IUT2 Université Grenoble Alpes

Département INFO

LICENCE PROFESSIONNELLE

METIERS DE L'INFORMATIQUE ADMINISTRATION ET SECURITE DES SYSTEMES ET DES RESEAUX (ASSR)

PROGRAMME DE LA FORMATION

TABLE DES MATIERES

UE0 : ENSEIGNEMENTS FONDAMENTAUX

EF1 : ALGORITHMIQUE – PROGRAMMATION EN PYTHON (24H)

Pré-requis : Quelques notions de programmation

Objectifs - Compétences minimales : Maîtrise des bases algorithmiques par la programmation en Python

Contenu :

- Le langage Python (syntaxe, types primitifs)
- Les techniques de programmation en Python (programmation impérative, utilisation des exceptions, modularisation du code)
- La bibliothèque standard de Python (manipulation de données textuelles)

Indications de mise en œuvre: Cours et Travaux pratiques. Le contenu dispensé sera adapté au niveau de chaque étudiant.

EF2 : BASES DE PHP (12H)

Pré-requis : aucun

Objectifs – Compétences minimales : Maîtrise des bases de programmation en PHP, mise en place d'un serveur web dynamique.

Contenu :

- Principaux concepts de HTML5, CSS3 et Javascript.
- Installation et configuration d'un serveur Web
- Introduction à PHP-7

Indications de mise en œuvre : Cours et Travaux pratiques, mise en place d'une machine virtuelle serveur web

EF3 : GESTION DE PROJETS (12H)

Pré-requis : aucun

Objectifs – Compétences minimales : sensibilisation aux enjeux et aux méthodes de la gestion de projets pour les mettre en pratique dans les projets réalisés pendant le temps de formation passé en entreprise.

Contenu : enjeux de la gestion de projets ; principales méthodes : gestion participative, méthodes agiles et notions de sprint-design, co-design et design de service ; outils de gestion de projets (Trello, Slack, Padlet, AirTable).

Indications de mise en œuvre : projet réalisé en groupe de 4 ou 5 étudiants.

EF4 : SYSTEME ET RESEAUX (18H)

Pré-requis : aucun

Objectifs – Compétences minimales : acquérir des notions pratiques sur les réseaux et l'administration de systèmes

Contenu :

Ethernet, IP, TCP, UDP, configuration réseau
administration d'ordinateurs sous les systèmes Windows et Linux, maîtrise du shell Unix, gestion des ressources d'un système.

Indications de mise en œuvre : Travaux pratiques sur machine virtuelle pour analyser des flux réseaux et configurer les paramètres IP et DNS d'un système Linux.

UE1 : MODULES « ENVIRONNEMENT » - ASSR

ASSR-ENV1 : L'ANGLAIS POUR LA SECURITE INFORMATIQUE (24H)

Pré-requis : Quelques connaissances et des compétences en anglais général et en anglais de spécialité en informatique.

Objectifs – Compétences minimales : connaissance et utilisations des outils linguistiques disponibles en ligne, autonomisation de l'apprentissage, mises en situation de compréhension et de production à l'oral et à l'écrit. Anglais de spécialité de l'informatique et de la sécurité.

Contenu : Un programme d'enseignement axé sur les compétences et sur les spécificités de l'anglais de spécialité de l'informatique.

Indications de mise en œuvre : Travail en collaboration axé sur des problèmes et des contenus réalistes. Exploitation de sites et de ressources sur l'informatique en anglais.

ASSR-ENV2 : ANALYSE DE RISQUES & MANAGEMENT DE LA SECURITE IT (24H)

Pré-requis : Aucun

Objectifs - Compétences minimales : Connaître les menaces extérieures et les moyens de s'en prémunir ; Garder les informations utiles à une enquête en cas de problème de sécurité ; Apprendre à trouver, hiérarchiser et classer les informations permettant de rester à jour dans le domaine de la sécurité ; Prendre conscience des composantes du système d'information à prendre en compte dans la gestion des risques Prendre conscience des avantages d'une méthode et des conditions du succès de sa mise en œuvre

Contenu : le management de la sécurité IT (Intelligence économique & Cybercriminalité ; Analyse des menaces / EBIOS ; Système de management de la sécurité de l'information / ISO 27001 ; Management des services IT / ITIL).

Indications de mise en œuvre : Application du cours sur la base d'études de cas.

ASSR-ENV3 : DROIT DES DONNEES, DE L'INTERNET ET DE LA SECURITE (18H)

Pré-requis : aucun

Objectifs – Compétences minimales : acquérir les notions de base en droit : Environnement juridique, principes et concepts élémentaires de droit. Gestion des risques juridiques et judiciaires liés à l'utilisation de l'Informatique et des réseaux dans les organisations.

Contenu :

- la protection des données personnelles et de la vie privée, applications de la LIL 1978-2004 et du secret des correspondances privées
- atteintes aux systèmes de traitement automatisés des données (STAD) : réglementation de la fraude informatique
- sécurité des systèmes informatiques et droit du travail : mise en place de la cybersurveillance
- droits de propriété intellectuelle et mesures techniques de protection
- Rédaction et validité des chartes informatiques

Indications de mise en œuvre : Cours/TD. : Le travail s'appuie sur des présentations préparées par les étudiants faisant l'objet d'une discussion et de compléments en cours et, donnant lieu à la réalisation de fiche de synthèse d'analyse risques et de définition des bonnes pratiques.

ASSR-ENV-4 : MATHEMATIQUES POUR LA SECURITE (18H)

Pré-requis : Quelques notions d'arithmétique (pgcd, modulo, division euclidienne)

Objectifs : acquérir des notions de base en cryptographie

Contenu :

- Rappels d'arithmétique
- Présentation de techniques de chiffrement d'hier et d'aujourd'hui (chiffrement à clé publique/ clé privée)
- Etude de la robustesse de ces chiffrements et étude des techniques classiques de cryptanalyse.

ASSR-ENV-5 : SEMINAIRES D'ENTREPRISE (6H)

Objectifs - Compétences minimales : Interventions courtes d'entreprises partenaires sur le thème d'administration et de la sécurité. Études de cas de problèmes de sécurité et les solutions apportées.

UE2 : MODULES « INFORMATIQUE-DEVELOPPEMENT » - ASSR

ASSR-MI1 : PROGRAMMATION EN LANGAGE C ET SECURITE(24H)

Pré-requis : module EF-1

Objectifs - Compétences minimales : Maîtriser la programmation d'une application écrite en langage C, comprendre les risques liés à certains bugs des programmes mal conçus, souvent exploités par les attaquants, par exemple pour prendre le contrôle d'une machine ou collecter des données.

Contenu :

- éléments de base du langage C et bibliothèques standards
- chaîne de compilation et makefile
- outil d'aide à la mise au point
- - bugs classiques liés à la mémoire et exploitation de ces derniers.

Indication de mise en œuvre : Travaux pratiques progressifs et exemples d'approfondissement liés à la sécurité

ASSR-MI2 : DEVELOPPEMENT WEB EN PHP (24H)

Pré-requis : modules EF-1, EF-2.

Objectifs - Compétences minimales : Compétences minimales : Installation et configuration d'un serveur Web/PHP. Maîtriser la programmation objet en PHP5 pour accéder à une base de données depuis un serveur web. Structurer son code selon le schéma Modèle-Vue-Contrôleur (MVC).

Contenu :

- Particularisation de la programmation WEB, langage objet PHP-7
- Lien entre une base de données et un serveur web (couche PDO).
- Structuration de code selon le schéma Modèle-Vue-Contrôleur (MVC)
- Authentification et session de navigation sur une application web
- Étude des failles classiques vis-à-vis du code PHP, et comment les éviter.

Indications de mise en œuvre : Développement d'une petite application (base de données + site web avec gestion d'utilisateurs)

ASSR-MI3 : TESTS ET QUALITE DES LOGICIELS (18H)

Objectifs - Compétences minimales : Comprendre les besoins de qualité logicielle, maîtriser les concepts de gestion de version et de tests (en pratique, git et pytest).

Contenu :

- Objectifs conflictuels de qualité, compromis faits en pratique
- Traçabilité des logiciels, gestion de version
- Différents types de tests, importance de la non régression, intégration continue
- Programmation par contrat, test-driven development
- Contrôle d'environnement logiciel, intérêt des approches descriptives

Indications de mise en œuvre : Cours, Travaux Pratiques, Mini-projet.

ASSR-MI4 : ARCHITECTURE DEVOPS (24H)

Pré-requis : modules EF, MI3- Tests et qualité des logiciels

Objectifs - Compétences minimales : Maîtriser les architectures et les outils de déploiement des applications en continu.

Contenu :

- Principes, vocabulaire de DevOps, relations avec les méthodes agiles, le Lean et l'IT Service Management
- Conteneurisation d'applications, gestion d'applications conteneurisées
- Automatisation du cycle de vie d'une application

Indications de mise en œuvre : Cours et Travaux pratiques, réalisation d'un mini-projet.

ASSR-MI5: PROGRAMMATION RESEAUX EN LANGAGE PYTHON (24H)

Prérequis : module EF-1.

Objectifs - Compétences minimales : Maîtrise de la programmation objet en Python et des librairies réseaux

Contenu :

- Les techniques de programmation objet en Python
- La bibliothèque standard de Python pour la programmation réseaux

Indications de mise en œuvre: Cours et Travaux pratiques, réalisation d'un mini-projet.

UE3 : MODULES « INFORMATIQUE - ADMINISTRATION » - ASSR

ASSR-ADMIN1 : ADMINISTRATION UNIX (24H)

Pré-requis : EF-4, notions de shell

Objectifs – Compétences minimales : installer un système, personnaliser et configurer une installation, utiliser les commandes de base et les commandes d'administration.

Contenu :

- Panorama des systèmes Unix et des distributions Linux
- Choix et tests du matériel
- Bonne utilisation du compte root
- Gestion de packages
- Gestion des utilisateurs
- SSH
- PGP/GnuPG
- Gestion des disques (partitions, gestionnaire de volumes, RAID, SGF)
- Processus de boot

Indications de mise en œuvre :

- Le cours porte sur les systèmes Linux, MacOS X, *BSD. Les TP font une mise en œuvre sur Linux et les distributions Debian GNU/Linux et Ubuntu.
- Shell bash
- Virtualisation Qemu/KVM

ASSR-ADMIN2 : ADMINISTRATION LINUX (18H)

Pré-requis : administration Unix

Objectifs - Compétences minimales : vérifier et améliorer la sécurité d'un système Linux, installer des logiciels provenant de multiples canaux

Contenu :

- Gestion du noyau
- Suivi et correction des failles de sécurité
- Installation de logiciels et backports
- Mise à jour de version de distribution
- Durcissement d'un système

Indications de mise en œuvre : Distributions Debian GNU/Linux et Ubuntu, utilitaires spécifiques pour suivre la sécurité du système.

ASSR-ADMIN3 : ADMINISTRATION WINDOWS (30H)

Pré-requis : aucun

Objectifs – Compétences minimales : L'objectif est d'acquérir les compétences et connaissances nécessaires pour mettre en œuvre une infrastructure Windows dans un environnement d'entreprise.

Contenu :

- Installation et réinstallation de postes clients Windows, sécurisation et protection (antivirus, sécurisation des média, blocage de fonctionnalités utilisateurs, ...).
- Premiers pas de la gestion centralisée sous Windows, déploiement et maintenance.
- Paramétrage d'un contrôleur de domaine.
- Tâches d'administration courante de Windows Server 2019 telles que la gestion des utilisateurs et des groupes, ou l'accès réseau.
- Planification du déploiement initial des services Windows Server 2019.
- Installation des rôles et fonctionnalités avec le tableau de bord.
- Transformation d'un serveur graphique en serveur Core et inversement.
- Introduction au Powershell.
- Configuration du DNS.
- Gestion des services de domaines Active Directory.
- Gestion des comptes d'utilisateurs et de service et mise en œuvre de l'infrastructure de stratégie de groupe.
- Mise en œuvre de la protection d'accès réseau.
- Optimisation des services de fichiers avec DFS.
- Mise en œuvre de la gestion des mises à jour avec WSUS.
- Surveillance de Windows Server 2019.
- Introduction à Azure et aux services Office 365.

Indications de mise en œuvre : Cours et TD/TP

ASSR-ADMIN4 : ADMINISTRATION DE PARCS HETEROGENES (24H)

Pré-requis : connaissances de l'administration de base des systèmes d'exploitations (ASSR-ADMIN1 à 3)

Objectifs - Compétences minimales : L'intérêt de l'hétérogénéité au sein d'une entité ne doit pas se faire au détriment de la sécurité, de l'intégration et de l'expérience de l'utilisateur final. Le but de ce module est de comprendre les bases de l'hétérogénéité dans un réseau d'entreprise et de pouvoir réaliser une intégration harmonieuse de ces différents matériels et systèmes d'exploitation.

Contenu :

- Intégration dans une infrastructure mixte
- Gestion des utilisateurs : comprendre les mécanismes mis en œuvre dans un environnement hétérogène pour réaliser les correspondances d'utilisateur entre les systèmes
- Gestion d'annuaires LDAP
- Gestion des données sur le réseau (disque partagés, services, NAS, cloud)
- Impression, sauvegarde et restauration
- Accès et prise en main à distance (SSH, VNC, RDP, x2go…)
- Utilisation des tablettes/téléphones dans un réseau d'entreprise

Indications de mise en œuvre : Cours et TD/TP

ASSR-ADMIN5 : FAILLES LOGICIELLES (18H)

Pré-requis : Techniques fondamentales de programmation, Concepts des OS, Notions élémentaires de sécurité.

Objectifs : Connaître les différents types de failles logicielles et leurs exploitations, comment les combler et les prévenir. Comment concevoir/dimensionner un logiciel/système pour limiter les attaques et les défauts.

Contenu :

1. Classification des failles avec des cas d'exploitations.
2. Explications détaillées (avec démonstration) de quelques-unes des failles les plus emblématiques (buffer overflow, injection sql ...).
3. Techniques de programmations pour combler et prévenir les failles.
4. Architectures d'applications pour limiter les impacts.
5. Tests préventifs (tests unitaires aux limites et fuzzing).

Indications de mise en œuvre : Cours et TD/TP

UE4 : MODULES «SECURITE» - ASSR

ASSR-SECU1 : RESEAUX SECURISES (24H)

Pré-requis : notions fondamentales des sécurités : réseaux locaux, TCP/IP.

Objectifs - Compétences minimales : Maîtrise des notions fondamentales des réseaux sécurisés pour les réseaux locaux Ethernet et TCP/IP.

Contenu :

Notions avancées :

- Fonctionnement des réseaux locaux : Ethernet, wifi, etc.
- Protocoles : ARP, TCP/IP, UDP, IPv6.

Sécurité des réseaux :

- Faiblesses des réseaux et contres-mesures : principales failles protocolaires,
- Principes et usage du chiffrement : WEP/WPA, IPSec, SSH, SSL, VPN,
- Filtrage : Firewall, détection d'intrusion

Indications de mise en œuvre : Cours et Travaux pratiques.

ASSR-SECU2 : TESTS DE VULNERABILITE ET DE PENETRATION (18H)

Pré-requis : Aucun

Objectifs - Compétences minimales : Savoir mettre en œuvre des tests de vulnérabilité et un audit d'une infrastructure : outils de tests (scripts PHP, SQL, ...), validation et certification, outils d'audit (Nessus)

Indications de mise en œuvre : Cours/TP

ASSR-SECU3 : GESTION DES INCIDENTS ET SI DE LA SECURITE (30H)

Pré-requis : Réseaux sécurisés (ASSR-SECU1)

Objectifs - Compétences minimales : Maîtriser et comprendre les techniques pour la supervision des systèmes et des réseaux : administration SNMP, outils de supervision, remontée d'alertes.

Capacité à traiter et gérer les incidents de sécurité : collecte / analyse des alertes systèmes & envoi des demandes d'intervention (centre d'appel sortant). Connaissance de l'architecture d'un système de gestion d'alarmes. Création d'un scénario d'alarme. Sécurité renforcée (auto diagnostic).

Contenu :

Partie théorique « supervision » :

- Le modèle FCAPS, le protocole SNMP, la MIB.
- Les types de fournisseurs de solution de supervision, l'offre Open Source, les "Big Four", les "Small Four".
- Les fonctions attendues d'un outil de supervision, les étapes d'un projet de supervision.
- Les fonctions attendues d'un outil de gestion de performance.

Partie pratique « supervision » :

- Installation de l'agent SNMP sur Windows, sécurisation de l'agent SNMP : v3 only, Netsnmp + agent SNMP Windows en mode proxy.
- Installation du serveur virtuel centreon, ajout d'un host + installation de l'agent NSClient++, tests du service centreon windows sans agent + avec agent SNMP + avec agent NSClient.
- Installation du serveur virtuel OpenNMS, corrélation + déduplication des alarmes avec OpenNMS.
- Notification de Centreon vers OpenNMS, tests service OpenNMS windows sans agent + avec agent SNMP + avec agent nagios
- Installation du serveur virtuel Ossim + découverte du réseau + scan de vulnérabilité
- Partie « gestion des alarmes » :
- Description d'un système de diffusion d'alarmes, découverte des protocoles d'acquisition (Snmp, OPC, Modbus, BACNet ...) et des protocoles télécom (SIP, ESPA, SMPP ...).
- Notion de scénario d'alarme et modélisation d'une astreinte.
- Mise en place d'une acquisition SNMP, Modbus et OPC. Établissement d'appels en SIP, SMTP et gsm (SMS et voix). Élaboration de scénarios d'alarmes.

Indications de mise en œuvre : Cours/TD/TP, études de cas, plateforme expérimentale.

ASSR-SECU4 : INFRASTRUCTURE D'AUTHENTIFICATION (18H)

Pré-requis : Aucun

Objectifs - Compétences minimales :

- Comprendre le fonctionnement des principales méthodes d'authentification,
- Comprendre les différentes méthodes de gestion des autorisations,
- Savoir mettre en œuvre une infrastructure pour l'authentification
- Savoir sécuriser les échanges à l'aide de certificats

Contenu

- Rappels / Introduction : stéganographie, cryptographie : chiffrements de César, Vigenère, chiffrement symétrique, asymétrique et hybride, fonctions de hachage, signature, mise en pratique (openssl, SSH)
- Infrastructure de clef publique (PKI) : principes, implémentation d'une mini PKI à l'aide de openssl
- Certificats, Tiers de confiance : principes, mise en pratique (Openssl, sécurisation d'un serveur Apache)
- Méthodes d'authentification : Basique, LDAP, Radius, Certificats (NAC), Tokens, Kerberos
- Méthodes d'autorisation : OAuth
- SSO : Kerberos, CAS, Open ID
- Fédération d'identité : SAML

Indications de mise en œuvre : Cours/TD.
Les TDs seront l'opportunité d'utiliser des infrastructures Cloud lorsque possible ainsi que de mettre en pratique les outils de sécurité les plus connus relatifs aux méthodes d'authentification (brute force, auth. bypass, MITM…).

ASSR-SECU5 : ANALYSE DE LA SECURITE ET DE LA VIE PRIVEE LIEES AU WI-FI (18H)

Pré-requis : Réseaux sécurisés (ASSR-SECU1)

Objectifs - Compétences minimales : Ce module s'intéresse à plusieurs facettes de la sécurité et du respect de la vie privée au sein des réseaux, avec une orientation très pratique. Nous aborderons en particulier les risques associés aux réseaux Wi-Fi aux objets connectés : les attaques sur les systèmes de chiffrement (WEP, WPA), les attaques de type "evil-twin" et les fuites de données personnelles sur les canaux radio. Nous nous intéresserons également aux risques associés aux applications mobiles, en particulier sous l'angle de la vie privée (attaques Man-in-the-middle, applications indiscrètes, modèle de sécurité).

Contenu :

- Mécanismes de base de Wi-Fi et des protocoles de sécurité (WEP, WPA)
- Technologies Bluetooth et BLE pour les objets connectés
- Capture de trafic Wi-Fi et observation des failles de sécurité
- Simulation de l'attaque d'un réseau sécurisé (WEP, WPA) par injection de trafic
- Applications mobiles et vie privée

Indications de mise en œuvre : Cours et TD/TP avec utilisation d'une plate-forme expérimentale dédiée.

ASSR-SECU6 : SECURISATION DES ARCHITECTURES D'HEBERGEMENT (18H)

Pré-requis : ASRR- ADMIN1 et ASSR-ADMIN2

Objectifs - Compétences minimales : Maîtriser la sécurisation des architectures d'hébergement de services :

- architectures pour la sécurité : firewall, DMZ, proxy, filtres ;
- infrastructure de lutte contre la compromission des flux : serveurs de réparation, anti-virus, anti-spam
- répartition de charge : utilisation du "cloud" pour prendre en charge les pics de trafic

Indications de mise en œuvre : Cours/TP