

► Sécurité  
► Formation Inter-entreprises



**Sécurité Linux**

2  
jours  
[ 14 heures ]  
SELX130



plan de cours disponible à l'adresse <http://www.adhara.fr/selx130.aspx>

## OBJECTIF

*Sécuriser une machine linux dans tous ses aspects, matériel et logiciel, poste autonome et serveur. Savoir paramétrer le pare-feu des noyaux linux récents.*

## PUBLIC

Administrateurs systèmes et réseaux.

## PROGRAMME

### 1 Vue d'ensemble

- > contexte
- > Les risques

### 2 Intrusion d'utilisateur

- > Ingénierie sociale
- > Découverte des services (scan de ports)
- > Utilisation de services non protégés ou peu protégés
- > Usurpation d'identité d'utilisateur
- > Usurpation d'adresse IP (IP spoofing)

### 3 Intrusion de programme

- > Pgm destructeur : virus
- > Pgm cassant la sécurité : cheval de Troie
- > Exploitation d'une « backdoor »

### 4 Déni de service

- > Ping Mortel
- > Finger récursif
- > Inondation de SYN

### 5 Sécuriser la mise en place

► Sécurité

► Formation Inter-entreprises



## Sécurité Linux

2  
jours  
[ 14 heures ]  
SELX130



plan de cours disponible à l'adresse <http://www.adhara.fr/selx130.aspx>

► Sécurité  
► Formation Inter-entreprises



**Sécurité Linux**

2  
jours  
[ 14 heures ]  
SELX130



plan de cours disponible à l'adresse <http://www.adhara.fr/selx130.aspx>

- > Sécurisation physique
- > Sécurisation de l'amorçage
- > Sécuriser l'installation du système

## 6 Sécuriser les comptes

- > Utiliser la PAM
- > Renforcer les mots de passe
- > Limiter su avec wheel
- > Restreindre les shells

## 7 Sécuriser les disques

- > Permissions
- > Attributs étendus
- > Contrôler les programmes en setuid et setgid
- > Cryptage GPG et effacement de sécurité

## 8 Partitionnement sécurisé

## 9 Sécuriser les services

- > N'installer que le nécessaire
- > N'activer que le nécessaire
- > TCP wrappers : Limiter les hôtes ayant accès à un service
- > Crypter les accès aux services avec SSL ou SSH
- > Auditer

## 10 Le pare-feu NETFILTER

- > Les hooks
- > Le NAT
- > Fonctionnement
- > Syntaxe : iptables

► Sécurité  
► Formation Inter-entreprises



**Sécurité Linux**

2  
jours  
[ 14 heures ]  
SELX130



plan de cours disponible à l'adresse <http://www.adhara.fr/selx130.aspx>

> Outils d'administration