Sécurité : Analyse de malware - les fondamentaux

Référence : **SECMALW1** Durée : **5 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Connaissances de base d'un langage de programmation compilé. • Connaissances solides en systèmes d'exploitation et réseau.

PROFIL DES STAGIAIRES

• Tout public intéressé par l'analyse de malware..

OBJECTIFS

• Configurer et utiliser un laboratoire d'analyse sur une machine virtuelle. • Connaître les modes opératoires des attaquants. • Connaître les techniques classiques de détection de malware. • Savoir effectuer une collecte d'informations forensics. • Savoir identifier les différentes familles de malwares.

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

Jour 1

- Présentation des différentes familles de malwares (ransomware, trojan...)
- Présentation des differents vecteurs d'infections les plus communs (Water Holing, Spear Phishing...)
- Les modes opératoires des attaquants (reconnaissance, intrusion initiale, persistance, pivot, exfiltration)
- Techniques classiques de detection (yara, IOC, containment...)
- Configuration d'un laboratoire d'analyse dans une machine virtuelle (VirtualBox ou VMware)
- Collect forensics via l'outil libre FastIR

Jour 2

- Analyse des données forensiques acquises lors de la journée précedente
- Analyse d'une image mémoire (RAM dump)
- Plateforme d'analyse de type sandbox (Cuckoo) et multi-antivirus
- Découverte de l'API Windows
- Présentation des techniques fréquement utilisées par les malwares (contournement de l'UAC, Hooks, injection de code...)

Jour 3

- Présentation des techniques de protections de Windows (EMET, credential guard, device guard, ASLR/DEP/SEHOP/CFG/...)
- Présentation de certains types de fichiers vecteurs de malware (pdf, Flash, Java, Office, Macro...)
- Etude du format de binaire Windows (PE)
- Apprentissage de l'assembleur X86 ainsi que les specificités de l'assembler X64 (mémoire, registres...)

- Architecture Win32 et création de processus (PEB, TEB, ...)

Jour 4

- Présentation de l'analyse statique (via IDA Pro / Radare2 / relyze)
- Présentation de l'analyse dynamique (via Immunity Debugger / WinDBG)
- Présentation des API de developpement sur ces deux logiciels
- Présentation des techniques d'obfuscation (chaines de caractères, API, ...)
- Analyse de packers
- Analyse d'un ransomware

Jour 5

- Analyse d'un exploit
- Analyse d'une ROP chain
- Analyse d'un shellcode
- Divers exercices
- Suivant le public: reverse kernel (configuration du lab, mecanisme, ...)