

# Les fondamentaux du HACKING

## (Travaux Pratiques)

➤ Du 9 au 11 Janvier 2012

➤ Du 6 au 8 Février 2012

➤ Du 12 au 14 Mars 2012

## Objectifs

Cette formation, destinée aux décideurs, professionnels du SI et utilisateurs avertis, vise à faire connaître les techniques de piratage informatique et à évaluer leur portée et leurs impacts.

A la fin de cette formation, les participants pourront identifier les risques encourus par leur système d'information et établir les priorités des actions palliatives.

## Pré-requis

Les participants à cette formation doivent avoir des connaissances de base sur :

- Les réseaux et les applications (TCP/IP)
- La sécurité informatique
- Les systèmes Windows et Unix
- Internet

## Prix

Prix : 1975 € HT

## Programme détaillé

La formation présente une démarche complète et aboutie de l'intrusion réseau, système et applications, de la découverte des informations jusqu'à la réalisation réelle des intrusions.

Jour 1	Jour 2	Jour 3
<p><b>Module 1 : présentation générale</b></p> <ul style="list-style-type: none"> <li>◆ Revoir les bases fondamentales de la sécurité informatique (DICA+)</li> <li>◆ Présenter les démarches suivies par un hacker : (énumération, recherche de failles, pénétration, escalation, etc.)</li> </ul> <p><b>Module 2 : attaquer les réseaux</b></p> <ul style="list-style-type: none"> <li>◆ Capture de trafic</li> <li>◆ Vulnérabilités / contournement des équipements de sécurité</li> <li>◆ Déni de Service</li> <li>◆ Spoofing, attaques Men in the Middle</li> <li>◆ Attaques des réseaux Wifi (rogue AP, DNS tunneling, crack de clés WEP/WAP, etc.)</li> </ul>	<p><b>Module 3 : attaquer les systèmes d'exploitation</b></p> <ul style="list-style-type: none"> <li>◆ Les Malwares (Rootkit, Trojan, Backdoor, Keylogger, Spyware, etc.)</li> <li>◆ Crack des mots de passe systèmes</li> <li>◆ Attaques de brute force</li> <li>◆ Débordement de tampon (buffer overflow)</li> <li>◆ Recherche et exploitation de vulnérabilités système (RPC DCOM, etc.)</li> <li>◆ Exécution de commandes à distance</li> <li>◆ Escalation de privilèges</li> <li>◆ Les attaques des services (NETBIOS, FTP, partage de fichiers, spooler d'impression, etc.)</li> </ul>	<p><b>Module 4 : attaquer les applications web</b></p> <ul style="list-style-type: none"> <li>◆ SQL Injection</li> <li>◆ Cross Site Scripting</li> <li>◆ File Upload, File Include</li> <li>◆ Vol des sessions</li> <li>◆ Buffer Overflow</li> <li>◆ Attaques des web services</li> </ul> <p><b>Module 5 : solutions de protection</b></p> <p>Panorama des solutions de sécurité et de protection du SI : filtrage, contrôle de contenu, authentification, détection d'intrusions, gestion de vulnérabilités, authentification forte, gestion des traces, etc.)</p>

## Boite à outils

BackTrack, Metasploit, OpenVas, Nmap, Netcat, Metasploit, Nessus, Ettercap, Wireshark, Hping, Yersinia, Kismet, Aircrack, Aircrack-ng, KARMA, PAROS, Webscarab, nikto, SqlNinja, SQLInjector, Cain & Abel, John the Ripper, Ophcrack, Hydra, UCSNIFF, OAT, VideoJak, VAST, etc.

## Logistique

Le cours est essentiellement fondé sur des travaux pratiques.

Les supports fournis :

- ◆ CD-ROM incluant les outils utilisés
- ◆ Le support du cours (papier)