



Département d'informatique
IFT 508 – Introduction aux attaques informatiques
Plan d'activité pédagogique
Automne 2026

Enseignant	Julio Tcheutchoua Wafo
Courriel :	julio.tcheutchoua.wafo@usherbrooke.ca
Local :	
Téléphone :	
Disponibilités :	Sur Teams en dehors des heures de cours. Par courriel.

Site web du cours : <https://moodle.usherbrooke.ca/course/view.php?id=45375>

Horaire Exposé magistral : Vendredi 15 h 30 à 18 h 20 salle D3-2040

Description officielle de l'activité pédagogique¹

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 trousseaux et outils de piratage de façon éthique. Connaître 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	3.0 heures d'exposé magistral par semaine 6.0 heures de travail personnel par semaine
Préalable	Avoir obtenu 45.0 crédits
Particularités	Aucune

¹<https://www.usherbrooke.ca/admission/fiches-cours/ift508>

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 Département d'informatique, constitue la version officielle.

1.1 Mise en contexte

Cette activité de formation s'inscrit en tant qu'activité optionnelle du baccalauréat en informatique. Son positionnement permet à l'étudiant d'acquérir les connaissances de base fondamentales à la compréhension de ce qu'est une attaque informatique.

Le cours est aussi offert également en tant que cours optionnel aux programmes de maîtrise en informatique et génie logiciel.

Le cours permet de contextualiser la mise en application des différentes techniques d'attaque cybernétique dans un contexte d'entreprise et des impacts que celles-ci peuvent occasionner dans un contexte d'entreprise.

1.2 Cibles de formation spécifiques

À la fin de ce cours, l'étudiante ou l'étudiant saura :

1. Maîtriser la nature, le rythme et les outils des cyberattaques contre divers types d'infrastructure
2. Savoir détecter les signes et artefacts d'une intrusion, pouvoir mesurer son ampleur et pouvoir en déterminer la chaîne causale
3. 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	Mise en contexte : portrait de la cybercriminalité, piratage éthique, modèles d'attaques informatiques	3	
2	Faillles humaines et physiques : méthodologie d'attaque, ingénierie sociale – cas de l'hameçonnage, influence et manipulation psychologique, accès physique à un ordinateur, usurpation d'identité et collecte d'information	3	
3	Stratégie de reconnaissance : encadrement des tests d'intrusion, méthodologie de prise d'empreinte, les essentiels (<i>Google Hacking</i> , <i>Google Dorking</i> , moteurs de recherche spécialisés, réseaux sociaux, etc.), énumération (IP, DNS)	3	
4	Stratégie de détection : rappels sur les réseaux TCP/IP, passerelle, masque, sous-réseau, services, ports, TCP/UDP, IP publiques et IP privées, analyse de l'entête Unix d'un courriel (RFC 5321 et RFC 5322), balayage de ports, détection d'un système d'exploitation, reniflage de paquets	3	
5	Exploitation des failles réseau : configuration par défaut, vulnérabilités non corrigées, déni de service, déni de service distribué, amplification et périphérique de démarrage, tunnel SSH, VoIP, WIFI, l'homme du milieu et jumeau maléfique	3	
6	Exploitation des failles système : configuration par défaut, vulnérabilités non corrigées, identification de mots de passe, élévation de privilèges, séquence de démarrage	3	
7	Exploitation des failles applicatives et web : OWASP, vulnérabilités non corrigées, dépassements de pile (<i>buffer overflow</i>), division par zéro, outrepasser les protections témoins, paramètres du client, etc.	3	

Thème	Contenu	Nbr. d'heures	Objectifs
8	Ne pas attirer l'attention : éviter d'être repéré (extraction des fichiers, signatures, détection d'anomalies, analyse des journaux, analyse des flux), éviter les pièges (pots de miel et réseaux leurres, etc.)	3	
9	Exfiltration : Marché noir, toile profonde, toile noire, etc.	3	
10	Gestion des incidents de sécurité et conclusion : processus de gestion des incidents de sécurité, mise en commun des lectures personnelles, partage d'expérience, retour sur les apprentissages, solution du CTF	3	

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

Le cours IFT508 – Introduction aux attaques informatiques privilégie la méthode d'apprentissage par démonstration et exécution, décomposée en quatre parties :

1. Explication des concepts théoriques par l'enseignant ;
2. Démonstration des cas pratiques par l'enseignant ;
3. Exécution par l'élève dans les travaux dirigés, laboratoires et projet ;
4. Encadrement et évaluation par l'enseignant.

La personne enseignante s'assure d'encadrer et de baliser le travail attendu de la part de la personne étudiante. Toutes les ressources et les consignes sont disponibles sur Moodle : <http://www.usherbrooke.ca/moodle2-cours/>.

2.2 Calendrier

Semaine	Commençant le	Thème	Devoirs
1	2026-08-31	1	
2	2026-09-07	2	Devoir #1
3	2026-09-14	3	Devoir #2
4	2026-09-21	4	
5	2026-09-28	Laboratoire	Quiz #1
6	2026-10-05	5 et 6	
7	2026-10-12	6	
8	2026-10-19	Semaine des examens périodiques	
9	2026-10-26	Relâche	
10	2026-11-02	Projet	Présentation du projet
11	2026-11-09	7	Quiz #2
12	2026-11-16	Laboratoire	Devoir #3
13	2026-11-23	8 et 9	
14	2026-11-30	10	
15	2026-12-07	Révision	
16	2026-12-14	Semaine des examens finals	
17	2026-12-21	Semaine des examens finals	

2.3 Évaluation

Type de l'évaluation	Pondération	Utilisation des IAG ¹
Devoirs (5)	25 %	Balisée 
Projet	35 %	Balisée 
Examen final	40 %	Interdite 

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

Les travaux sont individuels et doivent être remis uniquement en format électronique. Aucun document imprimé ne sera accepté. Le travail remis doit répondre aux exigences énoncées dans l'énoncé du devoir.

La présentation du projet et l'examen final sont informatisés et se feront en présentiel, au laboratoire et sous surveillance.

2.3.1 Qualité de la langue et de la présentation

Conformément à l'article 17 du Règlement facultaire d'évaluations des apprentissages² 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 études³. 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'avez 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.

2.4 Échéancier des travaux

Le devoir est à remettre avant le jour et l'heure indiqués comme étant la date de remise sur Moodle. Tout retard dans la remise des travaux sera sanctionné par une pénalité de 10 % de la note finale par jour de retard.

2.5 Utilisation d'appareils électroniques et du courriel

Selon le règlement complémentaire des études, section 4.2.3⁴, 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 4.2.3⁵, 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.

²https://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/>

⁴https://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/>

3 Matériel nécessaire pour l'activité pédagogique

Une machine personnelle Windows 10/11 avec les caractéristiques minimales recommandées suivantes :

- Processeur Intel Core i5 de 11ème génération ou AMD Ryzen 5 Mobile Processor de série 5000
- Mémoire RAM d'au moins 16 Go
- Disque dur SSD d'au moins 512 Go. (Les HDDs peuvent causer des ralentissements)
- Carte WIFI 802.11ac ou mieux.
- Idéalement, une carte graphique compatible avec OpenGL 4.x.
- Une résolution d'écran de 1080 lignes ou plus.
- Connexion Internet d'une vitesse minimale de 30 Mbps.

4 Références

- [1] ATT&CK : tactiques et techniques. est une base de connaissances accessible dans le monde entier sur les tactiques et techniques de l'adversaire, basée sur des observations du monde réel. <https://attack.mitre.org/matrices/enterprise/>.
- [2] CENTRE CANADIEN POUR LA CYBERSÉCURITÉ : Centre canadien pour la cybersécurité. <https://www.cyber.gc.ca/fr>.
- [3] CIS : Guide et normes. Center for Internet Security : pour le durcissement des systèmes d'exploitation. <https://www.cisecurity.org/>.
- [4] GEORGIA WEIDMAN : *Penetration Testing : A Hands-On Introduction to Hacking*. No Starch Press, 2014.
- [5] NIST : Normes. Institut national des normes et de la technologie américaine. <https://www.nist.gov/>.
- [6] OPEN WEB APPLICATION SECURITY PROJECT : OWASP. La sécurité des applications Web et guide de testing. <https://owasp.org/>.
- [7] PATRICK ENGBRETSON : *Les bases du hacking*. PEARSON EDUCATION, 2013.

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;

[...]

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

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](#).



Utilisation limitée

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



Utilisation guidée

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



Utilisation balisée

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 normes¹ 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



Utilisation libre

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 normes¹ 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.

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](#).