

Objectifs

- ▶ Introduction aux outils incontournables du reverse engineering
- ▶ Compréhension des techniques et méthodologies d'analyse de code
- ▶ Apprentissage par la pratique sur exercices et cas réels

Des travaux pratiques seront effectués tout au long de la formation sur des systèmes Windows et Unix.

Pré-requis

- ▶ Connaissance approfondie du fonctionnement des systèmes d'exploitation
- ▶ Bonne connaissance du langage C
- ▶ Bonne connaissance du langage assembleur x86

Contenu

- ▶ Introduction au reverse engineering et analyse statique
Notions fondamentales pour l'analyse code
Présentation de l'outil IDA PRO
- ▶ Analyse dynamique : debugging userland et présentation des outils
- ▶ Analyse des malwares

Programme détaillé au dos.

Informations pratiques

- ▶ Participants : un maximum de 10 inscrits
- ▶ Formateur : expert sécurité/R&D
- ▶ Matériel : poste individuel, mêmes systèmes et outils que le formateur
- ▶ Locaux : 75 avenue Victor Hugo 92 500 Rueil-Malmaison
5 minutes à pieds du RER Rueil-Malmaison (sortie 5 Victor Hugo)
(Parking disponible sur simple demande)

Durée : 3 jours

Code : REW

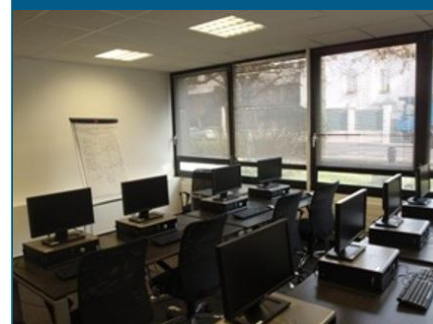
Prix : 2 400 € HT

Catalogue :

www.atlab.fr/formations.html

Inscription :

contact@atlab.fr
Tél : 01 47 08 88 00



Jour 1 : Introduction au reverse engineering et analyse statique

Notions fondamentales pour l'analyse de code	L'assembleur x86 (rappel, conventions d'appels en assembleur : stdcall, cdecl, fastcall, thiscall) Variables locales et arguments Langage haut niveau (boucles, switch, structures) Compilateur
Outil IDA PRO	Présentation (architecture, FLIRT, SDK) Configuration Code graphing Remote debugging IDC Scripting

Démonstration IDA PRO

Jour 2 : Analyse dynamique : Debugging userland et présentation des outils

OllyDbg	Présentation Configuration Plugins
<i>Démonstration Ollydbg</i>	
Immunity Debugger	Présentation Configuration Scripting
<i>Travaux pratiques : Immunity Debugger</i>	
Syser et WinDbg	Présentation Configuration
<i>Travaux pratiques : Syser et Windbg</i>	
Méthodologies	Utilisation d'un désassembleur et d'un debugger pour la création d'un exploit Localisation de la vulnérabilité avec IDA Récupération d'informations nécessaires à l'exploitation avec Ollydbg Exploitation d'un binaire vulnérable

Jour 3 : Analyse des malwares

Démonstration d'analyses de virus polymorphiques

Présentation des techniques d'analyse	Chiffrement du code Technique anti-debugging et obfuscation de code Automatisation du décryptage à l'aide d'ollyscript Analyse de virus (présentation du moteur polymorphique et de l'infection) Unpacking
---------------------------------------	--

Travaux Pratiques : exercices sur cas réels