

Guide de l'utilisateur Nessus 5.2 HTML5

16 janvier 2014

(Révision 20)

Table des matières

Introduction	4
Normes et conventions	4
Nouveautés dans Nessus 5.2	4
Vue d'ensemble de l'IU Nessus	5
Description	5
Plateformes prises en charge	5
Installation	5
Fonctionnement	5
Vue d'ensemble	5
Connexion à l'interface graphique Nessus	5
User Profile (Profil utilisateur)	11
Settings (Paramètres)	11
Raccourcis de l'interface	12
Vue d'ensemble des stratégies	13
Création d'une nouvelle stratégie	14
Utilisation de l'assistant de stratégies	14
Création avancée d'une stratégie	17
Paramètres généraux	17
Identifiants	21
Plug-ins	25
Préférences	28
Importation, exportation et copie des stratégies	32
Création, lancement et programmation d'un scan	33
Parcourir les résultats du scan	38
Filtres des rapports	47
Captures d'écran de rapport	53
Scan Knowledge Base (Base de connaissances de scan)	53
Comparer (Diff Results)	54
Téléchargement en amont et exportation	55
Format de fichier .nessus	57
Suppression	58
Mobile	58
SecurityCenter	59
Configuration de SecurityCenter pour l'utilisation avec Nessus	59
Pare-feu de l'hôte	60
Détails des préférences de scan	61
ADSI Settings (Paramètres ADSI)	61
Apple Profile Manager API Settings (Paramètres d'API de gestionnaire de profil Apple)	61
Check Point GAIa Compliance Checks (Contrôles de conformité Check Point GAIa)	62
Cisco IOS Compliance Checks (Contrôles de conformité Cisco IOS)	63
Citrix XenServer Compliance Checks (Contrôles de conformité Citrix XenServer)	63
Database Compliance Checks (Contrôles de conformité des bases de données)	64
Database settings (Paramètres de base de données)	65
Do not scan fragile devices (Ne pas scanner les périphériques fragiles)	65
FireEye Compliance Checks (Contrôles de conformité FireEye)	66

Global variable settings (Paramètres des variables globales)	67
Good MDM Settings (Paramètres Good MDM)	68
HP ProCurve Compliance Checks (Contrôles de conformité HP ProCurve)	69
HTTP cookies import (Importation des cookies HTTP)	69
HTTP login page (Page de connexion HTTP).....	70
IBM iSeries Compliance Checks (Contrôles de conformité IBM iSeries)	73
IBM iSeries Credentials (Identifiants IBM iSeries).....	73
ICCP/COTP TSAP Addressing (Adressage ICCP/COTP TSAP).....	74
Juniper Junos Compliance Checks (Contrôles de conformité Juniper Junos)	74
LDAP 'Domain Admins' Group Membership Enumeration (Énumération de la participation du groupe 'Domain Admins' LDAP).....	74
Login configurations (Configurations de connexion)	75
Malicious Process Detection (Détection de processus malveillants).....	76
Modbus/TCP Coil Access (Accès à la bobine Modbus/TCP).....	76
Nessus SYN scanner et Nessus TCP scanner (Scanner Nessus SYN et Scanner Nessus TCP)	77
NetApp Data ONTAP Compliance Checks (Contrôles de conformité NetApp Data ONTAP)	78
Oracle Settings (Paramètres Oracle)	78
PCI DSS Compliance (Conformité PCI DSS)	79
Patch Management (Gestion de correctifs)	79
Palo Alto Networks PAN-OS Settings (Paramètres Palo Alto Networks PAN-OS).....	79
Patch Report (Rapport sur les correctifs).....	80
Ping the remote host (Sonder l'hôte à distance)	80
Port scanner settings (Paramètres de scanner des ports).....	81
Remote web server screenshot (Capture d'écran de serveur Web distant)	82
SCAP Linux Compliance Checks (Contrôles de conformité SCAP Linux).....	82
SCAP Windows Compliance Checks (Contrôles de conformité SCAP Windows).....	83
SMB Registry: Start the Registry Service during the scan (Registre SMB : démarrer le service de registre pendant le scan)	84
SMB Registry : Start the Registry Service during the scan (Registre SMB : démarrer le service de registre pendant le scan)	84
SMB Scope (Portée SMB)	84
SMB Use Domain SID to Enumerate Users (SMB utilise le SID de domaine pour énumérer les utilisateurs).....	85
SMB Use Host SID to Enumerate Local Users (SMB utilise le SID d'hôte pour énumérer les utilisateurs locaux)	85
SMTP settings (Paramètres SMTP).....	86
SNMP settings (Paramètres SNMP).....	87
Service Detection (Détection du service)	88
Unix Compliance Checks (Contrôles de conformité Unix)	88
VMware SOAP API Settings (Paramètres de l'API SOAP VMware).....	89
VMware vCenter SOAP API Settings (Paramètres de l'API SOAP VMware vCenter)	90
VMware vCenter/vSphere Compliance Checks (Contrôles de conformité VMware vCenter/vSphere)	91
Wake-on-LAN (WOL, éveil sur réseau local).....	91
Web Application Tests Settings (Paramètres des tests des applications Web)	92
Web mirroring (Mise en miroir Web)	95
Windows Compliance Checks (Contrôles de conformité Windows)	96
Windows File Contents Compliance Checks (Contrôles de conformité du contenu des fichiers Windows).....	96
Pour plus d'informations	97
À propos de Tenable Network Security	99

Introduction

Ce document décrit comment utiliser l'**interface utilisateur (IU) de Nessus** de Tenable Network Security. Veuillez envoyer vos commentaires et suggestions à support@tenable.com.

L'IU Nessus est une interface basée sur le Web du scanner de vulnérabilité Nessus. Pour utiliser l'interface graphique, il est nécessaire d'avoir déployé un scanner Nessus opérationnel et d'être familiarisé avec son utilisation.

Normes et conventions

Dans l'ensemble de la documentation, les noms de fichiers, les démons (daemons) et les exécutables sont indiqués par la police **courier bold**, par exemple `gunzip`, `httpd` et `/etc/passwd`.

Les options de ligne de commande et les mots clés sont aussi indiqués par la police **courier bold**. Les exemples de ligne de commande peuvent inclure ou non l'invite de ligne de commande et le texte provenant des résultats de la commande. Les exemples de ligne de commande sont affichés en **courier bold** dans la commande en cours d'exécution afin de montrer la saisie de l'utilisateur, tandis que l'exemple de sortie généré par le système utilisera la police **courier** (mais pas en gras). Voici ci-dessous un exemple d'exécution de la commande Unix `pwd` :

```
# pwd
/opt/nessus/
#
```



Les remarques et considérations importantes sont mises en évidence avec ce symbole dans une boîte de texte grise.



Les conseils, exemples et meilleures pratiques sont mis en évidence avec ce symbole en texte blanc sur fond bleu.

Nouveautés dans Nessus 5.2

À dater du 22 août 2013, les noms de produit Nessus ont été révisés comme suit :

Ancien nom de produit	Nouveau nom de produit
Nessus ProfessionalFeed	Nessus
Nessus HomeFeed	Nessus Home

La liste qui suit présente les noms officiels des produits Nessus :

- Nessus®
- Nessus Perimeter Service
- Offres groupées Nessus Auditor
- Nessus Home

Vue d'ensemble de l'IU Nessus

Description

L'interface utilisateur (IU) Nessus est une interface Web du scanner Nessus, constituée simplement d'un serveur HTTP et d'un client Web, et ne nécessitant aucune installation de logiciel, sauf le serveur Nessus. Comme pour Nessus 4, toutes les plateformes utilisent la même base de code, ce qui élimine les erreurs spécifiques de plateforme et permet le déploiement plus rapide des nouvelles fonctionnalités. Les fonctions principales sont :

- Création de fichiers `.nessus` que les produits Tenable utilisent comme norme pour les données de vulnérabilité et les stratégies de scan.
- Une session de stratégie, une liste de cibles et les résultats de plusieurs scans peuvent tous être enregistrés dans un seul fichier `.nessus` qui peut être facilement exporté. Voir le guide « [Nessus v2 File Format](#) » (Format de fichier Nessus v2) pour plus d'informations.
- L'interface graphique affiche les résultats du scan en temps réel, si bien qu'il n'est pas nécessaire d'attendre la fin d'un scan pour visualiser les résultats.
- Mise à disposition d'une interface unifiée du scanner Nessus, quelle que soit la plateforme de base. Les mêmes fonctionnalités existent sur Mac OS X, Windows et Linux.
- Les scans continuent à être exécutés sur le serveur, même en cas de déconnexion.
- Les comptes-rendus de scan Nessus peuvent être téléchargés par l'IU Nessus et comparés à d'autres rapports.
- Un assistant de stratégie, qui permet de créer rapidement des stratégies de scan efficaces pour l'audit du réseau.

Plateformes prises en charge

Comme l'IU Nessus est un client Web, elle peut être exécutée sur toute plateforme équipée d'un navigateur Internet moderne.



L'interface utilisateur Nessus de type Web donnera les meilleurs résultats avec Microsoft Internet Explorer 10, Mozilla Firefox 24, Google Chrome 29, Opera 16 ou Apple Safari 6. De plus, Nessus est compatible avec Chrome 29 pour Android, ainsi qu'avec les navigateurs de la plateforme iOS 7.



L'interface Web Nessus exige Microsoft Internet Explorer version 9 ou supérieure.

Installation

La gestion des utilisateurs du serveur Nessus 5 est assurée par une interface Web ou SecurityCenter uniquement. Le client NessusClient autonome n'est plus mis à jour ou pris en charge.

Voir le « [Nessus 5.2 Installation and Configuration Guide](#) » (Guide d'installation et de configuration Nessus 5.2) pour des instructions concernant l'installation de Nessus. À partir de Nessus 5.0, [Oracle Java](#) (auparavant l'application Java de Sun Microsystems) est requis pour la fonction de rapport PDF.

Fonctionnement

Vue d'ensemble

Nessus fournit une interface simple mais performante pour gérer l'activité de scan des vulnérabilités.

Connexion à l'interface graphique Nessus

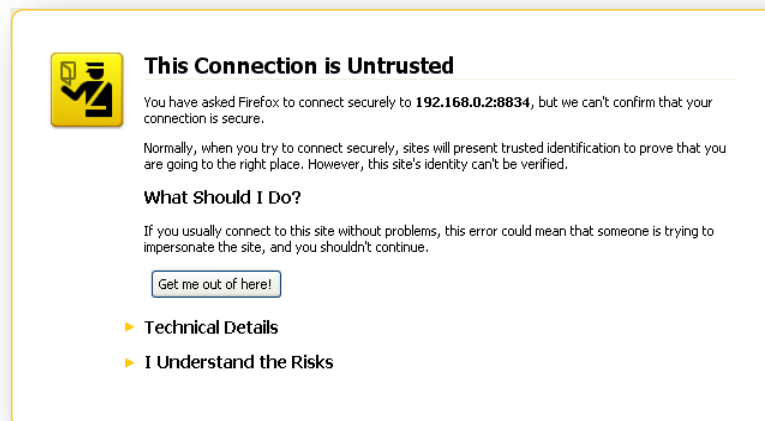
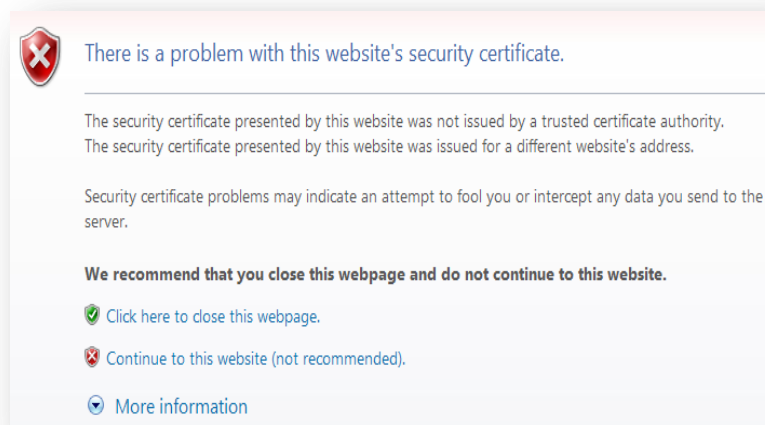
Pour lancer l'interface graphique Nessus HTML5, procédez comme suit :

- Ouvrez le navigateur Internet choisi.
- Saisissez `https://[server IP]:8834/` dans la barre de navigation

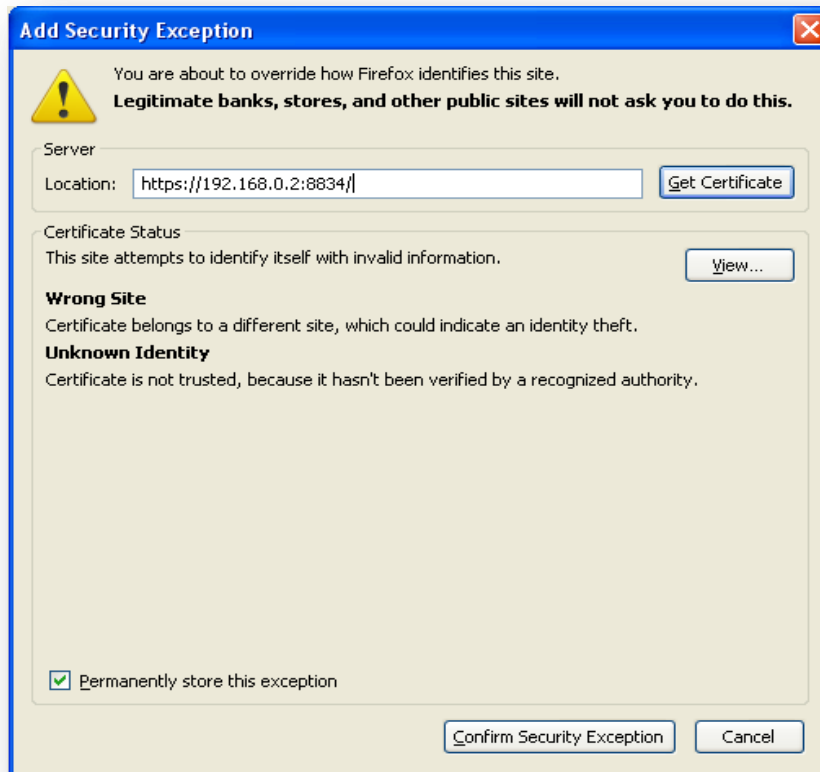


Veillez à vous connecter à l'interface utilisateur par HTTPS, car les connexions HTTP non cryptées ne sont pas compatibles.

La première fois que vous essayez de vous connecter à l'interface utilisateur Nessus, les navigateurs Internet affichent normalement une erreur indiquant que le site n'est pas sécurisé à cause du certificat SSL auto-signé :

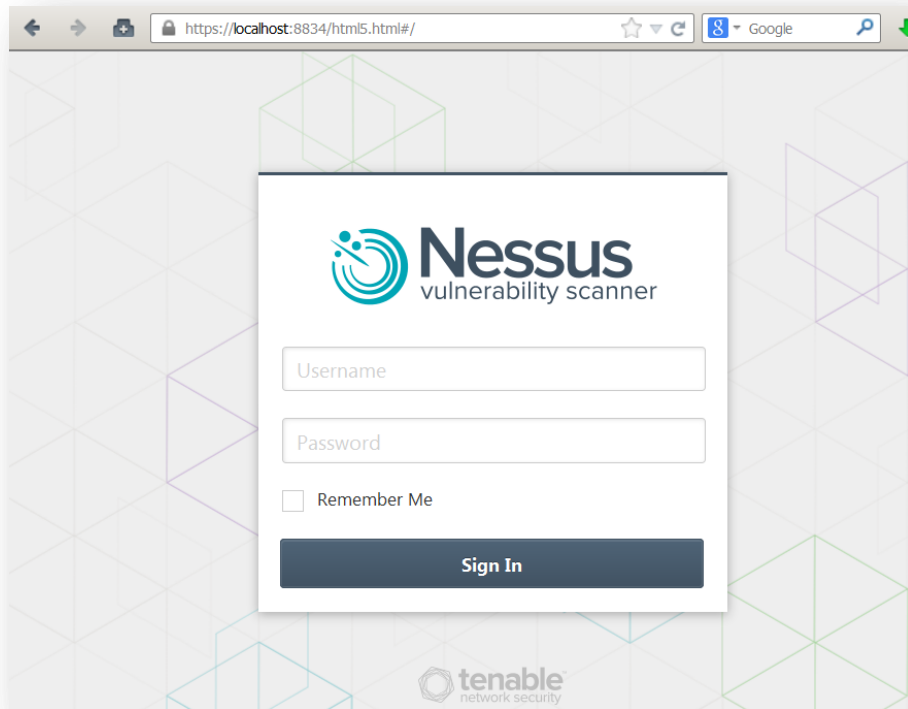


Les utilisateurs de Microsoft Internet Explorer peuvent cliquer sur « **Continue to this website (not recommended)** » (Poursuivre sur ce site Web (non recommandé)) pour charger l'interface utilisateur Nessus. Les utilisateurs de Firefox peuvent cliquer sur « **I Understand the Risks** » (Je comprends les risques), puis sur « **Add Exception...** » (Ajouter une exception...) pour accéder à la boîte de dialogue d'exception du site :

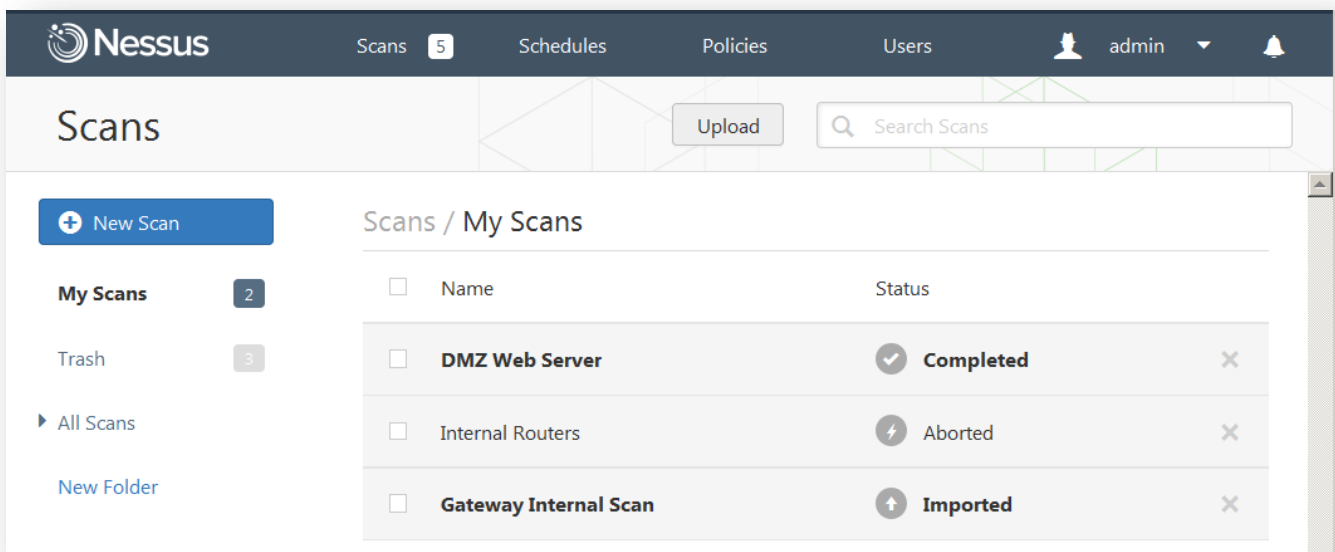


Vérifiez que la barre « Location : » (Adresse :) reflète l'URL du serveur Nessus et cliquez sur « **Confirm Security Exception** » (Confirmer l'exception de sécurité). Pour plus d'informations concernant l'installation d'un certificat SSL personnalisé, consultez le « [Nessus 5.2 Installation and Configuration Guide](#) » (Guide d'installation et de configuration Nessus 5.2).

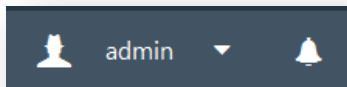
Après confirmation de l'exception par le navigateur, un écran de démarrage s'affiche comme suit :



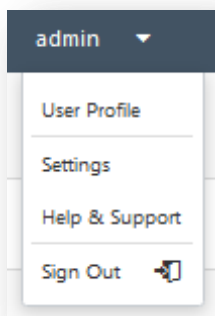
Identifiez-vous en utilisant un compte administratif et un mot de passe créés précédemment au cours de l'installation. Lorsque vous ouvrez une session, vous pouvez éventuellement indiquer à votre navigateur de mémoriser le nom d'utilisateur sur cet ordinateur. Veillez à n'utiliser cette option que si l'ordinateur se trouve toujours dans un emplacement sécurisé ! Si l'identification réussit, l'IU affiche les menus permettant de consulter les rapports, d'exécuter les scans et de gérer les stratégies. Les utilisateurs administratifs peuvent également voir les options pour la gestion des utilisateurs, ainsi que les options de configuration pour le scanner Nessus :



Les options en haut à gauche sont toujours affichées pendant l'utilisation de Nessus. L'indication « admin » en haut à droite dans l'écran ci-dessus présente le compte connecté, un menu déroulant et une cloche permettant un accès rapide aux notifications importantes relatives à l'utilisation de Nessus :



Lorsque vous cliquez sur cette flèche vers le bas, vous affichez un menu qui contient les options permettant d'accéder à votre profil utilisateur, à la configuration Nessus générale, aux informations sur l'installation, à l'aide et aux options de prise en charge, ainsi qu'à une option de déconnexion.



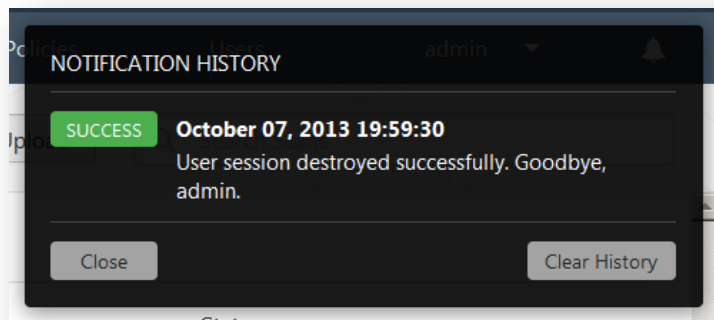
L'option « **User Profile** » (Profil utilisateur) affiche un menu proposant plusieurs pages d'options relatives au compte d'utilisateur, dont la page portant sur la fonction de changement du mot de passe, la gestion des dossiers et les règles des plugins. Vous trouverez plus d'informations sur ces options ci-dessous.

L'option « **Settings** » (Paramètres) permet d'accéder à la page « **About** » (À propos de), aux options de configuration du serveur de messagerie (si vous êtes un administrateur), au feed de plugin (si vous êtes un administrateur) et aux options avancées de scanner (si vous êtes un administrateur). Vous trouverez plus d'informations sur ces options ci-dessous.

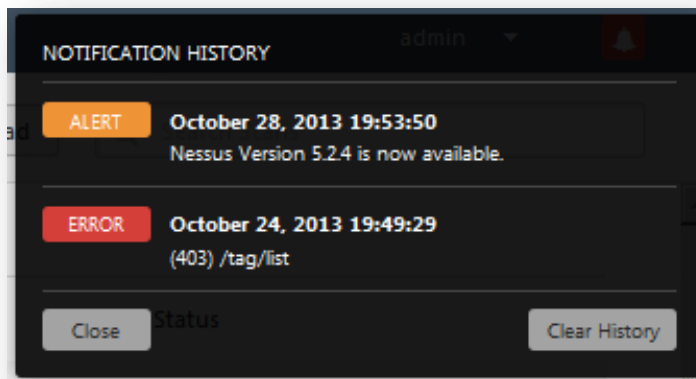


Le lien « **Help & Support** » (Aide et assistance) charge la page d'assistance Tenable dans un nouvel onglet ou une nouvelle fenêtre. « **Sign Out** » (Déconnexion) ferme la session Nessus en cours.

Vous pouvez cliquer sur l'icône de cloche dans la partie supérieure droite de la fenêtre pour afficher tous les messages relatifs aux activités Nessus, notamment les erreurs, la notification des nouvelles versions de Nessus et les événements de session :

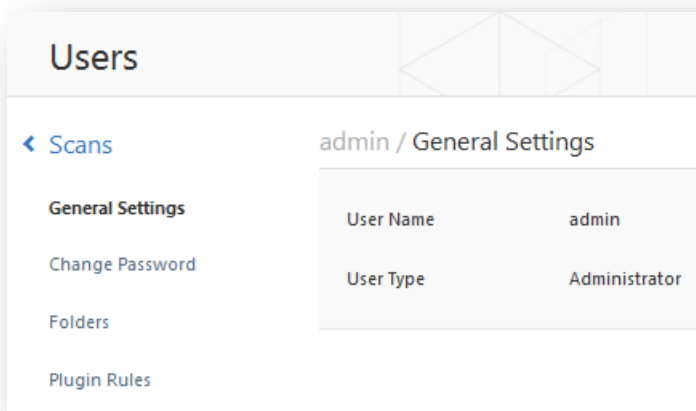


Les autres alertes ou erreurs s'affichent également à cet emplacement, par le biais de messages contextuels qui s'estomperont rapidement et restent consignés dans l'historique des notifications tant que vous ne les supprimez pas :



User Profile (Profil utilisateur)

Les options du profil utilisateur permettent de manipuler les options relatives à votre compte.



Le champ « **General Settings** » (Paramètres généraux) affiche l'utilisateur authentifié en cours, ainsi que son type (administrateur ou utilisateur).

L'option « **Change Password** » (Changer le mot de passe) permet de modifier le mot passe. Il est recommandé de le changer tous les 3 mois.

L'option « **Folders** » (Dossiers) permet de gérer les dossiers dans lesquels les résultats des scans seront consignés. Vous avez ainsi la possibilité d'organiser et de stocker les résultats des scans pour en faciliter la gestion.

L'option « **Plugin Rules** » (Règles de plugin) offre une fonction permettant de créer un ensemble de règles qui régiront le comportement de certains plugins pour tous les scans effectués. Une règle peut être basée sur l'hôte (ou sur tous les hôtes), sur l'ID de plugin, sur une date d'expiration facultative et sur la manipulation du niveau de gravité. Les mêmes règles peuvent être définies à partir de la page des résultats du scan.

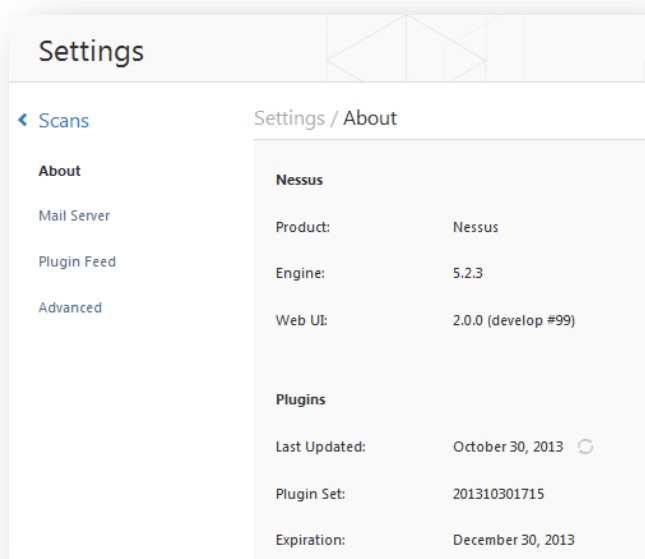
Settings (Paramètres)

La section « About » (À propos de) propose des informations relatives à l'installation de Nessus, notamment la version du moteur, la version de l'interface utilisateur Web, la date de mise à jour du plugin, la version du jeu de plugins et la date d'expiration du feed.

La section « Mail Server » (Serveur de messagerie) permet de définir les paramètres relatifs au serveur SMTP. Pour plus d'informations, consultez le « [Nessus 5.2 Installation and Configuration Guide](#) » (Guide d'installation et de configuration Nessus 5.2).

Le paramètre « Plugin Feed » (Feed de plugin) permet de désigner un hôte de mise à jour des plugins personnalisés (pour les mises à jour hors ligne à partir d'un serveur interne central) et un proxy pour les mises à jour de plugin. Pour plus d'informations, consultez le « [Nessus 5.2 Installation and Configuration Guide](#) » (Guide d'installation et de configuration Nessus 5.2).

La section « Advanced » (Paramètres avancés) propose une large gamme d'options de configuration afin de fournir un contrôle plus précis pour le fonctionnement du scanner. Pour plus d'informations, consultez le « [Nessus 5.2 Installation and Configuration Guide](#) » (Guide d'installation et de configuration Nessus 5.2).



Raccourcis de l'interface

L'interface HTML5 comprend plusieurs raccourcis qui facilitent la navigation à partir du clavier vers les principales sections de l'interface, ainsi que l'exécution des activités courantes. Vous pouvez utiliser ces raccourcis à tout moment, à partir de n'importe quelle section de l'interface :

Interface principale	
R	Results (Résultats)
S	Scans
T	Templates (Modèles)
P	Policies (Stratégies)
U	Users (Utilisateurs)

C	Configuration
Maj + Flèche gauche/droite	Commutation des onglets à gauche ou à droite
Maj + S	Nouveau scan
Vues des listes	
Maj + Flèche haut/bas	Déplacer la sélection vers le haut ou le bas
Maj + Entrée	Ouvrir l'entrée sélectionnée
Vue Résultats	
Maj + U	Télécharger un rapport en amont
Échap	Revenir à la liste des résultats
Flèche gauche/droite	Vulnérabilité précédente/suivante en mode Détails
D	Supprimer le résultat sélectionné
Vue Scan	
N	Nouveau scan
Vue Stratégie	
Maj + U	Télécharger une nouvelle stratégie en amont
Vue utilisateur	
N	Nouvel utilisateur

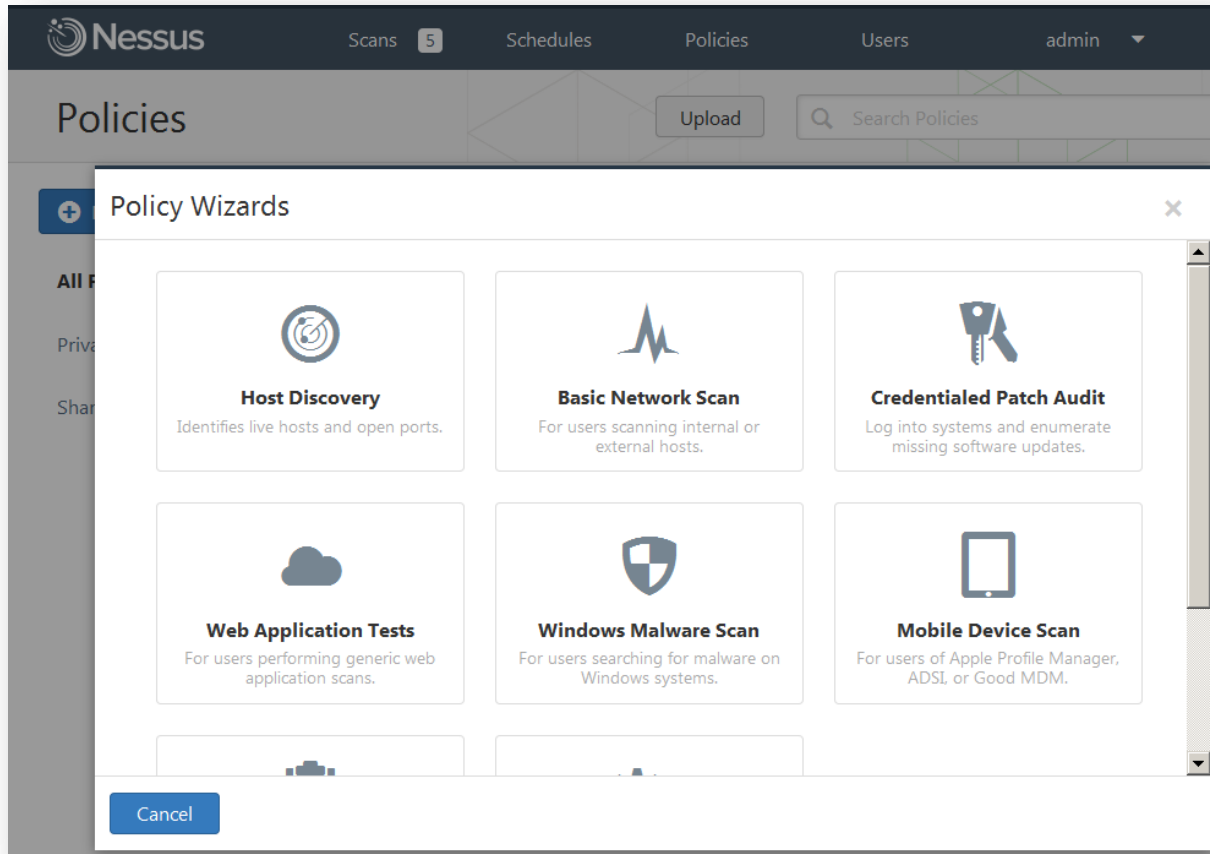
Vue d'ensemble des stratégies

Une stratégie de Nessus inclut des options de configuration liées à l'exécution d'un scan des vulnérabilités. Ces options incluent notamment :

- Des paramètres qui contrôlent les aspects techniques du scan, par exemple les temporisations, le nombre d'hôtes et le type de scanner des ports.
- Des identifiants pour les scans locaux (par exemple Windows, SSH), les scans de base de données Oracle authentifiés, les identifiants basés sur HTTP, FTP, POP, IMAP ou Kerberos.
- Spécification de scan basée sur niveau de granularité ou plugin.
- Contrôles de stratégie pour vérifier la conformité à la base de données, la verbosité des rapports, les paramètres de scan pour la détection de service, les contrôles de conformité Unix, etc.

Création d'une nouvelle stratégie

Une fois que vous êtes connecté à une IU de serveur Nessus, vous pouvez créer une stratégie personnalisée en cliquant sur l'option « **Politiques** » (Stratégies) sur la barre du haut, puis sur le bouton « **+ New Policy** » (Nouvelle stratégie) à gauche. L'écran d'ajout de stratégie s'affiche comme suit :



Utilisation de l'assistant de stratégies

La première option consiste à faire appel à l'assistant de stratégies (Policy Wizard), le cas échéant, pour vous aider à créer une stratégie répondant à un besoin spécifique. Les modèles d'assistant par défaut sont les suivants :

Nom de l'assistant de stratégies	Description
Host Discovery (Détection des hôtes)	Identifie les hôtes actifs et les ports ouverts.
Basic Network Scan (Scan réseau de base)	Destiné aux utilisateurs qui scannent des hôtes internes ou externes.
Credentialed Patch Audit (Audit des correctifs avec identifiants)	Connexion aux systèmes et énumération des mises à jour logicielles manquantes.

Web Application Tests (Test des applications Web)	Destiné aux utilisateurs qui effectuent des scans d'applications Web génériques.
Windows Malware Scan (Scan des programmes malveillants sur Windows)	Destiné aux utilisateurs qui recherchent la présence de logiciels malveillants sur les systèmes Windows.
Mobile Device Scan (Scan des périphériques mobiles)	Destiné aux utilisateurs du Gestionnaire de profil Apple, d'ADSI ou de Good MDM.
Prepare for PCI DSS Audits (Préparation aux audits PCI DSS)	Permet aux utilisateurs de préparer l'audit sur les critères de la conformité PCI DSS.
Advanced Policy (Stratégie avancée)	Destiné aux utilisateurs qui souhaitent disposer d'un contrôle total sur la configuration des stratégies.

L'assistant de stratégie proposera progressivement d'autres assistants destinés à aider les clients, et les assistants existants seront certainement améliorés. Vous trouverez ci-dessous une présentation générale relative à l'utilisation de l'un de ces assistants. Il ne s'agit que d'un exemple, étant donné que chaque assistant est différent.

New Basic Network Scan Policy / Step 1 of 3

1 Define your policy name, description, visibility, and post-scan editing preferences:

Policy Name

Visibility

Description

Allow Post-Scan Report Editing

Next Cancel

Pour chaque assistant, la première étape consiste à définir le nom de la stratégie, sa visibilité (privée ou partagée) et une description. Par défaut, les stratégies d'assistant permettent de modifier le rapport à l'issue d'un scan. Cliquez sur « **Next** » (Suivant) pour passer à l'étape suivante :

New Basic Network Scan Policy / Step 2 of 3

2 Choose the type of scan to configure:

Scan type
Internal

Next Cancel

Cette stratégie vous demande de choisir si elle sera utilisée pour des hôtes internes ou externes, puisque ses options varient en fonction de la réponse. Cliquez sur « **Next** » (Suivant) pour passer à la dernière étape :

New Basic Network Scan Policy / Step 3 of 3

3 Provide credentials to detect missing patches and client-side vulnerabilities (optional):

Authentication method Windows

Windows

Nessus can enumerate Windows settings, detect insecure configurations, and identify missing Microsoft or third-party updates. Please provide the credentials for a user account that has local administrative privileges on the targets being scanned.

Username

Password

Domain

Start the Remote Registry service during the scan

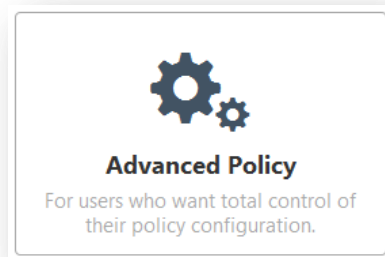
Enable administrative shares during the scan

Save Cancel

La dernière étape vous permet d'ajouter des identifiants afin d'améliorer le scan. Comme indiqué, certaines des étapes d'un assistant de stratégie peuvent être facultatives. Une fois créée, la stratégie sera enregistrée avec les paramètres recommandés. Vous pouvez modifier les options de l'assistant ou tout autre aspect de la stratégie à votre convenance.

Création avancée d'une stratégie

Si vous ne souhaitez pas utiliser l'assistant de stratégie, l'option **Advanced** (Paramètres avancés) vous permet de faire appel à la méthode classique pour créer une stratégie ; vous aurez alors un contrôle total sur l'ensemble des options tout au long de la procédure.



Il y a quatre onglets de configuration : **General Settings** (Paramètres généraux), **Credentials** (Identifiants), **Plugins** et **Preferences** (Préférences). Pour la plupart des environnements, il n'est pas nécessaire de modifier les paramètres par défaut, mais ils fournissent un meilleur contrôle granulaire pour le fonctionnement du scanner Nessus. Ces onglets sont décrits ci-dessous.

Paramètres généraux



L'onglet « **General Settings** » (Paramètres généraux) permet de nommer la stratégie et de configurer les opérations associées au scan. Quatre éléments du menu déroulant permettent de contrôler le comportement du scanner :

L'écran « **Basic** » (Cadre de base) est utilisé pour définir les aspects de la stratégie elle-même :

Option	Description
Name (Nom)	Définit le nom qui sera affiché dans l'IU Nessus pour identifier la stratégie.
Visibility (Visibilité)	Détermine si la stratégie est <i>partagée</i> (« Shared ») avec d'autres utilisateurs ou si elle reste <i>privée</i> (« Private ») et à l'usage exclusif de l'utilisateur. Seuls les utilisateurs administratifs peuvent partager les stratégies.
Description (Description)	Permet de fournir une brève description de la stratégie de scan, typiquement pour résumer l'objectif d'ensemble (par exemple « Web Server scans without local checks or non HTTP services » (le serveur Web scanne sans vérification locale ni services non-HTTP)).
Allow Post-Scan Report Editing (Autoriser la modification des rapports après le scan)	Si cette fonction est activée, elle permet aux utilisateurs de supprimer des éléments du rapport. Si vous effectuez un scan de conformité ou d'autres types de vérification, vous devez décocher cette case afin de pouvoir prouver que le scan n'a pas été altéré.

Le menu « **Port Scanning** » (Scan des ports) comprend les options relatives au scan des ports, notamment les plages de port et les méthodes :



Option	Description
Port Scan Range (Plage de scan de port)	<p>Indique au scanner de cibler une plage particulière de ports. Les valeurs autorisées sont : « default » (valeur par défaut), qui scanne environ 4 790 ports communs répertoriés dans le fichier <code>nessus-services</code> et « all » (tous), qui scanne 65 535 ports ou une liste personnalisée de ports spécifiée par l'utilisateur. Par exemple « 21,23,25,80,110 » ou « 1-1024,8080,9000-9200 » sont autorisés. Si « 1-65535 » est spécifié, tous les ports seront scannés.</p> <p>Vous pouvez également spécifier une plage fractionnée spécifique à chaque protocole. Par exemple, si vous souhaitez effectuer un scan sur une autre plage de ports pour TCP et UDP dans la même stratégie, vous devez spécifier « T:1-1024,U:300-500 ». Vous pouvez également spécifier un groupe de ports afin d'effectuer un scan pour les deux protocoles, ainsi que des plages individuelles pour chaque protocole séparé (« 1-1024,T:1024-65535,U:1025 »). Si vous effectuez un scan sur un même protocole, sélectionnez uniquement ce scanner de ports et spécifiez les ports normalement.</p>
Consider Unscanned Ports as Closed (Considérer les ports non scannés comme fermés)	<p>Si un port n'est pas scanné avec un scanner des ports sélectionné (par exemple, hors de la plage spécifiée), Nessus le considère comme fermé.</p>
Nessus SNMP Scanner (Scanner Nessus SNMP)	<p>Demande à Nessus de scanner des cibles pour un service SNMP. Nessus devinera les paramètres SNMP pertinents pendant un scan. Si les paramètres sont fournis par l'utilisateur sous la rubrique « Preferences » (Préférences), ceci permettra à Nessus de mieux tester l'hôte distant et de produire des résultats d'audit plus détaillés. Par exemple, il existe un grand nombre de contrôles de routeur Cisco qui déterminent les vulnérabilités existantes en examinant la version de la chaîne SNMP renvoyée. Ces informations sont nécessaires pour les audits.</p>
Nessus UDP Scanner (Scanner Nessus UDP)	<p>Cette option utilise le scanner UDP intégré de Nessus pour identifier les ports UDP ouverts sur les cibles.</p> <div data-bbox="516 1276 591 1346" style="float: left; margin-right: 10px;"> </div> <div data-bbox="630 1276 1487 1430" style="border: 1px solid #ccc; padding: 5px;"> <p>UDP est un protocole « sans état » ; autrement dit, les communications ne sont pas effectuées avec des dialogues de protocole de transfert. Les communications basées sur UDP ne sont pas toujours fiables et, en raison de la nature des services UDP et des dispositifs de détection, elles ne sont pas toujours décelables à distance.</p> </div>
netstat portscanner (SSH) (Scanner de ports netstat (SSH))	<p>Cette option utilise <code>netstat</code> pour rechercher les ports ouverts du périphérique local. Elle est basée sur la disponibilité de la commande <code>netstat</code> via une connexion SSH à la cible. Ce scan est destiné aux systèmes Unix et nécessite des identifiants de connexion.</p>
Ping the remote host (Sonder l'hôte à distance)	<p>Cette option permet à Nessus de sonder les hôtes à distance sur plusieurs ports pour déterminer s'ils sont activés.</p>
Netstat Portscanner (WMI) (Scanner de ports Netstat (WMI))	<p>Cette option utilise <code>netstat</code> pour rechercher les ports ouverts du périphérique local. Elle est basée sur la disponibilité de la commande <code>netstat</code> via une connexion WMI à la cible. Ce scan est destiné aux systèmes Windows et nécessite des identifiants de connexion.</p>

	 <p>Un scan basé sur WMI utilise netstat pour déterminer les ports ouverts, en ignorant ainsi toute plage de ports spécifiée. Si tout énumérateur de port (netstat ou SNMP) réussit, la plage de ports devient « all » (tous). Cependant, Nessus respectera toujours l'option « consider unscanned ports as closed » (Considérer les ports non scannés comme fermés) si elle est sélectionnée.</p>
Nessus TCP scanner (Scanner Nessus TCP)	<p>Utilise le scanner TCP intégré de Nessus pour identifier les ports TCP ouverts sur les cibles. Ce scanner est optimisé et possède certaines fonctions d'auto-ajustement.</p>  <p>Sur certaines plateformes (par exemple Windows et Mac OS X), la sélection de ce scanner indique à Nessus d'utiliser le scanner SYN pour éviter de graves problèmes de performance propres à ces systèmes d'exploitation.</p>
Nessus SYN scanner (Scanner Nessus SYN)	<p>Utilise le scanner SYN intégré de Nessus pour identifier les ports TCP ouverts sur les cibles. Les scans SYN constituent une méthode courante pour effectuer des scans de port, considérée en général comme un peu moins intrusive que les scans TCP. Le scanner envoie un paquet de données SYN au port, il attend la réponse SYN-ACK et détermine l'état du port en fonction de la réponse ou de l'absence de réponse.</p>

L'option « **Port Scan Range** » (Plage de scan de port) indique au scanner de cibler une plage particulière de ports. Les valeurs suivantes sont autorisées :


Valeur	Description
“default” (valeur par défaut)	Si vous utilisez le mot clé « default », Nessus scanne environ 4 790 ports communs. La liste des ports est disponible dans le fichier nessus-services .
“all” (tous)	Si vous utilisez le mot clé « all », Nessus scanne l'ensemble des 65 535 ports.
Custom List (Liste personnalisée)	<p>Une plage personnalisée de ports peut être sélectionnée au moyen d'une liste de ports ou de plages de ports délimitée par des virgules. Par exemple « 21,23,25,80,110 » ou « 1-1024,8080,9000-9200 » sont autorisés. Si « 1-65535 » est spécifié, tous les ports seront scannés.</p> <p>Vous pouvez également spécifier une plage fractionnée spécifique à chaque protocole. Par exemple, si vous souhaitez effectuer un scan sur une autre plage de ports pour TCP et UDP dans la même stratégie, vous devez spécifier « T:1-1024,U:300-500 ». Vous pouvez également spécifier un groupe de ports afin d'effectuer un scan pour les deux protocoles, ainsi que des plages individuelles pour chaque protocole séparé (« 1-1024,T:1024-65535,U:1025 »). Si vous effectuez un scan sur un même protocole, sélectionnez uniquement ce scanner de ports et spécifiez les ports normalement.</p>

Le menu « **Performance** » (Performance) fournit les options contrôlant le nombre de scans qui seront effectués. Ces options sont peut-être les plus importantes lorsque vous configurez un scan, car elles ont le plus grand impact sur les durées des scans et l'activité du réseau.

Option	Description
Max Checks Per Host (Vérifications max. par hôte)	Ce paramètre limite le nombre maximum de contrôles qu'un scanner Nessus effectue par rapport à un seul hôte à un moment donné.
Max Hosts Per Scan (Hôtes max. par scan)	Ce paramètre limite le nombre maximum d'hôtes qu'un scanner Nessus scanne en même temps.
Network Receive Timeout (secondes) (Temporisation de réception réseau (en secondes))	La valeur par défaut est de cinq secondes. Il s'agit de la durée pendant laquelle Nessus attend une réponse de l'hôte, sauf spécification contraire dans un plugin. Si vous effectuez un scan via une connexion lente, utilisez un nombre de secondes plus élevé.
Max Simultaneous TCP Sessions Per Host (Sessions TCP simultanées max. par hôte)	Ce paramètre limite le nombre maximum des sessions TCP établies pour un seul hôte.  Cette option de limitation TCP contrôle également le nombre de paquets par seconde que le scanner SYN enverra en fin de compte (par exemple, si la valeur de cette option est 15, le scanner SYN enverra jusqu'à 1 500 paquets par seconde).
Max Simultaneous TCP Sessions Per Scan (Sessions TCP simultanées max. par scan)	Ce paramètre limite le nombre maximum de sessions TCP établies pour l'ensemble du scan, quel que soit le nombre d'hôtes scannés.  Pour les scanners Nessus installés sur des hôtes Windows XP, Vista, 7 et 8, cette valeur doit être égale ou inférieure à 19 pour obtenir des résultats précis.
Reduce Parallel Connections on Congestion (Réduire les connexions parallèles en cas de congestion)	Permet à Nessus de détecter s'il envoie trop de paquets de données et si le pipe réseau est proche de sa capacité. En cas de détection, Nessus modifie la vitesse du scan pour tenir compte de la congestion et la limiter. Une fois la congestion contenue, Nessus réessaie automatiquement d'utiliser l'espace disponible dans le pipe réseau.
Use Kernel Congestion Detection (Linux Only) (Utiliser la détection de congestion de noyau (Linux seulement))	Permet à Nessus de surveiller l'UC et les autres périphériques internes pour déceler la congestion et la réduire selon les besoins. Nessus essaie toujours d'utiliser le plus de ressources disponibles. Cette fonction est disponible uniquement pour les scanners Nessus déployés sur Linux.

Le menu « **Advanced** » (Paramètres avancés) définit encore davantage les options concernant le comportement du scan :

Option	Description
Safe Checks (Vérifications sécurisées)	Safe Checks désactive tous les plugins qui peuvent avoir un effet nuisible sur l'hôte distant.
Silent Dependencies (Dépendances muettes)	Si cette option est cochée, la liste des dépendances n'est pas incluse dans le rapport. Si vous souhaitez inclure la liste des dépendances dans le rapport, décochez la case.
Log Scan Details to Server (Enregistrer les détails du scan sur le serveur)	Sauvegardez des détails supplémentaires du scan dans le journal du serveur Nessus (<code>nessusd.messages</code>) y compris le lancement d'un plugin, la fin d'un plugin ou l'arrêt d'un plugin. Le journal résultant peut être utilisé pour confirmer que des plugins particuliers ont été utilisés et des hôtes scannés.

Stop Host Scan on Disconnect (Arrêter le scan de l'hôte à la déconnexion)	<p>Si cette case est cochée, Nessus arrête le scan s'il détecte que l'hôte ne répond plus. Ceci peut se produire si les utilisateurs arrêtent leur ordinateur pendant un scan, si un hôte a cessé de répondre après un plugin de déni de service ou si un mécanisme de sécurité (par exemple IDS) a commencé à bloquer le trafic vers un serveur. Si les scans se poursuivent sur ces machines, un trafic superflu sera envoyé sur le réseau et retardera le scan.</p>
Avoid Sequential Scans (Éviter les scans séquentiels)	<p>Par défaut, Nessus scanne une liste d'adresses IP dans un ordre séquentiel. Si cette case est cochée, Nessus scanne la liste d'hôtes dans un ordre aléatoire. Ceci est normalement utile pour aider à répartir le trafic du réseau dirigé vers un sous-réseau spécifique pendant les longs scans.</p> <div data-bbox="613 583 1511 709" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Avant juillet 2013, cette option était appliquée par sous-réseau. Elle a depuis fait l'objet d'améliorations qui lui permettent d'appliquer un ordre aléatoire sur l'ensemble de l'espace IP cible.</p> </div>
Designate Hosts by their DNS Name (Désigner les hôtes par leur nom DNS)	<p>Utilise le nom de l'hôte au lieu de l'adresse IP pour l'émission des comptes-rendus.</p>



La plage spécifiée pour un scan de port sera utilisée pour les scans TCP et UDP.

Identifiants

L'onglet « **Credentials** » (Identifiants) illustré ci-dessous permet de configurer le scanner Nessus afin qu'il utilise des identifiants pendant le scan. Si des identifiants sont configurés, Nessus peut effectuer une grande variété de vérifications qui produisent des résultats de scan plus précis.

L'élément du menu déroulant « **Windows credentials** » (Informations d'identification Windows) comporte des paramètres qui fournissent à Nessus des informations telles que le nom du compte SMB, le mot de passe et le nom de domaine. Le protocole SMB (Server Message Block) est un protocole de partage de fichiers qui permet aux ordinateurs de partager des informations de façon transparente sur le réseau. Si Nessus obtient ces informations, il pourra rechercher les informations locales à partir d'un hôte Windows distant. Par exemple, l'utilisation des identifiants permet à Nessus de déterminer si des correctifs de sécurité importants ont été appliqués. Il n'est pas nécessaire de modifier les paramètres par défaut des autres paramètres SMB.



Lorsque plusieurs comptes SMB sont configurés, Nessus tente de se connecter avec les identifiants fournis de manière séquentielle. Une fois que Nessus est en mesure de s'authentifier avec un ensemble d'identifiants, il vérifie les identifiants fournis par la suite, mais il les utilise uniquement si des privilèges administratifs sont accordés lorsque les comptes précédents ont fourni un accès utilisateur.

Certaines versions de Windows vous permettent de créer un nouveau compte et de le désigner en tant qu'« administrator » (administrateur). Ces comptes ne sont pas toujours adaptés à l'exécution de scans authentifiés. Tenable recommande d'utiliser le compte administratif original, nommé « Administrator » (Administrateur) pour les opérations de scan authentifiés afin de garantir un accès complet. Ce compte peut être caché sur certaines versions de Windows. Le compte administratif réel peut être révélé par l'exécution d'une invite DOS dotée de privilèges administratifs et la saisie de la commande suivante :

```
C:\> net user administrator /active:yes
```

Si un compte SMB de maintenance est créé avec des privilèges administrateur limités, Nessus peut scanner plusieurs domaines facilement et en toute sécurité.

Tenable recommande aux administrateurs réseau d'envisager la création de comptes de domaine spécifiques pour faciliter les tests. Nessus inclut divers contrôles de sécurité pour Windows NT, 2000, Server 2003, XP, Vista, Windows 7, Windows 8 et Windows 2008 qui sont plus précis si un compte de domaine est fourni. Nessus tente normalement plusieurs contrôles si aucun compte n'est fourni.



Le service d'accès à distance au Registre de Windows permet aux ordinateurs distants disposant d'identifiants d'accéder au registre de l'ordinateur en cours d'audit. Si le service n'est pas exécuté, la lecture des clés et des valeurs du registre n'est pas possible, même avec des identifiants complets. Pour plus d'informations, consultez l'article du blog de Tenable intitulé « [Dynamic Remote Registry Auditing - Now you see it, now you don't!](#) » (Audit dynamique de registre à distance - entrée et sortie immédiates !). Ce service doit être démarré pour un scan avec identifiants Nessus afin d'exécuter l'audit complet d'un système qui utilise les identifiants.

The screenshot shows the configuration interface for a new advanced policy in Nessus, specifically for Windows credentials. The breadcrumb path is 'New Advanced Policy / Credentials / Windows credentials'. On the left, a sidebar lists 'Policies', 'General Settings', 'Credentials', 'Plugins', and 'Preferences'. The main content area has a 'Credential Type' dropdown menu set to 'Windows credentials'. Below this, there are several input fields for SMB account, password, and domain, along with a dropdown for 'SMB password type' set to 'Password'. There are also checkboxes for 'Never send SMB credentials in clear text' (checked) and 'Only use NTLMv2' (unchecked).

Les utilisateurs peuvent sélectionner « **SSH settings** » (Paramètres SSH) dans le menu déroulant et entrer les identifiants pour scanner les systèmes Unix. Ces identifiants sont utilisés pour obtenir des informations locales à partir de systèmes Unix distants pour l'audit des correctifs ou les contrôles de conformité. Il existe un champ dans lequel saisir le nom de l'utilisateur SSH pour le compte qui va effectuer les contrôles sur le système Unix cible, ainsi que pour le mot de passe SSH ou la paire constituée de la clé publique SSH et de la clé privée. Il existe aussi un champ pour saisir la phrase de passe pour la clé SSH, si elle est requise.



Nessus prend en charge les algorithmes de cryptage `blowfish-cbc`, `aes-cbc` et `aes-ctr`.

Les scans authentifiés les plus efficaces sont ceux pour lesquels les identifiants fournis ont des privilèges « root ». Puisqu'un grand nombre de sites ne permettent pas une ouverture de session à distance au niveau root, les utilisateurs Nessus peuvent invoquer « `su` », « `sudo` », « `su+sudo` », « `dzdo` » ou « `pbrun` » avec un mot de passe séparé pour un compte qui a été établi avec les privilèges « `su` » ou « `sudo` ». De plus, Nessus peut augmenter les privilèges sur les périphériques Cisco en sélectionnant « **Cisco 'enable'** » (Cisco – activer).

Nessus peut utiliser l'accès basé sur clé SSH pour l'authentification sur un serveur distant. Si un fichier `known_hosts` SSH est disponible et fourni dans le cadre de la stratégie de scan, Nessus tentera uniquement d'accéder aux hôtes de ce fichier. Enfin, le « Preferred SSH port » (Port SSH préféré) peut être configuré pour indiquer à Nessus de se connecter à SSH s'il est activé sur un port autre que le port 22.

Nessus crypte tous les mots de passe mémorisés dans les stratégies. Toutefois, il est recommandé d'utiliser les clés SSH pour l'authentification, plutôt que des mots de passe SSH. Ceci permet de vérifier que la combinaison nom d'utilisateur-mot de passe utilisée pour l'audit des serveurs SSH connus n'est pas utilisée pour tenter d'établir une connexion à un système dont vous n'avez peut-être pas le contrôle. Il n'est donc pas recommandé d'utiliser les mots de passe SSH, sauf en cas de nécessité absolue.

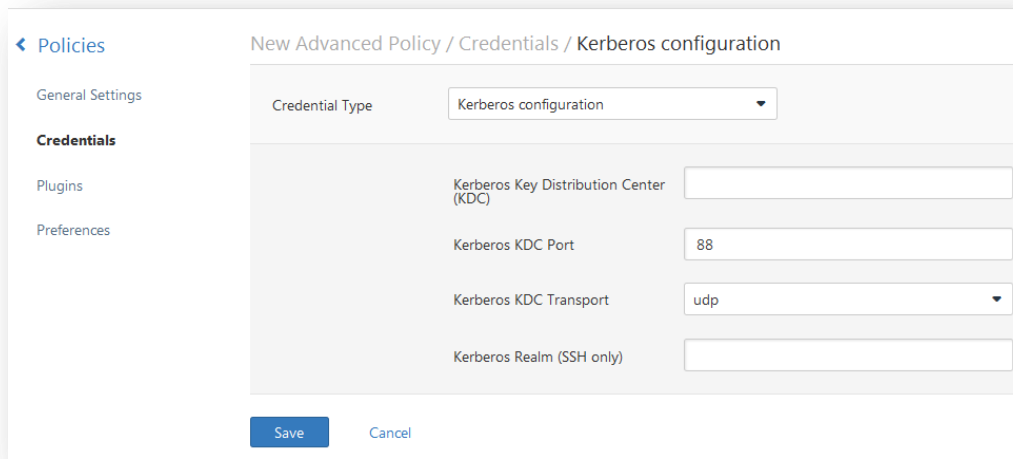
La capture d'écran suivante montre les options SSH disponibles. Le menu déroulant « Elevate privileges with » (Élever les privilèges avec) propose plusieurs méthodes pour accroître les privilèges après l'authentification.

The screenshot shows the 'New Advanced Policy / Credentials / SSH settings' configuration page. On the left, there is a sidebar with 'Policies' selected, and sub-sections for 'General Settings', 'Credentials', 'Plugins', and 'Preferences'. The main area is titled 'New Advanced Policy / Credentials / SSH settings' and contains a form with the following fields:

Field Name	Value / Action
Credential Type	SSH settings
SSH user name	root
SSH password (unsafe!)	
SSH public key to use	Add File
SSH private key to use	Add File
Passphrase for SSH key	
Elevate privileges with	Nothing
Privilege elevation binary path (directory)	
su login	
Escalation account	root
Escalation password	
SSH known_hosts file	Add File
Preferred SSH port	22

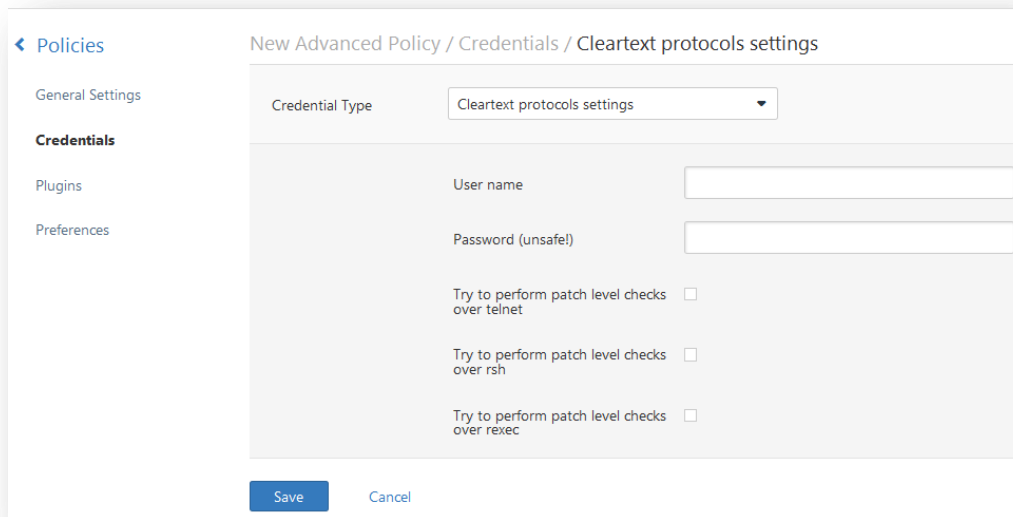
Si un compte autre que `root` doit être utilisé pour l'élévation des privilèges, il peut être spécifié sous « **Escalation account** » (Compte d'élévation) avec « **Escalation password** » (Mot de passe d'élévation).

« **Kerberos configuration** » (Configuration Kerberos) permet de préciser les identifiants en utilisant les clés Kerberos à partir d'un système distant :



The screenshot shows the 'New Advanced Policy / Credentials / Kerberos configuration' window. On the left, there is a sidebar with 'Policies' selected, and sub-sections for 'General Settings', 'Credentials', 'Plugins', and 'Preferences'. The main area has a 'Credential Type' dropdown set to 'Kerberos configuration'. Below this are four input fields: 'Kerberos Key Distribution Center (KDC)', 'Kerberos KDC Port' (with '88' entered), 'Kerberos KDC Transport' (with 'udp' selected in a dropdown), and 'Kerberos Realm (SSH only)'. At the bottom are 'Save' and 'Cancel' buttons.

Enfin, si aucune méthode sécurisée d'exécution des contrôles authentifiés n'est disponible, les utilisateurs peuvent forcer Nessus à tenter d'effectuer les contrôles à l'aide de protocoles non sécurisés, en configurant l'élément de menu déroulant « **Cleartext protocol settings** » (Paramètres de protocole texte en clair). Les protocoles de texte en clair pris en charge par cette option sont **telnet**, **rsh** et **rexec**. De plus, des cases indiquent spécifiquement à Nessus de tenter d'exécuter les contrôles de niveaux de correctif à l'aide des protocoles non sécurisés :



The screenshot shows the 'New Advanced Policy / Credentials / Cleartext protocols settings' window. The sidebar is the same as in the previous screenshot. The main area has a 'Credential Type' dropdown set to 'Cleartext protocols settings'. Below this are three input fields: 'User name', 'Password (unsafe)', and three checkboxes: 'Try to perform patch level checks over telnet', 'Try to perform patch level checks over rsh', and 'Try to perform patch level checks over rexec'. At the bottom are 'Save' and 'Cancel' buttons.

Par défaut, tous les mots de passe (et la stratégie elle-même) sont cryptés. Si la stratégie est sauvegardée dans un fichier `.nessus` et si ce fichier `.nessus` est ensuite copié sur une installation Nessus différente, aucun mot de passe de la stratégie ne sera utilisable par le deuxième scanner Nessus car ce dernier sera incapable de les décrypter.



Il n'est pas recommandé d'utiliser les identifiants texte en clair ! Si les identifiants sont envoyés de façon distante (par exemple par un scan Nessus), ils peuvent être interceptés par toute personne ayant accès au réseau. Utilisez dans la mesure du possible les mécanismes d'authentification cryptés.

Plugins

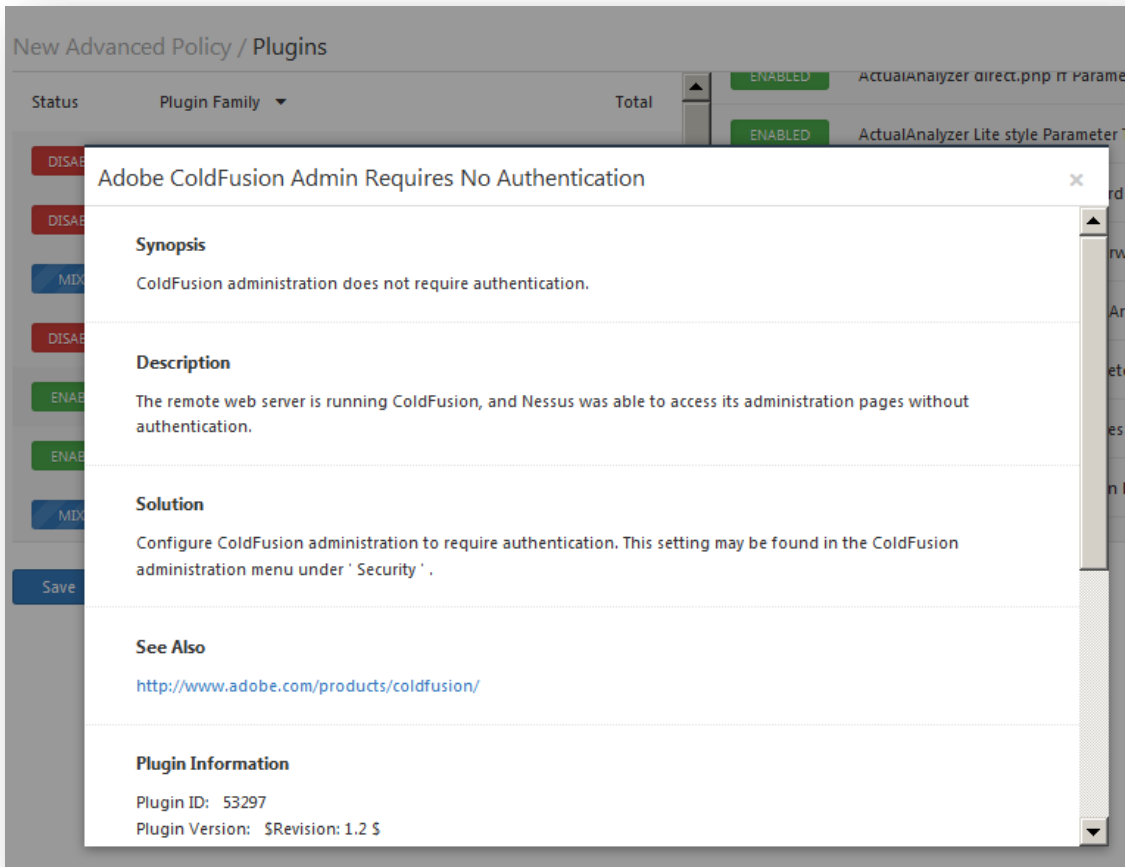
L'onglet « **Plugins** » permet à l'utilisateur de choisir des contrôles de sécurité spécifiques en fonction du groupe de plugins ou des contrôles individuels.

Status	Plugin Family	Total
DISABLED	ADX Local Security Checks	11024
DISABLED	Amazon Linux Local Security Checks	229
MIXED	Backdoors	90
DISABLED	CentOS Local Security Checks	1567
ENABLED	CGI abuses	2723
ENABLED	CGI abuses : XSS	523
MIXED	CISCO	395

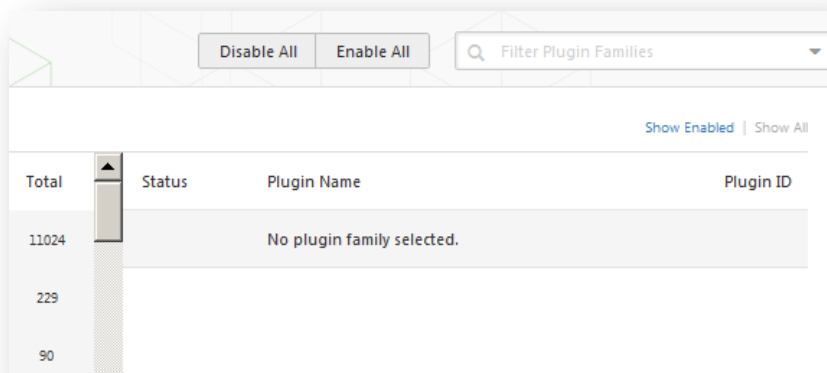
Status	Plugin Name	Plugin ID
ENABLED	.svn/entries Disclosed via Web Server	33821
ENABLED	/doc Directory Browsable	10056
ENABLED	/doc/packages Directory Browsable	10518
ENABLED	2BGal disp_album.php id_album Parameter SQL Inj...	16046
ENABLED	3Com Network Supervisor Traversal Arbitrary File Ac...	19939
ENABLED	4D WebSTAR Tomcat Plugin Remote Buffer Overflow	18212
ENABLED	4Images <= 1.7.1 index.php template Parameter Tra...	21020

Cliquez sur la famille de plugins pour activer (vert) ou désactiver (rouge) l'ensemble du groupe. Si une famille est sélectionnée, la liste de ses plugins s'affiche. Les plugins individuels peuvent être activés et désactivés pour créer des stratégies de scan très particulières. Si certains plugins sont désactivés, la famille passe en bleu et affiche la mention « mixed » (mixte) pour indiquer que seuls certains des plugins sont activés. Le fait de cliquer sur la famille de plugins aura pour effet de charger la liste complète des plugins et d'autoriser la sélection précise à partir de vos préférences de scan.

Si un plugin spécifique est sélectionné, la sortie du plugin s'affiche telle qu'elle sera consignée dans un rapport. Le synopsis et la description fournissent plus d'informations sur la vulnérabilité examinée. Si vous faites défiler dans votre navigateur, vous pouvez également afficher des informations sur les solutions, des références supplémentaires si disponibles, des informations sur les risques et sur les failles, ainsi que la base de données des vulnérabilités ou les références croisées d'informations.



En haut de la page des familles de plugins, vous pouvez créer des filtres afin de constituer une liste de plugins à inclure dans la stratégie, ainsi que pour désactiver ou activer tous les plugins. Les filtres permettent de contrôler de façon précise la sélection de plugins. Plusieurs filtres peuvent être définis dans une même stratégie.



Vous pouvez saisir des informations dans la case de recherche pour filtrer rapidement des plugins par nom afin de les localiser et d'afficher des informations. Cette opération va filtrer les plugins à la volée. En plus des recherches de texte,

vous pouvez saisir `id:10123` pour filtrer rapidement un plugin spécifique. Pour créer un filtre, cliquez sur le bouton « **Filter Options** » (Options de filtre) :

Advanced Search

Match **All** of the following:

Bugtraq ID is equal to NUMBER

Apply Cancel Clear Filters

Chaque filtre créé propose plusieurs options pour affiner une recherche. Les critères de filtre peuvent reposer sur « Any » (N'importe lequel - n'importe quel critère renvoie des correspondances) ou sur « All » (Tous - tous les critères de filtre doivent être présents). Par exemple, pour définir une stratégie incluant uniquement les plugins qui présentent une faille **ou** peuvent être utilisés sans faille scriptée, créez deux filtres et sélectionnez « Any » pour les critères :

Advanced Search

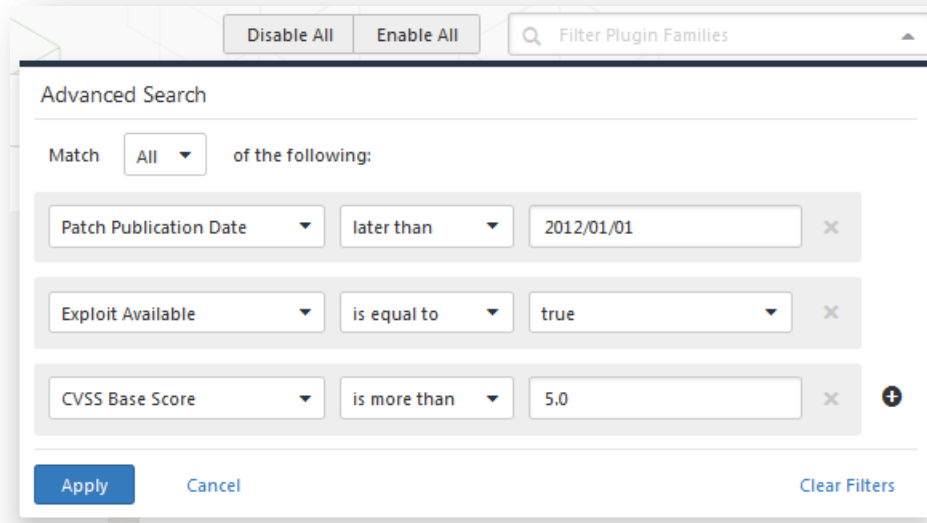
Match **Any** of the following:

Exploitability Ease is equal to Exploits are available

Exploitability Ease is equal to No exploit is required

Apply Cancel Clear Filters

Pour créer une stratégie qui comprend les plugins correspondant à plusieurs critères, sélectionnez « All » et ajoutez les filtres voulus. Par exemple, la stratégie ci-dessous inclurait toute vulnérabilité avec correctif publiée après le 1^{er} janvier 2012 qui présente une faille publique et une note de base CVSS supérieure à 5.0 :



Pour consulter la liste complète des détails et des critères de filtre, reportez-vous à la section [Filtres des rapports](#) de ce document.



Pour utiliser les filtres afin de créer une stratégie, il est recommandé de commencer par désactiver tous les plugins. Utilisez les filtres de plugin pour préciser les plugins à inclure dans votre stratégie. Sélectionnez ensuite chaque famille de plugin et cliquez sur « Enable Plugins » (Activer les plugins).

Lorsqu'une stratégie est créée et sauvegardée, elle enregistre tous les plugins qui ont été sélectionnés initialement. Lorsque de nouveaux plugins sont reçus par l'intermédiaire d'une mise à jour des ressources de plugin, ils sont automatiquement activés si la famille avec laquelle ils sont associés est activée. Si elle a été désactivée ou partiellement activée, les nouveaux plugins de cette famille sont automatiquement désactivés eux aussi.



La famille « Denial of Service » (Déni de service) contient certains plugins susceptibles de causer des pannes sur un réseau si l'option « Safe Checks » (Contrôles sans danger) n'est pas activée. Elle comporte toutefois certains contrôles utiles qui ne causeront pas de problème. Le groupe « Denial of Service » peut être utilisé avec « Safe Checks » pour interdire l'exécution de tout plugin potentiellement dangereux. Toutefois, il est déconseillé d'utiliser la famille « Denial of Service » sur un réseau de production, sauf si cette utilisation est programmée pendant une fenêtre de maintenance et avec l'assistance d'un personnel prêt à répondre à tout problème éventuel.

Préférences

L'onglet « **Préférences** » (Préférences) inclut des fonctions de contrôle précis sur les paramètres de stratégie de scan. Si un élément du menu déroulant est sélectionné, des éléments de configuration supplémentaires sont affichés pour cette catégorie. Il s'agit d'une liste dynamique d'options de configuration qui dépend de la version de Nessus, des stratégies d'audit et des fonctionnalités supplémentaires auxquelles le scanner Nessus connecté a accès. Une version commerciale de Nessus peut avoir des options de configuration plus avancées que Nessus Home. Cette liste change à mesure que des plugins sont ajoutés ou modifiés.

Le tableau suivant fournit un aperçu de toutes les préférences. Pour des informations plus détaillées sur chaque élément de préférence, consultez la section [Détails des préférences de scan](#) de ce document.

Menu déroulant Préférence (Préférence)	Description
ADSI settings (Paramètres ADSI)	L'option Active Directory Service Interfaces (interfaces ADSI) extrait des informations du serveur MDM (serveur de gestion des appareils mobiles) concernant les périphériques Android et iOS.
Apple Profile Manager API Settings (Paramètres d'API de gestionnaire de profil Apple)	Fonction commerciale qui permet l'énumération et le scan des vulnérabilités des périphériques Apple iOS (par exemple, iPhone, iPad).
Cisco IOS Compliance Checks (Contrôles de conformité Cisco IOS)	Option commerciale permettant de spécifier un fichier de stratégie qui sera utilisé pour tester les périphériques basés sur Cisco IOS par rapport aux normes de conformité.
Database Compliance Checks (Contrôles de conformité des bases de données)	Option commerciale permettant de spécifier un fichier de stratégie qui sera utilisé pour tester les bases de données telles que DB2, SQL Server, MySQL et Oracle par rapport aux normes de conformité.
Database Settings (Paramètres de base de données)	Options servant à spécifier le type de base de données à tester, ainsi que les identifiants à utiliser.
Do not scan fragile devices (Ne pas scanner les périphériques fragiles)	Groupe d'options qui indique à Nessus de ne pas scanner des périphériques spécifiques, en raison du risque accru de panne de la cible.
Global variable settings (Paramètres des variables globales)	Large gamme d'options de configuration pour le serveur Nessus.
HTTP cookies import (Importation des cookies HTTP)	Pour les tests des applications Web, cette préférence spécifie un fichier externe pour importer des cookies HTTP afin de permettre l'authentification auprès de l'application.
HTTP login page (Page de connexion HTTP)	Paramètres relatifs à la page de connexion pour le test des applications Web.
IBM iSeries Compliance Checks (Contrôles de conformité IBM iSeries)	Option commerciale permettant de spécifier un fichier de stratégie qui sera utilisé pour tester les systèmes IBM iSeries par rapport aux normes de conformité.
IBM iSeries Credentials (Identifiants IBM iSeries)	C'est ici que sont spécifiés les identifiants pour les systèmes IBM iSeries.
ICCP/COTP TSAP Addressing Weakness (Faiblesse d'adressage ICCP/COTP TSAP)	Option commerciale relative aux tests SCADA [Supervisory Control And Data Acquisition (Réseau de contrôle du système et d'acquisition des données)].
Login configurations (Configurations de connexion)	Sert à spécifier les identifiants pour les tests des services HTTP, NNTP, FTP, POP et IMAP de base.

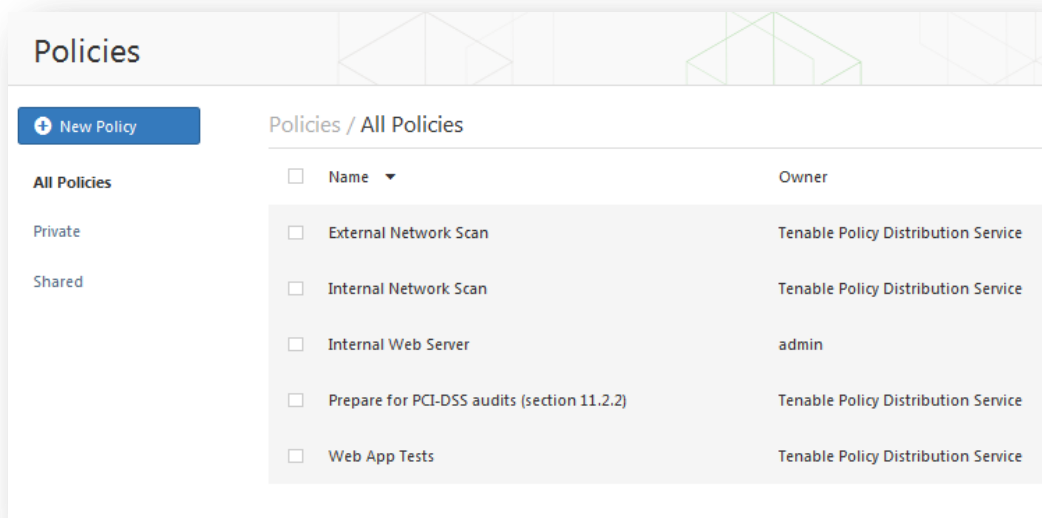
Modbus/TCP Coil Access (Accès à la bobine Modbus/TCP)	Option commerciale relative aux tests SCADA [Supervisory Control And Data Acquisition (Réseau de contrôle du système et d'acquisition des données)].
Nessus SYN scanner (Scanner Nessus SYN)	Options relatives au scanner SYN intégré.
Nessus TCP scanner (Scanner Nessus TCP)	Options relatives au scanner TCP intégré.
News Server (NNTP) Information Disclosure (Divulgarion d'information de serveur de nouvelles (NNTP))	Groupe d'options permettant de tester l'existence de vulnérabilités de divulgation d'informations sur les serveurs NNTP.
Oracle Settings (Paramètres Oracle)	Options relatives au test des installations de base de données Oracle.
PCI DSS compliance (Conformité PCI DSS)	Option commerciale qui indique à Nessus de comparer les résultats des scans par rapport aux PCI DSS standards (Normes PCI DSS).
Patch Management: Red Hat Satellite Server Settings (Gestion de correctifs : paramètres de serveur Red Hat Satellite)	Options permettant d'intégrer Nessus au serveur de gestion de correctifs Red Hat Satellite. Consultez le document Patch Management Integration (Intégration de la gestion de correctifs) pour plus d'informations.
Patch Management: SCCM Server Settings (Gestion de correctifs : paramètres de serveur SCCM)	Options permettant d'intégrer Nessus au serveur de gestion de correctifs SCCM (System Center Configuration Manager). Consultez le document Patch Management Integration (Intégration de la gestion de correctifs) pour plus d'informations.
Patch Management: VMware Go Server Settings (Gestion de correctifs : paramètres de serveur VMware Go)	Options permettant d'intégrer Nessus au serveur de gestion de correctifs VMware Go Server (auparavant Shavlik). Consultez le document Patch Management Integration (Intégration de la gestion de correctifs) pour plus d'informations.
Patch Management: WSUS Server Settings (Gestion de correctifs : paramètres de serveur WSUS)	Options permettant d'intégrer Nessus au serveur de gestion de correctifs WSUS (Windows Server Update Service). Consultez le document Patch Management Integration (Intégration de la gestion de correctifs) pour plus d'informations.
Ping the remote host (Sonder l'hôte à distance)	Paramètres qui contrôlent la détection de réseau basée sur ping de Nessus.
Port scanner settings (Paramètres de scanner des ports)	Deux options qui offrent un plus grand contrôle sur l'activité de scan des ports.
SMB Registry : Start the Registry Service during the scan (Registre SMB : démarrer le service de registre pendant le scan)	Indique à Nessus de démarrer le service de registre SMB sur les hôtes sur lesquels il n'est pas activé.
SMB Scope (Portée SMB)	Indique à Nessus d'interroger les utilisateurs de domaine à la place des utilisateurs locaux.

SMB Use Domain SID to Enumerate Users (SMB utilise le SID de domaine pour énumérer les utilisateurs)	Option permettant de spécifier la plage de SID à utiliser pour effectuer une recherche SMB des utilisateurs de domaine.
SMB Use Host SID to Enumerate Local Users (SMB utilise le SID d'hôte pour énumérer les utilisateurs locaux)	Option permettant de spécifier la plage de SID à utiliser pour effectuer une recherche SMB des utilisateurs locaux.
SMTP Settings (Paramètres SMTP)	Options permettant de tester le protocole SMTP (Simple Mail Transport Protocol).
SNMP Settings (Paramètres SNMP)	Informations de configuration et d'authentification pour le protocole SNMP (Simple Network Management Protocol).
Service Detection (Détection du service)	Options indiquant à Nessus comment tester les services SSL.
Unix Compliance Checks (Contrôles de conformité Unix)	Option commerciale permettant de spécifier un fichier de stratégie qui sera utilisé pour tester les systèmes Unix par rapport aux normes de conformité.
VMware SOAP API Settings (Paramètres de l'API SOAP VMware)	Informations de configuration et d'authentification pour l'API SOAP de VMware.
Wake-on-LAN (WOL, éveil sur réseau local)	Indique à Nessus d'envoyer des paquets WOL (éveil sur réseau local) avant d'effectuer un scan.
Web Application Test Settings (Paramètres des tests des applications Web)	Options relatives au test des applications Web.
Web mirroring (Mise en miroir Web)	Détails de configuration qui contrôlent le nombre de page Web que Nessus va mettre en miroir, afin d'analyser le contenu pour détecter les vulnérabilités potentielles.
Windows Compliance Checks (Contrôles de conformité Windows)	Option commerciale permettant de spécifier un fichier de stratégie qui sera utilisé pour tester les systèmes Windows par rapport aux normes de conformité.
Windows File Contents Compliance Checks (Contrôles de conformité du contenu des fichiers Windows)	Option commerciale permettant de spécifier un fichier de stratégie qui sera utilisé pour tester les systèmes placés sur les systèmes Windows par rapport aux normes de conformité.



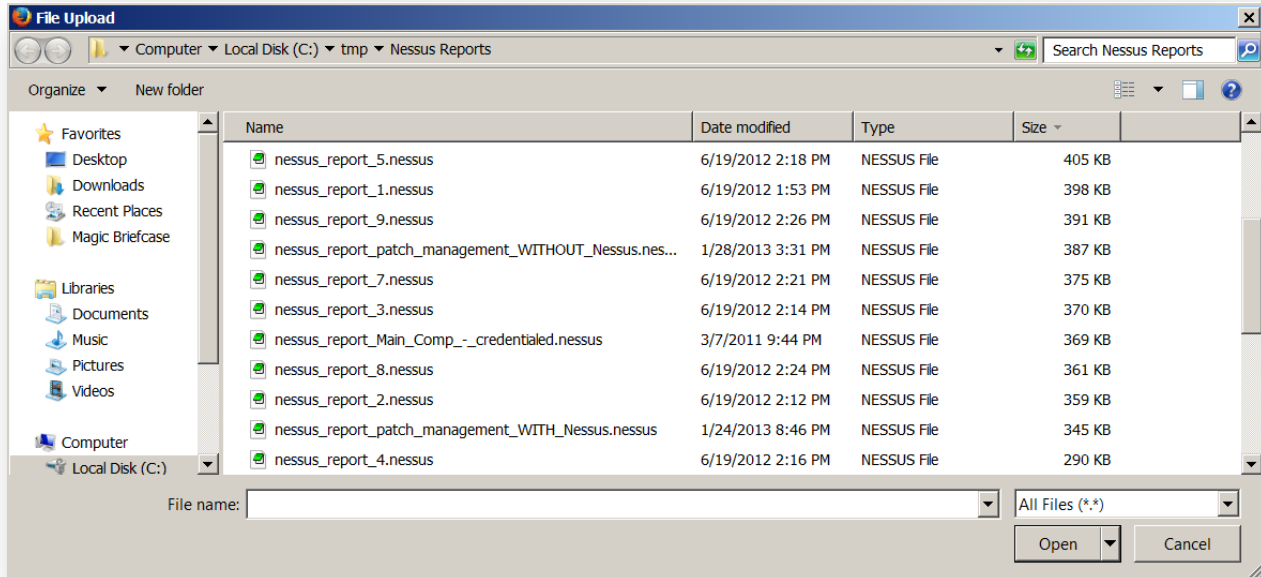
En raison des mises à jour des métadonnées XML dans Nessus 5, les données de conformité générées dans Nessus 4 ne seront pas disponibles dans le chapitre relatif aux contrôles de conformité des rapports exportés. Cependant, les données de conformité seront disponibles dans l'interface utilisateur de Nessus.

Pour faciliter l'organisation, Nessus propose deux filtres prédéfinis sur le côté gauche de la fenêtre, correspondant aux stratégies « Private » (Privées) et « Shared » (Partagées) :



Importation, exportation et copie des stratégies

Le bouton « **Upload** » (Télécharger) de la barre de menu Policies (Stratégies) permet de télécharger vers le scanner des stratégies créées précédemment. En utilisant la boîte de dialogue du navigateur de fichiers natif, sélectionnez la stratégie sur le système local et cliquez sur « **Open** » (Ouvrir) :



Le bouton « **Options** » (Options) de la barre de menu permet de télécharger une stratégie sélectionnée du scanner vers le système de fichiers local. La boîte de dialogue de téléchargement du navigateur permet d'ouvrir la stratégie dans un programme externe (par exemple, un éditeur de texte) ou d'enregistrer la stratégie dans le répertoire de votre choix.

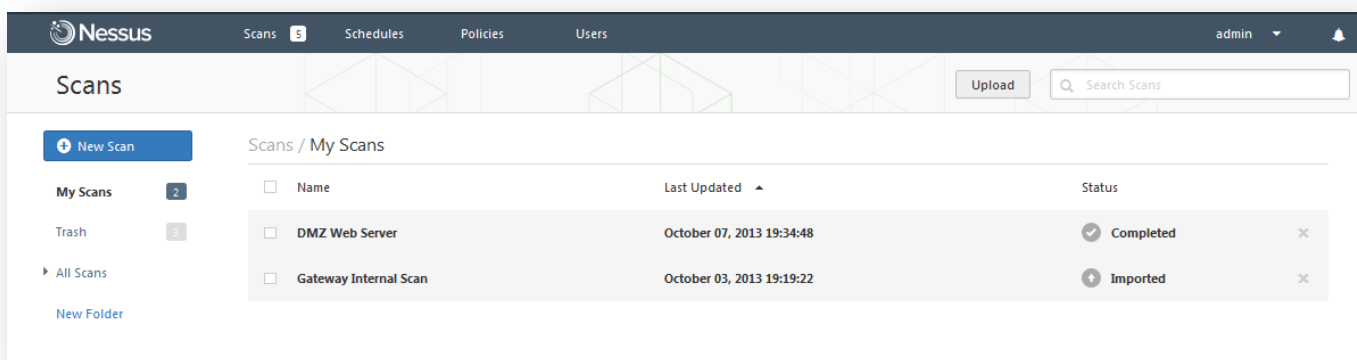


Les mots de passe et les fichiers `.audit` contenus dans une stratégie ne seront pas exportés.

Si vous souhaitez créer une stratégie similaire à une stratégie existante avec des modifications mineures, vous pouvez sélectionner la stratégie de base dans la liste et cliquer sur « **Options** » (Options), puis sur « **Copy Policy** » (Copier la stratégie) dans la barre de menu. Ceci crée une copie de la stratégie initiale qui peut être éditée pour y apporter les modifications requises. Cette opération est utile pour créer des stratégies standard avec des modifications mineures, requises dans certains environnements.

Création, lancement et programmation d'un scan

Les utilisateurs peuvent créer leurs propres rapports par chapitres : Vulnerability Centric, Host Centric, Compliance ou Compliance Executive. Le format HTML est toujours pris en charge par défaut ; cependant, si Java est installé sur l'hôte scanner, il est également possible d'exporter des rapports au format PDF. En utilisant les filtres de rapport et les fonctions d'exportation, les utilisateurs peuvent créer les rapports dynamiques de leur choix au lieu de les sélectionner à partir d'une liste spécifique.

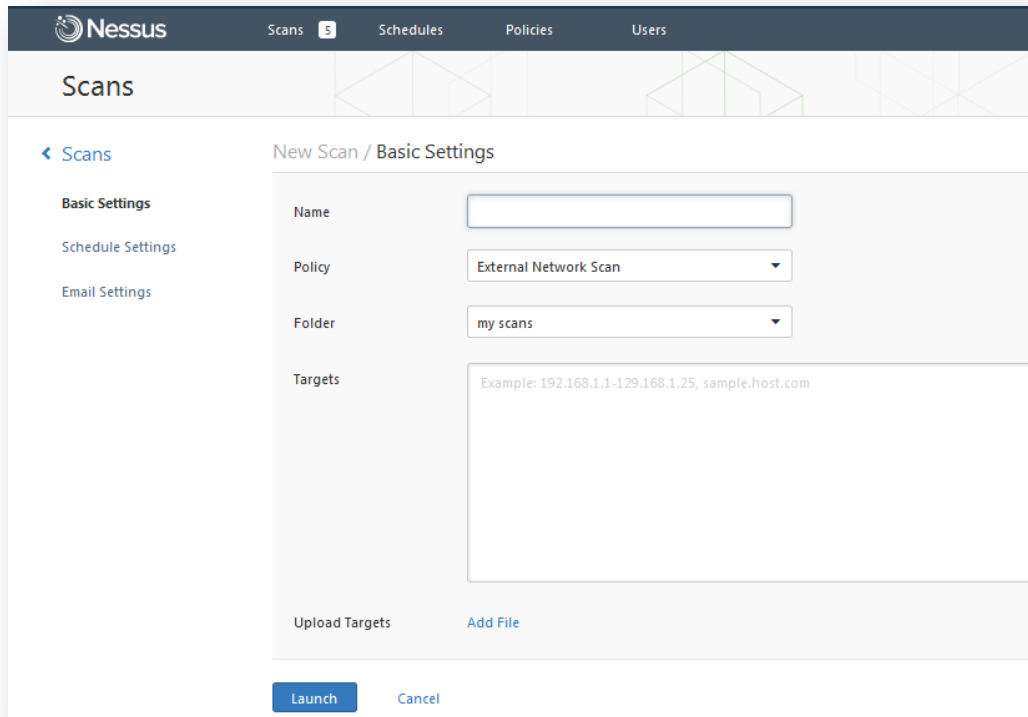


Les états de scan suivants sont disponibles dans le tableau des listes de scan :

État du scan	Description
Completed (Terminé)	Le scan est totalement terminé.
Canceled (Annulé)	L'utilisateur a arrêté le scan avant la fin.
Aborted (Abandonné)	Le scan a été abandonné du fait d'une liste cible non valide ou d'une erreur de serveur (par exemple, redémarrage, panne)
Imported (Importé)	Le scan a été importé à l'aide de la fonctionnalité de téléchargement en amont.

Ces états s'appliquent uniquement aux nouveaux scans. Les anciens scans sont tous considérés comme « completed » (terminés). Les scans possédant le même état peuvent être répertoriés dans les dossiers virtuels du volet de navigation de gauche.

Après avoir créé ou sélectionné une stratégie, vous pouvez créer un nouveau scan en cliquant sur l'option « **Scans** » (Scans) dans la barre de menu du haut, puis en cliquant sur le bouton « **+ New Scan** » (Nouveau scan) à droite. L'écran « **New Scan** » (Nouveau scan) s'affiche comme suit :



Sous l'onglet « **Basic Settings** » (Paramètres de base), cinq champs servent à saisir le scan cible :

- **Name** (Nom) : définit le nom qui sera affiché dans l'IU Nessus pour identifier le scan.
- **Policy** (Stratégie) : sélectionnez une stratégie créée précédemment que le scan utilisera pour définir les paramètres contrôlant le comportement de scan du serveur Nessus.
- **Folder** (Dossier) : dossier d'IU Nessus dans lequel les résultats de scan seront consignés.
- **Scan Targets** (Cibles de scan) : les cibles peuvent être saisies selon les adresses IP simples (par exemple 192.168.0.1), une plage IP (par exemple 192.168.0.1-192.168.0.255), un sous-réseau avec notation CIDR (par exemple 192.168.0.0/24) ou un hôte résolvable (par exemple www.nessus.org).
- **Upload Targets** (Télécharger les cibles en amont) :- un fichier texte avec une liste d'hôtes peut être importé en cliquant sur « **Add File** » (Ajouter un fichier) et en sélectionnant un fichier sur l'ordinateur local.



Le fichier des hôtes doit être formaté comme texte ASCII avec un hôte par ligne, sans aucun espace ou ligne supplémentaire. Le codage Unicode/UTF-8 n'est pas pris en charge.

Exemples de format de fichier hôte :

Hôtes individuels :

192.168.0.100

192.168.0.101
192.168.0.102

Plage d'hôtes :

192.168.0.100-192.168.0.102

Bloc d'hôtes CIDR :

192.168.0.1/24

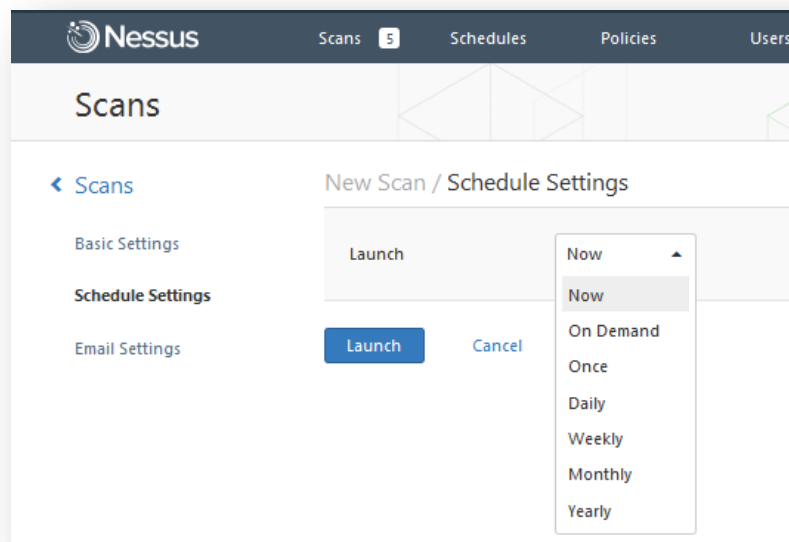
Serveurs virtuels :

www.tenable.com[192.168.1.1]
www.nessus.org[192.168.1.1]
www.tenablesecurity.com[192.168.1.1]



En fonction de vos paramètres de scan comme « **max hosts** » (nombre d'hôtes max.) ou « **max checks per host** » (vérifications max. par hôte), un ralentissement des hôtes virtuels peut se produire puisque Nessus les considère comme une adresse IP unique. Sur les hôtes autres que Windows, les administrateurs Nessus peuvent ajouter le paramètre `multi_scan_same_host`, un paramètre avancé personnalisé, et lui attribuer la valeur `true`. Cette opération permettra au scanner d'effectuer plusieurs scans sur la même adresse IP. Sous Windows, le pilote PCAP ne permet pas cette opération, quelle que soit la configuration Nessus. Cette fonctionnalité est disponible dans Nessus 5.2.0 et versions ultérieures.

L'onglet « **Schedule Settings** » (Paramètres de programmation) propose un menu déroulant qui contrôle le lancement du scan :



Les options de lancement sont les suivantes :

- **Now** (Maintenant) – Démarre le scan immédiatement.
- **On Demand** (À la demande) – Crée le scan sous forme de modèle afin qu'il puisse être lancé manuellement à tout moment (cette fonction était auparavant proposée sous l'option « Scan Template » (Modèle de scan)).

- **Once** (Une fois) – Programme le scan à une heure spécifique.
- **Daily** (Chaque jour) – Programme le scan pour une exécution quotidienne, à une heure spécifique ou à intervalle pouvant aller jusqu'à 20 jours.
- **Weekly** (Chaque semaine) – Programme le scan pour une exécution récurrente, par heure et jour de la semaine, pour une période pouvant aller jusqu'à 20 semaines.
- **Monthly** (Chaque mois) – Programme le scan pour une exécution mensuelle, par heure et jour du mois, pour une période pouvant aller jusqu'à 20 mois.
- **Yearly** (Chaque année) – Programme le scan pour une exécution annuelle, par heure et jour, pour une période pouvant aller jusqu'à 20 ans.

Voici un exemple de scan programmé :

New Scan / Schedule Settings

Launch: Weekly

Starts On: 10/15/2013 21:30 Mountain Standard Time

Repeat: 1 Weeks

Repeat On: S M T W T F S

Save Cancel

Une fois créés, les scans programmés sont accessibles à partir du menu « Schedules » (Programmations) en haut de la fenêtre. Cette page permet de gérer les scans programmés et de les mettre à jour selon les besoins :

Schedules

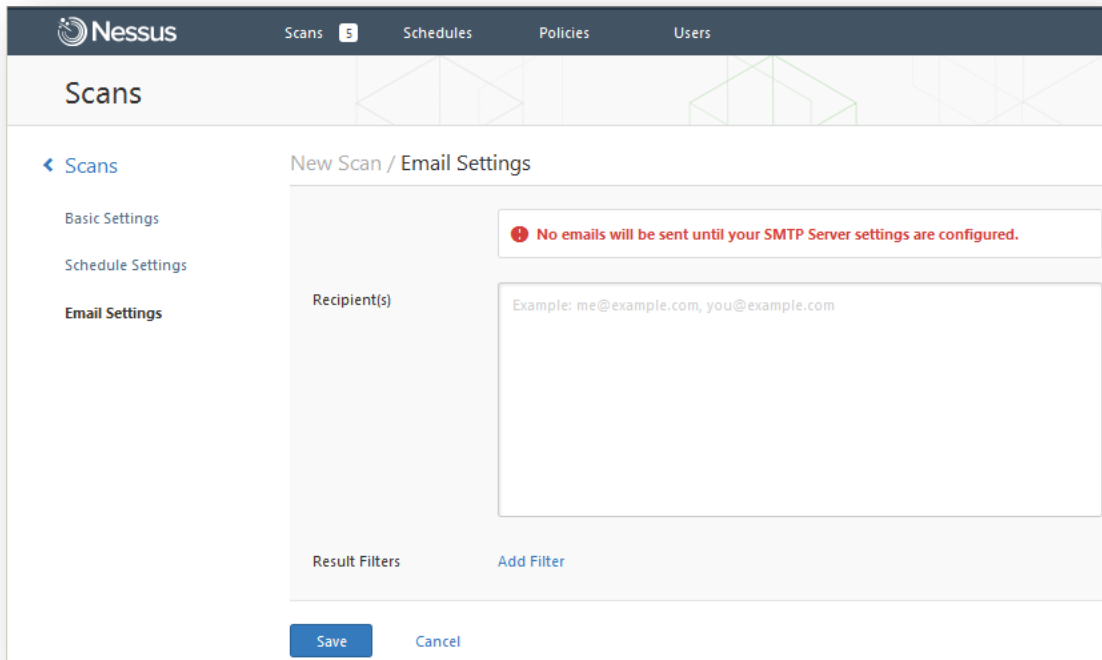
New Schedule

All Schedules

Schedules / All Schedules

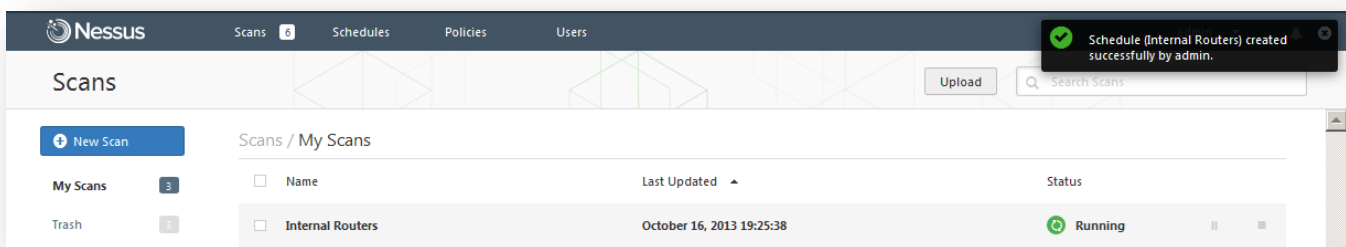
<input type="checkbox"/>	Name	Time	Policy		
<input type="checkbox"/>	Web App 14 Dev Server	On Demand	Web App Tests	▶	✕
<input type="checkbox"/>	Weekly Router Scan	On Demand	External Network Scan	▶	✕

L'onglet « **Email Settings** » (Paramètres de courrier électronique) permet de configurer, le cas échéant, les adresses électroniques auxquelles les résultats du scan seront envoyés à l'issue du scan.

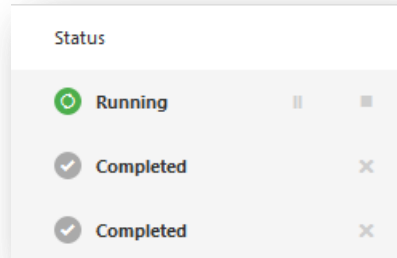


La fonction « **Email Scan Results** » (Envoi des résultats de scan par e-mail) exige qu'un administrateur Nessus configure les paramètres SMTP. Pour plus d'informations sur la configuration des paramètres SMTP, consultez le [Nessus 5.2 Installation and Configuration Guide](#) (Guide d'installation et de configuration Nessus 5.2). Si vous n'avez pas encore configuré ces paramètres, Nessus vous avertit qu'ils doivent être définis pour garantir la bonne exécution de cette fonctionnalité.

Après avoir saisi les informations sur le scan, cliquez sur « **Save** » (Enregistrer). Une fois la soumission effectuée, le scan commence immédiatement si « **Now** » (Maintenant) a été sélectionné, avant que l'affichage ne revienne à la page générale « **Scans** » (Scans). La barre de menu du haut actualise également le nombre qui recouvre le bouton « **Scans** » pour indiquer le nombre total de scans présents.



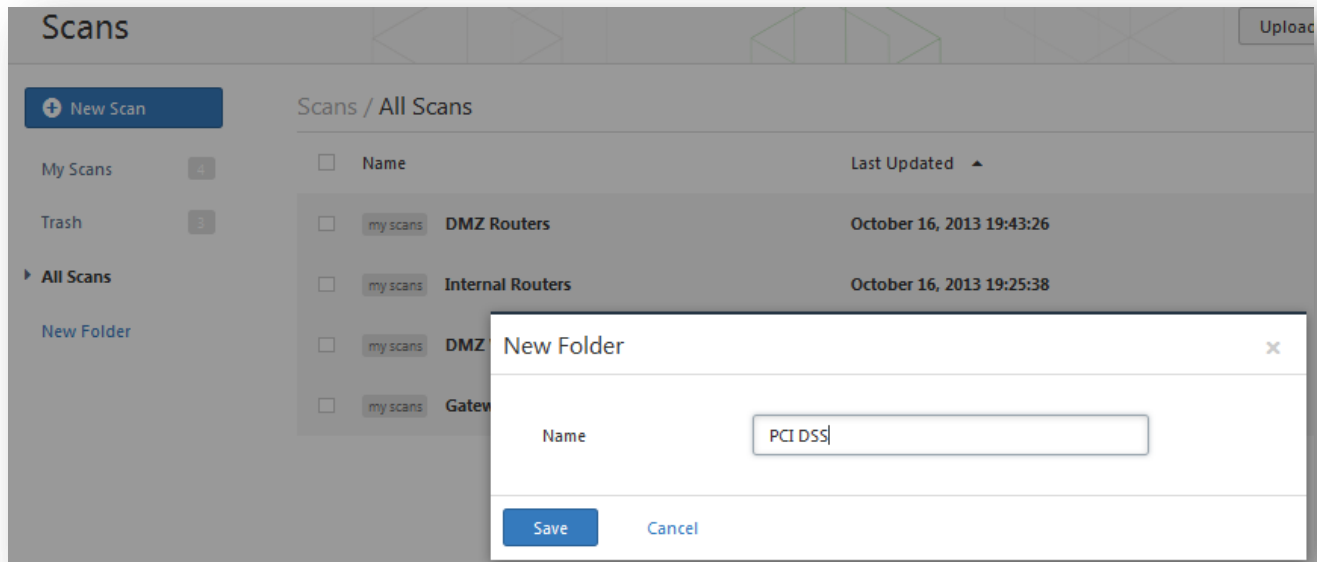
Une fois qu'un scan est lancé, la liste « **Scans** » (Scans) affiche une liste de tous les scans en cours d'exécution ou en pause, ainsi que des informations de base sur les scans. Pendant l'exécution d'un scan, vous pouvez utiliser le bouton de pause et d'arrêt qui s'affichent à gauche pour change l'état :



Lorsque vous sélectionnez un scan spécifique dans la liste à l'aide de la case de gauche, les boutons « **More** » (Plus) et « **Move To** » (Déplacer vers) dans le coin supérieur droit vous permettent d'effectuer d'autres actions, comme renommer le scan, manipuler son état, le marquer comme lu ou le déplacer dans un autre dossier.

Parcourir les résultats du scan

Les scans peuvent être organisés dans des dossiers. Vous voyez deux dossiers par défaut à gauche, My Scans (Mes scans) et Trash (Corbeille). Par défaut, les nouveaux scans apparaissent toujours dans le dossier virtuel **My Scans**. Vous pouvez changer l'emplacement par défaut pour les nouveaux scans et créer des dossiers supplémentaires à l'aide de l'option « **New Folder** » (Nouveau dossier), montrée ci-dessous :

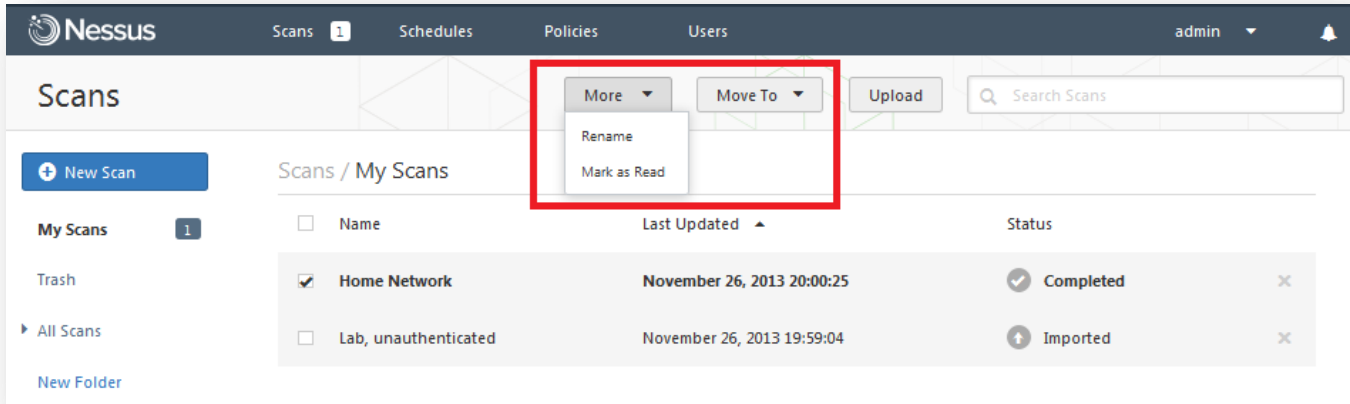


Les dossiers peuvent également être gérés au moyen du menu « **User Profile** » -> « **Folders** » (Profil utilisateur -> Dossiers).

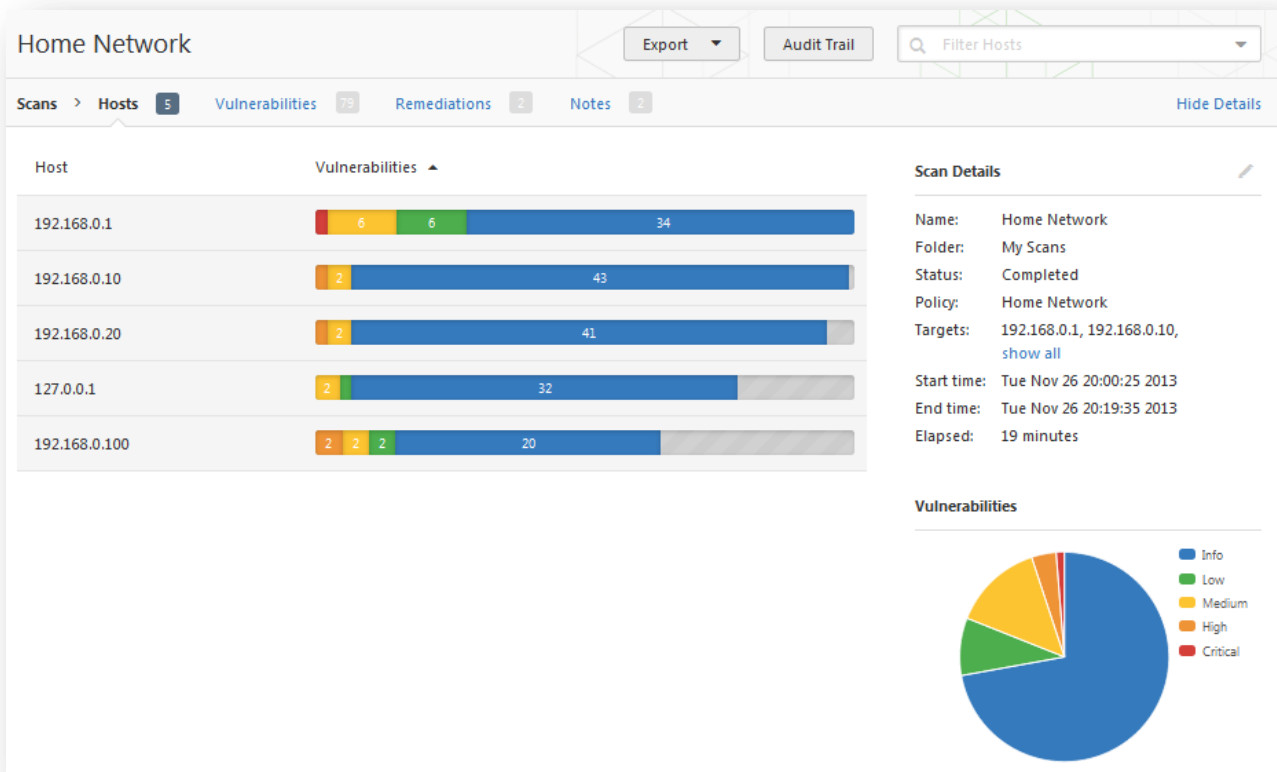


Les scans placés dans le dossier « Trash » (Corbeille) sont automatiquement supprimés après 30 jours. Vous pouvez les supprimer individuellement à votre convenance ou vous pouvez sélectionner « **Empty Trash** » (Vider la corbeille) en haut de la fenêtre.

Pour déplacer les résultats de scan d'un dossier à l'autre, sélectionnez le scan en cochant la case placée à gauche. Lorsque la case est cochée, d'autres menus déroulants apparaissent en haut. L'un d'eux propose les options « More » (Plus), qui permettent notamment de renommer le scan ou de le marquer comme lu ou non lu. Le deuxième menu permet de déplacer le scan dans le dossier voulu.



Pour parcourir les résultats d'un scan, cliquez sur un rapport dans la liste. Ceci permet d'afficher les résultats en naviguant vers les résultats par vulnérabilités ou par hôte, en affichant les ports et les informations de vulnérabilités spécifiques. La vue/L'onglet par défaut est un résumé par hôte, qui affiche la liste des hôtes avec un résumé des vulnérabilités par hôte, doté d'un code couleur :



Si des erreurs surviennent au cours du scan, une notation apparaît au début des résultats :

Network interface not supported

The network interface '\\Device\NPF{F3957D14-D708-454D-93A7-C7DFF8F076F6}' does not support packet forgery. This prevents Nessus from determining whether some of the target hosts are alive and from performing a full port scan against them. You may partially work around this problem by editing your scan settings to disable 'Ping' (Uncheck General->Ping host) and by providing Nessus with credentials to the remote host to prevent a port scan from taking place, however it would be preferable to scan over a different network interface.

Cliquez sur « Hide Details » (Masquer les résultats) en haut à droite pour supprimer les détails du scan afin d'afficher plus d'informations relatives au résumé des hôtes.

Dans la vue récapitulative « Hosts » (Hôtes), chaque résumé contient des détails sur les résultats de vulnérabilité ou d'informations, ainsi que des **Host Details** (Détails de l'hôte) qui fournissent des informations générales sur l'hôte scanné. Si l'option « **Allow Post-Scan Report Editing** » (Autoriser la modification des rapports après le scan) a été sélectionnée pour la stratégie de scan, l'utilisateur peut supprimer un hôte du rapport en sélectionnant l'icône de corbeille, à droite de l'option **Host Details** (Détails de l'hôte).

Home Network

Export Audit Trail Filter Vulnerabilities

Hosts > 192.168.0.1 > Vulnerabilities 34 Hide Details

Severity	Plugin Name	Plugin Family	Count
CRITICAL	Portable SDK for UPnP Devices (libupnp) ...	Gain a shell remotely	1
MEDIUM	DNS Server Cache Snooping Remote Info...	DNS	1
MEDIUM	SSL Certificate Cannot Be Trusted	General	1
MEDIUM	SSL Certificate Signed using Weak Hashi...	General	1
MEDIUM	SSL Medium Strength Cipher Suites Supp...	General	1
MEDIUM	SSL Version 2 (v2) Protocol Detection	Service detection	1
MEDIUM	SSL Weak Cipher Suites Supported	General	1
LOW	Unencrypted Telnet Server	Misc.	2
LOW	DHCP Server Detection	Service detection	1
LOW	SSL / TLS Renegotiation Handshakes MIT...	General	1

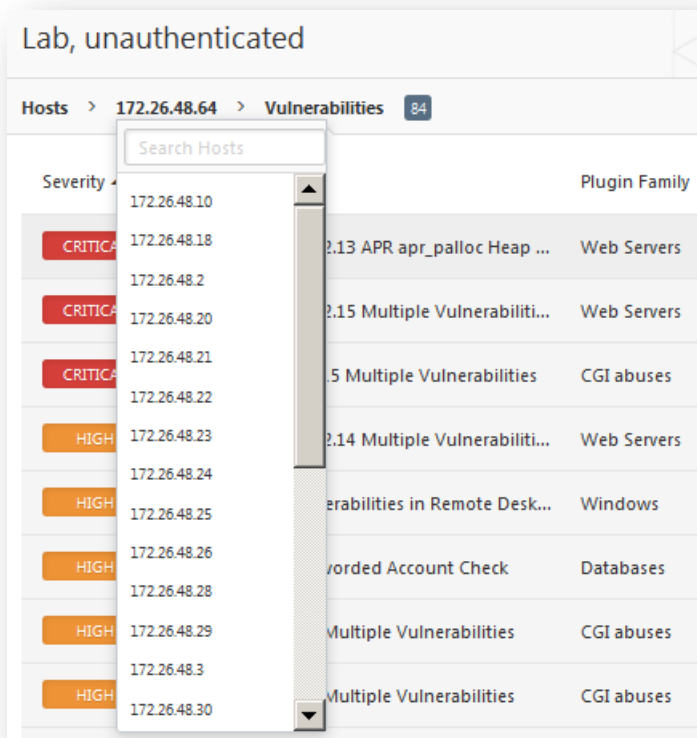
Host Details

IP: 192.168.0.1
MAC: 00:24:7b:b9:2b:4c
OS: Linux Kernel 2.4
Linux Kernel 2.6
Start time: Tue Nov 26 20:00:25 2013
End time: Tue Nov 26 20:19:25 2013
KB: Download

Vulnerabilities

Severity	Count
Info	10
Low	3
Medium	7
High	0
Critical	1

Pour passer rapidement à un autre hôte, cliquez sur l'hôte indiqué dans le flux de navigation en haut pour afficher un menu déroulant qui répertorie les autres hôtes. S'il y a beaucoup d'hôtes, une case de recherche permet de localiser rapidement l'hôte voulu :



Lorsque vous cliquez sur une vulnérabilité dans l'onglet Hosts (Hôtes) ou Vulnerabilities (Vulnérabilités), le programme affiche des informations de vulnérabilité, notamment une description, une solution, des références et les sorties de plugin disponibles. La zone **Plugin Details** (Détails du plugin) s'affiche à droite pour fournir des informations supplémentaires sur le plugin et la vulnérabilité associée. À partir de cet écran, l'icône de crayon à droite de la zone **Plugin Details** (Détails du plugin) permet de modifier la vulnérabilité affichée :

Home Network
Export ▼
Audit Trail

Hosts > 192.168.0.1 > Vulnerabilities 34
Hide Details

CRITICAL

Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack ...

< >

Description

According to its banner, the version of Portable SDK for UPnP Devices (libupnp) running on the remote host is older than 1.6.18, and therefore, has multiple stack buffer overflow vulnerabilities. A remote, unauthenticated attacker could exploit any of these vulnerabilities to execute arbitrary code. Many applications that use this library execute the vulnerable code as root.

Solution

Upgrade to libupnp 1.6.18 or later. If libupnp is used as a third party library by a different application, contact the vendor of that application for a fix.

See Also

<http://www.nessus.org/u?37da582a>
<https://community.rapid7.com/docs/DOC-2150>
<http://www.nessus.org/u?ef4b795d>
<http://www.nessus.org/u?698e06b3>

Plugin Output

▼ 192.168.0.1
1

Port: 53 / tcp

Service: www

```

Server banner : Linux/2.4.17_mv121-malta-mips_fp_1e, UPnP/1.0, Intel SDK for UPnP devices
/1.2
Installed version : 1.2
Fixed version : 1.6.18

```

Plugin Details

Severity: Critical
ID: 64394
Version: \$Revision: 1.7 \$
Type: remote
Family: Gain a shell remotely
Published: 2013/02/01
Modified: 2013/09/20

Risk Information

Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C
CVSS Temporal Score: 8.3

Vulnerability Information

Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: 2013/01/29
Vulnerability Pub Date: 2013/01/29

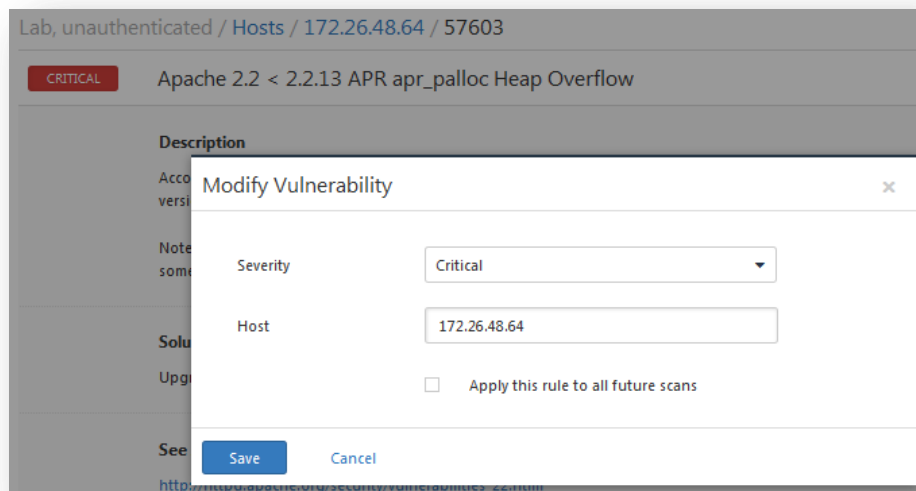
Exploitable With

Metasploit (Portable UPnP SDK
unique_service_name) Remote Code Execution

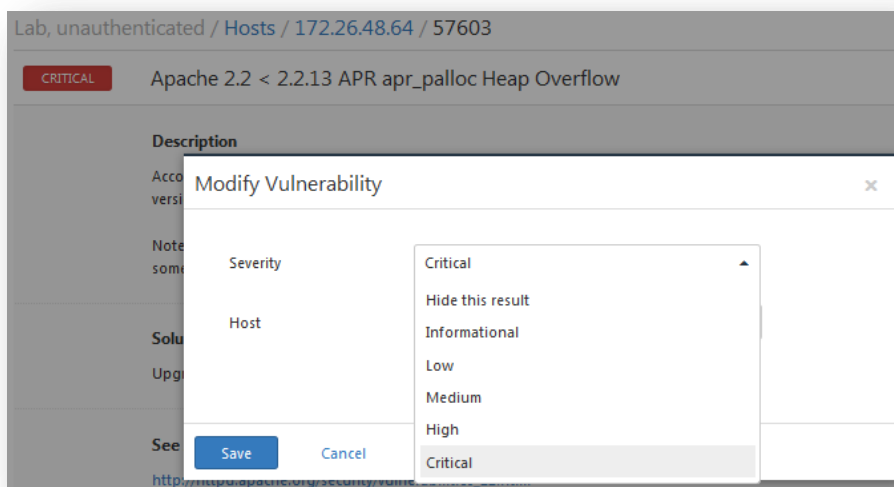
Reference Information

CVE: [CVE-2012-5958](#), [CVE-2012-5959](#),
[CVE-2012-5960](#), [CVE-2012-5961](#), [CVE-2012-5962](#)

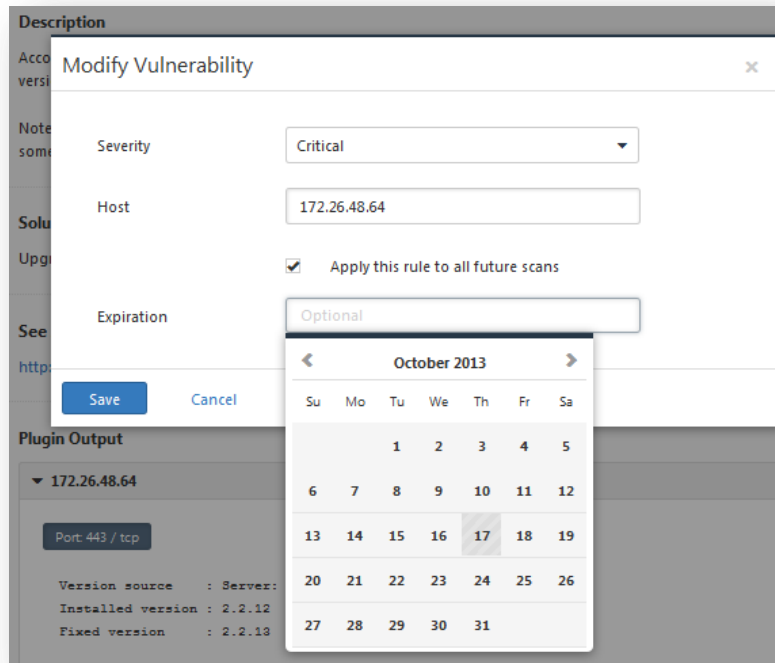
Cliquez sur l'icône de crayon pour afficher la boîte de dialogue montrée ci-dessous :



Le menu déroulant Severity (Gravité) permet de modifier le niveau de gravité de la vulnérabilité en question, ainsi que de la masquer dans le rapport :



Une fois que vous avez apporté cette modification, cliquez sur « **Save** » (Enregistrer) pour l'enregistrer et l'appliquer à la vulnérabilité en question. De plus, il vous suffit de cliquer sur l'option pour appliquer la modification à tous les rapports ultérieurs. Vous ouvrez ainsi une boîte de dialogue qui permet de définir une date d'expiration facultative pour la règle de modification :



Vous pouvez utiliser le calendrier pour sélectionner la date d'expiration. À la date sélectionnée, la règle de modification spécifiée ne sera plus appliquée à ces résultats.

Les règles globales régissant la redéfinition du risque/de la gravité du plugin peuvent être établies dans la zone « **User Profile** » -> « **Plugin Rules** » (Profil utilisateur -> Règles de plugin) de Nessus.



Le degré de gravité provient de la note CVSS associée, où 0 correspond à « Info », moins de 4 à « Bas », moins de 7 à « Moyen », moins de 10 à « Haut » et une note CVSS de 10 est signalée comme étant « Critique ».

Sélectionnez l'onglet « **Vulnerabilities** » (Vulnérabilités) en haut de la fenêtre pour passer dans la vue Vulnérabilité. Cette vue trie les résultats en fonction des vulnérabilités plutôt que des hôtes et elle indique le nombre d'hôtes affectés à droite. La sélection d'une vulnérabilité fournit les mêmes informations que précédemment et inclut en plus, au bas de la fenêtre, la liste des hôtes affectés.

Home Network Export ▼ Audit Trail

Scans > Hosts 5 Vulnerabilities 79 Remediations 2 Notes 2 Hide Details

HIGH Microsoft Windows SMB Shares Unprivileged Access < >

Description

The remote has one or more Windows shares that can be accessed through the network with the given credentials.

Depending on the share rights, it may allow an attacker to read/write confidential data.

Solution

To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing' tab, and click on 'permissions'.

Affected Host List

▶ 192.168.0.20	1
▶ 192.168.0.10	1

Plugin Details ✎

Severity: High
 ID: 42411
 Version: \$Revision: 1.7 \$
 Type: remote
 Family: Windows
 Published: 2009/11/06
 Modified: 2011/03/27

Risk Information

Risk Factor: High
 CVSS Base Score: 7.5
 CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P
 CVSS Temporal Vector: CVSS2#E:H/RL:U/RC:ND
 CVSS Temporal Score: 7.5

Vulnerability Information

Exploit Available: true
 Exploit Ease: No exploit is required
 Vulnerability Pub Date: 1999/07/14

Reference Information

CVE: [CVE-1999-0519](#), [CVE-1999-0520](#)
 OSVDB: [299](#)
 BID: [8026](#)

Si vous cliquez sur un hôte affecté, vous chargez la vue des vulnérabilités par hôte.

Si un scan lancé utilise une [compliance policy](#) (stratégie de conformité), les résultats sont affichés dans un nouvel onglet latéral du rapport de scan, l'onglet « **Compliance** » (Conformité) :

POL_Windows_2003_Domain_Controller_...

Export

Filter Compliance

Scans > Hosts 1 Vulnerabilities 89 Compliance 216 Hide Details

Status	Plugin Name	Plugin Family	Count
FAILED	2 Auditing and Account Policies (Minor A...	Windows Compliance Checks	2
FAILED	3 Security Settings (Minor Settings): 111.2...	Windows Compliance Checks	2
FAILED	3 Security Settings (Minor Settings): 111.2...	Windows Compliance Checks	2
FAILED	3 Security Settings (Minor Settings): 111.2...	Windows Compliance Checks	2
FAILED	3 Security Settings (Minor Settings): 111.2...	Windows Compliance Checks	2
FAILED	3 Security Settings (Minor Settings): 111.2...	Windows Compliance Checks	2
FAILED	3 Security Settings (Minor Settings): 111.2...	Windows Compliance Checks	2
FAILED	3 Security Settings (Minor Settings): 111.2...	Windows Compliance Checks	2

Scan Details

Name: POL_Windows_2003_Domain_Controller_PRO
 Folder: My Scans
 Status: Imported

Compliance

Legend:
 - Passed (Green)
 - Warning (Orange)
 - Failed (Red)

Nessus propose deux autres onglets en plus des onglets **Hosts** (Hôtes) et **Vulnerabilities** (Vulnérabilités). L'onglet **Remediations** (Solutions) propose des informations récapitulatives qui permettent de remédier aux principaux problèmes détectés. Ces recommandations vous fourniront les solutions les plus efficaces pour réduire considérablement le nombre de vulnérabilités :

Home Network

Export Audit Trail

Scans > Hosts 5 Vulnerabilities 79 Remediations 2 Notes 2 Hide Details

Taking the following actions across 2 hosts would resolve 42% of the vulnerabilities on the network:

Action to take	Vulns	Hosts
Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack Buffer Overflows: Upgrade to libupnp 1.6.18 or later. If libupnp is used as a third party library by a different application, contact the vendor of that application for a fix.	8	1
Apache 2.0 < 2.0.65 Multiple Vulnerabilities: Either ensure that the affected modules are not in use or upgrade to Apache version 2.0.65 or later.	6	1

Scan Details

Name: Home Network
 Folder: My Scans
 Status: Completed
 Policy: Home Network
 Targets: 192.168.0.1, 192.168.0.10, [show all](#)
 Start time: Tue Nov 26 20:00:25 2013
 End time: Tue Nov 26 20:19:35 2013
 Elapsed: 19 minutes

L'onglet Notes propose des recommandations pour améliorer les résultats du scan :

The screenshot shows the Nessus interface for a scan titled "Home Network". At the top, there are navigation tabs for "Scans", "Hosts" (5), "Vulnerabilities" (79), "Remediations" (2), and "Notes" (2). The "Notes" tab is active. On the left, under "Scan Notes", there are two entries: "Missing SSH credentials" with a link to a step-by-step guide, and "Windows compliance checks not enabled" with a link to compliance checks. On the right, the "Scan Details" panel shows: Name: Home Network, Folder: My Scans, Status: Completed, Policy: Home Network, Targets: 192.168.0.1, 192.168.0.10, Start time: Tue Nov 26 20:00:25 2013, End time: Tue Nov 26 20:19:35 2013, and Elapsed: 19 minutes.

Filtres des rapports

Nessus offre un système polyvalent de filtres qui facilite l'affichage des résultats spécifiques des rapports. Ces filtres peuvent être utilisés pour afficher les résultats en fonction de tout aspect des découvertes des vulnérabilités. Lorsque plusieurs filtres sont utilisés, des vues de rapport plus détaillées et personnalisées peuvent être créées.

Le premier type de filtre est une chaîne de texte simple saisie dans la zone « **Filter Vulnerabilities** » (Filtrer les vulnérabilités), en haut à droite. Dès que vous commencez la saisie, Nessus commence immédiatement à filtrer les résultats sur la base de votre texte et de sa correspondance avec les titres des résultats. Le deuxième type de filtre est plus exhaustif et il vous permet de spécifier davantage de détails. Pour créer ce type de filtre, commencez par cliquer sur la flèche vers le bas placée à droite de la zone « **Filter Vulnerabilities** » (Filtrer les vulnérabilités). Des filtres peuvent être créés à partir de tout onglet de rapport. Plusieurs filtres peuvent être créés à partir d'une logique permettant un filtrage complexe. Un filtre est créé en sélectionnant l'attribut de plugin, un argument de filtre et une valeur de filtrage. Si vous sélectionnez plusieurs filtres, le mot-clé « Any » (N'importe lequel) ou « All » (Tous) doit être spécifié en conséquence. Si vous sélectionnez « All », seuls les résultats correspondant à **tous** les filtres sont affichés :

The screenshot shows the "Advanced Search" dialog box in Nessus. At the top, there is a search bar with the text "Filter Vulnerabilities" and a search icon. Below the search bar, the "Match" dropdown is set to "All". The dialog contains two filter criteria: "Risk Factor" is set to "is not equal to" and "None"; "CVSS Base Score" is set to "is more than" and "4.0". There are "Apply", "Cancel", and "Clear Filters" buttons at the bottom.

Une fois qu'un filtre a été défini, il peut être supprimé individuellement par un clic sur la croix (✖) à droite. Vous pouvez supprimer tous les filtres en même temps en sélectionnant « **Clear Filters** » (Supprimer les filtres). Les filtres du rapport proposent de nombreux critères pour le contrôle précis des résultats :

Option	Description
Plugin ID (ID du plugin)	Filtre les résultats si l'ID du plugin est égal à (« <i>is equal to</i> »), n'est pas égal à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple 42111).
Plugin Description (Description du plugin)	Filtre les résultats si la description du plugin contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « remote »).
Plugin Name (Nom du plugin)	Filtre les résultats si l'ID du plugin est égal à (« <i>is equal to</i> »), n'est pas égal à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « windows »).
Plugin Family (Famille de plugin)	Filtre les résultats si le nom du plugin est égal à (« <i>is equal to</i> ») ou n'est pas égal à (« <i>is not equal to</i> ») l'une des familles de plugins Nessus désignées. Les correspondances possibles sont fournies dans un menu déroulant.
Plugin Output (Sortie de plugin)	Filtre les résultats si la description du plugin est égale à (« <i>is equal to</i> »), n'est pas égale à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « PHP »).
Plugin Type (Type de plugin)	Filtre les résultats si le type du plugin est égal à (« <i>is equal to</i> ») ou n'est pas égal à (« <i>is not equal to</i> ») l'un des deux types de plugins : local ou à distance.
Solution (Solution)	Filtre les résultats si la solution du plugin contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « upgrade »).
Synopsis (Synopsis)	Filtre les résultats si la solution du plugin contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « PHP »).
Hostname (Nom d'hôte)	Filtre les résultats si l'hôte est égal à (« <i>is equal to</i> »), n'est pas égal à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « 192.168 » ou « lab »).
Port (Port)	Filtre les résultats si un port est égal à (« <i>is equal to</i> »), n'est pas égal à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « 80 »).
Protocol (Protocole)	Filtre les résultats si un protocole est égal à (« <i>is equal to</i> ») ou n'est pas égal à (« <i>is not equal to</i> ») une chaîne donnée (par exemple « http »).
CPE (CPE)	Filtre les résultats si le CPE (Common Platform Enumeration) est égal à (« <i>is equal to</i> »), n'est pas égal à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « solaris »).
CVSS Base Score (Note de base CVSS)	Filtre les résultats si une note de base CVSS (CVSS base score) est inférieure à (« <i>is less than</i> »), est supérieure à (« <i>is more than</i> »), est égale à (« <i>is equal to</i> »), n'est pas égale à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « 5 »).



Ce filtre peut être utilisé pour effectuer la sélection par niveau de risque. Le degré de gravité provient de la note CVSS associée, où 0 correspond à « Info », moins de 4 à « Bas », moins de 7 à « Moyen », moins de 10 à « Haut » et une note CVSS de 10 est signalée comme étant « Critique ».

CVSS Temporal Score (Note temporelle CVSS)	Filtre les résultats si une note temporelle CVSS (CVSS temporal score) est inférieure à (« <i>is less than</i> »), est supérieure à (« <i>is more than</i> »), est égale à (« <i>is equal to</i> »), n'est pas égale à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « 3.3 »).
CVSS Temporal Vector (Vecteur temporel CVSS)	Filtre les résultats si un vecteur temporel CVSS (CVSS temporal vector) est égal à (« <i>is equal to</i> »), n'est pas égal à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « E:F »).
CVSS Vector (Vecteur CVSS)	Filtre les résultats si un vecteur CVSS (CVSS vector) est égal à (« <i>is equal to</i> »), n'est pas égal à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « AV:N »).
Vulnerability Publication Date (Date de publication de la vulnérabilité)	Filtre les résultats si une date de publication de la vulnérabilité est antérieure à (« <i>earlier than</i> »), est postérieure à (« <i>later than</i> »), intervient le (« <i>on</i> »), n'intervient pas le (« <i>not on</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « 01/01/2012 »). Remarque : Cliquez sur le bouton  à côté de la date pour afficher une interface de calendrier qui facilitera la sélection de date.
Patch Publication Date (Date de publication du correctif)	Filtre les résultats si une date de publication de <u>correctif</u> de vulnérabilité est inférieure à (« <i>is less than</i> »), est supérieure à (« <i>is more than</i> »), est égale à (« <i>is equal to</i> »), n'est pas égale à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « 12/01/2011 »).
Plugin Publication Date (Date de publication de plugin)	Filtre les résultats si une date de publication de plugin Nessus est inférieure à (« <i>is less than</i> »), est supérieure à (« <i>is more than</i> »), est égale à (« <i>is equal to</i> »), n'est pas égale à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « 06/03/2011 »).
Plugin Modification Date (Date de modification de plugin)	Filtre les résultats si une date de modification de plugin Nessus est inférieure à (« <i>is less than</i> »), est supérieure à (« <i>is more than</i> »), est égale à (« <i>is equal to</i> »), n'est pas égale à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « 02/14/2010 »).
CVE (CVE)	Filtre les résultats si une référence CVE (CVE reference) est égale à (« <i>is equal to</i> »), n'est pas égale à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « 2011-0123 »).
Bugtraq ID (ID Bugtraq)	Filtre les résultats si un ID Bugtraq (Bugtraq ID) est égal à (« <i>is equal to</i> »), n'est pas égal à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « 51300 »).
CERT Advisory ID (ID consultatif CERT)	Filtre les résultats si un ID consultatif CERT (CERT Advisory ID), maintenant appelé Alerte de cyber-sécurité technique (Technical Cyber Security Alert), est égal à (« <i>is equal to</i> »), n'est pas égal à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « 51300 »).

	pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « TA12-010A »).
OSVDB ID (ID OSVDB)	Filtre les résultats si un ID OSVDB (Open Source Vulnerability Database) est égal à (« <i>is equal to</i> »), n'est pas égal à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « 78300 »).
Secunia ID (ID Secunia)	Filtre les résultats si un ID Secunia (Secunia ID) est égal à (« <i>is equal to</i> »), n'est pas égal à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « 47650 »).
Exploit Database ID (ID de base de données de failles)	Filtre les résultats si une référence EBD-ID (Exploit Database ID) est égale à (« <i>is equal to</i> »), n'est pas égale à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « 18380 »).
Metasploit Name (Nom Metasploit)	Filtre les résultats si un nom Metasploit (Metasploit name) est égal à (« <i>is equal to</i> »), n'est pas égal à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « xslt_password_reset »).
Exploit Hub (Hub de faille)	Filtre les résultats suivant qu'une faille ExploitHub a la valeur « <i>true</i> » (vrai) ou « <i>false</i> » (faux).
IAVA (IAVA)	Filtre les résultats si une référence IAVA est égale à (« <i>is equal to</i> »), n'est pas égale à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple 2012-A-0008).
IAVB (IAVB)	Filtre les résultats si une référence IAVB est égale à (« <i>is equal to</i> »), n'est pas égale à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple 2012-A-0008).
IAVT (IAVT)	Filtre les résultats si une référence IAVT est égale à (« <i>is equal to</i> »), n'est pas égale à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple 2012-A-0008).
See Also (Voir aussi)	Filtre les résultats si une référence « see also » (voir aussi) de plugin Nessus est égale à (« <i>is equal to</i> »), n'est pas égale à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « seclists.org »).
Exploits Available (Failles disponibles)	Filtre les résultats selon que la vulnérabilité a une faille publique connue.
Exploitability Ease (Niveau de faille)	Filtre les résultats selon que le niveau de faille est égal (« <i>is equal to</i> ») ou n'est pas égal (« <i>is not equal to</i> ») aux valeurs suivantes : « <i>Exploits are available</i> » (Failles disponibles), « <i>No exploit is required</i> » (Aucune faille requise) ou « <i>No known exploits are available</i> » (Aucune faille connue disponible).
Metasploit Exploit Framework (Cadre de faille Metasploit)	Filtre les résultats selon que la présence d'une vulnérabilité dans le Metasploit Exploit Framework est égale à (« <i>is equal to</i> ») ou n'est pas égale à (« <i>is not equal to</i> ») true (vrai) ou false (faux).
CANVAS Exploit Framework (Cadre de faille CANVAS)	Filtre les résultats selon que la présence d'une faille dans le CANVAS Exploit Framework est égale à (« <i>is equal to</i> ») ou n'est pas égale à (« <i>is not equal to</i> ») true (vrai) ou false (faux).
CANVAS Package (Progiciel CANVAS)	Filtre les résultats selon le CANVAS Exploit Framework Package pour lequel une faille est présente. Les options incluent CANVAS, D2ExploitPack ou White_Phosphorus.

CORE Exploit Framework (Cadre de faille CORE)	Filtre les résultats selon que la présence d'une faille dans le CORE Exploit Framework est égale à (« <i>is equal to</i> ») ou n'est pas égale à (« <i>is not equal to</i> ») true (vrai) ou false (faux).
Elliot Exploit Framework (Cadre de faille Elliot)	Filtre les résultats selon que la présence d'une faille dans le Elliot Exploit Framework est égale à (« <i>is equal to</i> ») ou n'est pas égale à (« <i>is not equal to</i> ») true (vrai) ou false (faux).
Elliot Exploit Name (Nom de faille Elliot)	Filtre les résultats si une faille Elliot est égale à (« <i>is equal to</i> »), n'est pas égale à (« <i>is not equal to</i> »), contient (« <i>contains</i> ») ou ne contient pas (« <i>does not contain</i> ») une chaîne donnée (par exemple « Typo3 FD »).
ExploitHub (Hub de faille)	Filtre les résultats selon que la présence d'une faille sur le site Web ExploitHub est égale à (« <i>is equal to</i> ») ou n'est pas égale à (« <i>is not equal to</i> ») true (vrai) ou false (faux).

Lorsqu'un filtre est utilisé, la chaîne ou la valeur numérique peut être délimitée par une virgule pour filtrer en fonction de chaînes multiples. Par exemple, pour filtrer les résultats afin d'afficher uniquement les serveurs Web, vous pouvez créer un filtre « Ports » (Ports), sélectionner « is equal to » (est égal à) et entrer « 80,443,8000,8080 ». Ceci affichera les résultats associés à ces quatre ports.



Les critères de filtre ne sont pas sensibles à la casse.

Si une option de filtre n'est pas disponible, cela signifie que le rapport ne contient aucun élément correspondant aux critères. Par exemple, si « Microsoft Bulletin » ne figure pas dans la liste déroulante de filtre, aucune vulnérabilité faisant référence à un Microsoft Bulletin n'a été trouvée.

Lorsqu'un filtre est créé, les résultats du scan sont mis à jour pour refléter les nouveaux critères de filtre après la sélection de « **Apply** » (Appliquer). La flèche vers le bas dans la zone « **Filter Vulnerabilities** » (Filtrer les vulnérabilités) est remplacée par une représentation numérique indiquant le nombre de filtres actuellement appliqués.

Une fois que les résultats ont été filtrés pour fournir l'ensemble de données souhaité, cliquez sur « **Export Results** » (Exporter les résultats) pour exporter uniquement les résultats filtrés. Pour recevoir un rapport répertoriant tous les résultats, supprimez tous les filtres et utilisez la fonction d'exportation.

Les résultats de scan de Nessus proposent une liste concise des plugins qui ont détecté des problèmes sur l'hôte. Cependant, il peut arriver que vous souhaitiez savoir pourquoi un plugin **n'a pas** renvoyé de résultats. La fonctionnalité « **Audit Trail** » (Piste d'audit) fournira cette information. Commencez par cliquer sur « Audit Trail » (Piste d'audit) en haut à droite :

Home Network Export ▼ Audit Trail

Hosts > 192.168.0.100 > Vulnerabilities 24 Hide Details

HIGH
Apache 2.0 < 2.0.65 Multiple Vulnerabilities
< >

Description

According to its banner, the version of Apache 2.0 installed on the remote host is older than 2.0.65. Such versions may be affected by several vulnerabilities :

- A flaw exists in the byte-range filter, making it vulnerable to denial of service. (CVE-2011-3192)
- A flaw exists in 'mod_proxy' where it doesn't properly interact with 'RewriteRule' and 'ProxyPassMatch' in reverse proxy configurations. (CVE-2011-3368)
- A privilege escalation vulnerability exists relating to a heap-based buffer overflow in 'ap_pregsub' function in 'mod_setenvif' module via .htaccess file. (CVE-2011-3607)
- A local security bypass vulnerability exists within scoreboard shared memory that may allow the child process to cause the parent process to crash. (CVE-2012-0031)

Plugin Details

Severity: High
ID: 68914
Version: \$Revision: 1.4 \$
Type: remote
Family: Web Servers
Published: 2013/07/16
Modified: 2013/11/14

Risk Information

Risk Factor: High
CVSS Base Score: 7.8
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:N/E:N/A:C
CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C
CVSS Temporal Score: 6.4

La boîte de dialogue Audit Trail (Piste d'audit) s'affiche. Commencez par saisir l'ID de plugin sur lequel vous voulez obtenir des informations. Cliquez sur « **Submit** » (Soumettre) pour afficher un hôte ou une liste d'hôtes relatifs à votre interrogation. Vous pouvez, si vous le souhaitez, fournir un IP hôte pour l'interrogation initiale afin de limiter les résultats à une cible d'intérêt. Une fois le ou les hôtes affichés, cliquez sur celui de votre choix pour afficher des informations indiquant pourquoi le plugin ne s'est pas déclenché :

DMZ Web Server / Audit Trail

Plugin ID

Host

▼ 192.168.0.100 0

Apache 2.0.64 is listening on port 2 and is not affected.

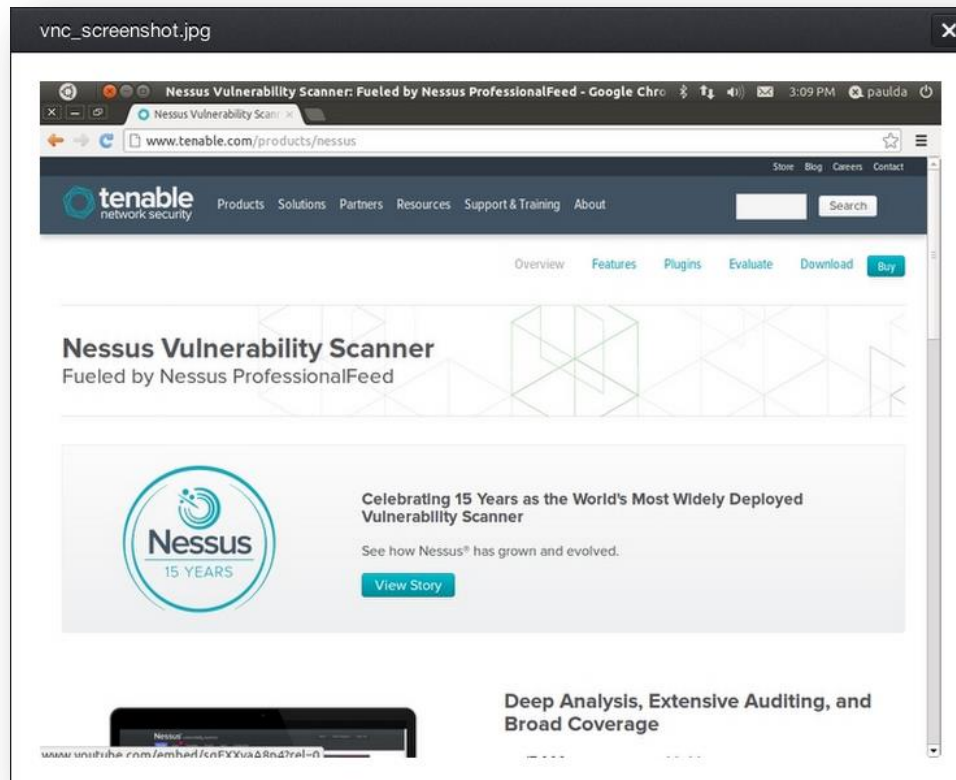


En raison des ressources requises pour la piste d'audit, il peut arriver que seule une piste d'audit non exhaustive soit fournie. Si vous scannez un seul hôte, la piste d'audit complète est disponible. Si vous scannez entre 2 et 512 hôtes, une piste d'audit complète est disponible uniquement si le serveur Nessus est doté de plus d'1 UC et de 2 Go de RAM. Si vous scannez plus de 512 hôtes, vous obtenez toujours une piste d'audit non exhaustive.

La piste d'audit est uniquement disponible pour les scans provenant de l'hôte. Elle ne s'applique pas aux scans importés.

Captures d'écran de rapport

Nessus 5.2 peut également prendre des captures d'écran pendant un scan des vulnérabilités et les inclure dans un rapport. Par exemple, si Nessus découvre qu'un VNC est exécuté sans restriction d'accès par mot de passe, une capture d'écran sera prise pour afficher la session et incluse dans le rapport. Dans l'exemple ci-dessous, un VNC a été découvert alors que l'utilisateur naviguait dans le site Web de Tenable :



Cette fonction doit être activée dans la section « **Préférences** » (Préférences) d'une stratégie de scan, sous « **Remote web server screenshot** » (Capture d'écran de serveur Web distant). Voir la section [Scanning Preferences in Detail](#) (Détails des préférences de scan) de ce document pour plus d'informations.

Scan Knowledge Base (Base de connaissances de scan)

Une base de connaissances (Knowledge Base - KB) est enregistrée avec chaque scan effectué. Il s'agit d'un fichier texte ASCII contenant un journal d'informations relatif au scan effectué et aux résultats trouvés. Une KB est souvent utile lorsque vous avez besoin du support de Tenable, car elle permet aux représentants du support technique de comprendre exactement les actions de Nessus et les informations trouvées.

Pour télécharger une KB, sélectionnez un rapport puis un hôte spécifique. À droite de l'IP ou du nom d'hôte se trouve le lien « **Host Details** » (Détails de l'hôte). Cliquez sur ce lien ; l'un des détails de l'hôte est « **KB** » avec un lien « **Download** » (Télécharger) :

Host Details

IP: 192.168.0.1

MAC: 00:24:7b:b9:2b:4c

OS: Linux Kernel 2.4
Linux Kernel 2.6

Start time: Tue Nov 26 20:00:25 2013

End time: Tue Nov 26 20:19:25 2013

KB: [Download](#)



Seuls les scans effectués sur l'hôte auront une KB associée. Les scans importés ne sont pas dotés d'une KB.

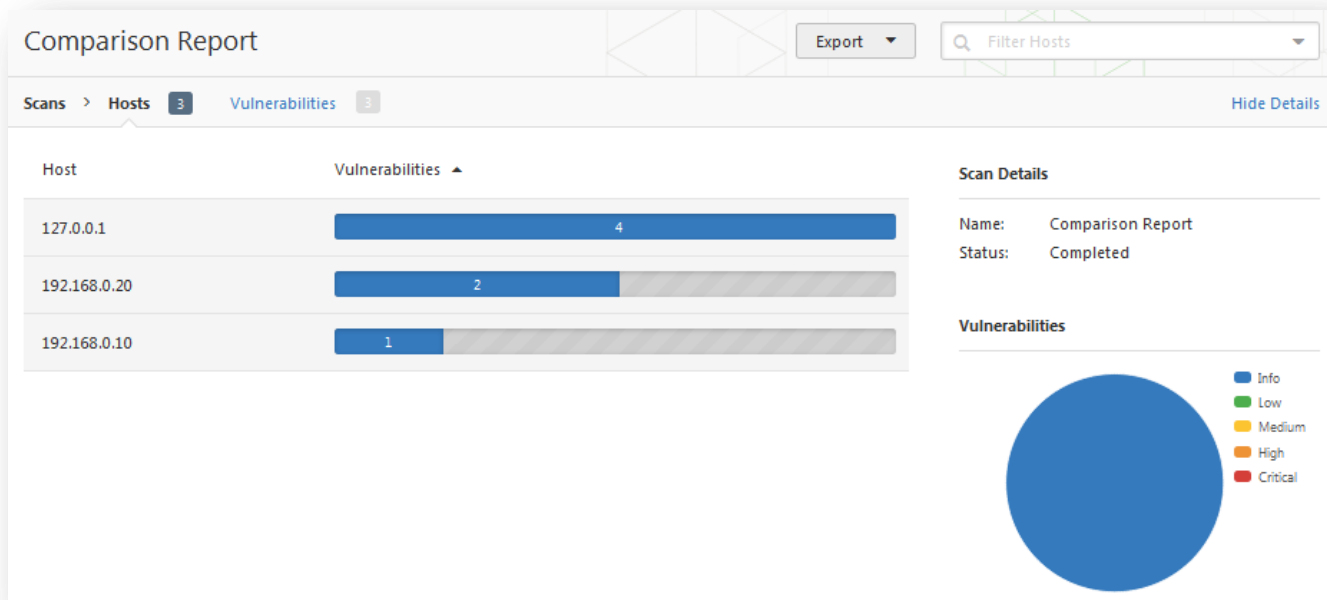
Comparer (Diff Results)

Avec Nessus, vous pouvez comparer deux rapports de scan pour afficher toutes les différences. La capacité d'affichage des différences de scan permet de signaler comment un système ou un réseau donné change en fonction du temps. Ceci aide à analyser la conformité en montrant comment les vulnérabilités sont corrigées, si les systèmes sont sujets à des correctifs à mesure que de nouvelles vulnérabilités sont découvertes, ou comment deux scans peuvent ne pas cibler les mêmes hôtes.

Pour comparer les rapports, commencez par sélectionner deux scans dans la liste « **Scans** » (Scans), cliquez sur « **More** » (Plus) et sélectionnez « **Diff** » (Comparaison) dans le menu déroulant :

Name	Updated	Status
<input checked="" type="checkbox"/> Home Network	January 04, 2014 21:01:51	Completed
<input type="checkbox"/> mdm scan	December 11, 2013 19:31:06	Imported
<input type="checkbox"/> Comp x3	December 11, 2013 14:09:58	Imported
<input type="checkbox"/> POL_Windows_2003_Domain_Contr...	December 11, 2013 14:06:59	Imported
<input checked="" type="checkbox"/> Home Network	November 26, 2013 20:00:25	Completed

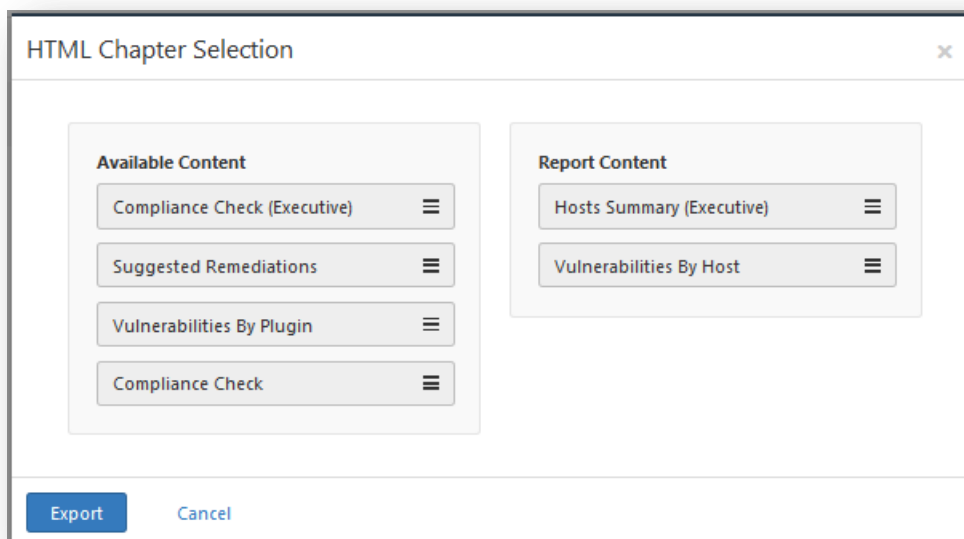
Nessus comparera le premier rapport sélectionné au deuxième, et générera une liste de résultats différents par rapport au premier. La fonction de comparaison montre les nouveautés par rapport à la base (le premier rapport sélectionné), sans produire un rapport de différences entre deux rapports quelconques. Cette comparaison souligne les vulnérabilités qui ont été détectées ou corrigées entre les deux scans. Dans l'exemple ci-dessus, « DMZ Web Server » (Serveur Web DMZ) est un scan non authentifié d'un seul serveur Web, effectué plusieurs fois. Les résultats affichent les différences, soulignant les vulnérabilités qui n'ont pas été trouvées dans le scan du 7 octobre :



Téléchargement en amont et exportation

Les résultats du scan peuvent être exportés depuis un scanner Nessus et importés sur un autre scanner Nessus. Les fonctions « **Upload** » (Téléchargement en amont) et « **Export** » (Exporter) améliorent la gestion du scan, la comparaison des rapports, la sauvegarde des rapports et la communication entre les groupes ou les organismes d'une entreprise.

Pour exporter un scan, commencez par sélectionner le rapport dans l'écran « **Scans** » (Scans), cliquez sur le menu déroulant « **Export** » (Exporter) en haut et choisissez le format voulu. Cette opération affiche une fenêtre qui vous permet de spécifier les informations (réparties en « chapitres ») à inclure. Le contenu disponible est indiqué à gauche et le contenu qui sera exporté à droite. Vous pouvez faire glisser le contenu d'un côté à l'autre pour créer l'exportation personnalisée :





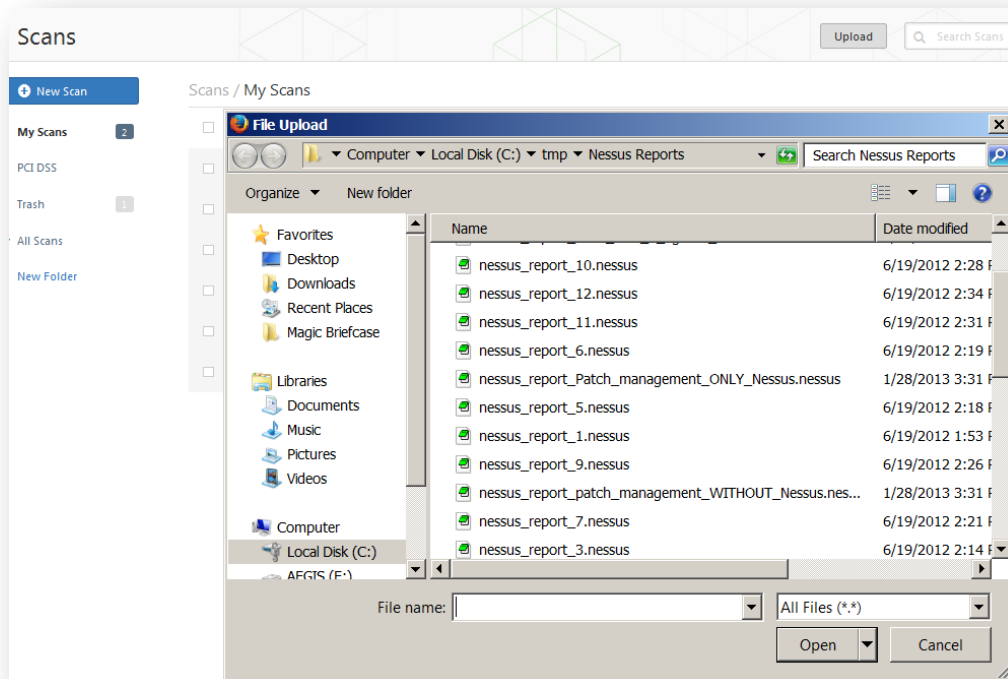
Seuls les scans de conformité effectués avec Nessus 5 peuvent être exportés aux formats PDF ou HTML avec les chapitres de conformité. Les scans importés des versions précédentes de Nessus ne seront pas exportés selon cette procédure.

Les rapports peuvent être téléchargés en plusieurs formats. Veuillez noter que certains formats n'autorisent pas la sélection de chapitres et incluent toutes les informations.

Option	Description
<code>.nessus</code>	Format basé sur XML et la norme de facto dans Nessus 4.2 et les versions ultérieures. Ce format utilise de nombreuses balises XML pour améliorer la précision de l'extraction et du transfert d'informations. Ce rapport n'autorise pas la sélection de chapitres.
<code>.nessus (v1)</code>	Format basé sur XML et utilisé dans les versions Nessus 3.2 à 4.0.2, compatible avec Nessus 4.x et SecurityCenter 3. Ce rapport n'autorise pas la sélection de chapitres.
HTML	Rapport généré au format HTML standard qui autorise la sélection de chapitres. Ce rapport s'ouvre dans un nouvel onglet dans votre navigateur.
PDF	Rapport généré au format PDF qui autorise la sélection de chapitres. Suivant la taille du rapport, la génération du PDF peut prendre plusieurs minutes. <div data-bbox="516 940 594 1010" data-label="Image"></div> <p>Oracle Java (auparavant l'application Java de Sun Microsystems) est requis pour la fonction de rapport PDF.</p>
CSV	Exportation de type CSV (valeurs séparées par des virgules) qui permet d'importer des données dans différents programmes externes comme les bases de données ou les feuilles de calcul. Ce rapport n'autorise pas la sélection de chapitres.

Une fois le format voulu sélectionné, la boîte de dialogue « **Save File** » (Enregistrer le fichier) du navigateur Web standard s'ouvre, permettant d'enregistrer les résultats du scan à l'emplacement choisi.

Pour importer un rapport, cliquez sur le bouton « **Upload** » (Télécharger en amont) dans la barre supérieure de l'écran « **Scans** » (Scans) pour ouvrir une fenêtre de navigation de fichiers :



Sélectionnez le fichier de scan **.nessus** que vous souhaitez importer et cliquez sur « **Open** » (Ouvrir). Nessus analyse les informations et les met à votre disposition dans l'interface « **Scans** ».

Format de fichier **.nessus**

Nessus utilise un format de fichier particulier (**.nessus**) pour l'exportation et l'importation des scans. Ce format présente les avantages suivants :

- Basé sur XML pour faciliter la compatibilité en aval et en amont et la mise en place.
- Autonome : un seul fichier **.nessus** contient la liste des cibles, les stratégies définies par l'utilisateur ainsi que les résultats des scans eux-mêmes.
- Sécurisé : les mots de passe ne sont pas sauvegardés dans le fichier. À la place, une référence à un mot de passe mémorisé dans un emplacement sûr de l'hôte local est utilisée.

La méthode de création d'un fichier **.nessus** qui contient les cibles, les stratégies et les résultats de scan consiste d'abord à créer la stratégie et à l'enregistrer. Ensuite, créez la liste des adresses cibles et, pour finir, exécutez un scan. Une fois que le scan est terminé, toutes les informations peuvent être enregistrées dans un fichier **.nessus** en utilisant l'option « **Export** » (Exporter) des résultats de « **Scans** ». Voir le document « [Nessus v2 File Format](#) » (Format de fichier Nessus v2) pour plus d'informations sur les fichiers **.nessus**.

Suppression

Une fois que vous avez fini de traiter les résultats du scan, vous pouvez cliquer sur le « X » à droite du scan dans l'onglet « Scans » :

<input type="checkbox"/>	DMZ Web Server	October 07, 2013 19:34:48	✔ Completed	✕
<input type="checkbox"/>	Gateway Internal Scan	October 03, 2013 19:19:22	⊕ Imported	✕
<input type="checkbox"/>	Lab, unauthenticated	October 02, 2013 21:34:54	✔ Completed	✕



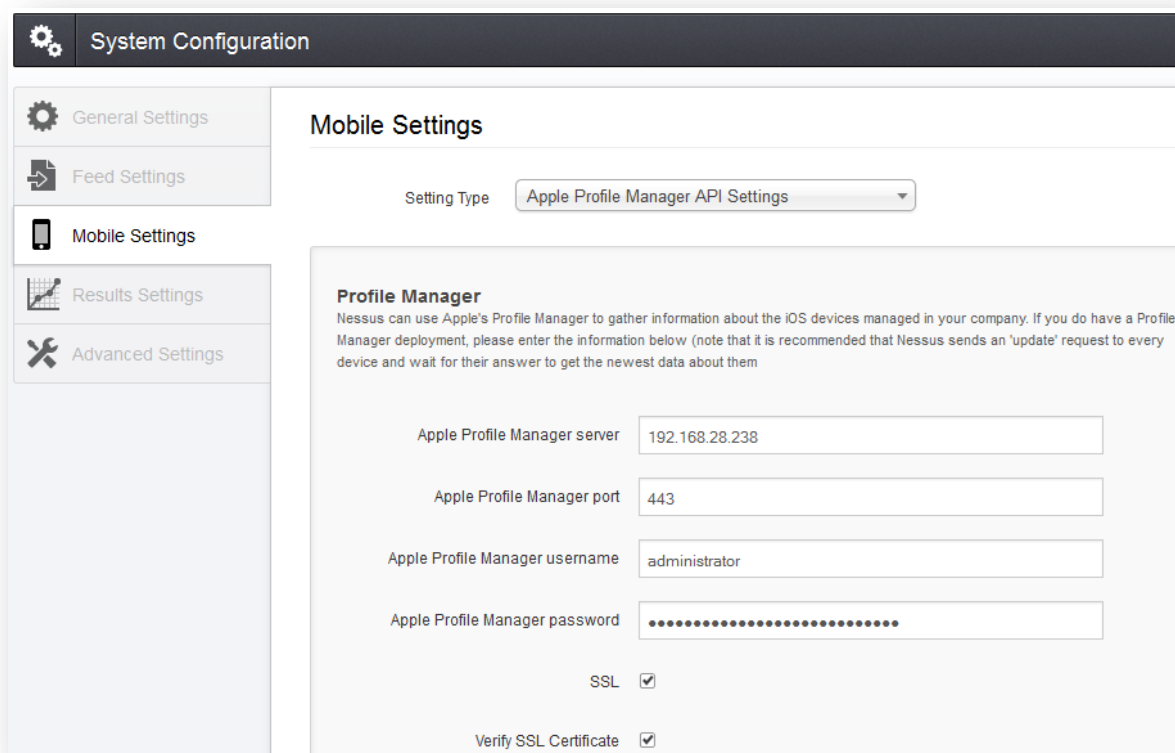
Cette action ne peut pas être annulée ! Utilisez la fonction « **Export** » (Exporter) pour exporter les résultats du scan avant la suppression.

Mobile

Nessus 5 peut scanner les interfaces ADSI ([Active Directory Service Interfaces](#)) et le Gestionnaire de profil Apple ([Apple Profile Manager](#)). Les inventaires et les vulnérabilités peuvent ainsi être scannés sur les périphériques Apple iOS et Android. Nessus peut être configuré pour effectuer l'authentification sur ces serveurs, demander les informations relatives aux périphériques mobiles et signaler les problèmes.

Pour scanner les périphériques mobiles, Nessus doit être configuré à l'aide des informations d'authentification relatives au(x) serveur(s) de gestion.

La fonctionnalité de scan Mobile est spécifiée dans le menu « **Configuration** » (Configuration). L'onglet « **Mobile Settings** » (Paramètres mobiles) permet de configurer dans la même section le Gestionnaire de profil Apple et les informations ADSI. Puisque Nessus effectue directement l'authentification sur les serveurs de gestion, une stratégie de scan mobile sera automatiquement créée par l'activation de la seule famille de plugins Mobile et un scan Mobile sera créé sous « **Templates** » (Modèles). Ce modèle de scan permet de scanner les périphériques mobiles aussi souvent que nécessaire.



SecurityCenter

Configuration de SecurityCenter pour l'utilisation avec Nessus

L'interface d'administration SecurityCenter est utilisée pour configurer l'accès et contrôler tout scanner Nessus de version 4.2.x ou supérieure. Cliquez sur l'onglet « **Resources** » (Ressources), puis sur « **Nessus Scanners** » (Scanners Nessus). Cliquez sur « **Add** » (Ajouter) pour ouvrir la boîte de dialogue « **Add Scanner** » (Ajouter un scanner). L'adresse IP ou le nom d'hôte du scanner Nessus, le port Nessus (8834 par défaut), le type d'authentification (créé lors de la configuration de Nessus), l'ID de connexion et le mot de passe administratifs ou les informations de certificat sont requis. Les champs de mot de passe ne sont pas disponibles si l'authentification « **SSL Certificate** » (Certificat SSL) est sélectionnée. La capacité de vérification du nom d'hôte est fournie afin de vérifier le CN (CommonName- Nom commun) du certificat SSL présenté par le serveur Nessus. L'état du scanner Nessus peut être défini, le cas échéant, sur Enabled (Activé) ou Disabled (Désactivé). Vous pouvez sélectionner l'utilisation d'un proxy et les zones (Scan Zones) auxquelles le scanner Nessus peut être affecté.

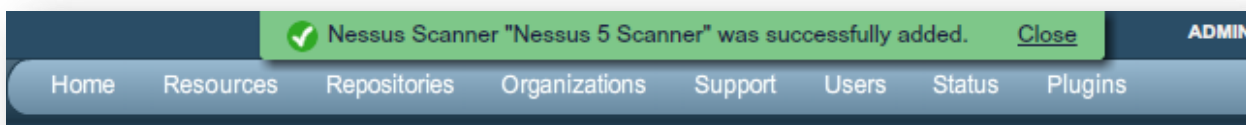
Voici un exemple de capture d'écran de la page « **Add Scanner** » (Ajouter un scanner) de SecurityCenter 4.7 :

The screenshot shows the 'Add Scanner' configuration interface. It includes the following fields and options:

- Name:** Local Scanner
- Description:** Local SecurityCenter Scanner
- Scanner:**
 - Host: 127.0.0.1
 - Port: 8834
 - State: Enabled Disabled
 - Verify Hostname:
 - Use Proxy:
- Authentication:**
 - Authentication Type: Password
 - Username: nessusadmin
 - Password: [masked]
- Zones:**
 - Target Zone: Web Farm Zone, Database Servers

Buttons: Cancel, Submit

Une fois le scanner ajouté, la bannière suivante s'affiche :



Pour plus d'informations sur l'intégration de Nessus et de SecurityCenter, consultez le « SecurityCenter Administration Guide » (Guide d'administration de SecurityCenter), disponible sur le [Tenable Support Portal](#) (Portail d'assistance de Tenable).

Pare-feu de l'hôte

Si le serveur Nessus est configuré avec un pare-feu local tel que ZoneAlarm, BlackICE, le pare-feu Windows XP ou tout autre logiciel pare-feu, les connexions doivent être ouvertes à partir de l'adresse IP de SecurityCenter.

Par défaut, le port 8834 est utilisé pour communiquer avec SecurityCenter. Sur les systèmes Microsoft XP Service Pack 2 et les versions ultérieures, vous pouvez cliquer sur l'icône « **Security Center** » (Centre de sécurité) du « **Control Panel** » (Panneau de configuration) pour pouvoir gérer les paramètres du pare-feu Windows. Pour ouvrir le port 8834, choisissez l'onglet « **Exceptions** » (Exceptions) puis ajoutez le port « 8834 » à la liste.

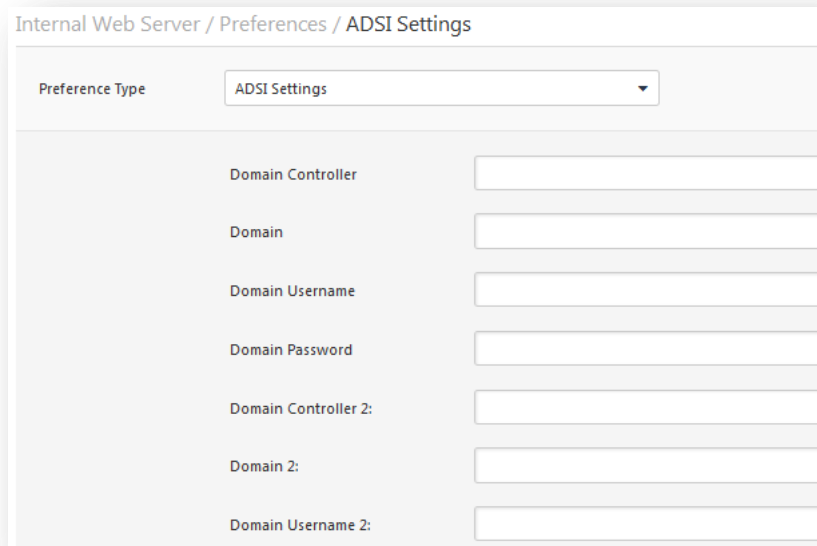
Détails des préférences de scan

L'onglet « **Préférences** » (Préférences) placé sous « **Policies** » (Stratégies) propose une quarantaine de menus déroulants qui permettent un contrôle plus précis sur les paramètres de scan. Prenez le temps d'explorer et de configurer chaque menu afin de bénéficier d'une plus grande flexibilité et d'accroître considérablement la précision des résultats du scan par rapport à une stratégie par défaut. La section qui suit fournit des détails complets sur chaque option de « **Préférences** » (Préférences). Il s'agit d'une liste dynamique d'options de configuration qui dépend de la version de Nessus, des stratégies d'audit et des fonctionnalités supplémentaires auxquelles le scanner Nessus connecté a accès. Un scanner commercial peut avoir des options de configuration plus avancées qu'un scanner Nessus Home. Cette liste peut aussi changer à mesure que des plugins sont ajoutés ou modifiés.

ADSI Settings (Paramètres ADSI)

Le menu « **ADSI Settings** » (Paramètres ADSI) autorise Nessus à interroger un serveur ActiveSync afin de déterminer si des périphériques Android ou iOS sont connectés. À partir des identifiants et des informations sur les serveurs, Nessus est authentifié auprès du contrôleur de domaine (et non du serveur Exchange) pour lui demander directement des informations sur les périphériques. Cette fonction n'exige pas que des ports soient spécifiés dans la stratégie de scan. Ces paramètres sont requis pour le scan des périphériques mobiles. Nessus collectera des informations à partir de tout téléphone mis à jour par ADSI au cours des 365 derniers jours.

Remarque : Pour « **ADSI Settings** » (Paramètres ADSI), « **Apple Profile Manager API Settings** » (Paramètres d'API de gestionnaire de profil Apple) et « **Good MDM Settings** » (Paramètres Good MDM), il n'est pas nécessaire de scanner directement les périphériques hôte afin d'obtenir des informations à leur sujet. Le scanner Nessus doit pouvoir joindre le serveur MDM (mobile device management - gestion de périphérique mobile) pour lui demander des informations. Lorsque l'une de ces options est configurée, la stratégie de scan n'exige pas un hôte cible à scanner ; vous pouvez cibler « localhost » et la stratégie demandera toujours des informations au serveur MDM.



Preference Type	Value
ADSI Settings	
Domain Controller	<input type="text"/>
Domain	<input type="text"/>
Domain Username	<input type="text"/>
Domain Password	<input type="text"/>
Domain Controller 2:	<input type="text"/>
Domain 2:	<input type="text"/>
Domain Username 2:	<input type="text"/>

Apple Profile Manager API Settings (Paramètres d'API de gestionnaire de profil Apple)

Le menu « **Apple Profile Manager API Settings** » (Paramètres d'API de gestionnaire de profil Apple) permet à Nessus d'interroger un serveur Gestionnaire de profil Apple pour énumérer les périphériques Apple iOS (par exemple, iPhone, iPad) sur le réseau. À partir des identifiants et des informations sur les serveurs, Nessus est authentifié auprès du Gestionnaire de profil pour lui demander directement des informations sur les périphériques. Il est également possible de spécifier des communications via SSL ou d'indiquer au serveur de forcer la mise à jour des informations sur les périphériques (chaque périphérique actualisera alors ses informations sur la base du serveur Profile Manager (Gestionnaire de profil)).

Cette fonction n'exige pas que des ports soient spécifiés dans la stratégie de scan. Ces paramètres sont requis pour le scan des périphériques mobiles.

The screenshot shows a configuration window titled "Internal Web Server / Preferences / Apple Profile Manager API Settings". At the top, there is a "Preference Type" dropdown menu set to "Apple Profile Manager API Settings". Below this, several fields are listed:

- Apple Profile Manager server: [Empty text box]
- Apple Profile Manager port: [443]
- Apple Profile Manager username: [Empty text box]
- Apple Profile Manager password: [Empty text box]
- SSL:
- Verify SSL Certificate:
- Force Device Updates:
- Device Update Timeout (Minutes): [5]

At the bottom of the window, there are two buttons: "Save" and "Cancel".

Check Point GAiA Compliance Checks (Contrôles de conformité Check Point GAiA)

Le menu « **Check Point GAiA Compliance Checks** » (Contrôles de conformité Check Point GAiA) permet aux clients commerciaux de télécharger en amont des fichiers de stratégie qui seront utilisés pour déterminer si un système Check Point GAiA testé satisfait aux normes de conformité spécifiées. Jusqu'à cinq stratégies peuvent être sélectionnées à la fois.

The screenshot shows a configuration window titled "Internal Web Server / Preferences / Check Point GAiA Compliance Checks". At the top, there is a "Preference Type" dropdown menu set to "Check Point GAiA Compliance Checks". Below this, there is a list of five policy files, each with an "Add File" button next to it:

- Policy file #1: Add File
- Policy file #2: Add File
- Policy file #3: Add File
- Policy file #4: Add File
- Policy file #5: Add File

At the bottom of the window, there are two buttons: "Save" and "Cancel".

Cisco IOS Compliance Checks (Contrôles de conformité Cisco IOS)

Le menu « **Cisco IOS Compliance Checks** » (Contrôles de conformité Cisco IOS) permet aux clients commerciaux de télécharger en amont des fichiers de stratégie qui seront utilisés pour déterminer si un système Cisco IOS testé satisfait aux normes de conformité spécifiées. Jusqu'à cinq stratégies peuvent être sélectionnées à la fois. Les stratégies peuvent être exécutées avec les configurations Saved (**show config**) [Enregistrées], Running (**show running**) [En cours d'exécution] ou Startup (**show startup**) [Démarrage].

The screenshot shows a web-based configuration window titled "Internal Web Server / Preferences / Cisco IOS Compliance Checks". At the top, there is a "Preference Type" dropdown menu set to "Cisco IOS Compliance Checks". Below this, there is a section for "IOS Config File To Audit" with a dropdown menu set to "Saved/(show config)". Underneath, there are five rows, each labeled "Policy file #1" through "Policy file #5", with an "Add File" link next to each. At the bottom of the window, there are "Save" and "Cancel" buttons.

Citrix XenServer Compliance Checks (Contrôles de conformité Citrix XenServer)

Le menu « **Citrix XenServer Compliance Checks** » (Contrôles de conformité Citrix XenServer) permet aux clients commerciaux de télécharger en amont les fichiers de stratégie qui seront utilisés pour déterminer si un système Citrix XenServer testé satisfait aux normes de conformité spécifiées. Jusqu'à cinq stratégies peuvent être sélectionnées à la fois.

New Advanced Policy / Preferences / Citrix XenServer Compliance Checks

Preference Type:

Policy file #1	Add File
Policy file #2	Add File
Policy file #3	Add File
Policy file #4	Add File
Policy file #5	Add File

Database Compliance Checks (Contrôles de conformité des bases de données)

Le menu « **Database Compliance Checks** » (Contrôles de conformité des bases de données) permet aux clients commerciaux de télécharger en amont des fichiers de stratégie qui seront utilisés pour déterminer si une base de données testée satisfait aux normes de conformité spécifiées. Jusqu'à cinq stratégies peuvent être sélectionnées à la fois.

Internal Web Server / Preferences / Database Compliance Checks

Preference Type:

Policy file #1	Add File
Policy file #2	Add File
Policy file #3	Add File
Policy file #4	Add File
Policy file #5	Add File

Database settings (Paramètres de base de données)

Les options « **Database settings** » (Paramètres de base de données) sont utilisées pour spécifier le type de base de données à tester, les paramètres et les identifiants pertinents :

Option	Description
Login (Connexion)	Nom d'utilisateur pour la base de données.
Password (Mot de passe)	Mot de passe correspondant au nom d'utilisateur fourni.
DB Type (Type DB)	Oracle, SQL Server, MySQL, DB2, Informix/DRDA et PostgreSQL sont pris en charge.
Database SID (ID de système de la base de données)	ID de la base de données à vérifier.
Database port to use (Port de base de données à utiliser)	Port auquel la base de données est connectée.
Oracle auth type (Type d'auth. Oracle)	NORMAL, SYSOPER et SYSDBA sont pris en charge.
SQL Server auth type (Type d'auth. de serveur SQL)	Windows ou SQL sont pris en charge.

Internal Web Server / Preferences / Database settings

Preference Type: Database settings

Login:

Password:

DB Type: Oracle

Database SID:

Database port to use:

Oracle auth type: NORMAL

SQL Server auth type: Windows

Save Cancel

Do not scan fragile devices (Ne pas scanner les périphériques fragiles)

Le menu « **Do not scan fragile devices** » (Ne pas scanner les périphériques fragiles) propose deux options qui indiquent au scanner Nessus de ne pas scanner les hôtes qui ont un historique de fragilité ou qui risquent de tomber en panne

lorsqu'ils reçoivent des données inattendues. Les utilisateurs peuvent sélectionner « **Scan Network Printers** » (Scanner les imprimantes réseau) ou « **Scan Novell Netware hosts** » (Scanner les hôtes Novell Netware) pour indiquer à Nessus de scanner ces périphériques spécifiques. Nessus scanne ces périphériques uniquement si ces options sont cochées. Il est recommandé d'effectuer le scanning de ces périphériques d'une manière permettant au personnel informatique de surveiller l'apparition de problèmes sur ces systèmes.

Internal Web Server / Preferences / Do not scan fragile devices

Preference Type: Do not scan fragile devices

Scan Network Printers	<input type="checkbox"/>
Scan Novell Netware hosts	<input type="checkbox"/>

Save Cancel

FireEye Compliance Checks (Contrôles de conformité FireEye)

Le menu « **FireEye Compliance Checks** » (Contrôles de conformité FireEye) permet aux clients commerciaux de télécharger en amont des fichiers de stratégie qui seront utilisés pour déterminer si un périphérique FireEye testé satisfait aux normes de conformité spécifiées. Jusqu'à cinq stratégies peuvent être sélectionnées à la fois.

New Advanced Policy / Preferences / FireEye Compliance Checks

Preference Type: FireEye Compliance Checks

Policy file #1	Add File
Policy file #2	Add File
Policy file #3	Add File
Policy file #4	Add File
Policy file #5	Add File

Save Cancel

Global variable settings (Paramètres des variables globales)

Le menu « **Global variable settings** » (Paramètres des variables globales) contient de nombreuses options de configuration pour le serveur Nessus.

Internal Web Server / Preferences / Global variable settings

Preference Type: Global variable settings

Probe services on every port

Do not log in with user accounts not specified in the policy

Enable CGI scanning

Network type: Mixed (use RFC 1918)

Enable experimental scripts

Thorough tests (slow)

Report verbosity: Normal

Report paranoia: Normal

HTTP User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5

SSL certificate to use: Add File

SSL CA to trust: Add File

SSL key to use: Add File

SSL password for SSL key:

Save Cancel

Le tableau suivant fournit des informations plus détaillées sur chaque option disponible :

Option	Description
Probe services on every port (Sonder les services sur chaque port)	Essaie de mapper chaque port ouvert avec le service qui est exécuté sur ce port. Dans de rares cas, ceci pourrait perturber certains services et causer des effets secondaires imprévus.
Do not log in with user accounts not specified in the policy (Ne se connecter avec des comptes d'utilisateur non spécifiés dans la stratégie)	Sert à empêcher les blocages de compte si la stratégie de mot de passe est configurée de façon à bloquer les comptes après plusieurs tentatives non valides.

Enable CGI scan (Activer le scan CGI)	Active les contrôles CGI. La désactivation de cette option accélérera considérablement l'audit d'un réseau local.
Network type (Type de réseau)	Permet de spécifier si vous utilisez des IP routables en mode public, des IP privés non routables sur Internet ou un mélange des deux. Sélectionnez « Mixed » (Mixte) si vous utilisez des adresses RFC 1918 et si vous disposez de plusieurs routeurs sur le réseau.
Enable experimental scripts (Activer les scripts expérimentaux)	Permet d'utiliser dans le scan des plugins qui sont considérés comme expérimentaux. N'activez pas ce paramètre pour le scan d'un réseau de production.
Thorough tests (slow) (Tests approfondis (lents))	Fait « travailler de façon plus intense » divers plugins. Par exemple, lors de l'examen des partages de fichier SMB, un plugin peut analyser sur une profondeur de 3 niveaux au lieu d'un seul. Cette situation risque dans certains cas d'intensifier l'analyse et le trafic réseau. Avec ce contrôle plus approfondi, le scan sera toutefois plus intrusif et il risque davantage de perturber le réseau, tout en fournissant potentiellement de meilleurs résultats d'audit.
Report verbosity (Niveau de détail du rapport)	Un paramètre plus élevé fournira plus d'informations concernant l'activité des plugins dans le rapport.
Report paranoia (Paranoïa du rapport)	Dans certains cas, Nessus ne peut pas déterminer à distance la présence d'un défaut. Si vous affectez la valeur « Paranoid » (Paranoïde) à ce paramètre, un défaut sera signalé à chaque fois, même lorsqu'il existe un doute concernant les effets sur l'hôte distant. À l'inverse, la valeur « Avoid false alarm » (Éviter les fausses alarmes) indiquera à Nessus de ne pas signaler les défauts lorsque les effets sur l'hôte distant sont incertains. L'option par défaut (« Normal ») est une option intermédiaire entre ces deux paramètres.
HTTP User-Agent (Utilisateur-agent HTTP)	Spécifie le type de navigateur Internet que Nessus imitera pendant le scan.
SSL certificate to use (Certificat SSL à utiliser)	Permet à Nessus d'utiliser un certificat SSL client pour communiquer avec un hôte distant.
SSL CA to trust (CA SSL à laquelle se fier)	Spécifie une CA (Certificate Authority, autorité de certificat) à laquelle Nessus fera confiance.
SSL key to use (Clé SSL à utiliser)	Spécifie une clé SSL locale à utiliser pour communiquer avec l'hôte distant.
SSL password for SSL key (Mot de passe SSL pour clé SSL)	Mot de passe utilisé pour gérer la clé SSL spécifiée.

Good MDM Settings (Paramètres Good MDM)

Le menu « **Good MDM Settings** » (Paramètres Good MDM) autorise Nessus à interroger un serveur de gestion de périphériques Good mobile afin de déterminer si des périphériques Android ou iOS sont connectés. À partir des identifiants et des informations sur les serveurs, Nessus est authentifié auprès du serveur GMC pour lui demander directement des informations sur les périphériques. Cette fonction n'exige pas que des ports soient spécifiés dans la stratégie de scan. Ces paramètres sont requis pour le scan des périphériques mobiles.

Remarque : Pour « **ADSI Settings** » (Paramètres ADSI), « **Apple Profile Manager API Settings** » (Paramètres d'API de gestionnaire de profil Apple) et « **Good MDM Settings** » (Paramètres Good MDM), il n'est pas nécessaire de scanner directement les périphériques hôte afin d'obtenir des informations à leur sujet. Le scanner Nessus doit pouvoir joindre le serveur MDM (Mobile Device Management - gestion de périphérique mobile) pour lui demander des informations. Lorsque l'une de ces options est configurée, la stratégie de scan n'exige pas un hôte cible à scanner ; vous pouvez cibler « localhost » et la stratégie demandera toujours des informations au serveur MDM.

Internal Web Server / Preferences / Good MDM Settings

Preference Type: Good MDM Settings

GMC Server	<input type="text"/>
Port	<input type="text"/>
Domain	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
SSL	<input checked="" type="checkbox"/>
Verify SSL Certificate	<input type="checkbox"/>

Save Cancel

HP ProCurve Compliance Checks (Contrôles de conformité HP ProCurve)

Le menu « **HP ProCurve Compliance Checks** » (Contrôles de conformité HP ProCurve) permet aux clients commerciaux de télécharger en amont des fichiers de stratégie qui seront utilisés pour déterminer si un périphérique HP ProCurve testé satisfait aux normes de conformité spécifiées. Jusqu'à cinq stratégies peuvent être sélectionnées à la fois.

New Advanced Policy / Preferences / HP ProCurve Compliance Checks

Preference Type: HP ProCurve Compliance Checks

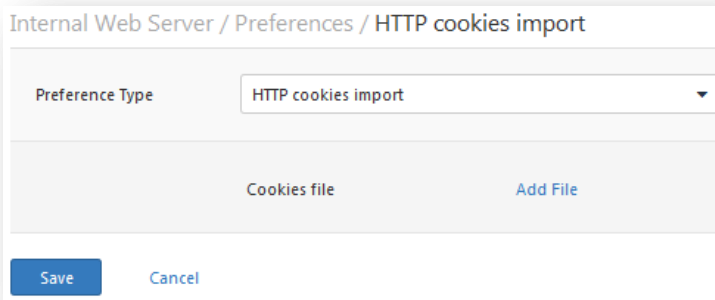
HP ProCurve File To Audit	Saved/(show config)
Policy file #1	Add File
Policy file #2	Add File
Policy file #3	Add File
Policy file #4	Add File
Policy file #5	Add File

Save Cancel

HTTP cookies import (Importation des cookies HTTP)

Pour faciliter les tests des applications Web, Nessus peut importer des cookies HTTP d'un autre logiciel (par exemple navigateur Internet, proxy Internet, etc.) avec les paramètres « **HTTP cookies import** » (Importation des cookies HTTP).

Un fichier de cookies peut être téléchargé de sorte que Nessus utilise les cookies lorsqu'il tente d'accéder à une application Web. Le fichier de cookies doit être au format Netscape.



HTTP login page (Page de connexion HTTP)

Les paramètres « **HTTP login page** » (Page de connexion HTTP) permettent de contrôler le point de départ des tests authentifiés d'une application Web personnalisée.

Option	Description
Login page (Page de connexion)	Chemin absolu de la page de connexion de l'application, par exemple « /login.html ».
Login form (Forme de connexion)	Paramètre « action » pour la méthode de forme. Par exemple, la forme de connexion pour <code><form method="POST" name="auth_form" action="/login.php"></code> serait « /login.php ».
Login form fields (Champs de forme de connexion)	Spécifie les paramètres d'authentification (par exemple <code>login=%USER%&password=%PASS%</code>). Si les mots clés %USER% et %PASS% sont utilisés, ils seront remplacés par les valeurs fournies dans le menu déroulant « Login configurations » (Configurations de connexion). Ce champ peut être utilisé pour fournir plus de deux paramètres si nécessaire (par exemple, un nom de « groupe » ou une autre information est requis pour le processus d'authentification).
Login form method (Méthode de forme de connexion)	Précise si l'action de connexion est effectuée sur une demande GET ou POST.
Automated login page search (Recherche de page de connexion automatisée)	Indique à Nessus de rechercher une page de connexion.
Re-authenticate delay (seconds) (Retard de réauthentification (secondes))	Intervalle de temps entre les tentatives d'authentification. Ce paramètre est utile pour éviter de déclencher les mécanismes de blocage en force.
Check authentication on page (Vérifier l'authentification sur la page)	Chemin absolu d'une page Web protégée qui nécessite une authentification, permettant à Nessus de mieux déterminer l'état d'authentification, par exemple « /admin.html ».
Follow 30x redirections (# of levels) (Suivre les	Si un code 30x de redirection est reçu d'un serveur Web, ceci indique à Nessus de suivre ou non le lien fourni.

redirections 30x (nbre de niveaux)	
Authenticated regex (regex authentifiée)	Motif regex à rechercher sur la page de connexion. La simple réception d'un code de réponse 200 n'est pas toujours suffisante pour déterminer l'état de la session. Nessus peut essayer d'émuler une chaîne donnée telle que « Authentication successful! » (Authentification réussie).
Invert test (disconnected if regex matches) (Inverser le test (déconnecté si la regex correspond))	Motif regex à rechercher sur la page de connexion qui, s'il est trouvé, informe Nessus que l'authentification a échoué, par exemple « Authentication failed! » (Échec de l'authentification).
Match regex on HTTP headers (Faire correspondre la regex sur les en-têtes HTTP)	Au lieu de rechercher le corps d'une réponse, Nessus peut rechercher les en-têtes de réponse HTTP pour un motif regex donné afin de mieux déterminer l'état d'authentification.
Case insensitive regex (regex non sensible à la casse)	Les recherches regex sont sensibles à la casse par défaut. Ce paramètre demande à Nessus d'ignorer la casse.
Abort web application tests if login fails (Abandonner les tests d'application Web si la connexion échoue)	Si les identifiants fournis ne fonctionnent pas, Nessus abandonne les tests d'application Web personnalisée (mais pas les familles de plugins CGI).

Internal Web Server / Preferences / HTTP login page

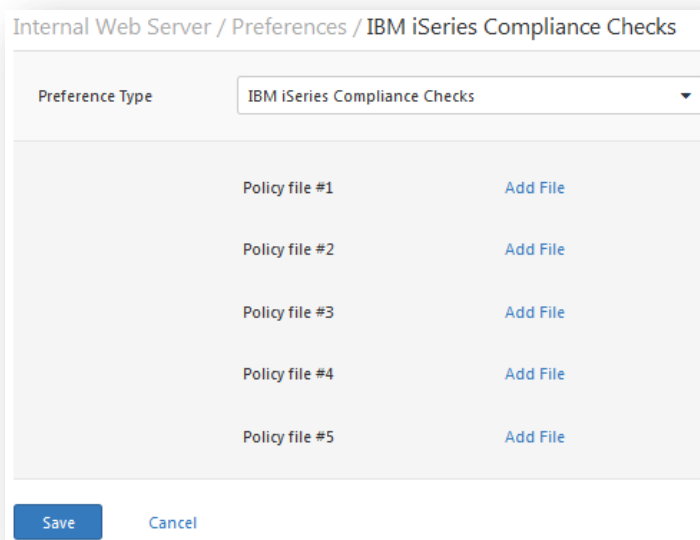
Preference Type: HTTP login page

Login page	/
Login form	
Login form fields	user=%USER%&pass=%PASS%
Login form method	POST
Automated login page search	<input type="checkbox"/>
Re-authenticate delay (seconds)	
Check authentication on page	
Follow 30x redirections (# of levels)	2
Authenticated regex	
Invert test (disconnected if regex matches)	<input type="checkbox"/>
Match regex on HTTP headers	<input type="checkbox"/>
Case insensitive regex	<input type="checkbox"/>
Abort web application tests if login fails	<input type="checkbox"/>

Save Cancel

IBM iSeries Compliance Checks (Contrôles de conformité IBM iSeries)

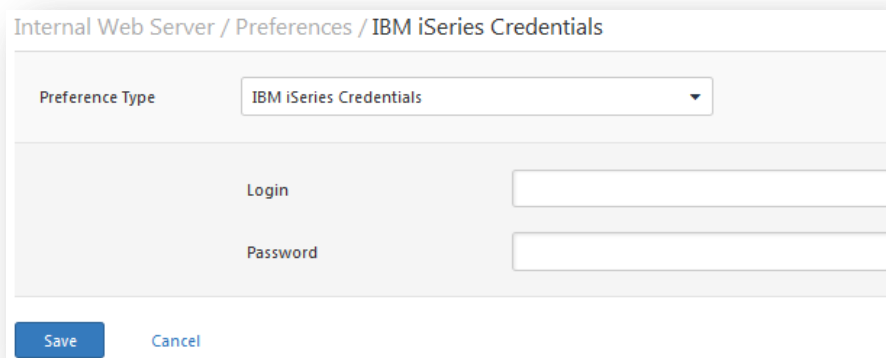
Le menu « **IBM iSeries Compliance Checks** » (Contrôles de conformité IBM iSeries) permet aux clients commerciaux de télécharger en amont des fichiers de stratégie qui seront utilisés pour déterminer si un système IBM iSeries testé satisfait aux normes de conformité spécifiées. Jusqu'à cinq stratégies peuvent être sélectionnées à la fois.



The screenshot shows a dialog box titled "Internal Web Server / Preferences / IBM iSeries Compliance Checks". At the top, there is a "Preference Type" dropdown menu set to "IBM iSeries Compliance Checks". Below this, there is a list of five "Policy file" entries, each with an "Add File" button to its right. The entries are labeled "Policy file #1" through "Policy file #5". At the bottom of the dialog, there are "Save" and "Cancel" buttons.

IBM iSeries Credentials (Identifiants IBM iSeries)

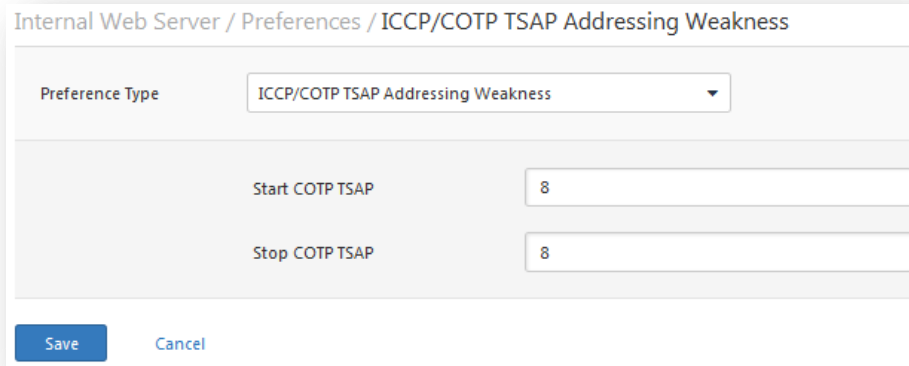
Les préférences « **IBM iSeries Credentials** » (Identifiants IBM iSeries) fournissent un emplacement qui permet d'indiquer les identifiants Nessus à authentifier sur un système IBM iSeries. Ces informations sont nécessaires pour un audit de conformité, notamment.



The screenshot shows a dialog box titled "Internal Web Server / Preferences / IBM iSeries Credentials". At the top, there is a "Preference Type" dropdown menu set to "IBM iSeries Credentials". Below this, there are two input fields: "Login" and "Password". At the bottom of the dialog, there are "Save" and "Cancel" buttons.

ICCP/COTP TSAP Addressing (Adressage ICCP/COTP TSAP)

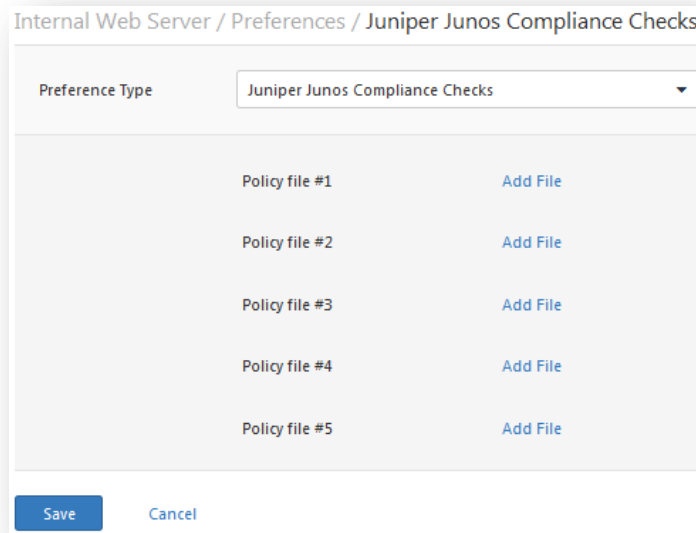
Le menu « **ICCP/COTP TSAP Addressing** » (Adressage ICCP/COTP TSAP) traite spécifiquement des contrôles SCADA. Il détermine une valeur TSAP (Transport Service Access Points, points d'accès de service de transport) pour le protocole COTP (Connection Oriented Transport Protocol, protocole de transport orienté vers la connexion) sur un serveur ICCP en essayant des valeurs possibles. La valeur de départ et d'arrêt par défaut est « 8 ».



The screenshot shows a configuration window titled "Internal Web Server / Preferences / ICCP/COTP TSAP Addressing Weakness". It features a "Preference Type" dropdown menu set to "ICCP/COTP TSAP Addressing Weakness". Below this, there are two input fields: "Start COTP TSAP" and "Stop COTP TSAP", both containing the value "8". At the bottom, there are "Save" and "Cancel" buttons.

Juniper Junos Compliance Checks (Contrôles de conformité Juniper Junos)

Le menu « **Juniper Junos Compliance Checks** » (Contrôles de conformité Juniper Junos) permet aux clients commerciaux de télécharger en amont des fichiers de stratégie qui seront utilisés pour déterminer si un système Juniper Junos testé satisfait aux normes de conformité spécifiées. Jusqu'à cinq stratégies peuvent être sélectionnées à la fois.



The screenshot shows a configuration window titled "Internal Web Server / Preferences / Juniper Junos Compliance Checks". It features a "Preference Type" dropdown menu set to "Juniper Junos Compliance Checks". Below this, there are five rows, each with a "Policy file #1" through "Policy file #5" label and an "Add File" button. At the bottom, there are "Save" and "Cancel" buttons.

LDAP 'Domain Admins' Group Membership Enumeration (Énumération de la participation du groupe 'Domain Admins' LDAP)

Le menu « **LDAP 'Domain Admins' Group Membership Enumeration** » (Énumération de la participation du groupe 'Domain Admins' LDAP) permet de saisir un groupe d'identifiants LDAP qui peut servir à énumérer une liste de membres du groupe « Domain Admins » dans le répertoire LDAP distant.

Internal Web Server / Preferences / LDAP 'Domain Admins' Group Membership Enumeration

Preference Type: LDAP 'Domain Admins' Group Membership Enumeration

LDAP user:

LDAP password:

Max results:

Login configurations (Configurations de connexion)

Le menu « **Login configurations** » (Configurations de connexion) permet au scanner Nessus d'utiliser les identifiants pour tester HTTP, NNTP, FTP, POP2, POP3 ou IMAP. Si vous fournissez des identifiants, Nessus aura peut-être la possibilité d'effectuer des contrôles plus poussés pour déterminer les vulnérabilités. Les identifiants HTTP fournis ici seront utilisés uniquement pour l'authentification Basic et Digest. Pour la configuration des identifiants pour une application Web personnalisée, utilisez le menu déroulant « HTTP login page » (Page de connexion HTTP).

Internal Web Server / Preferences / Login configurations

Preference Type: Login configurations

HTTP account:

HTTP password (sent in clear):

NNTP account:

NNTP password (sent in clear):

FTP account:

FTP password (sent in clear):

FTP writeable directory:

POP2 account:

POP2 password (sent in clear):

POP3 account:

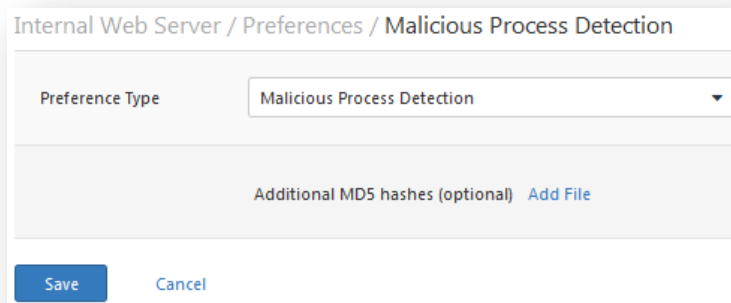
POP3 password (sent in clear):

IMAP account:

IMAP password (sent in clear):

Malicious Process Detection (Détection de processus malveillants)

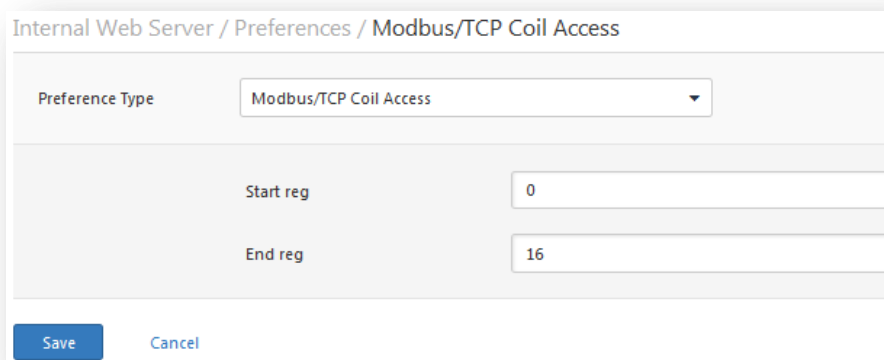
Le menu « **Malicious Process Detection** » (Détection de processus malveillants) permet de spécifier la liste des empreintes numériques MD5 supplémentaires que Nessus va utiliser pour scanner un système afin de détecter des programmes malveillants connus. Cette liste est utilisée par le plugin « Malicious Process Detection: User Defined Malware Running » (ID de plugin 65548), qui fonctionne comme le plugin « Malicious Process Detection » de Tenable (ID de plugin 59275). Des empreintes numériques supplémentaires peuvent être téléchargées en amont via un fichier texte contenant une empreinte numérique MD5 par ligne. Il est possible d'ajouter (en option) une description pour chacune des empreintes numériques figurant dans le fichier téléchargé en amont. Il suffit pour cela d'ajouter une virgule après l'empreinte numérique, suivie de la description. Si des correspondances sont trouvées pendant le scan d'une cible alors qu'une description avait été fournie pour l'empreinte numérique, la description s'affiche dans les résultats du scan. Des commentaires standard basés sur les empreintes numériques (par exemple, #) peuvent éventuellement être ajoutés aux commentaires délimités par des virgules.



The screenshot shows a web interface window titled "Internal Web Server / Preferences / Malicious Process Detection". It features a "Preference Type" dropdown menu set to "Malicious Process Detection". Below this, there is a section for "Additional MD5 hashes (optional)" with an "Add File" link. At the bottom, there are "Save" and "Cancel" buttons.

Modbus/TCP Coil Access (Accès à la bobine Modbus/TCP)

Les options « **Modbus/TCP Coil Access** » (Accès à la bobine Modbus/TCP) sont disponibles pour les utilisateurs commerciaux. Cet élément de menu déroulant est créé dynamiquement par les plugins SCADA disponibles avec la version commerciale de Nessus. Modbus utilise un code de fonction de 1 pour lire les « bobines » dans un Modbus asservi. Les bobines représentent des paramètres de sortie binaire et sont normalement mappées sur les actionneurs. La capacité à lire les bobines peut aider un attaquant à profiler un système et identifier les gammes de registres à altérer à l'aide d'un message « write coil » (écrire bobine). Les valeurs par défaut pour cela sont « 0 » pour le Start reg (Registre de départ) et « 16 » pour le End reg (Registre de fin).



The screenshot shows a web interface window titled "Internal Web Server / Preferences / Modbus/TCP Coil Access". It features a "Preference Type" dropdown menu set to "Modbus/TCP Coil Access". Below this, there are two input fields: "Start reg" with the value "0" and "End reg" with the value "16". At the bottom, there are "Save" and "Cancel" buttons.

Nessus SYN scanner et Nessus TCP scanner (Scanner Nessus SYN et Scanner Nessus TCP)

Les options « **Nessus SYN scanner** » et « **Nessus TCP scanner** » permettent de mieux ajuster les scanners natifs SYN et TCP afin de détecter la présence d'un pare-feu.

Valeur	Description
Automatic (normal) (Automatique (normal))	Cette option peut aider à déterminer si un pare-feu est situé entre le scanner et la cible (default - valeur par défaut).
Disabled (softer) (Désactivé (moins agressif))	Désactive la fonction Firewall detection (Détection de pare-feu).
Do not detect RST rate limitation (soft) (Ne pas détecter la limitation du taux RST (non agressif))	Désactive la capacité de surveiller la fréquence de définition des réinitialisations et de déterminer s'il existe une limitation configurée par un périphérique réseau en aval.
Ignore closed ports (aggressive) (Ignorer les ports fermés (agressif))	Tentera d'exécuter les plug-ins même si le port semble être fermé. Il est recommandé de ne pas utiliser cette option sur un réseau de production.

Internal Web Server / Preferences / Nessus SYN scanner

Preference Type:

Firewall detection:

Internal Web Server / Preferences / Nessus TCP scanner

Preference Type:

Firewall detection:

NetApp Data ONTAP Compliance Checks (Contrôles de conformité NetApp Data ONTAP)

Le menu « **NetApp Data ONTAP Compliance Checks** » (Contrôles de conformité NetApp Data ONTAP) permet aux clients commerciaux de télécharger en amont des fichiers de stratégie qui seront utilisés pour déterminer si un périphérique NetApp Data ONTAP testé satisfait aux normes de conformité spécifiées. Jusqu'à cinq stratégies peuvent être sélectionnées à la fois.

The screenshot shows a web interface window titled "Internal Web Server / Preferences / NetApp Data ONTAP Compliance Checks". At the top, there is a "Preference Type" dropdown menu set to "NetApp Data ONTAP Compliance Checks". Below this, there is a list of five "Policy file" entries, each with an "Add File" button next to it. At the bottom of the window, there are "Save" and "Cancel" buttons.

Policy file #	Action
Policy file #1	Add File
Policy file #2	Add File
Policy file #3	Add File
Policy file #4	Add File
Policy file #5	Add File

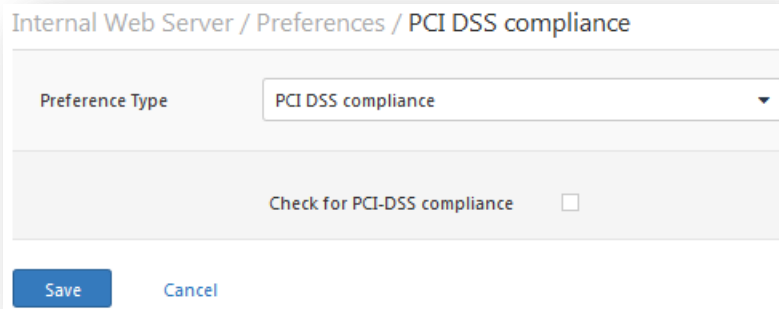
Oracle Settings (Paramètres Oracle)

Le menu « **Oracle Settings** » (Paramètres Oracle) configure Nessus avec Oracle Database SID (SID de base de données Oracle) et inclut une option pour rechercher les comptes par défaut connus dans le logiciel Oracle.

The screenshot shows a web interface window titled "Internal Web Server / Preferences / Oracle Settings". At the top, there is a "Preference Type" dropdown menu set to "Oracle Settings". Below this, there is a text input field for "Oracle SID". Underneath, there is a checkbox labeled "Test default accounts (slow)". At the bottom of the window, there are "Save" and "Cancel" buttons.

PCI DSS Compliance (Conformité PCI DSS)

L'option « **PCI DSS Compliance** » (Conformité PCI DSS) commande à Nessus de comparer les résultats du scan aux normes de conformité PCI DSS en cours. Cette fonction est uniquement disponible pour les clients commerciaux.



Internal Web Server / Preferences / PCI DSS compliance

Preference Type: PCI DSS compliance

Check for PCI-DSS compliance

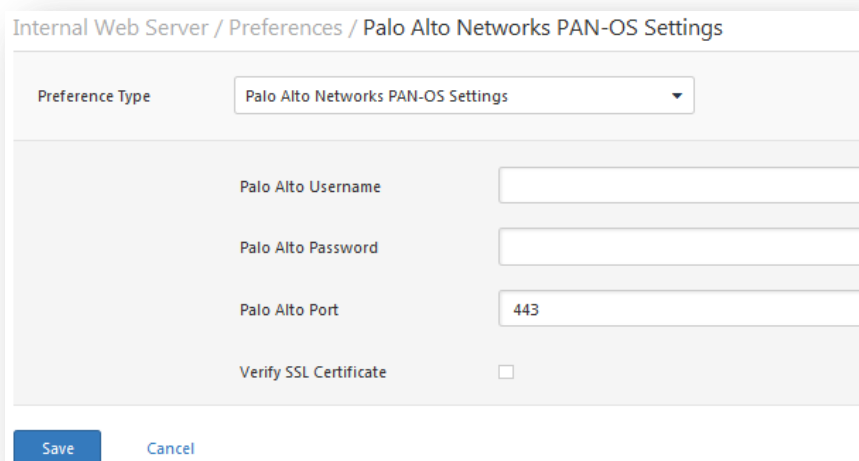
Save Cancel

Patch Management (Gestion de correctifs)

Nessus peut tirer parti des identifiants pour les systèmes de gestion de correctifs Red Hat Satellite Server, WSUS, SCCM et VMware Go (anciennement Shavlik) afin d'effectuer l'audit de correctifs sur les systèmes pour lesquels les identifiants peuvent ne pas être mis à la disposition du scanner Nessus. Les options pour ces systèmes de gestion de correctifs se trouvent sous « Preferences » (Préférences) dans leurs menus déroulants respectifs : « **Patch Management: IBM Tivoli Endpoint Manager Server Settings** » (Gestion de correctifs : paramètres de serveur IBM Tivoli Endpoint Manager), « **Patch Management: Red Hat Satellite Server Settings** » (Gestion de correctifs : paramètres de serveur Red Hat Satellite), « **Patch Management: SCCM Server Settings** » (Gestion de correctifs : paramètres de serveur SCCM), « **Patch Management: VMware Go Server Settings** » (Gestion de correctifs : paramètres de serveur VMware Go) et « **Patch Management: WSUS Server Settings** » (Gestion de correctifs : paramètres de serveur WSUS). Vous trouverez plus d'informations sur l'utilisation de Nessus pour scanner les hôtes via ces systèmes de gestion de correctifs dans le document « [Patch Management Integration](#) » (Intégration de la gestion de correctifs).

Palo Alto Networks PAN-OS Settings (Paramètres Palo Alto Networks PAN-OS)

Le menu « **Palo Alto Networks PAN-OS Settings** » (Paramètres Palo Alto Networks PAN-OS) permet aux clients commerciaux de contrôler les périphériques Palo Alto PAN-OS. Cette opération exige des identifiants valides ; elle permet de configurer le port et éventuellement de vérifier totalement le certificat SSL avant de continuer.



Internal Web Server / Preferences / Palo Alto Networks PAN-OS Settings

Preference Type: Palo Alto Networks PAN-OS Settings

Palo Alto Username:

Palo Alto Password:

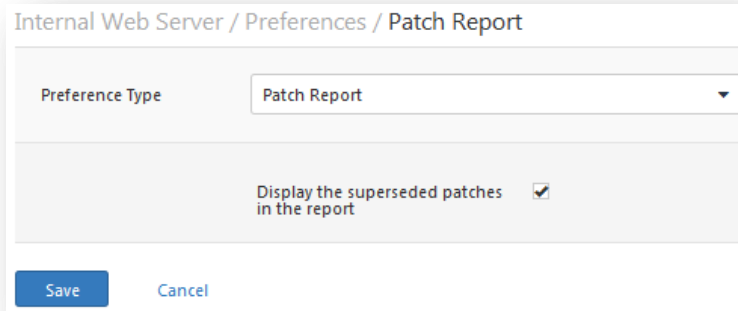
Palo Alto Port: 443

Verify SSL Certificate

Save Cancel

Patch Report (Rapport sur les correctifs)

Le menu « **Patch Report** » (Rapport sur les correctifs) permet de configurer Nessus de façon à inclure ou supprimer des informations dépassées sur les correctifs dans le compte-rendu de scan. Cette option est activée par défaut.



Ping the remote host (Sonder l'hôte à distance)

Les options « **Ping the remote host** » (Sonder l'hôte à distance) permettent de contrôler avec précision la capacité de Nessus à sonder les hôtes pendant le scan de détection. Cette opération peut être effectuée à l'aide du ping ARP, TCP ICMP ou du ping applicatif UDP.

Option	Description
TCP ping destination port(s) (Port(s) de destination de ping TCP)	Spécifie la liste des ports qui seront contrôlés par le ping TCP. En cas de doute sur les ports, conservez la valeur par défaut « built-in » (intégré).
Number of Retries (ICMP) (Nombre de nouvelles tentatives (ICMP))	Permet de spécifier le nombre de tentatives effectuées pour sonder l'hôte distant. La valeur par défaut est 6.
Do an applicative UDP ping (DNS, RPC...) (Effectuer un sondage UDP applicatif (DNS, RPC...))	Effectue un sondage UDP pour des applications spécifiques basées sur UDP, y compris DNS (port 53), RPC (port 111), NTP (port 123) et RIP (port 520).
Make the dead hosts appear in the report (Faire apparaître les hôtes sans réponse dans le rapport)	Si cette option est sélectionnée, les hôtes qui n'ont pas répondu à la demande ping sont inclus dans le rapport de sécurité en tant qu'hôtes morts.
Log live hosts in the report (Enregistrer les hôtes actifs dans le rapport)	Sélectionnez cette option pour inclure spécifiquement dans le rapport la capacité à sonder avec succès un hôte distant.
Test the local Nessus host (Tester l'hôte Nessus local)	Cette option permet d'inclure l'hôte Nessus local dans le scan ou de l'exclure du scan. Ce paramètre est utilisé lorsque l'hôte Nessus est situé dans la plage de réseau cible pour le scan.
Fast network discovery (Détection rapide de réseau)	Par défaut, lorsque Nessus « sonde » un IP à distance et reçoit une réponse, il effectue des contrôles supplémentaires pour s'assurer qu'il ne s'agit pas d'un proxy transparent ou d'un équilibreur de charge qui renverrait du bruit mais pas de résultat (certains périphériques répondent à chaque port 1-65535 mais ne sont pas en service). De tels contrôles peuvent prendre du temps, en particulier si l'hôte distant est

protégé par un pare-feu. Si l'option « fast network discovery » (détection rapide de réseau) est activée, Nessus n'effectue pas ces contrôles.



Pour scanner les systèmes invités VMware, « ping » doit être désactivé. Dans la stratégie de scan, sous la rubrique « Advanced » (Avancé) -> « Ping the remote host » (Sonder l'hôte à distance), décochez les pings TCP, ICMP et ARP.

Internal Web Server / Preferences / Ping the remote host

Preference Type: Ping the remote host

TCP ping destination port(s): built-in

Do an ARP ping:

Do a TCP ping:

Do an ICMP ping:

Number of retries (ICMP): 2

Do an applicative UDP ping (DNS,RPC...):

Make the dead hosts appear in the report:

Log live hosts in the report:

Test the local Nessus host:

Fast network discovery:

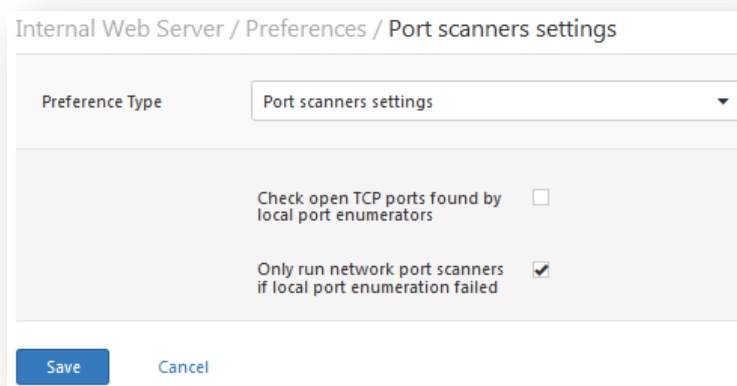
Save Cancel

Port scanner settings (Paramètres de scanner des ports)

Le menu « **Port scanner settings** » (Paramètres de scanner des ports) fournit deux options pour contrôler davantage l'activité de scan des ports :

Option	Description
Check open TCP ports found by local port enumerators (Vérifier les ports TCP ouverts détectés par les énumérateurs de ports locaux)	Si un énumérateur de port local (par exemple WMI ou netstat) détecte un port, Nessus vérifie également s'il est ouvert à distance. Ce paramètre aide à déterminer si un certain type de contrôle d'accès est utilisé (par exemple, wrappers TCP, pare-feu).
Only run network port scanners if local port enumeration failed	Sinon, fiez-vous d'abord à l'énumération des ports locaux.

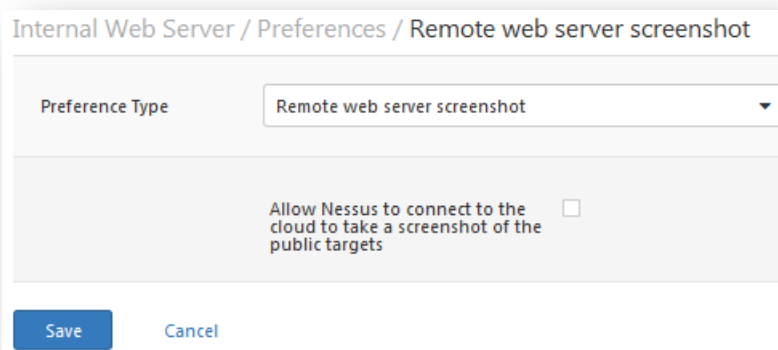
(Exécuter les scanners de port de réseau uniquement si l'énumération des ports locaux a échoué)



Remote web server screenshot (Capture d'écran de serveur Web distant)

Le menu « **Remote web server screenshot** » (Capture d'écran de serveur Web distant) permet à Nessus de prendre des captures d'écrans pour mieux expliciter certains résultats. Cette fonction inclut certains services (par exemple, VNC, RDP) ainsi que des options spécifiques de la configuration (par exemple, indexation des répertoires de serveur web). La fonction s'applique uniquement aux hôtes avec accès via Internet, puisque les captures d'écran sont générées sur un serveur géré et envoyées au scanner Nessus.

Les captures d'écran **ne sont pas** exportées avec un compte-rendu de scan Nessus.



SCAP Linux Compliance Checks (Contrôles de conformité SCAP Linux)

Le menu « **SCAP Linux Compliance Checks** » (Contrôles de conformité SCAP Linux) permet aux clients commerciaux de télécharger en amont les fichiers d'audit de configuration SCAP zip qui seront utilisés pour déterminer si un système Linux testé satisfait aux normes de conformité spécifiées dans SP 800-126. Pour plus d'informations sur SCAP, veuillez visiter le site [NIST Security Content Automation Protocol](https://nvd.nist.gov/SCAP/) (Protocole d'automatisation de contenu de sécurité NIST).

Internal Web Server / Preferences / SCAP Linux Compliance Checks

Preference Type: SCAP Linux Compliance Checks

SCAP File (zip) #1	Add File
SCAP Version #1	1.2
SCAP Data Stream ID (1.2 only) #1	
SCAP Benchmark ID #1	
SCAP Profile ID #1	
OVAL Result Type #1	Full results w/ system characteristics
SCAP File (zip) #2	Add File
SCAP Version #2	1.2

SCAP Windows Compliance Checks (Contrôles de conformité SCAP Windows)

Le menu « **SCAP Windows Compliance Checks** » (Contrôles de conformité SCAP Windows) permet aux clients commerciaux de télécharger en amont les fichiers SCAP zip qui seront utilisés pour déterminer si un système Windows testé satisfait aux normes de conformité spécifiées dans SP 800-126. Pour plus d'informations sur SCAP, veuillez visiter le site [NIST Security Content Automation Protocol](#) (Protocole d'automatisation de contenu de sécurité NIST).

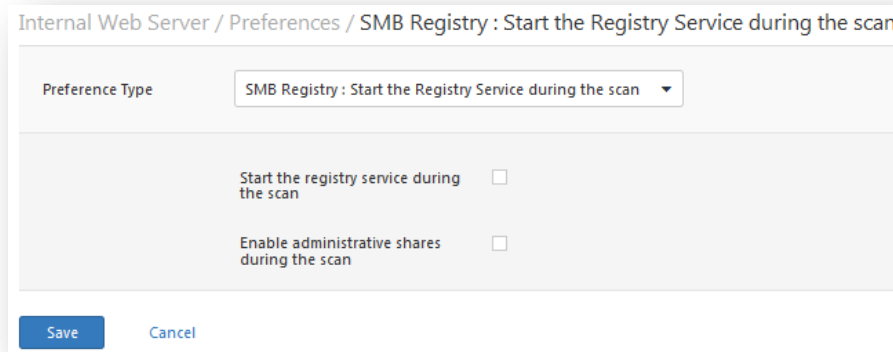
Internal Web Server / Preferences / SCAP Windows Compliance Checks

Preference Type: SCAP Windows Compliance Checks

SCAP File (zip) #1	Add File
SCAP Version #1	1.2
SCAP Data Stream ID (1.2 only) #1	
SCAP Benchmark ID #1	
SCAP Profile ID #1	
OVAL Result Type #1	Full results w/ system characteristics
SCAP File (zip) #2	Add File
SCAP Version #2	1.2

SMB Registry: Start the Registry Service during the scan (Registre SMB : démarrer le service de registre pendant le scan)

Le menu « **SMB Registry: Start the Registry Service during the scan** » (Registre SMB : démarrer le service de registre pendant le scan) permet au service de faciliter quelques-unes des exigences de scan pour les ordinateurs sur lesquels le registre SMB peut ne pas être exécuté en permanence.



Internal Web Server / Preferences / SMB Registry : Start the Registry Service during the scan

Preference Type: SMB Registry : Start the Registry Service during the scan

Start the registry service during the scan

Enable administrative shares during the scan

Save Cancel

SMB Registry : Start the Registry Service during the scan (Registre SMB : démarrer le service de registre pendant le scan)

Le menu « **SMB Registry : Start the Registry Service during the scan** » (Registre SMB : démarrer le service de registre pendant le scan) permet à Nessus d'utiliser les identifiants pour démarrer temporairement le service de registre SMB afin d'effectuer des opérations d'audit supplémentaires. Nessus désactive le service à l'issue de la procédure.



Preference Type: SMB Registry : Start the Registry Service dur...

Start the registry service during the scan

Enable administrative shares during the scan

SMB Scope (Portée SMB)

Sous le menu « **SMB Scope** » (Portée SMB), si l'option « **Request information about the domain** » (Demande d'information au sujet du domaine) est définie, les utilisateurs de domaine seront interrogés à la place des utilisateurs locaux.

Preference Type: SMB Scope

Request information about the domain

SMB Use Domain SID to Enumerate Users (SMB utilise le SID de domaine pour énumérer les utilisateurs)

Le menu « **SMB Use Domain SID to Enumerate Users** » (SMB utilise le SID de domaine pour énumérer les utilisateurs) spécifie la plage de SID à utiliser pour effectuer une recherche inversée des noms d'utilisateur sur le domaine. Le paramètre par défaut est recommandé pour la plupart des scans.

Internal Web Server / Preferences / SMB Use Domain SID to Enumerate Users

Preference Type: SMB Use Domain SID to Enumerate Users

Start UID: 1000

End UID: 1200

Save Cancel

SMB Use Host SID to Enumerate Local Users (SMB utilise le SID d'hôte pour énumérer les utilisateurs locaux)

Le menu « **SMB Use Host SID to Enumerate Local Users** » (SMB utilise le SID d'hôte pour énumérer les utilisateurs locaux) spécifie la plage de SID à utiliser pour effectuer une recherche inversée des noms d'utilisateur locaux. Le paramètre par défaut est recommandé.

Internal Web Server / Preferences / SMB Use Host SID to Enumerate Local Users

Preference Type

Start UID

End UID

SMTP settings (Paramètres SMTP)

Le menu « **SMTP settings** » (Paramètres SMTP) spécifie les options pour les tests SMTP (Simple Mail Transport Protocol, protocole de transfert de courrier simple) qui sont effectués sur tous les périphériques du domaine scanné exécutant les services SMTP. Nessus tente de transmettre les messages par l'intermédiaire du périphérique au « **Third party domain** » (Domaine tiers) spécifié. Si le message envoyé au « **Third party domain** » est rejeté par l'adresse spécifiée dans le champ « **To address** » (Adresse de destination), la tentative de spam a échoué. Si le message est accepté, le serveur SMTP a été utilisé avec succès pour transmettre du spam.

Option	Description
Third party domain (Domaine tiers)	Nessus tentera d'envoyer un spam via chaque périphérique SMTP à l'adresse indiquée dans ce champ. Cette adresse de domaine tiers doit être hors de la plage du site scanné ou du site exécutant le scan. Sinon, le test sera peut-être abandonné par le serveur SMTP.
From address (Adresse d'origine)	Les messages de test envoyés aux serveurs SMTP apparaissent comme s'ils provenaient de l'adresse spécifiée dans ce champ.
To address (Adresse de destination)	Nessus tentera d'envoyer les messages adressés au destinataire indiqué dans ce champ. L'adresse du postmaster est la valeur par défaut puisqu'il s'agit d'une adresse valide sur la plupart des serveurs de messagerie.

Internal Web Server / Preferences / SMTP settings

Preference Type: SMTP settings

Third party domain: example.com

From address: nobody@example.com

To address: postmaster@[AUTO_REPLACED_IP]

Save Cancel

SNMP settings (Paramètres SNMP)

Le menu « **SNMP settings** » (Paramètres SNMP) permet de configurer Nessus pour la connexion et l'identification au service SNMP de la cible. Pendant le scan, Nessus tente un certain nombre de fois de deviner la chaîne de communauté et pouvoir l'utiliser pour les tests suivants. Jusqu'à quatre chaînes de nom de communauté séparées sont prises en charge par la stratégie de scan. Si Nessus est incapable de deviner la chaîne de communauté et/ou le mot de passe, il ne pourra peut-être pas effectuer d'audit complet du service.

Option	Description
Community name (0-3) (Nom de communauté, 0 à 3)	Nom de communauté SNMP.
UDP port (Port UDP)	Indique à Nessus de scanner un port différent si SNMP est exécuté sur un port autre que 161.
SNMPv3 user name (Nom d'utilisateur SNMPv3)	Nom d'utilisateur pour un compte basé sur SNMPv3.
SNMPv3 authentication password (Mot de passe d'authentification SNMPv3)	Mot de passe pour le nom d'utilisateur spécifié.
SNMPv3 authentication algorithm (Algorithme d'authentification SNMPv3)	Sélectionnez MD5 ou SHA1 selon l'algorithme pris en charge par le service distant.
SNMPv3 privacy password (Mot de passe du domaine privé SNMPv3)	Mot de passe utilisé pour protéger les communications SNMP cryptées.
SNMPv3 privacy algorithm (Algorithme du domaine privé SNMPv3)	Algorithme de cryptage à utiliser pour le trafic SNMP.

Internal Web Server / Preferences / SNMP settings

Preference Type: SNMP settings

Community name: public

Community name (1):

Community name (2):

Community name (3):

UDP port: 161

SNMPv3 user name:

SNMPv3 authentication password:

SNMPv3 authentication algorithm: MD5

SNMPv3 privacy password:

SNMPv3 privacy algorithm: DES

Save Cancel

Service Detection (Détection du service)

Le menu « **Service Detection** » (Détection du service) contrôle la façon dont Nessus testera les services SSL : ports SSL connus (par exemple le port 443), tous les ports ou aucun. Les tests de capacité SSL sur tous les ports peuvent perturber l'hôte testé.

Internal Web Server / Preferences / Service Detection

Preference Type: Service Detection

Test SSL based services: Known SSL ports

Save Cancel

Unix Compliance Checks (Contrôles de conformité Unix)

Le menu « **Unix Compliance Checks** » (Contrôles de conformité Unix) permet aux clients commerciaux de télécharger en amont les fichiers d'audit de configuration Unix qui seront utilisés pour déterminer si un système testé satisfait aux normes de conformité spécifiées. Jusqu'à cinq stratégies peuvent être sélectionnées à la fois.

Internal Web Server / Preferences / Unix Compliance Checks

Preference Type: Unix Compliance Checks

Policy file #1	Add File
Policy file #2	Add File
Policy file #3	Add File
Policy file #4	Add File
Policy file #5	Add File

Save Cancel

VMware SOAP API Settings (Paramètres de l'API SOAP VMware)

Le menu « **VMware SOAP API Settings** » (Paramètres de l'API SOAP VMware) fournit à Nessus les identifiants requis pour effectuer l'authentification sur les systèmes de gestion VMware ESX, ESXi et vSphere Hypervisor via leur propre API SOAP, puisque l'accès SSH est déprécié. L'API est destinée à l'audit des hôtes vSphere 4.x / 5.x, ESXi et ESX, et **non** des machines virtuelles exécutées sur les hôtes. Cette méthode d'authentification peut être utilisée pour effectuer des scans authentifiés ou des audits de conformité.

Internal Web Server / Preferences / VMware SOAP API Settings

Preference Type: VMware SOAP API Settings

VMware user name:

VMware password:

Ignore SSL Certificate:

Save Cancel

Option	Description
VMware user name (Nom d'utilisateur VMware)	Nom d'utilisateur à utiliser pour l'authentification. Les identifiants peuvent être les comptes Active Directory (AD) pour les hôtes intégrés ou les comptes locaux, et les comptes doivent se trouver dans le groupe local <code>root</code> . Les identifiants de domaine sont au format <code>utilisateur@domaine</code> , les comptes créés localement sont l'utilisateur et le mot de passe.

VMware password (unsafe!) (Mot de passe VMware (non sécurisé))	Ce mot de passe n'est pas envoyé en mode sécurisé et il peut être intercepté à l'aide d'un mouchard réseau.
Ignore SSL Certificate (Ignorer le certificat SSL)	Ignore le certificat SSL éventuellement présent sur le serveur.

VMware vCenter SOAP API Settings (Paramètres de l'API SOAP VMware vCenter)

Le menu « **VMware vCenter SOAP API Settings** » (Paramètres de l'API SOAP VMware vCenter) fournit à Nessus les identifiants requis pour effectuer l'authentification sur VMware vCenter via leur propre API SOAP, puisque l'accès SSH est déprécié. L'API est destinée à l'audit de vCenter, et **non** des machines virtuelles exécutées sur les hôtes. Cette méthode d'authentification peut être utilisée pour effectuer des scans authentifiés ou des audits de conformité.

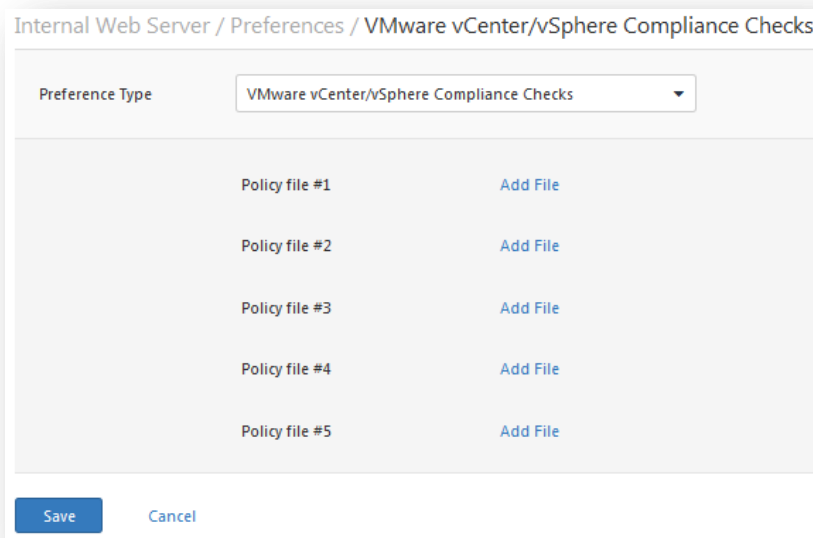
Option	Description
VMware vCenter host (Hôte VMware vCenter)	Nom d'hôte ou adresse IP de l'installation vCenter à contrôler.
VMware vCenter port (Port VMware vCenter)	Port que vCenter utilise pour répondre (par défaut : 443).
VMware vCenter user name (Nom d'utilisateur VMware vCenter)	Nom d'utilisateur à utiliser pour l'authentification. Les identifiants peuvent être les comptes Active Directory (AD) pour les hôtes intégrés ou les comptes locaux, et les comptes doivent se trouver dans le groupe local <code>root</code> . Les identifiants de domaine sont au format <code>utilisateur@domaine</code> , les comptes créés localement sont l'utilisateur et le mot de passe.
VMware vCenter password (Mot de passe VMware vCenter)	Ce mot de passe n'est pas envoyé en mode sécurisé et il peut être intercepté à l'aide d'un mouchard réseau, sauf si SSL est spécifié.
SSL (SSL)	Utilise SSL pour se connecter à l'hôte.

**Verify SSL Certificate
(Vérifier le certificat SSL)**

Vérifie l'intégrité du certificat SSL éventuellement présent sur le serveur.

VMware vCenter/vSphere Compliance Checks (Contrôles de conformité VMware vCenter/vSphere)

Le menu « **VMware vCenter/vSphere Compliance Checks** » (Contrôles de conformité VMware vCenter/vSphere) permet aux clients commerciaux de télécharger en amont les fichiers d'audit VMware vCenter ou vSphere qui seront utilisés pour déterminer si un système testé satisfait aux normes de conformité spécifiées. Jusqu'à cinq stratégies peuvent être sélectionnées à la fois.



Wake-on-LAN (WOL, éveil sur réseau local)

Le menu « **Wake-on-LAN** » (WOL) [WOL, éveil sur réseau local] contrôle l'hôte destinataire des Magic Packets WOL avant d'effectuer un scan et la durée d'attente (en minutes) pour que les systèmes s'initialisent. La liste des adresses MAC pour WOL est saisie en utilisant un fichier texte téléchargé avec une adresse MAC d'hôte par ligne. Par exemple :

```
00:11:22:33:44:55  
aa:bb:cc:dd:ee:ff  
[...]
```

Internal Web Server / Preferences / Wake-on-LAN

Preference Type:

List of MAC addresses for Wake-on-LAN: [Add File](#)

Time to wait (in minutes) for the systems to boot:

Web Application Tests Settings (Paramètres des tests des applications Web)

Le menu « **Web Application Tests Settings** » (Paramètres des tests des applications Web) teste les arguments des CGI (Common Gateway Interface, interface de passerelle commune) distants détectés lors du processus de mise en miroir Web en essayant de passer les erreurs fréquentes de programmation CGI telles que le scriptage intersite, l'inclusion de fichiers distants, l'exécution des commandes, les attaques de traversée et l'injection SQL. Activez cette option en cochant la case « Enable web applications tests » (Activer les tests des applications Web). Ces tests dépendent des plugins NASL suivants :

- [11139](#), [42424](#), [42479](#), [42426](#), [42427](#), [43160](#) – SQL Injection (CGI abuses)
- [39465](#), [44967](#) – Command Execution (CGI abuses)
- [39466](#), [47831](#), [42425](#), [46193](#), [49067](#) – Cross-Site Scripting (CGI abuses: XSS)
- [39467](#), [46195](#), [46194](#) – Directory Traversal (CGI abuses)
- [39468](#) – HTTP Header Injection (CGI abuses: XSS)
- [39469](#), [42056](#), [42872](#) – File Inclusion (CGI abuses)
- [42055](#) – Format String (CGI abuses)
- [42423](#), [42054](#) – Server Side Includes (CGI abuses)
- [44136](#) – Cookie Manipulation (CGI abuses)
- [46196](#) – XML Injection (CGI abuses)
- [40406](#), [48926](#), [48927](#) – Error Messages
- [47830](#), [47832](#), [47834](#), [44134](#) – Additional attacks (CGI abuses)



Remarque : Cette liste de plugins associés aux applications Web est mise à jour fréquemment et n'est peut-être pas complète. Des plugins supplémentaires peuvent dépendre des paramètres de cette option de préférence.

Option	Description
Maximum run time (min) (Temps d'exécution maximum (min))	Cette option gère la durée d'exécution des tests d'applications Web, en minutes. Elle a une valeur par défaut de 60 minutes et concerne tous les ports et les CGI d'un site Internet donné. Le scan du réseau local pour les sites Internet comprenant de petites applications s'exécute généralement en moins d'une heure ; toutefois, les sites Internet avec de grandes applications peuvent nécessiter une valeur plus élevée.
Try all HTTP methods (Essayer toutes les méthodes HTTP)	Par défaut, Nessus effectue les tests à l'aide des demandes GET uniquement. Cette option indique à Nessus d'utiliser également les « POST requests » (demandes POST) pour tester les formats améliorés du Web. Par défaut, les tests d'application Web utilisent uniquement les demandes GET, sauf si cette option est activée. En général, les applications plus complexes utilisent la méthode POST lorsqu'un utilisateur soumet des données à l'application. Ce paramètre fournit des tests plus complets mais peut augmenter considérablement la durée requise. Lorsqu'il est sélectionné, Nessus teste chaque script/variable avec les deux demandes GET et POST.
Combinations of arguments values (Combinaisons des valeurs d'argument)	Cette option gère la combinaison des valeurs d'argument utilisées dans les demandes HTTP. Ce menu déroulant comporte trois options : <p>one value (une valeur) – Teste un paramètre à la fois avec une chaîne d'attaque, sans essayer les variations de « non-attaque » pour les paramètres supplémentaires. Par exemple, Nessus peut tenter « /test.php?arg1=XSS&b=1&c=1 » où « b » et « c » autorisent d'autres valeurs, sans tester chaque combinaison. C'est la méthode de test la plus rapide avec le plus petit ensemble de résultats produits.</p> <p>All pairs (slower but efficient) [Toutes les paires (plus lent mais efficace)] – Ce type d'essai est légèrement plus lent mais plus efficace que le test « one value ». Pendant les tests de paramètres multiples, il teste une chaîne d'attaque, des variations pour une seule variable, puis il utilise la première valeur pour toutes les autres variables. Par exemple, Nessus peut tenter « /test.php?a=XSS&b=1&c=1&d=1 », puis parcourir les variables de sorte que l'une reçoive la chaîne d'attaque, une autre reçoive successivement toutes les valeurs possibles (détectées lors du processus de mise en miroir) et les autres variables reçoivent la première valeur. Dans ce cas, Nessus ne testera jamais « /test.php?a=XSS&b=3&c=3&d=3 » si la première valeur de chaque variable est « 1 ».</p> <p>All combinations (extremely slow) [Toutes les combinaisons (extrêmement lent)] – Cette méthode de test effectuera un test complet de toutes les combinaisons possibles de chaînes d'attaque avec entrée valide de variable. Alors que les tests « All-pairs » (toutes les paires) cherchent à réduire la taille d'un ensemble de données comme compromis avec la vitesse, « all combinations » (toutes les combinaisons) ne fait pas de compromis avec la durée et utilise un ensemble complet de tests. L'exécution de cette méthode de test peut être très longue.</p>
HTTP Parameter Pollution (Pollution de paramètre HTTP)	Lors de l'exécution des tests d'application Web, tente de contourner tout mécanisme de filtrage en injectant un contenu dans une variable tout en fournissant aussi à cette même variable un contenu valide. Par exemple, un test d'injection SQL normal pourrait être « /target.cgi?a='&b=2 ». Lorsque le paramètre HPP (HTTP Parameter Pollution) est activé, la demande peut être similaire à la suivante : « /target.cgi?a='&a=1&b=2 ».
Stop at first flaw (Arrêt au premier défaut)	Cette option détermine le moment où un nouveau défaut est ciblé. Elle s'applique au niveau du script. La recherche d'un défaut XSS ne désactive pas la recherche d'une injection SQL ou d'une injection d'en-tête, mais vous recevrez au plus un rapport pour chaque type sur un port donné, sauf si « thorough tests » (tests complets) est utilisé.

	<p>Plusieurs défauts du même type (par exemple XSS, SQLi, etc.) peuvent parfois être signalés s'ils ont été décelés par la même attaque. Le menu déroulant contient quatre options :</p> <p>per CGI (par CGI) – Dès qu'un défaut est découvert sur un CGI par un script, Nessus passe au CGI connu suivant sur le même serveur ou, s'il n'y a pas d'autre CGI, au port/serveur suivant. Il s'agit de l'option par défaut.</p> <p>per port (quicker) [par port (plus rapide)] – Dès qu'un défaut est découvert sur un serveur Web par un script, Nessus s'arrête et passe à un autre serveur Web sur un port différent</p> <p>per parameter (slow) [par paramètre (lent)] – Dès qu'un type de défaut est découvert dans un paramètre d'un CGI (par exemple XSS), Nessus passe au paramètre suivant du même CGI, au CGI connu suivant ou au port/serveur suivant</p> <p>look for all flaws (slower) [regarder tous les défauts (plus lent)] – Effectue des tests généralisés quels que soient les défauts trouvés. Cette option peut produire un rapport extrêmement détaillé et elle est souvent déconseillée.</p>
<p>Test Embedded web servers (Tester les serveurs Web intégrés)</p>	<p>Les serveurs Web intégrés sont souvent statiques et ne contiennent pas de scripts CGI personnalisables. En outre, les serveurs Web intégrés peuvent être sujets à des pannes fréquentes ou peuvent ne pas répondre lorsqu'ils sont scannés. Tenable recommande de scanner les serveurs Web intégrés séparément des autres serveurs Web au moyen de cette option.</p>
<p>URL for Remote File Inclusion (URL pour l'inclusion des fichiers à distance)</p>	<p>Pendant les tests RFI (Remote File Inclusion), cette option spécifie un fichier sur un hôte distant à utiliser pour les tests. Par défaut, Nessus utilise un fichier sécurisé sur le serveur Web de Tenable pour les tests RFI. Si le scanner ne peut pas être connecté à Internet, l'utilisation d'un fichier hébergé en interne est recommandée pour des tests RFI plus précis.</p>

Internal Web Server / Preferences / Web Application Tests Settings

Preference Type: Web Application Tests Settings

Enable web applications tests

Maximum run time (min): 60

Try all HTTP methods

Combinations of arguments values: one value

HTTP Parameter Pollution

Stop at first flaw: per CGI

Test embedded web servers

URL for Remote File Inclusion: http://rfi.nessus.org/rfi.txt

Save Cancel

Web mirroring (Mise en miroir Web)

Le menu « **Web mirroring** » (Mise en miroir Web) définit les paramètres de configuration pour l'utilitaire de mise en miroir du contenu de serveur Web natif de Nessus. Nessus met en miroir le contenu Web pour mieux analyser ses vulnérabilités et réduire au minimum l'impact sur le serveur.



Si les paramètres de mise en miroir Web sont configurés de façon à mettre en miroir un site Web complet, ceci peut entraîner la génération d'un trafic important pendant le scan. Par exemple, s'il existe 1 gigaoctet de données sur un serveur Web et si Nessus est configuré pour tout mettre en miroir, le scan produira au moins 1 gigaoctet de trafic entre le serveur et le scanner Nessus.

Option	Description
Number of pages to mirror (Nombre de pages à dupliquer)	Nombre maximum de pages à mettre en miroir.
Maximum depth (Profondeur maximale)	Limite le nombre de liens que Nessus suivra pour chaque page de démarrage.
Start page (Page de démarrage)	URL de la première page qui sera testée. Si plusieurs pages sont requises, utilisez deux points pour les séparer (par exemple « <code>/:/php4:/base</code> »).
Excluded items regex (regex des éléments exclus)	Exclut certaines parties du site Web de l'analyse. Par exemple, pour exclure le répertoire « <code>/manual</code> » et tous les Perl CGI, utilisez la valeur suivante pour ce champ : <code>(^/manual) (\.pl (\?.*) ?\$)</code> .
Follow dynamic pages (Suivre les pages dynamiques)	Si cette option est sélectionnée, Nessus suivra les liens dynamiques et peut excéder les paramètres définis ci-dessus.

Internal Web Server / Preferences / Web mirroring

Preference Type: Web mirroring

Number of pages to mirror:

Maximum depth:

Start page:

Excluded items regex:

Follow dynamic pages:

[Save](#) [Cancel](#)

Windows Compliance Checks (Contrôles de conformité Windows)

Le menu « **Windows Compliance Checks** » (Contrôles de conformité Windows) permet aux clients commerciaux de télécharger en amont les fichiers d'audit de configuration Microsoft Windows qui seront utilisés pour déterminer si un système testé satisfait aux normes de conformité spécifiées. Jusqu'à cinq stratégies peuvent être sélectionnées à la fois.

Internal Web Server / Preferences / Windows Compliance Checks

Preference Type: Windows Compliance Checks

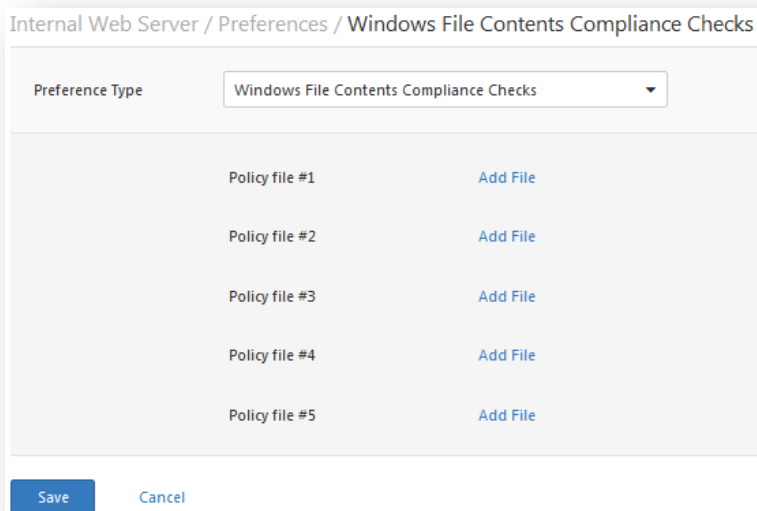
Policy file #1	Add File
Policy file #2	Add File
Policy file #3	Add File
Policy file #4	Add File
Policy file #5	Add File

[Save](#) [Cancel](#)

Windows File Contents Compliance Checks (Contrôles de conformité du contenu des fichiers Windows)

Le menu « **Windows File Contents Compliance Checks** » (Contrôles de conformité du contenu des fichiers Windows) permet aux clients commerciaux de télécharger en amont des fichiers d'audit basés sur Windows qui recherchent un type de contenu particulier sur un système (par exemple cartes de crédit, numéro de sécurité sociale) afin de déterminer la conformité avec la réglementation de l'entreprise ou les normes tierces.

Lorsque toutes les options ont été configurées de la façon souhaitée, cliquez sur « **Submit** » (Soumettre) pour enregistrer la stratégie et revenir à l'onglet Politiques. Vous pouvez à tout moment cliquer sur « **Edit** » (Éditer) pour apporter des changements à une stratégie déjà créée, ou sur « **Delete** » (Supprimer) pour éliminer complètement une stratégie.



Pour plus d'informations

Tenable a créé plusieurs autres documents expliquant en détail l'installation, le déploiement, la configuration, l'utilisation et les tests d'ensemble de Nessus. Ceux-ci sont répertoriés ci-dessous :

- **Nessus 5.2 Installation and Configuration Guid** (Guide d'installation et de configuration Nessus 5.2) : explication pas à pas des étapes d'installation et de configuration
- **Nessus Credential Checks for Unix and Windows** (Contrôles des identifiants Nessus pour Unix et Windows) : informations sur la façon d'effectuer des scans de réseau authentifiés avec le scanner de vulnérabilité Nessus
- **Nessus Compliance Checks** (Contrôles de conformité Nessus) : guide de haut niveau pour comprendre et exécuter les contrôles de conformité au moyen de Nessus et de SecurityCenter
- **Nessus Compliance Checks Reference** (Référence pour les contrôles de conformité Nessus) : guide complet sur la syntaxe des contrôles de conformité Nessus
- **Nessus v2 File Format** (Format de fichier Nessus v2) : décrit la structure du format de fichier `.nessus`, qui a été introduit avec Nessus 3.2 et NessusClient 3.2
- **Nessus 5.0 REST Protocol Specification** (Caractéristique du protocole Nessus 5.0 REST) : décrit le protocole REST et l'interface dans Nessus
- **Nessus 5 and Antivirus** (Nessus 5 et les antivirus) : présente le mode d'interaction des progiciels de sécurité les plus courants avec Nessus et fournit des conseils et des solutions qui favoriseront une meilleure coexistence des logiciels, sans compromettre la sécurité ou faire obstacle à vos opérations de scan des vulnérabilités
- **Nessus 5 and Mobile Device Scanning** (Nessus 5 et scan des périphériques mobiles) : décrit comment Nessus s'intègre à Microsoft Active Directory et aux serveurs MDM (serveurs de gestion des périphériques mobiles) afin d'identifier les périphériques mobiles utilisés sur le réseau

- **Nessus 5.0 and Scanning Virtual Machines** (Nessus 5.0 et scan des machines virtuelles) : présente comment utiliser le scanner de vulnérabilité Nessus de Tenable Network Security pour effectuer l'audit de la configuration des plateformes virtuelles et des logiciels exécutés sur ces plateformes
- **Strategic Anti-malware Monitoring with Nessus, PVS, and LCE** (Surveillance stratégique des programmes malveillants avec Nessus, PVS et LCE) : décrit comment la plateforme USM de Tenable peut détecter divers logiciels malveillants, identifier les infections de ces programmes malveillants et en déterminer l'étendue
- **Patch Management Integration** (Intégration de la gestion de correctifs) : décrit comment Nessus et SecurityCenter peuvent tirer parti des identifiants pour les systèmes de gestion de correctif IBM TEM, Microsoft WSUS et SCCM, VMware Go et Red Hat Network Satellite afin d'effectuer l'audit de correctifs sur les systèmes pour lesquels les identifiants peuvent ne pas être mis à la disposition du scanner Nessus
- **Real-Time Compliance Monitoring** (Surveillance de conformité en temps réel) : décrit comment les solutions de Tenable peuvent être utilisées pour faciliter le respect d'un grand nombre de types de règlements gouvernementaux et financiers
- **Tenable Products Plugin Families** (Familles de plugins des produits Tenable) : fournit la description et le résumé des familles de plugins pour Nessus, Log Correlation Engine et Passive Vulnerability Scanner
- **SecurityCenter Administration Guide** (Guide d'administration de SecurityCenter)

D'autres ressources en ligne sont répertoriées ci-dessous :

- Forum de discussions Nessus : <https://discussions.nessus.org/>
- Blog Tenable : <http://www.tenable.com/blog>
- Podcast Tenable : <http://www.tenable.com/podcast>
- Vidéos d'exemples d'utilisation : <http://www.youtube.com/user/tenablesecurity>
- Feed Twitter Tenable : <http://twitter.com/tenablesecurity>

N'hésitez pas à contacter Tenable aux adresses support@tenable.com et sales@tenable.com, ou consultez notre site internet sur <http://www.tenable.com/>.

À propos de Tenable Network Security

Les solutions de Tenable Network Security sont utilisées par plus de 20 000 organisations, dont tous les services du Département de la Défense des États-Unis (DOD, Department of Defense) ainsi que de nombreuses grandes entreprises internationales et agences gouvernementales, pour prendre une longueur d'avance sur les vulnérabilités, menaces et risques de conformité émergents. Ses solutions Nessus et SecurityCenter continuent de définir la norme pour l'identification des vulnérabilités, la prévention des attaques et le respect de nombreuses exigences réglementaires. Pour plus d'informations, veuillez consulter www.tenable.com.

SIÈGE MONDIAL

Tenable Network Security

7021 Columbia Gateway Drive

Suite 500

Columbia, Maryland 21046

410.872.0555

www.tenable.com

