|  |  |
| --- | --- |
|  | **Analyse de vulnérabilités** |

# Présentation

Nessus est un **balayeur (*scanner*) de vulnérabilité** propriétaire développé par Tenable.

Les analyses Nessus couvrent un large éventail de technologies, notamment …

* les **systèmes d'exploitation** ;
* les **périphériques réseau** ;
* les **hyperviseurs** ;
* les **bases de données** ;
* les **serveurs Web**   
  et
* les **infrastructures critiques**.

Les **résultats de l'analyse** peuvent être **rapportés dans divers formats**, tels que **texte brut**, **XML**, **HTML** et **LaTeX** .   
Les résultats peuvent également être enregistrés dans une base de connaissances pour le débogage.

Sous **Linux**, l'analyse peut être **automatisée à l’aide de l'utilisation d'un client en ligne de commande**.   
Il existe de nombreux outils commerciaux, gratuits et open source pour Linux et Windows pour gérer les balayeurs Nessus individuels ou distribués.

Nessus fournit des **fonctionnalités supplémentaires** au-delà du **test des vulnérabilités réseau connues**.   
Par exemple, il peut utiliser les **informations d'identification Windows** pour examiner les **niveaux de correctifs** sur les ordinateurs exécutant le système d'exploitation Windows.   
Nessus peut également **prendre en charge les audits de configuration et de conformité**, les **audits SCADA** et la **conformité PCI**.

# Opération

Voici des exemples de vulnérabilités et d'expositions que Nessus peut rechercher …

* **Vulnérabilités** qui pourraient permettre un **contrôle ou un accès non autorisé à des données sensibles** sur un système ;
* **Mauvaise configuration** (relais de messagerie ouvert, correctifs manquants, ...) ;
* **Mots de passe par défaut**, quelques mots de passe courants et mots de passe vides/absents sur certains comptes système.   
  Nessus peut également appeler Hydra (un outil externe) pour lancer une attaque par dictionnaire ;
* **Vulnérabilités par dénis de service**.

# Mise en place

Nessus existe sous deux formats …

* une **version gratuite limitée**   
  et
* une **option d'abonnement payante complète**.

Nessus est disponible pour **Linux**, **Windows** et **macOS**.

**Site de téléchargement**<https://fr.tenable.com/products/nessus?tns_redirect=true>

On peut télécharger une version gratuite …

Une image contenant texte

Description générée automatiquement

Nessus exige une authentification et un code d’activation.  
On doit donc fournir une adresse de courriel valide.

Une image contenant texte

Description générée automatiquement

# Analyse de vulnérabilités

Nessus étant installé, on peut effectuer une première analyse de vulnérabilités.

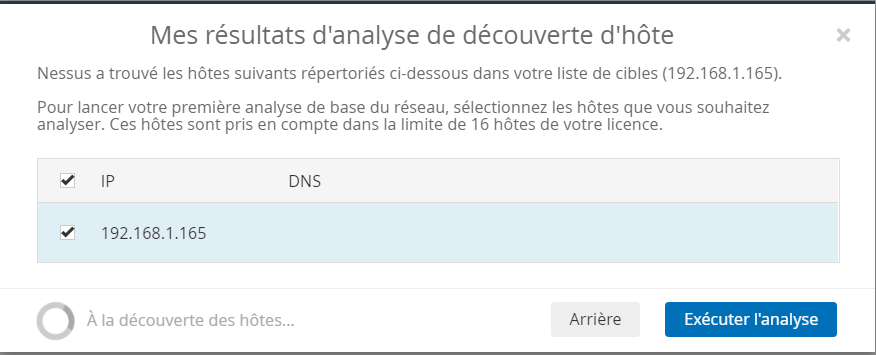
Pour ce faire, on ouvre un fureteur (*browser*) et on saisit l’URL suivante …  
**https://localhost:8834/#/scans/folders/my-scans**

Une boite de dialogue propose d’identifier un ou des hôtes à balayer …

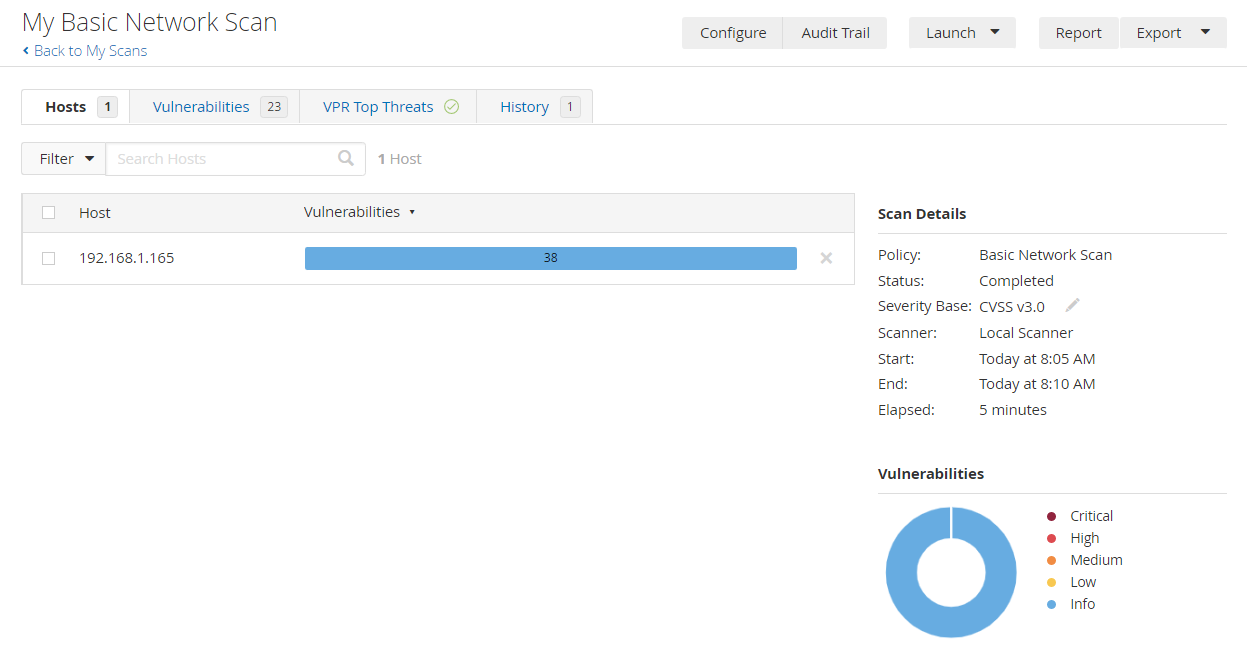
Une image contenant texte

Description générée automatiquement

Nessus devrait identifier l’hôte ou les hôtes …

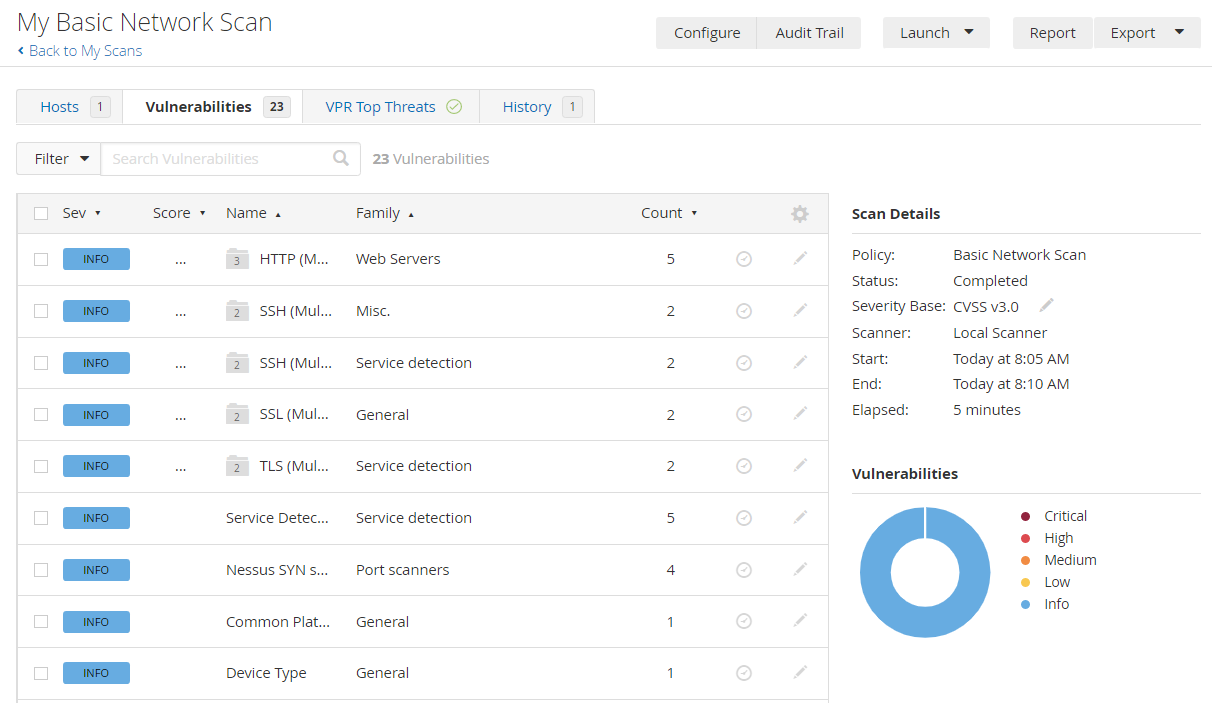


On consulte ensuite le tableau de bord afin de consulter les balayages demandés.



Pour consulter le résultat du balayage, on clique sur **Vulnérabilités** afin d’en afficher la liste  


Nessus affiche la liste des vulnérabilités identifiées.  
Les vulnérabilités trouvées sont affichées par catégories.



On peut cliquer sur l’une d’entre elle pour en afficher une catégorie et les vulnérabilités identifiées pour cette catégorie.

Une image contenant texte

Description générée automatiquement

Pour plus de détails sur une vulnérabilité, on clique sur son identifiant.

Une image contenant texte

Description générée automatiquement

