Contribution ID: **2** Type: **Présentation courte**

DFIR4vSphere: Investigation numérique sur la solution de virtualisation VMWare vSphere

Tuesday, June 7, 2022 11:30 AM (25 minutes)

VMWare vSphere est une solution de virtualisation composée d'hyperviseurs de type 1 (ESXi) et d'une console de gestion centralisée (VCenter). Selon VMWare, en entreprise près de 80% des environnements virtualisées reposent sur cette technologie. En conséquence c'est une cible de choix pour un attaquant. Dans cette présentation nous allons montrer comment utiliser le module PowerShell DFIR4vSphere pour collecter des journaux et artéfacts forensique aussi bien sur les hôtes ESXi que sur la console VCenter.

Primary author: SAVINA, Léonard (ANSSI)

Presenter: SAVINA, Léonard (ANSSI)

Track Classification: Investigation numérique: Techniques et outils d'analyse de supports numériques (forensic)