Université du Québec
à Rimouski
Département de mathématiques, informatique et de génie

PLAN DE COURS

SESSION HIVER 2023

SIGLE :	INF36207
TITRE :	Sécurité informatique
GROUPE :	MS
HORAIRE DES COURS :	Mardi 19h15 à 22h05
DÉBUT / FIN :	10 janvier au 25 avril 2023
LOCAL :	Campus de Rimouski E-409 / Campus de Lévis 2060
CHARGÉ DE COURS :	Martin Arsenault, ing., MBA, MGP martin_arsenault@uqar.ca
COMMIS RESPONSABLE :	Jacqueline Thériault jacqueline_theriault@uqar.ca

DESCRIPTION DU COURS SELON L'ANNUAIRE

Objectifs :

Connaître les problèmes liés à la sécurité des systèmes informatiques et s'initier aux différentes techniques de détection des attaques et de protection des systèmes et de leurs données.

Contenu :

Historique. Cibles probables et courantes. Vulnérabilités et types d'attaques. Sécurité dans les systèmes d'exploitation. Sécurité dans les bases de données, Sécurité dans les réseaux. Sécurité dans les logiciels. Cryptographie et cryptanalyse.

Insertion du cours dans le programme :

Ce cours est disponible dans différents programmes offerts à l'UQAR dont le programme court de 1er cycle en informatique appliquée, de même que le certificat, la majeure et le baccalauréat en informatique. Ce cours reprend des éléments d'autres cours (notamment la réalisation de programmes robustes et des notions de téléinformatique) pour permettre à l'étudiant de bien comprendre (du point de vue des attaquants comme des programmeurs et des administrateurs de systèmes) les failles de sécurité possibles tout en l'outillant sur des techniques et des méthodes permettant une prévention et une remédiation efficaces.

Préalables :
INF14107 Architecture des systèmes informatiques, **INF15107** Bases de données & **INF26207** Téléinformatique

Mise en contexte du cours :

À la base de la sécurité informatique, on retrouve des outils technologiques permettant d'assurer la sécurité des systèmes et des réseaux de même que la protection de données. On retrouve également des principes qui dictent les bonnes pratiques assurant une sécurité accrue des systèmes et des infrastructures. Ce cours portera principalement sur les aspects technologiques de la sécurité informatique (réseaux, systèmes, outils, failles, protocoles, cryptographie, etc.) tout en abordant les différents enjeux sociaux liés à la problématique de la sécurité informatique (sensibilisation des acteurs sur les risques, déontologie, « hacktivisme », pirates, fraude, protection de la vie privée et confidentialité des données personnelles, etc.).

De plus en plus de systèmes et d'objets sont connectés à des réseaux privés et publics et assurent des fonctions de transmission, de traitement ou d'entreposage de données pour eux-mêmes ou au nom de tiers systèmes. Ces systèmes et objets reliés sont souvent la cible d'attaques de toutes sortes. L'étudiant qui œuvra avec ces systèmes devra s'assurer de comprendre la nature des attaques possibles et les risques qui s'y rattachent. Il devra en tenir compte dans le but d'en assurer leur sécurité afin de garantir la disponibilité, l'intégrité et la confidentialité du système et des données qu'il comporte.

Dans l'ère dans laquelle nous évoluons, où la sensibilité du public à la sécurité et à la protection des renseignements personnels est hautement élevée, il est essentiel que l'étudiant puisse évaluer la portée de ses actions et ses responsabilités quant à son apport sur la sécurisation des systèmes qu'il sera appelé à exploiter et/ou développer. Dans cette optique, les aspects légaux liés à la sécurité informatique seront également abordés.

Objectifs spécifiques du cours :

Le cours a pour but de transmettre à l'étudiant les concepts de base en sécurité informatique. Entre autres, l'étudiant sera amené à :

- Connaître la terminologie de base, les enjeux et le domaine de la sécurité informatique, distinguer les aspects politiques et légaux des aspects technologiques et comprendre comment ils s'influencent mutuellement;
- Comprendre comment les enjeux changent à cause des technologies qui évoluent sans cesse;
- Comprendre les problèmes principaux de la sécurité, soit l'authentification, l'autorisation, la confidentialité, l'intégrité, la disponibilité, l'imputabilité, la non-répudiation et la traçabilité;
- Comprendre les protocoles de communication et comment le réseau interagit avec les applications;
- Comprendre la nature de certaines attaques (injection de données malicieuses, déni de service, etc.);
- Se familiariser avec les techniques de codage et de décodage de données sécurisées;
- Se familiariser avec les applications de surveillance et d'analyse de réseau;
- Se familiariser avec les technologies de sécurisation des réseaux (réseaux virtuels privés, pare-feu, etc.);
- Se familiariser avec des outils de pénétration et de tests de réseau;
- Identifier les risques dans un système informatique et proposer/concevoir des architectures sécurisées, filaires et/ou mobiles afin d'atténuer les risques identifiés;
- Connaitre les modalités légales en termes de protection des renseignements personnels;
- Comprendre la catégorisation des actifs informationnels et les processus de mise en place de plans de relève appropriés assurant la continuité des affaires.

Bien sûr, cette liste n'est pas exhaustive. Le but du cours demeure introductoire avec un fort côté technique. L'étudiant sera donc amené à maîtriser les différentes technologies par la pratique, soit en ateliers supervisés, soit par des devoirs qu'il devra faire seul ou en équipe (certains devoirs nécessiteront de la programmation).

Calendrier des rencontres :

#	Dates	Descriptions	Évaluations
1	10 janvier	Présentation du cours. Qu'est-ce que la sécurité informatique? Qu'est-ce qu'une attaque informatique? Qui sont les attaquants? Qu'est-ce qui motive les attaquants? Cybercriminalité, cyberterrorisme, et « hacktivisme » : mythes et réalités. Stratégies de défense.	
2	17 janvier	Aspects légaux et lois en vigueur sur la protection des renseignements personnels. Actifs informationnels : catégorisation et inventaire. Analyse de risque et son importance. Plan de relève et continuité des affaires. Responsabilités légales. Aspects déontologiques.	
3	24 janvier	Les rôles de la sécurité informatique. Aspects technologiques (authentification, autorisation, disponibilité, intégrité) et aspects sociaux (confidentialité, imputabilité, non-répudiation). Technologies et algorithmes. Sécurité physique. Sensibilisation des utilisateurs/usagers.	Énoncé TP#1
4	31 janvier	Enjeux de la sécurité informatique : vie privée, traçabilité et anonymisation. Pérennité des données et les conséquences sociales. Êtes-vous le produit? Est-ce vraiment confidentiel? Sécurité des données et ingénierie sociale.	
5	7 février	Cryptographie (partie #1). Historique. Exemples de chiffrements simples (substitution, transposition, etc.). Systèmes à clefs uniques. Cryptanalyse des systèmes simples.	
6	14 février	Cryptographie (partie #2). Principes de base des systèmes de chiffrement modernes. Partages de secrets communs, systèmes à clefs publiques/privées. Cryptanalyse des systèmes complexes. Signatures numériques. Stéganographie. Futurs de la cryptographie : algorithmes et physique quantique. Politiques de sécurité et mots de passe. Outils de chiffrement.	Remise du TP#1 Énoncé TP#2
7	21 février	Sécurité et réseaux (partie #1). Modèle OSI et applications. Protocoles de communication (raw sockets, ICMP, UDP, TCP, etc.). Rôle du pare-feu. Règles de routage, ports, redirections/translation, liste de contrôle d'accès. Filtrage par MAC. Protocoles sécurisés : IPSec, VPN, SSH et tunnels SSH. Capture de trafic et intrusion. Exploration et découverte des réseaux. Outils de sécurité pour les réseaux.	
8	28 février	Semaine de lecture	
9	7 mars	---------- Examen intra ----------	Examen intra
10	14 mars	Sécurité et réseaux (partie #2). Nouvelles installations et parcs informatiques. Importance des mises à jour. Gestion de parcs informatiques : scripts, SNMP, Nagios, MDM, InTune. BYOD & réseau d'entreprise. Types d'attaques réseau.	Remise du TP#2 Énoncé du TP#3
11	21 mars	Authentification et autorisation. Pourquoi authentifier? Authentification, autorisation, traçabilité, imputabilité. Systèmes d'authentification : Kerberos, Radius, TACACS, LDAP et AzureAD. Protocoles OAUTH & SAML.	
12	28 mars	La sécurisation des contenus (DRM). Enjeux : protection de la propriété intellectuelle et aspect légaux. Études de cas. Mathématiques des DRM. Casser les DRM : stratégies et conséquences. Mécanismes de sécurité des systèmes d'exploitation. Niveaux de Privilèges. Sécurisation des fichiers. Groupes, accès, attributs, et particularités. Restrictions d'accès au matériel (clés USB, Bluetooth, etc.). Sandboxing au niveau des applications, au niveau du système d'exploitation.	
13	4 avril	Hacking, cracking et exploitations. Exploitation de failles logicielles. Injection de données malicieuses, injections SQL, HTML, XSS et autres attaques spécifiques au langage de programmation/logiciel. Comment solidifier le code.	Remise du TP#3 Énoncé du TP#4
14	11 avril	Réseaux sans fil et protocoles. Niveaux de sécurité et vulnérabilités de WEP/WPA. Danger des appareils sans fil pour l'entreprise. Conception d'une architecture sans fil sécurisée. Évolution de la sécurité des réseaux sans-fil. Attaques à grande échelle, déni de service, etc. Botnets et cybercriminalité. Confidentialité et anonymisation. Cybercrime, anonymat et « Web obscur ». Cryptomonnaies.	
15	18 avril	Systèmes d'exploitation et leurs outils de sécurité intégrés : SELinux, Windows Defender, etc. Systèmes de fichiers. Autres sujets à déterminer.	
16	25 avril	---------- Examen final ----------	Remise du TP#4 Examen final

* L'enseignant se réserve le droit de modifier le calendrier des rencontres et son contenu, s'il le juge nécessaire et approprié, après en avoir préalablement informé les étudiants.

FORMULES PÉDAGOGIQUES

La formule se compose d'une rencontre de trois heures chaque semaine comportant des leçons magistrales, démonstrations/travaux pratiques, exercices et analyses de mise en situation. Étant donné que le cours sera en vidéoconférence entre Lévis et Rimouski, l'enseignant se déplacera entre les sites en fonction de ses disponibilités et des conditions météorologiques.

Quatre travaux pratiques sont également prévus. Ils seront en équipe de 2 ou 3 personnes au maximum, au choix des étudiants. Toutefois, l'enseignant se réserve le droit d'assigner les équipes pour certains travaux. Les dates de remises sont indiquées dans le calendrier des rencontres et les sujets des travaux seront connus au moment de la mise en disponibilité des énoncés.

Modalités d'évaluations :

- Quatre travaux pratiques pour un total de 60 %.
- Deux examens écrits pour un total de 40 %.

La pondération des épreuves dans le cours est répartie ainsi :

Épreuves	Pondérations
Travaux pratiques #1 à #4	15%
Examen Intra	20%
Examen final	20%
Total	100%

Note : La moyenne pondérée des deux examens doit atteindre un minimum de 50% sans quoi il y aura un échec.

Une absence non justifiée préalablement à un examen entraine une note de 0.

À moins d'entente avec l'enseignant, tout retard dans le dépôt des travaux pratiques entrainera une perte de 10% par jour de retard sur la note obtenue, et ce, jusqu'à concurrence de 0 après la dixième journée de retard.

Politique du français :

Jusqu'à 10 % des points peuvent être accordés à la qualité du français écrit dans les travaux et les examens.

Notation proposée :

L'établissement de la cote finale est basé sur le barème des cotes fixes suivant :

Notes	Cotes		Notes	Cotes
96% - 100%	A+		73% - 77%	C+
92% - 96%	A		70% - 73%	C
88% - 92%	A-		66% - 70%	C-
84% - 88%	B+		62% - 66%	D+
80% - 84%	B		60% - 62%	D
77% - 80%	B-		< 60%	E

Modalités particulières :

Bien que dans un cours régulier la ponctualité et le sérieux des étudiants sont de rigueur, ce principe devient d'une importance capitale dans le cas de la tenue de cours par vidéoconférence. Ainsi, dans votre intérêt et dans l'intérêt de tous les étudiants assistant au cours à vos côtés et à distance, il est demandé de limiter les bruits et les discussions avec les voisins.

Le plagiat ne sera pas toléré. Vous devrez toujours citer correctement vos sources (livres, articles, collègues, sites Web, etc.). De plus, vous devrez toujours déclarer les sources dont vous vous serez inspirés (livres, articles, site Web, etc.). Une collaboration non avouée est considérée comme un plagiat et sera traitée conséquemment. Il en va de même pour tout matériel dont vous ne seriez pas l'auteur (code, texte, image, etc.). Il sera évidemment considéré comme un plagiat tout code copié-collé (oui, même en changeant les noms de variables), qu'il y ait une référence ou non à la source. Tout étudiant suspecté de plagiat verra son cas traité selon les modalités en vigueur du Règlement 5 du Régime des études de premier cycle de l'UQAR.

Notez que le but n'est pas de vous empêcher d'utiliser des sources externes, mais de vous obliger à les déclarer, les citer, et à les comprendre suffisamment pour arriver à vos solutions originales.

L'étudiant veillera par ailleurs à compléter l'évaluation de l'enseignement selon les modalités prévues.

RÉFÉRENCES BIBLIOGRAPHIQUES

Aucun livre n'est obligatoire pour ce cours, plusieurs références sur Internet seront fournies durant le cours en plus des notes de cours de l'enseignant qui seront rendues disponibles sur Moodle en version électronique.

Les ouvrages ci-dessous peuvent servir comme références bibliographiques complémentaires sur différents sujets abordés durant le cours. Ces manuels sont généralement disponibles sur les sites de vente de livres en ligne :

- Tanner N. H., *Cybersecurity Blue Team Toolkit*, WILEY, 2019
- OccupyTheWeb, *Linux Basics for Hackers – Getting started with Networking, Scripting and Security in Kali*, No Starch Press, 2019
- Chapple M., Stewart, J.M., Gibson, D., *Certified Information Systems Security Professional (CISSP) - Official Study Guide*, SYBEX, 8e édition, 2018
- Dieterle D.W., *Basic Security Testing With Kali Linux – Vol 2*, Cyberarms, 2016
- Santos O., Stuppi J., *CCNA Security 210-260 – Official Cert Guide*, CiscoPress, 2015
- Gregg M., *The Network Security Test Lab: A Step-by-Step Guide*, WILEY, 2015
- Bejtlich R., *The practice of network security monitoring : understanding incident detection and response*, No Starch Press, 2013
- Weidman G., *Penetration Testing – A hands-on Introduction to Hacking*, No Starch Press, 2013
- ACCISSI, *Sécurité informatique – Ethical Hacking : apprendre l'attaque pour mieux se défendre*, Éditions ENI, 2009