

Sommaire

1. **Introduction à la sécurité sous Linux**
 - Concepts fondamentaux
 - Politique de sécurité
2. **Sécurité des comptes utilisateurs**
 - Gestion des utilisateurs et groupes
 - Authentification et mots de passe
 - PAM (Pluggable Authentication Modules)
3. **Sécurisation des connexions**
 - SSH
 - Chiffrement des communications
 - Accès distants sécurisés
4. **Sécurité du système de fichiers**
 - Permissions et ACL
 - Attributs de fichiers
 - Protection des données
5. **Sécurité réseau**
 - Services réseau
 - Contrôle des accès
 - Protection contre les attaques réseau
6. **Pare-feu Linux**
 - Netfilter et iptables
 - Configuration des règles
 - NAT et filtrage
7. **Journalisation et audit**
 - Syslog
 - Analyse des journaux
 - Outils d'audit
8. **Détection des intrusions**
 - Vérification de l'intégrité
 - Outils de surveillance
 - Détection des rootkits
9. **Sécurisation des services Internet**
 - Serveur Web
 - Serveur FTP
 - Serveur DNS
 - Serveur de messagerie
10. **Sauvegarde et restauration**
 - Stratégies de sauvegarde
 - Plan de reprise après incident
11. **Études de cas et ateliers pratiques**
 - Exercices de configuration
 - Mise en œuvre d'une politique de sécurité
 - Bonnes pratiques d'administration