

GWENDAL LE COGUIC

FORMATIONS

Chaque formation est axée sur des démonstrations pratiques, des exercices interactifs et des discussions sur des situations réelles afin de garantir l'acquisition de compétences clés.

Chaque session peut être suivie :

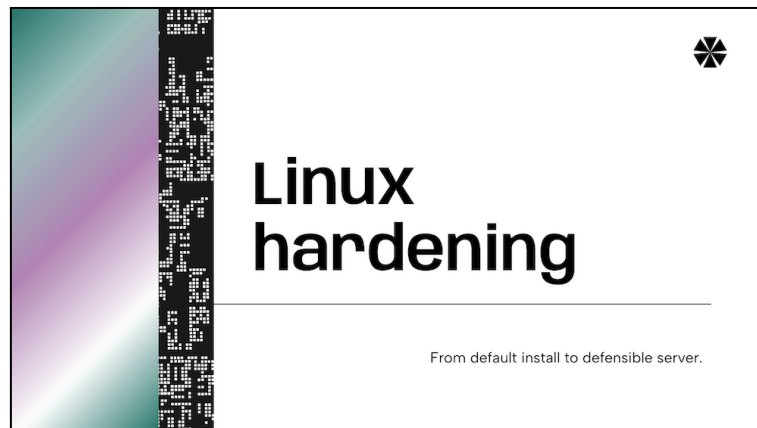
- sur site ou à distance
- en français ou en anglais
- individuellement ou en groupe

Devis sur demande

Tel: +33 7 69 02 25 10

Email: contact@glc.st

DURCISSEMENT LINUX



a. Description

Cette formation intensive d'une journée vous apprend à durcir un serveur Linux de fond en comble. Vous apprendrez à **réduire l'empreinte du système**, à **restreindre les privilèges des utilisateurs**, à **sécuriser l'exposition réseau** et à **renforcer les services critiques**. Grâce à des exercices pratiques, vous mettrez en œuvre des **techniques de durcissement concrètes** utilisées par les professionnels de la sécurité.

b. Objectifs pédagogiques

- Identifier les points d'entrée courants, les vecteurs d'élévation de privilèges et les erreurs de configuration
- Réduire le nombre de logiciels installés et mettre en œuvre des protections au niveau du noyau et du système de fichiers
- Configurer une authentification forte, des politiques sudo sécurisées et des environnements utilisateur contrôlés
- Sécuriser les interfaces réseau, les règles de pare-feu et les voies d'accès à distance
- Déployer des mécanismes de journalisation, d'audit et de détection d'intrusion de base

c. Pré-requis

- Connaissance des bases de l'administration Linux
- Être à l'aise avec le mode CLI

d. Public cible

- Administrateurs systèmes
- Ingénieurs Dev(Sec)Ops

e. Programme

Introduction

- Pourquoi le durcissement est-il important ?
- Comprendre la surface d'attaque
- Défense en profondeur
- Principe du moindre privilège
- Philosophie d'installation minimale
- Le durcissement dépend du rôle
- Cadres de référence
- Configuration de base, durcissement et conformité

Configuration de base du système

- Stratégie de partitionnement
- Paquets et services inutiles
- Modules du noyau inutilisés
- Durcissement du noyau

Durcissement des comptes

- Contrôle d'accès obligatoire (MAC)
- Durcissement des comptes et de sudo
- Politique de mots de passe et d'authentification

Durcissement du réseau

- Exposition réseau
- Filtrage réseau (pare-feu)
- Atténuation des attaques par force brute

Durcissement des services

- Utilisateurs dédiés
- Permissions de fichiers
- Isolation (sandboxing) des services

Système de fichiers, permissions et intégrité

- Audit SUID/SGID
- Sticky bit et ACLs
- Attributs immuables
- Surveillance de l'intégrité des fichiers

Journalisation, audit et surveillance

- Événements de sécurité au niveau du noyau
- Journalisation centralisée
- Concepts de détection d'intrusion

Automatisation et validation de la conformité

- Évaluation du score avec Lynis
- Évaluation formelle de conformité avec OpenSCAP
- Durcissement « as-code » avec Ansible

Ressources

- Livres
- Plateformes interactives
- Cours & vidéos
- Outils