INF600C
Sécurité des logiciels et exploitation de vulnérabilités

Plan de cours

Responsable(s) du cours

Coordination : PRIVAT, Jean
PK-4830
privat.jean@uqam.ca
http://info.uqam.ca/~privat/

Enseignement :

PEPOS-PETITCLERC, Phillipe
pepos-petitclerc.philippe@uqam.ca
Groupes : 030

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.

Objectif 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.

La note finale (en lettre, A+, A, etc.) pour le trimestre sera attribuée en fonction de l'atteinte des objectifs spécifiques à travers les évaluations. La distribution des résultats dans le groupe pourrait aussi être utilisée. Aucune autre opportunité (travail supplémentaire, etc.) d'augmenter le nombre de points ne sera accordée.

Materiel

Le matériel est disponible sur le site du cours https://ppepos.github.io/inf600c/

Médiagraphie

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

Livres

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

Monitorat de programme

Le département d'informatique offre un service de monitorat gratuit s'adressant plus particulièrement aux étudiant.e.s du baccalauréat et du certificat en informatique. Il concerne principalement les cours de base comme INF1070, INF1120, INF1132, INF2120 et INF2171, mais, selon la connaissance du moniteur ou de la monitrice, un support dans d'autres cours peut également être offert.

Objectifs. Permettre aux étudiant.e.s de :

- Bénéficier d'un encadrement par les pairs ;
- Recevoir un suivi personnalisé en cas de difficulté ;
- Profiter d'un soutien supplémentaire à la matière vue en classe ;
- Obtenir un support technique sur les technologies, les outils, les bibliothèques et les cadriciels utilisés dans les cours (installation, configuration, utilisation)

Informations.

- Voir https://info.uqam.ca/aide/ pour la grille horaire et tous les détails
- Le service est généralement disponible à partir de la deuxième semaine
- D'autres plages horaires pourraient être ajoutées en cours de session selon les besoins
- Clavardage en direct : ~aide (Mattermost)

Politique d'absence aux examens

Reprise d'examen. 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.

Conflits d'horaire. 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.**

Procédure. 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 http://info.uqam.ca/repriseexamen/.

Pièces justificatives. 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.e étudiant.e a un comportement récurrent d'absence aux examens, l'étudiant.e peut se voir refuser une reprise d'examen.

Pour plus d'informations. Consulter la page http://info.uqam.ca/politiques.

Règlement numéro 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 personne, quelles que soient 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 :

- http://www.infosphere.uqam.ca/rediger-un-travail/eviter-plagiat
- http://r18.uqam.ca/

Politique no 16 visant à prévenir et combattre le sexisme et les violences à caractère sexuel

Les violences à caractère sexuel se définissent comme étant des comportements, propos et attitudes à caractère sexuel non consentis ou non désirés, avec ou sans contact physique, incluant ceux exercés ou exprimés par un moyen technologique, tels les médias sociaux ou autres médias numériques. Les violences à caractère sexuel peuvent se manifester par un geste unique ou s'inscrire dans un continuum de manifestations et peuvent comprendre la manipulation, l'intimidation, le chantage, la menace implicite ou explicite, la contrainte ou l'usage de force.
Les violences à caractère sexuel incluent, notamment :

- la production ou la diffusion d'images ou de vidéos sexuelles explicites et dégradantes, sans motif pédagogique, de recherche, de création ou d'autres fins publiques légitimes ;
- les avances verbales ou propositions insistantes à caractère sexuel non désirées ;
- la manifestation abusive et non désirée d'intérêt amoureux ou sexuel ;
- les commentaires, les allusions, les plaisanteries, les interpellations ou les insultes à caractère sexuel, devant ou en l'absence de la personne visée ;
- les actes de voyeurisme ou d'exhibitionnisme ;
- le (cyber) harcèlement sexuel ;
- la production, la possession ou la diffusion d'images ou de vidéos sexuelles d'une personne sans son consentement ;
- les avances non verbales, telles que les avances physiques, les attouchements, les frôlements, les pincements, les baisers non désirés ;
- l'agression sexuelle ou la menace d'agression sexuelle ;
- l'imposition d'une intimité sexuelle non voulue ;
- les promesses de récompense ou les menaces de représailles, implicites ou explicites, liées à la satisfaction ou à la non-satisfaction d'une demande à caractère sexuel.

Pour consulter la politique no 16

https://instances.uqam.ca/wp-content/uploads/sites/47/2018/05/Politique_no_16.pdf

Pour obtenir de l'aide, faire une divulgation ou une plainte

Bureau d'intervention et de prévention en matière de harcèlement
514-987-3000, poste 0886

Pour obtenir la liste des services offerts à l'UQAM et à l'extérieur de l'UQAM

https://harcelement.uqam.ca

Soutien psychologique (Services à la vie étudiante)

514-987-3185
Local DS-2110

CALACS Trêve pour Elles – point de services UQAM

514 987-0348
calacs@uqam.ca
http://trevepourelles.org

Service de la prévention et de la sécurité

514-987-3131

Politique no 44 d'accueil et de soutien des étudiant.e.s en situation de handicap

Politique. Par sa politique, l'Université reconnait, en toute égalité des chances, sans discrimination ni privilège, aux étudiant.e.s en situation de handicap, le droit de bénéficier de l'ensemble des ressources du campus et de la communauté universitaire, afin d'assurer la réussite de leurs projets d'études, et ce, dans les meilleures conditions possibles. L'exercice de ce droit est, par ailleurs, tributaire du cadre réglementaire régissant l'ensemble des activités de l'Université.

Responsabilité de l'étudiant.e. Il incombe aux étudiant.e.s en situation de handicap de rencontrer les intervenant.e.s (conseiller.ère.s à l'accueil et à l'intégration du Service d'accueil et de soutien des étudiant.e.s en situation de handicap, professeur.e.s, chargé.e.s de cours, direction de programmes, associations étudiantes concernées, etc.) qui pourront faciliter leur intégration à la communauté universitaire ou les assister et les soutenir dans la résolution de problèmes particuliers en lien avec les limitations entraînées par leur déficience.

Service d'accueil et de soutien aux étudiant.e.s en situation de handicap. Le Service d'accueil et de soutien aux étudiant.e.s en situation de handicap (SASESH) offre des mesures d'aménagement dont peuvent bénéficier certains étudiant.e.s. Il est fortement recommandé aux de se prévaloir de ces services afin de réussir ses études, sans discrimination. Pour plus d'information, visiter le site de ce service : https://vie-etudiante.uqam.ca/etudiant-situation-handicap/nouvelles-ressources.html et celui de la politique institutionnelle d'accueil et de soutien aux étudiant.e.s en situation de handicap : https://instances.uqam.ca/wp-content/uploads/sites/47/2018/05/Politique_no_44.pdf
Il est important d'informer le SASESH de votre situation le plus tôt possible :

- En personne : 1290, rue Saint-Denis, Pavillon Saint-Denis, local AB-2300
- Par téléphone : 514 987-3148
- Par courriel : situation.handicap@uqam.ca
- En ligne : https://vie-etudiante.uqam.ca/