Guía del usuario de Nessus 5.0 HTML5

4 de diciembre de 2012

(Revisión 4)

Índice

Introducción

Este documento describe cómo usar la **interfaz de usuario (UI) de Nessus** de Tenable Network Security. Envíe sus comentarios y sugerencias por correo electrónico a support@tenable.com.

La UI de Nessus es una interfaz web del analizador de vulnerabilidades Nessus. Para usar el cliente, debe contar con un analizador Nessus en funcionamiento y que haya sido implementado, y debe tener conocimientos sobre su uso.

Estándares y convenciones

Este documento ha sido traducido de una versión originalmente redactada en inglés. Parte del texto aparece en inglés para mostrar cómo está representado en el producto.

Los nombres de archivos, demonios y archivos ejecutables se indican con la fuente **courier negrita** en toda la documentación, por ejemplo **gunzip**, **httpd** y **/etc/passwd**.

Las opciones de líneas de comandos y las palabras clave también se indican con fuente **courier negrita**. Los ejemplos de líneas de comandos pueden incluir o no el indicador de la línea de comandos y el texto de salida de los resultados del comando. Los ejemplos de líneas de comando mostrarán el comando que se ejecuta en **courier negrita** para indicar lo que el usuario escribió, y el resultado de muestra generado por el sistema se indicará en courier (normal). A continuación se presenta un ejemplo de ejecución del comando **pwd** de Unix:

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

Las consideraciones y notas importantes se resaltan con este símbolo y cuadros de texto grises.

Las sugerencias, los ejemplos y las prácticas recomendadas se resaltan con este símbolo y con letras blancas en cuadros de texto azules.

Descripción general de la ui de Nessus

Descripción

La interfaz de usuario (UI) de Nessus es una interfaz web del analizador Nessus que está compuesta por un simple servidor HTTP y cliente web, por lo que no requiere la instalación de ningún software además del servidor Nessus. A partir de Nessus 4 todas las plataformas usan la misma base de código, con lo cual se elimina la mayoría de los errores específicos de las plataformas y se permite una implementación más rápida de las nuevas características. Las características principales son las siguientes:

- Genera archivos **.nessus** que son usados por los productos de Tenable como estándar para directivas de análisis y datos de vulnerabilidades.
- Una sesión de directivas, una lista de destinos y los resultados de varios análisis pueden almacenarse todos juntos en un único archivo **.nessus** que se puede exportar fácilmente. Consulte la Guía de formatos de archivos de Nessus para obtener más detalles.
- La interfaz gráfica de usuario (GUI) muestra los resultados de los análisis en tiempo real, por lo que no deberá esperar que finalice el análisis para ver los resultados.
- Brinda una interfaz unificada para el analizador Nessus que es independiente de la plataforma base. Existen las mismas funcionalidades en Mac OS X, Windows y Linux.

- Los análisis seguirán ejecutándose en el servidor, aun si usted se desconecta por cualquier motivo.
- Los informes de los análisis de Nessus pueden cargarse mediante la UI de Nessus y compararse con otros informes.

Plataformas admitidas

Dado que la UI de Nessus es un cliente web, puede ejecutarla en cualquier plataforma mediante un explorador web actual.

Se logra una experiencia óptima de la interfaz de usuario web de Nessus si se usa Microsoft Internet Explorer 9 o 10, Mozilla Firefox 15.x, Google Chrome 16.x, Opera 12.x o Apple Safari 5.x.

Instalación

La administración de los usuarios del servidor Nessus 5 se lleva a cabo mediante una interfaz web o SecurityCenter, y ya no es necesario usar un NessusClient independiente. Los NessusClient independientes aún se conectarán y operarán el analizador, pero no recibirán actualizaciones ni soporte técnico.

Consulte la Guía de instalación y configuración de Nessus 5.0 para obtener instrucciones sobre cómo instalar Nessus. A partir de Nessus 5.0 se necesita Oracle Java (anteriormente conocido como Java de Sun Microsystems) para la función de informes en PDF.

Operación

Descripción general

Nessus proporciona una interfaz simple pero versátil para administrar las actividades de análisis de vulnerabilidades.

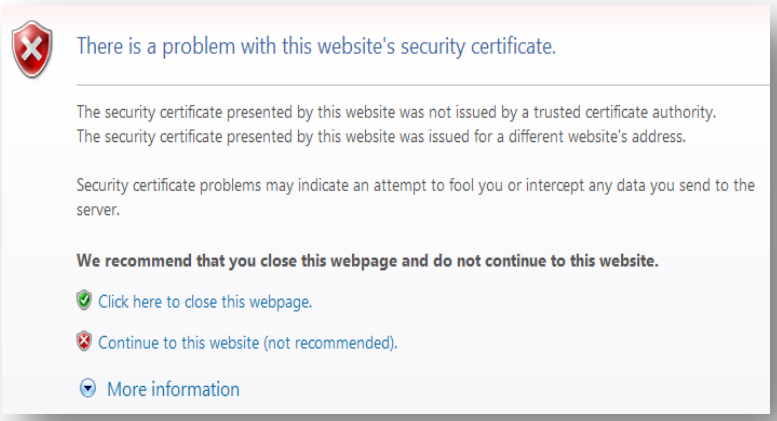
Conexión con la GUI de Nessus

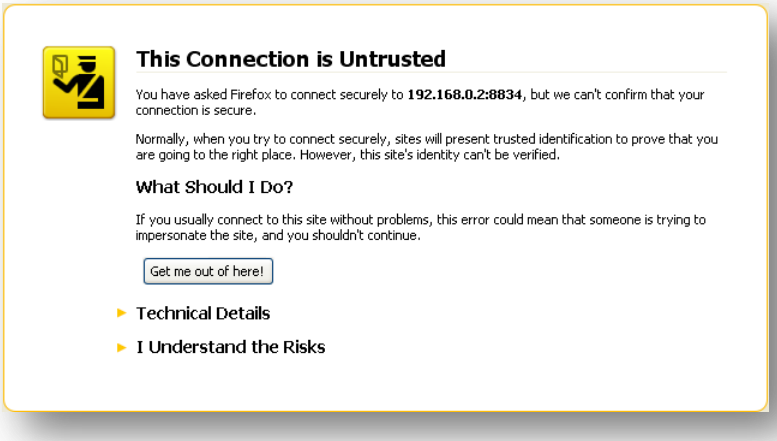
Para iniciar la GUI de Nessus HTML5, realice lo siguiente:

- Abra el explorador web de su preferencia.
- Introduzca `https://[server IP]:8834/html5.html#/` en la barra de navegación.

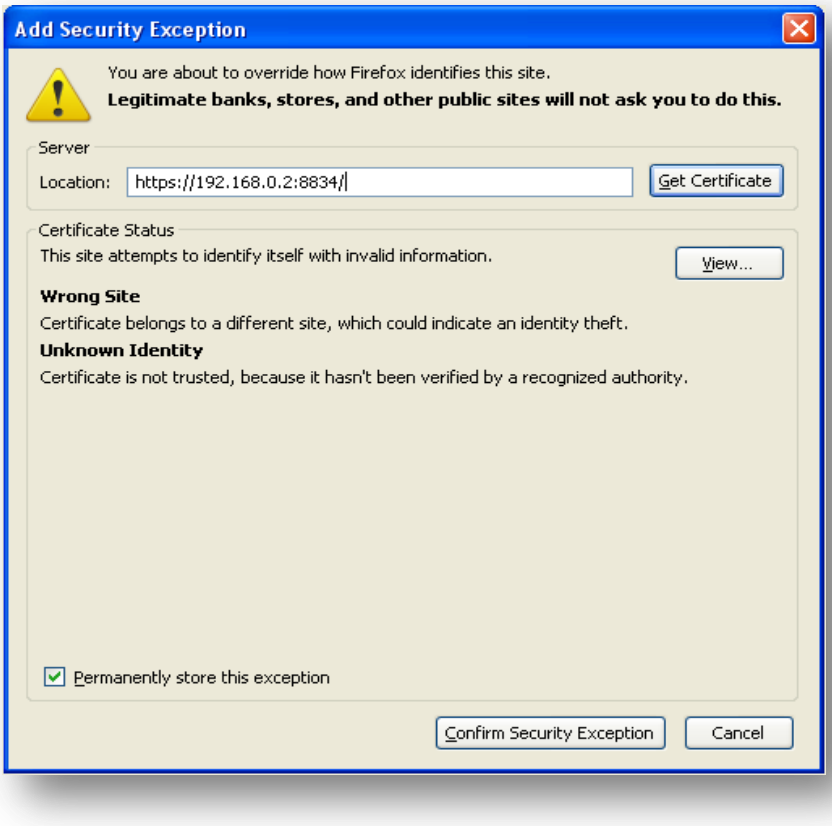
Asegúrese de conectarse con la interfaz de usuario mediante HTTPS, ya que no se admiten las conexiones HTTP sin cifrar.

La primera vez que intente conectarse con la interfaz de usuario de Nessus, la mayoría de los exploradores web mostrará un error que indicará que el sitio no es confiable a raíz del certificado SSL autofirmado:



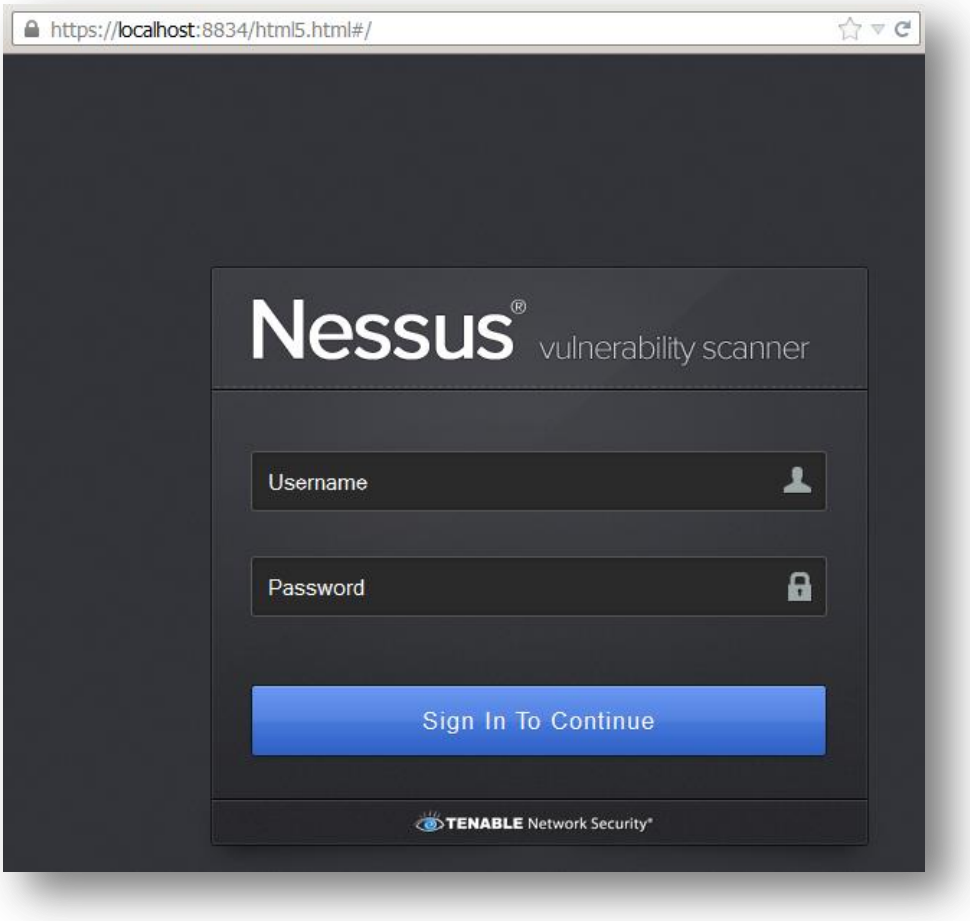


Los usuarios de Microsoft Internet Explorer pueden hacer clic en “Continue to this website (not recommended)” (Pasar a este sitio web [no recomendado]) para cargar la interfaz de usuario de Nessus. Los usuarios de Firefox 3.x a 16.x pueden hacer clic en “I Understand the Risks” (Entiendo los riesgos) y luego, en “Add Exception…” (Agregar excepción) para que aparezca el cuadro de diálogo de excepción de sitios:

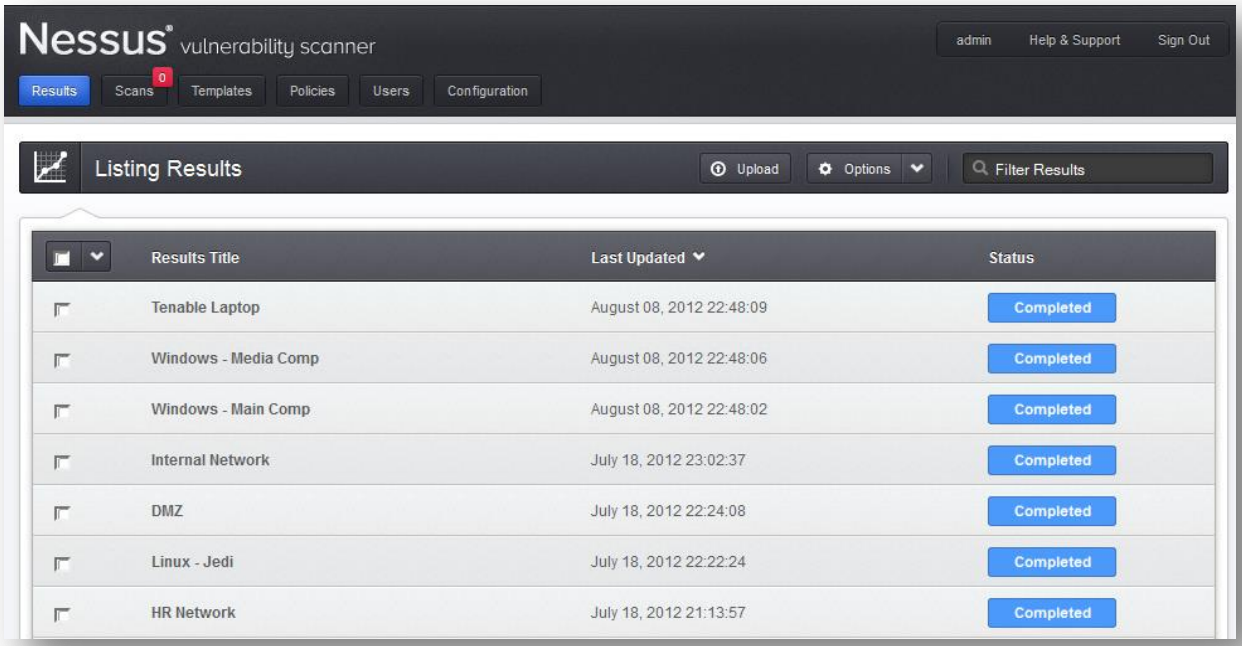


Verifique que la barra “Location:” (Ubicación:) refleje la dirección URL del servidor Nessus, y haga clic en “**Confirm Security Exception**” **(Confirmar excepción de seguridad)**. Para obtener información sobre cómo instalar un certificado SSL personalizado, consulte la Guía de instalación y configuración de Nessus.

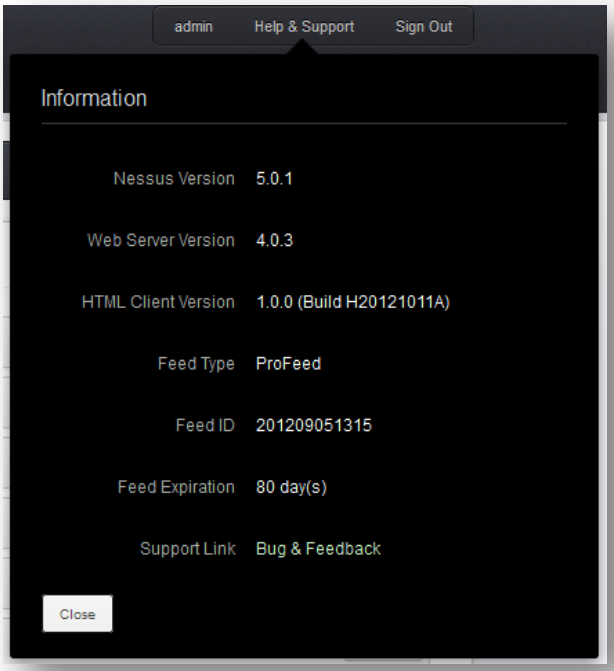
Después de que el explorador haya confirmado la excepción, aparecerá la siguiente pantalla de presentación:



Realice una autenticación mediante la cuenta administrativa y la contraseña que había creado durante el proceso de instalación. Después de que la autenticación se haya realizado correctamente, la UI presentará menús para consultar informes, llevar a cabo análisis y administrar directivas. Los usuarios administrativos también verán opciones de administración de usuarios y de configuración del analizador Nessus:



En todo momento durante el uso de Nessus estarán presentes las opciones de la esquina superior izquierda. La notación "admin" que se observa en la esquina superior derecha de la captura de pantalla anterior representa la cuenta con la que se inició sesión en ese momento. Si hace clic en esta, podrá cambiar la contraseña actual. El botón "**Help & Support**" **(Ayuda y soporte)** muestra información acerca de la instalación de Nessus, como la versión, la versión del servidor web, la versión del cliente HTML, el tipo de fuente, la identificación de la fuente y la fecha de vencimiento de la fuente, y un enlace para enviar informes de errores o comentarios generales. "**Sign out**" **(Cerrar sesión)** finalizará la sesión actual.



La interfaz HTML5 tiene varias teclas de acceso rápido que permiten una navegación rápida con el teclado en las secciones más importantes de la interfaz y ejecutar las tareas comunes. Estas teclas pueden usarse en cualquier momento, desde cualquier parte de la interfaz:

Interfaz principal	
R	Resultados
S	Análisis
T	Plantillas
P	Directivas
U	Usuarios
C	Configuración
Shift + Flecha izquierda/derecha	Pasar a la pestaña izquierda o derecha
Shift + S	Nuevo análisis
Vistas de lista	
Shift + Flecha arriba/abajo	Mover la selección hacia arriba o hacia abajo
Shift + Enter	Abrir la entrada seleccionada

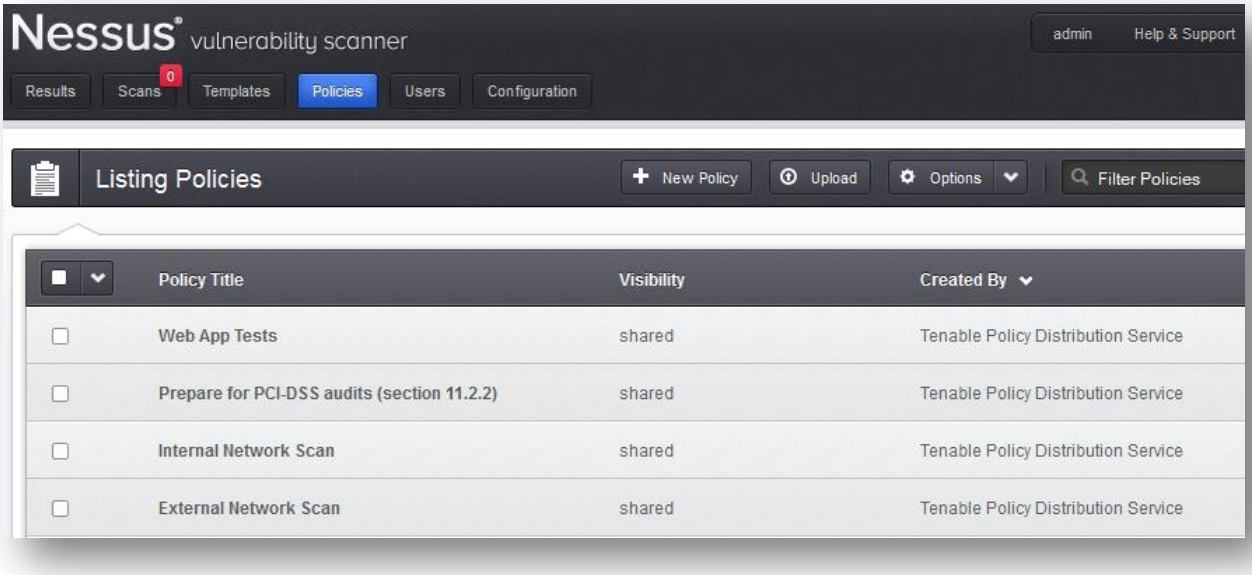
Vista de resultados	
Shift + U	Subir informe
Esc	Regresar a la lista de resultados
Flecha izquierda/derecha	Vulnerabilidad anterior/siguiente en modo Details (Detalles)
D	Eliminar resultado seleccionado
Vista de análisis	
N	Nuevo análisis
Vista de directivas	
Shift + U	Subir nueva directiva
Vista de usuarios	
N	Nuevo usuario

Descripción general de directivas

Una “directiva” de Nessus está compuesta por opciones de configuración que se relacionan con la realización de un análisis de vulnerabilidades. Entre estas opciones se incluyen, sin limitarse a ellas, las siguientes:

- Parámetros que controlan aspectos técnicos del análisis, tales como tiempos de espera, cantidad de hosts, tipo de analizador de puertos, etc.
- Credenciales para análisis locales (por ejemplo, Windows, SSH), análisis de bases de datos Oracle autenticados, autenticación basada en HTTP, FTP, POP, IMAP o Kerberos.
- Especificaciones de análisis pormenorizadas en función de plugins o familias.
- Comprobaciones de directivas de compatibilidad de bases de datos, nivel de detalle de los informes, configuración de los análisis para la detección de servicios, comprobaciones de compatibilidad de Unix, etc.

Directivas predeterminadas



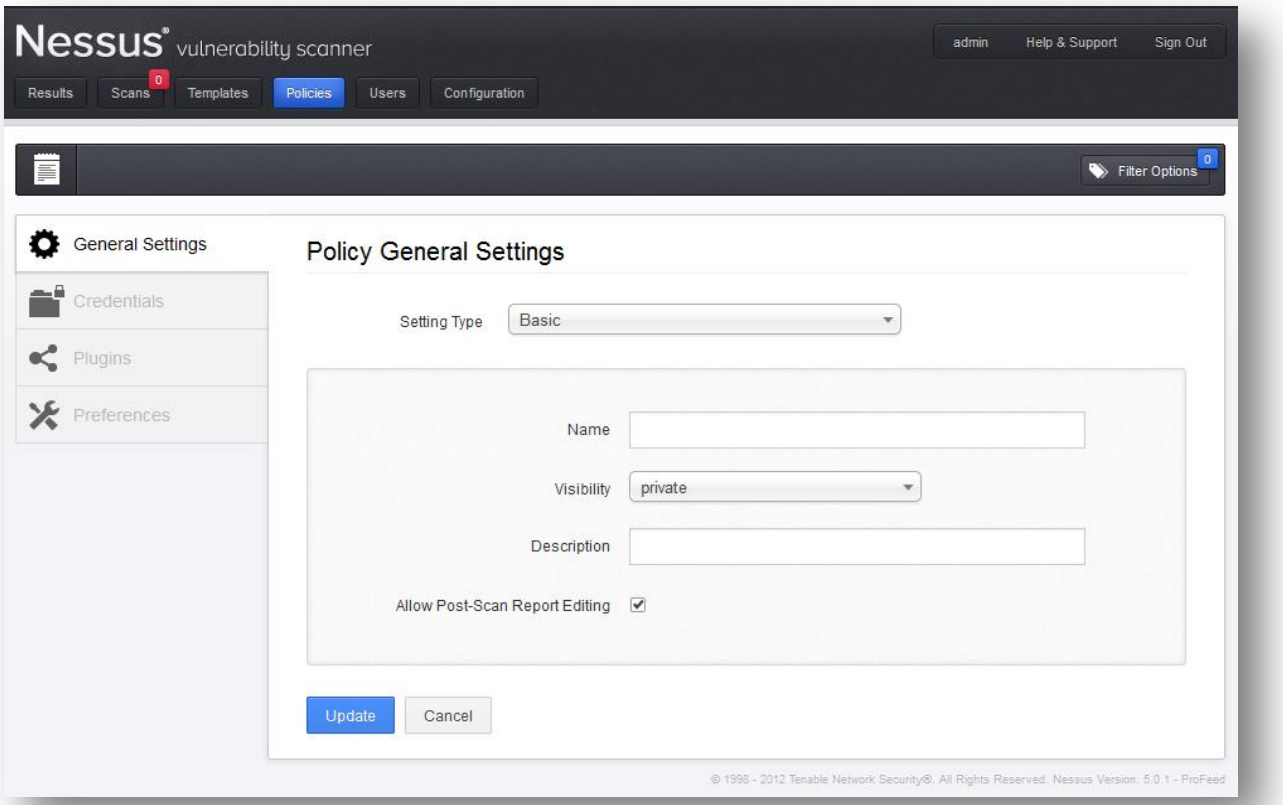
Nessus se distribuye con varias directivas predeterminadas proporcionadas por Tenable Network Security, Inc. Se brindan como plantillas para ayudarle a crear directivas personalizadas para su organización o usarlas en su estado actual para iniciar análisis básicos de sus recursos. Asegúrese de leer y comprender las directivas predeterminadas antes de usarlas en análisis de sus recursos.

Nombre de la directiva	Descripción
"External Network Scan" (Análisis de red externo)	Esta directiva está ajustada para analizar hosts con conexiones externas, que normalmente presentan menor cantidad de servicios para la red. En esta directiva se habilitan los plugins relacionados con vulnerabilidades de aplicaciones web conocidas (familias de plugins CGI Abuses y CGI Abuses: XSS). Además, se analizan los 65 536 puertos (incluso el puerto 0 por medio de un plugin independiente) para cada destino.
"Internal Network Scan" (Análisis de red interno)	Esta directiva está ajustada para ofrecer un mejor rendimiento, teniendo en cuenta que se puede usar para analizar redes internas grandes con muchos hosts, varios servicios expuestos y sistemas incrustados, como las impresoras. Las comprobaciones de la CGI se deshabilitan y se analiza un conjunto de puertos estándar, no los 65 535.
"Web App Tests" (Pruebas de aplicaciones web)	Si desea analizar sus sistemas e indicar que Nessus detecte vulnerabilidades conocidas y desconocidas en sus aplicaciones web, esta es la directiva de análisis adecuada para usted. En esta directiva se habilita la capacidad de "pruebas de exploración de vulnerabilidades mediante datos aleatorios" de Nessus, que hará que Nessus recorra todos los sitios web descubiertos y busque las vulnerabilidades que se encuentren en cada parámetro, incluidos XSS, SQL, inserción de comandos y varios más. Esta directiva identificará problemas a través de HTTP y HTTPS.
"Prepare for PCI DSS audits" (Preparar para auditorías de PCI DSS)	Esta directiva habilita las comprobaciones de compatibilidad PCI DSS incorporadas que comparan los resultados de los análisis con los estándares de PCI, y genera un informe sobre su posición de compatibilidad. Es muy importante destacar que un análisis de compatibilidad de resultado correcto no garantiza la compatibilidad ni una infraestructura segura. Las organizaciones que se preparen para una evaluación según PCI DSS pueden usar esta directiva a fin de preparar su red y sus sistemas para tener compatibilidad PCI DSS.

Si quiere usar una directiva predeterminada de Tenable como base para su propia directiva personalizada, utilice la función Copy (Copiar). Al modificar una directiva predeterminada, esta se convertirá en propiedad del usuario y ya no aparecerá en la interfaz.

Creación de una nueva directiva

Una vez que se haya conectado con la UI de un servidor Nessus, puede crear una directiva personalizada haciendo clic en la opción "**Policies**" (Directivas) de la barra situada en la parte superior, y luego en el botón "**+ New Policy**" (+ Nueva directiva) de la derecha. Aparecerá la pantalla para agregar directivas como se muestra a continuación:



Observe que hay cuatro fichas de configuración: "**General Settings**" **(Configuración general)**, "**Credentials**" **(Credenciales)**, "**Plugins**" **(Plugins)** y "**Preferences**" **(Preferencias)**. En la mayoría de los entornos no es necesario modificar las opciones de configuración predeterminadas, pero estas proporcionan un control más pormenorizado de la operación del analizador Nessus. Estas fichas se describen a continuación.

Configuración general

La ficha "**General Settings**" **(Configuración general)** le permite nombrar la directiva y configurar las operaciones relacionadas con el análisis. Existen cuatro elementos del menú desplegable que controlan el comportamiento del analizador:

La pantalla "**Basic**" **(Opciones básicas)** se usa para definir aspectos de la directiva en sí:

Opción	Descripción
“Name” (Nombre)	Establece el nombre que aparecerá en la UI de Nessus para identificar la directiva.
“Visibility” (Visibilidad)	Controla si la directiva se *comparte* con otros usuarios o se mantiene *privada* para su uso exclusivo. Solo los usuarios administrativos pueden compartir directivas.
“Description” (Descripción)	Se usa para brindar una breve descripción de la directiva de análisis, que es habitualmente una buena opción para resumir el propósito general (por ejemplo, “El servidor web analiza sin comprobaciones locales ni servicios que no sean HTTP”).
“Allow Post-Scan Report Editing” (Permitir edición después del análisis)	Cuando está activada, esta característica les permite a los usuarios eliminar elementos del informe. Al hacer un análisis de cumplimiento de las normas u otros tipos de auditoría, debe desactivarse para poder probar que el análisis no fue alterado.

El menú “**Port Scanning**” **(Análisis de puertos)** controla las opciones relacionadas con el análisis de puertos, como los métodos e intervalos de puertos:

La opción “**Port Scan Range**” **(Intervalo de análisis de puertos)** indica al analizador que tenga como destino un intervalo de puertos específico. Se permiten los siguientes valores:

Valor	Description
“default” (valor predeterminado)	Si se emplea la palabra clave “default” (valor predeterminado), Nessus analizará aproximadamente 4 790 puertos comunes. La lista de puertos se puede encontrar en el archivo `nessus-services`.
“all” (todos)	Si se emplea la palabra clave “all” (todos), Nessus analizará los 65 535 puertos.
“Custom List” (Lista personalizada)	Mediante una lista de puertos o intervalos de puertos delimitada por comas, se puede seleccionar un intervalo de puertos personalizado. Por ejemplo, se permiten “21,23,25,80,110” o “1-1024,8080,9000-9200”. Si especifica “1-65535”, se analizarán todos los puertos. También puede especificar un intervalo dividido específico para cada protocolo. Por ejemplo, si quiere analizar un intervalo de puertos diferente para TCP y UDP en la misma directiva, debe especificar “T:1-1024,U:300-500”. También puede especificar un conjunto de puertos a analizar para ambos protocolos y los intervalos específicos de cada protocolo por separado ("1-1024,T:1024-65535,U:1025"). Si está analizando un solo protocolo, seleccione solo el analizador de puertos correspondiente y especifique los puertos normalmente.

Estas son las otras opciones disponibles:

Opción	Descripción
“Consider Unscanned Ports as Closed” (Considerar los puertos no analizados como cerrados)	Si no se analiza un puerto con un analizador de puertos seleccionado (por ejemplo, debido a que se encuentra fuera del intervalo especificado), Nessus considerará que está cerrado.

“Nessus SNMP Scanner” (Analizador SNMP de Nessus)	Ordena a Nessus que analice los destinos en busca de un servicio SNMP. Nessus estimará la configuración SNMP correspondiente durante un análisis. Si el usuario proporciona la configuración en “Preferences” (Preferencias), esto permitirá que Nessus pruebe mejor el host remoto y produzca resultados de auditoría más detallados. Por ejemplo, existen muchas comprobaciones para enrutadores de Cisco que determinan las vulnerabilidades existentes mediante el examen de la versión de la cadena SNMP devuelta. Esta información es necesaria para estas auditorías.
“Nessus UDP Scanner” (Analizador UDP de Nessus)	Esta opción activa el analizador UDP incorporado de Nessus para identificar los puertos UDP abiertos en los destinos.  UDP es un protocolo “sin estado”, lo cual significa que la comunicación no se realiza con diálogos de protocolo de enlace. La comunicación basada en UDP no es confiable en todo momento y, dada la naturaleza de los servicios UDP y los dispositivos de filtrado, no siempre se los puede detectar de manera remota.
“netstat portscanner (SSH)” (Analizador de puertos netstat [SSH])	Esta opción usa **`netstat`** para comprobar la existencia de puertos abiertos desde el equipo local. Depende de la disponibilidad del comando **`netstat`** mediante una conexión SSH con el destino. Este análisis está destinado a sistemas basados en Unix y requiere credenciales de autenticación.
“Ping the remote host” (Efectuar pings al host remoto)	Esta opción permite que se efectúen pings a hosts remotos en varios puertos para determinar si están activos.
“Netstat Portscanner (WMI)” (Analizador de puertos netstat [WMI])	Esta opción usa **`netstat`** para comprobar la existencia de puertos abiertos desde el equipo local. Depende de la disponibilidad del comando **`netstat`** mediante una conexión WMI con el destino. Este análisis está destinado a sistemas basados en Windows y requiere credenciales de autenticación.  Un análisis basado en WMI emplea **`netstat`** para determinar los puertos abiertos, con lo cual se omiten los intervalos de puertos especificados. Si cualquier enumerador de puertos (**`netstat`** o SNMP) es satisfactorio, el intervalo de puertos será “all” (Todos). Sin embargo, Nessus aún cumplirá con la opción “consider unscanned ports as closed” si está seleccionada.
“Nessus TCP Scanner” (Analizador TCP de Nessus)	Use el analizador TCP incorporado de Nessus para identificar los puertos TCP abiertos en los destinos. Este analizador está optimizado y posee algunas características de ajuste automático.  En algunas plataformas (por ejemplo, Windows y Mac OS X), si selecciona este analizador Nessus utilizará el analizador SYN para evitar problemas de rendimiento graves específicos de esos sistemas operativos.
“Nessus SYN Scanner” (Analizador SYN de Nessus)	Use el analizador SYN incorporado de Nessus para identificar los puertos TCP abiertos en los destinos. Los análisis SYN constituyen un método de análisis de puertos usado con frecuencia, y generalmente se consideran un poco menos intrusivos que los análisis TCP. El analizador envía un paquete SYN al puerto, espera la respuesta SYN-ACK y determina el estado del puerto de acuerdo con la respuesta o la ausencia de esta.

El menú “**Performance**” **(Rendimiento)** brinda opciones que controlan la cantidad de análisis que se iniciarán. Estas opciones son tal vez las más importantes al configurar un análisis, ya que producen el mayor efecto en los tiempos de análisis y la actividad de la red.

Opción	Descripción
“Max Checks Per Host” (Comprobaciones máximas por host)	Esta opción limita la cantidad máxima de comprobaciones que realizará un analizador Nessus respecto de un único host cada vez.
“Max Hosts Per Scan” (Hosts máximos por análisis)	Esta opción limita la cantidad máxima de hosts que examinará un analizador Nessus al mismo tiempo.
“Network Receive Timeout (seconds)” (Tiempo de espera de recepción de red [segundos])	Se encuentra establecido en cinco segundos de forma predeterminada. Es el tiempo que esperará Nessus para obtener una respuesta del host, a menos que se especifique lo contrario en un plugin. Si realiza un análisis con una conexión lenta, es recomendable que ajuste esta opción en una cantidad de segundos mayor.
“Max Simultaneous TCP Sessions Per Host” (Sesiones TCP simultáneas máximas por host)	Esta opción limita la cantidad máxima de sesiones TCP establecidas para un único host.  Esta opción de aceleración de TCP controla también la cantidad de paquetes por segundo que el analizador SYN enviará finalmente (por ejemplo, si esta opción está definida en 15, el analizador SYN enviará 1 500 paquetes por segundo como máximo).
“Max Simultaneous TCP Sessions Per Scan” (Sesiones TCP simultáneas máximas por análisis)	Esta opción limita la cantidad máxima de sesiones TCP establecidas para todo el análisis, independientemente de la cantidad de hosts que se analicen.  En el caso de los analizadores Nessus instalados en hosts de Windows XP, Vista y 7, este valor debe establecerse en 19 o menos para obtener resultados precisos.
“Reduce Parallel Connections on Congestion” (Reducir conexiones en paralelo si hay congestión)	Esta opción permite que Nessus detecte cuándo envía demasiados paquetes y el canal de la red está por alcanzar su capacidad máxima. Si esto se detecta, Nessus acelerará el análisis para tener en cuenta y paliar la congestión. Una vez que haya disminuido la congestión, Nessus intentará automáticamente usar otra vez el espacio disponible en el canal de la red.
“Use Kernel Congestion Detection (Linux Only)” (Usar detección de congestión de kernel [Linux únicamente])	Permite que Nessus supervise la CPU y demás funciones internas en busca de congestiones y reduzca la actividad en función de ello. Nessus siempre intentará usar todos los recursos que estén disponibles. Esta característica solo se encuentra disponible para los analizadores Nessus que se implementen en Linux.

El menú “**Advanced**” **(Opciones avanzadas)** define además opciones relacionadas con la forma en que se debe comportar el análisis:

Opción	Descripción
“Safe Checks” (Comprobaciones seguras)	Safe Checks deshabilitará todos los plugins que puedan producir efectos adversos en el host remoto.
“Silent Dependencies” (Dependencias silenciosas)	Si esta opción está marcada, la lista de dependencias no se incluirá en el informe. Si desea incluirla, desmarque la casilla.

“Log Scan Details to Server” (Guardar detalles del análisis en el registro del servidor)	Guarda detalles adicionales del análisis en el registro del servidor Nessus (`nessusd.messages`), como el inicio de los plugins, el final de los plugins o si se elimina un plugin. El registro resultante se puede emplear para confirmar que se usaron plugins específicos y que se analizaron hosts específicos.
“Stop Host Scan on Disconnect” (Detener el análisis de host en caso de desconexión)	Si se marca la opción, Nessus dejará de realizar análisis si detecta que el host no responde. Esto puede producirse si los usuarios apagan su equipo durante un análisis, o si un host deja de responder después de que un plugin de denegación de servicio o un mecanismo de seguridad (por ejemplo, IDS) haya comenzado a bloquear el tráfico a un servidor. Continuar con los análisis en estos equipos producirá un tráfico innecesario en toda la red y demorará el análisis.
“Avoid Sequential Scans” (Evitar análisis secuenciales)	De manera predeterminada, Nessus analiza una lista de direcciones IP en orden secuencial. Si la opción está marcada, Nessus analizará la lista de hosts en orden aleatorio. Normalmente, esto resulta de utilidad para ayudar a distribuir el tráfico de la red que se dirige a una subred en particular durante análisis extensos.
“Designate Hosts by their DNS Name” (Designar hosts por su nombre DNS)	Usa el nombre del host en lugar de la dirección IP para generar los informes.

El intervalo especificado para un análisis de puertos se aplicará tanto a los análisis TCP como a los UDP.

Credenciales

La ficha “**Credentials**”, **(Credenciales)** cuya imagen se incluye más adelante, le permite configurar el analizador Nessus para que use credenciales de autenticación durante los análisis. Al configurar las credenciales, Nessus podrá realizar una variedad más amplia de comprobaciones que produzcan resultados de análisis más precisos.

El elemento de menú desplegable “**Windows credentials**” (**Credenciales de Windows)** posee parámetros de configuración para proporcionar a Nessus información tal como el nombre de la cuenta SMB, la contraseña y el nombre del dominio. El Bloque de mensajes del servidor (SMB) es un protocolo de uso compartido de archivos que permite a los equipos compartir información de forma transparente en la red. Proporcionar esta información a Nessus le permitirá buscar información local desde un host de Windows remoto. Por ejemplo, usar credenciales permite a Nessus determinar si se han aplicado revisiones de seguridad importantes. No es necesario modificar otros parámetros SMB de la configuración predeterminada.

Cuando se configuran varias cuentas de SMB, Nessus intentará iniciar sesión con las credenciales suministradas de manera secuencial. Una vez que Nessus pueda autenticarse con un conjunto de credenciales, comprobará las siguientes credenciales proporcionadas, pero solo las utilizará si se otorgan privilegios administrativos cuando las cuentas anteriores brindaron acceso al usuario.

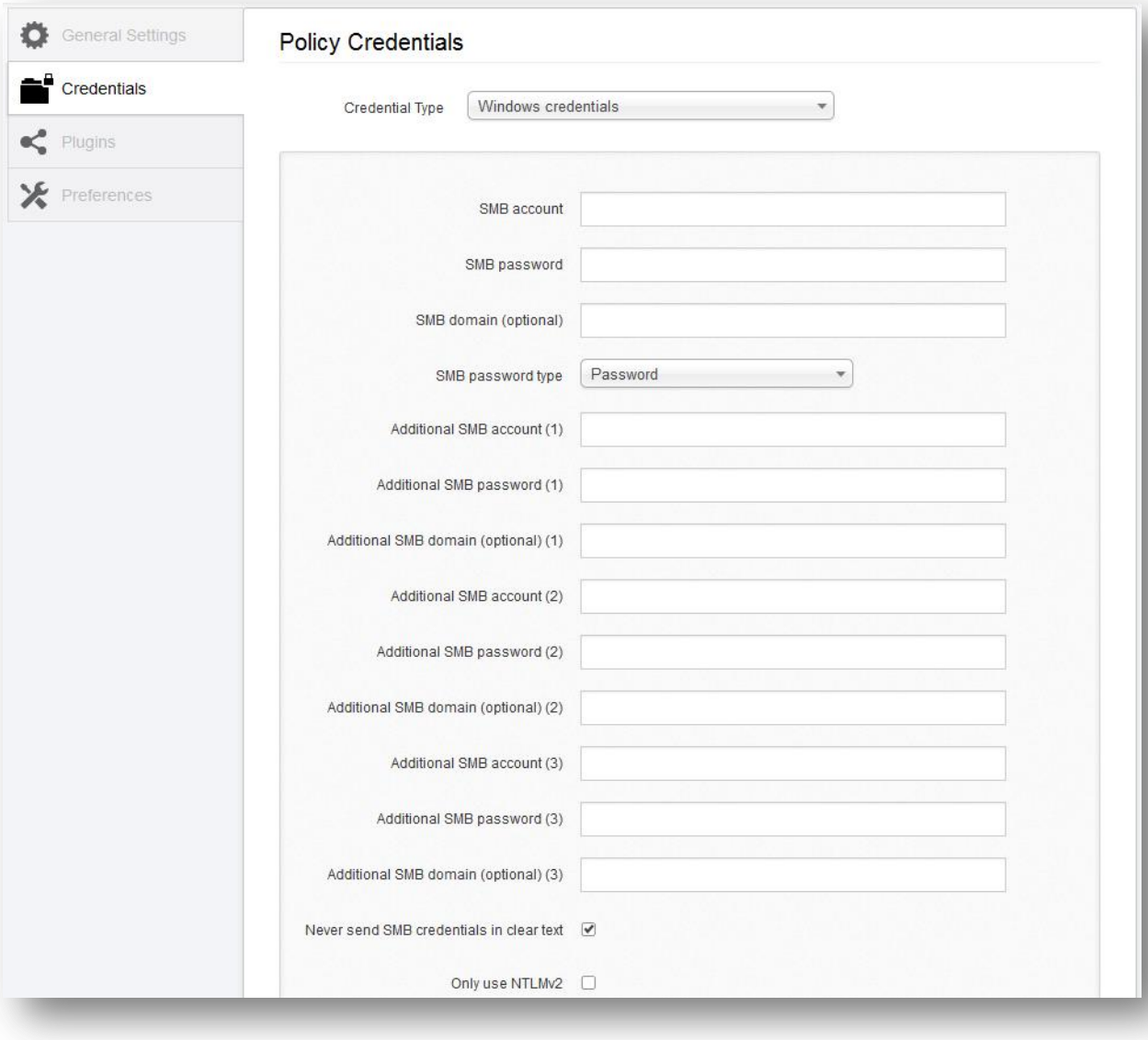
Algunas versiones de Windows le permiten crear una nueva cuenta y designarla como “administrador”. Estas cuentas no son siempre adecuadas para llevar a cabo análisis con credenciales. Tenable recomienda que se utilice la cuenta administrativa original, llamada “Administrador”, para análisis con credenciales, a fin de garantizar que se permita el acceso total. En algunas versiones de Windows esta cuenta puede estar oculta. La cuenta de administrador real puede hacerse visible ejecutando un comando de DOS con privilegios administrativos y escribiendo el siguiente comando:

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

Si se crea una cuenta SMB de mantenimiento con privilegios de administrador limitados, Nessus puede analizar varios dominios de forma sencilla y segura.

Tenable recomienda que los administradores de redes consideren la creación de cuentas de dominio específicas para facilitar la realización de pruebas. Nessus incluye una variedad de comprobaciones de seguridad para Windows NT, 2000, Server 2003, XP, Vista, Windows 7 y Windows 2008 que son más precisas si se proporciona una cuenta de dominio. En la mayoría de los casos, si no se brinda una cuenta, Nessus efectivamente intenta varias comprobaciones.

El servicio Registro remoto de Windows permite que equipos remotos con credenciales accedan al registro del equipo en el que se realiza la auditoría. Si el servicio no está en ejecución, no será posible leer claves y valores del registro, **incluso si se cuenta con todas las credenciales**. Consulte en el blog de Tenable la publicación denominada "Dynamic Remote Registry Auditing - Now you see it, now you don't!" ("Auditoría dinámica de Registro remoto: ahora se ve, ahora no") para obtener más información. Este servicio **debe iniciarse** para que el análisis con credenciales de Nessus haga la auditoría completa de un sistema usando credenciales.



Los usuarios pueden seleccionar "**SSH settings**" **(Configuración de SSH)** del menú desplegable e introducir las credenciales para el análisis de sistemas de Unix. Estas credenciales se usan a fin de obtener información local de los sistemas remotos de Unix para auditorías de revisiones o comprobaciones de compatibilidad. Hay un campo para

introducir el nombre de usuario de SSH para la cuenta que realizará las comprobaciones en el sistema de Unix de destino, junto con la contraseña SSH o la pareja de claves pública y privada de SSH. También existe un campo para introducir la frase de contraseña para la clave SSH, de ser necesaria.

Nessus 4 admite los algoritmos de cifrado **`blowfish-cbc`**, **`aes-cbc`**, y **`aes-ctr`**.

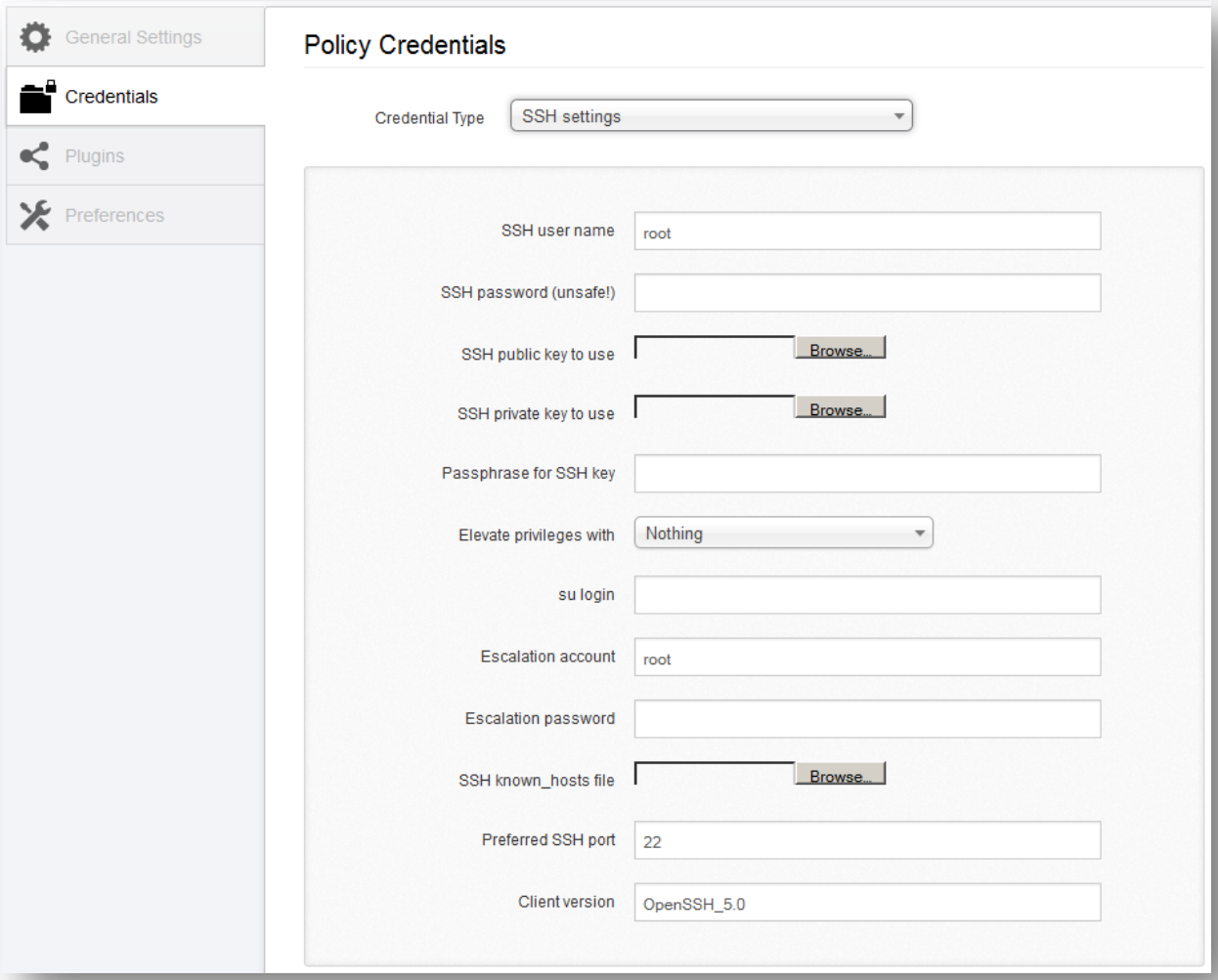
Los análisis con credenciales más eficaces son aquellos que se realizan cuando las credenciales proporcionadas tienen privilegios “root” (raíz / usuario principal). Como muchos sitios no permiten un inicio de sesión remoto como raíz, los usuarios de Nessus pueden invocar “**`su`**”, “**`sudo`**”, “**`su+sudo`**”, o “**`dzdo`**” con una contraseña separada para una cuenta que se haya configurado para tener privilegios “**`su`**” o “**`sudo`**”. Además, Nessus puede escalar privilegios en los dispositivos Cisco seleccionando “**`Cisco 'enable'`**”.

Nessus puede usar el acceso basado en clave de SSH para efectuar una autenticación en un servidor remoto. Si un archivo **`known_hosts`** de SSH se encuentra disponible y se proporciona como parte de la directiva de análisis, Nessus solo intentará iniciar sesión en los hosts en este archivo. Por último, la opción “Preferred SSH port” (Puerto SSH preferido) se puede ajustar para ordenar a Nessus que se conecte con SSH si se ejecuta en un puerto que no sea el 22.

Nessus cifra todas las contraseñas almacenadas en las directivas. Sin embargo, entre las prácticas recomendadas se incluye el uso de claves de SSH para la autenticación, en lugar de contraseñas de SSH. Esta acción ayuda a garantizar que el nombre de usuario y contraseña que está usando para auditar sus servidores de SSH conocidos no se use también para intentar iniciar sesión en un sistema que quizás no esté bajo su control. En ese caso, no se recomienda usar contraseñas de SSH a menos que sea absolutamente necesario.

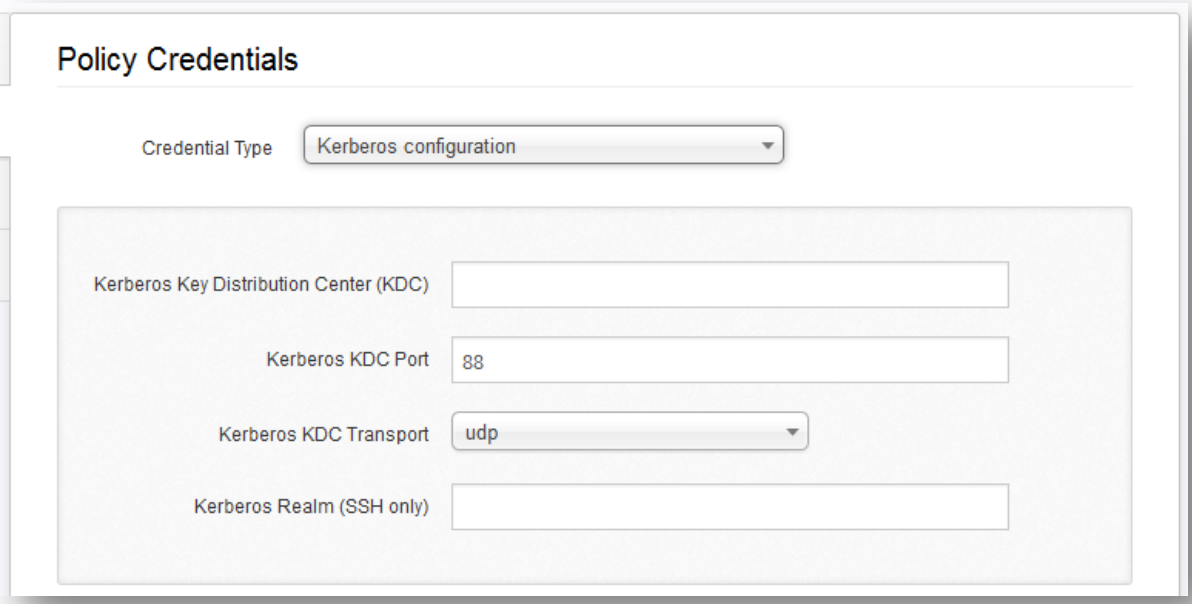
Nessus también admite una opción “su+sudo” que se puede usar en caso de que un sistema no permita privilegios de inicio de sesión remoto para cuentas con privilegios.

La siguiente captura de pantalla muestra las opciones de SSH disponibles. El menú desplegable “Elevate privileges with” (Elevar privilegios con) brinda varios métodos para aumentar los privilegios después de la autenticación.

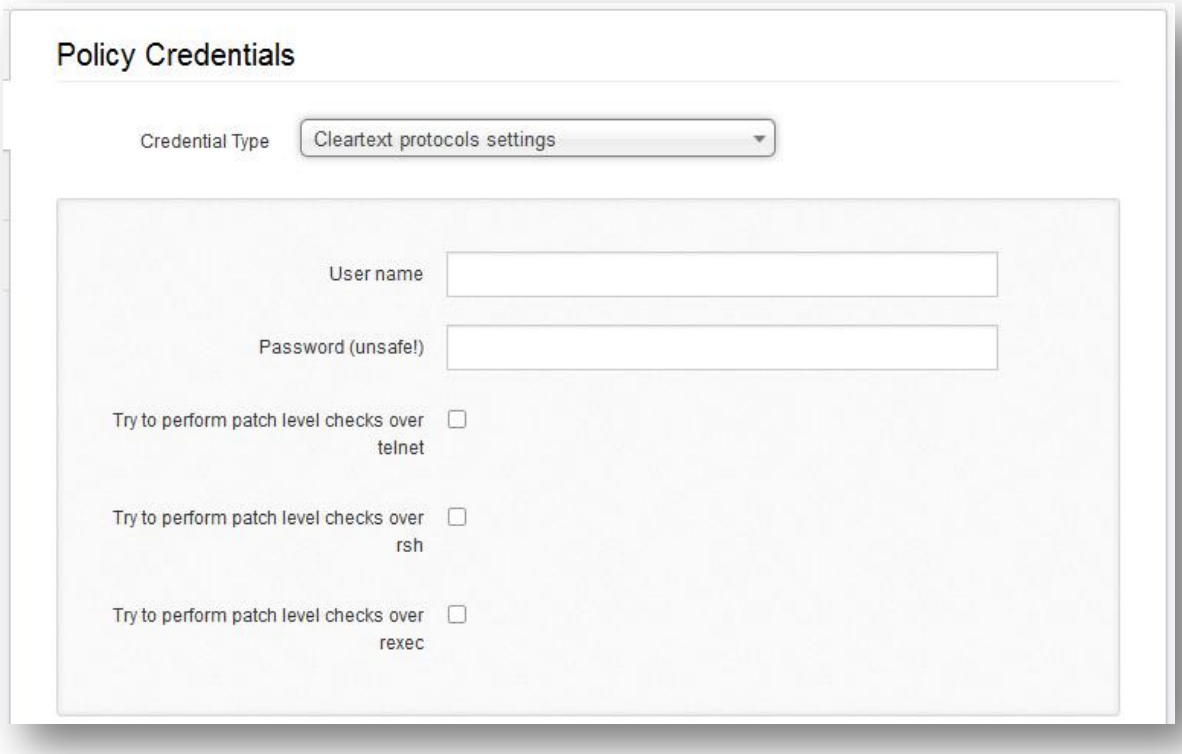


Si se debe utilizar otra cuenta que no sea `root` para escalar privilegios, puede especificarse en "**Escalation account**" **(Cuenta de escalación)** con la "**Escalation password**" **(Contraseña de escalación)**.

"**Kerberos configuration**" **(Configuración de Kerberos)** le permite especificar credenciales mediante claves Kerberos desde un sistema remoto:



Por último, si no se encuentra disponible un método seguro para realizar comprobaciones con credenciales, los usuarios pueden forzar a Nessus para que intente llevar a cabo comprobaciones en protocolos no seguros mediante la configuración del elemento del menú desplegable "**Cleartext protocol settings**" **(Opciones de protocolo de texto no cifrado)**. Los protocolos de texto no cifrado admitidos para esta opción son **telnet**, **rsh** y **rexec**. Además, hay casillas de verificación para ordenar específicamente a Nessus que intente ejecutar comprobaciones de nivel de revisión en protocolos no seguros:

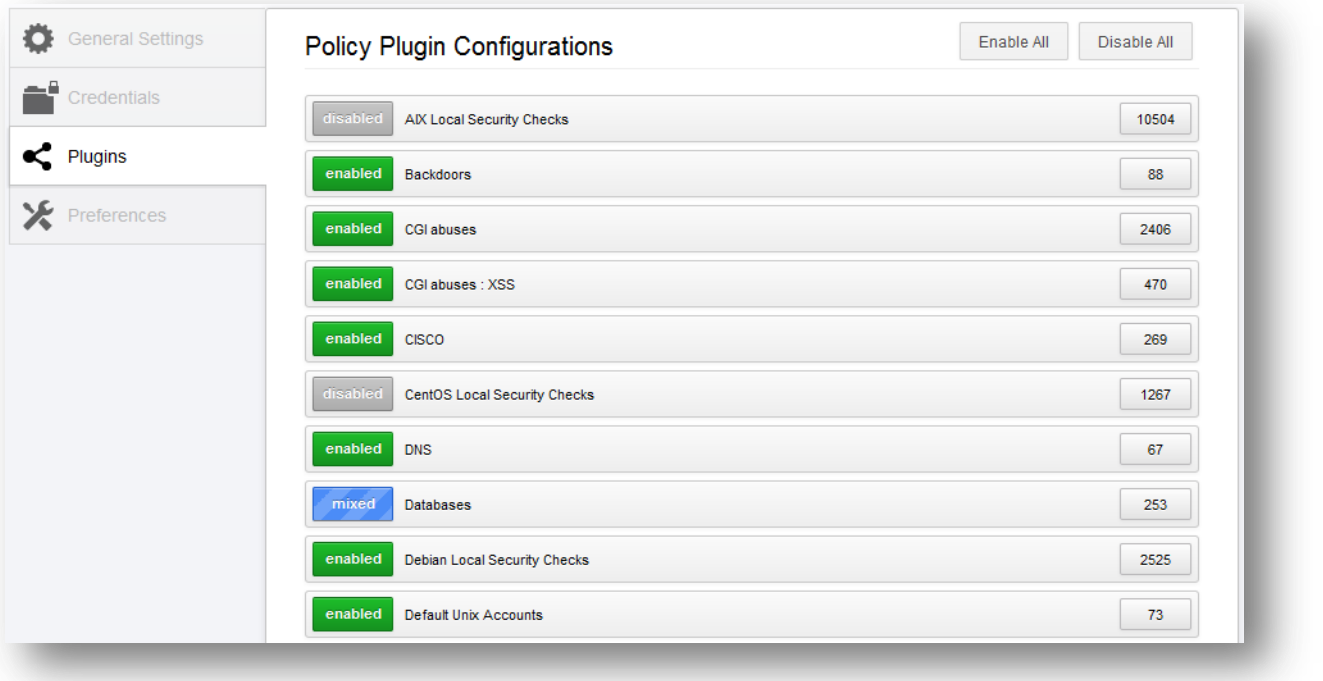


De forma predeterminada, todas las contraseñas (y la directiva en sí) se encuentran cifradas. Si la directiva se guarda en un archivo `.nessus` y luego ese archivo se copia en una instalación diferente de Nessus, ninguna de las contraseñas de la directiva podrá ser usada por el segundo analizador Nessus, ya que no podrá descifrarlas.

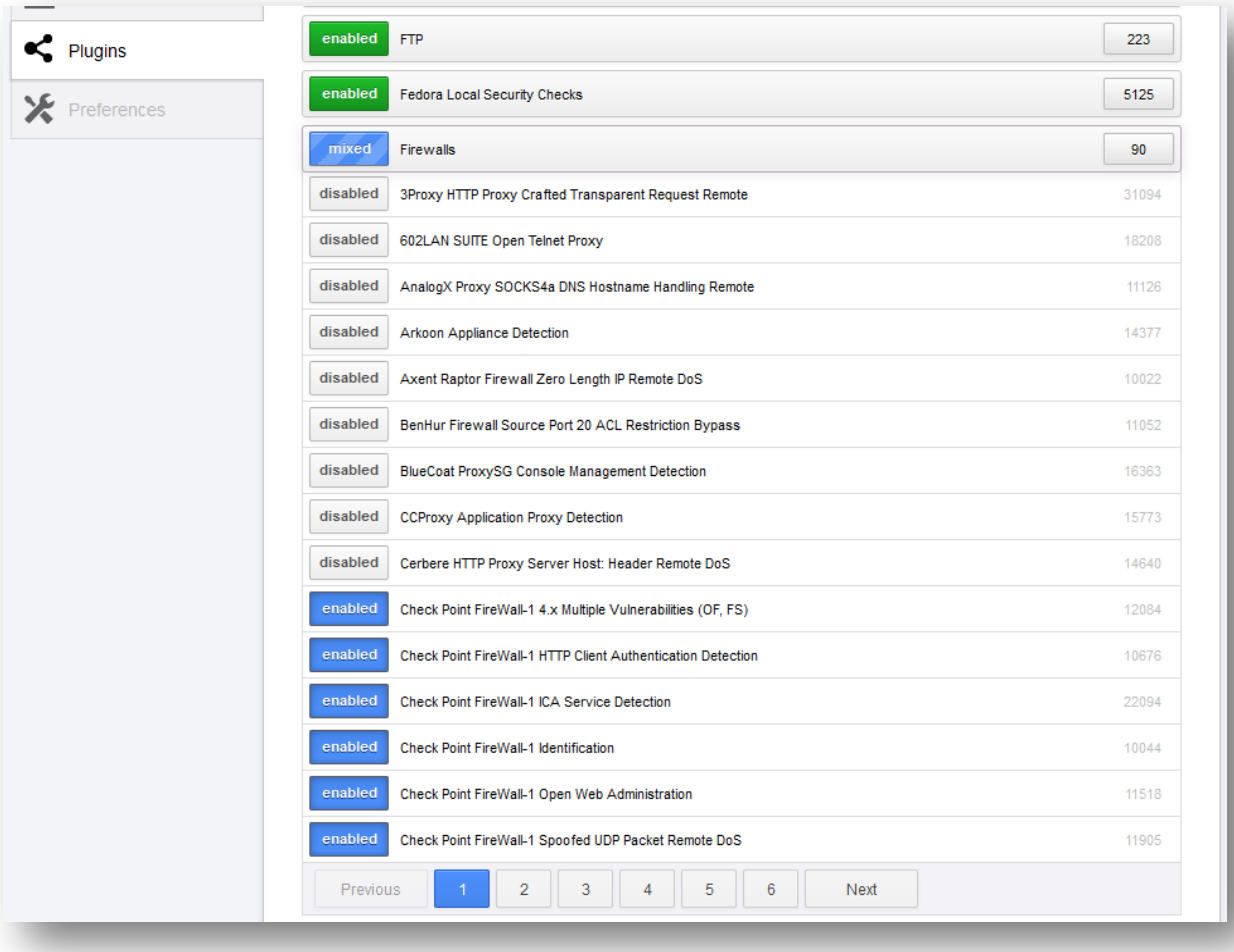
No se recomienda usar credenciales de texto no cifrado de forma alguna. Si las credenciales se envían de manera remota (por ejemplo, mediante un análisis de Nessus), estas podrían ser interceptadas por cualquier persona con acceso a la red. Siempre que sea posible, emplee mecanismos de autenticación cifrados.

Plugins

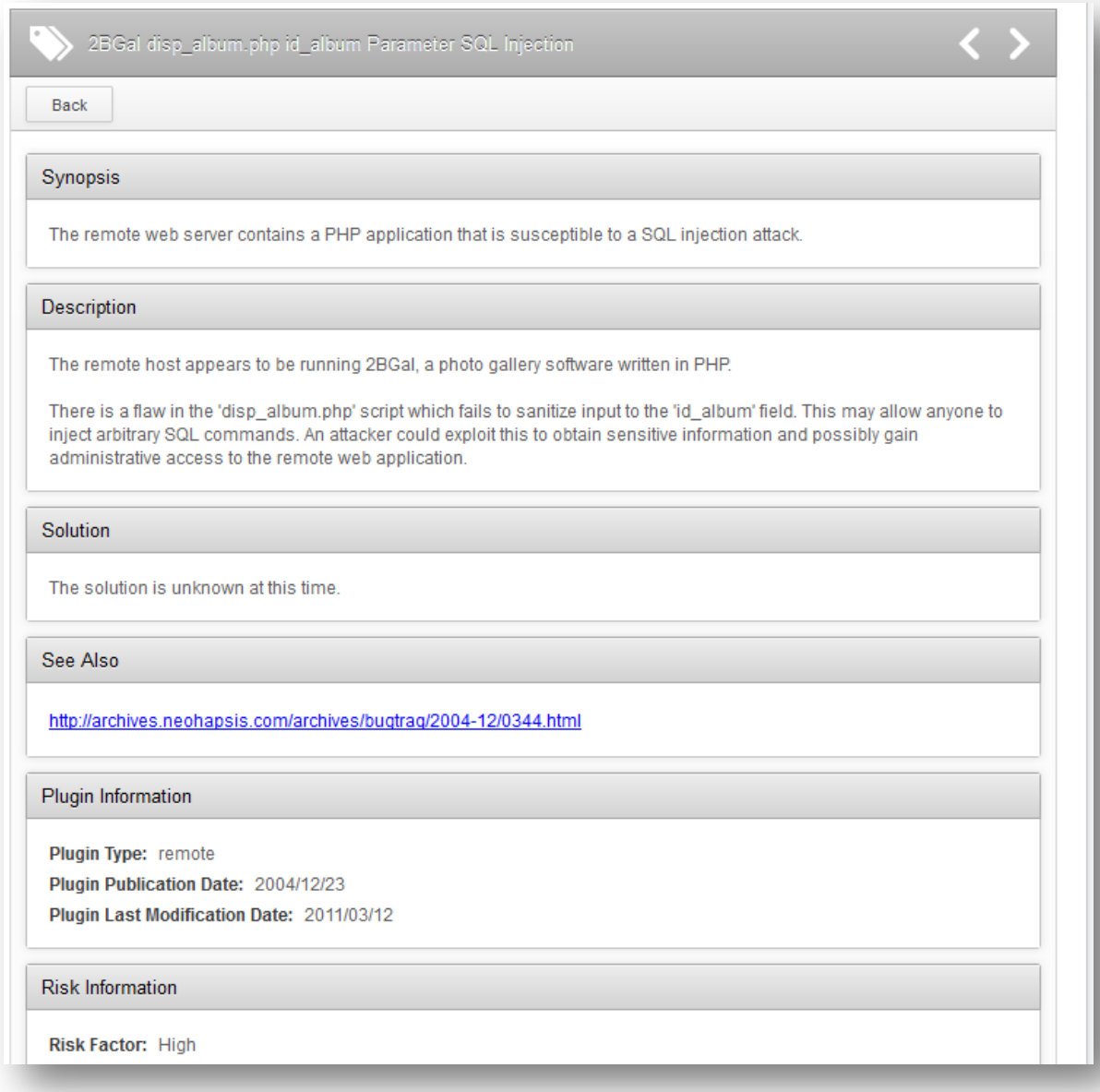
La ficha "**Plugins**" permite al usuario elegir comprobaciones de seguridad específicas por familia de plugins o comprobaciones individuales.



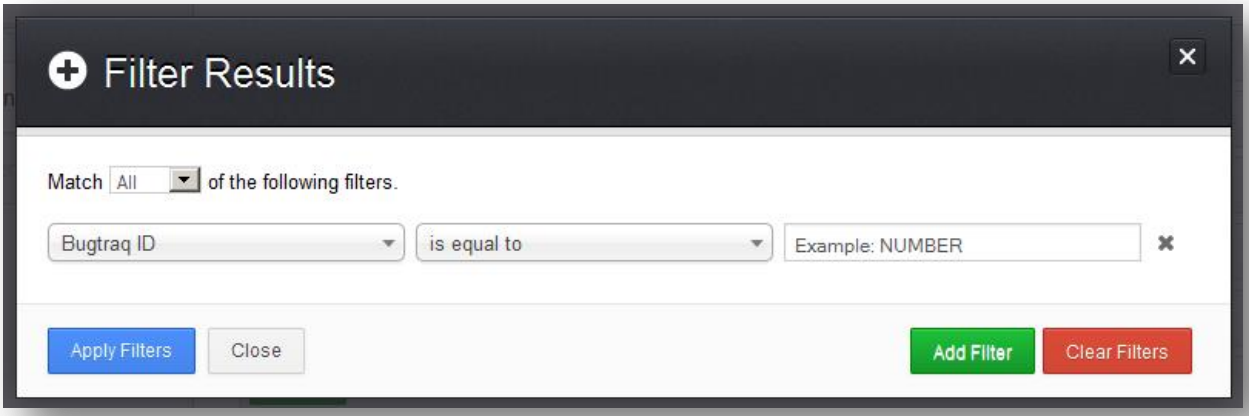
Al hacer clic en la familia de plugins puede habilitar (verde) o deshabilitar (gris) toda la familia. Seleccione una familia para ver la lista de sus plugins. Se pueden habilitar o deshabilitar plugins individuales para crear directivas de análisis muy específicas. Si una familia tiene algunos plugins deshabilitados, se pondrá en azul y mostrará el mensaje “mixed” (mezclados) para indicar que solo algunos plugins están habilitados. Si hace clic en la familia del plugin se cargará toda la lista de plugins y se permitirá la selección pormenorizada según sus preferencias de análisis:



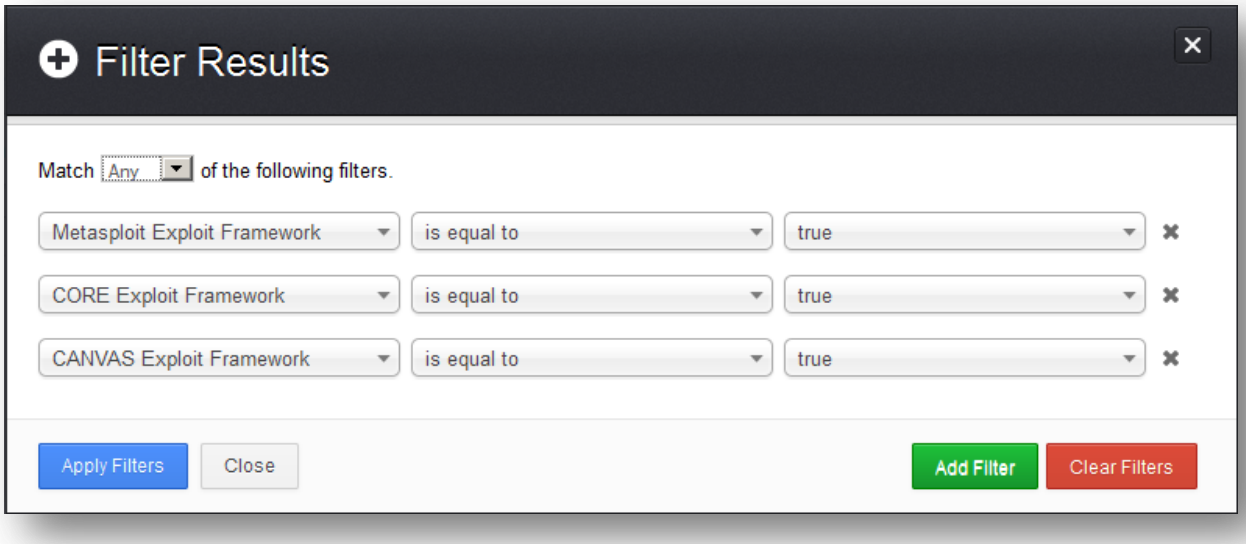
Si selecciona un plugin específico, el resultado de ese plugin aparecerá como se visualiza en un informe. La sinopsis y la descripción brindarán más detalles de la vulnerabilidad que se está examinando. Desplácese hacia abajo en su explorador para ver información de la solución, más referencias que estén disponibles, información de riesgo, información de vulnerabilidades de seguridad y toda referencia cruzada informativa o base de datos de vulnerabilidades.


2BGal disp_album.php id_album Parameter SQL Injection
Back
Synopsis
The remote web server contains a PHP application that is susceptible to a SQL injection attack.
Description
The remote host appears to be running 2BGal, a photo gallery software written in PHP.
There is a flaw in the 'disp_album.php' script which fails to sanitize input to the 'id_album' field. This may allow anyone to inject arbitrary SQL commands. An attacker could exploit this to obtain sensitive information and possibly gain administrative access to the remote web application.
Solution
The solution is unknown at this time.
See Also
http://archives.neohapsis.com/archives/bugtraq/2004-12/0344.html
Plugin Information
Plugin Type: remote
Plugin Publication Date: 2004/12/23
Plugin Last Modification Date: 2011/03/12
Risk Information
Risk Factor: High

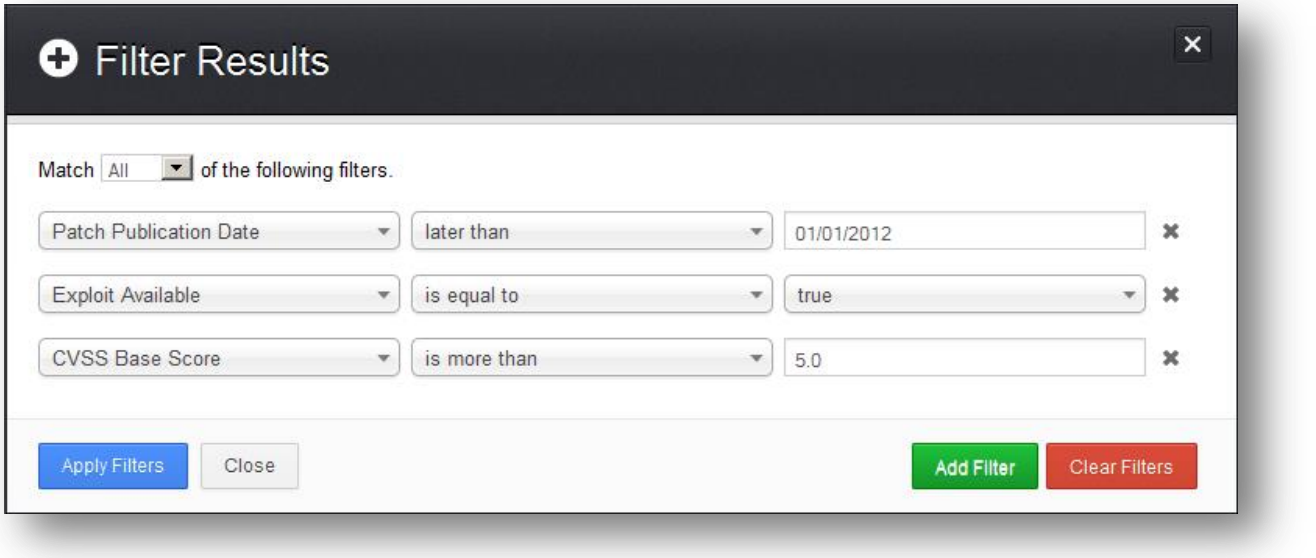
En la parte superior de la página de la familia de plugins, puede crear filtros para elaborar una lista de plugins a incluir en la directiva. Los filtros permiten un control pormenorizado de la selección de plugins. Pueden establecerse varios filtros en una sola directiva. Para crear un filtro, haga clic en el botón "**Filter Options**" **(Opciones de filtros)**:



Cada filtro creado le da varias opciones para restringir una búsqueda. Los criterios de filtro pueden basarse en "Any" (Cualquiera), en cuyo caso cualquier criterio dará coincidencias, o "All" (Todos), en cuyo caso todos los criterios del filtro deben cumplirse. Por ejemplo, si queremos una directiva que solo incluya plugins que tengan una vulnerabilidad de seguridad asociada en un marco de trabajo de vulnerabilidad de seguridad comercial, creamos tres filtros y marcamos "Any" (Cualquiera) para los criterios:



Si queremos crear una directiva que contenga plugins que coincidan con varios criterios, seleccionamos “All” y agregamos los filtros deseados. Por ejemplo, la directiva a continuación incluiría cualquier plugin publicado después del 1.º de enero de 2012 que tenga una vulnerabilidad de seguridad pública y una puntuación total CVSS mayor de 5.0:



Para obtener una lista completa de los criterios y detalles de los filtros, consulte la sección Filtros de informes de este documento.

Para usar filtros a fin de crear una directiva, se recomienda que comience por deshabilitar todos los plugins. Usando los filtros de plugins, deje solo los plugins que quiere en su directiva. Una vez que haya terminado, escoja cada familia de plugins y haga clic en “Enable Plugins” (Habilitar plugins).

Cuando se crea y guarda una directiva, esta registra todos los plugins que se seleccionan inicialmente. Cuando se reciben nuevos plugins a través de una actualización de la fuente de plugins, automáticamente se habilitarán si la familia con la que están relacionados está habilitada. Si la familia fue deshabilitada o parcialmente habilitada, los nuevos plugins de esa familia también se deshabilitarán automáticamente.

La familia “Denial of Service” (Denegación de servicio) contiene algunos plugins que podrían provocar interrupciones en una red si no se habilitó la opción “Safe Checks” (Comprobaciones seguras). Sin embargo, contiene algunas comprobaciones de utilidad que no producirán daño alguno. La familia “Denial of Service” (Denegación de servicio) se puede emplear junto con “Safe Checks” (Comprobaciones seguras) para garantizar que no se ejecute ningún plugin potencialmente peligroso. Sin embargo, se recomienda que la familia “Denial of Service” (Denegación de servicio) no se use en una red de producción.

Preferencias

La ficha “**Preferences**” **(Preferencias)** incluye medios para lograr un control pormenorizado de la configuración de las directivas de análisis. Si selecciona un elemento del menú desplegable, aparecerán elementos de configuración adicionales para esa categoría. Tenga en cuenta que se trata de una lista dinámica de opciones de configuración que depende de la fuente de plugins, las directivas de auditoría y otras funciones a las que tenga acceso el analizador Nessus conectado. Un analizador con una ProfessionalFeed puede contar con opciones de configuración más avanzadas que un analizador configurado con la HomeFeed. Esta lista también cambiará a medida que se añadan o modifiquen plugins.

Esta tabla proporciona una descripción general de todas las preferencias. Para obtener información más detallada de cada elemento de preferencia, consulte la sección Detalles de las preferencias de análisis de este documento.

Menú desplegable Preference	Descripción
“ADSI settings” (Configuración ADSI)	Active Directory Service Interfaces (Interfaces de servicio de Active Directory) toma información del servidor de administración de dispositivos móviles (MDM) relacionada con dispositivos Android e iOS.
“Apple Profile Manager API Settings” (Configuración API de Apple Profile Manager)	Característica de ProfessionalFeed que habilita los análisis de enumeración y vulnerabilidad de los dispositivos Apple iOS (por ejemplo, iPhone y iPad).
“Cisco IOS Compliance Checks” (Comprobaciones de compatibilidad de Cisco IOS)	Una opción de ProfessionalFeed que permite especificar un archivo de directiva para probar dispositivos con Cisco IOS según estándares de compatibilidad.
“Database Compliance Checks” (Comprobaciones de compatibilidad de bases de datos)	Una opción de ProfessionalFeed que permite especificar un archivo de directiva para probar bases de datos como DB2, SQL Server, MySQL y Oracle según estándares de compatibilidad.
“Database Settings” (Configuración de base de datos)	Opciones utilizadas para especificar el tipo de base de datos que se probará y qué credenciales se utilizarán.
“Do not scan fragile devices” (No analizar dispositivos frágiles)	Un conjunto de opciones que le ordena a Nessus **no** analizar determinados dispositivos, debido al mayor riesgo de bloqueo del destino.
“Global variable settings” (Opciones de configuración variables generales)	Una amplia variedad de opciones de configuración para Nessus.
“HTTP cookies import” (Importación de cookies HTTP)	Para las pruebas de aplicaciones web, esta preferencia especifica un archivo externo para importar las cookies HTTP y así permitir la autenticación de la aplicación.
“HTTP login page” (Página de inicio de sesión HTTP)	Configuración relacionada con la página de inicio de sesión para las pruebas de aplicación web.
“IBM iSeries Compliance Checks” (Comprobaciones de compatibilidad de IBM iSeries)	Una opción de ProfessionalFeed que permite especificar un archivo de directiva para probar sistemas IBM iSeries según estándares de compatibilidad.
“IBM iSeries Credentials” (Credenciales de IBM iSeries)	Donde se especifican las credenciales para los sistemas IBM iSeries.
“ICCP/COTP TSAP Addressing Weakness” (Punto débil de direccionamiento ICCP/COTP TSAP)	Una opción de ProfessionalFeed relacionada con las pruebas de Sistemas de control de supervisión y adquisición de datos (SCADA).
“Login configurations” (Configuraciones de inicio de sesión)	Donde se especifican las credenciales para pruebas de servicio básicas de HTTP, NNTP, FTP, POP e IMAP.
“Modbus/TCP Coil Access” (Acceso a bobinas de Modbus/TCP)	Una opción de ProfessionalFeed relacionada con las pruebas de Sistemas de control de supervisión y adquisición de datos (SCADA).
“Nessus SYN Scanner” (Analizador SYN de Nessus)	Opciones relacionadas con el analizador SYN incorporado.
“Nessus TCP Scanner” (Analizador TCP de Nessus)	Opciones relacionadas con el analizador TCP incorporado.

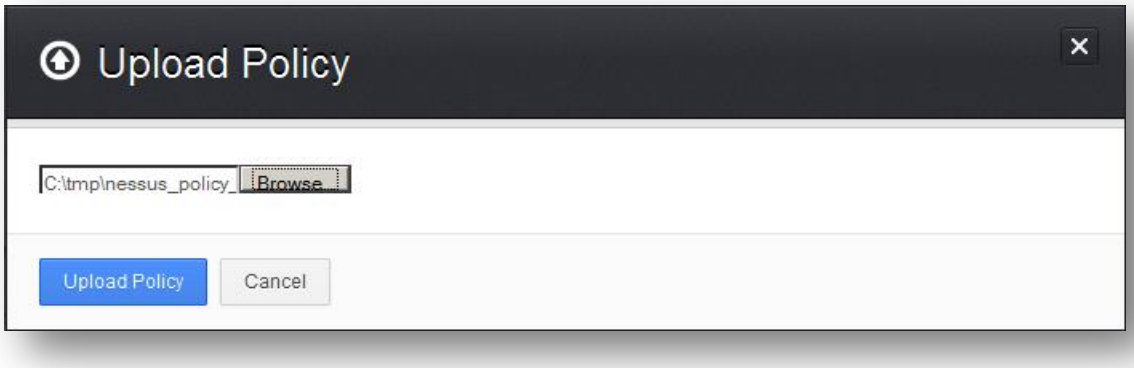
“News Server (NNTP) Information Disclosure” (Divulgación de información de servidores de noticias [NNTP])	Un conjunto de opciones para probar vulnerabilidades de divulgación de información de servidores NNTP.
“Oracle Settings” (Opciones de configuración de Oracle)	Opciones relacionadas con las pruebas de instalaciones de bases de datos Oracle.
“PCI DSS compliance” (Compatibilidad PCI DSS)	Una opción de ProfessionalFeed que le ordena a Nessus que compare los resultados del análisis con los PCI DSS standards (Estándares PCI DSS).
“Patch Management: Red Hat Satellite Server Settings” (Administración de revisiones: configuración de servidor Red Hat Satellite)	Opciones para integrar Nessus al servidor de administración de revisiones Red Hat Satellite. Consulte el documento "Patch Management Integration” (“Integración de administración de revisiones”) para obtener más información.
“Patch Management: SCCM Server Settings” (Administración de revisiones: configuración de servidor SCCM)	Opciones para integrar Nessus al servidor de administración de revisiones del System Center Configuration Manager (SCCM). Consulte el documento “Patch Management Integration” (“Integración de administración de revisiones”) para obtener más información.
“Patch Management: VMware Go Server Settings” (Administración de revisiones: configuración de VMware Go Server)	Opciones para integrar Nessus al servidor de administración de revisiones VMware Go Server (ex Shavlik). Consulte el documento “Patch Management Integration” (“Integración de administración de revisiones”) para obtener más información.
“Patch Management: WSUS Server Settings” (Administración de revisiones: configuración de servidor WSUS)	Opciones para integrar Nessus al servidor de administración de revisiones de Windows Server Update Service (WSUS). Consulte el documento “Patch Management Integration” (“Integración de administración de revisiones”) para obtener más información.
“Ping the remote host” (Efectuar pings al host remoto)	Configuración que controla la detección de redes por ping de Nessus.
“Port scanner settings” (Opciones de configuración de analizador de puertos)	Dos opciones que ofrecen más control sobre la actividad de análisis de puertos.
“SMB Registry : Start the Registry Service during the scan” (Registro SMB: iniciar el Servicio de registro durante el análisis)	Ordena a Nessus iniciar el servicio de registro SMB en hosts que no lo tengan habilitado.
“SMB Scope” (Alcance SMB)	Ordena a Nessus consultar a los usuarios de dominio en lugar de los usuarios locales.
“SMB Use Domain SID to Enumerate Users” (SMB, usar SID de dominio para enumerar usuarios)	Una opción que le permite especificar el rango de SID para búsquedas de SMB de usuarios de dominio.
“SMB Use Host SID to Enumerate Local Users” (SMB, usar SID de host para enumerar usuarios locales)	Una opción que le permite especificar el rango de SID para búsquedas de SMB de usuarios locales.
“SMTP Settings” (Opciones de configuración de SMTP)	Opciones para probar el Protocolo simple de transferencia de correo (SMTP).
“SNMP Settings” (Opciones de configuración de SNMP)	Información de configuración y autenticación para el Protocolo simple de administración de redes (SNMP).

“Service Detection” (Detección de servicios)	Opciones que le indican a Nessus cómo probar los servicios SSL.
“Unix Compliance Checks” (Comprobaciones de compatibilidad con Unix)	Una opción de ProfessionalFeed que permite especificar un archivo de directiva para probar sistemas Unix según estándares de compatibilidad.
“VMware SOAP API Settings” (Opciones de configuración de API SOAP de VMware)	Información de configuración y autenticación para la API SOAP de VMware.
“Wake-on-LAN” (Paquetes Wake-on-LAN)	Le ordena a Nessus que envíe paquetes Wake-on-LAN (WOL) antes de ejecutar un análisis.
“Web Application Test Settings” (Opciones de prueba de aplicaciones web)	Opciones relacionadas con la prueba de aplicaciones web.
“Web mirroring” (Reflejo web)	Detalles de configuración que controlan cuántas páginas web Nessus reflejará para analizar el contenido en busca de vulnerabilidades.
“Windows Compliance Checks” (Comprobaciones de compatibilidad con Windows)	Una opción de ProfessionalFeed que permite especificar un archivo de directiva para probar sistemas Windows según estándares de compatibilidad.
“Windows File Contents Compliance Checks” (Comprobaciones de compatibilidad de contenido de archivos de Windows)	Una opción de ProfessionalFeed que permite especificar un archivo de directiva para probar archivos en un sistema Windows según estándares de compatibilidad.

Debido a las actualizaciones de metadatos XML en Nessus 5, los datos de compatibilidad generados con Nessus 4 no estarán disponibles en el capítulo de las comprobaciones de compatibilidad de los informes exportados. Sin embargo, los datos de compatibilidad estarán disponibles en la GUI Web de Nessus.

Importación, exportación y copia de directivas

El botón “**Upload**” **(Cargar)** de la barra de menús le permitirá cargar en el analizador directivas creadas con anterioridad. Mediante el cuadro de diálogo “**Browse…**” **(Explorar…)**, seleccione la directiva de su sistema local y haga clic en “**Upload Policy**” **(Cargar directiva)**:

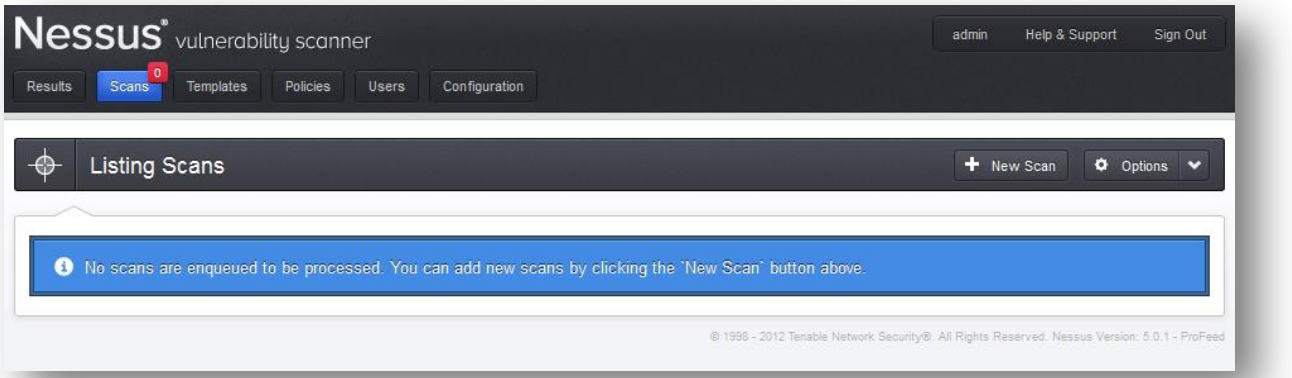


El botón “**Options**” **(Opciones)** de la barra de menús le permitirá descargar una directiva seleccionada del analizador al sistema de archivos local. El cuadro de diálogo de descarga del explorador le permitirá abrir la directiva en un programa externo (por ejemplo, un editor de texto) o guardarla en el directorio que elija.

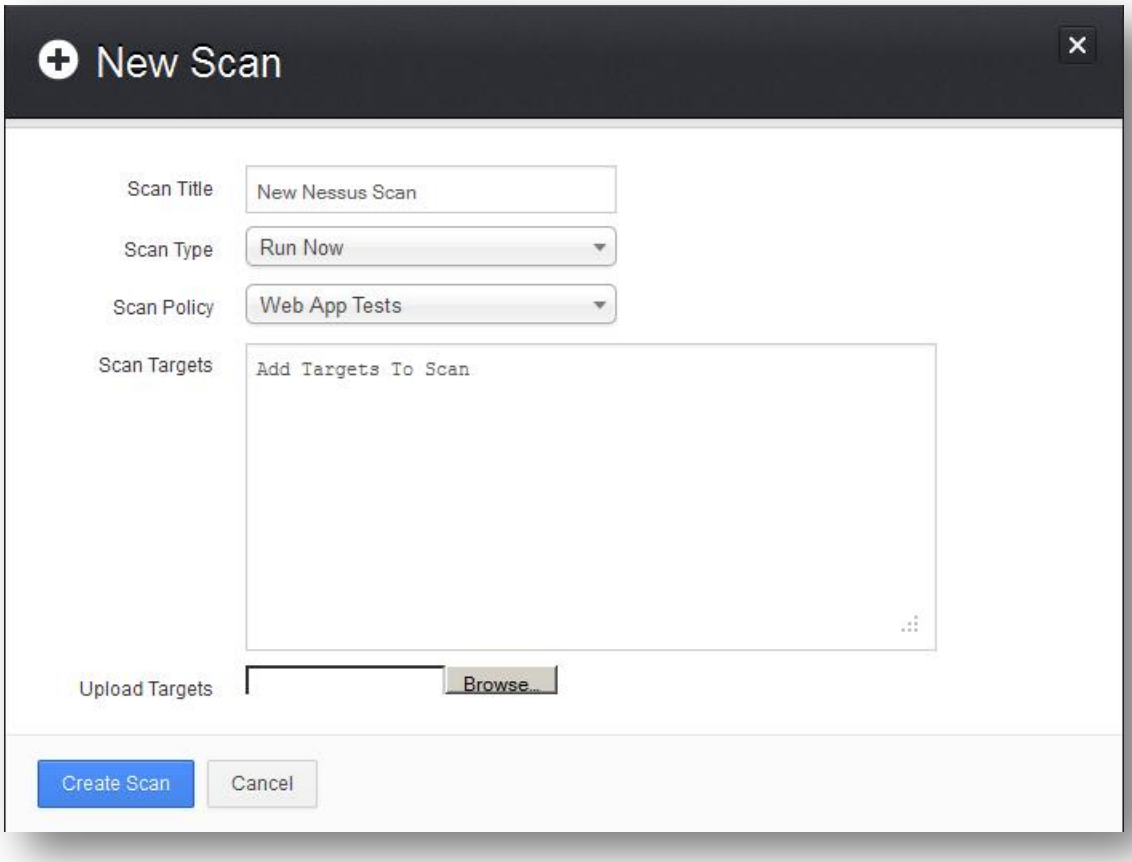
Las contraseñas y los archivos `.audit` contenidos en la directiva **no** serán exportados.

Si desea crear una directiva similar a una existente con pequeñas modificaciones, puede seleccionar la directiva de base de la lista y hacer clic en “**Options**” **(Opciones)** y luego en “**Copy Policy**” **(Copiar directiva)** en la barra de menús. Esto creará una copia de la directiva original que podrá editarse para efectuar cualquier modificación requerida. Lo anterior resulta de utilidad para crear directivas estándar con pequeños cambios según sean necesarios para un entorno determinado.

Creación, inicio y programación de un análisis



Después de crear o seleccionar una directiva puede crear un nuevo análisis; para ello haga clic en la opción “**Scans**” **(Análisis)** de la barra de menús situada en la parte superior y luego haga clic en el botón “**+ New Scan**” **(+ Nuevo análisis)** de la derecha. Aparecerá la pantalla “**New Scan**” **(Nuevo análisis)**, como se muestra a continuación:



Hay cinco campos para introducir el destino del análisis:

- **Scan Title (Título del análisis)**: establece el nombre que aparecerá en la UI de Nessus para identificar el análisis.
- **Scan Type (Tipo de análisis)**: seleccione entre “Run Now” (Ejecutar ahora) (para ejecutar el análisis inmediatamente después de ejecutar el comando “Submit” [Enviar]), “Scheduled” (Programado) (para seleccionar la hora en que debe comenzar el análisis) o “Template” (Plantilla) (para guardar como plantilla para otro análisis posterior).
- **Scan Policy (Directiva de análisis)**: seleccione una directiva creada anteriormente, que usará el análisis para establecer los parámetros que controlan el comportamiento de análisis del servidor Nessus.
- **Scan Targets (Destinos de análisis)**: los destinos se pueden introducir mediante una dirección IP única (por ejemplo, 192.168.0.1), un intervalo de IP (por ejemplo, 192.168.0.1-192.168.0.255), una subred con notación CIDR (por ejemplo, 192.168.0.0/24) o un host que se pueda resolver (por ejemplo, www.nessus.org).
- **Upload Targets (Cargar destinos)**: se puede importar un archivo de texto con una lista de hosts haciendo clic en “**Browse…**” **(Explorar…)** y seleccionando un archivo del equipo local.

Al archivo de hosts se le debe asignar el formato de texto ASCII, con un host por línea y sin espacios ni líneas adicionales. No se admite la codificación Unicode/UTF-8.

Ejemplos de formatos de archivos de hosts:

Hosts individuales:

192.168.0.100
192.168.0.101
192.168.0.102

Intervalo de hosts:

192.168.0.100-192.168.0.102

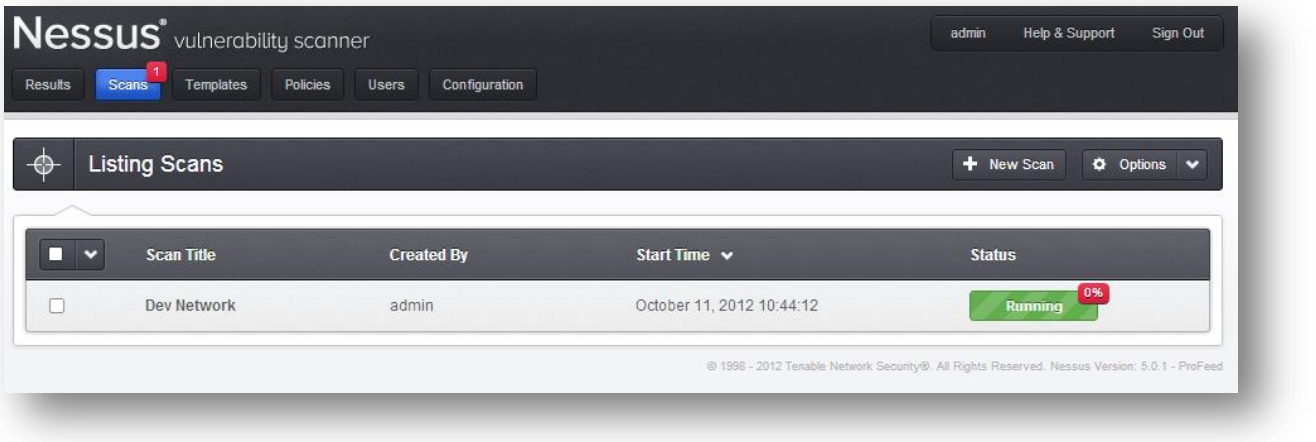
Bloque CIDR de hosts:

192.168.0.1/24

Servidores virtuales:

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

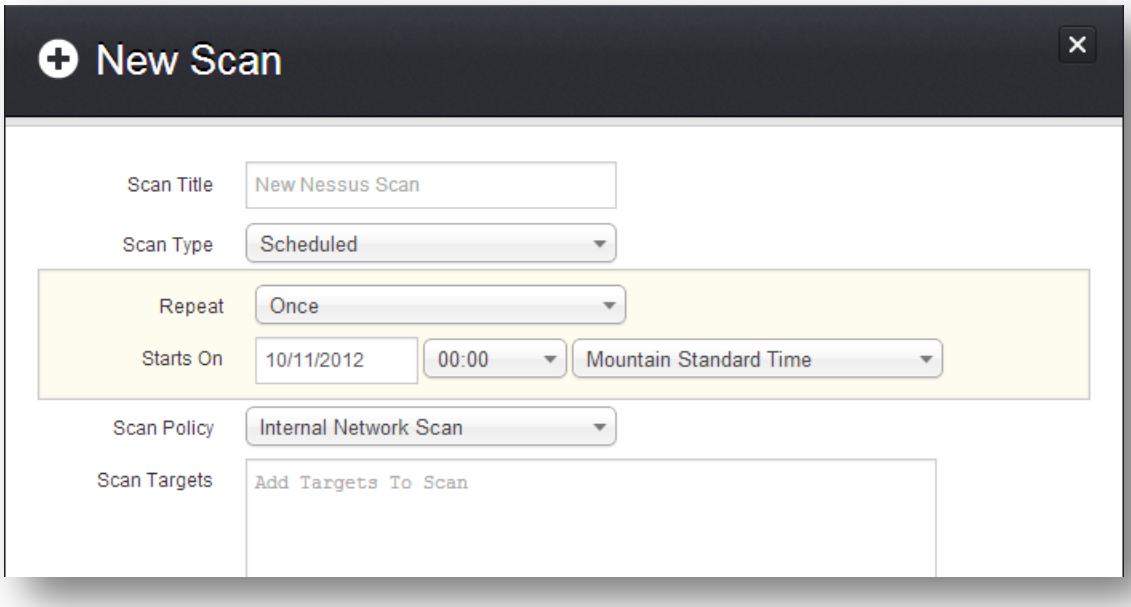
Después de haber introducido la información del análisis, haga clic en "**Create Scan**" **(Crear análisis)**. El análisis comenzará de inmediato (si se seleccionó "Run Now" [Ejecutar ahora]), antes de que la pantalla vuelva a la página general "**Scans**" **(Análisis)**. La barra de menú superior también actualizará el número superpuesto al botón "**Scans**" **(Análisis)** para indicar cuántos análisis se están ejecutando en ese momento.



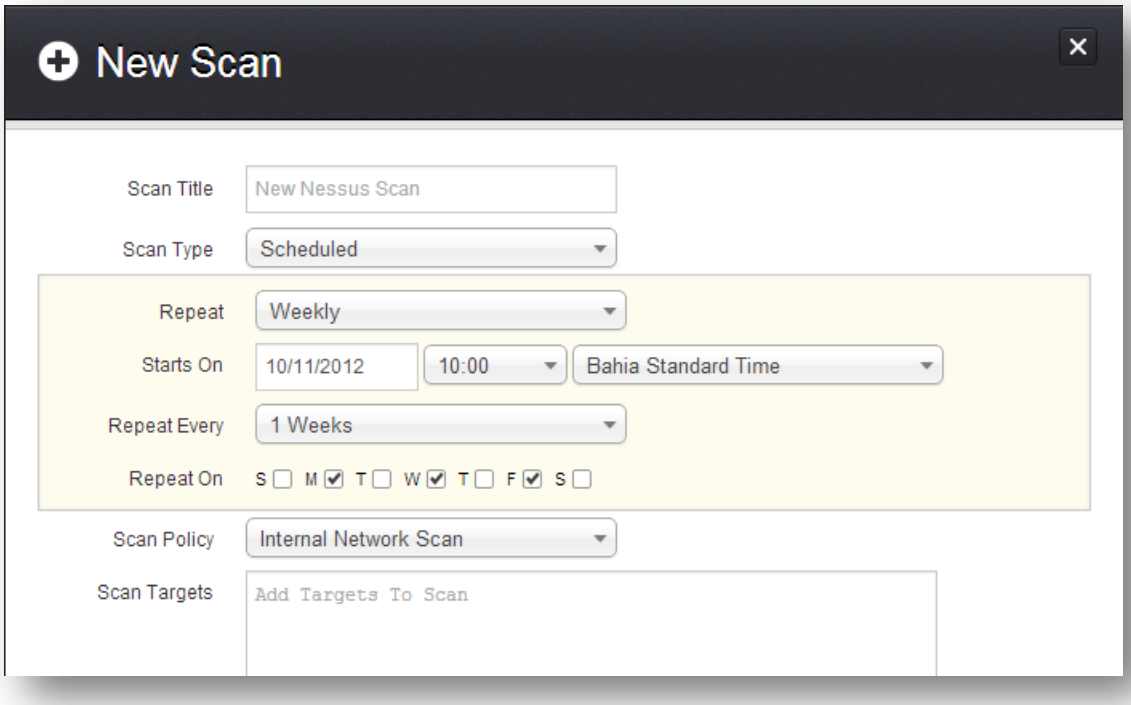
Una vez iniciado el análisis, en "Scans" (Análisis) se mostrará una lista de todos los análisis que estén en ese momento en curso o pausados, junto con la información básica del análisis. Después de seleccionar un análisis específico de la lista, el botón "**Options**" **(Opciones)** en la esquina superior derecha le permitirá "**Pause**" (pausar), "**Resume**" (reanudar) o "**Stop**" (detener) el análisis.

Una vez finalizado un análisis (por cualquier motivo), se quitará de la lista "**Scans**" **(Análisis)** y estará disponible para su revisión en la ficha "**Results**" **(Resultados)**.

Si un nuevo análisis recibe la designación "Scheduled" **(Programado)**, aparecerá una opción para establecer la hora de inicio y la frecuencia deseadas:

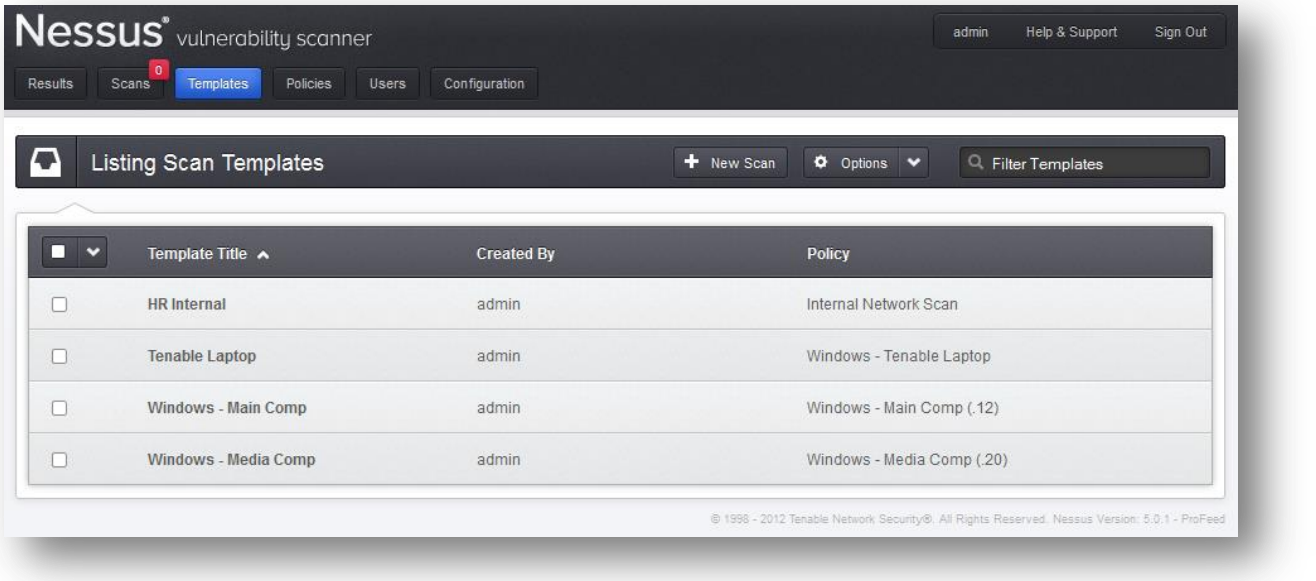


Mediante el menú desplegable “Repeat” (Repetir) se puede programar un análisis para que se ejecute una vez, diariamente, semanalmente, mensualmente o anualmente. Esta opción se puede especificar aun más para que comience en una fecha y hora determinadas. Una vez guardado el análisis, Nessus lo iniciará a la hora especificada.



Los análisis programados solo están disponibles para los clientes de ProfessionalFeed.

Si se guarda un nuevo análisis como plantilla, aparecerá en la ficha “Templates” (Plantillas) a la derecha de la ficha “Scans” (Análisis) en la barra de menús. Desde la ficha “Templates” (Plantillas), los usuarios pueden modificar, eliminar o iniciar análisis basados en plantillas.

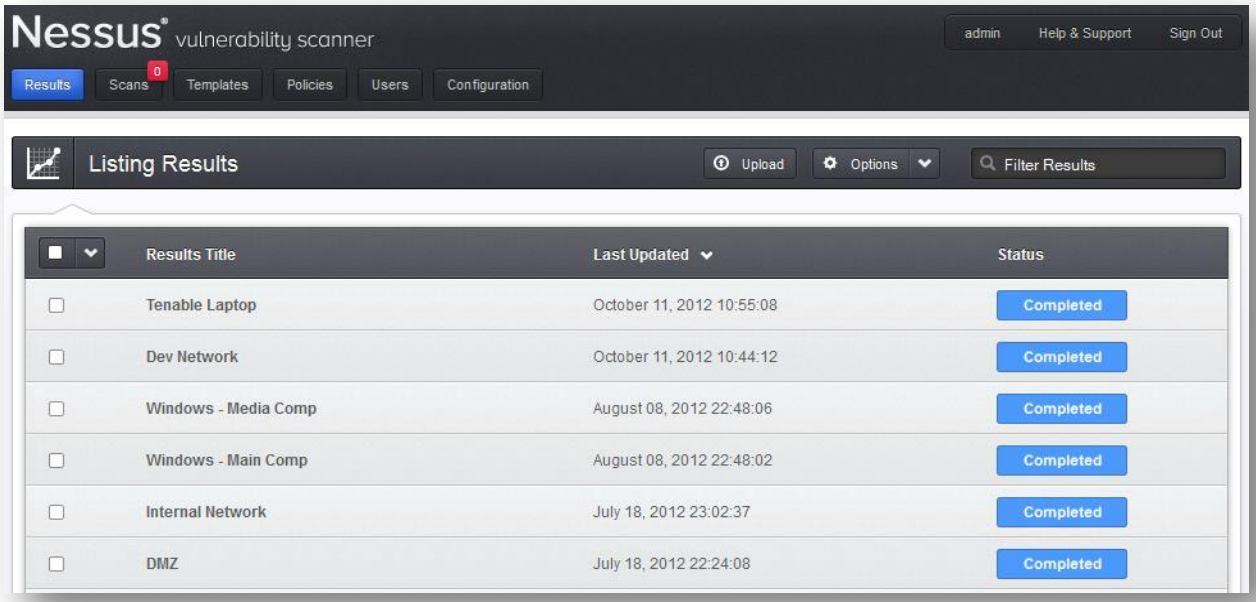


También puede acceder a la misma funcionalidad para crear un nuevo análisis desde esta ficha. Además, se dispone de un cuadro de entrada de filtros que le permite filtrar las plantillas según el campo de título. Si borra el texto ingresado en este cuadro, se restablecerá el filtro y se mostrarán todas las plantillas.

Resultados

Con la versión Nessus 5, los usuarios pueden crear su propio informe por capítulos: Vulnerability Centric (Enfocado en vulnerabilidades), Host Centric (Enfocado en hosts), Compliance (Compatibilidad) o Compliance Executive (Compatibilidad ejecutiva). El formato HTML se sigue admitiendo de manera predeterminada; sin embargo, si Java está instalado en el host del analizador, también es posible exportar informes en PDF. Al usar los filtros de informes y las características de exportación, los usuarios pueden crear informes dinámicos de su propia elección en lugar de seleccionarlos de una lista específica.

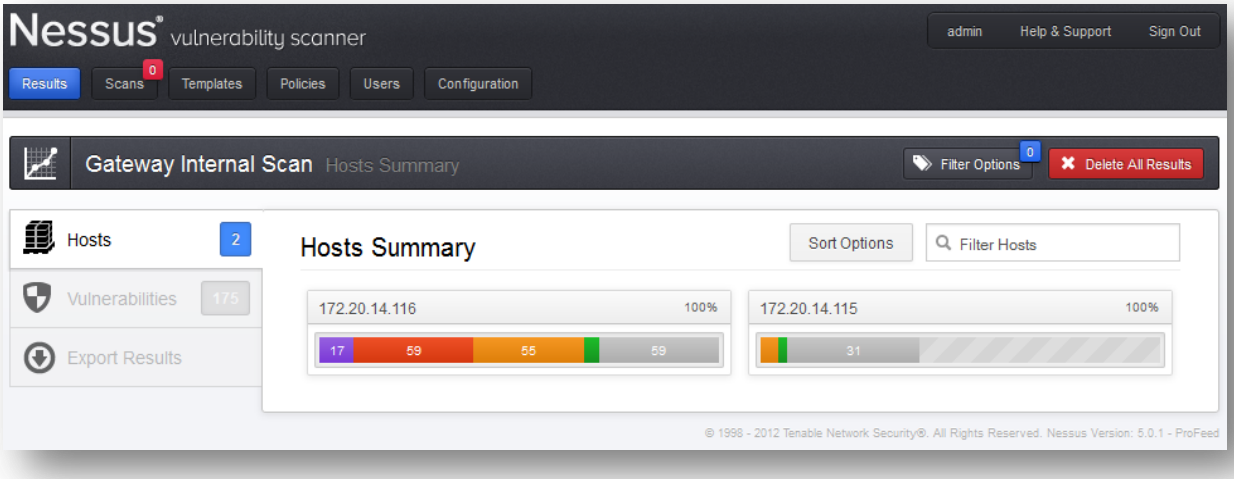
Si hace clic en la ficha “**Results**” **(Resultados)**, en la barra de menús situada en la parte superior de la interfaz, aparecerá la lista de análisis en ejecución y terminados:



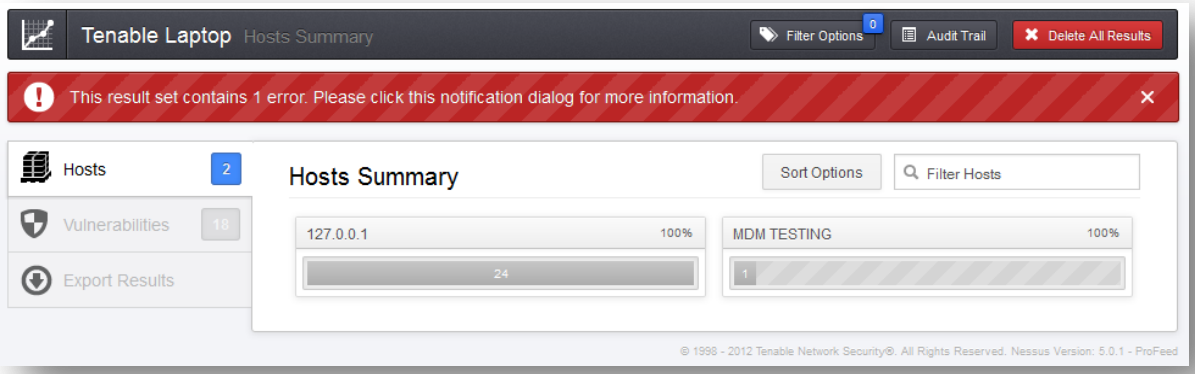
La pantalla "**Results**" **(Resultados)** se desempeña como punto central para ver, comparar, cargar y descargar resultados de análisis.

Explorar los resultados de un análisis

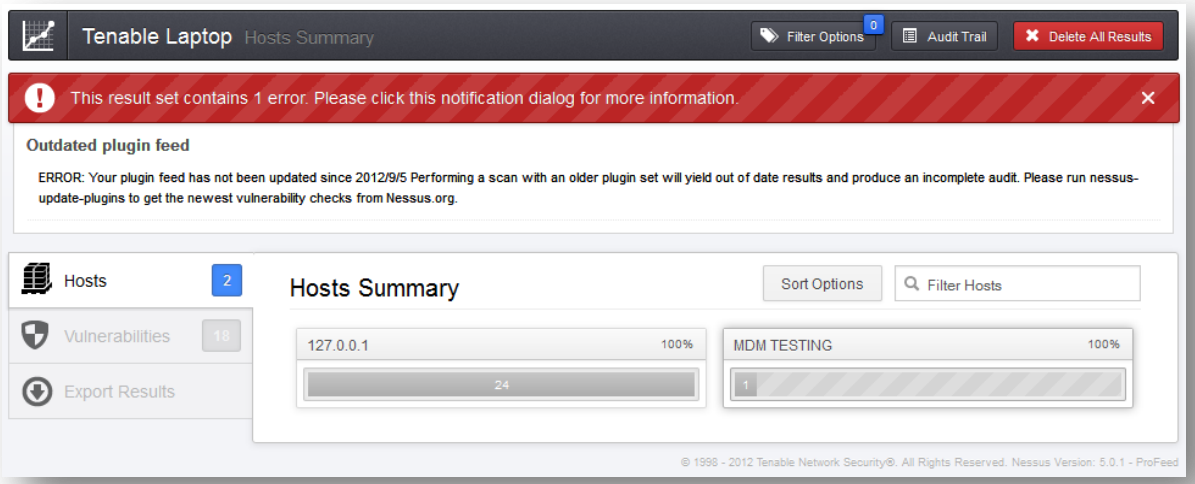
Para explorar los resultados de un análisis, haga clic en un informe de la lista "**Results**" **(Resultados)**. Esto le permite ver resultados al navegar por vulnerabilidades o hosts, y ver puertos e información específica de las vulnerabilidades. La vista/ficha predeterminada es por resumen de hosts, que muestra una lista de hosts con un resumen de vulnerabilidades, codificadas con color, por host:



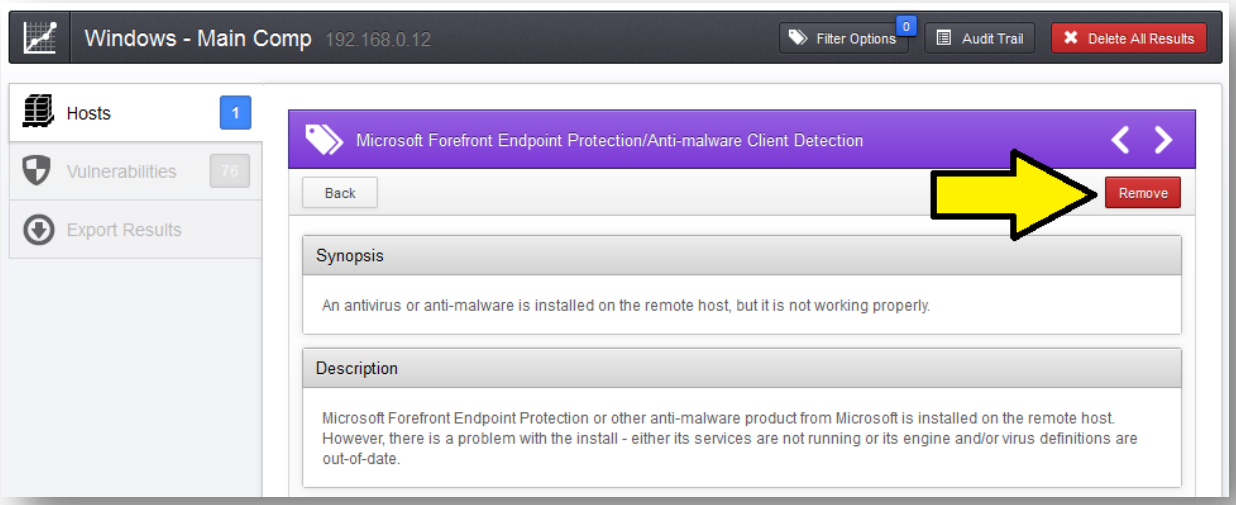
Si se produjeron errores durante el análisis, habrá una nota en la parte superior de los resultados.



Haga clic en el error para proporcionar más información:

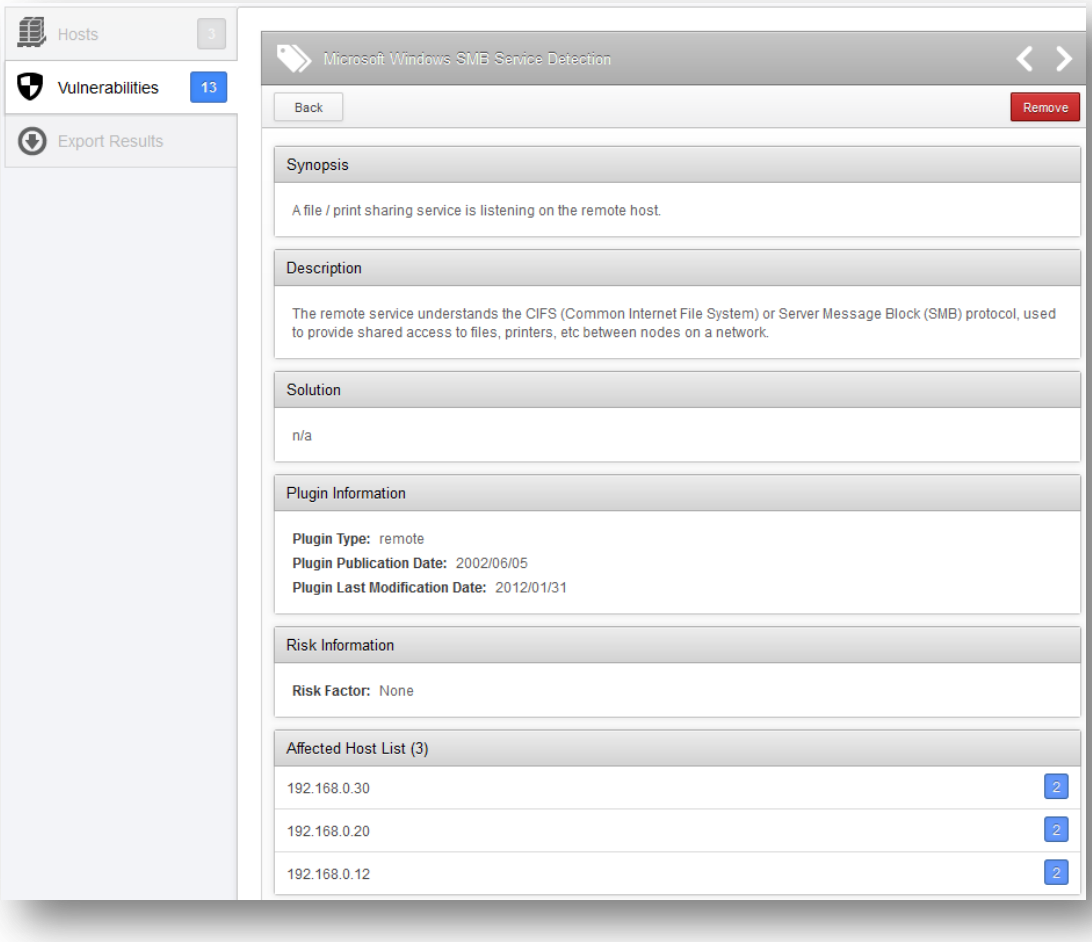


Si hace clic en un host verá la vista "**Vulnerability Summary**" **(Resumen de vulnerabilidades)**. El usuario puede ver selectivamente información detallada de las vulnerabilidades del informe, como la sinopsis, descripción, solución, referencias, información de riesgo y actualización de plugin. En la esquina superior derecha, "**Remove**" **(Quitar)** puede usarse para eliminar la vulnerabilidad que se muestra:



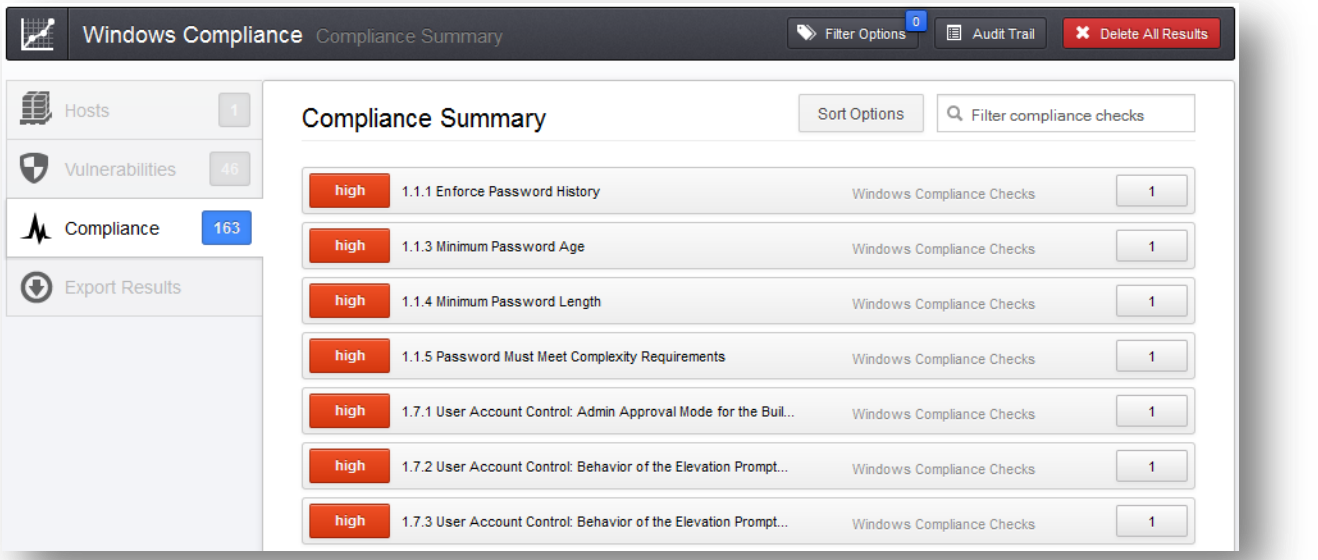
Asegúrese de seleccionar “**Remove**” **(Quitar)** justo encima de la vulnerabilidad en lugar de “**Delete All Results**” **(Eliminar todos los resultados)** en la barra de menús Results (Resultados). Use las flechas blancas en la barra de título de la vulnerabilidad para moverse entre los resultados uno por uno.

Seleccione la ficha “Vulnerabilities” (Vulnerabilidades) a la izquierda para pasar a la vista Vulnerability. Esto ordenará los resultados por vulnerabilidades en lugar de hacerlo por hosts. Si selecciona una vulnerabilidad verá la misma información que antes, pero también incluirá una lista de los hosts afectados abajo.



Si hace clic en un host afectado abajo, cargará la vista de vulnerabilidades por host.

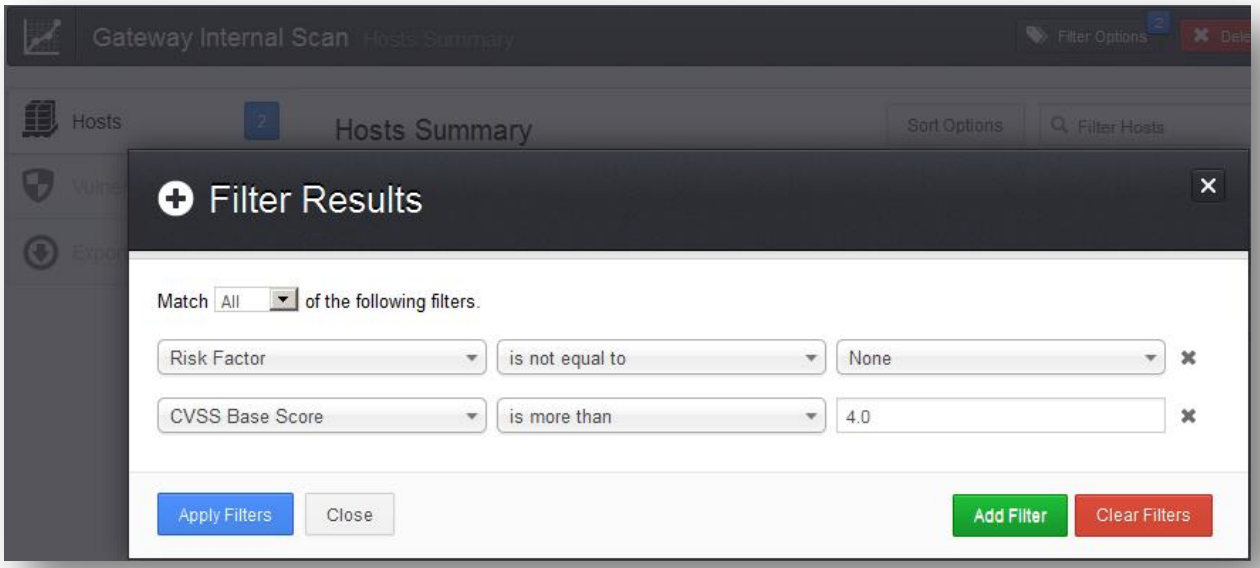
Si se inicia un análisis que utiliza una directiva de compatibilidad, los resultados aparecerán en una nueva ficha lateral debajo del informe del análisis, bajo el nombre “**Compliance**”:



Filtros de informes

Nessus ofrece un sistema flexible de filtros para ayudar en la visualización de resultados de informes específicos. Los filtros se pueden usar para mostrar resultados de acuerdo con cualquier aspecto de los resultados de vulnerabilidades. Cuando se usan varios filtros, se pueden crear vistas de informes más detalladas y personalizadas.

Para crear un filtro, haga clic en “**Filter Options**” **(Opciones de filtro)** encima de los resultados de informes. Se pueden crear filtros desde cualquier ficha de informes. Se pueden crear varios filtros con una lógica que permita un filtrado complejo. Para crear un filtro se selecciona el atributo del plugin, un argumento de filtro y un valor respecto al cual filtrar. Al seleccionar varios filtros, se debe especificar la palabra clave “Any” (Cualquiera) o “All” (Todos) según corresponda. Si selecciona “All” (Todos), solo se mostrarán los resultados que coincidan con **todos** los filtros:



Una vez que estableció un filtro, puede eliminarlo individualmente haciendo clic en la ✖ a la derecha. Además, puede eliminar todos los filtros al mismo tiempo seleccionando "Clear Filters" (Borrar filtros). Los filtros de informes permiten una amplia variedad de criterios para un control pormenorizado de los resultados:

Opción	Descripción
"Plugin ID" (Identificación del plugin)	Filtra resultados si la identificación del plugin "*is equal to*" (es igual a), "*is not equal to*" (no es igual a), "*contains*" (contiene) o "*does not contain*" (no contiene) determinada cadena (por ejemplo, 42111).
"Plugin Description" (Descripción del plugin)	Filtra resultados si la descripción del plugin "*contains"* (contiene) o "*does not contain"* (no contiene) determinada cadena (por ejemplo, "remote").
"Plugin Name" (Nombre del plugin)	Filtra resultados si el nombre del plugin "*is equal to*" (es igual a), "*is not equal to*" (no es igual a), "*contains*" (contiene) o "*does not contain*" (no contiene) determinada cadena (por ejemplo, "windows").
"Plugin Family" (Familia del plugin)	Filtra resultados si el nombre del plugin "*is equal to"* (es igual a) o "*is not equal to"* (no es igual a) una de las familias de plugins designadas de Nessus. Las coincidencias posibles aparecen en un menú desplegable.
"Plugin Output" (Salida del plugin)	Filtra resultados si la descripción del plugin "*is equal to*" (es igual a), "*is not equal to*" (no es igual a), "*contains*" (contiene) o "*does not contain*" (no contiene) determinada cadena (por ejemplo, "PHP").
"Plugin Type" (Tipo de plugin)	Filtra resultados si el tipo de plugin "*is equal to"* (es igual a) o "*is not equal to"* (no es igual a) uno de los dos tipos de plugins: local o remoto.
"Solution" (Solución)	Filtra resultados si la solución del plugin "*contains"* (contiene) o "*does not contain"* (no contiene) determinada cadena (por ejemplo, "upgrade").
"Synopsis" (Sinopsis)	Filtra resultados si la sinopsis del plugin "*contains"* (contiene) o "*does not contain"* (no contiene) determinada cadena (por ejemplo, "PHP").

"Hostname" **(Nombre del host)**	Filtra resultados si el host "*is equal to*" (es igual a), "*is not equal to*" (no es igual a), "*contains*" (contiene) o "*does not contain*" (no contiene) determinada cadena (por ejemplo, "192.168" o "lab").
"Port" **(Puerto)**	Filtra resultados según si un puerto "*is equal to*" (es igual a), "*is not equal to*" (no es igual a), "*contains*" (contiene) o "*does not contain*" (no contiene) determinada cadena (por ejemplo, "80").
"Protocol" **(Protocolo)**	Filtra resultados si un protocolo "*is equal to*" (es igual a) o "*is not equal to*" (no es igual a) determinada cadena (por ejemplo, "http").
"CPE" **(CPE)**	Filtra resultados según si la Common Platform Enumeration (Enumeración de plataforma común) (CPE) "*is equal to*" (es igual a), "*is not equal to*" (no es igual a), "*contains*" (contiene) o "*does not contain*" (no contiene) determinada cadena (por ejemplo, "solaris").
"CVSS Base Score" **(Puntuación CVSS total)**	Filtra resultados según si una "CVSS Base Score" (Puntuación CVSS total) "*is less than*" (es menor que), "*is more than*" (es mayor que), "*is equal to*" (es igual a), "*is not equal to*" (no es igual a), "*contains*" (contiene) o "*does not contain*" (no contiene) determinada cadena (por ejemplo, "5"). Este filtro puede utilizarse para seleccionar por nivel de riesgo. Las clasificaciones de gravedad derivan del puntaje CVSS asociado, en el que 0 es "Info" (Información), menos de 4 es "Low" (Baja), menos de 7 es "Medium" (Media), menos de 10 es "High" (Alta), y un puntaje CVSS de 10 se marcará como "Critical" (Crítico).
"CVSS Temporal Score" **(Puntuación CVSS temporal)**	Filtra resultados según si una "CVSS Temporal Score" (Puntuación CVSS temporal) "*is less than*" (es menor que), "*is more than*" (es mayor que), "*is equal to*" (es igual a), "*is not equal to*" (no es igual a), "*contains*" (contiene) o "*does not contain*" (no contiene) determinada cadena (por ejemplo, "3.3").
"CVSS Temporal Vector" **(Vector CVSS temporal)**	Filtra resultados según si un "CVSS Temporal Vector" (Vector CVSS temporal) "*is equal to*" (es igual a), "*is not equal to*" (no es igual a), "*contains*" (contiene) o "*does not contain*" (no contiene) determinada cadena (por ejemplo, "E:F").
"CVSS Vector" **(Vector CVSS)**	Filtra resultados según si un "CVSS Vector" (vector CVSS) "*is equal to*" (es igual a), "*is not equal to*" (no es igual a), "*contains*" (contiene) o "*does not contain*" (no contiene) determinada cadena (por ejemplo, "AV:N").
"Vulnerability Publication Date" **(Fecha de publicación de la vulnerabilidad)**	Filtra resultados según si la fecha de publicación de una vulnerabilidad es "*earlier than*" (anterior a), "*later than*" (posterior a), "*on*" (el día), "*not on*" (otro día que no sea), o "*contains*" (contiene) o "*does not contain*" (no contiene) una cadena (por ejemplo, "01/01/2012"). Importante: presione el botón junto a la fecha para ir a una interfaz de calendario y facilitar la selección de fechas.
"Patch Publication Date" **(Fecha de publicación de la revisión)**	Filtra resultados según si la fecha de publicación de una revisión de vulnerabilidad "*is less than*" (es menor que), "*is more than*" (es mayor que), "*is equal to*" (es igual a), "*is not equal to*" (no es igual a), "*contains*" (contiene) o

	"*does not contain*" (no contiene) determinada cadena (por ejemplo, "12/01/2011").
"PluginPublication Date" (Fecha de publicación del plugin)	Filtra resultados según si la fecha de publicación de un plugin de Nessus "*is less than*" (es menor que), "*is more than*" (es mayor que), "*is equal to*" (es igual a), "*is not equal to*" (no es igual a), "*contains*" (contiene) o "*does not contain*" (no contiene) determinada cadena (por ejemplo, "06/03/2011").
"Plugin Modification Date" (Fecha de modificación del plugin)	Filtra resultados según si la fecha de modificación de un plugin de Nessus "*is less than*" (es menor que), "*is more than*" (es mayor que), "*is equal to*" (es igual a), "*is not equal to*" (no es igual a), "*contains*" (contiene) o "*does not contain*" (no contiene) determinada cadena (por ejemplo, "02/14/2010").
"CVE" (CVE)	Filtra resultados según si una CVE Reference (Referencia CVE) "*is equal to*" (es igual a), "*is not equal to*" (no es igual a), "*contains*" (contiene) o "*does not contain*" (no contiene) determinada cadena (por ejemplo, "2011-0123").
"Bugtraq ID" (Identificación Bugtraq)	Filtra resultados según si una Bugtraq ID (Identificación Bugtraq) "*is equal to*" (es igual a), "*is not equal to*" (no es igual a), "*contains*" (contiene) o "*does not contain*" (no contiene) determinada cadena (por ejemplo, "51300").
"CERT Advisory ID" (Identificación de Asesoría CERT)	Filtra resultados según si una CERT Advisory ID (Identificación de Asesoría CERT) [ahora llamada Technical Cyber Security Alert (Alerta técnica de ciberseguridad)] "*is equal to*" (es igual a), "*is not equal to*" (no es igual a), "*contains*" (contiene) o "*does not contain*" (no contiene) determinada cadena (por ejemplo, "TA12-010A").
"OSVDB ID" (Identificación de OSVDB)	Filtra resultados según si una Open Source Vulnerability Database (OSVDB) ID (Identificación de Base de datos de vulnerabilidades de código abierto [OSVDB]) "*is equal to*" (es igual a), "*is not equal to*" (no es igual a), "*contains*" (contiene) o "*does not contain*" (no contiene) determinada cadena (por ejemplo, "78300").
"Secunia ID" (Identificación Secunia)	Filtra resultados según si una Secunia ID (Identificación Secunia) "*is equal to*" (es igual a), "*is not equal to*" (no es igual a), "*contains*" (contiene) o "*does not contain*" (no contiene) determinada cadena (por ejemplo, "47650").
"Exploit Database ID" (Identificación de Base de datos Exploit)	Filtra resultados según si una referencia de Exploit Database ID (EBD-ID) (Identificación de Base de datos Exploit) "*is equal to*" (es igual a), "*is not equal to*" (no es igual a), "*contains*" (contiene) o "*does not contain*" (no contiene) determinada cadena (por ejemplo, "18380").
"Metasploit Name" (Nombre Metasploit)	Filtra resultados según si un Metasploit name (Nombre Metasploit) "*is equal to*" (es igual a), "*is not equal to*" (no es igual a), "*contains*" (contiene) o "*does not contain*" (no contiene) determinada cadena (por ejemplo, "xslt_password_reset").
"Exploit Hub" (Exploit Hub)	Filtra resultados según si una vulnerabilidad de seguridad de ExploitHub es "*true*"(verdadera) o "*false*" (falsa).
"IAVA" (IAVA)	Filtra resultados según si una referencia IAVA "*is equal to*" (es igual a), "*is not equal to*" (no es igual a), "*contains*" (contiene) o "*does not contain*" (no contiene) determinada cadena (por ejemplo, "2012-A-0008").
"See Also" (Ver también)	Filtra resultados según si la referencia "see also" (ver también) de un plugin de Nessus "*is equal to*" (es igual a), "*is not equal to*" (no es igual a), "*contains*" (contiene) o "*does not contain*" (no contiene) determinada cadena (por ejemplo, "seclists.org").

“Exploits Available” (Vulnerabilidades de seguridad disponibles)	Filtra resultados en función de la vulnerabilidad de seguridad pública conocida.
“Exploitability Ease” (Facilidad de vulnerabilidad de seguridad)	Filtra resultados según si la facilidad de vulnerabilidad de seguridad “*is equal to*” (es igual a) o “*is not equal to*” (no es igual a) en comparación con los siguientes valores: “*Exploits are available*” (Las vulnerabilidades de seguridad están disponibles), “*No exploit is required*” (No se requieren vulnerabilidades de seguridad) o “*No known exploits are available*” (No hay vulnerabilidades de seguridad conocidas disponibles).
“Metasploit Exploit Framework” (Exploit Framework de Metasploit)	Filtra resultados según si la presencia de una vulnerabilidad en Metasploit Exploit Framework (Exploit Framework de Metasploit) “*is equal to”* (es igual a) “*true”* (verdadera) o “*false*” (falsa).

Al usar un filtro, la cadena o el valor numérico pueden delimitarse por comas para filtrar en función de varias cadenas. Por ejemplo, para que los resultados del filtro muestren solo servidores web, usted podría crear un filtro “Ports” (Puertos), seleccionar “is equal to” (es igual a) e introducir “80,443,8000,8080”. Esto le mostrará los resultados relacionados con esos cuatro puertos.

Los criterios de filtro **no** distinguen mayúsculas de minúsculas.

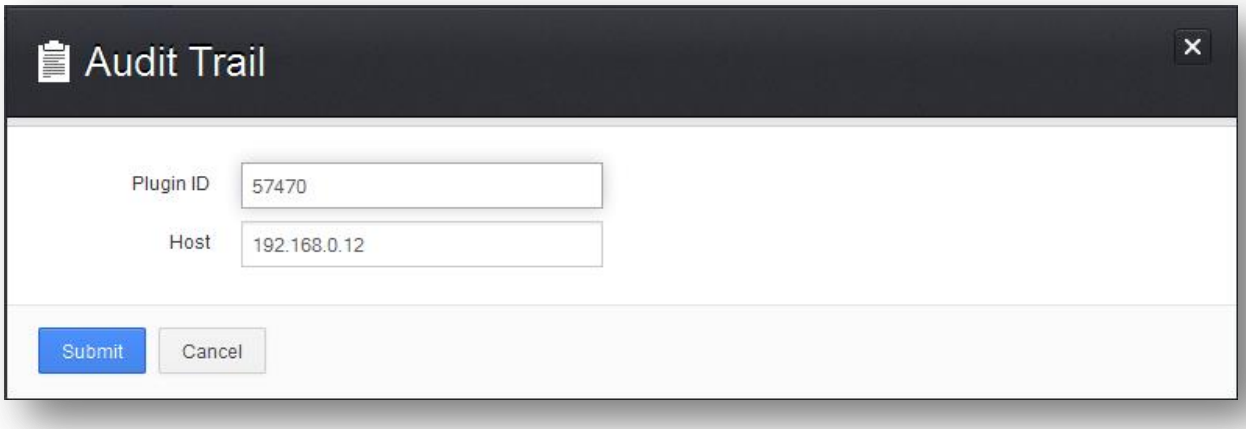
Si una opción de filtro no está disponible, significa que el informe no contiene nada que coincida con los criterios. Por ejemplo, si “Microsoft Bulletin” (Boletín Microsoft) no está en la lista desplegable de filtros, entonces no se encontraron vulnerabilidades que hagan referencia a Microsoft Bulletin (Boletín Microsoft).

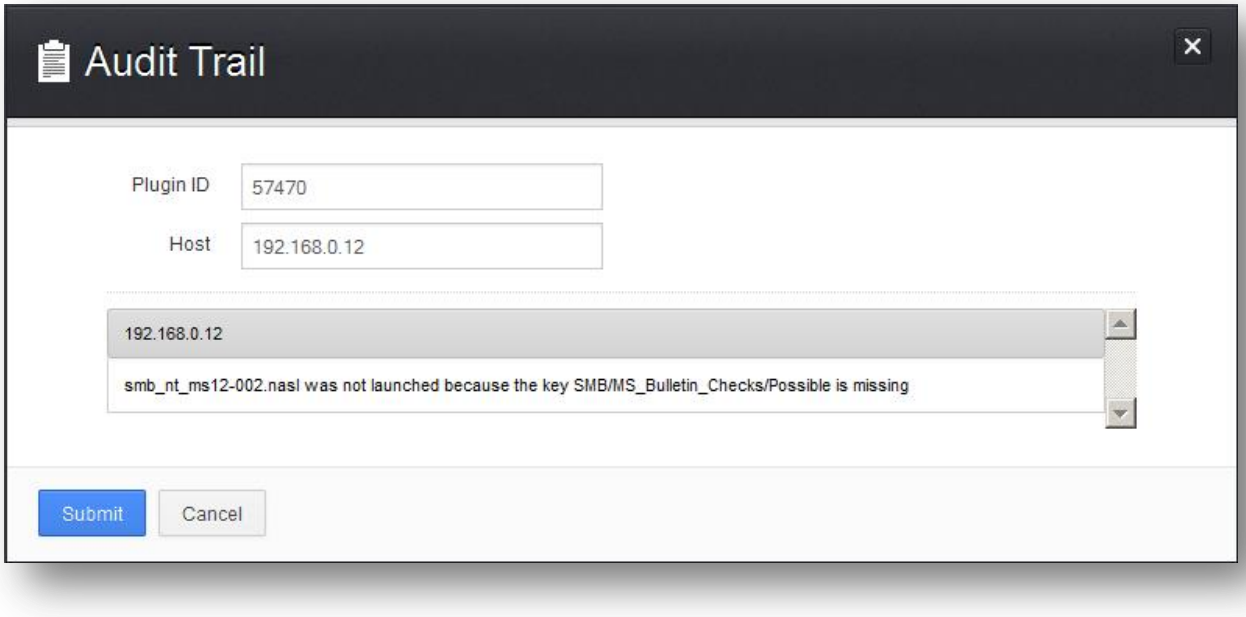
Apenas se cree un filtro, se actualizarán los resultados del análisis para que reflejen los nuevos criterios de filtro después de seleccionar “**Apply Filters**” **(Aplicar filtros)**.

Una vez que se filtraron los resultados para que brinden el conjunto de datos que desea, haga clic en “**Export Results**” **(Exportar resultados)** para exportar únicamente los resultados filtrados. Para recibir un informe con todos los resultados, elimine todos los filtros y utilice la función de exportación.

Los resultados de análisis de Nessus proporcionan una lista concisa de plugins que detectaron problemas en el host. Sin embargo, en algunos casos puede querer saber por qué un plugin no dio resultados. La funcionalidad “Audit Trail” (Registro de auditoría) brindará esta información. Comience haciendo clic en “Audit Trail” (Registro de auditoría) en la parte superior.

Esto abrirá el diálogo Audit Trail (Registro de auditoría). Primero, escriba la identificación del plugin sobre el que quiere más información. Haga clic en “Submit” (Enviar) y verá un host o una lista de hosts relacionados con su consulta. Además puede suministrar un IP de host para que la consulta inicial limite los resultados al destino que le interesa. Una vez que vea el/los host/s, haga clic en uno para ver información acerca de por qué el plugin no se activó:

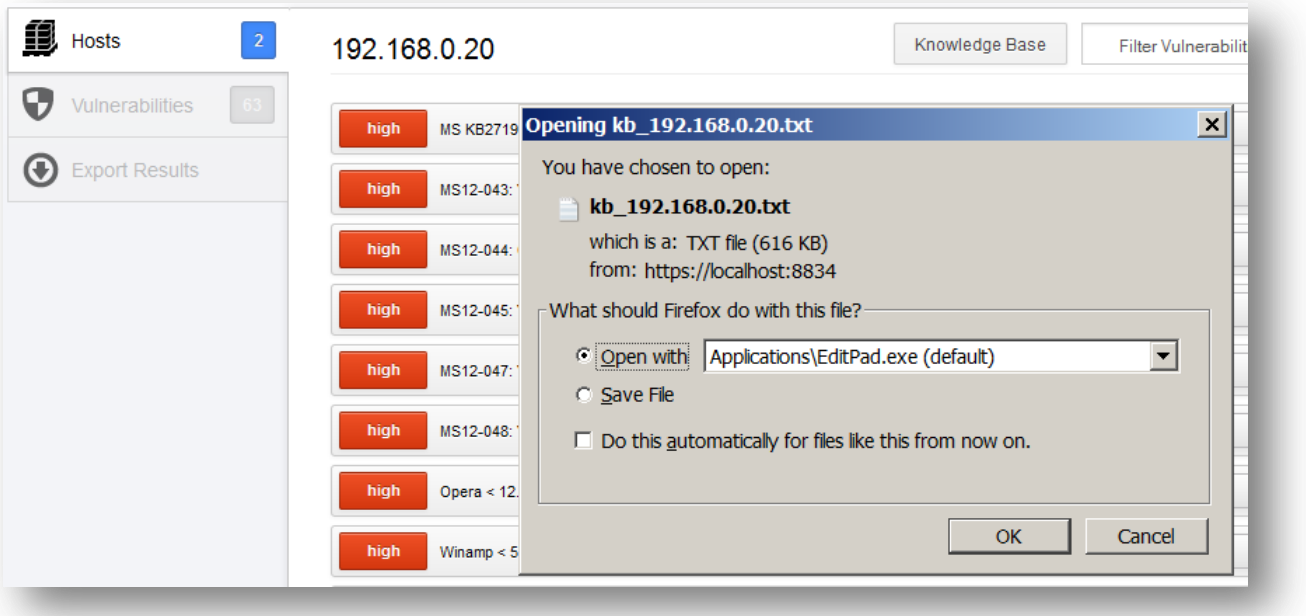




Debido a los recursos necesarios para el registro de auditoría, en algunos casos solo se proporcionará un registro de auditoría parcial. En el caso de analizar un solo host, se dispondrá del registro de auditoría completo. Si se analizan entre 2 y 512 hosts, solo está disponible un registro de auditoría completo si el servidor de Nessus tiene más de 1 CPU y 2 GB de RAM. El análisis de más de 512 hosts siempre dará como resultado un registro de auditoría parcial.

Con Nessus 5, cada vez que se realiza un análisis se guarda una Base de conocimiento (KB). Esta base es un archivo de texto ASCII que contiene un registro de la información relacionada con el análisis ejecutado y los resultados encontrados. La KB suele ser útil en los casos en que necesita soporte de Tenable, ya que le permite al personal de soporte comprender exactamente lo que hizo Nessus y qué información se encontró.

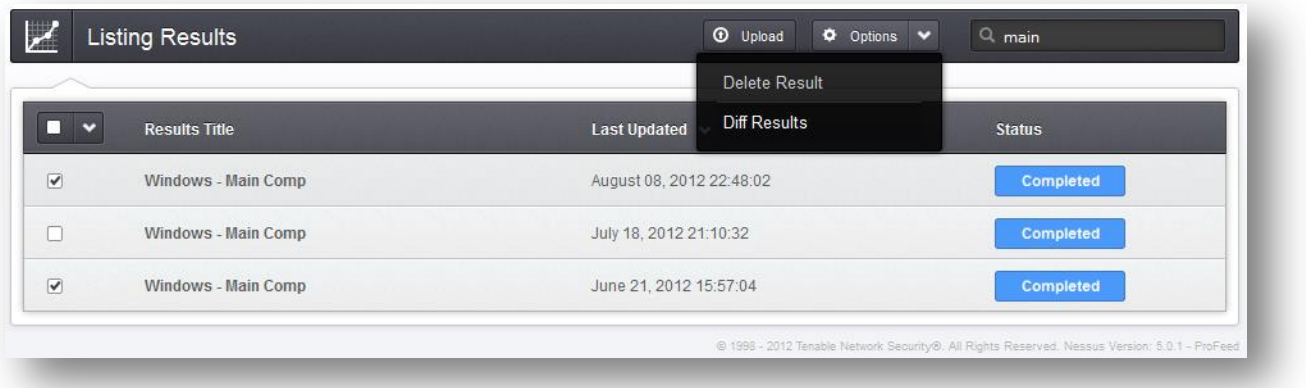
Para descargar una KB, seleccione un informe y luego un host específico. A la derecha del nombre del host o de la IP hay un botón llamado “Knowledge Base” (Base de conocimiento). Haga clic aquí para descargar la KB:



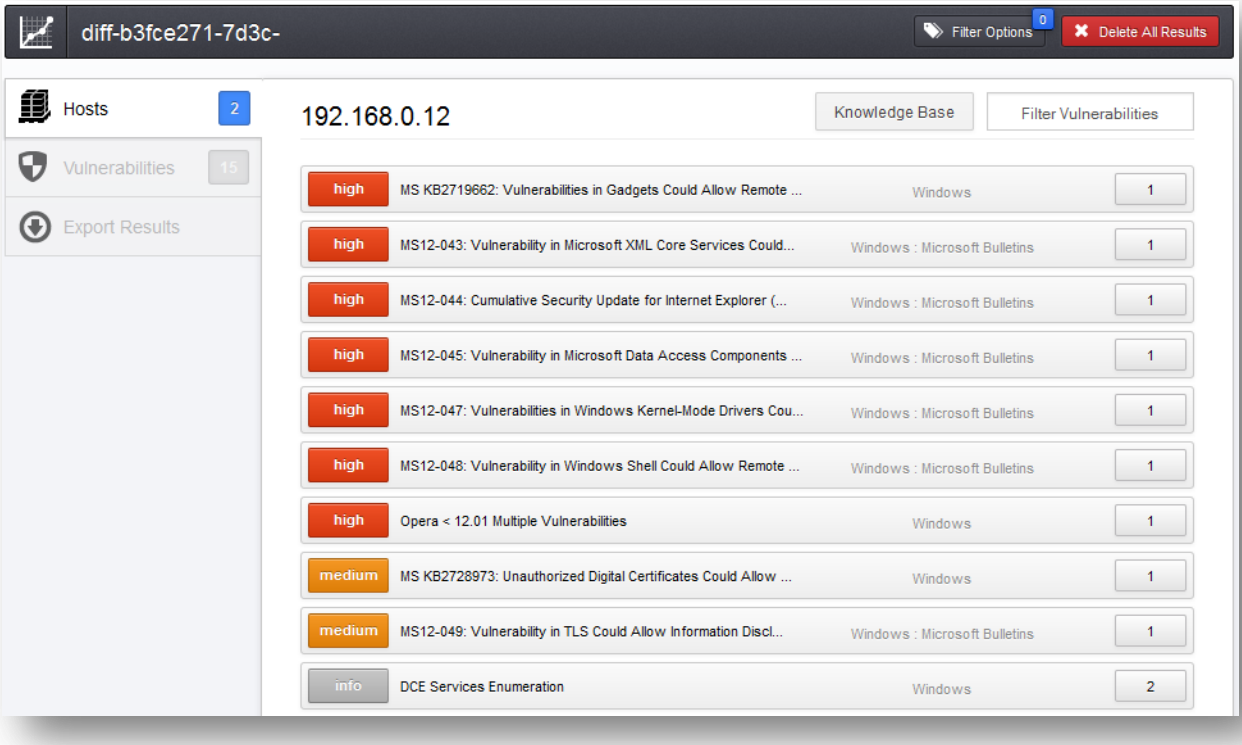
Comparar (diferentes resultados)

Con Nessus, usted puede comparar dos informes de análisis entre sí para visualizar cualquier diferencia. La capacidad para mostrar diferenciales de análisis permite indicar la forma en que un sistema o una red en particular cambiaron con el tiempo. Esto ayuda en el análisis de compatibilidad, al mostrar la forma en que se solucionan las vulnerabilidades, si los sistemas se revisan a medida que se encuentran nuevas vulnerabilidades, o la forma en que dos análisis pueden no tener como destino los mismos hosts.

Para comparar informes, primero seleccione dos análisis de la lista “**Results**” **(Resultados)**, haga clic en “**Options**” **(Opciones)** y seleccione “**Diff Results**” **(Diferentes resultados)** del menú desplegable:



Nessus comparará el primer informe seleccionado con el segundo y producirá una lista de los resultados que son diferentes desde el primero. La función de comparación muestra lo nuevo desde la línea de referencia (es decir, desde el primer informe seleccionado); no produce un diferencial de dos informes cualesquiera. Esta comparación destaca qué vulnerabilidades se encontraron o solucionaron entre los dos análisis. En el ejemplo anterior, “Windows – Main Comp” (Windows – Comparación principal) es un análisis autenticado de un solo host de Microsoft Windows, ejecutado varias veces. La función “Compare” (Comparar) muestra las diferencias, y se destacan las vulnerabilidades que no se analizaron en el análisis del 21 de junio:

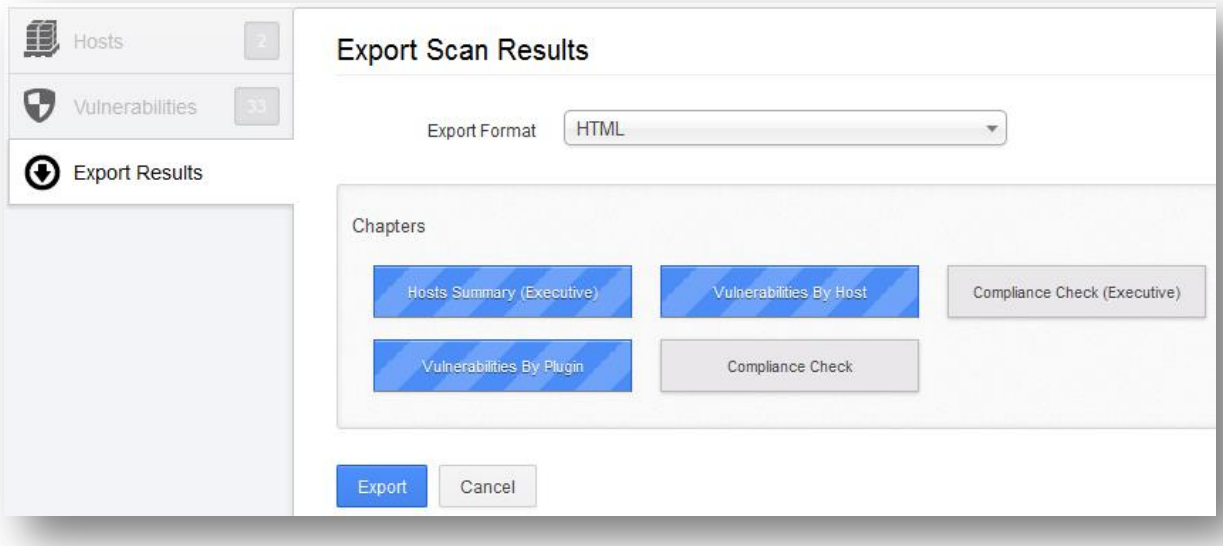


La función “Compare” (Comparar) solo está disponible para los usuarios de ProfessionalFeed.

Carga y descarga (exportación)

Los resultados de análisis pueden exportarse desde un analizador Nessus e importarse en uno diferente. Las funciones “**Upload**” **(Cargar)** y “**Export**” **(Exportar)** permiten una mejor administración de análisis, comparación de informes, creación de copias de seguridad de los informes y comunicación entre grupos u organizaciones dentro de una empresa.

Para exportar un análisis, comience por seleccionar el informe de la pantalla “**Results**” **(Resultados)**, seleccione la ficha “**Export Results**” **(Exportar resultados)**, escoja las opciones que desea y haga clic en “**Export**” **(Exportar)**. Las opciones especifican qué formato desea, además de información específica (dividida en “chapters” [capítulos]) que debe incluirse. Si hace clic en el capítulo que desea, se destacará en azul para indicar que estará incluido en el informe:



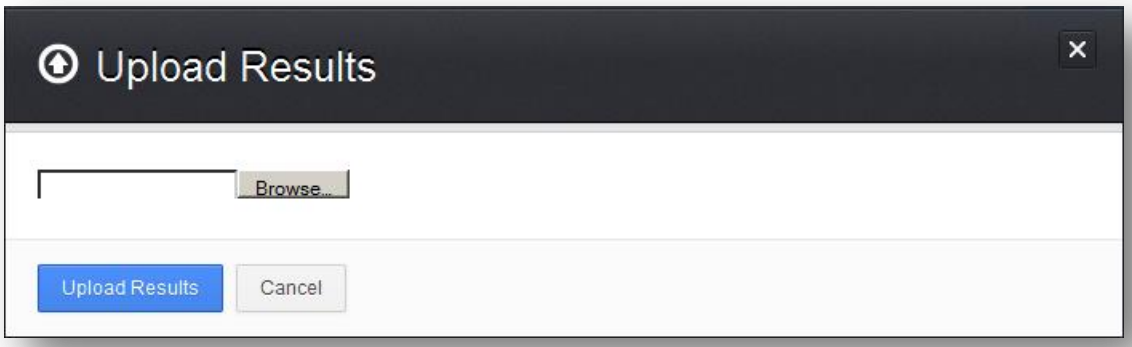
Solo los análisis de compatibilidad realizados con Nessus 5 pueden exportarse a formatos PDF o HTML con capítulos de compatibilidad. Los análisis importados de versiones anteriores de Nessus no se exportarán de esa manera.

Los informes pueden descargarse en varios formatos. Tenga en cuenta que algunos formatos no permitirán la selección de capítulos ni incluirán toda la información.

Opción	Descripción
“.nessus”	Formato basado en XML, y el estándar de facto en Nessus 4.2 y versiones posteriores. Este formato emplea un conjunto ampliado de etiquetas XML para que la extracción y el análisis sintáctico de la información sean más pormenorizados. Este informe no permite la selección de capítulos.
“.nessus (v1)”	Formato basado en XML, que se usa en las versiones de Nessus 3.2 a 4.0.2 y es compatible con Nessus 4.x y Security Center 3. Este informe no permite la selección de capítulos.
“HTML”	Un informe generado con HTML estándar que permite la selección de capítulos. Este informe se abrirá en una nueva ficha en su explorador.
“PDF”	Un informe generado con formato PDF que permite la selección de capítulos. Según el tamaño del informe, la generación del PDF puede tomar varios minutos. Se necesita Oracle Java (Java de Oracle) (anteriormente conocido como Java de Sun Microsystems) para la función de informes en PDF.
“CSV”	Una exportación en valores separados por coma (CSV) que puede utilizarse para importar a muchos programas externos como bases de datos, hojas de cálculo y otros. Este informe no permite la selección de capítulos.
“NBE export” (Exportación NBE)	Exportación basada en delimitadores de barras verticales que se puede usar para ser importada a muchos programas externos. Este informe no permite la selección de capítulos.

Después de seleccionar el formato, aparecerá el cuadro de diálogo estándar “Save File” (Guardar archivo) de su explorador web, que le permitirá guardar los resultados del análisis en la ubicación que elija.

Para importar un informe, haga clic en el botón “**Upload**” **(Cargar)** en la barra superior de la pantalla “**Results**” **(Resultados)**:



Mediante el botón “**Browse…**” **(Explorar…)**, seleccione el archivo de análisis `.nessus` que desee importar y haga clic en “**Upload Results**” **(Cargar resultados)**. Nessus analizará sintácticamente la información y la pondrá a su disposición a través de la interfaz “**Results**” **(Resultados)**.

Formato de archivo .nessus

Nessus usa un formato de archivo específico (`.nessus`) para exportar e importar análisis. Este formato brinda las siguientes ventajas:

- Está basado en XML, lo cual facilita la implementación y la compatibilidad con versiones anteriores y posteriores.
- Es autosuficiente: un único archivo `.nessus` contiene la lista de destinos, las directivas definidas por el usuario y también los resultados mismos del análisis.
- Es seguro: las contraseñas no se guardan en el archivo. En cambio, se usa una referencia a una contraseña almacenada en una ubicación segura del host local.

El proceso para crear un archivo `.nessus` que contenga los destinos, las directivas y los resultados de análisis consiste en, primero, generar la directiva y guardarla. Luego, generar la lista de direcciones de destino y, por último, ejecutar un análisis. Una vez finalizado el análisis, toda la información se podrá guardar en un archivo `.nessus` mediante la opción “**Export Results**” **(Exportar resultados)** de la ficha “**Results**” **(Resultados)**. Consulte el documento “Nessus v2 File Format” (Formato de archivo de Nessus v2) para obtener más detalles sobre los archivos `.nessus`.

Eliminar

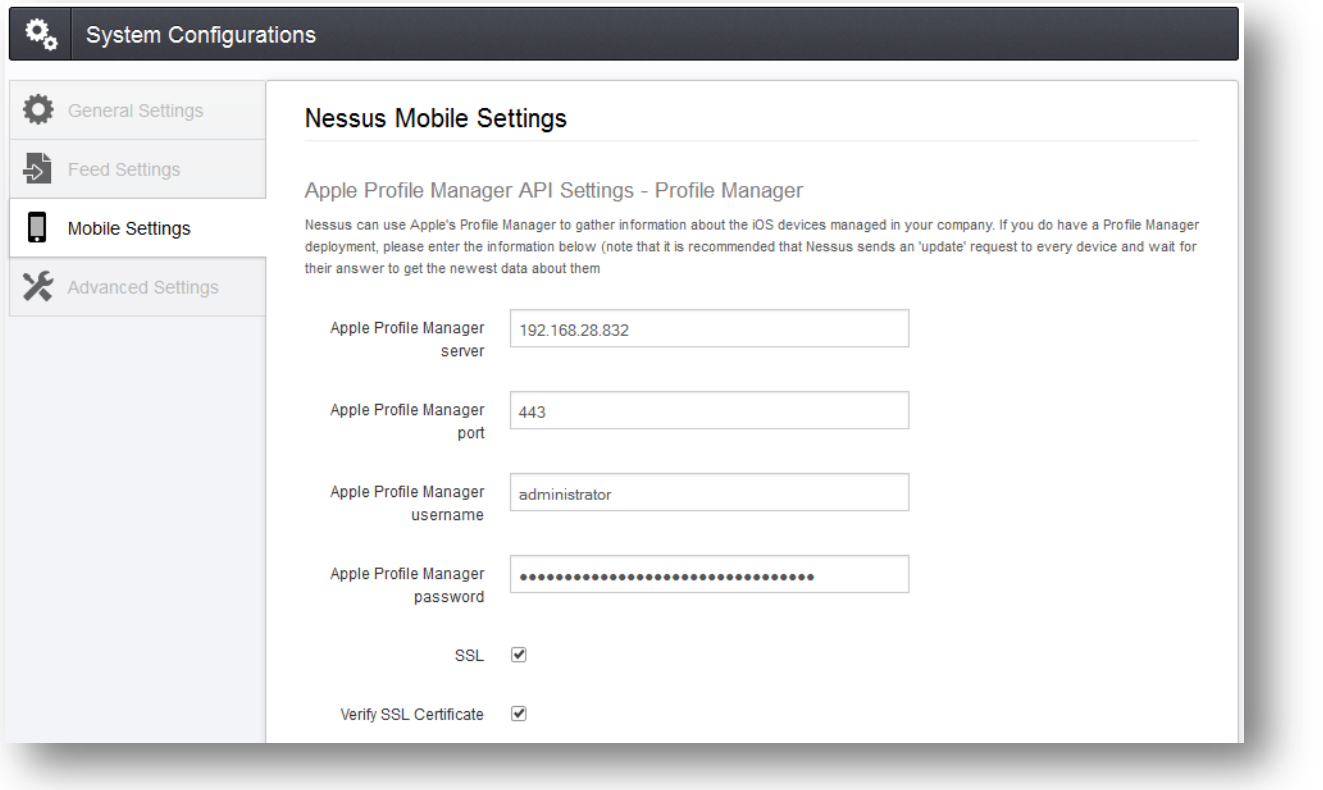
Una vez que haya terminado de usar los resultados del análisis, puede seleccionar un análisis de “**Results**” **(Resultados)**, hacer clic en “**Options**” **(Opciones)** y hacer clic en el botón “**Delete Results**” **(Eliminar resultados)**. Esto eliminará el análisis de la interfaz de usuario. **No se puede deshacer esta acción**. Use la función “**Download**” **(Descargar)** para exportar los resultados de su análisis antes de eliminarlo.

Dispositivos móviles

Nessus 5 tiene la capacidad para analizar Active Directory Service Interfaces (Interfaces de servicio de Active Directory) y Apple Profile Manager (Apple Profile Manager), lo que permite analizar el inventario y las vulnerabilidades de dispositivos con Apple iOS y Android. Nessus puede configurarse para autenticarse en estos servidores, hacer búsquedas de información en dispositivos móviles y notificar cualquier problema.

Para analizar dispositivos móviles, Nessus debe estar configurado con información de autenticación para los servidores de administración.

La funcionalidad de análisis de dispositivos móviles se detalla en el menú “**Configuration**” **(Configuración)**. La ficha “Mobile Settings” (Configuración de dispositivos móviles) ofrece un lugar para configurar el Apple Profile Manager (Apple Profile Manager) y la información del ADSI. Debido a que Nessus se autentica directamente en los servidores de administración, se creará automáticamente una directiva de análisis de dispositivos móviles con la familia de plugins móviles adecuada habilitada, y se creará un análisis de dispositivos móviles en “**Templates**” **(Plantillas)**. Con el análisis de plantillas, los dispositivos móviles se analizarán con la frecuencia necesaria.

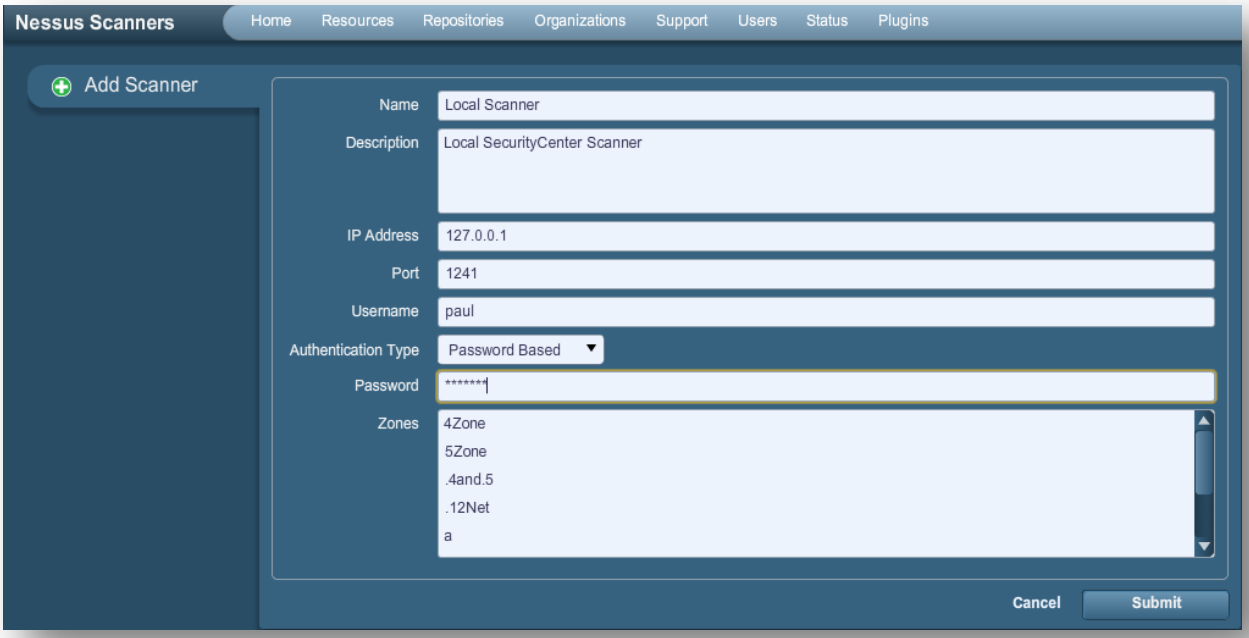


SecurityCenter

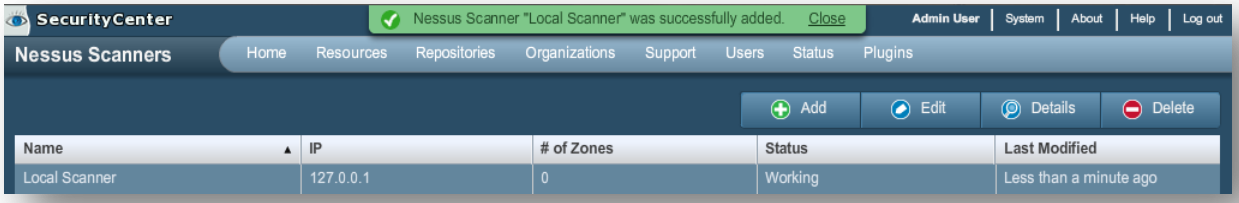
Configuración de SecurityCenter 4.0-4.2 para funcionar con Nessus

Se puede añadir un servidor “Nessus Server” (Servidor Nessus) mediante la interfaz de administración de SecurityCenter. Mediante ella, SecurityCenter se puede configurar para obtener acceso y controlar prácticamente cualquier analizador Nessus. Haga clic en la ficha “Resources” (Recursos) y luego en “**Nessus Scanners**” **(Analizadores Nessus)**. Haga clic en “**Add**” **(Agregar)** para abrir el cuadro de diálogo “Add Scanner” (Agregar analizador). Son necesarios: la dirección IP del analizador Nessus, el puerto de Nessus (el predeterminado es 1241), la identificación de inicio de sesión administrativo, el tipo de autenticación y la contraseña (creada durante la configuración de Nessus). Los campos de contraseña no se encuentran disponibles si se seleccionó la autenticación “SSL Certificate” (Certificado SSL). Además, se pueden seleccionar las Zonas a las que se asignará el analizador Nessus.

A continuación se muestra una captura de pantalla de un ejemplo de la página “Add Scanner” (Agregar analizador) de SecurityCenter:



Después de añadir correctamente el analizador, aparecerá la siguiente página tras la selección del analizador:

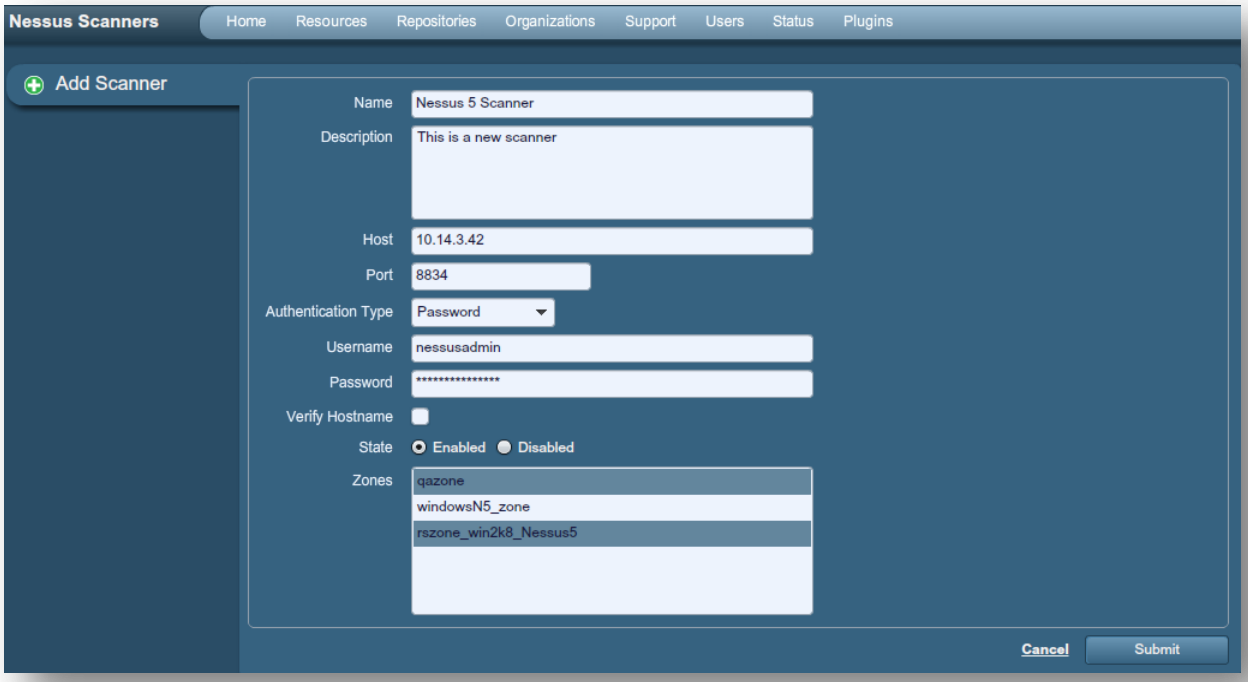


Para obtener más información, consulte la “SecurityCenter Administration Guide” (“Guía de administración de SecurityCenter”).

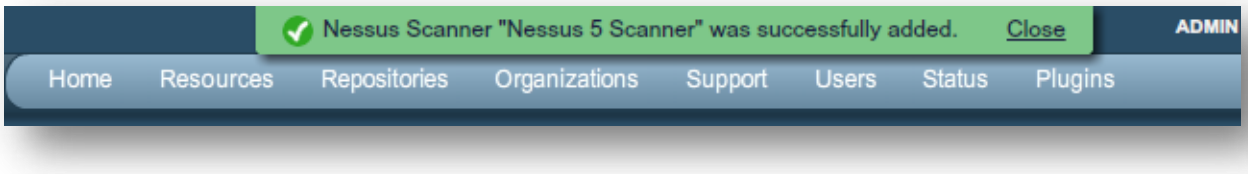
Configuración de SecurityCenter 4.4 para funcionar con Nessus

La interfaz de administración de SecurityCenter se utiliza para configurar el acceso y el control de cualquier analizador Nessus que sea versión 4.2.x o superior. Haga clic en la ficha “**Resources**” **(Recursos)** y luego en “**Nessus Scanners**” **(Analizadores Nessus)**. Haga clic en “**Add**” **(Agregar)** para abrir el cuadro de diálogo “**Add Scanner**” **(Agregar analizador)**. Son necesarios: la dirección IP o nombre del host del analizador Nessus, el puerto de Nessus (el predeterminado es 8834), el tipo de autenticación (creada durante la configuración de Nessus) y la información del certificado o contraseña e identificación de inicio de sesión administrativo. Los campos de contraseña no se encuentran disponibles si se seleccionó la autenticación “SSL Certificate” (Certificado SSL). La capacidad de verificar el nombre del host se incluye para comprobar el CommonName (CN) del certificado SSL presentado por el servidor de Nessus. El estado del analizador Nessus puede definirse como Enabled (Habilitado) o Disabled (Deshabilitado) según lo requiera; el predeterminado es Enabled (Habilitado). Pueden seleccionarse las Zonas a las que puede asignarse el analizador Nessus.

A continuación se muestra una captura de pantalla de un ejemplo de la página “**Add Scanner**” **(Agregar analizador)** de SecurityCenter 4.4:



Después de haber agregado correctamente el analizador, se muestra el siguiente banner:



Para obtener más información sobre cómo integrar Nessus y SecurityCenter, consulte la “SecurityCenter Administration Guide” (“Guía de administración de SecurityCenter”).

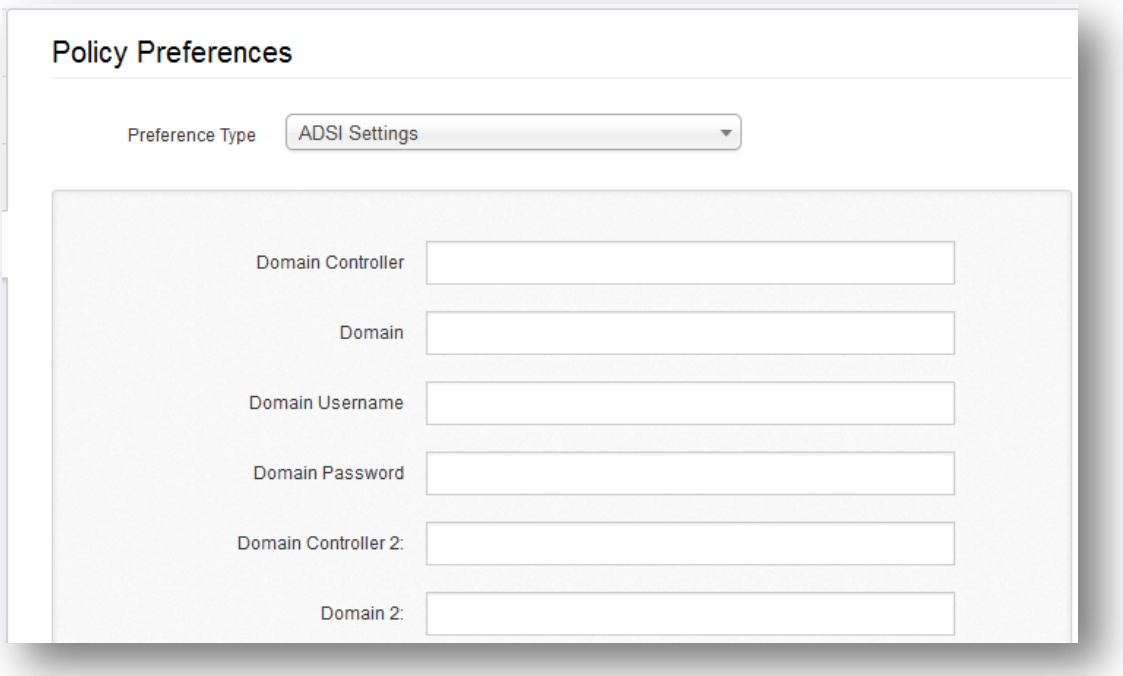
Firewalls basados en hosts
Si su servidor Nessus está configurado con un firewall local como ZoneAlarm, Sygate, BlackICE, el firewall de Windows XP o cualquier otro software de firewall, es necesario que se abran las conexiones desde la dirección IP del SecurityCenter.

De forma predeterminada, se usa el puerto 8834. En los sistemas Microsoft XP Service Pack 2 y posteriores, hacer clic en el icono “**Security Center**” **(Security Center)** que se encuentra en “**Control Panel**” **(Panel de control)**, le da al usuario la oportunidad de administrar la configuración del “Windows Firewall” (Cortafuegos de Windows). Para abrir el puerto 8834, seleccione la ficha “**Exceptions**” **(Excepciones)** y luego añada el puerto “8834” a la lista.

Si SecurityCenter está utilizando el protocolo NTP desactualizado a través del puerto 1241, los comandos anteriores usarán 1241 en lugar de 8834.

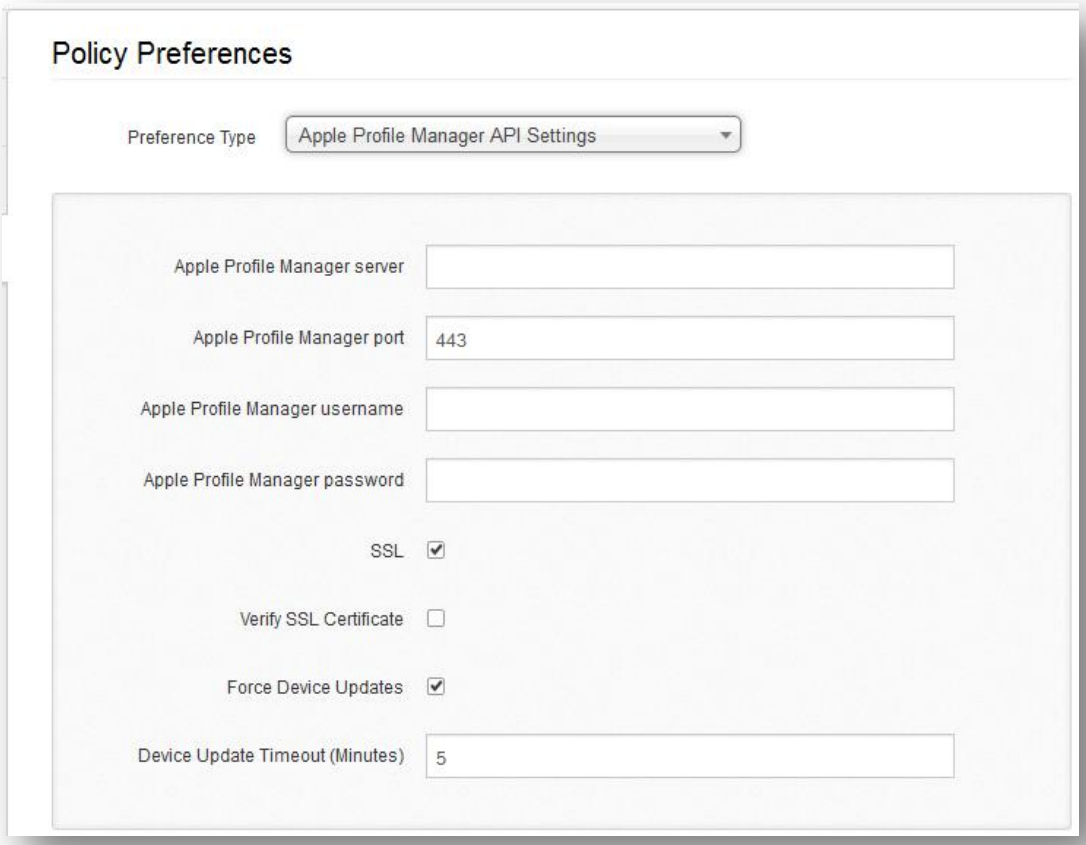
Preferencias de análisis en detalle

La ficha “**Preferences**” **(Preferencias)** en “**Policies**” **(Directivas)** incluye casi 40 menús desplegables que proporcionan un control pormenorizado de la configuración de análisis. Dedicar tiempo a explorar y configurar cada menú puede dar una gran flexibilidad y resultados de análisis mucho más precisos que si se utiliza una directiva predeterminada. En esta sección se incluye información completa sobre cada opción de “**Preferences**” **(Preferencias)**. Tenga en cuenta que se trata de una lista dinámica de opciones de configuración que depende de la fuente de plugins, las directivas de auditoría y otras funciones a las que tenga acceso el analizador Nessus conectado. Un analizador con una ProfessionalFeed puede contar con opciones de configuración más avanzadas que un analizador configurado con la HomeFeed. Esta lista también puede cambiar a medida que se añaden o modifican plugins.



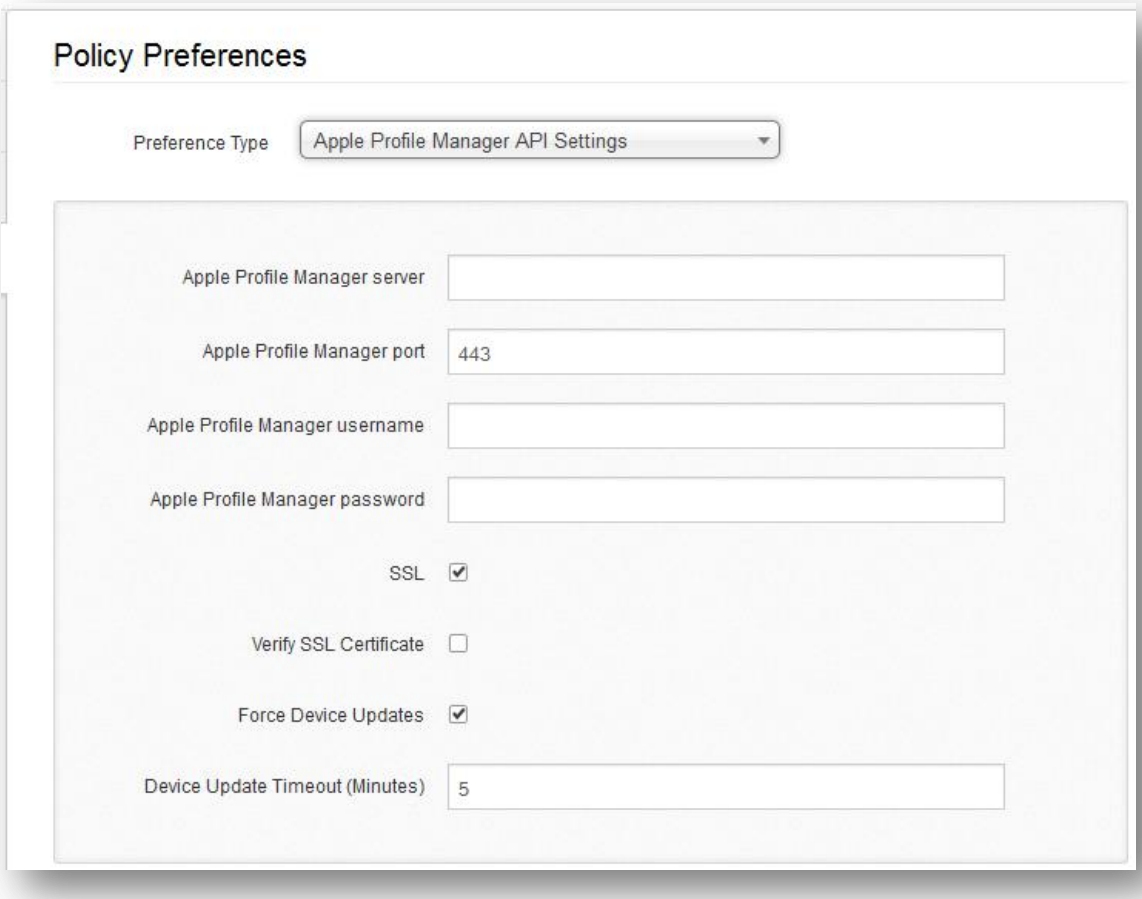
“**ADSI Settings**” **(Configuración ADSI)** le permite a Nessus consultar un servidor ActiveSync para determinar si hay algún dispositivo Android o iOS conectado. Usando las credenciales y la información del servidor, Nessus se autentica en el controlador del dominio (no en el servidor Exchange) para hacer una consulta directa de información del dispositivo. Para esta característica no es necesario especificar ningún puerto en la directiva del análisis. Esta configuración es necesaria para el análisis de dispositivos móviles.

Importante: para “ADSI Settings” (Configuración ADSI) y “Apple Profile Manager API Settings” (Configuración API de Apple Profile Manager), no es necesario que los dispositivos host se analicen directamente para obtener información sobre ellos. El analizador Nessus debe poder conectarse con el servidor de administración de dispositivos móviles (MDM) para consultar la información. Cuando se configura cualquiera de estas opciones, la directiva de análisis no requiere analizar un host de destino; usted puede usar como destino “localhost” (host local), y la directiva podrá aún conectarse con el servidor MDM para solicitar la información.

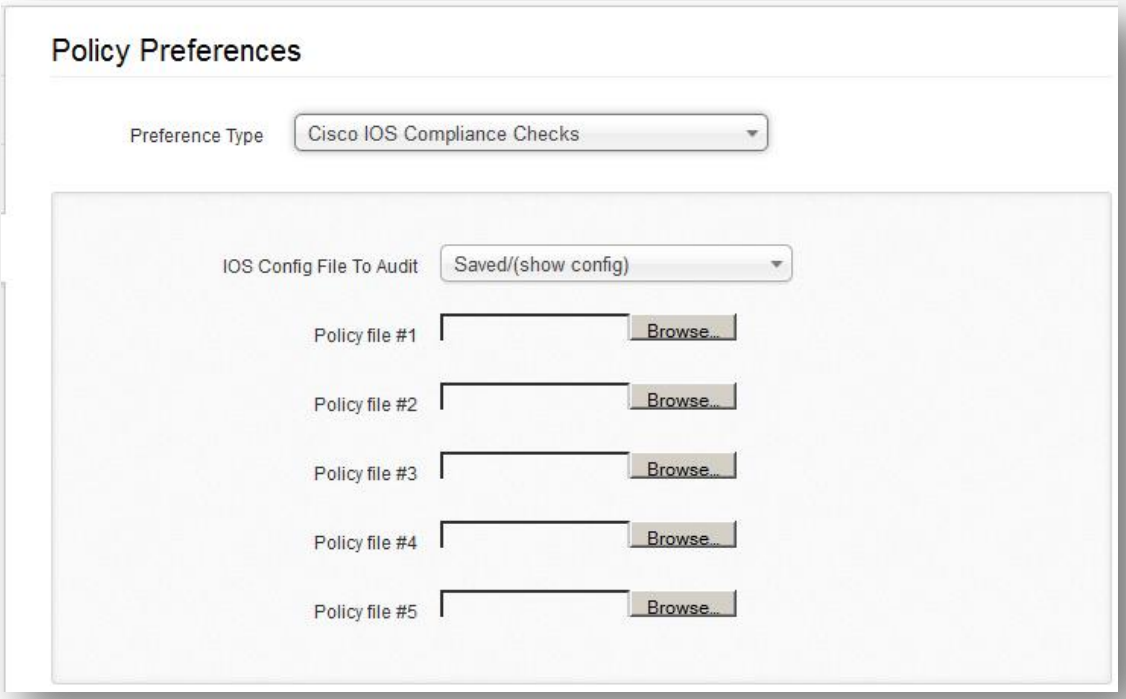


"**Apple Profile Manager API Settings**" **(Configuración API de Apple Profile Manager)** le permite a Nessus hacer una consulta al servidor Apple Profile Manager (Apple Profile Manager) para enumerar los dispositivos Apple iOS (por ejemplo, iPhone, iPad) en la red. Usando las credenciales y la información del servidor, Nessus se autentica en el Profile Manager (Profile Manager) para hacer una consulta directa de información del dispositivo. Además, puede especificar comunicaciones por SSL y ordenar al servidor que fuerce la actualización de información de un dispositivo (es decir, que cada dispositivo actualizará su información con el servidor Profile Manager [Profile Manager]).

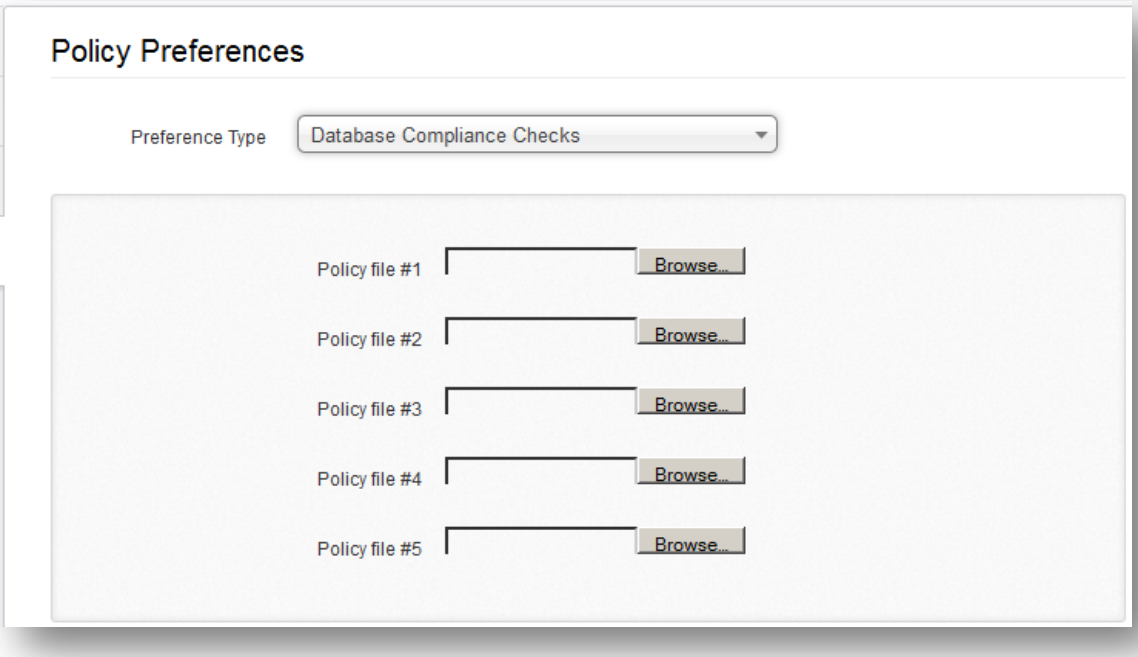
Para esta característica no es necesario especificar ningún puerto en la directiva del análisis. Esta configuración es necesaria para el análisis de dispositivos móviles.



“**Cisco IOS Compliance Checks**” **(Comprobaciones de compatibilidad con Cisco IOS)** permite a los clientes de ProfessionalFeed cargar archivos de directivas que se usarán para determinar si un dispositivo basado en Cisco IOS que se haya probado cumple con los estándares de compatibilidad especificados. Pueden seleccionarse hasta cinco directivas a la vez. Las directivas se pueden ejecutar en configuraciones Saved (Guardada) (**`show config`**), Running (En ejecución) (**`show running`**) o Startup (Inicio) (**`show startup`**).

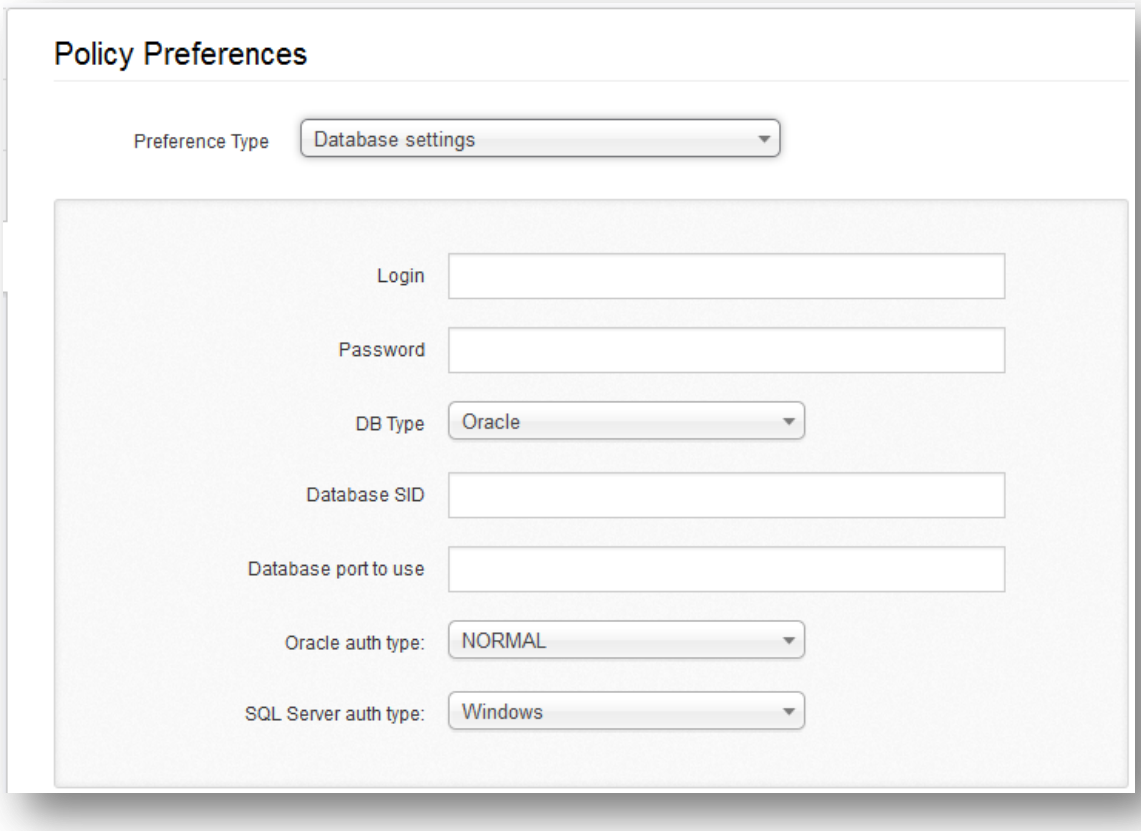


"**Database Compliance Checks**" **(Comprobaciones de compatibilidad de bases de datos)** permite a los clientes de ProfessionalFeed cargar archivos de directivas que se usarán para determinar si una base de datos que se haya probado cumple con los estándares de compatibilidad especificados. Pueden seleccionarse hasta cinco directivas a la vez.

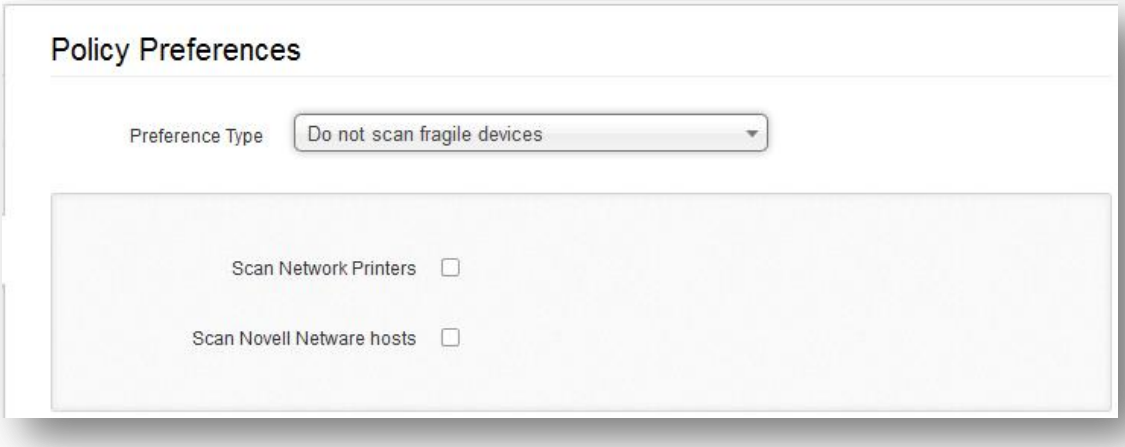


Las opciones de “**Database settings**” **(Configuración de base de datos)** se usan para especificar el tipo de base de datos que se probará, la configuración correspondiente y las credenciales:

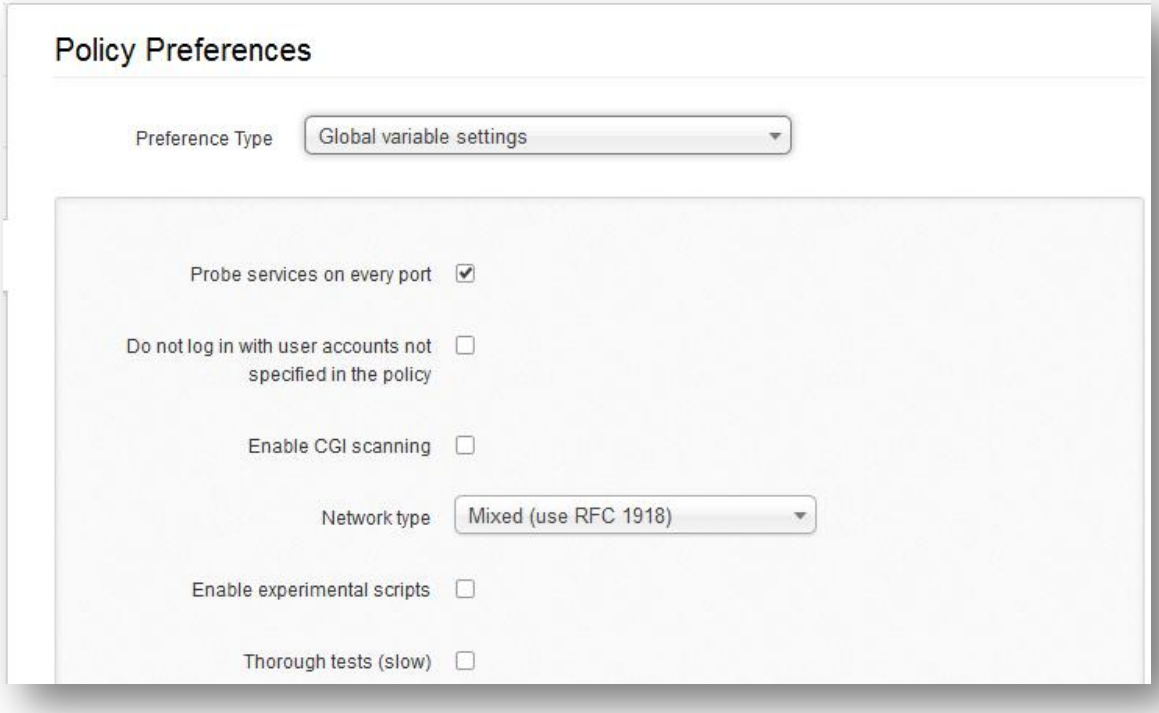
Opción	Descripción
“Login” **(Inicio de sesión)**	El nombre de usuario para la base de datos.
“Password” **(Contraseña)**	La contraseña correspondiente al nombre de usuario proporcionado.
“DB Type” **(Tipo de base de datos)**	Se admiten Oracle, SQL Server, MySQL, DB2, Informix/DRDA y PostgreSQL.
“Database SID” **(SID de base de datos)**	Identificación de la base de datos que se someterá a una auditoría.
“Database port to use” **(Puerto usado en la base de datos)**	Puerto en el que escucha la base de datos.
“Oracle auth type” **(Tipo de autenticación de Oracle)**	Se admiten NORMAL, SYSOPER y SYSDBA.
“SQL Server auth type” **(Tipo de autenticación de SQL Server)**	Se admiten Windows o SQL.



“**Do not scan fragile devices**” **(No analizar dispositivos frágiles)** ofrece dos opciones que le ordenan al analizador Nessus no analizar hosts con historial de ser “fragile” (frágiles) o propensos a bloquearse cuando reciben una entrada inesperada. Los usuarios pueden seleccionar “Scan Network Printers” (Analizar impresoras de red) o “Scan Novell Netware hosts” (Analizar hosts de Novell Netware) para ordenarle a Nessus que analice esos dispositivos específicos. Nessus los analizará solo si estas opciones están marcadas. Se recomienda que el análisis de estos dispositivos se realice de manera tal que el personal de TI pueda supervisar los sistemas en busca de problemas.



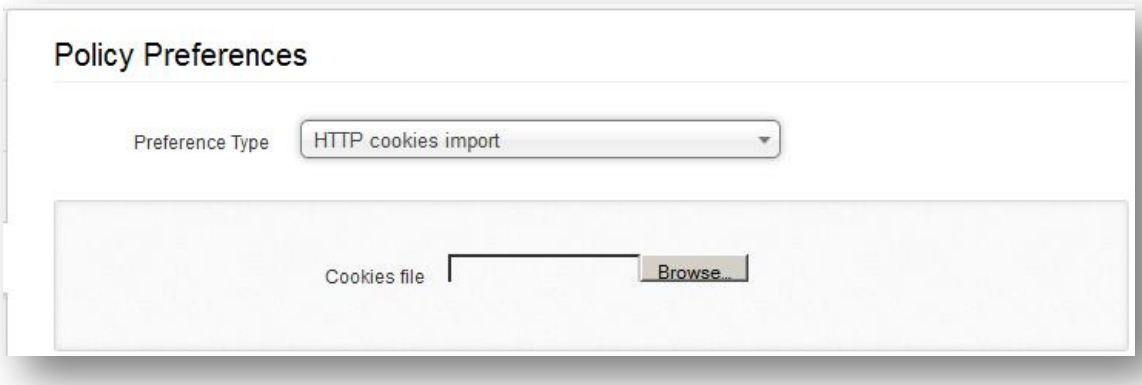
“**Global variable settings**” **(Opciones de configuración variables generales)** contiene una amplia variedad de opciones de configuración para el servidor Nessus.



Esta tabla incluye más información sobre cada opción disponible:

Opción	Descripción
“Probe services on every port” (Investigar servicios en cada puerto)	Intenta asociar cada puerto abierto con el servicio que se ejecuta en ese puerto. Tenga en cuenta que, en algunos casos poco frecuentes, esto podría alterar algunos servicios y producir efectos secundarios no previstos.
“Do not log in with user accounts not specified in the policy” (No iniciar sesión con cuentas de usuario no especificadas en la directiva)	Se usa para evitar bloqueos de cuentas si su directiva de contraseñas está ajustada para bloquear cuentas después de varios intentos no válidos.
“Enable CGI scanning” (Habilitar análisis de CGI)	Activa la comprobación de la CGI. Si se deshabilita esta opción, la auditoría de una red local se acelerará enormemente.
“Network type” (Tipo de red)	Le permite especificar si usa direcciones IP enrutables públicas, direcciones IP enrutables privadas fuera de Internet, o una mezcla de ambas. Seleccione “Mixed” (Mezcladas) si usa direcciones RFC 1918 y posee varios enrutadores dentro de su red.
“Enable experimental scripts” (Habilitar secuencias de comandos experimentales)	Hace que se usen en el análisis los plugins que se consideran experimentales. No habilite esta opción al analizar una red de producción.
“Thorough tests (slow)” (Pruebas minuciosas [lentas])	Hace que distintos plugins “work harder” (funcionen con mayor intensidad). Por ejemplo, al realizar búsquedas en recursos compartidos de archivos SMB, un plugin puede analizar 3 niveles de profundidad en lugar de 1. Esto podría ocasionar mucho más tráfico de red y mayor análisis en algunos casos. Tenga en cuenta que, por ser más minucioso, el análisis será más intrusivo y hay más probabilidades de que produzca alteraciones en la red. No obstante, cabe la posibilidad de que se produzcan mejores resultados de auditoría.
“Report verbosity” (Nivel de detalle del informe)	Una opción superior o inferior brindará más o menos información sobre la actividad del plugin en el informe.
“Report paranoia” (Paranoia del informe)	En algunos casos, Nessus no puede determinar de forma remota si hay errores o no. Si se ajusta la “report paranoia” (paranoia del informe) en “**Paranoid**” **(Paranoide)**, entonces se informarán los errores todas las veces, aun cuando haya dudas sobre el host remoto afectado. Por otra parte, una opción de paranoia “**Avoid false alarm**” **(Evitar falsa alarma)** hará que Nessus no informe ningún error cuando haya indicios de incertidumbre sobre el host remoto. La opción predeterminada (“**Normal**”) **(Normal)** constituirá el término medio entre estas dos.
“HTTP User-Agent” (Agente de usuario HTTP)	Especifica el tipo de explorador web al que Nessus suplantará durante el análisis.
“SSL certificate to use” (Certificado de SSL a usar)	Permite que Nessus use un certificado SSL del lado cliente para comunicarse con un host remoto.
“SSL CA to trust” (Entidad de certificación [CA] en la que confiar)	Especifica una Certificate Authority (CA) (Entidad de certificación) en la que confiará Nessus.
“SSL key to use” (Clave de SSL a usar)	Especifica una clave de SSL local que se usará para comunicarse con el host remoto.
“SSL password for SSL key” (Contraseña de SSL para la clave de SSL)	La contraseña para administrar la clave de SSL especificada.

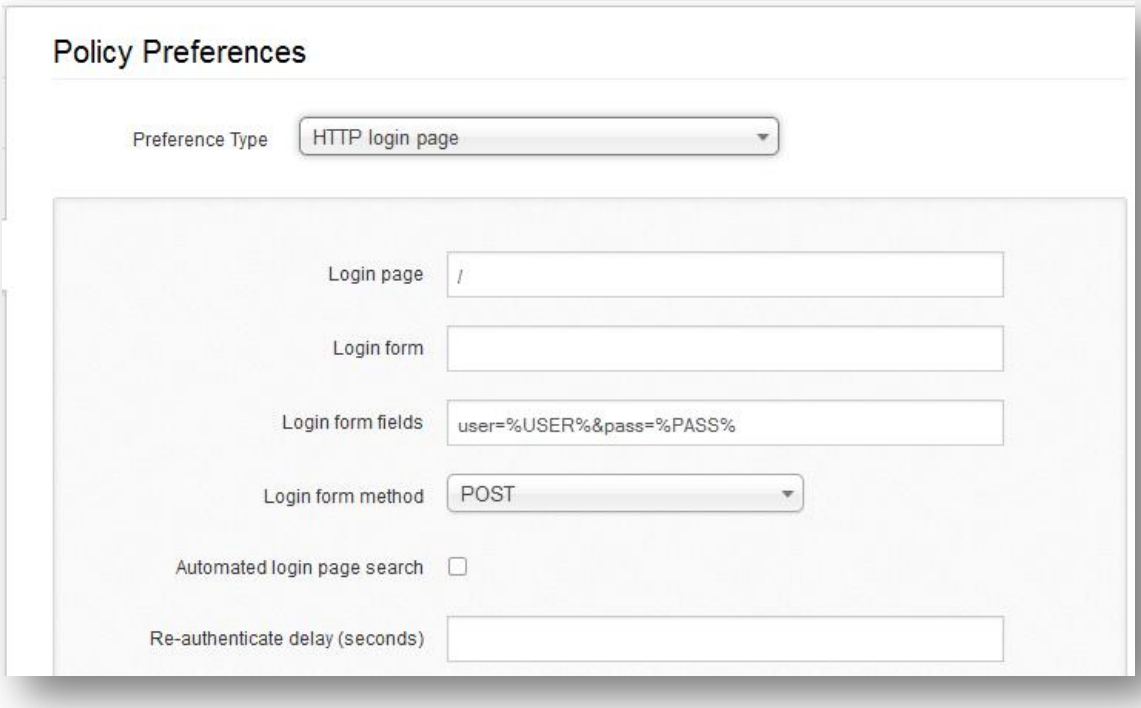
Para facilitar las pruebas de aplicaciones web, Nessus puede importar cookies HTTP de otro software (por ejemplo, un explorador web, un proxy web, etc.) mediante la configuración "**HTTP cookies import**" **(Importación de cookies HTTP)**. Se puede cargar un archivo de cookies para que Nessus use las cookies al intentar obtener acceso a la aplicación web. Este archivo debe estar en formato Netscape.



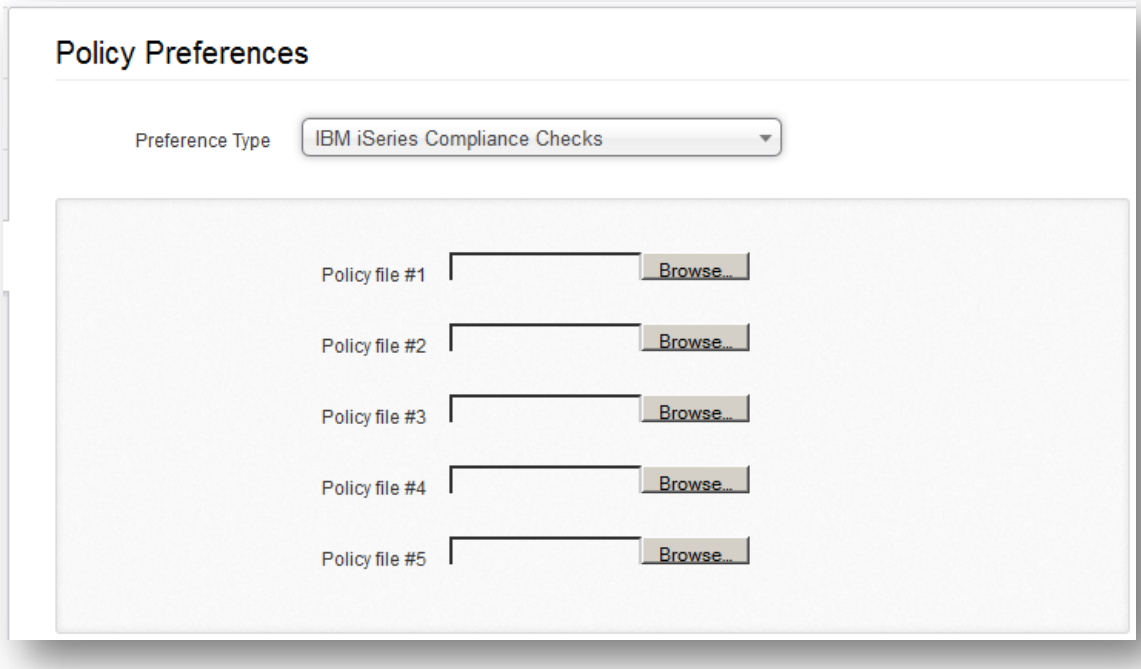
La configuración "**HTTP login page**" **(Página de inicio de sesión HTTP)** permite controlar el lugar en el que comienzan las pruebas autenticadas de una aplicación web personalizada.

Opción	Descripción
"Login page" (Página de inicio de sesión)	La dirección URL base de la página de inicio de sesión de la aplicación.
"Login form" (Formulario de inicio de sesión)	El parámetro "action" (acción) correspondiente al método de formulario. Por ejemplo, el formulario de inicio de sesión para `<form method="POST" name="auth_form" action="/login.php">` sería "`/login.php`".
"Login form fields" (Campos de formulario de inicio de sesión)	Especifica los parámetros de autenticación (por ejemplo, `login=%USER%&password=%PASS%`). Si se usan las palabras clave %USER% y %PASS%, se reemplazarán por los valores que se proporcionan en el menú desplegable "Login configurations". Este campo se puede usar para proporcionar más de dos parámetros, de ser necesarios [por ejemplo, para el proceso de autenticación se requiere un nombre de "group" (grupo) u otro dato].
"Login form method" (Método de formulario de inicio de sesión)	Especifica si la acción de inicio de sesión se lleva a cabo mediante una solicitud GET o POST.
"Automated login page search" (Búsqueda automatizada de página de inicio de sesión)	Ordena a Nessus que busque una página de inicio de sesión.
"Re-authenticate delay (seconds)" (Retardo de nueva autenticación [segundos])	La demora entre los intentos de autenticación. Esto resulta de utilidad para evitar que se activen mecanismos de bloqueo de fuerza bruta.
"Check authentication on page" (Comprobar autenticación en la página)	La dirección URL de una página web protegida que requiere autenticación, con el fin de brindar mayor ayuda a Nessus al determinar el estado de la autenticación.

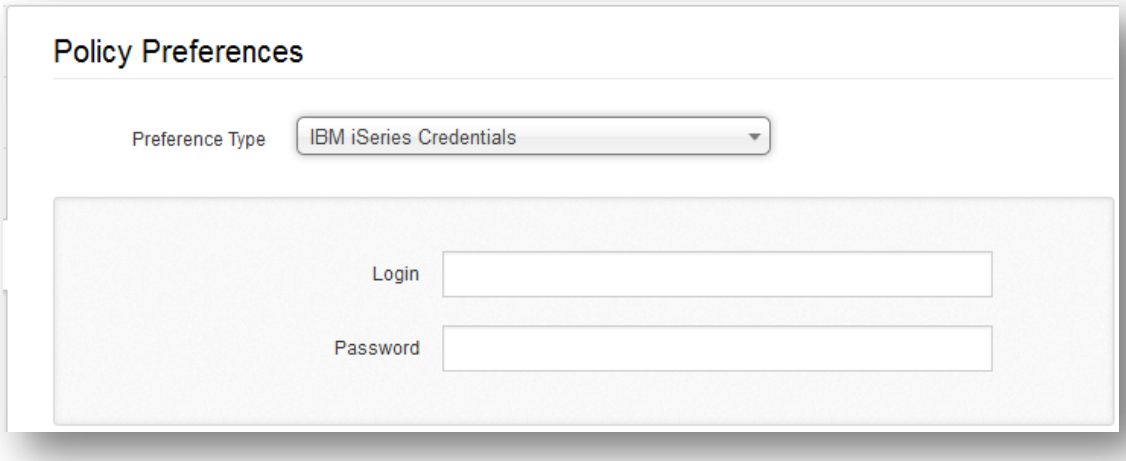
“Follow 30x redirections (# of levels)” (Seguir redireccionamientos 30x [cantidad de niveles])	Si se recibe un código de redireccionamiento 30x por parte de un servidor web, esto indica a Nessus que siga o no el enlace proporcionado.
“Authenticated regex” (Regex autenticada)	Es el patrón de regex que se buscará en la página de inicio de sesión. Para determinar el estado de la sesión, no siempre es suficiente con solo recibir un código de respuesta 200. Nessus puede intentar buscar coincidencias con una cadena determinada, tal como “Authentication successful!” (Autenticación correcta).
“Invert test (disconnected if regex matches)” (Invertir prueba [se desconecta si la regex coincide])	Es el patrón de regex que se buscará en la página de inicio de sesión y, si se encuentra, indicará a Nessus que se produjo un error en la autenticación (por ejemplo, “Authentication failed!” [Error de autenticación]).
“Match regex on HTTP headers” (Buscar coincidencia de regex en encabezados HTTP)	En lugar de buscar el cuerpo de la respuesta, Nessus puede buscar los encabezados de las respuestas HTTP que contengan un patrón de regex específico y así determinar mejor el estado de autenticación.
“Case insensitive regex” (Regex sin distinción de mayúsculas y minúsculas)	Las búsquedas de regex distinguen mayúsculas de minúsculas de forma predeterminada. Esta opción ordena a Nessus que no distinga entre mayúsculas y minúsculas.
“Abort web application tests if login fails” (Interrumpir las pruebas de aplicaciones web si hay error de inicio de sesión)	Si no funcionan las credenciales suministradas, Nessus interrumpirá las pruebas de aplicaciones web personalizadas (pero no las familias de plugins de CGI).



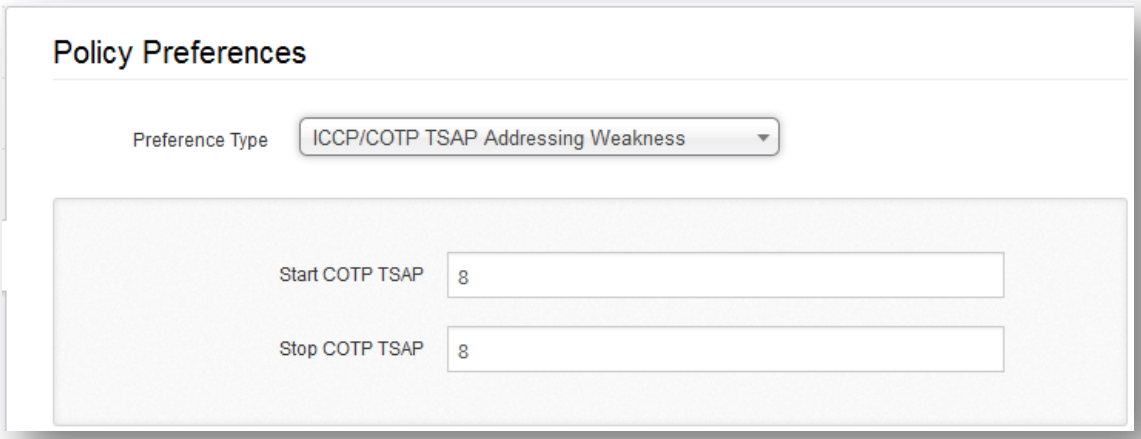
"**IBM iSeries Compliance Checks**" **(Comprobaciones de compatibilidad de IBM iSeries)** permite a los clientes de ProfessionalFeed cargar archivos de directivas que se usarán para determinar si un sistema IBM iSeries que se haya probado cumple con los estándares de compatibilidad especificados. Pueden seleccionarse hasta cinco directivas a la vez.



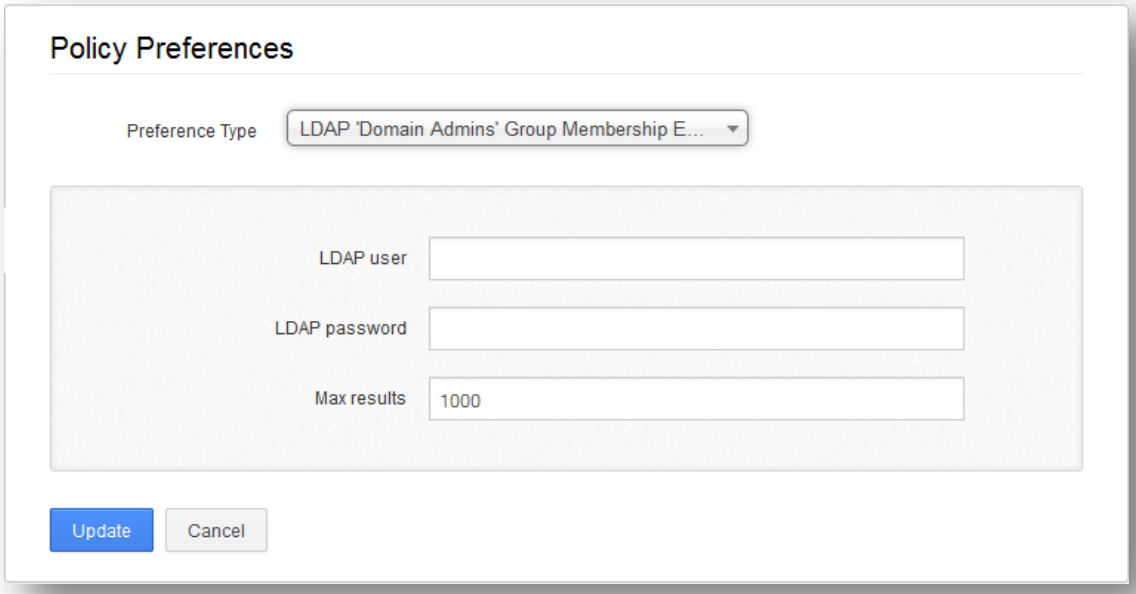
Las preferencias "**IBM iSeries Credentials**" **(Credenciales de IBM iSeries)** proporcionan un lugar que le dé a Nessus credenciales para autenticarse en un sistema IBM iSeries. Esto es necesario para la auditoría de compatibilidad, por ejemplo.



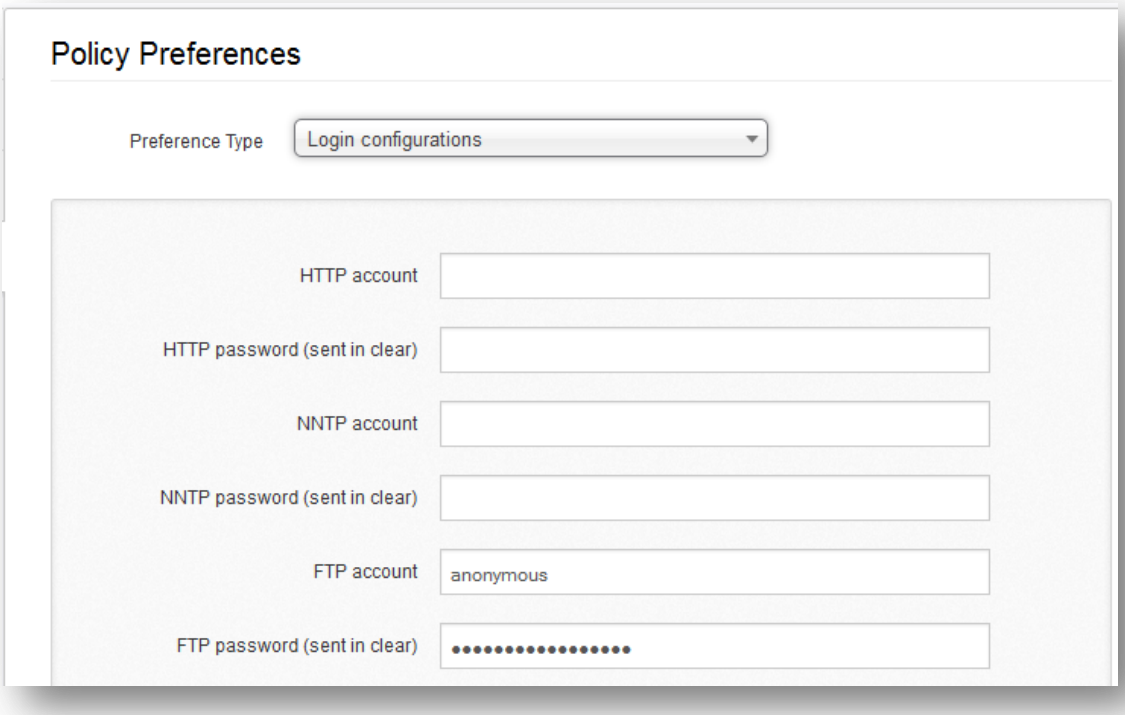
El menú "**ICCP/COTP TSAP Addressing**" **(Direccionamiento ICCP/COTP TSAP)** aborda específicamente las comprobaciones SCADA. Determina un valor de Transport Service Access Points, TSAP (Puntos de acceso al servicio de transporte) del Connection Oriented Transport Protocol, COTP (Protocolo de transporte orientado a la conexión) en un servidor ICCP, mediante la prueba de posibles valores. De manera predeterminada, los valores de inicio y detención están establecidos en "8".



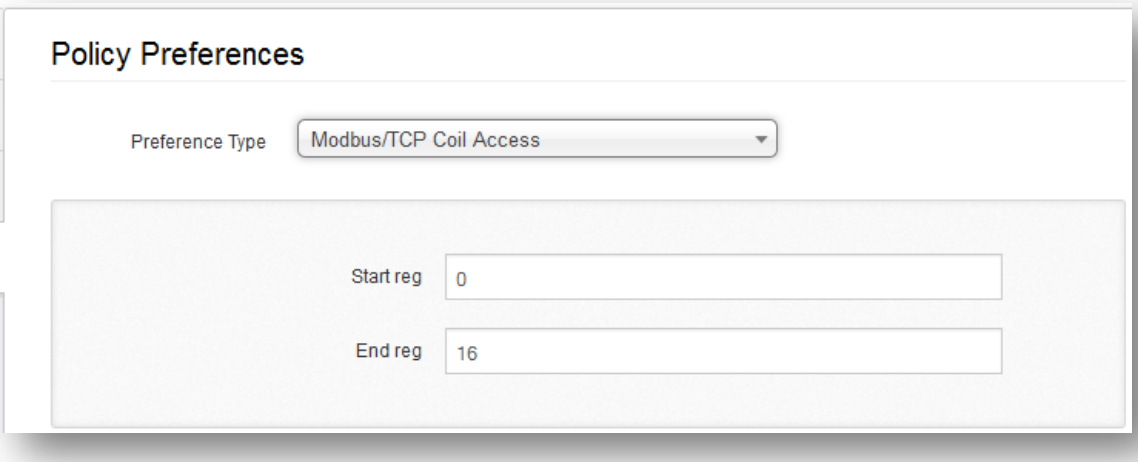
El menú “LDAP ‘Domain Admins’ Group Membership Enumeration” (Enumeración de pertenencia a grupo ‘Domain Admins’ de LDAP) le permite introducir un conjunto de credenciales LDAP que se pueden utilizar para enumerar una lista de miembros del grupo “Domain Admins” (Administradores de dominio) en el directorio remoto LDAP.



“**Login configurations**” **(Configuraciones de inicio de sesión)** permite al analizador Nessus usar credenciales al probar HTTP, NNTP, FTP, POP2, POP3 o IMAP. Al proporcionar credenciales, es posible que Nessus tenga la capacidad de llevar a cabo comprobaciones más minuciosas para determinar vulnerabilidades. Las credenciales HTTP suministradas aquí se usarán solo para autenticación básica e implícita. Para configurar credenciales para una aplicación web personalizada, use el menú desplegable “HTTP login page” (Página de inicio de sesión HTTP).

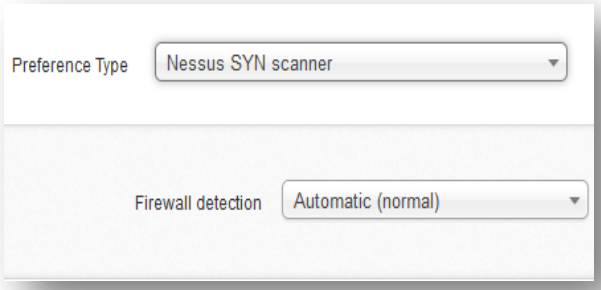


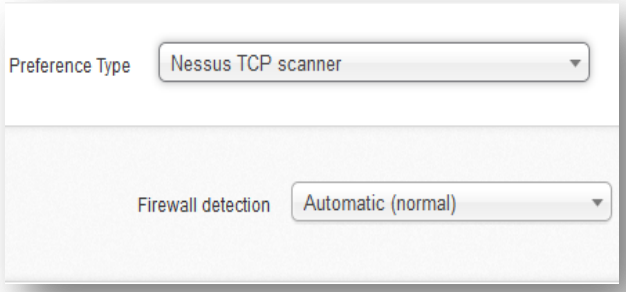
Las opciones “**Modbus/TCP Coil Access**” **(Acceso a bobinas de Modbus/TCP)** se encuentran disponibles para los usuarios de ProfessionalFeed. Este elemento de menú desplegable es generado de manera dinámica por los plugins de SCADA, disponibles mediante la ProfessionalFeed. Modbus usa un código de función de 1 para leer “coils” (bobinas) en un dispositivo esclavo Modbus. Las bobinas representan valores de salidas binarias, y normalmente se asignan a actuadores. La capacidad de leer bobinas puede ayudar a un atacante a perfilar un sistema e identificar rangos de registros para alterar mediante el mensaje “write coil” (escribir bobinas). Los valores predeterminados para esta opción son “0” para el registro inicial y “16” para el registro final.



Las opciones “**Nessus SYN scanner**” **(Analizador SYN de Nessus)** y “**Nessus TCP scanner**” **(Analizador TCP de Nessus)** le permiten ajustar mejor los analizadores nativos SYN y TCP para que detecten la presencia de un firewall.

Valor	Descripción
“Automatic (normal)” (Automática [normal])	Esta opción puede ayudar a identificar si se encuentra un firewall entre el analizador y el destino (**predeterminado**).
“Disabled (softer)” (Deshabilitada [más laxa])	Deshabilita la característica de **detección de firewall**.
“Do not detect RST rate limitation (soft)” (No detectar limitación de frecuencia RST [laxa])	Deshabilita la capacidad de supervisar la frecuencia con la que se efectúan los restablecimientos y de determinar si se configuró una limitación en un dispositivo de red descendente.
“Ignore closed ports (aggressive)” (Ignorar puertos cerrados [agresiva])	Intentará ejecutar plugins, aun si el puerto parece cerrado. Se recomienda no usar esta opción en una red de producción.

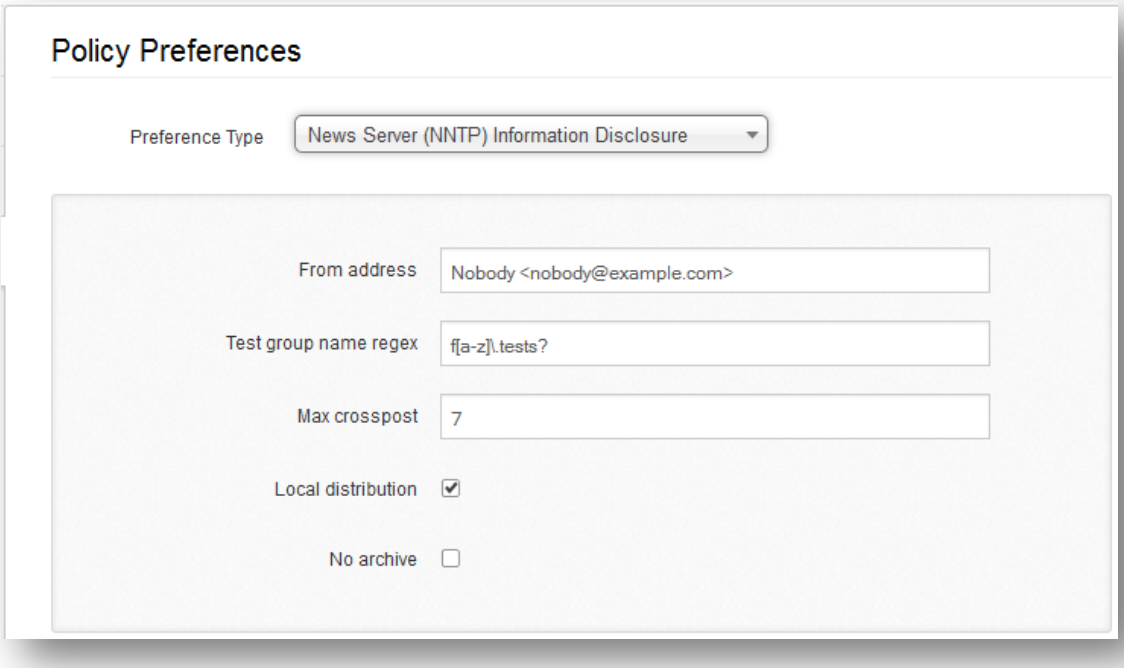




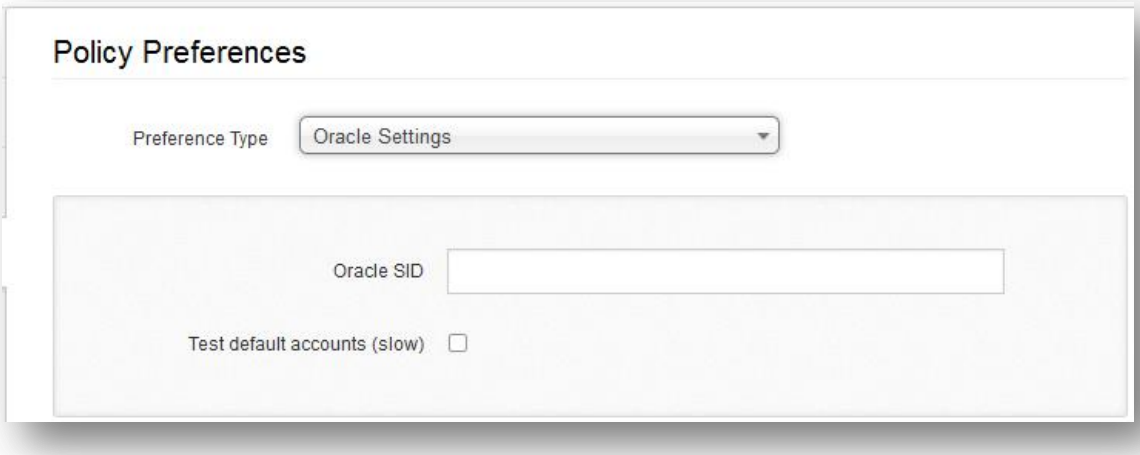
“**News Server (NNTP) Information Disclosure**” **(Divulgación de información de servidores de noticias [NNTP])** se puede usar para determinar si hay servidores de noticias con la capacidad de retransmitir correo no deseado. Nessus intentará publicar un mensaje de noticias en un servidor/servidores NNTP (Protocolo de transporte de noticias en red), y puede probar si también es posible publicar un mensaje en los servidores de noticias ascendentes.

Opción	Descripción
“From address” (De dirección)	La dirección que Nessus usará cuando intente publicar un mensaje en el (los) servidor(es) de noticias. Este mensaje se eliminará a sí mismo de forma automática después de un corto período.
“Test group name regex” (Regex de nombre de grupo de prueba)	El nombre del (de los) grupo(s) de noticias que recibirá(n) un mensaje de prueba desde la dirección especificada. El nombre se puede especificar como una expresión regular (regex) para que el mensaje se pueda publicar en varios grupos de noticias de forma simultánea. Por ejemplo, el valor predeterminado “**f[a-z]\.tests?**” difundirá un mensaje de correo a todos los grupos de noticias con nombres que comiencen con cualquier letra (de la “a” a la “z”) y que finalicen con “.tests” (o alguna variación que coincidiera con la cadena). El signo de pregunta funciona como carácter comodín opcional.
“Max crosspost” (Publicación cruzada máxima)	La cantidad máxima de servidores de noticias que recibirán la publicación de prueba, sin importar la cantidad de coincidencias con el nombre. Por ejemplo, si Max crosspost (Publicación cruzada máxima) es “**7**”, el mensaje de prueba solo se enviará a siete servidores de noticias, aun cuando haya 2000 servidores de noticias que coincidan con la regex en este campo.

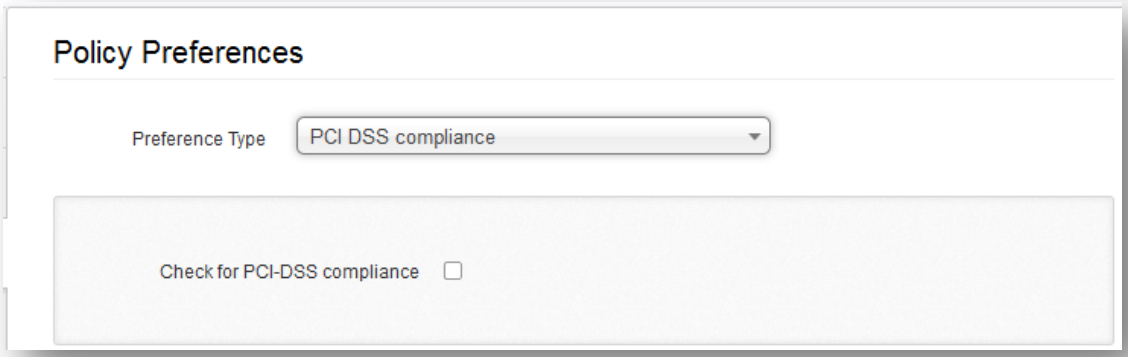
“Local distribution” (Distribución local)	Si se selecciona esta opción, Nessus únicamente intentará publicar un mensaje en el (los) servidor(es) de noticias local(es). De lo contrario, se intentará reenviar el mensaje por el canal ascendente.
“No archive” (No archivar)	Si se selecciona esta opción, Nessus solicitará que no se archive el mensaje de prueba que se envía al (a los) servidor(es) de noticias. De lo contrario, el mensaje se archivará como cualquier otra publicación.



“**Oracle Settings**” **(Opciones de configuración de Oracle)** configura Nessus con el Oracle Database SID (SID de base de datos Oracle) e incluye una opción para probar si existen cuentas predeterminadas conocidas en el software de Oracle.



“**PCI DSS Compliance**” **(Compatibilidad PCI DSS)** indicará a Nessus que compare los resultados del análisis con los estándares de compatibilidad de PCI DSS actuales. Esta característica solo está disponible para los clientes de ProfessionalFeed.



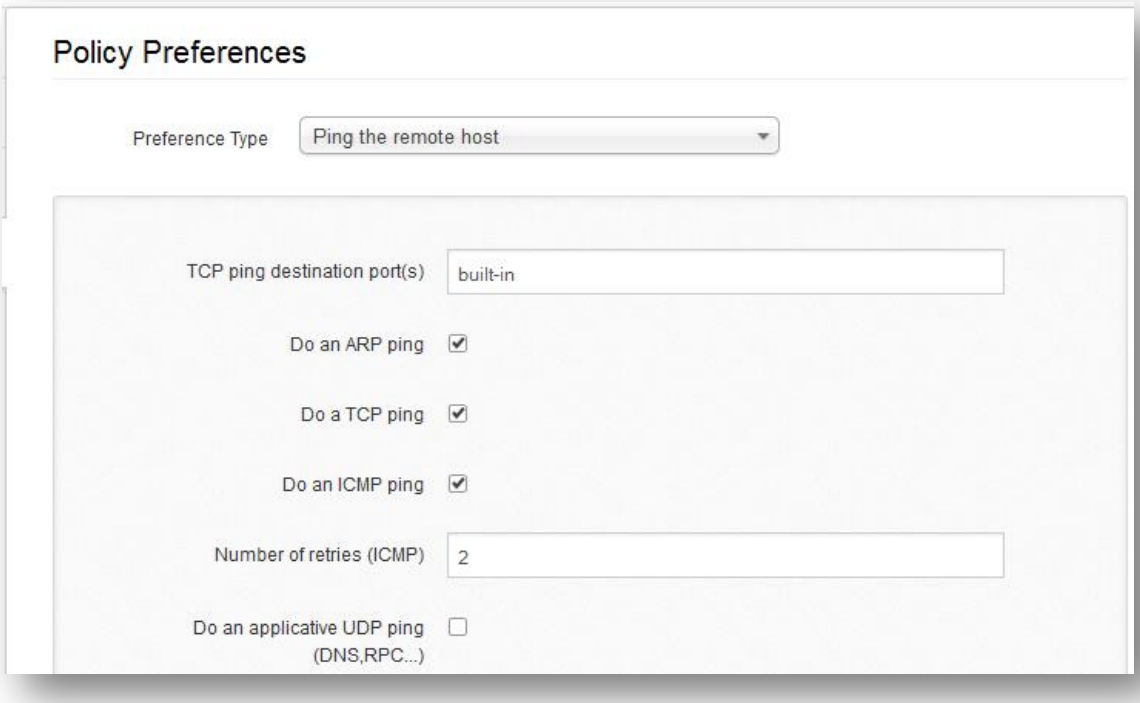
Nessus puede aprovechar las credenciales para los sistemas de administración de revisiones Red Hat Satellite Server, WSUS, SCCM y VMware Go (ex Shavlik) a fin de ejecutar auditorías de revisiones en sistemas para los que pueda no haber credenciales disponibles para el analizador Nessus. Puede encontrar opciones para estos sistemas de administración de revisiones en “Preferences” (Preferencias) en sus menús desplegables correspondientes: “**Patch Management: Red Hat Satellite Server Settings**” **(Administración de revisiones: configuración de servidor Red Hat Satellite)**, “**Patch Management: SCCM Server Settings**” **(Administración de revisiones: configuración de servidor SCCM)**, “**Patch Management: VMware Go Server Settings**” **(Administración de revisiones: configuración de VMware Go Server)** y “**Patch Management: WSUS Server Settings**” **(Administración de revisiones: configuración de servidor WSUS)**. Puede encontrar más información acerca de cómo usar Nessus para analizar hosts a través de estos sistemas de administración de revisiones en el documento “Patch Management Integration” (“Integración de administración de revisiones”).

Las opciones de “**Ping the remote host**” **(Efectuar pings al host remoto)** permiten el control pormenorizado de la capacidad de Nessus para efectuar pings a hosts durante los análisis de detección. Esto se puede realizar mediante los pings ARP, TCP, ICMP o UDP de aplicación.

Opción	Descripción
“TCP ping destination port(s)” (Puerto[s] de destino de pings TCP)	Especifica la lista de puertos que se comprobarán mediante el ping TCP. Si no tiene seguridad sobre los puertos, deje este parámetro con el valor predeterminado “built-in” (Incorporado).
“Number of Retries (ICMP)” (Cantidad de reintentos [ICMP])	Le permite especificar la cantidad de intentos para tratar de efectuar un ping al host remoto. El valor predeterminado está establecido en 6.
“Do an applicative UDP ping (DNS, RPC…)” (Hacer un ping de aplicaciones UDP [DNS, RPC…])	Efectúa un ping UDP respecto de aplicaciones basadas en UDP específicas, incluidos DNS (puerto 53), RPC (puerto 111), NTP (puerto 123) y RIP (puerto 520).
“Make the dead hosts appear in the report” (Hacer que los hosts inactivos aparezcan en el informe)	Si se selecciona esta opción, los hosts que no respondieron a la solicitud de ping se incluirán en el informe de seguridad como hosts inactivos.

“Log live hosts in the report” (Registrar los hosts activos en el informe)	Seleccione esta opción para informar específicamente de la capacidad de realizar pings satisfactorios a hosts remotos.
“Test the local Nessus host” (Probar el host local de Nessus)	Esta opción le permite incluir el host local de Nessus en el análisis o excluirlo de este. Se usa cuando el host de Nessus se encuentra dentro del rango de redes de destino del análisis.
“Fast network discovery” (Detección rápida de red)	De forma predeterminada, cuando Nessus efectúa “pings” a una IP remota y recibe una respuesta, realiza comprobaciones adicionales para verificar que no se trate de un proxy transparente ni de un equilibrador de carga que pudieran devolver ruido y ningún resultado (algunos dispositivos responden a cada puerto 1-65535, pero no hay servicio detrás de ellos). Dichas comprobaciones pueden llevar cierto tiempo, en especial si el host remoto tiene un firewall. Si la opción “fast network discovery” (Detección rápida de red) se encuentra habilitada, Nessus no realizará estas comprobaciones.

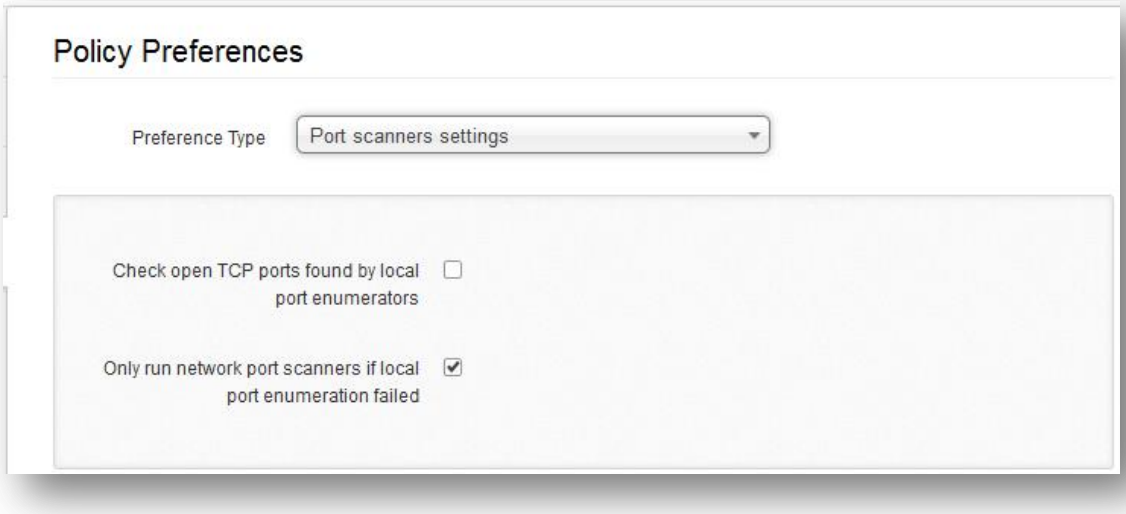
Para analizar sistemas invitados VMware, “ping” debe estar deshabilitado. En la directiva de análisis situada en “Advanced” -> “Ping the remote host” (Opciones avanzadas - > Efectuar pings al host remoto), desmarque los pings TCP, ICMP y ARP.



“**Patch Management**” **(Administración de revisiones)** brinda varias opciones para usar servidores de administración de revisiones de terceros a fin de hacer consultas a hosts sobre información de vulnerabilidades. Puede encontrar más información acerca de estas opciones de configuración en el documento “Patch Management Integration” “Integración de administración de revisiones”).

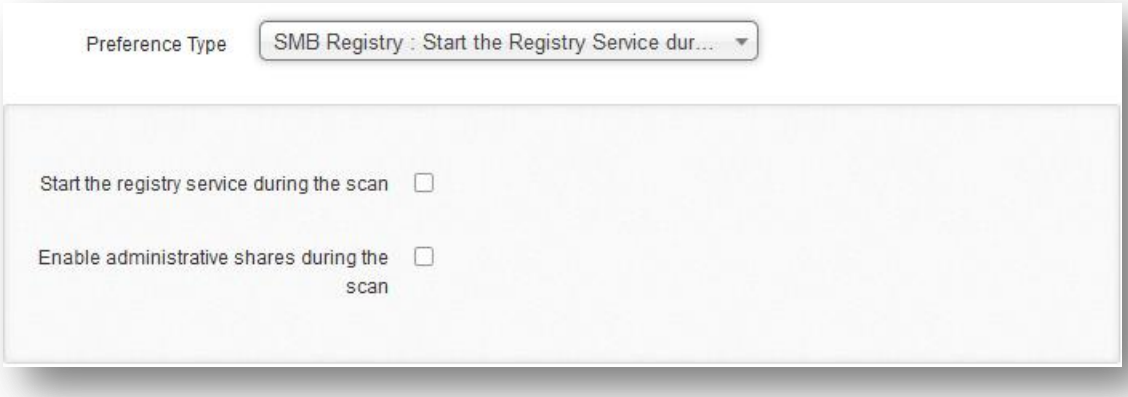
“**Port scanner settings**” **(Opciones de configuración de analizador de puertos)** proporciona dos opciones para el control adicional de la actividad de análisis de puertos:

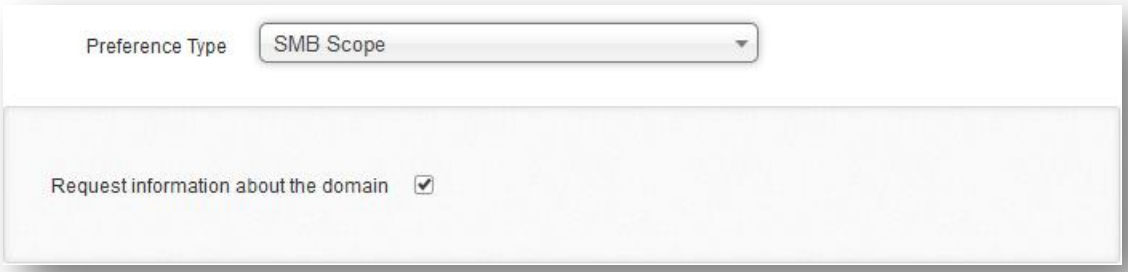
Opción	Descripción
“Check open TCP ports found by local port enumerators” (Comprobar puertos TCP abiertos encontrados por enumeradores de puertos locales)	Si un enumerador de puertos local (por ejemplo, WMI o netstat) encuentra un puerto, Nessus también verificará que esté abierto de forma remota. Esto ayuda a determinar si se está usando algún tipo de control de acceso (por ejemplo, contenedores TCP o firewalls).
“Only run network port scanners if local port enumeration failed” (Ejecutar analizadores de puertos de red únicamente si hay error de enumeración de puertos local)	De lo contrario, tenga en cuenta primero la enumeración de puertos local.



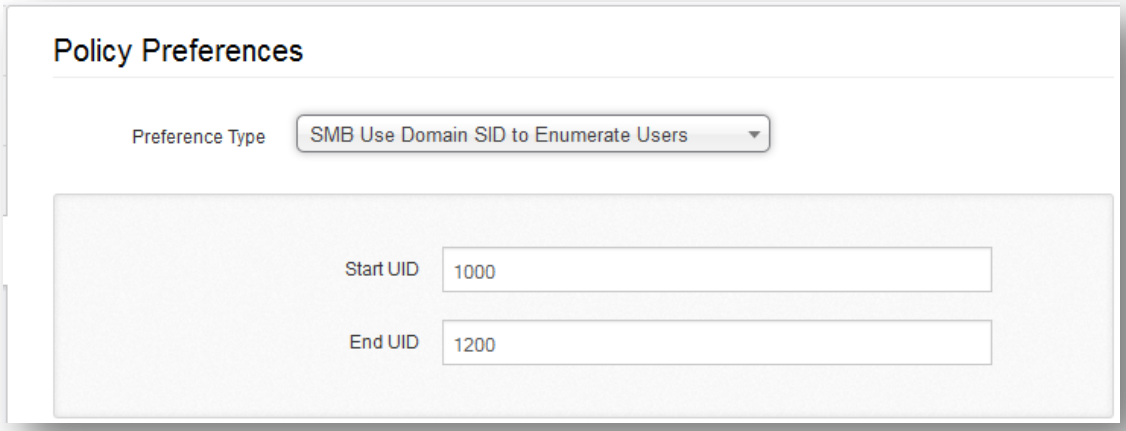
“**SMB Registry: Start the Registry Service during the scan**” **(Registro SMB: iniciar el Servicio de registro durante el análisis)** permite al servicio facilitar algunos de los requisitos de análisis para equipos que pueden no tener en ejecución el Registro SMB de forma permanente.

En el menú “**SMB Scope**” **(Alcance SMB)**, si está establecida la opción “**Request information about the domain**” **(Solicitar información acerca del dominio)**, se consultará a los usuarios del dominio en lugar de los usuarios locales.

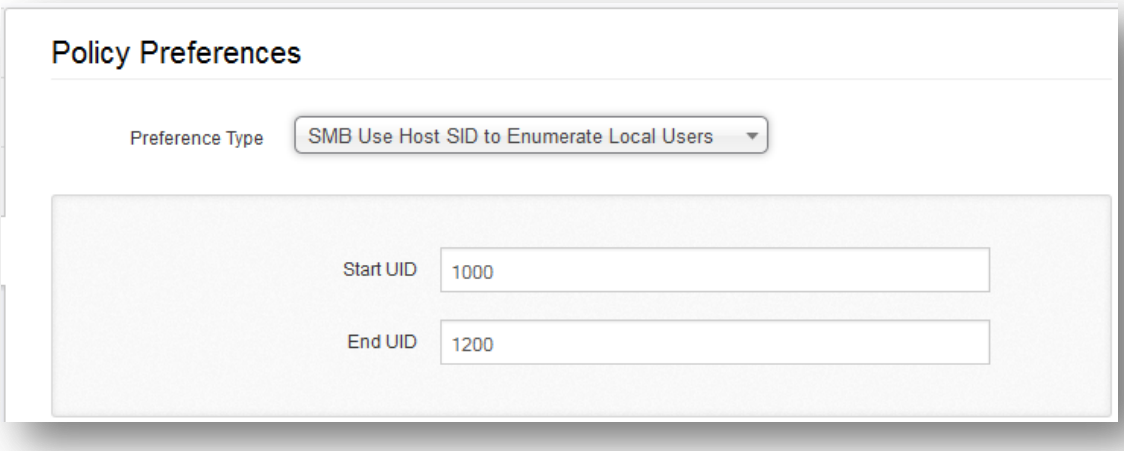




"**SMB Use Domain SID to Enumerate Users**" **(SMB, usar SID de dominio para enumerar usuarios)** especifica el rango de SID para usar en la realización de búsquedas inversas de nombres de usuarios en el dominio. Para la mayoría de los análisis se recomienda la opción predeterminada.

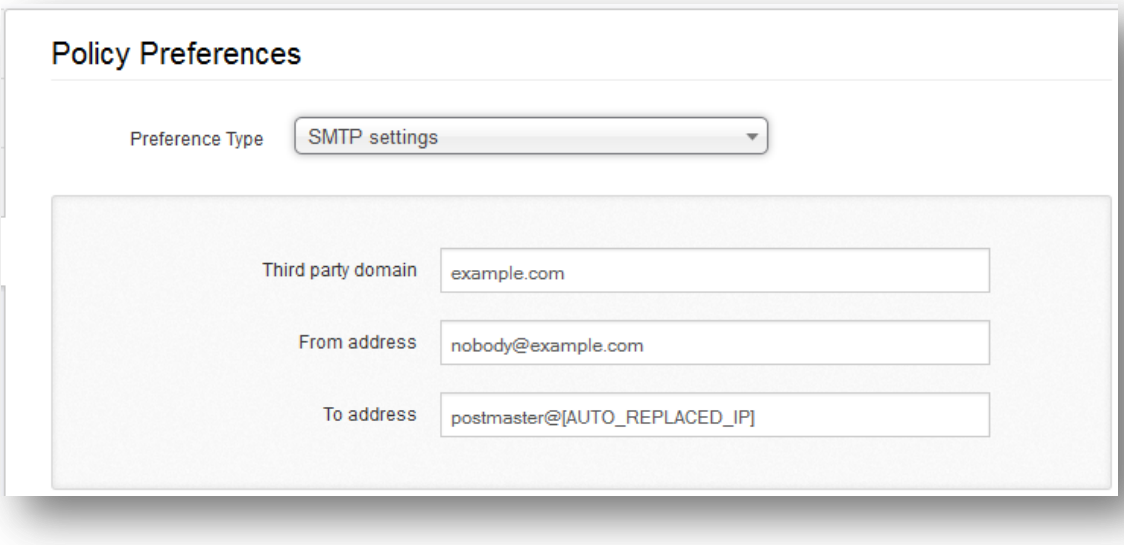


"**SMB Use Host SID to Enumerate Local Users**" **(SMB, usar SID de host para enumerar usuarios locales)** especifica el rango de SID para usar en la realización de búsquedas inversas de nombres de usuarios locales. Se recomienda la opción predeterminada.



“**SMTP settings**” **(Opciones de configuración de SMTP)** especifica opciones para pruebas SMTP (Protocolo simple de transferencia de correo) que se ejecutan en todos los dispositivos dentro del dominio analizado que ejecutan servicios SMTP. Nessus intentará retransmitir mensajes a través del dispositivo hasta el “**Third party domain**” **(Dominio de terceros)** especificado. Si el mensaje enviado al “**Third party domain**” **(Dominio de terceros)** es rechazado por la dirección especificada en el campo “**To address**” **(A dirección)**, significa que el intento de enviar correo no deseado no tuvo éxito. Si se acepta el mensaje, significa que se logró utilizar el servidor SMTP para retransmitir correo no deseado.

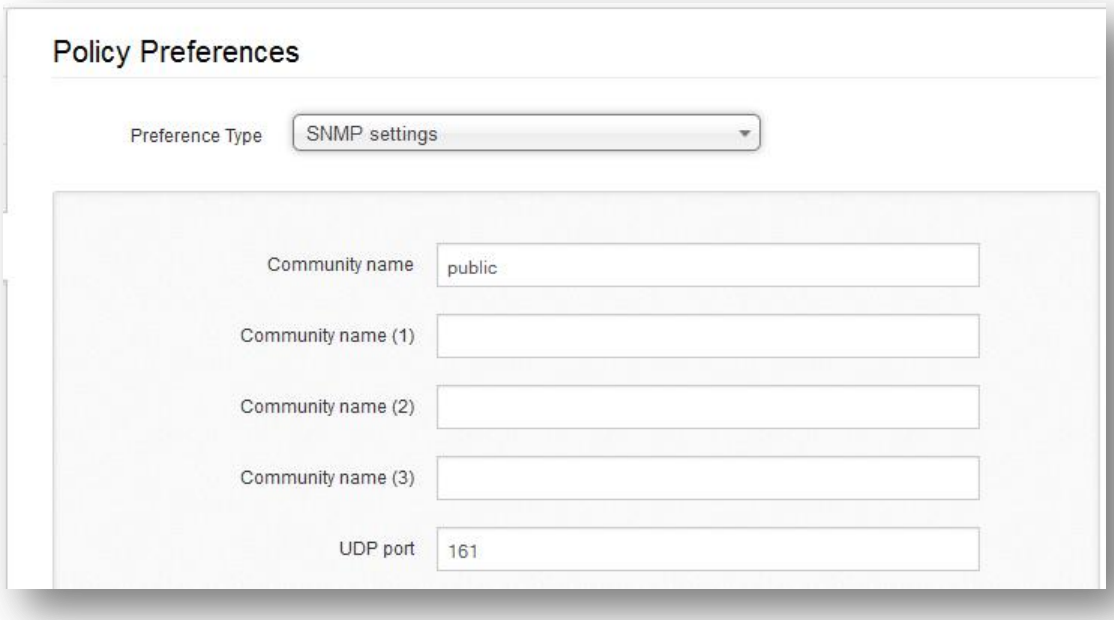
Opción	Descripción
“Third party domain” (Dominio de terceros)	Nessus intentará enviar correo no deseado a través de cada dispositivo SMTP a la dirección indicada en este campo. Esta dirección de dominio de terceros debe encontrarse fuera del rango del sitio que se está analizando y del sitio que realiza el análisis. De lo contrario, es posible que el servidor SMTP anule la prueba.
“From address” (De dirección)	Los mensajes de prueba enviados al (a los) servidor(es) SMTP aparecerán como si se hubieran originado en la dirección especificada en este campo.
“To address” (A dirección)	Nessus intentará enviar mensajes dirigidos al destinatario del correo que se indica en este campo. La dirección **postmaster** (administrador de correo) constituye el valor predeterminado, ya que es una dirección válida en la mayoría de los servidores de correo.



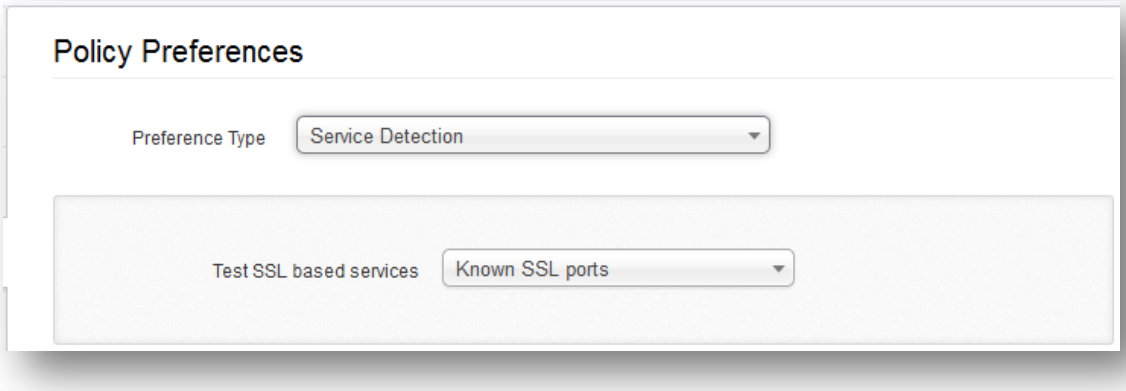
“**SNMP settings**” **(Opciones de configuración de SNMP)** le permite configurar a Nessus para que se conecte y se autentique en el servicio SNMP del destino. En el transcurso del análisis, Nessus hará algunos intentos de estimar la cadena de comunidad y la usará en pruebas subsiguientes. Se admiten hasta cuatro cadenas de nombres de comunidades individuales por cada directiva de análisis. Si Nessus no puede estimar la contraseña y/o cadena de comunidad, es posible que no realice una auditoría completa del servicio.

Opción	Descripción
“Community name (0-3)” (Nombre de comunidad [0-3])	El nombre de comunidad SNMP.
“UDP port”	Ordena a Nessus analizar un puerto diferente si SNMP se ejecutara en un

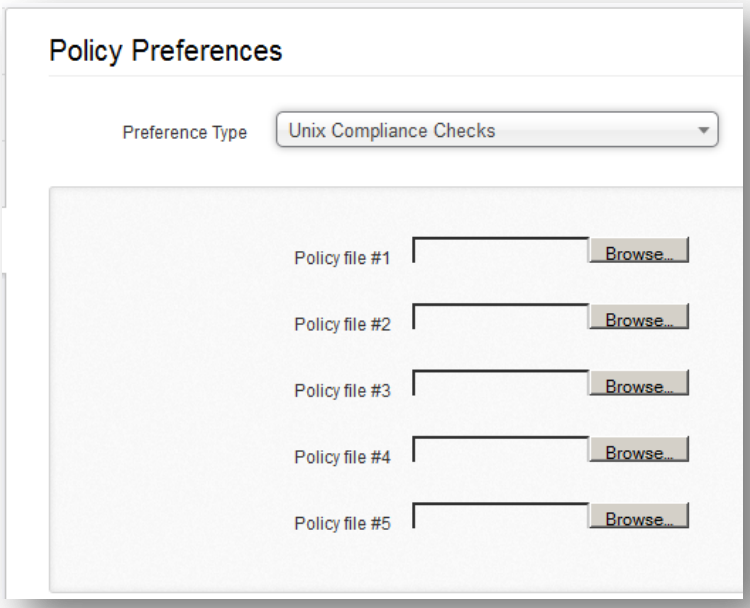
(Puerto UDP)	puerto distinto del 161.
“SNMPv3 user name” (Nombre de usuario de SNMPv3)	El nombre de usuario para una cuenta basada en SNMPv3.
“SNMPv3 authentication password” (Contraseña de autenticación de SNMPv3)	La contraseña correspondiente al nombre de usuario especificado.
“SNMPv3 authentication algorithm” (Algoritmo de autenticación de SNMPv3)	Selecciona MD5 o SHA1 de acuerdo con el algoritmo que admita el servicio remoto.
“SNMPv3 privacy password” (Contraseña de privacidad de SNMPv3)	La contraseña usada para proteger la comunicación SNMP cifrada.
"SNMPv3 privacy algorithm” (Algoritmo de privacidad de SNMPv3)	El algoritmo de cifrado que se usará para el tráfico SNMP.



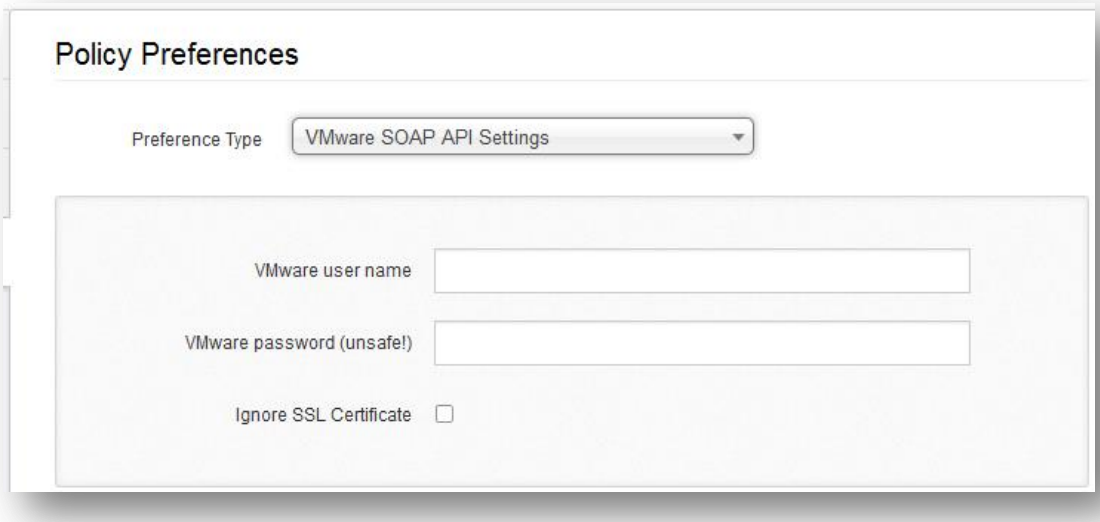
“**Service Detection**” **(Detección de servicio)** controla la forma en que Nessus probará los servicios basados en SSL: los puertos SSL conocidos (por ejemplo, 443), todos los puertos o ninguno. Probar todos los puertos para determinar las capacidades SSL puede resultar perturbador para el funcionamiento del host en el que se realiza la prueba.



"**Unix Compliance Checks**" **(Comprobaciones de compatibilidad con Unix)** permite a los clientes de ProfessionalFeed cargar archivos de auditoría Unix que se usarán para determinar si un sistema que se haya probado cumple con los estándares de compatibilidad especificados. Pueden seleccionarse hasta cinco directivas a la vez.



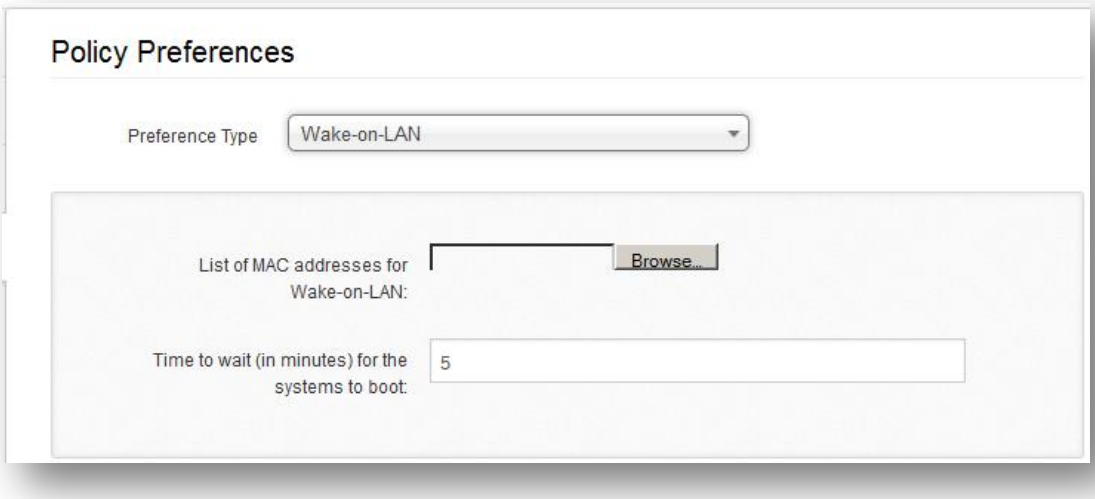
"**VMware SOAP API Settings**" **(Opciones de configuración de API SOAP de VMware)** le brinda a Nessus las credenciales necesarias para autenticarse en los sistemas de administración VMware ESX, ESXi y vSphere Hypervisor a través de su propio SOAP API, ya que el acceso SSH está desactualizado. La API está diseñada para la auditoría de los hosts vSphere 4.x / 5.x, ESXi y ESX hosts, no las máquinas virtuales que se ejecutan en los hosts. Este método de autenticación puede utilizarse para realizar análisis con credenciales o auditorías de compatibilidad.



Opción	Descripción
"VMware user name" (Nombre de usuario de VMware)	El nombre de usuario con el que autenticarse. Las credenciales pueden ser cuentas de Active Directory (AD) para hosts integrados o cuentas locales; la cuenta debe estar en el grupo local **`root`**. Las credenciales de dominio son user@domain, y las cuentas creadas localmente son el usuario y la contraseña.
"VMware password (unsafe!)" (Contraseña de VMware [¡insegura!])	Esta contraseña se envía de manera insegura y puede ser interceptada por husmeadores de la red.
"Ignore SSL Certificate" (Ignorar certificado SSL)	Si hay un certificado SSL presente en el servidor, ignórelo.

"**Wake-on-LAN**" (WOL) **(Paquetes Wake-on-LAN)** controla a qué hosts enviar paquetes mágicos WOL antes de realizar un análisis y cuánto tiempo esperar (en minutos) para que se inicien los sistemas. La lista de direcciones MAC para WOL se introduce mediante la carga de un archivo de texto con una sola dirección MAC de host por línea. Por ejemplo:

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



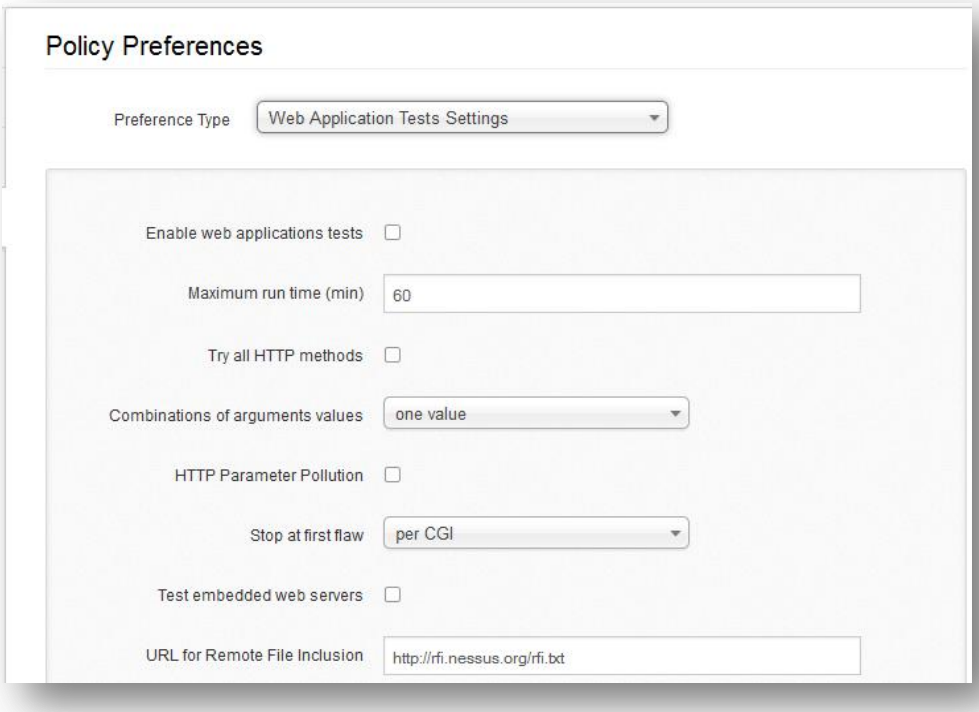
"**Web Application Tests Settings**" **(Opciones de prueba de aplicaciones web)** prueba los argumentos de las Common Gateway Interfaces, CGI (interfaces de puertas de enlace comunes) remotas detectadas en el proceso de creación de reflejo web mediante el intento de pasar errores de programación de CGI comunes, tales como ataques de scripts (secuencias de comandos) de sitios, inclusión de archivos remota, ejecución de comandos, ataques de cruces seguros e inyección de código SQL. Habilite esta opción seleccionando la casilla de verificación "Enable web applications tests" (Habilitar pruebas de aplicaciones web). Estas pruebas dependen de los siguientes plugins NASL:

- 11139, 42424, 42479, 42426, 42427, 43160 – SQL Injection (CGI abuses) (Inyección de código SQL [Abusos CGI])
- 39465, 44967 – Command Execution (CGI abuses) (Ejecución de comandos [Abusos CGI])
- 39466, 47831, 42425, 46193, 49067 – Cross-Site Scripting (CGI abuses: XSS) (Secuencias de comandos de sitios [Abusos CGI: XSS])
- 39467, 46195, 46194 – Directory Traversal (CGI abuses) (Cruce de directorios [Abusos CGI])
- 39468 – HTTP Header Injection (CGI abuses: XSS) (Inyección de encabezados HTTP [Abusos CGI: XSS])
- 39469, 42056, 42872 –File Inclusion (CGI abuses) (Inclusión de archivos [Abusos CGI])
- 42055 - Format String (CGI abuses) (Cadena de formato [Abusos CGI])
- 42423, 42054 - Server Side Includes (CGI abuses) (Server Side Includes [Abusos CGI])
- 44136 - Cookie Manipulation (CGI abuses) (Manipulación de cookies [Abusos CGI])
- 46196 - XML Injection (CGI abuses) (Inyección XML [Abusos CGI])
- 40406, 48926, 48927 - Error Messages (Mensajes de error)
- 47830, 47832, 47834, 44134 - Additional attacks (CGI abuses) (Ataques adicionales [Abusos CGI])

Importante: esta lista de plugins relacionados con aplicaciones web se actualiza frecuentemente y puede no estar completa. Es posible que haya plugins adicionales que dependan de la configuración en esta opción de preferencias.

Opción	Descripción
“Maximum run time (min)” (Tiempo de ejecución máximo [min.])	Esta opción administra la cantidad de tiempo en minutos dedicada a la realización de pruebas de aplicaciones web. El valor predeterminado de esta opción es 60 minutos, y se aplica a todos los puertos y las CGI de un sitio web determinado. El análisis de la red local en busca de sitios web con aplicaciones pequeñas normalmente finalizará en menos de una hora. Sin embargo, los sitios web con aplicaciones de gran tamaño pueden requerir un valor superior.
“Try all HTTP methods” (Probar todos los métodos HTTP)	De manera predeterminada, Nessus solo probará con solicitudes GET. Esta opción le ordenará a Nessus que use también “POST requests” (Solicitudes POST) para mejorar las pruebas de formularios web. De manera predeterminada, las pruebas de aplicaciones web solo usarán las solicitudes GET, a menos que esté habilitada esta opción. Normalmente, las aplicaciones más complejas emplean el método POST cuando un usuario envía datos a la aplicación. Esta opción brinda pruebas más minuciosas, pero puede aumentar considerablemente el tiempo requerido. Si se selecciona, Nessus probará cada secuencia de comandos o variable con solicitudes GET y POST.
“Combinations of arguments values” (Combinaciones de valores de argumentos)	Esta opción administra la combinación de valores de argumentos usados en las solicitudes HTTP. Este menú desplegable ofrece tres opciones: **one value (un valor)**: prueba un parámetro por vez con una cadena de ataque, sin intentar variaciones de “non-attack” (no ataque) en el caso de parámetros adicionales. Por ejemplo, Nessus intentaría usar “`/test.php?arg1=XSS&b=1&c=1`”, donde “b” y “c” permiten otros valores, sin probar cada combinación. Este es el método de prueba más rápido con el menor conjunto de resultados generados. **All pairs (slower but efficient) (Todos los pares [más lento pero eficiente])**: esta forma de prueba es ligeramente más lenta pero más eficaz que la prueba “one value” (un valor). Al probar varios parámetros, probará una cadena de ataque y variaciones de una única variable, y luego usará el primer valor para todas las otras variables. Por ejemplo, Nessus intentaría usar “`/test.php?a=XSS&b=1&c=1&d=1`” y luego recorrería las variables, de modo que una reciba la cadena de ataque, otra pase por todos los valores posibles (según se detecten durante el proceso de reflejo) y todas las otras variables reciban el primer valor. En este caso, Nessus nunca realizaría una prueba de “`/test.php?a=XSS&b=3&c=3&d=3`” cuando el primer valor de cada variable sea “1”. **All combinations (extremely slow) (Todas las combinaciones [extremadamente lento])**: este método efectuará una prueba exhaustiva y completa de todas las posibles combinaciones de cadenas de ataque con información válida de las variables. Mientras que las pruebas “All-pairs” (Todos los pares) procuran crear conjuntos de datos más pequeños y lograr a cambio mayor velocidad, “All combinations” (Todas las combinaciones) no garantiza rapidez y usa un conjunto completo de datos de pruebas. Este método de prueba puede tardar **mucho** tiempo en completarse.
“HTTP Parameter Pollution” (Contaminación de parámetros HTTP)	Al efectuar pruebas de aplicaciones web, intenta sortear los posibles mecanismos de filtrado mediante la inserción de contenido en una variable a la vez que se proporciona también a esa variable contenido válido. Por ejemplo, una prueba de inyección de código SQL normal puede tener la siguiente apariencia: “`/target.cgi?a='&b=2`”. Con la opción "HTTP Parameter Pollution” (HPP) (Contaminación de parámetros HTTP [HPP]) habilitada, la solicitud puede tener la siguiente apariencia: “`/target.cgi?a='&a=1&b=2`”.

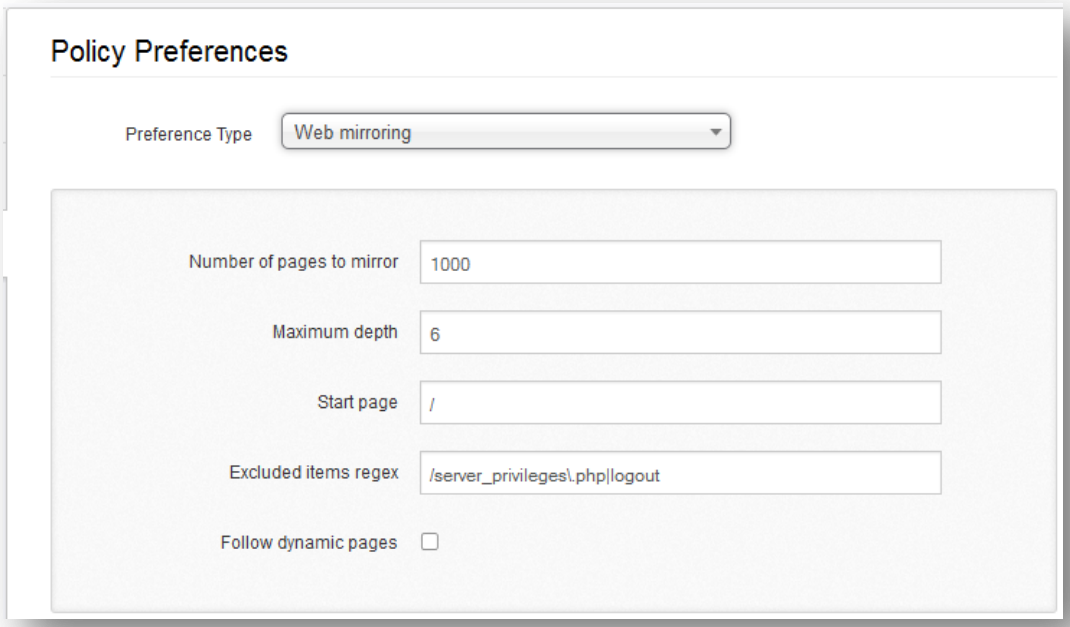
“Stop at first flaw” (Detener ante el primer error)	Esta opción determina cuándo se debe apuntar a un nuevo error. Se aplica en el nivel de la secuencia de comandos. Encontrar errores XSS no deshabilitará la búsqueda de la inyección de código SQL ni la inserción de encabezados. No obstante, se producirá como máximo un informe por cada tipo en un puerto específico, a menos que se haya establecido “thorough tests” (pruebas minuciosas). Tenga en cuenta que es posible que en ocasiones se informen varios errores del mismo tipo (por ejemplo, XSS, SQLi, etc.) si estos fueron detectados por el mismo ataque. El menú desplegable ofrece cuatro opciones: **per CGI (por CGI):** cuando se detecta un error en una CGI mediante una secuencia de comandos, Nessus cambiará a la siguiente CGI conocida en el mismo servidor o, si no hay otra CGI, al siguiente puerto o servidor. Esta es la opción predeterminada. **per port (quicker) (por puerto [más rápida]):** cuando se detecta un error en un servidor web mediante una secuencia de comandos, Nessus se detendrá y cambiará a otro servidor web en un puerto diferente. **per parameter (slow) (por parámetro [lenta]):** cuando se detecta un tipo de error en un parámetro de una CGI (por ejemplo, XSS), Nessus cambia al siguiente parámetro de la misma CGI o a la siguiente CGI conocida, o bien al siguiente puerto o servidor. **look for all flaws (slower) (buscar todos los errores [más lenta]):** realiza pruebas minuciosas independientemente de los errores detectados. Esta opción puede producir un informe muy detallado y, en la mayoría de los casos, no se recomienda.
“Test Embedded web servers” (Probar servidores web incrustados)	Los servidores web incrustados son a menudo estáticos, y no contienen secuencias de comandos CGI personalizables. Además, es posible que los servidores web incrustados sean propensos a bloquearse o no responder cuando se analizan. Tenable recomienda el análisis de servidores web incrustados de manera independiente de otros servidores web mediante esta opción.
“URL for Remote File Inclusion” (URL para Inclusión de archivos remota)	Durante las pruebas de Remote File Inclusion, RFI (Inclusión de archivos remota), esta opción especifica un archivo en un host remoto a fin de usarlo para las pruebas. De forma predeterminada, Nessus usará un archivo seguro hospedado en el servidor web de Tenable para realizar las pruebas de RFI. Si el analizador no puede conectarse a Internet, se recomienda usar un archivo hospedado internamente para lograr pruebas de RFI más precisas.



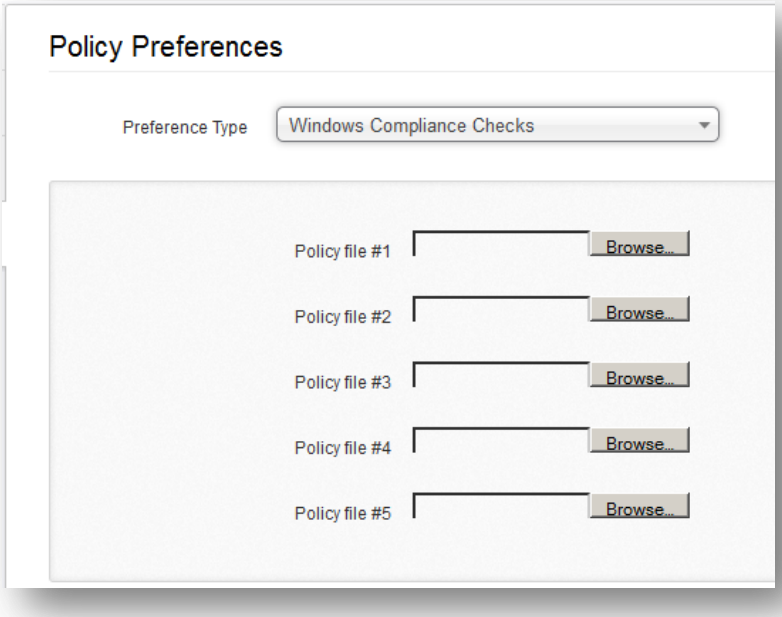
"**Web Mirroring**" **(Reflejo web)** establece los parámetros de configuración para la utilidad de creación de reflejo de contenido de servidores web nativos de Nessus. Nessus creará el reflejo del contenido web para analizarlo mejor en busca de vulnerabilidades y ayudar a minimizar el efecto en el servidor.

Si los parámetros de creación de reflejo web están establecidos de forma que se refleje todo el sitio web, esto puede generar una cantidad considerable de tráfico durante el análisis. Por ejemplo, si en un servidor web hay 1 gigabyte de material y Nessus está configurado para reflejar todo, el análisis generará al menos 1 gigabyte de tráfico desde el servidor hasta el analizador Nessus.

Opción	Descripción
"Number of pages to mirror" (Cantidad de páginas a reflejar)	La cantidad máxima de páginas que se reflejarán.
"Maximum depth" (Profundidad máxima)	Limita la cantidad de enlaces que Nessus seguirá para cada página de inicio.
"Start page" (Página de inicio)	La dirección URL de la primera página que se probará. Si se requieren varias páginas, use un delimitador de dos puntos para separarlas (por ejemplo, "/:/php4:/base").
"Excluded items regex" (Regex de elementos excluidos)	Habilita la exclusión de porciones del sitio web para que no sean rastreadas. Por ejemplo, para excluir el directorio "/manual" y toda la CGI de Perl, establezca este **campo en:** `(^/manual)|(\.pl(\?.*)?$).`
"Follow dynamic pages" (Seguir páginas dinámicas)	Si se selecciona esta opción, Nessus seguirá enlaces dinámicos y es posible que supere los parámetros establecidos anteriormente.

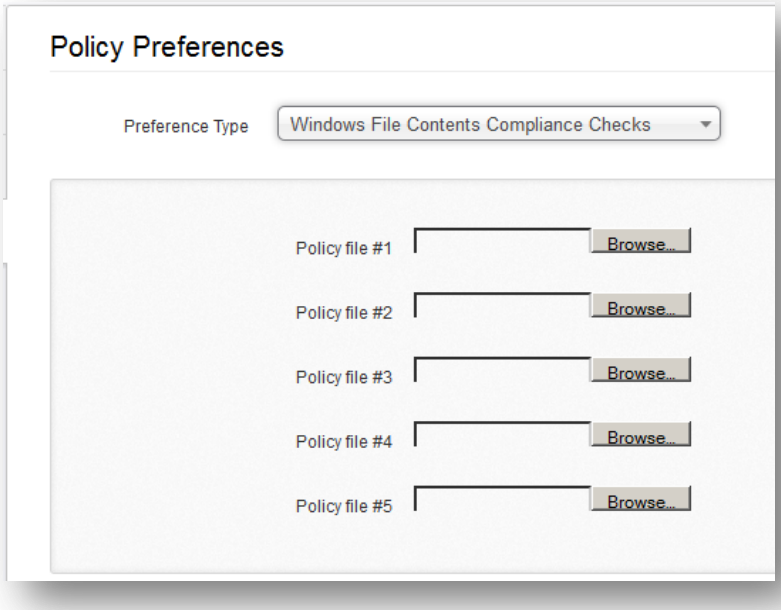


"**Windows Compliance Checks**" **(Comprobaciones de compatibilidad con Windows)** permite a los clientes de ProfessionalFeed cargar archivos de auditorías de configuración de Microsoft Windows que se usarán para determinar si un sistema que se haya probado cumple con los estándares de compatibilidad especificados. Pueden seleccionarse hasta cinco directivas a la vez.



"**Windows File Contents Compliance Checks**" **(Comprobaciones de compatibilidad de contenido de archivos de Windows)** le permite a los clientes de ProfessionalFeed cargar archivos de auditoría basados en Windows que realizan búsquedas en un sistema para detectar un tipo específico de contenido (por ejemplo, tarjetas de crédito, números de seguro social) para ayudar a determinar la compatibilidad con reglamentaciones corporativas o estándares de terceros.

Una vez configuradas todas las opciones según lo deseado, haga clic en "**Submit**" **(Enviar)** para guardar la directiva y volver a la ficha Policies. En cualquier momento puede hacer clic en "**Edit**" **(Editar)** para efectuar cambios en una directiva que ya haya creado, o hacer clic en "**Delete**" **(Eliminar)** para eliminar una directiva por completo.



Para obtener más información

Tenable ha producido una variedad de otros documentos en los que se detallan la instalación, implementación, configuración, operación del usuario y pruebas generales de Nessus. Estos se incluyen aquí:

- **Nessus Installation Guide (Guía de instalación de Nessus)**: instrucciones paso a paso sobre la instalación.
- **Nessus Credential Checks for Unix and Windows (Comprobaciones con credenciales de Nessus para Unix y Windows)**: información sobre cómo llevar a cabo análisis de red autenticados mediante el analizador de vulnerabilidades Nessus
- **Nessus Compliance Checks (Comprobaciones de compatibilidad con Nessus)**: guía de alto nivel para comprender y ejecutar las comprobaciones de compatibilidad con Nessus y SecurityCenter.
- Nessus Compliance Checks Reference (Referencia para comprobaciones de compatibilidad con Nessus): guía completa de la sintaxis de las comprobaciones de compatibilidad con Nessus.
- **Nessus v2 File Format (Formato de archivo de Nessus v2)**: describe la estructura del formato de archivo `.nessus`, que se presentó con Nessus 3.2 y NessusClient 3.2.
- Nessus XML-RPC Protocol Specification (Especificación del protocolo XML-RPC en Nessus): describe la interfaz y el protocolo XML-RPC en Nessus.
- **Real-Time Compliance Monitoring (Supervisión de compatibilidad en tiempo real)**: describe el modo en que pueden usarse las soluciones de Tenable para colaborar con el cumplimiento de distintos tipos de normas gubernamentales y financieras.
- **Guía de administración de SecurityCenter**

Estos son otros recursos en línea:

- Foros de debate de Nessus: https://discussions.nessus.org/
- Blog de Tenable: http://blog.tenable.com/
- Podcast de Tenable: http://blog.tenablesecurity.com/podcast/
- Videos de ejemplos de uso: http://www.youtube.com/user/tenablesecurity
- Canal de Twitter de Tenable: http://twitter.com/tenablesecurity

No dude en comunicarse con Tenable a través de support@tenable.com o sales@tenable.com, o bien visite nuestro sitio web: http://www.tenable.com/.

Acerca de Tenable Network Security

Tenable Network Security, líder en Supervisión de seguridad unificada, es el proveedor del analizador de vulnerabilidades Nessus, y ha creado soluciones de clase empresarial sin agente para la supervisión continua de vulnerabilidades, puntos débiles de configuración, filtración de datos, administración de registros y detección de compromisos para ayudar a garantizar la seguridad de redes y la compatibilidad con FDCC, FISMA, SANS CSIS y PCI. Los galardonados productos de Tenable son utilizados por muchas organizaciones de la lista Forbes Global 2000 y organismos gubernamentales con el fin de minimizar de forma proactiva el riesgo de las redes. Para obtener más información, visite www.tenable.com.

GLOBAL HEADQUARTERS

Tenable Network Security
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046
410.872.0555
www.tenable.com