Analyse des malwares – les fondamentaux

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Éligible au CPF : Non

Domaine : Sécurité informatique & cybersécurité

Action collective : Non

Filière : Sécurité défensive

PRÉSENTATION

Objectifs & compétences

À l'issue de cette formation, les participants seront capables de :
• Connaissances généralistes sur les malwares et leur fonctionnement
• Acquérir des notions d'analyse statique et dynamique
• Prise en main des outils d'analyse
• Acquérir des notions d'assembleur pour les appliquer à la rétro-ingénierie.

Public visé

Développeurs / administrateurs / Analystes en sécurité

Pré-requis

• Utilisation d'un système linux/Windows et des outils open source
• Base en scripting ou programmation (python, powershell)
• Notion théorique en réseau (Routage/ IP privée/publique, NAT)
• Notion théorique en cybersécurité (types d'attaque, concept d'élévation de privilège, persistance)

PROGRAMME

1. Etat de l'art

○ Introduction : Définition d'un malware, Présentation des différentes classifications, Les différentes typologies des malwares, La terminologie utilisée en cybersécurité
○ Vecteurs d'infection : Phishing, Drive By Download, Malvertising / scam
○ Réponse à incident : Description du rôle de l'analyste lors d'un incident (collecte, triage, containment, investigation), Méthodologies couramment utilisées en réponse à incident, Cas pratique
○ Détection antivirale : Approche de détection via Antivirus et EDR, Description des différentes méthodes de détection, Type de détection

2. Infrastructure d'analyse

○ Infrastructure : Infrastructure isolée et contrôlée en s'appuyant sur des machines virtuelles ou physiques, Configuration réseau pour limiter les risques (réseau isolé, NAT, simulation de services), Bonnes pratiques
○ Environnement d'analyse : Systèmes spécialisés tels que FlareVM (Windows) et REMnux (Linux), pour l'analyse statique et dynamique, Projets communautaires avec apport de scripts, règles et bases de connaissances, Plateformes d'analyse en ligne, Gestion et manipulation sécurisée des échantillons de malware

3. Analyse statique simple

○ Principe : Avantages / Inconvénients, Principales techniques d'analyse, Outils couramment utilisés, Règles YARA pour la détection et la classification des menaces
○ Analyse de documents malveillants (maldoc) : Présentation des formats les plus utilisés, les outils dédiés à leur analyse et les méthodes pour identifier macros, scripts, TP1 / analyse complète d'un document malveillant
○ Bases système 1 : Compréhension des exécutables malveillants (Notions de compilation, Structure du format PE, Mécanismes de Packer/crypters utilisés pour masquer le code et compliquer l'analyse)

Code de formation : MAFOUND

#CYBERSÉCURITÉ

€ Tarifs

Tarif & financement :
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :
Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
Le dispositif FNE-Formation.
L'OPCO (opérateurs de compétences) de votre entreprise.
France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
Contactez nous pour plus d'information : contact@aston-institut.com

Lieux & Horaires

Durée : 35 heures

Rythme : 5 jours. 12 au 16 Octobre 202630 Novembre au 4 Décembre 2026

Délai d'accès : Jusqu'a 8 jours avant le début de la formation, sous condition d'un dossier d'insciption complet

Prochaines sessions

Consultez-nous pour les prochaines sessions.

○ Analyse d'un exécutable : Méthodologie depuis l'identification du fichier jusqu'à l'extraction d'artefacts, Présentation des outils d'analyse, TP2 / Analyse d'un exécutable, TP BONUS / Analyse d'exécutable semi-compilé

4. Analyse dynamique simple

○ Principe : Observation du comportement d'un programme lors de son exécution dans un environnement contrôlé, Techniques d'analyse et Outils hybrides
○ Bases système 2 : Fonctionnement du Kernel, Distinction entre espace kernelland et userland, Rôle des API dans l'exécution des processus, Analyse de la structure interne d'un processus pour mieux comprendre les mécanismes d'injection et de manipulation mémoire
○ Analyse dynamique d'un exécutable : Observation concrète d'un exécutable malveillant à l'aide des outils Sysinternals et de solutions open source, TP3 / Analyse d'un exécutable
○ Analyse mémoire : Principales techniques d'injection de code, Utilisation des modules volatility, TP4 / Analyse mémoire

5. Introduction assembleur

○ Introduction : Présentation des principaux langages et syntaxes pour la compréhension des portions de code issues de désassemblage
○ Instructions fondamentales : Présentation des instructions les plus couramment rencontrés (MOV, ADD / SUB / MUL, AND / OR / XOR / NOT, PUSH / POP, JMP / CMP)
○ Registres : Présentation des différents registres et leurs rôles (Registres généraux, Registres d'index, Registres de pointeur, Registre d'instructions)
○ Pile et appel de fonctions : Structure mémoire de la pile, Notion de Stack Frame, Déroulement d'un appel de fonction, Usages des pointeurs ESP et EBP, Appels systèmes Syscalls (Fonctionnalités et librairies, Principe des tables des syscalls, Exemples illustrant leur usage dans des contextes malveillants)

6. Analyse avancée

○ Principe d'analyse statique : Rappel du cadre légal et éthique, Avantages / inconvénients de l'approche, Présentation des techniques avancées
○ Utilisation d'un debugger (Cutter) : Processus de désassemblage, Fonctionnalités clés de Cutter, Lecture hexadécimale
○ Utilisation de breakpoint (cutter) : Positionnement des breakpoints pour l'analyse du comportement d'un programme d'exécution, Interprétation de l'état des registres
○ Méthodologie d'analyse & patching : Formalisation d'une méthodologie de rétro-ingénierie, Introduction des techniques de patching, TP5 - Crackme

MODALITÉS

Modalités

1. Modalités d'organisation

○ Format : en présentiel, distanciel ou mixte
○ Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H
○ Interventions en Intra et Inter entreprise

2. Pédagogie

○ Pédagogie essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique
○ Alternance d'apports théoriques et d'outils pratiques

3. Ressources techniques et pédagogiques

○ Support de formation au format PDF ou PPT
○ Matériel : Ordinateur, vidéoprojecteur, Tableau blanc
○ Visioconférence : Cisco Webex / Teams / Zoom

4. Pendant la formation

○ Mises en situation
○ Autodiagnostics
○ Travail individuel ou en sous-groupe sur des cas réels

Méthode

1. Fin de formation

- Entretien individuel

2. Satisfaction des participants

- Questionnaire de satisfaction réalisé en fin de formation

3. Assiduité et validation

- Certificat de réalisation (validation des acquis)