LINUX ADMINISTRATION – NIVEAU 2 - Durée 35h

OBJECTIFS

- ❍ Acquérir un niveau d'expertise plus élevé sur Linux
- ❍ Apprendre à paramétrer finement le système

PUBLIC CIBLE

- ❍ Administrateur systèmes
- ❍ Techniciens

PRE-REQUIS

- ❍ Connaissance de base en informatique

PROGRAMME

Architecture Moderne, Boot et Stockage Avancé

L'objectif est de maîtriser les fondations du système, de l'amorçage jusqu'à la gestion des disques modernes.

Connaissance de base en informatique

- ❍ Rappels sur les distributions modernes et le cycle de vie (LTS, Rolling release).
- ❍ Processus de boot moderne : UEFI, Secure Boot et GRUB2.
- ❍ **Sécurité :** Sécuriser le chargeur d'amorçage (mot de passe GRUB, protection physique).

Gestion du Stockage et des Systèmes de Fichiers

- ❍ Abandon du partitionnement classique (MBR/FDISK) au profit de GPT (gdisk, parted).
- ❍ Les systèmes de fichiers modernes : Ext4, XFS.
- ❍ Introduction aux systèmes de fichiers de nouvelle génération (concepts ZFS / Btrfs).
- ❍ Gestionnaire de volumes logiques (LVM) : création, redimensionnement, snapshots.
- ❍ **Sécurité :** Chiffrement des partitions avec LUKS, options de montage sécurisées (nosuid, noexec, nodev).

Droits d'accès avancés

- ❍ Rappels droits standards et Umask.
- ❍ Les listes de contrôle d'accès (ACL).
- ❍ Les attributs étendus (chattr/lsattr) pour l'immutabilité des fichiers.

Cœur du Système, Processus et Automatisation

Passage des anciens scripts de démarrage init à systemd, et introduction aux bonnes pratiques de Scripting.

Gestion des Processus et Systemd

- Le rôle central de systemd (remplaçant d'init).
- Gestion des services, cibles (targets) et sockets.
- Analyse de l'état des processus (htop, atop, ps avancé).
- **Sécurité :** Isolation des services avec systemd (Sandboxing, limitation des privilèges, cgroups).

Planification et Logs

- Remplacement progressif de cron par les *Timers* systemd.
- Supervision des logs avec journald et rsyslog.
- **Sécurité :** Centralisation des logs, détection d'anomalies.

Automatisation et Programmation Shell Avancée

- Environnement utilisateur avancé et variables d'environnement.
- Scripting Bash robuste : gestion des erreurs, signaux, bonnes pratiques (utilisation de ShellCheck).
- *Ouverture :* Pourquoi l'administration moderne passe par l'Infrastructure as Code (concepts Ansibl/ OpenTofu).

Réseau Moderne et Filtrage

Actualisation complète de la pile réseau et mise en place de défenses périmétriques.

Pile Réseau et Configuration (TCP/IP & IPv6)

- Les bases de l'adressage (focus sur la cohabitation IPv4/IPv6).
- Utilisation de la suite iproute2 (ip a, ip r, ss au lieu de netstat).
- Configuration via NetworkManager (nmcli) et systemd-networkd.
- **Sécurité :** Analyse de trames avec Wireshark / tcpdump, protection contre le spoofing et le déni de service réseau au niveau du noyau (sysctl).

Filtrage Réseau (Pare-feu)

- De iptables à nftables : syntaxe, tables, chaînes, règles.
- Utilisation de surcouches de gestion (UFW ou Firewalld).
- **Sécurité :** Mise en place d'une politique de "Default Deny", limitation de taux (Rate Limiting) pour contrer les attaques par force brute.

Sécurité Approfondie et Durcissement (Hardening)

Une journée entière dédiée aux standards de sécurité en entreprise.

Gestion des Identités et des Accès (IAM)

- Gestion stricte de l'environnement utilisateur.
- Configuration de PAM (Pluggable Authentication Modules) : complexité des mots de passe, verrouillage de comptes.
- Sécurisation de l'élévation de privilèges avec sudoers restrictif.

Contrôle d'Accès Obligatoire (MAC)

- Les limites du modèle Discrétionnaire (DAC - droits classiques).
- Implémentation de profils de sécurité avec **AppArmor** (ou SELinux) pour confiner les applications vulnérables.

Audit et Conformité

- Application des référentiels de sécurité (Guides de l'ANSSI, CIS Benchmarks).
- Outils d'audit système (auditd).
- Recherche de vulnérabilités et détection de compromission (Lynis, rkhunter, chkrootkit).

Services Sécurisés, Conteneurisation et Synthèse

Déploiement de services courants avec les normes d'aujourd'hui, et évaluation.

Déploiement de Services Sécurisés

- **OpenSSH :** Hardening strict (authentification par clés Ed25519 uniquement, désactivation root, Fail2Ban, gestion des ports).
- **DNS/DHCP :** Rappels, implémentation sécurisée (DNSSEC, chroot).
- *Optionnel/Remplacement de Samba :* Partage de fichiers moderne et sécurisé, ou présentation d'un stockage distribué (concepts Ceph).

Le Noyau Linux (Aujourd'hui)

- Pourquoi on ne recompile presque plus son noyau en entreprise.
- Gestion dynamique des modules (lsmod, modprobe).
- **Sécurité :** Désactivation de modules inutiles/vulnérables.

Ouverture vers l'écosystème moderne

- L'isolation logicielle par la conteneurisation (introduction aux conteneurs rootless via Podman).

MOYENS TECHNIQUES ET HUMAINS :

- ❍ Intervenant : Formateur Professionnel
- ❍ Mobilisation des outils et auxiliaires utiles : paperboard, vidéoprojecteur…
- ❍ Possibilité de mettre à disposition des PC portables pour les stagiaires

METHODES PEDAGOGIQUES MOBILISEES :

- ❍ Alternance de méthodes affirmatives, interrogatives et actives
- ❍ Ressources de type formatives, évaluatives, de synthèses, de soutien, de mémorisation…
- ❍ Utilisation de Padlet

MODALITES D'EVALUATION :

- Des acquis
  - ❍ Fiche de renseignements en amont et questions
  - ❍ Evaluations formatives réalisées à l'aide de grilles critériées ;
  - ❍ Attestation de fin de formation mentionnant l'atteinte des objectifs de la formation
  - ❍ Evaluation différée
- Evaluation satisfaction

- Rédaction d'un bilan d'action remis au commanditaire en cas de formation intra-entreprise