Présentation d'un cours d'analyse forensique et application de méthodes de ludification à des exercices de stéganographie

CTF&Stégano

O.Cros, G. Chenevert, A. Thiroux

18 décembre, 2020

CERISE Team, ISEN Lille, Junia, France

Qui sommes-nous ?

Nous

Equipe CERISE, ISEN Lille
Equipe de recherche spécialisée en cybersécurité pour les réseaux industriels et les systèmes embarqués
Ecole d'ingénieurs en informatique, majeure cybersécurité

Moi

Olivier Cros
Enseignant-Chercheur en cybersécurité
Analyse forensique, réseaux, cryptographie

Plan

- Cours d'analyse forensique
- Mise en pratique et évaluation
- Retour d'expérience

Structure du cours

4 blocs :

- Systèmes de fichiers et analyse mémoire
- Stéganographie et analyse de fichiers
- Pagination mémoire et exploîtation de pile
- Reverse engineering et analyse de malware
- + Un sous-bloc : méthodologie d'analyse forensique

Chaque bloc : 2h de cours + 6h de TP, 30 étudiants

Contenu du cours

Pré-requis

Etudiants de dernière année, déjà très sensibilisés
Réseaux, administration système, bases du développement scripté

Méthodes

- Image : Méthodes LSB, ADS, EXIF, analyse d'en-tête, chunks PNG
- Son : LSB, DSS, phase-coding, echo hiding
- Introduction au watermarking

Objectifs

Compétences visées

- Comprendre les enjeux de la Stéganographie
- Distinguer stéganographie et cryptographie
- Connaître les technologies usuelles
- Maîtriser les concepts et l'application des méthodes
- Comprendre les mécanismes de réflexion

Pourquoi la stégano ?

Moins classique, moins protocolaire
Travailler sur l'inventivité, la créativité, la réflexion

Mise en pratique

Format

Mise à disposition d'une copie de la mémoire d'une clé usb (fichier img)

Structure

3 exercices
Exercice 1 : 2 flags (analyse d'un pdf, analyse de données de géolocalisation)
Exercice 2 : 2 flags (chunks PNG, utilisation d'un flag pour déchiffrer une photo)
Exercice 3 : 5 flags (en-tête PDF, déconcaténation d'images, analyse d'exif, code morse, combinaison des flags)

Ludification

3 axes majeurs

Mise en contexte

Prendre le temps d'introduire un problème dans un cas réel (ou fictif), décoller les aspects académiques de l'exercice

Favoriser l'autonomie

Mettre à disposition une série de ressources mais laisser les étudiants travailler sous forme de micro-projet

Scoring

Associer des points aux flags, limiter l'effet tiroir des exercices
Paralléliser le barême académique et l'évaluation technique donnée par le scoring

Retours d'expérience

Etudiants

Bonne implication des étudiants déjà motivés
Perte légère de repères lié à l'aspect très autonome
Plus de curiosité sur des sujets connexes

Analyse pédagogique

Très bonne appropriation des connaissances
Développement global de la curiosité
Moins de formalisme sur les rendus

Conclusion

Protocol

Bonne réception des étudiants
Résultats pédagogiques satisfaisants
Charge de préparation similaire

Perspectives

Adapter l'exercice à des sujets de sécu non techniques
Coupler avec une plate-forme de CTF interne

Questions

Merci !

olivier.cros@junia.com - www.isen-lille.fr