

Rapport de Scan de Ports

Analyse de Sécurité Réseau

Informations Système

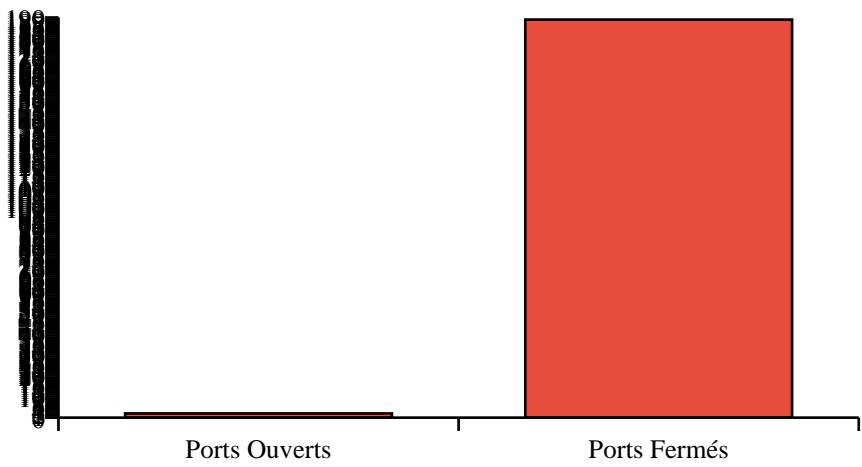
| | |
|--------------|---------------------|
| Système | Windows |
| Version | 11 |
| Architecture | AMD64 |
| Nom d'hôte | 404NotFound |
| Adresse IP | 10.21.1.160 |
| Date du scan | 17/06/2025 11:56:52 |

Paramètres du Scan

| | |
|----------------|-----------|
| Cible | 127.0.0.1 |
| Port de début | 10 |
| Port de fin | 200 |
| Plage de ports | 191 ports |

Résumé des Résultats

Résumé du Scan de Ports



| Statut | Nombre | Pourcentage | Niveau de Risque |
|---------------|--------|-------------|------------------|
| Ports Ouverts | 2 | 1.0% | Élevé |
| Ports Fermés | 189 | 99.0% | Faible |

Détails des Ports Ouverts

Description

Les ports ouverts représentent des points d'entrée potentiels pour les attaquants. Chaque port ouvert doit être analysé et sécurisé.

| Port | Service Commun | Niveau de Risque | Recommandation |
|------|----------------|------------------|-------------------------|
| 22 | SSH | Moyen | Utiliser des clés SSH |
| 135 | MSRPC | Élevé | Restreindre l'accès RPC |

Recommandations Détaillées

Sécurité des Ports

- Fermer tous les ports non essentiels
- Utiliser un pare-feu pour filtrer le trafic
- Mettre en place des règles de filtrage strictes

Surveillance

- Mettre en place une surveillance continue des ports
- Configurer des alertes pour les nouveaux ports ouverts
- Analyser régulièrement les logs de connexion

Bonnes Pratiques

- Maintenir les services à jour
- Utiliser des protocoles sécurisés (HTTPS, SFTP, etc.)
- Implémenter une politique de sécurité stricte

Documentation

- Documenter tous les ports ouverts

- Maintenir un inventaire des services
- Créer des procédures de réponse aux incidents

Ce rapport a été généré automatiquement par l'outil de scan de ports

Date de génération : 17/06/2025 11:56:52