HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

Département des Technologies de l'Information et de la Communication (TIC)

Projet d'audit de sécurité technique (AST)

3ème année Bachelor, orientations TS
Semestre 5 (16.09.2019 – 26.01.2020)
Année 2019-20

Organisation de l'unité

1. Objectifs

A la fin du cours les étudiants devront être capable de :

(expliquer l'organisation sécurité d'une entreprise)

- Décrire les principes fondamentaux de la sécurité de l'information dans une entreprise (confidentialité, intégrité, disponibilité, menace, vulnérabilité, asset, risque…). Décrire les différents types de contrôles ainsi que le lien entre les objectifs de sécurité et les contrôles nécessaires.
- Donner la définition de système de gestion de sécurité de l'information (SMSI) et expliquer le processus de son implémentation au sein de l'entreprise.

(effectuer un test d'intrusion)

- Expliquer les différents types de test d'intrusion ainsi que différentes phases, Démontrer la connaissance du framework pour les tests d'intrusion
- Conduire les phases préparatoires, discuter/valider le scope avec les responsables de l'entreprise. Rédiger le scope et définir les règles d'engagement pour le projet.
- Effectuer le scanning et l'exploitation des targets d'une manière responsable en limitant au maximum l'impact sur l'environnement de l'entreprise.
- Rédiger le rapport et présenter les résultats aux responsables de l'entrerprise.

(décrire les bases d'un audit de sécurité)

- Expliquer la différence entre un audit, par exemple de certification ISO 27001, une évaluation technique de la sécurité d'un système, un test d'intrusion via ethical hacking
- Nommer les concepts et principes fondamentaux d'un audit ISO 27001. Enumérer les parties d'une certification ISO 27001, les différents acteurs qui interviennent ainsi que les différents types d'évidence servant à l'audit.
- Décrire les phases et activités d'un audit ISO 27001 (scope, collection d'évidences, établissement de plan de test, interviews, rapport, mise en lumière des non-conformités, présentation finale).

2. Contenu

1. **L'audit ISO 27001 des systèmes de gestion de sécurité de l'information**
   - 1.1. Introduction
   - 1.2. Système de gestion de sécurité de l'information
     - Aspects de communication, comportement chez un client et gestion de conflit

2. **Évaluations de sécurité et tests d'intrusion**
   - 2.1. Introduction aux évaluations techniques et tests d'intrusion
     Préparation – planification, scoping et reconnaissance
   - 2.2. Scanning
   - 2.3. Gestion des vulnérabilités
   - 2.4. Exploitation
     - Outils
   - 2.5. Présentation des résultats et rapport, les aspects de communication

3. **Projet pratique**

3. Philosophie du cours

3.1. Cours

Certaines notions seront enseignées par le professeur.

3.2. Exercices théoriques et pratiques

Les exercices permettent à l'étudiant-e de tester et d'approfondir les concepts appris. Ce sont des questions théoriques, des études de cas, des problèmes à résoudre et des manipulations pratiques. Les exercices seront annoncés pendant les cours. Selon le temps à disposition, certains exercices pourront être démarrés ou effectués en classe. Sinon, ils seront à réaliser en tant que travail personnel.

De manière générale, les exercices ne seront pas notés.

3.3. Projet

Le projet constitue la plus importante partie du travail de ce cours. Les modalités détaillées seront expliquées dans un document séparé.

Pour rendre son projet, un email avec les éléments à fournir pour l'évaluation (voir les modalités précises) devra être envoyé au professeur et à l'assistant au plus tard à la date d'échéance.

L'assimilation des connaissances et l'acquisition des connaissances prévues dans les projets pourront être vérifiées lors des présentations effectuées par l'étudiant.

3.4. Présentation du projet

Les résultats du projet seront présentés à la fin du semestre selon les modalités détaillées.

4. Examen

Il n'y a pas d'examen pour ce cours. La note du cours sera basée sur la note du projet et contrôle continu.

5. Documents de l'unité

Les éventuelles informations concernant l'unité seront disponibles à cet emplacement :

Mac OS X	cifs://eistore1.einet.ad.eivd.ch/profs/AKV/cours/2018-19-AST
Windows	\\eistore1\profs\AKV\cours\2018-19-AST

6. Sanctions

6.1. Rendu en retard

Pour les rendus en cours de semestre (archives, présentations, projets, etc.), en cas de retard, les pénalités suivantes seront appliquées sur la note du sujet :

Entre 0 et 1 heures :	-0.5pt
Entre 1 et 3 heures :	-1.0pt
Entre 3 et 12 heures :	-1.5pt
Entre 12 et 24 heures :	-2.0pt
Entre 1 et 2 jours :	-3.0pt
Dès 2 jours :	la note de 1 est assignée au sujet

6.2. Travail non-rendu, absence

Pour rappel, la note de "un" est attribuée par défaut pour tout laboratoire non rendu (projet) ou pour toute absence lors d'une évaluation (présentations) ou à l'examen final (EF) (sauf certificat médical ou autre justificatif valable validé par le secrétariat).

6.3. Plagiat

Les cas de plagiat ou de tricherie détectés lors de laboratoires, les travaux écrits, ou l'examen final sont considérés comme graves. La note de "un" sera attribuée à toutes les personnes impliquées (y compris celles qui mettent leurs travaux "à disposition"), et le cas sera dénoncé au doyen.

7. Note finale

Calcul de la note de contrôle continu :

La note de contrôle continu est déterminée sur la base du test réalisé en cours, lors de la partie théorique du cours ainsi que la présentation sur la partie scoping du projet.

Calcul de la note finale :

La note finale est composée de

- 20 % de la note de tests (**contrôle continu**),
- 20 % de la note du scoping pour le projet (**contrôle continu**),
- 60 % de la note du **projet (rendu et présentation finale)**.

8. Répartition des heures

8.1. Répartition des heures selon la fiche d'unité

Travail encadré	80 périodes
Travail personnel	80 périodes
Total	160 périodes (soit 120 heures)

8.2. Répartition du travail encadré

Exposés en classe	19 périodes
Exercices en classe (labos)	3 périodes
Contrôle continu (présentations)	0 périodes
Projet	58 périodes
Total	80 périodes

8.3. Répartition du travail personnel

Révision du cours	0	Revue du cours et lecture de divers supports
Présentations des étudiants	30	Préparation des sujet et présentations
Exercices théoriques/pratiques	0	Résolution d'exercices et manipulations pratiques
Projet	50	Finalisation des laboratoires et projets et rédaction des rapports
Préparation au contôles	0	Préparation aux travaux écrits
Total	80 périodes	

9. Livres de référence et supports

Cf cours.

10. Calendrier prévu AST

Ce calendrier est donné à titre indicatif et peut être changé en tout temps.

S	S	Séance	Date	Chap.	Contenu	Rendus
1	38	a	19.09	0, 1.1 ARS	Admin/Intro + Infosec fundamentals	
		b	20.09		Project – free/search for a company	
2	39	a	26.09	1.2, 2.1 JEB	Standards, Pentest	
		b	27.09	2.2, 2.3 ARS	Discovery and scanning, vulnerability management	
3	40	a	03.10		Discovery and scanning lab	
		b	04.10	2.4, 2.5 JEB	Exploitation and tools, Preparation of pentest (SOW), communications and reporting	
4	41	a	10.10		Exploitation lab	
		b	11.10		Exploitation lab	Project proposals to be approved by 13.10
	42	a	17.10		Exploitation lab	Quiz
		b	18.10		Lab and training	
5	43	a	24.10		Interruption des cours	
		b	25.10			
6	44	a	31.10		Project – free	
		b	01.11		Project – free	
7	45	a	07.11		Project – free	
		b	08.11		Project - free/ Q&A session G05	Optional deliverable (Lab pentest report) by 09.11 at 18:00
8	46	a	14.11		Project – free	
		b	15.11		Project - free/ Q&A session G05	
9	47	a	21.11		Project – Scoping presentations	
		b	22.11		Project – Scoping presentations	All scoping presentations done by 24.11
10	48	a	28.11		Project - free	
		b	29.11		Project - free/ Q&A session G05	
11	49	a	05.12		Project - free	
		b	06.12		Project - free/ Q&A session G05	
12	50	a	12.12		Project - free	
		b	13.12		Project - free/ Q&A session G05	
13	51	a	19.12		Project - free	Quiz ?
		b	20.12		Project - free/ Q&A session G05	
	52				Interruption des cours	
	1				Interruption des cours	
14	2	a	09.01		Project - free	
		b	10.01		Project - free/ Q&A session G05	
15	3	a	16.01		Project - free	
		b	17.01		Project - free/ Q&A session G05	Deliverables by 19.01 at 18:00
16	4	a	23.01		Presentations	
		b	24.01		Presentations	