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

Sigle : CYB6043 Gr. 01
Titre : Atelier pratique en cybersécurité
Session : Automne 2024 Horaire et local
Professeurs : Allili, Mohand Saïd - Khoury, Raphaël

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 classification de malware à l'aide de l'apprentissage automatique. Les étudiants seront familiarisés avec plusieurs familles de malware et les différentes propriétés les caractérisant. Ils pourront réaliser des modèles classification e malware.

3. Stratégies pédagogiques :

Généralement, la séance de cours de 3h00 contient une présentation magistrale d'un contenu académique lié au projet suivie d'une discussion 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 générale de l'atelier (Raphaël et Mohand) • Définition des objectifs généraux et spécifiques • Répartition des équipes	03 sept 2024
2	Généralités sur les logiciels malicieux (malwares) (Mohand & Raphaël) • Taxonomie des différents types de malwares • Modes de propagation des malwares	10 sept 2024
3	Les jeux de données pour la détection de malware (Raphaël) Caractérisation et classification des malwares • Caractérisation statique (ex. analyse d'entête, structure code) • Caractérisation dynamique (ex. trace mémoire, appels systèmes)	17 sept 2024
4	Devoir 1 : Présentations de jeux de données du cours (Présentation étudiante)	24 sept 2024
5	Introduction à l'apprentissage automatique (Mohand)	01 oct. 2024

	• Généralités sur les techniques d'apprentissages • Collecte et préparation des données	
6	Méthodes de classification (Mohand) • Classification binaire • Classification multi-classes • Critères d'évaluation de modèles de classification	08 oct. 2024
7	**Semaine d'études**	15 oct. 2024
8	Apprentissage profond pour la classification (Mohand) • Introduction aux réseaux de neurones, • Types de réseaux de neurones • Retro-propagation et entrainement d'un RN Devoir 2	22 oct. 2024
9	Présentation intermédiaire des projets Analyse des bases de données de malware existantes	29 oct. 2024
10	Aspects avancés sur la détection de malware (Raphaël) • Le code vulnérable • Méthodes de détection et de protection des malwares • Caractérisation et classification des malwares	05 nov. 2024
11	Discussion sur les projets	12 nov. 2024
12	Discussion sur les projets	19 nov. 2024
13	Conférencier invité 1	26 nov. 2024
14	Conférencier invité 2	03 déc. 2024
15	**Présentation finale des projets**	10 déc. 2024

6. Évaluation du cours :

L'évaluation du cours se fera comme suit :

- Devoir 1 : 5%
- Devoir 2 : 5%
- Présentation du projet à la mi-session : 15%
- Présentation finale du projet : 30%
- Rapport écrit : 30 %
- Participation aux discussions sur le projet : 15 %

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.

9. Page Web du cours :

https://moodle.uqo.ca