Sécurité : Analyse de malware - avancé

Référence : **SECMALW2** Durée : **5 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Bonne connaissance de Windows, savoir ce qu'est un processus, un malware, avoir des notions de Python ou Ruby.

PROFIL DES STAGIAIRES

• Analystes des CERT, CSIRT et structures ayant besoin d'analyser des codes malveillants.

OBJECTIFS

• Apprendre à développer un faux serveur C&C. • Connaître des techniques d'obscurcissement, d'extraction de configuration de malware. • Savoir comment analyser des malwares grâce à la rétro-conception.

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

Mise en place d'un environnement d'analyse

- Création d'une machine virtuelle orientée analyse
- Cloisonnement d'un code malveillant
- Exploitation des traces générées

Reverse Engineering et Assembleur x86 (32/64)

- Instructions / Registres / Mémoire
- Structure des fonctions
- Analyse statique de code exécutable

Analyse dynamique

- Debug d'exécutables
- Instrumentation d'un programme pour en extraire les actions

Analyse de malwares

- Méthode d'analyse
- Modification de l'environnement par le malware
- Techniques d'anti-analyse courantes
- Packing / Unpacking

Automatisation

- Développement d'outils de pré-analyse
- Extraction de configuration de malware
- Développement d'un faux C&C