SÉCURISATION LINUX

Protégez efficacement vos systèmes Linux contre toute attaque

Code : SL

Ce cours a pour objectif d'aborder les problèmes de la sécurisation des serveurs et postes Linux, ce qu'il est nécessaire de savoir et de mettre en place pour protéger son parc. Il comprendra une présentation de GNU Linux et de son fonctionnement, les méthodes de durcissement du noyau ainsi que les principes généraux de l'utilisation de Linux de façon sécurisée (gestion des droits, politique de mot de passe, etc.). Les protections mises en place par le système contre les dépassements de mémoire tampon seront étudiées ainsi que les principes de leur contournement. Des démonstrations des bonnes pratiques à appliquer pour utiliser sûrement les services les plus répandus, ainsi que les techniques d'isolation des services feront également partie de la formation. L'automatisation des processus d'automatisation et de déploiement de configuration sera mise en œuvre.

PROGRAMME

Méthodes mobilisées : Cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : Les objectifs sont régulièrement évalués tout au long de la formation (70% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences en fin de module par le formateur.

JOUR 1

Présentation des politiques de sécurité

Présentation du système Linux

Mise en place des premières sécurisations
- Secure Boot
- Signatures MOK / EFI
- Grub
- Attaques DMA

Journalisation avancée
- Monitoring avec auditd
- Journalisation centralisée

Gestion des droits et des accès
- Le système d'authentification PAM
  - Double Authentification
  - Authentification centralisée (Kerberos)
- SUDO
- Kernel capabilities
- SELinux / AppArmor

JOUR 2

Sécurité réseau
- Firewalls
  - IPTables
    - ACCEPT/DROP/REJECT
    - Rate Limiting
    - Connection Limiting / Tracking
    - Syn Proxy
  - NFtables
- VPN
  - OpenVPN
  - Strongswan / L2TP / IPSec

System Hardening
- Kernel Hardening
  - Sysctl
- Application Hardening
  - Protection des secrets

Détection d'intrusion
- NIDS - SURICATA
- HIDS - OSSEC

JOUR 3

Sauvegardes
- Gestion des sauvegardes
- Sauvegardes complètes
  - Write-Only Backups
- Sauvegardes bases de données
  - Delayed Syncs

Système de fichier
- Permissions
  - SUID/SGID
- ACL / Quotas
- Chiffrement
  - Dm-crypt
  - LUKS
- ZFS/BTRFS
- Effacement sécurisé
  - Software
  - Hardware

Sécurité des services
- Chroot
- Sandboxing (policycoreutils-sandbox)
- Containers (Namespace, Cgroups, Seccomp) : Docker/LXC/LXD/SystemD
- Virtualization KVM

PROCHAINES DATES

23 janvier 2023,
15 mai 2023,
28 août 2023,
18 décembre 2023

OBJECTIFS

- Définir une politique de sécurité efficace
  - Définir les besoins des clients
  - Identifier les points de sensibilité
  - Choisir une politique efficace
- Mettre en place une politique de sécurité efficace
  - Connaître les dangers de configuration Linux
  - Comprendre la sécurité mise en place
  - Déployer des configurations robustes
- Ajouter des mécanismes de protection
  - Bien configurer son firewall
  - Compléter son firewall avec d'autres mécanismes
  - Isoler l'exécution des applications

INFORMATIONS GÉNÉRALES

Code : SL
Durée : 3 jours
Prix : 2 010 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92)

PUBLIC VISÉ

- Administrateurs
- Ingénieurs / Techniciens
- Consultants

PRÉ-REQUIS

- Avoir des connaissances en administration Linux
- Avoir des connaissances en réseau
- Avoir des connaissances en système virtualisé

RESSOURCES

- Support de cours
- 1 PC par personne / Internet
- 60% d'exercices pratiques
- Environnement Linux (Fedora, Debian, Kali Linux)