Sécurité et Criminalistique des Bases de Données

Introduction

M. Laïdi FOUGHALI

l.foughali@univ-skikda.dz

(Site ⇒ al-moualime.com)

Université de Skikda — Département d'Informatique

1re Année Master Sécurité Informatique (SI)

Année académique 2025-2026

Version v1.0 — 2026-02-10 à 08:36:06

Plan

Présentation du cours

Informations pratiques

- **Cours** : Sécurité et Criminalistique des Bases de Données
- **Niveau** : Master 1 Sécurité Informatique, Semestre 2
- **Code** : UEF21 (*Unité d'Enseignement Fondamentale*)
- **Horaire** : 1h30 cours + 1h30 TP par semaine
- **Évaluation** : 40% TP (3 notes) + 60% Examen final
- **Crédits** : 4 (Coefficient 3)

Livre de référence

Database Security
Auteurs : Alfred Basta & Melissa Zgola (2011)
Éditeur : Cengage Learning

La devise du cours

Ce cours a été conçu selon une approche centrée sur l'efficacité pédagogique, la compréhension active et l'application pratique des connaissances.

Vision du cours : Sécurité et investigation des bases de données

Trois compétences fondamentales à maîtriser

1. **Sécuriser — Avant l'attaque**
   - Configurer un SGBD (*Database Management System*) selon les bonnes pratiques
   - Mettre en place authentification forte et contrôles d'accès
   - Chiffrer et protéger les données sensibles
2. **Détecter — Pendant l'incident**
   - Surveiller les journaux d'activité en temps réel
   - Identifier anomalies et comportements suspects
   - Réagir rapidement pour limiter les impacts
3. **Analyser — Après l'incident**
   - Reconstituer le déroulement de l'attaque
   - Collecter et préserver les preuves numériques
   - Rédiger un rapport d'analyse et proposer des mesures correctives

Pourquoi étudier ce sujet ?

Un problème mondial

Aujourd'hui, tout est numérique :

- Vos données bancaires → Dans une base de données
- Votre dossier médical → Dans une base de données
- Vos achats en ligne → Dans une base de données
- Vos messages Facebook → Dans une base de données

Résultat : Les BD sont les cibles N°1 des pirates de données !

Exemples concrets : Chaque minute dans le monde

- 5.9 millions de recherches Google
- 231 millions d'emails envoyés
- 400 000 transactions bancaires

Toutes ces données sont stockées dans des bases de données.

Modèle CIA appliqué aux bases de données

Le modèle CIA — Fondement de la sécurité des données

C — Confidentialité

- Empêcher l'accès non autorisé aux données
- Exemples : chiffrement, authentification forte, contrôle d'accès
- Risque : fuite de données personnelles ou financières

I — Intégrité

- Garantir que les données ne sont pas modifiées illégalement
- Exemples : journalisation, signatures, contraintes BD
- Risque : altération des comptes bancaires ou résultats

A — Disponibilité

- Assurer que la base reste accessible aux utilisateurs légitimes
- Exemples : sauvegardes, réplication, protection anti-DDoS
- Risque : interruption des services critiques

Cycle réel d'une attaque contre une base de données

Étapes typiques observées dans les incidents réels

1. Reconnaissance — Scan du serveur et recherche de vulnérabilités
2. Intrusion — Exploitation (SQL Injection, mot de passe faible)
3. Élévation de privilèges — Accès administrateur
4. Mouvement latéral — Accès à d'autres systèmes
5. Exfiltration — Vol progressif des données
6. Effacement de traces — Suppression ou modification des logs

Lien avec le cours

Sécuriser → empêche l'intrusion Détecter → repère l'attaque en cours Analyser → reconstruit la chronologie

Scénario fil rouge du cours

Cas pratique : Plateforme e-commerce compromise

Une entreprise possède une base PostgreSQL contenant :

- Comptes clients et mots de passe
- Transactions bancaires
- Historique des commandes

Un attaquant exploite une injection SQL et accède à la base.

Votre mission tout au long du cours

- Chapitre sécurité : empêcher l'attaque
- Chapitre détection : identifier l'intrusion
- Chapitre forensique : analyser les traces
- Chapitre final : produire un rapport professionnel

Quelles données sont en danger ?

Trois types de données critiques

1. **Données personnelles**
   - Identité, contacts, photos, messages
   - Historique navigation et achats
2. **Données financières**
   - Cartes bancaires, comptes, transactions
3. **Secrets d'entreprise**
   - Formules secrètes, stratégies, clients

Pourquoi c'est grave ?

Ces données valent de l'argent sur le marché noir !

Ce que vous allez apprendre (1/2)

Compétences techniques — Protéger

À la fin du cours, vous saurez :

Sécuriser une base de données

1. Installer et configurer PostgreSQL en mode sécurisé
2. Créer des mots de passe forts et des contrôles d'accès
3. Chiffrer les données sensibles (les rendre illisibles)
4. Empêcher les attaques SQL Injection

Compétences transférables

Les principes appris s'appliquent à tous les SGBD (*Database Management Systems*) : Oracle, MySQL, SQL Server, MongoDB, etc.

Ce que vous allez apprendre (2/2)

Compétences techniques — Investigation

Investigation après une attaque

1. Lire et analyser les journaux système (logs)
2. Reconstituer la chronologie des événements (démarche d'investigation)
3. Collecter et préserver des preuves numériques à valeur légale
4. Rédiger un rapport d'investigation professionnel

Ce cours vous prépare à

- Administrer des bases de données sécurisées
- Exercer en tant qu'analyste forensique numérique
- Préparer des certifications délivrées par des références internationales en cybersécurité (CEH Certified Ethical Hacker, CISSP Certified Information Systems Security Professional, CISM Certified Information Security Manager)

Le grand problème de sécurité

Où va l'argent de la sécurité ?

Les entreprises dépensent beaucoup d'argent pour la sécurité :

- 40% pour protéger le réseau (Internet, WiFi)
- 35% pour protéger les ordinateurs et logiciels
- Seulement 10% pour protéger les bases de données

Mais attention !

80% des données sensibles sont dans les bases de données !
C'est comme avoir une maison avec :

- Une porte blindée (réseau sécurisé)
- Des fenêtres avec barreaux (ordinateurs protégés)
- Mais un coffre-fort ouvert (base de données non protégée)

Qui attaque les bases de données ? (1/2)

Deux types d'attaquants

1. **Les pirates externes (45%)**
   - Utilisent des techniques comme SQL Injection
   - Cherchent des failles dans le système
   - Volent des milliers de comptes d'un coup
2. **Les menaces internes (55% — DANGER ! !)**
2. **Menaces internes**
   - Erreurs humaines, mauvaise configuration
   - Utilisateurs négligents ou malveillants
   - Abus de privilèges

Source : Verizon DBIR et rapports IBM — part significative des incidents implique des acteurs internes ou des erreurs humaines

Le paradoxe

55% des violations sont internes, mais 80% des budgets sont dépensés contre les menaces externes !

Qui attaque les bases de données ? (2/2)

Les quatre vecteurs d'attaque principaux

1. **Ingénierie sociale**
   - Phishing et manipulation humaine
   - Impliqués dans une grande majorité des incidents

Source : Verizon Data Breach Investigations Report (DBIR) — facteur humain présent dans plus des deux tiers des violations

2. **Vulnérabilités Web**
   - SQL Injection, XSS (*Cross-Site Scripting*), CSRF (*Cross-Site Request Forgery*)
3. **Malware (logiciels malveillants)**
   - Virus, Vers, Chevaux de Troie, Ransomware (rançongiciels)
4. **Applications trompeuses**
   - Faux sites qui imitent les vrais pour voler vos données

Combien coûte une cyberattaque ?

Coûts moyens d'une violation de données

Selon le rapport **IBM Cost of a Data Breach** :

- **Coût moyen mondial** : environ 4.4 millions USD
- **Aux États-Unis** : environ 10 millions USD
- **Secteur santé** : souvent le plus coûteux

Source : IBM Cost of a Data Breach Report (analyses Ponemon Institute)

Pourquoi c'est si cher ?

- Amendes réglementaires (RGPD, PCI-DSS)
- Perte de confiance et de clients
- Interruption d'activité
- Investigation forensique et remédiation

Temps de détection d'une attaque

Durée moyenne d'une violation

Les études industrielles indiquent qu'une violation de données peut prendre en moyenne **entre 240 et 280 jours** pour être détectée et contenue.

Source : IBM Cost of a Data Breach Report

Conséquences du retard

- Exfiltration progressive des données
- Disparition ou altération des preuves
- Réinfection ou accès persistant
- Augmentation significative des coûts

Cas réels célèbres

Trois cyberattaques qui ont marqué l'histoire

1. **Equifax (2017) — États-Unis**
   - 147 millions de personnes piratées
   - Numéros de sécurité sociale, permis de conduire volés
   - Coût : Plus de 1.4 milliard de dollars
   - Cause : Un bug non corrigé dans le logiciel
2. **Yahoo (2013-2014)**
   - 3 milliards de comptes compromis (tous les utilisateurs !)
   - Mots de passe et questions secrètes volés
   - Yahoo a perdu 350 millions lors de sa vente à Verizon
3. **Marriott (2018) — Hôtels**
   - 500 millions de clients touchés
   - Numéros de passeports et cartes bancaires volés
   - Les pirates sont restés cachés pendant 4 ans !

La criminalistique numérique : principe

Qu'est-ce que la criminalistique numérique ?

Même logique qu'une scène de crime physique :

- Recherche méthodique d'indices
- Documentation avant toute manipulation
- Preuves copiées et scellées
- Reconstruction de la chronologie

Objectif : comprendre précisément ce qui s'est passé dans le système.

Application aux bases de données

On analyse :

- Les journaux (logs) d'accès et de modifications
- Les traces d'authentification
- Les modifications de données suspectes
- Les actions des utilisateurs

Investigation : étapes et traçabilité

Cycle d'une investigation numérique

1. **Préparation** — outils et procédures
2. **Identification** — localiser les preuves
3. **Préservation** — copie sans altération
4. **Collecte** — extraction des traces
5. **Analyse** — reconstruction des faits
6. **Rapport** — conclusions documentées

Chaîne de conservation (*Chain of Custody*)

Traçabilité complète des preuves : qui → quand → où → comment.
Chaîne rompue = preuve juridiquement fragile.

Aperçu du contenu du cours

Les grands chapitres

Chapitre 1 — Menaces et Malware

- Identification des menaces externes et internes
- Les 5 familles de malware : Virus, Vers, Trojans, Ransomware, Botnets
- Cycle de sécurité et défense en profondeur

Chapitre 2 — Architecture sécurisée

- Configuration sécurisée de PostgreSQL
- Chiffrement et protection des données

Chapitre 3 — Contrôle d'accès

- Gestion des utilisateurs et permissions
- Principes du moindre privilège

Chapitre 4 — Investigation forensique

- Analyse de logs et reconstruction d'attaques
- Collecte de preuves légales

Organisation du cours

Cours magistraux pour comprendre la théorie — 1h30/semaine

- Concepts de sécurité des bases de données
- Techniques et stratégies d'attaque
- Analyse de cas réels
- Normes : ISO 27001, NIST (*National Institute of Standards and Technology*), RGPD

Travaux pratiques pour mise en œuvre — 1h30/semaine

- Installation et configuration sécurisée PostgreSQL
- Gestion des utilisateurs et permissions
- Chiffrement des données sensibles
- Tests d'attaque en environnement contrôlé
- Analyse de logs après simulation

Ce que vous devez déjà savoir (1/2)

Connaissances essentielles

Bases de données (IMPORTANT !)

- Savoir ce qu'est une table, une clé primaire, une clé étrangère
- Comprendre le modèle relationnel
- Maîtriser SQL : SELECT, INSERT, UPDATE, DELETE
- Connaître les jointures et les vues

Systèmes et réseaux

- Utiliser la ligne de commande Linux
- Comprendre TCP/IP, HTTP, HTTPS
- Savoir ce qu'est une adresse IP, un port

Ce que vous devez déjà savoir (2/2)

Connaissances essentielles (suite)

Sécurité de base

- Comprendre : Confidentialité, Intégrité, Disponibilité (CIA)
- Savoir ce qu'est le chiffrement
- Connaître les menaces courantes (virus, phishing)

Si vous avez des lacunes

- Révisez SQL sur **SQLZoo.net** (gratuit)
- Pratiquez Linux sur **Ubuntu** en machine virtuelle
- Lisez les chapitres 1-2 du livre de référence

Quels outils utiliser ? (1/2)

Logiciels à installer

Base de données

- **PostgreSQL 14+** : Le SGBD qu'on va utiliser
- **pgAdmin 4** : Interface graphique pour PostgreSQL
- **DBeaver** : Éditeur SQL pratique

Pourquoi PostgreSQL ?

- **Industriel** : Utilisé par Apple, Instagram, Spotify
- **Open source** : Gratuit, code source accessible
- **Pédagogique** : Concepts valables pour tous les SGBD

Quels outils utiliser ? (2/2)

Outils de sécurité

- **sqlmap** : Tests d'injection SQL automatisés
- **Wireshark** : Analyse du trafic réseau
- **OpenSSL** : Chiffrement et certificats

Système d'exploitation

- Linux (Ubuntu recommandé)
- Ou machine virtuelle Linux sur Windows

À faire dès maintenant

Installez PostgreSQL pour pratiquer chez vous.
Guide d'installation fourni dans les ressources du cours.

Où trouver de l'aide ? (1/2)

Documentation officielle

Référence du cours

- Database Security — Basta & Zgola (2011)

Documentation en ligne (gratuite !)

- PostgreSQL Security Documentation officielle
- OWASP (*Open Web Application Security Project*) — Guide sécurité BD
- NIST SP 800-53 — Standards de sécurité

Où trouver de l'aide ? (2/2)

Pour rester à jour

- **The Hacker News** — Actualités cybersécurité
- **Krebs on Security** — Blog expert
- **CVE** (*Common Vulnerabilities and Exposures*) — Liste des vulnérabilités découvertes

Lois importantes à connaître

- **RGPD** — Loi européenne protection données personnelles
- **PCI-DSS** (*Payment Card Industry Data Security Standard*) — Norme sécurité cartes bancaires
- Violation = Amendes jusqu'à 4% du chiffre d'affaires !

Quels métiers après ce cours ? (1/2)

Opportunités de carrière (Métiers accessibles)

- **DBA Sécurité** — Administrateur de bases de données sécurisées
- **Analyste Forensique** — Expert en investigation numérique
- **Pentester** — Pirate éthique qui teste la sécurité
- **Auditeur Sécurité** — Vérifie si l'entreprise est bien protégée
- **CISO** (*Chief Information Security Officer*) — Responsable de toute la sécurité informatique

Quels métiers après ce cours ? (2/2)

Secteurs qui recrutent

- Banques et assurances
- Hôpitaux et pharmacies
- Sites e-commerce
- Gouvernement et armée
- Cabinets de conseil en cybersécurité

Marché de l'emploi

- **3.5 millions de postes vacants** en cybersécurité dans le monde
- Croissance de **+30% par an**
- Salaires parmi les **plus élevés** de l'informatique
- Spécialistes BD sécurisée = Très recherchés !

Mot de la fin

Bienvenue !

Pourquoi ce cours est passionnant ?

- Vous allez apprendre à penser comme un pirate (pour mieux vous défendre)
- Vous allez jouer au détective numérique
- Vous allez protéger des données critiques
- Vous aurez un métier recherché et bien payé

La philosophie du cours

- **Comprendre** plutôt que mémoriser
- **Pratiquer** plutôt que juste lire
- **Questionner** plutôt qu'accepter
- **Apprendre continuellement** (la sécurité évolue chaque jour)