

# Neteye

Un scanner réseau puissant programmé en  
Rust

Lien :  
<https://github.com/DanielaCe18/NetEye.git>

Réalisé par : Daniela Ceraku



# PLAN

01

Présentation Projet

02

Problématique

03

Fonctionnalités

04

Conception

05

Démonstration

06

Perspectives



# PRÉSENTATION PROJET

- Définition: Neteye est un scanner de ports TCP/UDP multi-thread et un utilitaire de détection de services intégré à Shodan, écrit entièrement en Rust.
- Public cible: Professionnels de la sécurité réseau et pentesteurs.
- Objectif: Offrir un outil de reconnaissance réseau puissant et flexible.



# CAS D'USAGE

**01** Préparation aux certifications: Utilisé pour préparer les certifications en sécurité réseau telles que CEH (Certified Ethical Hacker) ou OSCP (Offensive Security Certified Professional), en fournissant une pratique réelle des techniques de scan de ports.

**02** Pentesting: Effectuer des tests de pénétration pour identifier les vulnérabilités sur les réseaux cibles, aidant ainsi à renforcer la sécurité des systèmes avant qu'ils ne soient exploités par des attaquants malveillants.

**03** Exercices d'audit: Réaliser des audits de sécurité pour des entreprises ou des réseaux, permettant de fournir des rapports détaillés sur l'état de la sécurité et des recommandations pour améliorer les défenses.

# FONCTIONNALITÉS

## flexibilité

Fonctionne sur Windows et Unix, offrant une grande flexibilité dans différents environnements.

## TCP,UDP

Prise en charge des protocoles TCP et UDP, permettant des scans complets et variés.

## multi-thread

Support multi-thread pour des opérations de scan rapides et efficaces.

## Sauvegarde

Sauvegarde des résultats de scan dans un fichier pour une analyse ultérieure.

## Shodan

Intégration avec Shodan pour des capacités de scan enrichies, permettant de tirer parti de la base de données de Shodan pour des analyses plus approfondies.

## Informations

Informations détaillées sur les versions des services détectés. Vérification de la portée (Ping check) pour identifier rapidement les cibles accessibles.

# AVANTAGES



Rapidité et efficacité grâce à la prise en charge multi-thread et aux délais de timeout configurables.



Polyvalence grâce à la prise en charge multi-protocole (TCP et UDP) et aux nombreuses options de scan.



Intégration enrichie avec Shodan pour des capacités de reconnaissance réseau avancées.

# OPTIONS

- h, --help:** Affiche les informations d'aide pour comprendre l'utilisation de chaque option.
- a, --address <adresse>:** Spécifie l'adresse IP ou le nom d'hôte à scanner (par défaut : 127.0.0.1).
- T, --tcp:** Active le scan des ports TCP, essentiel pour la plupart des analyses réseau.
- U, --udp:** Active le scan des ports UDP, utile pour détecter des services spécifiques comme DNS.
- s, --startPort <port-début>:** Définit le port de départ du scan (par défaut : 1).
- e, --endPort <port-fin>:** Définit le port de fin du scan (par défaut : 65535).
- i, --inspect:** Inspecte les ports ouverts en détail pour obtenir plus d'informations sur les services.
- o, --output <fichier>:** Spécifie le fichier de sortie pour sauvegarder les résultats, facilitant l'analyse post-scan.
- p, --ping-check:** Effectue une vérification de portée pour identifier les hôtes accessibles.
- S, --shodan:** Utilise Shodan pour scanner une adresse publique, tirant parti de la puissance de Shodan pour une analyse approfondie.
- j, --threads <nombre>:** Définit le nombre de threads à utiliser pour le scan, permettant de gérer la charge et la vitesse du scan.
- t, --timeout <timeout>:** Définit le délai d'attente pour chaque vérification de port (par défaut : 3000 ms).
- v, --verbose:** Affiche des détails supplémentaires sur le processus de scan, utile pour le débogage et l'analyse détaillée.



# REVUE DU CODE ET DÉMONSTRATION



# CONCLUSION

## Perspectives

Améliorations potentielles de la vitesse de scan.  
Intégration avec d'autres outils de sécurité.

---

## Limitations

Performances comparées à Nmap et Shodan: Bien que Neteye soit très performant, il n'atteint pas encore le niveau de puissance et de fonctionnalités offertes par des outils établis comme Nmap ou le service Shodan.

# Merci de votre attention

Daniela Ceraku

<https://github.com/DanielaCe18/NetEye.git>

