Sécurité des logiciels et exploitation de vulnérabilités

Groupe 30
Mercredi, de 14h00 à 17h00 PK-1620 (cours)

Jeudi, de 13h30 à 15h30 PK-S1565 (atelier)

Responsable(s) du cours

Nom du coordonnateur : PRIVAT, Jean

Nom de l'enseignant : PRIVAT, Jean
Local : PK-4830
Téléphone : (514) 987-3000 #3314
Courriel : privat.jean@uqam.ca
Site Web : http://info.uqam.ca/~privat/

Description du cours

Ce cours à contenu variable vise à permettre d'aborder de nouvelles approches prometteuses en informatique et génie logiciel non couvertes par les autres activités de la banque de cours.

Objectifs du cours

Acquérir les ressources nécessaires à la recherche autonome de vulnérabilités logicielles. Saisir la gravité et l’impact réel des différents types de vulnérabilités logicielles et systèmes. Comprendre le processus d’exploitation logicielle et être en mesure d’accomplir le cheminement complet d’une attaque logicielle (audit de codes, rétro-ingénierie, reconnaissance et exploitation de vulnérabilités). Saisir les interactions possibles entre plusieurs vulnérabilités et les conséquences résultantes sur la sécurité des applications. Être en mesure de conduire une analyse forensique de base sur un système d’information Linux.

Contenu du cours

Audits de code: Analyse logicielle autant avec que sans code source. Recherche de vulnérabilités et stratégies efficaces d’analyse.
Logique d’exploitation: Initiation à l’exploitation système au travers des librairies standards des systèmes UNIX contemporains.
Sécurité Web: Survol des vulnérabilités les plus communes, selon le top 10 de l’OWASP. Étude de leur exploitation et des mécanismes de prévention.
Science forensique: Application de techniques de recouvrement et de restauration d’informations basées sur les mécanismes des systèmes d’exploitations modernes. Introduction à la stéganographie.
Cryptographie: Étude et reconnaissance des mauvaises pratiques courantes dans l’utilisation d’algorithmes cryptographiques. Être en mesure de démontrer la déficience d’un protocole par son attaque.
Rétro-ingénierie et exploitation binaire: Analyse du code machine compilé d’une application: désassemblage, traçage et instrumentation. Corruption de mémoire et altération de l'exécution normale d’un logiciel pour l’exécution de code arbitraire. Abus du fonctionnement de la pile, du tas et de l’éditeur de liens.

Modalités d'évaluation

- Examen intra 25%
- Examen final 25%
- TP1 20%
- TP2 20%
- TP Spécial 10%

Une note moyenne cumulée aux examens inférieure à 50% entrainera un échec au cours.

Politique d'absence aux examens

L'autorisation de reprendre un examen en cas d'absence est de caractère exceptionnel. Pour obtenir un tel privilège, l'étudiant-e doit avoir des motifs sérieux et bien justifiés.

Il est de la responsabilité de l'étudiant-e de ne pas s'inscrire à des cours qui sont en conflit d'horaire, tant en ce qui concerne les séances de cours ou d'exercices que les examens. **De tels conflits d'horaire ne constituent pas un motif justifiant une demande d'examen de reprise.**

Dans le cas d'une absence pour raison médicale, l'étudiant-e doit joindre un certificat médical original et signé par le médecin décrivant la raison de l'absence à l'examen. Les dates d'invalidité doivent être clairement indiquées sur le certificat. Une vérification de la validité du certificat pourrait être faite. Dans le cas d'une absence pour une raison non médicale, l'étudiant-e doit fournir les documents originaux expliquant et justifiant l'absence à l'examen – par exemple, lettre de la Cour en cas de participation à un jury, copie du certificat de décès en cas de décès d'un proche, etc. Toute demande incomplète sera refusée. Si la direction du programme d'études de l'étudiant-e constate qu'un étudiant a un comportement récurrent d'absence aux examens, l'étudiant-e peut se voir refuser une reprise d'examen.

L'étudiant-e absent-e lors d'un examen doit, dans les cinq (5) jours ouvrables suivant la date de l'examen, présenter une demande de reprise en utilisant le formulaire prévu, disponible sur le site Web du département à l'adresse suivante : **http://info.uqam.ca/politiques/**

L'étudiant-e doit déposer le formulaire dûment complété au secrétariat de la direction de son programme d'études : PK-3150 pour les programmes de premier cycle, PK-4150 pour les programmes de cycles supérieurs. Pour plus de détails sur la politique d'absence aux examens du Département d'informatique, consultez le site web suivant : **http://info.uqam.ca/politiques**

Renseignements utiles

Les étudiants qui ont une lettre signée de leur conseillère ou conseiller de l'Accueil et de soutien aux étudiants en situation de handicap (ASESH), dans laquelle il est fait état de leur inscription au ASESH à titre d'étudiant(e) en situation de handicap, sont invités à remettre ce document à leurs professeur(e)s et chargé(e)s de cours dès le début de la session afin que les aménagements dans le respect des exigences académiques soient déterminées de concert avec chacun des professeur(e)s et chargé(e)s de cours. Les étudiants qui ont une déficience et qui ne seraient pas inscrits au ASESH sont priés de se présenter au AB-2300.
Étudiants avant une déficience de type visuelle, auditive, motrice, trouble d'apprentissage, trouble envahissant du développement et trouble de santé mentale:
Les étudiant(e)s qui ont une lettre d'*Attestation des mesures d'aménagements académiques* obtenue auprès d'une conseillère, d'un conseiller de l'**Accueil et soutien aux étudiants en situation de handicap (ASESH)** doivent rencontrer leurs enseignant(e)s au début de la session afin que des mesures d'aménagement en classe ou lors des évaluations puissent être mises en place. Ceux et celles qui ont une déficience ou une incapacité mais qui n'ont pas cette lettre doivent contacter l'**ASESH** au (514) 987-3148 ou se présenter au AB-2300 le plus tôt possible.

Intégrité académique

PLAGIAT Règlement no 18 sur les infractions de nature académique. (extraits)

Tout acte de plagiat, fraude, copiage, tricherie ou falsification de document commis par une étudiante, un étudiant, de même que toute participation à ces actes ou tentative de les commettre, à l'occasion d'un examen ou d'un travail faisant l'objet d'une évaluation ou dans toute autre circonstance, constituent une infraction au sens de ce règlement.

La liste non limitative des infractions est définie comme suit :

- **la substitution de personnes;**
- **l'utilisation totale ou partielle du texte d'autrui en la faisant passer pour sien ou sans indication de référence;**
- **la transmission d'un travail pour fins d'évaluatiion alors qu'il constitue essentiellement un travail qui a déjà été transmis pour fins d'évaluation académique à l'Université ou dans une autre institution d'enseignement, sauf avec l'accord préalable de l'enseignante, l'enseignant;**
- **l'obtention par vol, manoeuvre ou corruption de questions ou de réponses d'examen ou de tout autre document ou matériel non autorisés, ou encore d'une évaluation non méritée;**
- **la possession ou l'utilisation, avant ou pendant un examen, de tout document non autorisé;**
- **l'utilisation pendant un examen de la copie d'examen d'une autre personne;**
- **l'obtention de toute aide non autorisée, qu'elle soit collective ou individuelle;**
- **la falsification d'un document, notamment d'un document transmis par l'Université ou d'un document de l'Université transmis ou non à une tierce persone, quelles que aoient les circonstances;**
- **la falsification de données de recherche dans un travail, notamment une thèse, un mémoire, un mémoire-création, un rapport de stage ou un rapport de recherche;**
- **Les sanctions reliées à ces infrations sont précisées à l'article 3 du Règlement no 18.**

Les règlements concernant le plagiat seront strictement appliqués. Pour plus de renseignements, veuillez consulter les sites suivants : **http://www.sciences.uqam.ca/etudiants/integrite-academique.html** et **http://www.bibliotheques.uqam.ca/recherche/plagiat/index.html**

Matériel requis

Le matériel est disponible sur le site du cours http://info.uqam.ca/~privat/INF600C/

Médiagraphie

Il n'y a de manuel obligatoire, les ressources complémentaires ci-dessous sont néamons pertinantes

- J. ERICKSON -- Hacking, The Art of Exploitation (2e édition) -- No Starch Press, 2008.
- D. STUTTARD, M. PINTO -- The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws (2e édition) -- Wiley, 2011.
- B. SCHNEIER -- Applied Cryptography: protocols, algorithms, and source code in C (2e édition) -- John Wiley & Sons, Inc. New York, NY, USA, 1995.
- B. DANG, A. GAZET, E. BACHAALANY, S. JOSSE -- Practical Reverse Engineering: x86, x64 ARM, Windows Kernel, Reversing Tools, and Obfuscation -- Wiley, 2011.
- M. SIKORSKI, A. HONIG -- Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software -- No Starch Press, 2012.
- T. KLEIN -- Bug Hunter’s Diary: A Guided Tour Through the Wilds of Software Security -- No Starch Press, 2011.
- C. ANLEY, J. HEASMAN, F. LINDNER, G. RICHARTE -- The Shellcoder’s Handbook: Discovering and Exploiting Security Holes (2e édition) -- Wiley, 2007.
- B. NIKKEL -- Practical Forensic Imaging, Securing Digital Evidence with Linux Tools -- No Starch? ?Press,? ?2016.

Outils et plateformes d’apprentissage

- Exploit-Exercises https://exploit-exercises.com/ (nebula, protostar, etc.)
- Cryptopals http://cryptopals.com/
- Ringzer0 https://ringzer0team.com/
- CTF AGEEI https://ctf.ageei.uqam.ca/

A : article - C : comptes rendus - L : logiciel S: Standard - U : uri - V : volume	C : complémentaire - O : Obligatoire - R : recommandé