



TENABLE

Network Security®

Guía del usuario de Nessus 4.4

14 de junio de 2011

(Revisión 10)

Índice

Introducción	3
Estándares y convenciones	3
Descripción general de la UI de Nessus	3
Descripción	3
Plataformas admitidas.....	4
Instalación.....	4
Operación..	4
Descripción general	4
Conexión con la GUI de Nessus	4
Descripción general de directivas.....	8
Directivas predeterminadas.....	9
Creación de una nueva directiva	10
<i>General</i>	10
<i>Credenciales</i>	15
<i>Plugins</i>	18
<i>Preferencias</i>	21
Importación, exportación y copia de directivas	38
Creación, inicio y programación de un análisis.....	39
Informes.....	42
<i>Explorar</i>	42
<i>Filtros de informes</i>	46
<i>Comparar</i>	49
<i>Carga y descarga</i>	50
<i>Formato de archivo .nessus</i>	52
<i>Eliminar</i>	52
Usuarios.....	53
Otros clientes de Nessus.....	53
Interfaz de líneas de comandos	53
<i>Conversión de un informe</i>	55
<i>Línea de comandos que utiliza archivos .nessus</i>	56
<i>Comando de análisis</i>	57
SecurityCenter	58
<i>Configuración de SecurityCenter</i>	58
Para obtener más información	59
Acerca de Tenable Network Security	61

INTRODUCCIÓN

Este documento describe cómo usar la interfaz de usuario (UI) de Nessus de Tenable Network Security. Si desea realizar comentarios o aportar sugerencias, envíe un mensaje de 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 es una traducción de la versión original escrita en inglés. Algunos fragmentos permanecen en inglés con el fin de mostrar cómo aparecen realmente en el producto.

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

Las opciones de líneas de comandos y las palabras clave también se indican con fuente **courier negrita**. Las opciones 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. Por lo general, el comando que se está ejecutando se escribirá en negrita para indicar lo que ha escrito el usuario. 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.



Se logra una experiencia óptima de la interfaz de usuario web de Nessus si se usa Microsoft Internet Explorer 7 y 8, Mozilla Firefox 3.5.x y 3.6.x o Apple Safari.

INSTALACIÓN

A partir de Nessus 4.2, la administración de los usuarios del servidor Nessus se lleva a cabo mediante una interfaz web o SecurityCenter, y ya no es necesario usar un NessusClient independiente. Los NessusClients independientes aún conectarán y operarán el analizador, pero no recibirán actualizaciones.

Consulte la Guía de instalación de Nessus 4.4 para obtener instrucciones sobre cómo instalar Nessus. No se requiere la instalación de ningún otro software.

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, realice lo siguiente:

- > Abra el explorador web de su preferencia.
- > Introduzca `https://[server IP]:8834/` 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:





There is a problem with this website's security certificate.


The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.


Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

 [Click here to close this webpage.](#)

 [Continue to this website \(not recommended\).](#)

 [More information](#)



This Connection is Untrusted

You have asked Firefox to connect securely to **192.168.0.2:8834**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

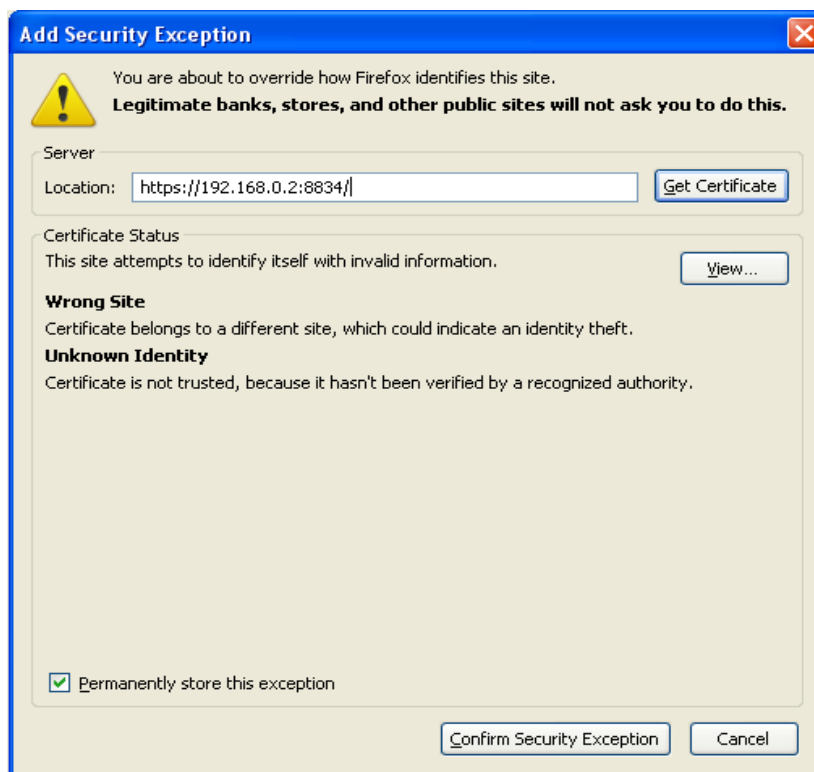
What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

[Get me out of here!](#)

- ▶ **Technical Details**
- ▶ **I Understand the Risks**

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 pueden hacer clic en "I Understand the Risks" (Comprendo los riesgos) y luego, en "Add Exception..." (Agregar excepción) para que aparezca el cuadro de diálogo de excepción de sitios:

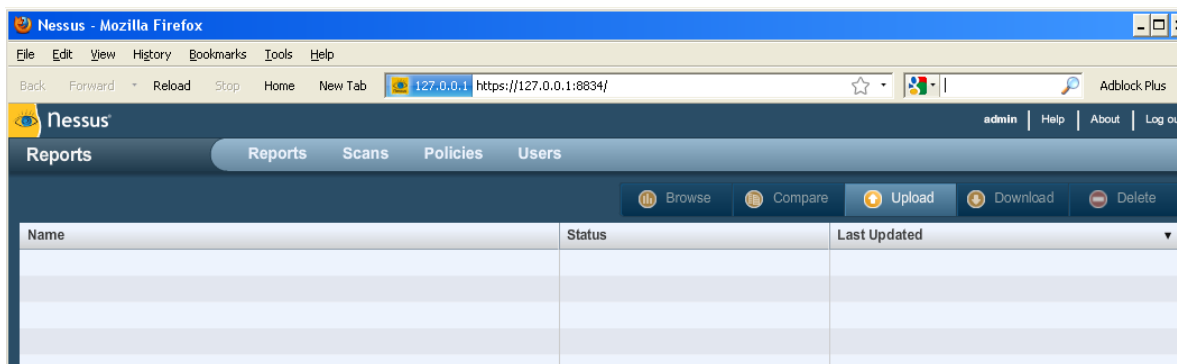


Verifique que la barra "Location:" (Ubicación:) refleje la dirección URL del servidor Nessus, y haga clic en **"Confirm Security Exception"** (Confirmar excepción de seguridad). Para obtener información sobre cómo instalar un certificado SSL personalizado, consulte la Guía de instalación de Nessus.

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



Realice una autenticación mediante una cuenta y una contraseña previamente creadas con el administrador del servidor. Después de que la autenticación se haya realizado correctamente, la UI presentará menús para llevar a cabo análisis:



En todo momento durante el uso de Nessus estarán presentes las opciones de la esquina superior derecha. La notación “admin” que se observa en la esquina superior derecha de la pantalla anterior representa la cuenta con la que se inició sesión en ese momento. Si hace clic en esta, podrá cambiar la contraseña actual. “Help” es un enlace a la documentación de Nessus, donde se brindan instrucciones detalladas sobre cómo usar el software. “About” muestra información sobre la instalación de Nessus, incluidas la versión, el tipo de fuente, la fecha de vencimiento de la fuente, la compilación del cliente y la versión del servidor web. “Log out” finalizará la sesión actual.



DESCRIPCIÓN GENERAL DE DIRECTIVAS

Nessus			admin Help About Log out
Policies			Reports Scans Policies Users
			Add Import Export Copy Edit Delete
Name	Visibility	Owner	
Default Policy	Private	admin	
DocPolicy	Private	admin	
Host Discovery	Private	admin	
LAN Scan	Private	admin	
Large Scale Portscan	Private	admin	

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 en función de plugins o familias pormenorizadas.
- > 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



Name	Visibility	Owner
External Network Scan	Shared	Tenable Policy Distribution Service
Internal Network Scan	Shared	Tenable Policy Distribution Service
Prepare for PCI DSS audits	Shared	Tenable Policy Distribution Service
Web App Tests	Shared	Tenable Policy Distribution Service

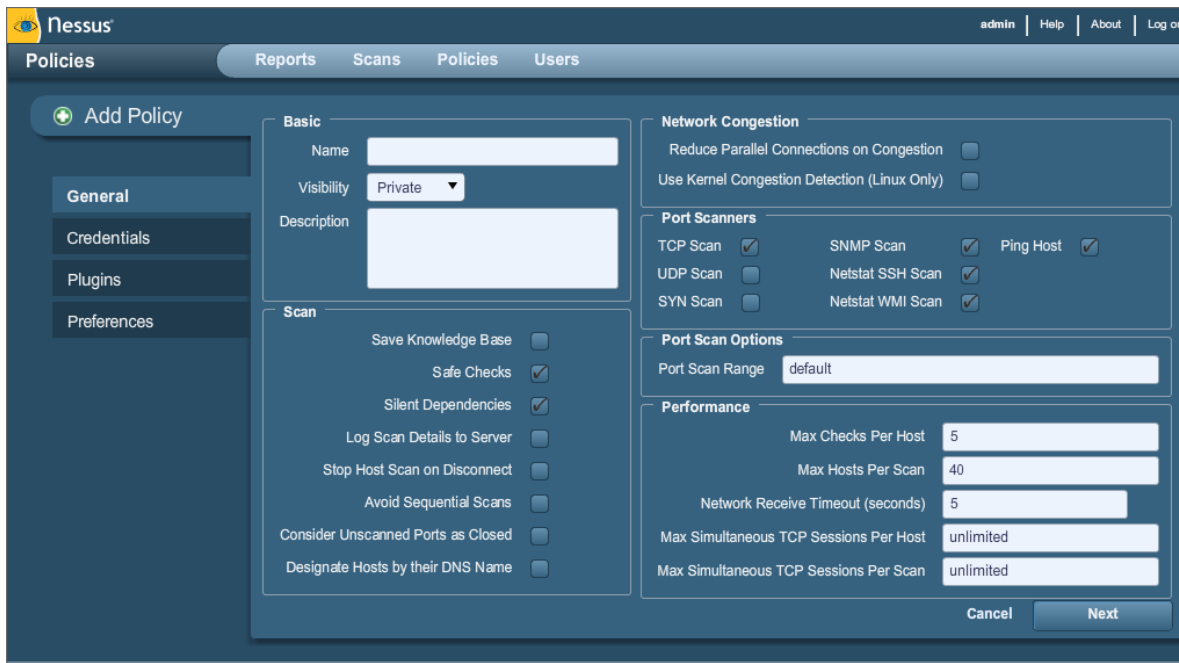
Nessus se distribuye con varias directivas predeterminadas proporcionadas por Tenable Network Security, Inc. Se brindan como plantillas para ayudarle a crear directivas personalizadas para su organización o usarlas en su estado actual para iniciar análisis básicos de sus recursos.

Nombre de la directiva	Descripción
External Network Scan	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 (CGI Abuses y CGI Abuses: familias de plugins XSS). Además, para cada destino se analizan los 65.535 puertos.
Internal Network Scan	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. Los plugins "CGI Abuse" no están habilitados, y se analiza un conjunto estándar de puertos, no los 65.535.
Web App Tests	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 está habilitada 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.
Prepare for PCI DSS audits	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 de PCI DSS pueden usar esta directiva a fin de preparar su red y sus sistemas para tener compatibilidad PCI DSS.

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"** de la barra situada en la parte superior, y luego en el botón **"Add Policy"** de la derecha. Aparecerá la pantalla **"Add Policy"**, como se muestra a continuación:



Observe que hay cuatro fichas de configuración: **General**, **Credentials**, **Plugins** y **Preferences**. En la mayoría de los entornos no es necesario modificar la configuración predeterminada, pero estas proporcionan un control más pormenorizado de la operación del analizador Nessus. Estas fichas se describen a continuación.

General

La ficha General le permite nombrar la directiva y configurar las operaciones relacionadas con el análisis. Hay seis cuadros de opciones agrupadas que controlan el comportamiento del analizador:

El marco "Basic" se usa para definir aspectos de la directiva en sí:

Opción	Descripción
Name	Establece el nombre que aparecerá en la UI de Nessus para identificar la directiva.
Visibility	Controla si la directiva se comparte con otros usuarios ("Shared"), o se mantiene <i>privada</i> para su uso exclusivo

	("Private"). Solo los usuarios administrativos pueden compartir directivas.
Description	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").

El marco "Scan" define de forma adicional las opciones relacionadas con la forma en que se debe comportar el análisis:



Opción	Descripción
Save Knowledge Base	El analizador Nessus puede guardar la información del análisis en la base de conocimiento del servidor Nessus para usarla posteriormente. Esto incluye los puertos abiertos, los plugins generados correctamente, los servicios descubiertos, etc.
Safe Checks	Safe Checks deshabilitará todos los plugins que puedan producir efectos adversos en el host remoto.
Silent Dependencies	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	Guarda detalles adicionales del análisis en el registro del servidor Nessus (<code>nessusd.messages</code>), incluido 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	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	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.
Consider Unscanned Ports as Closed	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.


Designate Hosts by their DNS Name	Usa el nombre del host en lugar de la dirección IP para generar los informes.
--	---

El marco **“Network”** brinda opciones que controlan mejor el análisis en función de la red de destino que se está analizando:

Opción	Descripción
Reduce Parallel Connections on Congestion	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)	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 marco **“Port Scanners”** controla qué métodos de análisis de puertos deben habilitarse para el análisis:

Opción	Descripción
TCP Scan	<p>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.</p> <div>  <p>En algunas plataformas (por ejemplo, Windows y Mac OS X), si el sistema operativo produce graves problemas de rendimiento al usar el analizador TCP, Nessus iniciará el analizador SYN.</p> </div>
UDP Scan	<p>Esta opción activa el analizador UDP incorporado de Nessus para identificar los puertos UDP abiertos en los destinos.</p> <div>  <p>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</p> </div>

	<div> <div></div> <div>manera remota.</div> </div>
SYN Scan	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.
SNMP Scan	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", 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 examinando la versión de la cadena SNMP devuelta. Esta información es necesaria para estas auditorías.
Netstat SSH Scan	Esta opción usa <code>netstat</code> para comprobar la existencia de puertos abiertos desde el equipo local. Depende de la disponibilidad del comando <code>netstat</code> mediante una conexión SSH con el destino. Este análisis está destinado a sistemas basados en Unix y requiere credenciales de autenticación.
Netstat WMI Scan	<p>Esta opción usa <code>netstat</code> para comprobar la existencia de puertos abiertos desde el equipo local. Depende de la disponibilidad del comando <code>netstat</code> mediante una conexión WMI con el destino. Este análisis está destinado a sistemas basados en Windows y requiere credenciales de autenticación.</p> <div>  <p>Un análisis basado en WMI emplea <code>netstat</code> 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).</p> </div>
Ping Host	Esta opción permite que se efectúen pings a hosts remotos en varios puertos para determinar si están activos.

El marco **"Port Scan Options"** indica al analizador que tenga como destino un intervalo específico de puertos. Para la opción "Port Scan Range", se permiten los siguientes valores:


Valor	Descripción
-------	-------------

"default"	Si se emplea la palabra clave "default", Nessus analizará aproximadamente 4790 puertos comunes. La lista de puertos se puede encontrar en el archivo <code>nessus-services</code> .
"all"	Si se emplea la palabra clave "all", Nessus analizará los 65.535 puertos.
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.



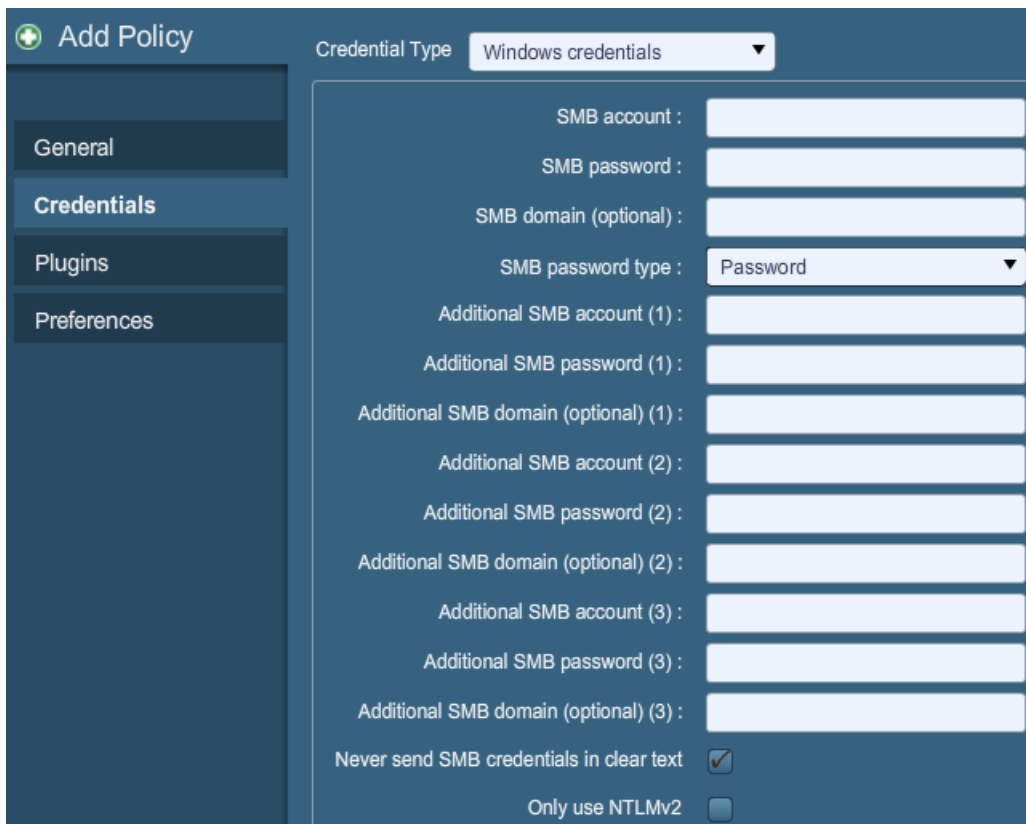
El intervalo especificado para un análisis de puertos se aplicará tanto a los análisis TCP como a los UDP.

El marco **"Performance"** brinda dos 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	Esta opción limita la cantidad máxima de comprobaciones que realizará un analizador Nessus respecto de un único host en una sola vez.
Max Hosts Per Scan	Esta opción limita la cantidad máxima de hosts que examinará un analizador Nessus al mismo tiempo.
Network Receive Timeout (seconds)	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	Esta opción limita la cantidad máxima de sesiones TCP establecidas para un único host.
Max Simultaneous TCP Sessions Per Scan	Esta opción limita la cantidad máxima de sesiones TCP establecidas para todo el análisis, independientemente de la cantidad de hosts que se analicen. <div data-bbox="604 1619 683 1688" data-label="Image">  </div> <div data-bbox="716 1619 1373 1751" data-label="Text"> <p>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.</p> </div>

Credenciales

La ficha Credentials, cuya imagen se incluye a continuación, 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.



The screenshot shows the 'Add Policy' window in Nessus. On the left is a sidebar with a green plus icon and the text 'Add Policy'. Below it are four tabs: 'General', 'Credentials' (which is selected and highlighted in blue), 'Plugins', and 'Preferences'. The main area is titled 'Credential Type' with a dropdown menu set to 'Windows credentials'. Below this, there are several input fields: 'SMB account :', 'SMB password :', 'SMB domain (optional) :', and 'SMB password type :'. The 'SMB password type' dropdown is set to 'Password'. Below these are three sets of fields for 'Additional SMB account', 'Additional SMB password', and 'Additional SMB domain (optional)', each with a count in parentheses (1), (2), and (3). At the bottom, there are two checkboxes: 'Never send SMB credentials in clear text' (checked) and 'Only use NTLMv2' (unchecked).

El elemento de menú desplegable **"Windows credentials"** 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.

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!](#)" para obtener más información.

Los usuarios pueden seleccionar "**SSH settings**" 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 de **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". Como muchos sitios no permiten un inicio de sesión remoto como raíz, los usuarios de Nessus pueden invocar "**su**" o "**sudo**" con una contraseña separada para una cuenta que se haya configurado para tener privilegios "**su**" o "**sudo**".

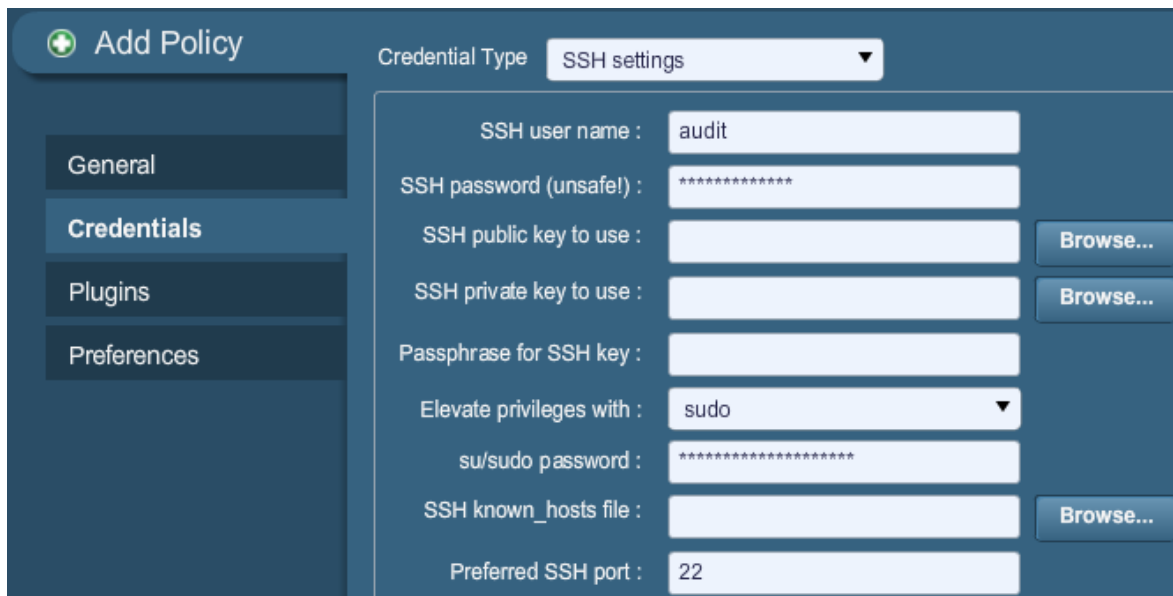
Nessus puede usar el acceso basado en clave de SSH para efectuar una autenticación en un servidor remoto. Si un archivo `known_hosts` de SSH se encuentra disponible y se proporciona como parte de la directiva de análisis, Nessus solo intentará iniciar sesión en los hosts en este archivo. Por último, la opción "Preferred SSH port" 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 mismo nombre de usuario y contraseña que está usando para auditar sus servidores de SSH conocidos no se usen 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.



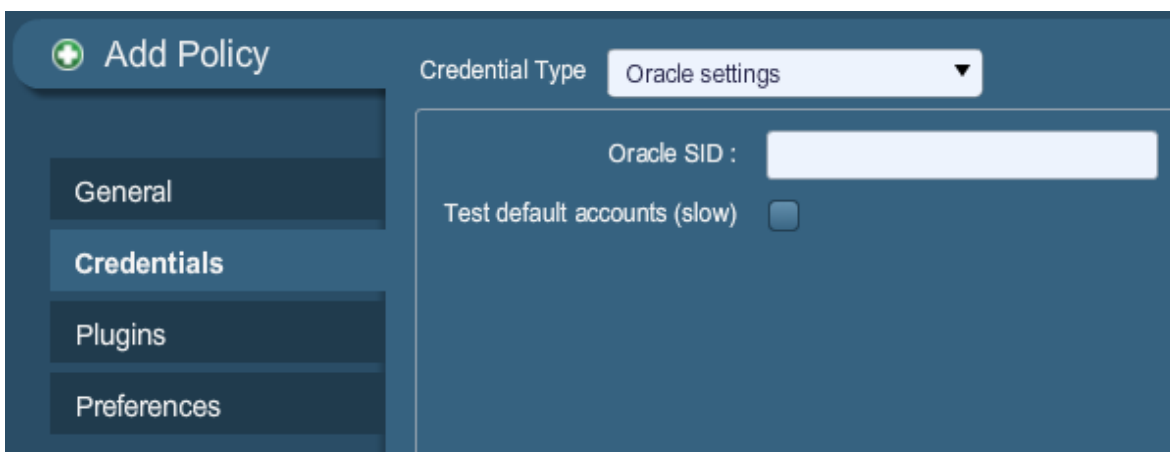
Nessus también admite una opción "**su+sudo**" que se puede usar en caso de que un sistema no permita privilegios de inicio de sesión remoto para cuentas con privilegios.

A continuación se presenta un ejemplo de captura de pantalla del uso de "**sudo**" a fin de elevar privilegios para un análisis. A los fines de este ejemplo, la cuenta de usuario es "audit", que se ha añadido al archivo `/etc/sudoers` en el sistema que se analizará. La contraseña proporcionada es la misma que para la cuenta "audit", no la contraseña raíz:



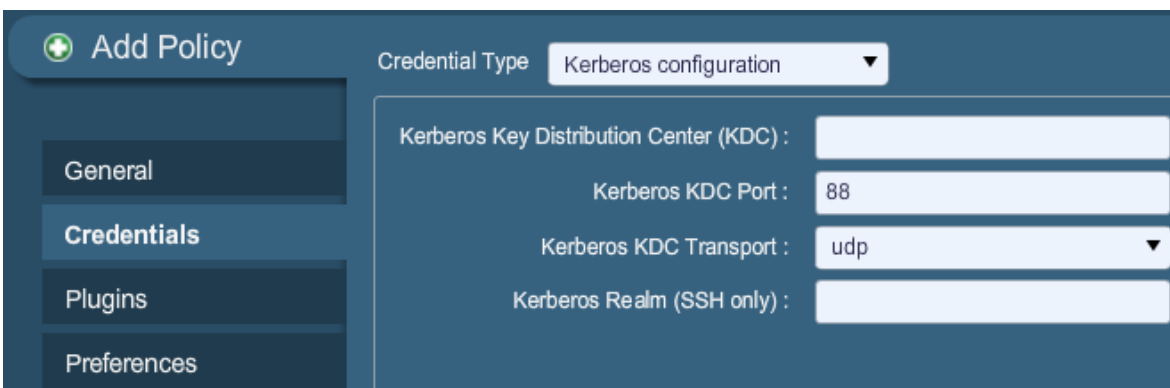
The screenshot shows the 'Add Policy' interface. On the left is a sidebar with a green plus icon and the text 'Add Policy'. Below it are four menu items: 'General', 'Credentials' (highlighted), 'Plugins', and 'Preferences'. The main area has a 'Credential Type' dropdown set to 'SSH settings'. The form contains the following fields: 'SSH user name' (text input with 'audit'), 'SSH password (unsafe!)' (password input with masked characters), 'SSH public key to use' (text input with a 'Browse...' button), 'SSH private key to use' (text input with a 'Browse...' button), 'Passphrase for SSH key' (text input), 'Elevate privileges with' (dropdown menu with 'sudo'), 'su/sudo password' (password input with masked characters), 'SSH known_hosts file' (text input with a 'Browse...' button), and 'Preferred SSH port' (text input with '22').

La ficha **Credentials** también brinda una opción en el menú desplegable para configurar **"Oracle settings"**, específicamente el Oracle SID y una opción para probar si existen cuentas predeterminadas conocidas en el software de Oracle:



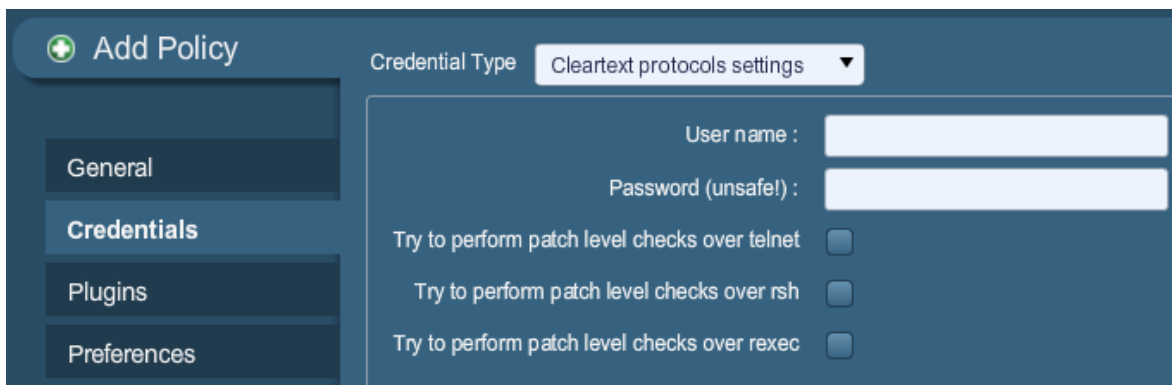
The screenshot shows the 'Add Policy' interface with 'Oracle settings' selected in the 'Credential Type' dropdown. The form contains the following fields: 'Oracle SID' (text input) and 'Test default accounts (slow)' (checkbox, currently unchecked). The sidebar and 'Add Policy' header are the same as in the previous screenshot.

"Kerberos configuration" le permite especificar credenciales mediante claves Kerberos desde un sistema remoto:



The screenshot shows the 'Add Policy' interface with 'Kerberos configuration' selected in the 'Credential Type' dropdown. The form contains the following fields: 'Kerberos Key Distribution Center (KDC)' (text input), 'Kerberos KDC Port' (text input with '88'), 'Kerberos KDC Transport' (dropdown menu with 'udp'), and 'Kerberos Realm (SSH only)' (text input). The sidebar and 'Add Policy' header are the same as in the previous screenshots.

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**". Los protocolos de texto no cifrado admitidos para esta opción son **telnet**, **rsh** y **rexec**.



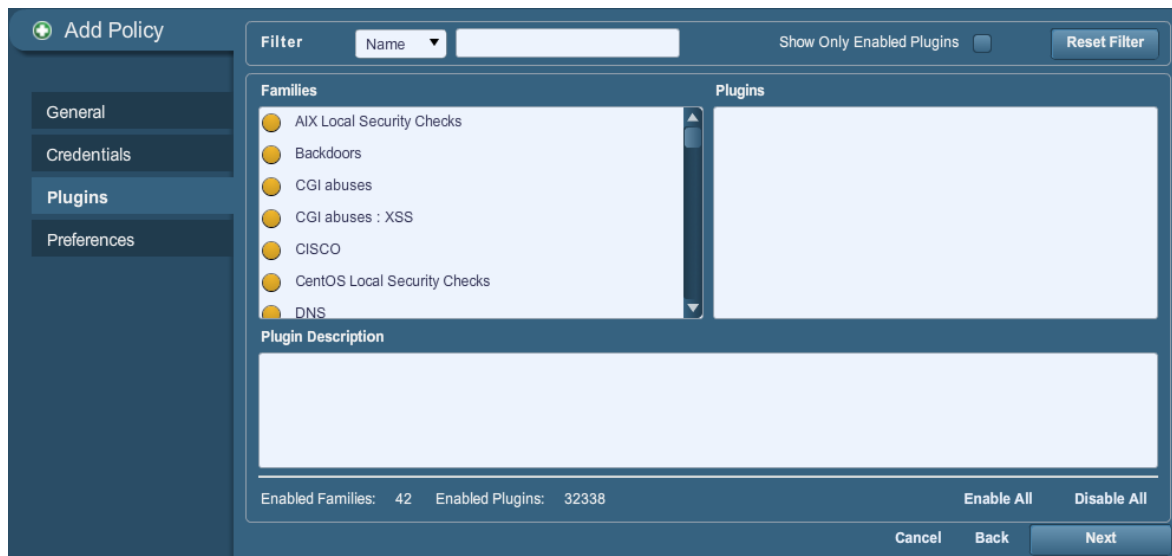
De forma predeterminada, todas las contraseñas (y la directiva en sí) se encuentran cifradas. Si la directiva se guarda en un archivo `.nessus` y luego ese archivo se copia en una instalación diferente de Nessus, ninguna de las contraseñas de la directiva podrá ser usada por el segundo analizador Nessus,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



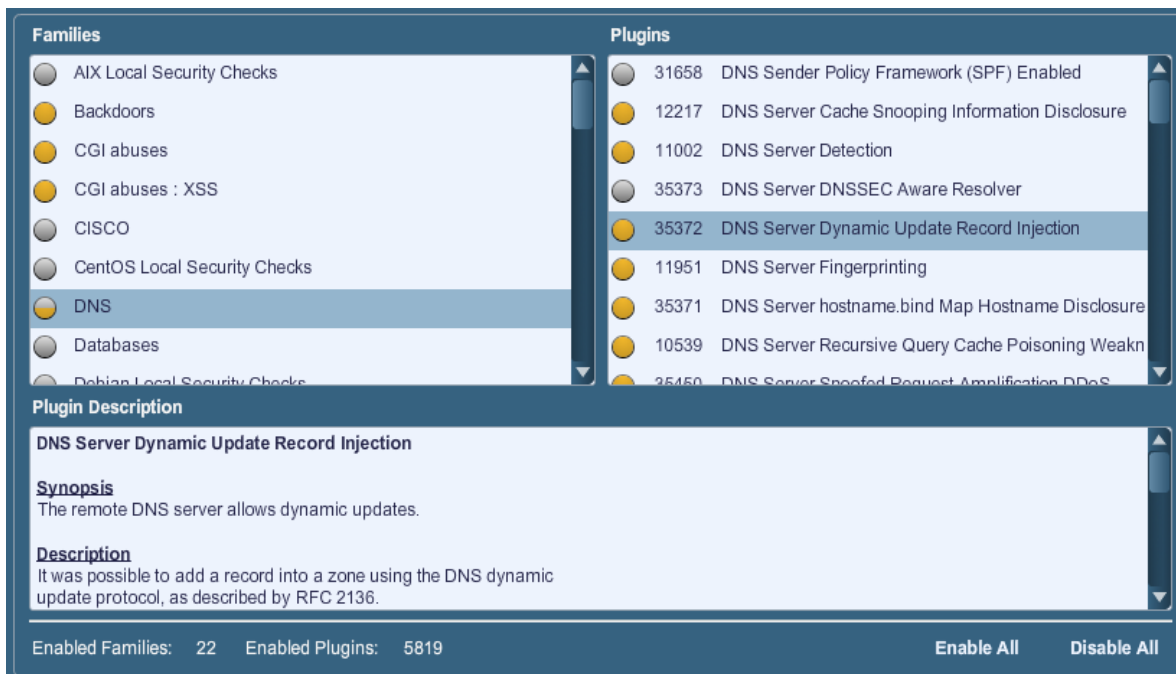
No se recomienda usar credenciales de texto no cifrado de forma alguna. Si las credenciales se envían de manera remota (por ejemplo, mediante un análisis de Nessus), estas podrían ser interceptadas por cualquier persona con acceso a la red. Siempre que sea posible, emplee mecanismos de autenticación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

Plugins

La ficha Plugin Selection permite al usuario elegir comprobaciones de seguridad específicas por familia de plugins o comprobaciones individuales.



Si hace clic en el círculo amarillo junto a una familia de plugins, podrá habilitar o deshabilitar la familia entera. Si selecciona una familia, aparecerá en pantalla la lista de sus plugins en el panel superior derecho. Se pueden habilitar o deshabilitar plugins individuales para crear directivas de análisis muy específicas. A medida que se efectúan ajustes, la cantidad total de familias y plugins seleccionados aparece en la parte inferior. Si el círculo que está junto a una familia de plugins es mitad gris y mitad amarillo, esto indica que algunos de los plugins están habilitados, pero no todos ellos.



Families

- ☐ AIX Local Security Checks
- ☐ Backdoors
- ☐ CGI abuses
- ☐ CGI abuses : XSS
- ☐ CISCO
- ☐ CentOS Local Security Checks
- ☒ DNS
- ☐ Databases
- ☐ Debian Local Security Checks

Plugins

- ☐ 31658 DNS Sender Policy Framework (SPF) Enabled
- ☐ 12217 DNS Server Cache Snooping Information Disclosure
- ☐ 11002 DNS Server Detection
- ☐ 35373 DNS Server DNSSEC Aware Resolver
- ☒ 35372 DNS Server Dynamic Update Record Injection
- ☐ 11951 DNS Server Fingerprinting
- ☐ 35371 DNS Server hostname.bind Map Hostname Disclosure
- ☐ 10539 DNS Server Recursive Query Cache Poisoning Weakness
- ☐ 35450 DNS Server Spoofed Request Amplification DDOS

Plugin Description

DNS Server Dynamic Update Record Injection

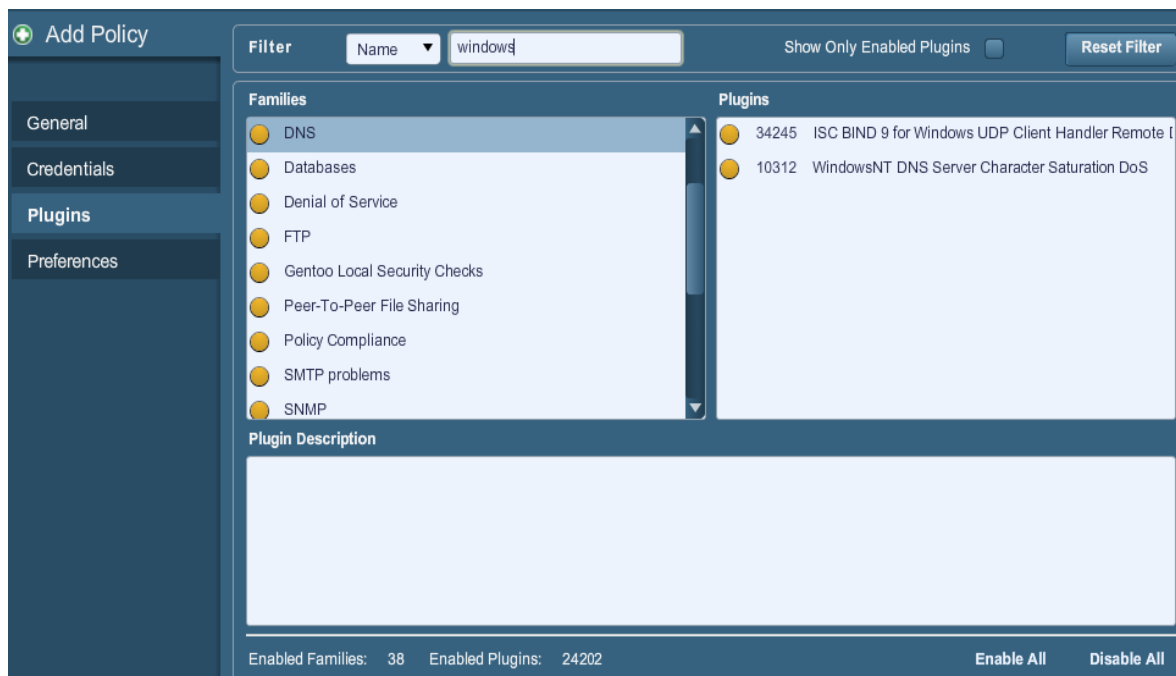
Synopsis
The remote DNS server allows dynamic updates.

Description
It was possible to add a record into a zone using the DNS dynamic update protocol, as described by RFC 2136.

Enabled Families: 22 Enabled Plugins: 5819 **Enable All** **Disable All**

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. Si se desplaza hacia abajo por el panel "Plugin Description" encontrará también información sobre soluciones, referencias adicionales –si están disponibles– y el puntaje CVSSv2 que ofrece una clasificación del riesgo básica.

En la parte superior de la ficha de familias de plugins puede buscar un plugin específico, por nombre o identificación. En el cuadro que está junto a **"Filter"** escriba el texto que se usará en la búsqueda, y pulse la tecla Enter (Intro):



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 esta familia también se deshabilitarán automáticamente.



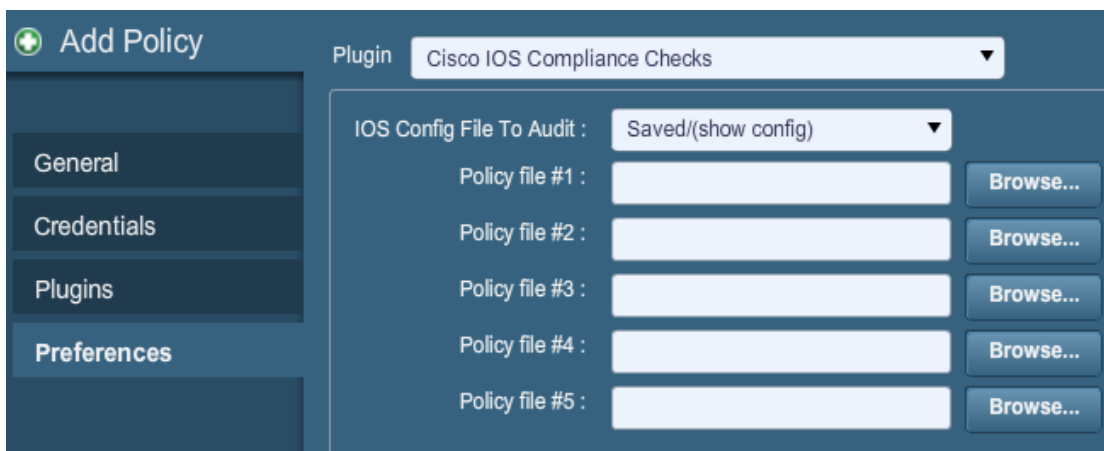
La familia "Denial of Service" contiene algunos plugins que podrían provocar interrupciones en redes corporativas si no se habilitó la opción "Safe Checks". Sin embargo, contiene algunas comprobaciones de utilidad que no producirán daño alguno. La familia "Denial of Service" se puede emplear junto con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

Debajo de la ventana que muestra los plugins, encontrará dos opciones que le ayudarán a seleccionar plugins.

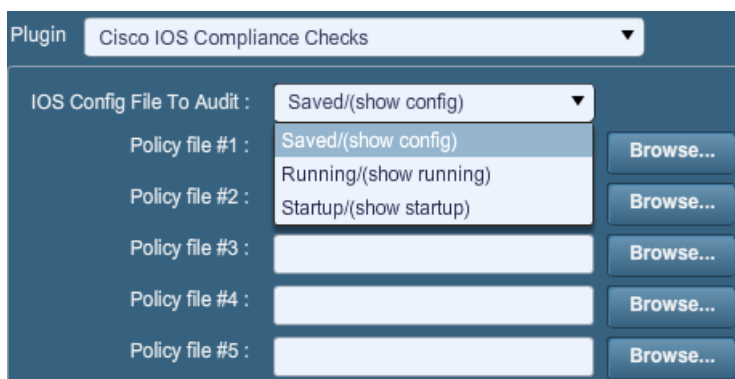
Opción	Descripción
Enable all	Marca y habilita todos los plugins y sus familias. Esta es una forma sencilla para volver a habilitar todos los plugins luego de crear una directiva con algunas familias o plugins deshabilitados. Tenga en cuenta que algunos plugins pueden requerir más opciones de configuración.
Disable all	Desmarca y deshabilita todos los plugins y sus familias. Si ejecuta un análisis con todos los plugins deshabilitados, no obtendrá ningún resultado.

Preferencias

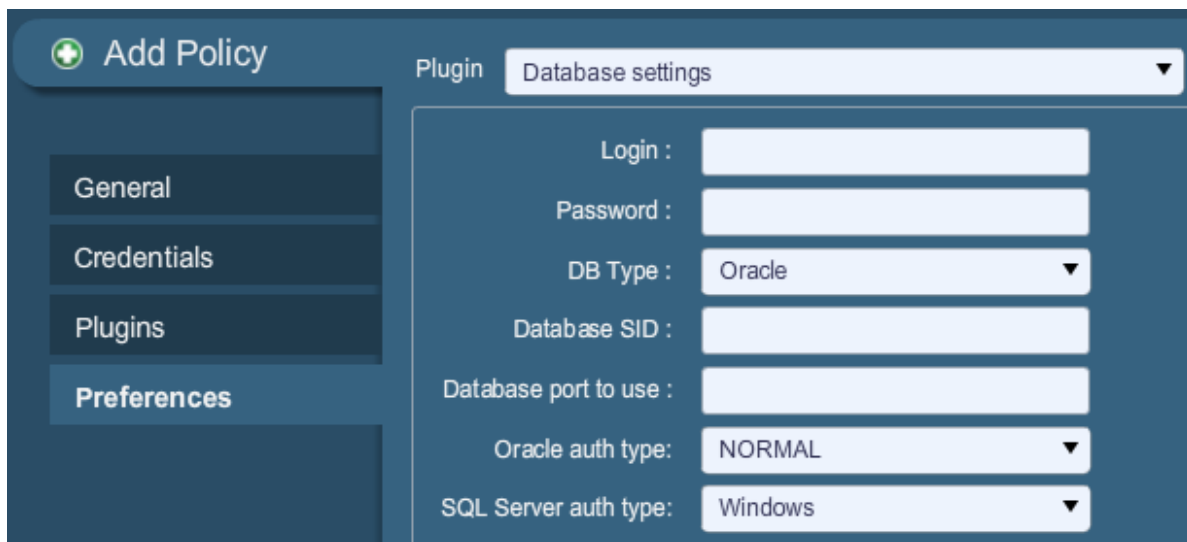
La ficha **"Preferences"** incluye medios para lograr un control pormenorizado de la configuración de los análisis. Si selecciona un elemento del menú desplegable, aparecerán elementos de configuración adicionales para la categoría seleccionada. Tenga en cuenta que se trata de una lista dinámica de opciones 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.



"Cisco IOS Compliance Checks" 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 (**show config**), Running (**show running**) o Startup (**show startup**).



"Database Compliance Checks" 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"** se usan para especificar el tipo de base de datos que se probará, la configuración correspondiente y las credenciales:

Opción	Descripción
Login	El nombre de usuario para la base de datos.
Password	La contraseña correspondiente al nombre de usuario proporcionado.
DB Type	Se admiten Oracle, SQL Server, MySQL, DB2, Informix/DRDA y PostgreSQL.
Database SID	La identificación de sistema de la base de datos para auditar.
Database port to use	Puerto en el que escucha la base de datos.
Oracle auth type	Se admiten NORMAL, SYSOPER y SYSDBA.
SQL Server auth type	Se admiten Windows o SQL.

Si se selecciona, **"Do not scan fragile devices"** ordena al analizador Nessus que no analice impresoras ni hosts de Novell Netware. Dado que estas dos tecnologías son más propensas a condiciones de denegación de servicio, Nessus puede omitir su análisis. Lo anterior se recomienda si los análisis se llevan a cabo durante el horario laboral.

Plugin Global variable settings ▼

Probe services on every port ☒

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

Enable CGI scanning ☐

Network type Mixed (use RFC 1918) ▼

Enable experimental scripts ☐

Thorough tests (slow) ☐

Report verbosity Normal ▼

Report paranoia Normal ▼

HTTP User-Agent Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)

SSL certificate to use : Browse...

SSL CA to trust : Browse...

SSL key to use : Browse...

SSL password for SSL key :

“Global variable settings” contiene una amplia variedad de opciones de configuración para el servidor Nessus.

Opción	Descripción
Probe services on every port	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 interferir con algunos servicios y producir efectos secundarios no previstos.
Do not log in with user accounts not specified in the policy	Se usa para evitar bloqueos de cuentas si su directiva de contraseña está ajustada para bloquear cuentas después de varios intentos no válidos.
Enable CGI scanning	Activa la comprobación de la CGI. Si se deshabilita esta opción, la auditoría de una red local se acelerará enormemente.
Network type	Le permite especificar si usa direcciones IP enrutables públicas, direcciones IP enrutables privadas fuera de Internet, o una mezcla de ambas. Seleccione “Mixed” si usa direcciones RFC 1918 y posee varios enrutadores dentro de su red.
Enable experimental scripts	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)	Hace que distintos plugins “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 interrupciones en la red. No obstante, cabe la posibilidad de que se produzcan mejores resultados de auditoría.
Report verbosity	Una opción superior o inferior brindará más o menos información sobre la actividad del plugin en el informe.
Report paranoia	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” , 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” hará que Nessus no informe ningún error cuando haya indicios de incertidumbre sobre el host remoto. La opción predeterminada (“Normal”) constituirá el término medio entre estas dos.
HTTP User-Agent	Especifica el tipo de explorador web al que Nessus suplantaré durante el análisis.
SSL certificate to use	Permite que Nessus use un certificado SSL del lado cliente para comunicarse con un host remoto.
SSL CA to trust	Especifica una Entidad de certificación (Certificate Authority, CA) en la que confiará Nessus.
SSL key to use	Especifica una clave de SSL local que se usará para comunicarse con el host remoto.
SzSSL password for SSL key	La contraseña para administrar la clave de SSL especificada.



Plugin: HTTP cookies import ▼

Cookies file : [Browse...](#)

Para facilitar las pruebas de la aplicación web, Nessus puede importar cookies HTTP de otro software (por ejemplo, un explorador web, un proxy web, etc.) mediante la configuración **“HTTP cookies import”**. 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.

Plugin
HTTP login page ▼

Login page : /

Login form :

Login form fields : user=%USER%&pass=%PASS%

Login form method : POST ▼

Automated login page search ☐

Re-authenticate delay (seconds) :

Check authentication on page :

Follow 30x redirections (# of levels) : 2

Authenticated regex :

Invert test (disconnected if regex matches) ☐

Match regex on HTTP headers ☐

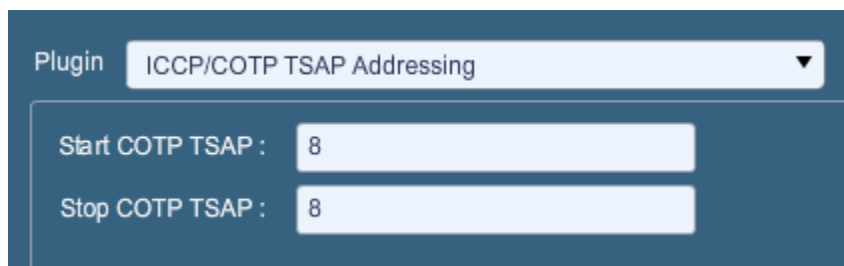
Case insensitive regex ☐

Abort web application tests if login fails ☐

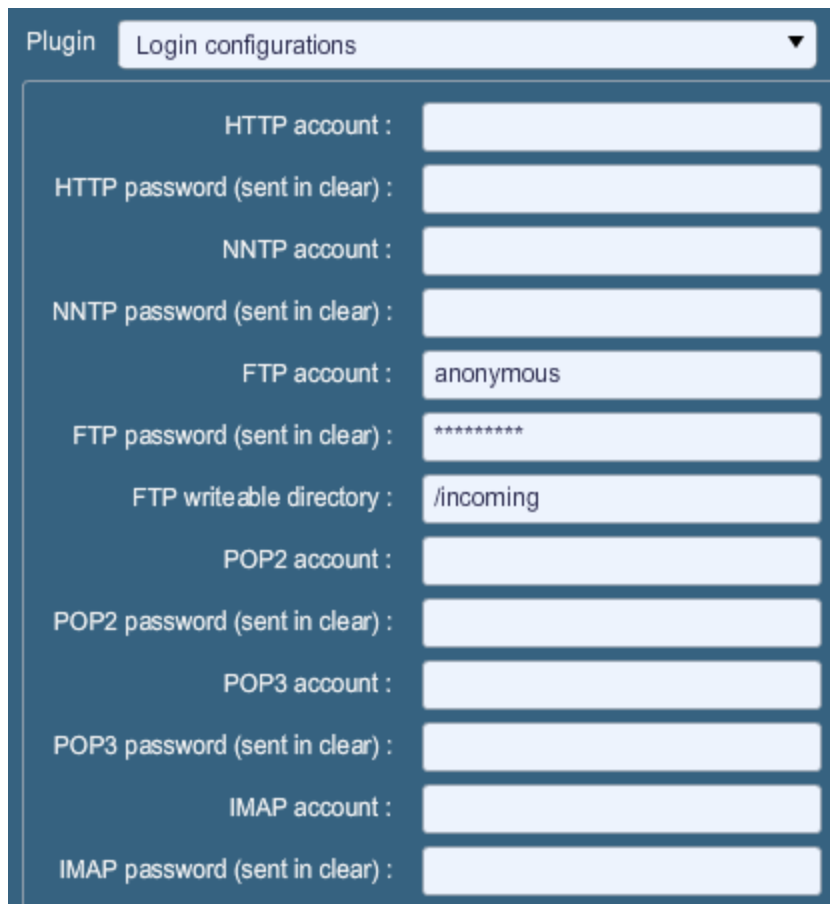
La configuración **"HTTP login page"** permite controlar el lugar en el que comienzan las pruebas autenticadas de una aplicación web personalizada.

Opción	Descripción
Login page	La dirección URL base de la página de inicio de sesión de la aplicación.
Login form	El parámetro "action" correspondiente al método de formulario. Por ejemplo, el formulario de inicio de sesión para <code><form method="POST" name="auth_form" action="/login.php"></code> sería <code>/login.php</code> .
Login form fields	Especifica los parámetros de autenticación (por ejemplo, <code>login=%USER%&password=%PASS%</code>). Si se usan las palabras clave <code>%USER%</code> y <code>%PASS%</code> , 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 "grupo" u otro dato).
Login form method	Especifica si la acción de inicio de sesión se lleva a cabo mediante una solicitud GET o POST.
Automated login page search	Ordena a Nessus que busque una página de inicio de sesión.
Re-authenticate delay (seconds)	La demora entre los intentos de autenticación. Esto resulta de utilidad para evitar que se activen mecanismos de bloqueo

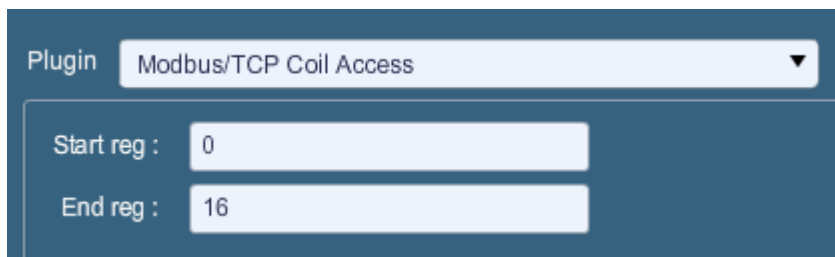
	de fuerza bruta.
Check authentication on page	La dirección URL de una página web protegida que requiere autenticación, con el fin de brindar mayor ayuda a Nessus al determinar el estado de la autenticación.
Follow 30x redirections (# of levels)	Si se recibe un código de redireccionamiento 30x por parte de un servidor web, esto indica a Nessus que siga o no el enlace proporcionado.
Authenticated regex	Es el patrón de la 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)	Es el patrón de la 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	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	Las búsquedas de regex distinguen mayúsculas de minúsculas de forma predeterminada. Esta opción ordena a Nessus que omita mayúsculas y minúsculas.
Abort web application tests if login fails	Si no funcionan las credenciales suministradas, Nessus interrumpirá las pruebas personalizadas de la aplicación web (pero no las familias de plugins de CGI).



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



“Login configurations” 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”.

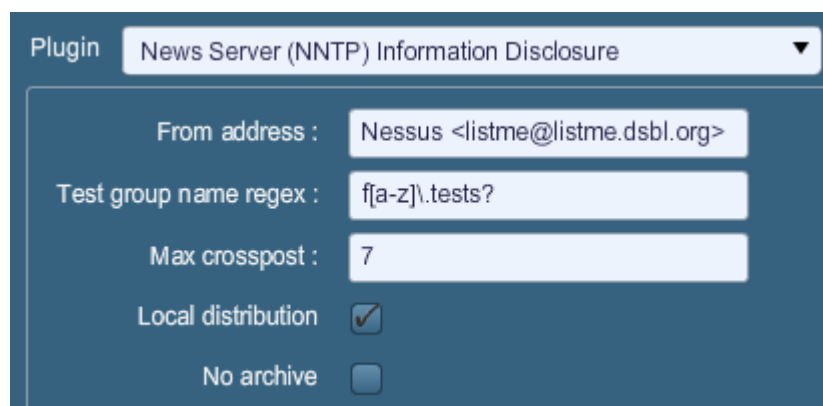


Las opciones **“Modbus/TCP Coil Access”** se encuentran disponibles para los usuarios de ProfessionalFeed. Este elemento del menú desplegable es generado de manera dinámica por los plugins de SCADA, disponibles mediante la ProfessionalFeed. Modbus usa un código de función de 1 para leer “bobinas” en 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**" y "**Nessus TCP scanner**" le permiten ajustar mejor los analizadores nativos SYN y TCP para que detecten la presencia de un firewall.


Valor	Descripción
Automatic (normal)	Esta opción puede ayudar a identificar si se encuentra un firewall entre el analizador y el destino (predeterminado).
Disabled (softer)	Deshabilita la característica de detección de firewall .
Do not detect RST rate limitation (soft)	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)	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**" 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	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	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	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 si hay 2000 servidores de noticias que coincidan con la regex en este campo.
Local distribution	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	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" configura Nessus con el Oracle Database SID e incluye una opción para probar si existen cuentas predeterminadas conocidas en el software de Oracle.

"PCI DSS Compliance" 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.

Plugin
Ping the remote host ▼

TCP ping destination port(s) : built-in

Do an ARP ping ☒

Do a TCP ping ☒

Do an ICMP ping ☒

Number of retries (ICMP) : 2

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

Make the dead hosts appear in the report ☐

Log live hosts in the report ☐

Test the local Nessus host ☒

Fast network discovery ☐

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

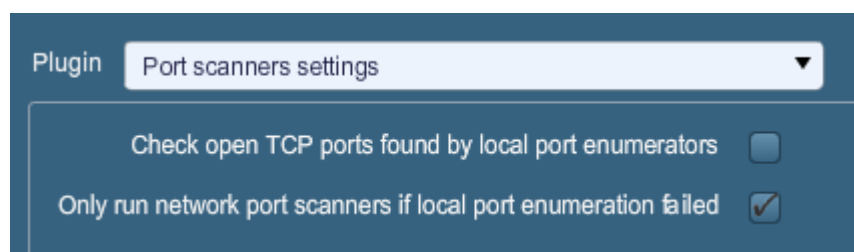
Opción	Descripción
TCP ping destination port(s)	Especifica la lista de puertos que se comprobarán mediante el ping TCP. Si no tiene seguridad sobre los puertos, deje este parámetro con el valor predeterminado "built-in" (Incorporado).
Number of Retries (ICMP)"	Le permite especificar la cantidad de intentos para tratar de efectuar un ping al host remoto. El valor predeterminado está establecido en 6.
Do an applicative UDP ping (DNS, RPC...)	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	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	Seleccione esta opción para informar específicamente de la capacidad de realizar pings satisfactorios a hosts remotos.
Test the local Nessus host	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

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”, desmarque los pings TCP, ICMP y ARP.



“Port scanner settings” proporciona dos opciones para control adicional de la actividad de análisis de puertos:

Opción	Descripción
Check open TCP ports found by local port enumerators	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	De lo contrario, tenga en cuenta primero la enumeración de puerto local.

“SMB Use Host SID to Enumerate Local Users” 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" 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"** especificado. Si el mensaje enviado a **"Third party domain"** es rechazado por la dirección especificada en el campo "To address", se habrá producido un error en el intento de enviar correo no deseado. Si se acepta el mensaje, significa que el servidor SMTP se usó satisfactoriamente para retransmitir correo no deseado.

Opción	Descripción
Third party domain	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 o del sitio que realiza el análisis. De lo contrario, es posible que el servidor SMTP anule la prueba.
From address	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	Nessus intentará enviar mensajes dirigidos al destinatario del correo que se indica en este campo. La dirección postmaster constituye el valor predeterminado, ya que es una dirección válida en la mayoría de los servidores de correo.

Plugin
SNMP settings

Community name : public

Community name (1) :

Community name (2) :

Community name (3) :

UDP port : 161

SNMPv3 user name :

SNMPv3 authentication password :

SNMPv3 authentication algorithm : MD5

SNMPv3 privacy password :

SNMPv3 privacy algorithm : DES

“SNMP settings” 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. Según la directiva de análisis, se admiten hasta cuatro cadenas de nombres de comunidades individuales. Si Nessus no puede estimar la cadena de comunidad o la contraseña, es posible que no realice una auditoría completa del servicio.

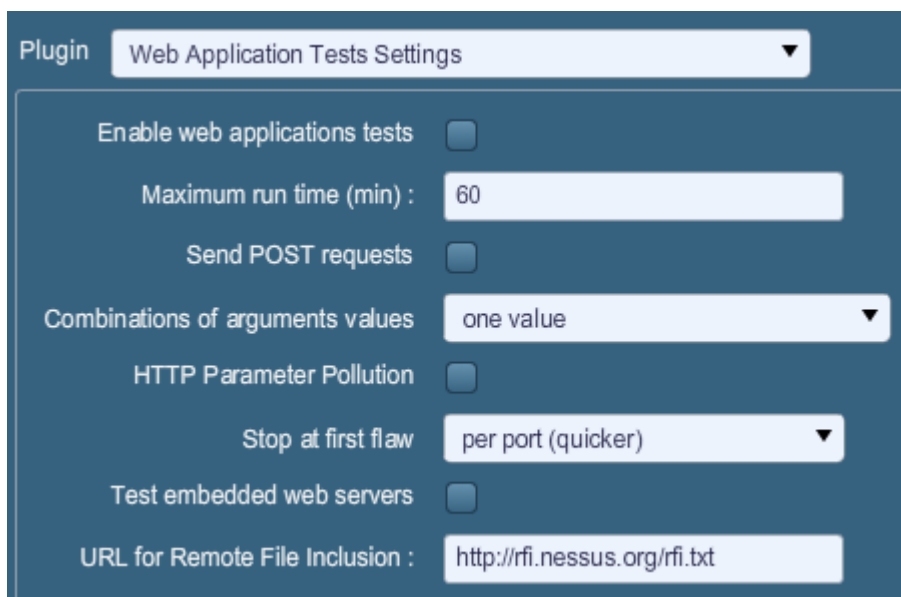
Opción	Descripción
Community name (0-3)	El nombre de comunidad SNMP.
UDP port	Ordena a Nessus analizar un puerto diferente si SNMP se ejecutara en un puerto distinto del 161.
SNMPv3 user name	El nombre de usuario para una cuenta basada en SNMPv3.
SNMPv3 authentication password	La contraseña correspondiente al nombre de usuario especificado.
SNMPv3 authentication algorithm	Seleccione MD5 o SHA1 de acuerdo con el algoritmo que admita el servicio remoto.
SNMPv3 privacy password	La contraseña usada para proteger la comunicación SNMP cifrada.
SNMPv3 privacy algorithm	El algoritmo de cifrado que se usará para el tráfico SNMP.

“Service Detection” 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 interrumpir el funcionamiento del host en el que se realiza la prueba.

“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  
[...]
```

“**Unix Compliance Checks**” 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.



“**Web Application Tests Settings**” prueba los argumentos de las interfaces de puertas de enlace comunes (Common Gateway Interface, CGI) 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 remotos, ejecución de comandos, ataques de cruces seguros o inyección de código SQL. Habilite esta opción seleccionando la casilla de verificación “Enable web applications tests”. Estas pruebas dependen de los siguientes plugins NASL:

- > [11139](#), [42424](#), [42479](#), [42426](#), [42427](#), [43160](#) – SQL Injection (CGI abuses)
- > [39465](#), [44967](#) – Command Execution (CGI abuses)
- > [39466](#), [47831](#), [42425](#), [46193](#), [49067](#) – Cross-Site Scripting (CGI abuses: XSS)
- > [39467](#), [46195](#), [46194](#) – Directory Traversal (CGI abuses)
- > [39468](#) – HTTP Header Injection (CGI abuses: XSS)
- > [39469](#), [42056](#), [42872](#) – File Inclusion (CGI abuses)
- > [42055](#) – Format String (CGI abuses)
- > [42423](#), [42054](#) – Server Side Includes (CGI abuses)

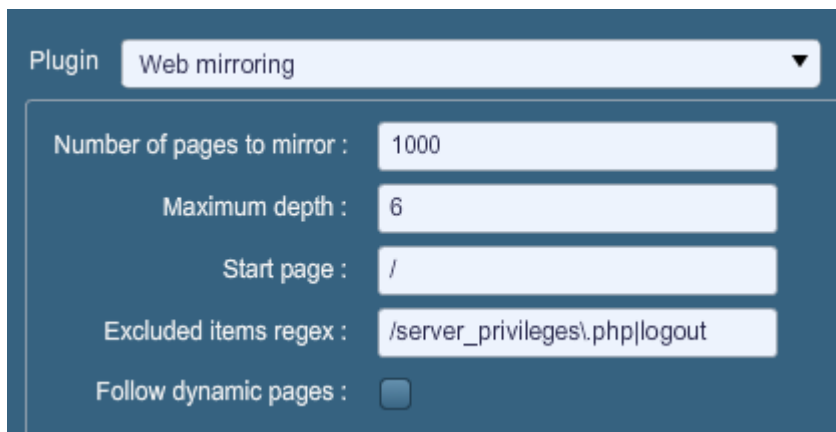
- > [44136](#) – Cookie Manipulation (CGI abuses)
- > [46196](#) – XML Injection (CGI abuses)
- > [40406](#), [48926](#), [48927](#) – Error Messages
- > [47830](#), [47832](#), [47834](#), [44134](#) – Additional attacks (CGI abuses)

Importante: Esta lista de plugins relacionados con aplicaciones web se actualiza con frecuencia. Es posible que haya plugins adicionales que dependan de la configuración en esta opción de preferencias.

Opción	Descripción
Maximum run time (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 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.
Send POST requests	Las pruebas de "solicitudes POST" se usan en pruebas de formularios web mejorados. 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 sus 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	<p>Esta opción administra la combinación de valores de argumentos usados en las solicitudes HTTP. Este menú desplegable ofrece tres opciones:</p> <p>one value: prueba un parámetro por vez con una cadena de ataque, sin intentar variaciones de "no ataque" en el caso de parámetros adicionales. Por ejemplo, Nessus intentaría usar <code>"/test.php?arg1=XSS&b=1&c=1"</code>, 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.</p> <p>All pairs (slower but efficient): esta forma de prueba es ligeramente más lenta pero más eficaz que la prueba "one value". Al probar varios parámetros, probará una cadena de ataque, variaciones de una única variable, y luego usará el primer valor para todas las otras variables. Por ejemplo, Nessus intentaría usar <code>"/test.php?a=XSS&b=1&c=1&d=1"</code> y luego recorrería las variables, de modo que una reciba una cadena de ataque, la otra pase por todos los valores posibles</p>

	<p>(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 <code>"/test.php?a=XSS&b=3&c=3&d=3"</code> cuando el primer valor de cada variable sea <code>"1"</code>.</p> <p>All combinations (extremely slow): 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" procuran crear conjuntos de datos más pequeños y lograr a cambio mayor velocidad, "all combinations" no garantiza rapidez y usa un conjunto completo de datos de pruebas. Este método de prueba puede tardar mucho tiempo en completarse.</p>
HTTP Parameter Pollution	<p>Al efectuar pruebas de aplicaciones web, intenta sortear los 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: <code>"/target.cgi?a='&b=2"</code>. Con la opción HTTP Parameter Pollution (HPP) (Contaminación de parámetros http [HPP]) habilitada, la solicitud puede tener la siguiente apariencia: <code>"/target.cgi?a='&a=1&b=2"</code>.</p>
Stop at first flaw	<p>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". 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:</p> <p>per 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.</p> <p>per port (quicker) – 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.</p> <p>per parameter (slow) – Cuando se detecta un error en un parámetro de una CGI (por ejemplo, XSS), Nessus cambia al siguiente parámetro de la misma CGI o a la siguiente CGI</p>

	<p>conocida, o bien al siguiente puerto o servidor.</p> <p>look for all flaws (slower) – 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.</p>
Test Embedded web servers	<p>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.</p>
URL for Remote File Inclusion	<p>Durante las pruebas de Inclusión de archivos remotos (Remote File Inclusion, RFI), 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.</p>



The screenshot shows the 'Web mirroring' plugin configuration in Nessus. The 'Plugin' dropdown is set to 'Web mirroring'. Below it, there are several input fields: 'Number of pages to mirror' is set to 1000, 'Maximum depth' is set to 6, 'Start page' is set to '/', and 'Excluded items regex' is set to '/server_privileges\.php|logout'. The 'Follow dynamic pages' checkbox is unchecked.

“Web Mirroring” 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 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	La cantidad máxima de páginas que se reflejarán.
Maximum depth	Limita la cantidad de enlaces que Nessus seguirá para cada página de inicio.
Start page	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	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: <code>(^/manual) (\.pl (\?.*) ?\$) .</code>
Follow dynamic pages	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" 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" para guardar la directiva y volver a la ficha Políticas. En cualquier momento puede hacer clic en "Edit" para efectuar cambios en una directiva que ya haya creado, o hacer clic en "Delete" para eliminar una directiva por completo.

IMPORTACIÓN, EXPORTACIÓN Y COPIA DE DIRECTIVAS

El botón **"Import"** de la barra de menús situada en la esquina superior derecha le permitirá cargar en el analizador directivas creadas con anterioridad. Mediante el cuadro de diálogo **"Browse..."**, seleccione la directiva de su sistema local y haga clic en **"Submit"**.

El botón **"Export"** de la barra de menús le permitirá descargar una directiva existente del analizador al sistema local de archivos. 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.

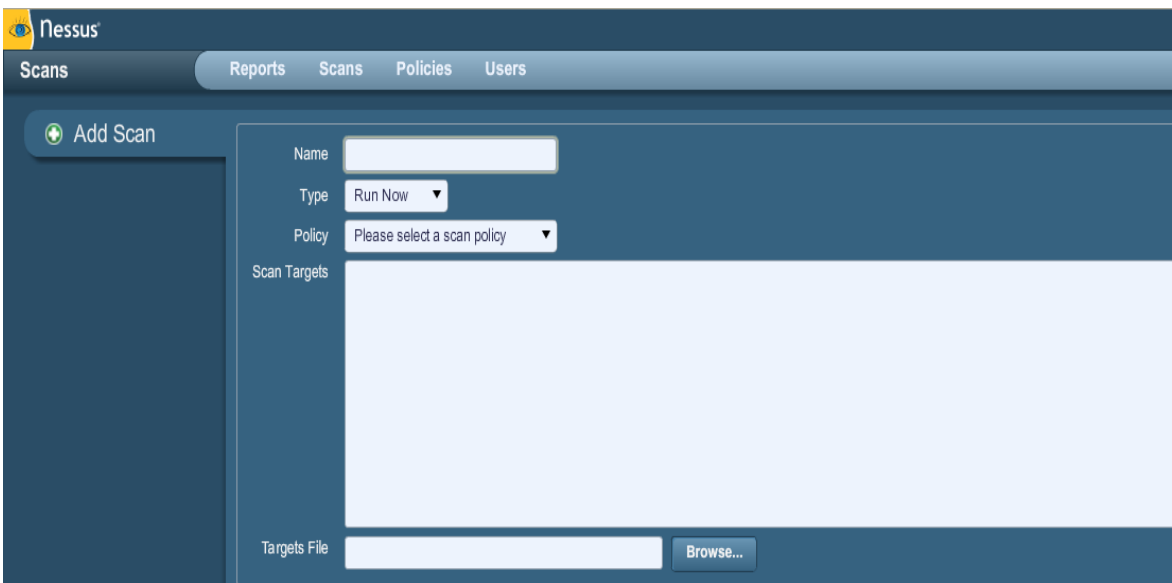
Si desea crear una directiva similar a una existente con pequeñas modificaciones, puede seleccionar la directiva de base de la lista y hacer clic en **"Copy"** en la barra de menús de la esquina superior derecha. Esto creará una copia de la directiva original que podrá editarse para efectuar cualquier 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



Name	Owner	Status	Start Time
Discovery 5	admin	Template	Never
Media Machine	admin	Template	Never
Payment Network	admin	Template	Never

Después de crear una directiva puede crear un nuevo análisis; para ello haga clic en la opción **"Scans"** de la barra de menús situada en la parte superior y luego haga clic en el botón **"Add Scan"** de la derecha. Aparecerá la pantalla **"Add Scan"**, como se muestra a continuación:



The 'Add Scan' form in Nessus includes the following fields:

- Name:** A text input field for the scan name.
- Type:** A dropdown menu with 'Run Now' selected.
- Policy:** A dropdown menu with 'Please select a scan policy'.
- Scan Targets:** A large text area for specifying targets.
- Targets File:** A text input field for a file path, accompanied by a 'Browse...' button.

Hay cinco campos para introducir el destino del análisis:

- > **Name:** establece el nombre que aparecerá en la UI de Nessus para identificar el análisis.
- > **Type:** seleccione entre "Run Now" (para ejecutar el análisis inmediatamente después de ejecutar el comando "Submit" [Enviar]), "Scheduled" (para seleccionar la hora en que debe comenzar el análisis) o "Template" (para guardar como plantilla para otro análisis posterior).

- > **Policy:** seleccione una directiva creada anteriormente que usará el análisis para establecer los parámetros que controlan el comportamiento de análisis del servidor Nessus.
- > **Scan Targets:** 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).
- > **Targets File:** se puede importar un archivo de texto con una lista de hosts haciendo clic en "**Browse...**" y seleccionando un archivo del equipo local.



Al archivo de host 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 "**Submit**". Después de realizar esta acción (Enviar) el análisis comenzará de inmediato (si se seleccionó "Run Now"), antes de que la pantalla vuelva a la página general "**Scans**".

Nessus


admin | Help | About | Log out


Scans

ReportsScansPoliciesUsers


Add

Edit

Browse

Launch

Pause

Stop

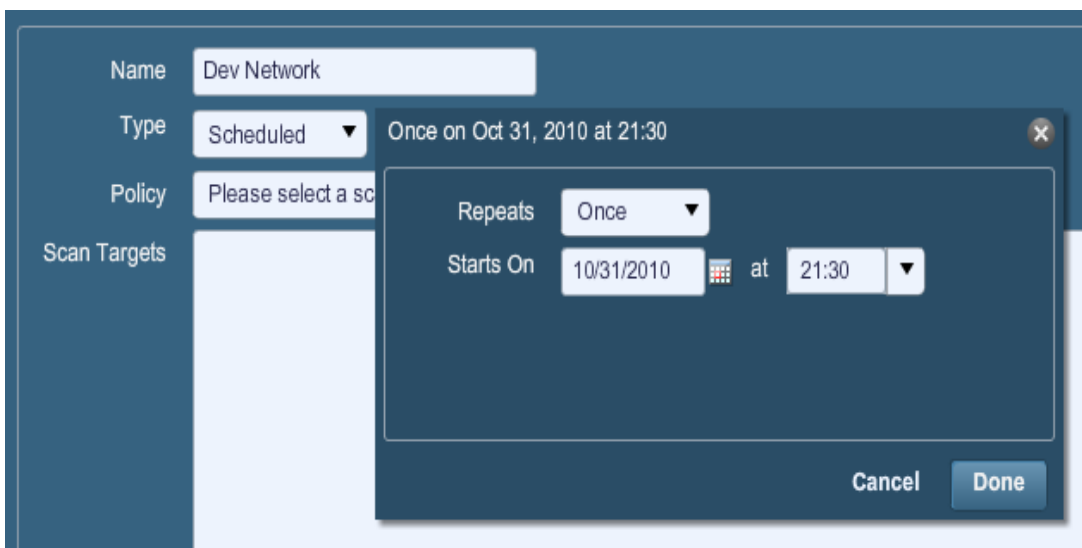
Delete

Name	Owner	Status	Start Time
Discovery 5	admin	Template	Never
HR Subnet	admin	0 IPs / 206 IPs	Oct 28, 2010 20:00
Media Machine	admin	Template	Never
Payment Network	admin	Template	Never

Una vez iniciado el análisis, en la lista Scans se mostrará una lista de todos los análisis que estén en curso en ese momento, pausados o basados en plantillas, junto con la información básica del análisis. Después de seleccionar un análisis de la lista en particular, los botones de acción situados en la parte superior derecha le permitirán explorar (**"Browse"**) los resultados del análisis en curso, poner en pausa (**"Pause"**) y reanudar (**"Resume"**) el análisis, o detenerlo (**"Stop"**) y eliminarlo (**"Delete"**) por completo. Los usuarios también pueden modificar (**"Edit"**) los análisis basados en plantillas.

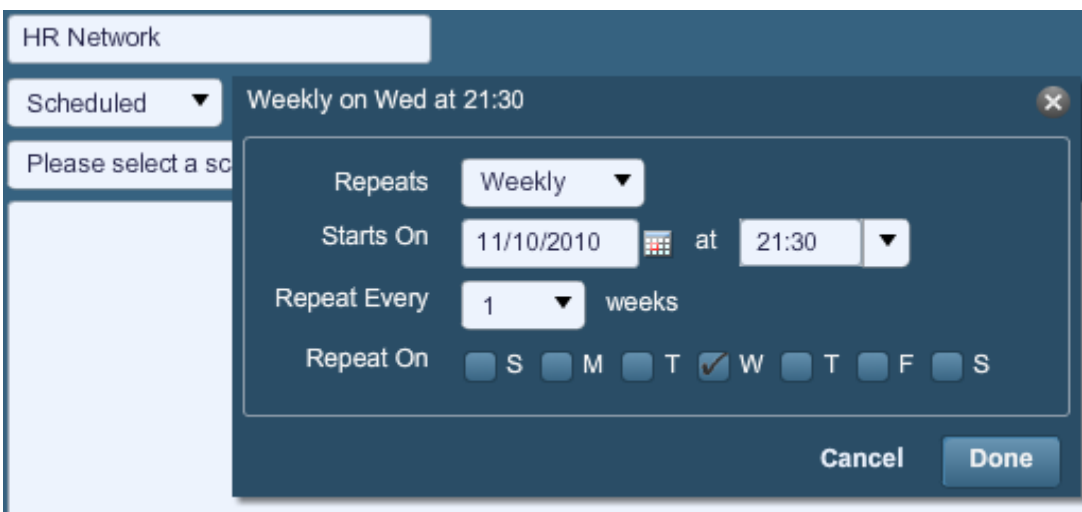
Una vez finalizado un análisis (por cualquier motivo), se quitará de la lista **"Scans"** y estará disponible para su revisión en la ficha **"Reports"**.

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



The screenshot shows the configuration for a scan named "Dev Network". The "Type" is set to "Scheduled". A modal dialog is open for scheduling, showing "Repeats" as "Once" and "Starts On" as "10/31/2010 at 21:30". The dialog has "Cancel" and "Done" buttons.

Mediante el menú desplegable "Repeats" 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.



The screenshot shows the configuration for a scan named "HR Network". The "Type" is set to "Scheduled". A modal dialog is open for scheduling, showing "Repeats" as "Weekly", "Starts On" as "11/10/2010 at 21:30", "Repeat Every" as "1 weeks", and "Repeat On" with checkboxes for S, M, T, W, T, F, S. The "W" checkbox is checked. The dialog has "Cancel" and "Done" buttons.



Los análisis se inician de acuerdo con la hora establecida en el servidor del analizador Nessus.

Si un análisis se guarda como plantilla, aparecerá en la lista de análisis como tal y esperará a ser iniciado.



The screenshot shows the Nessus web interface with the 'Scans' tab selected. The top navigation bar includes 'admin', 'Help', 'About', and 'Log out'. Below the navigation bar, there are tabs for 'Reports', 'Scans', 'Policies', and 'Users'. The 'Scans' tab is active, and it contains a toolbar with buttons for 'Add', 'Edit', 'Browse', 'Launch', 'Pause', 'Stop', and 'Delete'. Below the toolbar is a table with the following data:

Name	Owner	Status	Start Time
Payment Network	admin	Template	Never



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

INFORMES

Con el lanzamiento de Nessus 4.2, en el sistema de generación de informes se integraron mejor las hojas de estilo para informes. 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. Además, se mejoró la compatibilidad con hojas de estilo para que se puedan realizar actualizaciones o adiciones de hojas de estilo mediante la fuente de plugins. Esto permitirá a Tenable lanzar hojas de estilo adicionales sin que sean necesarias actualizaciones o nuevas versiones principales.

Si hace clic en la ficha **"Reports"**, en la barra de menús situada en la parte superior de la interfaz, aparecerá la lista de análisis en ejecución y terminados:



The screenshot shows the Nessus web interface with the 'Reports' tab selected. The top navigation bar includes 'admin', 'Help', 'About', and 'Log out'. Below the navigation bar, there are tabs for 'Reports', 'Scans', 'Policies', and 'Users'. The 'Reports' tab is active, and it contains a toolbar with buttons for 'Browse', 'Compare', 'Upload', 'Download', and 'Delete'. Below the toolbar is a table with the following data:

Name	Status	Last Updated
Dev Subnet	Completed	Nov 3, 2009 24:35
HR Subnet	Running	Nov 3, 2009 24:38
Local Desktop	Completed	Nov 3, 2009 24:40

La pantalla **"Reports"** se desempeña como punto central para ver, comparar, cargar y descargar resultados de análisis. Use la tecla "Shift" o "Ctrl" para seleccionar varios informes a la vez.

Explorar

Para explorar los resultados de un análisis, seleccione un nombre de la lista "Reports" y haga clic en **"Browse"**. Esto le permite ver resultados al navegar por hosts, puertos y

vulnerabilidades específicas. La primera pantalla de resumen muestra cada host analizado, junto con un detalle de las vulnerabilidades y los puertos abiertos:

[illegible]

Con un host seleccionado, el informe se dividirá por números de puerto y aparecerá información relacionada, tal como el protocolo y el nombre del servicio, así como también un resumen de las vulnerabilidades clasificadas por gravedad del riesgo. A medida que navega por los resultados del análisis, la interfaz de usuario mantendrá la lista de hosts y una serie de flechas interactivas para ayudarle a navegar rápidamente hasta un componente específico del informe:

Report Info	LAN Scan						6 results
Hosts	192.168.0.10						
	Port	Protocol	SVC Name	Total	High	Medium	Low
192.168.0.1	0	tcp	general	7	0	0	7
192.168.0.10	0	udp	general	1	0	0	1
192.168.0.20	137	udp	netbios-ns	1	0	0	1
192.168.0.100	139	tcp	smb	1	0	0	1
	445	tcp	cifs	13	1	1	11
	2869	tcp	www	3	0	0	3

Si selecciona un puerto, aparecerán todos los resultados de las vulnerabilidades que se relacionan con el puerto y el servicio:

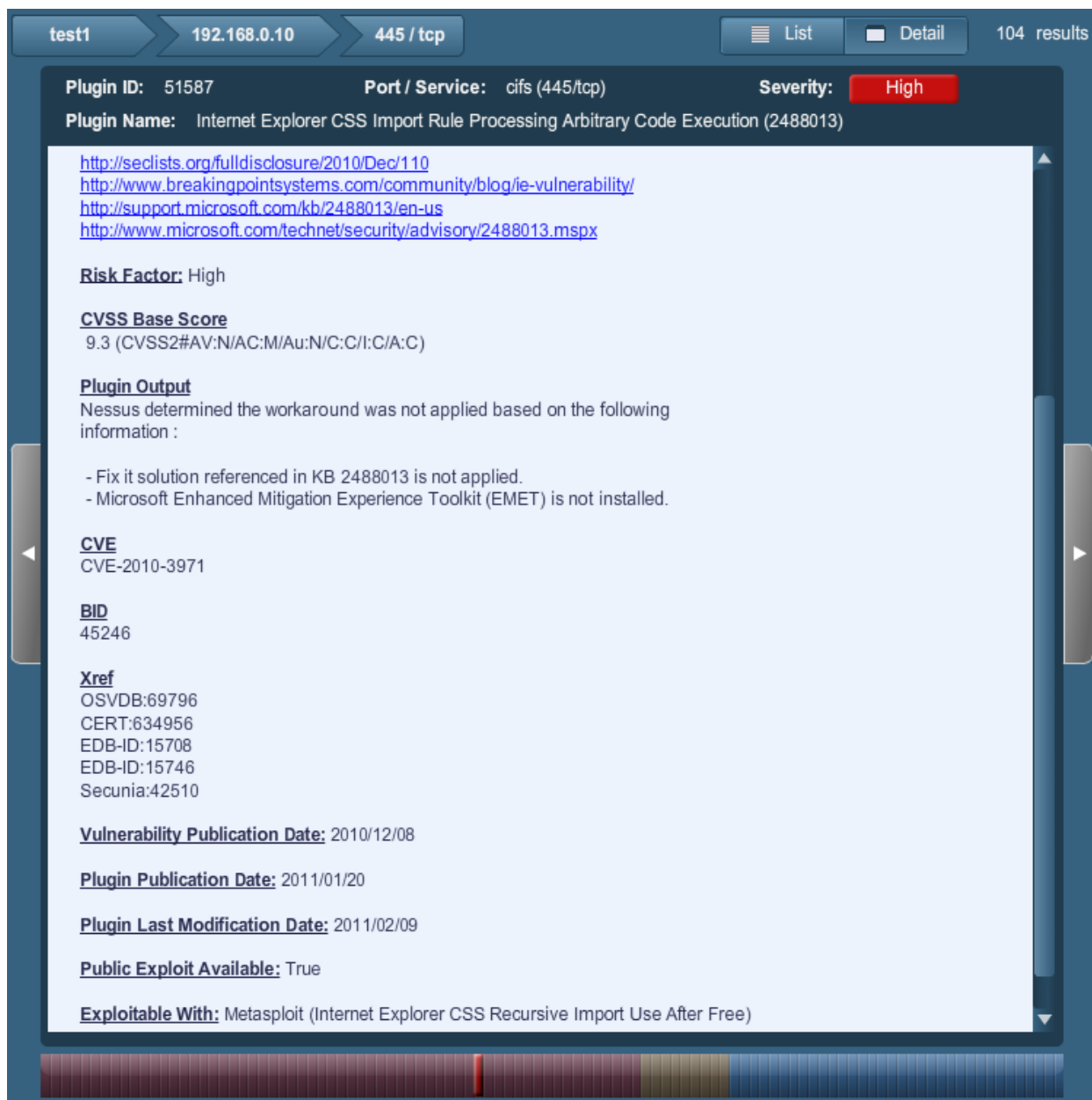
<div> <div>LAN Scan</div> <div>192.168.0.10</div> <div>445 / tcp</div> <div>List</div> <div>Detail</div> <div>13 results</div> </div>			
Plugin ID	Name	Port	Severity
11011	SMB Detection	cifs (445/tcp)	Low
10785	SMB NativeLanMan	cifs (445/tcp)	Low
10394	SMB log in	cifs (445/tcp)	Low
10859	SMB get host SID	cifs (445/tcp)	Low
10860	SMB use host SID to enumerate local users	cifs (445/tcp)	Low
10395	SMB shares enumeration	cifs (445/tcp)	Low
26919	SMB guest account for all users	cifs (445/tcp)	Medium
10397	SMB LanMan Pipe Server browse listing	cifs (445/tcp)	Low
10396	Microsoft Windows SMB Shares Access	cifs (445/tcp)	High
23974	SMB Share Hosting Office Files	cifs (445/tcp)	Low
10400	SMB accessible registry	cifs (445/tcp)	Low
10428	SMB fully accessible registry	cifs (445/tcp)	Low
26920	SMB NULL session	cifs (445/tcp)	Low

En el ejemplo anterior vemos que el host 192.168.0.10 tiene 13 vulnerabilidades relacionadas con el puerto TCP 445 (CIFS o Sistema de archivos de Internet común). El resumen de los resultados muestra la identificación de los plugins de Nessus, el nombre de las vulnerabilidades, el puerto, el protocolo y la gravedad. Si hace clic una vez en el encabezado de cualquier columna, los resultados se pueden clasificar en función del contenido de la columna. Si hace clic otra vez, invertirá el orden de los resultados:

<div> <div>LAN Scan</div> <div>192.168.0.10</div> <div>445 / tcp</div> <div>List</div> <div>Detail</div> <div>13 results</div> </div>			
Plugin ID	Name	Port	Severity ▼
10396	Microsoft Windows SMB Shares Access	cifs (445/tcp)	High
26919	SMB guest account for all users	cifs (445/tcp)	Medium
10397	SMB LanMan Pipe Server browse listing	cifs (445/tcp)	Low
10859	SMB get host SID	cifs (445/tcp)	Low
10860	SMB use host SID to enumerate local users	cifs (445/tcp)	Low
10395	SMB shares enumeration	cifs (445/tcp)	Low
11011	SMB Detection	cifs (445/tcp)	Low
10394	SMB log in	cifs (445/tcp)	Low
10785	SMB NativeLanMan	cifs (445/tcp)	Low
23974	SMB Share Hosting Office Files	cifs (445/tcp)	Low
10400	SMB accessible registry	cifs (445/tcp)	Low
10428	SMB fully accessible registry	cifs (445/tcp)	Low
26920	SMB NULL session	cifs (445/tcp)	Low

Si selecciona una vulnerabilidad de la lista aparecerán detalles completos de los resultados, incluidos una sinopsis, una descripción técnica, la solución, el factor de riesgo, el puntaje

CVSS, salidas relevantes que prueben los resultados, referencias externas, la fecha de publicación de la vulnerabilidad, la fecha de publicación o modificación de los plugins y la disponibilidad de las vulnerabilidades de seguridad:



The screenshot shows the Tenable Nessus interface for a specific vulnerability. At the top, navigation tabs show 'test1', '192.168.0.10', and '445 / tcp'. On the right, there are buttons for 'List' and 'Detail', and a count of '104 results'. The main content area displays the following details:

- Plugin ID:** 51587
- Port / Service:** cifs (445/tcp)
- Severity:** High (indicated by a red box)
- Plugin Name:** Internet Explorer CSS Import Rule Processing Arbitrary Code Execution (2488013)
- References:** <http://seclists.org/fulldisclosure/2010/Dec/110>, <http://www.breakingpointsystems.com/community/blog/ie-vulnerability/>, <http://support.microsoft.com/kb/2488013/en-us>, <http://www.microsoft.com/technet/security/advisory/2488013.msp>
- Risk Factor:** High
- CVSS Base Score:** 9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)
- Plugin Output:** Nessus determined the workaround was not applied based on the following information:
 - Fix it solution referenced in KB 2488013 is not applied.
 - Microsoft Enhanced Mitigation Experience Toolkit (EMET) is not installed.
- CVE:** CVE-2010-3971
- BID:** 45246
- Xref:** OSVDB:69796, CERT:634956, EDB-ID:15708, EDB-ID:15746, Secunia:42510
- Vulnerability Publication Date:** 2010/12/08
- Plugin Publication Date:** 2011/01/20
- Plugin Last Modification Date:** 2011/02/09
- Public Exploit Available:** True
- Exploitable With:** Metasploit (Internet Explorer CSS Recursive Import Use After Free)

At the bottom of the interface, there is a horizontal bar with a red indicator, likely representing a risk or severity level.

En la disponibilidad de las vulnerabilidades de seguridad se mostrarán las vulnerabilidades de seguridad conocidas y públicas, incluidas las encontradas en marcos de trabajo de vulnerabilidades (públicos o comerciales), tales como CANVAS, CORE o Metasploit.

La pantalla de detalles de vulnerabilidades brinda varios métodos para navegar por el informe:

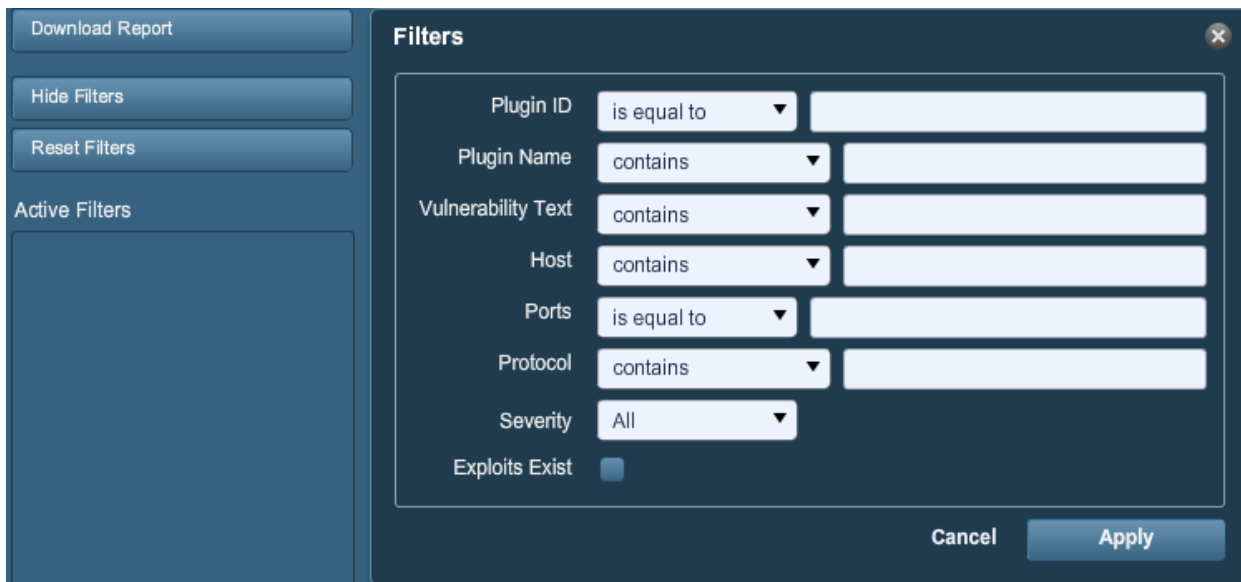
- Se pueden seleccionar las teclas de flechas de la parte superior para retroceder a la descripción general de un análisis, un puerto o un host.

- > Los botones "List" y "Detail" alternan entre el detalle de las vulnerabilidades y la última vista de lista (en el ejemplo anterior, las vulnerabilidades relacionadas con el puerto 445).
- > Las flechas grises hacia la izquierda o la derecha recorrerán las otras vulnerabilidades relacionadas con el puerto seleccionado.
- > La barra de botones de la parte inferior proporciona una forma de saltar a una vulnerabilidad particular de la lista, de acuerdo con la gravedad del riesgo. En el ejemplo anterior se destacan las vulnerabilidades de riesgo medio y alto.


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, comience por hacer clic en "Show Filters" a la izquierda de la pantalla. Los filtros se pueden crear a partir de las pantallas de detalle de nivel de puerto o host, o resumen de informes.



Para crear un filtro se selecciona el campo, un argumento de filtro y un valor respecto al cual filtrar:



permiten una amplia variedad de criterios:

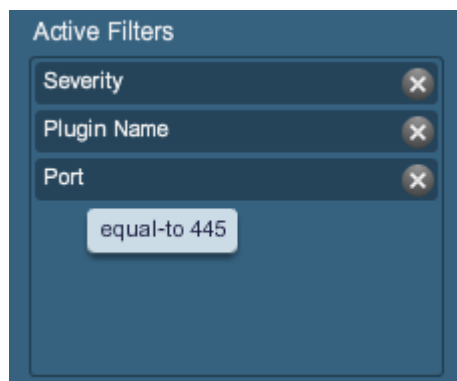
Opción	Descripción
Plugin ID	Filtra los resultados si la identificación del plugin es igual a ("is equal to") o no es igual a ("is not equal to") un número específico (por ejemplo, 42111).
Plugin Name	Filtra los resultados si el nombre del plugin contiene ("contains"), no contiene ("does not contain"), comienza con ("starts with") o no comienza con ("does not start with") una cadena específica (por ejemplo, "Microsoft Windows").
Vulnerability Text	Filtra los resultados si la salida del plugin contiene ("contains"), no contiene ("does not contain"), comienza con ("starts with") o no comienza con ("does not start with") una cadena específica (por ejemplo, "denial of service" [denegación de servicio]).
Host	Filtra los resultados si el host contiene ("contains"), no contiene ("does not contain"), comienza con ("starts with"), no comienza con ("does not start with"), es igual a ("is equal to") o no es igual a ("is not equal to") una cadena específica (por ejemplo, 192.168).
Ports	Filtra los resultados si un puerto es igual a ("is equal to") o no es igual a ("is not equal to") un número específico (por ejemplo, 443).
Protocol	Filtra los resultados si el protocolo contiene ("contains"), no contiene ("does not contain"), comienza con ("starts with") o no comienza con ("does not start with") una cadena específica (por ejemplo, http).
Severity	<p>Filtra los resultados de acuerdo con la gravedad del riesgo: baja ("Low"), media ("Medium"), alta ("High") o crítica ("Critical").</p> <div>  <p>Las clasificaciones de gravedad derivan del puntaje CVSS asociado, en el que menos de 5 es "baja", menos de 7 es "media", menos de 10 es "alta" y un puntaje CVSS de 10 se marcará como "crítico".</p> </div>
Exploits Exist	Filtra en función de la vulnerabilidad de seguridad pública conocida.

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", seleccionar "is equal to" 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.

A medida que se crean filtros, aparecerán en la lista de la izquierda. Para ver los detalles de los filtros activos, desplace el puntero del mouse sobre el nombre del filtro:



Apenas se cree un filtro, se actualizarán los resultados del análisis para que reflejen los nuevos criterios de filtro. En el ejemplo a continuación, si se crea un filtro que solo muestre resultados que tengan "Microsoft" en el nombre del plugin, se eliminarán la mayoría de los resultados:

LAN Scan

4 results

Host	Total	High	Medium	Low	Open Port
192.168.0.1	17	0	1	14	2
192.168.0.10	29	1	1	24	3
192.168.0.20	29	1	1	24	3
192.168.0.100	18	0	2	14	2

Filters

Plugin ID

is equal to

Plugin Name

contains

microsoft

Vulnerability Text

contains

Host

contains

Ports

is equal to

Protocol

contains

Severity

All

Cancel

Apply

Después de aplicar el filtro:

[illegible]

Una vez que se filtraron los resultados para que brinden el conjunto de datos que desea, puede hacer clic en **"Download Report"** para exportar únicamente los resultados filtrados.

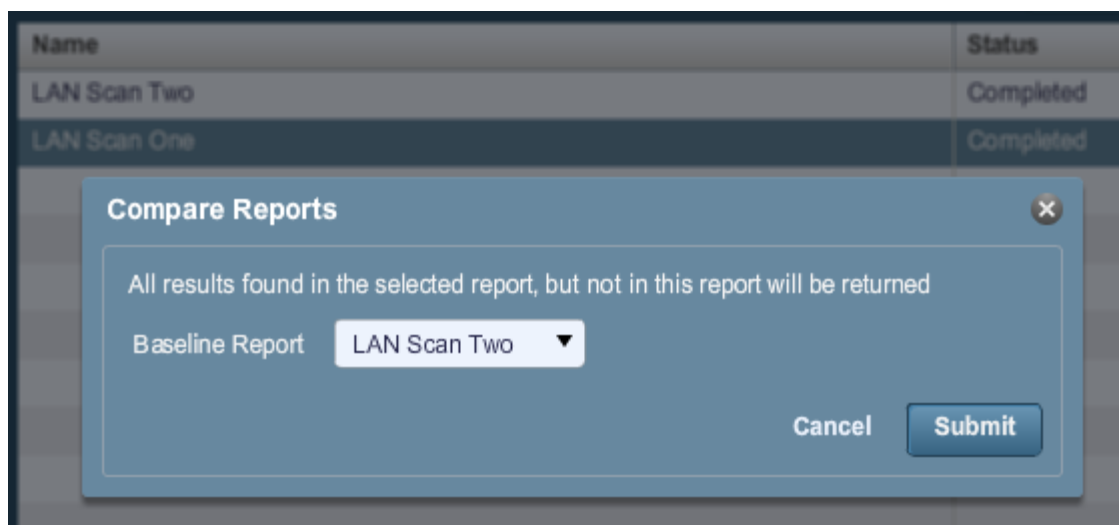
Comparar



La función "Compare" solo está disponible para los usuarios de ProfessionalFeed.

Con Nessus 4.4, usted puede comparar dos informes de análisis entre sí para visualizar las diferencias. 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 los informes, comience por seleccionar un análisis de la lista **"Reports"** y haga clic en **"Compare"** desde la barra de menús de la derecha. El menú de diálogo resultante le brindará una lista desplegable de los demás informes que se compararán. Seleccione uno y haga clic en **"Submit"**:



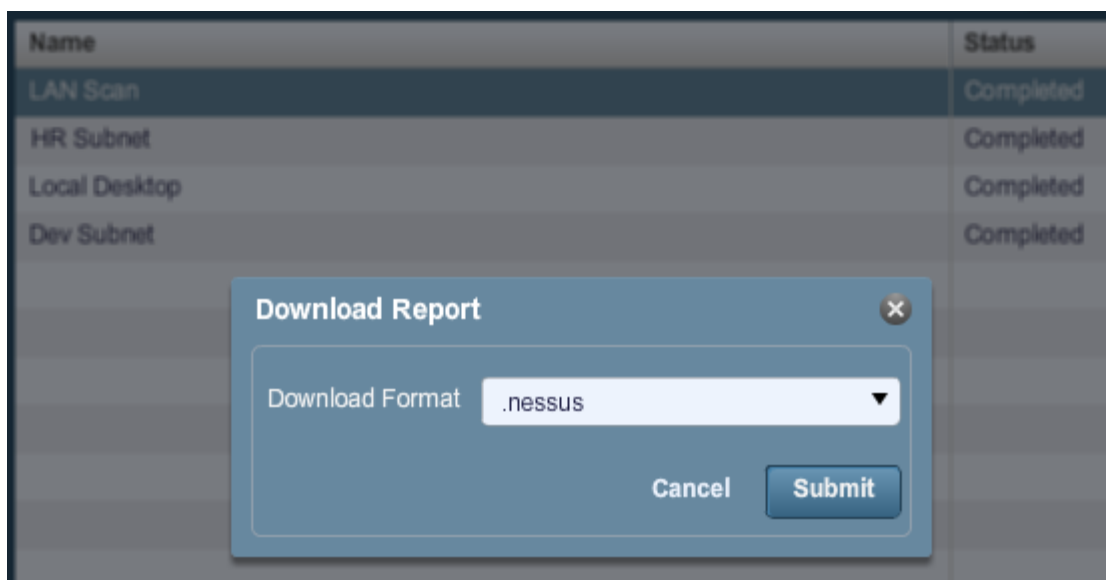
Nessus comparará los dos informes y producirá una lista de resultados que no se encuentran en ambos informes. Estos resultados constituyen el diferencial de análisis, y destacan qué vulnerabilidades se encontraron y se solucionaron entre los dos análisis. En el ejemplo anterior, "LAN Scan One" es un análisis de toda la subred 192.168.0.0/24 y "LAN Scan Two" es un análisis de tres hosts seleccionados de la subred 192.168.0.0/24. La característica "Compare" muestra las diferencias, y se destacan los hosts que no se analizaron en "LAN Scan Two":

Report Info		Comparison Report					2 results
New Report Name: LAN Scan One Last Update: Nov 12, 2009 22:57 Baseline Report Name: LAN Scan Two Last Update: Nov 12, 2009 23:05		Host	Total	High	Medium	Low	Open Port
		192.168.0.2	43	0	1	31	11
		192.168.0.100	19	0	2	15	2

Carga y descarga

Los resultados de análisis se pueden exportar desde un analizador e importarse en uno diferente. Las características **"Upload"** y **"Download"** 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 seleccionarlo de la pantalla **"Reports"** y haga clic en **"Download"**. De esta forma, aparecerá el cuadro de diálogo de descarga de informes:



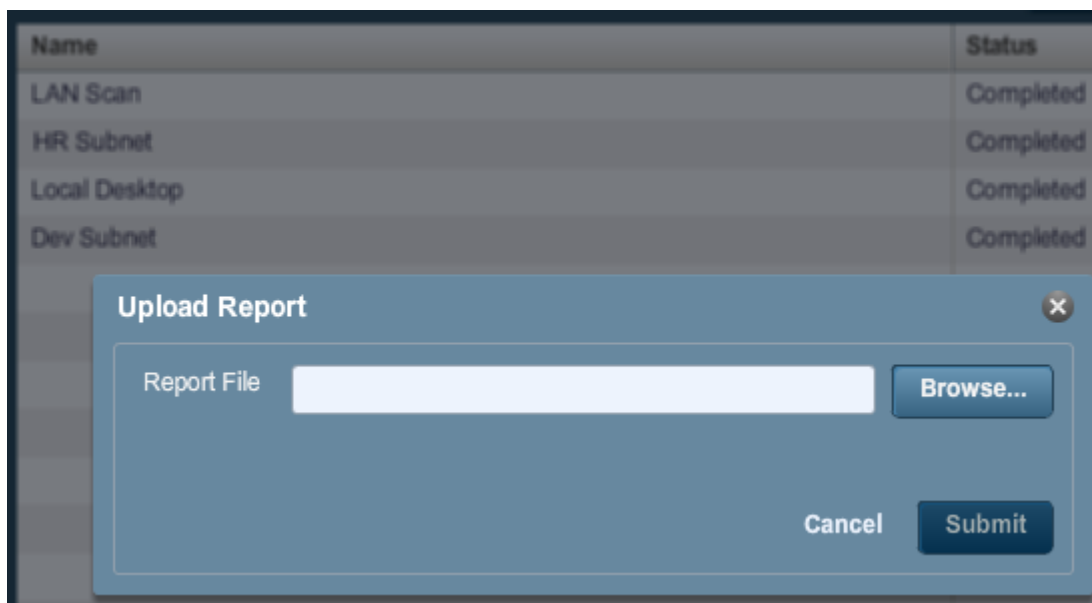
Los informes se pueden descargar en cualquiera de estos cuatro formatos:

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.
.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.
Detailed HTML Report (by finding)	Informe generado mediante HTML estándar que se puede visualizar en cualquier explorador web, detallado por vulnerabilidad (Nessus Plugin ID).
Detailed RTF Report (by finding)	Informe generado mediante la vista de formato de texto enriquecido (Rich Text Format, RTF).
Executive HTML export (top 10 most vulnerable hosts)	Informe generado mediante HTML estándar que solo incluye los 10 hosts con la mayor cantidad de vulnerabilidades.
HTML export	Informe generado mediante HTML estándar, detallado por host.
NBE export	Exportación basada en delimitadores de barras verticales que se puede usar para ser importada en muchos programas externos.

Después de seleccionar el formato **.nessus** o NBE, aparecerá el cuadro de diálogo estándar "Save File" de su explorador web, que le permitirá guardar los resultados del análisis en la

ubicación que elija. Los informes HTML se podrán ver en su explorador, y guardar a través de la función "File -> Save" de este.

Para importar un análisis, haga clic en el botón **"Upload"** de la pantalla **"Reports"**:



Mediante el botón **"Browse..."**, seleccione el archivo de análisis **.nessus** que desee importar y haga clic en **"Submit"**. Nessus analizará sintácticamente la información y la pondrá a su disposición a través de la interfaz **"Reports"**.

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 **"Download"** de la ficha **"Reports"**. Consulte el documento "Nessus File Format" (Formato de archivos Nessus) para obtener más detalles sobre los archivos **.nessus**.

Eliminar

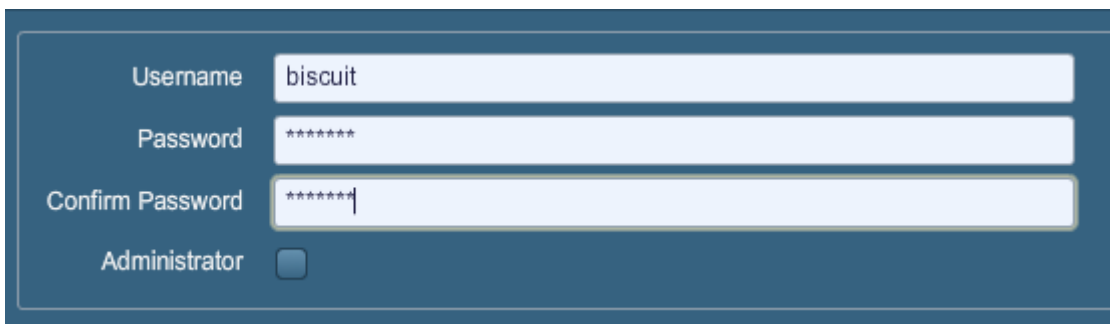
Una vez que haya terminado de usar los resultados del análisis, puede seleccionar un análisis de la lista **"Reports"** y hacer clic en el botón **"Delete"**. Esto eliminará el análisis de la interfaz de usuario. **No se puede deshacer esta acción.** Use la característica **"Download"** para exportar los resultados de su análisis antes de eliminarlo.

USUARIOS



Name	Username	Role	Last Login
admin	admin	Administrator	Nov 20, 2009 24:49
figlet	figlet	User	Never Logged In

La ficha **"Users"** brinda una interfaz para la administración de los usuarios del analizador Nessus. Se pueden añadir nuevos usuarios mediante Nessus Server Manager (Mac OS X/Windows), el comando `nessus-adduser` (*nix) o la interfaz de usuario (todas las plataformas). Para crear un nuevo usuario mediante la interfaz de usuario de Nessus, haga clic en **"Add"** en el menú situado en la esquina superior derecha. Luego se le pedirá su nombre de usuario, contraseña y la opción para hacer que el usuario sea administrador del analizador Nessus:



Para modificar o eliminar un usuario, seleccione el nombre de usuario de la lista **"Users"** y haga clic en **"Edit"** o **"Delete"** en el menú situado en la esquina superior derecha, según sea necesario.

OTROS CLIENTES DE NESSUS

Además de la GUI de Nessus, Tenable admite otros dos métodos para comunicarse con el servidor Nessus: la interfaz de líneas de comandos y SecurityCenter.

INTERFAZ DE LÍNEAS DE COMANDOS

La Interfaz de líneas de comandos (CLI) se encuentra disponible en el servidor Nessus. Para ejecutar un análisis mediante una operación de línea de comandos, se debe hacer en modo por lotes y con la siguiente sintaxis de comandos:

Sistema operativo	Comando
Linux, Solaris, Enterasys	# /opt/nessus/bin/nessus -q [-pPS] <host> <port> <user> <password> <targets-file> <result-file>

FreeBSD	# /usr/local/nessus/bin/nessus -q [-pPS] <host> <port> <user> <password> <targets-file> <result-file>
Mac OS X	# /Library/Nessus/run/bin/nessus -q [-pPS] <host> <port> <user> <password> <targets-file> <result-file>
Windows	%programfiles%\Tenable\Nessus\nessus -q [-pPS] <host> <port> <user> <password> <targets-file> <result-file>

La tabla a continuación explica los distintos argumentos que se usarán para ejecutar un análisis en modo por lotes.

Argumento	Descripción
-q	Modo por lotes. Ejecuta el análisis de Nessus de forma no interactiva.
-p	Obtiene una lista de los plugins instalados en el servidor.
-P	Obtiene una lista de las preferencias del servidor y los plugins.
-S	Genera resultados SQL para -p y -P.
<host>	El host nessusd al que se conectará.
<port>	El puerto al que usted se conectará en el host nessusd remoto.
<user>	El nombre de usuario con el que se conectará a nessusd .
<password>	La contraseña relacionada con el nombre de usuario.
<targets-file>	El nombre del archivo que contiene los equipos de destino que se analizarán.
<results-file>	El nombre del archivo en el que se almacenarán los resultados cuando finalice el análisis.

Existen otras opciones que también están disponibles al ejecutar un análisis en modo por lotes. Estas se explican en la siguiente tabla.

Opción	Descripción
-v	Hace que el modo por lotes muestre mensajes de estado en pantalla.

-x	No verifica los certificados SSL.
-v	Versión. Muestra el número de la versión y cierra.
-h	Ayuda. Muestra un resumen de los comandos y cierra.
-T <type>	Guarda los datos como <type>, donde <type> puede ser "nbe", "html", "nessus" o "text".

Conversión de un informe

Usted puede usar Nessus para efectuar una conversión entre formatos de informes. Nessus puede tomar cualquier informe NBE y transformarlo en formato de texto, HTML o **.nessus**.

Para convertir un informe, use el siguiente comando:

Sistema operativo	Comando
Linux, Solaris, Enterasys	# /opt/nessus/bin/nessus -i in.nbe -o out. [html txt nessus]
FreeBSD	# /usr/local/nessus/bin/nessus -i in.nbe -o out. [html txt nessus]
Mac OS X	# /Library/Nessus/run/bin/nessus -i in.nbe -o out. [html txt nessus]
Windows	%programfiles%\Tenable\Nessus\nessus -i in.nbe -o out. [html txt nessus]

La opción **-i** especifica el archivo NBE que se está convirtiendo. La opción **-o** especifica el nombre y el tipo del archivo en el que se convertirá el informe, que puede ser formato de texto, HTML o **.nessus**.

Los informes contenidos en archivos **.nessus** también se pueden convertir en HTML desde la línea de comandos. La sintaxis para lo anterior es la siguiente:



El archivo **.nessus** debe guardarse mediante el formato de descarga "nessus (v1)" para que funcione la conversión en HTML.

Sistema operativo	Comando
Linux, Solaris, Enterasys	# /opt/nessus/bin/nessus --dot-nessus in.nessus -i <ReportName> -o out.html
FreeBSD	# /usr/local/nessus/bin/nessus --dot-nessus in.nessus -i <ReportName> -o out.html
Mac OS X	# /Library/Nessus/run/bin/nessus --dot-nessus in.nessus -i <ReportName> -o out.html

Windows	<code>%programfiles%\Tenable\Nessus\nessus --dot-nessus in.nessus -i <ReportName> -o out.html</code>
----------------	--

El parámetro `--dot-nessus` indica el archivo de entrada `.nessus` que se usará. `<ReportName>` es el nombre del informe como aparece dentro del archivo de entrada `.nessus`.

Línea de comandos que utiliza archivos .nessus

Existen varios argumentos que se pueden pasar para poder trabajar con archivos `.nessus` como entrada o salida desde la línea de comandos. Estos se detallan en la siguiente tabla:

Argumento	Descripción
<code>--dot-nessus <file></code>	Al usar esta opción, siempre se proporciona como primer parámetro pasado al binario <code>nessus</code> para indicar que se usará un archivo <code>.nessus</code> . <code><file></code> es la ubicación y el nombre del archivo <code>.nessus</code> que se usará.
<code>--policy-name <policy></code>	El nombre de la directiva contenida en el archivo <code>.nessus</code> designado. El parámetro de la directiva se proporciona al iniciar un análisis desde la línea de comandos. Tenga en cuenta que el nombre de la directiva proporcionado debe ser el nombre exacto e incluir comillas simples, de la misma manera que aparece en pantalla cuando se usa el parámetro <code>--list-policies</code> (ver a continuación).
<code>--list-policies</code>	Proporciona los nombres de todas las directivas de análisis contenidas en el archivo <code>.nessus</code> designado.
<code>--list-reports</code>	Proporciona los nombres de todos los informes contenidos en el archivo <code>.nessus</code> designado.
<code>--target-file <file></code>	Anula los destinos proporcionados en el archivo <code>.nessus</code> designado y usa aquellos contenidos en el archivo especificado.

El siguiente comando mostrará una lista de todos los informes contenidos en el archivo `"scan.nessus"`:



El archivo `.nessus` se debe guardar con el formato de descarga `"nessus (v1)"` para que funcione el cambio `--list-reports`.

Sistema operativo	Comando
Linux, Solaris, Enterasys	<code># /opt/nessus/bin/nessus --dot-nessus scan.nessus --list-reports</code>
FreeBSD	<code># /usr/local/nessus/bin/nessus --dot-nessus scan.nessus --list-reports</code>

Mac OS X	<code># /Library/Nessus/run/bin/nessus --dot-nessus scan.nessus --list-reports</code>
Windows	<code>%programfiles%\Tenable\Nessus\nessus --dot-nessus scan.nessus --list-reports</code>

A continuación, se muestra un ejemplo de resultados generados:

```
List of reports contained in scan.nessus:
- '08/03/10 11:19:55 AM - Full Safe w/ Compliance'
- '08/03/10 01:01:01 PM - Full Safe w/ Compliance'
- '08/03/10 01:32:10 PM - Full Safe w/ Compliance'
- '08/03/10 02:13:01 PM - Full Safe w/ Compliance'
- '08/03/10 02:45:00 PM - Full Safe w/ Compliance'
```

El siguiente comando mostrará una lista de todas las directivas contenidas en el archivo "scan.nessus":



El archivo .nessus se debe guardar con el formato de descarga "nessus (v1)" para que funcione el cambio `--list-policies`.

Sistema operativo	Comando
Linux, Solaris, Enterasys	<code># /opt/nessus/bin/nessus --dot-nessus scan.nessus --list-policies</code>
FreeBSD	<code># /usr/local/nessus/bin/nessus --dot-nessus scan.nessus --list-policies</code>
Mac OS X	<code># /Library/Nessus/run/bin/nessus --dot-nessus scan.nessus --list-policies</code>
Windows	<code>%programfiles%\Tenable\Nessus\nessus --dot-nessus scan.nessus --list-policies</code>

A continuación se muestra un ejemplo de los resultados de este comando:

```
List of policies contained in scan.nessus:
- 'Full Safe w/ Compliance'
```

Tenga en cuenta que cuando se pasen los nombres de los informes y las directivas como parámetros a Nessus en modo de línea de comandos, el nombre se debe pasar exactamente como aparece en pantalla desde los comandos anteriores, e incluir las comillas simples ('Safe w/ Compliance').

Comando de análisis

Suponiendo que existe la directiva indicada en el ejemplo anterior, se puede iniciar un análisis con la siguiente configuración:



El archivo `.nessus` especificado en el análisis debe estar en formato "nessus (v1)" para que este lo procese.

Sistema operativo	Comando
Linux, Solaris, Enterasys	<pre># /opt/nessus/bin/nessus --dot-nessus scan.nessus --policy-name 'Full Safe w/ Compliance' <host> <port> <user> <password> <results-file></pre>
FreeBSD	<pre># /usr/local/nessus/bin/nessus --dot-nessus scan.nessus --policy-name 'Full Safe w/ Compliance' <host> <port> <user> <password> <results-file></pre>
Mac OS X	<pre># /Library/Nessus/run/bin/nessus --dot-nessus scan.nessus --policy-name 'Full Safe w/ Compliance' <host> <port> <user> <password> <results-file></pre>
Windows	<pre>%programfiles%\Tenable\Nessus\nessus --dot-nessus scan.nessus --policy-name "Full Safe w/Compliance" <host> <port> <user> <password> <results-file></pre>

En el ejemplo anterior, los parámetros `<host>`, `<port>`, `<user>`, `<password>` y `<results-file>` se proporcionan como se documentó anteriormente. La opción `<targets-file>` no es necesaria, ya que para el análisis se usarán los destinos contenidos en el archivo `.nessus`.

El formato correspondiente al informe que se generará se determinará en función de la extensión del archivo proporcionado en el comando `nessus`. En la línea de comandos, si el nombre proporcionado para el parámetro `<results-file>` fue `"report.nbe"`, el informe estará en formato `.nbe`. Si el nombre hubiera sido `"report.nessus"`, el informe hubiese tenido formato `.nessus`.

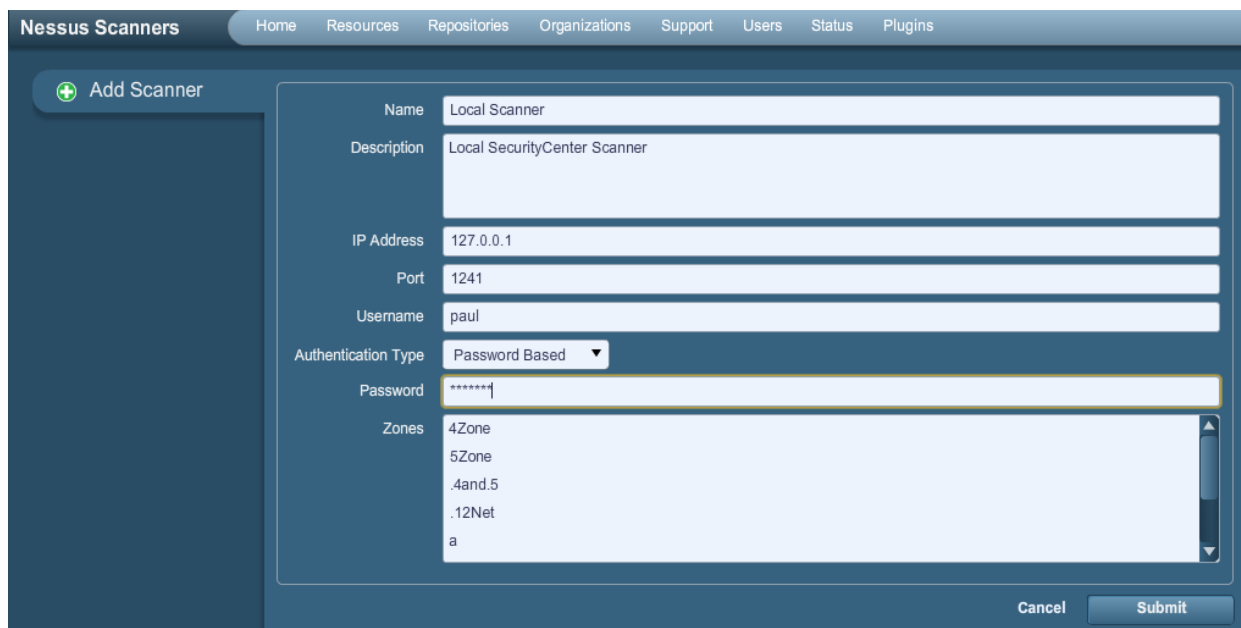
Si el parámetro `<results-file>` hubiera estado vacío, el informe se hubiese añadido al archivo `scan.nessus`.

SECURITYCENTER

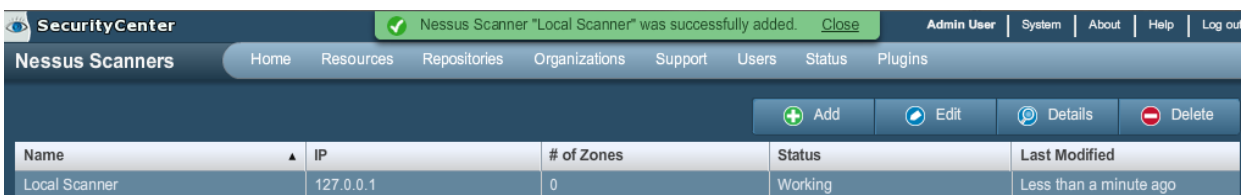
Configuración de SecurityCenter

Se puede añadir un servidor "Nessus Server" mediante la interfaz de administración de SecurityCenter. Con ella, SecurityCenter se puede configurar para obtener acceso y controlar prácticamente cualquier analizador Nessus. Haga clic en la ficha "Resources", y luego en **"Nessus Scanners"**. Haga clic en **"Add"** para abrir el cuadro de diálogo "Add Scanner". Son obligatorios 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". 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" de SecurityCenter:



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



Name	IP	# of Zones	Status	Last Modified
Local Scanner	127.0.0.1	0	Working	Less than a minute ago

Para obtener más información, consulte la "Guía de administración de SecurityCenter".

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 un 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

No dude en comunicarse con nosotros 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 red y la compatibilidad con FDCC, FISMA, SANS CAG 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 en forma proactiva el riesgo de las redes. Para obtener más información, visite <http://www.tenable.com/>.

Tenable Network Security, Inc.
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046 - EE. UU.
410.872.0555
www.tenable.com