Mastère Spécialisé
« Sécurité de l'Information et des Systèmes »
de l'ESIEA
(MS-SIS)

Programme détaillé

- Analyse de malwares (cours de 6H + TP de 6H + projet)
Analyse statique (reverse engineering).
Analyse dynamique (en sandbox).
Projet : analyse d'un binaire spécifique par étudiant.

- Antivirus core programming (cours de 10H + TP de 10H) – cours en anglais -
1. Introductory part: The history of viruses from John von Neumann works till DOS viruses, Who creates malware and why (hacktivism, criminals, government) Different types of viruses which exist "in the wild", Definition of different types of malicious behavior
2. Malware detection techniques : Static analysis (Patterns and Signatures,Integrity checking. Intermediate representations, CFG and Call graph metrics, Entropy metrics, Heuristics) Emulation, Dynamic analysis and behavioral detection, API monitoring Sandbox, HIPS, Telemetry analysis
3. Obfuscation techniques and how malware could protect itself against detection.
4. Rootkits for Windows x32/x64
5. Mobile malware from Symbian till Android platforms
6. Ransomware
7. Threats for MacOS operating system
8. Threats for Linux operating system
In the practical part of our course, we show how to analyse virus in IDA and automate such processes using python. Also we present several ways for unpacking files in OllyDBG.

- Applications réseau sécurisées (cours de 10H + TP de 11H + projet)
Dans ce module on va découvrir comment mettre au point des applications réseaux sécurisées en utilisant la plateforme java et ses spécificités notamment en sécurité. Notamment, une application de type discussion instantanée sera utilisé comme cas d'école pour illustrer comment l'adjonction de mesures de sécurité à une application qui en est initialement dépourvue est possible.
Projet : réalisation par chaque étudiant d'une application non web (programmes client et serveur) dotée de services spécifiques.

- Architecture et sécurité réseau (cours de 10H + TP de 22H30)
Les objectifs de ce cours sont:
Expliquer les vulnérabilités rencontrées sur les réseaux locaux (LAN), notamment avec les équipements OSI niveau 2 (switch - A.P.) et les protocoles (Ethernet - WIFI - Bt): sécurisation des équipements et des protocoles OSI niveau 2
Présentation de l'organisation et des outils utilisés lors d'un contrôle technique de sûreté (ou évaluation de sécurité): préparation d'un contrôle technique de sécurité. Gérer et maîtriser les outils de sécurité. Comprendre l'éthique lors de l'exécution d'un contrôle sur un système opérationnel.

- Architecture Windows (cours de 9H + TP de 6H + projet)
L’objectif de ce cours est de comprendre l’architecture d’un système Windows depuis le démarrage jusqu’au lancement de la session et des différents organes.
On étudie les mécanismes de sécurité : protection contre l’exploitation de BO, Secured Boot, Mandatory Integrity Control, ...
Il y a par la suite une partie sur le développement noyau dans le but de faire un rookit simple, à base de SSDT hooking et de modification de structure noyau.
Projet : réalisation d’un programme fortif en mode noyau.

- Atelier CV (cours de 3H + TP de 1H30)
L’objectif de ce cours est d’apprendre à rédiger un CV de manière professionnelle.
Mise en valeur des projets ainsi que des compétences

- Audit de Sécurité (cours de 8H + TP de 10H)
Présentation d'une mission de test d'intrusion classique.
Présentation des outils classiques de tests d'intrusion au fur et à mesure.
Audit d'une application web.
Audit d'une application lourde.

- Cartes à puce (cours de 10H + TP de 11H + projet)
L'utilisation des cartes à puce est essentielle dès lors que l'on souhaite mettre en place les systèmes ayant le plus haut niveau de sécurité.
Dans ce module on va découvrir ce que sont les cartes à puce, pourquoi elles permettent d'apporter les plus hauts niveaux de sécurité lorsqu'elles sont utilisées à bon escient, et comment réaliser des programmes en tirant parti.
Projet : réalisation d’une application carte complète avec les parties on-card et off-card.

- Crise en entreprise (cours de 12H)
Pas une seule entreprise aujourd'hui ne peut s'affranchir d'une gestion des risques et des incidents. Chaque entreprise développe des objectifs métiers qui reposent sur des drivers compétitifs et des indicateurs de performance. Le système d'information joue un rôle majeur. Son optimisation, son agilité et sa sécurite sont autant de facteur clés pour la compétitivité.
L’objectif de ce module est d’apporter un regard critique et opérationnel sur le déploiement d’une culture de gestion de risque efficace et appropriée au sein de l’entreprise afin de mieux prévenir, détecter et protéger son actif numérique.

- Construction d’une architecture de réseaux IP (cours de 2H30 + TP de 5H)
1) Dans un premier temps, étude de cas à réaliser en binôme ou trinôme aboutissant à un cahier des charges techniques :
Proposition d’une architecture réseaux répondant aux besoins.
Infrastructure maillée.
Plan d’adressage avec masques de longueur variable.
Tables de routages détaillées.
2) Dans un second temps, mise en place de l’architecture avec tous les équipements réseaux réels (hubs et routeurs) :
Construction par étape de l’architecture

Infrastructure de câblage
Configuration IP des différents équipements
Stations de travail
Routeurs
Implémentation des différents routages
Routage statique
Routage dynamique
Protocole à vecteur de distance : RIP
Protocole à état des liens : OSPF
Tests, analyses et comparaisons des différents routages
Analyse de trames (PING, TRACEROUTE, RIP, OSPF)
Détermination des routes
Création de pannes, observations et mesures temps de convergence

- Cryptographie à clef privée (cours de 7H30 + TP de 7H30 + projet)
Dans un premier temps on étudie les méthodes de chiffrement historiques à savoir, le chiffrement de Jules César, Vigenère , masque jetable ainsi que la machine Énigma.
On étudie ensuite en détail les cryptosystèmes modernes tels que L'AES, le DES (3DES).
On voit également le fonctionnement des fonctions de hachage (MD4, MD5, SHA-1, etc.) ainsi que la mise en oeuvre de la signature électronique.
Projet : réalisation d'un programme mettant en œuvre de la cryptographie symétrique.

- Cryptographie à clef publique (cours de 7H30 + TP de 7H30 + projet)
Ce cours a pour objectif de présenter les éléments de base de la cryptographie à clé publique.
On commence par présentr les fondements de la théorie des nombres pour présenter le problème de la factorisation, le problème RSA, le logarithme discret et le problème Diffie-Hellman.
Cela permet de décrire le chiffrement RSA, le chiffrement ElGamal, la signature électronique et des protocoles de mise en accord de clefs, tel SSL/TLS. On expliquera par la suite les preuves à divulgation nulle de connaissance, ainsi que la cryptographie distribuée.
Des constructions concrètes ainsi que des attaques explicites seront détaillées.
Projet : réalisation d'un programme mettant en œuvre de la cryptographie asymétrique.

- Développement crypto SSL/TLS (cours de 6H + TP de 6H + projet)
Ce module permet d'orchestrer les connaissances théoriques en Cryptographie apprises dans d'autres modules de la formation afin de designer et d'implémenter des solutions cryptographiques.
Les élèves utiliseront la bibliothèque OpenSSL en ligne de commande et prendront en main la bibliothèque mbedTLS afin de développer des programmes de chiffrement de fichiers et de stockage de mots de passe, par exemple.
Projet : développement d'un programme mettant en œuvre la bibliothèque PolarSSL.

- Droit de la sécurité des systèmes d'information (conférences de 6H)
Ce thème revêt aujourd'hui une importance toute particulière au sein des entreprises, des administrations et des associations. La législation en cette manière est complexe et s'impose à tous (RSSI, DSI, Chief Data Officer, etc.), tant à l'échelle nationale qu'européenne.
Ce module est l'occasion d'aborder les notions élémentaires du droit (notamment en termes de responsabilité pénale et civile des divers acteurs du SI) appliquées à la protection des données sensibles ainsi que des stratégies de protection du SI grâce au droit.

- Droit des données personnelles (conférence de 3H)
Notions de données personnelles et de traitement.
Obligations légales du responsable de traitement et droits des personnes concernées.
Principes de licéité des traitements. Formalités préalables obligatoires.
Textes juridiques de référence actuels et à venir.
Pouvoir de contrôle et de sanction de la CNIL.
Jurisprudence des sanctions administratives et pénales.

- Droit du numérique (conférences de 6H)
Liberté d'expression sur internet et limites légales
Responsabilité de la publication de contenus
Obligations des hébergeurs
E-réputation et vie privée
Protection de la propriété intellectuelle (contenus publiés, développements informatiques, sites, …)
Données publiques et libres
Droit du e-commerce
Droit d'accès de l'employeur aux outils numériques de l'employé

- Droit et biométrie (conférence de 3H)
Principes
Historique et évolution
Techniques biométriques
Encadrement juridique
Performances

- Editeur de texte: vi (cours de 3H)
Que cela soit pour modifier des fichiers de configuration système ou bien pour écrire des programmes, et ce en local ou bien sur un système distant, il est nécessaire de savoir maîtriser un éditeur de texte. Le choix d'utiliser l'éditeur vi plutôt qu'un autre éditeur repose essentiellement sur sa disponibilé sur un grand nombre d'environnements, sa relative rapidité d'apprentissage (tout en n'étant pas un util intuitif) et sa forte résiliance sur un système défaillant.
Les étudiants vont apprendre à maîtriser cet outil afin de gagner en efficacité lors des nombreuses séances de TP à venir dans les autres modules.

- Firewalling: théorie et application (cours de 6H + TP de 9H)
Après avoir présenté le filtrage de port et la notion de firewall à états, les étudiants mettent en œuvre pour chaque groupe au minimum un firewall, un serveur en DMZ et un poste en réseau interne. Un switch Cisco et un routeur Linux complètent le dispositif pour permettre une communication entre les groupes et en direction d'Internet.
Chaque machine est protégée par un ensemble de règles iptables pour configurer le firewall Linux Netfilter. Les différents groupes mettent en oeuvre aussi bien des règles de filtrage que de la translation d'adresse.
Des scans de ports sont effectués pour vérifier la bonne application des règles de sécurité.

- Introduction et enjeux de la cryptographie asymétrique (conférence de 3H)
Courte introduction au RSA, usage pour la distribution de clé et la signature, à l'échange de clé Diffie-Hellman et aux courbes elliptiques.
Introduction à l'histoire : idée de clé publique à travers les âges (depuis 1943 à 1975).
Génération des paramètres : nombres premiers, factorisation, etc.
Exponentielle discrète.
Problématique du calcul quantique versus la sécurité (cryptographie post-quantique).

- Introduction et enjeux de la cryptographie symétrique (conférence de 3H)
Les algorithmes mis en oeuvre dans le cadre de la cryptographie à algorithmes symétriques utilisent la même clef pour chiffrer et déchiffrer les informations. On parle dans ce cas de clef secrète, ou clef privée, qui ne doit en aucun cas être révélée au risque de compromettre la sécurité du système.
Dans ce module on se propose d'introduire ce type de cryptographie qui est très utilisée, notamment grâce aux débits qu'elle permet par rapport aux algorithmes cryptographiques asymétriques (ou dits à clef publique) et qui autorisent son utilisation massive.
On introduira notamment les notions de chiffrement par blocs et chiffrement par flux.

- Identité numérique (conférence de 3H)
Encadrement juridique français et européen de l'identité numérique.
Niveaux de sécurité.
Techniques d'identité numérique, PKI.
Identités régaliennes et identités gérées par des acteurs privés.

- Infrastructures sécurisées (cours de 8H + TP de 4H)
Ce cours est dédié à la sécurité transversale des architectures de traitement des données.
Nous y traitons des différents maillons de la sécurité d'un SI : en partant de la sécurité d'un unique serveur, nous évoluons vers la protection de son réseau environnant (et de son hyperviseur, le cas échéant), pour dériver vers la sécurité de l'infrastructure logique, en englobant la protection des communications vers les réseaux externes tels qu'Internet (ou qui utilisent Internet comme les connexions VPN), mais aussi la sécurité physique et humaine de ces architectures.
Nous étudions alors la gestion de la sécurité dans sa globalité, ainsi que l'empilement des protections permettant d'atteindre un niveau de confiance satisfaisant en terme de qualité, respectant les contraintes de coûts, de complexité et de temps.

- Initiation aux techniques d'audit de sécurité/pentest (cours de 4H + TP de 5H)
Ce module a pour but de sensibiliser les étudiants aux méthodes et techniques des tests de pénétration des systèmes d'information (SI), aussi appelés pentests.
Il comporte une présentation des différentes phases d'un pentest, telles que la reconnaissance, l'identification des vulnérabilités, l'exploitation de ces dernières, et la mise en place de mécanismes de persistance. Afin de ne pas rester dans un cadre purement théorique, cette présentation est agrémentée d'exemples réel anonymisés. Différents outils sont introduits tout au long de la présentation.
Dans un second temps, le module se déroule sous la forme de travaux pratiques.
Un environnement virtualisé de plusieurs machines (volontairement vulnérables) est mis à disposition des étudiants. Chaque étudiant dispose de son propre environnement, pour ne pas influer sur le travail des autres étudiants. Durant cette partie, les élèves seront logiquement amenés à appliquer les méthodologies présentées auparavant, le choix des outils étant libre.

- Intelligence économique (cours de 10H + TP de 2H)
Ce module traite de dimensions organisationnelles de la sécurité: prise en compte du facteur humain avec ses fragilités, compréhension des modèles économiques en présence, acteurs impliqués, enjeux, modes opératoires, buts poursuivis. L'articulation entre la sécurité technique et cette facette plus immatérielle vise à former des experts et des responsables d'unités, aptes à gérer, anticiper, et à communiquer au sein de leur structure d'exercice.

- Introduction à Git (cours de 3H + TP de 1H30)
L’objectif de ce cours est de donner les rudiments de l’utilisation d’un gestionnaire de version : récupérer un code, gestion des branches, merge, etc.

- Introduction à l'assembleur (cours de 4H + TP de 2H)
Ce module a pour objectif de donner des bases suffisamment solides en assembleur pour aborder le module de rétro-conception, il se décompose pour cela en deux parties.
La première partie du module est un cours magistral qui commence par des généralités sur les systèmes numériques (décimal, hexadécimal et binaire) puis l’architecture des ordinateurs en parlant particulièrement de la mémoire et du processeur. La suite du cours aborde les différents systèmes d’adressage utilisés dans les instructions, puis les instructions les plus régulièrement rencontrées. La fin du cours porte une attention particulière aux appels de fonction, aux conventions d’appels ainsi qu’à l’établissement d’un cadre de pile.
La seconde partie du module est un TP qui permet aux étudiants de mettre en pratique les notions rencontrées en insistant particulièrement sur les variables locales et variables globales. L’exercice consiste à écrire une fonction récursive qui force une rigueur sur la gestion de la mémoire.

- Introduction au reverse Engineering (cours de 9H + TP de 6H)
Ce module a pour but de donner aux étudiants un aperçu de ce domaine encore top peu enseigné dans les écoles. Il commence par une partie théorique afin de mettre l’accent sur les notions importantes de l’assembleur x86, la gestion de la pile et les conventions d'appels. Puis Il s'ensuit une partie pratique avec des exercices de niveau progressif. Les exercices consistent à reverser des programmes développés pour ce module.
Ce module permet également de prendre en main les outils adéquats pour ce domaine. - Introduction au Big Data: (r)évolution des bases de données (cours de 3H)
Cette sensibilisation a pour objectif de présenter l'écosystème Big Data et la révolution du concept de base de données. L'intervention met en perspective l'évolution des technologies Big Data entre les papiers de Google en 2004 et les enjeux actuels liés à l'IoT, l'Open Data et la mobilité. Ensuite les concepts fondamentaux des architectures distribuées sont introduits avec notamment le rôle de l'écosystème Open Source. Puis les différents types de bases de données sont présentés ainsi que les enjeux de sécurité associés.

- IPSec (cours de 3H + TP de 3H)
L’objectif de ce module est de présenter en détails le fonctionnement d’IPSec. Après avoir présenté ce que permettent de faire chaque mode (AH et ESP), leurs apports en terme de sécurité (confidentialité/intégrité) et les champs qui sont chiffrés/authentifiés, nous nous intéressons ensuite aux deux modes d’utilisation: tunnel et transport en application AH et ESP à chaque fois.
Le cours est très orienté pratique. A chaque fois, on visualisera les trames avec des logiciels adaptés.
Configuration à base de démon ISAKMP et racoon.

- Introduction à la programmation GPU (cours de 4H + TP de 8H)
Présentation des architectures GPUs.
Initiation à la programmation CUDA.
Ecrire un kernel CUDA.
Réaliser des transferts mémoires entre CPU et GPU.
Introduction à l’asynchronisme entre CPU et GPU.
Introduction à la programmation multithreads + GPU.

- Introduction aux Critères Communs (cours de 3H)
Cette sensibilisation a pour objectif de présenter le projet Critères Communs, de ses origines à son organisation actuelle en passant par ses acteurs clés et sa déclinaison dans le schéma français géré par l'ANSSI. L'intervention dresse un historique des principes de certification, du projet CC, des normes et des accords internationaux. Ensuite la philosophie de l'évaluation d'un produit et la terminologie CC sont introduits. Puis l'organisation du schéma français et les concepts de cible de sécurité sont détaillés.

- Lutte contre la cyber-criminalité (conférence de 3H)
La cybercriminalité regroupe des réalités diverses touchant des domaines multiples des sociétés développées. L'image du pirate informatique, si elle reste d'actualité, ne couvre pas l'ensemble des profils délinquants. Les cybercriminels peuvent porter atteinte aux moyens de paiement avec de fausses cartes de crédit. Ils peuvent aussi organiser des escroqueries complexes via les systèmes financiers internationaux. Enfin, l'emploi d'outils spécialisés comme des logiciels malveillants et la prolifération de ceux-ci a eu pour conséquence de massifier le phénomène, faisant de lui un enjeu majeur. Pour répondre à ce problème, la Police nationale s'est organisée pour adapter ses structures à cette nouvelle forme de cybercriminalité : en prolongement de l'action judiciaire traditionnelle, une approche plus proactive a été adoptée pour faire face à ces nouveaux défis.

- OSINT ou le renseignement en sources ouvertes (cours de 5H30 + TP de 6H30)
Ce cours rappelle les fondamentaux de la recherche en source ouverte en détaillant les différentes sources disponibles et leurs modes d'interrogations. Dès que la volumétrie de recherche est importante, il devient impératif d'automatiser les recherches et leurs recoupements. Les étudiants vont donc étudier les différents format (text plain, html, json) et les modes d'interactions (scrapper, api) en utilisant soit des scripts python soit des outils comme Maltego.

- Origines des réseaux de données (conférence de 3H)
L'Internet résulte d'apports multiples, datagrammes (France), DNS (USA), WEB (CERN), moteur de recherche (DEC), gouvernance (ICANN), et de développements constants d'applications intégrant des services antérieurement fournis dans le cadre de réseaux dédiés (courrier, fax, téléphone, radio, télévision, cinéma, jeux et paris, sondages, alarmes, météo, et bien d'autres).
L'avance prise par les USA à partir des années 80 leur a permis de s'installer dans tous les secteurs critiques de l'internet: standards de protocoles, identifiants de réseaux (adresses IP, noms de domaine), chiffrement, certificats, gouvernance, services trans-nationaux (GAFAS), juridictions, et de diriger les quelques structures internationales censées rechercher un équilibre entre les pouvoirs des Etats et des sociétés multinationales.Ce quasi monopole des USA est cependant contrarié par des initiatives de diversité. Dès 2005 la Chine a construit son propre réseau internet en caractères chinois indépendant de l'ICANN. Des DNS indépendants ont été créés d'abord aux USA, puis en Europe, p.ex. Parti Pirate en Allemagne et Open-Root en France. La vétusté du protocole TCP a suscité une diversité de modes spécifiques d'échanges pour lutter contre l'absence de sécurité et la vulnérabilité aux attaques de pirates, et à la surveillance de masse mise en place depuis 2000 par les USA. En bref, l'internet a été conçu au début des années 70 comme un réseau expérimental, et il l'est resté.
Une nouvelle architecture de réseau est indispensable pour disposer d'un socle de niveau industriel, notamment pour la sécurité, la confidentialité, et la qualité de service.

- Présentation de l'ANSSI (conférence de 3H)
Des représentants de l’Agence Nationale de la Sécurité des Systèmes d’Information, incluant des anciens du MS-SIS, viennent présenter les missions de l’agence aux étudiants, qui auront peut-être à intéragir avec elle plus tard dans leur cadre professionnel, pour ainsi leur permettre de mieux cerner son fonctionnement et ses objectifs.

- Présentation du Ministère de la Défense (conférence de 3H)
Des représentants du Ministère de la Défense, incluant des anciens du MS-SIS, viennent présenter les missions du Ministère aux étudiants, ainsi que les différentes filières internes dans lesquels ces derniers pourraient être amenés à prendre part dans le cadre de leur vie professionnelle en rapport avec la SSI.

- Présentation du Ministère de l'Intérieur (conférence de 3H)
Des représentants du Ministère de l’Intérieur, incluant des anciens du MS-SIS, viennent présenter le cadre de fonctionnement du Ministère aux étudiants, avec les différentes possibilités qu’il y a d’y pratiquer la SSI dans différents métiers très divers, ainsi que les besoins actuels en fonction des missions liées à l’actualité.

- Programmation python (cours de 10H + TP de 5H)
L'objectif du module est de permettre aux étudiants de comprendre du code Python et d'écrire rapidement et efficacement des scripts dans ce langage. Ces aptitudes sont ensuite utilisées pour la réalisation d'un projet qui doit permettre aux étudiants d'utiliser Python pour interagir avec des serveurs réseau et pour analyser des données.

- Programmation sécurisée (cours de 8H + TP de 7H)
Les étudiants seront capables de reconnaître des fonctions vulnérables à des attaques et comment on peut les exploiter. Ils utiliseront aussi différents outils d'analyse statique/dynamique, ainsi que des primitives sécurisées pour éviter ce genre d'attaques.
Savoirs associés
- Les analyseurs statiques et leurs utilisations
- Les analyseurs dynamiques et leurs utilisations
- Les primitives en C sécurisées pour Visual Studio
- Les primitives en C pour un développement « cross-platform »
- Les différents types de vulnérabilités

- Recherche et exploitation de vulnérabilités logicielles (cours de 10H + TP de 8H)
Ce cours est une introduction à la recherche et l'exploitation de vulnérabilités logicielles, et s'appuie très largement sur des exercices pratiques. La première partie du cours est consacrée à un rappel rapide des fondamentaux (qu'est ce qu'un registre, une pile, une convention d'appel, les instructions assembleurs basiques, etc). Les élèves se familiarisent ensuite avec les vulnérabilités du type stack based buffer overflows, d'abord avec des exemples simples, puis sur des programmes utilisant des mécanismes de protection spécifiques contre l'exploitation. Les vulnérabilités du type format string puis les heap based buffer overflows sont vus. À chaque fois les concepts sont appris en s'appuyant sur des exemples concrets de programmes vulnérables sous linux. Quand plusieurs méthodes sont possibles pour arriver à un but donné, les élèves sont encouragés à toutes les découvrir, puis les avantages et inconvénient sont ensuite discutés. Enfin, l'exploitation de vulnérabilités sous Windows est abordée avec les mécanismes de protection modernes du système.

- Récupération de données et approche du forensic (cours de 8H + TP de 7H)
Sont abordés les supports courants de stockage numérique, l'organisation des données sur un disque dur mécanique, le partionnement PC Intel ET EFI GPT, les systèmes de fichiers, les formats de fichiers, les métadonnées, la récupération de données par data carving, etc.
Les exercices se font avec des outils opensource: file, hexdump, dd, ddrescue, testdisk, photorec, sleuthkit, autopsy, etc.
Les étudiants sont invités à partager leurs expériences de perte de données et à apporter différents supports pour évaluer la quantité d'information récupérable sur un support vu comme "vide" par le système d'exploitation. L'accent est mis sur l'intégrité des données, la traçabilité et la reproductibilité des analyses afin de pouvoir opérer dans un cadre légal/forensic.

- Rappels programmation C (cours de 11H + TP de 10H)
Le but de ce module est de faire une remise à niveau en C aux étudiants qui n'auraient pas pratiqué ce langage récemment. Toutes les thématiques seront étudiées à savoir les tableaux, les pointeurs, l'allocation dynamique de mémoire, les structures, les fichiers, etc. À la fin du module, un projet est donné aux étudiants dans lequel toutes ces thématiques seront à appliquer.

- Rappels Linux (cours de 10H + TP de 5H)
Alternant présentation formelle et application pratique, cette mise à niveau permet d'acquérir ou de réacquérir les connaissances minimales pour utiliser le système d'exploitation Linux et réaliser des taches d'administration courantes. Sont couverts notamment l'arborescence de fichiers, la gestion des fichiers et répertoires, les permissions Unix, la gestion des entrées/sorties, la gestion des taches, l'édition de texte sous vi/vim, l'archivage et la compression, la création et l'application de patch sur du code source, la création d'utilisateurs, l'installation de packages.

- Rappels programmation Java (cours de 11H + TP de 10H)
Ce module n'est pas un cours de Java à proprement parlé : il nécessite des étudiants qui le suivent d'avoir déjà appris la programmation Java auparavant. Il s'agit d'une remise à niveau pour se remettre dans les doigts ce langage de programmation. Intégré dans la partie "remise à niveau" du cursus, on s'assure dans ce module que les étudiants vont bien être en mesure de mettre en oeuvre la programmation Java lorsqu'ils en auront besoin plus tard dans d'autres modules du cursus.

- Rappels réseaux IP (cours de 11H + TP de 10H)
L'objectif de ce cours est de reprendre les bases du monde IP (modèles OSI et TCP/IP).
Rappel sur les calculs d'adressage et sur l'établissement des tables de routage.
Manipulation avec l'outil Marionnet et étude des trames réseau.
Rappels sur les principaux protocoles : Ethernet, IP, TPC, UDP, ICMP, DNS, DHCP, etc.

- Scapy (cours de 6H + TP de 6H + projet)
L'objectif de ce module est double : il s'agit à la fois d'utiliser l'outil Scapy pour rendre concret les protocoles et couches réseau, les échanges de données, ainsi que la capture et l'analyse de paquets, mais aussi d'apprendre à utiliser cet outil pour écrire une preuve de concept simple (envoi d'un paquet mal formé) ou plus complexe (implémentation d'un nouveau protocole et réalisation d'un outil capable de dialoguer en utilisant ce protocole).
Scapy est ici utilisé à la fois comme outil pédagogique et comme outil à connaître.
Projet : réalisation d'un programme n'utilisant pas la couche réseau de manière conventionnelle.

- SDR ou la sécurité des communications radio (cours de 5H + TP de 10H)
De plus en plus répandues, en particulier avec la montée en puissance des objets communicants, les radiocommunications sont souvent préférées à des communications filaires. Cependant, elles présentent des spécificités qui peuvent impacter la sécurité de l'information. En particulier, le médium de transmission implique une impossibilité de garantir l'émission d'information à un interlocuteur unique. Par ailleurs, l'évolution des technologies de traitement du signal et l'avènement des radios logicielles fournissent de nouveaux outils d'analyse, tout en contribuant à diminuer les moyens requis pour un attaquant.
Cette session de formation permettra de se familiariser avec les outils et techniques permettant d'analyser la sécurité de radiocommunications et d'assimiler les concepts théoriques relatifs aux problématiques de transmissions radiofréquence. Une base théorique, complétée par des travaux pratiques en utilisant le matériel nécessaire, fournira un cadre permettant d'estimer les risques pesant sur les interfaces et protocoles de communication sans fil.

- Sécurité Android (cours de 16H + TP de 14H)
Dans un premier temps, les étudiants sont formés aux techniques de reverse engineering (statique/dynamique/...) utilisables sur Android. Puis, dans un second temps, les différentes vulnérabilités que l'on peut rencontrer dans une application Android sont présentées. Enfin, les étudiants sont invités à mettre en pratique ces connaissances sur des applications spécialement vulnérables, afin de recenser et exploiter l'ensemble des vulnérabilités présentes.

- Sécurité, authentification et mots de passe (cours de 3H + TP de 4H30)
Identification, authentification, relations de confiance, cycle de vie des mots de passe, biométrie, cadre légal à son utilisation, authentification forte, traçabilité sont autant de thèmes abordés dans ce module à travers les aspects de la vie quotidienne (digicode, badge Vigik, clé, code PIN, mot de passe, CB, pass Navigo, carte vitale…).
Des cas pratiques d'attaque (dictionnaire, force-brute, rainbow tables...) sont effectués sur différentes implémentations de stockage de mots de passe Linux, Windows et Cisco.

- Sécurité dans les projets et homologation de systemes d'information (cours de 6H)
Une homologation permet de disposer d'une part d'une assurance de maîtrise des risques et d'autre part d'une autorisation d'utilisation d'un système d'information sensible auprès d'une autorité reconnue. Ce processus réclame une approche par les risques sur tout le cycle de vie d'un système, permettant une prise de décision entre les risques à couvrir et les risques acceptés. Il s'agit d'associer les enjeux métiers, les besoins de sécurité, de concevoir les fonctions selon les exigences de sécurité appropriées, de contrôler leurs bonnes intégration et efficacité au regard des contraintes économiques ou de performances du système. Cette approche s'appuie sur les référentiels nationaux et intrnationaux (RGS, EBIOS, ISO).

- Sécurité dans les réseaux mobiles, télécom et infrastructures critiques (cours de 3H30 + TP de 4H)
Plate-forme mobile (s) de sécurité, surface d'attaque.
Quels vecteurs d'attaque (points d'entrée, plans de contrôle vs. plan média).
Pentest de très grande infrastructure (PS, CS, MPLS, MSAN FTTH ADSL, OAM).
Protocoles exotiques pour applications rares.
Le moteur d'inférence d'un pentester, mis à l'échelle.
L'applicabilité réelle de la sécurité: les différences entre l’état de l’art et les réalisations réelles.

- Sécurité des applications Big Data (cours de 3H)
Cette sensibilisation a pour objectif de présenter les enjeux de sécurité des applications Big Data. L'intervention dresse un panorama des technologies incontournables des architectures Big Data et présente les 5 piliers de sécurité. Puis les vulnérabilités, les risques et les bonnes pratiques associés à ces architectures sont détaillés.

- Sécurité des applications web (cours de 12H + TP de 12H + projet)
Les objectifs de ce cours sont de se familiariser avec les architectures des applications Web et de mettre en évidence, à travers l'étude de leurs mécanismes de fonctionnement, les risques de sécurité. Apprendre à identifier les vecteurs d'attaque, les faiblesses et les impacts sur une Application Web et mettre en œuvre un ensemble de contre-mesures pour se prémunir d'un ensemble d'attaques.
Projet : mise en place d'une infrastructure vulnérable à un type de faille web donnée puis sécurisation de celle-ci dans un second temps.

- Sécurité des cartes bancaires dans le système CB (conférence de 4H)
1) La sécurité des cartes dans le système CB:
Anatomie des cartes et des sécurités.
Evolutions sécuritaires : attaques et contre-mesures.
Nouveautés: sans contact, cryptogrammes dynamiques, paiement mobile (ApplePay, HCE…).
2) La sécurité du réseau CB:
Architecture du réseau IP.
Détection de la fraude et des POC (Points Of Compromission).

- Sécurité des grands réseaux (cours de 15H + TP de 3H)
Ce cours présente les architectures, les technologies et la sécurité des réseaux multi-services d'opérateurs de télécom. Il permet de connaître et de comprendre les algorithmes de routage mis en œuvre et leurs criticités (ISIS, BGP/MP_BGP, PIM, etc.) ainsi que les architectures de services (VPLS, VPN BGP/MPLS, etc.). Enfin, des TP de programmation permettent de mener des campagnes de vérification sur des configurations réseaux Cisco à des fins sécuritaire ou pour calculer des périmètres (MPLS BGP/VPN, VLAN, BGP, etc.).

- Sécurité de la Voix sur IP (cours de 2H + TP de 5.5H)
1/ Cours sur la voix sur IP avec focus sur les mécanismes de sécurité :
Voix IP
Caractéristique de la voix et de son transport sur les réseaux
Transport de flux temps réel sur les réseaux IP
Signalisation de la voix sur IP (SIP)
Traversée des NAT et des Firewall par la voix sur IP
Problématique
Solutions à base d'ALG
Solutions à base de protocoles (STUN, TURN, ICE …)
Sécurisation de la Voix sur IP et vulnérabilité de la Voix sur IP
Sécurisation de la signalisation
Sécurisation du flux
2/ Expérimentation de la sécurité de la Voix sur IP :
Utilisation d'équipements physiques (hubs, routeurs, téléphones IP)
Utilisation de logiciels spécifiques (softphones IP)
Scénarios réalisés

Appels VoIP entre les différents matériels et logiciels
Analyse et écoute des communications
Sécurisations des communications VoIP
Sécurisation réseaux via mise en place d'un tunnel IPSEC
Sécurisation spécifique du flux temps réel (SRTP et ZRTP)
Traversée de NAT, mise en place d'une architecture NAT
Implémentation d'une solution SIP ALG NAT
Capture de trames, observation et analyse dans les différents scénarios

- Sécurité des systèmes embarqués (cours de 5H + TP de 10H)
Introduction aux menaces (physiques et logiques) qui pèsent sur les implantations matérielles (systèmes embarqués, etc.). Présentation des vecteurs de compromission de la sécurité des systèmes embarqués pour mieux en appréhender la conception ou l'analyse. Parallèlement à l'évolution des capacités matérielles des technologies de l'information et des systèmes de communication, on assiste à un déploiement croissant de systèmes embarqués (réseaux de capteurs, objets connectés, pacemakers, ordiphones,etc.) qui manipulent et échangent de l'information critique.
Ce déploiement impliquant la possibilité d'un accès physique malveillant, le profil d'attaquant est spécifique et les pratiques de sécurité «classiques» ne sont plus suffisantes. Ce cours met en lumière cette spécificité via notamment:
une analyse détaillée de la surface d'attaque spécifique aux systèmes embarqués;
une introduction pratique aux interfaces exploitables sur ce type d'équipements;
une présentation des outils nécessaires à l'analyse et l'exploitation de la surface d'attaque;
une illustration de l'évolution de la menace et de sa prise en compte à travers des exemples;
une discussion des bonnes pratiques et des vulnérabilités résiduelles au travers des TP.

- Sécurité Internet, détection, exploitation et correction de failles web (cours de 3H30 + TP de 4H)
Ce cours alterne présentation théorique de failles web et exploitation pratique de failles à travers des exercices de OWASP Webgoat. Des mesures correctives ou préventives sont présentées notamment en langage PHP. Le cours se termine par la réalisation d'un test d'intrusion sur une infrastructure LAMP (Linux, Apache, MySQL, PHP).

- Sécurité iOS (cours de 6H)
Présentation du système d'exploitation et de ses mécanismes de sécurité.
Jailbreak et présentation de backdoor basiques.
Présentation des points de faiblesses inhérent à l'OS.

- Sécurité organisationnelle/ISO27001 (cours de 12H)
Ce cours permet aux participants d'acquérir les connaissances nécessaires à la réalisation d'audits de la conformité d'un système de management de la sécurité de l'information par rapport aux exigences de la norme ISO 27001 version 2013.

- Sécurité physique et crochetage de serrures (cours de 4H + TP de 2H)
Les mots de passe, double-authentification et autres pare-feux ne sont d'aucun secours face à un intrus compétent dans les techniques de crochetage et d'ouverture fine. Le cours consiste en la découverte et la pratique des moyens d'intrusion physique permettant à un attaquant potentiel de pénétrer le système d'information autrement que par les moyens électroniques traditionnels afin de déjouer ces techniques.

- Sécurité SCADA (cours de 3H + TP de 3H)
Afin de fournir aux élèves une vision d'ensemble sur la problématique cyber des installations industrielles, le module est découpé en 2 parties complémentaires:
La première vise à donner une vision d'ensemble sur les enjeux de la cybersecurité, l'état de la menace, les normes et standards du domaine et les grands principes de sécurisation.
La seconde partie est plus orientée sur le côté offensif, avec notamment un cours de pentest spécifique à la cible particulière que sont les automates industriels.

- Sensibilisation à la stéganographie (cours de 3H + TP de 4H30)
Ce module présente une sensibilisation aux méthodes de stéganographie et de stéganalyse, principalement dans le domaine des images compressées.
L'accent sera mis sur la compréhension des formats d'images et les méthodes récentes d'insertion et de détection d'informations cachées.

- Sécurité, plans de pérennité et gestion des situations critiques (cours de 12H)
Approche des Risques : Approche et limites de l'analyse des risques. Méthodes en vigueur. Diagramme de Farmer, risques avérés et non avérés, dispositifs de prévention et de protection, risques acceptés et principe de précaution, évaluation du préjudice résiduel. Pratique du risk management et mitigation des risques. Politique d'assurances.
Sécurité physique en conception des data center :
Site : Surveillance périmétrique et gestion des accès. Redondance des servitudes.
Locaux techniques : climatisation, zones froides/chaudes ; redondance électrique, isolement, cage de Faraday, incendie et dégâts des eaux, Connaître les niveaux tier 1 à 4.
Plan de Secours Informatique (PSI) : conception d'un PSI, choix d'architecture et vulnérabilités résiduelles (sites actif/actif, actif/passif, liaisons synchrones/asynchrones, etc.). Politique de sauvegarde.
Plan de Continuité d'Activité : BIA (Bilan d'Impacts sur Activité/Business Impact Analysis), DMIA (Durée Maximale d'Interruption Admissible) et PDMA (Perte de Données Maximale Admissible), Tolérance, Gestion des dépendances. Site de repli utilisateurs. Intégration des Plan de Continuité d'Activité et Plan de Secours Informatique.
Gestion de crise : notion et dynamique de crise, spécificités des phases d'une crise, organisation et fonctionnement d'une cellule de crise, identification et cartographie des parties prenantes. Décision de crise, pièges mentaux (Dissonance Cognitive, Sunk Cost Effect et Prospekt Theory) et décisions absurdes.
Communication de crise : pourquoi communiquer, spécificités des attentes des parties prenantes, savoir créer un message de communication de crise, gestion des médias et autorités de tutelle, story telling. Communication interne : conception d'un Executive Summary.

- Shell UNIX (cours de 3H + TP de 1H30)
L'objectif de ce cours est la maitrise du shell UNIX dans le but de parvenir à faire des scripts efficaces. Tout se fait exclusivement par la pratique.

- Stratégie et recherche de vulnérabilités (TP de 3H)
Ce cours est destiné à faire prendre conscience aux étudiants que la recherche de vulnérabilités n'est pas le fruit du hasard. C'est un travail avec une probabilité d'échec élevée, le but étant de la minimiser. Il faut faire du fuzzing, lire le code ligne à ligne, partir d'anciens bugs, etc. Avoir une bonne stratégie est un facteur primordial pour une bonne recherche de vulnérabilités.

- Suricata, détection d'intrusion et monitoring réseau (cours de 6H + TP de 6H + projet)
Ce module est une initiation à la détection d'intrusion réseau et au monitoring réseau orienté sécurité, réalisé par le biais du logiciel Suricata. Une présentation théorique des problématiques est faite et les étudiants expérimentent ensuite sur les sujets de l'analyse de trafic, les canaux de contrôle de malwares, l'extraction de fichiers des flux réseaux et enfin une utilisation de Suricata en mode prévention d'intrusion.
Projet : développement d'un module Suricata sur un thème donné.

- Visite d'un Data Center (conférence de 4H)
Un datacenter met à disposition une infrastructure pour héberger des serveurs dans de bonnes conditions de sécurité, garanties par contrat. Une visite permet de voir et de discuter des différentes possibilités et des choix techniques/financiers sur les aspects de la redondance et de la continuité de l'alimentation électrique des serveurs, la climatisation, la sécurité incendie, le contrôle d'accès, la vidéo-protection, l'interconnexion réseau avec différents opérateurs ou d'autres clients, les services de proximité...

- Virologie (cours de 5H30 + TP de 6H30 + projet)
Ce module consiste en une courte introduction à la virologie informatique et à l'utilisation de cette technique pour développer un virus bénéfique à des fins d'administration d'un réseau informatique. Les étudiants développent leur propre virus et l'utilisent pour découvrir le réseau et administrer à distance un parc d'ordinateurs.
Projet : développement d'un programme mettant en œuvre une technique virale donnée.

- Vulnérabilités et Sécurité des SI en environnements partagés (cours de 6H)
Systèmes d'Information multi-niveaux : conception et organisation des IT infrastructures multi-niveaux (SI, OS, réseaux et couches ISO, etc.). Gestion et sécurisation des environnements multi-niveaux, systèmes de systèmes, réseaux multi-niveaux. Bonnes pratiques. Répartition des responsabilités dans les SI multi-niveaux.
Cloud (Informatique nébuleuse) : identifier les risques et vulnérabilités issues du partage d'infrastructures IT, d'applications mutualisées et d'environnements de stockage de données sur le Cloud. Bonnes pratiques et dispositifs de protection des données à caractère personnel stockées/partagées dans le Cloud. Responsabilités de l'entreprise et de l'utilisateur.
Poste de travail mobile : définition de la PAN (Private Area Network) et des vulnérabilités qu'elle induit en termes de sécurité des accès aux IT infrastructures et aux bases de données. Bonnes pratiques en gestion des droits d'accès des postes de travail mobiles, VPN et remote access, chiffrement des données stockées sur le poste de travail mobile, PKI et usage d'un poste de travail mobile hors territoire national. Responsabilités du propriétaire et de l'utilisateur du poste de travail mobile.
Sous-traitance et infogérance : engagements de services des prestataires (SLA : Service Level Agreement) et respect du DICP (Disponibilité, Intégrité, Confidentialité, imPutabilité). Maintien en conditions opérationnelles et GTI (Garantie de Temps d'Intervention). Gestion des accès distants des prestataires. Sécurité des données stockées hors du périmètre de l'entreprise. Responsabilités du prestataire de services et du client. Points clefs dans les contrats.