



SYLLABUS MASTÈRE SPÉCIALISÉ[®]

Cybersécurité : Attaque et défense des Systèmes Informatiques

Module	Syllabus	Compétences
Malware, retro-ingénierie de code (45 h, 6 ECTS)	<ul style="list-style-type: none"> - Méthodes d'offuscation de code binaire - Aspects systèmes pour l'obfuscation: PEB, interruptions - Modèles du code binaire: graphe de contrôle de flot, vagues de code - Conception de code auto-modifiant - Extraction de charges à partir d'exécutable - Rétro-ingénierie statique à l'aide d'IDA - Rétro-ingénierie dynamique à l'aide de Pintool 	<ul style="list-style-type: none"> - Evaluer la vulnérabilité d'un système - Evaluer la dangerosité d'un programme, en décrire les anomalies - Décrypter les protections d'un malware et les contourner - Rechercher la « payload » d'un malware par analyse statique, retourner les fonctionnalités - Décrire les dégâts provoqués par un malware sur un système
Analyse de la sécurité d'un réseau (45 h, 6 ECTS)	<ul style="list-style-type: none"> - Présentation des différents types d'attaques réseaux et logicielles - Analyse de l'architecture de sécurité IPsec - Configuration de VPN 	<ul style="list-style-type: none"> - Connaître les principales catégories d'attaques réseaux et logicielles - Comprendre les éléments clés d'une politique de sécurité d'entreprise

	<p>sécurisés</p> <ul style="list-style-type: none"> - Configuration de pare-feux - Monitoring et outils d'audit pour la sécurité (nmap/nessus) - Sécurité des applications web et bonnes pratiques (owasp) 	<ul style="list-style-type: none"> - Être capable de configurer des outils de protection usuels (pare-feux, VPN sécurisés) - Savoir utiliser des outils d'audit pour évaluer la sécurité d'une infrastructure et de ses services - Connaître les bonnes pratiques liées au développement d'applications web sécurisées
<p>Cryptographie, analyse des protocoles de communication (45 h, 6 ECTS)</p>	<ul style="list-style-type: none"> - Introduction aux protocoles cryptographiques - Modélisation des protocoles, et des attaquants - Introduction au logiciel ProVerif - Cas d'utilisation du protocole Needham-Schroeder - Protocole de vote électronique - Protocole TLS et Triple Handshake attack 	<ul style="list-style-type: none"> - Savoir spécifier un protocole de communication sécurisé - Etre en mesure d'anticiper les attaques - Comprendre les modèles d'attaquant, en évaluer les conséquences pratiques - Connaître un logiciel de vérification de protocole, évaluer la faisabilité de scénarii d'attaques réseau
<p>Politique de sécurité, gestion de crise (45 h, 6 ECTS)</p>	<ul style="list-style-type: none"> - intro au droit pénal et infractions principales en lien avec le numérique - enquête pénale et cybercriminalité (perquisitions, expertise judiciaire, accès à la preuve) interaction entre la réponse à incidents et l'enquête pénale - se préparer à l'incident 	<ul style="list-style-type: none"> - Connaître les principes d'une politique de sécurité - Evaluer, rechercher les indices de compromission - Connaître les principes d'un « pentest » - Connaître les aspects légaux en sécurité informatique, savoir gérer ces aspects dans le contexte

	<p>cyber, au dépôt de plainte et gestion de crise du point de vue de ces incidents judiciairisés</p> <ul style="list-style-type: none"> - intégrer la lutte contre la fraude et les atteintes cyber dans la conception et l'évolution des produits et des services - normes ISO pour la sécurité - recherche d'indices de compromission 	de l'entreprise ou auprès des tribunaux
<p>Systèmes cyber-physiques (45 h, 6 ECTS)</p>	<ul style="list-style-type: none"> - Architectures et protocoles de communication pour les systèmes industriels : Modbus, Profinet, DNP3 - Vulnérabilités et attaques dans les systèmes industriels - Détection d'intrusions et mécanismes de protection. - Travaux pratiques sur la réalisation des attaques sur une plate-forme expérimentale (Automates SIEMENS et Schneider) 	<ul style="list-style-type: none"> - Savoir gérer les communications entre l'infrastructure informatique et un automate industriel - Evaluer la vulnérabilité d'un système par modélisation d'attaques (fuzzing,...) - Reconnaître une attaque par analyse des paramètres - Savoir simuler une attaque sur un système concret
<p>Introduction à l'Investigation Numérique et à la Réponse à Incidents (45 h, 6 ECTS)</p>	<ul style="list-style-type: none"> - Concepts fondamentaux - Méthodologie d'investigation (préparation, identification, collecte) - Sécurisation (image disque, capture de RAM) - Reconstruction système de fichiers - Récupération d'éléments effacés (data carving) - Vérification des signatures - Utilisation des empreintes 	<ul style="list-style-type: none"> - Savoir réunir les preuves ou les éléments physiques éventuellement dans un cadre légal - Connaître la méthodologie d'extraction de données depuis les supports physiques dans un cadre sécurisé - Recherche d'informations cachées (fichiers supprimés) par analyse des données brutes - Analyser et rechercher les données sur une machine

	<p>numériques (MD5)</p> <ul style="list-style-type: none"> - Utilisation d'outils de corrélation de données - Analyse de dump de RAM - Définition de règles yara / IOC 	<p>"vivante" et compromise</p> <ul style="list-style-type: none"> - Analyse et recherche d'IOC
<p>OS et virtualisation (45 h, 6 ECTS)</p>	<ul style="list-style-type: none"> - Politique de sécurité, - Conformité, cloisonnement, surveillance - Supervision, - authentification des utilisateurs - Segmentation des rôles, - Développement d'exploits, - Développement des charges - Persistance, infrastructure 	<ul style="list-style-type: none"> - Connaître les principes de compartimentation d'une infrastructure physique - Mettre en place une infrastructure logicielle sur une structure physique (DMZ, ...) - Piloter, gérer et mettre en place des machines virtuelles à distance - Connaître les phases d'attaque d'un système - Etre capable de reconstruire un scénario d'attaque - Savoir retrouver des IOC dans les journaux
<p>Projet (45 h, 3 ECTS)</p>	<p>Projet scientifique sur les connaissances de la formation</p> <p>Recherche bibliographique</p>	<ul style="list-style-type: none"> - Gestion de projet - Apprentissage de l'autonomie - Mise en œuvre pratique des compétences des autres modules