UNIVERSITÉ DE SHERBROOKE

IDENTIFICATION ET RENSEIGNEMENTS GÉNÉRAUX

Titre officiel du cours :	**INF806 – Système et réseau**
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 2019
Date de début :	6 janvier 2020
Date de fin :	20 avril 2020
Date limite d'abandon :	15 mars 2020
Rencontres synchrones :	Tous les lundis de 18h à 21h
Personne(s)-ressource(s) :	Hector Bustillo
Courriel(s) :	Hector.Bustillo@usherbrooke.ca

1. MISE EN CONTEXTE

DESCRIPTION OFFICIELLE DU COURS

Cible(s) de formation :

Connaître les caractéristiques de l'architecture des composantes des réseaux informatiques dans un contexte de sécurité. Comprendre les principes d'architecture réseau et de sécurité.

Contenu :

Éléments physiques et logiques d'une architecture réseau, détection de logiciels malveillants, services de base en réseautique et virtualisation, principes d'architecture réseau et de sécurité, attaques réseau, «sandboxing », cryptologie, analyses de cas.

PLACE DU COURS DANS LE PROGRAMME

Le cours INF806 « Système et réseau » permet de mieux comprendre les mesures et contrôles de sécurité à mettre en place au sein d'une architecture réseau.

UNIVERSITÉ DE SHERBROOKE

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.

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	12 heures
Conférences	0 heures
Lecture personnelle	45 heures
Activités de consolidation	45 heures
TOTAL	135 heures

2. DÉROULEMENT DU COURS

Séance	Description	Enseignant
Séance 1 : Introduction aux éléments d'architecture (6 janvier 2020)	• Présentation du cours • Introduction • Les points terminaux (postes, serveurs, tablettes, cellulaires) • Les commutateurs, routers, NGFW, PA.	HB

[1] Extrait de la fiche signalétique

UNIVERSITÉ DE SHERBROOKE

Séance	Description	Enseignant
Séance 2 : Éléments d'architecture réseau (13 janvier 2020)	• Active directory • Jumpoint • Proxy • Connexions sans fil • Firewall • Connexion locale et distante **Devoir 1 (10%)**	HB
Séance 3 : Détection de fichiers malveillants (20 janvier 2020)	• Analyse de fichiers malveillants • Outils de détection • SIEM • FIM • IDS/IPS	HB
Séance 4 : Services réseau (27 janvier 2020)	• TCP/IP • ARP, RARP • Routage, adressage • NAT, PAT • DNS, DHCP • SNMP • Netflow	HB
Séance 5 : Sécurisation des couches inférieures (3 février 2020)	• Sécurité par ports • Protocoles sécurisés • Autorisation DHCP • Contrôles des accès • Filtrage IP	HB
Séance 6 : Sécurisation des couches supérieures (10 février 2020)	• Analyse et inspection de paquets • NGFW • Déchiffrement SSL • Sécurité applicative	HB
Séance 7 : Examen Intra (Séance 1 à 6) (30%) (17 février 2020)		HB

UNIVERSITÉ DE SHERBROOKE

Séance	Description	Enseignant
Séance 8 : Principes et conception d'architecture (24 février 2020)	• Catégorisation des services réseau • Zonage • Segmentation • Ségrégation • ZIP • Matrice de flux	HB
Séance 9 : Principes d'architecture (suite) (02 mars 2020)	• ACL • Sécurité inter zone • Authentification 802.X • RADIUS • VPN • MFA **Travail de session (20%)**	HB
Séance 10 : Gestion de vulnérabilités réseau (09 mars 2020)	• Vulnérabilités des couches inférieures • Vulnérabilités des couches supérieures • Outils de scan de vulnérabilités • Analyse et consignation des vulnérabilités • Renforcement et remédiation	HB
Séance 11 : Attaques réseau (16 mars 2020)	• Introduction aux attaques réseau • Outils d'attaque • Metasploit • Attaques ARP poisonning, MITM, DNS Redirect, DHCP poisonning • Attaques sans fil	HB
Séance 12 : Système de protection pour les points terminaux (23 mars 2020)	• EDR • Bac à sable (Sandboxing) • Renforcement serveurs • Protection mobilité (Android, IOS, MAC) • Antiphishing • Antimalware	HB

Séance	Description	Enseignant
Séance 13 : Cryptologie (30 mars 2020)	• Mécanismes de chiffrement • Fonction de hachage • Outils de chiffrement • Chiffrement des sauvegardes • Utilisation des connexions chiffrées pour les composantes réseau	HB
Séance 14 : Analyse de cas (06 avril 2020)	Analyse de cas révision	HB
Séance 15 : Examen final (sur Moodle) (20 avril 2020)		HB

3. CONSIDÉRATIONS MÉTHODOLOGIQUES

APPROCHES MÉTHODOLOGIQUE ET PÉDAGOGIQUE

Le cours INF806 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: **DEVOIR 1**

- ***Compétence mobilisée:*** Comprendre les fondements des services et éléments réseau au sein d'une architecture sécurisée.
- ***Description:*** Faire une synthèse et approfondir les notions vues en classe sous forme de rapport.
- ***Critères d'évaluation*** Les consignes seront données en classe.
- ***Notation:*** 10%
- ***Date de remise:*** Le 3 février 2020 à 23h55

ÉVALUATION N^{O} 2: **Travail de session**

- ***Compétence mobilisée:*** Faire la conception d'une architecture réseau sécurisée et comprendre les fondements de la sécurité informatique au sein d'une architecture réseau
- ***Description:*** Faire la conception d'une architecture réseau sécurisé et incorporer les éléments de sécurité requis.
- ***Critères d'évaluation*** Les consignes seront données en classe.
- ***Notation:*** 20 %
- ***Date de remise:*** 30 mars 2020 à 23h55

ÉVALUATION N^{O} 3: **EXAMEN INTRA**

- ***Compétence mobilisée:*** Comprendre les services de base et éléments réseau au sein d'une architecture sécurisée.
- ***Description:*** Sous la forme d'un quiz contenant 2 question à développement (5 pts chacune) et 10 questions à choix multiples (2 pt chacune), démontrer la compréhension des principes d'architecture réseau 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:*** 30 %
- ***Date de remise:*** 26 septembre 2019, de 18h00 à 19h00

ÉVALUATION N^{O} 3: **EXAMEN FINAL**

- ***Compétence mobilisée:*** Faire la conception d'une architecture réseau sécurisée et comprendre les fondements de la sécurité informatique au sein d'une architecture réseau
- ***Description:*** Sous la forme d'un quiz contenant 2 questions à développement (5 pts chacune) et 15 questions à choix multiple (2 pt chacune), démontrer la compréhension de la matière vue dans le cours. Il s'agit d'un examen de deux heures à faire sur la plateforme Moodle.
- ***Critères d'évaluation*** Parmi les critères:
  - Justesse et complétude de la réponse
  - Richesse des éléments fournis
- ***Notation:*** 40 %
- ***Date de remise:*** 20 avril 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]

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 2017-2019

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.

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.

[3] Extrait du Règlement des études 2017-2019

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

Tout le matériel sera fourni en classe.

[4] Extrait du Règlement des études 2017-2019