Université du Québec en Outaouais **Département d'informatique et d'ingénierie**

Sigle : INF1443 Gr. 01
Titre : Sécurité des réseaux informatiques
Session : Automne 2021 Horaire et local
Professeur : Couture, Mathieu

1. Description du cours paraissant à l'annuaire :

Objectifs

Permettre à l'étudiant d'approfondir par la pratique les techniques d'analyse de vulnérabilités, d'élaboration de scénario d'attaques et de sécurisation des systèmes et réseaux informatiques.

Contenu

Démarche utilisée par un intrus pour attaquer un réseau informatique : reconnaissance, acquisition d'informations, exploitation, sécurisation d'accès, élimination des traces. Principaux outils utilisés pour analyser et attaquer un réseau : whireshark, nmap, nessus, metasptoit, etc. Vulnérabilités des systèmes Windows et Unix. Vulnérabilité des applications. Contre-mesures disponibles pour faire face aux différentes attaques réseaux. Sécurité des réseaux sans fils. Réseaux virtuels privés et leurs vulnérabilités. Ce cours comporte des séances obligatoires de travaux dirigés (TD) de deux heures par semaine.

Descriptif – Annuaire

2. Objectifs spécifiques du cours :

- Maîtriser la démarche utilisée par un intrus pour attaquer un réseau informatique : reconnaissance, acquisition d'informations, exploitation, sécurisation d'accès, élimination des traces;
- Découvrir les principaux outils utilisés pour analyser et attaquer un réseau : whireshark, nmap, nessus, metasptoit, etc.;
- Comprendre les principales vulnérabilités des systèmes Windows et Unix;
- Comprendre les principales vulnérabilités des applications;
- Découvrir les différentes contre-mesures disponibles pour faire face aux différentes attaques réseaux;
- Démystifier la sécurité des réseaux sans fils;
- Comprendre les réseaux virtuels privés et leurs vulnérabilités;
- Comprendre les différents types de pare-feu.

3. Stratégies pédagogiques :

Le cours est développé de manière magistrale :

- Séances de cours de 3 h/semaine comprenant un cours magistral en mode présentiel.
- Des questions pourront être posées sur Moodle sur le forum de discussion du cours.
- Huit laboratoires obligatoires en mode présentiel sont prévus pour mettre en pratique les concepts du cours. Les étudiant(e)s devront avoir un ordinateur personnel avec la technologie de virtualisation VMware (disponible gratuitement) et un minimum de 8GB de mémoire vive.
- Un projet à présenter en classe est également prévu.
- Des points seront attribués pour la participation hebdomadaire à une revue de presse des événements marquants de la semaine en cybersécurité. On demande aux étudiant(e)s de publier un résumé d'article chaque semaine (avant l'heure du cours) sur le site Moodle du cours.

4. Heures de disponibilité ou modalités pour rendez-vous :

- Disponible pour répondre aux courriels dans un délai typique de 48 heures à **mathieu.couture@uqo.ca**

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	**Cours 1 : Introduction** • Présentation du contenu du cours • La chaîne de frappe Lockheed Martin • Rappel sur les protocoles TCP/IP : TCP, IP, UDP, ARP et ICMP • Interception et analyse du trafic via Wireshark	09 sept. 2021
2	**Cours 2 : Gestion d'incidents** • Organiser une équipe de réponse aux incidents • Répondre à un incident • Coordination et partage	16 sept. 2021
3	**Cours 3 : Reconnaissance** • Techniques et outils de reconnaissance passive d'un réseau • Techniques et outils de reconnaissance active d'un réseau • Énumération des versions de logiciel installées sur un client Web **Séance de laboratoire 1 :** Le 21 septembre 2021	23 sept. 2021
4	**Cours 4 : Armement** • Vulnérabilités au niveau du code • Étude de cas : Injection de code SQL • Vulnérabilités des serveurs • Étude de cas : Exécution de code à distance • Vulnérabilités des clients et applications • Études de cas : Vulnérabilité de Java **Séance de laboratoire 2 :** Le 28 septembre 2021	30 sept. 2021
5	**Cours 5 : Livraison** • Le SPAM • L'ingénierie sociale • L'affichage publicitaire malicieux • Les dispositifs USB • Les attaques par trou d'eau **Séance de laboratoire 3 :** Le 05 octobre 2021	07 oct. 2021
6	**Semaine d'études**	14 oct. 2021
7	**Cours 6 : Exploitation** • Kits d'exploitation de vulnérabilités	21 oct. 2021

	• Études de cas : Blacole, Neutrino, Fiesta • L'analyseur Bro **Séance de laboratoire 4 :** Le 19 octobre 2021	
8	**Examen intra**	28 oct. 2021
9	**Cours 7 : Installation** • Les téléchargeurs • Les rootkits • La persistance • L'analyse forensic • Les outils FTK et EnCase • Les règles Yara **Séance de laboratoire 5 :** Le 02 novembre 2021	04 nov. 2021
10	**Cours 8 : Commande et contrôle** • Le protocole IRC • Le protocole HTTP • Algorithmes de génération de domaines • Étude de cas : Andromeda, Asprox • Les protocoles de pair à pair • Études de cas : Zeus, ZeroAccess • Le déroutement **Séance de laboratoire 6 :** Le 09 novembre 2021	11 nov. 2021
11	**Cours 9 : Actions sur l'objectif** • La fraude de clics • Le forage de crypto-monnaies • Les Trojan bancaires • Le vol d'identité • L'extorsion • Audits de sécurité **Séance de laboratoire 7 :** Le 16 novembre 2021	18 nov. 2021
12	**Cours 10 : Infrastructures sécurisées** • Différents types de pare-feu (*firewall*) • Les systèmes de détection d'intrusions (IDS) • Les proxys Web • Zones démilitarisées (DMZ) • Les tunnels SSH • Les réseaux privés virtuels **Séance de laboratoire 8 :** Le 23 novembre 2021	25 nov. 2021
13	**Cours 11 : La sécurité SSL/TLS** • Architecture de SSL/TLS	02 déc. 2021

	• Les vulnérabilités de SSL/TLS • Les utilisations malicieuses de SSL/TLS • Étude de cas : le téléchargeur Upatre	
14	**Cours 12 : Présentation des projets** • Une présentation de 20 à 30 minutes dans laquelle vous présenterez votre projet devra être faite en classe dans les dernières semaines.	09 déc. 2021
15	**Examen final**	16 déc. 2021

6. Évaluation du cours :

L'évaluation du cours se fera comme suit :

(Examen intra en présentiel 25 %) + (Examen final en présentiel 25 %) + (Laboratoires 24 %) + (Projet 16 %) + (Revues de presse 10 %)

7. Politiques départementales et institutionnelles :

- Politique du département d'informatique et d'ingénierie relative à la tenue des examens
- Note sur le plagiat et sur la fraude
- Politique relative à la qualité de l'expression française écrite chez les étudiants et les étudiantes de premier cycle à l'UQO
- Absence aux examens : cadre de gestion, demande de reprise d'examen (formulaire)

8. Principales références :

Plusieurs références Web seront fournies tout au long du cours.

9. Page Web du cours :

https://moodle.uqo.ca