Utilisation de l'outil d'analyse logicielle IDA Pro

FORMATION

- **Titre : Utilisation de l'outil d'analyse logicielle IDA Pro**

- **École :** Mines Nancy

- **Objectifs pédagogiques :**
  - Prise en main du logiciel IDA Pro

- **Descriptif du cours :**

  Ce cours a pour principal objectif la présentation du logiciel IDA Pro. Durant ce cours, les différentes fonctions clé de l'outil sont abordées: le module de désassemblage, le débogueur ainsi que les scripts Python.
  L'analyse de programmes binaires avec IDA est couverte dans ce cours étape par étape.
  Un volet du cours traite de la visualisation binaire de programmes afin de détecter et d'analyser les techniques d'offuscation et de dissimulation de code. Le cours présente différentes techniques pour manipuler les codes offusqués.

(Voir plan du cours en page 2)

MODALITÉS PRATIQUES

- **Durée/nombre d'heures :**
  3 jours / 18 heures

- **Prérequis d'accès à la formation :**
  - Connaissances de base sur les systèmes d'exploitation
  - Connaissances élémentaires en langage Python (boucles, listes, ensemble, chaînes de caractères) et de bash/console

- **Équipement nécessaire :**
  Ordinateur portable disposant des éléments suivants :
  - Système d'exploitation à jour (Windows XP, 7 ou 8)
  - RAM : 4 Go minimum
  - WiFi
  - VMWare

- **Lieu de formation :**
  Mines Nancy

- **Tarifs :**
  16 500€ net par personne, déjeuner compris

CONTACT

- **Responsable pédagogique**
  Guillaume BONFANTE
  guillaume.bonfante@univ-lorraine.fr

- **Contact administratif**

  Mines Nancy
  Service de la DFSC
  mines-nancy-dfsc@univ-lorraine.fr
  Tél : +33 3 55 66 26 82

MINESnancy
ARTEM

Utilisation de l'outil d'analyse logicielle IDA Pro

PLAN DU COURS

Module 1 : présentation générale d'IDA Pro

Désassemblage d'IDA Pro, limites et problèmes, Rappels sur le chargement par l'OS d'un exécutable, Code, données, les différentes vues d'un programme, Description des informations de structure de code, segments, fonctions, graphe de flot de contrôle

Module 2 : Présentation des structures de données

Reconnaissance de fonctions système et des fonctions de librairie standard, Exploration de codes binaires offusqués, Utilisation de FLIRT pour tenir compte d'informations spécifiques d'un système, Identification manuelle de boucles de chiffrement simples

Module 3 : bonnes pratiques

Recherche de fonctions spécifiques, Points d'arrêts, emploi de conditions, Suivi de données, Patch de programmes et de données, Suivi de threads

Module 4 : utilisation avancée d'IDA

Présentation de scripts Python pour l'analyse de code :

- Les grandes fonctionnalités du binding Python
- Enumération des instructions, des fonctions, des segments, etc.

Module 5/6 : Identification et analyse des techniques d'offuscation de code

Ecriture de scripts Python pour : Recherche de boucles de chiffrement par opérations arithmétiques, Recherche d'appels de fonctions cachées, e.g. par jump directs, Identification de boucles de chiffrement typiques (RC4, AES), Déchiffrement statique, Identification d'obfuscations typique : call/ret, push/ret, flattening, Reconstruction de code désobfusqué (par simplifcation syntaxique), Teinte de données, Identification des appels de fonction, des arguments.