# Audit Technique des ${SRV\_TITLE}

L’objectif de cette opération d’audit est d’identifier les failles de sécurité au niveau des ${SRV\_TITLE}, 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 encouru par les ${SRV\_TITLE} et ses utilisateurs. Cette phase a été effectuée en Trois étapes :

**Première étape :** Scan des vulnérabilités des Serveurs via des outils de scan (Nessus, OpenVas, ..)

**Deuxième étape :** Audit des ${SRV\_TITLE} si applicable via une check-list inspirée des benchmarks de sécurité regroupant les bonnes pratiques des ${SRV\_TITLE}

# 1. Analyse récapitulative

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

## 1.2 Synthèse de Scan des Vulnérabilités

# 

# 2. Scan des Vulnérabilités et Configurations ${SRV\_TITLE}: 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 de ${SRV\_TITLE}** | | | | | | | | | |
|  | **Nom** | **Adresse IP** | **Système d’exploitation** | **Vulnérabilité** | | | | | **Configuration** | |
| Malware | Critique | Élevé | Moyenne | Faible | Non Conforme | Conforme |
| **${id}** | **${SRV\_Name}** | **${SRV\_IP}** | **${SRV\_OS}** | ${SRV\_MLW} | **${SRV\_CR\_Exp}**/${SRV\_CR} | **${SRV\_HI\_Exp}**/${SRV\_HI} | **${SRV\_MO\_Exp}**/${SRV\_ME} | ${SRV\_LO} | ${SRV\_NC} | ${SRV\_CF} |
|  | **Total (${TLT\_SRV})** | | | ${TLT\_SRV\_MLW} | **${TLT\_SRV\_CR\_Ex}/**${TLT\_SRV\_CR} | **${TLT\_SRV\_HI\_Ex}/**${TLT\_SRV\_HI} | **${TLT\_SRV\_MO\_Ex}/${TLT\_SRV\_ME}** | **${TLT\_SRV\_LO}** | **${TLT\_SRV\_NC}** | **${TLT\_SRV\_CF}** |

# 3. Vulnérabilités exploitables détectées

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Gravité (CVSS v3.0)** | **Vulnérabilité** | **Exploitabilité** | **Nbr des hôtes** | **Adresses IP** |
| **${id\_c\_serv}** | **${SRV\_Risk\_Factor\_Critical}** | **${SRV\_Synopsis\_Critical}** | ${SRV\_exploi} | ${SRV\_count} | **${SRV\_nbr\_Critical}** |
| ${id\_h\_serv} | **${SRV\_Risk\_Factor\_High}** | **${SRV\_Synopsis\_High}** | **${SRV\_exploi}** | **${SRV\_count}** | **${SRV\_nbr\_High}** |
| ${id\_m\_serv} | **${SRV\_Risk\_Factor\_Medium}** | **${SRV\_Synopsis\_Medium}** | **${SRV\_exploi}** | **${SRV\_count}** | **${SRV\_nbr\_Medium}** |

# 4. Détails des Vulnérabilités

**${Block\_Vun}**

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID de Plugin** | **${SRV\_VULN\_ID}** | | | | **RISQUE** | | ${**SRV**\_VULN\_RISK} | | **CVSS score** | | | | ${SRV\_VULN\_CVSS} |
| **Synopsis** | **${SRV\_VULN\_Synopsis}** | | | | | | | | | | | | |
| **ÉLÉMENTS IMPACTÉS** | **${SRV\_VULN\_Hosts}** | | | | | | | | | | | | |
| **Exploitable :** | | **${SRV\_VULN\_available}** | | | | **Par Malware :** | | | | | **${SRV\_VULN\_malware}** | | |
| **Metasploit** | | | ${SRV\_VULN\_Metasploit} | **Core Impact** | | | | ${SRV\_VULN\_Core\_Impact} | | **CANVAS** | | ${SRV\_VULN\_CANVAS} | |
| **DESCRIPTION** | | | | | | | | | | | | | |
| ${**SRV**\_VULN\_Desc} | | | | | | | | | | | | | |
| **RÉFÉRENCES** | | | | | | | | | | | | | |
| **${SRV\_VULN\_ref}** | | | | | | | | | | | | | |
| **RECOMMENDATIONS** | | | | | | | | | | | | | |
| **${SRV\_VULN\_Recomendations}** | | | | | | | | | | | | | |

**${/Block\_Vun}**