Sécurité défensive

Analyse de Malwares - Les fondamentaux

3 jours (21h00) | ★★★★★ 5/5 | SEC-MALW | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Document mis à jour le 29/03/2023

Objectifs pédagogiques

- Utiliser vos connaissances généralistes sur le fonctionnement des malwares
- Décrire une méthodologie d'analyse statique et dynamique
- Créer des charges encodées.

Modalités et moyens pédagogiques

Formation délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode* démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour les cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

** ratio variable selon le cours suivi*

Niveau requis

Avoir des connaissances généralistes en programmation, système et réseaux.

Public concerné

Pentesters, développeurs, administrateurs et analystes.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Jour 1

Etat de l'art

- Introduction
- Historique
- Vecteurs d'infection
- Compromission
- Impacts business
- Défenses classiques

Bases système

- Séquence de boot
- Dissection d'un processus
- Dissection d'un exécutable
- Gestion de la mémoire
- Techniques communes
- Obfuscation, packers et encoders (évasion)

Environnement

- Infrastructure
- Bonnes pratiques et création d'un lab

Exemple de travaux pratiques (à titre indicatif)

- *Dépacking et désobfuscation d'une charge*

Outils d'analyse

- Analyse statique
- Analyse dynamique
- Présentation des outils d'analyse
- Découverte de la suite Sysinternals
- Introduction à la suite FLARE Mandiant
- Sandbox
  - VirusTotal
  - Cuckoo
  - AnyRun
- Signatures
  - YARA
  - Création de règles
  - Implémentation YARA
  - Plateformes d'échanges

Exemples de travaux pratiques (à titre indicatif)

- *Analyse d'un PDF*
- *Analyse Meterpreter, Unicorn et Macros*
- *Analyse d'une charge dans une Sandbox*
- *Signer des Malwares*

Jour 2

Exemple de travaux pratiques (à titre indicatif)

- *Analyse d'une attaque et rédaction d'un rapport*

Analyse de dumps mémoire

- Acquisition
- Volatility
  - Processus
  - DLL
  - Ruches
  - Injections
  - Connexions

Exemple de travaux pratiques (à titre indicatif)

- *Analyse de dumps mémoire*

Introduction à l'assembleur (ia-32)

- Introduction
- Registres
- Flags
- Instructions
- La pile

Exemples de travaux pratiques (à titre indicatif) : premiers programmes

- *Hello World (Write)*
- *Boucles*
- *Execve (/bin/sh)*

Jour 3

Shellcoding

- Introduction à GDB
- Commandes utiles
- Shellcode méthode stack
- Shellcode méthode Jmp-Call-Pop
- Les encoders
- Les stagers
- Où trouver des shellcodes ?
- Encoder des shellcodes existants (Metasploit)

Exemples de travaux pratiques (à titre indicatif)

- *Création d'un encodeur XOR*
- *Création d'un stager*
- *Reverse d'une charge*

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

Modalités d'évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation ou une certification (M2i ou éditeur)