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

Sigle : CYB6043 Gr. 01
Titre : Atelier pratique en cybersécurité
Session : Hiver 2025 **Horaire et local**
Professeur : Adi, Kamel & Myria Bouhaddi

1. Description du cours paraissant à l'annuaire :

Objectifs

Au terme de ce cours, l'étudiant.e aura réalisé un projet pratique d'envergure en cybersécurité intégrant les connaissances acquises dans les cours du programme.

Contenu

Le contenu du projet est variable selon les intérêts des étudiant.e.s et de l'expertise professorale disponible.

Descriptif – Annuaire

2. Objectifs spécifiques du cours :

Le projet porte sur la conception et la réalisation d'un système de détection d'intrusion basé sur l'apprentissage machine. La génération des jeux de données d'apprentissage et de validation seront réalisée via un serveur « Pot de miel (Honeypot) » qui sera installé et configuré par les étudiants.

3. Stratégies pédagogiques :

Généralement la séance de cours de 3h00 contient une présentation magistrale d'un contenu académique lié au projet suivi d'une discussions sur l'avancement des projets des équipes.

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

Sur rendez-vous.

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	• Introduction • Présentation du projet • Répartition des équipes	14 janv. 2025
2	• Taxonomie d'attaques informatiques • Discussions sur le projet	21 janv. 2025
3	• Technologies pots de miel (Honeypots) • Discussions sur le projet	28 janv. 2025
4	• Détection d'intrusion – Snort • Discussions sur le projet	4 févr. 2025
5	• Cybersécurité et apprentissage automatique (1) • Discussions le projet	11 févr. 2025
6	• Cybersécurité et apprentissage automatique (2) • Discussions sur le projet	18 févr.2025
7	• Les jeux de données pour la détection d'intrusion • Discussions sur le projet	25 févr. 2025

8	**Semaine d'études**	**4 mars 2025**
9	Présentation intermédiaire des projets	11 mars 2025
10	• Conférencier invité 1 • Discussions sur le projet	18 mars 2025
11	• Automatisation de la cyberdéfense. • Discussions sur le projet	25 mars 2025
12	• Conférencier invité 2 • Discussions sur le projet	1 avril 2025
13	Discussions sur le projet	8 avril 2025
14	Discussions sur le projet	15 avril 2025
15	**Présentation finale des projet**	22 avril 2025

6. Évaluation du cours :

L'évaluation du cours se fera comme suit :

- Présentation du projet à la mi-session : 20%
- Présentation finale du projet : 30%
- Rapport écrit : 30 %
- Participation aux discussions sur le projet : 20 %

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. Leigh Metcalf, Jonathan Spring, Using Science in Cybersecurity, World Scientific Publishing, April 28 2021.

2. Security in Computing, 5e Edition, Charles P. Pfleeger Shari Lawrence Pfleeger, Jonathan Margulies, Prentice Hall,2023.

3. Halder, Soma, and Sinan Ozdemir. *Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem*. Packt Publishing Ltd, 2018.

4. Alessandro Parisi. *Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies*. Packt Publishing Ltd, 2019.

5. Jake VanderPlas. Python Data Science Handbook: Essential Tools for Working with Data. O'Reilly Media; 2e édition, 2023.

6. Ghorbani, Ali A., Wei Lu, and Mahbod Tavallaee. *Network intrusion detection and prevention: concepts and techniques*. Vol. 47. Springer Science & Business Media, 2009.

7. Ammar Boulaiche, Kamel Adi. An auto-learning approach for network intrusion detection. Telecommun. Syst. 68(2): 277-294 (2018)

8. Ammar Boulaiche, Hatem Bouzayani, Kamel Adi. A Quantitative Approach for Intrusions Detection and Prevention based on Statistical N-Gram Models. ANT/MobiWIS 2012: 450-457

9. Page Web du cours :

https://moodle.ugo.ca