MINESnancy
ARTEM

Code Malveillant et analyse mémoire avec Volatility

FORMATION

Titre : Code Malveillant et analyse mémoire avec Volatility

Objectifs pédagogiques

- Acquisition de mémoire RAM
- Fonctionnement de volatility
- Structure interne de la mémoire

Descriptif du cours

Savoir mener une investigation numérique ou à une réponse à incident est devenu une compétence indispensable pour de nombreux professionnels. Malheureusement, la plupart des analystes forensiques fait encore l'impasse sur la collecte et le traitement des données volatiles contenues notamment au sein de la mémoire vive (RAM).

La mémoire volatile contient une quantité importante d'informations en rapport avec l'état du système perdues lors de l'extinction de ce dernier. Les données peuvent concerner les informations réseaux, le registre, le système de fichiers, mais aussi l'utilisateur directement (mots de passe, clés de chiffrement, historique de navigation, traces ...).

(Voir programme du cours 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 3 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

MINESnancy
ARTEM

Code Malveillant et analyse mémoire avec Volatility

PLAN DU COURS

Module 1
acquisition de mémoire ram

Acquisition directe à partir de la RAM, Acquisition de la RAM d'une VM, Acquisition physique, Acquisition à partir de fichiers d'hibernation.

Module 2
le fonctionnement de Volatility

Architecture du framework Volatility, Présentation générale des plugins, Présentation générale des modules et leur intérêt, Utilisation des profils, Principes et limitations de Volatility.

Module 3
investigation sur l'utilisateur

Emploi de commandes de Volatility : Présentation des commandes, Interface avec l'utilisateur, Traitement des résultats.

Cas pratiques présentés : Recherche de clés maitres pour TrueCrypt et pour BitLocker, Recherche d'exécutables en mémoire (PE), Localisation d'images.

Module 4
structure interne de la mémoire I

Identification des indices d'utilisation de la machine

Cas pratiques présentés : Identification des sites visités, recherche de fichiers effacés, historique des connexions, timeline et analyse de logs, liste des applications utilisées.

Module 5
structure interne de la mémoire II

Reconstitution de l'utilisation d'une machine, Développement d'un plugin pour Volatility

Cas pratique présentés : recherche de mots de passe, recherche de clés PGP pour le mail.

Module 6
mise en pratique

Reconstitution de l'utilisation d'une machine, Développement d'un plugin pour Volatility

Cas pratique présentés : recherche de mots de passe, recherche de clés PGP pour le mail.