**Test d’intrusion <TYPE >**

Sommaire

[1. Introduction 3](#_Toc91492599)

[1.1 Rappel du périmètre 3](#_Toc91492600)

[1.2 Présentation des échelles utilisées 4](#_Toc91492601)

[2. Synthèse du test d’intrusion 5](#_Toc91492602)

[2.1 Bilan de l’audit 5](#_Toc91492603)

[2.2 Synthèse des vulnérabilités 7](#_Toc91492604)

[2.3 Preuves 8](#_Toc91492605)

[3. Vulnérabilités identifiées 9](#_Toc91492606)

[3.1 9](#_Toc91492607)

[3.2 10](#_Toc91492608)

[3.3 11](#_Toc91492609)

[3.4 12](#_Toc91492610)

[3.5 13](#_Toc91492611)

[3.6 14](#_Toc91492612)

# Introduction

## Rappel du périmètre

Le test d’intrusion a porté sur le périmètre suivant :

**Périmètre :**

* X.X.X.X
* X.X.X.X

## Présentation des échelles utilisées

L’échelle de **risque** est classée selon 4 niveaux :

|  |  |
| --- | --- |
| **Niveau de risque** | **Description** |
| Mineur | Faible risque sur le système d’information et pouvant nécessiter une correction |
| Important | Risque modéré sur le système d’information et nécessitant une correction à moyen terme |
| Majeur | Risque majeur sur le système d’information nécessitant une correction à court terme |
| **Critique** | Risque critique sur le système d’information et nécessitant une correction immédiate ou imposant un arrêt immédiat du service |

Le niveau de risque d’une vulnérabilité est calculé est fonction de deux valeurs, sa **facilité d’exploitation** :

|  |  |
| --- | --- |
| **Difficulté d'exploitation** | **Description** |
| Difficile | Exploitation de vulnérabilités non publiées nécessitant une expertise en sécurité des Systèmes d’information et le développement d’outils spécifiques et ciblés |
| Elevée | Exploitation de vulnérabilités publiques nécessitant des compétences en sécurité des Systèmes d’information et le développement d’outils simples |
| Modérée | Exploitation nécessitant des techniques simples et des outils disponibles  Publiquement |
| **Facile** | Exploitation triviale, sans outil ni compétences particulières |

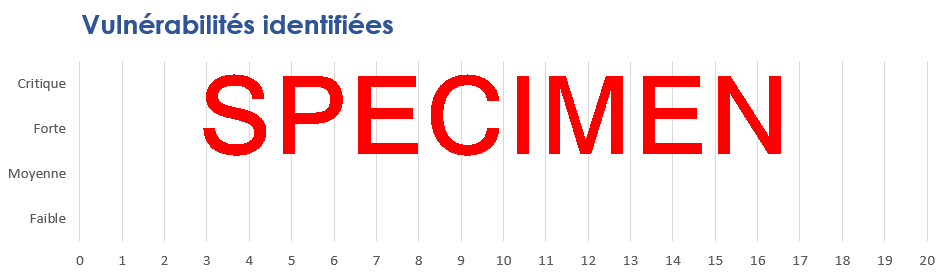
Ainsi que l’impact technique CVSS de la vulnérabilité

|  |  |
| --- | --- |
| **Gravité** | **Description** |
| Faible | Faible impact sur le composant |
| Moyenne | Impact moyen sur le composant |
| **Forte** | Impact fort sur le composant |
| **Critique** | Impact critique sur le composant |

# Synthèse du test d’intrusion

## Bilan de l’audit

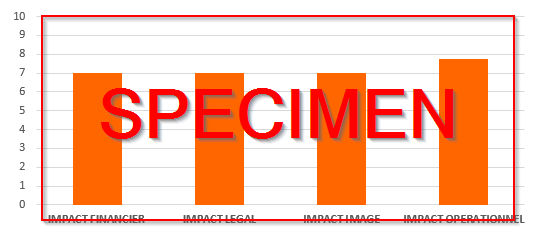
Le test d’intrusion a permis d’identifier plusieurs vulnérabilités sur le périmètre cible, le diagramme ci-dessous représente la répartition en termes de gravité technique :



Les vulnérabilités de gravité forte et critique constituent la principale source de menace envers le SI, celles-ci permettent à un attaquant de Compromettre rapidement et facilement l’organisation

Les vulnérabilités moyennes et faibles sont principalement des vulnérabilités liées à un non-respect des bonnes pratiques de configuration et sécurité pouvant amener (mise bout à bout) une compromission du SI

Enfin, le diagramme ci-dessous présente les impacts “business” sur l’organisation, la moyenne se trouve entre \_\_\_ et \_\_\_ qui est un score \_\_\_



Le système d’information possède un score de risque de \_\_ %

Une image contenant texte, parapluie, accessoire, signe

Description générée automatiquement

## Synthèse des vulnérabilités

Une image contenant texte

Description générée automatiquement

## Preuves

Les images suivantes apportent en guise de preuve l’atteinte des objectifs de l’attaquant

# Vulnérabilités identifiées

## 

## 

## 

## 

## 

## 