Rapport Global

# rapport\_scan\_192.168.100.15\_20240615\_145013.docx

# rapport\_scan\_cve\_20240615\_145907\_48bb64ac-0b9f-40a6-8b67-24aefa4c6237.docx

Rapport de scan pour 192.168.100.15

## Généré le : 15-06-2024 14:50:13

# Scan des ports:

Port 135 (Service inconnu): open

Port 137 (NetBIOS Name Service): filtered

Port 139 (NetBIOS Session Service): open

Port 445 (Microsoft-DS Active Directory, partages Windows): open

Port 902 (Service inconnu): open

Port 912 (Service inconnu): open

# Supposition du système d'exploitation:

Microsoft Windows 10 1809 - 2004 (Précision: 100%)

# Services détectés:

Port 135: msrpc

Port 139: netbios-ssn

Port 445: microsoft-ds

Port 902: vmware-auth

Port 912: vmware-auth

Port 3389: ms-wbt-server

Port 5357: http

# Bannières collectées:

Port 135: Microsoft Windows RPC

Port 139: Microsoft Windows netbios-ssn

Port 445:

Port 902: VMware Authentication Daemon

Port 912: VMware Authentication Daemon

Port 3389: Microsoft Terminal Services

Port 5357: Microsoft HTTPAPI httpd

Rapport de Scan CVE

# Services

Service: nagios-nsca, Version:

Description: Le service nagios-nsca est un outil de passage de données sécurisé permettant à Nagios de collecter des informations de surveillance provenant de systèmes distants de manière sécurisée.

Service: http, Version: 10.0

Description: Le service HTTP (Hypertext Transfer Protocol) est un protocole de communication utilisé sur Internet pour transférer des données entre un serveur Web et un navigateur Web. Il permet d'afficher des pages web, de télécharger des fichiers et de communiquer avec des applications en ligne.

Service: msrpc, Version:

Description: Le service msrpc (Microsoft Remote Procedure Call) est un protocole utilisé pour permettre la communication entre différents processus sur un réseau, en facilitant l'exécution de fonctions à distance. Il est couramment utilisé dans les environnements Windows pour la communication inter-processus et les opérations à distance. Cependant, il peut également être exploité par des attaquants pour mener des attaques sur le réseau, c'est pourquoi il est important de sécuriser correctement son utilisation.

Service: netbios-ssn, Version:

Description: Le service NetBIOS-SSN (Session Service) est un protocole de communication utilisé pour établir et maintenir des sessions entre ordinateurs. Il facilite la communication et le partage de ressources dans un réseau local. Cependant, il peut présenter des vulnérabilités en matière de sécurité, notamment en ce qui concerne l'authentification et la confidentialité des données échangées. Il est donc important de configurer et surveiller ce service de manière appropriée pour prévenir les risques de sécurité.

Service: https, Version:

Description: Le service HTTPS est un protocole de communication sécurisé utilisé sur internet pour crypter les échanges de données entre un navigateur web et un serveur web, assurant ainsi la confidentialité et l'intégrité des informations transmises.

Service: microsoft-ds, Version:

Description: Le service microsoft-ds est un service Microsoft qui permet le partage de fichiers et d'imprimantes en réseau, notamment sur des systèmes Windows. Il utilise le protocole SMB (Server Message Block) pour assurer la communication entre les machines.

Service: ms-wbt-server, Version:

Description: Le service ms-wbt-server est le service Remote Desktop Services (RDS) de Windows qui permet aux utilisateurs d'accéder à distance à des ordinateurs et serveurs Windows via une connexion Bureau à distance (RDP). Il permet de contrôler un ordinateur à distance de manière sécurisée.

# Vulnérabilités

## Service: msrpc (Version: )

**CVE ID: CVE-2002-1873**Description: Le CVE-2002-1873 est une vulnérabilité de type débordement de tampon affectant le noyau Linux 2.4.x. Cette faille pourrait permettre à un attaquant distant d'exécuter du code arbitraire ou de provoquer un déni de service. Il est recommandé de mettre à jour les systèmes concernés pour éviter toute exploitation de cette vulnérabilité.  
*Recommandation: La vulnérabilité CVE-2002-1873 est une faille de sécurité permettant des attaques par injection SQL. Pour mitiger cette vulnérabilité, assurez-vous d'utiliser des requêtes SQL préparées, de valider et filtrer les entrées utilisateur, et de limiter les privilèges d'accès à la base de données.*

**CVE ID: CVE-2018-8407**Description: Le CVE-2018-8407 est une vulnérabilité de type déni de service (DoS) qui affecte le noyau de Windows. Elle permet à un attaquant distant de provoquer un plantage du système en envoyant des paquets malveillants. L'exploitation de cette faille peut entraîner des interruptions de service et perturber les activités des utilisateurs.  
*Recommandation: La vulnérabilité CVE-2018-8407 concerne une exposition d'informations sensibles dans Microsoft Edge. Pour atténuer cette vulnérabilité, assurez-vous de mettre à jour votre navigateur Edge avec les derniers correctifs de sécurité disponibles. Envisagez également d'utiliser une solution de sécurité supplémentaire pour renforcer la protection de votre navigateur.*

## Service: https (Version: )

**CVE ID: CVE-2024-4107**Description: Le CVE-2024-4107 est une vulnérabilité de type exécution de code à distance qui affecte le système d'exploitation Windows. Si exploitée avec succès, cette faille permettrait à un attaquant distant de prendre le contrôle total du système compromis. Il est fortement recommandé de patcher rapidement les systèmes Windows pour se prémunir contre cette faille critique.  
*Recommandation: La vulnérabilité CVE-2024-4107 est due à une faille dans le système d'authentification qui peut être exploitée pour des attaques d'injection de code. Pour mitiger cette vulnérabilité, il est recommandé de mettre en place des contrôles d'entrée stricts, de valider et d'échapper les données utilisateur et de mettre à jour le système affecté avec les correctifs de sécurité disponibles.*

**CVE ID: CVE-2024-5770**Description: Le CVE-2024-5770 est une vulnérabilité de type injection SQL affectant le système de gestion de bases de données MySQL version 5.5 à 5.7. Elle permet à un attaquant d'exécuter des requêtes SQL malveillantes et potentiellement d'accéder ou modifier des données sensibles. L'impact potentiel de cette faille est la divulgation d'informations confidentielles, la modification de données ou même la prise de contrôle du système.  
*Recommandation: La vulnérabilité CVE-2024-5770 peut être atténuée en appliquant immédiatement le correctif fourni par le fournisseur concerné. Assurez-vous que tous les systèmes affectés sont mis à jour régulièrement pour éviter toute exploitation potentielle de la vulnérabilité. Surveillez attentivement les activités suspectes ou non autorisées sur le réseau pour détecter rapidement toute tentative d'exploitation de la vulnérabilité.*

## Service: microsoft-ds (Version: )

**CVE ID: CVE-2024-35927**Description: Le CVE-2024-35927 est une vulnérabilité de type exécution de code à distance affectant les systèmes d'exploitation Windows. Un attaquant pourrait exploiter cette faille pour prendre le contrôle complet du système cible, compromettant ainsi la confidentialité et l'intégrité des données. Il est recommandé de mettre à jour les systèmes affectés dès que possible pour se prémunir contre cette menace.  
*Recommandation: La vulnérabilité CVE-2024-35927 peut être mitigée en appliquant rapidement le correctif de sécurité fourni par le fournisseur du logiciel concerné. Assurez-vous de surveiller régulièrement les mises à jour de sécurité et de mettre en place des mesures de détection et de réponse en cas d'exploitation de la vulnérabilité. Enfin, limitez l'accès aux ressources sensibles uniquement aux utilisateurs autorisés pour réduire les risques liés à l'exploitation de cette vulnérabilité.*

**CVE ID: CVE-2024-35931**Description: Le CVE-2024-35931 est une vulnérabilité de type exécution de code à distance touchant le système d'exploitation Windows. Cette faille permet à un attaquant distant d'exécuter du code malveillant et de prendre le contrôle de la machine, potentiellement compromettant la sécurité des données. Il est recommandé d'appliquer les correctifs de sécurité fournis par le fournisseur pour se protéger contre cette menace.  
*Recommandation: Pour le CVE-2024-35931, je vous recommande de désactiver les services non essentiels, de limiter l'exposition des systèmes vulnérables et de surveiller de près les activités suspectes sur le réseau. Assurez-vous également de mettre à jour régulièrement les logiciels et les correctifs de sécurité pour réduire les risques d'exploitation de la vulnérabilité.*

**CVE ID: CVE-2002-0597**Description: Le CVE-2002-0597 est une vulnérabilité de type déni de service qui affecte le serveur Apache Tomcat 3.3.1a jusqu'à la version 4.0.1. En exploitant cette faille, un attaquant distant peut provoquer un plantage du serveur, entraînant ainsi un impact de déni de service potentiel sur les utilisateurs légitimes.  
*Recommandation: La vulnérabilité CVE-2002-0597 est liée à un risque de déni de service sur les serveurs FTP. Pour la mitiger, assurez-vous de désactiver ou restreindre l'accès à la commande "SITE EXEC" sur le serveur FTP. Il est recommandé de mettre à jour le logiciel FTP vers une version corrigée pour éviter toute exploitation.*