8a avenue Maistriau
7000 Mons

www.heh.be

Intitulé de l'UE	Cybersécurité 1
Section(s)	- **(4 ECTS)** Bachelier en Informatique et Systèmes orientation Réseaux et Télécommunications / Cycle 1 Bloc 2 option Sécurité

Responsable(s)	Heures	Période
Denis MANDOUX	45	**Quad 2**

Activités d'apprentissage	Heures	Enseignant(s)
Cybersécurité - théorie	20h	**Denis MANDOUX**
Cybersécurité - travaux pratiques	25h	**Denis MANDOUX**

Prérequis	Corequis

Répartition des heures
Cybersécurité - théorie : 20h de théorie
Cybersécurité - travaux pratiques : 25h d'exercices/laboratoires

Langue d'enseignement
Cybersécurité - théorie : Français, Anglais
Cybersécurité - travaux pratiques : Français, Anglais

Connaissances et compétences préalables

- Aucun prérequis n'est nécessaire, il est cependant fortement recommandé d'avoir réussi l'unité d'enseignement "Télécommunications et réseaux".

Objectifs par rapport aux acquis d'apprentissage programme (AAP)
Cette UE contribue au développement de la/des compétence(s) suivante(s)

- Communiquer et informer
- Collaborer à la conception, à l'amélioration et au développement de projets techniques
- S'engager dans une démarche de développement professionnel
- S'inscrire dans une démarche de respect des réglementations
- Collaborer à l'analyse et à la mise en œuvre d'un système informatique
- Intégrer des solutions télécoms sécurisées autour des réseaux locaux en y incluant la qualité de service

Acquis d'apprentissage de l'UE:

A l'issue des activités d'apprentissage les apprenants doivent être capable de :

- Connaitre et expliquer les concepts essentiels relatifs à la cybersécurité.
- Situer différents éléments de sécurisation dans un environnement IT et expliquer leur(s) fonction(s).
- Adopter une approche proactive dans la mise en oeuvre de solution de sécurité.
- Renforcer la sécurité des différents plans fonctionnels de routeurs et commutateurs.
    - Sécurité physique, sécurisation des accès (SSH, niveaux de privilèges), authentification des mises à jour de routage, sécurité des ports, private VLAN, Listes de contrôle d'accès, DHCP snooping, Dynamic ARP Inspection, IP Source Guard, ...
- Configurer diverses fonctionnalités d'un UTM (Unified Threat Management).
    - Configuration de base (gestion des comptes, logs, accès administratifs, ...)
    - Configuration des règles de pare-feu.
    - Configuration du proxy
    - Configuration du NAT
    - Configuration du routage
    - Configuration de l'antivirus
    - Configuration du filtrage Web
    - Configuration du contrôle d'application
- Respecter les normes, méthodologies et règles de bonne pratique liés à la fonction d'administrateur réseau/sécurité.

Contenu de l'AA Cybersécurité - théorie

Le contenu de l'activité est principalement basée sur :

- Les notions de base sur la cybersécurité.
- Les principaux équipements de sécurité rencontré dans un réseau local.
- Les menaces sur les réseaux IT modernes.
- La sécurisation de routeurs et commutateurs.
- La sécurisation périphérique d'un réseau (Routeurs filtrants et UTM).

Contenu de l'AA Cybersécurité - travaux pratiques

Projet de mise en oeuvre et de sécurisation d'un interréseau sur matériel physique

- Conception d'un réseau composé d'un site central et de plusieurs agences.
- Configuration des différents équipements afin de disposer d'un réseau fonctionnel.
- Sécurisation des périphériques réseau du site central et des agences.
- Configuration d'un UTM pour la sécurité périmétrique du réseau
- Documentation du réseau.

Méthodes d'enseignement

Cybersécurité - théorie : cours magistral, approche par projets

Cybersécurité - travaux pratiques : approche par projets

Supports

Cybersécurité - théorie : copies des présentations

Cybersécurité - travaux pratiques :

Ressources bibliographiques de l'AA Cybersécurité - théorie

- Copies de présentations, Mandoux D. *Cybersécurité*, HEH Campus Technique, année académique 2017-18.
- Fortinet, Inc., *FortiOS™ Handbook - System Administration VERSION 5.4.0*, http://docs.fortinet.com/uploaded/files/3337/fortigate-system-administration-54.pdf, 2015.
- Fortinet, Inc., *FortiOS™ Handbook - Firewall VERSION 5.4.3*, http://docs.fortinet.com/uploaded/files/3095/fortigate-firewall-54.pdf, pp. 28-51, 2017.
- Fortinet, Inc., *FortiOS™ Handbook - Security Profiles VERSION 5.4.0*, http://docs.fortinet.com/uploaded/files/2810/fortigate-security-profiles-540.pdf, pp. 38-45, 2017.
- O. Santos, J. Stuppi, *CCNA Security 210-260 Official Cert Guide*, Cisco Press, septembre 2015.
- Cisco System Inc, *Cisco Guide to Harden Cisco IOS Devices*, [en ligne] http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html, page consultée le 10 janvier 2017.

Ressources bibliographiques de l'AA Cybersécurité - travaux pratiques

- Cisco System Inc, *Cisco Guide to Harden Cisco IOS Devices*, [en ligne] http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html, page consultée le 10 janvier 2017.
- Fortinet, Inc., *FortiOS™ Handbook - System Administration VERSION 5.4.0*, http://docs.fortinet.com/uploaded/files/3337/fortigate-system-administration-54.pdf, 2015.
- Fortinet, Inc., *FortiOS™ Handbook - Firewall VERSION 5.4.3*, http://docs.fortinet.com/uploaded/files/3095/fortigate-firewall-54.pdf, 2017.
- O. Santos, J. Stuppi, *CCNA Security 210-260 Official Cert Guide*, Cisco Press, septembre 2015.

Évaluations et pondérations	
Évaluation	Épreuve intégrée
Langue(s) d'évaluation	Français, Anglais
Méthode d'évaluation	Examen oral 70% Autre 30% (non remédiable en 2e session) Evaluation continue, réalisation et présentation du projet pendant les séances de TP Un système de bonifications permet aux étudiants qui ont prouvé leurs connaissances et compétences lors des activités d'apprentissage de bénéficier de bonus pouvant aller jusqu'à 10% de la note globale. Les détails sont disponibles sur la plate-forme e-learning.

Année académique : **2018 - 2019**