Une image contenant Graphique, Police, logo, symbole

Description générée automatiquement

**Rapport Annexe Technique**

**Version 1.0**

**${LN}**

**${PRJ} pour l’année ${Y}**

${icon:200:200}

**SOMMAIRE**

[I. Synthèse du résultat d’audit de SI de ${SN} 3](#__RefHeading___Toc959_1071293927)

[II. Audit Technique des Serveurs 9](#__RefHeading___Toc961_1071293927)

[1. Analyse récapitulative 9](#__RefHeading___Toc963_1071293927)

[1.1 Top 5 des systèmes d'exploitation détectés lors de l'analyse 9](#__RefHeading___Toc965_1071293927)

[1.2 Synthèse de Scan des Vulnérabilités 9](#__RefHeading___Toc967_1071293927)

[2. Scan des Vulnérabilités et Configurations Serveurs : Vue d’ensemble 1](#__RefHeading___Toc969_1071293927)

[3. Vulnérabilités exploitables détectées 2](#__RefHeading___Toc971_1071293927)

[4. Détails des Vulnérabilités 3](#__RefHeading___Toc975_1071293927)

[III. Audit Technique des Bases de données 4](#__RefHeading___Toc977_1071293927)

[1. Analyse récapitulative 4](#__RefHeading___Toc979_1071293927)

[1.1 Top 5 des systèmes d'exploitation détectés lors de l'analyse 4](#__RefHeading___Toc981_1071293927)

[1.2 Synthèse de Scan des Vulnérabilités 5](#__RefHeading___Toc983_1071293927)

[2. Scan des Vulnérabilités et Configurations : Vue d’ensemble 1](#__RefHeading___Toc985_1071293927)

[3. Vulnérabilités exploitables détectées 2](#__RefHeading___Toc987_1071293927)

[4. Détails des Vulnérabilités 3](#__RefHeading___Toc991_1071293927)

[IV. Audit Technique des Postes de travail 4](#__RefHeading___Toc993_1071293927)

[1. Analyse récapitulative 4](#__RefHeading___Toc995_1071293927)

[1.1 Top 5 des systèmes d'exploitation détectés lors de l'analyse 4](#__RefHeading___Toc997_1071293927)

[1.2 Synthèse de Scan des Vulnérabilités 4](#__RefHeading___Toc999_1071293927)

[2. Scan des Vulnérabilités et Configurations : Vue d’ensemble 1](#__RefHeading___Toc1001_1071293927)

[3. Vulnérabilités exploitables détectées 2](#__RefHeading___Toc1003_1071293927)

[4. Détails des Vulnérabilités 3](#__RefHeading___Toc1007_1071293927)

[V. Audit Technique Externe 4](#__RefHeading___Toc1009_1071293927)

[1. Analyse récapitulative 4](#__RefHeading___Toc1011_1071293927)

[1.1 Top 5 des systèmes d'exploitation détectés lors de l'analyse 4](#__RefHeading___Toc1013_1071293927)

[1.2 Synthèse de Scan des Vulnérabilités 5](#__RefHeading___Toc1015_1071293927)

[2. Collectes d’information de DarkWeb 1](#__RefHeading___Toc1017_1071293927)

[3. Scan des Vulnérabilités et Configurations : Vue d’ensemble 1](#__RefHeading___Toc1019_1071293927)

[4. Vulnérabilités exploitables détectées 3](#__RefHeading___Toc1021_1071293927)

[5. Détails des Vulnérabilités 4](#__RefHeading___Toc1025_1071293927)

[VI. Audit Technique des applications 5](#__RefHeading___Toc1027_1071293927)

[1. Analyse récapitulative 5](#__RefHeading___Toc1029_1071293927)

[1.1 Top 5 des systèmes d'exploitation détectés lors de l'analyse 5](#__RefHeading___Toc1031_1071293927)

[1.2 Synthèse de Scan des Vulnérabilités 5](#__RefHeading___Toc1033_1071293927)

[2. Scan des Vulnérabilités et Configurations : Vue d’ensemble 1](#__RefHeading___Toc1035_1071293927)

[3. Vulnérabilités exploitables détectées 2](#__RefHeading___Toc1037_1071293927)

[4. Détails des Vulnérabilités 3](#__RefHeading___Toc1041_1071293927)

# Synthèse du résultat d’audit de SI de ${SN}

|  |
| --- |
| **Serveurs** |
| * + **Analyse des vulnérabilités** |
| Une image contenant diagramme, texte, capture d’écran, cercle  Description générée automatiquement |
| * + **Analyse de configuration** |
| Une image contenant capture d’écran, diagramme, texte, cercle  Description générée automatiquement |
| **Postes de travail** |
| * + **Analyse des vulnérabilités** |
| Une image contenant diagramme, capture d’écran, texte, cercle  Description générée automatiquement |
| **Équipements infrastructure réseau** |
| * + **Analyse des vulnérabilités** |
| Une image contenant diagramme, capture d’écran, texte, Tracé  Description générée automatiquement |
| **Applications** |
| * **Analyse des vulnérabilités** |
| Une image contenant diagramme, capture d’écran, Caractère coloré, cercle  Description générée automatiquement |
|  |
|  |

# Audit Technique des Serveurs

L’objectif de cette opération d’audit est d’identifier les failles de sécurité au niveau des serveurs, 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 serveurs et ses utilisateurs. Cette phase a été effectuée en Trois étapes :

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

**Deuxième étape :** Audit des serveurs via une check-list inspirée des benchmarks de sécurité regroupant les bonnes pratiques des serveurs 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 Serveurs : 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 du Serveur** | **@IP** | **Système d’exploitation** | **Vulnérabilité** | | | | **Configuration** | |
| Critique | Élevé | Moyenne | Faible | Non Conforme | Conforme |
| **${id}** | **${SRV\_Name}** | **${SRV\_IP}** | **${SRV\_OS}** | **${SRV\_CR\_Exp}**/${SRV\_CR} | **${SRV\_HI\_Exp}**/${SRV\_HI} | **${SRV\_MO\_Exp}**/${SRV\_ME} | ${SRV\_LO} | ${SRV\_NC} | ${SRV\_CF} |
|  | **Total** | | | **${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** | **Nbr des hôtes** | **Adresses IP** |
| **${id\_c\_serv}** | **${SRV\_Risk\_Factor\_Critical}** | **${SRV\_Synopsis\_Critical}** | **${SRV\_count\_Critical}** | **${SRV\_nbr\_Critical}** |
| ${id\_h\_serv} | **${SRV\_Risk\_Factor\_High}** | **${SRV\_Synopsis\_High}** | **${SRV\_count\_High}** | **${SRV\_nbr\_High}** |
| ${id\_m\_serv} | **${SRV\_Risk\_Factor\_Medium}** | **${SRV\_Synopsis\_Medium}** | **${SRV\_count\_Medium}** | **${SRV\_nbr\_Medium}** |

# 4. Détails des Vulnérabilités

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

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID DE LA VULNÉRABILITÉ** | **${SRV\_VULN\_ID}** | | | **RISQUE** | ${**SRV**\_VULN\_RISK} | | **CVSS score** | | | ${SRV\_VULN\_CVSS} |
| **Synopsis** | **${SRV\_VULN\_Synopsis}** | | | | | | | | | |
| **ÉLÉMENTS IMPACTÉS** | **${SRV\_VULN\_Hosts}** | | | | | | | | | |
| **Exploitable par :** | | | | | | | | | | |
| **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}** | | | | | | | | | | |