Université de Sherbrooke

Centre de formation en technologie de l'information

INF 805 / IFT 508 – Introduction aux attaques informatiques

Plan d'activité pédagogique

Hiver 2026

Enseignant	Guillaume Séguin
Courriel :	guillaume.seguin3@usherbrooke.ca
Local :	
Téléphone :	
Disponibilités :	Pour me rencontrer, envoyez-moi une **invitation Teams contenant un bref résumé de l'objectif de la rencontre** pour que je puisse me préparer. Je suis généralement libre l'après-midi. Sauf exception, j'offre ma disponibilité en ligne.

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

Horaire Exposé magistral : Lundi 9 h 00 à 12 h 20 salle L1-2633

Description officielle de l'activité pédagogique[1]

Cibles de formation :	Comprendre les étapes d'une cyberattaque. Faire la recherche d'informations sur une cible d'attaque. Différencier les types d'attaques. Utiliser des trousses et outils de piratage de façon éthique. Connaitre les techniques pour détecter des cyberattaques.
Contenu :	Analyse d'attaque ; montage et préparation des attaques. Les vulnérabilités et leur exploitation ; vulnérabilités logicielles, exploitation et construction de maliciel. Introduction et test d'intrusion ; OWASP + Guide de tests d'intrusion (pentest) OWASP : atelier ou projet de tests d'intrusion Web ; tests d'intrusion serveur : exploit, pivot, « metasploit » et Armitage. Analyse des attaques d'hameçonnage : trace réseau, analyse des postes, détection de l'attaquant. Tests d'intrusion (pentest) comme méthode d'attaque. Détection de cyberattaques : par extraction des fichiers, par signatures, par anomalies, par analyse de journaux, analyse de flux.
Crédits	3
Organisation	3 heures d'exposé magistral par semaine 6 heures de travail personnel par semaine
Particularités	Aucune

[1] https ://www.usherbrooke.ca/admission/fiches-cours/inf805

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

1.2 Cibles de formation spécifiques

Le Microprogramme en sécurité informatique - volet réaction permet à l'étudiante ou à l'étudiant de :

• Maîtriser la nature, le rythme et les outils des cyberattaques contre divers types d'infrastructure

• Savoir détecter les signes et artefacts d'une intrusion, pouvoir mesurer son ampleur et pouvoir en déterminer la chaîne causale

• Savoir dresser et exécuter un plan d'intervention en cas d'incident et de brèche de données, de manière à trouver le meilleur compromis entre la minimisation des dommages et l'interruption des activités de l'organisation.

1.3 Contenu détaillé

Thème	Contenu	Nbr. d'heures	Objectifs
1	Rencontre de démarrage et mise en contexte : • Présentation du cours INF805 • Portrait de la cybercriminalité • Piratage éthique • Modèles d'attaques informatiques • Présentation du laboratoire de travail	3	Pourquoi tant t'attaques
2	Failles humaines et physiques : • Règles d'engagement lors d'une attaque éthique • Ingénierie sociale – cas de l'hameçonnage • Influence et manipulation psychologique • Usurpation d'identité et collecte d'information sur les réseaux sociaux • Accès physique	3	Comprendre le maillon faible : l'humain
3	Reconnaissance passive : • Encadrement des tests d'intrusion • Méthodologie de prise d'empreinte • Énumération (IP, DNS) • Les essentiels (Google Hacking, Google Dorking, moteurs de recherche spécialisés, etc.)	3	Connaître la victime pour mieux la protéger
4	Maîtriser le réseau pour le plaisir et le profit : • Rappel sur les réseaux TCP/IP • Passerelle, masque, sous-réseau, services, ports, TCP/UDP, IP publiques et IP privées • Les requêtes http mises à nu • Reniflage de paquets et attaque par interception (*man-in-the-middle*)	3	Le réseau est l'ordinateur
5	Planifier un test d'intrusion éthique, TP1 et laboratoire : • Les cadres d'encadrement des tests d'intrusion • Instructions pour le TP1 • Laboratoire : Plateforme Hack the Box	3	Organiser un test d'intrusion

Table 1 :

Thème	Contenu	Nbr. d'heures	Objectifs
6	Balayage et exploitation des vulnérabilités : • Outils de balayage de vulnérabiltés • Configuration par défaut et vulnérabilités non corrigées • Déni de service distribué, amplification et « booter » • Attaque par interception et failles cryptographiques • Exfiltration de données	3	Outils de balayage
7	Exploitation des failles système : • L'écosystème des vulnérabilités • Dépassements de pile (*buffer overflow*) • Exécution de code à distance (RCE), code de commandes (*shellcode*) • Isolation des processus, conteneurs et machines virtuelles	3	Injection de code à bas niveau
8	Exploitation des clients : • Les règles immuables de la sécurité • Accès physique et logique • Faire dérailler l'exécution d'un programme en mémoire • Recherche avancée avec Metasploit	3	Exploitation de failles en mémoire
9	Exploitation à distance des failles de sécurité : • Interpréteur de commande distant (*reverse shell*) • Exploiter une vulnérabilité non corrigée • Élévation de privilèges • Comprendre et outrepasser les contrôles de sécurité en place	3	Prendre le contrôle à distance
10	Exploitation des failles applicatives (http) : • Le top 10 de l'OWASP • Trouver des mots de passe • Injection SQL • Conception défaillante • Combiner des attaques	3	Les failles dans les applications web
11	Présentation du TP2 et atelier : • Présentation du TP2 • Processus d'attaque, comment être dans le bon état d'esprit pour trouver les failles • Démonstration d'outils de piratage Web • Atelier collaboratif de résolution de problèmes avec votre environnement de piratage	3	Utiliser les outils
12	Attaque de la chaîne logistique : • Catalogue d'attaques (*framework*) MITRE ATT&CK • Attques de la chaîne logistique • Solorigate, Cuckoo's nest, xz : analyse détaillées d'attaques mémorables • Déploiement et intégration continue	3	Multiplier l'effet d'une attaque ciblée
13	Surveillance et gestion des incidents de sécurité : • Processus de gestion des incidents de sécurité • Alertes et réponse aux incidents • Confinement • Retour synthèse sur les principaux outils	3	Voir et réagir

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 matière est d'abord présentée de façon magistrale. Des exercices pratiques sont fait en classe et les personnes étudiantes sont invités à suivre les étapes sur leur ordinateur personnel. Les démonstrations sont enregistrées et disponible sur Moodle. Des devoirs sont donnés pour aider la personne étudiante à revoir la matière en allant un peu plus loin que la matière vue en classe.

2.2 Calendrier

Semaine	Commençant le	Thème
1	2026-01-05	Rencontre de démarrage et mise en contexte
2	2026-01-12	Failles humaines et physiques
3	2026-01-19	Reconnaissance passive
4	2026-01-26	Maîtriser le réseau pour le plaisir et le profit
5	2026-02-02	Planifier un test d'intrusion éthique, TP1 et laboratoire
6	2026-02-09	Balayage et exploitation des vulnérabilités
7	2026-02-16	Exploitation des failles système
8	2026-02-23	Exploitation des clients
9	2026-03-02	Relâche
10	2026-03-09	Exploitation à distance des failles de sécurité
11	2026-03-16	Exploitation des failles applicatives (http)
12	2026-03-23	Présentation du TP2 et atelier
13	2026-03-30	Attaque de la chaîne logistique
14	2026-04-06	Lundi de Pâques
15	2026-04-13	Surveillance et gestion des incidents de sécurité
16	2026-04-20	Semaine des examens finals
17	2026-04-27	Semaine des examens finals

Il n'y a pas d'examen dans le cours. Il n'y a pas de cours durant les périodes d'examen, pour vous permettre de réaliser les travaux pratiques.

2.3 Évaluation

Type de l'évaluation	Pondération	Utilisation des IAG[1]
Planifier un test d'intrusion	40 %	Balisée
Réaliser un test d'intrusion éthique	40 %	Libre
Devoirs	20 %	Balisée

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

Il y a 10 devoirs à faire. Ils sont évalués en mode tout-ou-rien, c'est à dire qu'il faut respecter la démarche et atteindre l'objectif pour avoir les points.

Le travail pratique 1 est fait seul ou en équipe de 2 ou 3 personnes étudiantes.

Le travail pratique 2 est fait seul.

Les travaux et devoirs doivent être remis dans Moodle, les remises par courriel ne seront pas acceptées.

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

La date de remise des devoirs et des travaux pratiques est dans Moodle. Les retards ne sont pas tolérés.

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.

Je réponds généralement dans les 24h, moins les fins de semaines et jours fériés. Si vous m'écrivez vendredi après-midi, il est possible que je ne puisse vous répondre que le lundi matin suivant. Utilisez Teams de préférence, sauf pour les demandes de révisions de notes qui devront être faites par courriel.

3 Matériel nécessaire pour l'activité pédagogique

Vous devrez lancer des machines virtuelles (libre de droits) sur une architecture Intel sur votre poste de travail ou sur un fournisseur infonuagique.

[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.