

Séminaire Informatique

Analyse Forensique

(8INF918)

Professeur :

Trimestre: Été 2023

Objectifs du cours

Sensibiliser les futurs professionnels du monde numérique aux problématiques de sécurité des systèmes et des réseaux. L'approche de ce cours sera à la fois offensive et défensive. Elle permettra non seulement de comprendre et d'utiliser les outils actuellement à la disposition des pirates informatiques mais aussi de travailler sur les moyens d'investigation et de protection.

Contenu général

Les attaques informatiques font malheureusement partie intégrante de notre monde ultra-connecté. Le but de ce séminaire est d'assurer que les futurs professionnels du monde numérique soient :

- Conscients des risques en termes de cybersécurité encourus par les composants des systèmes d'information modernes,
- Capables d'identifier des anomalies et de les investiguer,
- En mesure de s'en protéger.

La première partie de ce séminaire sera orientée "offensif" et permettra, au travers de divers travaux pratiques, d'appréhender la sécurité telle que vue par l'attaquant. Différents scénarios et cas de figure seront ainsi étudiés afin de permettre aux participants de bien cerner différents aspects de la sécurité d'un système d'information (réseau, système, applicatif).

La seconde partie permettra aux étudiants d'appréhender différentes techniques forensiques afin d'être capable d'investiguer différents scénarii liés à une utilisation non conforme de moyens numériques.

À la fin de ce module, les participants devront être capables d'identifier les points faibles d'une architecture informatique et de proposer des éléments de mitigation permettant d'accroître les niveaux de sécurité d'une architecture existante.

Contenu spécifique

Introduction générale

- Présentation des enjeux de la sécurité des systèmes d'information
- Pourquoi est-ce que la sécurité est un sujet si complexe ?

Les risques principaux d'un environnement numérique

- Les risques liés aux réseaux
- Les risques liés aux systèmes
- Les risques associés au développement applicatif

L'informatique légale (computer forensics)

- Les différents aspects de l'informatique légale et sa place en sécurité informatique
- Les analyses réseaux & systèmes
- Les analyses liées aux systèmes de fichiers

Les contre-mesures et la gestion du risque

- Comment se protéger activement ?
- Anticipation et gestion du risque

Formule pédagogique

Les contenus théoriques et les concepts de base seront présentés sous la forme de cours magistraux.

Pour diverses thématiques, des expérimentations pratiques des différents concepts seront réalisées afin de non seulement les comprendre mais également de les appréhender et d'en comprendre les risques & impacts.

Des présentations réalisées par les étudiants sur des points spécifiques complèteront le séminaire.

Un accès aux cours Cisco Netacad Cyberops et IoT Security seront également disponibles pour travail personnel complémentaire.

Modes d'évaluation

QCM sur la base de ce qui a été vu en cours :	30 %
Travaux pratiques (sur la base des documents remis en fin de TP) :	40 %
Présentations :	30 %

Intervalles des notes

A+	de 94 à 100
A	de 87 à 93
A-	de 80 à 86
B+	de 73 à 79
B	de 66 à 72
B-	de 59 à 65
C+	de 52 à 58
C	de 45 à 51
I	Incomplet

Dates de QCM

Mi-juin : QCM final

La date précise sera donnée dès le début du cours en fonction des créneaux mis en place. En cas de modification, les informations seront données en cours et sur le site Moodle de l'UQAC.

Précisions

En fonction des contraintes organisationnelles, les premiers cours pourraient se dérouler à distance. Cependant, la majeure partie du module se fera en présentiel. Les TP utiliseront des environnements sécurisés permettant de tester réellement les différents outils abordés en cours.

Certains TP donneront lieu à un compte-rendu qui devra être remis au plus tard au début de la séance suivante.

Présentations

Les thèmes des présentations, leurs dates ainsi que les étudiants ayant choisi le sujet seront publiés et mis à jour sur le site Moodle du cours.

Maîtrise du français

Le pourcentage de pénalité possible pour les déficiences linguistiques pour chaque travail ou examen est fixé à 20.

Site du cours

Consultez régulièrement le site du cours pour des instructions complémentaires sur l'organisation, les diapos de cours, les sujets de TP, les références bibliographiques, les documents complémentaires...

Bibliographie

Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, Terron Williams, "Grey Hat Hacking, The Ethical Hacker's Handbook", Third Edition, Mc Graw Hill, 2011

Brian Carrier, "File System forensic analysis", Addison Wesley, 2005

Dafydd Stuttard, Marcus Pinto, "The Web Application Hacker's Handbook", Second Edition, Wiley Publishing Inc, 2011

David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni, "Metasploit : The Penetration Tester's Guide", no starch press, 2011

Keith Makan, "Penetration Testing with the Bash shell", Packt Publishing Ltd, 2014

Kevin M. Henry, "Penetration Testing: Protecting networks and systems", IT Governance Publishing, 2012

Lee Allen, "Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide", Packt Publishing Ltd, 2012

Lee Allen, Tedi Heriyanto, Shakeel Ali, "Kali Linux - Assuring Security by Penetration Testing", Packt Publishing Ltd, 2014

Patrick Engebretson, "The Basics of Hacking and Penetration Testing", Second Edition, Syngress, 2013

Rafay Baloch, "Ethical Hacking and Penetration Testing Guide", CRC Press, 2014

Stuart McClure, Joel Scambray, George Kurtz, "Hacking Exposed 6: Network Security Secrets & Solutions", Mc Graw Hill, 2009

Thomas J. Mowbray, "Cybersecurity: Managing Systems, Conducting Testing and Investigating Intrusions", Wiley, 2014

Thomas Wilhelm, "Professional Penetration Testing", Second Edition, Syngress, 2009

Willie L. Pritchett, "Kali Linux Cookbook", Packt Publishing Ltd. 2012

Aditya Gupta , "The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things", Apress 2019

Aaron Guzman, Aditya Gupta, "IoT Penetration Testing Cookbook: Identify vulnerabilities and secure your smart devices", Packt, 2017

Roger A. Grimes, "Hacking the Hacker: Learn from the Experts Who Take Down Hackers", Wiley 2017

Penetration Testing Essentials – Sean-Philip Oriyano, Sybex, 2017

Cisco Netacad CyberOps Associate, version 1.02

Cisco Netacad IoT Security, version 1.1