

Les fondamentaux du HACKING

(Travaux Pratiques)

➤ Du 30 Mai au 1er Juin 2011

➤ Du 22 au 24 Juin 2011

➤ Du 22 au 24 Août 2011

Objectifs:

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

Boîte 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)