

Les fondamentaux du HACKING

(Travaux Pratiques)

Objectifs:

Cette formation, destinée aux décideurs, professionnels et utilisateurs avertis, vise à faire connaître les techniques de piratage informatique et 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
- Internet

Durée

0,5 à 2 jours

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 :

- Revue des bases fondamentales de la sécurité informatique: intégrité, disponibilité, confidentialité,
- Présentation des démarches suivies par un hacker :
 - collecte d'information
 - recherche de vulnérabilités
 - pénétration
 - élévation de privilèges
 - effacement de traces
- Présentation de quelques démarches de tests d'intrusions
 - OWASP
 - ISSAF
 - OSSTMM
- Travaux Pratiques
 - scénario 0: le Google hacking
 - scénario 1: collecte d'informations dans un LAN
 - scénario 2: attaque et contrôle d'un serveur vulnérable
 - scénario 3: vol de mots de passe systèmes
 - scénario 4: attaques avec/ciblant les disques amovibles
 - scénario 5: attaque et contrôle d'un routeur vulnérable
 - scénario 6: vol d'identité (spoofing – Man in the Middle)
 - scénario 7: attaque d'un serveur web vulnérable
 - scénario 8: attaque d'une application web vulnérable

Quelques outils utilisés

- ◆ Wireshark
- ◆ Etherape
- ◆ Nessus
- ◆ Nmap
- ◆ Netbus Pro
- ◆ Cain & Abel
- ◆ Dsniff
- ◆ OPHCRACK
- ◆ Pwdump
- ◆ John the Ripper
- ◆ Hydra
- ◆ Nikto
- ◆ IIS Exploit
- ◆ C99, rc57 shells
- ◆ Metasploit
- ◆ Backtrack