# Techniques de hacking et tests d'intrusions


Comment les hackers exploitent les failles de nos systèmes ? Quels sont les risques encourus ? Comment s'en prémunir ? Autant de questions auxquelles les responsables du système d'information sont confrontés

## Objectifs

- Comprendre les risques, évaluer leur portée
- Connaître les techniques de hacking, repérer les failles
- Identifier les mesures à adopter, engager des actions préventives et correctives
- Définir les priorités d'investissement en terme de sécurité
- Savoir parer les attaques les plus courantes

## Public concerné

- Responsable réseau
- Responsables sécurité des systèmes d'information (RSSI)
- Toute personne en charge de la sécurité

## Pré requis

- Avoir suivi les formations "Soyez autonome avec TCP/IP" (SR230), "Mettre en oeuvre la sécurité réseaux" (SR211) ou "Concevoir et mettre en oeuvre la sécurité du système d'information" (SR220) ou connaissances équivalentes

## Une formation de 3 jours

| Caractéristiques |
|---|
| **Tarif : 1875 € HT par personne** |
| **Numéro de formateur : 11753687675** |
| **Nombre d'heures : 21** |
| **Référence : SR225** |
| **Contact : Patrick LE GOFF** |
| **Telephone : 01.76.60.66.10** |
| **Email : contact@kaptive.com** |

| Paris |
|---|
| **28/02/2011** |
| **06/06/2011** |
| **19/09/2011** |
| **02/11/2011** |

## Description des modules

| num | Module |
|---|---|
| 1 | **Environnement** |
| **Détails** | - Présentation<br>- Évolution des SI<br>- Aggravation des risques<br>- Les types de menaces<br>- Les risques actuels |
| 2 | **Les forces en présence** |
| **Détails** | - Les éléments à prendre en compte<br>- Les acteurs : hacker, cracker, RSSI...<br>- Les normes et préconisations<br>- Le contrôle et la circulation de l'information |
| 3 | **Le piratage** |
| **Détails** | - Chapellerie des pirates : white, black et gray hat hackers<br>- Rappels sur TCP/IP<br>- Aspects juridiques<br>- Sources d'informations<br>- Nomenclature d'une attaque : approche, analyse, attaque... |
| 4 | **Les attaques** |
| **Détails** | - Les différents types d'attaques<br>- Le traçage réseau : traceroute, DNS...<br>- La collecte d'information : Portscanning, Daemon Fingerprint, Social Engineering...<br>- Les attaques réseau : sniffing, spoofing, Man in the middle, Sessions Hijacking, DoS, DDoS...<br>- Les attaques système : Buffer Overflow, vulnérabilités, DoS...<br>- Les attaques applicatives : configuration, Buffer Overflow, Source Disclosure, Spamming, Injection SQL...<br>- Confidentialité des informations échangées<br>- Considérations sur la messagerie<br>- Attaques XSS : considérations sur les technologies Web (ASP, PHP, Java, .NET...)<br>- Les attaques cryptographiques |
| 5 | **Protection** |
| **Détails** | - Définir et mettre en place une politique de sécurité<br>- Mettre en place une veille technologique<br>- Les produits de protection disponibles<br>- Les audits<br>- Conclusion |