintes et les risques acceptés.
- La formule de calcul du risque :

$$\text{Risque} = \frac{\text{Menace} \times \text{Vulnérabilité}}{\text{Contre-mesure}}$$

- **Menace** : Le danger potentiel (ex : un pirate, un malware).
- **Vulnérabilité (Faille)** : Une faiblesse dans un système qui peut être exploitée par une menace.
- **Contre-mesure** : Une mesure de protection qui réduit le risque (ex : un firewall, une formation).

Le Point de Vue de l'Attaquant

Vecteurs d'Attaque Communs

Où les attaquants cherchent-ils en premier ?

- Authentification faible ou mots de passe par défaut.
- Logiciels et systèmes non mis à jour (failles connues non corrigées).
- Configurations par défaut non sécurisées.
- Services réseau inutiles laissés ouverts.
- Manque de séparation des privilèges et des réseaux.

Le Point de Vue de l'Attaquant

Cycle de Vie d'une Attaque

1. **Reconnaissance** : Collecte d'informations sur la cible (adresses IP, technologies utilisées, employés).
2. **Scan (Balayage)** : Identification des systèmes actifs, des ports ouverts et des vulnérabilités potentielles.
3. **Obtention de l'accès (Exploitation)** : Exploitation d'une faille pour pénétrer dans le système.
4. **Maintien de l'accès** : Installation de portes dérobées (backdoors) ou de rootkits pour garantir un accès futur.
5. **Effacement des traces** : Suppression des journaux (logs) et des preuves de l'intrusion.