Université de Sherbrooke

Département d'informatique

IFT 508 – Introduction aux attaques informatiques

Plan d'activité pédagogique

Automne 2024

Enseignant	Henry NGONGA
Courriel :	Henry.NGONGA@USherbrooke.ca
Local :	
Téléphone :	
Disponibilités :	Sur Teams en dehors des heures de cours

Site web du cours : https://moodle.usherbrooke.ca/course/view.php?id=37266

Horaire Exposé magistral : Mardi 14h30 à 17h20 salle D3-2035/Réunion Microsoft Teams

Description officielle de l'activité pédagogique[1]

Cibles de formation :	Comprendre les étapes d'une cyberattaque. Faire la recherche d'informations sur une cible d'attaque. Différencier les types d'attaques. Utiliser des trousses et outils de piratage de façon éthique. Connaitre les techniques pour détecter des cyberattaques.
Contenu :	Analyse d'attaque ; montage et préparation des attaques. Les vulnérabilités et leur exploitation ; vulnérabilités logicielles, exploitation et construction de maliciel. Introduction et test d'intrusion ; OWASP + Guide de tests d'intrusion (pentest) OWASP : atelier ou projet de tests d'intrusion Web ; tests d'intrusion serveur : exploit, pivot, « metasploit » et Armitage. Analyse des attaques d'hameçonnage : trace réseau, analyse des postes, détection de l'attaquant. Tests d'intrusion (pentest) comme méthode d'attaque. Détection de cyberattaques : par extraction des fichiers, par signatures, par anomalies, par analyse de journaux, analyse de flux.
Crédits	3
Organisation	3 heures d'exposé magistral par semaine 6 heures de travail personnel par semaine
Particularités	Aucune

[1] https://www.usherbrooke.ca/admission/fiches-cours/ift508

1 Présentation

Cette section présente les cibles de formation spécifiques et le contenu détaillé de l'activité pédagogique. Cette section, non modifiable sans l'approbation du comité de programme du Département d'informatique, constitue la version officielle.

1.1 Mise en contexte

Cette activité de formation s'inscrit en tant qu'activité optionnelle du baccalauréat en informatique. Son positionnement permet à l'étudiant d'acquérir les connaissances de base fondamentales à la compréhension de ce qu'est une attaque informatique. Le cours est aussi offert également en tant que cours optionnel aux programmes de maîtrise en informatique et génie logiciel. Le cours permet de contextualiser la mise en application des différentes techniques d'attaque cybernétique dans un contexte d'entreprise et des impacts que celles-ci peuvent occasionner dans un contexte d'entreprise.

1.2 Cibles de formation spécifiques

À la fin de ce cours, l'étudiante ou l'étudiant saura :

1. Maîtriser la nature, le rythme et les outils des cyberattaques contre divers types d'infrastructure
2. Savoir détecter les signes et artefacts d'une intrusion, pouvoir mesurer son ampleur et pouvoir en déterminer la chaîne causale
3. Savoir dresser et exécuter un plan d'intervention en cas d'incident et de brèche de données, de manière à trouver le meilleur compromis entre la minimisation des dommages et l'interruption des activités de l'organisation.

1.3 Contenu détaillé

Thème	Contenu	Nbr. d'heures	Objectifs
1	Mise en contexte : • Portrait de la cybercriminalité • Piratage éthique • Modèles d'attaques informatiques	3	
2	Failles humaines et physiques : • Méthodologie d'attaque • Ingénierie sociale – cas de l'hameçonnage • Influence et manipulation psychologique • Accès physique à un ordinateur • Usurpation d'identité et collecte d'information	3	
3	Stratégie de reconnaissance : • Encadrement des tests d'intrusion • Méthodologie de prise d'empreinte • Les essentiels (Google Hacking, Google Dorking, moteurs de recherche spécialisés, réseaux sociaux, etc.) • Énumération (IP, DNS)	3	
4	Stratégie de détection : • Rappel sur les réseaux TCP/IP • Passerelle, masque, sous-réseau, services, ports, TCP/UDP, IP publiques et IP privées • Analyse de l'entête Unix d'un courriel (RFC 5321 et RFC 5322) • Scan de ports • Détection d'un système d'exploitation • Reniflage de paquets	3	
5	Exploitation des failles réseau : • Configuration par défaut • Vulnérabilités non corrigées • Déni de service, déni de service distribué, amplification et « booter » • Tunnel SSH, VoIP, WIFI • L'homme du milieu et jumeau maléfique	3	
6	Exploitation des failles système : • Configuration par défaut • Vulnérabilités non corrigées • Identification de mots de passe • Élévation de privilèges • Séquence de démarrage	3	
7	Exploitation des failles applicatives et web : • OWASP • Vulnérabilités non corrigées • Dépassements de pile (buffer overflow) • Division par zéro • Outrepasser les protections cookies, paramètres du client, etc.	3	
8	Ne pas attirer l'attention : • Éviter d'être repéré (extraction des fichiers, signatures, détection d'anomalies, analyse des journaux, analyse des flux) • Éviter les pièges (honey pots and honey net, etc.)	3	
9	Exfiltration : Marché noir, Deep Web, Dark Web, Dark Net, etc.	3	

Table 1:

Thème	Contenu	Nbr. d'heures	Objectifs
10	Gestion des incidents de sécurité et conclusion : • Processus de gestion des incidents de sécurité • Mise en commun des lectures personnelles • Partage d'expérience • Retour sur les apprentissages • Solution du CTF	3	

2 Organisation

Cette section propre à l'approche pédagogique de chaque enseignante ou enseignant présente la méthode pédagogique, le calendrier, le barème et la procédure d'évaluation ainsi que l'échéancier des travaux. Cette section doit être cohérente avec le contenu de la section précédente.

2.1 Méthode pédagogique

Le cours IFT508 – Introduction aux attaques informatiques privilégie la méthode d'apprentissage par démonstration et exécution décomposée en 5 parties :

1. Explication des concepts théoriques par l'enseignant ;
2. Démonstration des cas pratiques par l'enseignant ;
3. Exécution par l'élève dans les travaux dirigés, laboratoires et projet ;
4. Encadrement et évaluation par l'enseignant

L'enseignant permet d'encadrer et de baliser le travail attendu de la part de l'étudiant. 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/.

2.2 Calendrier

Semaine	Date	Thème	Devoir
1	2024-08-26	1	
2	2024-09-02	3	
3	2024-09-09	3	Distribution du devoir 1
4	2024-09-16	5	
5	2024-09-23	6	
6	2024-09-30	2	
7	2024-10-07	Révision	Remise du devoir 1
8	2024-10-14	Examen périodique	
9	2024-10-21	Relâche	
10	2024-10-28	7	Distribution du devoir 2
11	2024-11-04	7	
12	2024-11-11	8	
13	2024-11-18	9	
14	2024-11-25	4	Remise du devoir 2
15	2024-12-02	10	
16	2024-12-09	Examen final	
17	2024-12-16	Examen final	

2.3 Évaluation

Devoirs (2)	30 %
Examen intra	30 %
Examen final	40 %

Les travaux des devoirs sont uniquement électronique. Aucun document imprimé ne sera accepté. Le travail remis doit répondre aux exigences énoncées dans l'énoncé du devoir.

Les examens intra et finaux sont Informatisés : en ligne, en presentiel et avec surveillance.

2.3.1 Qualité de la langue et de la présentation

Conformément à l'article 17 du règlement facultaire d'évaluation des apprentissages[2] l'enseignante ou l'enseignant peut retourner à l'étudiante ou à l'étudiant tout travail non conforme aux exigences quant à la qualité de la langue et aux normes de présentation.

2.3.2 Plagiat

Le plagiat consiste à utiliser des résultats obtenus par d'autres personnes afin de les faire passer pour sien et dans le dessein de tromper l'enseignante ou l'enseignant. Vous trouverez en annexe un document d'information relatif à l'intégrité intellectuelle qui fait état de l'article 9.4.1 du Règlement des études[3]. Lors de la correction de tout travail individuel ou de groupe une attention spéciale sera portée au plagiat. Si une preuve de plagiat est attestée, elle sera traitée en conformité, entre autres, avec l'article 9.4.1 du Règlement des études de l'Université de Sherbrooke. L'étudiante ou l'étudiant peut s'exposer à de graves sanctions qui peuvent être soit l'attribution de la note E ou de la note zéro (0) pour un travail, un examen ou une activité évaluée, soit de reprendre un travail, un examen ou une activité pédagogique. Tout travail suspecté de plagiat sera transmis au Secrétaire de la Faculté des sciences. Ceci n'indique pas que vous n'ayez pas le droit de coopérer entre deux équipes, tant que la rédaction finale des documents et la création du programme restent le fait de votre équipe. En cas de doute de plagiat, l'enseignante ou l'enseignant peut demander à l'équipe d'expliquer les notions ou le fonctionnement du code qu'elle ou qu'il considère comme étant plagié. En cas d'incertitude, ne pas hésiter à demander conseil et assistance à l'enseignante ou l'enseignant afin d'éviter toute situation délicate par la suite.

2.4 Échéancier des travaux

Le devoir est à remettre avant le jour et l'heure indiqués comme étant la date de remise sur Moodle. Tout retard dans la remise des travaux sera sanctionné d'une pénalité de 10 % de la note finale par jour de retard.

2.5 Utilisation d'appareils électroniques et du courriel

Selon le règlement complémentaire des études, section 4.2.3 [4], l'utilisation d'ordinateurs, de cellulaires ou de tablettes pendant une prestation est interdite à condition que leur usage soit explicitement permise dans le plan de cours.

Dans ce cours, l'usage de téléphones cellulaires, de tablettes ou d'ordinateurs est autorisées. Cette permission peut être retirée en tout temps si leur usage entraîne des abus.

Tel qu'indiqué dans le règlement universitaire des études, section 4.2.3[5], toute utilisation d'appareils de captation de la voix ou de l'image exige la permission de la personne enseignante.

Note : Je réponds aux questions posées par courriel à l'extérieur des périodes de cours.

3 Matériel nécessaire pour l'activité pédagogique

Une machine personnelle Windows 10/11 avec les caractéristiques minimales recommandées suivantes :

- Processeur Intel core i5 de11eme génération ou AMD Ryzen 5 Mobile Processor de série 5000
- Mémoire RAM d'au moins 16 Go
- Disque dur SSD d'au moins 512 Go. (Les HDDs peuvent causer des ralentissements)
- Carte WIFI 802.11ac ou mieux.
- Idéalement, une carte graphique compatible avec OpenGL 4.x.
- Une résolution d'écran de 1080 lignes ou plus.
- Connexion Internet d'une vitesse minimale de 30Mbps.

4 Références

[1] GEORGIA WEIDMAN : *Penetration Testing : A Hands-On Introduction to Hacking*. No Starch Press, 2014.

[2] https://www.usherbrooke.ca/sciences/fileadmin/sites/sciences/documents/Etudiants_actuels/Informations_academiques_et_reglements/2017-10-27_Reglement_facultaire_-_evaluation_des_apprentissages.pdf

[3] https://www.usherbrooke.ca/registraire/droits-et-responsabilites/reglement-des-etudes/

[4] https://www.usherbrooke.ca/sciences/fileadmin/sites/sciences/documents/Etudiants_actuels/Informations_academiques_et_reglements/Sciences_Reglement_complementaire.pdf

[5] https://www.usherbrooke.ca/registraire/droits-et-responsabilites/reglement-des-etudes/

[2] PATRICK ENGEBRETSON : *Les bases du hacking*. PEARSON EDUCATION, 2013.

UNIVERSITÉ DE SHERBROOKE

L'intégrité intellectuelle passe, notamment, par la reconnaissance des sources utilisées.
À l'Université de Sherbrooke, on y veille!

Extrait du *Règlement des études* (Règlement 2575-009)

9.4.1 DÉLITS RELATIFS AUX ÉTUDES

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 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 des 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 tirée de l'œuvre d'autrui);

b) commettre un autoplagiat, 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) obtenir par vol ou toute autre manœuvre frauduleuse, posséder ou utiliser du matériel de toute forme (incluant le numérique) non autorisé avant ou pendant une production faisant l'objet d'une évaluation;

f) copier, contrefaire ou falsifier un document pour l'évaluation d'une activité pédagogique;

[…]

Par plagiat, on entend notamment :

- Copier intégralement une phrase ou un passage d'un livre, d'un article de journal ou de revue, d'une page Web ou de tout autre document en omettant d'en mentionner la source ou de le mettre entre guillemets;
- reproduire des présentations, des dessins, des photographies, des graphiques, des données… sans en préciser la provenance et, dans certains cas, sans en avoir obtenu la permission de reproduire;
- utiliser, en tout ou en partie, du matériel sonore, graphique ou visuel, des pages Internet, du code de programme informatique ou des éléments de logiciel, des données ou résultats d'expérimentation ou toute autre information en provenance d'autrui en le faisant passer pour sien ou sans en citer les sources;
- résumer ou paraphraser l'idée d'un auteur sans en indiquer la source;
- traduire en partie ou en totalité un texte en omettant d'en mentionner la source ou de le mettre entre guillemets ;
- utiliser le travail d'un autre et le présenter comme sien (et ce, même si cette personne a donné son accord);
- acheter un travail sur le Web ou ailleurs et le faire passer pour sien;
- utiliser sans autorisation le même travail pour deux activités différentes (autoplagiat).

Autrement dit : mentionnez vos sources