Année académique 2024 - 2025 Département des Sciences, des Technologies et du Vivant

Bachelier en informatique orientation technologie de l'informatique

HELHa Tournai - Frinoise Rue Frinoise 12 7500 TOURNAI
Tél : +32 (0) 69 89 05 60 Fax : +32 (0) 69 89 05 65 Mail : tech.tournai@helha.be

1. Identification de l'Unité d'Enseignement

UE3101 Sécurité Informatique			
Ancien Code	TEIC3B01	Caractère	Obligatoire
Nouveau Code	XIIT3010		
Bloc	3B	Quadrimestre(s)	Q1
Crédits ECTS	2 C	Volume horaire	36 h
Coordonnées des **responsables** et des intervenants dans l'UE	**Emmanuel WILFART** (emmanuel.wilfart@helha.be)		
Coefficient de pondération		2	
Cycle et niveau du Cadre Francophone de Certification		bachelier / niveau 6 du CFC	
Langue d'enseignement et d'évaluation		Français	

2. Présentation

Introduction

Combattre la cybercriminalité, le cyberespionnage et les autres menaces qui visent les réseaux ne sont que quelques exemples de carrières qu'offre la cybersécurité dans tous les secteurs d'activité. Au travers de cet UE, l'étudiant développera les compétences nécessaires pour se lancer dans ce domaine en pleine évolution et saisir des opportunités dans les centres opérationnels de sécurité. Faites du monde un endroit plus sûr en exerçant dans ce domaine.

Contribution au profil d'enseignement (cf. référentiel de compétences)

Cette Unité d'Enseignement contribue au développement des compétences et capacités suivantes :

Compétence 1 **Communiquer et informer**
- 1.4 Utiliser le vocabulaire adéquat

Compétence 2 **Collaborer à la conception, à l'amélioration et au développement de projets**
- 2.1 Elaborer une méthodologie de travail
- 2.2 Planifier des activités et évaluer la charge et la durée de travail liées à une tâche
- 2.3 Analyser une situation donnée sous ses aspects techniques et scientifiques
- 2.4 Rechercher et utiliser les ressources adéquates
- 2.5 Proposer des solutions qui tiennent compte des contraintes

Compétence 3 **S'engager dans une démarche de développement professionnel**
- 3.1 Prendre en compte les aspects éthiques et déontologiques

Compétence 4 **S'inscrire dans une démarche de respect des réglementations**
- 4.3 Respecter les prescrits légaux relatifs au contexte dans lequel s'exerce l'activité (exemple code du bien-être au travail, RGPD, le droit à l'image, licences logiciels ...)

Acquis d'apprentissage visés

Approfondir les connaissances qui vous aident à mieux détecter les incidents liés à la sécurité et à y réagir.
Acquérir des compétences professionnelles pratiques dans le domaine de la cybersécurité.
Développer un esprit critique et des compétences en matière de résolution des problèmes en utilisant des équipements réels et Cisco Packet Tracer.

Liens avec d'autres UE

Prérequis pour cette UE : aucun

Corequis pour cette UE : aucun

3. Description des activités d'apprentissage

Cette unité d'enseignement comprend l(es) activité(s) d'apprentissage suivante(s) :

TEIC3B01A	Cybersécurité et sécurité	36 h / 2 C

Les descriptions détaillées des différentes activités d'apprentissage sont reprises dans les fiches descriptives jointes.

4. Modalités d'évaluation

Les 2 points attribués dans cette UE sont répartis entre les différentes activités de la manière suivante :

TEIC3B01A	Cybersécurité et sécurité	2

Les formes d'évaluation et les dispositions complémentaires particulières des différentes activités d'apprentissage sont reprises dans les fiches descriptives jointes.

Dispositions complémentaires relatives à l'UE

D’autres modalités d’évaluation peuvent être prévues en fonction du parcours académique de l'étudiant. Celles-ci seront alors consignées dans un contrat didactique spécifique proposé par le responsable de l’UE, validé par la direction ou son délégué et signé par l’étudiant pour accord.

Référence au RGE

En cas de force majeure, une modification éventuelle en cours d’année peut être faite en accord avec le Directeur de département, et notifiée par écrit aux étudiants. (article 66 du règlement général des études 2024-2025).

Année académique 2024-2025 Département des Sciences, des Technologies et du Vivant

Bachelier en informatique orientation technologie de l'informatique

HELHa Tournai - Frinoise Rue Frinoise 12 7500 TOURNAI
Tél : +32 (0) 69 89 05 60 Fax : +32 (0) 69 89 05 65 Mail : tech.tournai@helha.be

1. Identification de l'activité d'apprentissage

Cybersécurité et sécurité			
Ancien Code	24_TEIC3B01A	Caractère	Obligatoire
Nouveau Code	TIIT3011		
Bloc	3B	Quadrimestre(s)	Q1
Crédits ECTS	2 C	Volume horaire	36 h
Coordonnées du **Titulaire** de l'activité et des intervenants	**Emmanuel WILFART** (emmanuel.wilfart@helha.be)		
Coefficient de pondération		2	
Langue d'enseignement et d'évaluation		Français	

2. Présentation

Introduction

Combattre la cybercriminalité, le cyberespionnage et les autres menaces qui visent les réseaux ne sont que quelques exemples de carrières qu'offre la cybersécurité dans tous les secteurs d'activité. Développer les compétences nécessaires pour vous lancer dans ce domaine en pleine évolution. Faire du monde un endroit plus sûr en exerçant dans ce domaine.

Objectifs / Acquis d'apprentissage

Agir en professionnel éthique et responsable

Etre capable de détecter les faiblesses dans un environnement informatique et d'apporter les correctifs nécessaires.

Connaître les techniques utilisées par les Hacker pour mieux s'en protéger

Identifier les types d'attaque qu'une infrastructure informatique peut subir

Mettre en oeuvre des équipements de sécurité sur une infrastructure réseau

3. Description des activités d'apprentissage

Contenu

- Qu'est ce que la cybersécurité et l'Ethical Hacking
- La triade CIA
- Législations
- Modèle OSI et la sécurité sur toutes les couches
- La sécurité en couche 2
- Bonne pratiques de protections
- La cybersécurité et les framework
- Les surfaces d'attaque
- Les reconnaissances actives et passives
- Les outils de découverte
- Les recherches de vulnérabilité
- Exploitation des vulnérabilités

Démarches d'apprentissage

Chaque chapitre comprend une partie théorique, complétée par des exemples de manipulation.
Grâce aux ateliers, les étudiants peuvent mettre directement en pratique la théorie vue et donc autonomiser les démarches à réaliser par rapport aux différentes notions.

Dispositifs d'aide à la réussite

Séances plénières permettant aux étudiants d’acter et/ou corriger et/ou approuver l'étude, les recherches et les manipulations effectuées

Sources et références

Powerpoint

Cours Cisco CCNA Cybersecurity.

Cours Fortinet NSE1 et NSE2.

Utilisation du framework Metasploit.

Supports en ligne

Les supports en ligne et indispensables pour acquérir les compétences requises sont :

Support de cours en ligne Cisco

Support de cours en ligne Fortinet

Support de cours interne PowerPoint

4. Modalités d'évaluation

Principe

Évaluation finale: examen mixte, pratique et théorique (oral + écrit).
Cette évaluation sera pondérée par le taux de présence en classe.

L'examen comprend une évaluation théorique des connaissances mais comprendra aussi un test de pénétration sur du matériel physique existant.

Pondérations

	Q1		Q2		Q3	
	Modalités	%	Modalités	%	Modalités	%
production journalière						
Période d'évaluation	Exm	100			Exm	100

Exm = Examen mixte

La pondération de cette activité d'apprentissage au sein de l'UE dont elle fait partie vaut 2

Dispositions complémentaires

La présence aux activités d'apprentissages (cours) est obligatoire.
Un certificat médical entraîne, au cours de la même session, la représentation d’une épreuve similaire (dans la mesure des possibilités d’organisation).
En cas d'échec, la production journalière est conservée
Cette évaluation sera pondérée par le taux de présence en classe.

Référence au RGE

En cas de force majeure, une modification éventuelle en cours d’année peut être faite en accord avec le Directeur de département, et notifiée par écrit aux étudiants. (article 66 du règlement général des études 2024-2025).