# 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}. Cette phase a été effectuée en deux 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

# 2. Scan des Vulnérabilités et Configurations ${SRV\_TITLE}: Vue d’ensemble

Ci-dessous l’état des vulnérabilités et configuration selon leur criticités :

|  |  |  |
| --- | --- | --- |
| **C**: Critique | **E**: Elevé | **M**: Moyen |
| **F**: Faible | **NC**: Non conforme | **CF**: Conforme |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | | | | |
|  | **Nom** | **Adresse IP** | **Système d’exploitation** | **Vulnérabilités exploitables** | | | | **Autres Vulnérabilités** | | | | **Configuration** | |
| **Par malware** | **C** | **E** | **M** | **C** | **E** | **M** | **F** | **NC** | **CF** |
| **${id}** | **${SRV\_Name}** | **${SRV\_IP}** | **${SRV\_OS}** | ${SRV\_MLW} | **${SRV\_CR\_Exp}** | **${SRV\_HI\_Exp}** | **${SRV\_MO\_Exp}** | ${SRV\_CR} | ${SRV\_HI} | ${SRV\_ME} | ${SRV\_LO} | ${SRV\_NC} | ${SRV\_CF} |
|  | **Total (${TLT\_SRV})** | | | ${TLT\_SRV\_MLW} | **${TLT\_SRV\_CR\_Ex}** | **${TLT\_SRV\_HI\_Ex}** | **${TLT\_SRV\_MO\_Ex}** | ${TLT\_SRV\_CR} | ${TLT\_SRV\_HI} | ${TLT\_SRV\_ME} | ${TLT\_SRV\_LO} | ${TLT\_SRV\_NC} | ${TLT\_SRV\_CF} |

# 3. Vulnérabilités détectées

# 3.1 Vue d’ensemble

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **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}** |
| ${id\_l\_serv} | **${SRV\_Risk\_Factor\_Low}** | **${SRV\_Synopsis\_Low}** | **${SRV\_exploi}** | **${SRV\_count}** | **${SRV\_nbr\_Low}** |

# 3.2 Vulnérabilités par actif

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Gravité (CVSS v3.0)** | **Vulnérabilité** | **Exploitabilité** | **Ports** | **Age de la vulnérabilité** |
| **${id\_c2\_serv}** | **${SRV\_Risk\_Factor\_Critical\_host}** | **${SRV\_Synopsis\_host}** | ${SRV\_exploi**\_host**} | ${SRV\_vuln\_port\_host} | ${SRV\_vuln\_age\_host} |
| ${id\_h2\_serv} | **${SRV\_Risk\_Factor\_High\_host}** | **${SRV\_Synopsis\_High}** | **${SRV\_exploi\_host}** | ${SRV\_vuln\_port\_host} | ${SRV\_vuln\_age\_host} |
| ${id\_m2\_serv} | **${SRV\_Risk\_Factor\_Medium\_host}** | **${SRV\_Synopsis\_Medium}** | **${SRV\_exploi\_host}** | ${SRV\_vuln\_port\_host} | ${SRV\_vuln\_age\_host} |
| $id\_l2\_serv} | **${SRV\_Risk\_Factor\_Low\_host}** | **${SRV\_Synopsis\_Low}** | **${SRV\_exploi\_host}** | ${SRV\_vuln\_port\_host} | ${SRV\_vuln\_age\_host} |

# 4. Détails des Vulnérabilités détectées

**${Block\_Vun}**

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

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID de Plugin** | **${SRV\_VULN\_pluginID}** | | | **RISQUE** | | ${**SRV**\_VULN\_RISK} | **CVSS score** | | | ${SRV\_VULN\_CVSS} | |
| **Synopsis** | **${SRV\_VULN\_Synopsis}** | | | | | | | | | | |
| **ÉLÉMENTS IMPACTÉS** | **${SRV\_VULN\_Hosts}** | | | | | | | | | | |
| **Ports associés** | **${SRV\_VULN\_Hosts\_ports}** | | | | | | | | | | |
| **Exploitable :** | | **${SRV\_VULN\_available}** | **Par Malware :** | | **${SRV\_VULN\_malware}** | | | | **Age de la vulnérabilité :** | | ${SRV\_VULN\_Age} |
| **Metasploit** | | ${SRV\_VULN\_Metasploit} | **Core Impact** | | ${SRV\_VULN\_Core\_Impact} | | | **CANVAS** | ${SRV\_VULN\_CANVAS} | | |
| **DESCRIPTION** | | | | | | | | | | | |
| ${**SRV**\_VULN\_Desc} | | | | | | | | | | | |
| **Résultats de Plugin** | | | | | | | | | | | |
| ${**SRV**\_VULN\_PluginOutput} | | | | | | | | | | | |
| **RÉFÉRENCES** | | | | | | | | | | | |
| **${SRV\_VULN\_ref}** | | | | | | | | | | | |
| **RECOMMENDATIONS** | | | | | | | | | | | |
| **${SRV\_VULN\_Recomendations}** | | | | | | | | | | | |

**${/Block\_Vun}**