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

Sigle : CYB1023 Gr. 01
Titre : Sécurité des réseaux informatiques
Session : Automne 2026 Horaire et local
Professeure : Ben Mimoune, Abderrahmane

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 :

Consolider les connaissances sur les architectures des réseaux informatiques et les propriétés fondamentales de la sécurité (confidentialité, intégrité, disponibilité). Développer les compétences pour identifier, analyser et gérer les vulnérabilités au sein des réseaux informatiques.
Compréhension des scénarios d'attaques et des contre-mesures. Étudier et mettre en œuvre les contre-mesures appropriées pour prévenir et répondre à ces attaques. Aprendre à utiliser les principaux outils d'analyse, de détection et de simulation d'attaques réseau (Wireshark, Nmap, Nessus, etc.). Mettre en œuvre des stratégies de sécurité réseau, y compris le zonage, la défense en profondeur, et la gestion des accès pour protéger les infrastructures. Maîtriser les spécificités de la sécurité des réseaux sans fil et des accès à distance (IPSEC, VPN). Application pratique des concepts. Résoudre des problématiques réelles de sécurité des réseaux informatiques à travers des séances pratiques et des études de cas. Comprendre et appliquer les contrôles de sécurité conformément aux cadres réglementaires tels que le NIST 800-53.
Détection et protection avancées. Utiliser des technologies de détection et de prévention (pare-feux, IDS/IPS, filtrage de courriels) pour identifier et neutraliser les menaces.

3. Stratégies pédagogiques :

Disponibilité d'une page MOODLE contenant le matériel du cours et les résultats des évaluations.

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

Je ne reçois aucun travail par courriel. Tous les travaux doivent être remis dans Moodle.

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

Communication par courriel (Abderrahmane.BenMimoune@uqo.ca). Période de consultation sur rendez-vous seulement (prévoir 72 heures d'avance pour la prise de rendez-vous).

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	14 sept. 2026
2	Les architectures réseau, les protocoles de communication et concepts de sécurité	21 sept. 2026
3	Comprendre les mécanismes de défense, périmètre de sécurité, sécurité par couches **Séance de travaux pratiques 1** : Le 30 sept. 2026	28 sept. 2026
4	Renfoncement de la sécurité, durcissement du réseau : segmentation, services et protocoles	05 oct. 2026
5	**Semaine d'études**	12 oct. 2026
6	Principes fondamentaux de la technologie VPN et de la cryptographie **Séance de travaux pratiques 2** : Le 20 oct. 2026	19 oct. 2026
7	**Examen de mi-session**	26 oct. 2026
8	Les concepts du contrôle d'accès et fonctionnement de l'AAA	02 nov. 2026
9	Comprendre les fondamentaux des pares-feux et les politiques basées sur les zones **Séance de travaux pratiques 3** : Le 10 nov. 2026	09 nov. 2026
10	Principes fondamentaux des systèmes de détection/prévention d'intrusion **Séance de travaux pratiques 4** : Le 17 nov. 2026	16 nov. 2026
11	Surveillance du réseau, les données sur la sécurité du réseau et l'évaluation des alertes **Séance de travaux pratiques 5** : Le 24 nov. 2026	23 nov. 2026
12	Protection des terminaux, évaluation des vulnérabilité et tests de sécurité du réseau	30 nov. 2026
13	Études de cas	07 déc. 2026
14	**Examen final**	14 déc. 2026
15	**Présentation des projets**	21 déc. 2026

6. Évaluation du cours :

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

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.

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 d'effort à mettre sur le travail ainsi que le moment où appliquer cet effort. Les étudiants disposeront d'un délai suffisant pour compléter et remettre leurs travaux. Par conséquent, aucun travail remis en retard ne sera accepté. Tout travail non remis dans les délais prescrits se verra attribuer la note de zéro (0).

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. L'utilisation d'un logiciel de médiagraphie comme Zotéro est fortement suggérée.
- 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