UNIVERSITÉ DE SHERBROOKE

1. IDENTIFICATION ET RENSEIGNEMENTS GÉNÉRAUX

Titre officiel du cours :	**INF805 – Introduction aux attaques informatiques**
Nombre de crédits :	3 crédits – 135 heures
Programme :	Microprogramme de 2e cycle en sécurité informatique - volet réaction Diplôme d'étude supérieures spécialisées de 2e cycle en sécurité informatique Maîtrise en génie logiciel Maîtrise en informatique
Cours préalables ou concomitants :	INF801 – Concept de base en sécurité des TI
Lieu du cours :	Moodle
Session :	Automne 2021
Date de début :	1 septembre 2021
Date de fin :	8 décembre 2021
Date limite d'abandon :	À confirmer
Rencontres synchrones :	Chaque mercredi de 18:30 à 21:30
Personne(s)-ressource(s) :	Éric Daigneault
Courriel(s) :	eric.daigneault@usherbrooke.ca

2. MISE EN CONTEXTE

DESCRIPTION OFFICIELLE DU COURS

Cible(s) 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.

PLACE DU COURS DANS LE PROGRAMME

Cette activité de formation s'inscrit en tant qu'activité obligatoire du microprogramme de 2e cycle en sécurité informatique – volet réaction. 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.

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.

[1] Extrait de la fiche signalétique

UNIVERSITÉ DE SHERBROOKE

OBJECTIFS DU DESS[2]

Ce diplôme vise à mettre à niveau des professionnels et des professionnelles en exercice dont l'expertise en cybersécurité répondra aux nouvelles réalités mondiales en matière de cyberattaque.

Plus précisément, il permettra à la personne étudiante de :

- Maîtriser les tenants et aboutissants de la sécurité informatique contemporaine;
- Maîtriser la nature des surfaces d'attaque exposées par une infrastructure de TI;
- Savoir concevoir, mettre en œuvre et documenter une stratégie efficace pour protéger et défendre ces surfaces d'attaque, en tenant compte d'un budget de ressources donné;
- Pouvoir critiquer une telle stratégie telle que mise en place dans une organisation, de manière à en corriger les faiblesses;
- 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 trois (3) crédits équivalent à 135 heures, réparties de la façon suivante :

Enseignement magistral	25 heures
Laboratoire en classe (étude de cas et/ou simulation)	20 heures
Lecture personnelle	45 heures
Lectures	14 heures
TOTAL	135 heures

[2] Extrait de la fiche signalétique

3. DÉROULEMENT DU COURS

Module	Description
Séance 1 : **Rencontre de démarrage et mise en contexte** *1 septembre 2021*	• Présentation du cours INF805 • Présentation de la trousse à outils • Portrait de la cybercriminalité • Piratage éthique • Modèles d'attaques informatiques
Séance 2 : **Failles humaines et physiques** *8 septembre 2021*	• 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 • **Labo** : Maltego CE, etc.
Séance 3 : **Stratégie de reconnaissance** *15 septembre 2021*	• Encadrement des tests d'intrusion • Méthodologie de prise d'empreinte • Les essentiels (Google Hacking, Google Dorking, moteurs de recherche spécialisés, réseaux sociaux, etc.) • Énumération (IP, DNS) • **Labo** : Shodan, Whois, NSLookup, Host, Dig, MXToolbox, Dmitry, Nmap…
Séance 4 : **Stratégie de détection** *22 septembre 2021*	• Rappel 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) • Scan de ports • Détection d'un système d'exploitation • Reniflage de paquets • **Labo** : Nessus, Wireshark, Nmap, etc.

Séance 5 : Retour d'expérience *29 septembre 2021*	• Réponses aux questions • Résolution en groupe des problèmes rencontrés dans la définition de votre stratégie de reconnaissance et l'utilisation des outils.
Séance 6 : Failles réseau et exploitation *6 octobre 2021*	• Configuration par défaut • Vulnérabilités non corrigées • Déni de service, déni de service distribué, amplification et « booter » • Tunnel SSH, VoIP, WIFI • L'homme du milieu et jumeau maléfique • **Labo** : Sparta (nmap, nickto, etc.), Armitage
Séance 7 : Failles système et exploitation *13 octobre 2021*	• Configuration par défaut • Vulnérabilités non corrigées • Identification de mots de passe • Élévation de privilèges • Séquence de démarrage • **Labo** : Metasploit
Séance 8 : Retour d'expérience *20 octobre 2021*	• Réponses aux questions • Résolution en groupe des problèmes rencontrés dans l'exploration des outils de la suite Kali-Linux pour l'exploitation des failles de type réseau et système
Séance 9 : Failles applicative *27 octobre 2021*	• OWASP • Vulnérabilités non corrigées • Dépassements de pile (*buffer overflow*) • Division par zéro • Outrepasser les protections cookies, paramètres du client, etc. • **Labo** : Metasploit
Séance 10 : Failles web *3 novembre 2021*	• OWASP • Technologies Web et échanges HTML • Saisie de données inattendues (URL, formulaire, entête, cookies) • Détournement de CAPTCHA • Principe des injections SQL

	• **Labo** : Metasploit
Séance 11 : Retour d'expérience *10 novembre 2021*	• Réponses aux questions • Résolution en groupe des problèmes rencontrés dans l'exploration des outils de la suite Kali-Linux pour l'exploitation des failles de type applicative et web
Séance 12 : Ne pas attirer l'attention *17 novembre 2021*	• Éviter d'être repéré (extraction des fichiers, signatures, détection d'anomalies, analyse des journaux, analyse des flux) • Éviter les pièges (*honey pots and honey net*, etc.)
Séance 13 : Exfiltration *24 novembre 2021*	• Marché noir, Deep Web, Dark Web, Dark Net, etc. • **Labo** : Tor, Onion
Séance 14 : Incident de sécurité *1 décembre 2021*	• Processus de gestion des incidents de sécurité
Séance 15 : Conclusion *8 décembre 2020*	• Mise en commun des lectures personnelles • Partage d'expérience • Retour sur les apprentissages • Solution du CTF

4. CONSIDÉRATIONS MÉTHODOLOGIQUES

APPROCHES MÉTHODOLOGIQUE ET PÉDAGOGIQUE

Le cours **INF805 – Introduction aux attaques informatiques** 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.

L'enseignant permet d'encadrer et de baliser le travail attendu de la part de l'étudiant

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: **Élaboration d'une stratégie de test d'intrusion**

- ***Compétence mobilisée:*** Comprendre les étapes d'une cyberattaque. Faire la recherche d'informations sur une cible d'attaque. Différencier les types d'attaques. Connaître les techniques pour détecter des cyberattaques.
- ***Description:*** Rédiger un rapport sur la démarche et les outils envisagés pour répondre à la demande d'un client qui souhaite avoir un test d'intrusion sur un de ses systèmes informatiques.
- ***Critères d'évaluation*** *Pour les consignes précises, de même que les modalités de remise et la grille d'évaluation, consultez Moodle.*
- ***Notation:*** 50 % de la note finale
- ***Date de remise:*** Séance 10, 3 novembre 2021 18:29 (Avant le cours)

ÉVALUATION N^{O} 2: **Défi de piratage éthique**

- ***Compétence mobilisée:*** Comprendre les étapes d'une cyberattaque. Différencier les types d'attaques. Utiliser des trousses et outils de piratage de façon éthique.
- ***Description:*** Appliquer les techniques et outils de test d'intrusion utilisés dans le cours afin d'identifier puis si possible exploiter les vulnérabilités d'un système livré par l'enseignant dans un environnement de laboratoire.
- ***Critères d'évaluation*** *Pour les consignes précises, de même que les modalités de remise et la grille d'évaluation, consultez Moodle.*
- ***Notation:*** 50 % de la note finale
- ***Date de remise:*** Séance 14, le 8 décembre 2021 18:29 (Avant le cours)

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[3]

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);

[3] Extrait du Règlement des études 2019-2020

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[4]

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]

[4] Extrait du Règlement des études 2019-2020

- 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[5]

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

Learning-Kali-Linux (O'Reilly, Rick Messier, 2018)

Par ailleurs, les étudiants sont incités à élaborer leur propre bibliographie à la partager avec les autres étudiants sur le forum du cours. Pour cela, les étudiants sont incités à utiliser les services de la bibliothèque de l'Université de Sherbrooke ainsi que les services ressources numériques de la Bibliothèque et Archives nationales du Québec (BAnQ).

[5] Extrait du Règlement des études 2019-2020