UNIVERSITÉ DE SHERBROOKE

1. IDENTIFICATION ET RENSEIGNEMENTS GÉNÉRAUX

Titre officiel du cours :	**INF808 – Réaction aux attaques et analyses des attaques**
Nombre de crédits :	3 crédits – 135 heures
Programme :	Microprogramme de 2e cycle en sécurité informatique - volet réaction
Cours préalables ou concomitants :	aucun
Lieu du cours :	Moodle
Session :	Automne 2020
Date de début :	31 août 2020
Date de fin :	21 décembre 2020
Date limite d'abandon :	15 novembre 2020
Rencontres synchrones :	
Personne(s)-ressource(s) :	Daniel Migault
Courriel(s) :	Daniel.Migault@USherbrooke.ca

2. MISE EN CONTEXTE

DESCRIPTION OFFICIELLE DU COURS

Cible(s) 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.

PLACE DU COURS DANS LE PROGRAMME

INF808 a pour but de sensibiliser les étudiants au déroulement des attaques connues et largement répandues aujourd'hui afin de pouvoir adresser les attaques futures. Les objectif du cours se déclinent de la manière suivante:

UNIVERSITÉ DE SHERBROOKE

1. Connaître les principaux types d'attaques
2. Analyser une attaque lorsqu'elle survient
3. Établir un plan d'intervention suite a une attaques
4. Mettre en place une solution afin de se protéger face a une telle attaque
5. Lier la gestion des risques et l'identification des attaques

OBJECTIFS DU MICROPROGRAMME[1]

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.

De manière générale, les attaques de demain seront différentes de celles d'aujourd'hui ;

- elles incluront toujours celles d'aujourd'hui…
- les usages seront différents
- les infrastructures seront différentes
- les solutions réseaux seront différentes
- la détection sera différente
- les risques seront différents
- les plans d'intervention seront différents

Il est difficilement imaginable de sortir de ce micro programme avec une procédure applicable en tout temps, en toutes circonstances. L'idée de ce cours est donc de vous donner des bases qui devront sans cesse être actualisées.

CHARGE DE TRAVAIL

Les 3 crédits équivalent à 135 heures, soit 45 heures de rencontres collectives et 90 heures de travail personnel, réparties de la façon suivante : (distinguer le temps de lecture personnelle, le

1Extrait de la fiche signalétique

temps de travail sur le site, le temps de réalisation des travaux, etc.)

Enseignement magistral	37 heures
Laboratoires en classe	12 heures
Conférences	2 heures
Lecture personnelle	45 heures
Activités de consolidation	45 heures
TOTAL	135 heures

3. DÉROULEMENT DU COURS

Séance	Description	Enseignant
Séance 1 : *31 août 2020*	Chapitre 1 – Introduction du cours	DM
Séance 2 : *14 septembre 2020*	Chapitre 2 – Attaques Cryptographiques (cryptographie symétriques)	DM
Séance 3 : *21 septembre 2020*	Chapitre 2 – Attaques Cryptographiques (cryptographie asymétrique)	DM
Séance 4 : *28 septembre 2020*	Chapitre 2 – Introduction a python3 / Travaux pratique	DM
Séance 5 : *05 octobre 2020*	Chapitre 3 – Attaques des protocoles réseau : ex :DNS	DM
Séance 6 : *19 octobre 2020*	Chapitre 3 – Attaques des protocoles réseau : ex :DNS (extension de sécurité, DoH, DoT)	DM

Séance 7 : *26 octobre 2020*	**Examen Intra**	DM
Séance 8 : *02 novembre 2020*	Chapitre 4 – Attaques DDoS	DM
Séance 9 : *09 novembre 2020*	Chapitre 4 – Attaques DDoS	DM
Séance 10 : *16 novembre 2020*	Chapitre 5 - Cyber Threat Intelligence	DM
Séance 11 : *23 novembre 2020*	Chapitre 6 - IPsec	DM
Séance 12 : *30 novembre 2020*	Chapitre 7 - Firewalls	DM
Séance 13 : *07 décembre 2020*	Chapitre 8 - TLS	DM
Séance 14 : *14 décembre 2020*	révision	DM
Séance 15 : *21 décembre 2020*	**Examen Final**	

4. CONSIDÉRATIONS MÉTHODOLOGIQUES

APPROCHES MÉTHODOLOGIQUE ET PÉDAGOGIQUE

Le cours INF808 privilégie une diversité de méthodes pédagogiques, dont la pratique réflexive, les groupes de discussion, l'apprentissage par problèmes, la méthode des cas et l'apprentissage par projet. Il est attendu que chaque individu participant au cours s'engage de manière active et régulière en intervenant dans les séances AdobeConnect et les forums de discussion.

Puisqu'il s'agit d'un cours en ligne, toutes les ressources et les consignes sont disponibles sur

UNIVERSITÉ DE SHERBROOKE

Moodle 2: http://www.usherbrooke.ca/moodle2-cours/.

5. ÉVALUATION DES APPRENTISSAGES

ÉVALUATION N^{O} 1: **Laboratoires**

- ***Compétence mobilisée:*** Compréhension d'une problématique de sécurité, application pratique.
- ***Description:*** Cf description plus bas
- ***Critères d'évaluation*** *Consulter Moodle*
- ***Notation:*** **15 %** de la note finale
- ***Date de remise:*** *Consultez Moodle*

ÉVALUATION N^{O} 2: **Quiz (plusieurs durant la session)**

- ***Compétence mobilisée:*** Compréhension du cours
- ***Description:***
- ***Critères d'évaluation*** *Consultez Moodle*
- ***Notation:*** **15 %** de la note finale
- ***Date de remise:*** *Consultez Moodle*

ÉVALUATION N^{O} 3: **Examen Intra**

- ***Compétence mobilisée:*** Compréhension globale du cours
- ***Description:***
- ***Critères d'évaluation*** *Consultez Moodle*
- ***Notation:*** **20 %** de la note finale
- ***Date de remise:*** *Consultez Moodle*

ÉVALUATION N^{O} 3: **Examen Final**

- ***Compétence mobilisée:*** Compréhension globale du cours
- ***Description:***
- ***Critères d'évaluation*** *Consultez Moodle*

- ***Notation:*** **20 %** de la note finale
- ***Date de remise:*** *Consultez Moodle*

ÉVALUATION N^{O} 5: **Rapport Technique**

- ***Compétence mobilisée:*** Présentation et exposition d'une thématique de son choix (validée par l'instructeur)
- ***Description:***
- ***Critères d'évaluation*** *Consultez Moodle*
- ***Notation*** **30 %** de la note finale
- ***:***

QUIZ

L'objectif du Quiz est de vérifier la compréhension du cours. Par défaut, il y aura un quiz par sceance de cours. Le quiz sera envoyé a l'avance et devra être effectue par l'étudiant sur mooddle.

Les Quizs comptent pour 15% de la note finale.

EXAMEN INTRA / FINAL

Les examen intra et finaux testeront la compréhension du cours. Il pourront comporter des questions théorique ainsi que des questions plus pratiques comme de la programmation.

Les questions / réponses pourront être de divers format comme des questions a choix multiples,

des questions ouvertes, voire du code en python.

Les examens seront entièrement faits sur moodle durant un séance dédiée et compteront chacun pour 20%.

LABORATOIRES

Le but du laboratoire est de permettre une approche plus pratique sur une problématique. Le laboratoire doit permettre a l'étudiant de réfléchir sur une problématique donnée, rechercher certaines informations, implémenter et tester.

Il y aura au moins un laboratoire pendant la session.

La soumission d'un laboratoire comportera un rapport sous format PDF avec les fichiers nécessaires comme des fichiers de codes ou des fichiers de donnes.

Le laboratoire compteront pour 15% de la note.

RAPPORT TECHNIQUE

Le rapport technique permettra a l'étudiant d'exposer une problématique de sécurité a l'ensemble des membres du groupe. La thématique est libre et devra être validée par l'enseignant au préalable. L'objectif est de permettre a l'étudiant d'explorer une thématique de son choix. La thématique pourra développer une expertise technique ou être un sujet exploratoire.

La démarche devra être exposée clairement ainsi que les objectifs cherches. Le sujet, la démarche devra être validée par l'enseignant.

Le rapport technique sera évaluée sur un rapport qui devra être remis sous format PDF ainsi qu'une présentation qui devra être remise sous format PDF également. La présentation sera donnée par l'étudiant pendant une séance préalablement choisie. La présentation devra durer environ 20 minutes en comprenant les questions.

Le rapport sera évalué par rapport a sa clareté, et sa capacité a remplir les objectifs fixes. L'examinateur évaluera le rapport indépendamment de la présentation et le rapport devra donc être un document contenant l'ensemble des informations nécessaires.

La présentation sera évaluée par rapport a sa clarete.

Il est attendu que le sujet choisi et les objectifs soient valides par l'enseignant. Un point optionnel a mi-parcours sera également fait avec l'enseignant afin de confirmer le contenu et la cohérence de ce dernier vis a vis des objectifs.

Le présentation en ligne comptera pour 30%.

6. RÈGLEMENTS ET AUTRES

PROMOTION DE LA QUALITÉ DE LA LANGUE

Pour promouvoir la qualité du français, les fautes d'orthographe, de lexique et de syntaxe sont prises en considération. Dans tous les travaux, elles seront comptabilisées comme suit : 0,25 pour chaque faute jusqu'à concurrence de 10 % de la note maximale pour chaque objet d'évaluation.

Vous êtes fortement encouragés à effectuer une relecture attentive des travaux avant leur remise officielle et à utiliser les outils de correction disponibles.

PRÉSENTATION DES TRAVAUX

Les travaux doivent obligatoirement être soumis sur le site Moodle 2 du cours à la date d'échéance prévue.

Les fichiers électroniques doivent obligatoirement être soumis en format PDF pour faciliter l'insertion de commentaires.

L'intitulé du fichier doit comprendre le numéro du travail, votre nom et votre prénom (exemple: pour le travail 1: Travail1_Nom_Prénom.docx).

DÉLITS RELATIFS AUX ÉTUDES[2]

Le terme « délit » désigne toute infraction ou toute tentative de commettre une infraction, ainsi que toute participation à une infraction ou à une tentative de commettre une infraction, par une personne assujettie à une règle qui lui est applicable en raison de son statut.

Outre la contravention à toute règle applicable à la personne assujettie en vertu d'une source autre que le Règlement des études (Règlement 2575-009), l'Université considère trois (3) types de délits : les délits relatifs aux études, les délits relatifs à l'Université ou aux membres de la communauté universitaire et les délits relatifs aux activités de stage. Ces délits sont présentés aux articles suivants :

Un délit relatif aux études désigne tout acte trompeur ou toute tentative de commettre un tel

2Extrait du Règlement des études 2017-2018

acte, quant au rendement scolaire ou une exigence relative à une activité pédagogique, à un programme d'études ou à un parcours libre. 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 ou des passages ou idées tirés de l'œuvre d'autrui (ce qui inclut notamment le fait de ne pas indiquer la source d'une production, d'un passage ou d'une idée tirés de l'œuvre d'autrui);
b) commettre un auto-plagiat, 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 aide non autorisée, qu'elle soit collective ou individuelle, pour une production faisant l'objet d'une évaluation;
e) copier, contrefaire ou falsifier un document pour l'évaluation d'une activité pédagogique.

RESPECT DES DÉLAIS[3]

Tout défaut de remplir les exigences d'évaluation prévues au plan de l'activité pédagogique, par exemple pour une production attendue ou un examen, entraîne la **valeur zéro (0)**, à moins que les raisons et les preuves fournies par l'étudiante ou l'étudiant n'aient été acceptées par la faculté ou le centre universitaire de formation.

L'étudiante ou l'étudiant doit **justifier par écrit** son défaut de se soumettre à une évaluation auprès de la faculté ou du centre universitaire de formation. Cette justification doit être **déposée dans le respect du délai** déterminé au règlement complémentaire de la faculté ou du centre universitaire de formation.

Le cas échéant, la faculté ou le centre universitaire de formation peut accorder un délai pour la présentation d'une production, soumettre l'étudiante ou l'étudiant à un examen supplémentaire, apporter des modifications aux exigences de stage ou ne pas tenir compte de cet élément d'évaluation dans l'attribution de la note finale.

7. NOTATION

Comment une cote est évaluée au CeFTI ?

3Extrait du Règlement des études 2017-2018

L'attribution d'une cote au CeFTI n'a rien du hasard. Les enseignants doivent identifier les frontières de cote en fonction d'un modèle basé sur la loi de probabilité de Laplace-Gauss. Voici les règles d'attribution en vigueur au CeFTI.

1. Identification d'une moyenne cible pour l'activité par la direction

- Début de programme : [2,6..3,0]
- Milieu de programme : [2,9..3,3]
- Fin de programme : [3.2..3,7]

2. L'enseignant propose des coupures en conformité avec le règlement des études de l'Université, https://www.usherbrooke.ca/registraire/droits-et-responsabilites/reglement-des-etudes/

- A+, A, A- : Excellent
- B+, B, B- : Très bien
- C+, C, C- : Bien
- D+, D : Passable
- E : Échec

3. Les cotes sont transmises à la direction du CeFTI avant d'être officialisées.

L'avantage d'un tel système est la transposition du rendement de l'étudiant en fonction du groupe dans lequel il évolue. L'évaluation reste équitable entre les cohortes. L'enseignant a la liberté de proposer une répartition qui déroge de la règle, lorsqu'il juge avoir un groupe particulier.

Ce processus a été discuté et approuvé par le comité de programme au CeFTI le 25 mai 2017.

RÉVISION D'UNE NOTE[4]

L'Université reconnaît à toute étudiante ou étudiant le droit à une révision de la note finale sous forme de lettre qui lui est attribuée pour une activité pédagogique ou le test institutionnel de français (TIF), à la condition qu'elle ou qu'il en fasse la demande au moyen du formulaire institutionnel **au plus tard vingt (20) jours ouvrables** après que la note confirmée par la faculté ou le centre universitaire de formation apparaît à son dossier.

8. RÉFÉRENCES BIBLIOGRAPHIQUES

4Extrait du Règlement des études 2017-2018

Afin de suivre l'actualité en matière de sécurité, on suivra par exemple les blogs suivants :

* [Krebs on Security](https://krebsonsecurity.com/)

* [Schneier on Security](https://www.schneier.com/)