

**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** |
|  |
| * + **Analyse de configuration** |
|  |
| **Postes de travail** |
| * + **Analyse des vulnérabilités** |
|  |
| **Équipements infrastructure réseau** |
| * + **Analyse des vulnérabilités** |
|  |
| **Applications** |
| * **Analyse des vulnérabilités** |
|  |
|  |
|  |

# Audit Technique des Serveurs

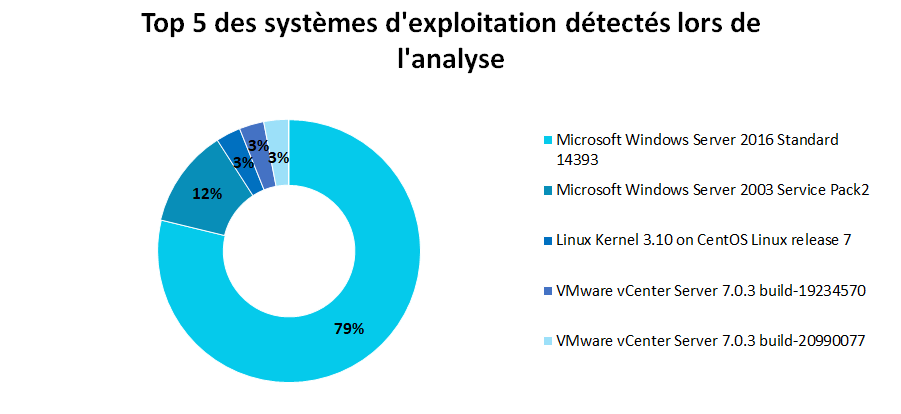
L’objectif de cette opération d’audit est d’identifier les failles de sécurité au niveau des serveurs, mesurer le degré de criticité et proposer une solution pour éliminer et minimiser les risques. Dans ce rapport, nous allons présenter les résultats de l’opération d’audit en exposant la liste des vulnérabilités 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

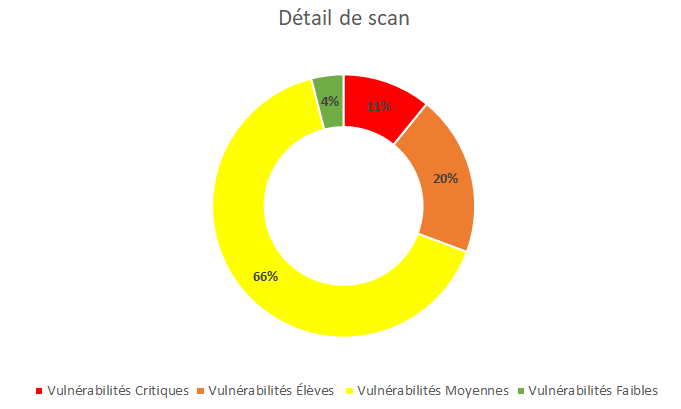
**Deuxième étape :** Audit des serveurs via une check-list inspirée des benchmarks de sécurité regroupant les bonnes pratiques des serveurs Microsoft, Linux et Scan des Ports et Service Réseaux.

# 1. Analyse récapitulative

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



## 1.2 Synthèse de Scan des Vulnérabilités



# 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}** | | | | | | | | | | |

**${Block\_Vun}**

**Customer: ${customer\_name}**

**Address: ${customer\_address}**

**${/Block\_Vun}**

# Audit Technique des Bases de données

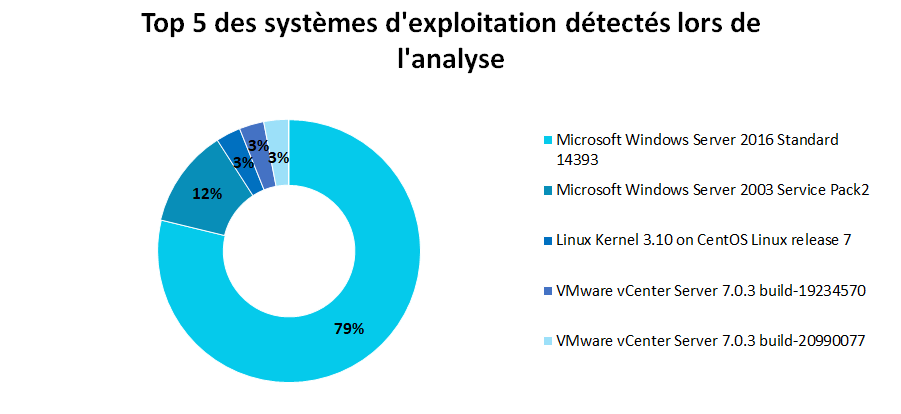
L’objectif de cette opération d’audit est d’identifier les failles de sécurité au niveau des Bases de données, mesurer le degré de criticité et proposer une solution pour éliminer et minimiser les risques. Dans ce rapport, nous allons présenter les résultats de l’opération d’audit en exposant la liste 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

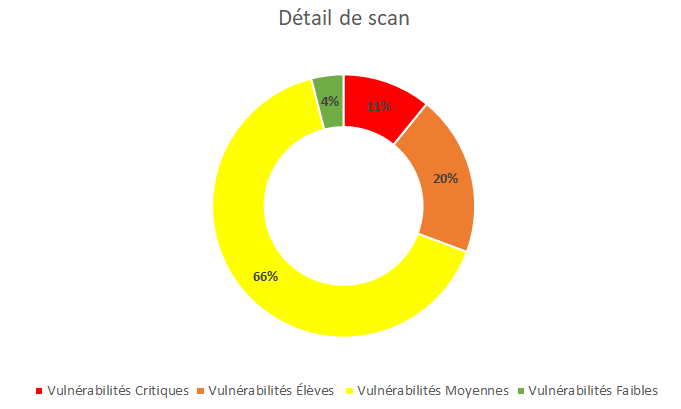
**Deuxième étape :** Audit des configurations via une check-list inspirée des benchmarks de sécurité regroupant les bonnes pratiques des configurations Microsoft, Linux et Scan des Ports et Service Réseaux.

# 1. Analyse récapitulative

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



## 1.2 Synthèse de Scan des Vulnérabilités



# 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}** | | | | | |

# Audit Technique des Postes de travail

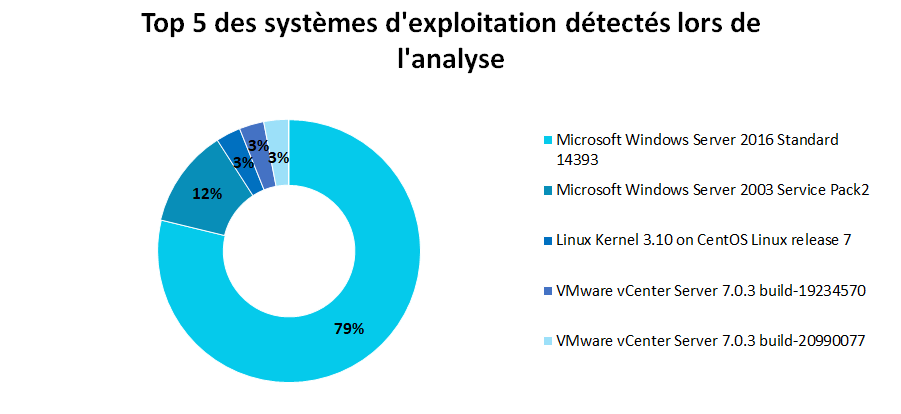
L’objectif de cette opération d’audit est d’identifier les failles de sécurité au niveau des postes de travail, mesurer le degré de criticité et proposer une solution pour éliminer et minimiser les risques. Dans ce rapport, nous allons présenter les résultats de l’opération d’audit en exposant la liste 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

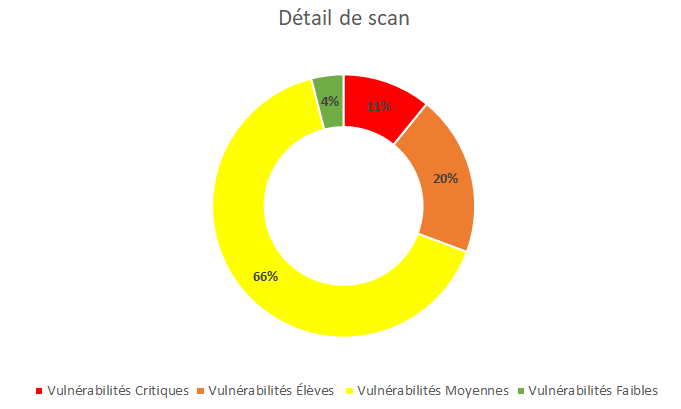
**Deuxième étape :** Audit des configurations via une check-list inspirée des benchmarks de sécurité regroupant les bonnes pratiques des configurations Microsoft, Linux et Scan des Ports et Service Réseaux.

# 1. Analyse récapitulative

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



## 1.2 Synthèse de Scan des Vulnérabilités



# 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 |
| **${id}** | **${PC\_Name}** | **${PC\_IP}** | **${PC\_OS}** | **{PC\_CR\_Exp}**/${PC\_CR} | **${PC\_HI\_Exp}**/${PC\_HI} | ${PC\_ME} | ${PC\_LO} | ${PC\_NC} | ${PC\_CF} |
|  | **Total** | | | **${TLT\_PC\_CR}** | **${TLT\_PC\_HI}** | **${TLT\_PC\_ME}** | **${TLT\_PC\_LO}** | **${TLT\_PC\_NC}** | **${TLT\_PC\_CF}** |

# 3. Vulnérabilités exploitables détectées

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

# 4. Détails des Vulnérabilités

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

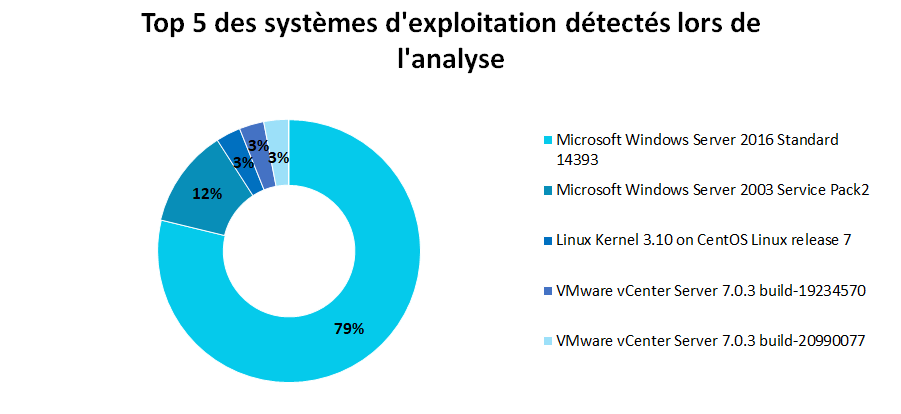
|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID DE LA VULNÉRABILITÉ** | | **${PC\_VULN\_ID}** | | **RISQUE** | | ${PC\_VULN\_RISK} | | **CVSS score** | | ${PC\_VULN\_CVSS} |
| **Synopsis** | | **${PC\_VULN\_Synopsis}** | | | | | | | | |
| **ÉLÉMENTS IMPACTÉS** | | **${PC\_VULN\_Hosts}** | | | | | | | | |
| **Exploitable par :** | | | | | | | | | | |
| **Metasploit** | ${PC\_VULN\_MSPLOIT} | | **Core Impact** | | ${PC\_VULN\_CoreImpact} | | **CANVAS** | | ${PC\_VULN\_CANVAS} | |
| **DESCRIPTION** | | | | | | | | | | |
| ${PC\_VULN\_Desc} | | | | | | | | | | |
| **RÉFÉRENCES** | | | | | | | | | | |
| **${PC\_VULN\_ref}** | | | | | | | | | | |
| **RECOMMENDATIONS** | | | | | | | | | | |
| **${PC\_VULN\_Recomendations}** | | | | | | | | | | |

# Audit Technique Service Mail

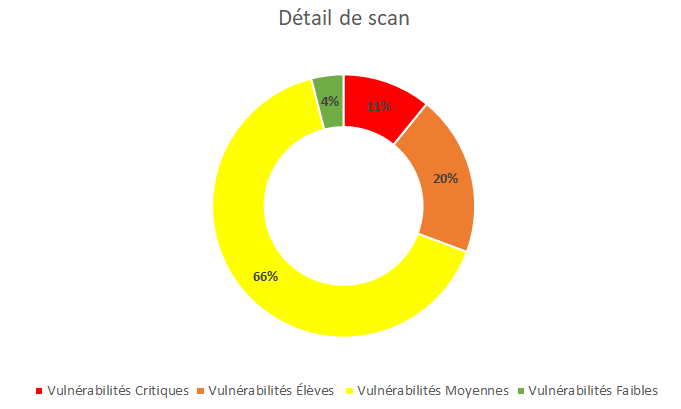
L’objectif de cette opération d’audit est d’identifier les failles de sécurité pour la messagerie, mesurer le degré de criticité et proposer une solution pour éliminer et minimiser les risques. Dans ce rapport, nous allons présenter les résultats de l’opération d’audit en exposant la liste des vulnérabilités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

# 1. Analyse récapitulative

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



## 1.2 Synthèse de Scan des Vulnérabilités



# 3. 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 l’actif** | **@IP** | **Système d’exploitation** | **Vulnérabilité** | | | |
| Critique | Élevé | Moyenne | Faible |
| **${id}** | **${MAIL\_Name}** | **${MAIL\_IP}** | **${MAIL\_OS}** | **{MAIL\_CR\_Exp}**/${MAIL\_CR} | **${MAIL\_HI\_Exp}**/${MAIL\_HI} | ${MAIL\_ME} | ${MAIL\_LO} |
|  | **Total** | | | **${TLT\_MAIL\_CR}** | **${TLT\_MAIL\_HI}** | **${TLT\_MAIL\_ME}** | **${TLT\_MAIL\_LO}** |

# 4. Vulnérabilités exploitables détectées

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

# 5. Détails des Vulnérabilités

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

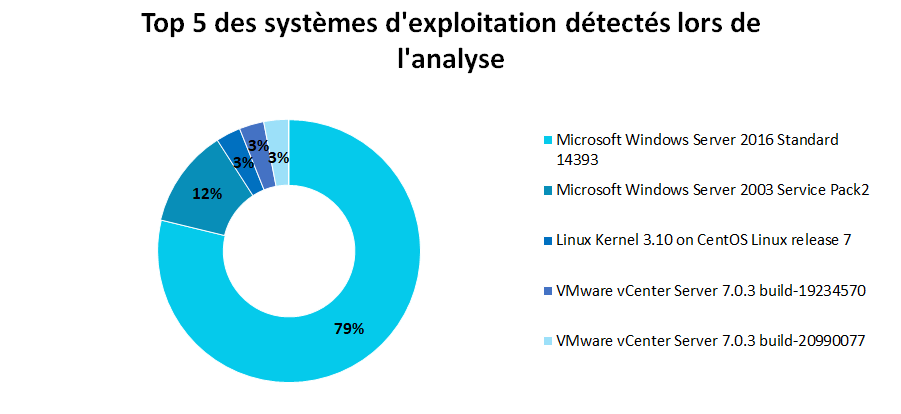
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID DE LA VULNÉRABILITÉ** | **${MAIL\_VULN\_ID}** | **RISQUE** | ${MAIL\_VULN\_RISK} | **CVSS score** | ${MAIL\_VULN\_CVSS} |
| **Synopsis** | **${MAIL\_VULN\_Synopsis}** | | | | |
| **ÉLÉMENTS IMPACTÉS** | **${MAIL\_VULN\_Hosts}** | | | |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

# Audit Technique Service VOIP

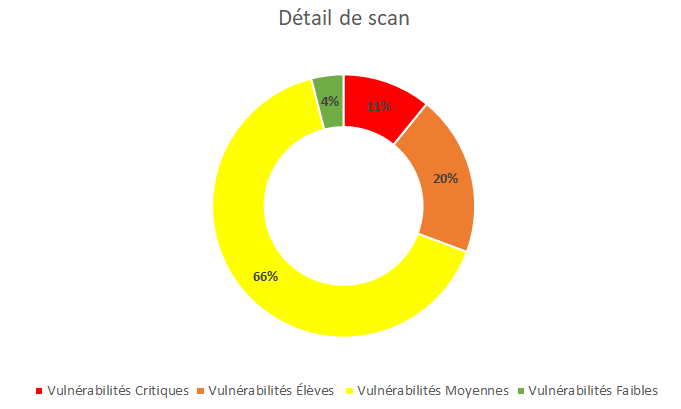
L’objectif de cette opération d’audit est d’identifier les failles de sécurité pour la messagerie, mesurer le degré de criticité et proposer une solution pour éliminer et minimiser les risques. Dans ce rapport, nous allons présenter les résultats de l’opération d’audit en exposant la liste des vulnérabilités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

# 1. Analyse récapitulative

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



## 1.2 Synthèse de Scan des Vulnérabilités



# 3. 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 l’actif** | **@IP** | **Système d’exploitation** | **Vulnérabilité** | | | |
| Critique | Élevé | Moyenne | Faible |
| **${id}** | **${VOIP\_Name}** | **${VOIP\_IP}** | **${VOIP\_OS}** | **{VOIP\_CR\_Exp}**/${VOIP\_CR} | **${VOIP\_HI\_Exp}**/${VOIP\_HI} | ${VOIP\_ME} | ${VOIP\_LO} |
|  | **Total** | | | **${TLT\_VOIP\_CR}** | **${TLT\_VOIP\_HI}** | **${TLT\_VOIP\_ME}** | **${TLT\_VOIP\_LO}** |

# 4. Vulnérabilités exploitables détectées

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

# 5. Détails des Vulnérabilités

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

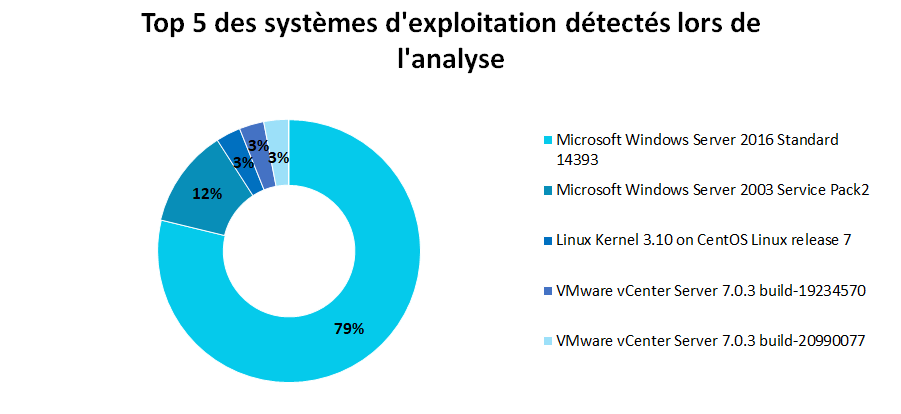
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID DE LA VULNÉRABILITÉ** | **${VOIP\_VULN\_ID}** | **RISQUE** | ${VOIP\_VULN\_RISK} | **CVSS score** | ${VOIP\_VULN\_CVSS} |
| **Synopsis** | **${VOIP\_VULN\_Synopsis}** | | | | |
| **ÉLÉMENTS IMPACTÉS** | **${VOIP\_VULN\_Hosts}** | | | |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

# Audit Technique Externe

L’objectif de cette opération d’audit est d’identifier les failles de sécurité pour les actifs exposés à l’internet, 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 .

# 1. Analyse récapitulative

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



## 1.2 Synthèse de Scan des Vulnérabilités

# 2. Collectes d’information de DarkWeb

* **Informations sur le Dark Web :**

**${pictureDarkWeb1:800:800}**

**${pictureDarkWeb2:800:800}**

# 3. 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 l’actif** | **@IP** | **Système d’exploitation** | **Vulnérabilité** | | | |
| Critique | Élevé | Moyenne | Faible |
| **${id}** | **${EXT\_Name}** | **${EXT\_IP}** | **${EXT\_OS}** | **{EXT\_CR\_Exp}**/${EXT\_CR} | **${EXT\_HI\_Exp}**/${EXT\_HI} | ${EXT\_ME} | ${EXT\_LO} |
|  | **Total** | | | **${TLT\_EXT\_CR}** | **${TLT\_EXT\_HI}** | **${TLT\_EXT\_ME}** | **${TLT\_EXT\_LO}** |

# 4. Vulnérabilités exploitables détectées

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

# 5. Détails des Vulnérabilités

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

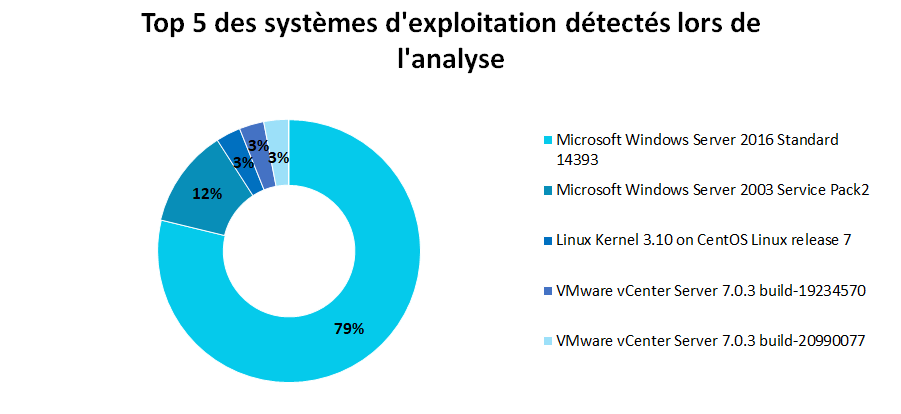
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID DE LA VULNÉRABILITÉ** | **${EXT\_VULN\_ID}** | **RISQUE** | ${EXT\_VULN\_RISK} | **CVSS score** | ${EXT\_VULN\_CVSS} |
| **Synopsis** | **${EXT\_VULN\_Synopsis}** | | | | |
| **ÉLÉMENTS IMPACTÉS** | **${EXT\_VULN\_Hosts}** | | | | |
| **DESCRIPTION**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

# Audit Technique des applications

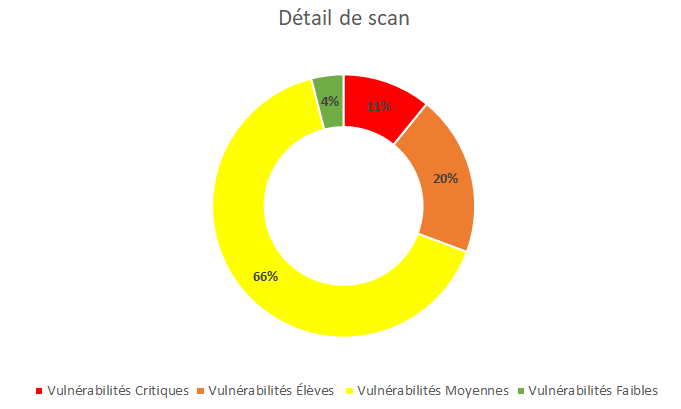
L’objectif de cette opération d’audit est d’identifier les failles de sécurité pour les applications, mesurer le degré de criticité et proposer une solution pour éliminer et minimiser les risques. Dans ce rapport, nous allons présenter les résultats de l’opération d’audit en exposant la liste des vulnérabilités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

# 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 : 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 l’application** | **@IP** | **Système d’exploitation** | **Vulnérabilité** | | | |
| Critique | Élevé | Moyenne | Faible |
| **${id}** | **${APP\_Name}** | **${APP\_IP}** | **${APP\_OS}** | **{APP\_CR\_Exp}**/${APP\_CR} | **${APP\_HI\_Exp}**/${APP\_HI} | ${APP\_ME} | ${APP\_LO} |
|  | **Total** | | | **${TLT\_APP\_CR}** | **${TLT\_APP\_HI}** | **${TLT\_APP\_ME}** | **${TLT\_APP\_LO}** |

# 3. Vulnérabilités exploitables détectées

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

# 4. Détails des Vulnérabilités

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

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