

Objectifs

- ▶ Connaissance des différentes techniques d'intrusion utilisées par les attaquants
- ▶ Compréhension des techniques et méthodologies d'analyse de logs
- ▶ L'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 du fonctionnement des systèmes d'exploitation
- ▶ Connaissance des protocoles courants basés sur TCP/IP

Contenu

- ▶ Attaques informatiques et logs
- ▶ Les outils d'analyse et de récupération
- ▶ La législation autour des logs

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 : 2 jours

Code : FOR

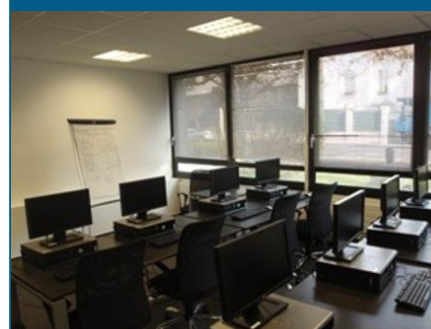
Prix : 1 400 € HT

Catalogue :

www.atlab.fr/formations.html

Inscription :

contact@atlab.fr
Tél : 01 47 08 88 00



Jour 1 : Attaques informatiques et logs

Les attaques informatiques

Comment procèdent les attaquants pour s'introduire sur un système d'information ?
Quelles sont les différentes attaques informatiques existantes ?
Comment les attaques peuvent ne pas être détectées ?
Comment les attaquants effacent leurs traces ?

Travaux pratiques : analyses des différentes techniques utilisées par les attaquants

Les logs

Quels sont les différents formats de logs ?
Quels fichiers de logs à analyser et dans quelles circonstances ?
Comment reconnaître une attaque dans un fichier de logs ?
Quels sont les outils existants pour analyser les logs ?
Comment récupérer des logs effacés sur Windows et Linux ?

Travaux pratiques : analyse de logs suite à une attaque informatique

Jour 2 : Attaques tout en mémoire et la législation

Les attaques « tout en mémoire »

La puissance des attaques tout en mémoire
Le runtime patching, théorie et pratique
L'analyse de la mémoire sous Windows et les outils existants

Travaux pratiques : simulation d'une attaque tout en mémoire et analyse

Les investigations informatiques et la législation

Quelles sont les obligations légales et jurisprudentielles ?
Combien de temps les logs doivent-ils être conservés ?
Quelles informations détenus par les logs peuvent-elles être conservées ?
Quelle valeur ont les logs d'un point de vue juridique ?