

# La sécurité informatique : système et réseaux

La formation « Sécurité informatique : système et réseaux » vous permettra d'apprendre à veiller à la sécurité informatique au sein de votre entreprise. Le programme est donné à titre indicatif et sera adapté à vos besoins et votre niveau après audit. N'hésitez pas à nous contacter pour toute demande spécifique.

## Pré-requis

Connaitre les protocoles réseaux.

## Public concerné

Les informaticiens souhaitant acquérir des notions avancées sur la sécurité informatique au sein de leur entreprise.

## Durée de la formation

La durée de la formation varie en fonction du niveau de base de l'apprenant et des objectifs d'utilisation formulés.

## Contenu de la formation

---

### TCP/IP

- Les protocoles TCP/IP
- Les forces et les faiblesses du protocole TCP/IP

### Etat des lieux

- Quels sont les enjeux de la sécurité ?
- Quels sont les risques ?
- Identifier les critères de sécurité
- Quelles sont les normes liées à la sécurité ?

### Identifier les vulnérabilités des postes utilisateurs

- Les intrusions à distance : navigation Web, clients de messagerie...
- Les chevaux de Troie...

### Identifier les vulnérabilités du réseau

- Attaques des règles de Firewalling, interception/analyse des transmissions réseaux cryptées
- Sniffing réseau

### La sécurité des échanges de données

- Quelles sont les contraintes de sécurité ? (intégrité, confidentialité...)
- Quels sont les différents principes de chiffrement ?
- Quelles sont les contraintes liées au support ? (espionnage...)

### Sécurisation de Linux

- Permissions standards et étendues
- Gestion des profils de sécurité et des
- Limitations des applications
- Utilisation de PAM
- Mise en place du pare-feu sur Linux
- Manipulation du chiffrement disque sur Linux
- Gestion des intrusions et des journaux (logs)

### Sécurisation de Windows

- Gestion des droits
- Gestion des services
- Accès problématiques pour le réseau et les périphériques

- Spoofing réseau / Bypassing de firewall
- Idle Host Scanning
- Détournement de connexions
- Attaque des protocoles sécurisés
- Dénis de service

- Configuration du pare-feu, et réflexions
- Possibilités de chiffrement
- Gestion du journal d'évènement et des audits

### **Identifier les vulnérabilités du web**

- Attaque des scripts Web dynamiques (PHP, Perf...), et des bases de données associées (MySQL, Oracle...)
- Cartographie du site
- Failles PHP (include, fopen...)
- Attaques CGI (Escape shell...)
- Injections SQL
- XSS

### **Identifier les vulnérabilités applicatives**

- Intrusion à distance d'un système Windows et Linux par l'exploitation des services de type applicatif, avec la plateforme Metasploit
- Escape shell
- Buffer overflow

### **Audit d'un système**

- Analyse externe au niveau réseau
- Inventaire des risques opérationnels
- Vérification du cloisonnement applicatif et utilisateur
- Risques liés à la maintenance du système (versions des logiciels, mauvaises configurations)
- Tentatives d'intrusion ciblées

### **Mise en pratique**