Malwares : détection, identification et éradication

Référence : **SECMALWARE** Durée : **3 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Connaissances du Système Microsoft Windows.

PROFIL DES STAGIAIRES

• Auditeurs techniques, Analystes de sécurité. • Responsables gestion incident. • Techniciens réponse incident.

OBJECTIFS

• Connaitre les différents malwares. • Identifier un malware. • Mettre en œuvre des contre-mesures adéquates. • Apprendre à manier les outils d'inspection du système.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité défensive

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

JOUR 1

Introduction aux malwares

- Virus
- Vers
- Botnet
- Rançongiciels
- Rootkits (userland – kernel-land)
- Bootkit

Eradication réponse à incident

- Processus inforensique et analyste de logiciels malveillants
- Réponse à incident automatisée sur un parc

JOUR 2

Détection

- Les anti-virus et leurs limites
- Chercher des informations sur un malware
- NIDS / HIDS
- EDR
- Concept d'IOC dans le cadre d'un SOC / CERT (hash, motifs, etc.)

JOUR 3

Identification

- Analyse dynamique manuelle
- Analyse dynamique automatisée (sandboxes)
- Analyse statique basique
- Introduction à l'analyse mémoire avec Volatility
- Introduction à la rétro-conception