Sécuriser un Système Linux/Unix

DURÉE
4 jours (28h)

RÉFÉRENCE
SEC106

CATÉGORIE
Sécurité des Systèmes, Sécurité des Serveurs

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Etre capable de bâtir une sécurité forte autour de Linux
- Connaître les solutions de sécurisation du système
- Mettre en place la sécurité d'une application Linux
- Sécuriser les échanges réseaux en environnement hétérogène grâce à Linux

POUR QUI ?

- Techniciens et administrateurs systèmes et réseaux

Programme détaillé

1/ Introduction

- Les enjeux de la sécurité Linux
- Pourquoi sécuriser un système ?
- Les attaques, les techniques des hackers
- Panorama des solutions
- La politique de sécurité
- Définir une stratégie d'authentification sécurisée

2/ La cryptologie

- Les différents algorithmes de chiffrement
- Chiffrement d'un mot de passe
- Vérification d'un mot de passe
- La signature numérique, les certificats X-509, la notion de PKI

3/ La sécurité et l'Open Source

- Les corrections sont rapides, les bugs rendus publics
- La technique d'approche d'un hacker
- Exemple d'une vulnérabilité et solution de sécurisation

4/ Les utilisateurs et les droits

- Rappels sur la gestion des utilisateurs et des droits, les ACLs
- La dangerosité des droits d’endossement
- La sécurité de connexion, le paquetage SHADOW

5/ Le système SELinux ou la sécurité dans le noyau

- L’architecture du système SELinux
- Modifier les règles de comportement des exécutables

6/ La sécurité locale du système

- Exemples de malveillance et d'inadvertance
- Faible permissivité par défaut
- Vérification des droits des fichiers, scripts et commandes efficaces pour diagnostiquer
- FS en lecture seule : les attributs des fichiers, disponibilité et intérêt. Outils Tripwire
- Conservation des logs, combien de temps ?
- L'outil d'analyse des logs : logwatch
- Réagir en temps réel : exemple de script. Utiliser RPM comme HIDS
- Paramétrage de PAM dans les différents contextes
- Confinement de l'exécution des processus
- Terminologie DAC, MAC, RBAC, contexte, modèle...

7/ La sécurité au niveau réseau

- Panorama des techniques pare-feux
- Mettre en place des filtres d'accès aux services
- Configurer un firewall de manière sécurisée
- Les commandes de diagnostic
- Mise en place d'un firewall NetFilter sous Linux
- Philosophie et syntaxe de iptables
- La bibliothèque tcpd ou l’enveloppe de sécurité, la sécurisation via xinetd

8/ Les VPN

- Panorama des techniques tunnels et VPN
- Le logiciel OpenVPN
- La sécurisation des applications

9/ Les principaux protocoles cryptographiques en client/serveur

- SSH, le protocole et les commandes ssh
- SSL, l’utilisation de SSL et des certificats X-509 dans Apache et stunnel
- Kerberos et les applications kerbérorérisées

10/ Principes généraux

- Sécurisation du Web, d’email, du DNS, du FTP
- Les techniques d’audit

11/ Les utilitaires d'audit de sécurité

- Les produits propriétaires et les alternatives libres
- Crack, John the Ripper, Qcrack
- Les systèmes de détection d'intrusion HIDS et NIDS
- Tester la vulnérabilité avec Nessus
- La mise en œuvre d'un outil de sécurité

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

30 Juin au 03 Juil. 2026	Casablanca - Maroc
25 au 28 Août 2026	Casablanca - Maroc
20 au 23 Oct. 2026	Casablanca - Maroc

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Scannez pour accéder à la fiche en ligne