Module spécifique CAS IN

Malwares et CTI (Cyber Threat Intelligence) : Récolte de traces et exploitation au profit de l'enquête

Cette formation de quatre jours a pour but de familiariser les participantes et participants avec une approche technique des attaques par malware (p. ex. Ransomware) dans le but de récolter des traces et des informations susceptibles d'être exploitées au profit de l'enquête.

Objectifs

- Approfondir les connaissances en matière de modes d'infection
- Développer des compétences en matière d'analyse de malwares
- Comprendre comment récolter des artefacts potentiellement exploitables
- Partager les expériences et avis au sujet des potentiels et limites en matière échange d'informations techniques avec les organismes étatiques (NCSC, partenaires étrangers, …)

Pré-requis

- Pratique des systèmes Windows, LinuxNotions TCP/IP
- Ligne de commande Linux
- Administration Windows/Linux
- Pratique des machines virtuelles (VM)

Equipements - infrastructure

- Le cours se déroule en salle informatique (salle 137) sur des machines configurées pour ce module
- Pour les personnes souhaitant venir avec leur propre équipement, il est judicieux de disposer d'une machine sur laquelle des VM peuvent être exploitées. Caractéristiques :
  - Hyperviseur permettant de faire fonctionner des machines virtuelles (x86), VMware/VirtualBox
  - Minimum 4 CPU
  - Minimum 16GB RAM
  - Minimum 60GB d'espace disque (SSD de préférence)
  - Les machines virtuelles seront basées sur Windows (7,10), Linux (Kali, Ubuntu)

Organisation

- Date : du 4 au 7 mars 2024 de 8h45 à 12h00 et de 13h15 à 16h30
- Lieu : Campus Arc 1, Espace de l'Europe 21, Neuchâtel, salle 137, 1er étage
- Repas : les repas de midi ne sont pas organisés par l'école. Une soirée facultative, à charge des participants et sur inscription (doodle), est prévue dans un restaurant de la région le mardi 5 mars.

Coût

- CHF 1280.- (un rabais de CHF 5.- est accordé en cas de paiement en ligne)

Chargé de cours

- M. Marc Doudiet, Senior Director – Global incident response – Kudelski Security

Module spécifique CAS IN

Malwares et CTI (Cyber Threat Intelligence) : Récolte de traces et exploitation au profit de l'enquête

Plan du cours

- **Lundi 4 mars 2024** :
  - Introduction, revues de menaces actuelles et particulièrement les attaques Ransomware.
  - Utilisation de la matrice MITRE, définition des TTPs.
  - Aperçu des outils de récoltes de CTI (Cyber Threat Intelligence). Aperçu des TIP (Threat Intelligence Platform).
- **Mardi 5 mars 2024** :
  - Analyse d'une attaque type lié à des acteurs utilisant des Ransomware.
  - Extraction d'artefacts lié à ce type d'attaque.
  - Création d'une ligne du temps rassemblant la totalité des artefacts extraits.
  - Laboratoire (hands-on)
- **Mercredi 6 mars 2024** :
  - Comment attribuer une attaque à un groupe d'attaquants, outils et méthodologie.
  - Prendre en considération les possibles fausses pistes des attaquants.
  - Extraction des outils (malware) utilisés par les attaquants.
  - Analyse des outils en vue d'extraction d'indicateurs de compromission
  - Laboratoire (hands-on)
- **Jeudi 7 mars 2024** :
  - Revue de la méthodologie complète
  - Analyses d'autres attaques et comment appliquer la méthodologie à d'autres attaques.
  - Aperçu des attaques étatiques.
  - Laboratoire (hands-on)
  - Partage d'expérience sur le partage d'information entre entités étatiques (Traffic Light Protocol, outils, …)