# Rapport sur l‘installation et la configuration de Nessus sous Ubuntu et Window 10

Amadou SY
Etudiant en M1 SSIM
Ecole de formation : IZI

Sous la supervision de : Monsieur Lo

# Table des matières

# 1 Présentation de Nessus

## 1.1 Description générale

Nessus est une solution professionnelle d'analyse des vulnérabilités. Il permet de scanner des systèmes et des réseaux à la recherche de failles de sécurité. Il est développé par **Tenable** et est largement adopté dans l'industrie de la cybersécurité.

## 1.2 Fonctionnalités principales

- Scans de vulnérabilités
- Analyse des configurations
- Génération de rapports détaillés
- Recommandations pour corriger les failles

# 2 Installation et configuration

## 2.1 Prérequis système

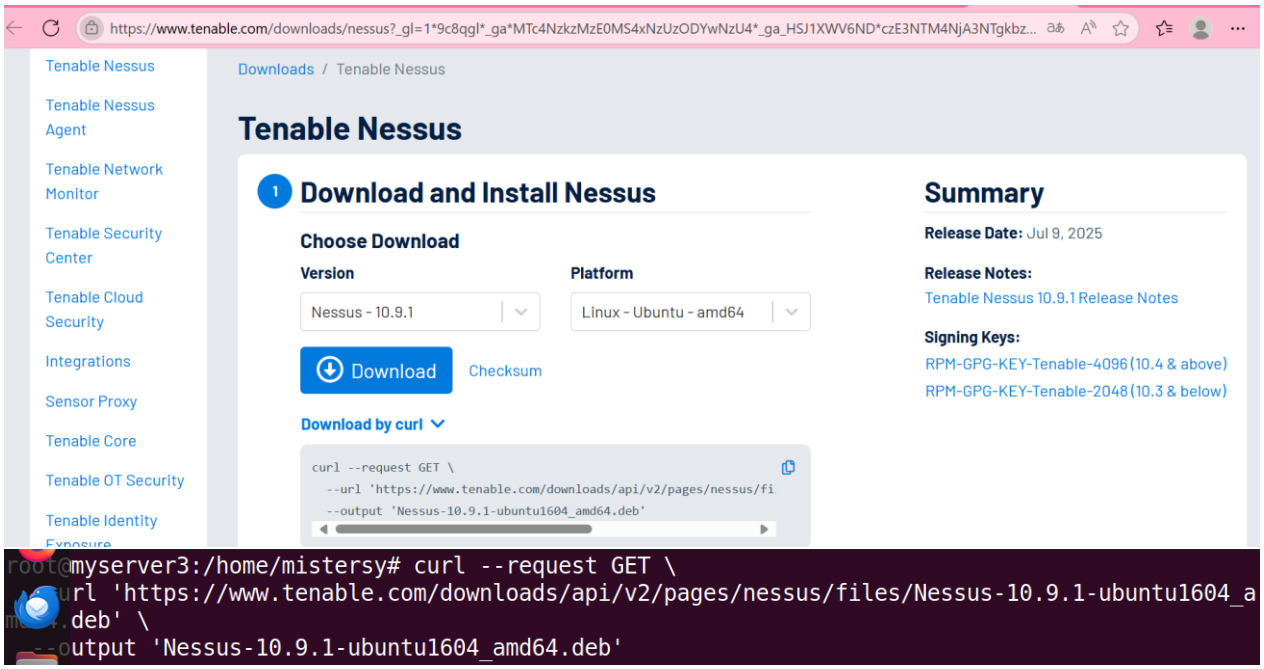
• Un système sous Linux ou Windows.

• Un accès administrateur pour l'installation.

• Une connexion Internet pour les mises à jour de la base de vulnérabilités.

## 2.2 Installation et configuration sous ubuntu

1. **Télécharger** Nessus depuis le site officiel de Tenable.




```
root@myserver3:/home/mistersy# curl --request GET \
  --url 'https://www.tenable.com/downloads/api/v2/pages/nessus/files/Nessus-10.9.1-ubuntu1604_a
md64.deb' \
  --output 'Nessus-10.9.1-ubuntu1604_amd64.deb'
```

2. **Installer le package téléchargé**

```
root@myserver3:/home/mistersy# dpkg -i Nessus-10.9.1-ubuntu1604_amd64.deb
```

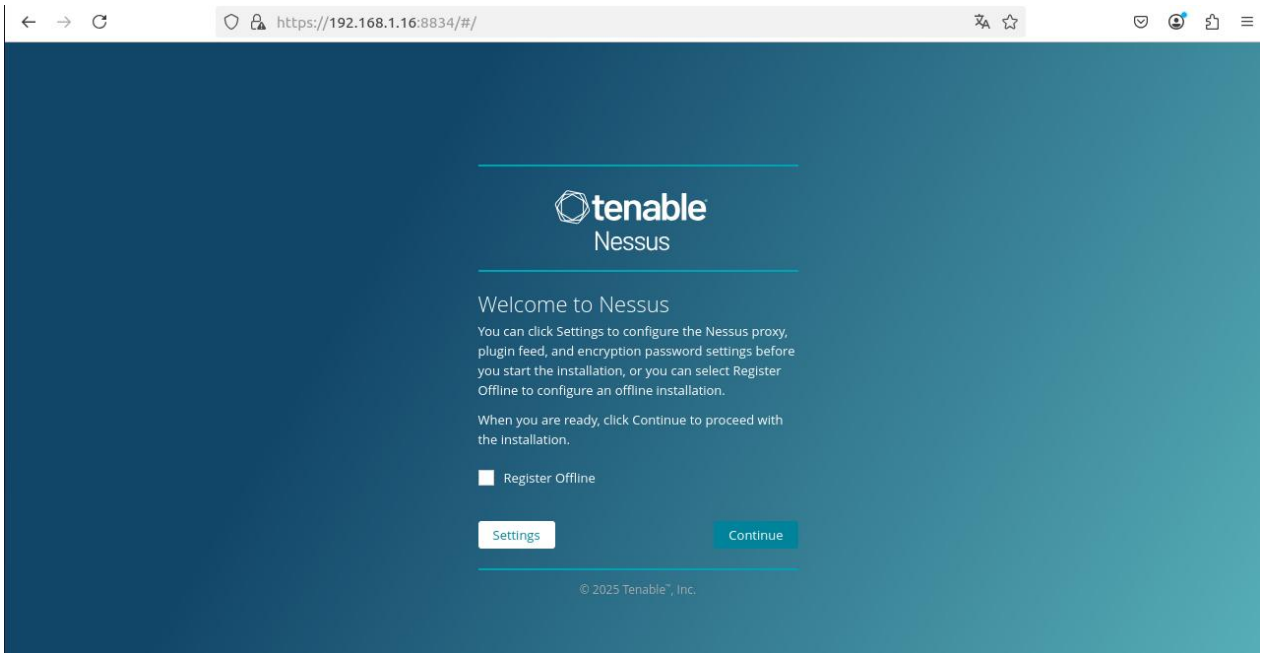
```
INSTALL PASSED
Unpacking Nessus Scanner Core Components...
Created symlink /etc/systemd/system/nessusd.service → /lib/systemd/system/nessusd.service.
Created symlink /etc/systemd/system/multi-user.target.wants/nessusd.service → /lib/systemd
/system/nessusd.service.

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://NESSUS_HOSTNAME_OR_IP:8834/ to configure your scanner

root@myserver3:/home/mistersy#
```

3. **Démarrer le service**

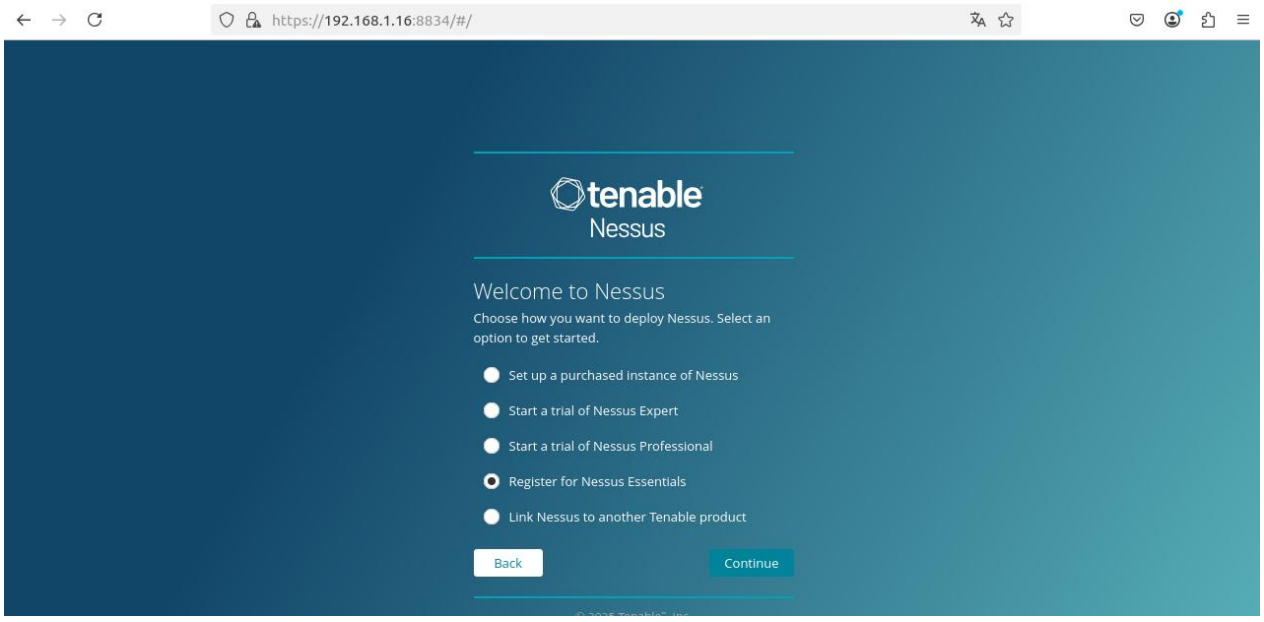
```
root@myserver3:/home/mistersy# systemctl start nessusd
```

```
root@myserver3:/home/mistersy# systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/lib/systemd/system/nessusd.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2025-07-30 08:13:49 GMT; 7s ago
   Main PID: 92927 (nessus-service)
      Tasks: 15 (limit: 4606)
     Memory: 57.1M
        CPU: 6.921s
     CGroup: /system.slice/nessusd.service
             ├─92927 /opt/nessus/sbin/nessus-service -q
             └─92928 nessusd -q
```

4. Accéder à l'interface de Nessus via le navigateur : [https://«ipduserveur»:8834](https://«ipduserveur»:8834)

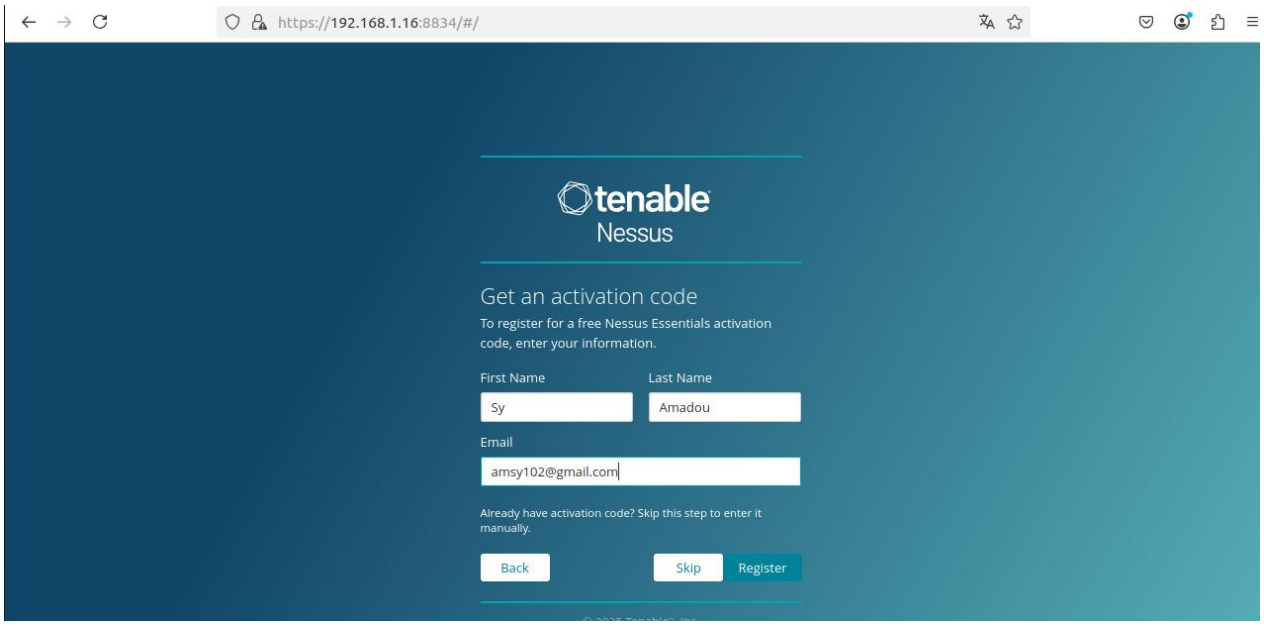


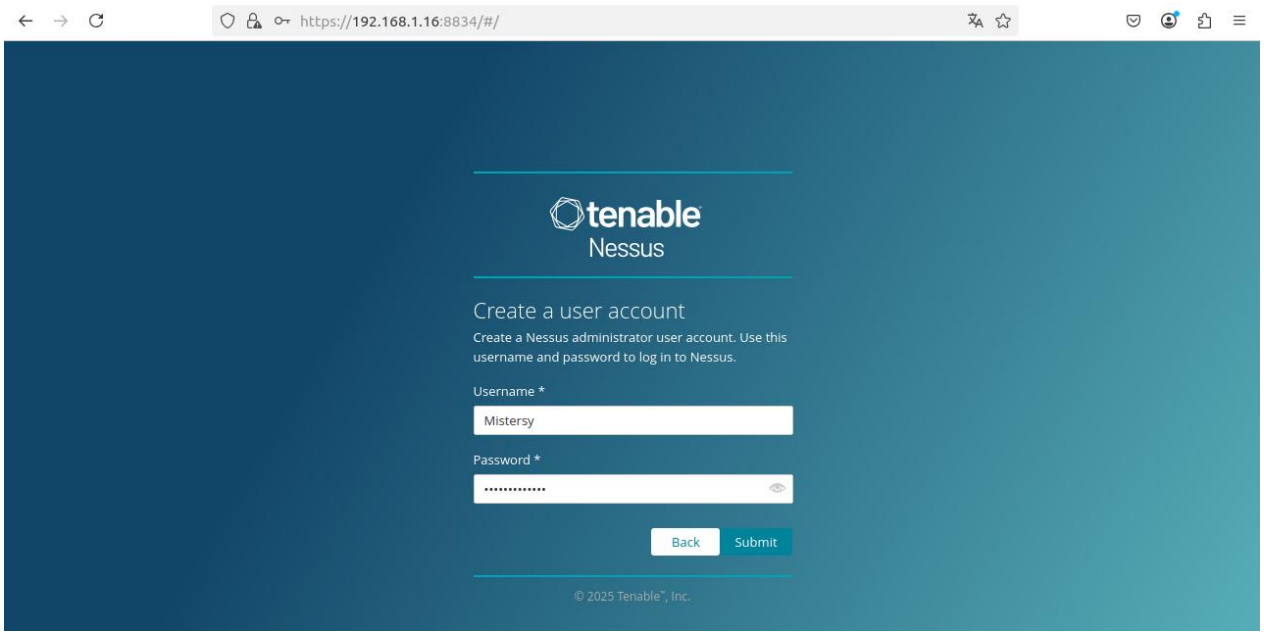

5. **Choisir Nessus Essentials (ou la version souhaitée )**



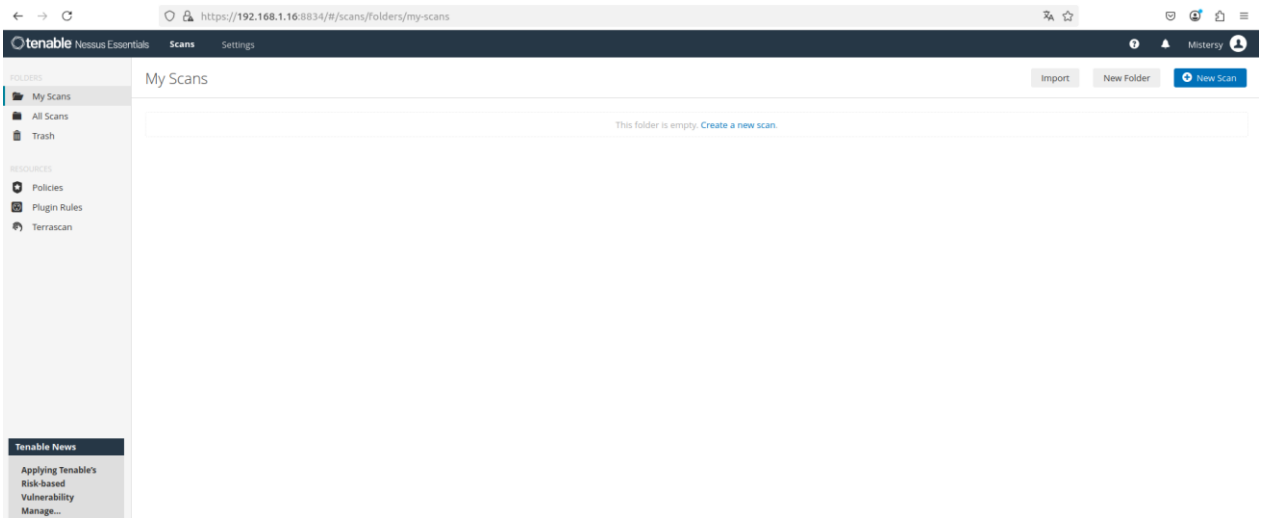

**Remarque :** Nessus Essentials est la version gratuite proposée par Tenable, limitée en nombre de cibles analysables.

6. **Créer un compte et enregistrer Nessus avec une clé de licence.**


https://192.168.1.16:8834/#/
tenable
Nessus
Get an activation code
To register for a free Nessus Essentials activation code, enter your information.
First Name
Sy
Last Name
Amadou
Email
amsy102@gmail.com
Already have activation code? Skip this step to enter it manually.
Back
Skip
Register

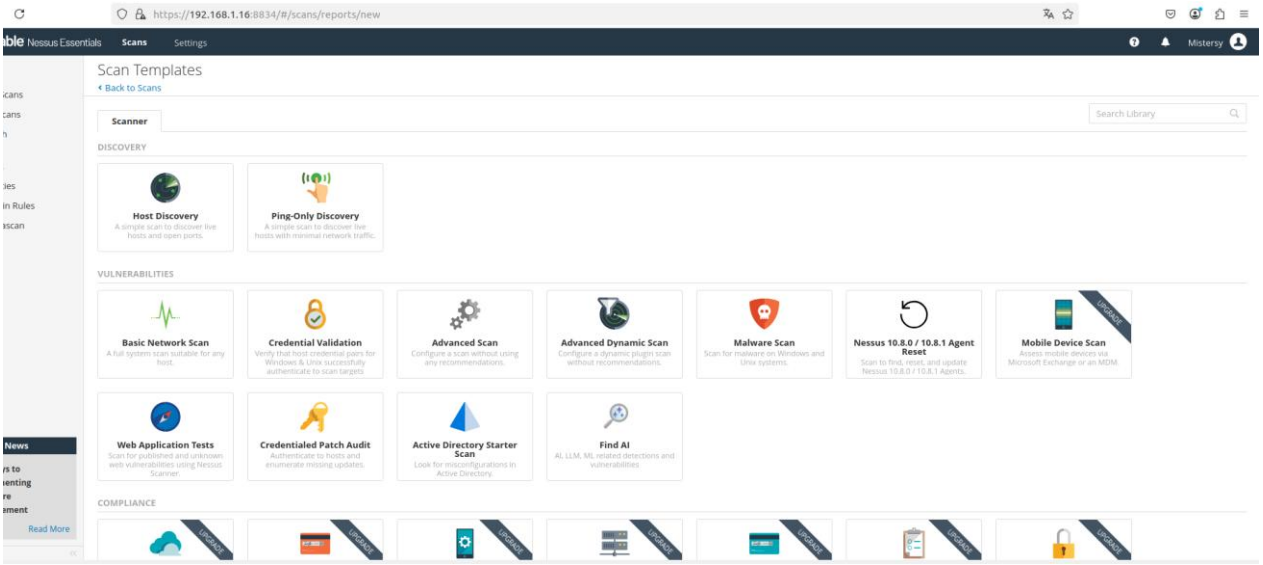

https://192.168.1.16:8834/#/
tenable
Nessus
Create a user account
Create a Nessus administrator user account. Use this username and password to log in to Nessus.
Username *
Mistersy
Password *
Back
Submit
© 2025 Tenable™, Inc.


Page d’accueil de Nessus :




## 2.3 Détection des vulnérabilités

Nessus propose plusieurs types de scans :

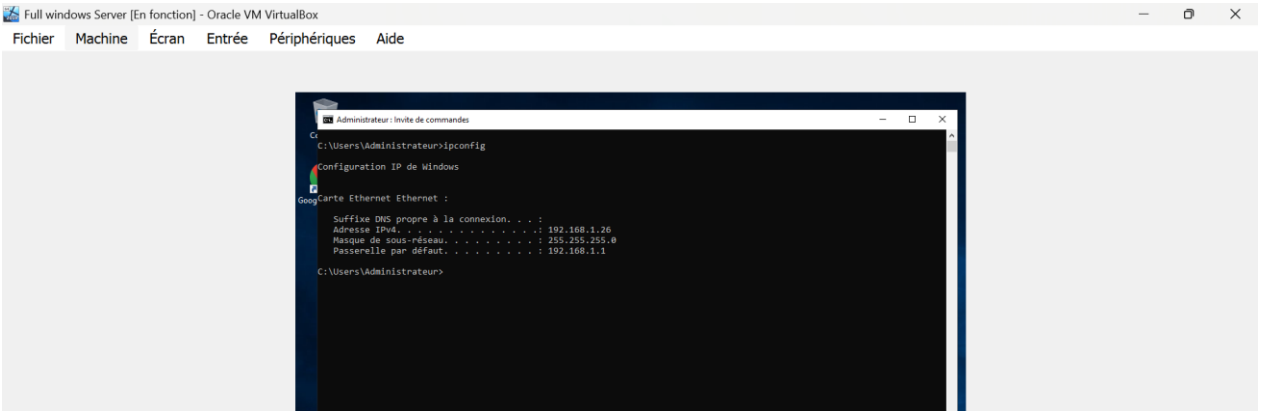


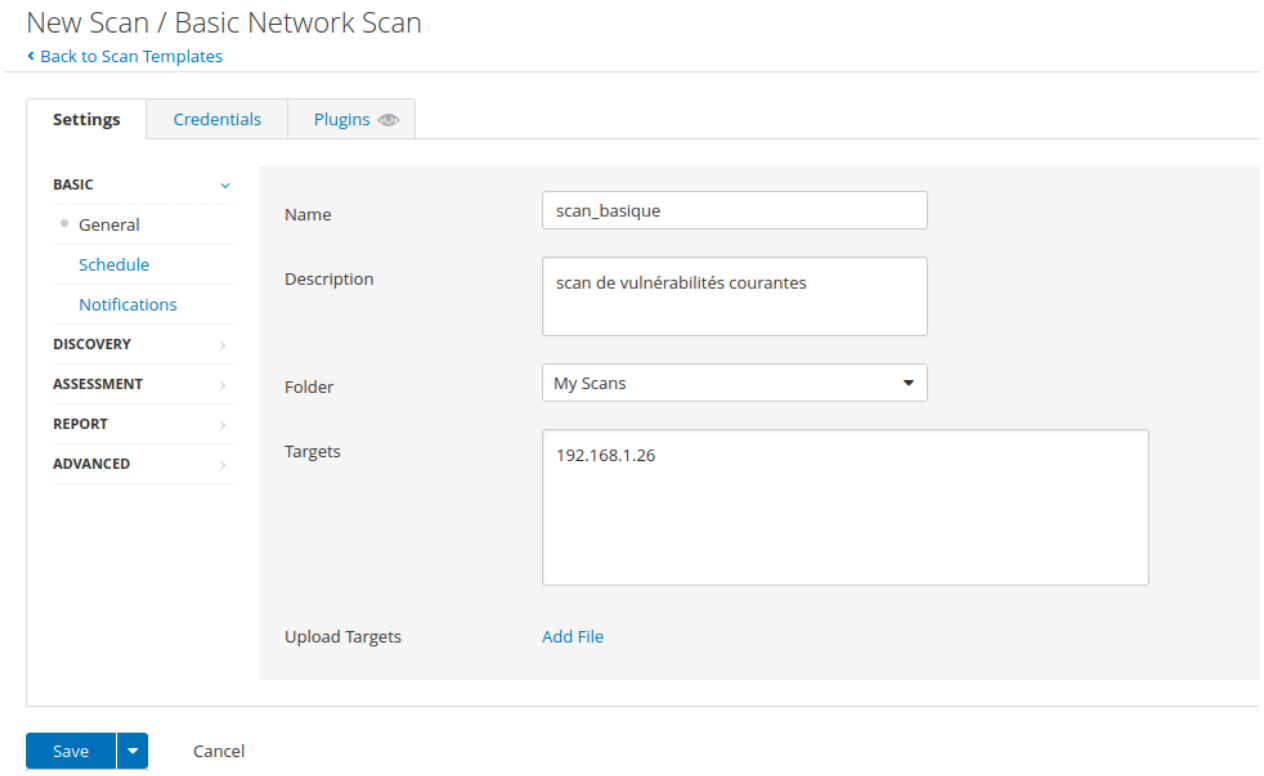

- **Scan de vulnérabilités générales**
- **Scan des ports ouverts :** identification des services accessibles depuis l'extérieur.
- **Scan de configuration :** vérification des paramètres système pour détecter des mauvaises configurations.
- **Scan des correctifs manquants :** analyse des mises à jour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

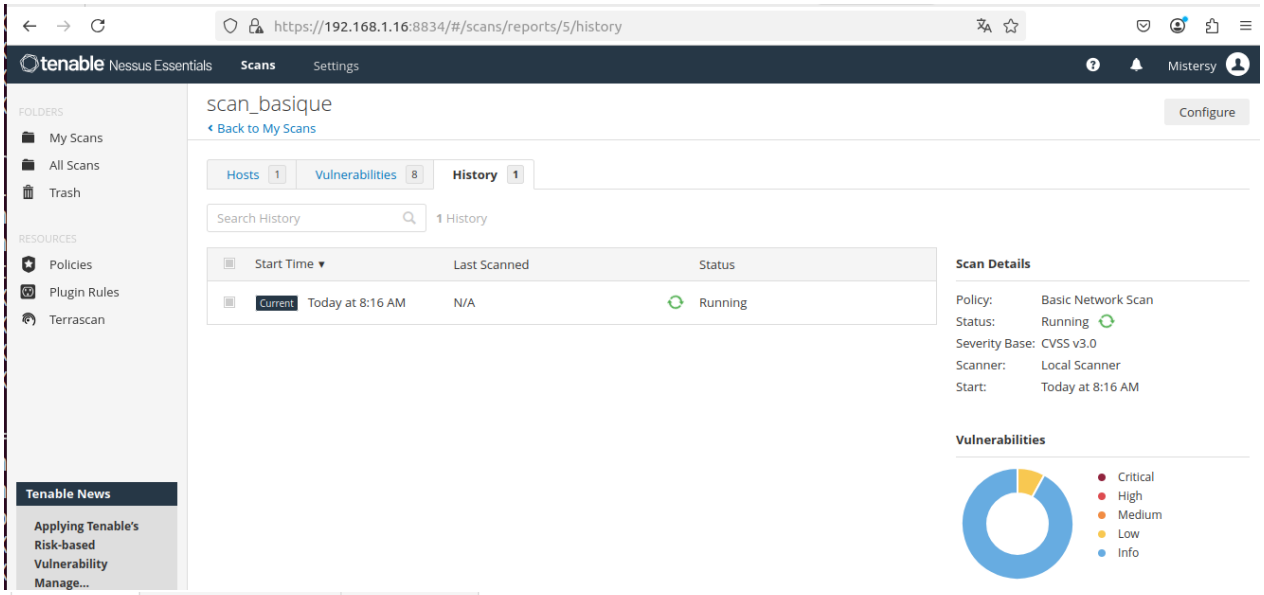
➢ **Exemple – Scan de vulnérabilités générales**

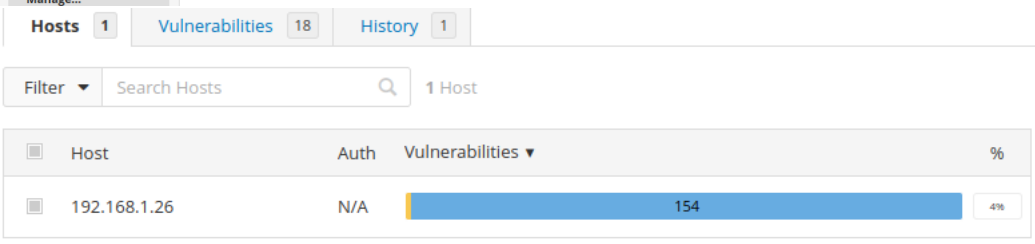
Ce scan a pour objectif d'identifier les failles de sécurité courantes présentes sur le système. Il permet de détecter les services exposés, les configurations faibles ou les vulnérabilités connues susceptibles d'être exploitées par un attaquant.

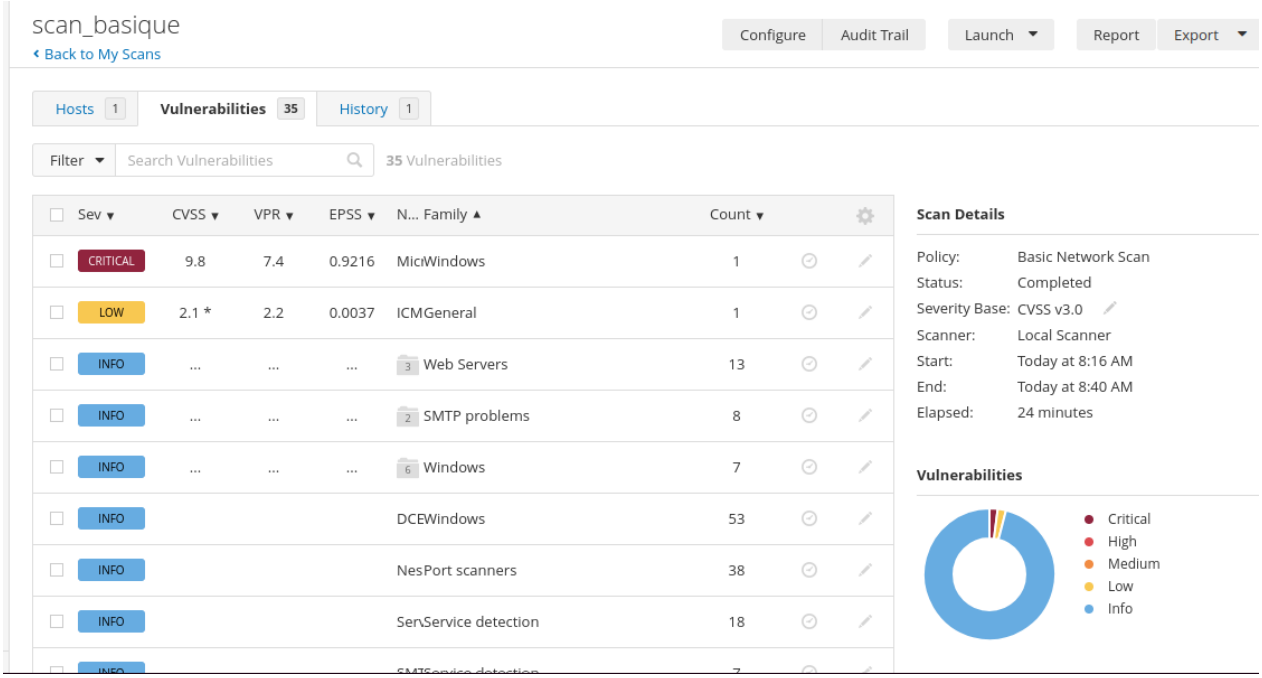
- Cible: Windows Server 2019 – IP : 192.168.1.26




New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
scan_basique
Description
scan de vulnérabilités courantes
Folder
My Scans
Targets
192.168.1.26
Upload Targets
Add File
Save
Cancel


https://192.168.1.16:8834/#/scans/reports/5/history
tenable Nessus Essentials
Scans
Settings
Mistersy
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Applying Tenable's Risk-based Vulnerability Manage...
scan_basique
Back to My Scans
Configure
Hosts 1
Vulnerabilities 8
History 1
Search History
1 History
Start Time
Last Scanned
Status
Current
Today at 8:16 AM
N/A
Running
Scan Details
Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 8:16 AM
Vulnerabilities
Critical
High
Medium
Low
Info


Hosts 1
Vulnerabilities 18
History 1
Filter
Search Hosts
1 Host
Host
Auth
Vulnerabilities
%
192.168.1.26
N/A
154
4%




**Résultats :**

Au total, **35 vulnérabilités** ont été identifiées, réparties comme suit :

- **1 vulnérabilité critique (CRITICAL)** avec un **score CVSS de 9.8**, ce qui représente un **risque majeur** pour la sécurité du système. Cette vulnérabilité appartient à la famille **MicWindows**.
- **1 vulnérabilité de type faible (LOW)**, avec un **score CVSS de 2.1**, liée à l'exposition de l'horodatage ICMP.
- **33 vulnérabilités informatives (INFO)**, qui ne représentent pas un danger direct, mais indiquent la présence de services exposés ou de configurations réseau visibles (ex. : services HTTP, SMTP, SMB, DCE, etc.).

**Indicateurs de risque complémentaires :**

- La vulnérabilité critique affiche un **VPR (Vulnerability Priority Rating) de 7.4** et un **EPSS (Exploit Prediction Scoring System) de 0.9216**, ce qui traduit une **probabilité élevée d'exploitation réelle**.
- La vulnérabilité faible a un VPR de 2.2 et un EPSS très bas de 0.0037, indiquant un faible niveau de priorité.

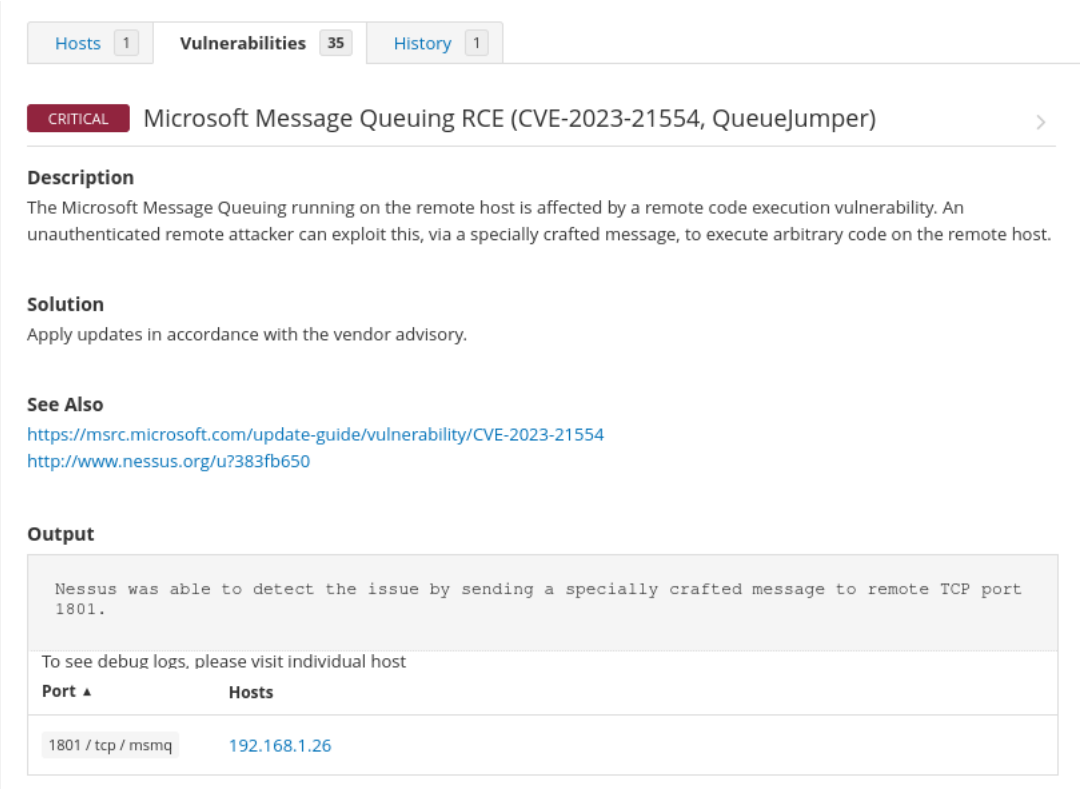
**Représentation graphique :**

Le graphique circulaire situé à droite de la capture montre visuellement que l'environnement présente **majoritairement des vulnérabilités informatives**. Toutefois, la présence d'une **vulnérabilité critique** nécessite une **action immédiate**.

**Remarque :**

Le **score CVSS** (Common Vulnerability Scoring System) est un **système standardisé** utilisé pour évaluer la **gravité des vulnérabilités de sécurité informatique**. Il attribue un score numérique allant de **0 à 10**, où :

- 0.0 : Aucune gravité
- 0.1 à 3.9 : Faible (Low)
- 4.0 à 6.9 : Moyenne (Medium)
- 7.0 à 8.9 : Élevée (High)
- 9.0 à 10.0 : Critique (Critical)



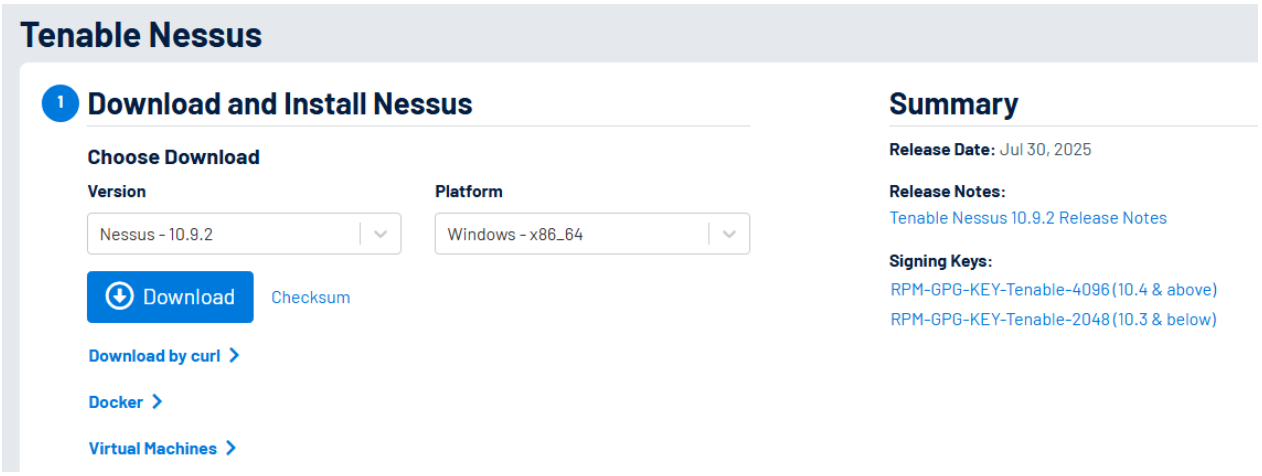

Une vulnérabilité critique (CVE-2023-21554) affectant le service Microsoft Message Queuing a été détectée sur le port 1801/TCP de l'hôte 192.168.1.26. Cette faille permet à un attaquant non authentifié d'exécuter du code à distance.

**Recommandation :**

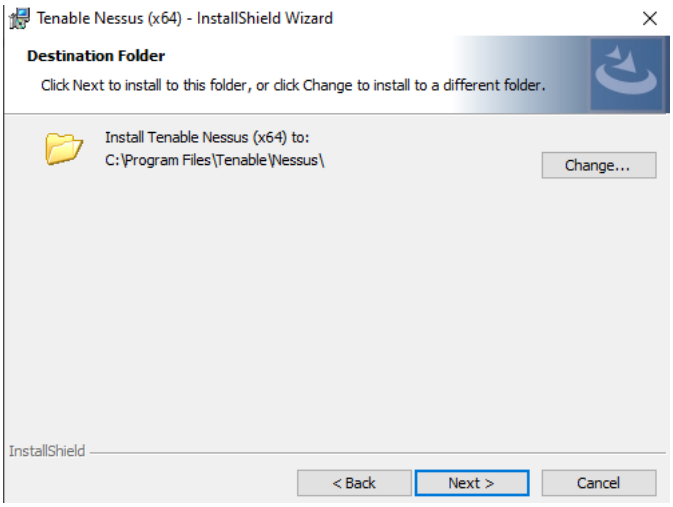
- Appliquer immédiatement le correctif Microsoft via Windows Update.
- Désactiver le service **MSMQ** si non nécessaire.
- Restreindre l'accès réseau si le service doit rester actif.

## 2.4 Installation et configuration sur Windows

1) Télécharger Nessus pour Windows sur le site officielle

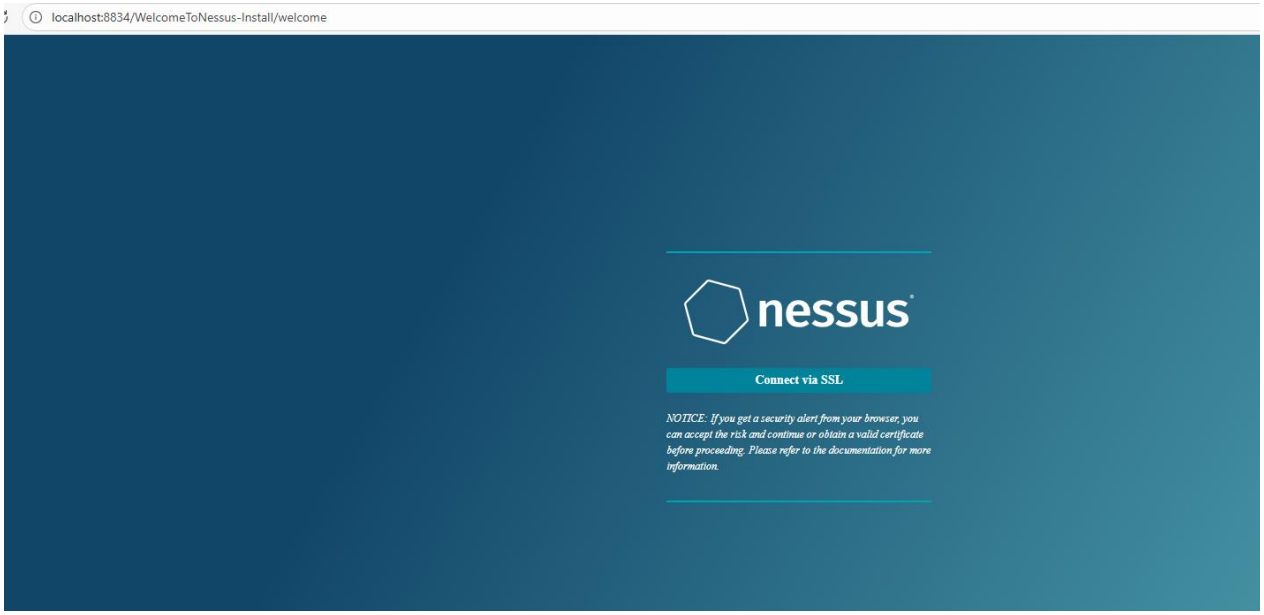



2) Lancer l'installateur

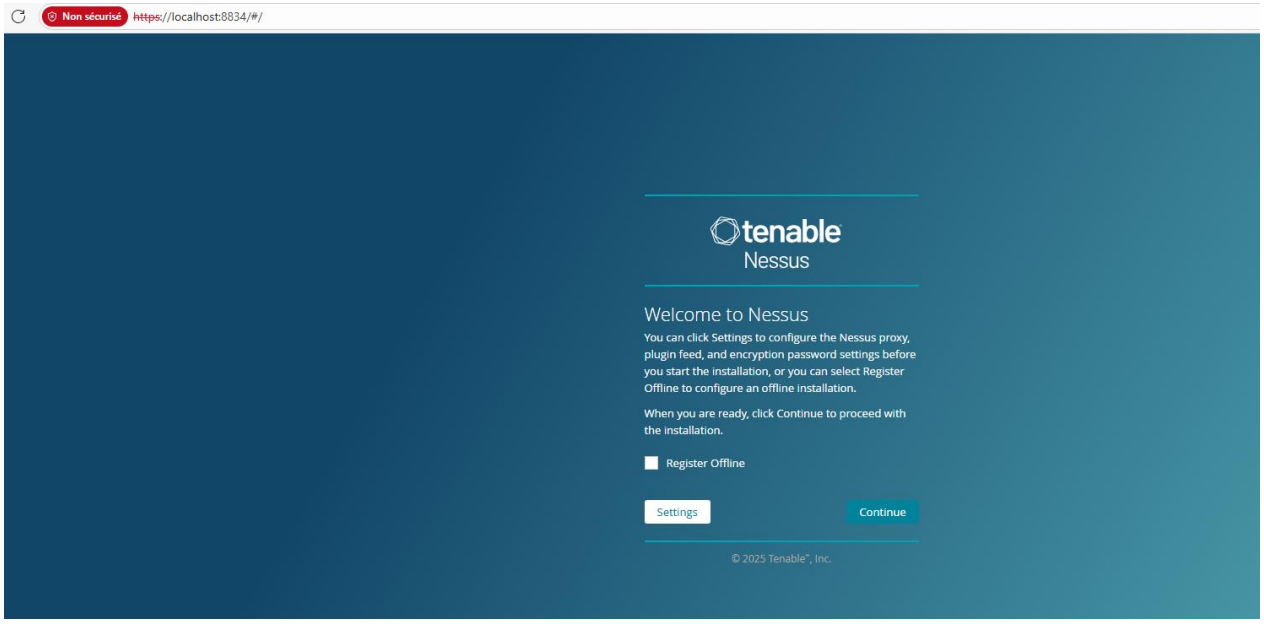



3) Une fois installé, l'interface s'ouvre automatiquement dans le navigateur :

https://localhost:8834/




Appuyer sur le Button «Connect via SSH»



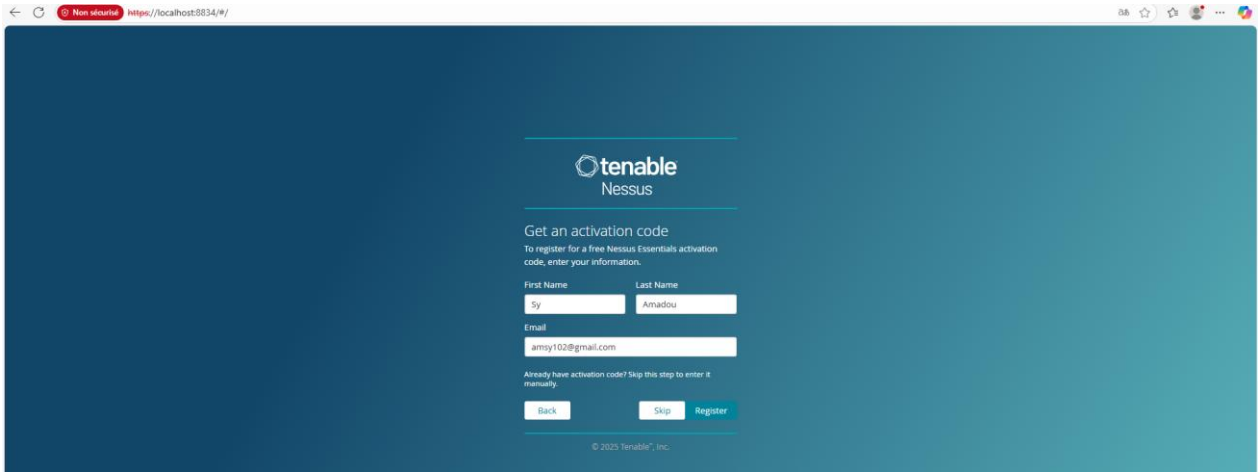

4) Créez un compte administrateur local pour Nessus(si absent) .
5) Entrez la **clé d'activation** reçue par mail.
6) Sélectionnez **"Nessus Essentials"** pour utiliser la version gratuite.

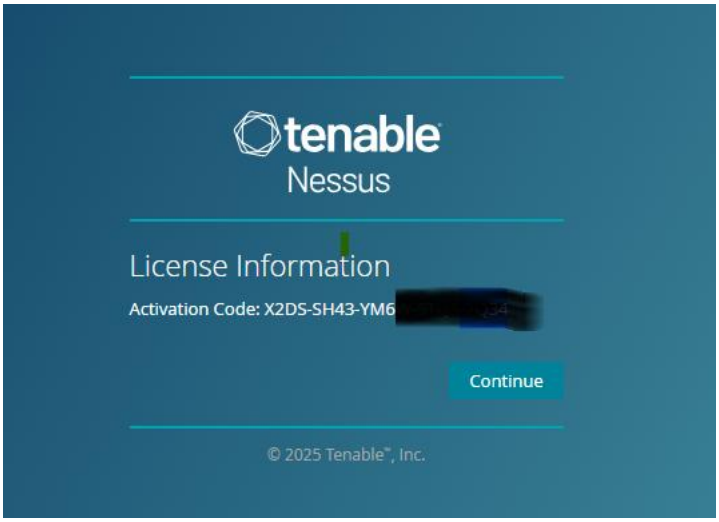
Puisque qu'on a déjà créer un compte Tenable, on va **demander une nouvelle clé gratuite** (en utilisant le **même compte Tenable**).

Pour obtenir une nouvelle clé gratuite :

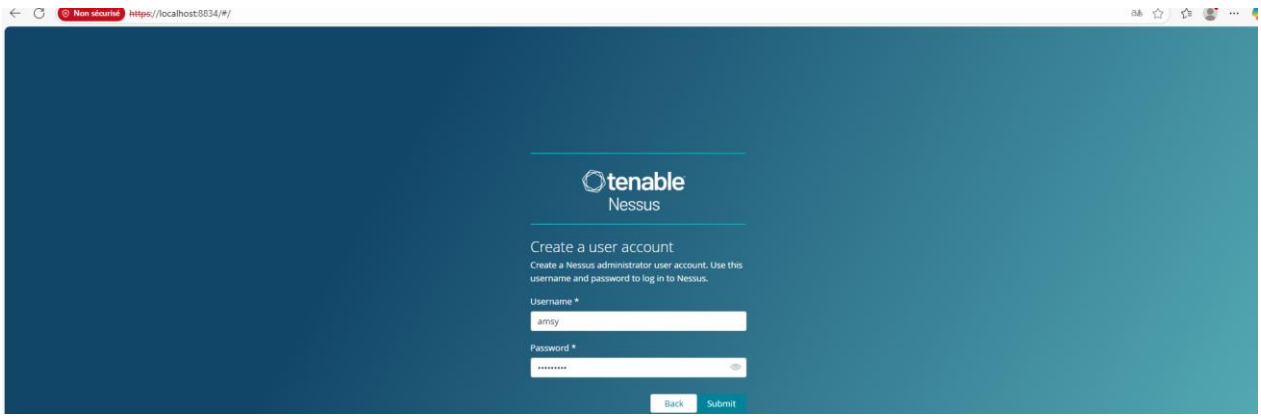
1. Entrer le même e-mail  utilisé pour Nessus sur Ubuntu.
2. Cliquer sur "Register".

3. une nouvelle clé d’activation est envoyé par e-mail (même compte, nouvelle clé gratuite).
4. Copie-coller cette nouvelle clé quand Nessus sur Windows la demandera.



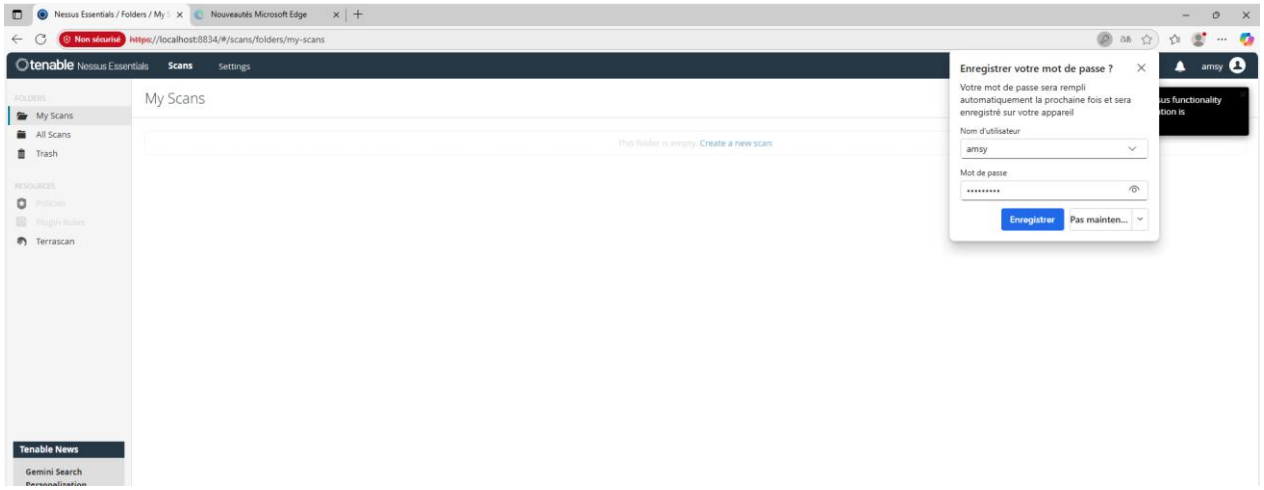




7) Créer un administrateur



8) Cliquer sur Submit pour passer a l'installation des plugins puis au demarrage de nessus


9) Accés a l'interface de la page d'accueil de nessus

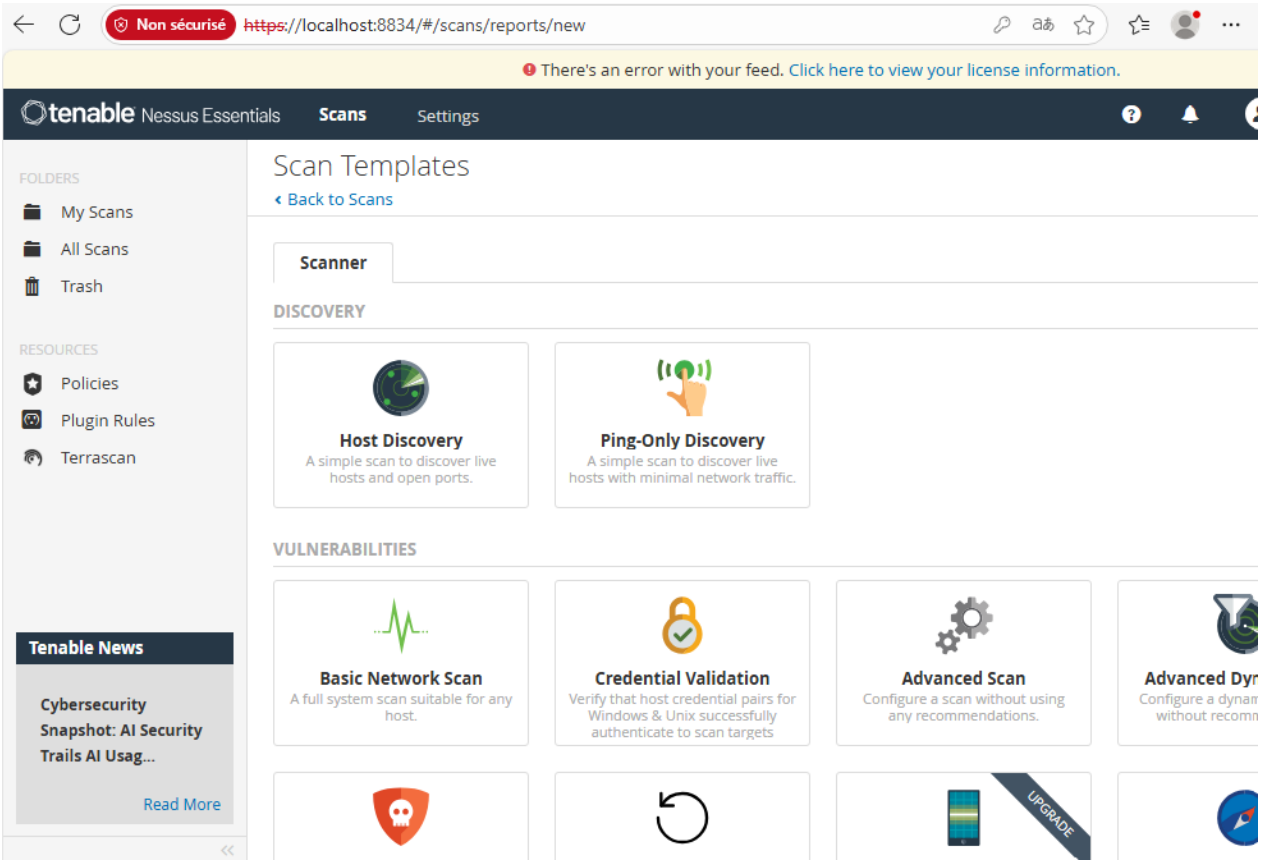


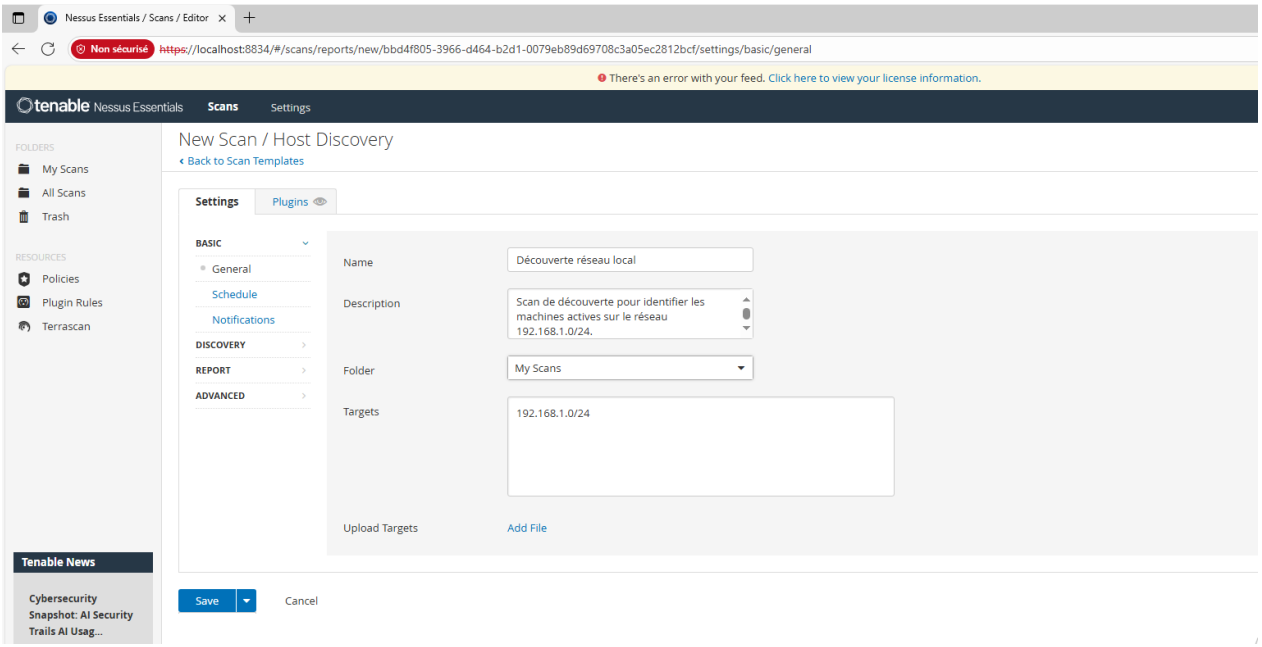

# 3 Analyse réseau – Host Discovery

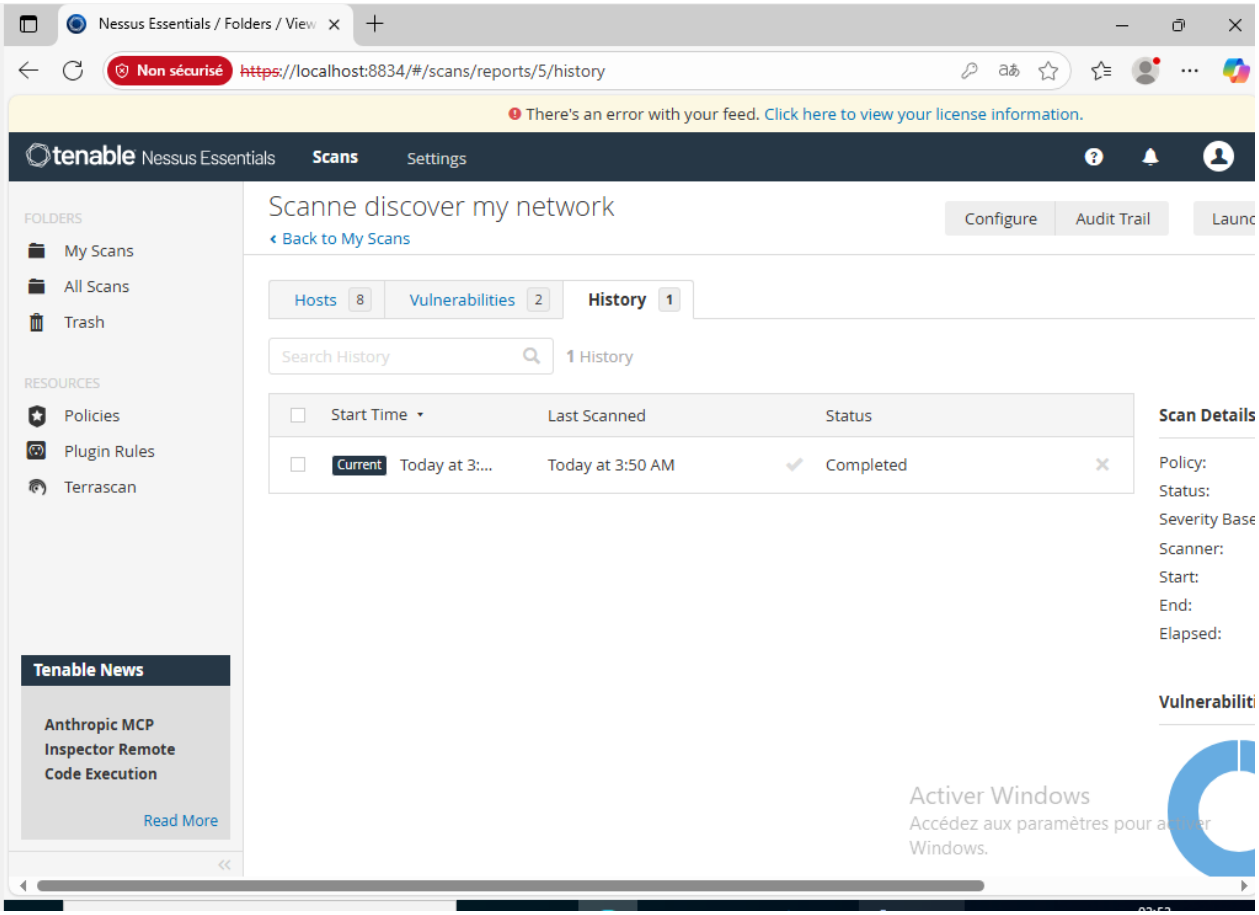
Procéder à un scan de type **"Host Discovery"** afin de détecter les machines connectées au **même réseau que la machine Windows exécutant Nessus**.

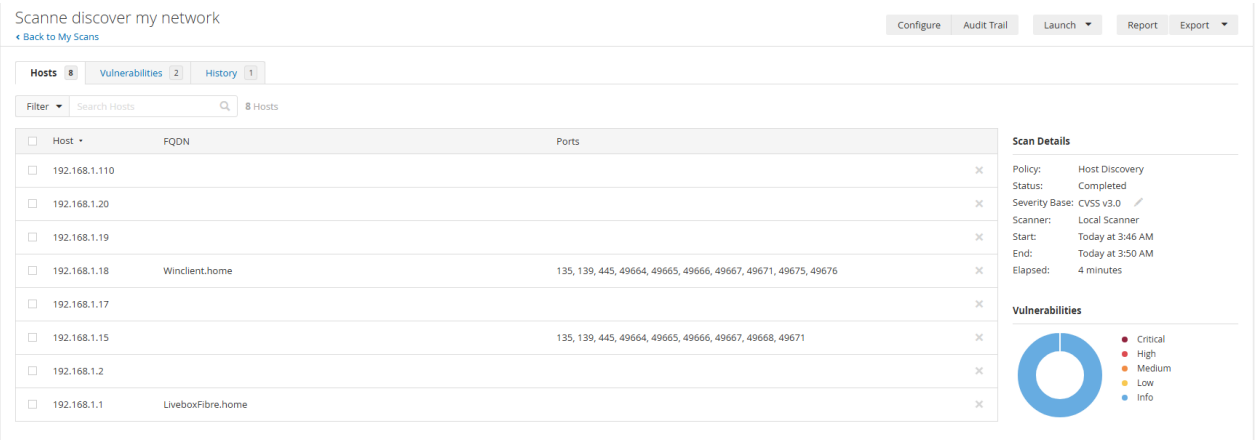
**Procédure :**

- Lancer un scan **Host Discovery** depuis Nessus Windows.


Non sécurisé
https://localhost:8834/#/scans/reports/new
There's an error with your feed. Click here to view your license information.
tenable Nessus Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Cybersecurity Snapshot: AI Security Trails AI Usag...
Read More
Scan Templates
Back to Scans
Scanner
DISCOVERY
Host Discovery
A simple scan to discover live hosts and open ports.
Ping-Only Discovery
A simple scan to discover live hosts with minimal network traffic.
VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
Credential Validation
Verify that host credential pairs for Windows & Unix successfully authenticate to scan targets
Advanced Scan
Configure a scan without using any recommendations.
UPGRADE


Nessus Essentials / Scans / Editor
Non sécurisé
https://localhost:8834/#/scans/reports/new/bbd4f805-3966-d464-b2d1-0079eb89d69708c3a05ec2812bcf/settings/basic/general
There's an error with your feed. Click here to view your license information.
tenable Nessus Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Cybersecurity Snapshot: AI Security Trails AI Usag...
New Scan / Host Discovery
Back to Scan Templates
Settings
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
REPORT
ADVANCED
Name
Découverte réseau local
Description
Scan de découverte pour identifier les machines actives sur le réseau 192.168.1.0/24.
Folder
My Scans
Targets
192.168.1.0/24
Upload Targets
Add File
Save
Cancel



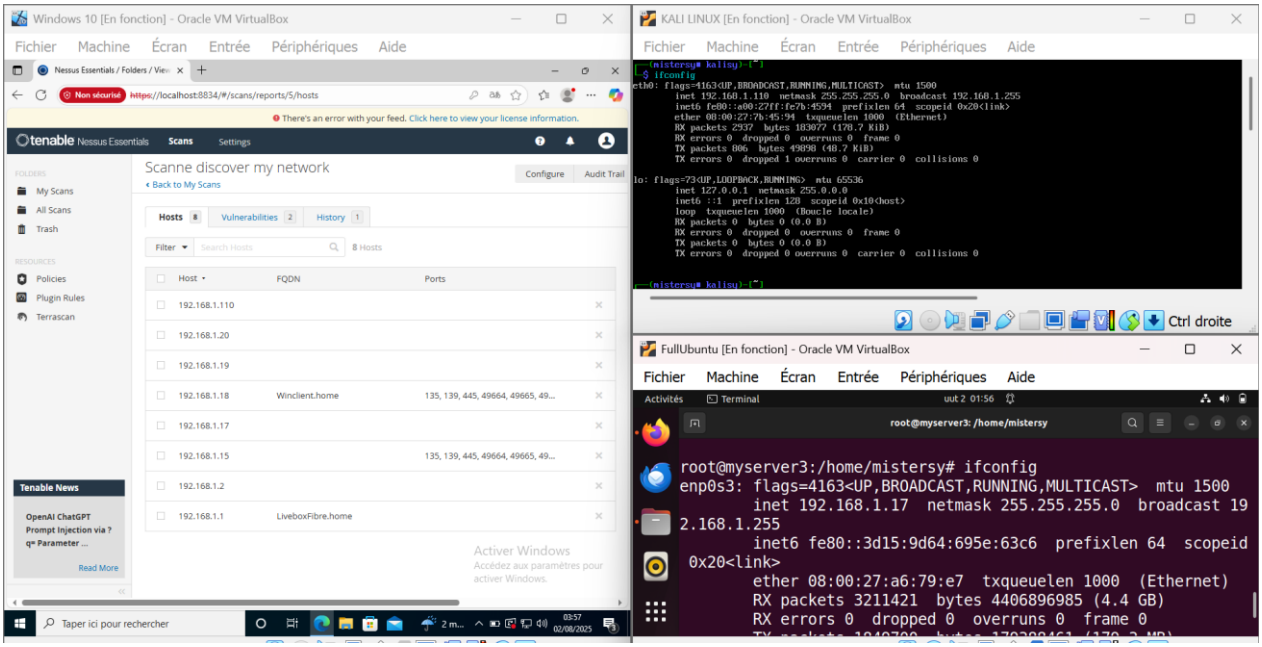




Le scan a permis d'identifier **8 hôtes actifs** sur le réseau local, avec des adresses IP comprises entre 192.168.1.1 et 192.168.1.120. Certains hôtes disposent d'un **nom d'hôte complet (FQDN)**, tels que Winclient.home ou LiveboxFibre.home, ce qui indique une résolution correcte via DNS ou NetBIOS.

Parmi les machines détectées, on note notamment :

- Une machine **Ubuntu**, associée à l'adresse IP 192.168.1.17

- Une machine **Kali Linux**, associée à l'adresse IP 192.168.1.110




Ces systèmes ont été identifiés sur la base de leur réponse au scan ainsi que des services réseau exposés.

**Vulnérabilités :**

La section de droite présente un graphique circulaire indiquant qu'aucune vulnérabilité critique, haute, moyenne ou faible n'a été identifiée à ce stade. Cela est normal pour un scan de type découverte, qui ne réalise pas de tests de vulnérabilité poussés, mais seulement une identification de la présence et de certains services des hôtes.

# 4 Conclusion

L'utilisation de **Nessus Essentials** dans le cadre de ce projet a permis de mettre en évidence la puissance et la flexibilité de cet outil dans le domaine de l'analyse des vulnérabilités réseau et système. Grâce à ses fonctionnalités avancées, Nessus offre aux administrateurs et aux professionnels de la cybersécurité une solution fiable pour :

- Identifier les hôtes actifs sur un réseau local (grâce aux scans de type *Host Discovery*),
- Détecter des vulnérabilités critiques, faibles ou informatives sur des systèmes ciblés,
- Évaluer les configurations système et les services exposés,
- Et recommander les mesures correctives à appliquer en fonction du niveau de risque (CVSS, VPR, EPSS, etc.).

L'installation sur les plateformes **Ubuntu** et **Windows** s'est déroulée sans difficulté majeure, démontrant la compatibilité multi-OS de la solution. Les étapes de configuration, d'enregistrement de licence (Essentials), et de lancement des premiers scans sont simples à suivre et bien documentées.

Le scan de vulnérabilités réalisé sur une machine Windows Server 2019 a révélé la présence d'une **faille critique (CVE-2023-21554)**, nécessitant une action immédiate. Ce cas concret illustre l'importance d'un audit régulier des systèmes pour prévenir les risques d'intrusion, d'exploitation ou de compromission.

Par ailleurs, l'exécution d'un scan *Host Discovery* a permis de recenser les machines actives sur le réseau (192.168.1.0/24), parmi lesquelles figuraient des systèmes Ubuntu et Kali Linux. Ce type de scan est essentiel pour cartographier l'environnement réseau avant d'engager des audits de sécurité plus poussés.

# 5 Recommandations finales

- Intégrer **Nessus** dans un processus de surveillance continue pour garantir un niveau de sécurité optimal.
- Automatiser les scans planifiés, notamment pour les environnements critiques.
- Compléter les analyses avec d'autres outils (comme OpenVAS, Nmap ou Metasploit) pour enrichir la posture de cybersécurité.
- Mettre en place un plan de remédiation basé sur les rapports Nessus.