

Intitulé de l'UE	Sécurité informatique 1
Section(s)	- (6 ECTS) Master en Sciences de l'Ingénieur industriel / Finalité Informatique / Cycle 2 Bloc 1 option Réseaux et Sécurité - (6 ECTS) Master en Sciences de l'Ingénieur industriel / Finalité Informatique / Cycle 2 Bloc 1 option Réseaux et Sécurité - Passerelle

Responsable(s)	Heures	Période
Jean-Sébastien LERAT	60	Quad 1

Activités d'apprentissage	Heures	Enseignant(s)
Introduction à la sécurité informatique : exercices	15h	Jean-Sébastien LERAT
Introduction à la sécurité informatique : théorie	30h	Jean-Sébastien LERAT
Virtualisation et protection des applications	15h	Jean-Sébastien LERAT

Prérequis	Corequis

Répartition des heures
Introduction à la sécurité informatique : exercices : 15h de travaux
Introduction à la sécurité informatique : théorie : 30h de théorie
Virtualisation et protection des applications : 10h de théorie, 5h d'exercices/laboratoires

Langue d'enseignement
Introduction à la sécurité informatique : exercices : Français
Introduction à la sécurité informatique : théorie : Français
Virtualisation et protection des applications : Français

Connaissances et compétences préalables
Maîtrise de la programmation C
Notions de systèmes d'exploitation

Objectifs par rapport au référentiel de compétences ARES
Cette UE contribue au développement des compétences suivantes

- Master en Sciences de l'ingénieur industriel :

- Identifier, conceptualiser et résoudre des problèmes complexes
 - Intégrer les savoirs scientifiques et technologiques afin de faire face à la diversité et à la complexité des problèmes rencontrés
 - Modéliser, calculer et dimensionner des systèmes
- S'intégrer et contribuer au développement de son milieu professionnel
 - Évaluer les coûts et la rentabilité de son projet
- Entreprendre et innover, dans le cadre de projets personnels ou par l'initiative et l'implication au sein de l'entreprise
 - S'impliquer dans la politique d'amélioration de la qualité
- Communiquer face à un public de spécialistes ou de non-spécialistes, dans des contextes nationaux et internationaux
 - Maîtriser les méthodes et les moyens de communication en les adaptant aux contextes et aux publics
- S'engager dans une démarche de développement professionnel
 - Réaliser une veille technologique dans sa sphère d'expertise

- Master en Sciences de l'ingénieur industriel en Informatique :

- Analyser, concevoir, implémenter et maintenir des systèmes informatiques logiciels et matériels
 - Analyser l'existant, identifier les besoins, les formaliser et appliquer la méthodologie adéquate (cascade, agile, ...) et les techniques de modélisation (Entité/Association, UML, ...).
 - Maîtriser et mettre en oeuvre les techniques de sécurité logicielle et matérielle (cryptologie, architectures d'authentifications, ...)
 - Maîtriser, optimiser et administrer les systèmes d'exploitation.

Acquis d'apprentissage spécifiques

- Énumérer et décrire les différentes vulnérabilités vues au cours
- Expliquer et illustrer le fonctionnement des vulnérabilités vues au cours
- Énumérer et décrire les différentes contre mesures et bonnes pratiques de programmation vues au cours
- Expliquer et illustrer le fonctionnement des contres mesures et bonnes pratiques vues au cours
- Évaluer et critiquer la sécurité mise en place dans un système informatique
- Énumérer et décrire les différentes notions vues au cours (Virtualisation & Cloud-Computing)
- Expliquer et illustrer le fonctionnement des différents concepts vus au cours (Virtualisation & Cloud-Computing)
- Évaluer et critiquer la mise en place d'un système de Virtualisation et/ou de Cloud-Computing
- Utiliser des outils de gestion de virtualisation et de Cloud-Computing
- Mettre en place un système de Cloud-Computing
- Concevoir et implémenter une implémentation personnalisée de Virtualisation (KVM)
- Dimensionner et optimiser l'utilisation de composants virtuels
- Sécuriser une infrastructure de Cloud-Computing
- Sécuriser un système de virtualisation

Contenu de l'AA Introduction à la sécurité informatique : exercices

- Principe d'exécution de programmes : pile, allocation, tas, ...
 - Shellcode (injection de code) et techniques d'exploitation :
1. buffer/heap overflow, formatage des chaînes de caractères, ...
 2. network sniffing
 3. Denial of Service
 4. TCP/IP hijack
 5. port scanning
 6. hameçonnage
 7. Cassage de mots de passe
- Contre-mesures
 - Programmation sécurisée :
1. Initialisation sûre
 2. Contrôle d'accès
 3. Validation des entrées
 4. Implication de la cryptographie
 5. Authentification
 6. L'aléatoire
 7. Anti-tampering

- Droits utilisateurs et groupes
- Etude de cas : application WEB (injection SQL, XSS, CSRF, HTTP, Random, upload de fichier, htaccess, session ...) et programmes d'exemples

Contenu de l'AA Introduction à la sécurité informatique : théorie

- crf. théorie

Contenu de l'AA Virtualisation et protection des applications

- Notion : virtualisation, hyperviseur, machine virtuelle
- Gestion des composants virtuels : CPU, mémoire vive, stockage, réseau, périphériques
- Disponibilité et applications de la virtualisation
- KVM : principe et fonctionnement, installation, gestion, commandes et déploiement, stockage et réseau, template et snapshot
- Cycle de vie d'une machine virtuelle
- Outils de gestion : Kimchi, vSwitch, oVirt
- Performances : CPU, mémoire vive, pages du kernel (noyau), Numa, stockage et clock (horloge)
- Cloud computing : notions et mécanismes
- Modèles de services et qualité
- Migration de machines virtuelles
- Cloud privé avec OpenStack
- Sécurité du cloud et des applications

Méthodes d'enseignement

Introduction à la sécurité informatique : exercices : cours magistral, approche par projets, approche avec TIC, utilisation de logiciels

Introduction à la sécurité informatique : théorie : cours magistral, approche par projets, approche avec TIC, utilisation de logiciels

Virtualisation et protection des applications : cours magistral, approche par projets, approche avec TIC, utilisation de logiciels

Supports

Introduction à la sécurité informatique : exercices : copies des présentations

Introduction à la sécurité informatique : théorie : copies des présentations

Virtualisation et protection des applications : copies des présentations

Ressources bibliographiques de l'AA Introduction à la sécurité informatique : exercices

Erickson, J. (2008). *Hacking, 2nd Edition: The Art of Exploitation*. No Starch Press

Viega, J. & Messier, M. (2003). *Secure Programming Cookbook for C and C++: Recipes for Cryptography, Authentication, Input Validation & More*. O'Reilly Media

Cannings, R., Zane Lackey, H.D.R.C., Dwivedi, H. & Lackey, Z. (2008). *Hacking sur le Web 2.0: Vulnérabilité du Web 2.0 et sécurisation*. Pearson

Goupille, P.A. (2008). *Technologie des ordinateurs et des réseaux - 8e éd.: Cours et exercices corrigés*. Dunod

Stallings, W. (2013). *Computer Organization and Architecture: International Edition*. Pearson Education Limited

Ressources bibliographiques de l'AA Introduction à la sécurité informatique : théorie

Erickson, J. (2008). *Hacking, 2nd Edition: The Art of Exploitation*. No Starch Press

Viega, J. & Messier, M. (2003). *Secure Programming Cookbook for C and C++: Recipes for Cryptography, Authentication, Input Validation & More*. O'Reilly Media

Cannings, R., Zane Lackey, H.D.R.C., Dwivedi, H. & Lackey, Z. (2008). *Hacking sur le Web 2.0: Vulnérabilité du Web 2.0 et sécurisation*. Pearson

Goupille, P.A. (2008). *Technologie des ordinateurs et des réseaux - 8e éd.: Cours et exercices corrigés*. Dunod

Stallings, W. (2013). *Computer Organization and Architecture: International Edition*. Pearson Education Limited

Ressources bibliographiques de l'AA Virtualisation et protection des applications

Bellovin, S. M. (2015). *Thinking security: Stopping next year's hackers*. Addison-Wesley Professional.

Chiramal, H. D., Mukhedkar, P., & Vettathu, A. (2016). *Mastering kvm virtualization*. Packt Publishing.

Erl, T., Puttini, R., & Mahmood, Z. (2013). *Cloud computing: Concepts, technology & architecture (the prentice hall service technology series from thomas erl)*. Prentice Hall.

Hsu, T. (2018). *Hands-on security in devops: Ensure continuous security, deployment, and delivery with devsecops*. Packt Publishing.

Kalsi, T. (2018). *Securing applications on the cloud*. Packt Publishing. Portnoy, M. (2016). *Virtualization essentials, 2nd edition*. Sybex.

Évaluations et pondérations

Évaluation	Note globale à l'UE
Langue(s) d'évaluation	Français, Anglais
Méthode d'évaluation	<p>La note d'UE est calculée sur base des notes aux AA.</p> <p>20% de travaux et d'évaluation continue, 80% examen oral (En cas d'examen à distance, une partie préliminaire pratique peut être demandée à l'étudiant afin de personnaliser l'examen). Dans la note, l'évaluation de la présentation de vulgarisation d'un article scientifique en cybersécurité est reprise.</p> <p>Les supports de cours sont anglais mais le cours est enseigné en Français.</p> <p><u>Attention</u> : les étudiants de l'option doivent réaliser un travail dans le cadre des AA "Introduction à la sécurité informatique" et le présenter. Les étudiants présents (non-Erasmus+) s'entraîneront également afin de participer au Cybersecurity Challenge (CSC, https://www.cybersecuritychallenge.be/). Cela signifie qu'ils s'engagent à y participer durant le second quadrimestre. Les étudiants qui doivent réaliser un stage doivent contacter le responsable de stage afin d'intégrer la participation au CSC dans la convention de stage.</p>

Report de note d'une année à l'autre pour l'AA réussie en cas d'échec à l'UE

Introduction à la sécurité informatique : exercices : **non**
Introduction à la sécurité informatique : théorie : **non**
Virtualisation et protection des applications : **non**

Année académique : **2020 - 2021**