

Durée : 3 jours

Réf : SECLINUX-RH (Red Hat/Rocky)
SECLINUX-DEB (Debian/Ubuntu)

Savoir sécuriser Linux

Cette formation permet de maîtriser les techniques de sécurité des systèmes Linux de la famille Red Hat ou de la famille Debian.

Elle s'appuie sur les recommandations officielles (ANSSI, CIS) et permet de suivre et corriger les non-conformités.

Objectifs

- Situer une configuration par rapport aux niveaux de durcissement ANSSI-BP-028 et CIS Benchmark
- Durcir un système Linux
- Configurer l'authentification
- Mettre en œuvre un contrôle d'accès obligatoire
- Filtrer et protéger le réseau
- Sécuriser les services courants
- Auditer le système
- Automatiser et maintenir la conformité

Public

- Administrateurs Linux, gestionnaires de parc.
- Administrateurs réseau
- Responsables sécurité informatique

Prérequis

- Connaissance de l'administration Linux (ligne de commande, systemctl, réseau)
- Notions de base d'Ansible pour le chapitre 8

Évaluation des acquis

- TP et QCM pendant la formation

Méthodes et moyens pédagogiques

- Travaux pratiques

1 Menaces et référentiels

Modèle de menaces actuel
Niveaux de durcissement ANSSI (ANSSI-BP-028 v2)
Correspondance CIS et ANSSI
NIS2

2 Durcissement système

sysctl noyau
Options de montage et partitionnement
SUID/SGID
ACL
Capabilities
Chiffrement disque
Protection du démarrage
sudo

3 Authentification**3.1 PAM**

Intérêt du système PAM
Architecture du système
Paramétrage
Les modules

3.2 SSH

Durcissement de sshd_config
Authentification par clés
Restrictions d'accès

3.3 TLS/PKI

Versions et suites de chiffrement
Gestion des certificats
Autorité interne

4 Contrôle d'accès obligatoire

Remarque : un seul type de contrôle d'accès sera abordé, suivant le système choisi pour la session

4.1 SELinux (famille Red Hat)

Architecture
Contextes et étiquetage des fichiers
Booléens
Diagnostic des refus (AVC)
Modules de politique

4.2 AppArmor (Debian)

Profils
Modes enforce/complain
Génération et affinage

5 Réseau

Politique de filtrage nftables
Zones firewall (uniquement Red Hat)
Présentation d'un VPN (au choix : WireGuard, IPsec, OpenVPN)

- Pédagogie active basée sur des exemples, des démonstrations, des partages d'expériences, des cas pratiques et une évaluation des acquis tout au long de la formation
- Un poste de travail par personne
- Support électronique

Points forts

- Groupe de 4 personnes maximum
- Alternance théorie/pratique
- Assistance après la formation

Contact

- 04 58 00 02 22
- contact@webformation.fr

Plus d'infos sur

<https://www.webformation.fr>

Optionnel : Rôle du proxy (SQUID)

6 Services**6.1 Durcissement des services**

Apache/nginx

Postfix

Optionnel : DNS

6.2 Directives systemd

bac à sable (sandboxing)

7 Audit et détection

fail2ban

rsyslog

SIEM

auditd

AIDE

Lynis

OpenSCAP

Journalisation

8 Automatisation et conformité continue

Mises à jour de sécurité

Suivi des CVE

Rôle Ansible de durcissement

Scan puis remédiation

Dérive de configuration