

Durée : 3 jour(s)

## Objectifs

Connaître les failles du système, savoir s'en protéger et surveiller les accès.

## Pré-requis

Administrateurs système ou réseau, responsables informatiques, autres professionnels de l'informatique  
Pratique courante de Linux en tant qu'administrateur

## Plan de cours

### 1. Linux / Unix et la sécurité

Parvenir à la sécurité de Linux / Unix  
Détection des intrusions avec audits/journaux  
Éviter des défauts de sécurité  
Identifier les vulnérabilités d'un logiciel et les erreurs de configuration  
Protection avec la cryptographie  
PGP (Pretty Good Privacy)  
GnuPG (Gnu Privacy Guard)  
Authenticité et intégrité grâce aux signatures numériques et aux «hash codes»

### 2. Renforcer l'authentification

Connexion au réseau  
Risque des protocoles d'applications  
Authentification plus forte lors de la connexion grâce à la cryptographie et aux jetons  
Mise en tunnel de protocoles d'application avec SSH

### 3. Limiter les privilèges utilisateur

Contrôle de l'accès aux racines  
Configuration de terminaux sûrs  
Empêcher l'accès aux réseaux non sécurisés  
Acquérir des privilèges root avec su  
Utilisation de groupes au lieu de l'identité root  
Contrôle de l'accès basé sur le rôle (RBAC)  
Risques de l'accès «tout ou rien» de Linux / Unix  
RBAC avec Solaris  
Ajout de RBAC avec sudo

### 4. Sécuriser les systèmes de fichiers locaux et en réseau

Structure et partitionnement de répertoires  
Fichiers, répertoires, périphériques et liens  
Utilisation de partitions en lecture seule  
Permissions d'accès et propriété  
Fichiers immuables et en ajout seul  
Vulnérabilités de NFS  
Renforcement des systèmes Linux / Unix  
Amélioration de l'assurance de l'information avec yassp, TITAN et Bastille

Scan de réseaux avec Nessus pour déceler les vulnérabilités  
Détection de mauvais choix de configuration avec Sussen

### 5. Éviter l'exécution de programmes

Risques provenant d'exécutions non souhaitées de programmes  
Démarrage subreptice des programmes  
Exécution de programmes en tant qu'autre utilisateur  
Planification de programmes avec cron et at  
Diminution des vulnérabilités dans les scripts de démarrage  
Réagir aux attaques et aux intrusions  
Trouver des signes d'intrusion dans des données syslog  
Analyse d'un système compromise

### 6. Réduire les effets des exploits de BO(buffer overflow)

Minimiser les risques des services réseau  
TCP/IP et ses points faibles de sécurité  
Sniffer des mots de passe avec Ethereal et dsniff  
Tester l'exposition du réseau avec netstat, isof et nmap  
La sécurité des services réseau internes  
Amélioration des enregistrements  
Configuration de OpenSSH et OpenSSL  
Authentification du réseau avec Kerberos  
Système X Window : vulnérabilités/solutions  
Connexion sûre aux réseaux externes  
Contrôle et enregistrement de l'accès aux serveurs avec des tcp wrappers et xinetd  
Réduction des problèmes de «buffer overflow»  
Réduction des fuites d'information  
Sécurisation des accès de type messagerie, FTP et Web (sécurisation des ports)