A Machine Learning Approach for Security Deception

Type de contenu : Texte

Titre(s) : A Machine Learning Approach for Security Deception / Enseigne de vaisseau Lefevre Thibaut ; Enseigne de vaisseau Locke Simon ; Directeur de projet : Bellekens Xavier (Dr.) ; Organisme d'accueil : Division of Cyber Security, Abertay University of Dundee, Scotland

Editeur, producteur : Lanvéoc-Poulmic : Ecole Navale, 2018

Description matérielle : 41p. : ill.en coul. ; 29,5 cm

Note de thèses et écrits académiques : PFE Masters 2018 Ecole Navale

Résumé ou extrait : La cyber-déception est un type de cyber-défense dont le but est de leurrer un attaquant en lui faisant croire qu'il s'attaque à un système authentique alors que ses données sont en réalité enregistrées. Le but de notre projet a été de créer un module Difficulty Engine au sein d'un système de cyber-déception en développement. Le Difficulty Engine a pour objectif de proposer à un attaquant le contenu qui lui est le plus adapté afin de le garder intéressé dans l'attaque qu'il mène sur un système leurre. Afin d'entraîner un modèle identifiant le niveau d'un attaquant avec des logiciels de machine learning - de type clustering - nous avons créé un système proposant à des attaquants différents niveaux de difficultés sur des pages vulnérables aux injections SQL et qui nous permettait de récupérer des données sur leurs essais. Les résultats ont montré que les attaquants pouvaient être groupés selon le temps passé sur un type de défense ou sur la structure des chaînes de caractères utilisées pour contourner celle-ci.