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

Programme détaillé

Intitulé de l'unité

Unité 1 : Sécurité dans les réseaux

Intitulé du cours

Application réseau sécurisée

Durée

21 heures

Objectifs

Développer from Scratch une application réseau (la partie serveur et la partie cliente) dans un premier temps, en la sécurisant ensuite en ajoutant l'utilisation d'éléments sécurisés pour gérer la partie cryptographique avec un niveau de sécurité beaucoup plus élevé que ne le permettrait une prise en charge purement logicielle de la sécurité.

Contenu

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 ainsi que l'utilisation pratique d'éléments de sécurité/carte à puce. Notamment, une application de type discussion instantannée sera utilisée comme cas d'école pour illustrer comment l'adjonction de mesures de sécurité à une application qui en est initialement dépourvue est possible.

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

Programme détaillé

Intitulé de l'unité

Unité 1 : Sécurité dans les réseaux

Intitulé du cours

Architecture et sécurité réseau

Durée

30 heures

Objectifs

* Décrire une architecture de sécurisation d'un S.I. d'entreprise.

* Inventorier et expliquer les vulnérabilités rencontrées sur les Réseaux Locaux d'Entreprise (RLE). Présenter les solutions permettant de supprimer ou de limiter les risques induits

* Comprendre l'organisation et maitriser les techniques d'investigation mises en œuvre à l'occasion des audits ou des contrôles de cybersécurité (prestations commerciales, management d'audit, éthique, inventaire des systèmes, des services et des vulnérabilités, etc.)

* Comprendre l'organisation et maitriser les briques organisationnelles et technologiques constitutives des systèmes de cybersurveillance (SOC + SIEM)

Contenu

* Network security architecture
* LAN security
* Network reminders (Tagged VLAN, static & dynamic routing, TCP/UDP, DNS, NAT/PAT, packet forging, etc.)
* Internet access (french & european laws, traçability, NAC) + LAB
* Securing the access to media (frame analysis, L2 security) + LAB
* Controls & Audits
* Organization
* Port scanning (+LAB)
* vulnerability detection (+LAB)
* Network services knowledge & WIFI mapping (+LAB)
* Cybermonitoring
* SOC/SIEM (+LAB)

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

Programme détaillé

Intitulé de l'unité

Unité 2 : Sécurité des systèmes d'information et des applications

Intitulé du cours

Architecture de sécurité Windows

Durée

15 heures

Objectifs

Comprendre l'architecture d'un système Windows depuis le démarrage jusqu'au lancement de la session et des différents organes.

Contenu

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.

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

Programme détaillé

Intitulé de l'unité

Unité 1 : Sécurité dans les réseaux

Intitulé du cours

Audit de Sécurité

Durée

18 heures

Objectifs

Méthodologie d'audit de sécurité d'applications 2 et 3 tiers.

Prise en main des outils d'audit.

Recherche et exploitation de vulnérabilités applicatives.

Rédaction de rapport d'audit.

Contenu

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.

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

Programme détaillé

Intitulé de l'unité

Unité 4 : Sécurité des données et cryptographie

Intitulé du cours

Cartes à puce

Durée

21 heures

Objectifs

Comprendre comment l'adjonction de carte à puce/éléments sécurisés, dans un système d'information dépourvu initialement de sécurité, va permettre de créer un noyau de confiance absolu autour duquel on va pouvoir mettre en oeuvre des fonctionnalités de sécurité.

Contenu

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.

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

Programme détaillé

Intitulé de l'unité

Unité 3 : Sécurité organisationnelle

Intitulé du cours

Gestion de crise

Durée

12 heures

Objectifs

Posséder 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.

Contenu

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.

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

Programme détaillé

Intitulé de l'unité

Unité 1 : Sécurité dans les réseaux

Intitulé du cours

Etude et mise en place d'un réseau IP de A à Z

Durée

7,5 heures

Objectifs

Maîtrise des notions, protocoles, architectures à la base de l'internet.

Contenu

1ère partie (1H30) : Etude de cas réalisés en séance par les étudiants après étude du cahier des charges communiqué au préalable.

Le cahier des charges présente le besoin d'une entreprise emménageant sur deux sites distants et devant mettre en place une architecture réseaux répondant à ses besoins. En plus des besoins réseaux et services une liste d'équipements à ré-utiliser est fournie.

2ème partie (3H00) : Mise en place de l'infrastructure et de l'architecture réseau définie par les étudiants suite à leur réponse au cahier des charges. L'ensemble du matériel est distribué aux étudiants et ceux-ci doivent se répartir en équipe pour réaliser les différentes parties du réseau de A à Z. Chaque équipe à la responsabilité d'un sous-ensemble du réseau et des équipements qui le constituent.

3ème partie (1H30) : Mise en place du routage statique sur l'architecture réseau réalisée. Chaque équipe définit et saisit dans le routeur qui lui est affecté la table de routage statique. Une fois le réseau global fonctionnel, les étudiants sont amenés à réaliser des pannes sur le réseau afin de voir les impacts/dysfonctionnements et

tenter de les solutionner. A l'issue de ces expérimentations les étudiants synthétisent les avantages et surtout les limites du routage statique.

4ème partie (1H30) : Mise en place du routage dynamique sur l'architecture réseau réalisée. Les étudiants rappellent les différents algorithmes de routage intra-domaine. Suivant le temps, un ou deux protocoles de routage dynamique seront mis en place. Chaque équipe définit et saisit les commandes appropriées dans le routeur qui lui est affecté. Une fois le réseau global fonctionnel, les étudiants sont amenés à réaliser une panne non corrigée par le routage statique afin d'observer cette fois sa correction et le temps pris par le protocole pour le faire (temps de convergence).

Tout au long de la séance, des présentations de schémas fonctionnels, des analyses protocolaires et des vérifications sont organisées aux différentes étapes clés par les étudiants qui présentent ensuite leur résultat et compréhension du sujet au reste du groupe. De nombreux tests de bon fonctionnement sont réalisés et ils amènent la résolution des pannes qui immanquablement apparaissent dans cette expérimentation.

Le professeur étant là pour guider les étudiants, leur rappeler les notions théoriques sous-jacentes ainsi que les méthodologies à suivre.

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

Programme détaillé

Intitulé de l'unité

Unité 1 : Sécurité dans les réseaux

Intitulé du cours

Sécurité VoIP

Durée

7,5 heures

Objectifs

Comprendre les spécificités et les contraintes des applications temps réels afin de maitriser l'ensemble des mécanismes, architectures et protocoles mis en place sur les réseaux IP nécessaire à leur bonne intégration, fonctionnement et protection. Cette acquisition se fait autour des services et applications voix avec un approfondissement spécifique sur la sécurité.

Contenu

Caractéristique de la voix et de son transport sur les réseaux

- Transport de flux temps réel sur les réseaux IP (RTP/RTCP) 1H30

- Signalisation de la voix sur IP (Focus SIP/SDP) 1H30 2/ Traversée des NAT et des Firewall

- Problématiques 1H30

- Solutions à base d'ALG 1H30

- Solutions à base de protocoles (STUN, TURN, ICE …) 1H30 3/ Sécurisation de la Voix sur IP et vulnérabilité de la Voix sur IP

- Problématiques et Solutions 1H30

- Sécurisation de la signalisation (SIPS, TLS ...)1H30

- Sécurisation du flux (IPSEC / SRTP, ZRTP ...) 1H30

Utilisation d'équipements physiques (hubs, routeurs, téléphones IP) / Utilisation de logiciels spécifiques (softphones IP) Utilisation de logiciels génériques (wireshark, putty, ...)

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

Programme détaillé

Intitulé de l'unité

Unité 4 : Sécurité des données et cryptographie

Intitulé du cours

Cryptographie symétrique

Durée

18 heures

Objectifs

1. Fournir une compréhension de base de l'histoire et des concepts de base de la cryptographie symétrique

2. Présenter les différents algorithmes de chiffrement symétrique couramment utilisés et les modes d'opération associés.

3. Discuter des mécanismes d'authentification et d'intégrité des données utilisés en conjonction avec la cryptographie symétrique.

4. Analyser les différentes attaques possibles contre les systèmes de chiffrement symétrique.

5. Présenter les dernières tendances et les perspectives d'avenir pour la cryptographie symétrique.

Contenu

1. Introduction à la cryptographie symétrique : histoire, concepts de base, types de chiffrement symétrique classiques

2. Cryptographie à clé secrète : principes de fonctionnement, exemples de systèmes (DES, 3DES, AES, Blowfish, etc.)

3. Modes d'opération : mode ECB, CBC, CFB, OFB, CTR, XTS, etc.

4. Authentification et intégrité des données : utilisation de codes de hachage, de signatures numériques, de macs

5. Cryptographie à clé secrète avancée : cryptographie de flux, cryptographie de blocs, cryptographie à sens unique

6. Attaques sur les systèmes de chiffrement symétrique : analyse différentielle, analyse linéaire, attaques par dictionnaire, cryptanalyse algébrique, etc.

7. Protection des mots de passe

8. Conclusion : résumé des concepts clés, perspectives d'avenir pour la cryptographie symétrique.

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

Programme détaillé

Intitulé de l'unité

Unité 4 : Sécurité des données et cryptographie

Intitulé du cours

Cryptographie asymétrique

Durée

18 heures

Objectifs

Présenter les éléments de base de la cryptographie à clé publique.

Contenu

On commence par présenter 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.

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

Programme détaillé

Intitulé de l'unité

Unité 4 : Sécurité des données et cryptographie

Intitulé du cours

Cryptographie appliquée

Durée

12 heures

Objectifs

Savoir mettre en application ses connaissances cryptographiques

Contenu

Ce module permet de revoir et d'appliquer les concepts fondamentaux de la cryptographie. Du chiffrement de fichier à l'établissement d'une connexion réseau sécurisée (ex. le protocole TLS) en passant par le stockage de mots de passe, toutes les propriétés cryptographiques y sont détaillées et justifiées à travers des exercices concrets en faisant appel à des logiciels comme la ligne de commande OpenSSL ou encore la bibliothèque cryptographique pycryptodome.

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

Programme détaillé

Intitulé de l'unité

Unité 3 : Sécurité organisationnelle

Intitulé du cours

Cycle de 4 conférences : Biométrie, technologie et droit ; Identité numérique ; Propriété intellectuelle dans le numérique ; Protection des données personnelles et RGPD

Durée

12 heures

Objectifs

Protection des données personnelles et RGPD : Sensibiliser aux situations impliquant des données personnelles et inculquer les premiers réflexes à avoir

Contenu

Protection des données personnelles et RGPD : 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.

Principes / Historique et évolution / Techniques biométriques / Encadrement juridique / Performances

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.

Exposer les principes de la biométrie, les différentes technologies, leurs usages et leurs limites

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

Programme détaillé

Intitulé de l'unité

Unité 3 : Sécurité organisationnelle

Intitulé du cours

Droit numérique & Principes RGPD

Durée

6 heures

Objectifs

Connaître les principaux principes Connaissance des infractions pénales relatives aux atteintes aux systèmes d'information

Maîtrise des obligations juridiques en matière de cybersécurité

Maîtrise les réflexes juridiques de la gestion de crise

Contenu

Appréhender les Notions clés : Cyberattaque, cybersécurité, cyberdéfense, données à caractère personnel, incident de sécurité, systèmes d'information et réseaux, système de traitement automatisé de données (STAD)

Présentation du cadre réglementaire lié à la cybersécurité

• Identifier les qualifications juridiques liées aux cyberattaques (obligations)

• Gérer les obligations afférentes aux obligations de notifications aux autorités de contrôle

o Réactions juridiques à la suite d'une cyberattaque

o Dépôt de plainte : éléments à rassembler

o Réparation des préjudices : points d'attention

o La cyber-assurance

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

Programme détaillé

Intitulé de l'unité

Unité 2 : Sécurité des systèmes d'information et des applications

Intitulé du cours

Editeur de texte axé programmation

Durée

3 heures

Objectifs

Apprendre un éditeur de programmation afin de gagner en efficacité lors des sessions de programmation, nombreuses dans le MS-SIS

Contenu

Exemples de cas concrets de mise en pratique d'édition de texte ou les commandes de l'éditeur permettent de gagner du temps par rapport à la même édition avec un simple éditeur de texte. Liste des commandes les plus utiles au quotidien pour un programmeur.

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

Programme détaillé

Intitulé de l'unité

Unité 1 : Sécurité dans les réseaux

Intitulé du cours

Firewalling

Durée

15 heures

Objectifs

Principe de ségrégation réseau

Principe théorique de la gestion d'état d'un firewall

Mise en oeuvre sous Linux d'un firewall netfilter avec iptables

Utilisation de nmap pour identifier les ports ouverts, fermés ou identifier l'OS de la cible et l'influence des règles de filtrage

Contenu

Après avoir présenté le filtrage de port et la notion de firewall à états, les étudiants mettent en oeuvre 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.

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

Programme détaillé

Intitulé de l'unité

Unité 4 : Sécurité des données et cryptographie

Intitulé du cours

Contexte de la cryptographie

Durée

6 heures

Objectifs

Faire un tour d'horizon complet du domaine de la cryptographie, en insistant sur les bases, sur l'actualité et les application en vue d'une bonne introduction aux autres cours

Contenu

Chiffrement, clé, fonctions de hachage, recherche exhaustive. Courte introduction au RSA, usage pour la distribution de clé et la signature, à l'échange de clé Diffie-Hellman et aux courbes elliptiques, ainsi que leur sécurité. Cartes à puce.

> 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), blockchains.

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

Programme détaillé

Intitulé de l'unité

Unité 3 : Sécurité organisationnelle

Intitulé du cours

Intelligence économique

Durée

12 heures

Objectifs

Etre à même de mieux appréhender les risques de fragilités humaines, complémentaires des fragilités informatiques dans une analyse de risque globale. Savoir cartographier et anticiper les menaces concurrentielles et leurs sources. Maîtriser les processus organisationnels généraux de protection du patrimoine des entreprises

Contenu

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.

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

Programme détaillé

Intitulé de l'unité

Unité 2 : Sécurité des systèmes d'information et des applications

Intitulé du cours

Initiation à l'assembleur x86

Durée

7,5 heures

Objectifs

Acquérir des bases suffisamment solides en assembleur pour aborder le module de rétro-conception, il se décompose pour cela en deux parties.

Contenu

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.

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

Programme détaillé

Intitulé de l'unité

Unité 2 : Sécurité des systèmes d'information et des applications

Intitulé du cours

Reverse Engineering x86

Durée

15 heures

Objectifs

Initier les étudiants au domaine du Reverse Engineering et au logiciel IDA Pro

Contenu

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.

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.

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)

esiea
INGÉNIEUR·E·S D'UN NUMÉRIQUE UTILE

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

Programme détaillé

Intitulé de l'unité

Unité 2 : Sécurité des systèmes d'information et des applications

Intitulé du cours

Programmation GPU

Durée

12 heures

Objectifs

At the end of this course, you will have learned the following :

* How to assess algorithmic complexity ;

* Heuristic solutions and their uses ;

* A schematic view of how CPU and GPU work ;

* How and what to profile ;

* How to write SIMD and GPU optimized functions.

Contenu

Introduction / rappel des objectifs / point de la situation des semi-conducteurs Rappels rapides sur la complexité algorithmique, notion de solutions approximatives Notions de cassage de mots de passe Architecture des CPUs, notions de ports d'exécution, micro-opérations, ordre d'exécution, pipe-lines, ...

TP -> optimiser un programme de cassage de mots de passe en C Instructions vectorielles (SIMD) TP -> écrire un casseur de mots de passe SIMD Fonctionnement des GPUs TP -> écrire un casseur de mots de passe GPU Récapitulatif sur les notions d'optimisation, profilage, etc.

80% du temps est censé être passé sur les TPs SIMD et GPU.

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

Programme détaillé

Intitulé de l'unité

Unité 3 : Sécurité organisationnelle

Intitulé du cours

Les critères communs

Durée

3 heures

Objectifs

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.

Contenu

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.

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

Programme détaillé

Intitulé de l'unité

Unité 3 : Sécurité organisationnelle

Intitulé du cours

OSINT ou le renseignement en sources ouvertes

Durée

12 heures

Objectifs

Méthodologie du cycle de renseignement

Mener une investigation en OSINT

Reconnaissance PENTEST

Reconnaissance Threat Intel

Contenu

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.

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

Programme détaillé

Intitulé de l'unité

Unité 1 : Sécurité dans les réseaux

Intitulé du cours

Historique d'internet

Durée

3 heures

Objectifs

Mesurer les évolutions d'Internet : de sa création à aujourd'hui

Posséder une culture générale sur le réseau internet

Contenu

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.

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

Programme détaillé

Intitulé de l'unité

Unité 3 : Sécurité organisationnelle

Intitulé du cours

Présentation des partenaires institutionnels : ANSSI, Ministère de la Défense, Ministère de l'Intérieur

Durée

9 heures

Objectifs

Faire connaître le fonctionnement d'institutions généralement peu communicantes sur leur fonctionnement interne afin que les futurs diplômés du MS-SIS puissent en toute connaissance de cause envisager des collaborations éventuelles avec ces entités.

Contenu

Des représentants de nos 3 partenaires institutionnels, incluant des anciens du MS-SIS, viennent présenter les missions de l'ANSSI ou des Ministères aux étudiants, qui auront peut-être à intéragir avec eux plus tard dans leur cadre professionnel, pour ainsi leur permettre de mieux cerner leur fonctionnement et leurs objectifs.

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

Programme détaillé

Intitulé de l'unité

Unité 2 : Sécurité des systèmes d'information et des applications

Intitulé du cours

Rappels Python

Durée

15 heures

Objectifs

Assimiler le code Python et écrire rapidement et efficacement des scripts dans ce langage.

Contenu

Algorithmie de bases

Création d'une API REST

Client QT

Utilisation d'une API

Utilisant des dataframes Pandas

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

Programme détaillé

Intitulé de l'unité

Unité 2 : Sécurité des systèmes d'information et des applications

Intitulé du cours

Programmation sécurisée

Durée

12 heures

Objectifs

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.

Contenu

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

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

Programme détaillé

Intitulé de l'unité

Unité 2 : Sécurité des systèmes d'information et des applications

Intitulé du cours

Recherche et exploitation de vulnérabilités sous Linux

Durée

24 heures

Objectifs

Parvenir à exploiter des vulnérabilités dans des programmes linux

Être capable de découvrir des vulnérabilité simples de type corruption de mémoire dans des programmes C

Contenu

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.

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

Programme détaillé

Intitulé de l'unité

Unité 2 : Sécurité des systèmes d'information et des applications

Intitulé du cours

Récupération de données et introduction au forensic

Durée

15 heures

Objectifs

Etre capable de reconnaitre les structures bas-niveau des systèmes de fichiers FAT12/16/32

Entêtes des formats de fichiers courants (MS Office, zip, jpg, gif...)

Etre en mesure de récupérer des fichiers effacés

Compréhension des difficultés pratiques du traitement de gros volume, des systèmes de fichiers NTFS, ext4.

Contenu

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.

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

Programme détaillé

Intitulé de l'unité

Unité 2 : Sécurité des systèmes d'information et des applications

Intitulé du cours

Rappels programmation C

Durée

18 heures

Objectifs

Assimiler le code C et écrire rapidement et efficacement dans ce langage.

Contenu

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.

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

Programme détaillé

Intitulé de l'unité

Unité 2 : Sécurité des systèmes d'information et des applications

Intitulé du cours

Rappels Linux

Durée

15 heures

Objectifs

Assimiler et utiliser de manière fluide le système d'exploitation Linux

Contenu

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 tâches 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.

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

Programme détaillé

Intitulé de l'unité

Unité 2 : Sécurité des systèmes d'information et des applications

Intitulé du cours

Rappels de Java

Durée

18 heures

Objectifs

Java fait partie des pré requis du MS-SIS mais les étudiants n'ayant pas la même aisance en programmation Java, le but de ce module est de s'assurer que tous les étudiants ont le niveau requis pour le démarrage de la formation.

Contenu

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 remémorer la mise en oeuvre de 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.

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

Programme détaillé

Intitulé de l'unité

Unité 1 : Sécurité dans les réseaux

Intitulé du cours

Rappels de réseaux

Durée

22,5 heures

Objectifs

Reprendre les bases du monde IP (modèles OSI et TCP/IP).

Contenu

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.

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

Programme détaillé

Intitulé de l'unité

Unité 1 : Sécurité dans les réseaux

Intitulé du cours

Scapy

Durée

12 heures

Objectifs

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

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).

Contenu

Scapy est ici utilisé à la fois comme outil pédagogique et comme outil à connaître.

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

Programme détaillé

Intitulé de l'unité

Unité 2 : Sécurité des systèmes d'information et des applications

Intitulé du cours

Communications Radio et Radio logicielle - SDR

Durée

15 heures

Objectifs

Se familiariser avec les outils et techniques permettant d'analyser la sécurité de radiocommunications

Assimiler les concepts théoriques relatifs aux problématiques de transmissions radiofréquence.

Contenu

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.

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.

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

Programme détaillé

Intitulé de l'unité

Unité 2 : Sécurité des systèmes d'information et des applications

Intitulé du cours

Sécurité Android

Durée

30 heures

Objectifs

Mettre en pratique les connaissances acquises sur des applications spécialement vulnérables, afin de recenser et exploiter l'ensemble des vulnérabilités présentes.

Contenu

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.

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

Programme détaillé

Intitulé de l'unité

Unité 4 : Sécurité des données et cryptographie

Intitulé du cours

Sécurité des mots de passe

Durée

7,5 heures

Objectifs

Comprendre les limites de sécurité d'objets du quotidien (Code de Luhn des cartes bancaires, verrou mecanique des portes, norme A2P des

serrures/clés...)

Réalité des compromissions des mots de passe https://haveibeenpwned.com/

Etre capable de retrouver les mots de passe (en clair ou sous forme chiffré) d'une configuration Cisco

Utiliser un multiboot grub pour contourner l'authentification Linux

Etre capable d'utiliser John THe Ripper pour attaquer des mots de passe chiffrés (des, lanman, NTLM...)

Contenu

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…).

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

Programme détaillé

Intitulé de l'unité

Unité 1 : Sécurité dans les réseaux

Intitulé du cours

Sécurité réseaux mobiles, télécom et gros réseaux d'infrastructures critiques

Durée

7,5 heures

Objectifs

a) Se familiariser avec l'infrastructure d'un réseau télécom

b) Comprendre les mécanismes mis en jeu lors de l'attachement et la mobilité d'un abonné, y compris en itinérance

c) Apprécier les vecteurs d'attaques possibles d'une telle infrastructure

Contenu

a/ Description de l'infrastructure d'un réseau cellulaire, et des mécanismes protocolaires permettant l'identification, l'authentification et la gestion de la mobilité d'un abonné mobile.

b/ Description de mécanismes pour l'établissement d'un appel, d'une session de données IP, et la transmission d'un SMS.

c/ Présentation des mécanismes de sécurité mis en oeuvre: authentification, chiffrement des transmissions radio, contrôle d'intégrité de la signalisation. Evolution de ces mécanismes d'une génération cellulaire à l'autre (2G, 3G, 4G...), et possibilités d'attaques (déni de service, écoute des transmissions, localisation d'abonnés, fraudes...).

d/ Description des mécanismes d'itinérance entre opérateurs, permettant aux abonnés de se connecter aux réseaux cellulaires du monde entier.

e/ Possibilité d'attaques sur les fournisseurs d'interconnexion : risques liés aux scénarios de déni de service, localisation, détournement d'appels, de sessions de données et de SMS d'abonnés.

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

Programme détaillé

Intitulé de l'unité

Unité 1 : Sécurité dans les réseaux

Intitulé du cours

Sécurité du Big Data

Durée

6 heures

Objectifs

Présenter l'écosystème Big Data et la révolution du concept de base de données.

Contenu

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.

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

Programme détaillé

Intitulé de l'unité

Unité 1 : Sécurité dans les réseaux

Intitulé du cours

Audit Web

Durée

7,5 heures

Objectifs

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.

Contenu

Apprendre à identifier les vecteurs d'attaque, les faiblesses et les impacts sur une Application Web et mettre en oeuvre un ensemble de contre-mesures pour se prémunir d'un ensemble d'attaques.

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).

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

Programme détaillé

Intitulé de l'unité

Unité 1 : Sécurité dans les réseaux

Intitulé du cours

Sécurité des grands réseaux

Durée

18 heures

Objectifs

* Comprendre les enjeux et algorithmes de routage dans les grands réseaux

* Comprendre la mise en œuvre des algorithmes de routage et leurs criticités (ISIS, BGP/MP_BGP, PIM, etc.) ainsi que les architectures de services (VPLS, VPN BGP/MPLS, etc.)

* Mettre en en œuvre des algorithmes de vérification des configurations réseaux

Contenu

* Cours magistral : Routage, théorie des graphes et applications dans les réseaux.

* Cours magistral : Réseaux multi-services, MPLS et services associés (protocole LDP, MPLS, etc.), services VPLS, VPN BGP/MPLS, etc.

* Cours magistral : Réseaux multi-services, éléments de sécurité, étude de calculs de périmètres de sécurité et préparation aux TPs

* Travaux dirigés : Codage de tests de sécurité sur des configurations CISCO, langages en awk, python, perl.

* Travaux dirigés : Codage de calcul de périmètres de sécurité sur des configurations CISCO (VPN BGP/MPLS, VLANS, BGP AS, IPSEC VPN), langages awk et sage (calcul sur les graphes)

* Travaux dirigés : Codage de tests de sécurité sur des gros volumes de configurations CISCO, langages C/FLEX

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

Programme détaillé

Intitulé de l'unité

Unité 2 : Sécurité des systèmes d'information et des applications

Intitulé du cours

Sécurité des systèmes embarqués

Durée

12 heures

Objectifs

Se familiariser avec les outils et techniques permettant d'analyser la sécurité de systèmes embarqués.

Assimiler les concepts théoriques relatifs aux problématiques de confiance au sein de systèmes embarqués face à des menaces considérant un accès physique à l'électronique.

Contenu

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.

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

Programme détaillé

Intitulé de l'unité

Unité 2 : Sécurité des systèmes d'information et des applications

Intitulé du cours

Sécurité iPhone/iOS

Durée

7,5 heures

Objectifs

* Appréhender les fonctions de sécurité du système d'exploitation iOS d'Apple.

* Se familiariser avec les outils et techniques permettant d'analyser la sécurité d'applications iOS.

* Identifier et analyser les fonctions de sécurité d'une application iOS.

Contenu

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.

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

Programme détaillé

Intitulé de l'unité

Unité 3 : Sécurité organisationnelle

Intitulé du cours

Sécurité organisationnelle et normes 2700X

Durée

12 heures

Objectifs

Réaliser des audits de conformité

Contenu

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.

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

Programme détaillé

Intitulé de l'unité

Unité 3 : Sécurité organisationnelle

Intitulé du cours

Crochetage de serrures

Durée

6 heures

Objectifs

Acquérir les techniques de crochetage et d'ouverture fine

Contenu

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.

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

Programme détaillé

Intitulé de l'unité

Unité 2 : Sécurité des systèmes d'information et des applications

Intitulé du cours

Sécurité SCADA

Durée

6 heures

Objectifs

Les objectifs du cours sont les suivants :

- Comprendre les spécificités des SI industriels et les différences par rapport aux SI bureautiques

- Découvrir les menaces qui pèsent sur ces environnement et comprendre les attaques

- S'initier aux standards de sécurisation et notamment l'IEC 62443

- Être capable d'interagir avec ces systèmes pour évaluer leur niveau de sécurité, via l'utilisation de protocoles spécifiques (Modbus, S7, OPC-UA) et les outils associés

Contenu

Afin de fournir aux étudiants 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.

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

Programme détaillé

Intitulé de l'unité

Unité 4 : Sécurité des données et cryptographie

Intitulé du cours

Stéganographie

Durée

7,5 heures

Objectifs

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.

Contenu

Introduction au vocabulaire de la stéganographie, formats d'images, détail du format JPEG, insertion LSB matching, introduction à la stéganalyse

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

Programme détaillé

Intitulé de l'unité

Unité 3 : Sécurité organisationnelle

Intitulé du cours

Gestion de risque

Durée

12 heures

Objectifs

Fournir aux étudiants des connaissances pour être en mesure d'aborder et de connaître les problèmes de continuité d'activité et de gestion des situations de crise

Contenu

• "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. "Severity Assessment Table"/Analyse d'impacts. 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 Continuité d'Activité PCA)":

Bilan d'Impacts sur Activité (BIA): activités, applications, services, ressources, fournisseurs/prestataires et compétences critiques. Indicateurs clefs : DMIA/RTO, PDMA/RPO, MTPD/tolérance. Dépendances informatiques amont/aval. Définition de

solutions palliatives. Critères de basculement en PCA. Mise en place du PCA. Tests et actualisation.

• "Plan de Secours Informatique (PSI)":

Conception d'un PSI, choix d'architecture et vulnérabilités résiduelles (sites actif/actif, actif/passif, liaisons synchrones/asynchrones, etc.). Critères d'activation du PSI.

Stratégies de sauvegarde. Gestion des problèmes de restauration, latence, consistance et resynchronisation des données.

• "Plan de Reprise d'Activité Industrielle PRAI)":

Problèmes types de l'informatique industrielle. Gestion des automates de production, maintenance et PRAI.

• "Plan de Repli Utilisateurs" :

Identification des besoins et stratégies de relocalisation. Segmentation des capacités de production et d'administration.

• "Résilience d'infrastructures informatiques" :

Identification des chaînes de liaison critiques et de leurs vulnérabilités. Identification de solutions d'accroissement de la résilience par la réduction des vulnérabilités et de leurs gravités, face aux risques de panne, d'erreur humaine, de malveillance, de cyber-attaque, de défaillance de fournisseurs, etc. Préparation de plans d'action hiérarchisés par priorité.

• Alignement des différents plans sur les exigences business.

• "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.

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

Programme détaillé

Intitulé de l'unité

Unité 1 : Sécurité dans les réseaux

Intitulé du cours

Suricata

Durée

12 heures

Objectifs

Connaissance de l'analyse de traffic réseau orienté sécurité et des systèmes de detections d'intrusion réseau.

Contenu

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.

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

Programme détaillé

Intitulé de l'unité

Unité 1 : Sécurité dans les réseaux

Intitulé du cours

Fonctionnement d'un Data Center

Durée

4,5 heures

Objectifs

Apprendre les bases sur l'agencement d'une salle serveurs

Etre capable de sélectionner un hébergement selon des critères de sécurité

Contenu

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...

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

Programme détaillé

Intitulé de l'unité

Unité 4 : Sécurité des données et cryptographie

Intitulé du cours

Malwares

Durée

12 heures

Objectifs

"- acquisition d'une culture générale sur l'origine et l'histoire de la virologie informatiques

- définir formellement la notion de virus informatique

- comparaison entre les virus biologiques et les virus informatiques

- réaliser un focus sur des virus ou vers spécifiques

- décrire l'évolution de la notion de virus à la notion de malwares

- définir les malwares et décrire une classification

- détailler les grandes familles de malwares

- décrire une approche bénéfique des techniques virales

- développer, déployer et contrôler un virus informatique"

Contenu

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.

- 1. History of computer viruses

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

Programme détaillé

Intitulé de l'unité

Unité 1 : Sécurité dans les réseaux

Intitulé du cours

Pentest Active Directory

Durée

12 heures

Objectifs

Découvrir l'Active Directory, apprendre ses mécanismes de sécurité et étudier ses faiblesses / attaques existantes

Contenu

1 - Qu'est-ce que l'Active Directory

• Présentation

• Architecture, composants et authentification • Gestion des accès • Administration

2 - Les attaques sur l'Active Directory • Les vulnérabilités connues • Les défauts de configuration • Cas réels rencontrés en pentest

3 - Les solutions de défenses et les Meilleures Pratiques • Durcissement de configuration • Surveillance

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

Programme détaillé

Intitulé de l'unité

Unité 2 : Sécurité des systèmes d'information et des applications

Intitulé du cours

Introduction à l'IA pour la sécurité

Durée

12 heures

Objectifs

Introduction au domaine de l'IA et à ses applications en sécurité. A la fin de ce module, les étudiants auront une

connaissance théorique des concepts et techniques fondamentaux de l'IA. Ils apprendront à implémenter ces

techniques sur des données synthétiques puis sur des jeux de données cyber. Ils seront sensibilisés aux avancées

récentes du domaine et aux défis actuels liés à l'application de l'IA à la sécurité des systèmes d'information.

Les compétences visées sont :

- Compréhension des concepts et techniques fondamentaux de l'IA, y compris l'apprentissage supervisé et

non supervisé, les arbres de décision et les réseaux de neurones.

- Application de techniques d'IA pour résoudre des problèmes de type sécurité:

- Familiarité avec les techniques de prétraitement des données, y compris la gestion des valeurs

manquantes, la normalisation et la sélection des features.

- Expérience pratique d’implémentation, évaluation et interprétation des performances d'un modèle.

Familiarité avec python et scikit-learn pour l’implémentation de modèles d'IA.

- Compréhension des limites et des défis de l'application de l'IA aux problèmes de sécurité : interprétabilité,

robustesse, expertise interdisciplinaire, éthique, confidentialité, passage à l’échelle, apprentissage continu.

Contenu

1. Machine Learning: définition, taxonomie, concepts

a. IA vs ML vs Data Science, historique

b. apprentissage supervisé, non-supervisé, par renforcement

c. classification,régression, clustering

d. nlp, computer vision, contrôle, apprentissage multimodal

e. prétraitement des données

f. entrainement, validation, test et mesure de performance

2. Classification

a. théorie : type de données, familles de modèles, mesures de performance

b. exercice : arbre de décision

c. tp : random forest sur NSL-KDD

3. Clustering

a. théorie : but, type de données, familles de modèles, mesures de performance

b. exercice : k-means

c. tp : k-means/dbscan sur NSL-KDD

4. Réseaux de neurones

a. théorie : couches, fonctions d’activation, backpropagation

b. architectures : feed-forward, RNN, CNN, GAN, transformers

c. avantages et inconvénients : data, calcul, complexité, interprétabilité, vulnérabilité

d. demo : feed-forward network sur NSL-KDD

5. Exemples d’interaction IA/sécurité

a. IA=opportunité : contrôle, analyse/découverte, sécurité physique/forensic

b. IA=risque : adversarial ML, model backdooring, dataset poisoning, captcha solver, deepfakes

c. IA=outil : style classification, document summarization, information retrieval, editing

6. Projet individuel : étude de cas

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

Programme détaillé

Intitulé de l'unité

Unité 2 : Sécurité des systèmes d'information et des applications

Intitulé du cours

La sécurité du noyau Linux

Durée

15 heures

Objectifs

Appréhender les mécanismes de protection du système"

"Apprendre la programmation noyau Linux"

"Comprendre et savoir utiliser un mécanisme de contrôle d'accès obligatoire"

"Comprendre l'architecture du système Linux"

"Comprendre des éléments spécifiques de protection système"

Contenu

"Sécurisation du démarrage du PC à l'accès par l'utilisateur"

"Le fonctionnement d'un système d'authentification et son intégration sur le système"

"Comprendre le fonctionnement des différents systèmes de fichiers"

"Étudier le fonctionnement d'un contrôle d'accès obligatoire : SELinux"

"Développement noyau Linux

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

Programme détaillé

Intitulé de l'unité

Unité 3 : Sécurité organisationnelle

Intitulé du cours

Cyber Threat Intelligence - CTI

Durée

12 heures

Objectifs

Comprendre ce qu'est la Threat Intel

Savoir suivre un groupe d'attaquant

Contenu

TTPs

Threact Actors

Matrice MITRE Att&ck

Plateforme Threat Intel: Yeti, MISP

Format d'echange

Signatures et detection

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

Programme détaillé

Intitulé de l'unité

Unité 4 : Sécurité des données et cryptographie

Intitulé du cours

Sécurité et Blockchain

Durée

7,5 heures

Objectifs

Ce cours commence par une introduction à la blockchain avec la découverte de l'architecture et du fonctionnement des deux blockchains les plus connues, Bitcoin et Ethereum.

Ensuite, les élèves, à travers un TP pratique, compilent et déploient un "smart contract" Ethereum sur le réseau de test.

Pour finir, nous analyserons des exemples de contrats vulnérables et discutons des impacts des vulnérabilités présentent.

Contenu

Le concept de Blockchain

- Introduction a Bitcoin

- Analyse de transactions Bitcoin

- Introduction a Ethereum

- Analyse de transactions Ethereum

- Fonctionnement des contrats intelligents

- Sécurité et type de vulnérabilités présentent dans des "smart contract"