

Objectifs

- ▶ Connaître les backdoors installées par les attaquants
- ▶ Connaître le couplage backdoors/rootkit installé par les attaquants

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

Pré-requis

- ▶ Connaissance approfondie du fonctionnement du système d'exploitation Windows
- ▶ Connaissance approfondie du fonctionnement du système d'exploitation Unix
- ▶ Bonne connaissance du langage C

Contenu

- ▶ Revue générale
- ▶ Backdoors modernes et rootkits dans le système de fichiers
- ▶ Rootkits dans l'espace mémoire utilisateur et au niveau matériel
- ▶ Détection des rootkits et techniques anti-rootkits

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 : 4 jours

Code : RBWU

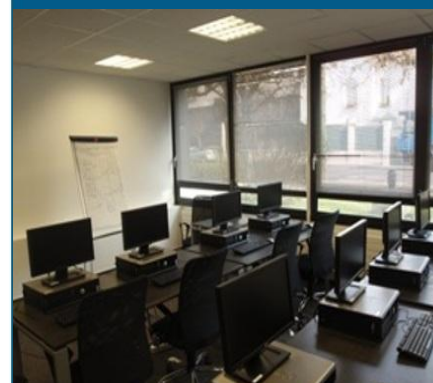
Prix : 3 200 € HT

Catalogue :

www.atlab.fr/formations.html

Inscription :

contact@atlab.fr
Tél : 01 47 08 88 00



Jour 1 : Revue générale

Préambule : synopsis d'une intrusion

Objectifs et motivations d'une intrusion
Techniques et outils d'intrusion
Définitions de termes techniques : rootkit, backdoor, trojan, ...
Que font les pirates après s'être introduit sur une machine ?

Notions fondamentales

Concept de système d'exploitation
Architecture x86
Présentation des systèmes d'exploitation Windows

Rootkits & Backdoors : anciennes techniques

Les anciennes backdoors
Les anciens rootkits

Jour 2 : Backdoors modernes et rootkits dans le système de fichiers

Caractéristiques des backdoors modernes

Architecture générale d'une backdoor
Communication avec le programme de contrôle
Les backdoors au niveau du système
Fonctionnalités offertes : concept de modularité
Conclusion : que faut-il cacher ?

Rootkits dans le système de fichiers

Structure du système de fichiers NTFS
Cacher des fichiers dans NTFS

Travaux pratiques : utilisation des ADS pour cacher un exécutable

Jour 3 : Rootkits dans l'espace mémoire utilisateur et au niveau matériel

Rootkits dans l'espace mémoire utilisateur : l'API Hooking

Concept d'API Hooking : présentation des différentes techniques
Application aux rootkits : altération du comportement

Travaux pratiques : programmation d'un outil masquant certains fichiers dans un autre processus

Avantages et inconvénients de cette famille de techniques

Travaux pratiques : tests de rootkits disponibles sur Internet en utilisant ces techniques

Rootkits au niveau matériel

Altération du processus de démarrage
Rootkits et virtualisation matérielle
Contournement des dumpers de RAM physiques par programmation des registres MMIO

Jour 4 : Détection des rootkits et techniques anti-rootkits

Détection des rootkits

Principales techniques de détection
Présentation d'outils de détection

Techniques anti-rootkits

Détection des rootkits
Rootkits et Vista

Travaux pratiques : utilisation d'outils de détection sur des rootkits réels