**Procédure d’utilisation Nessus**

**SOMMAIRE**

1 Objet du document 3

2 Nessus 3

2.1 Connexion à Nessus 3

2.2 Scan de vulnérabilités 3

2.2.1 Mise à jour des Plugins 3

2.2.2 Création et lancement du Scan 6

2.2.3 Résultat du scan 8

2.2.4 Export du résultat 10

2.3 Support 11

2.3.1 Problème d'indexation des plugins 11

# Objet du document

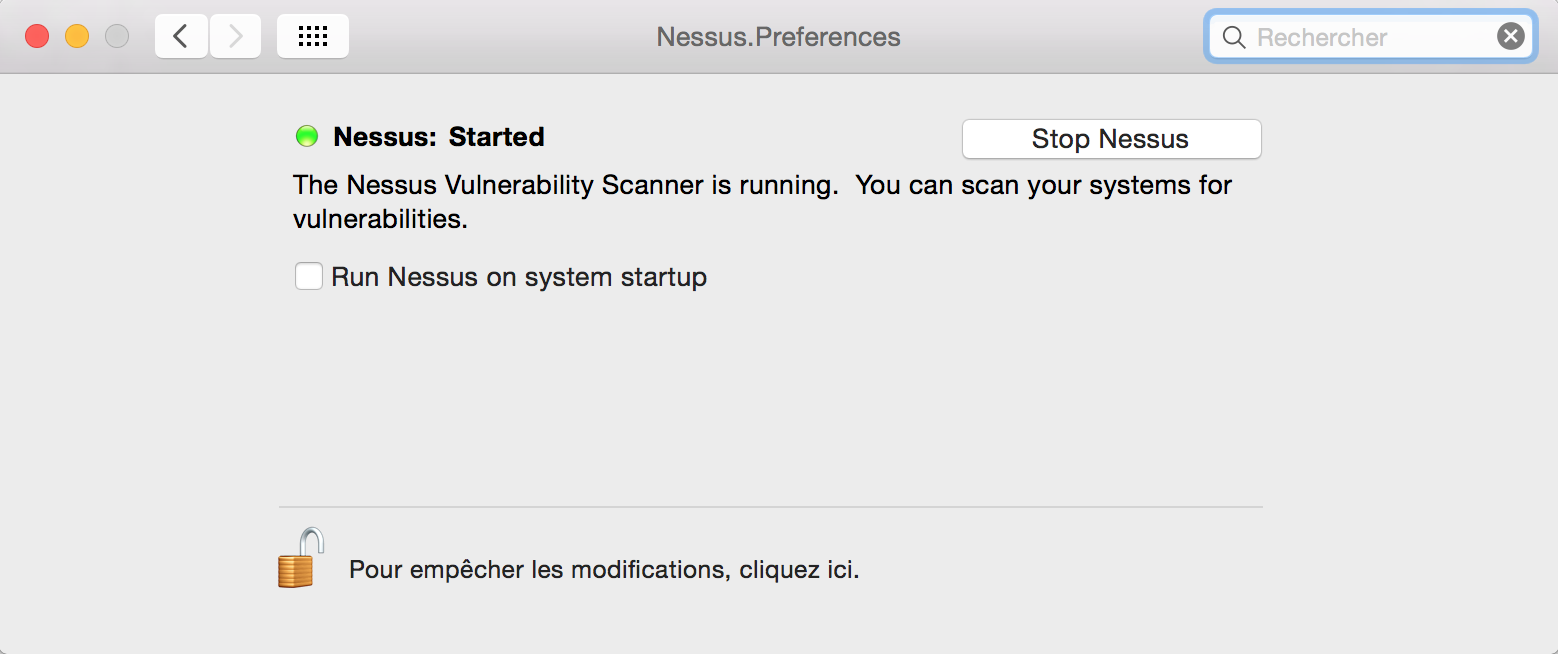
Ce document présente la procédure d’utilisation de l’outil **Nessus**.

# Nessus

## Connexion à Nessus

Pour utiliser Nessus, se connecter à l’adresse <https://localhost:8834>.

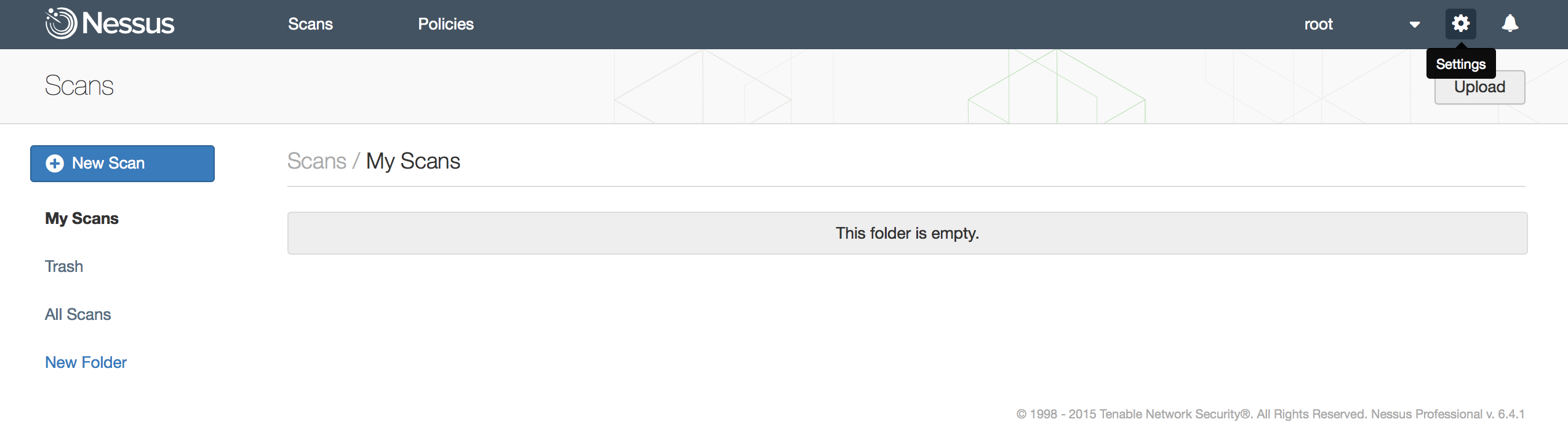
Si l’URL ne répond pas, aller dans **Préférences Système** du Mac, cliquer sur **Nessus** et cliquer sur le bouton **Start Nessus** pour démarrer le service :

****

## Scan de vulnérabilités

### Mise à jour des Plugins

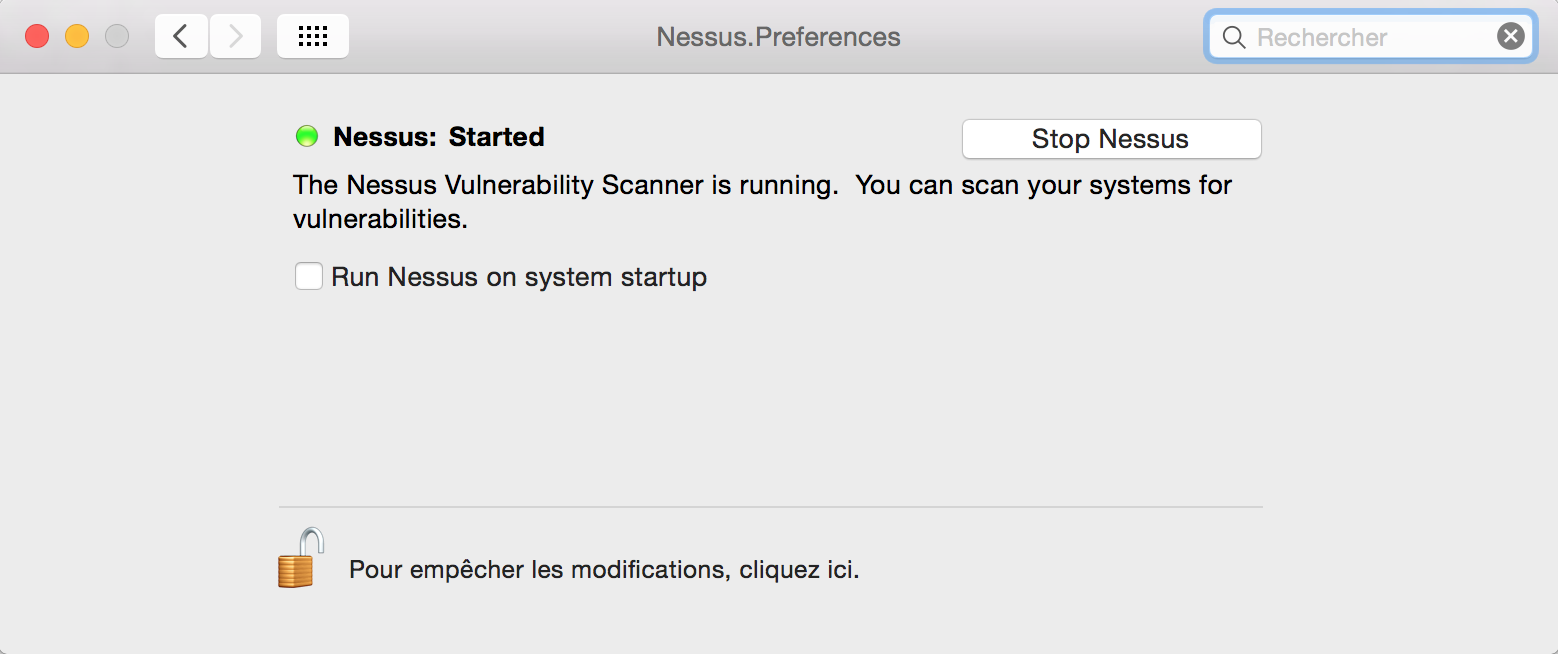
1. Cliquer sur le bouton **Settings** sous forme d'engrenage en haut à droite de l'interface.



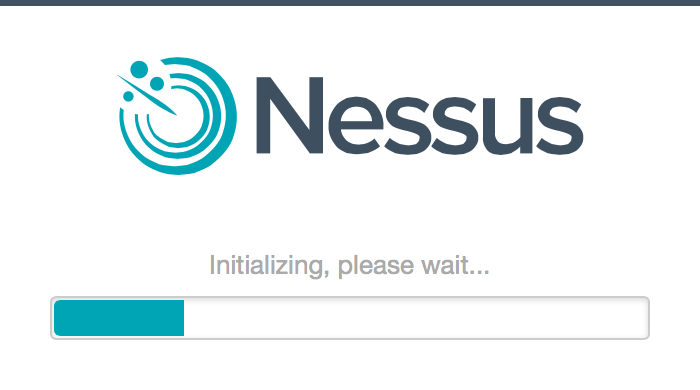
1. Dans la section **Plugins** de la fenêtre et en correspondance de **Last Updated**, cliquer sur le bouton en forme de flèches à droite de la date.

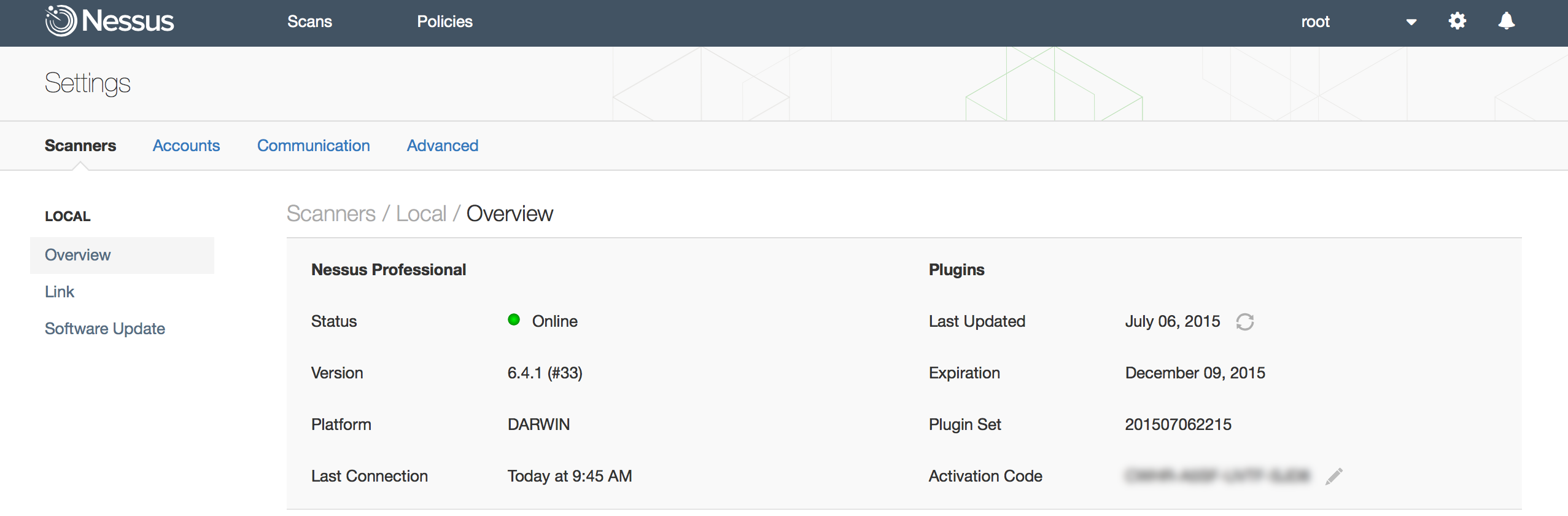
### 

1. Stopper et démarrer **Nessus**.  
   Aller dans le **Préférences Système** du Mac, cliquer sur **Nessus** et cliquer sur le bouton **Start Nessus** pour démarrer le service.

****

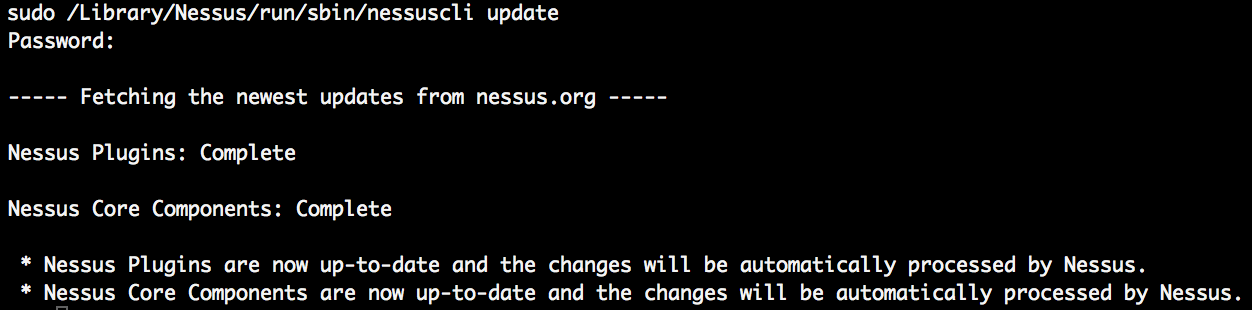
1. Se connecter à nouveau à l’adresse <https://localhost:8834>. Une barre de progression devrait apparait initialisant Nessus.  
   Les valeurs de **Last Updated** et de **Plugin Set** devraient être changées si la mise à jours a bien été effectuée.



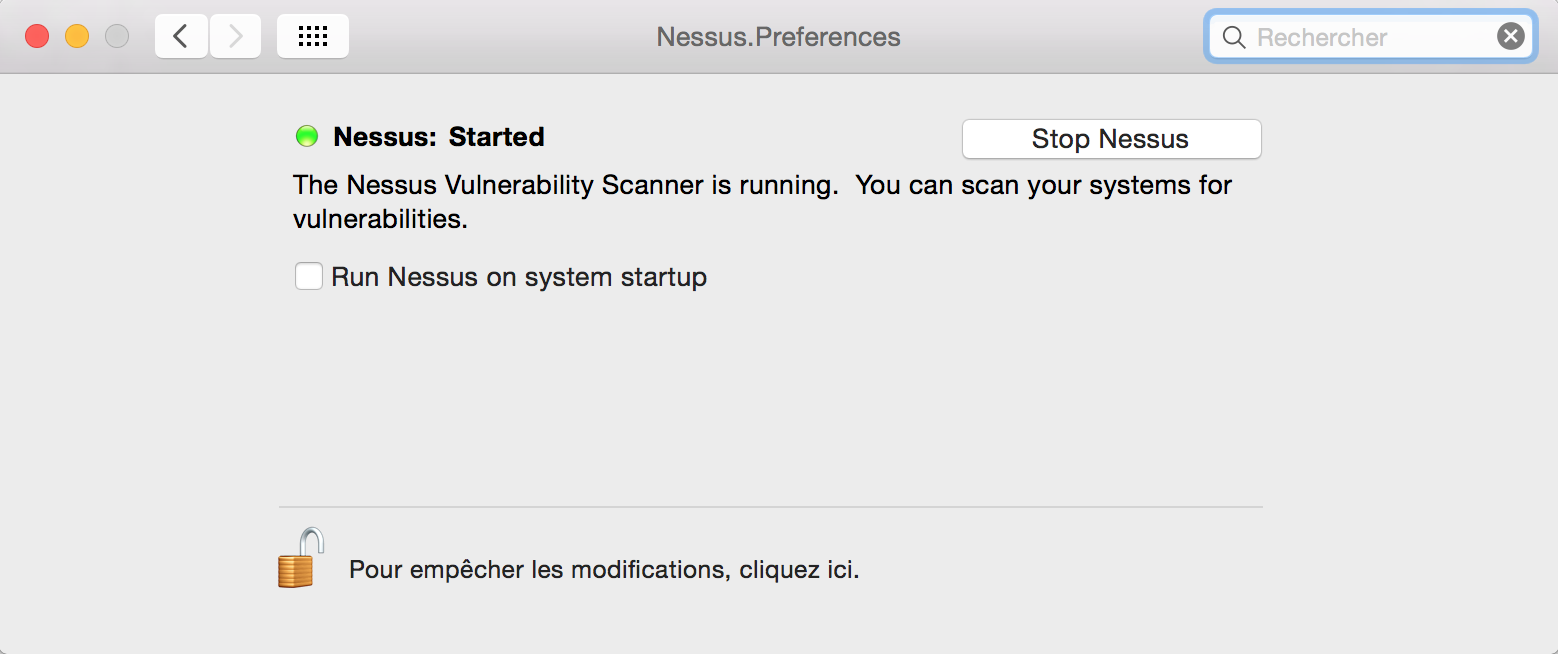


Si la mise à jour, par l’interface web ne s’exécute pas, procéder en ligne de commande.

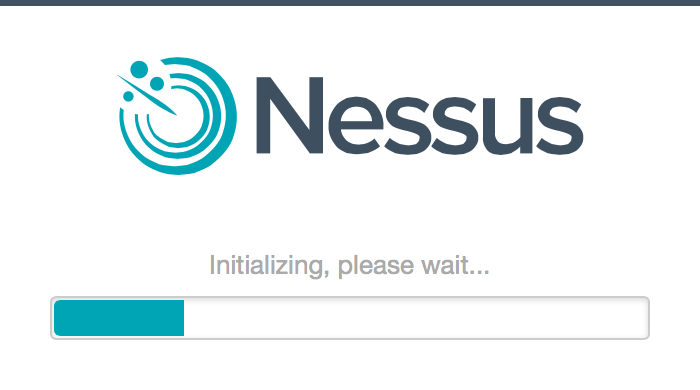
1. Stopper le service Nessus et exécuter la commande suivante dans un terminal : **sudo /Library/Nessus/run/sbin/nessuscli update**

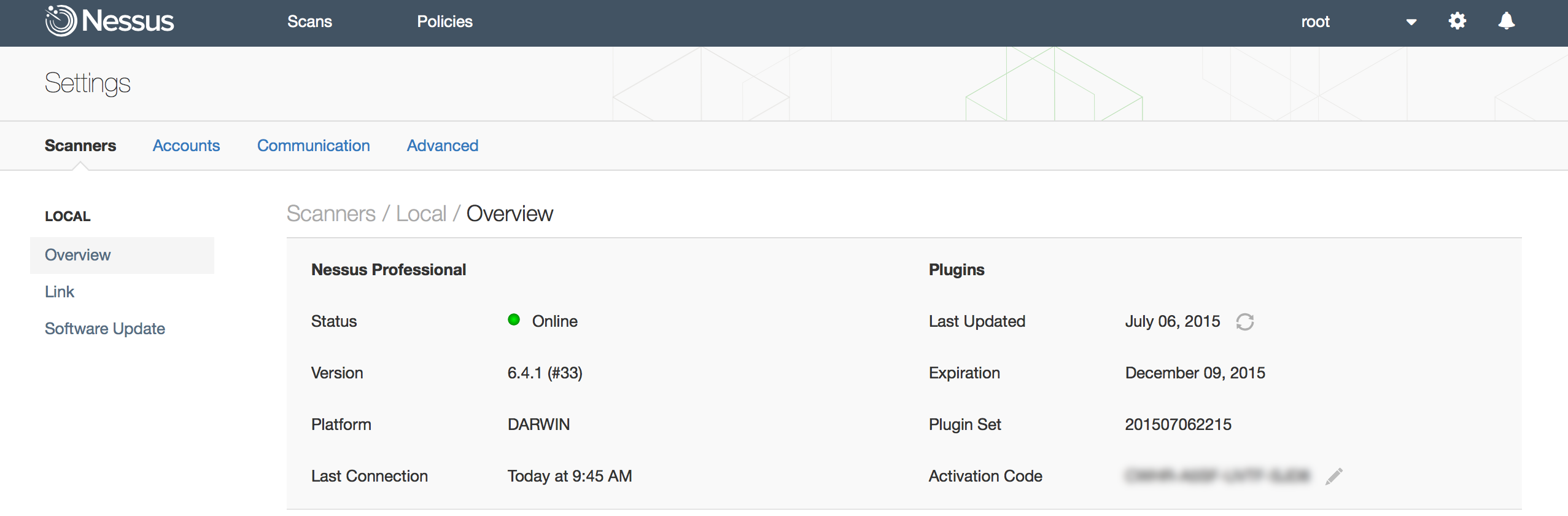


1. Stopper et démarrer **Nessus**.  
   Aller dans le **Préférences Système** du Mac, cliquer sur **Nessus** et cliquer sur le bouton **Start Nessus** pour démarrer le service.

****

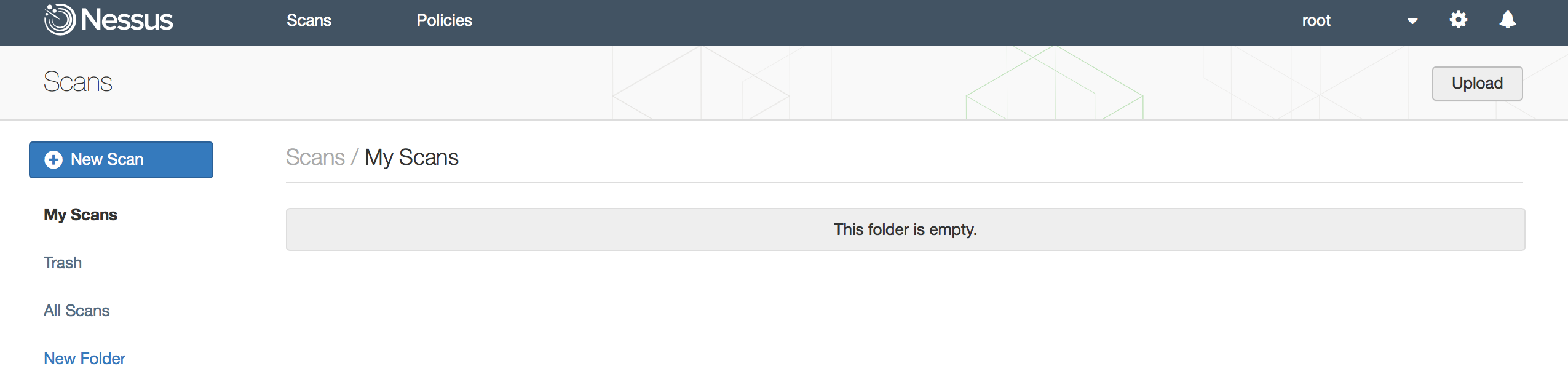
1. Se connecter à nouveau à l’adresse <https://localhost:8834>. Une barre de progression devrait apparait initialisant Nessus.  
   Les valeurs de **Last Updated** et de **Plugin Set** devraient être changées si la mise à jours a bien été effectuée.



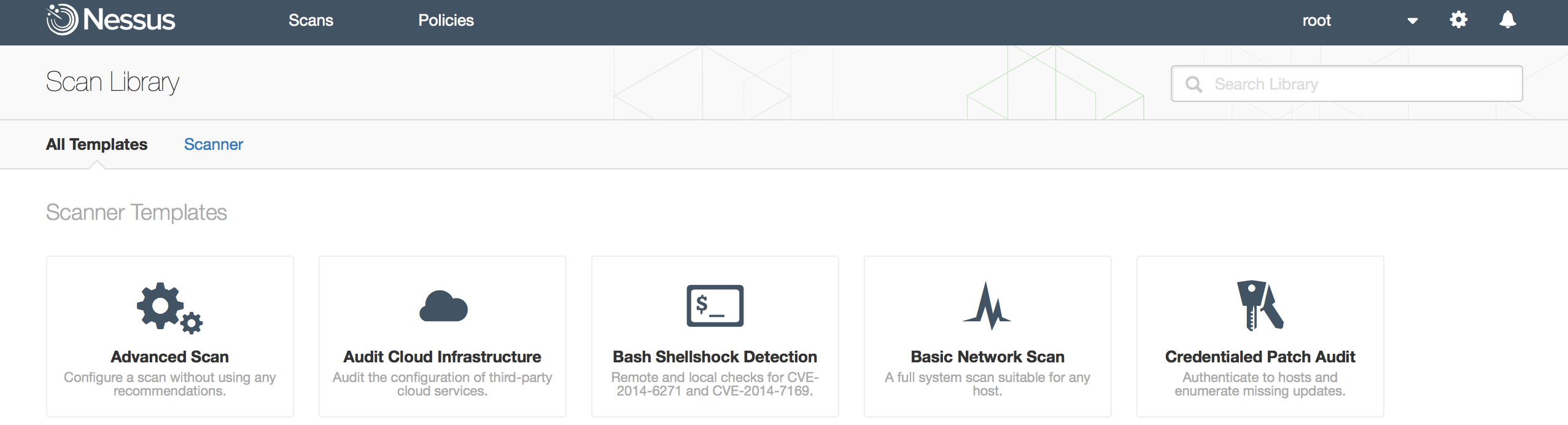


### Création et lancement du Scan

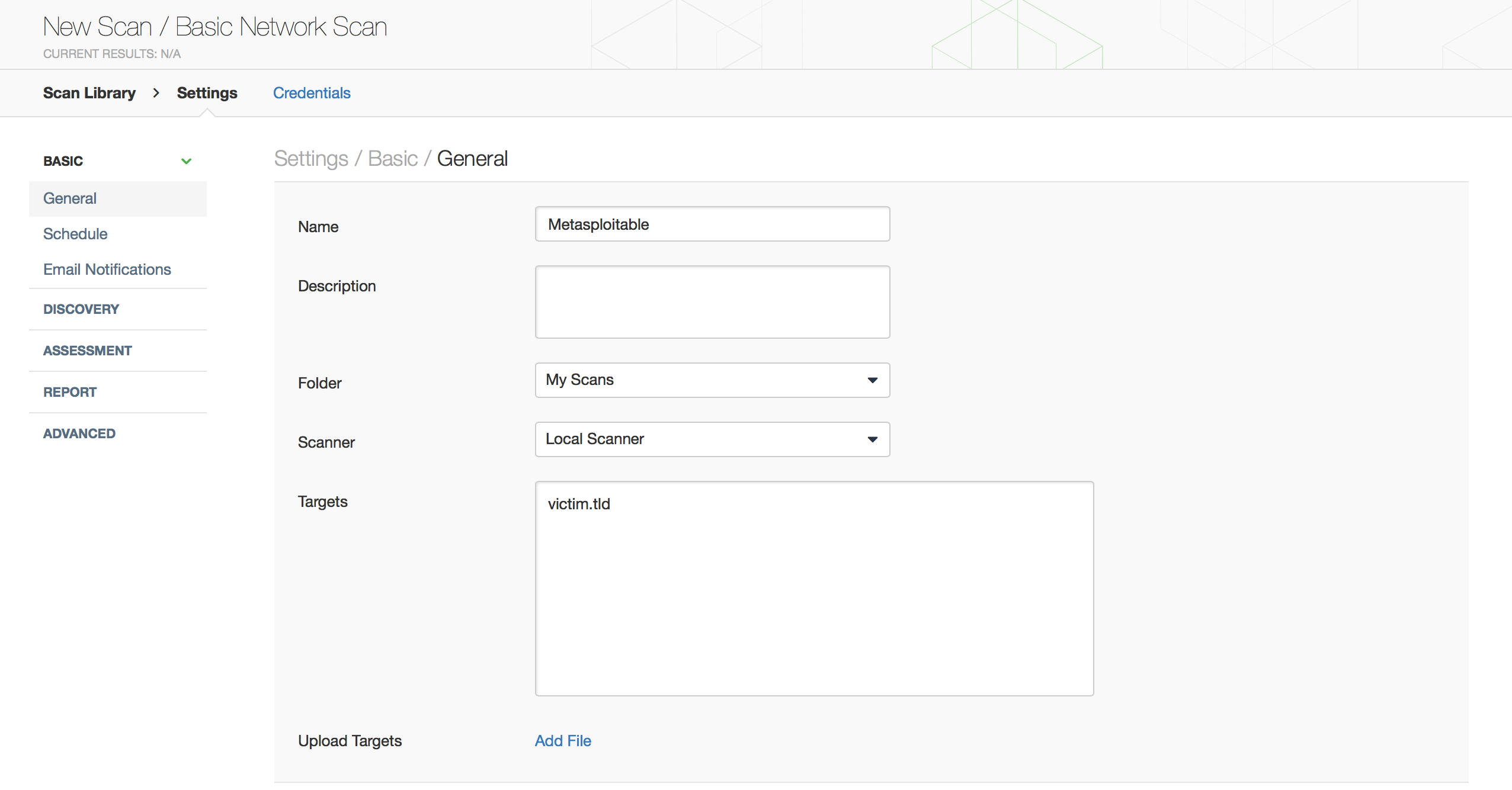
1. Pour commencer, cliquer sur le lien **Scan** situé en haut de la fenêtre et ensuite cliquer sur **New Scan**.



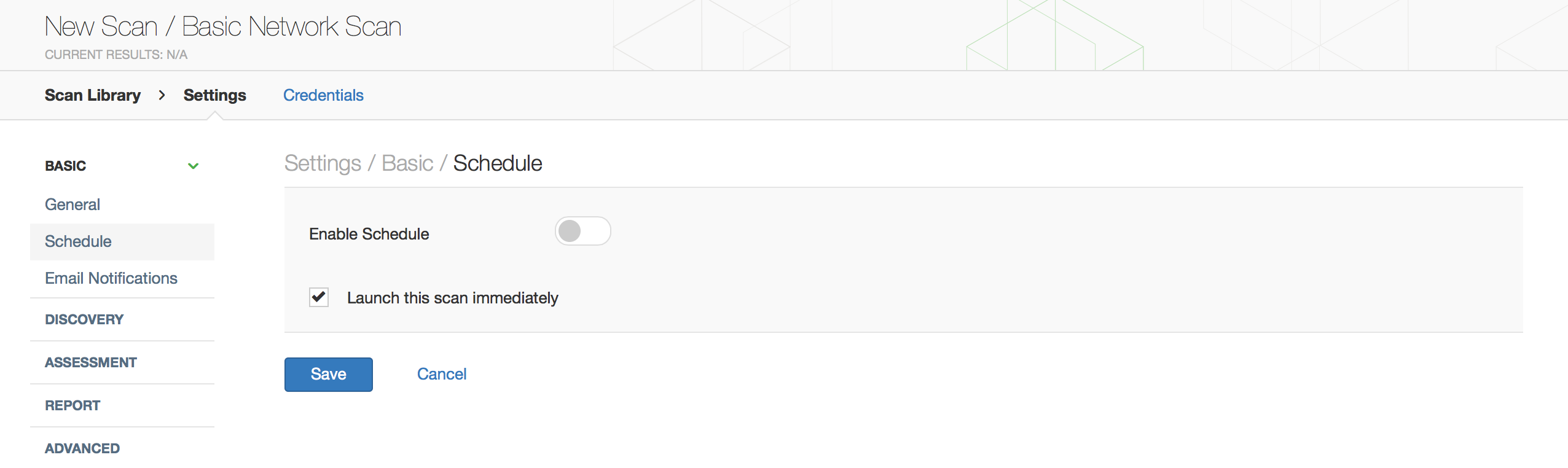
1. La fenêtre suivante montre plusieurs Templates de scan. Choisir **Basic Network Scan**.



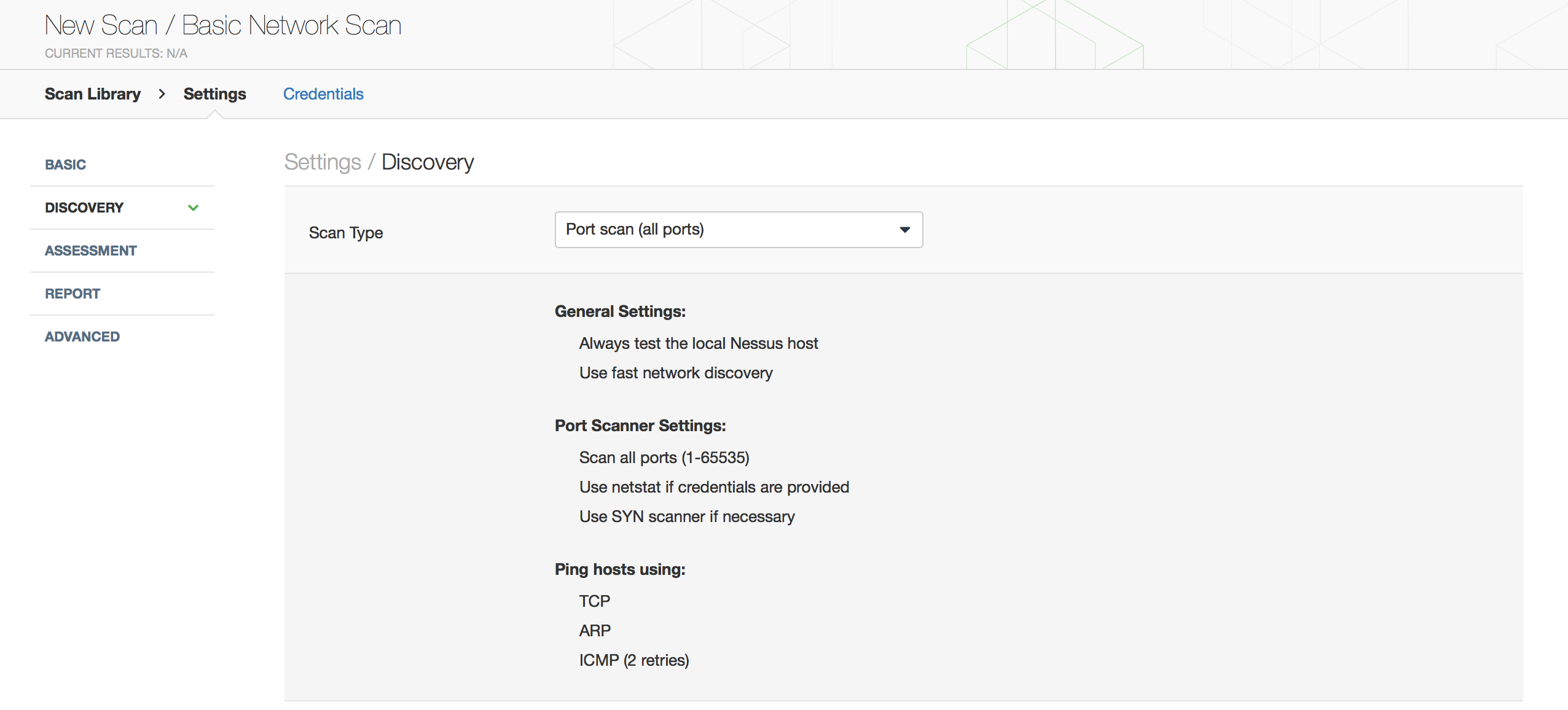
1. Donnez un nom au Scan et saisir, dans le champ **Targets**, les adresses IP et/ou les noms de domaine à scanner.



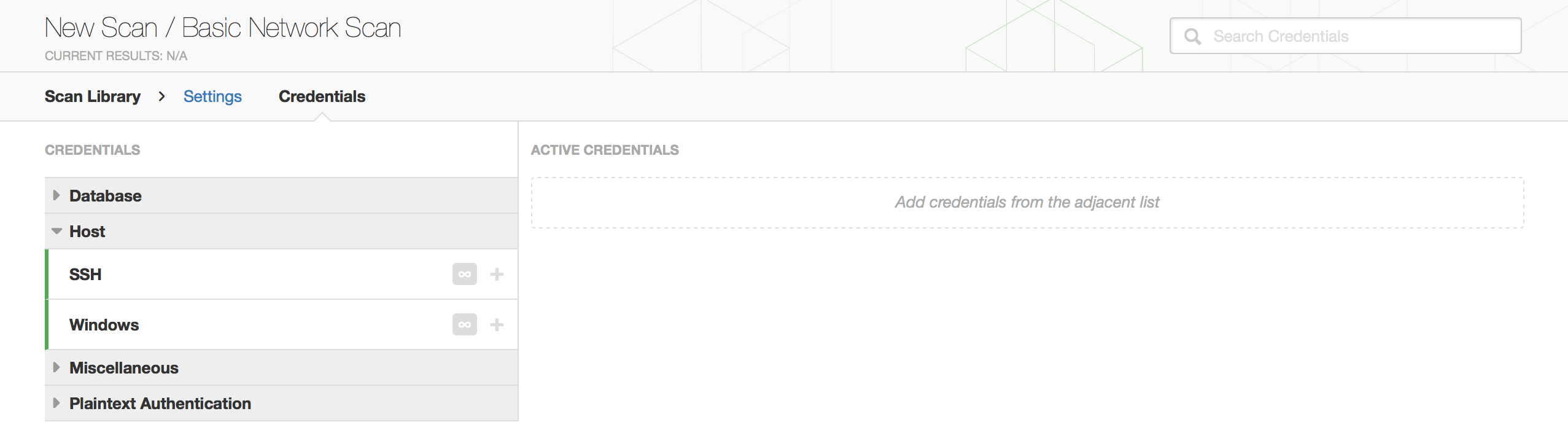
1. L’onglet **Schedule Settings** permet de configurer le scan pour qu’il s’exécute immédiatement, à une date ultérieure ou de façon récursive.



1. Cliquer sur l'onglet **Discovery** afin de sélectionner le type de scan de ports. Choisir **Port scan (all ports)**.



1. L'onglet **Credentials**, permet d'effectuer un scan en mode connecté.

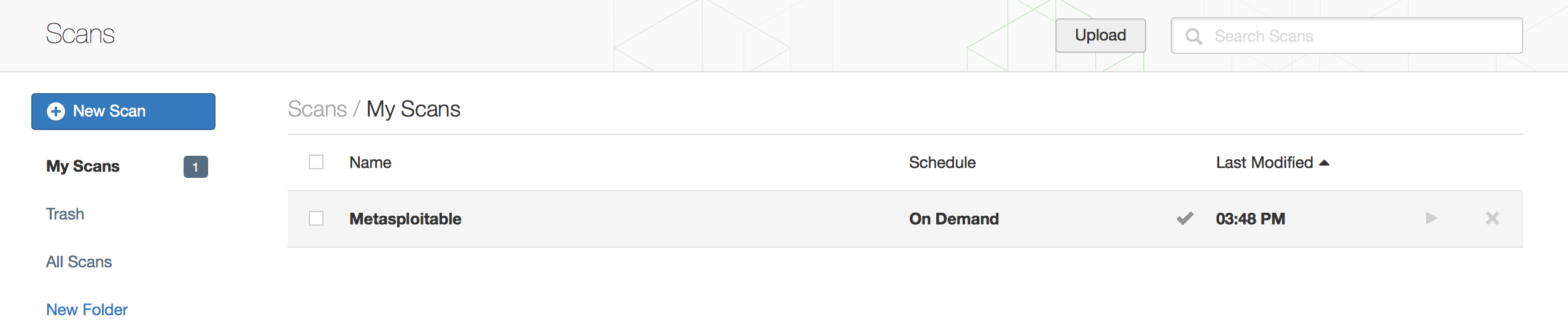


1. Cliquer sur le bouton **Save** afin de lancer le scan.

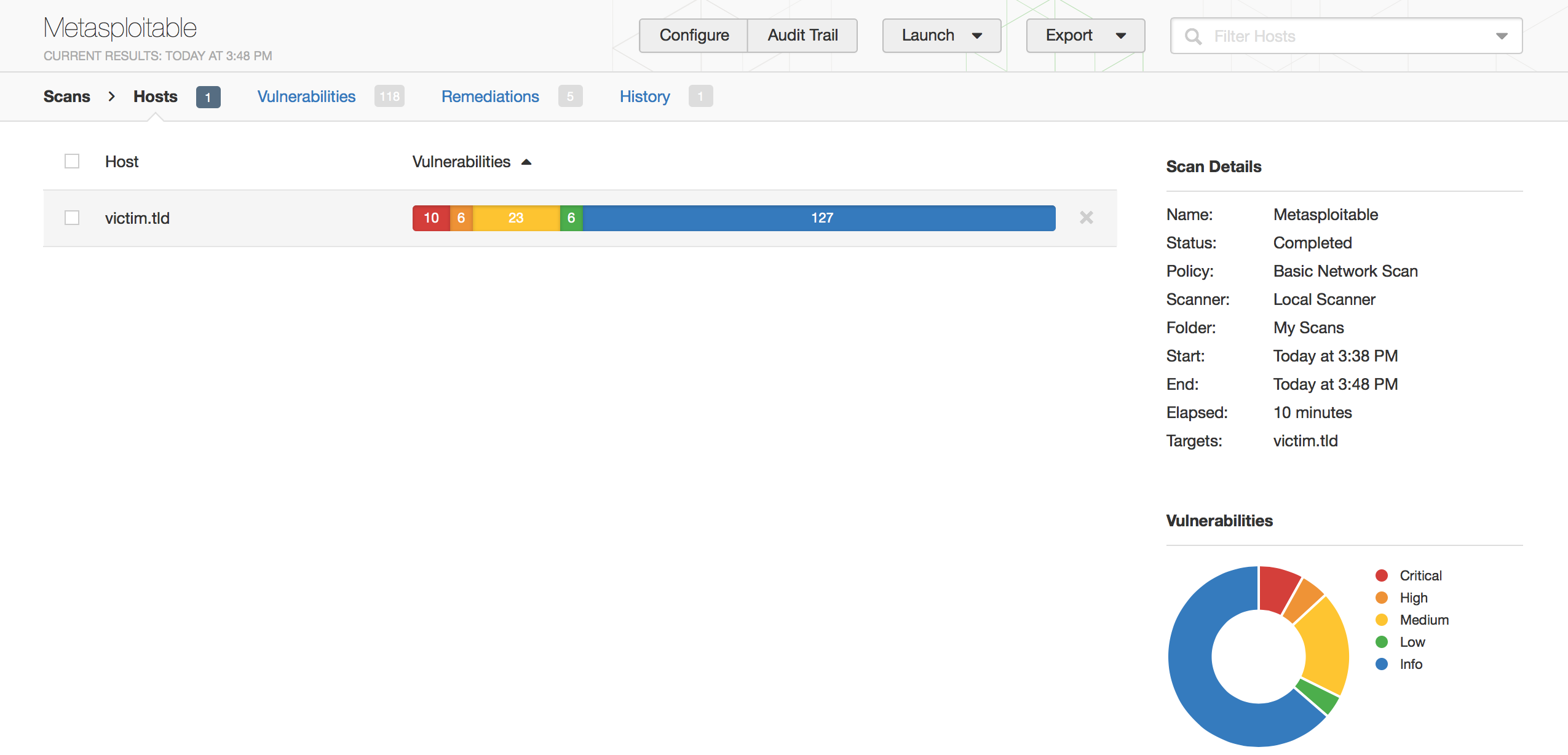


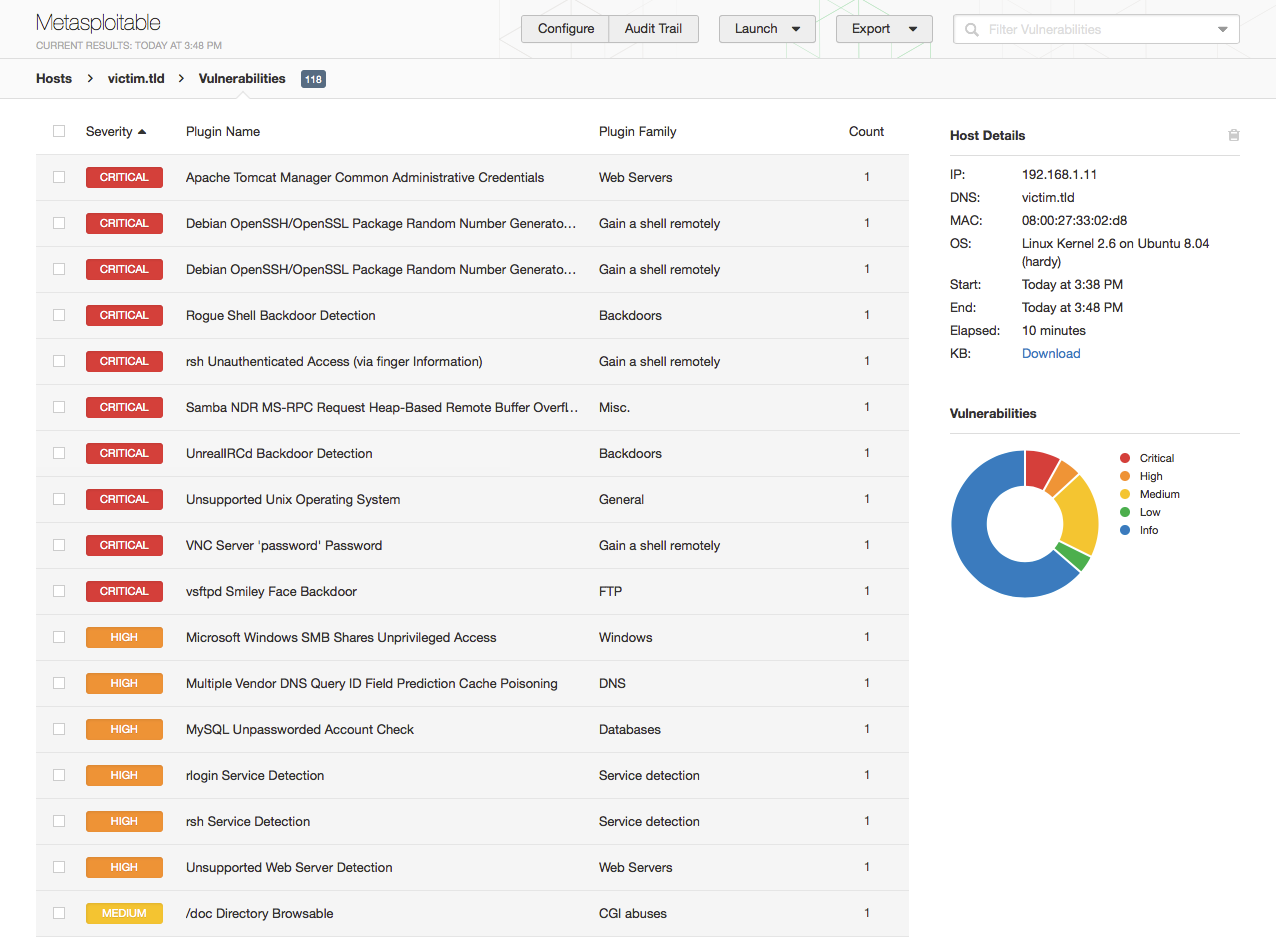
### Résultat du scan

1. Une fois le scan terminé, l’interface Nessus vous en informe.

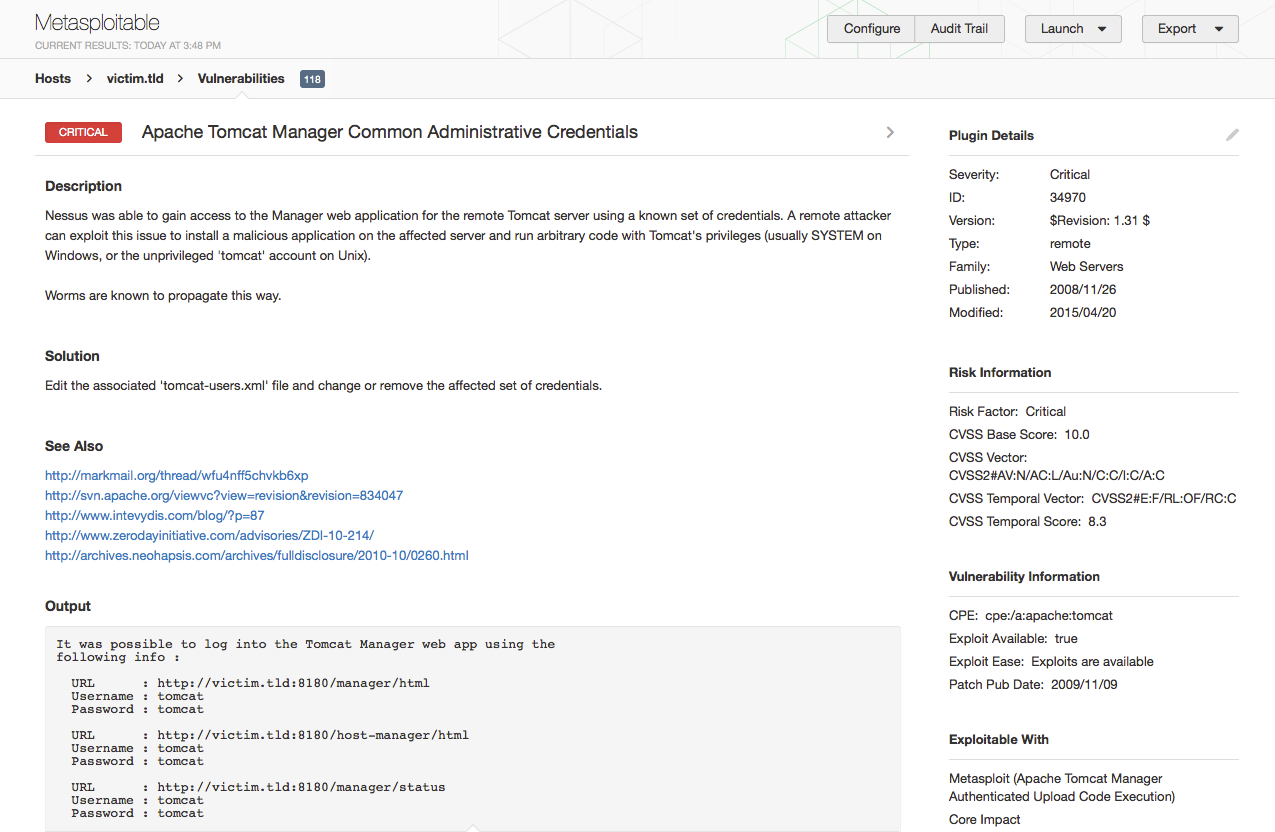


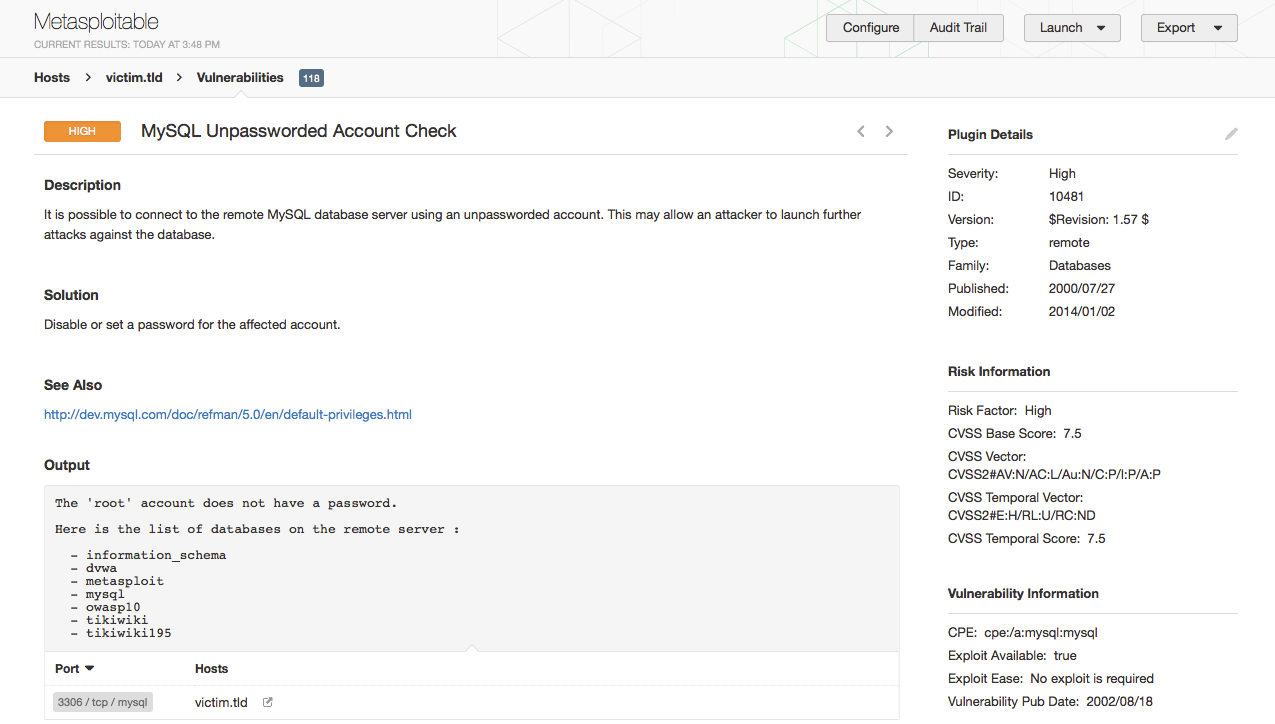
1. La fenêtre suivante donne un aperçu du résultat. Cliquer sur l’adresse IP ou le nom de domaine de la cible pour visualiser plus de détails.





1. En cliquant sur une vulnérabilité, il est possible d'en découvrir les détails et éventuellement comment pouvoir exploiter la faille. Dans l’exemple, le quarré nommé **Exploitable With**, permet de constater que la faille est exploitable avec l’outil Metasploit au travers de l’exploit nommé *Apache Tomcat Manager Authenticated Upload Code Execution* et aussi avec l’outil Core Impact. Dans le deuxième exemple il est possible de découvrer que le mot de passe *root* de MySQL est vide et Nessus a énuméré les bases de données trouvées sur le serveur.

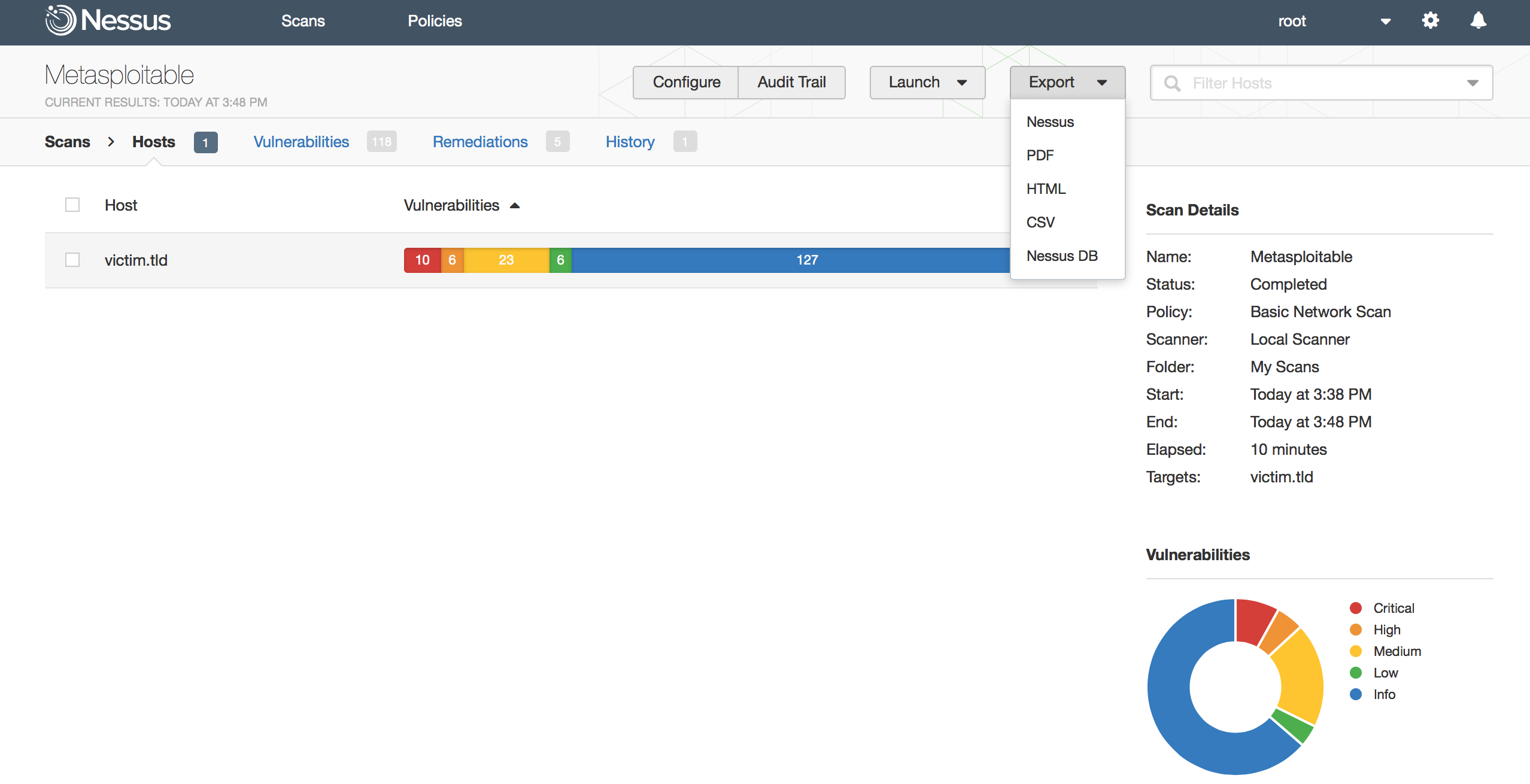




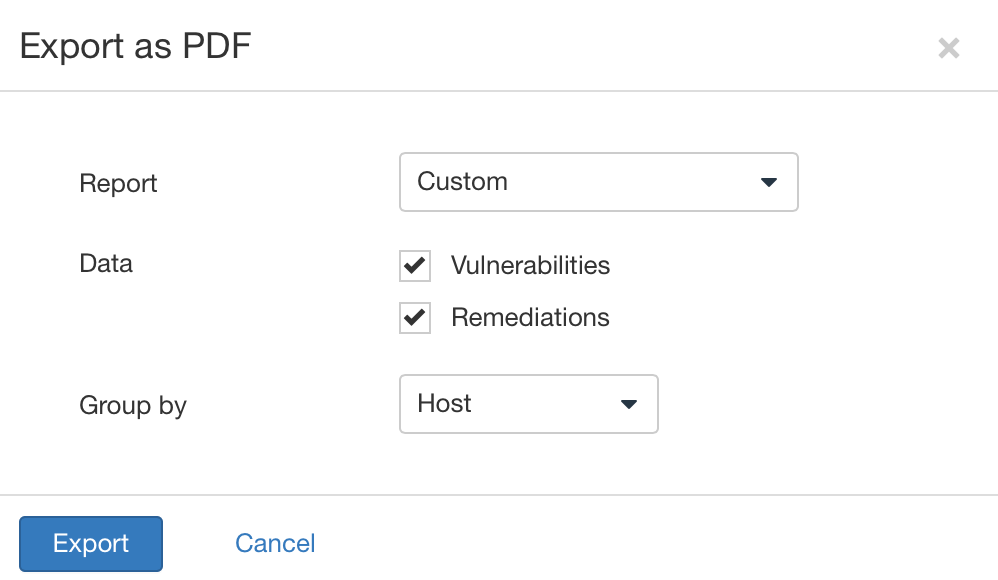
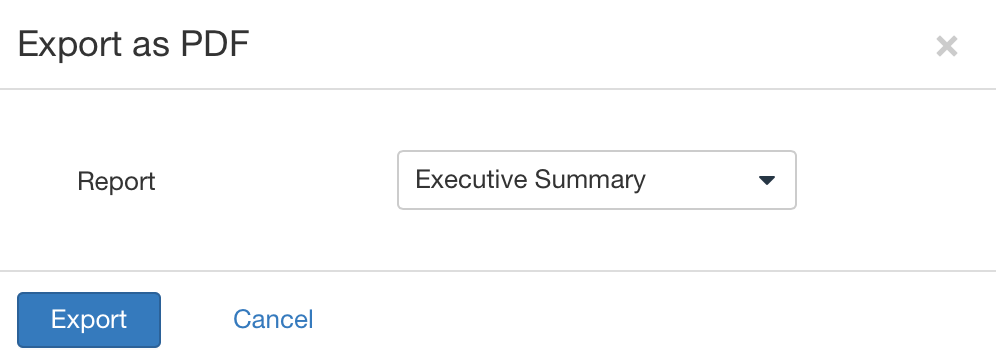
### Export du résultat

Il peut être intéressant d’exporter le résultat pour le réutiliser avec d’autres logiciels, dont ceux utilisés pour l’étape d’exploitation.

1. Pour exporter un rapport, se positionner sur le rapport de votre choix et cliquer sur le bouton **Export** et choisir le format désiré.



1. Sélectionner le type d'export désiré : **Executive Summary** ou personnaliser les éléments que vous souhaitez faire apparaitre dans le rapport. Cliquer sur **Export** pour terminer.

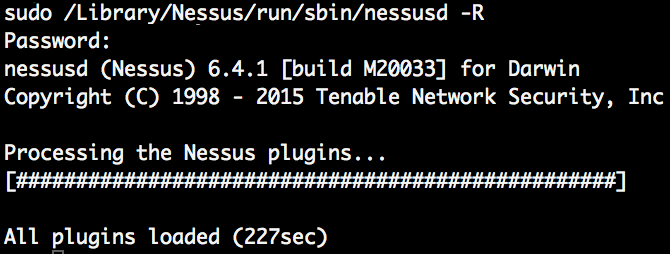


## Support

### Problème d'indexation des plugins

Il est possible de se trouver confrontés à un problème d'indexation des plugins. Ceci se matérialise lorsque les plugins n'apparaissent pas dans l'onglet **Plugins** ou lorsque la description des Plugins ne s'affiche pas correctement.

Pour remercier à cela, exécuter la commande suivante dans un terminal :



* XXXX
* XXXX