Mini Projets

Sécurité des Systèmes IA

1. **Détection d'attaques web par apprentissage automatique**
    - Construire un modèle ML pour classer des requêtes HTTP normales vs malveillantes (SQLi, XSS).
2. **Intrusion Detection System basé sur IA**
    - Utiliser des données réseau (ex. KDD99, CIC-IDS2017) pour entraîner un modèle de détection d'intrusions.
3. **Détection de phishing par NLP**
    - Utiliser un modèle de traitement du langage (BERT, DistilBERT) pour identifier les mails de phishing.
4. **Attaques adversariales sur un classifieur d'images**
    - Générer des exemples adversaires (FGSM, PGD) et tester la robustesse du modèle.
5. **Détection de données empoisonnées dans un dataset (Data Poisoning)**
    - Concevoir un algorithme qui repère des anomalies ou corruptions dans les données d'entraînement.
6. **SIEM intelligent basé sur IA**
    - Construire un prototype simple de SIEM qui utilise du ML pour corréler des événements de sécurité.
7. **Détection de spam/phishing par IA**
    - Utiliser un dataset de mails (spam/ham).
    - Entraîner un classifieur (Naive Bayes, SVM, Logistic Regression).
    - Résultat attendu : distinguer emails légitimes des mails suspects**.**
8. **Reconnaissance d'URLs malveillantes**
    - Créer un dataset d'URLs (benignes vs malicieuses).
    - Extraire quelques features simples (longueur, caractères spéciaux, "http vs https").
    - Entraîner un modèle simple (Random Forest).
9. **Détection de mots de passe faibles avec IA**
    - Créer un dataset de mots de passe (faibles vs forts).

- Entraîner un modèle simple (réseau de neurones ou logistic regression).
- Application : conseiller si un mot de passe proposé est fort ou faible.

10. Détection de messages frauduleux sur WhatsApp ou SMS

- Dataset de SMS (ham vs spam).
- Modèle simple de classification par NLP.

11. Détection de faux comptes sur un réseau social

- Utiliser un dataset public (Twitter, Facebook).
- Extraire des features simples (nombre d'amis, activité, date de création).
- Classifier en compte légitime vs faux compte.

12. Détection de tentatives d'injection SQL via IA

- Créer un petit dataset (requêtes SQL normales vs malicieuses).
- Entraîner un modèle simple (SVM ou Random Forest).

13. Quiz intelligent de sensibilisation à la cybersécurité

- Créer un chatbot simple qui pose des questions de sécurité (phishing, mots de passe).
- Adapter les questions en fonction des réponses (logique IA basique).

14. Système de recommandation de bonnes pratiques sécurité

- Exemple : un utilisateur entre son comportement (ex. utilise le même mot de passe partout).
- Le système IA recommande des bonnes pratiques personnalisées.