Sécurité : Analyse de malware - expert

Référence : **SECMALW3** Durée : **5 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Très bonne connaissance de Windows, savoir faire du Reverse Engineering, savoir développer en Python ou Ruby, bien connaître les API Windows et avoir déjà analysé des malwares.

PROFIL DES STAGIAIRES

• Analystes des CERT, CSIRT, structures possédant une expérience dans l'analyse de malware ayant besoin d'analyser des codes malveillants complexes.

OBJECTIFS

• Apprendre à développer des obscurcissements. • Savoir analyser des malwares utilisés lors d'APT. • Savoir analyser un malware en mode noyau.

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 Techniques Cybersécurité

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

Windbg

Analyse d'un malware utilisé lors d'APT

- Persistance non documentée
- Dissimulation du code
- Détection des anomalies
- Machines virtuelles

Reverse Engineering avancé

- Communications interprocessus
- Techniques d'anti-débug et d'anti-Analyse
- Packers et obfuscation avancée
- Implémentation de CPU exotique

Automatisation

- Désobfuscation
- Unpacking

Noyau

- Processus de boot
- Infection du processus de boot
- Modifications de l'espace noyau
- PatchGuard
- Identification de la présence de rootkit
- Emulation du code exécutable
- Analyse de deux bootkits 64b