Rapport d'Analyse Réseau

Analyse de Sécurité Réseau Détaillée

Informations Système

Système	Windows
Version	11
Architecture	AMD64
Nom d'hôte	404NotFound
Adresse IP	10.21.1.160
Date du scan	17/06/2025 11:14:48

Équipe de Développement

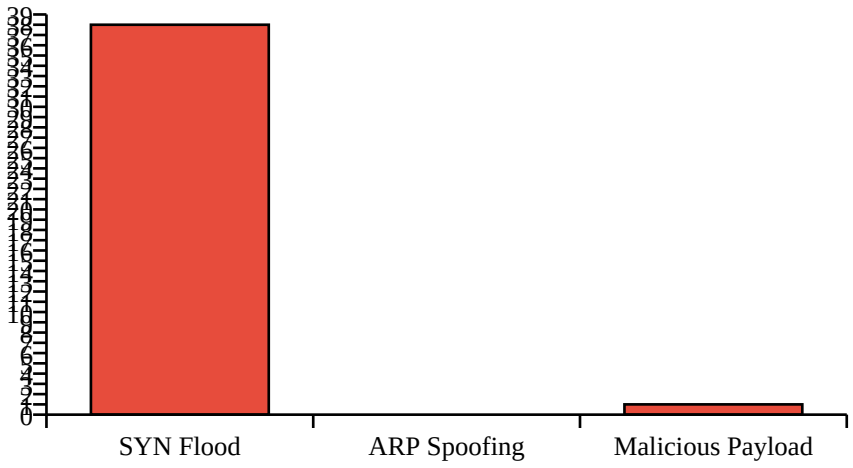
• Florian - Expert en Sécurité Réseau

• Yoann - Spécialiste en Analyse de Trafic

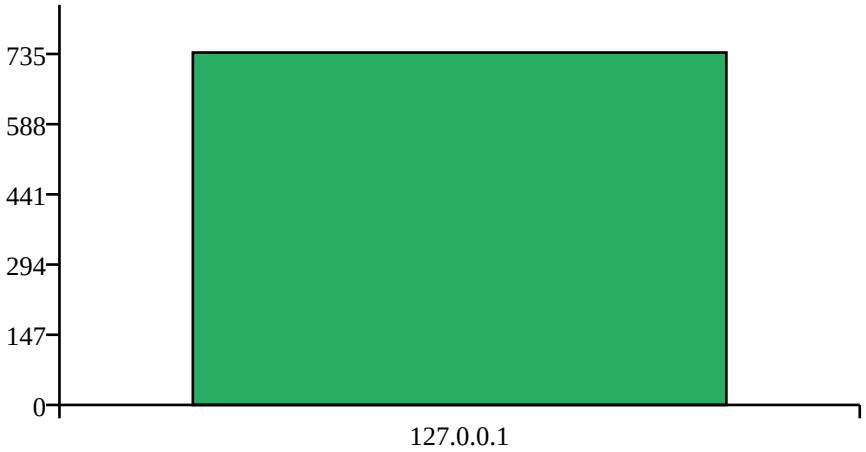
• Quentin - Développeur Full-Stack

Résumé des Détections

Résumé des Détections Réseau



Trafic par Adresse IP



Type de Détection	Nombre Détecté	Niveau de Risque	Impact Potentiel
SYN Flood	38	Élevé	Déni de Service
ARP Spoofing	0	Faible	Man in the Middle
Malicious Payload	1	Moyen	Exécution de Code

Détections SYN Flood

Description

Une attaque SYN Flood est une forme d'attaque par déni de service qui exploite le processus de poignée de main TCP à trois voies.

Nombre d'attaques SYN Flood détectées : 38

Impact :

• Surcharge des ressources du serveur

• Indisponibilité du service

• Perte de connectivité réseau

Détections ARP Spoofing

■ Aucune attaque ARP Spoofing détectée

Détections de Payloads Malveillants

Description

Les payloads malveillants sont des données ou du code conçus pour exploiter des vulnérabilités ou exécuter des actions non autorisées.

IP	Type de Payload	Niveau de Risque	Recommandation
127.0.0.1	b'malicious'	Moyen	Analyser et bloquer le trafic suspe

Analyse du Trafic Réseau

Statistiques de Trafic par IP

Adresse IP	Nombre de Paquets	Niveau de Trafic
127.0.0.1	738	Élevé

Recommandations Détaillées

Protection contre les SYN Flood

• Configurer un pare-feu pour limiter le nombre de connexions SYN

• Implémenter la protection SYN cookies

• Utiliser des systèmes de détection d'intrusion (IDS)

Protection contre l'ARP Spoofing

• Activer la détection d'ARP Spoofing sur les switches

• Utiliser des tables ARP statiques pour les équipements critiques

• Implémenter des outils de surveillance ARP

Gestion des Payloads Malveillants

• Mettre en place un système de filtrage de paquets

• Utiliser un IDS/IPS pour détecter les payloads malveillants

• Analyser régulièrement les logs de trafic

Surveillance du Trafic

• Mettre en place une surveillance continue du trafic réseau

• Définir des seuils d'alerte pour le trafic anormal

• Utiliser des outils d'analyse de trafic en temps réel

Sécurité Générale

- Mettre à jour régulièrement les équipements réseau
- Segmenter le réseau en zones de sécurité
- Implémenter une politique de sécurité réseau stricte

Ce rapport a été généré automatiquement par l'outil d'analyse réseau

Date de génération : 17/06/2025 11:14:48