HEH be Sciences et technologies

8a avenue Maistriau
7000 Mons

www.heh.be

Intitulé de l'UE	**Cybersécurité 2**
Section(s)	- **(2 ECTS)** Master en Sciences de l'Ingénieur industriel / Finalité Informatique / Cycle 2 Bloc 1

Responsable(s)	Heures	Période
Olivier CORTISSE	30	**Quad 2**

Activités d'apprentissage	Heures	Enseignant(s)
Projet en cybersécurité (CSC)	21h	**Olivier CORTISSE**
Sécurité des systèmes	9h	**Olivier CORTISSE**

Prérequis	Corequis

Répartition des heures
Projet en cybersécurité (CSC) : 21h de travaux
Sécurité des systèmes : 4h de théorie, 5h d'exercices/laboratoires

Langue d'enseignement
Projet en cybersécurité (CSC) : Français
Sécurité des systèmes : 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
  - Concevoir, développer et améliorer des produits, processus et systèmes techniques
  - Modéliser, calculer et dimensionner des systèmes

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

Objectifs de développement durable

Education de qualité
Objectif 4 Assurer l'accès de tous à une éducation de qualité, sur un pied d'égalité, et promouvoir les possibilités d'apprentissage tout au long de la vie

- 4.3 D'ici à 2030, faire en sorte que les femmes et les hommes aient tous accès dans des conditions d'égalité à un enseignement technique, professionnel ou tertiaire, y compris universitaire, de qualité et d'un coût abordable.
- 4.4 D'ici à 2030, augmenter considérablement le nombre de jeunes et d'adultes disposant des compétences, notamment techniques et professionnelles, nécessaires à l'emploi, à l'obtention d'un travail décent et à l'entrepreneuriat.
- 4.7 D'ici à 2030, faire en sorte que tous les élèves acquièrent les connaissances et compétences nécessaires pour promouvoir le développement durable, notamment par l'éducation en faveur du développement et de modes de vie durables, des droits de l'homme, de l'égalité des sexes, de la promotion d'une culture de paix et de non-violence, de la citoyenneté mondiale et de l'appréciation de la diversité culturelle et de la contribution de la culture au développement durable.

Egalité entre les sexes
Objectif 5 Parvenir à l'égalité des sexes et autonomiser toutes les femmes et les filles

- 5.2 Éliminer de la vie publique et de la vie privée toutes les formes de violence faite aux femmes et aux filles, y compris la traite et l'exploitation sexuelle et d'autres types d'exploitation.

Energie propre et d'un coût abordable
Objectif 7 Garantir l'accès de tous à des services énergétiques fiables, durables et modernes, à un coût abordable

- 7.1 D'ici à 2030, garantir l'accès de tous à des services énergétiques fiables et modernes, à un coût abordable.
- 7.2 D'ici à 2030, accroître nettement la part de l'énergie renouvelable dans le bouquet énergétique mondial.
- 7.3 D'ici à 2030, multiplier par deux le taux mondial d'amélioration de l'efficacité énergétique.

industrie, innovation et infrastructure
Objectif 9 Bâtir une infrastructure résiliente, promouvoir une industrialisation durable qui profite à tous et encourager l'innovation

- 9.1 Mettre en place une infrastructure de qualité, fiable, durable et résiliente, y compris une infrastructure régionale et transfrontière, pour favoriser le développement économique et le bien-être de l'être humain, en mettant l'accent sur un accès universel, à un coût abordable et dans des conditions d'équité.
- 9.2 Promouvoir une industrialisation durable qui profite à tous et, d'ici à 2030, augmenter nettement la contribution de l'industrie à l'emploi et au produit intérieur brut, en fonction du contexte national, et la multiplier par deux dans les pays les moins avancés.

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 bonnnes pratiques vues au cours

- Évaluer et critiquer la sécurité mise en place dans un système informatique
- Sécuriser un système de virtualisation

Contenu de l'AA Projet en cybersécurité (CSC)
Participation au Cybersecurity Challenge (CSC, https://www.cybersecuritychallenge.be/)

Contenu de l'AA Sécurité des systèmes
Règles de bonne pratique en sécurité et cybersécurité

Méthodes d'enseignement
Projet en cybersécurité (CSC) : cours magistral, approche par projets, étude de cas, utilisation de logiciels
Sécurité des systèmes : cours magistral, approche par projets, étude de cas, utilisation de logiciels

Supports
Projet en cybersécurité (CSC) : copies des présentations
Sécurité des systèmes : copies des présentations, syllabus, notes de cours

Ressources bibliographiques de l'AA Projet en cybersécurité (CSC)

- 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 Sécurité des systèmes

- 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

Évaluations et pondérations	
Évaluation	Note globale à l'UE
Langue(s) d'évaluation	Français
Méthode d'évaluation	La note d'UE est calculée sur base des notes aux AA. 20% de travaux et d'évaluation continue, 80% examen oral Les 20% de travaux et d'évaluation continue correspondent à la manière dont l'étudiant s'implique dans la réalisation des exercices présentés en cours ainsi qu'à la réalisation d'une tâche de vulgarisation scientifique (présentation orale, rédaction d'article, diffusion par les médias) en lien avec la sécurité informatique. Les supports de cours peuvent être en anglais, mais le cours est enseigné en Français. Attention : 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 signifient 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.
Report de note d'une année à l'autre pour l'AA réussie en cas d'échec à l'UE	
Projet en cybersécurité (CSC) : **oui** Sécurité des systèmes : **oui**	

Année académique : **2023 - 2024**