8a avenue Maistriau
7000 Mons

www.heh.be

Intitulé de l'UE	Complément en sécurité des réseaux
Section(s)	- **(4 ECTS)** Master en Sciences de l'Ingénieur industriel / orientation Informatique / Cycle 2 Bloc 1 option Réseaux et Sécurité - **(4 ECTS)** Master en Sciences de l'Ingénieur industriel / orientation Informatique / Cycle 2 Bloc 1 option Réseaux et Sécurité - Passerelle

Responsable(s)	Heures	Période
Olivier CORTISSE	44	**Quad 2**

Activités d'apprentissage	Heures	Enseignant(s)
Hacking et Forensic	20h	**Olivier CORTISSE**
Problématique de la criminalité numérique	24h	**Olivier CORTISSE**

Prérequis	Corequis
- Réseaux et systèmes informatiques 1 - Réseaux et systèmes informatiques 2	- Sécurité informatique 1

Répartition des heures
Hacking et Forensic : 8h de théorie, 12h d'exercices/laboratoires
Problématique de la criminalité numérique : 10h de théorie, 14h d'exercices/laboratoires

Langue d'enseignement
Hacking et Forensic : Français
Problématique de la criminalité numérique : Français

Connaissances et compétences préalables

- Connaissances générales des systèmes d'exploitations LINUX et Windows
- Connaissances de base des réseaux de communication

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
  - Analyser des produits, processus et performances, de systèmes techniques nouveaux et innovants
  - Concevoir, développer et améliorer des produits, processus et systèmes techniques

- Modéliser, calculer et dimensionner des systèmes
- Sélectionner et exploiter les logiciels et outils conceptuels les plus appropriés pour résoudre une tâche spécifique

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

- Analyser, concevoir, implémenter et maintenir des systèmes informatiques logiciels et matériels
  - Concevoir et mettre en oeuvre une architecture réseaux (physique ou virtualisée) sécurisée et en assurer la maintenance et la supervision.
  - Maîtriser et mettre en oeuvre les techniques de sécurité logicielle et matérielle (cryptologie, architectures d'authentifications, …)

Objectifs de développement durable (rubrique optionnelle pour l'année académique 2022-2023)

Aucun

Acquis d'apprentissage spécifiques

- identifier les points forts et les faiblesses en matière de sécurité des systèmes informatiques
- expliquer les problèmes liés à la criminalité numérique et exposer les principes fondamentaux utilisés pour lutter contre celle-ci
- mettre en oeuvre les méthodes actuelles de sécurité

Contenu de l'AA Hacking et Forensic

Théorie :

- Débogage sous Windows
- Fuzzing
- Forensic
- Contre-mesures techniques

Laboratoires :

- Outils de hacking (Python et Scapy)
- Recherche d'informations
- Prendre le rôle administrateur ou système
- Cryptage et CryptoLocker
- Extraire, casser, changer un mot de passe
- Outrepasser les restrictions logicielles
- Prendre le contrôle à distance
- Garder une porte ouverte
- Se cacher et effacer ses traces

Contenu de l'AA Problématique de la criminalité numérique

Théorie :

- Méthodologie d'une attaque
- Éléments d'ingénierie sociale
- Les failles physiques

- Les failles (réseaux, web, systèmes, applicatives)
- Les failles matérielles
- Prise d'empreinte ou Information Gathering
- Fuzzing
- Risques juridiques et solutions

Laboratoires :

- Outils de hacking (Python et Scapy)
- Distribution Kali Linux

Méthodes d'enseignement
Hacking et Forensic : cours magistral, travaux de groupes, approche par projets, étude de cas, utilisation de logiciels
Problématique de la criminalité numérique : cours magistral, travaux de groupes, approche par projets, étude de cas, utilisation de logiciels

Supports
Hacking et Forensic : copies des présentations, syllabus, notes de cours, protocoles de laboratoires, activités sur eCampus
Problématique de la criminalité numérique : copies des présentations, syllabus, notes de cours, protocoles de laboratoires, activités sur eCampus

Ressources bibliographiques de l'AA Hacking et Forensic

- « Sécurité informatique et réseaux. » Solange Ghernaouti-Hélie (Dunod)
- « Sécurité des systèmes d'information et des réseaux. » Raymond Panko (Pearson Education)
- « Sécuriser un réseau Linux. » Boutherin et Delaunay (Eyrolles)
- « Authentification réseau avec Radius.» Serge Bordères (Eyrolles)

Ressources bibliographiques de l'AA Problématique de la criminalité numérique

- « Sécurité informatique et réseaux. » Solange Ghernaouti-Hélie (Dunod)
- « Sécurité des systèmes d'information et des réseaux. » Raymond Panko (Pearson Education)
- « Sécuriser un réseau Linux. » Boutherin et Delaunay (Eyrolles)
- « Authentification réseau avec Radius.» Serge Bordères (Eyrolles)

Évaluations et pondérations	
Évaluation	Note globale à l'UE
Langue(s) d'évaluation	Français
Méthode d'évaluation	* présentation orale du projet (30 %) * travaux/rapports (20 %) * projet (50 %)

Report de note d'une année à l'autre pour l'AA réussie en cas d'échec à l'UE
Hacking et Forensic : **oui** Problématique de la criminalité numérique : **oui**

Année académique : **2022 - 2023**