Méthodologie d'audit de sécurité informatique

1. L'Audit de Configuration (Hardening)

Contrairement au scan de vulnérabilités qui cherche des failles logicielles, l'audit de configuration vérifie si les systèmes sont paramétrés selon l'état de l'art (référentiels **ANSSI** ou **CIS Benchmarks**).

- **Gestion des accès :** Vérification du principe du "moindre privilège". Les comptes administrateurs sont-ils nominatifs ? Le MFA (Multi-Facteur) est-il activé partout ?
- **Services inutiles :** Désactivation des protocoles obsolètes ou dangereux (Telnet, SMBv1, services d'impression inutilisés sur les serveurs).
- **Journalisation (Logging) :** Les logs sont-ils générés ? Sont-ils exportés vers un serveur centralisé (SIEM) pour éviter qu'un attaquant ne les efface ?
- **Chiffrement :** Vérification des certificats SSL/TLS (versions, force des clés) pour les flux de données.

---

2. Le Test d'Intrusion (Pentest) : Approche Offensive

C'est la phase de démonstration. L'auditeur se met dans la peau d'un attaquant pour prouver l'impact réel d'une vulnérabilité.

Les 4 étapes du Pentest :

1. **Reconnaissance (OSINT) :** Recherche d'informations publiques sur l'entreprise (fuites de mots de passe sur le Darknet, métadonnées de documents PDF, profils LinkedIn des employés).
2. **Exploitation :** Utilisation de techniques pour franchir les défenses.
    - *Web :* Injections SQL, Cross-Site Scripting (XSS).
    - *Réseau :* Empoisonnement de requêtes (LLMNR/NBT-NS), exploitation de CVE non patchées.
3. **Post-Exploitation :** Une fois le pied dans le réseau, l'auditeur tente le **mouvement latéral** (aller d'un PC vers un serveur) et l'**élévation de privilèges** (devenir "Domain Admin").
4. **Nettoyage :** Suppression de tous les outils et comptes créés durant le test pour ne pas laisser le système vulnérable.

---

3. L'Audit Organisationnel et Humain

La sécurité technique est inutile si les processus humains sont défaillants.

- **Gouvernance :** Existe-t-il une **Charte Informatique** signée par les employés ? Un plan de continuité d'activité (PCA) est-il documenté et testé ?

- **Sécurité Physique :** L'accès à la salle serveur est-il sécurisé (badge, registre) ? Les ports réseau dans les salles de réunion sont-ils actifs par défaut ?
- **Gestion des Tiers :** Comment les prestataires externes accèdent-ils au réseau ? Leurs accès sont-ils temporaires et tracés ?
- **Sensibilisation :** Test de "Vishing" (phishing par téléphone) ou dépôt de clés USB piégées dans les locaux pour tester les réflexes du personnel.

---

4. Matrice de Priorisation des Risques (Exemple)

Après l'audit, chaque faille est classée dans une matrice pour aider le décideur à allouer son budget.

Vulnérabilité	Probabilité	Impact	Niveau de Risque	Recommandation
Absence de MFA sur VPN	Élevée	Critique	**Maximum**	Déploiement immédiat (sous 48h)
Version PHP obsolète	Moyenne	Élevée	**Haut**	Mise à jour du serveur Web
Mots de passe simples	Élevée	Moyenne	**Moyen**	Durcir la politique de complexité
Pas de bannière légale	Faible	Faible	**Faible**	Ajout lors de la prochaine maintenance

---

5. Le Plan de Remédiation (Post-Audit)

L'audit n'est pas une fin en soi, c'est le point de départ de la sécurisation.

- **Correctifs à chaud :** Patch management, changement des mots de passe compromis.
- **Changements structurels :** Segmentation réseau (VLAN), mise en place d'un EDR (Endpoint Detection and Response).
- **Contrôle :** Un "Audit de vérification" doit être prévu 3 à 6 mois après pour s'assurer que les recommandations ont bien été appliquées.

Note importante : Pour un audit en entreprise, il est impératif de faire signer une **convention d'audit** (ou autorisation de test) qui protège juridiquement l'auditeur et définit précisément les plages horaires d'intervention pour ne pas perturber la production.