USCB1A - Introduction à la rétro conception et analyse de Malware

Mis à jour le 24-05-2024

Code : USCB1A

Unité spécifique de type mixte

3 crédits

Responsabilité nationale :
EPN05 - Informatique / 1

Contact national :

Cnam Centre Régional de Bretagne

Zoopôle Les Croix
2 rue Camille Guérin
22440 Ploufragan
0 972 311 312
Isabelle Guée
bzh_master_cybersecurite@lecnam.

Présentation

Objectifs pédagogiques

Description :

Lorsqu'un malware est détecté dans un système informatique, les responsables sécurité doivent en connaître le fonctionnement pour mieux contrer ses effets. Cette formation aborde des techniques d'analyses statiques de code, de la retro-conception ainsi que la connaissance de techniques de bases de conception d'exploits utilisés par différents malwares pour persister ou détourner le comportement d'un programme légitime afin d'obtenir plus de privilèges.

Objectifs pédagogiques :

Être capable de faire une retro-conception d'un logiciel malveillant, de caractériser son comportement afin de comprendre la menace. Publier un rapport de sécurité au profit des institutions.

Compétences

Compétences acquises :

- Savoir préparer un laboratoire d'analyse d'un malware
- Savoir analyser et comprendre le comportement de logiciels malveillants
- Savoir détecter et contourner les techniques d'autoprotection
- Savoir rédiger un rapport d'analyses sur un malware

Savoirs :

- Comprendre les techniques d'infection, d'exploitation de vulnérabilité, Shellcode, logiciel IDA, Cuckoo SandBox, mécanisme de protection anti-malware

Programme

Contenu

Contenu :

- Introduction
  - Cadre légal concernant la rétro conception
  - Typologie des malwares, vecteurs d'infection, mécanisme de persistance et de propagation
  - Triptyques moyens de l'attaquant / volonté / intérêt de la cible
- Introduction au binaire
  - Chargement et exécution en mémoire (code, données, imports et relocations)
  - Introduction à l'assembleur x86 (instructions, Piles / Tas, conventions d'appels, appels systèmes, etc.)
- Compréhension technique des vulnérabilités et exploits
  - Mise en place d'un laboratoire d'analyse
  - Les vulnérabilités de corruption mémoire
    - Buffer overflow sur la pile
    - Integer overflow (Explications, manipulation et contre-mesures)
    - Vulnérabilités sur le tas (Heap buffer overflow, User after free, Double free)
    - Les mitigations et contournements (canaris, ASLR, DEP) et mécanismes modernes (Windows 10)
- Les shellcodes
  - Différences avec un binaire

    - Indépendance vis-à-vis d’un loader
    - Création d’un shellcode linux en assembleur
- Analyse statique de malware
    - Utilisation du logiciel Ghidra (méthodologie, analyse statique de code)
    - Patterns et signatures, vérification d'intégrité, Métriques d'entropie, heuristiques, etc.
- Analyse dynamique de malware
    - Introduction à Cuckoo SandBox
    - Debug et suivi de traces
- Mécanismes d’anti-analyse
    - Packing / protection (chiffrement de codes, anti-désassemblage)
    - Protection contre les machines virtuelles, les débogueurs, outils de rétro-ingénierie
    - Offuscation, chiffrement, ancrage
- Le rapport d’analyse

Modalités de validation

- Examen final

Description des modalités de validation

Examen de 2 heures ou dossier à rendre (rapport d'analyse technique à produire concernant un malware à analyser)