INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

Ingénierie de la sécurité des systèmes d'information

Analyse Post mortem ou Forensic

IDENTIFICATION

CODE : MS-CYNU-ANPM
ECTS : 2.0

HORAIRES

Cours :	9.0 h
TD :	3.0 h
TP :	16.0 h
Projet :	0.0 h
Face à face pédagogique :	28.0 h
Travail personnel :	6.0 h
Total :	34.0 h

ÉVALUATION

Rapport

SUPPORTS PÉDAGOGIQUES

VirtualBox avec une VM Linux (de préférence SIFT Workstation) avec Volatility.

LANGUE D'ENSEIGNEMENT

Français

CONTACT

M. DE RENEVILLE Florent
@
M. IDRISSI BELKASMI Mohammed
khalid.idrissi@insa-lyon.fr

OBJECTIFS RECHERCHÉS PAR CET ENSEIGNEMENT

Les objectifs de ce module sont :

Comprendre le déroulement d'une mission de réponse à un incident cyber.
Apprendre les bases des analyses post mortem.

PROGRAMME

Cour théorique (0,5j)
TD 1 - Analyse post mortem de journaux Web (1j)
TD 2 - Analyse post mortem d'un dump mémoire (1,5j)

BIBLIOGRAPHIE

https://www.virtualbox.org/wiki/Downloads
https://digital-forensics.sans.org/community/downloads

PRÉ-REQUIS

Connaissances Systèmes (Windows/Linux) ; réseau/architecture.