

# Manuel Très Complet de Nessus

## Introduction à Nessus : Le Leader de l'Évaluation des Vulnérabilités

Nessus est un scanner de vulnérabilités développé par Tenable Network Security, reconnu mondialement comme l'un des outils les plus fiables et les plus complets pour identifier les faiblesses de sécurité dans les systèmes informatiques et les réseaux. Depuis sa création en 1998, Nessus est devenu une référence incontournable pour les professionnels de la cybersécurité, les auditeurs, les pentesters et les organisations soucieuses de renforcer leur posture de sécurité.

### Qu'est-ce qu'un Scanner de Vulnérabilités ?

Un scanner de vulnérabilités est un logiciel conçu pour identifier les failles de sécurité potentielles ou avérées dans un système, une application ou un réseau. Il fonctionne en analysant les cibles à la recherche de configurations erronées, de logiciels obsolètes, de ports ouverts non sécurisés, de mots de passe faibles, et d'autres indicateurs de vulnérabilités connues. L'objectif est de fournir un rapport détaillé des risques, permettant aux administrateurs de corriger les problèmes avant qu'ils ne soient exploités par des acteurs malveillants.

### Pourquoi Nessus est-il Indispensable ?

Nessus se distingue par plusieurs caractéristiques clés qui en font un outil de choix :

- **Précision et Exhaustivité** : Nessus est réputé pour sa capacité à détecter un très large éventail de vulnérabilités, y compris les CVE (Common Vulnerabilities and Exposures) les plus récentes. Il utilise une base de données de plugins massive (plus de 252 000) qui est constamment mise à jour (plus de 100 nouveaux plugins chaque semaine) par la recherche Zero-Day de Tenable.
- **Facilité d'Utilisation** : Malgré sa puissance, Nessus est conçu pour être intuitif, avec une interface utilisateur graphique (GUI) qui simplifie la configuration des scans, l'analyse des résultats et la génération de rapports.
- **Polyvalence** : Il peut scanner une grande variété de systèmes, y compris les serveurs, les postes de travail, les équipements réseau, les applications web, les bases de données, et même les environnements cloud et les conteneurs.

- **Rapports Détaillés et Actionnables** : Nessus génère des rapports clairs et concis qui non seulement listent les vulnérabilités, mais fournissent également des informations sur leur gravité, des preuves de leur existence et des recommandations concrètes pour leur correction.
- **Conformité** : Il aide les organisations à se conformer aux réglementations et aux normes de sécurité (PCI DSS, HIPAA, ISO 27001, etc.) en fournissant des preuves d'évaluation des vulnérabilités.

En somme, Nessus est bien plus qu'un simple scanner ; c'est une solution complète d'évaluation des vulnérabilités qui permet aux organisations de comprendre, de prioriser et de corriger leurs risques de sécurité de manière proactive.

## Installation de Nessus : Un Guide Étape par Étape

L'installation de Nessus est un processus relativement simple, mais il est crucial de suivre chaque étape attentivement pour assurer un fonctionnement optimal. Ce guide couvrira l'installation sur les systèmes d'exploitation les plus courants : Windows et Linux (en particulier les distributions basées sur Debian/Ubuntu, comme Kali Linux).

### 1. Téléchargement du Package Nessus

La première étape consiste à télécharger le package d'installation de Nessus depuis le site officiel de Tenable. Vous aurez besoin d'un compte Tenable pour accéder aux téléchargements.

1. **Accédez au Centre de Téléchargement Tenable** : Ouvrez votre navigateur web et naviguez vers : <https://www.tenable.com/downloads/nessus>.
2. **Connectez-vous ou Créez un Compte** : Si vous n'êtes pas déjà connecté, vous serez invité à vous connecter avec votre compte Tenable ID. Si vous n'en avez pas, vous devrez en créer un. C'est gratuit pour la version Nessus Essentials.
3. **Sélectionnez le Package Approprié** : Une fois connecté, vous verrez une liste de packages Nessus disponibles pour différents systèmes d'exploitation et architectures. Choisissez celui qui correspond à votre système (par exemple, `Nessus-X.Y.Z-x64.msi` pour Windows 64-bit, ou `Nessus-X.Y.Z-debian6_amd64.deb` pour Debian/Ubuntu 64-bit).

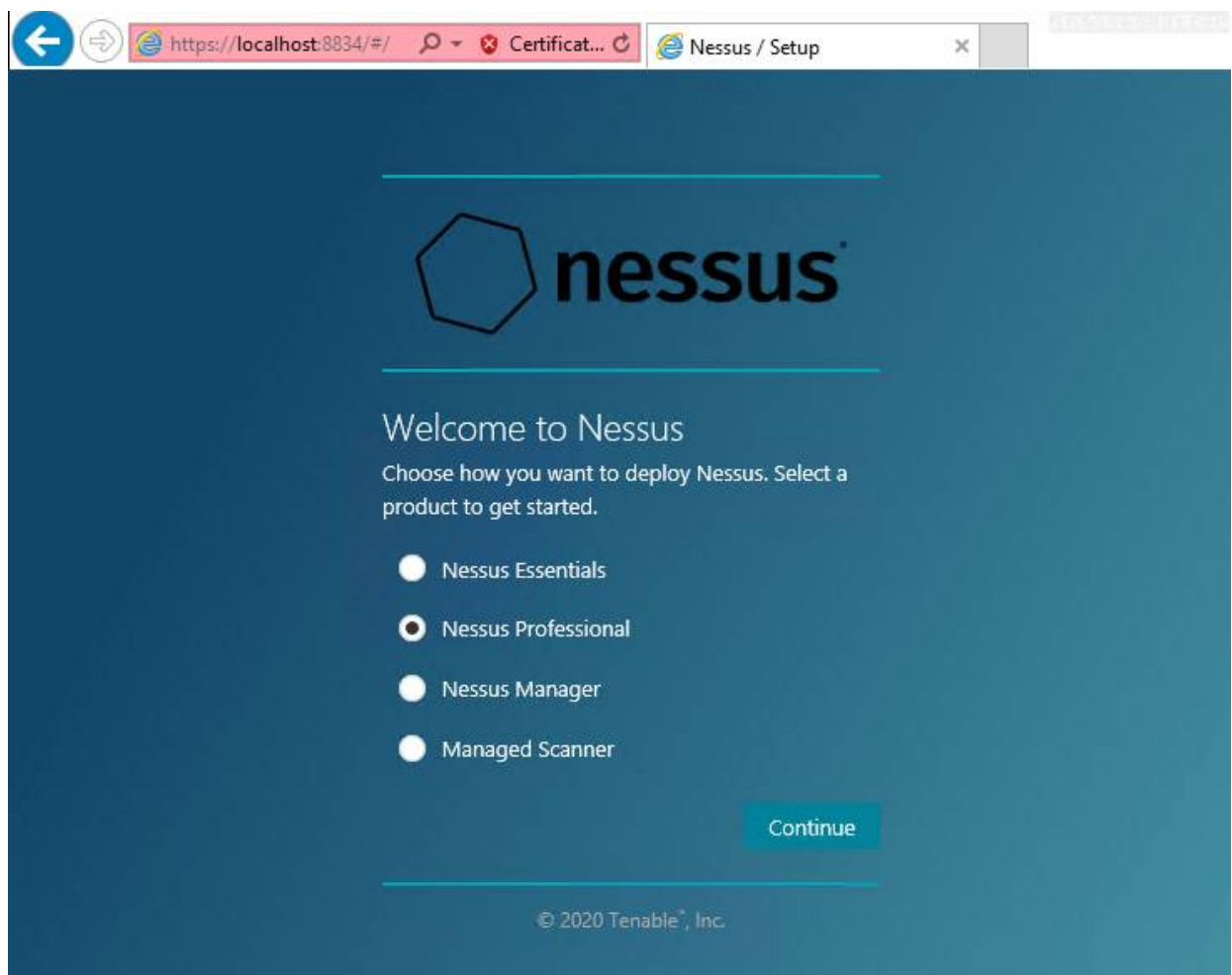


Figure 1: Sélection du package d'installation de Nessus sur le site de Tenable.

4. **Acceptez le Contrat de Licence et Téléchargez** : Lisez et acceptez le contrat de licence utilisateur final (EULA), puis cliquez sur le bouton de téléchargement.

## 2. Installation de Nessus sur Votre Système

Le processus d'installation varie légèrement selon le système d'exploitation.

### 2.1. Installation sur Windows

1. **Exécutez l'Installeur** : Localisez le fichier `.msi` téléchargé et double-cliquez dessus pour lancer l'assistant d'installation de Nessus.
2. **Suivez l'Assistant d'Installation** :
  - Cliquez sur `Next` (Suivant) sur l'écran de bienvenue.
  - Acceptez les termes du contrat de licence et cliquez sur `Next`.
  - Choisissez le dossier de destination pour l'installation (le chemin par défaut est généralement recommandé) et cliquez sur `Next`.
  - Cliquez sur `Install` (Installer) pour démarrer le processus d'installation.

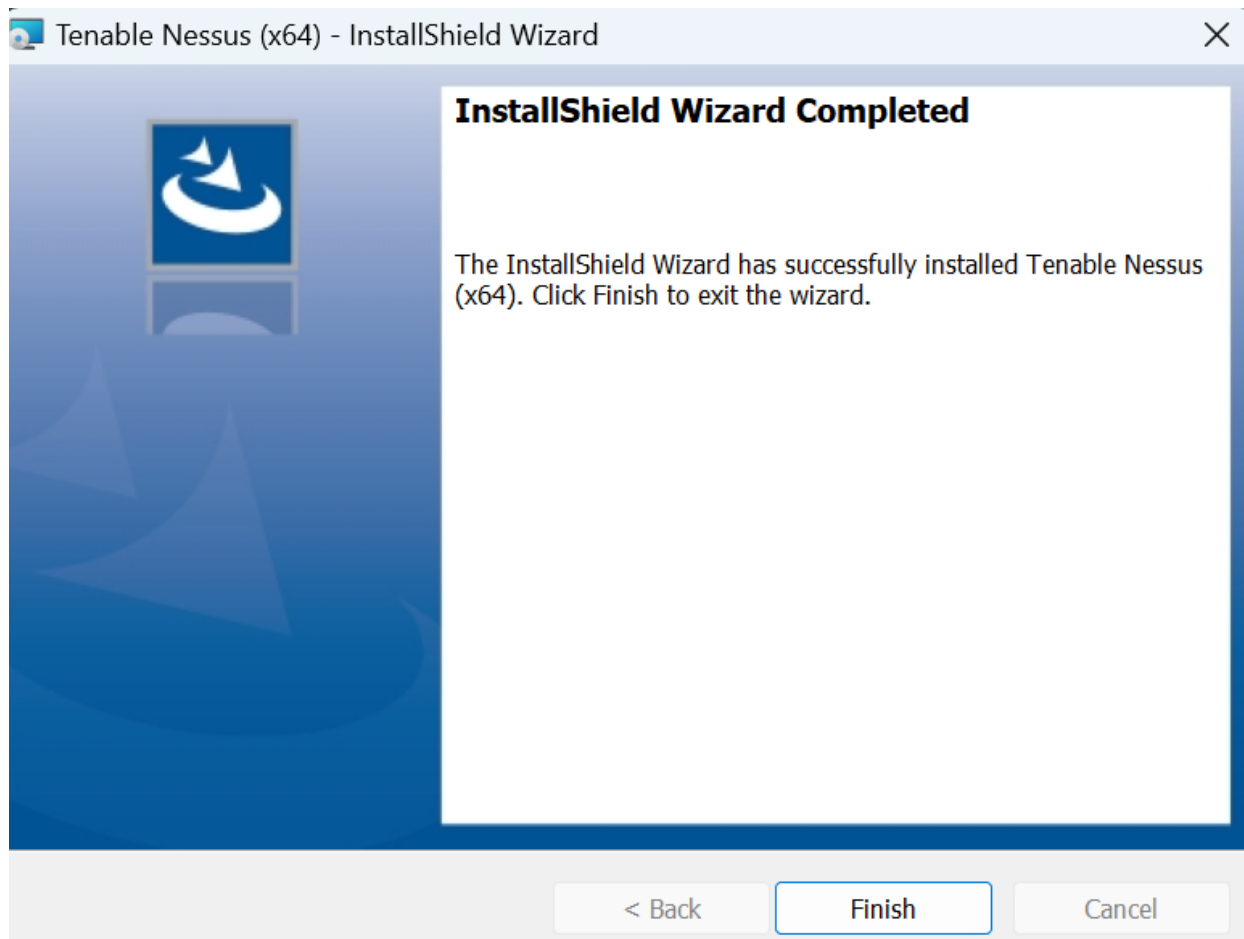


Figure 2: Assistant d'installation de Nessus sur Windows, montrant les étapes de configuration.

3. **Finalisation de l'Installation** : Une fois l'installation terminée, cliquez sur **Finish** (Terminer). Nessus devrait alors s'ouvrir automatiquement dans votre navigateur web par défaut.

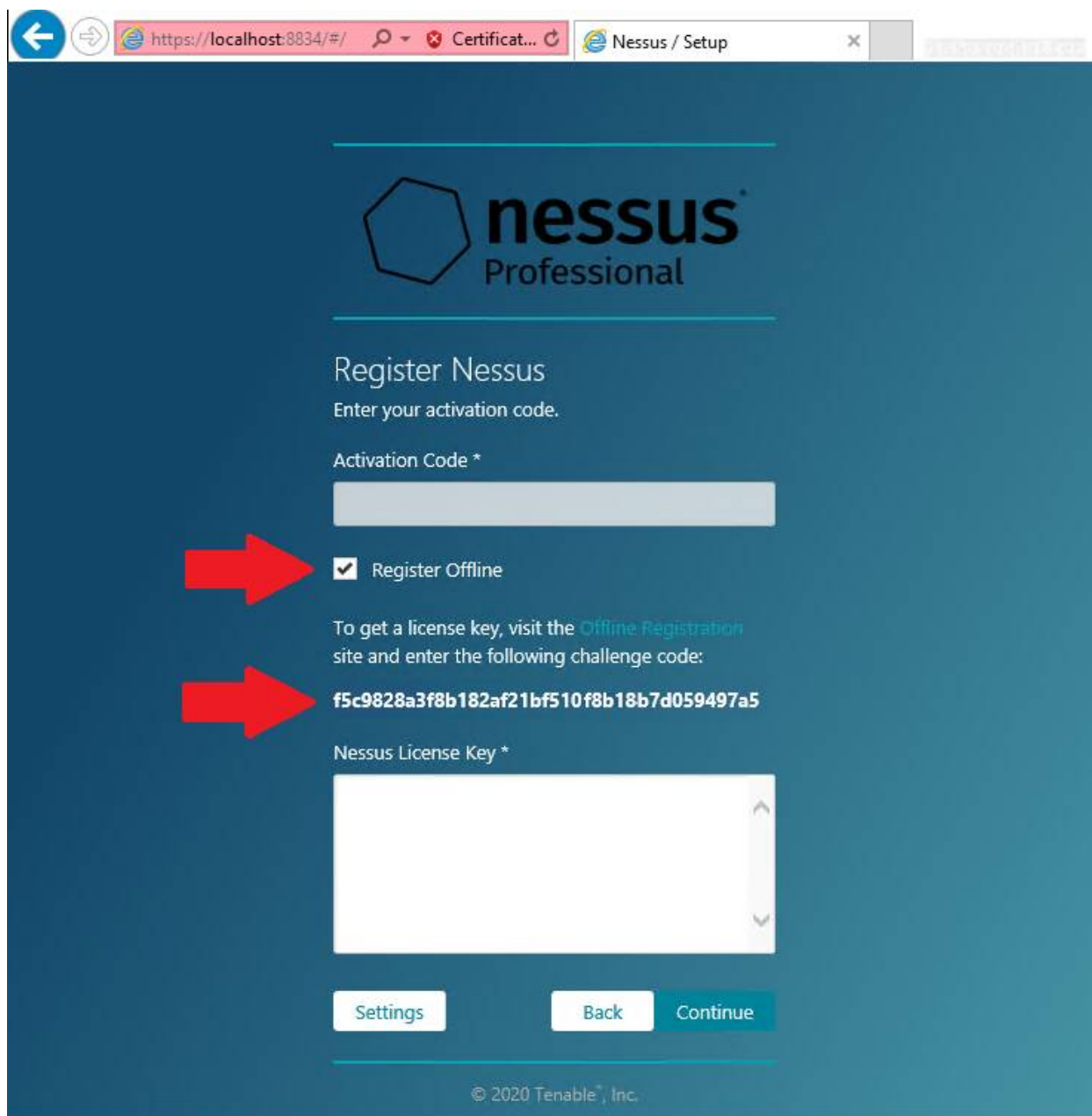


Figure 3: Écran de confirmation de la fin de l'installation de Nessus sur Windows.

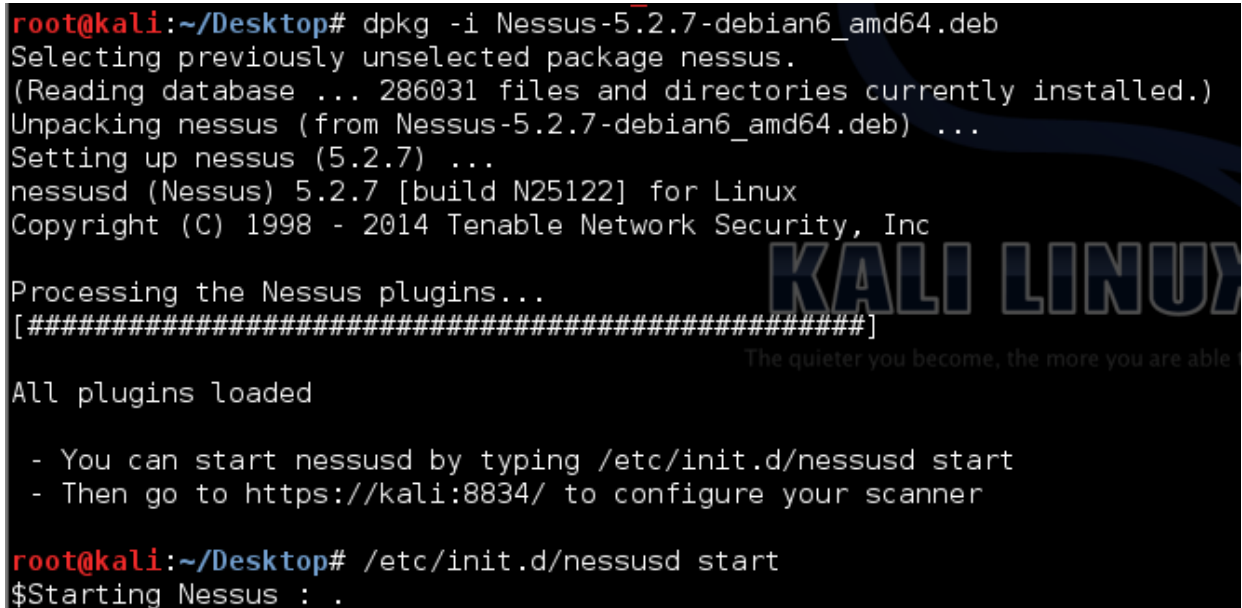
## 2.2. Installation sur Linux (Debian/Ubuntu/Kali Linux)

Pour les distributions basées sur Debian/Ubuntu, l'installation se fait via le package `.deb`.

1. **Ouvrez un Terminal** : Naviguez jusqu'au répertoire où vous avez téléchargé le fichier `.deb` de Nessus.
2. **Installez le Package** : Utilisez la commande `dpkg` pour installer le package. Remplacez `Nessus-X.Y.Z-debian6_amd64.deb` par le nom exact de votre fichier téléchargé. 

```
bash sudo dpkg -i Nessus-X.Y.Z-debian6_amd64.deb
```
3. **Démarrez le Service Nessus** : Après l'installation, démarrez le service Nessus. La commande peut varier légèrement selon la version ou la distribution, mais les plus

courantes sont: `bash sudo systemctl start nessusd` # Ou pour les anciennes versions : `# sudo /etc/init.d/nessusd start`

A terminal window on Kali Linux showing the installation of Nessus. The user runs 'dpkg -i Nessus-5.2.7-debian6\_amd64.deb'. The output shows the package being selected, unpacked, and configured. It lists the version (5.2.7) and build (N25122). It then processes the plugins and lists them. Finally, the user runs '/etc/init.d/nessusd start' and the terminal shows '\$Starting Nessus : .'.

```
root@kali:~/Desktop# dpkg -i Nessus-5.2.7-debian6_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 286031 files and directories currently installed.)
Unpacking nessus (from Nessus-5.2.7-debian6_amd64.deb) ...
Setting up nessus (5.2.7) ...
nessusd (Nessus) 5.2.7 [build N25122] for Linux
Copyright (C) 1998 - 2014 Tenable Network Security, Inc

Processing the Nessus plugins...
[#####]

All plugins loaded

- You can start nessusd by typing /etc/init.d/nessusd start
- Then go to https://kali:8834/ to configure your scanner

root@kali:~/Desktop# /etc/init.d/nessusd start
$Starting Nessus : .
```

Figure 4: Installation et démarrage du service Nessus sur Kali Linux via le terminal.

### 3. Configuration Initiale de Nessus via l'Interface Web

Après l'installation, vous devez configurer Nessus via son interface web. C'est là que vous créerez votre compte administrateur et enregistrerez votre scanner.

1. **Accédez à l'Interface Web de Nessus** : Ouvrez votre navigateur web et accédez à l'adresse suivante. Nessus utilise le port `8834` par défaut et une connexion HTTPS. `https://localhost:8834/`
  - Vous pourriez recevoir un avertissement de sécurité concernant le certificat SSL. Acceptez-le pour continuer, car il s'agit d'un certificat auto-signé.
2. **Bienvenue sur Nessus** : L'écran de bienvenue de Nessus apparaîtra.

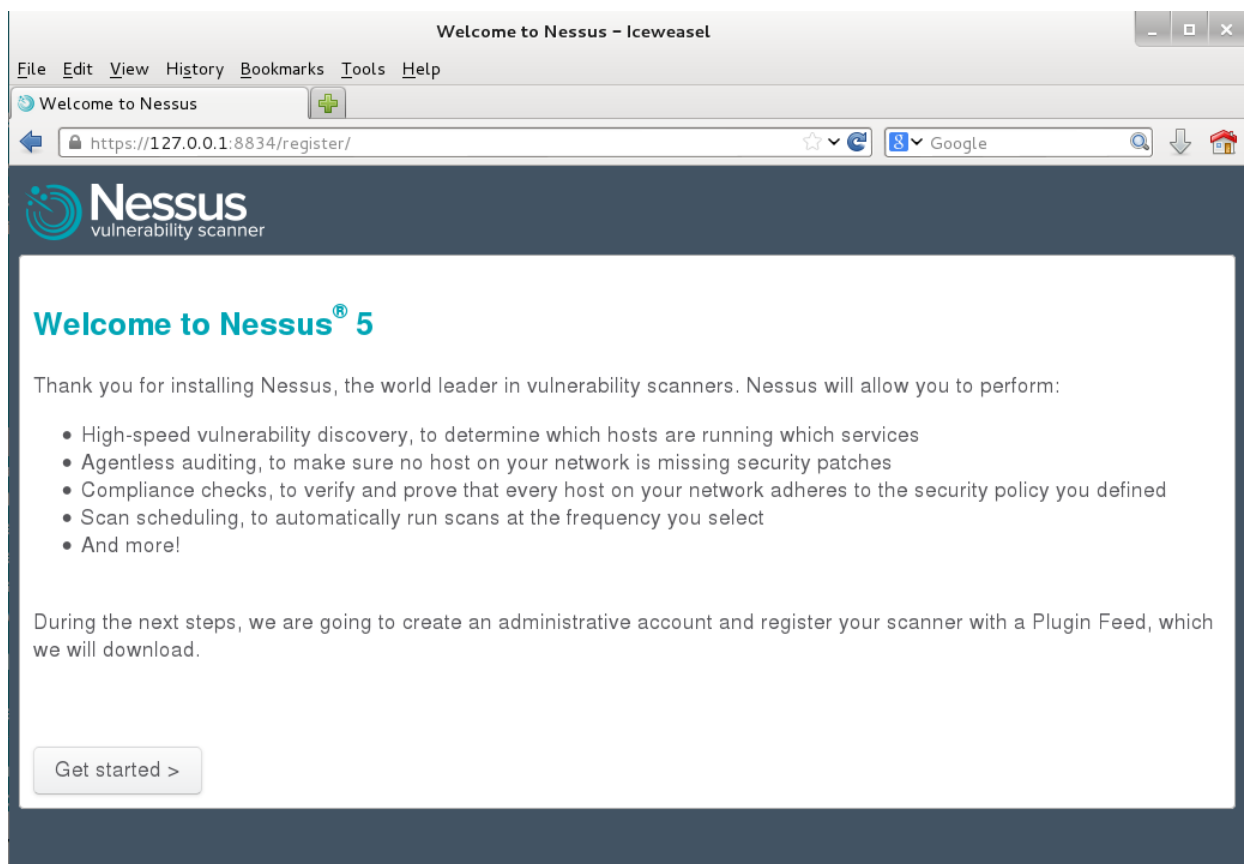


Figure 5: Écran de bienvenue de Nessus, invitant à la configuration initiale.

3. **Sélectionnez le Type de Produit** : Choisissez le type de Nessus que vous avez installé. Pour la version gratuite, sélectionnez **Nessus Essentials**.

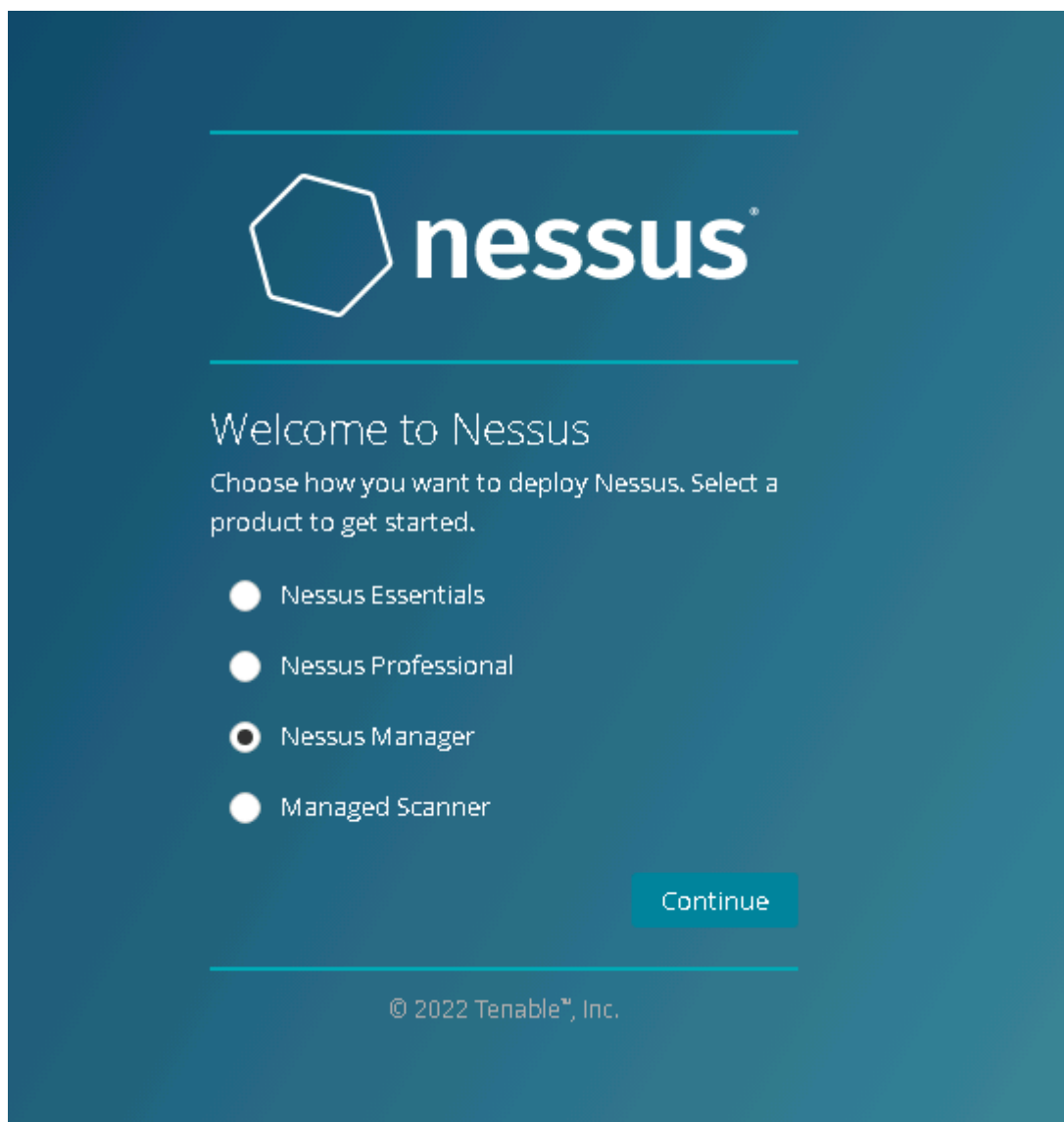


Figure 6:

Sélection de l'édition Nessus Essentials pour la configuration.

4. **Créez un Compte Administrateur** : Créez un nom d'utilisateur et un mot de passe pour le compte administrateur de Nessus. C'est ce compte que vous utiliserez pour vous connecter à l'interface web de Nessus.

5. **Enregistrez Nessus** :

- Si vous avez une clé d'activation (obtenue lors de l'enregistrement de Nessus Essentials sur le site de Tenable), entrez-la dans le champ `Activation Code`.
- Si vous n'avez pas encore de clé, cliquez sur le lien pour en obtenir une. Vous serez redirigé vers le site de Tenable pour enregistrer votre produit et recevoir la clé par e-mail.



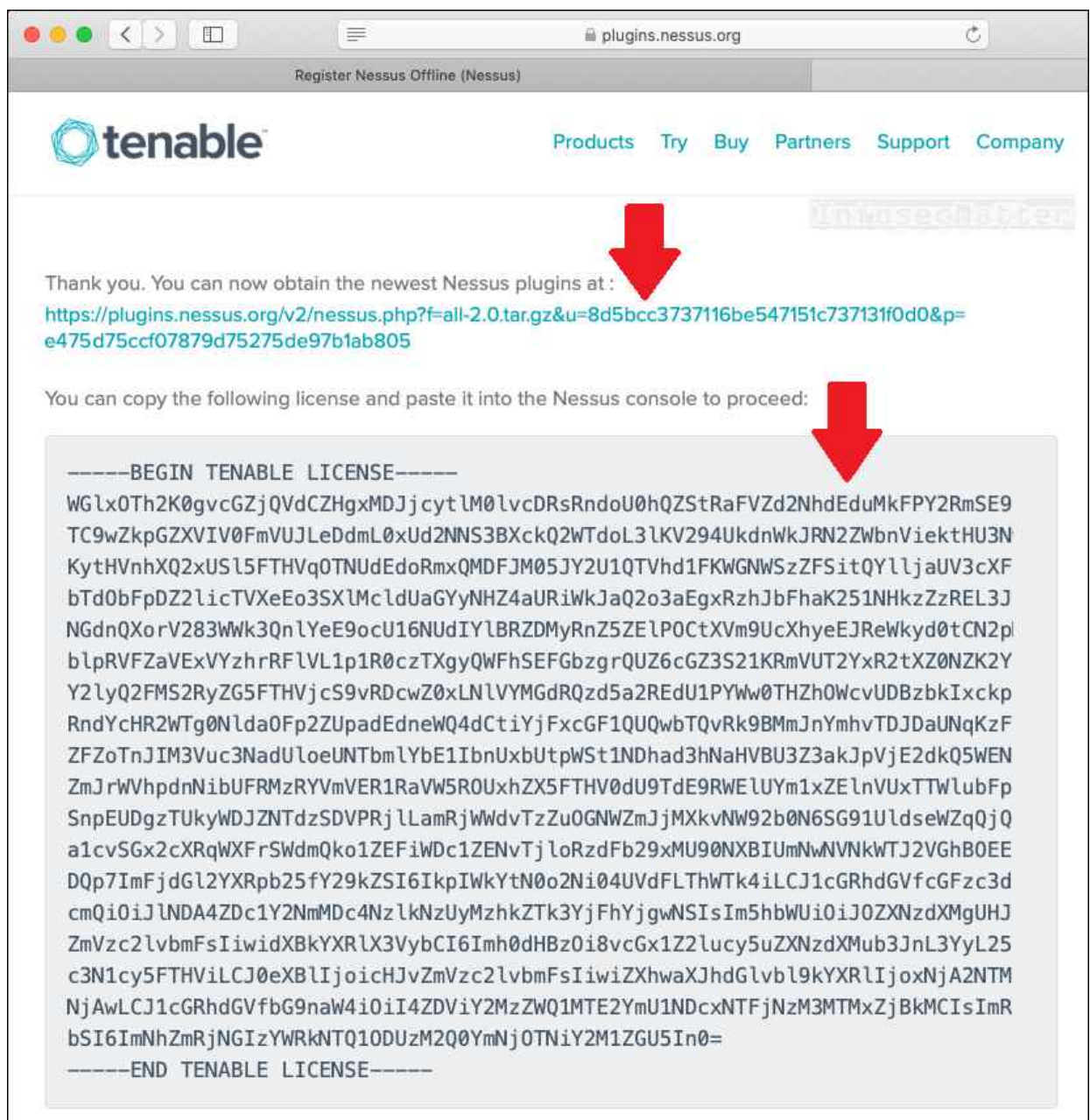


Figure 7: Fenêtre d'enregistrement de Nessus, où l'on entre la clé d'activation.

6. **Téléchargement des Plugins** : Une fois l'enregistrement terminé, Nessus commencera à télécharger et à compiler les plugins. Cette étape peut prendre un certain temps (plusieurs minutes à une heure ou plus, selon votre connexion Internet et la puissance de votre machine), car Nessus télécharge une base de données massive de signatures de vulnérabilités.

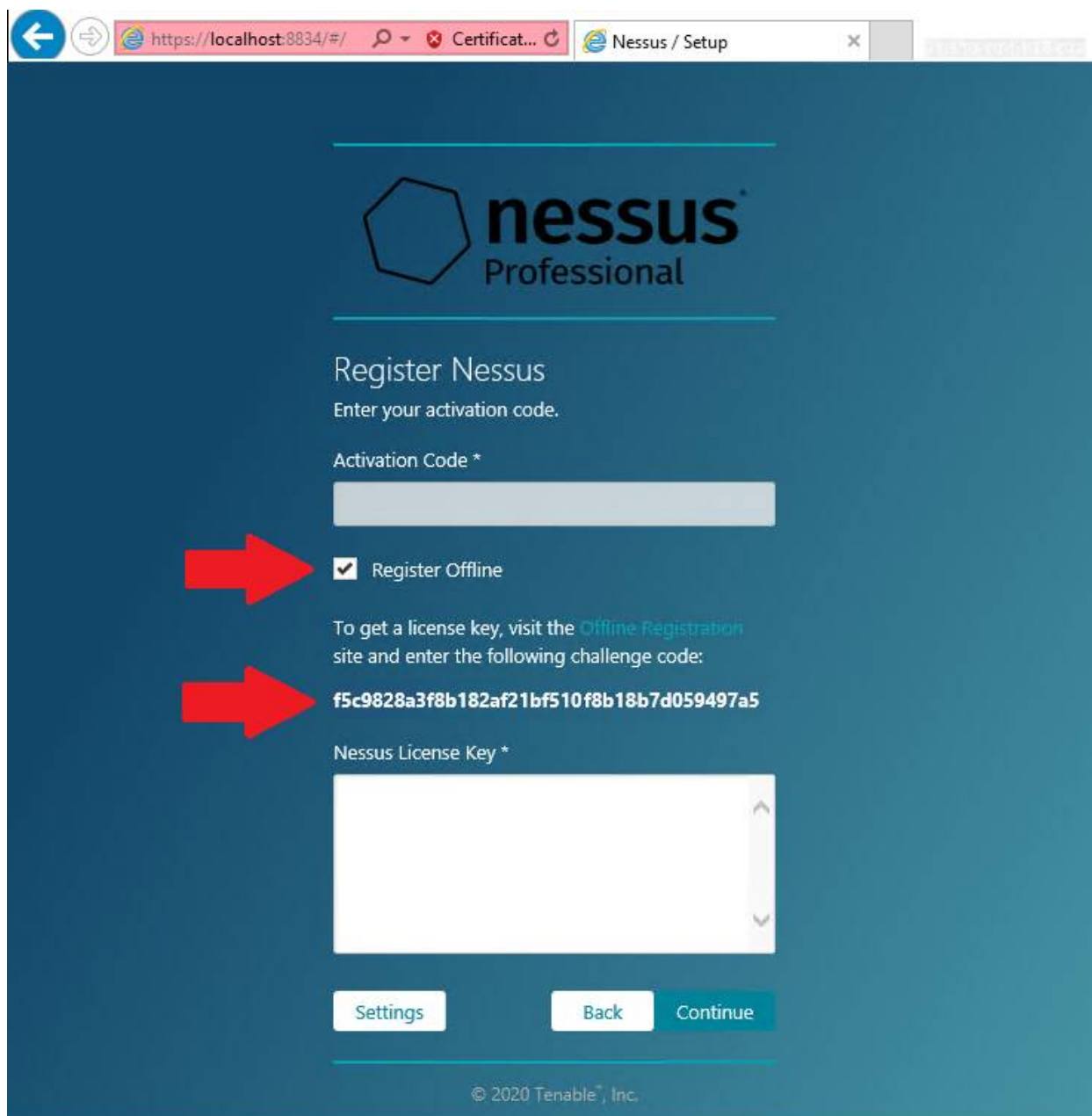


Figure 8: Nessus téléchargeant et compilant les plugins après l'enregistrement.

Une fois les plugins téléchargés et compilés, vous serez redirigé vers l'écran de connexion de Nessus. Vous pouvez alors vous connecter avec le compte administrateur que vous avez créé et commencer à utiliser Nessus.

## Utilisation de Nessus : Création et Exécution de Scans

Une fois Nessus installé et configuré, l'étape suivante consiste à créer et exécuter des scans pour identifier les vulnérabilités sur vos cibles. Cette section vous guidera à travers le processus de création d'un nouveau scan, la configuration des politiques et l'analyse des résultats.

### 1. Connexion à l'Interface Web de Nessus

1. Ouvrez votre navigateur web et accédez à `https://localhost:8834/`.

2. Entrez le nom d'utilisateur et le mot de passe du compte administrateur Nessus que vous avez créé lors de la configuration initiale.

## 2. Création d'un Nouveau Scan

### 1. Accédez à la Section des Scans :

- Une fois connecté, vous verrez le tableau de bord de Nessus. Dans la barre de navigation supérieure, cliquez sur **Scans**.
- Cela vous mènera à la page **My Scans** (Mes Scans), où vous pouvez voir tous les scans existants.

| <input type="checkbox"/> Name ^                        | Schedule  | Last Modified             |
|--|-----------|---------------------------|
| <input type="checkbox"/> 6.10.7 - Advance - 85 - Cred  | On Demand | ✓ June 16 at 6:36 PM ▶ ✕  |
| <input type="checkbox"/> 6.10.7 - Advance - Cred - 84  | On Demand | ✓ June 16 at 6:09 PM ▶ ✕  |
| <input type="checkbox"/> Active sync                   | On Demand | ✓ June 28 at 11:47 AM ▶ ✕ |
| <input type="checkbox"/> Agent Scan                    | Disabled  | ⬆ June 28 at 10:39 AM ✕   |
| <input type="checkbox"/> Agent Scan                    | Disabled  | ⬆ June 28 at 10:35 AM ✕   |
| <input type="checkbox"/> AIX 7.1 - Borken Policy       | On Demand | ✓ June 30 at 11:07 AM ▶ ✕ |
| <input type="checkbox"/> AIX 7.1 - working             | On Demand | ✓ June 30 at 10:04 AM ▶ ✕ |
| <input type="checkbox"/> <script>alert('lol')</script> | Disabled  | ⬆ June 28 at 4:31 PM ✕    |
| <input type="checkbox"/> <script>alert('lol')</script> | On Demand | ✓ June 28 at 12:33 PM ▶ ✕ |
| <input type="checkbox"/> apple PM                      | On Demand | ✓ June 28 at 11:31 AM ▶ ✕ |
| <input type="checkbox"/> Example 2                     | On Demand | ✓ July 26 at 10:28 AM ▶ ✕ |

Figure 9: La page 'My Scans' dans l'interface web de Nessus, affichant les scans existants.

### 2. Lancez la Création d'un Nouveau Scan :

- Dans le coin supérieur droit de la page **My Scans**, cliquez sur le bouton **New Scan** (Nouveau Scan).
- Cela ouvrira la page **Scan Templates** (Modèles de Scan), qui propose différents types de scans préconfigurés pour diverses situations.

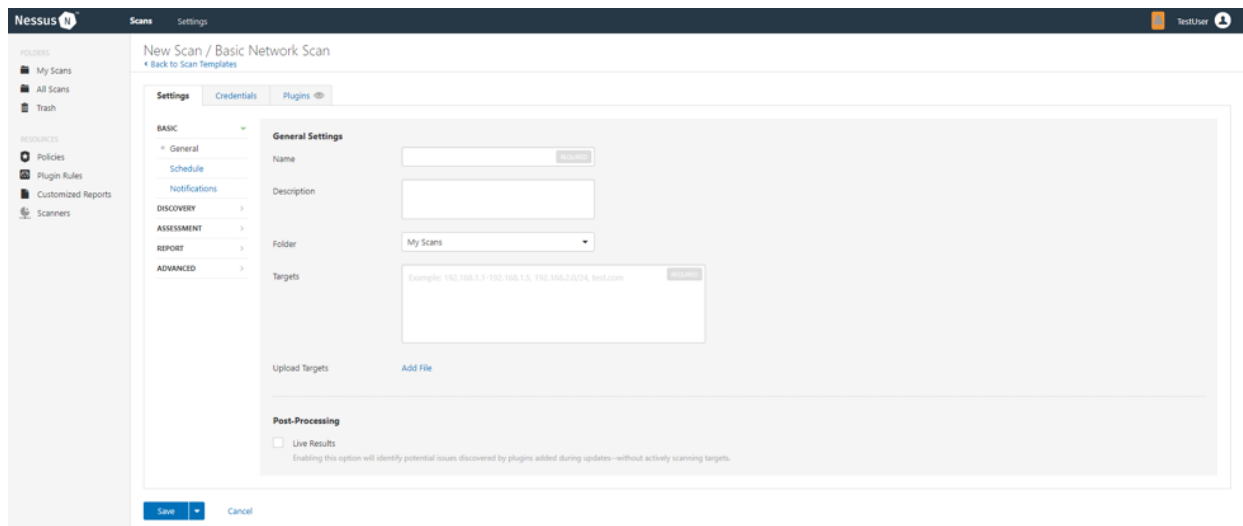


Figure 10: Le bouton 'New Scan' sur la page 'My Scans' de Nessus.

### 3. Choisissez un Modèle de Scan :

- Nessus offre une variété de modèles de scan, chacun optimisé pour un type d'analyse spécifique. Les modèles courants incluent :
  - **Basic Network Scan** : Un scan généraliste pour identifier les vulnérabilités sur les hôtes du réseau.
  - **Advanced Scan** : Permet une configuration très détaillée des paramètres de scan.
  - **Credentialed Patch Audit** : Un scan authentifié pour vérifier l'état des correctifs.
  - **Web Application Test** : Pour scanner les vulnérabilités spécifiques aux applications web.
  - **Malware Scan** : Pour détecter les logiciels malveillants.
- Pour commencer, sélectionnez **Basic Network Scan** en cliquant sur sa vignette.

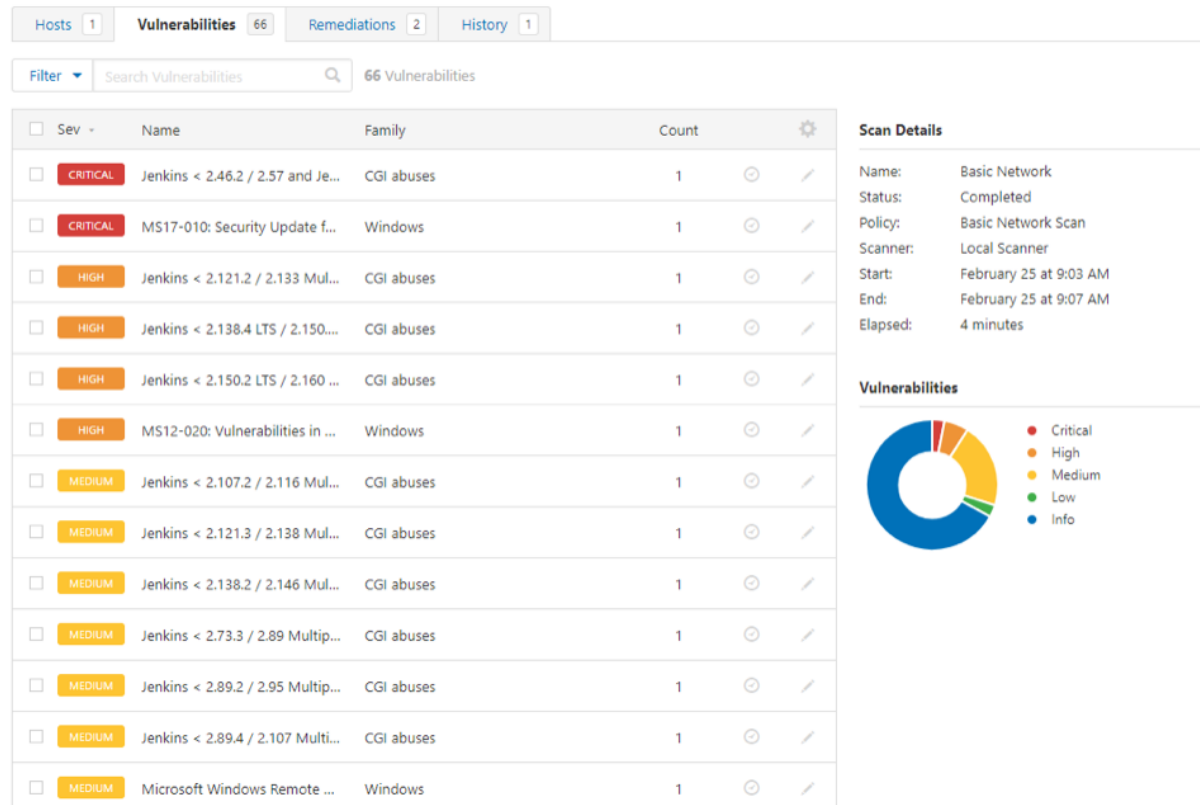


Figure 11: Sélection du modèle 'Basic Network Scan' parmi les modèles de scan disponibles.

### 3. Configuration des Paramètres du Scan

Après avoir choisi un modèle, vous serez redirigé vers la page de configuration du scan, où vous définirez les détails de votre analyse.

#### 1. Onglet **Settings** (Paramètres) - Général :

- **Name** (Nom) : Donnez un nom significatif à votre scan (par exemple, `Scan_Serveur_Web_Prod`).
- **Description** : Ajoutez une brève description du scan.
- **Folder** (Dossier) : Choisissez le dossier où le scan sera enregistré.
- **Targets** (Cibles) : C'est le champ le plus important. Entrez les adresses IP, les plages d'adresses IP, les noms d'hôtes ou les sous-réseaux que vous souhaitez scanner. Vous pouvez entrer plusieurs cibles, séparées par des virgules ou des sauts de ligne (par exemple, `192.168.1.10`, `192.168.1.11-192.168.1.20`, `10.0.0.0/24`).

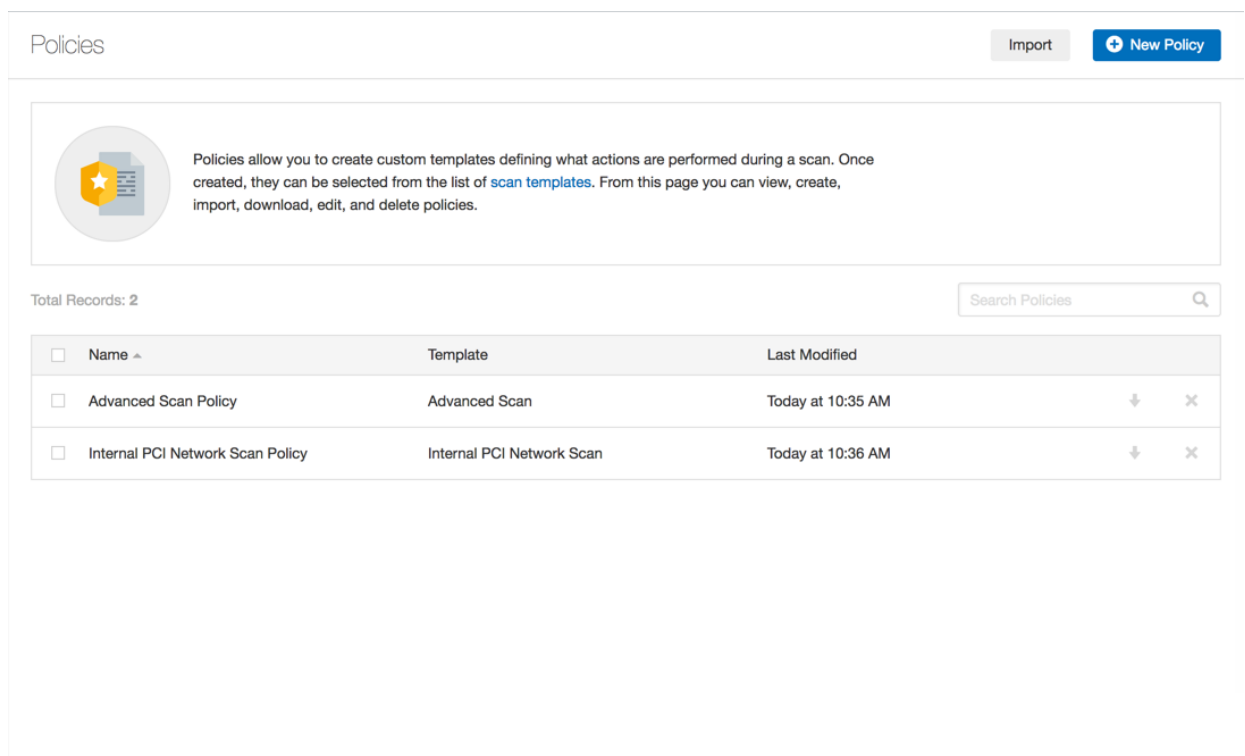


Figure 12: Configuration des paramètres généraux d'un scan, y compris le nom et les cibles.

## 2. Onglet **Settings** - **Discovery** (Découverte) :

- Configurez les méthodes de découverte des hôtes et des ports. Par défaut, Nessus effectue un scan de ports complet, mais vous pouvez le personnaliser (par exemple, scanner uniquement les ports courants, ou des ports spécifiques).

## 3. Onglet **Settings** - **Assessment** (Évaluation) :

- C'est ici que vous définissez les types de vulnérabilités que Nessus recherchera. Vous pouvez activer ou désactiver des familles de plugins spécifiques ou des plugins individuels.

## 4. Onglet **Settings** - **Credentials** (Identifiants) :

- Pour des scans plus approfondis (scans authentifiés), vous pouvez fournir des identifiants (nom d'utilisateur et mot de passe) pour les systèmes cibles. Cela permet à Nessus de se connecter aux systèmes et de vérifier les vulnérabilités internes, les configurations logicielles, les correctifs manquants, etc. C'est fortement recommandé pour des résultats plus précis.

## 5. Onglet **Settings** - **Plugins** (Plugins) :

- Cette section vous permet de voir les familles de plugins activées pour ce scan. Vous pouvez affiner la sélection si vous souhaitez exclure certains types de tests.

## 6. Onglet **Schedule** (Planification) :

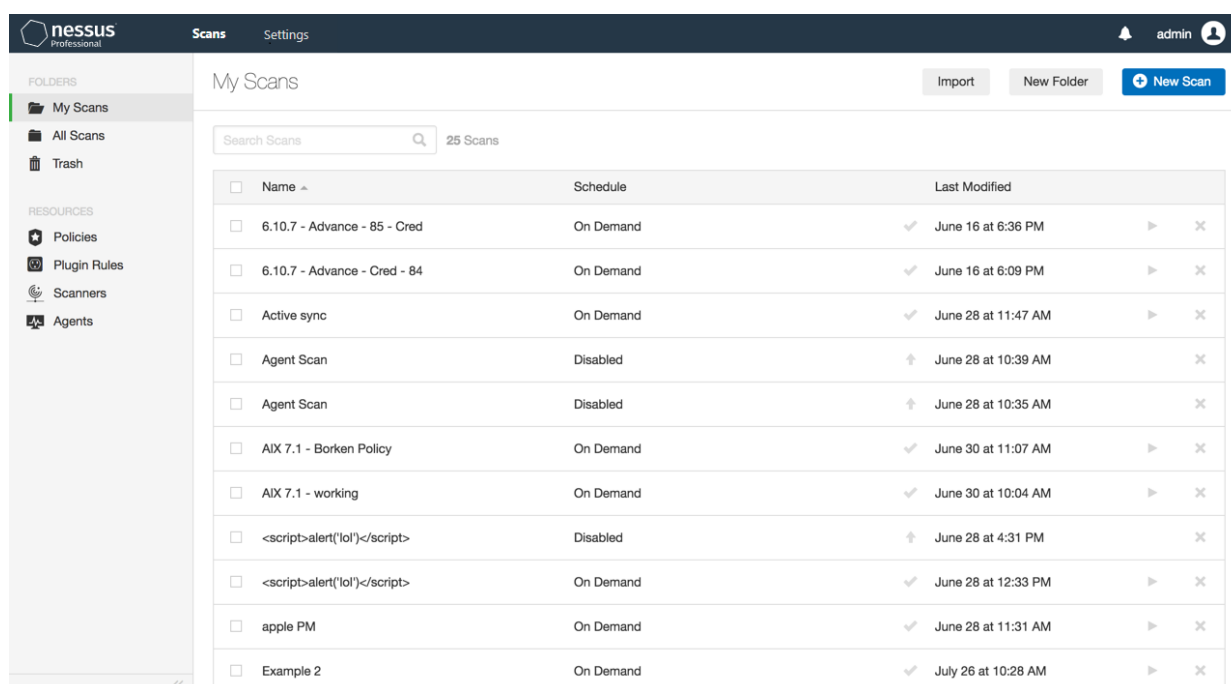
- Vous pouvez planifier le scan pour qu'il s'exécute une seule fois à une date et heure spécifiques, ou de manière récurrente (quotidienne, hebdomadaire, mensuelle).

## 7. Onglet **Notifications** (Notifications) :

- Configurez les notifications par e-mail pour être informé du début, de la fin ou des erreurs du scan.

## 4. Lancement du Scan

1. Une fois que vous avez configuré tous les paramètres, cliquez sur le bouton **Save** (Enregistrer) en bas de la page.
2. Le scan apparaîtra dans la liste sur la page **My Scans**.
3. Pour lancer le scan immédiatement, cliquez sur le bouton **Launch** (Lancer) (l'icône de lecture) à côté du nom du scan.



| <input type="checkbox"/> | Name                          | Schedule  | Last Modified         |   |   |
|--------------------------|-------------------------------|-----------|-----------------------|---|---|
| <input type="checkbox"/> | 6.10.7 - Advance - 85 - Cred  | On Demand | ✓ June 16 at 6:36 PM  | ▶ | ✕ |
| <input type="checkbox"/> | 6.10.7 - Advance - Cred - 84  | On Demand | ✓ June 16 at 6:09 PM  | ▶ | ✕ |
| <input type="checkbox"/> | Active sync                   | On Demand | ✓ June 28 at 11:47 AM | ▶ | ✕ |
| <input type="checkbox"/> | Agent Scan                    | Disabled  | ⬆ June 28 at 10:39 AM |   | ✕ |
| <input type="checkbox"/> | Agent Scan                    | Disabled  | ⬆ June 28 at 10:35 AM |   | ✕ |
| <input type="checkbox"/> | AIX 7.1 - Borken Policy       | On Demand | ✓ June 30 at 11:07 AM | ▶ | ✕ |
| <input type="checkbox"/> | AIX 7.1 - working             | On Demand | ✓ June 30 at 10:04 AM | ▶ | ✕ |
| <input type="checkbox"/> | <script>alert('lol')</script> | Disabled  | ⬆ June 28 at 4:31 PM  |   | ✕ |
| <input type="checkbox"/> | <script>alert('lol')</script> | On Demand | ✓ June 28 at 12:33 PM | ▶ | ✕ |
| <input type="checkbox"/> | apple PM                      | On Demand | ✓ June 28 at 11:31 AM | ▶ | ✕ |
| <input type="checkbox"/> | Example 2                     | On Demand | ✓ July 26 at 10:28 AM | ▶ | ✕ |

Figure 13: Lancement d'un scan Nessus depuis la page 'My Scans'.

4. Le statut du scan passera à **Running** (En cours d'exécution). Vous pouvez cliquer sur le nom du scan pour voir sa progression en temps réel.



## 5. Analyse des Résultats du Scan

Une fois le scan terminé, son statut passera à **Completed** (Terminé). Vous pouvez alors analyser les résultats.

### 1. Accédez aux Résultats du Scan :

- Sur la page **My Scans**, cliquez sur le nom du scan terminé.
- Cela vous mènera à la page de résumé du scan, qui fournit une vue d'ensemble des vulnérabilités découvertes.

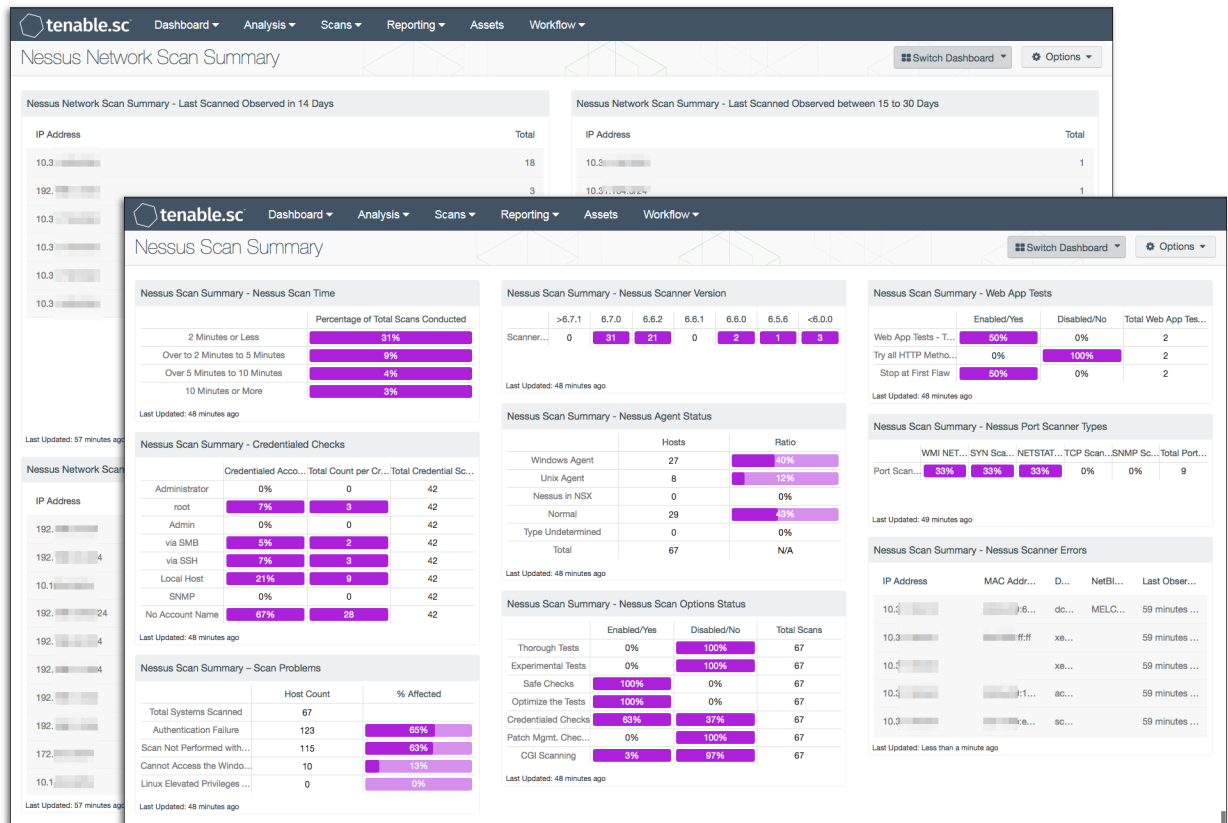


Figure 14: Page de résumé des résultats d'un scan Nessus, montrant les vulnérabilités par gravité.

### 2. Explorez les Vulnérabilités :

- La page de résumé affiche les vulnérabilités regroupées par gravité (Critique, Élevée, Moyenne, Faible, Informationnelle).
- Cliquez sur le nombre de vulnérabilités pour une catégorie de gravité (par exemple, **Critical**) pour voir la liste détaillée des vulnérabilités correspondantes.



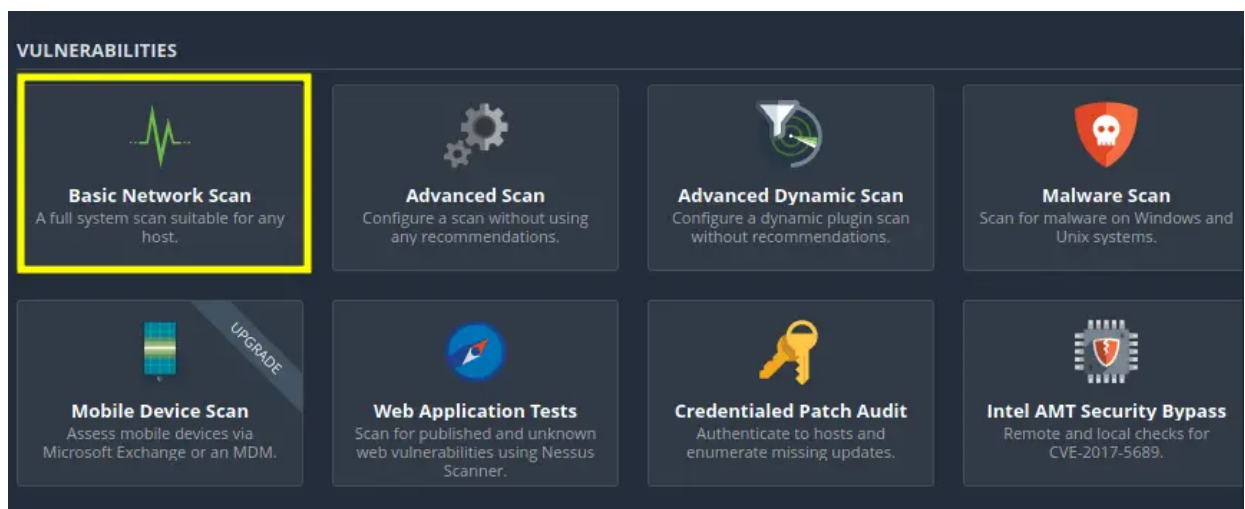


Figure 15: Liste détaillée des vulnérabilités découvertes, avec des informations sur chaque faille.

### 3. Détails de la Vulnérabilité :

- Cliquez sur une vulnérabilité spécifique pour afficher ses détails complets, y compris :
  - **Description** : Une explication de la vulnérabilité.
  - **Solution** : Les étapes recommandées pour corriger la vulnérabilité.
  - **Plugin Details** : Informations sur le plugin Nessus qui a détecté la vulnérabilité.
  - **Output** : La sortie brute du plugin, fournissant des preuves de la vulnérabilité.
  - **References** : Liens vers des bases de données de vulnérabilités (CVE, Bugtraq) pour plus d'informations.

New Scan / Policy1\_HTF

[Back to Scan Templates](#)

**Settings**

**BASIC**

- General
- Schedule
- Notifications

Name: Policy1\_HTF

Description:

Folder: My Scans

Targets: 192.168.43.161

Upload Targets Add File

Save Cancel

Figure 16: Vue détaillée d'une vulnérabilité, incluant la description, la solution et les références.

## 6. Génération de Rapports

Nessus permet de générer des rapports personnalisables pour documenter les résultats de vos scans.

### 1. Accédez aux Options de Rapport :

- Sur la page de résumé du scan, cliquez sur le bouton **Export** (Exporter) ou **Report** (Rapport).

### 2. Choisissez le Format du Rapport :

- Nessus prend en charge plusieurs formats de rapport, tels que PDF, HTML, CSV, et .nessus (pour l'importation dans d'autres instances Nessus ou Tenable.sc).
- Sélectionnez le format souhaité et les options de personnalisation (par exemple, inclure uniquement les vulnérabilités critiques, exclure les informations).

### 3. Générez et Téléchargez le Rapport :

Cliquez sur **Generate Report** (Générer le Rapport) et une fois le rapport prêt, vous pourrez le télécharger.

Ces étapes couvrent le processus fondamental de l'utilisation de Nessus pour l'évaluation des vulnérabilités. Pour des scénarios plus avancés, vous pouvez explorer les options de politiques de scan personnalisées, les scans authentifiés, et l'intégration avec d'autres outils de sécurité.

## Fonctionnalités Avancées et Bonnes Pratiques avec Nessus

Pour tirer pleinement parti de Nessus et optimiser vos efforts d'évaluation des vulnérabilités, il est essentiel de comprendre et d'appliquer ses fonctionnalités avancées ainsi que les bonnes pratiques en matière de gestion des vulnérabilités.

### 1. Gestion des Politiques de Scan (Scan Policies)

Les politiques de scan sont le cœur de la flexibilité de Nessus. Elles définissent comment un scan est effectué, quels plugins sont activés, comment les cibles sont découvertes, et bien plus encore. Bien que Nessus propose des modèles de scan prédéfinis, la création de politiques personnalisées vous offre un contrôle granulaire sur vos analyses.

#### Accéder aux Politiques :

1. Dans l'interface web de Nessus, naviguez vers **Politiques** dans le menu supérieur.
2. Vous verrez une liste des politiques existantes. Cliquez sur **New Policy** pour en créer une nouvelle ou sur une politique existante pour la modifier.

#### Configuration d'une Politique Personnalisée :

- **Type de Scan** : Choisissez le type de scan (par exemple, **Advanced Scan** pour une personnalisation maximale).
- **Découverte (Discovery)** : Définissez les méthodes de découverte des hôtes et des ports. Vous pouvez spécifier des plages de ports, des méthodes de ping, etc.
- **Plugins** : C'est la section la plus importante. Vous pouvez activer ou désactiver des familles de plugins entières ou des plugins individuels. Par exemple, si vous ne scannez pas de serveurs web, vous pouvez désactiver les plugins liés aux applications web pour accélérer le scan.
  - **Plugins par Famille** : Organisés par catégorie (par exemple, **General**, **Windows**, **Web Servers**, **Databases**).
  - **Plugins Individuels** : Vous pouvez rechercher des plugins spécifiques par leur ID ou leur nom.
- **Authentification (Credentials)** : Configurez les identifiants pour les scans authentifiés (voir section suivante).

- **Préférences** : Ajustez des paramètres avancés comme la simultanéité des hôtes, la simultanéité des vérifications par hôte, les délais d'attente, etc.

La personnalisation des politiques permet d'adapter Nessus à des environnements spécifiques, de réduire le temps de scan en excluant les vérifications non pertinentes, et d'améliorer la précision des résultats.

## 2. Scans Authentifiés vs. Non Authentifiés

La différence entre un scan authentifié et un scan non authentifié est cruciale pour la profondeur et la précision de vos évaluations de vulnérabilités.

- **Scan Non Authentifié (External Scan)** :
  - Simule une attaque externe, sans connaissance préalable du système cible.
  - Ne peut détecter que les vulnérabilités accessibles depuis l'extérieur (ports ouverts, services exposés, vulnérabilités web).
  - Ne peut pas vérifier les configurations internes, les correctifs manquants, les logiciels obsolètes installés localement, ou les faiblesses de configuration du système d'exploitation.
- **Scan Authentifié (Internal Scan / Credentialed Scan)** :
  - Nessus se connecte au système cible avec des identifiants valides (SSH pour Linux/Unix, SMB pour Windows, SNMP pour les équipements réseau, etc.).
  - Permet à Nessus d'accéder aux informations internes du système, comme les versions logicielles, les fichiers de configuration, les journaux d'événements, et l'état des correctifs.
  - **Avantages** : Détection beaucoup plus complète et précise des vulnérabilités, y compris les configurations erronées, les logiciels non patchés, les faiblesses de mots de passe locaux, et les vulnérabilités qui ne sont pas exposées publiquement.
  - **Recommandation** : Toujours privilégier les scans authentifiés lorsque cela est possible, car ils fournissent une image beaucoup plus fidèle de la posture de sécurité de vos systèmes.

### Configuration des Identifiants :

1. Lors de la création ou de la modification d'un scan, naviguez vers l'onglet **Credentials**.
2. Sélectionnez le type d'identifiants (par exemple, **Windows**, **SSH**, **SNMP**).
3. Entrez les informations d'identification requises (nom d'utilisateur, mot de passe, clé SSH, etc.).

4. Assurez-vous que les privilèges du compte utilisé sont suffisants pour permettre à Nessus d'accéder aux informations nécessaires (par exemple, un compte administrateur local pour Windows, ou un utilisateur avec des privilèges sudo pour Linux).

### 3. Gestion des Plugins et Mises à Jour

Les plugins sont les signatures de vulnérabilités utilisées par Nessus. Leur mise à jour régulière est essentielle pour garantir que Nessus peut détecter les menaces les plus récentes.

- **Mises à Jour Automatiques** : Par défaut, Nessus est configuré pour télécharger et compiler automatiquement les dernières mises à jour de plugins. Assurez-vous que votre instance Nessus a un accès Internet pour cela.
- **Mises à Jour Manuelles (Offline)** : Pour les environnements isolés, Nessus permet des mises à jour de plugins hors ligne via un fichier `nessus-fetch.rc`. Ce processus est plus complexe et nécessite de télécharger le fichier de mise à jour depuis un système connecté à Internet.
- **Comprendre les Plugins** : Chaque plugin a un ID unique et est associé à une ou plusieurs vulnérabilités. Vous pouvez rechercher des plugins spécifiques dans l'interface de Nessus pour comprendre ce qu'ils détectent et comment ils fonctionnent.

### 4. Analyse et Interprétation des Rapports

Les rapports de Nessus sont riches en informations. Une bonne interprétation est cruciale pour une gestion efficace des vulnérabilités.

- **Priorisation** : Concentrez-vous d'abord sur les vulnérabilités de gravité `Critical` et `High`. Ce sont celles qui présentent le risque le plus élevé pour votre organisation.
- **Solution** : Nessus fournit des recommandations de solution pour chaque vulnérabilité. Suivez ces recommandations pour corriger les failles.
- **Contexte** : Comprenez le contexte de la vulnérabilité. Une vulnérabilité critique sur un système non exposé à Internet peut avoir une priorité différente de la même vulnérabilité sur un serveur web public.
- **Faux Positifs** : Nessus est très précis, mais des faux positifs peuvent occasionnellement se produire. Vérifiez manuellement les vulnérabilités critiques si vous avez des doutes.
- **Tendances** : Utilisez les rapports de Nessus pour suivre les tendances de sécurité de votre environnement. Les vulnérabilités augmentent-elles ou diminuent-elles ? Les efforts de correction sont-ils efficaces ?

## 5. Intégration avec d'Autres Outils

Nessus peut être intégré à d'autres outils de sécurité pour automatiser les flux de travail et améliorer la gestion des vulnérabilités :

- **SIEM (Security Information and Event Management)** : Envoyez les résultats de scan Nessus à votre SIEM pour une corrélation avec d'autres événements de sécurité.
- **Ticketing Systems** : Créez automatiquement des tickets pour les vulnérabilités découvertes dans votre système de gestion des incidents ou des tâches.
- **Plateformes de Gestion des Vulnérabilités** : Tenable.sc (anciennement SecurityCenter) et Tenable.io sont des plateformes de gestion des vulnérabilités de Tenable qui s'intègrent nativement avec Nessus pour une gestion centralisée des scans, des rapports et des remédiations à grande échelle.

## 6. Bonnes Pratiques en Matière de Scans de Vulnérabilités

- **Scans Réguliers** : Effectuez des scans de vulnérabilités régulièrement (quotidiennement, hebdomadairement, mensuellement) pour détecter rapidement les nouvelles failles.
- **Scans Authentifiés** : Privilégiez toujours les scans authentifiés pour une couverture maximale.
- **Scans sur Différents Segments Réseau** : Scannez depuis différentes positions sur votre réseau (interne, externe, DMZ) pour avoir une vue complète de votre surface d'attaque.
- **Gestion des Correctifs** : L'identification des vulnérabilités n'est que la première étape. Mettez en place un processus robuste de gestion des correctifs pour corriger les failles découvertes.
- **Tests de Pénétration** : Les scans de vulnérabilités identifient les failles, mais les tests de pénétration simulent des attaques réelles pour valider l'exploitabilité des vulnérabilités et évaluer l'impact réel sur votre organisation.
- **Formation Continue** : Le paysage des menaces évolue constamment. Restez informé des dernières vulnérabilités et des meilleures pratiques de sécurité.

En adoptant ces fonctionnalités avancées et ces bonnes pratiques, Nessus deviendra un atout inestimable dans votre stratégie de cybersécurité, vous permettant de maintenir une posture de sécurité solide et de protéger vos actifs numériques contre les menaces en constante évolution.

# Conclusion : Nessus, Votre Allié Incontournable pour la Cybersécurité

Nessus s'est imposé comme l'outil de référence en matière d'évaluation des vulnérabilités, et ce manuel a eu pour objectif de vous guider à travers ses fonctionnalités, de l'installation initiale à l'analyse approfondie des résultats. Nous avons exploré comment Nessus, grâce à sa vaste base de plugins et ses capacités de scan authentifié, peut vous offrir une visibilité inégalée sur les faiblesses de votre infrastructure informatique.

La cybersécurité est un domaine en constante évolution, et la détection proactive des vulnérabilités est une composante essentielle de toute stratégie de défense robuste. Nessus ne se contente pas de pointer du doigt les problèmes ; il fournit des informations exploitables et des recommandations claires pour la remédiation, transformant ainsi la complexité des failles de sécurité en étapes concrètes pour renforcer votre posture.

En maîtrisant Nessus, vous acquérez la capacité de :

- **Identifier** rapidement et précisément les vulnérabilités.
- **Prioriser** les risques en fonction de leur gravité et de leur impact potentiel.
- **Gérer** efficacement le cycle de vie des vulnérabilités, de la détection à la correction.
- **Maintenir** la conformité avec les normes de sécurité et les réglementations.

N'oubliez pas que Nessus est un outil puissant, et comme tout outil puissant, il doit être utilisé de manière responsable et éthique. La pratique régulière, l'expérimentation avec différentes politiques de scan, et une compréhension approfondie des résultats sont les clés pour devenir un expert en évaluation des vulnérabilités.

Ce manuel est une fondation solide pour votre parcours avec Nessus. Continuez à explorer la documentation officielle de Tenable, à participer à la communauté de la cybersécurité, et à rester informé des dernières menaces et des meilleures pratiques. Avec Nessus à vos côtés, vous êtes mieux équipé pour protéger vos systèmes et vos données dans le paysage numérique actuel.