

## FORMATION

○ **TITRE : Utilisation de l'outil d'analyse  
logicielle IDA Pro**

○ **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 programme 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, campus Artem

○ **TARIFS**

1 650€ net par personne,  
déjeuner compris

## CONTACT

○ **RESPONSABLE PÉDAGOGIQUE**

Guillaume BONFANTE

✉ guillaume.bonfante  
@mines-nancy.univ-lorraine.fr  
Tél : +33 3 72 74 49 58

○ **CONTACT ADMINISTRATIF**

Mines Nancy

Service de la DFSC

✉ mines-nancy-dfsc@univ-lorraine.fr  
Tél : +33 3 72 74 48 67

## 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 simplification syntaxique), Teinte de données, Identification des appels de fonction, des arguments.