Compte rendu des exercices 1 à 3

Ces exercices nous ont aidé à explorer un environnement et à développer les bons réflexes d'observation, de détection de vulnérabilités et d'audit. Ceci passe notamment par :

1. Identification de la version du noyau Linux : # hostnamectl
2. Identification des services de sécurité actifs de l'environnement de travail :

   # systemctl list-units --type=service | grep -E 'firewalld|iptables|auditd|selinux'

   # sestatus
3. Identification des ports actuellement ouverts : netstat -tuln ou ss -tuln ou firewall-cmd --list-all
4. La recherche de tous les fichiers contenant des secrets potentiels Mots-clés à rechercher sans tenir compte de la casse : password, api_key, token, secret_key, .env.
   # find / -type f \(-iname "*secret*" -o -iname "*password*" -o -iname "token" -o -iname "*.env" -o -iname "*.pem" -o -iname "*.key" \) 2>/dev/null > secret_result.txt

   # grep -RiE --color 'password|passwd|secret|api[_-]?key|token|PRIVATE_KEY' / 2>/dev/null

   #find / -type f \(-name "*.env" -o -name "*.conf" -o -name "*.json" -o -name "*.php" \) -exec grep -iE 'password|passwd|secret|api[_-]?key|token|PRIVATE_KEY' {} \; 2>/dev/null > secret_result3.txt
5. Analyser les logs d'authentification Cat /var/log/secure sudo grep "Failed" /var/log/secure
6. Lister les fichiers récemment modifiés dans /etc : sudo find /etc -type f -mtime -1
7. Identification des groupes à privilèges sur notre système
   Sudo getent group
   Sudo getent group | awk -F: '$3 < 1000 { print $1 ":" $3 }
   getent group wheel

   awk -F: '($3 == 0) {printf "Utilisateur: %-20s UID: %s\n", $1, $3}' /etc/passwd

   grep -E '^[^#].*ALL' /etc/sudoers 2>/dev/null

   grep -E '^[^#].*ALL' /etc/sudoers.d/* 2>/dev/null

8. Les utilisateurs qui ont accès à un shell de connexion
   awk -F: '($7 !~ /(nologin|false)/) {print $1, $3, $7}' /etc/passwd

   awk -F: '($3 < 1000 && $7 ~ /(nologin|false)/) {print $1, $3, $7}' /etc/passwd