USCB19 - Analyse d'un système après incident

Mis à jour le 21-01-2025

Code : USCB19

Unité spécifique de type mixte

6 crédits

Responsabilité nationale :
EPN05 - Informatique / Nicolas PIOCH

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

Prérequis

RSX112, SMB101 ou SMB111

Objectifs pédagogiques

Description :

Suite à l'identification d'une attaque, il est essentiel d'être en mesure de faire une analyse des dommages subis et des traces laissées par les attaquants afin d'établir la chronologie événementielle pour reconstituer l'attaque et collecter des éléments exploitables en justice. Elle permet également d'identifier les actions d'ordre technique à mener pour neutraliser la menace et améliorer la protection du SI.

Objectifs pédagogiques :

Cette formation aborde l'analyse post-mortem d'un incident de sécurité (appelée également Inforensic). Elle vise à former à une méthodologie d'investigation numérique et aborde ensuite des ensembles d'éléments techniques à analyser suite à une attaque.

Compétences

Compétences acquises :

- Connaître les aspects juridiques de l'analyse forensic
- Mettre en pratique une investigation numérique
- Savoir collecter des informations utiles pour établir un dossier de preuves
- Comprendre, identifier le scénario d'attaque, être capable de le restituer

Savoirs :

- Repérer des anomalies, analyse réseau, mémoire, partitions, artefacts systèmes

Programme

Contenu

- Introduction à l'investigation numérique
  - Bases légales de la sécurité de l'information
  - Classification des crimes informatiques
  - Acteurs technico-juridiques : CERT, agences gouvernementales
- Méthodologie d'investigation légale
  - Audit préalable
  - Enregistrement et collecte de preuves (CoC) et mise sous séquestre
  - Rapport, constitution de la timeline
- Investigation Réseau
  - Acquisition des preuves et sondes
  - Compréhension des traces réseaux
  - Identification d'attaques (ARP Storm, ARP Spoofing, DHCP Starvation, Scan Réseau, exfiltration de données, etc.)
- Investigation Système
  - Analyse des systèmes de fichiers (FAT, NTFS)
  - Artefacts Systèmes (EVTX, Base de registres, Volumes Shadow Copies, Jumplist, prefetch, AMCache, etc.)
  - Analyse de la mémoire vive
  - Artefacts Applicatifs
  - Navigateur et messageries
- Investigation des Smartphone :
  - Pourquoi analyser un smartphone
  - Types de malware en PUA (Potentially Unwanted App)

    - Vecteurs d’infection
    - Exemple de détection d’attaques
    - Composants (Flash, SIM, CPU, RAM, SQLite DB)
    - Extraction de dump de téléphones
    - Application APK
- Investigation Web
    - Analyse de logs (déclinaison top 10 OWASP)
    - Analyse de bases de données
    - Désobfuscation

Modalités de validation

- Contrôle continu
- Mémoire

Description des modalités de validation

Contrôle continu + dossier