USCB10 - Etude de la posture de l'attaquant

Mis à jour le 21-01-2025

Code : USCB10

Unité spécifique de type mixte

3 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

UTC505 et RSX101

Objectifs pédagogiques

Description :

Ce cours fournit une présentation de l'écosystème cyber, des stratégies d'attaques (simple ou complexe) connues afin de donner à l'auditeur la possibilité d'envisager des scénarios d'attaques des SI.

Objectifs pédagogiques :

Cette formation a pour objectif de faire comprendre le déroulé d'une attaque ainsi que l'infrastructure et l'organisation nécessaire à un groupe malveillant. Cet apprentissage présente la notion de vulnérabilité, la méthodologie d'une attaque ainsi que la notion de TTP (Tactics, Techniques and Procedure). Un approfondissement est ensuite réalisé avec la présentation des classifications Attaque et Défense du MITRE (ATT&CK security Alerts et D3FEND Matrix). Enfin de nombreux rapports de sécurité significatifs seront analysés et présentés par les auditeurs afin de comprendre les stratégies et la complexité de chaque attaque.

Compétences

Compétences acquises :

- Connaître l'environnement Cyber
- Comprendre des méthodologies et typologies d'attaques
- Comprendre la complexité et les moyens mis en œuvre dans le cas d'attaques complexes
- Rechercher et comprendre un rapport de sécurité
- Comprendre les stratégies et tactiques mises en œuvre par les attaquants
- Envisager des scénarios d'attaques de SI

Savoirs :

- Typologies d'attaques, TTPs, principe d'anonymisation, reverse connecte, Command and Control, Man In The Middle, Point d'eau, Air Gap.

Programme

Contenu

- Présentation de l'écosystème Cyber (acteurs et responsabilités, gouvernance et institutions, scripts kiddies, Hackers, APT)
- Présentation et stratégies des principaux APT identifiés
- Présentation de la notion de vulnérabilité
- Méthodologie d'une attaque
  - Phase de reconnaissance
  - Phase de repérage de failles (humaines, physiques, réseau, web, systèmes, applicative)
  - Phase d'intrusion, déplacement latéral, extension de privilèges, stratégie de progression
  - Pérennisation des accès
  - Phase d'exploitation
- Classification Attaque et Défense du MITRE (ATT&CK security Alerts et D3FEND Matrix), notions de TTP
- Analyses de rapports d'attaques (simples et complexes)
  - Intrusion par attaque distante par RCE (Remote Code Execution)
  - Intrusion par fishing
  - Attaque par point d'eau

    - Attaque par Man In The Middle / Man On The Side
    - Attaque par Supply Chain
    - Attaque par cryptolocker
    - Passage d’un Air Gap
    - Etc.

Afin de montrer leur compréhension, les auditeurs devront, par groupes, analyser des rapports de sécurité et les présenter à l’ensemble des auditeurs afin de voir un panel représentatif d’attaques cyber réelles.

Modalités de validation

- Mémoire

Description des modalités de validation

Dossier : Analyse et présentation de rapports de sécurité