Descriptif de module

Domaine : Haute Ecole Arc Ingénierie

1. Intitulé de module — Attaques et Mitigations (ATAMI)

Type de formation : ☐ Bachelor ☐ Master ☐ MAS ☐ DAS ☒ CAS ☐ Autres :

Langue principale d'enseignement : ☒ Français ☐ Anglais ☐ Allemand

2. Organisation

Crédits ECTS : **2**

Périodes : **30** (6 soirs)

Volume de travail :

	heures
Enseignement	22.50
Travail personnel	37.50
Travail total	60

3. Prérequis

☐ Avoir validé le module
☐ Avoir suivi le module
☐ Pas de prérequis
☒ Autres : Développement système, développement C, bases du réseau
Module LEGAL ou équivalent

4. Compétences visées / Objectifs généraux d'apprentissage

Compétences visées par le module	**A l'issue du module, l'étudiant est capable de :** - Démontrer une maîtrise des outils de reverse-engineering et de développement en développant des preuves de concepts d'attaque courants. - Sécuriser un réseau classique ou IoT et en vérifier la sécurité de l'aide d'outils. - Appliquer des contre-mesures permettant de limiter la surface d'attaque. - Mettre en place les mitigations permettant de prévenir la réalisation d'un risque et de réagir correctement à la survenue de risques.

5. Modalités d'évaluation et de validation

Evaluation des apprentissages

Evaluation des apprentissages

- Evaluations des différentes Unités d'Enseignement (UE)

Note finale du module :

M = moyenne des notes obtenues (au dixième de point).

Conditions de réussite :

Note finale du module M ≥ 4.0 (arrondie au demi-point)
Moyennes

La note finale du module permet d'établir la note ECTS.

6. Modalités de remédiation

☒ Remédiation possible
☐ Pas de remédiation
☐ Autre (précisez) : …

6a. Modalités de remédiation (en cas de répétition)

☒ Remédiation possible
☐ Pas de remédiation
☐ Autre (précisez) : …

7. Contenu et formes d'enseignement

Module	**ATAMI**	
Méthode d'enseignement	- Exposé et exercices théoriques	
Modalités d'évaluation	- Questionnaire individuel (aspects théoriques) - Mini-projet par groupe de 2, rendu quelques semaines après la fin du module	
Description du contenu (mots clés)	**Ecrire des preuves de concept d'attaques (PoC) : sur quelques exemples Zero Day déjà patchés** - Microsoft : pratique avec WinDbg, IDA, OllyDbg - Linux : pratique avec gdb, dobj, etc… - P.ex. Hertbleed, bash DNS, cache poisonning (DNSSEC), ARP, … **Sécuriser un réseau (firewall, proxy-gateway IoT, IDS/IRS/ IPS, DNS cache poisoning, DNSSEC, ARP, 802.1x IPv6, …)** **Utiliser les outils du pirate dans le cadre d'un réseau (Kali linux) pour un audit.** **Réduire la potentialité d'attaques** - Confinement p.ex. modèle de sécurité Android - Protections fournies par le processus, l'OS (compilateurs, OS : ASLR, cookies / stack canary, NX, PAE/64) **Attaques résiduelles (p.ex. ROP, interaction néfaste entre applications, p.ex. applications web et facteur humain).**	
Supports de cours	Au choix de l'enseignant.	
Outils utilisés	Au choix de l'enseignant.	
Bibliographie	Communiqué par l'enseignant	
Particularité d'organisation	Lieu	Neuchâtel
	Responsable de module	Marc Schaefer
	Intervenant(s)	Marc Schaefer, Claudio Cortinovis, Nabil Ouerhani, Ninoslav Marina, HEG
	Dates	Selon planification