COMPÉTENCES VISÉES

Bac +3
Formation Numérique Option Cybersécurité

PREMIÈRE ANNÉE

PROTOCOLES & RÉSEAUX :
La compréhension des réseaux est fondamentale en cybersécurité, car la majorité des attaques et des mécanismes de défense transitent par les infrastructures réseau. Cette matière permet aux étudiants de maîtriser les protocoles essentiels (TCP/IP, DNS, HTTP), les architectures réseau (LAN, WAN, VPN), ainsi que les notions de segmentation et de topologie nécessaires à l'analyse et à la sécurisation des systèmes.

ARCHITECTURE MATÉRIELLE :
Cette matière permet de comprendre le fonctionnement interne des composants matériels et d'identifier les vulnérabilités au niveau physique. Elle est indispensable pour appréhender les attaques exploitant le matériel et les failles bas niveau.

SYSTÈMES D'EXPLOITATION :
Les systèmes d'exploitation constituent une couche logicielle critique et représentent une cible privilégiée des attaquants. Cette matière permet de comprendre et de renforcer les politiques de sécurité (permissions, contrôle d'accès), ainsi que de réaliser des analyses forensiques sur des systèmes compromis (logs, mémoire, processus).

ALGORITHMES ET PROGRAMMATION EN PYTHON :
Python est un langage de référence en cybersécurité, notamment pour l'automatisation et l'analyse. Cette matière permet d'automatiser les tests de sécurité, de développer des scripts d'analyse de logs, de détecter des intrusions et d'initier les étudiants à l'analyse de données de sécurité, y compris via des approches de détection d'anomalies.

BASES DE DONNÉES :
Les bases de données stockent les informations les plus sensibles des organisations. Cette matière est essentielle pour comprendre leur fonctionnement, sécuriser les accès et prévenir des attaques majeures telles que les injections SQL, qui figurent parmi les vulnérabilités web les plus critiques.

PRINCIPES ET RÉGLEMENTATION DE LA SÉCURITÉ INFORMATIQUE :
Cet enseignement fournit le cadre légal, éthique et organisationnel indispensable à toute démarche de cybersécurité. Il permet de comprendre non seulement comment sécuriser un système, mais également pourquoi et dans quelles limites légales et réglementaires.

PROGRAMMATION WEB :
Les applications web constituent aujourd'hui la surface d'attaque la plus exposée. Cette matière est donc cruciale, car plus de 70 % des cyberattaques exploitent des vulnérabilités applicatives. Elle permet aux étudiants de comprendre les failles web courantes et les bonnes pratiques de développement sécurisé.

COMPÉTENCES VISÉES

Bac +3
Formation Numérique Option Cybersécurité

DEUXIÈME ANNÉE

La deuxième année approfondit les compétences techniques et opérationnelles avec les matières suivantes :

PROGRAMMATION EN C++ :
Le C++ permet de travailler à un niveau proche du matériel et du système. Il est essentiel pour comprendre les mécanismes bas niveau, l'exploitation de failles mémoire et le fonctionnement interne des logiciels.

ADMINISTRATION LINUX :
Linux est au cœur des infrastructures critiques (serveurs, cloud, conteneurs, solutions de sécurité). Cette matière permet de sécuriser les systèmes Linux, d'analyser les attaques et de comprendre les mécanismes de défense avancés.

ADMINISTRATION WINDOWS :
Windows étant majoritaire dans les environnements professionnels, sa maîtrise est indispensable. Cette matière permet de sécuriser les postes et serveurs, de gérer les politiques de sécurité et de comprendre les attaques ciblant les systèmes d'entreprise.

VIRTUALISATION :
La virtualisation est un pilier des infrastructures modernes et du cloud computing. Elle constitue à la fois une nouvelle surface d'attaque et un puissant outil de défense, notamment pour les environnements de test et d'analyse sécurisés.

PIRATAGE ÉTHIQUE (ETHICAL HACKING) :
Cette discipline adopte une approche offensive visant à identifier les vulnérabilités avant qu'elles ne soient exploitées. Elle permet aux étudiants de développer une vision globale de la sécurité en apprenant à penser comme un attaquant afin de mieux se défendre.

TROISIÈME ANNÉE

La troisième année se déroule en alternance et comprend des enseignements avancés tels que :

— Sécurité des réseaux,
— Chiffrement et VPN,
— Piratage éthique avancé,
— Programmation sécurisée,
— Réseaux avancés,
— Préparation à la certification CEH (Certified Ethical Hacker).

esaip
École d'Ingénieurs La Salle