

Objectifs

- ▶ Apprentissage des données essentielles sur les techniques d'intrusion des systèmes et des réseaux
- ▶ Simulation d'une attaque informatique venant d'Internet
- ▶ Pratique de tests d'intrusion (seuls les cas de figures réels et fréquents seront étudiés)

Des travaux pratiques seront effectués tout au long de la formation. Ils serviront à démontrer les différentes étapes d'une attaque informatique sur des systèmes Windows et Unix.

Pré-requis

- ▶ Notion d'administration système en environnement Unix et Windows
- ▶ Notion d'administration réseau
- ▶ Connaissance des protocoles courants basés sur TCP/IP

Contenu

- ▶ Revue générale des bases
- ▶ Recueil d'informations
- ▶ Recherche et exploitation de vulnérabilités

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 : PTI

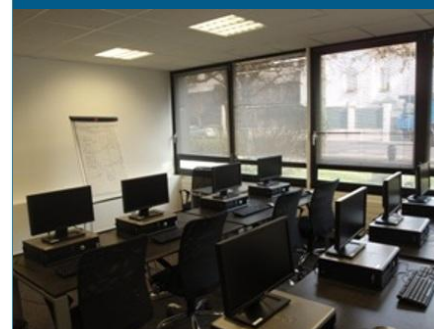
Prix : 2 400 € HT

Catalogue :

www.atlab.fr/formations.html

Inscription :

contact@atlab.fr
Tél : 01 47 08 88 00



Jour 1 : Revue générale des bases

Introduction	Risques et menaces présents sur Internet et les réseaux internes Atteinte à la vie privée Inadvertance et malveillance de la part des utilisateurs
Les systèmes d'information, architecture et fonctionnement	De quels composants systèmes et réseaux sont formés les SI ? Les acteurs rencontrés Les différentes sources d'informations sur Internet Le protocole réseau TCP/IP La terminologie utilisée
<i>Travaux pratiques : utilisation d'outils Unix (netcat, tcpdump, ...) et de manipulation de paquets TCP/IP (Scapy)</i>	
Les différentes étapes d'une attaque informatique	Définition et aspects juridiques Les différentes étapes d'une attaque informatique

Jour 2 : Recueil d'informations

Informations fournies consciemment	Les sites Web Les bases whois Les enregistrements DNS
<i>Travaux pratiques : utilisation de commandes Unix telles que wget, nslookup, dig, host, jwhois ...</i>	
Informations fournies inconsciemment	Les moteurs de recherche Les archives électroniques Le social engineering
<i>Travaux pratiques : apprendre à se servir de Google et Google API dans le cadre d'un test d'intrusion</i>	
Informations systèmes	Utilisation normale des services : domaines et partages Windows, les services Unix (HTTP, FTP, NFS ...) Daemon fingerprinting : identification des logiciels et de leurs versions associés aux services
Informations réseaux	Repérage des cibles potentielles (analyse de l'architecture réseau) Utilisation normales des protocoles (ping, connexion sur un port TCP ou UDP ...) Utilisation détournée des protocoles (fragmentation IP, paquets IP invalides ...) Analyse de l'architecture réseau Portscanning
<i>Travaux pratiques : utilisation d'outils tels que scapy, snmpwalk, nmap et netcat pour illustrer le cours</i>	

Jour 3 : Recherche et exploitation de vulnérabilités

Définitions et terminologie	Vulnérabilité, exploit ...
Recherche de vulnérabilités connues	Utilisation de scanners automatisés : références, avantages, inconvénients Exploitation des failles
Recherche de vulnérabilités inconnues	Classes de vulnérabilités Méthodologies avec un logiciel libre et commercial : Audit code source, reverse engineering
Exploitation des vulnérabilités des systèmes	Utilisation d'exploits Comptes par défaut des constructeurs Attaque par force brute ou par dictionnaire
Exploitations des vulnérabilités des réseaux	Fragmentation IP Spoofing ou l'art de se faire passer pour quelqu'un d'autre
<i>Travaux pratiques : plusieurs programmes vulnérables seront mis en place et leurs exploitations seront démontrées</i>	