Institut Supérieur d'Informatique

DAKAR

Département Réseaux et Systèmes

Classe : M1 SSIM

Module : Cryptologie

Prof : DR. KHALIFA

Rapport d'Analyse et de Surveillance Réseau avec NTOPNG, Nessus

Réalisé par :

Khadim Rassoul THIAM

Khadim MBAYE

Mamadou DIENG

Année Académique 2024 - 2025

SOMMAIRE

Introduction

La cybersécurité et la surveillance réseau sont des éléments essentiels pour garantir l'intégrité, la disponibilité et la confidentialité des systèmes d'information. Dans ce rapport, nous explorons l'utilisation de **NTOPNG** pour la surveillance du trafic réseau et **Nessus** pour l'analyse des vulnérabilités. Ces outils permettent d'améliorer la visibilité et la sécurité d'un réseau informatique en identifiant les menaces et en optimisant les performances.

---

1. NTOPNG : Surveillance du Trafic Réseau

1.1 Présentation de NTOPNG

NTOPNG (Next-Generation Network Traffic Monitoring) est un outil avancé de surveillance du trafic réseau. Il permet d'afficher en temps réel les flux réseau, d'identifier les utilisateurs et de détecter d'éventuelles anomalies. Ses principales fonctionnalités incluent :

- La visualisation du trafic en temps réel.
- L'analyse des protocoles et des connexions.
- L'intégration avec d'autres outils comme Elasticsearch.
- La détection de comportements suspects sur le réseau.

1.2 Installation et Configuration

1.2.1 Pré-requis système

- Un serveur sous Linux (Ubuntu/Debian/CentOS) ou Windows.
- Une carte réseau configurée en mode promiscuité pour capturer le trafic.
- Accès administrateur pour l'installation.

1.2.2 Étapes d'installation sous Linux

1. **Mettre à jour le système**

```
sudo apt update && sudo apt upgrade -y
```

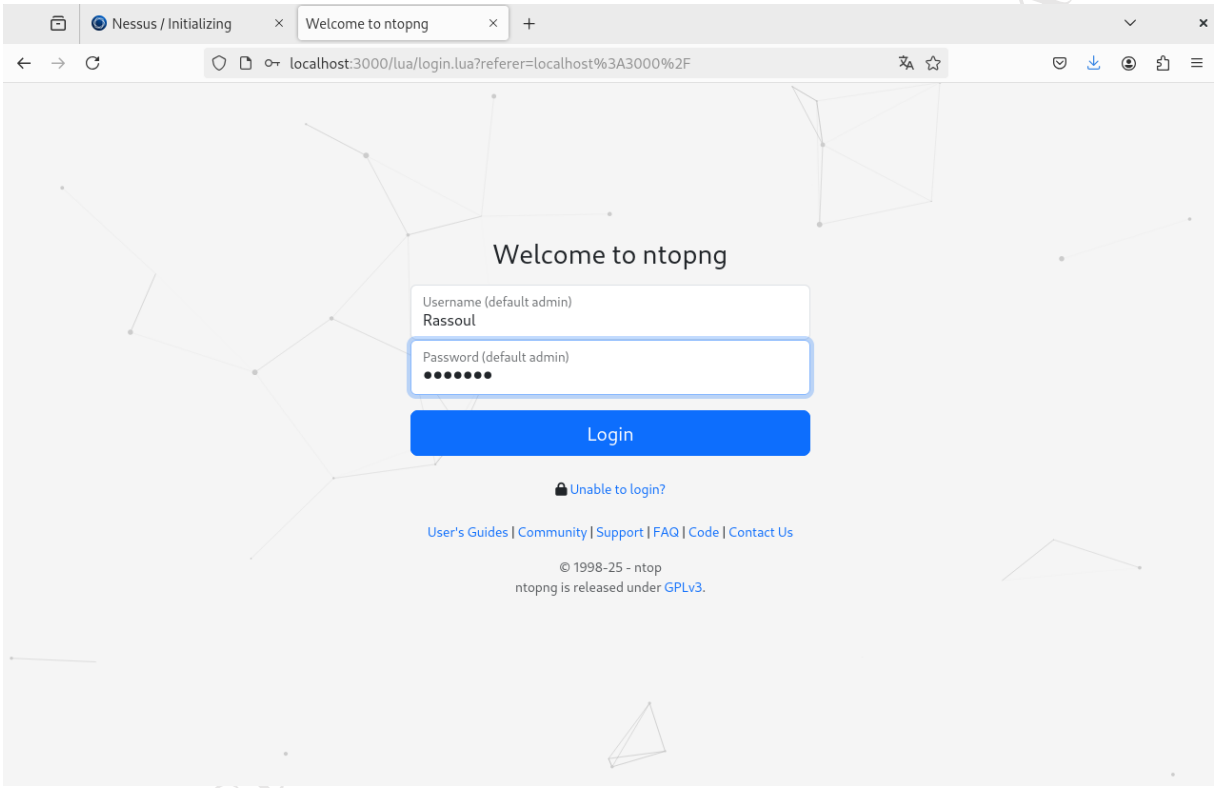
2. **Installer NTOPNG et ses dépendances**

```
sudo apt install ntopng -y
```

3. **Configurer NTOPNG** en éditant le fichier `/etc/ntopng/ntopng.conf`
4. **Démarrer le service**

```
sudo systemctl start ntopng
```

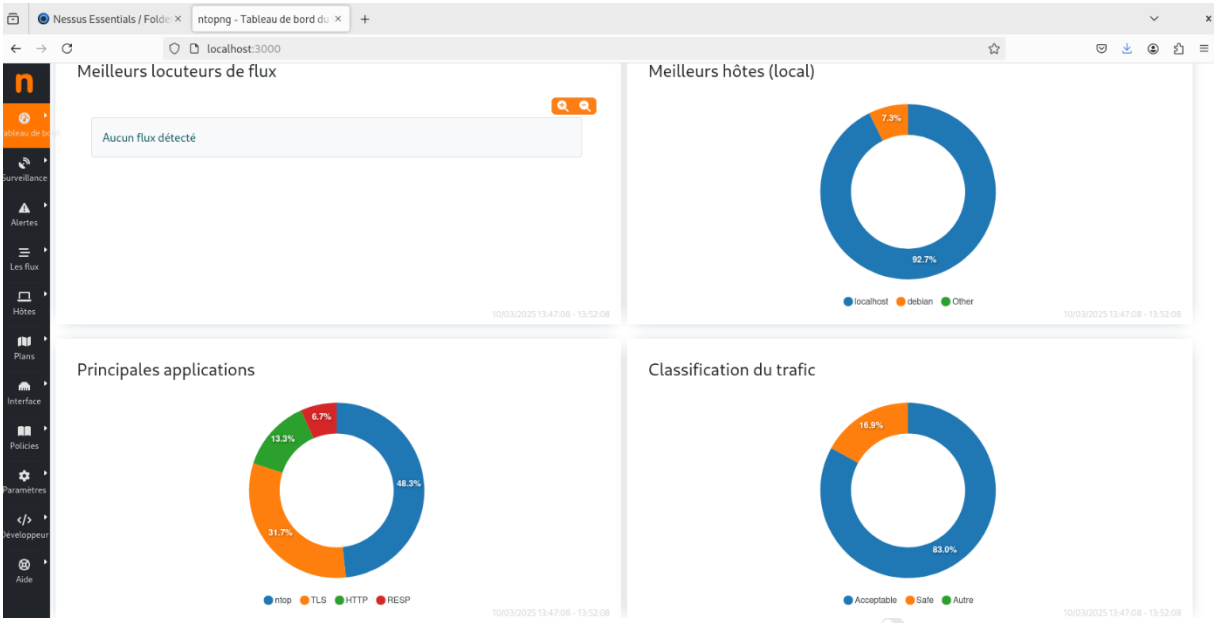
5. **Accéder à l'interface web** via `http://<IP_du_serveur>:3000`

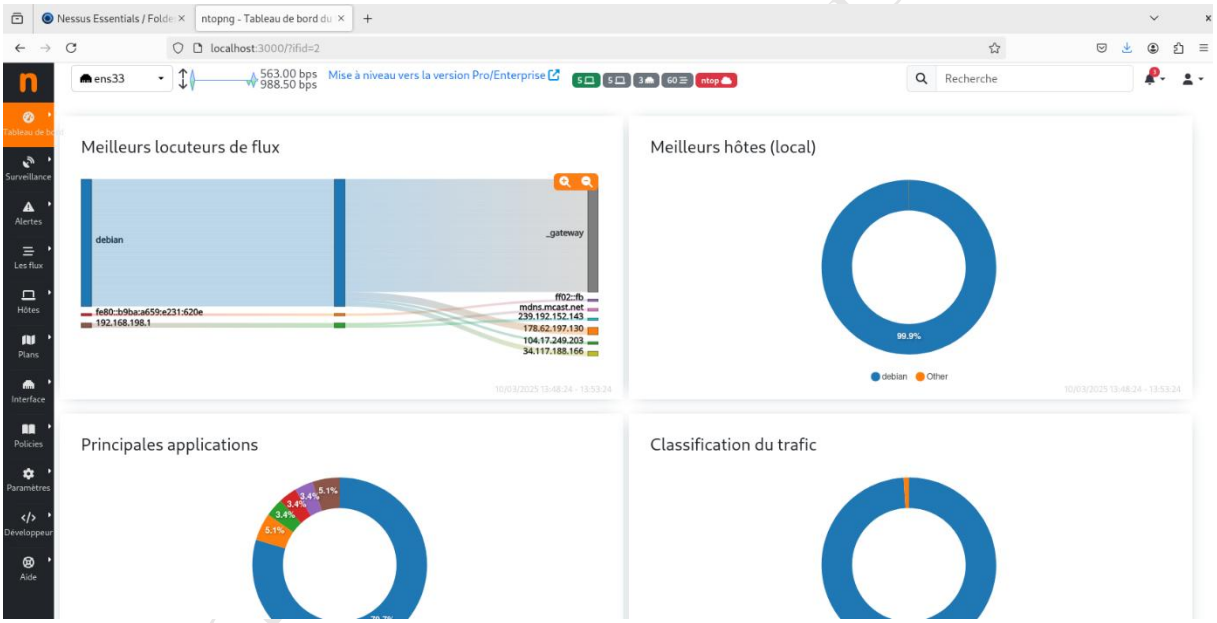


1.3 Analyse du trafic réseau

NTOPNG permet :

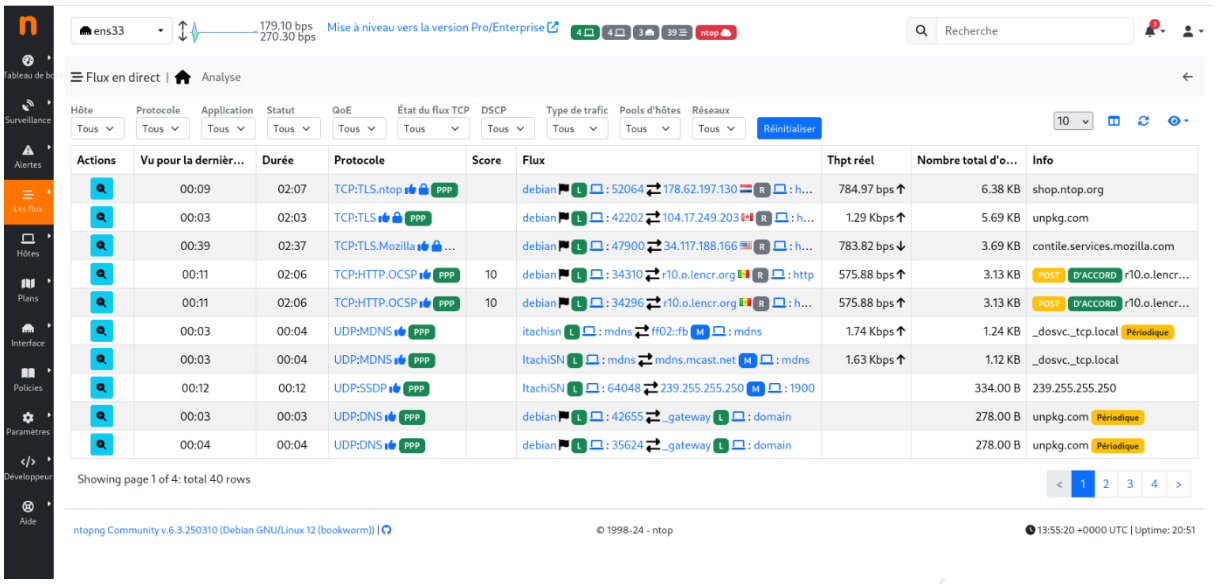
- **La surveillance en temps réel** des connexions actives.
- **L'identification des flux réseau** pour comprendre quels appareils consomment le plus de bande passante.
- **La détection des anomalies** en repérant des pics de trafic inhabituels ou des connexions suspectes.

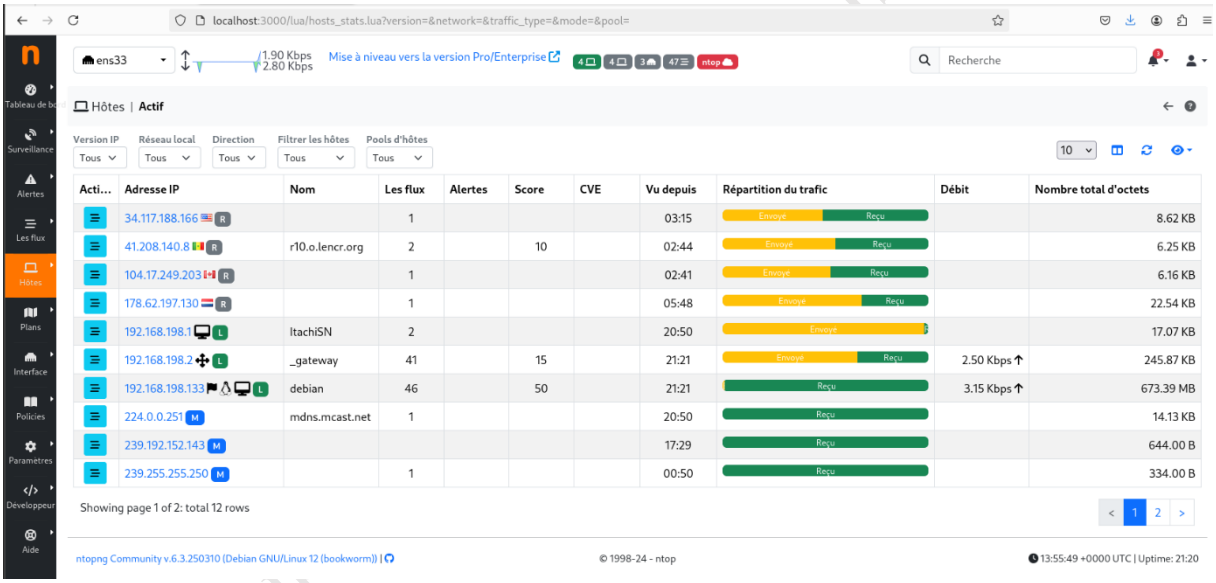




1.4 Cas d'utilisation et exemples

- **Optimisation du réseau** : identifier les applications gourmandes en bande passante.
- **Détection des menaces** : repérer un comportement anormal indiquant une attaque DDoS ou une exfiltration de données.
- **Audit des connexions** : suivre les accès des utilisateurs aux ressources critiques.





2. Nessus : Analyse des Vulnérabilités

2.1 Présentation de Nessus

Nessus est un scanner de vulnérabilités utilisé pour identifier les failles de sécurité sur un réseau ou un système. Il est développé par **Tenable** et est largement adopté dans l'industrie de la cybersécurité.

2.2 Installation et Configuration

2.2.1 Pré-requis système

- Un système sous Linux ou Windows.
- Un accès administrateur pour l'installation.
- Une connexion Internet pour les mises à jour de la base de vulnérabilités.

2.2.2 Étapes d'installation sous Linux

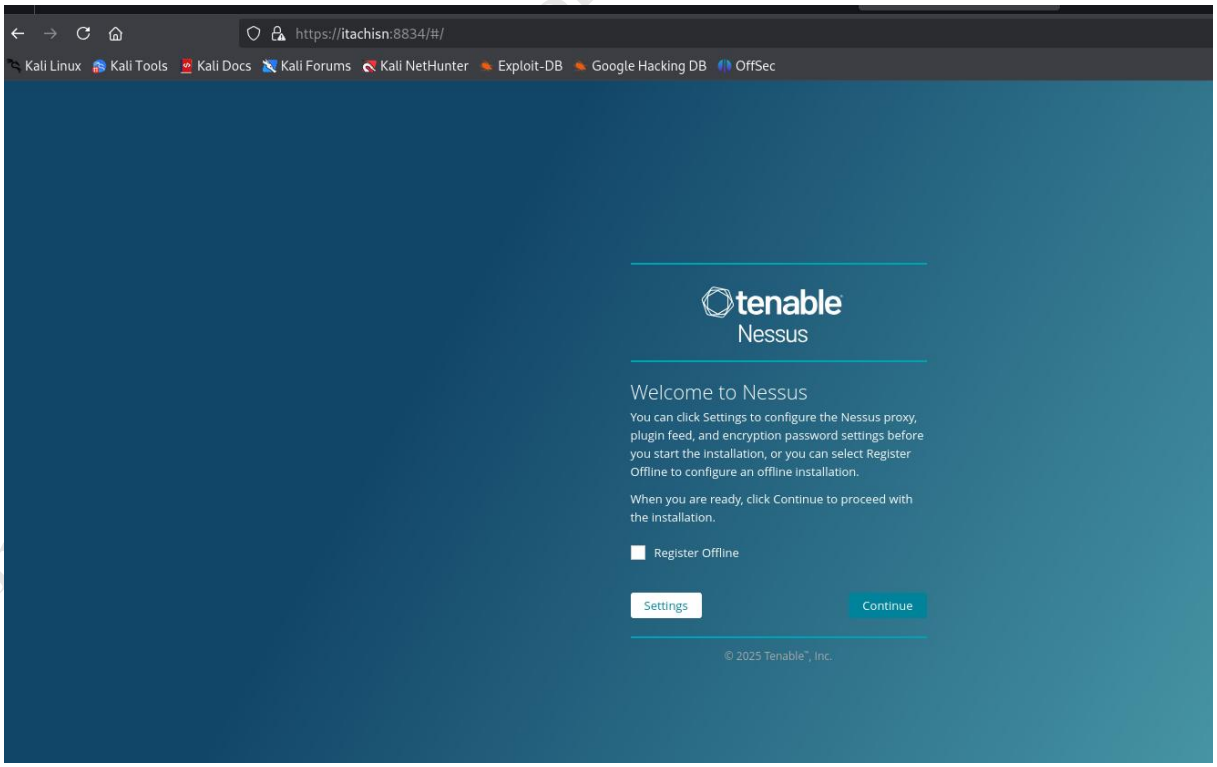
1. **Télécharger Nessus depuis le site officiel de Tenable**.
2. **Installer le package**

```
sudo dpkg -i Nessus-<version>.deb  # Debian/Ubuntu
sudo rpm -ivh Nessus-<version>.rpm  # CentOS/RHEL
```

3. **Démarrer le service**

```
sudo systemctl start nessusd
```

4. **Accéder à l'interface web** via `https://<IP_du_serveur>:8834`



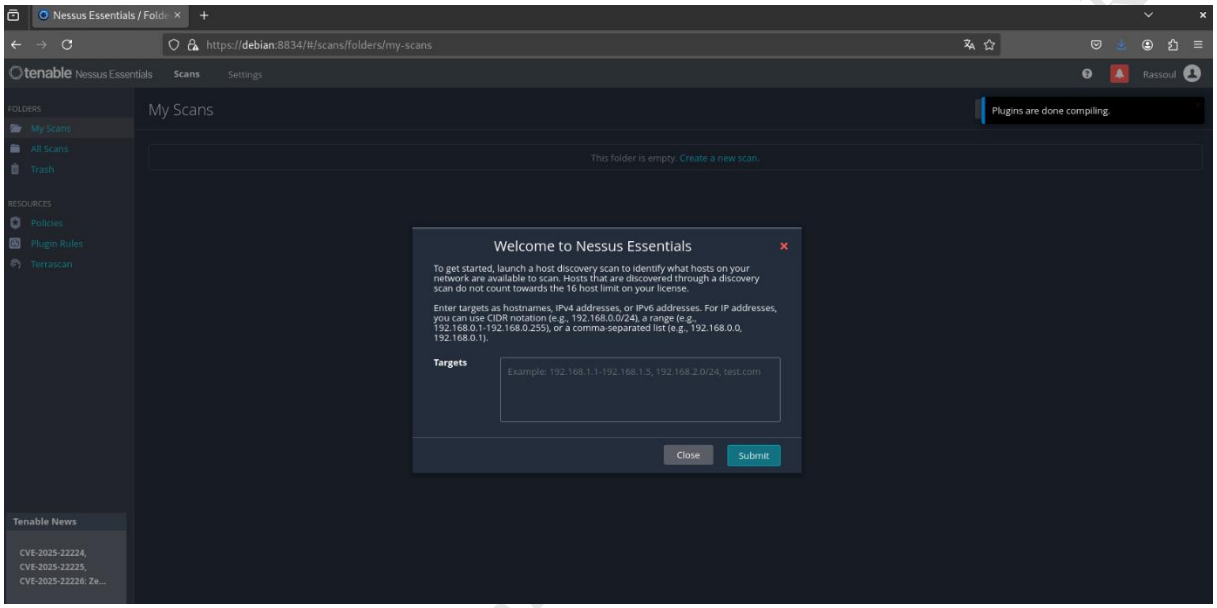
5. **Créer un compte et enregistrer Nessus** avec une licence.

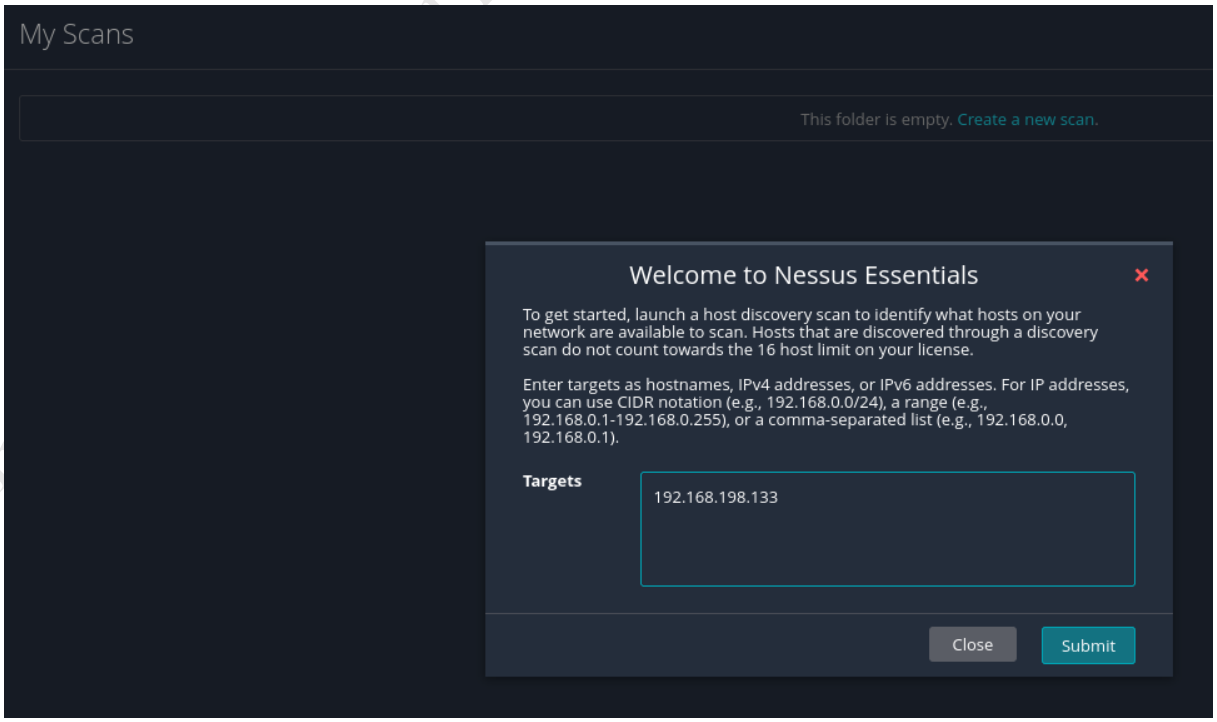
2.3 Détection des vulnérabilités

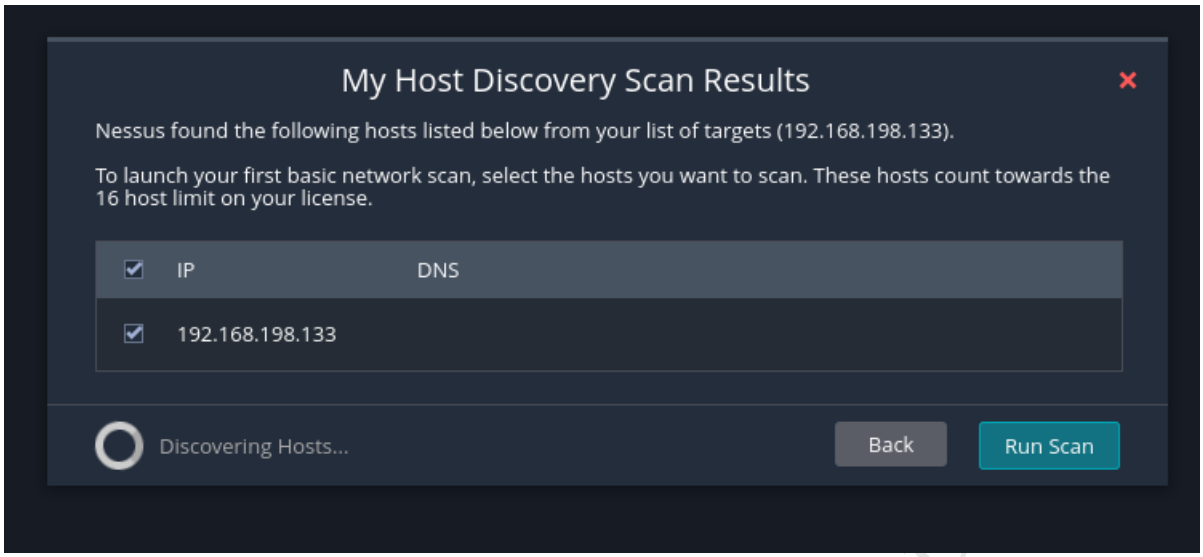
Nessus propose plusieurs types de scans :

- **Scan de vulnérabilités générales** : recherche des failles courantes.

On resigne l'hôte à scanner



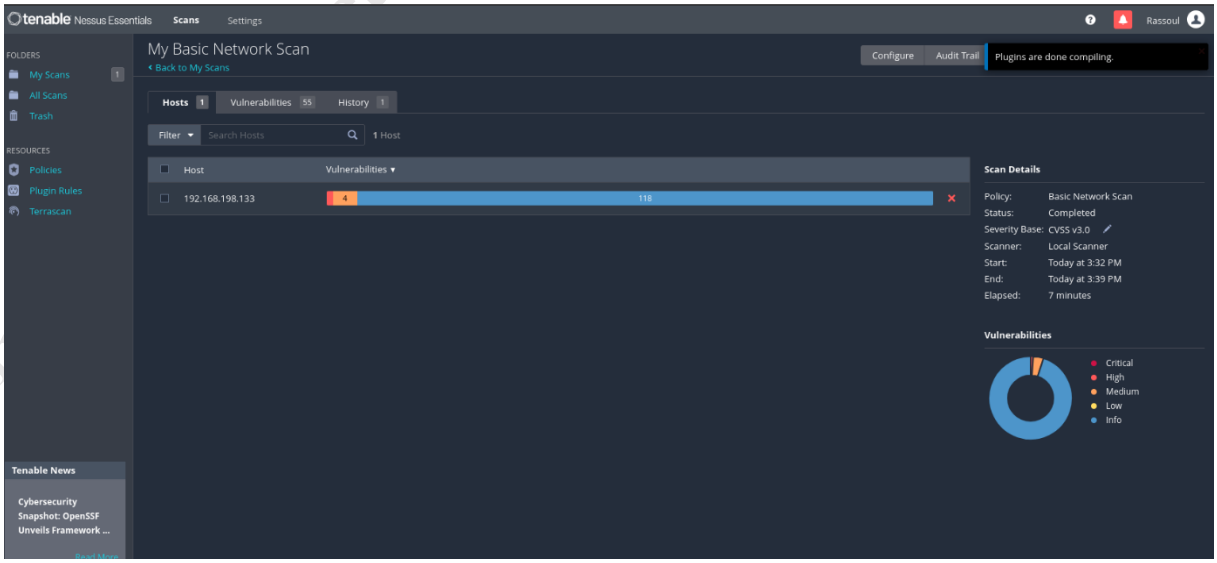


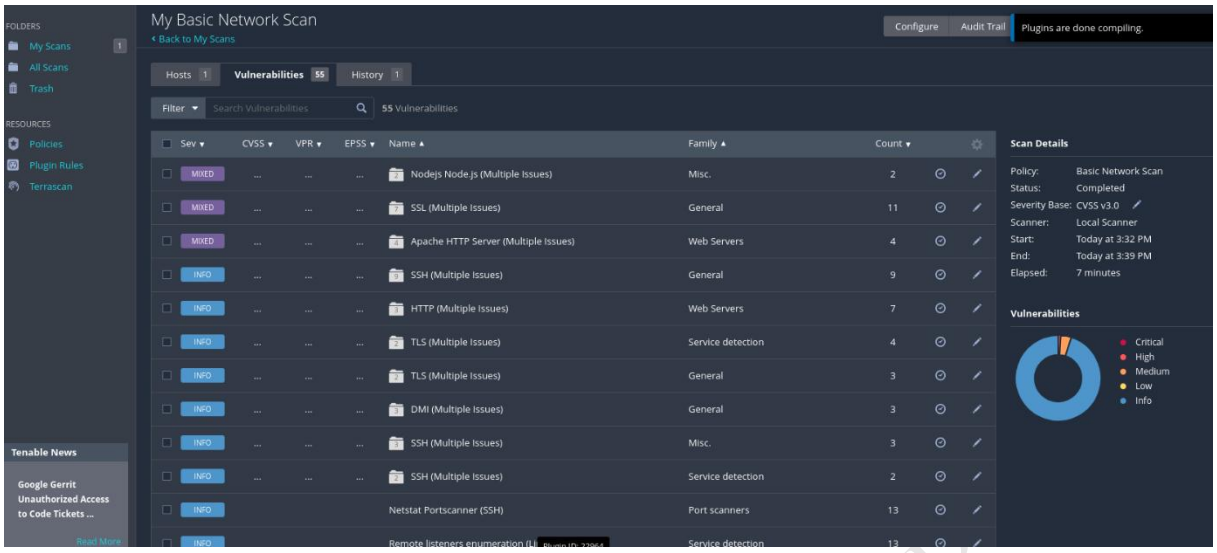


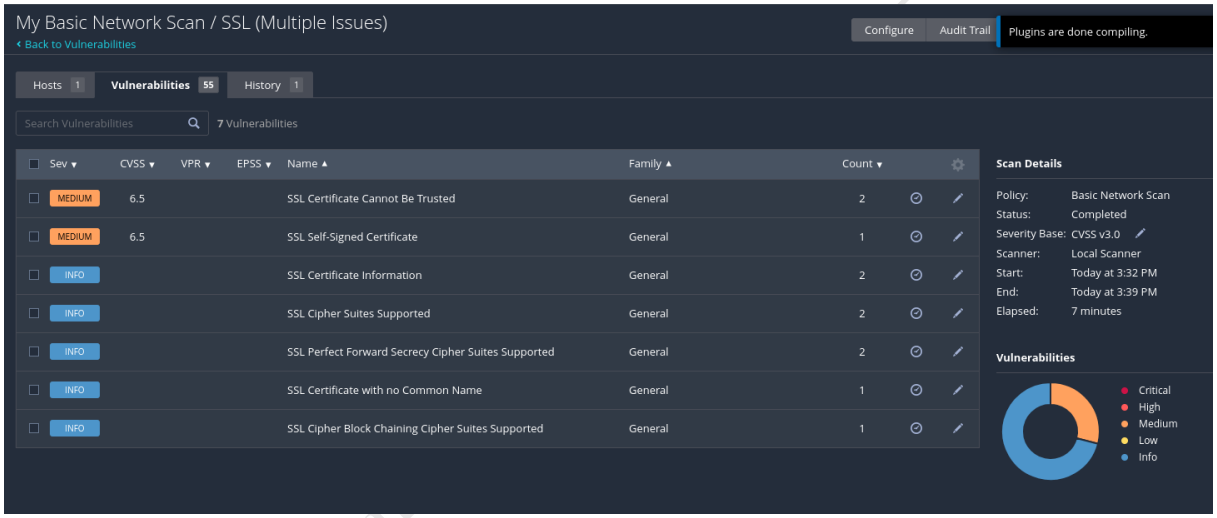
- **Scan des ports ouverts** : identification des services accessibles depuis l'extérieur.
- **Scan de configuration** : vérification des paramètres système pour détecter des mauvaises configurations.
- **Scan des correctifs manquants** : analyse des mises à jour de sécurité non appliquées.

Une fois un scan terminé, Nessus fournit un rapport détaillant :

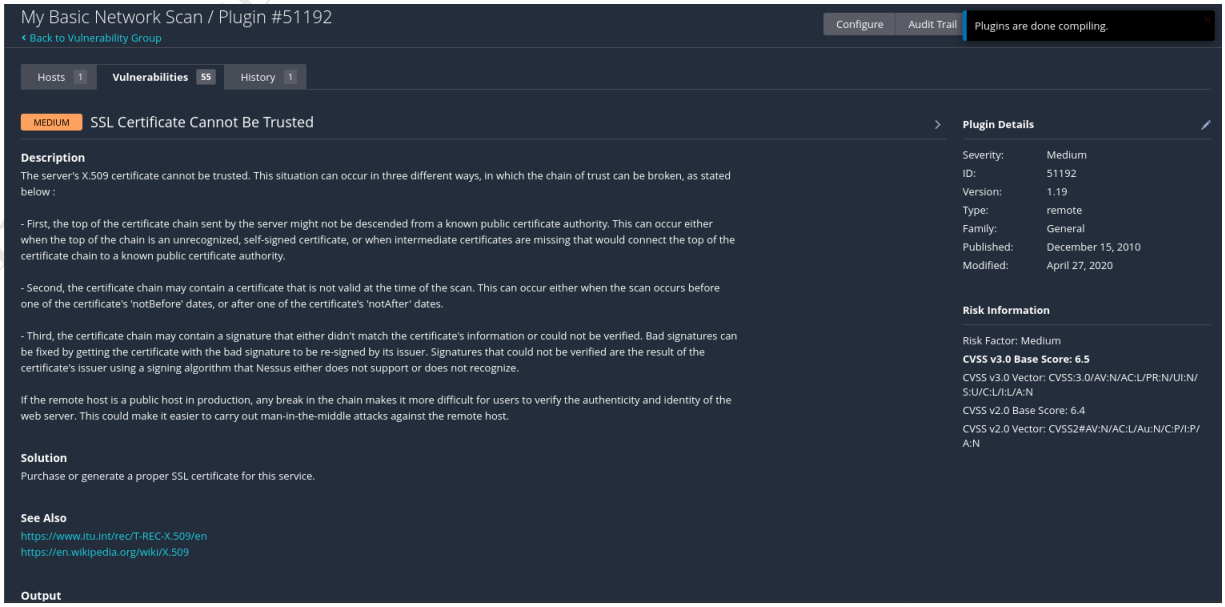
- **Les vulnérabilités critiques** avec des scores de sévérité.







- **Des recommandations** pour corriger les failles identifiées.



2.4 Cas d'utilisation et exemples

- **Audit de la sécurité d'un serveur** pour vérifier la présence de failles connues.
- **Test de conformité** pour s’assurer qu’un système respecte les bonnes pratiques de sécurité.
- **Simulation d’attaques** en identifiant les vecteurs d'exploitation possibles.

Conclusion

L'utilisation conjointe de **NTOPNG** et **Nessus** permet d'assurer une meilleure surveillance et sécurité du réseau. NTOPNG offre une visibilité en temps réel sur les activités réseau, tandis que Nessus identifie les vulnérabilités critiques nécessitant une remédiation. Ensemble, ces outils constituent une solution efficace pour protéger une infrastructure contre les menaces et optimiser ses performances.

Références

- Documentation officielle de NTOPNG : https://www.ntop.org/
- Documentation officielle de Nessus : https://www.tenable.com/products/nessus