Module ATAMI (attaques et mitigations)

Objectifs pédagogiques

A la fin du module, l'étudiant sera 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 à 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

Prérequis

- développement système, développement C, bases du réseau
- module LEGAL ou équivalent

Contenu

- écrire 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. Heartbleed, bash DNS, cache poisoning (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)

Formes d'enseignement

- 30% exposé et exercices théoriques
- 70% pratique

Evaluation

- questionnaire individuel (aspects théoriques)
- mini-projet par groupe de 2, rendu quelques semaines après la fin du module

Organisation

Crédits ECTS	2
Périodes	30 (6 soirs)
Lieu	Neuchâtel
Responsable de module	Marc Schaefer
Intervenant(s)	Marc Schaefer, Claudio Cortinovis, Nabil Ouerhani, Ninoslav Marina, Michaël Müller, HEG
Dates	selon planification