Université du Québec en Outaouais **Département d'informatique et d'ingénierie**

Sigle : CYB1003 Gr. 01
Titre : Introduction à la cybersécurité
Session : Été 2023 **Horaire et local**
Professeur : Bouhaddi, Myria

1. Description du cours paraissant à l'annuaire :

Objectifs

Au terme de ce cours, l'étudiant.e sera en mesure de comprendre les défis et enjeux de la cybersécurité et différentes approches permettant de relever ces défis.

Contenu

Définitions et concepts de base de la cybersécurité: triade CID (équilibre entre confidentialité, intégrité et disponibilité). Évolutions du cyberespace (interconnectivité des systèmes, actifs dans le cyberespace, aspects physiques et risques associés). Vulnérabilités logicielles et exploitation. Cadres de référence en cybersécurité (CIS, NIST-CSF, etc.). Moyens de protection (conception sécurisée du cyberespace, analyse, surveillance, contrôle, test, etc.). Sauvegarde et protection des données. Encodage et cryptographie. Cybermenaces, cyberattaques, gestion d'incidents, gouvernance et éthique en cybersécurité. Résolution de problèmes de cybersécurité, issus du monde réel, pour atténuer les cybermenaces.

Descriptif – Annuaire

2. Objectifs spécifiques du cours :

L'objectif de cette activité est que l'étudiante ou l'étudiant soit capable de comprendre de manière globale et cohérente le domaine de la cybersécurité, et qu'il ou elle soit au courant des enjeux, des problèmes et des solutions techniques présentés dans la littérature.

3. Stratégies pédagogiques :

Les séances de cours seront présentées sous forme magistrales, parsemées d'exercices de compréhension. Le matériel pédagogique est accessible à partir de la plateforme Moodle dédiée au cours. Un forum de discussion sera aussi disponible pour poser des questions liées à la matière enseignée.

Des travaux dirigés et pratiques seront également réalisés afin de consolider les concepts présentés durant les séances de cours.

4. Heures de disponibilité ou modalités pour rendez-vous :

Communication par courriel (myria.bouhaddi@uqo.ca) et via le forum de discussion.

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	Introduction et concepts de base • Enjeux et menaces • Objectifs de la sécurité informatique	26 juin 2023
2	Cryptographie • Historique • Cryptographie classique : mono et poly alphabétique	28 juin 2023
3	Cryptanalyse de la cryptographie classique • Historique • Classification des attaques • Cryptanalyse par recherche de clés • Cryptanalyse par analyse de fréquence	03 juil. 2023

	• **Travail dirigé 1 : 04 juillet 2023**	
4	Cryptographie moderne : symétrique et asymétrique **Travail dirigé 2 : 07 juillet 2023**	05 juil. 2023
5	Les protocoles de communication • Introduction à la réseautique • Protocoles TCP/IP **Travail pratique 1 : 11 juillet 2023**	10 juil. 2023
6	Systèmes de détection d'intrusion • Approches pour la détection d'intrusion • NIDS et HIDS • Outils pour la détection d'intrusion **Révisions pour l'examen de mi-session**	12 juil. 2023
7	**Examen de mi-session**	17 juil. 2023
8	Vulnérabilités des systèmes • Types de vulnérabilités • Techniques d'exploitation des vulnérabilités Cadres de référence en cybersécurité (CIS, NIST-CSF, etc.) Éthique en cybersécurité. **Travail pratique 2 : 21 juillet 2023**	19 juil. 2023
9	Systèmes pare-feux (*Firewalls*) • Principe de conception des pare-feu (*firewall*) • Configuration d'un pare-feu • Règles de filtrage • Architecture de sécurisation par pare-feu • Le « *proxy* » **Travail pratique 3 : 25 juillet 2023**	24 juil. 2023

10	Gestion de la sécurité informatique et analyse du risque
	
	• Analyse de structures organisationnelles
	• Gestion de risque
	• Méthodes d'analyse de risque
	  ○ La méthode Octave
	  ○ La méthode Mehari
	
	Travail pratique 4 : 28 juillet 2023
		26 juil. 2023

11	Les réseaux privés virtuels (VPN) • Principe de fonctionnement des VPN : *Tunneling*, routage, filtrage • Protocoles : IPsec, etc. • Mise en œuvre d'un VPN **Travail pratique 5 : 01 août 2023**	31 juil. 2023
12	Systèmes de contrôle d'accès • Architecture de contrôle d'accès • Modèles de contrôle d'accès : DAC, MAC, RBAC, etc. **Travail pratique 6 : 04 août 2023**	02 août 2023
13	Virologie informatique • Contexte et historique • Taxonomie d'infections • Cycle de vie d'un virus • Mécanismes d'infection • Techniques anti-virales	07 août 2023
14	**Examen final**	09 août 2023

6. Évaluation du cours :

L'évaluation est l'appréciation du niveau d'apprentissage atteint par l'étudiant(e) par rapport aux objectifs des cours et des programmes.

Dans le cas spécifique du cours **Introduction à la cybersécurité**, l'attribution des notes se fera selon la répartition suivante :

- **Examen de mi-session : 30 %**
- **Examen final : 40 %**
- **Travail de session : 30 %**

Une moyenne inférieure à 50 % aux examens est éliminatoire et conduit automatiquement à un échec.

7. Politiques départementales et institutionnelles :

- Politique du département d'informatique et d'ingénierie relative à la tenue des examens
- Note sur le plagiat et sur la fraude
- Politique relative à la qualité de l'expression française écrite chez les étudiants et les étudiantes de premier cycle à l'UQO
- Absence aux examens : cadre de gestion, demande de reprise d'examen (formulaire)

La communauté universitaire s'engage à lutter contre les inconduites, le harcèlement et les violences à caractère sexuel. Dénonçons toute forme de violence.
Ensemble, accomplissons un pas de plus en complétant la formation obligatoire en ligne : "La banalisation des violences à caractère sexuel".

uqo.ca/bimi/formation-obligatoire

Pour de plus amples renseignements consultez :

bimi@uqo.ca

UQO
BUREAU D'INTERVENTION EN MATIÈRE D'INCONDUITE

8. Principales références :

1. Marion AGÉ, Franck EBEL, Raphaël RAULT, Sébastien BAUDRU, Robert CROCFER, David PUCHE, Jérôme HENNECART, Sébastien LASSON , « Sécurité informatique, Ethical Hacking », ISBN : 978-2-7460-6248-1, ENI; Édition : 2e édition, 2011
2. Michael T. Goodrich. Roberto Tamassia, "Introduction to computer security", ISBN-10 : 0-321-51294-4, Pearson Education, 2011
3. Raymond Panko, « Sécurité des systèmes d'information et des réseaux », ISBN : 2-7440-7054-8, Pearson Education, (version traduite de l'anglais), 2004
4. Charles P. Pfleeger, Shari Lawrence Pfleeger, "Security in Computing", ISBN-10 : 0-13-035548-8, Prentice Hall, Third Edition, December 02, 2002
5. William Stallings, "Network Security Essentials: Applications and Standards", ISBN : 0132380331, Prentice Hall; 3rd Edition (July 19, 2006)
6. Dieter Gollmann, "Computer Security", ISBN : 0470862939, John Wiley & Sons; 2nd Edition (January 18, 2006)
7. Raymond Panko, "Corporate Computer and Network Security",ISBN : 0130384712, Prentice Hall; United States Edition (March 17, 2003)
8. Matt Bishop, "Introduction to Computer Security", ISBN : 0-321-24744-2, Addison-Wesley, 3rd Edition (October 2006)

9. Page Web du cours :

http://moodle.uqo.ca