

**Rapport d’empreinte numérique**

# Nom de domaine analysé

{TARGET}

# PrÉsentation du document

Le terme "rapport d'empreinte numérique" ou "surface potentielle d'attaque" se réfère à l'évaluation du niveau d’exposition du commanditaire et des vulnérabilités potentiellement applicables aux actifs exposés, sur la base d’informations publiques et d’actions passives (OSINT). Il s'agit d'une analyse des informations disponibles publiquement sur un système, telles que les services ouverts, les protocoles réseau utilisés, les versions de logiciels connues, les configurations par défaut, etc. Afin d'identifier les points d'accès et les faiblesses potentielles qui pourraient être exploitées par des attaquants.

L’analyse de l’empreinte numérique utilise des techniques d'énumération passive, ce qui signifie qu'elle ne perturbe pas activement le système en question. Au lieu de cela, elle se base sur des informations accessibles publiquement. Ces informations permettent de dresser un profil détaillé de la cible et de comprendre les éléments exposés et potentiellement vulnérables.

En analysant le rapport d'empreinte numérique, les équipes IT et/ou sécurité peuvent prendre des mesures pour réduire les risques et renforcer la sécurité du système. Cela peut impliquer la correction des vulnérabilités connues, la mise à jour des logiciels, la configuration appropriée des paramètres de sécurité, et d'autres mesures de protection.

À l'issue de l'analyse des résultats et des potentielles vulnérabilités identifiées dans le rapport d'empreinte numérique, il est courant d'établir une note qui représente le niveau de sécurité ou le niveau de risque global du système. Cette note va de A+ pour le meilleur résultat à D.

La note permet de synthétiser les résultats de l'évaluation et de communiquer de manière concise le degré de risque associé au système ou au réseau analysé. Elle facilite la compréhension et la prise de décision en fournissant une évaluation globale de la sécurité et en identifiant les domaines prioritaires à améliorer.

En se basant sur cette note, les équipes IT et/ou sécurité peuvent déterminer les actions à entreprendre pour renforcer la sécurité du système. Les vulnérabilités critiques ou présentant un risque élevé peuvent nécessiter une attention immédiate, tandis que celles de moindre importance peuvent être traitées de manière progressive.

*Certains sous-domaines peuvent ne pas apparaître dans les résultats du rapport détaillé des vulnérabilités découvertes en raison de la possibilité qu'ils appartiennent à la même adresse IP ou qu'il soit impossible de résoudre leur adresse IP. Cela peut se produire lorsque plusieurs sous-domaines partagent la même adresse IP, ce qui rend difficile la distinction des vulnérabilités spécifiques à chaque sous-domaine.*

*De plus, il peut y avoir des situations où la résolution de l'adresse IP des sous-domaines est impossible, ce qui signifie que l'adresse IP réelle associée à ces sous-domaines n'est pas disponible dans les résultats de l'évaluation. Cela peut être dû à des facteurs tels que des configurations de serveur spécifiques, des pare-feu ou d'autres mesures de protection qui bloquent la résolution IP.*

Navigation rapide

[Nom de domaine analysé 1](#_Toc135225038)

[Présentation du document 1](#_Toc135225039)

[note 2](#_Toc135225040)

[système analysé 2](#_Toc135225041)

[ÉNUMÉRATION DES SOUS DOMAINES 2](#_Toc135225042)

[Navigation rapide 3](#_Toc135225043)

[Rapport détaillé des vulnérabilités DÉCOUVERTES 4](#_Toc135225044)

note

La note globale est {NOTE}

Pour définir cette note nous avons retenu les résultats suivants :

{VULN\_CRITICAL} vulnérabilités critiques

{VULN\_HIGH} vulnérabilités élevées

{VULN\_MEDIUM} vulnérabilités moyennes

{VULN\_LOW} vulnérabilités faibles

# système analysÉ



# ÉNUMÉRATION DES SOUS DOMAINES

{SUBDOMAINS}

Rapport détaillÉ des vulnÉrabilitÉs DÉCOUVERTES

*Remarque : Les IP peuvent ne pas être affecté par toutes ces vulnérabilités. Elles sont implicites en fonction du logiciel et de la version utilisée.*

{CVE\_CONTENT}