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

Sigle : CYB1023 Gr. 01
Titre : Sécurité des réseaux informatiques
Session : Automne 2025 Horaire et local
Professeur : Abderrahmane Ben Mimoune

1. Description du cours paraissant à l'annuaire :

Objectifs

Au terme de ce cours, l'étudiant.e aura approfondi par la pratique les techniques d'analyse de vulnérabilités, d'élaboration de scénarios d'attaques et de sécurisation des réseaux informatiques.

Contenu

Rappel sur les architectures de réseaux informatiques et propriétés de sécurité. Anatomie d'une cyberattaque ("Cyber Kill Chain"). Mesures de sécurité (zonage, défense en profondeur, défense active, sécurité du périmètre, gestion des accès, etc). Gestion des vulnérabilités dans les réseaux informatiques. Principaux outils utilisés pour analyser et attaquer un réseau informatique (wireshark, nmap, nessus, metasploit, etc.). Contrôles de sécurité (NIST 800-53). Contre-mesures disponibles pour faire face aux différentes attaques réseau. Techniques de détection et de protection (pare-feux, système de prévention et de détection des intrusions, filtrage de courriels, etc.). Sécurité des réseaux sans fil. Sécurité d'accès à distance (IPSEC, VPN). Résolution de problèmes de sécurité des réseaux informatiques issus du monde réel. Ce cours comporte des séances obligatoires de travaux pratiques (TP).

Descriptif – Annuaire

2. Objectifs spécifiques du cours :

À la fin de ce cours, l'étudiant devrait être en mesure de:

- Expliquer les principes fondamentaux de la cybersécurité
- Analyser les différentes étapes d'une cyberattaque.
- Identifier et exploiter des vulnérabilités réseau à l'aide d'outils spécialisés.
- Concevoir et mettre en œuvre des mesures de sécurité réseau.
- Appliquer les contrôles de sécurité recommandés dans un contexte réseau.
- Utiliser des outils de détection et de prévention d'intrusion et pare-feu.
- Évaluer les vulnérabilités et les risques dans un environnement réseau donné.
- Mettre en œuvre des solutions sécurisées d'accès à distance.

3. Stratégies pédagogiques :

- Cours magistraux : 3 h/semaine de cours
- Les séances de travaux pratiques
- Un projet de session
- Un examen de mi-session
- Un examen final

Disponibilité d'une page MOODLE contenant le matériel du cours et les résultats des évaluations.
Je ne reçois aucun travail par courriel. Tous les travaux doivent être remis dans Moodle.

Note sur le plagiat et la fraude : Consulter la politique en vigueur à la section 7.
L'utilisation d'un logiciel de médiagraphie comme Zotéro est fortement suggérée.

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

- Disponible pour répondre aux courriels dans un délai typique de 72 heures.
- Disponible durant les séances du cours pour répondre aux questions.
- Pour communiquer avec le professeur, envoyez un courriel à : Abderrahmane.BenMimoune@uqo.ca

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	Présentation du plan de cours, des activités évaluées, introduction et mise en contexte	02 sept. 2025
2	Les architectures réseau, les protocoles de communication et concepts de sécurité	09 sept. 2025
3	Comprendre les mécanismes de défense, périmètre de sécurité, sécurité par couches **Séance de travaux pratiques 1** : Le 19 sept. 2025	16 sept. 2025 **(non présentiel)**
4	Renfoncement de la sécurité, durcissement du réseau : segmentation, services et protocoles	23 sept. 2025
5	Principes fondamentaux de la technologie VPN et de la cryptographie **Séance de travaux pratiques 2** : Le 03 oct. 2025	30 sept. 2025
6	Les concepts du contrôle d'accès et fonctionnement de l'AAA	07 oct. 2025
7	**Semaine d'études**	13-17 oct. 2025
8	**Examen de mi-session**	21 oct. 2025
9	Comprendre les fondamentaux des pares-feux et les politiques basées sur les zones **Séance de travaux pratiques 3** : Le 31 oct. 2025	28 oct. 2025
10	Principes fondamentaux des systèmes de détection/prévention d'intrusion **Séance de travaux pratiques 4** : Le 07 nov. 2025	04 nov. 2025
11	Surveillance du réseau, les données sur la sécurité du réseau et l'évaluation des alertes **Séance de travaux pratiques 5** : Le 14 nov. 2025	11 nov. 2025
12	Protection des terminaux, évaluation des vulnérabilités et tests de sécurité du réseau	18 nov. 2025 **(non présentiel)**
13	Études de cas	25 nov. 2025 **(non présentiel)**
14	**Présentation des projets**	02 déc. 2025
15	**Examen final**	09 déc. 2025

6. Évaluation du cours :

Activité évaluée	Mode et date de remise	Pondération
Examen intra	Individuel, le 21 octobre	25%
Travaux pratiques	En groupe de deux, remise selon les directives dans Moodle	20%
Projet de session	En groupe de deux, présentation le 02 décembre	15%
Examen final	Individuel, le 09 décembre	40%

Règles de présentation des travaux
Le numéro de l'équipe et les noms des équipiers doivent apparaître en page 1 de tout rapport remis. Les rapports relatifs aux travaux pratiques doivent utiliser le formulaire mis à la disposition des équipes. Les réponses demandées peuvent varier en longueur, allant d'un seul mot à plusieurs lignes. Chaque question doit être répondue indépendamment des autres questions. Les réponses doivent être aussi concises mais aussi précises que possible. Les réponses inutilement longues ne seront pas corrigées car il n'appartient pas au correcteur de choisir les éléments utiles de la réponse parmi les éléments inutiles.

Règles concernant les retards dans la remise des travaux
Les dates des remises des rapports des travaux pratiques ou projet sont connues dès le début de l'évaluation. Il appartient donc à l'étudiant(e) de planifier correctement la quantité de travail à mettre sur le travail ainsi que le moment où appliquer cet effort. Lorsqu'un travail est remis après la date d'échéance, l'équipe perd 5% pour chaque heure de retard. La remise est considérée en retard lorsque l'heure est commencée (donc : un retard d'une minute est considéré comme une heure de retard). Si l'équipe sait que la remise ne se fera pas en temps, elle peut prendre entente avec l'enseignant et convenir d'un nouveau moment pour la remise et de la pénalité qui résultera du retard. Le délai convenu et la pénalité doivent être raisonnables compte tenu des circonstances.

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)
- Politique sur la liberté académique

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 :

- CCNA Security 640-554 Official Cert Guide Hardcover – 2012
- Software Networks: Virtualization, SDN, 5G and Security - 2015
- Network Security Essentials: Applications and Standards – 2014
- Network Security Bible - 2005

9. Page Web du cours :

https://moodle.uqo.ca