Rapport d’audit technique



Contact

| Date | Auteur | Fonction |
| --- | --- | --- |
| 06/09/2024 | Jorge Martinez Pontijas | auditeur |

Diffusion du document

| Société | Interlocuteur | Fonction | Mail |
| --- | --- | --- | --- |
| X | John Doe | RSSI | john.doe@mail.fr |

# Table des matières

[**Table des matières 3**](#_heading=h.1fob9te)

[**1. Présentation de la démarche 5**](#_heading=h.c41bx21umpc0)

[1.1 Rappel du besoin 5](#_heading=h.1k3vd68tlxgc)

[1.2 Présentation de la démarche 5](#_heading=h.mq282zn05bu5)

[1.3 Objectifs visés 6](#_heading=h.m5f11o4l0z59)

[1.4 Mode opératoire 6](#_heading=h.77919egaxn3a)

[1.5 Exhaustivité des résultats 6](#_heading=h.ehghq68wben2)

[**2. Synthèse managériale 7**](#_heading=h.4d34og8)

[Vulnérabilité identifiées 7](#_heading=h.17dp8vu)

[2.1 Conclusion 8](#_heading=h.26in1rg)

[Synthèse des vulnérabilités 9](#_heading=h.44sinio)

[Plan d’action recommandé 10](#_heading=h.2jxsxqh)

[**3. Vulnérabilités découvertes 11**](#_heading=h.2xcytpi)

[3.1 Exposition de service d’administration sur internet 11](#_heading=h.10p11rrftfk6)

[3.1.1 Résumé 11](#_heading=h.8fgoj6am2953)

[3.1.2 Actif concernés 11](#_heading=h.dtlyna5x58s7)

[3.1.3 Références 11](#_heading=h.jdfkjgela93w)

[3.1.4 Recommandation 11](#_heading=h.shs7xp9iv8s4)

[3.1.5 Exploitation 12](#_heading=h.wdputlethjx)

[3.2 Le protocole HTTPS n'est pas mis en place 13](#_heading=h.gbd8ms2y0fdy)

[3.2.1 Résumé 13](#_heading=h.cnc5096l2won)

[3.2.2 Actif concernés 13](#_heading=h.sp8dyqs4tghw)

[3.2.3 Références 13](#_heading=h.htzofjg2wpwt)

[3.2.4 Recommandation 13](#_heading=h.mtxkabxrckor)

[3.2.5 Exploitation 13](#_heading=h.j2qu8u7l0l7g)

[3.3 Défaut de maintien en conditions de sécurité 15](#_heading=h.ftpdwefa0yvx)

[5.3.1 Résumé 15](#_heading=h.ev8qjwpnkr6p)

[3.3.2 Actif concernés 15](#_heading=h.xyed4l8gnf62)

[3.3.3 Références 15](#_heading=h.rkc9w5hne9vh)

[3.3.4 Recommandation 15](#_heading=h.303t87dv5rld)

[3.3.5 Exploitation 15](#_heading=h.5jgikdcxc53l)

[3.4 Absence de cloisonnement 17](#_heading=h.s09ur4wpxbfc)

[3.4.1 Résumé 17](#_heading=h.qkv5ar7xmcl6)

[3.4.2 Actif concernés 17](#_heading=h.bewzx6hi7tj6)

[3.4.3 Références 17](#_heading=h.7cj9xy4bmtj6)

[3.4.4 Recommandation 17](#_heading=h.dqng3qtbtn20)

[3.4.5 Exploitation 18](#_heading=h.gblm8b47iy1s)

[**4. Annexes 19**](#_heading=h.gt24i6lp8rgj)

[4.1 Classifications des vulnérabilités 19](#_heading=h.2p2csry)

[4.2 Conventions de représentation 21](#_heading=h.3o7alnk)

[Mesure de l’impact 21](#_heading=h.23ckvvd)

[Intégrité 21](#_heading=h.ihv636)

[Confidentialité 21](#_heading=h.32hioqz)

[Disponibilité 22](#_heading=h.41mghml)

[Mesure de l’exploitabilité 23](#_heading=h.vx1227)

[Complexité d’exploitation 23](#_heading=h.3fwokq0)

[Privilège requis 23](#_heading=h.1v1yuxt)

[Recommandations 24](#_heading=h.2u6wntf)

[Niveau de difficulté de correction 24](#_heading=h.19c6y18)

[Priorité 24](#_heading=h.3tbugp1)

# 

# Présentation de la démarche

## 1.1 Rappel du besoin

Le but est d'évaluer le niveau de sécurité du périmètre ciblé par une démarche présentée ci-dessous. Pour chaque risque identifié, des recommandations seront effectuées afin de limiter le défaut et atteindre un niveau de sécurité acceptable.

## 1.2 Présentation de la démarche

La démarche d’ est définie comme ci-dessous : 

Cette démarche s’articule autour de 4 étapes complémentaires :

• Collecte d’informations : A partir du niveau d’information initial, nous allons tenter de retrouver l’ensemble des informations sur la société cible, telles que l’organisation de l’entreprise, son architecture publique, etc… Cette étape permet d’évaluer le niveau d’exposition et d’opacité de la société sur Internet

• Cartographie du périmètre : Une fois le périmètre défini, nous tentons de découvrir l’ensemble des systèmes et services accessibles sur Internet. Pour chacun de ces services, nous évaluons le niveau de configuration et identifions les vulnérabilités éventuelles.

• Tentatives d’intrusion : Durant cette phase, nous tentons d’exploiter les vulnérabilités identifiées précédemment afin de nous introduire sur les systèmes. L’objectif est de démontrer l’exploitabilité de la faille de sécurité et d’évaluer le niveau de compétence nécessaire pour parvenir à l’exploiter

• Tentatives de rebonds : En fonction du résultat de l’étape précédente, nous tentons d’évaluer le niveau d’étanchéité de votre réseau interne par rapport aux éventuels serveurs compromis.

## 1.3 Objectifs visés

La prestation de test d’intrusion a pour objectif de dresser un état des lieux de la sécurité d’un système d’information ou d’une application à un instant donné. L’objectif est de mettre en lumière les failles de sécurité réellement exploitables par un individu malveillant dans un temps volontairement limité.

## 1.4 Mode opératoire

L'audit a été réalisé le 06/09/2024 depuis nos locaux, a travers d’un vpn que nous a asigne une des ip de l’entreprise.

Vous nous avez fourni l’ip sur le reseau suivante comme point de départ.

## 1.5 Exhaustivité des résultats

Les tests ont été réalisés sur une durée prédéfinie et limitée, cette démarche s'appuie sur une durée de challenge et n'a pas vocation à être exhaustive. Seules les fonctionnalités accessibles lors de l'audit ont été analysées.

# 

# 2. Synthèse managériale

## 

## Vulnérabilité identifiées

## Graphique

## 2.1 Conclusion

Le test d’intrusion réalisé par Jorge Martinez Pontijas sur l’adresse IP fournie par la société X a mis en évidence plusieurs vulnérabilités. Ces manquements permettent, une fois exploités conjointement de compromettre l’ensemble du domaine et ce, en disposant uniquement d’un accès au site web.

Un risque est présent concernant les données techniques du site web, pouvant impacter la confidentialité des données des utilisateurs. En effet, un utilisateur malveillant serait en mesure d’exploiter des vulnérabilités connues afin de récupérer la totalité ou une partie des données stockées sur le serveur. Cela correspond ici, aux adresses postales, mots de passe et dates de naissance des utilisateurs.

Nous pouvons mettre l'accent sur la vulnérabilité majeure de ces tests, soit l’absence de cloisonnement débloque la possibilité de rentrer sur le système pour tout attaquant. Cette vulnérabilité permet à un attaquant à travers une interface utilisateur de déployer des commandes administrateur et d'y installer de potentiel logiciel malveillant.

Bien que le risque de compromission reste élevé, un attaquant à tout de même besoin d’un accès utilisateur pour compromettre le système.

## Synthèse des vulnérabilités

| **ID** | **Nom de la vulnérabilité** | **Description** | **Risque** | **Score CVSS** |
| --- | --- | --- | --- | --- |
| VULN-01 |  |  |  |  |
| VULN-02 |  |  |  |  |
| VULN-03 |  |  |  |  |
| VULN-04 |  |  |  |  |

## 

## Plan d’action recommandé

| **ID** | **Vulnérabilités** | **Description** | **Réalisation** | **Risque** | **Priorité** |
| --- | --- | --- | --- | --- | --- |
| REC-01 | VULN-01 |  |  |  |  |
| REC-02 | VULN-02 |  |  |  |  |
| REC-03 | VULN-03 |  |  |  |  |
| REC-04 | VULN-04 |  |  |  |  |

# 

# 3. Vulnérabilités découvertes

| 3.1 | | | score |
| --- | --- | --- | --- |
| VULN-01 |  | Facilité d’exploitation : |  |
| Risque : |  |  |  |
| Impact : |  |  |  |
| Niveau de privilèges : |  | |  |
| Score CVSS : | | |  |

### 3.1.1 Résumé

### 3.1.2 Actif concernés

### 3.1.3 Références

* [EN] Mitre -
* [FR] OWASP -

Recomandation

### 3.1.5 Exploitation

Explication

Capture d’ecran

commande

### resultat capture d’ecran

page d’administration du serveur web

| 3.2 | | |  |
| --- | --- | --- | --- |
| Risque : |  | Facilité d’exploitation : |  |
| Impact : |  |  |  |
|  |  |  |  |
| Niveau de privilèges : |  | |  |
| Score CVSS : | | |  |

### 3.2.1 Résumé

### 3.2.2 Actif concernés

### 3.2.3 Références

[EN] Mitre

### 3.2.4 Recommandation

### 3.2.5 Exploitation

.

commande nmap utilisée pour le scan des services

# 

| 3.3 | | |  |
| --- | --- | --- | --- |
| Risque : |  | Facilité d’exploitation : |  |
| Impact : |  |  |  |
|  |  |  |  |
| Niveau de privilèges : |  | |  |
| Score CVSS : | | |  |

### 5.3.1 Résumé

### 3.3.2 Actif concernés

### 3.3.3 Références

### 3.3.4 Recommandation

### 3.3.5 Exploitation

capture

commande smb pour la détection de compte sans password

| 3.4 | | |  |
| --- | --- | --- | --- |
| Risque : |  | Facilité d’exploitation : |  |
| Impact : |  |  |  |
|  |  |  |  |
| Niveau de privilèges : |  | |  |
| Score CVSS : H | | |  |

### 3.4.1 Résumé

.

### 3.4.2 Actif concernés

### 3.4.3 Références

[EN] Mitre

### 3.4.4 Recommandation

### 

### 3.4.5 Exploitation

Explication

Capture

Interface utilisateur web ecatastrophe

comandes

invité de commande serveur à travers usermin

# 4. Annexes

## 4.1 Classifications des vulnérabilités

L’ANSSI propose l’échelle de classification des vulnérabilités suivante :

Les vulnérabilités, qu’elles soient d’origine technique ou organisationnelle, sont classées en

fonction du risque qu’elles font peser sur le système d’information, c'est-à-dire en fonction

de l’impact de la vulnérabilité sur le système d’information et de sa difficulté d’exploitation.

Le niveau du risque lié à chaque vulnérabilité est apprécié selon l’échelle de valeur suivante :

* 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.

La facilité d’exploitation correspond au niveau d’expertise et aux moyens nécessaires à la réalisation de l’attaque. Elle est appréciée selon l’échelle suivante :

* Facile : exploitation triviale, sans outil particulier ;
* Modérée : exploitation nécessitant des techniques simples et des outils disponibles publiquement ;
* Elevée : exploitation de vulnérabilités publiques nécessitant des compétences en sécurité des systèmes d’information et le développement d’outils simples ;
* Difficile : exploitation de vulnérabilités non publiées nécessitant une expertise en sécurité des systèmes d’information et le développement d’outils spécifiques et ciblés.

L’impact correspond aux conséquences que l’exploitation de la vulnérabilité peut entraîner sur le système d’information de l’audité. Il est apprécié selon l’échelle suivante :

* Mineur : pas de conséquence directe sur la sécurité du système d’information audité ;
* Important : conséquences isolées sur des points précis du système d’information audité ;
* Majeur : conséquences restreintes sur une partie du système d’information audité ;
* Critique : conséquences généralisées sur l’ensemble du système d'information audité.

|  | | **FACILITÉ D’EXPLOITATION** | | | |
| --- | --- | --- | --- | --- | --- |
| **Difficile** | **Elevée** | **Modérée** | **Facile** |
| **IMPACT** | **Mineur** | ***Mineur*** | ***Mineur*** | ***Important*** | ***Majeur*** |
| **Important** | ***Mineur*** | ***Important*** | ***Important*** | ***Majeur*** |
| **Majeur** | ***Important*** | ***Majeur*** | ***Majeur*** | ***Critique*** |
| **Critique** | ***Important*** | ***Majeur*** | ***Critique*** | ***Critique*** |

Les vulnérabilités sont également notées selon le “score commun de notation des vulnérabilités” version 3.1 créé par First. Il permet de noter et de communiquer sur les caractéristiques et la gravité des vulnérabilités logiciels. La chaîne de caractère vectorielle (CVSS) et le score final seront présentés au début de chaque vulnérabilité.

Exemple :

| Score CVSS | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N | 0.0 |
| --- | --- | --- |

## 

## 4.2 Conventions de représentation

### Mesure de l’impact

#### **Intégrité**

Cette mesure identifie l'impact sur l'intégrité d'une vulnérabilité exploitée avec succès. L'intégrité fait référence à la fiabilité et à la véracité des informations.

| Indicateur | Description |
| --- | --- |
|  | Il n'y a pas de perte d'intégrité au sein de la composante touchée. |
|  | La modification des données est possible, mais l'attaquant ne contrôle pas les conséquences d'une modification. |
|  | Il y a une perte totale d'intégrité, ou une perte totale de protection. |

#### **Confidentialité**

Cette mesure identifie l'impact sur la confidentialité d'une vulnérabilité exploitée avec succès. La confidentialité consiste à limiter l'accès aux informations et leur divulgation aux seuls utilisateurs autorisés, ainsi qu'à empêcher l'accès ou la divulgation d'informations par des personnes non autorisées.

| Indicateur | Description |
| --- | --- |
|  | ll n'y a pas de perte de confidentialité au sein de la composante  touchée. |
|  | Il y a une certaine perte de confidentialité. L'accès à certaines  informations restreintes est obtenu, mais l'attaquant n'a pas de  contrôle sur les informations obtenues, ou le montant ou le type de  perte est limité. |
|  | Il y a une perte totale de confidentialité, ce qui entraîne la divulgation  à l'agresseur de toutes les ressources au sein de l'élément touché.  Une autre solution consiste à n'obtenir l'accès qu'à certaines  informations restreintes, mais les informations divulguées  présentent un impact direct et grave. |

#### 

#### **Disponibilité**

Cette mesure identifie l'impact sur la disponibilité d'une vulnérabilité exploitée avec succès. Cette mesure fait référence à la perte de disponibilité du composant touché, comme un service en réseau (par exemple : le web, une base de données, le courrier électronique).

| Indicateur | Description |
| --- | --- |
|  | Il n'y a pas d'impact sur la disponibilité au sein de la composante concernée. |
|  | Il y a un léger impact sur la disponibilité, des ralentissements se font sentir mais n’entraînent pas de gêne par rapport à une activité normale. |
|  | Il y a une perte totale de disponibilité, ce qui permet à l'attaquant de refuser totalement l'accès aux ressources de la composante touchée ; cette perte est soit durable (pendant que l'attaquant continue à lancer l'attaque), soit persistante (l'état persiste même après la fin de l'attaque). |

### 

### Mesure de l’exploitabilité

#### Complexité d’exploitation

Cette mesure décrit les conditions indépendantes de la volonté de l'agresseur qui doivent exister pour exploiter la vulnérabilité.

| Valeur métrique | Description |
| --- | --- |
| Faible compétence | Il n'existe pas de conditions d'accès spécialisées ou de circonstances atténuantes. Un attaquant peut s'attendre à des succès répétés lorsqu'il s'attaque à l'élément vulnérable. Ou L’attaquant a un minimum de connaissance pour l’élément vulnérable et les conditions d’accès sont connues. |
| Haute compétence | Le succès d'une attaque dépend de conditions qui échappent au contrôle de l'attaquant. En d'autres termes, une attaque réussie ne peut pas être réalisée à volonté, mais exige de l'attaquant qu'il investisse dans un effort mesurable de préparation ou d'exécution contre l'élément vulnérable. La vulnérabilité est théorique et demande un nombre considérable de ressources ou de temps. |

#### Privilège requis

Cette métrique décrit le niveau de privilèges qu'un attaquant doit posséder avant de réussir à exploiter la vulnérabilité.

| Valeur métrique | Description |
| --- | --- |
| Aucun | L'attaquant n'est pas authentifié avant l'attaque, et n'a donc pas besoin d'accéder aux paramètres ou aux fichiers du système vulnérable pour effectuer une attaque. |
| Faible | L'attaquant a besoin de privilèges qui fournissent des capacités de base à l'utilisateur. |
| Haut | L'attaquant a besoin de privilèges qui lui permettent d'exercer un contrôle important (par exemple, administrateur) sur le composant vulnérable. |

#### 

### Recommandations

#### Niveau de difficulté de correction

| Valeur métrique | Description |
| --- | --- |
| Faible | Les corrections impliquent peu de compétences, de moyens et de temps pour être corrigées. |
| Moyen | Les corrections impliquent des compétences et un peu de temps ou des moyens raisonnables. |
| Elevé | Les corrections impliquent de nombreuses compétences, du temps ou des moyens. |

#### Priorité

| Indicateur | Valeur | Description |
| --- | --- | --- |
|  | Faible | Les actions sont à réaliser sur le long terme |
|  | Modéré | Les actions sont à réaliser sur le moyen terme. |
|  | Elever | Les actions sont à réaliser sur le court terme. |
|  | Urgent | Les actions sont à réaliser le plus tôt possible. |

#### 