UNIVERSITÉ DE SHERBROOKE

1. IDENTIFICATION ET RENSEIGNEMENTS GÉNÉRAUX

Titre officiel du cours :	**INF808/IFT511 – 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 2023
Date de début :	28 août 2023
Date de fin :	18 décembre 2023
Date limite d'abandon :	15 novembre 2023
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 :

Le contenu du cours est divisé en chapitres dans lesquels on aborde les différents types de cyberattaques, la manière de les détecter et de les contrer. En effet, bien que le chiffrement permette de protéger les données et les communications, une mauvaise mise en pratique présente un certain nombre de vulnérabilités, conférant ainsi une fausse idée de protection.

Le cours commencera donc avec le chapitre 1 qui décrit certains principes du chiffrement et expose les attaques afin de dégager des grands principes qui permettent de conférer au chiffrement la protection attendue. **Cette partie sera suivie d'un laboratoire qui se fera à l'aide d'un interpréteur du langage de programmation Python. Il est conseillé aux étudiants et**

étudiantes de connaître le langage Python à l'avance. Toutefois, les fonctions vues pendant le cours restent celles de bases et sont utilisées à des fins pédagogiques lors de la réalisation de travaux pratiques. Il peut être donc être appris lors de ce laboratoire mais il faudra prévoir du temps additionnel de travail personnel.

Le chapitre 2 illustre à partir de l'infrastructure et protocole DNS, comment détecter et protéger une infrastructure. On étudiera en particulier les attaques par amplifications, les botnets de type (double) fast flux ainsi que la génération « aléatoire » de nom de domaine afin d'établir un canal entre le botnet et son centre de commande et contrôle (DGA). On étudiera comment détecter et contrer de tels botnets. Enfin nous aborderons les aspects liés à la vie privée des résolutions DNS avec les différents déploiements de DNS sur TLS (DoT), DNS sur HTTPS (DoH) ainsi que les problèmes associés à la concentration de l'Internet.

Le chapitre 3 décrit le *Cyber Threat Intelligence* qui modélise la stratégie d'un attaquant et décrit le *killchain* ainsi que le *diamond model*. Ces deux modèles seront illustrés à l'aide des exemples d'attaques des centrales électriques Ukrainiennes ainsi que les attaques *Energetic Bears*. Ce chapitre decrira Le modele STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) qui a été initialement créé dans le cadre du processus de modélisation des menaces. STRIDE est un modèle de menaces, utilisé pour aider à raisonner et trouver des menaces sur un système. Il est utilisé en conjonction avec un modèle du système cible qui peut être construit en parallèle. Il est souvent utilisé par les experts en sécurité pour aider à répondre à la question "qu'est-ce qui peut mal tourner dans ce système sur lequel nous travaillons ?". Ce chapitre aborde egalement la matrice ATT&CK (pour Adversarial Tactics, Techniques, and Common Knowledge). Cette matrice est une base de connaissance aidant a modeler les tactiques et techniques utilisées par les cyberadversaires, ainsi qu'a comprendre comment les détecter et les stopper. Cette base de connaissance classifie et décrit les cyberattaques et les intrusions. Ce chapitre approndira l'analyse et la detection d'attaques en decrivant les outils et les methodologies du thread hunting.

Le chapitre 4 illustrera avec IPsec, la façon d'établir une communication chiffrée. Il illustre la mise en place d'une politique de sécurité et la protection associée à un *Virtual Private Network* (VPN) ainsi que la mise en pratique de divers principes cryptographiques auxquels l'étudiant et l'étudiante devra être familier. Il permettra également d'introduire la définition de protocole réseaux et les familiarisera avec les standards publiés par l'*Internet Engineering Task Force* (IETF). **Ce bref chapitre sera suivi d'un laboratoire qui permettra de continuer la familiarisation avec le langage Python.**

Le chapitre 5 se concentre sur les aspects DDoS. Ce chapitre détaille les mises en place d'attaques de type DDoS en utilisant différents protocoles et les différents types d'attaques DDoS

(volumétriques, réseaux, applicatives). On étudiera différentes manières de réagir à de telles attaques avec la mise en place de stratégies de réaction de type filtrage, des stratégies de réaction collaboratives (Pushback, SDN, DOTS, outsourcing…). Afin de monitorer l'activité du web, on étudiera le principe du télescope avant d'étudier deux exemples concrets que sont le DDoS-as-a service, et le botnet Mirai.

Le chapitre 6 permet d'aborder de manière optionnelle et si le temps le permet, divers sujets tels que c*onfidential computing* qui permet l'utilisation d'une infrastructure publique tout en se protégeant contre des attaques de type surveillance passive. Ce chapitre décrit l'architecture mise en place par Intel (SGX) ainsi que le principe de l'attestation.

D'autres sujets comme TLS 1.3, le fonctionnement d'un firewall, la sécurité du web, entre autres pourront etre abordes egalement.

La dernière séance (avant l'examen) est dédiée à la présentation des travaux personnels des étudiants et étudiantes. Le sujet sera choisi en accord avec le professeur pendant la session.

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 objectifs du cours se déclinent de la manière suivante:

1. Connaître les principaux types d'attaques
2. Analyser une attaque lorsqu'elle survient
3. Établir un plan d'intervention suite à une attaque
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]

[1]Extrait de la fiche signalétique

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.

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

Enseignement magistral	37 heures
Laboratoires (Python)	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 : *28 août 2023*	Introduction du cours	DM

Séance 2 : *11 septembre 2023*	Chapitre 1 – Attaques Cryptographiques (cryptographie symétrique) Lab 1 (Python)	DM
Séance 3 : *18 septembre 2023*	Chapitre 1 – Attaques Cryptographiques (cryptographie symétrique) Chapitre 2 – Détection et réaction aux attaques DNS	DM
Séance 4 : *25 septembre 2023*	Chapitre 2 – Détection et réaction aux attaques DNS	DM
Séance 5 : *16 octobre 2023*	Chapitre 2 – Détection et réaction aux attaques DNS	DM
Séance 6 : *23 octobre 2023*	Chapitre 3 – Cyber Threat Intelligence	DM
Séance 7 : *30 octobre 2023*	**Examen Intra**	DM
Séance 8 : *06 novembre 2023*	Chapitre 3 – Cyber Threat Intelligence	DM
Séance 9 : *13 novembre 2023*	Chapitre 3 – Cyber Threat Intelligence	DM
Séance 10 : *20 novembre 2023*	Chapitre 4 – Analyse d'une canal chiffré et mise en place d'une politique de sécurité (VPN) Lab 2 (Python)	DM
Séance 11 : *27 novembre 2023*	Chapitre 5 - Réaction aux attaques de type DDoS	DM
Séance 12 : *04 décembre 2023*	Chapitre 5 - Réaction aux attaques de type DDoS	DM
Séance 13 : *11 décembre 2023*	Chapitre 7 – (Optionnel) TLS, Firewalls, Securite du Web	DM
Séance 14 :	**Examen final**	DM

18 décembre 2023		

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 Teams et les forums de discussion.

Puisqu'il s'agit d'un cours en ligne, toutes les ressources et les consignes sont disponibles sur Moodle 2: http://www.usherbrooke.ca/moodle2-cours/.

5. ÉVALUATION DES APPRENTISSAGES

ÉVALUATION N^{O} 1: **Laboratoires**

- ***Critères d'évaluation*** *Consulter Moodle*
- ***Notation:*** **30 %** de la note finale
- ***Date de remise:*** *Consultez Moodle*

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

- ***Critères d'évaluation*** *Consultez Moodle*
- ***Notation:*** **10 %** de la note finale
- ***Date de remise:*** *Consultez Moodle*

ÉVALUATION N^{O} 3: **Examen Intra**

- ***Critères d'évaluation*** *Consultez Moodle*
- ***Notation:*** **30 %** de la note finale
- ***Date de remise:*** *Consultez Moodle*

ÉVALUATION N^{O} 3: **Examen final**

- ***Critères d'évaluation*** *Consultez Moodle*
- ***Notation:*** **30 %** de la note finale
- ***Date de remise:*** *Consultez Moodle*

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.

UNIVERSITÉ DE SHERBROOKE

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 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;

[2]Extrait du Règlement des études 2017-2018

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 ?

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

[3]Extrait du Règlement des études 2017-2018

- 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

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/)

[4]Extrait du Règlement des études 2017-2018