# Audit Technique des Bases de données

L’objectif de cette opération d’audit est d’identifier les failles de sécurité au niveau des Bases de données, mesurer le degré de criticité et proposer une solution pour éliminer et minimiser les risques. Dans ce rapport, nous allons présenter les résultats de l’opération d’audit en exposant la liste des vulnérabilités trouvées ainsi que les recommandations à mettre en place pour réduire le niveau de risque . Cette phase a été effectuée en Deux étapes :

**Première étape :** Scan des vulnérabilités via l’outil : Nessus, OpenVas

**Deuxième étape :** Audit des configurations via une check-list inspirée des benchmarks de sécurité regroupant les bonnes pratiques des configurations Microsoft, Linux et Scan des Ports et Service Réseaux.

# 1. Analyse récapitulative

## 1.1 Top 5 des systèmes d'exploitation détectés lors de l'analyse

Une image contenant texte, capture d’écran, cercle, Police

Description générée automatiquement

## 1.2 Synthèse de Scan des Vulnérabilités

Une image contenant texte, capture d’écran, cercle, Caractère coloré

Description générée automatiquement

# 2. Scan des Vulnérabilités et Configurations : Vue d’ensemble

Dans les deux cellules « Critique » et « Élevé » la 1ére valeur en gras représente le nombre des vulnérabilités dont un exploit est disponible (Metasploite, Core Impact ou CANVAS),

Exemple :

**26**/1250 : 26 vulnérabilités exploitable sur 1250 vulnérabilités de même criticité.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Synthèse de Scan** | | | | | | | | |
|  | **Nom de poste de travail** | **@IP** | **Système d’exploitation** | **Vulnérabilité** | | | | **Configuration** | |
| Critique | Élevé | Moyenne | Faible | Non Conforme | Conforme |
| **${id}** | **${DB\_Name}** | **${DB\_IP}** | **${DB\_OS}** | **{DB\_CR\_Exp}**/${DB\_CR} | **${DB\_HI\_Exp}**/${DB\_HI} | ${DB\_ME} | ${DB\_LO} | ${DB\_NC} | ${DB\_CF} |
|  | **Total** | | | **${TLT\_DB\_CR}** | **${TLT\_DB\_HI}** | **${TLT\_DB\_ME}** | **${TLT\_DB\_LO}** | **${TLT\_DB\_NC}** | **${TLT\_DB\_CF}** |

# 3. Vulnérabilités exploitables détectées

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Gravité (CVSS v3.0)** | **Vulnérabilité** | **Nbr des hôtes** | **Adresses IP** |
| **${id2}** | **${DB\_Risk\_Factor\_Critical}** | **${DB\_Synopsis\_Critical}** | **${DB\_count\_Critical}** | **${DB\_nbr\_Critical}** |
|  | **${DB\_Risk\_Factor\_High}** | **${DB\_Synopsis\_High}** | **${DB\_count\_High}** | **${DB\_nbr\_High}** |

# 4. Détails des Vulnérabilités

**Vulnérabilité ${DB\_VULN\_ID}: ${DB\_VULN\_Name}**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID DE LA VULNÉRABILITÉ** | **${DB\_VULN\_ID}** | **RISQUE** | ${DB\_VULN\_RISK} | **CVSS score** | ${DB\_VULN\_CVSS} |
| **Synopsis** | **${DB\_VULN\_Synopsis}** | | | | |
| **ÉLÉMENTS IMPACTÉS** | **${DB\_VULN\_Hosts}** | | | | |
| **DESCRIPTION** | | | | | |
| ${DB\_VULN\_Desc} | | | | | |
| **RÉFÉRENCES** | | | | | |
| **${DB\_VULN\_ref}** | | | | | |
| **RECOMMENDATIONS** | | | | | |
| **${DB\_VULN\_Recomendations}** | | | | | |