Université de Sherbrooke

Centre de formation en technologie de l'information

INF 808 – Réaction aux attaques et analyses des attaques

Plan d'activité pédagogique

Hiver 2026

Enseignant	Daniel Migault
Courriel :	daniel.migault@usherbrooke.ca
Local :	
Téléphone :	
Disponibilités :	L'enseignant est joignable par courriel.

Site web du cours : https ://moodle.usherbrooke.ca/

Horaire Exposé magistral : Mardi 16 h 00 à 18 h 50 salle L1-3620

Description officielle de l'activité pédagogique[1]

Cibles de formation :	Apprendre à caractériser différents types de cyberattaques. Apprendre la gestion d'incidents suite à une attaque.
Contenu :	Analyse d'attaque. Gestion des incidents. Analyse des attaques d'hameçonnage ; trace réseau ; analyse des postes ; comment détecter l'attaquant. Outils et techniques d'analyse de journaux. Journalisation des serveurs Web ; détection d'indices généraux d'activités suspectes. Balayages de vulnérabilités. Attaques de contournement. Attaques de sessions. Attaques par injection. Attaque de déni de service. Analyses d'attaque de serveurs Web. Désescalade postincident.
Crédits	3
Organisation	3 heures d'exposé magistral par semaine 6 heures de travail personnel par semaine
Préalable	INF805
Particularités	Aucune

[1] https ://www.usherbrooke.ca/admission/fiches-cours/inf808

1 Présentation

Cette section présente les cibles de formation spécifiques et le contenu détaillé de l'activité pédagogique. Cette section, non modifiable sans l'approbation du comité de programme du Centre de formation en technologie de l'information, constitue la version officielle.

1.1 Mise en contexte

Ce cours a pour but de sensibiliser les étudiants au déroulement des attaques connues et largement répandues aujourd'hui afin de pouvoir s'occuper des attaques futures.

1.2 Cibles de formation spécifiques

À la fin de cette activité pédagogique, l'étudiante ou l'étudiant sera capable :

1. De connaître les principaux types d'attaques ;
2. D'analyser une attaque lorsqu'elle survient ;
3. D'établir un plan d'intervention suite à une attaque ;
4. De mettre en place une solution afin de se protéger face a une telle attaque ;
5. De lier la gestion des risques et l'identification des attaques.

1.3 Contenu détaillé

Thème	Contenu	Nbr. d'heures	Objectifs
1	Introduction du cours	3	
2	Chapitre 1 — Fondements cryptographiques, protection des actifs et introduction à Python : Fondements cryptographiques, protection des actifs et introduction à Python : fonctions cryptographiques : chiffrement, hachage, MAC, certificats ; authentification, chaînes de confiance, AC et PKI ; vulnérabilités : chiffrement non authentifié, attaques par oracle (AES-CBC) ; Python pour l'analyse de données et les outils de cybersécurité	3	1, 2, 4, 5
3	Chapitre 2 — SOC, détection, gestion d'incidents et Threat Hunting : SOC : mission et structure d'un SOC (Niveaux 1–3, ingénieurs, CTI, red team) ; cycle de vie d'un incident : préparation, détection, analyse, réponse, rétablissement ; méthodologie TaHiTI, pyramide des difficultés ; gestion de crise et coordination opérationnelle	3	1, 2, 3, 5
4	Chapitre 3 — Cyber Threat Intelligence : outils et modèles (Kestrel, OpenCTI, STIX, OCSF) : Cyber Threat Intelligence et outils d'investigation : rôle de la CTI dans la détection et l'investigation ; structuration des données : STIX, OCSF ; automatisation d'enquêtes avec Kestrel ; corrélation de menaces et campagnes dans OpenCTI	9	1, 2, 4
5	Chapitre 4 — Modèles d'attaque : MITRE ATT&CK, Kill Chain, Diamond Model, STRIDE : Modèles d'attaque : modèles : MITRE ATT&CK, Diamond Model, Kill Chain ; analyse comportementale des adversaires ; décomposition des phases d'attaque : reconnaissance, accès initial, mouvement latéral, etc. ; évaluation des risques à l'aide de STRIDE ; études de cas réels : centrales ukrainiennes, Energetic Bear	6	1, 2, 3, 5
6	Chapitre 5 — DNS : cibles, vecteurs d'attaque et détection des botnets : DNS : DNS comme infrastructure critique et comme surface d'attaque ; fast flux, double flux, domaines générés algorithmiquement (DGA) ; analyse de traces réseau DNS pour la détection d'activités suspectes ; confidentialité : DoT, DoH, enjeux de centralisation	6	1, 2, 3, 4

Table 1 :

Thème	Contenu	Nbr. d'heures	Objectifs
7	Chapitre 6 — Attaques par déni de service (DDoS) : analyse et réaction : Attaques par déni de service distribué (DDoS) : typologies : volumétriques, protocolaires, applicatives ; détection d'un DDoS dans les journaux et dans le trafic ; mitigation : filtrage, SDN, DOTS, stratégies collaboratives ; études de cas : Mirai, DDoS-as-a-Service	6	1 - 5
8	Chapitre 7 (Optionnel) — IPsec, VPN et laboratoire Python : Architecture IPsec, négociation des SA, modes tunnel/transport ; Mise en place d'une politique de sécurité organisationnelle ; Manipulation de paquets chiffrés avec Python.	3	1, 2, 4, 5
9	Chapitre 8 (Optionnel) — Confidential Computing et thématiques avancées : Exécution en environnement sécurisé (Intel SGX) ; Attestation, modèles de confiance ; TLS 1.3, sécurité des applications Web, pare-feu (selon temps disponible).	3	1, 2, 4, 5

2 Organisation

Cette section propre à l'approche pédagogique de chaque enseignante ou enseignant présente la méthode pédagogique, le calendrier, le barème et la procédure d'évaluation ainsi que l'échéancier des travaux. Cette section doit être cohérente avec le contenu de la section précédente.

2.1 Méthode pédagogique

La méthode pédagogique retenue vise le développement progressif et intégré des compétences nécessaires à la détection, l'analyse et la gestion d'incidents de sécurité informatique. L'enseignement adopte une approche par compétences, centrée sur l'acquisition de savoirs, de savoir-faire et de savoir-agir professionnels appliqués à des contextes réels.

Les apprentissages sont structurés autour :

- **d'exposés ciblés** permettant l'acquisition des concepts fondamentaux (modèles d'attaque, traces d'intrusion, fonctionnement d'un SOC, mécanismes cryptographiques, typologie des attaques) ;
- de mises en situation pratiques où l'étudiante ou l'étudiant mobilise les outils et méthodes du domaine (analyse de journaux, inspection de traces réseau, utilisation d'outils CTI, simulations d'incidents) dans le but de résoudre des problématiques authentiques ;
- **d'activités d'intégration** permettant de transférer les apprentissages théoriques et pratiques à des scénarios complets d'analyse d'attaque et de réponse à incident ;
- **d'un travail personnel d'investigation**, qui favorise l'autonomie, la prise de décision, ainsi que l'application rigoureuse d'une démarche méthodologique d'analyse.

L'approche pédagogique est guidée par la mise en œuvre concrète des compétences suivantes :

- **détecter et interpréter des indicateurs d'intrusion** dans des systèmes réels ;
- **analyser les mécanismes d'une attaque** et identifier les vecteurs d'exploitation ;
- **sélectionner et utiliser adéquatement des outils professionnels** pour examiner journaux, traces et artefacts ;
- **élaborer et justifier un plan d'intervention** adapté au contexte organisationnel ;
- **intégrer les règles, contraintes et meilleures pratiques** propres à la gestion d'incidents.

Les activités pédagogiques favorisent l'apprentissage actif, la résolution de problèmes complexes et la mobilisation intégrée des savoirs. Elles visent à développer la compétence à intervenir efficacement dans un contexte réel de cybersécurité. , conformément aux attentes du milieu professionnel et aux standards ministériels en matière de formation axée sur les compétences.

2.2 Calendrier

Semaine	Commençant le	Thème	Projet Recherche	Lectures
1	2026-01-05	1		
2	2026-01-12	2		Chapitre 1 — Fondements cryptographiques, protection des actifs et introduction à Python
3	2026-01-19	3		Chapitre 2 — SOC, détection, gestion d'incidents et Threat Hunting
4	2026-01-26	4		Chapitre 3 — Cyber Threat Intelligence : outils et modèles (Kestrel, OpenCTI, STIX, OCSF)
5	2026-02-02	4		Chapitre 3 — Cyber Threat Intelligence : outils et modèles (Kestrel, OpenCTI, STIX, OCSF)

Table 2 :

Semaine	Commençant le	Thème	Projet Recherche	Lectures
6	2026-02-09	4		Chapitre 3 — Cyber Threat Intelligence : outils et modèles (Kestrel, OpenCTI, STIX, OCSF)
7	2026-02-16	5		Chapitre 4 — Modèles d'attaque : MITRE ATT&CK, Kill Chain, Diamond Model, STRIDE
8	2026-02-23			INTRA
9	2026-03-02	Relâche		
10	2026-03-09	5		Chapitre 4 — Modèles d'attaque : MITRE ATT&CK, Kill Chain, Diamond Model, STRIDE
11	2026-03-16	6		Chapitre 6 — Attaques par déni de service (DDoS) : analyse et réaction
12	2026-03-23	6		Chapitre 6 — Attaques par déni de service (DDoS) : analyse et réaction
13	2026-03-30	7		Chapitre 6 — Attaques par déni de service (DDoS) : analyse et réaction
14	2026-04-06	7		Chapitre 6 — Attaques par déni de service (DDoS) : analyse et réaction
15	2026-04-13			FINAL
16	2026-04-20	Semaine des examens finals	Réception Projet Recherche	Présentation du Projet Recherche
17	2026-04-27	Semaine des examens finals		

2.3 Évaluation

Type de l'évaluation	Pondération	Utilisation des IAG[1]
lab	15 %	Libre
Projet Recherche	35 %	Libre
Examen intra	25 %	Interdite
Examen final	25 %	Interdite

[1] Référez-vous à la page "Balises d'utilisation des outils d'intelligence artificielle générative" à la fin du document.

Laboratoire — 15 %
Travail individuel comprenant un questionnaire sur Moodle et du code Python à soumettre. Le laboratoire est à remettre à la mi-février. Tout retard entraîne une pénalité et l'absence de remise vaut une note de 0. L'usage de l'IA est autorisé.
Projet de recherche — 35 %
Travail en groupe (ou individuel, au choix). L'étudiant propose une thématique qui doit être approuvée par l'enseignant, puis les objectifs sont définis. L'évaluation porte sur la présentation, le rapport écrit et un dépôt GitHub. Tout retard entraîne une pénalité et
l'absence de remise vaut une note de 0. L'usage de l'IA est autorisé.

2.3.1 Qualité de la langue et de la présentation

Conformément à l'article 17 du Règlement facultaire d'évaluations des apprentissages[2] l'enseignante ou l'enseignant peut retourner à l'étudiante ou à l'étudiant tout travail non conforme aux exigences quant à la qualité de la langue et aux normes de présentation.

2.3.2 Plagiat

Le plagiat consiste à utiliser des résultats obtenus par d'autres personnes afin de les faire passer pour sien et dans le dessein de tromper l'enseignante ou l'enseignant. Vous trouverez en annexe un document d'information relatif à l'intégrité intellectuelle qui fait état de l'article 9.4.1 du Règlement des études[3]. Lors de la correction de tout travail individuel ou de groupe une attention spéciale sera portée au plagiat. Si une preuve de plagiat est attestée, elle sera traitée en conformité, entre autres, avec l'article 9.4.1 du Règlement des études de l'Université de Sherbrooke. L'étudiante ou l'étudiant peut s'exposer à de graves sanctions qui peuvent être soit l'attribution de la note E ou de la note zéro (0) pour un travail, un examen ou une activité évaluée, soit de reprendre un travail, un examen ou une activité pédagogique. Tout travail suspecté de plagiat sera transmis au Secrétaire de la Faculté des sciences. Ceci n'indique pas que vous n'ayez pas le droit de coopérer entre deux équipes, tant que la rédaction finale des documents et la création du programme restent le fait de votre équipe. En cas de doute de plagiat, l'enseignante ou l'enseignant peut demander à l'équipe d'expliquer les notions ou le fonctionnement du code qu'elle ou qu'il considère comme étant plagié. En cas d'incertitude, ne pas hésiter à demander conseil et assistance à l'enseignante ou l'enseignant afin d'éviter toute situation délicate par la suite.

[2] https://www.usherbrooke.ca/sciences/fileadmin/sites/sciences/documents/Etudiants_actuels/Informations_academiques_et_reglements/2017-10-27_Reglement_facultaire_-_evaluation_des_apprentissages.pdf
[3] https://www.usherbrooke.ca/registraire/droits-et-responsabilites/reglement-des-etudes/

2.4 Échéancier des travaux

Les dates de remise des travaux seront indiquées sur les énoncés.

2.5 Utilisation d'appareils électroniques et du courriel

Selon le règlement complémentaire des études, section 4.2.3 [4], l'utilisation d'ordinateurs, de cellulaires ou de tablettes pendant une prestation est interdite à condition que leur usage soit explicitement permise dans le plan de cours.

Dans ce cours, l'usage de téléphones cellulaires, de tablettes ou d'ordinateurs est autorisé. Cette permission peut être retirée en tout temps si leur usage entraîne des abus.

Tel qu'indiqué dans le règlement universitaire des études, section 4.2.3[5], toute utilisation d'appareils de captation de la voix ou de l'image exige la permission de la personne enseignante.

Note : Je réponds aux questions posées par courriel à l'extérieur des périodes de cours.

3 Matériel nécessaire pour l'activité pédagogique

aucun

[4] https://www.usherbrooke.ca/sciences/fileadmin/sites/sciences/documents/Etudiants_actuels/Informations_academiques_et_reglements/Sciences_Reglement_complementaire.pdf

[5] https://www.usherbrooke.ca/registraire/droits-et-responsabilites/reglement-des-etudes/

Faculté des sciences UdS

Délits relatifs aux études

Extrait du règlement des études (Règlement 2575-009)

Sont notamment considérés comme un délit relatif aux études les faits suivants :

a) commettre un plagiat, soit faire passer ou tenter de faire passer pour sien, dans une production évaluée, le travail d'une autre personne, des passages ou idées tirés de l'œuvre d'autrui ou du contenu, de toute forme, généré par un système d'intelligence artificielle (ce qui inclut notamment le fait de ne pas indiquer la source et la référence adéquate);
b) commettre un autoplagiat, soit soumettre, sans autorisation préalable, une même production, en tout ou en partie, à plus d'une activité pédagogique ou dans une même activité pédagogique (notamment en cas de reprise);
c) usurper l'identité d'une autre personne ou procéder à une substitution de personne lors d'une production évaluée ou de toute autre prestation obligatoire;
d) fournir ou obtenir toute forme d'aide non autorisée, qu'elle soit collective ou individuelle (incluant l'assistance provenant d'un système d'intelligence artificielle), pour une production faisant l'objet d'une évaluation;
e) obtenir par vol ou toute autre manœuvre frauduleuse, posséder ou utiliser du matériel non autorisé de toute forme (incluant le matériel numérique et celui généré par un système d'intelligence artificielle) avant ou pendant une production faisant l'objet d'une évaluation;
f) copier, contrefaire ou falsifier un document pour l'évaluation d'une activité pédagogique;
k) posséder ou avoir à sa portée un appareil électronique ou numérique interdit durant une activité d'évaluation;

[...]

Un guide sur l'intégrité intellectuelle vous est rendu disponible par le service des bibliothèques et des archives de l'Université de Sherbrooke, afin de bien comprendre les différents délits et ainsi éviter d'être aux prises avec un dossier disciplinaire et une ou des sanctions.

Les mesures pouvant être imposées à titre de sanctions disciplinaires sont les suivantes :

a) la réprimande simple ou sévère consignée au dossier étudiant pour la période fixée par l'autorité disciplinaire ou à défaut, définitivement. En cas de réprimande fixée pour une période déterminée, la décision rendue demeure au dossier de la personne aux seules fins d'attester de l'existence du délit en cas de récidive;
b) l'obligation de reprendre une production ou une activité pédagogique, dont la note pourra être établie en tenant compte du délit survenu antérieurement;
c) la diminution de la note ou l'attribution de la note E ou 0;

[...]

UDS Faculté des sciences

Balises d'utilisation des outils d'intelligence artificielle générative

Autorisés ou pas dans les situations d'apprentissage et d'évaluation ?

NIVEAU 0	NIVEAU 1	NIVEAU 2	NIVEAU 3	NIVEAU 4
L'utilisation des outils d'intelligence artificielle générative (IAg) est limitée, voire complètement interdite parce que la personne enseignante considère que l'usage de ces outils nuit au développement de compétences essentielles. Ces compétences peuvent être disciplinaires, comme elles peuvent être d'ordre méthodologique, rédactionnel ou informationnel. Considérant que l'utilisation des IAg requiert un esprit critique, il peut s'agir d'une situation d'apprentissage ou d'évaluation sans IAg qui vise à développer celui-ci. Dans ces situations, **la personne étudiante produit le travail**.			L'utilisation prononcée des IAg est permise parce que la personne enseignante considère que les personnes étudiantes sont en mesure d'exercer un esprit critique et sont capables de juger de la qualité des contenus produits par les IAg. Ou encore, l'utilisation est encouragée parce que la situation d'apprentissage ou d'évaluation proposée contribue à développer leur esprit critique. Dans ces situations, l'IAg produit le travail préliminaire, alors que **la personne étudiante s'assure de sa qualité en l'améliorant**.	
				
Utilisation interdite	**Utilisation limitée**	**Utilisation guidée**	**Utilisation balisée**	**Utilisation libre**
Le **NIVEAU 0** signifie que l'**utilisation est interdite**. Ceci signifie que si la personne enseignante a un motif de croire qu'il y a eu l'utilisation d'une IAg dans une situation d'évaluation, elle doit dénoncer les faits auprès de la personne responsable des dossiers disciplinaires universitaires. Il s'agit d'un délit relatif aux études tel que stipulé dans le Règlement des études.	Le **NIVEAU 1 D'UTILISATION** signifie que l'**utilisation est autorisée uniquement pour assister l'apprentissage dans le domaine disciplinaire ou des langues**. Dans ce contexte, la personne étudiante **est tenue de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation peut être considérée comme un délit. Par exemple : Domaine disciplinaire : - S'inspirer - Générer des idées - Explorer un sujet pour mieux le comprendre - Générer du matériel pour apprendre Domaine des langues : - Identifier ses erreurs et se les faire expliquer - Reformuler un texte - Générer un plan pour aider à structurer un texte - Traduire un texte	Le **NIVEAU 2 D'UTILISATION** signifie que l'**utilisation est autorisée pour améliorer un travail produit par la personne étudiante**. Dans ce contexte, la personne étudiante **est tenue de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation est considérée comme un délit. Par exemple : - Analyser des contenus - Obtenir une rétroaction - Évaluer la qualité de son travail à partir de critères - Demander à être confronté relativement à ses idées, à sa démarche - Diriger les processus de résolution de problèmes	Le **NIVEAU 3 D'UTILISATION** signifie que l'**utilisation est autorisée pour produire un travail qui sera amélioré.** Dans ce contexte, la personne étudiante **est tenue de citer selon les normes[1] le contenu généré par l'IAg** ou **de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation est considérée comme un délit. Par exemple : - Résumer ou rédiger des parties d'un texte - Générer un texte ou un modèle d'une production et l'adapter - Réaliser des calculs mathématiques - Produire du code informatique - Résoudre des problèmes complexes - Répondre à une question - Générer des images, ou autres contenus multimédias	Le **NIVEAU 4 D'UTILISATION** signifie qu'**aucune restriction spécifique n'est imposée**. Dans ce contexte, la personne étudiante **est tenue de citer selon les normes[1] le contenu généré par l'IAg** ou **de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation est considérée comme un délit. Ce niveau inclut tout ce qui précède, de l'exploration à la production, ainsi que toute autre tâche particulière jugée complexe.

UDS Faculté des sciences

À considérer avant l'utilisation d'outils d'intelligence artificielles génératives

Si, en tant que personne étudiante envisagez d'utiliser un outil d'intelligence artificielle générative (IAG) lorsque l'évaluation autorise les niveaux 1 à 4 d'utilisation mentionnés précédemment.

Dans ce cas, gardez à l'esprit les éléments clés suivants.

- Vous assumez la responsabilité de tout le contenu produit, avec ou sans IAG, et intégré à votre production.
- Les produits des outils d'IAG peuvent très souvent comporter **des erreurs ou des faussetés** (hallucinations) : on doit donc impérativement valider tout contenu généré par ces outils.
- Dans l'état actuel de la Loi sur le droit d'auteur du Canada, les **productions faites par l'IAG sont du domaine public,** puisque les outils d'IAG ne sont pas reconnus comme des auteurs au sens de la Loi et que les contenus générés ne répondent pas aux critères d'une œuvre protégée, notamment aux critères d'originalité.
- L'entreprise qui fournit le service pourrait émettre certaines exigences dans ses conditions d'utilisation. Comme l'algorithme et le code informatique appartiennent à l'entreprise qui les a développés, nous devons tenir compte de ces conditions. Celles-ci pourraient également fournir des précisions relatives à la **réutilisation des données soumises (confidentialité)**.

Comment déclarer l'utilisation d'outils d'intelligence artificielle générative

Dans l'esprit d'une conduite intègre et responsable, vous devez TOUJOURS mentionner de façon explicite toute utilisation de l'intelligence artificielle, conformément au Règlement des études (9.4.1 Délits relatifs aux études). De plus, à des fins pédagogiques, il est recommandé de toujours intégrer à la production les requêtes, de même que les réponses intégrales générées par les outils d'IAG. Celles-ci pourront être intégrées directement dans le corps du texte ou en note de bas de page. Les réponses longues pourraient être insérées en annexe de votre document ou dans des documents supplémentaires, selon les directives de la personne enseignante.

L'utilisation de ces deux documents s'avèrera utile, ils se trouvent sous licence libre, donc vous pouvez utiliser les tableaux et les adapter selon votre besoin:

1. Modèle de citation : Ce formulaire, à remplir par l'enseignant, donne un exemple aux étudiants de citation de l'IAg dans la réalisation d'un travail évalué ou non.
2. Déclaration d'usage : Ce formulaire, à remplir par les étudiants, doit être remis avec une réalisation afin de déclarer l'usage de l'IAg dans la réalisation, qu'elle soit évaluée ou non.

Référence

La Faculté des sciences tient à remercier le SSF pour la production des documents.

- Cabana, M. et Côté, J.-A. (2024). Balises d'utilisation des outils d'intelligence artificielle générative. Service de soutien à la formation, Université de Sherbrooke. Sous licence CC BY 4.0.
- Cabana, M. et Beaudet, M. (2024). Directives de déclaration de l'utilisation de l'intelligence artificielle générative dans une production étudiante. Service de soutien à la formation, Université de Sherbrooke. Sous licence CC BY 4.0.
- Cabana, M. (2024). Formulaire de déclaration de l'utilisation de l'intelligence artificielle générative dans une production étudiante. Service de soutien à la formation, Université de Sherbrooke. Sous licence CC BY 4.0.