

## FORMATION

- **TITRE : Analyse avancée de la mémoire RAM**
- **OBJECTIFS PÉDAGOGIQUES**
  - Savoir comment réaliser un dump de RAM exploitable,
  - Savoir comment effectuer une analyse de mémoire étape par étape,
  - Connaître les bonnes pratiques de travail.

- **DESCRIPTIF DU COURS**

Ce cours enseignera aux participants comment réaliser un dump de RAM exploitable, comment effectuer une analyse de mémoire étape par étape et enfin les bonnes pratiques de travail.

L'analyse de la mémoire est devenue une compétence requise pour tous les examinateurs intervenants sur les incidents et investigation numérique. Quel que soit le type d'enquête, la mémoire système et son contenu expose souvent le premier morceau de fil de preuve qui, lorsqu'il est tiré, dénoue toute l'image de ce qui s'est passé sur le système cible. Où est le malware? Comment la machine a été infectée? D'où vient l'attaquant? Qu'est-ce que l'employé mécontent a effectué sur le système?

(Voir programme en page 2)

## MODALITÉS PRATIQUES

- **DURÉE/NOMBRE D'HEURES**  
4 jours / 24 heures
- **PRÉREQUIS D'ACCÈS À LA FORMATION**
  - Connaissances de base sur les systèmes d'exploitation
  - Connaissances élémentaires en langage Python (boucles, listes, ensemble, chaînes de caractères) et bash/console.
- **ÉQUIPEMENT NÉCESSAIRE**  
Ordinateur portable disposant des éléments suivants :
  - Système d'exploitation à jour (Windows XP, 7 ou 8)
  - RAM : 4 Go minimum
  - WiFi
  - VMWare
- **LIEU DE FORMATION**  
Mines Nancy, campus Artem
- **TARIFS**  
2 200 € net par personne, déjeuner compris

## CONTACT

- **RESPONSABLE PÉDAGOGIQUE**  
Guillaume BONFANTE  
✉ guillaume.bonfante@mines-nancy.univ-lorraine.fr  
Tél : +33 72 74 49 58
- **CONTACT ADMINISTRATIF**  
Mines Nancy  
Service de la DFSC  
✉ mines-nancy-dfsc@univ-lorraine.fr  
Tél : +33 3 72 74 48 67

## PLAN DU COURS

### ○ **MODULE 1**

#### **INTRODUCTION**

Le premier module introduit les concepts fondamentaux concernant la RAM, structure de la RAM, rappels sur le fonctionnement des OS.

### ○ **MODULE 4**

#### **STRUCTURE INTERNE DE LA MÉMOIRE**

Rappels sur le fonctionnement du processeur (IDT et SSDT), Extraction des tables, Rappels sur le fonctionnement d'un driver (Windows), Identification des hooks IRP, des fonctions, Extraction du binaire d'un rootkit.

### ○ **MODULE 2**

#### **DONNÉES NON STRUCTURÉES**

Vous apprendrez comment utiliser « Bulk Extractor » et « Yara » pour analyser les images de la mémoire et extraire les pistes d'enquête telles que des adresses électroniques, des paquets réseaux, et plus encore.

### ○ **MODULE 5**

#### **STRUCTURE INTERNE DE LA MÉMOIRE**

Reconstitution de RAM à partir de fichiers d'hibernation, Présentation et utilisation de Volatility, Analyse de crash système avec Volatility, Présentation et utilisation de Windbg pour l'analyse de crash de système.

### ○ **MODULE 3**

#### **INVESTIGATIONS SUR LES CONNEXIONS**

Connexions réseaux, liste des socket, lien entre application et ports utilisés.

### ○ **MODULE 6**

#### **MISE EN PRATIQUE**

Nous demandons aux étudiants d'analyser un dump mémoire que nous avons reconstitué à partir d'une machine infectée par un malware de type Flame. Le travail est réalisé par groupe de deux étudiants. Un point est fait après 3h d'exercice pour faire progresser ensemble le groupe.