UNIVERSITÉ DE SHERBROOKE

IDENTIFICATION ET RENSEIGNEMENTS GÉNÉRAUX

Titre officiel du cours :	**INF801 - Concepts de base de la sécurité en TI**
Nombre de crédits :	3 crédits – 135 heures
Programme :	Microprogramme de 2e cycle en sécurité informatique - volet prévention
Cours préalables ou concomitants :	aucun
Lieu du cours :	Moodle
Session :	Automne 2020
Date de début :	3 septembre 2020
Date de fin :	20 octobre 2020
Date limite d'abandon :	15 septembre 2020
Rencontres synchrones :	(18h à 21h) **Mardis** : 1 septembre 8 septembre 15 septembre 22 septembre 29 septembre 6 octobre 13 octobre 20 octobre **Jeudis** : 3 septembre 10 septembre 17 septembre 24 septembre 1 octobre 8 octobre 15 octobre
Personne(s)-ressource(s) :	Dominic Brodeur, Pierre-Martin Tardif
Courriel(s) :	Dominic.Brodeur@usherbrooke.ca Pierre-Martin.Tardif@USherbrooke.ca

UNIVERSITÉ DE SHERBROOKE

1. MISE EN CONTEXTE

DESCRIPTION OFFICIELLE DU COURS

Cible(s) de formation :

Comprendre les fondements de la sécurité informatique (C1), dont la cryptologie (C2), la cybersécurité (C3) et l'authentification (C4). Comprendre et maîtriser les technologies de la sécurité (C5).

Contenu :

La sécurité en TI aujourd'hui ; sécurisation de la base avant les attaques trop avancées ; analyse et gestion de la sécurité et du risque; authentification. Sécurité dans le développement logiciel, sensibilisation à l'hameçonnage et à l'ingénierie sociale téléphonique; notions de système d'exploitation et de réseau; les vulnérabilités et les menaces communes, les attaques communes, les bonnes pratiques de base pour l'authentification, la segmentation réseau; introduction à la cryptographie; sécurité des mobiles; sécurité dans l'approche « prenez vos appareils personnels » (PAP) (*bring your own device*); sécurité des systèmes opérationnels (OT); sécurité des systèmes de contrôle industriels (ICS); modélisation de menaces.

PLACE DU COURS DANS LE PROGRAMME

INF801 est le premier cours du programme. Il donne une perspective large sur ce qu'est la cybersécurité, ses enjeux et certaines solutions existantes.

OBJECTIFS DU MICROPROGRAMME[1]

Le Microprogramme en sécurité informatique - volet prévention permet à l'étudiante ou à l'étudiant 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.

[1] Extrait de la fiche signalétique

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	39 heures
Laboratoire	6 heures
Lecture personnelle	45 heures
Activités de consolidation	45 heures
TOTAL	135 heures

2. DÉROULEMENT DU COURS

Séance	Description	Enseignant
Séance 1 : Introduction à la cybersécurité *1 septembre 2020* (C1), (C2)	• Présentation du cours • Sécurité – sécurité de l'information – cybersécurité • Dépendance technologique • État actuel de la cybersécurité	DB
Séance 2 : Concepts de base en cybersécurité *3 septembre 2020* (C1), (C2)	• Par où commencer ? • Modèles • Agent de menace • Actif informationnel • Classification des actifs • Sécurité physique, logique • Veille Quiz Séance 1 et 2	PMT
Séance 3 : Vulnérabilités et menaces communes *8 septembre 2020* (C5)	• Impacts des brèches de sécurité • Type d'attaques • Types de menaces • Vulnérabilités les plus communes • Comment se protéger, périmètre • Défense active Quiz Séance 3	DB
Séance 4 : Aspects humains *10 septembre 2020* (C1)	• Sensibilisation • Piratage psychologique • Facteurs de motivation Quiz Séance 4	PMT

UNIVERSITÉ DE SHERBROOKE

Séance	Description	Enseignant
Séance 5 : Modélisation des menaces *15 septembre 2020* (C2)	• Différence méthode de modélisation • Analyse comportementale • Gestion des événements de sécurité de l'information • Pattern d'attaque • Cycle de vie d'une attaque • Types de contrôles • Un exemple réel Quiz Séance 5	DB
Séance 6 : Cryptologie *17 septembre 2020* (C2), (C5)	• Historique • Principes • Algorithmes classiques • Protocoles • Informatique quantique Quiz Séance 6	PMT
Séance 7 : Analyse et gestion du risque de cybersécurité *22 septembre 2020* (C2)	• Gouvernance en gestion de la sécurité • Processus de gestion de la sécurité • Modèle de gestion du risque • Investissements en sécurité, ROSI Quiz Séance 7	DB
Séance 8 : Notions de base pour les systèmes d'exploitation et les réseaux *24 septembre 2020* (C2), (C5)	• Couches logicielles • Architecture de variantes populaires (Android, iOS, Linux, MacOS, Windows) • Couches OSI • Protocole TCP/IP • Composants d'un réseau **EXAMEN INTRA, séance 1 à 7**	PMT
Séance 9 : Gestion des identités et des accès *29 septembre 2020* (C1), (C4), (C5)	• Processus / cycle de vie • Sécurité en profondeur • Gestion des accès modèle cloud et vue holistique, Chaîne de confiance • IAAA • Biométrie, MFA • Contrôles d'accès • Les modèles de gestion des accès • Vulnérabilités et types d'attaque Quiz Séance 9	DB

Séance	Description	Enseignant
Séance 10 : Sécurité des appareils mobiles *1 octobre 2020* (C3), (C5)	• Sécurité physique • Authentification • BYOD Quiz Séance 10	PMT
Séance 11 : Protection des systèmes *6 octobre 2020* (C3), (C5)	• Architecture entreprise • Modélisation réseau • Segmentation de réseau • Durcissement d'un système • Pare-feu • Sécurité en profondeur • Architecture cloud IaaS, PaaS, SaaS • Sécurité avant et après le Cloud • CASB Courtiers de sécurité d'accès au nuage • Menaces et contrôle de l'environnement cloud Quiz Séance 11 Remise Laboratoire en ligne de CrypTool	DB
Séance 12 : Sécurité dans le développement logiciel *8 octobre 2020* (C1), (C5)	• Cycle de vie de développement d'un logiciel • Définition des besoins et exigences en sécurité • Analyse des exigences • Architecture de sécurité • Développement sécuritaire • Tests • Mises à jour • Retour sur OWASP top 10 Quiz Séance 12	PMT
Séance 13 : Technologies émergentes *13 octobre 2020* (C5)	• Systèmes opérationnels • Appareils intelligents, assistant vocal • Internet des objets • Intelligence artificielle Quiz Séance 13	DB

Séance	Description	Enseignant
Séance 14 : Infrastructures nationales critiques *15 octobre 2020* (C3), (C5)	• Définition • Systèmes de type SCADA • Systèmes en grille • Mesures gouvernementales	PMT
Séance 15 : Examen final *20 octobre 2020*	Examen final sur Moodle	DB

3. CONSIDÉRATIONS MÉTHODOLOGIQUES

APPROCHES MÉTHODOLOGIQUE ET PÉDAGOGIQUE

Le cours INF801 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 Moodle 2: http://www.usherbrooke.ca/moodle2-cours/.

4. ÉVALUATION DES APPRENTISSAGES

ÉVALUATION N^{O} 1: **QUIZ**

- ***Compétence mobilisée:*** Comprendre les fondements de la sécurité informatique (C1), dont la cryptologie (C2), la cybersécurité (C3) et l'authentification (C4) Comprendre et maîtriser les technologies de la sécurité (C5).
- ***Description:*** Sous la forme d'un quiz en ligne de 3 questions qui est à faire à la fin de chaque séance, de 18h45 à 19h00
- ***Critères d'évaluation*** Choix de la bonne réponse donne les points, 0 autrement.
- ***Notation:*** 11 quiz de 3 points chacun, 30% (les 10 meilleures Quiz comptent)
- ***Date de remise:*** 3, 8, 10, 15, 17, 22, 29 septembre (7 quiz)

  1, 6, 8, 13 octobre (4 quiz)

UNIVERSITÉ DE SHERBROOKE

ÉVALUATION N^{O} 2: **Laboratoire enligne de CrypTool**

- ***Compétence mobilisée:*** Comprendre les fondements de la sécurité informatique (C1), dont la cryptologie (C2)
- ***Description:*** Réaliser différents essais en cryptographie pour ensuite rapporter le résultats de ces observations.
- ***Critères d'évaluation*** *Pour les consignes précises, de même que les modalités de remise et la grille d'évaluation, consultez Moodle 2.*
- ***Notation:*** 15 %
- ***Date de remise:*** 6 octobre 2020

ÉVALUATION N^{O} 3: **EXAMEN INTRA**

- ***Compétence mobilisée:*** Comprendre les fondements de la sécurité informatique (C1), dont la cybersécurité (C3)
- ***Description:*** Sous la forme d'un quiz contenant 1 question à développement (10 pts) et 10 questions à choix multiples (1 pt chacune), démontrer la compréhension des principaux concepts en sécurité de l'information et de la cybersécurité. Il s'agit d'un examen d'une heure à faire sur la plateforme Moodle.
- ***Critères d'évaluation*** Parmi les critères:
  - Justesse et complétude de la réponse
  - Richesse des éléments fournis
- ***Notation:*** 20 %
- ***Date de remise:*** 24 septembre 2020, de 18h00 à 19h00

ÉVALUATION N^{O} 4: **EXAMEN FINAL**

- ***Compétence mobilisée:*** Comprendre les fondements de la sécurité informatique (C1), dont la cryptologie (C2), la cybersécurité (C3) et l'authentification (C4) Comprendre et maîtriser les technologies de la sécurité (C5).
- ***Description:*** Sous la forme d'un quiz contenant 2 questions à développement (10 pts) et 25 questions à choix multiple (25 pts), démontrer la compréhension de la matière vue dans le cours. Il s'agit d'un examen de trois heures à faire sur la plateforme Moodle.
- ***Critères d'évaluation*** *Pour les consignes précises, de même que les modalités de remise et la grille d'évaluation, consultez Moodle 2.*

  Parmi les critères:
- ***Notation:*** 35 %
- ***Date de remise:*** 20 octobre 2020, de 18h00 à 21h00

5. 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]

[2] Extrait du Règlement des études 2017-2020

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;
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**

[3] Extrait du Règlement des études 2017-2020

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.

6. 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
- 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.

7. RÉFÉRENCES BIBLIOGRAPHIQUES

Obligatoire

Shon Harris et Fernando Maymim, All in one CISSP exam guide, 8th edition, McGraw Hill Education, 2018, 1408 pages.

[4] Extrait du Règlement des études 2017-2020