UNIVERSITÉ DE SHERBROOKE

1. IDENTIFICATION ET RENSEIGNEMENTS GÉNÉRAUX

Titre officiel du cours :	**INF803 - Sécurité des systèmes**
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 :	Hiver 2022
Date de début :	6 janvier 2022
Date de fin :	14 avril 2022
Date limite d'abandon :	15 mars 2022
Rencontres synchrones :	Tous les jeudis de 18 h 30 à 21 h 30
Personne(s)-ressource(s) :	Stéphane Martel
Courriel(s) :	Stephane.Martel@USherbrooke.ca

2. MISE EN CONTEXTE

DESCRIPTION OFFICIELLE DU COURS

Cible(s) de formation :

Connaître et maîtriser les principaux systèmes d'exploitation disponibles sur le marché. Savoir renforcer la sécurité de ces systèmes. Comprendre les enjeux de sécurité entourant la virtualisation et les systèmes mobiles.

Contenu :

Sécurisation des réseaux. Sécurisation des systèmes d'exploitation. Sécurisation du Web et du nuage. Cryptographie. Sécurité des systèmes mobiles.

UNIVERSITÉ DE SHERBROOKE

PLACE DU COURS DANS LE PROGRAMME

L'objectif de formation est de réaliser un survol des principales perspectives théoriques et pratiques des principaux systèmes d'exploitation disponibles et d'assurer la sécurité entre elles.

OBJECTIFS DU MICROPROGRAMME[1]

Le microprogramme en sécurité informatique - volet prévention permet à l'étudiante et 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.

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	33 heures
Laboratoires en classe	10 heures
Conférences	2 heures
Lecture personnelle	45 heures
Activités de consolidation	45 heures
TOTAL	135 heures

[1] Extrait de la fiche signalétique

3. DÉROULEMENT DU COURS

Séance	Description	Enseignant

Séance 1 : Système d'exploitation et Poste de travail	• Présentation du cours
	• Présentation des différents systèmes d'exploitation
	• Windows 10 Environnement
	• Sécurité sur Windows 10
	  ○ Windows Defender
	  ○ Pare-feu
	  ○ Localisation de l'appareil
		SM

Séance 2 : Introduction à Windows Serveur	• Versions (éditions) de Windows • Architecture, installation et configuration • Rôles et fonctionnalités • Virtualisation, « Bac à sable » • Hyper V • Unix -Linux	SM
Séance 3 : Gestion et outils d'administration	• Gestionnaire de serveur • Service de domaine Active Directory • Les outils d'administration • LDAP, infrastructure logique, physique, site, forêt, domaine	SM
Séance 4 : Profils et permission	• Gestion des objets (utilisateurs, groupes…) • Unité d'organisation • Profils d'utilisateurs, script d'ouverture de session • Permission de partage	SM

UNIVERSITÉ DE SHERBROOKE

Séance	Description	Enseignant
Séance 5 : Stratégie et héritage d'accèes	• DFS (Distributed File System) • Infrastructure de stratégies de groupe (Group Policy) • Gestion des accès, héritages et restrictions • Comprendre les forêts ESAE	SM
Séance 6 : Gestion des accès et mise à jour	• Gestion des identités et des accès (GIA) • L'utilisation de l'authentification forte • Mise à jour de Windows Server WSUS	SM
Séance 7 : Serveur Web et Cloud	• Serveur web IIS • Azure AD • Cloud	SM
Séance 8 : Examen Pratique	• Connaître et maîtriser les principaux systèmes d'exploitation disponibles sur le marché.	SM
Séance 9 : Attaques et détection de brèche	• Comprendre les attaques • Utilisation d'un logiciel SIEM	SM
Séance 10 : Audit	• Auditer les événements d'ouverture de session sur un compte • Auditer la gestion des comptes utilisateur • Auditer les ouvertures et fermetures de sessions • Auditer les changements de stratégie • Auditer l'utilisation des privilèges	SM

Séance	Description	Enseignant
Séance 11 : Mettre en place une stratégie de récupération et Outils de sécurité	• Protection contre les menaces • Protection des données • Mettre en place la réplication Hyper-V • Windows Defender et Device Guard • Utiliser les stratégies de restriction des logiciels	SM
Séance 12 : Déploiement d'une infrastructure de serveurs	• Présentation de l'architecture haute disponibilité • Qu'est-ce qu'un cluster • Répartiteur de charge	SM
Séance 13 : PowerShell	• Notion de base sur l'outil PowerShell • Comment utiliser l'outil PowerShell en sécurité informatique	SM
Séance 14 : Sécuriser l'infrastructure de virtualisation	• Machines virtuelles protégées • Utiliser Security Compliance Manager • Introduction aux Nano servers • Comprendre les conteneurs	SM
Séance 15 : Système mobile	• Mobile Device Management • Mobile Application Management	

4. CONSIDÉRATIONS MÉTHODOLOGIQUES

APPROCHES MÉTHODOLOGIQUE ET PÉDAGOGIQUE

Le cours INF803 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 Adobe Connect 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: **QUIZ**

- ***Compétence mobilisée:*** Connaître et maîtriser les principaux systèmes d'exploitation disponibles sur le marché. Savoir renforcer la sécurité de ces systèmes. Comprendre les enjeux de sécurité entourant la virtualisation
- ***Description:*** Sous la forme d'un quiz en ligne de 2 questions qui est à faire à la fin de chaque séance.
- ***Critères d'évaluation*** Choisir la bonne réponse donne les points, 0 autrement.
- ***Notation:*** 5 quiz de 2 points chacun, 10 %
- ***Date de remise:*** Séance 3,6,9,11,14

ÉVALUATION N^{O} 2: **Laboratoire**

- ***Compétence mobilisée:*** Connaître et maîtriser les principaux systèmes d'exploitation disponibles sur le marché.
- ***Description:*** Réaliser une installation et une configuration d'un Windows Server 2019 pour comprendre les concepts de base d'Active Directory et les bonnes pratiques en sécurité.
- ***Critères d'évaluation*** *Pour les consignes précises, de même que les modalités de remise et la grille d'évaluation, consultez Moodle 2.*
- ***Notation:*** 40 %
- ***Date de remise:*** 24 février 2022 à 18h00

ÉVALUATION N^{O} 3: **ÉTUDE DE CAS – METTRE EN PLACE UNE SOLUTION PERMETTANT DE RENFORCER LA SÉCURITÉ DES SYSTÈMES**

- ***Compétence mobilisée:*** Comprendre les fondements de la sécurité des systèmes
- ***Description:*** Un cas fictif sera présenté avec une problématique devant laquelle l'étudiant devra résoudre le cas en proposant des solutions. L'étudiant devra proposer des solutions à une problématique soulevée dans une mise en situation

  L'étude de cas sera déposée sur Moodle

  Travail à compléter en équipe de deux
- ***Critères d'évaluation*** Pour les consignes précises, de même que les modalités de remise et la grille d'évaluation, consultez Moodle 2.
- ***Notation:*** 40 %
- ***Date de remise:*** 14 avril 2022 à 21 h 30

ÉVALUATION N^{O} 4: **PARTICIPATION AUX DISCUSSIONS DU COURS**

- ***Compétence mobilisée:*** L'ensemble de la matière vue durant le cours
- ***Description:*** L'étudiant doit participer aux échanges lors des discussions ouvertes ou par le bilan du forum de discussion. Plusieurs sujets sur la matière lue et/ou vue en cours seront proposés tout au long de la formation.
- ***Critères d'évaluation*** *Participation aux discussions*
- ***Notation:*** 10 %

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 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);

[2] Extrait du Règlement des études 2017-2018

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 ?

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]

[3] Extrait du Règlement des études 2017-2018

- 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

Windows Server 2019 - Les bases indispensables pour administrer (Français) – 21 août 2019 de Nicolas Bonnet (Author), ISBN 2409019676

Windows Security Monitoring: Scenarios and Patterns (Anglais) – 17 avril 2018 de Andrei Miroshnikov (Author), ISBN 1119390648

[4] Extrait du Règlement des études 2017-2018


UNIVERSITÉ DE
SHERBROOKE