Analyse avancée de la mémoire RAM
Utilisation de Volatility

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,
- Connaitre les bonnes pratiques de travail.
- Fonctionnement de Volatility

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?

MODALITÉS PRATIQUES

Durée/nombre d'heures
5 jours / 30 heures
Prochaine session : Janvier/Février 2022

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
2 750 € 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

(Voir programme en page 2)

MINESnancy
ARTEM

Analyse avancée de la mémoire RAM
Utilisation de Volatility

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 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 3
INVESTIGATIONS SUR LES CONNEXIONS

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

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 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 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.