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

Sigle : CYB1003 Gr. 01
Titre : Introduction à la cybersécurité
Session : Automne 2024 Horaire et local
Professeure : Moudoud, Hajar

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 (hajar.moudoud@uqo.ca) et via le forum de discussion.
Période de consultation flexible (lundi au vendredi) sur rendez-vous seulement (prévoir 48 heures d'avance pour la prise de rendez-vous).

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	03 sep. 2024
2	Cryptographie • Historique • Cryptographie classique : mono et poly alphabétique	10 sep. 2024
3	Cryptanalyse de la cryptographie classique • Historique • Classification des attaques	17 sep. 2024

	• Cryptanalyse par recherche de clés • Cryptanalyse par analyse de fréquence **Travail dirigé 1 : 16,18 et 20 septembre**	
4	Cryptographie moderne : symétrique et asymétrique	24 sep. 2024
5	Les protocoles de communication • Introduction à la réseautique • Protocoles TCP/IP **Travail dirigé 2 : 30 septembre, 2 et 4 octobre**	01 oct. 2024
6	Systèmes de détection d'intrusion • Approches pour la détection d'intrusion • NIDS et HIDS • Outils pour la détection d'intrusion **Travail dirigé 3 : 07, 09 et 11 octobre** **Révisions pour l'examen de mi-session**	08 oct. 2024
7	Semaine d'études	15 oct. 2024
8	**Examen de mi-session**	22 oct. 2024
9	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 1 : 28, 30 octobre et 01 novembre**	29 oct. 2024
10	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 2 : 04, 06 et 08 novembre**	05 nov. 2024

11	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 3 : 11, 13 et 15 novembre
		12 nov. 2024

12	Les réseaux privés virtuels (VPN) • Principe de fonctionnement des VPN : *Tunneling*, routage, filtrage • Protocoles : IPsec, etc. • Mise en œuvre d'un VPN **Travail pratique 4 : 18, 20 et 22 novembre**	19 nov. 2024
13	Systèmes de contrôle d'accès • Architecture de contrôle d'accès • Modèles de contrôle d'accès : DAC, MAC, RBAC, etc. **Travail pratique 5 : 25, 27 et 29 novembre**	26 nov. 2024
14	Virologie informatique • Contexte et historique • Taxonomie d'infections • Cycle de vie d'un virus • Mécanismes d'infection Techniques anti-virales **Révisions pour l'examen final**	03 déc. 2024
15	**Examen final**	10 déc. 2024

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 :

- Politiques relatives à la tenue des examens
- Note sur le plagiat et les fraudes
- 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)

Tolérance ZÉRO en matière de violence à caractère sexuel.

Le Bureau d'intervention et de prévention en matière de harcèlement (BIPH) a pour mission d'accueillir, soutenir et guider toute personne vivant une situation de harcèlement, de discrimination ou de violence à caractère sexuel. Le BIPH oriente ses actions afin de prévenir les violences à caractère sexuel pour que nous puissions étudier, travailler et s'épanouir dans un milieu sain et sécuritaire.

Vous vivez ou êtes une personne témoin d'une situation de violence à caractère sexuel ? Vous êtes une personne membre de la communauté étudiante ou une personne membre du personnel, autant à Gatineau qu'à Ripon et St-Jérôme, l'équipe du BIPH est là pour vous, sans jugement et en toute confidentialité.

Ensemble, participons à une culture de respect.

Pour de plus amples renseignements consultez UQO.ca/biph ou écrivez-nous au Biph@uqo.ca

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