Comprobaciones con credenciales Nessus para Unix y Windows

17 de enero de 2014

(Revisión 32)

Índice

Introducción

Este documento describe cómo realizar análisis de red autenticados con el analizador de vulnerabilidades **Nessus** de Tenable Network Security. Los análisis de red autenticados permiten que una auditoría de red remota obtenga datos "basados en host", tales como configuraciones de sistemas operativos y revisiones faltantes. Envíe sus comentarios o sugerencias por correo electrónico a support@tenable.com.

Nessus aprovecha la capacidad de iniciar sesión en hosts de Unix remotos a través del protocolo Shell seguro (SSH). Para hosts de Windows, Nessus usa una variedad de tecnologías de autenticación de Microsoft.

Tenga en cuenta que Nessus también usa el Protocolo simple de administración de redes (SNMP) para realizar consultas sobre información y versiones a enrutadores y conmutadores. Si bien este es un tipo de "comprobaciones locales", no se menciona en este documento.

Este documento hace amplia referencia a "Nessus", pero los conceptos básicos también son válidos para SecurityCenter de Tenable.

Estándares y convenciones

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`**. Los ejemplos de líneas de comandos pueden incluir o no el indicador de la línea de comandos y el texto de salida de los resultados del comando. Los ejemplos de líneas de comandos mostrarán el comando ejecutado en **`courier negrita`** para indicar lo que el usuario escribió, mientras que el resultado de muestra generado por el sistema se indicará en `courier` (normal). Este es un ejemplo de ejecución del comando **`pwd`** de Unix:

```
# pwd
/home/test/
#
```

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 las comprobaciones con credenciales de Nessus

El analizador Nessus de Tenable es un eficaz analizador de vulnerabilidades de red con una amplia base de datos de plugins (complementos), que comprueban una amplia variedad de vulnerabilidades que podrían explotarse de forma remota. Además del análisis remoto, el analizador Nessus también puede usarse para detectar exposiciones locales.

Objetivo

El análisis externo de vulnerabilidades de redes es útil para obtener una instantánea temporal de los servicios de red ofrecidos y de las vulnerabilidades que pueden contener. Sin embargo, solo se trata de una perspectiva externa. Es importante determinar qué servicios locales se encuentran en ejecución, e identificar exposiciones de seguridad a ataques locales u opciones de configuración que podrían exponer el sistema a ataques externos que tal vez no sean detectados por un análisis externo.

En una evaluación de vulnerabilidades de red común, se realiza un análisis remoto de los puntos de presencia externos y se realiza un análisis in situ dentro de la red. Ninguno de estos análisis puede determinar las exposiciones locales en el sistema de destino. Parte de la información obtenida se basa en la información de banner mostrada, la cual puede ser no concluyente o incorrecta. Mediante el uso de credenciales seguras, es posible que el analizador Nessus obtenga acceso

local para analizar el sistema de destino sin necesidad de un agente. Esto puede facilitar el análisis de una red muy grande, para determinar las exposiciones locales o las infracciones de compatibilidad.

El problema de seguridad más común de una organización es que las revisiones de seguridad no se apliquen en el momento apropiado. Los análisis con credenciales de Nessus pueden determinar rápidamente cuáles sistemas tienen instalaciones de revisión desactualizadas. Esto tiene una especial importancia cuando se hace pública una nueva vulnerabilidad y la gerencia ejecutiva desea una respuesta rápida sobre el efecto que puede tener en la organización.

Otro aspecto importante para las organizaciones es determinar la compatibilidad con las directivas del sitio, las normas de la industria (tales como los criterios de referencia del Center for Internet Security [CIS]) o la legislación (tal como Sarbanes-Oxley [SOX], Gramm-Leach-Bliley [GLBA] o HIPAA). Las organizaciones que aceptan información de tarjetas de crédito deben demostrar la compatibilidad con los Estándares de seguridad de datos de la industria de tarjetas de pago (Payment Card Industry Data Security Standards, PCI DSS). Hubo bastantes casos, sumamente difundidos, en los que quedó expuesta la información de tarjetas de crédito de millones de clientes. Esto representa una pérdida financiera significativa para los bancos responsables de restituir pagos, y cuantiosas multas o pérdida de la capacidad de aceptación de tarjetas de crédito por parte del procesador o el comerciante perjudicado.

Nivel de acceso

Los análisis con credenciales pueden realizar cualquier operación que pueda hacer un usuario local. El nivel de análisis depende de los privilegios que se le hayan otorgado a la cuenta de usuario que Nessus está configurado para usar.

Los usuarios que no tienen privilegios pero que cuentan con acceso local en los sistemas de Unix pueden determinar problemas de seguridad básicos, tales como entradas y niveles de revisión, en el archivo **`/etc/passwd`**. Para obtener información más detallada, como datos de configuración del sistema o permisos de archivos para todo el sistema, se requiere una cuenta con privilegios “root” (raíz).

Los análisis con credenciales en los sistemas de Windows requieren que se use una cuenta de administrador. Varias actualizaciones de software y boletines de Microsoft han provocado que la lectura del registro para determinar el nivel de revisión de software no sea confiable sin los privilegios de administrador. Es necesario contar con acceso administrativo para realizar una lectura directa del sistema de archivos. Esto permite que Nessus se instale en un equipo y realice un análisis de archivos directo para determinar el verdadero nivel de revisión de los sistemas que se encuentran en evaluación. En Windows XP Pro, el acceso a este archivo solo funcionará con una cuenta de administrador local si la directiva “Network access: Sharing and security model for local accounts” (Acceso a la red: modelo de seguridad y uso compartido para cuentas locales) se cambia a “Classic – local users authenticate as themselves” (Clásico: los usuarios locales se autentican como tales).

Una auditoría, para compatibilidad con SCAP, requiere enviar un ejecutable al host remoto. En los sistemas que ejecutan software de seguridad (por ejemplo, McAfee Host Intrusion Prevention), este puede bloquear o poner en cuarentena el ejecutable necesario para la auditoría. En estos sistemas, se debe hacer una excepción para el host o el ejecutable enviado.

Tecnologías usadas

El desafío de realizar un análisis con credenciales consiste en lograr que la provisión de las credenciales privilegiadas al analizador se haga automáticamente y de una forma segura. Se frustraría definitivamente el objetivo de detectar exposiciones de seguridad si al hacerlo se produjera una exposición aún mayor. Nessus admite el uso de varios métodos seguros para resolver este problema, tanto en plataformas de Unix como de Windows.

Sistemas de Unix

En los sistemas de Unix, Nessus usa programas basados en la versión 2 del protocolo Shell seguro (SSH) (por ejemplo, OpenSSH, Solaris SSH, etc.) para las comprobaciones basadas en hosts. Este mecanismo permite cifrar los datos que se encuentran en tránsito para impedir que los detecten los programas husmeadores detectores de paquetes (“sniffers”). Nessus es compatible con tres tipos de métodos de autenticación para usar con SSH: nombre de usuario y contraseña, claves públicas/privadas y Kerberos.

Nombre de usuario y contraseña
Si bien lo admite, Tenable no recomienda el uso de un nombre de usuario y contraseña para la autenticación con SSH. Las contraseñas estáticas están sujetas a ataques de tipo “Man in the middle” (intermediarios) y por fuerza bruta cuando se han usado durante un período prolongado.

Claves públicas/privadas
El cifrado de clave pública, también conocido como cifrado de clave asimétrica, brinda un mecanismo de autenticación más seguro mediante el uso de un par de claves, una pública y otra privada. En la criptografía asimétrica, la clave pública se usa para cifrar datos y la clave privada se usa para descifrarlos. El uso de claves pública y privada es una forma más segura y flexible para la autenticación de SSH. Nessus admite los formatos de clave DSA y RSA.

Kerberos
Kerberos, desarrollado por Project Athena del MIT, es una aplicación de cliente/servidor que usa un protocolo de cifrado de clave simétrica. En el cifrado simétrico, la clave que se usa para cifrar los datos es igual a la clave que se usa para descifrar los datos. Las organizaciones usan un Centro de distribución de claves (Key Distribution Center, KDC) que contiene todos los usuarios y los servicios que requieren autenticación de Kerberos. Los usuarios obtienen autenticación de Kerberos al solicitar un ticket de concesión de tickets (Ticket Granting Ticket, TGT). Cuando a un usuario se le concede un TGT, puede usarlo para solicitar tickets de servicio desde el KDC y así poder utilizar otros servicios basados en Kerberos. Kerberos usa el protocolo de cifrado DES (Data Encryption Standard) (Estándar de cifrado de datos) en modo CBC (Cipher Block Chain) (Encadenamiento de bloques de cifrado) para cifrar todas las comunicaciones.

La implementación de Nessus de la autenticación Kerberos para SSH admite los algoritmos de cifrado “aes-cbc” y “aes-ctr”. A continuación se presenta una descripción general del modo en que Nessus interactúa con Kerberos:

- El usuario final proporciona la IP del KDC
- **`nessusd`** le pregunta a **`sshd`** si admite la autenticación Kerberos
- **`sshd`** responde que sí
- **`nessusd`** solicita el TGT de Kerberos, junto con la identificación de inicio de sesión y la contraseña
- Kerberos le vuelve a enviar un ticket a **`nessusd`**
- **`nessusd`** le da el ticket a **`sshd`**
- **`nessusd`** inicia sesión

Sistemas de Windows
Nessus admite distintos métodos de autenticación para sistemas basados en Windows. Cada uno de estos métodos requiere un nombre de usuario, contraseña y nombre de dominio (a veces es opcional para la autenticación).

LANMAN
El método de autenticación Lanman se solía usar en Windows NT y en las primeras implementaciones de servidor de Windows 2000. En realidad, no se usa en las nuevas implementaciones de Windows, pero se lo conserva para fines de compatibilidad con versiones anteriores.

NTLM y NTLMv2
El método de autenticación NTLM, que apareció con Windows NT, proporcionó una mejora en la seguridad con respecto a la autenticación Lanman. Sin embargo, la versión mejorada NTLMv2 ofrece mayor seguridad criptográfica que NTLM, y es el método de autenticación predeterminado que elige Nessus al intentar iniciar sesión en un servidor de Windows.

Firma SMB
La firma SMB es una suma de comprobación criptográfica que se aplica a todo el tráfico SMB con destino a un servidor Windows y proveniente de este. Muchos administradores de sistema habilitan esta función en sus servidores para garantizar que los usuarios remotos estén completamente autenticados y pertenezcan a un dominio. Nessus la usa automáticamente si el servidor de Windows remoto lo requiere.

SPNEGO
El protocolo de negociación simple protegida (Simple and Protected Negotiate, SPNEGO) proporciona capacidad de inicio de sesión único (Single Sign On, SSO) desde un cliente de Windows a una variedad de recursos protegidos a través de las credenciales de inicio de sesión de Windows de los usuarios. Nessus admite el uso de SPNEGO con NTLMSSP con autenticación LMv2 o cifrado RC4 y Kerberos.

Kerberos
Nessus también admite el uso de la autenticación Kerberos en un dominio Windows. Para configurarla, se debe proporcionar la dirección IP de Kerberos Domain Controller (en realidad, la dirección IP de Servidor de Active Directory de Windows).

NTLMSSP (NT Lan Manager Security Support Provider) y LMv2
Si un esquema de seguridad ampliado (tales como Kerberos o SPNEGO) no es admitido o falla, Nessus intentará iniciar sesión a través de la autenticación NTLMSSP/LMv2. Si esta acción no da resultado, Nessus intentará iniciar sesión mediante la autenticación NTLM.

Nombres de usuario, contraseñas y dominios de Windows
El campo de dominio de SMB es opcional, y Nessus podrá iniciar sesión con las credenciales de dominio sin este campo. El nombre de usuario, la contraseña y el dominio opcional hacen referencia a una cuenta que el equipo de destino conoce. Por ejemplo, si se proporciona el nombre de usuario “joesmith” y la contraseña “`my4x4mpl3`”, un servidor de Windows primero busca este nombre de usuario en la lista de usuarios del sistema local, y luego determina si pertenece a un dominio de este.

El verdadero nombre de dominio solo es necesario si un nombre de cuenta que se encuentra en el dominio es distinto del que posee el equipo. Es perfectamente posible tener una cuenta de “Administrador” en un servidor de Windows y en el dominio. En este caso, para iniciar sesión en el servidor local, el nombre de usuario del “Administrador” se usa junto con la contraseña de esa cuenta. Para iniciar sesión en el dominio, también se usaría el nombre de usuario del “Administrador”, pero con la contraseña y el nombre del dominio.

Independientemente de las credenciales que se usen, Nessus siempre intenta iniciar sesión en un servidor de Windows con las siguientes combinaciones:

- “Administrador” sin contraseña
- Un nombre de usuario y contraseña aleatorios, para comprobar las cuentas de invitados
- Ningún nombre de usuario ni contraseña, para comprobar las sesiones nulas

Comprobaciones con credenciales en plataformas de Unix

El proceso descrito en esta sección le permite realizar comprobaciones de seguridad locales en los sistemas basados en Unix (como Linux, Solaris, Mac OS X). El demonio de SSH que se usa en este ejemplo es OpenSSH. Si cuenta con una variante comercial de SSH, es posible que su procedimiento sea ligeramente distinto.

Para habilitar las comprobaciones de seguridad locales se pueden usar dos métodos básicos:

1. Uso de un par de claves privada/pública de SSH
2. Credenciales de usuario y acceso a **`sudo`** o credenciales para acceso a **`su`**

Requisitos previos

Requisitos de configuración de SSH

Nessus 5 admite los algoritmos blowfish-CBC, AESXXX-CBC (AES128, AES192 y AES256), 3DES-CBC y AES-CTR.

Algunas variantes comerciales de SSH no admiten el algoritmo blowfish, posiblemente por motivos de exportación. También es posible configurar un servidor SSH para aceptar solo algunos tipos de cifrado. Compruebe su servidor SSH para asegurarse de que admita el algoritmo correcto.

Privilegios de usuario

Para lograr la máxima eficacia, el usuario de SSH debe tener la capacidad de ejecutar cualquier comando del sistema. En los sistemas de Unix, esto se conoce como privilegios "**root**" (raíz). Si bien es posible ejecutar algunas comprobaciones (tales como niveles de revisión) con el acceso sin privilegios, las comprobaciones de compatibilidad totales que auditan la configuración del sistema y los permisos de archivos requieren el acceso root (raíz). Por tal motivo, se recomienda enfáticamente que se usen las claves de SSH en lugar de las credenciales cuando sea posible.

Requisitos de configuración de Kerberos

Si se usa Kerberos, **sshd** debe configurarse con la compatibilidad de Kerberos para verificar el ticket con el KDC. Para que esto funcione, las búsquedas inversas de DNS deben configurarse correctamente. El método de interacción Kerberos debe ser **gssapi-with-mic**.

Habilitación de comprobaciones de seguridad locales de SSH en Unix

Esta sección tiene la finalidad de ofrecer un procedimiento de alto nivel para habilitar SSH entre los sistemas que están involucrados en las comprobaciones con credenciales de Nessus. No está destinada a cumplir la función de un tutorial detallado de SSH. Se supone que el lector cuenta con conocimientos previos de los comandos del sistema de Unix.

Generación de las claves pública y privada de SSH

El primer paso consiste en generar un par de claves privada/pública para que el analizador Nessus las use. Este par de claves puede generarse desde cualquiera de los sistemas de Unix, con cualquier cuenta de usuario. Sin embargo, es importante que las claves pertenezcan al usuario de Nessus definido.

Para generar el par de claves, use **ssh-keygen** y guarde la clave en un lugar seguro. En el siguiente ejemplo, las claves se generan en una instalación Red Hat ES 3.

```
# ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/Users/test/.ssh/id_dsa):
       /home/test/Nessus/ssh_key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in
/home/test/Nessus/ssh_key.
Your public key has been saved in
/home/test/Nessus/ssh_key.pub.
The key fingerprint is:
06:4a:fd:76:ee:0f:d4:e6:4b:74:84:9a:99:e6:12:ea
#
```

No transfiera la clave privada a ningún sistema que no sea el que ejecuta el servidor Nessus. Cuando **ssh-keygen** le solicite una frase de contraseña, introduzca una frase segura o bien presione dos veces la tecla "Return" (Intro) (es decir, no establezca ninguna frase de contraseña). Si se especifica una frase de contraseña, se la debe especificar en las opciones Policies (Directivas) -> Credentials (Credenciales) -> SSH settings (Configuración de SSH) a fin de que Nessus use la autenticación basada en claves.

Se sugiere que los usuarios de Nessus Windows copien las dos claves en el directorio de aplicación principal de Nessus que se encuentra en el sistema que ejecuta Nessus (**C:\Program Files\Tenable\Nessus,** de manera predeterminada), y luego copien la clave pública en los sistemas de destino según sea necesario. Esto facilita la administración de los archivos de las claves pública y privada.

Creación de una cuenta de usuario y configuración de la clave de SSH

En todo sistema de destino que se analizará con las comprobaciones de seguridad locales, cree una nueva cuenta de usuario dedicada a Nessus. Esta cuenta de usuario debe tener exactamente el mismo nombre en todos los sistemas. En este documento el usuario se denominará "nessus", pero es posible usar cualquier nombre.

Una vez que haya creado la cuenta para el usuario, asegúrese de que la cuenta no tenga ninguna contraseña válida establecida. En los sistemas Linux, las nuevas cuentas de usuario están bloqueadas de manera predeterminada, a menos que se haya establecido explícitamente una contraseña inicial. Si usa una cuenta para la que se había establecido una contraseña, use el comando "**passwd -l**" para bloquear la cuenta.

También debe crear, bajo el directorio principal de la nueva cuenta, el directorio para mantener la clave pública. A los fines de este ejercicio, el directorio será **/home/nessus/.ssh**. A continuación se presenta un ejemplo para los sistemas Linux:

```
# passwd -l nessus
# cd /home/nessus
# mkdir .ssh
#
```

Para los sistemas Solaris 10, Sun ha mejorado el comando "**passwd(1)**" para distinguir entre las cuentas bloqueadas y las cuentas sin inicio de sesión. La finalidad es garantizar que una cuenta de usuario que se haya bloqueado no pueda usarse para ejecutar comandos (por ejemplo, los trabajos cron). Las cuentas sin inicio de sesión solo se usan para ejecutar comandos, y no admiten una sesión de inicio interactiva. Estas cuentas tienen el token (símbolo) "NP" en el campo de contraseña de **/etc/shadow**. Para establecer una cuenta sin inicio de sesión y crear el directorio de clave pública de SSH en Solaris 10, ejecute los siguientes comandos:

```
# passwd -N nessus

# grep nessus /etc/shadow
nessus:NP:13579::::::
# cd /export/home/nessus
# mkdir .ssh
#
```

Ahora, una vez creada la cuenta de usuario, debe transferir la clave al sistema, colocarla en el directorio correspondiente y establecer los permisos correctos.

Ejemplo

Desde el sistema que contiene las claves, realice una copia segura de la clave pública en el sistema que se analizará para realizar comprobaciones de host, como se muestra a continuación. 192.1.1.44 es un sistema remoto de ejemplo que se probará con las comprobaciones en host.

```
# scp ssh_key.pub root@192.1.1.44:/home/nessus/.ssh/authorized_keys
#
```

También se puede copiar el archivo desde el sistema que tiene instalado Nessus con el comando FTP seguro, "**sftp**". Tenga en cuenta que el archivo del sistema de destino debe nombrarse "authorized_keys".

Vuelva al sistema que aloja la clave pública

Establezca los permisos del directorio **/home/nessus/.ssh** y del archivo **authorized_keys**.

```
# chown -R nessus:nessus ~nessus/.ssh/
# chmod 0600 ~nessus/.ssh/authorized_keys
# chmod 0700 ~nessus/.ssh/
#
```

Repita este proceso en todos los sistemas que se probarán para realizar comprobaciones de SSH (debe comenzar conforme a la sección anterior "Creación de una cuenta de usuario y configuración de la clave de SSH").

Realice una prueba para asegurarse de que las cuentas y las redes estén configuradas correctamente. Desde el analizador Nessus, use el comando simple de Unix "**id**" para ejecutar el siguiente comando:

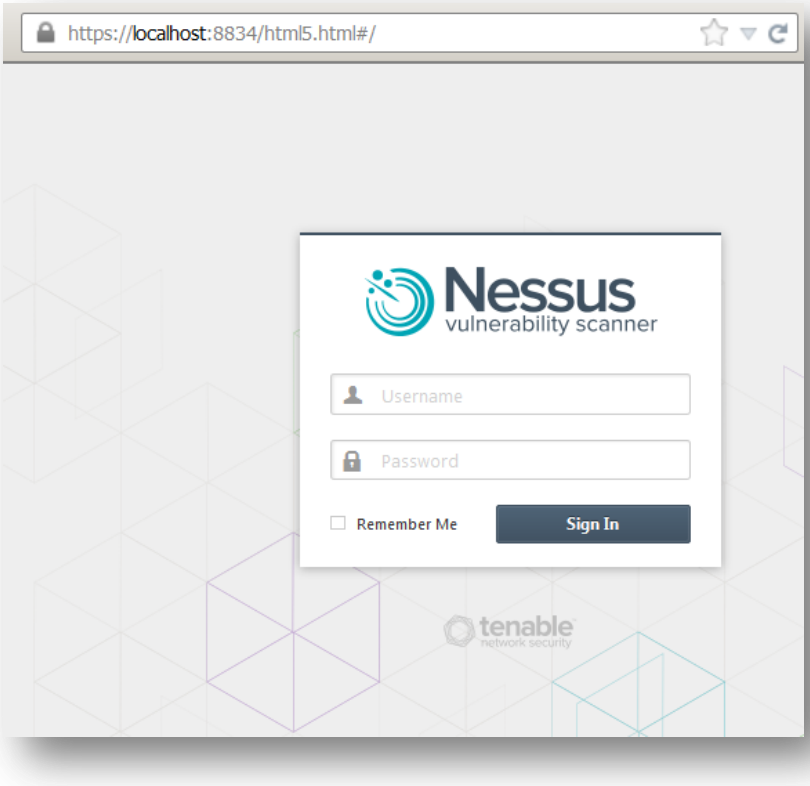
```
# ssh -i /home/test/nessus/ssh_key nessus@192.1.1.44 id
uid=252(nessus) gid=250(tns) groups=250(tns)
#
```

Si proporciona información sobre el usuario de nessus en forma correcta, significa que el intercambio de claves se realizó correctamente.

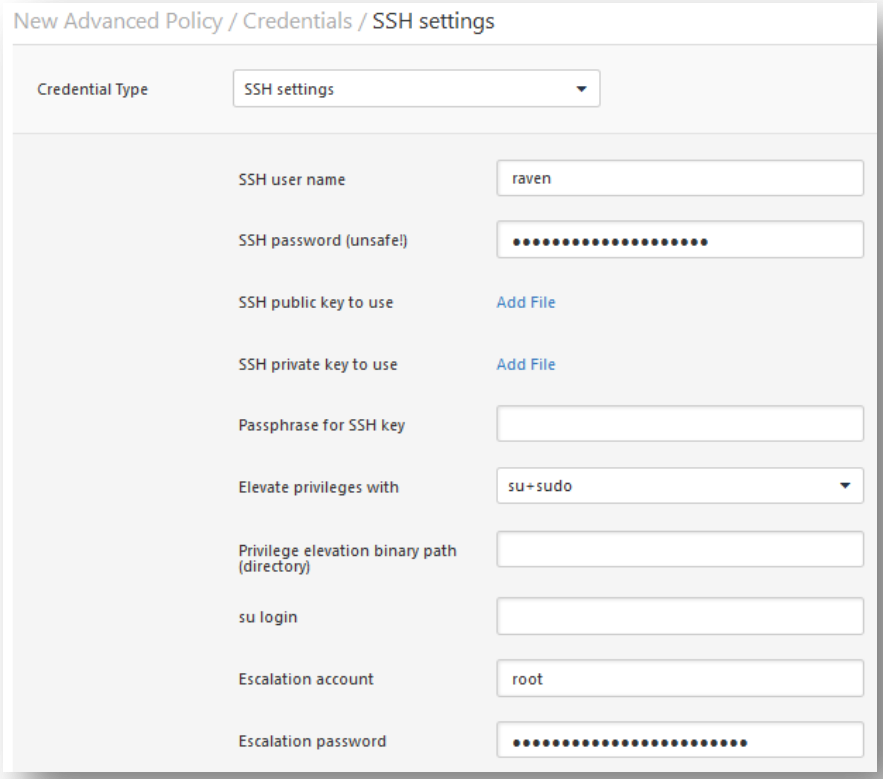
Configuración de Nessus para comprobaciones basadas en hosts de SSH

Interfaz de usuario de Nessus

Si aún no lo hizo, realice una copia segura de los archivos de las claves privada y pública en el sistema que usará para acceder al analizador Nessus.



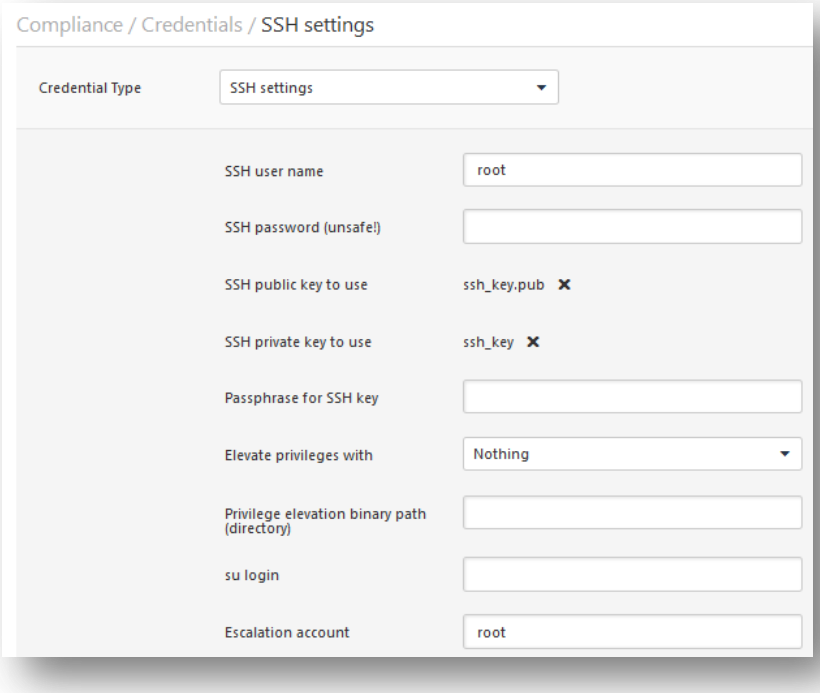
Abra un explorador web y conéctese a la interfaz de usuario del analizador Nessus, tal como se mostró anteriormente, y haga clic en la ficha "Policies" (Directivas). Cree una nueva directiva o modifique una directiva actual, y seleccione la ficha "Credentials" (Credenciales) que se encuentra a la izquierda. Seleccione "SSH settings" (Configuración de SSH) del menú desplegable que se encuentra en la parte superior, como se muestra a continuación:



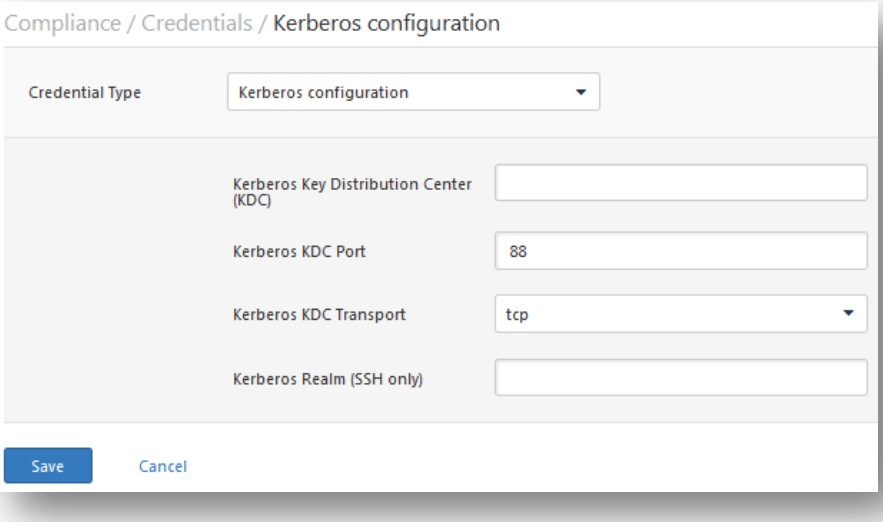
- Para el elemento “SSH user name” (Nombre de usuario de SSH), introduzca el nombre de la cuenta que está dedicada a Nessus en cada uno de los sistemas de destino de análisis. De manera predeterminada, se establece como “root”.
- Si usa una contraseña para SSH, introdúzcala en la casilla “SSH password” (Contraseña de SSH).
- Si usa las claves de SSH en lugar de una contraseña (recomendado), haga clic en el botón “Select” (Seleccionar) que se encuentra junto a la casilla denominada “SSH public key to use” (Clave pública de SSH a usar) y busque el archivo de clave pública en el sistema local.
- Para el elemento “SSH private key to use”(Clave privada de SSH a usar), haga clic en el botón “Select” (Seleccionar) y busque el archivo de clave privada (que está asociado con la clave pública anterior) en el sistema local.
- Si usa una frase de contraseña para la clave de SSH (opcional), introdúzcala en la casilla denominada “Passphrase for SSH key” (Frase de contraseña para la clave de SSH).
- Los usuarios de Nessus y SecurityCenter pueden también invocar “**`su`**” o “**`sudo`**” con el campo “Elevate privileges with” (Elevar privilegios con) y otra contraseña.
- Si se encuentra disponible un archivo de SSH **`known_hosts`** y se proporciona como parte de la directiva de análisis en el campo “SSH known_hosts file”, Nessus solo intentará iniciar sesión en los hosts en este archivo. Esta acción puede 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.

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

A continuación se presenta un ejemplo de captura de pantalla del uso de “**`sudo`**” junto con las claves de SSH. A los fines de este ejemplo, la cuenta de usuario es “audit” (auditoría), 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” (auditoría), no la contraseña raíz. Las claves de SSH se corresponden con las claves generadas para la cuenta “audit” (auditoría):



Si usa Kerberos, debe configurar un analizador Nessus para autenticarlo en un KDC. En el menú desplegable, seleccione “Kerberos configuration” (Configuración de Kerberos) como se muestra a continuación:



El puerto de KDC predeterminado es “88” y el protocolo de transporte predeterminado es “udp”. El otro valor para el transporte es “tcp”. Por último, el nombre Kerberos Realm y la dirección IP del KDC son obligatorios.

Tenga en cuenta que ya debe tener un entorno Kerberos establecido para usar este método de autenticación.

Al llegar a este punto haga clic en “**Submit**” (Enviar), que se encuentra en la parte inferior de la ventana, para finalizar la configuración. La nueva directiva de análisis se añadirá a la lista de directivas de análisis administradas.

Línea de comandos de Nessus Unix

La compatibilidad de Nessus para comprobaciones basadas en hosts se encuentra disponible en Nessus 2.2.0 y versiones posteriores, y requiere que la compatibilidad con SSL esté compilada. Ejecute el comando “**`nessusd -d`**” para asegurarse de tener la versión correcta y las bibliotecas SSL, de la siguiente manera:

```
# nessusd -d
[root@squirrel sbin]# ./nessusd -d
This is Nessus 5.0.1. [build R23100] for Linux 2.6.18-53.1.6.el5
compiled with gcc version 4.1.2 20070626 (Red Hat 4.1.2-14)
Current setup :
        flavor                          : es5-x86
        nasl                            : 5.0.1
        libnessus                       : 5.0.1
        SSL support                     : enabled
        SSL is used for client / server communication
        Running as euid                 : 0
Magic hash: 49edd1433ffad7b87b446a4201faeedf -
OpenSSL: OpenSSL 1.0.0g 18 Jan 2012
```

Uso de archivos .nessus

Nessus cuenta con capacidad para guardar directivas de análisis configuradas, destinos de red e informes como archivos **`.nessus`**. La sección presentada anteriormente, “Interfaz de usuario de Nessus”, describe cómo crear un archivo **`.nessus`** que contiene credenciales de SSH. Para obtener instrucciones sobre cómo ejecutar un análisis de líneas de comandos mediante el archivo **`.nessus`**, consulte la “Nessus User Guide” (“Guía del usuario de Nessus”), disponible en:

http://www.tenable.com/products/nessus/documentation

Uso de archivos .nessusrc

Si crea archivos “**`.nessusrc`**” en forma manual, existen varios parámetros que pueden configurarse para especificar la autenticación de SSH. A continuación se presenta un ejemplo de un listado sin rellenar:

```
Use SSH to perform local security checks[entry]:SSH user name : =
Use SSH to perform local security checks[file]:SSH public key to use : =
Use SSH to perform local security checks[file]:SSH private key to use : =
Use SSH to perform local security checks[password]:Passphrase for SSH key : =
SSH settings[entry]:SSH user name : =
SSH settings[password]:SSH password (unsafe!) : =
SSH settings[file]:SSH public key to use : = no
SSH settings[file]:SSH private key to use : =
SSH settings[password]:Passphrase for SSH key : =
```

Si usa Kerberos, debe configurar un analizador Nessus para autenticarlo en un KDC introduciendo la siguiente información en el archivo **`nessusrc`** del analizador:

```
Kerberos KDC port : 88
Kerberos KDC Transport : udp
Kerberos Realm (SSH Only) : myrealm
Kerberos Key Distribution Center (KDC): 192.168.20.66
```

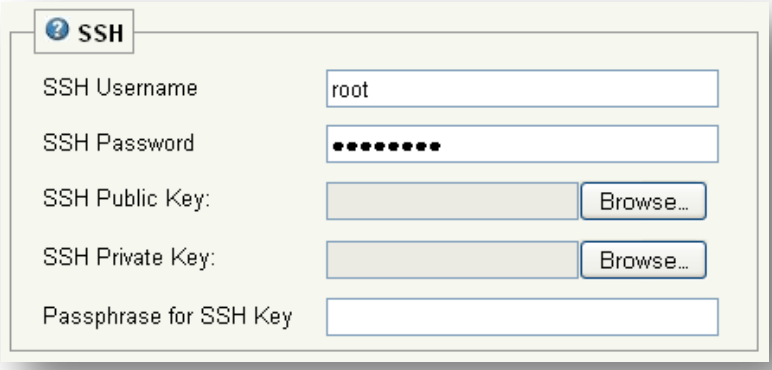
El puerto de KDC predeterminado es “88” y el protocolo de transporte predeterminado es “udp”. El otro valor para el transporte es “tcp”. Por último, el nombre Kerberos Realm y la dirección IP del KDC son obligatorios.

Tenga en cuenta que ya debe tener un entorno Kerberos establecido para usar este método de autenticación.

Uso de credenciales de SSH con Tenable SecurityCenter

Para usar las credenciales de SSH con SecurityCenter, cargue las claves pública y privada de SSH en la consola de SecurityCenter. No las instale directamente en los analizadores Nessus, ya que SecurityCenter descarga estas credenciales en el analizador Nessus cuando se inicia el análisis.

A continuación se presenta un ejemplo de una parte de la pantalla “Edit Scan Options” (Editar opciones de análisis) al editar las opciones de una directiva. Los últimos tres campos se usan para especificar una cuenta y las claves pública y privada de SSH específicas que se usarán al realizar pruebas. La clave pública de SSH debe colocarse en cada host de Unix al que se le realizarán las “comprobaciones locales”.



SecurityCenter incluye varias directivas de vulnerabilidades predefinidas que tienen habilitadas todas las “comprobaciones locales” para cada sistema operativo individual. Sin embargo, estas directivas deben copiarse y luego tener añadido un par específico de claves pública/privada de SSH, así como una cuenta de usuario específica, para que puedan usarse en forma operativa.

Los pares de claves pública/privada de SSH son administrados por SecurityCenter y se trasladarán a cada analizador Nessus administrado.

Una vez que estas claves públicas de SSH estén instaladas en los hosts Unix deseados y las claves privadas estén instaladas bajo SecurityCenter, se crea una relación de confianza por la que un usuario puede iniciar sesión en cada uno de los hosts de Unix desde los analizadores Nessus. Si la seguridad de los analizadores Nessus se ve comprometida, se deben generar nuevos pares de claves pública/privada de SSH.

Comprobaciones con credenciales en plataformas de Windows

Requisitos previos

Privilegios de usuario

Un error muy común consiste en crear una cuenta local que no tiene suficientes privilegios para iniciar sesión en forma remota ni para realizar ninguna acción útil. De manera predeterminada, Windows asignará a las nuevas cuentas locales privilegios de “invitado” si inician sesión en forma remota. De este modo se impide que las auditorías de vulnerabilidades remotas se realicen correctamente. Otro error común es ampliar el acceso que obtienen los usuarios “invitados”. De este modo se reduce la seguridad del servidor Windows.

Habilitación de inicios de sesión en Windows para auditorías locales y remotas

El aspecto más importante en cuanto a las credenciales de Windows es que la cuenta que se usa para realizar las comprobaciones debe tener privilegios para acceder a todas las entradas de registro y los archivos requeridos y, en muchos casos, esto significa privilegios administrativos. Si a Nessus no se le proporcionan las credenciales para una cuenta administrativa, a lo sumo puede usarse en la realización de comprobaciones del registro para verificar las revisiones. Si bien este es un método válido para determinar si una revisión se encuentra instalada, es incompatible con algunas herramientas de administración de revisiones de terceros que pueden omitir el establecimiento de la clave en la directiva. Si Nessus tiene privilegios administrativos, comprobará efectivamente la versión de la biblioteca de vínculos dinámicos (`.dll`) en el host remoto, lo cual es mucho más preciso.

Configuración de una cuenta local

Para configurar un servidor de Windows independiente con las credenciales que se usarán, que no forme parte de un dominio, simplemente cree una cuenta única como administrador.

Asegúrese de que la configuración de esta cuenta no esté definida de la manera predeterminada típica, como “Guest only: local users authenticate as guest” (Solo invitado: los usuarios locales se autentican como invitados). En su lugar, cambie a la configuración “Classic: local users authenticate as themselves”(Clásico: los usuarios locales se autentican como tales).

Para configurar el servidor con el fin de permitir inicios de sesión desde una cuenta de dominio, debe invocarse el modelo de seguridad “Classic” (Clásico). Para realizar esta acción, siga estos pasos:

1. Abra “Group Policy” (Directiva de grupo); para ello, haga clic en “start” (inicio), luego haga clic en “Run” (Ejecutar), escriba “**`gpedit.msc`**”, y luego haga clic en “OK” (Aceptar).

2. Seleccione Computer Configuration (Configuración del equipo) -> Windows Settings (Configuración de Windows) -> Security Settings (Configuración de seguridad) -> Local Policies (Directivas locales) -> Security Options (Opciones de seguridad).

3. En la lista de directivas, abra “Network access: Sharing and security model for local accounts” (Acceso de red: modelo de seguridad y uso compartido para cuentas locales).

4. En este cuadro de diálogo, seleccione “Classic – local users authenticate as themselves” (Clásico: los usuarios locales se autentican como tales) y luego haga clic en “OK” (Aceptar) para guardarlo.

Esto permitirá que los usuarios locales del dominio se autentiquen como tales, aunque en realidad no sean físicamente “locales” en tal servidor. Si no se realiza esta acción todos los usuarios remotos, incluidos los usuarios reales del dominio, se autenticarán como “invitado”, y es probable que no tengan las credenciales suficientes para realizar una auditoría remota.

Tenga en cuenta que la herramienta **`gpedit.msc`** no está disponible en algunas versiones como Windows 7 Home, que no es compatible con Tenable.

Configuración de una cuenta de dominio para análisis autenticados

Para crear una cuenta de dominio para auditorías remotas basadas en hosts de un servidor de Windows, en primer lugar el servidor debe ser Windows Vista, Windows XP Pro, Windows 2003, Windows 2008, Windows 7 o Windows 8, y debe

formar parte de un dominio. Debe llevar a cabo cinco pasos generales para facilitar este análisis teniendo en cuenta la seguridad.

Paso 1: crear un grupo de seguridad
Primero, cree un grupo de seguridad llamado **Nessus Local Access** (Acceso local a Nessus):

- Inicie sesión en un Controlador de dominio y abra Usuarios y equipos de Active Directory.
- Cree un grupo de seguridad desde **Menu** (Menú) y seleccione **Action** (Acción) -> **New** (Nuevo) -> **Group** (Grupo).
- Nombre el grupo como **Nessus Local Access**. Asegúrese de que el "Scope" (Alcance) sea `Global` y el "Type" (Tipo) sea `Security` (Seguridad).
- Agregue la cuenta que utilizará para hacer los análisis autenticados de Windows con Nessus al grupo **Nessus Local Access** (Acceso local a Nessus).

Paso 2: cree una directiva de grupo
A continuación, debe crear una directiva de grupo llamada **Local Admin GPO**.

- Abra la **Group Policy Management Console** (Consola de administración de directivas de grupo).
- Haga clic derecho en **Group Policy Objects** (Objetos de directiva de grupo) y seleccione **New** (Nuevo).
- Escriba el nombre de la directiva: "**Nessus Scan GPO**" (GPO [Objeto de directiva de grupo] de análisis de Nessus).

Paso 3: configure la directiva para agregar el grupo "Nessus Local Access" (Acceso local a Nessus) **como Administrators** (Administradores)
Aquí agregará el grupo **Nessus Local Access** (Acceso local a Nessus) a la directiva **Nessus Scan GPO** (GPO de análisis de Nessus), y los colocará en los grupos que desea que usen.

- Haga clic derecho en la directiva "**Nessus Scan GPO**" (GPO de análisis de Nessus) y seleccione **Edit** (Editar).
- Expanda ***Computer configuration\Policies\Windows Settings\Security Settings\Restricted Groups*** *(Configuración del equipo\Directivas\Configuración de Windows\Configuración de seguridad\Grupos restringidos)*.
- En el panel izquierdo en **Restricted Groups** (Grupos restringidos), haga clic derecho y seleccione "**Add Group**" (Agregar grupo).
- En el cuadro de diálogo **Add Group** (Agregar grupo), seleccione browse (explorar) y escriba **Nessus Local Access** (Acceso local a Nessus); luego haga clic en "**Check Names**" (Verificar nombres).
- Haga clic en **OK** (Aceptar) dos veces para cerrar el cuadro de diálogo.
- Haga clic en **Add** (Agregar) en "***This group is a member of:***" (Este grupo es miembro de)
- Agregue el grupo "*Administrators*" (*Administradores*).
- Haga clic en **OK** (Aceptar) dos veces.

Paso 4: garantice que los puertos correspondientes estén abiertos en el firewall para que Nessus se conecte al host.
Nessus utiliza SMB (Bloque de mensajes del servidor) y WMI (Instrumentación de administración de Windows); por esto, es necesario asegurarnos de que el Firewall de Windows permita acceso al sistema.

Permiso de WMI en el Firewall de Windows XP y 2003

- Haga clic derecho en la directiva "**Nessus Scan GPO**" (GPO de análisis de Nessus) y seleccione **Edit** (Editar).

- Expanda ***Computer configuration\Policies\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile*** *(Configuración del equipo\Directivas\Plantillas administrativas\Red\Conexiones de red\Firewall de Windows\Perfil de dominio)*.

  - ***Nota***: la razón principal por la que está configurado el Perfil de dominio y no el perfil estándar es que el Perfil de dominio se aplicará solo cuando Windows determine que está conectado a una red que es parte del dominio del que es miembro. El perfil estándar se aplicará cuando los hosts no puedan determinar si se encuentra en una red parte del dominio o en una red pública, por lo que minimizar la exposición a los puertos WMI disminuirá el riesgo.

- Seleccione **Windows Firewall: Define inbound program exceptions** (Firewall de Windows: definir excepciones de programas entrantes) y luego haga clic derecho y seleccione **Edit** (Editar) (o haga doble clic en él con el mouse).

  - Seleccione **Enabled** (Habilitado)

  - Haga clic en **Show** (Mostrar)

  - En las definiciones de **Program Exceptions** (Excepciones de programas), escriba:

    - %windir%\system32\wbem\unsecapp.exe:*:enable:wmi

    - %windir%\system32\dllhost.exe:*:enable:ddlhost

    - ***Nota***: en las entradas anteriores, * es el caracter comodín para permitir que cualquier dirección IP en el dominio se conecte a estos servicios; puede hacer esto más seguro permitiendo solo las direcciones IP o intervalos en los que las herramientas de administrador se conecten al puerto o donde se encuentre la dirección IP del analizador de Nessus.

  - Haga clic en **OK** (Aceptar)

  - Haga clic en **OK** (Aceptar) para ir a la lista de directivas para el firewall.

- Seleccione **Windows Firewall: Allow local port exceptions** (Firewall de Windows: permitir excepciones de puertos locales) y luego haga clic derecho y seleccione **Edit** (Editar) (o haga doble clic en él con el mouse).

  - Seleccione **Enabled** (Habilitado)

  - Haga clic en **OK** (Aceptar)

- Seleccione **Windows Firewall: Define inbound port exceptions** (Firewall de Windows: definir excepciones de puertos entrantes) y luego haga clic derecho y seleccione **Edit** (Editar) (o haga doble clic en él con el mouse).

  - Seleccione **Enabled** (Habilitado)

  - Haga clic en **Show** (Mostrar)

  - En las definiciones de **Port Exceptions** (Excepciones de puertos), escriba:

    - 135:TCP:*:enable

    - ***Nota***: en las entradas anteriores, * es el caracter comodín para permitir que cualquier dirección IP en el dominio se conecte a estos servicios; puede hacer esto más seguro permitiendo solo las direcciones IP o intervalos en los que las herramientas de administrador se conecten al puerto o donde se encuentre la dirección IP del analizador de Nessus.

  - Haga clic en **OK** (Aceptar) para ir a la lista de directivas para el firewall.

- Seleccione **Windows Firewall: Define inbound program exceptions** (Firewall de Windows: definir excepciones de programas entrantes) y luego haga clic derecho y seleccione **Edit** (Editar) (o haga doble clic en él con el mouse).
    - Seleccione **Enabled** (Habilitado)
    - Haga clic en el casillero **Allow unsolicited incoming messages from these IP addresses** (Permitir mensajes entrantes no solicitados de estas direcciones IP) y escriba *
    - ***Nota***: en las entradas anteriores, * es el caracter comodín para permitir que cualquier dirección IP en el dominio se conecte a estos servicios; puede hacer esto más seguro permitiendo solo las direcciones IP o intervalos en los que las herramientas de administrador se conecten al puerto o donde se encuentre la dirección IP del analizador de Nessus.
    - Haga clic en **OK** (Aceptar) para ir a la lista de directivas para el firewall.

Permiso de WMI en el Firewall de Windows Vista, 7, 8, 2008, 2008R2 y 2012

- Haga clic en la directiva "**Nessus Scan GPO**" (GPO de análisis de Nessus) y seleccione **Edit** (Editar).
- Expanda ***Computer configuration\Policies\Windows Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Inbound Rules*** *(Configuración del equipo\Directivas\Configuración de Windows\Firewall de Windows con seguridad avanzada\ Firewall de Windows con seguridad avanzada \Reglas entrantes).*
- Haga clic en el área de funcionamiento y escoja **New Rule...** (Nueva regla...)
- Escoja la opción Predefined (Predefinida) y escoja **Windows Management Instrumentation (WMI)** (Instrumentación de administración de Windows) de la lista desplegable.
- Haga clic en **Next** (Siguiente).
- Marque los casilleros de:
    - Windows Management Instrumentation (ASync-In)
    - Windows Management Instrumentation (WMI-In)
    - Windows Management Instrumentation (DCOM-In)
- Haga clic en **Next** (Siguiente).
- Haga clic en **Finish** (Finalizar).
- ***Nota***: más adelante puede editar la regla predefinida creada y limitar la conexión a los puertos por dirección IP y usuario de dominio, para disminuir cualquier riesgo de abuso de la WMI.

Paso 5: vincular GPO

- En la consola de administración de directivas de grupo, haga clic en el dominio o la OU y escoja Link an Existing GPO (Vincular GPO existente)
- Escoja Nessus Scan GPO (GPO de análisis de Nessus)

Configuración en Windows XP y 2003

Al realizar análisis autenticados en los sistemas Windows XP o 2003, existen varias opciones de configuración que deben habilitarse:

1. El servicio WMI debe habilitarse en el destino.

2. El servicio Remote Registry (Registro remoto) debe estar habilitado (está deshabilitado de manera predeterminada). Un administrador o Nessus pueden habilitarlo manualmente para auditorías continuas. Con los plugins 42897 y 42898, Nessus puede habilitar el servicio solo durante el análisis.

3. File and Printer Sharing (Compartir archivos e impresoras) debe habilitarse en la configuración de red de destino.

4. Los puertos 139 y 445 deben estar abiertos entre el analizador Nessus y el destino.

5. Debe usarse una cuenta de SMB que tenga derechos de administrador local en el destino.

Es posible que se le solicite que cambie sus directivas de seguridad locales de Windows; de lo contrario, podrían bloquear el acceso o los permisos inherentes. Una directiva común que afectará los análisis con credenciales se encuentra en la siguiente ruta:

Administrative Tools (Herramientas administrativas) -> Local Security Policy (Directiva de seguridad local) -> Security Settings (Configuración de seguridad) -> Local Policies (Directivas locales) -> Security Options (Opciones de seguridad) -> Network access: Sharing and security model for local accounts (Acceso de red: modelo de seguridad y uso compartido para cuentas locales).

Si esta directiva de seguridad local se establece con una configuración distinta de “Classic - local users authenticate as themselves” (Clásico: los usuarios locales se autentican como tales), el análisis de compatibilidad no se ejecutará correctamente.

Configuración en Windows 2008, Vista y 7

Al realizar análisis autenticados en los sistemas Windows 2008, Vista o 7, existen varias opciones de configuración que deben habilitarse:

1. En Windows Firewall (Firewall de Windows) -> Windows Firewall Settings (Configuración de Firewall de Windows), debe estar habilitado “File and Printer Sharing” (Compartir archivos e impresoras).

2. Al usar la herramienta **`gpedit.msc`** (a través del indicador “Run..” [Ejecutar..]), invoque el Group Policy Object Editor (Editor de objetos de directiva de grupo). Desplácese hasta Local Computer Policy (Directiva de equipo local) -> Administrative Templates (Plantillas administrativas) -> Network (Red) -> Network Connections (Conexiones de red) - > Windows Firewall (Firewall de Windows) -> Standard Profile (Perfil estándar) -> Windows Firewall: Allow inbound file and printer sharing exception (Firewall de Windows: permitir excepción de uso compartido de archivos e impresoras entrantes), y habilítelo.

3. En Group Policy Object Editor (Editor de objetos de directiva de grupo), Local Computer Policy (Directiva de equipo local) -> Administrative Templates (Plantillas administrativas) -> Network (Red) -> Network Connections (Conexiones de red) -> Prohibit use of Internet connection firewall on your DNS domain (Prohibir el uso del Firewall de conexión a Internet en su dominio DNS) debe establecerse “Disabled” (Deshabilitado) o “Not Configured” (Sin configurar).

4. El servicio Remote Registry (Registro remoto) debe estar habilitado (está deshabilitado de manera predeterminada). Un administrador o Nessus pueden habilitarlo manualmente para auditorías continuas. Con los plugins 42897 y 42898, Nessus puede habilitar el servicio solo durante el análisis.

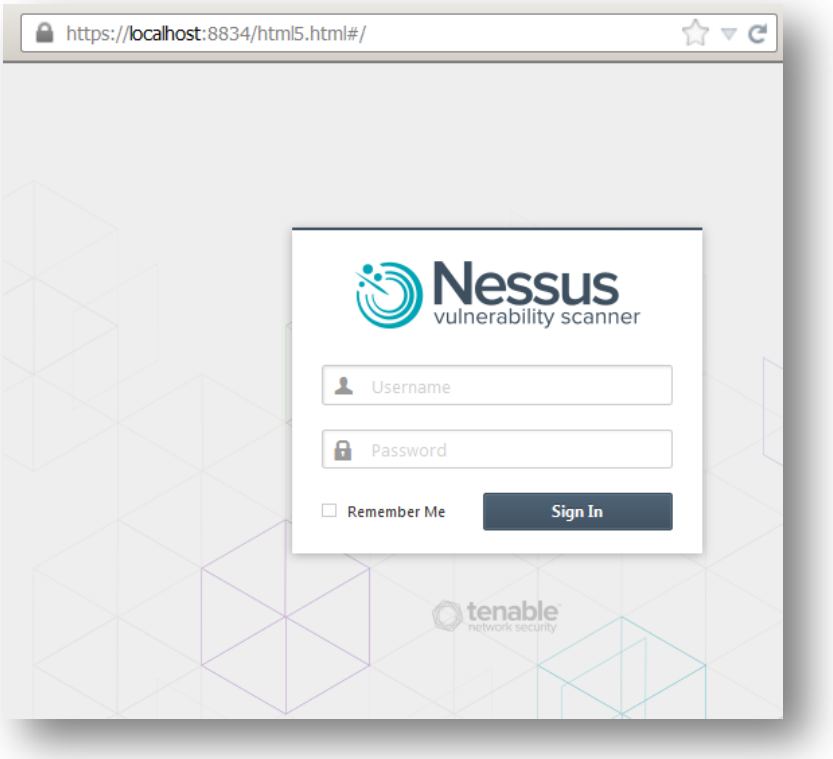
Nessus tiene la capacidad de habilitar y deshabilitar el servicio Remote Registry (Registro remoto). Para ello, el destino debe tener el servicio Registro remoto establecido en “Manual” (Manual) y no en “Disabled" (Deshabilitado).

El User Account Control (UAC) (Control de cuentas de usuario) de Windows también puede deshabilitarse, pero no se recomienda. Para desactivar completamente el UAC abra el Panel de control, seleccione “User Accounts” (Cuentas de usuario) y luego, en “Turn User Account Control On or Off” (Activar o desactivar el Control de cuentas de usuario) seleccione ‘Off’ (Desactivar). Opcionalmente, puede añadir una nueva clave de registro denominada “LocalAccountTokenFilterPolicy” y establecer su valor en “1”. Esta clave debe crearse en el registro

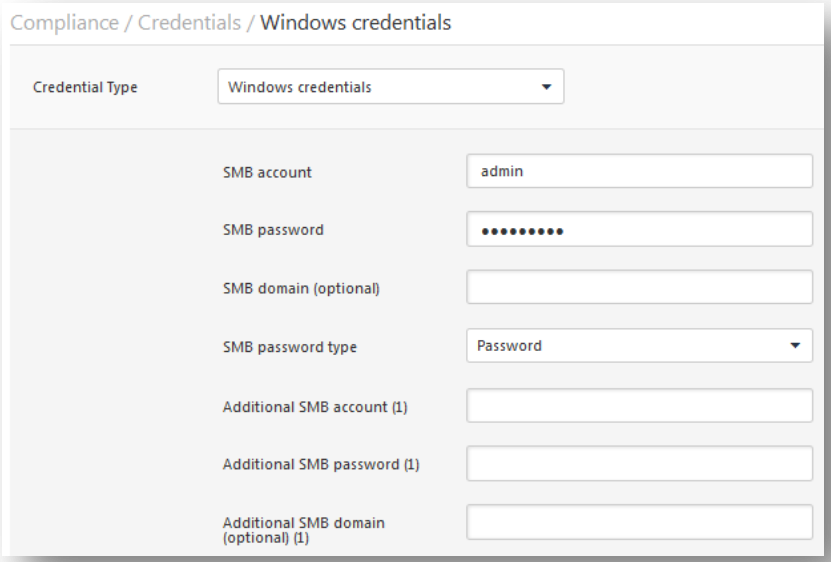
en la siguiente ubicación: **`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\LocalAccountTokenFilterPolicy`**. Para obtener más información sobre esta opción de registro, consulte la MSDN 766945 KB.

Configuración de Nessus para inicios de sesión en Windows

Interfaz de usuario de Nessus



Abra un explorador web y conéctese a la interfaz de usuario del analizador Nessus, tal como se muestra en la figura anterior, y haga clic en la ficha “Policies” (Directivas). Cree una nueva directiva o modifique una directiva actual, y seleccione la ficha “Credentials” (Credenciales) que se encuentra a la izquierda. Seleccione “Windows credentials” (Credenciales de Windows) del menú desplegable que se encuentra en la parte superior, como se muestra a continuación:



Especifique el nombre de cuenta de SMB, la contraseña y el dominio opcional.

Al llegar a este punto haga clic en "**Submit**" (Enviar), que se encuentra en la parte inferior de la ventana, para finalizar la configuración. La nueva directiva de análisis se añadirá a la lista de directivas de análisis administradas.

Línea de comandos de Nessus Unix

Uso de archivos .nessus

Nessus cuenta con capacidad para guardar directivas de análisis configuradas, destinos de red e informes como archivos `.nessus`. La sección presentada anteriormente, "Interfaz de usuario de Nessus", describe cómo crear un archivo `.nessus` que contiene credenciales de Windows. Para obtener instrucciones sobre cómo ejecutar un análisis de líneas de comandos mediante el archivo `.nessus`, consulte la "Nessus User Guide" ("Guía del usuario de Nessus"), disponible en:

http://www.tenable.com/products/nessus/documentation

Uso de archivos .nessusrc

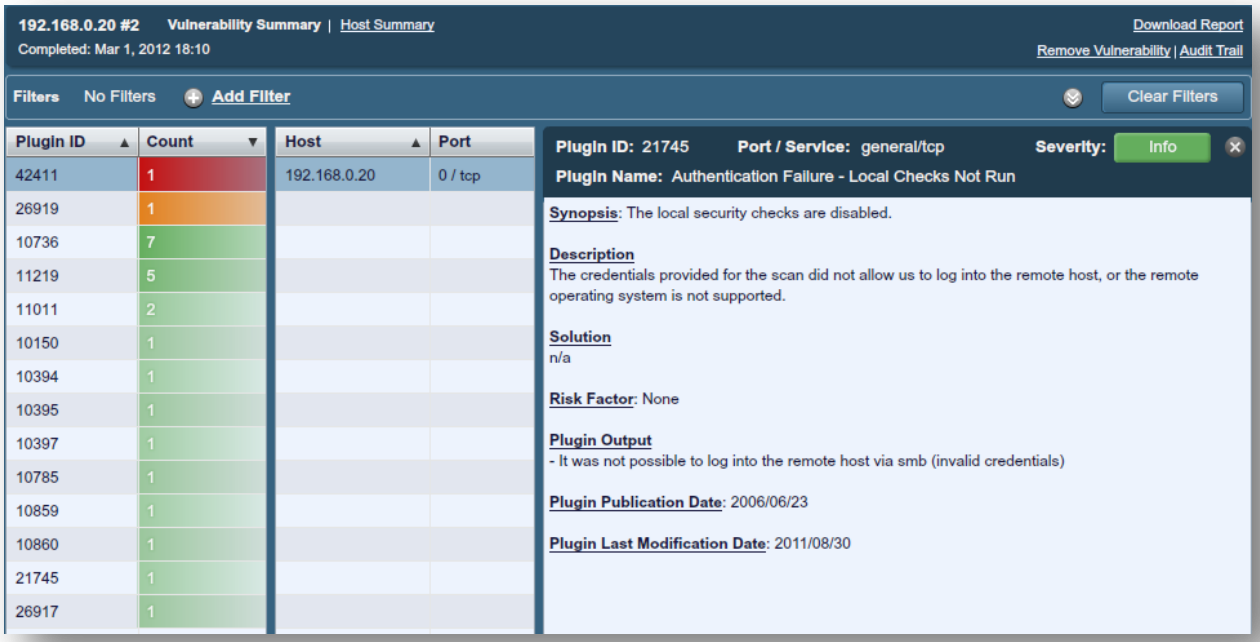
Si crea un archivo "`.nessusrc`" en forma manual, existen tres entradas que permiten realizar la configuración de nombre de usuario, contraseña y dominio opcional, como se muestra a continuación:

```
Login configurations[entry]:SMB account : =
Login configurations[password]:SMB password : =
Login configurations[entry]:SMB domain (optional) : =
```

Detección de fallas en las credenciales

Si usa Nessus para realizar auditorías con credenciales de los sistemas de Unix o Windows, el análisis de los resultados para determinar si recibió las contraseñas y claves de SSH correctas puede resultar complicado. Los usuarios de Nessus pueden ahora detectar con facilidad si sus credenciales no funcionan. Tenable ha agregado el plugin Nessus N.º 21745 a la familia de plugins "Settings" (Configuración).

Este plugin detecta si las credenciales de Windows o SSH no permitieron que el análisis inicie sesión en el host remoto. Cuando un inicio de sesión se realiza correctamente, este plugin no genera resultados. A continuación se presenta un ejemplo de informe que se produjo al intentar iniciar sesión en un equipo remoto con el nombre de usuario o contraseña incorrectos con Nessus:



Solución de problemas

P. ¿Cómo sé si el análisis local está funcionando?

R. A menos que tenga un servidor completamente revisado, es probable que los análisis locales generen algún tipo de información de revisión. Según el sistema operativo, también generarán una variedad de auditorías de información.

También puede resultar útil quitar a “Nessus” de la ecuación y realizar una prueba para asegurarse de que las cuentas y las redes estén configuradas correctamente. Desde el analizador Nessus, use el comando simple de Unix **`id`** para ejecutar el siguiente comando:

```
# ssh -i /home/test/nessus/ssh_key nessus@192.1.1.44 id
#
```

Asegúrese de usar la dirección IP del sistema con el que está configurada la relación de confianza, y la cuenta de usuario (en este caso el usuario es “nessus”). Si el comando es correcto, verá los resultados del comando **`id`** como si este se ejecutara en su sistema remoto.

En las auditorías de Unix, la secuencia de comandos **`ssh_get_info.nasl`** informará si la autenticación se realizó correctamente. Si los inicios de sesión de SSH no funcionan, puede aumentar la opción de “report_verbosity” de su análisis Nessus a “Verbose”(Detallado). De esta manera, se mostrará cualquier mensaje de diagnóstico o error mientras esta secuencia de comandos se encuentre en ejecución.

Para las auditorías de Windows, las secuencias de comandos **`smb_login.nasl`** y **`smb_registry_access.nasl`** indican si la identificación de inicio de sesión y contraseña proporcionadas durante el análisis funcionaron, y si fue posible leer el registro remoto. **`smb_registry_full_access.nasl`** advierte solo si no fue posible leer completamente el registro. La observación de los resultados de las comprobaciones basadas en hosts para las auditorías de un servidor Windows mostrará cómo funcionaron las credenciales.

Además, la secuencia de comandos **`hostlevel_check_failed.nasl`** detecta si las credenciales de Windows o SSH no permitieron que el análisis inicie sesión en el host remoto.

P. ¿Cómo sé si el análisis local no está funcionando?

R. En los sistemas de Windows, los eventos de error de inicio de sesión se generarán en el servidor. Si se encuentra en uso un controlador de dominio, los eventos de error de inicio de sesión también se guardarán en esa ubicación.

En los sistemas de Unix, los errores de inicio de sesión aparecerán en los registros del sistema (por ejemplo, **`/var/log/messages`**) a menos que un controlador Kerberos remoto se encuentre en uso.

Además, la secuencia de comandos **`hostlevel_check_failed.nasl`** detecta si las credenciales de Windows o SSH no permitieron que el análisis inicie sesión en el host remoto.

P. ¿Qué otros problemas pueden presentarse en las comprobaciones de hosts?

R. Hay varias cosas que pueden bloquear el acceso. A continuación se presentan algunas que deben tenerse en cuenta:

- Firewalls de red que filtran el puerto 22 para SSH en Unix o el puerto 445 para Windows
- Firewalls basados en hosts que bloquean las conexiones a los puertos mencionados
- En los sistemas de Unix, los administradores que trasladan SSH a otros puertos que no sean el 22
- Algunos sistemas de prevención de intrusión de red y host que impiden el acceso remoto
- El equipo que está analizando no es un servidor de Unix o Windows, y podría ser una impresora, enrutador, máquina de fax o dispositivo de pantalla de video

P. Estoy probando conexiones SSH desde el indicador de shell de hosts de destino de análisis hasta el sistema Nessus para garantizar que haya una conectividad correcta. Veo que se demora en conectarse, ¿por qué?

R. Lo más probable es que esto se deba a que el sistema realiza una búsqueda de DNS cuando DNS tiene una configuración errónea. Si su sitio usa DNS, comuníquese con su administrador de DNS para abordar problemas de configuración. Uno de los aspectos que podría causar problemas es la falta de zonas de búsqueda inversa. Para probar las búsquedas de DNS, realice lo siguiente:

```
# host IP_ADRR_OF_NESSUS_SERVER
```

Si tiene instalado “dig”, también se puede comprobar con lo siguiente:

```
# dig -x IP_ADRR_OF_NESSUS_SERVER
```

Si su sitio no usa DNS, los siguientes pasos omitirán el intento de realizar búsquedas de DNS.

1. Edite el archivo **`/etc/nsswitch.conf`** para que las líneas de “hosts:” tengan la leyenda “hosts: files”
   Nota: es posible que esto no se aplique a todas las versiones de OpenSSH.
2. Añada el IP o el nombre del servidor que ejecuta Nessus en el archivo **`/etc/hosts`** del sistema.
3. Para configurar el servidor OpenSSH remoto para que **no** realice búsquedas de DNS en un host, debe definir lo siguiente:
   - “UseDNS no” en el archivo **`sshd_config`** (para la versión 3.8); el valor predeterminado es yes (sí)
   - “VerifyReverseMapping no”

Protección del analizador

¿Por qué debo proteger el analizador?

Si configura un analizador Nessus para que use credenciales para iniciar sesión en un servidor de Unix o Windows, su sistema tendrá credenciales que un usuario malintencionado podría aprovechar. Para evitar esto, no solo debe llevar a cabo prácticas seguras y adecuadas con el sistema operativo en el que se ejecuta su analizador, sino que también debe saber cómo un adversario puede engañar al analizador para que divulgue información de seguridad.

¿Qué significa bloquear un analizador?

El analizador Nessus ideal se manejaría completamente desde una consola del sistema, sin aceptar ninguna conexión de red desde un host remoto. Tal sistema tendría la protección física necesaria para que solo las personas autorizadas pudieran acceder a él. Este servidor podría restringirse aún más a través de un conmutador o firewall externo que solo le permitiera analizar redes específicas. No instale software de firewall personal directamente en el sistema del analizador Nessus. Recuerde que Nessus puede configurarse para analizar solamente redes específicas.

Este tipo de analizador no es tan útil. Considere la posibilidad de proporcionar acceso de red remoto al servidor. Nessus admite conexiones HTTP al puerto 8834 de manera predeterminada. Un firewall del sistema puede configurarse para aceptar solamente conexiones en el puerto 8834 de clientes de Nessus válidos.

Si la caja se administrará u operará en forma remota, también puede usarse un acceso remoto seguro. En Unix se puede usar el protocolo Shell seguro (SSH). Mantenga actualizado el demonio de SSH, use contraseñas seguras y/o use técnicas de autenticación más seguras. En servidores de Windows pueden usarse los Servicios de Terminal Server remotos para proporcionar comando y control a los servicios de Nessus Windows. En ambos casos, mantenga actualizado el sistema y no ejecute servicios de red innecesarios. Consulte los Center for Internet Security (CIS) benchmarks (Criterios de referencia del Center for Internet Security [CIS]) para obtener orientación sobre fortalecimiento de sistemas.

Implementación segura de auditorías de SSH de Unix

Nunca use contraseñas de SSH para realizar análisis remotos. Si analiza una red, todo lo que los usuarios malintencionados o adversarios deberían hacer es ejecutar un demonio de SSH modificado y registrar el nombre de usuario y contraseña intentados. Aunque tenga una combinación única de nombre de usuario y contraseña para cada host, el uso de contraseñas estáticas sigue siendo vulnerable a la explotación.

Si inicia sesión en un servidor con una contraseña en un sistema que se ha visto comprometido, existe la posibilidad de que le roben la contraseña, porque la contraseña en sí atraviesa la conexión SSH. Una vez que se tiene propiedad sobre el servidor remoto, el atacante puede sustituir el demonio SSH con el propio y así registrar las contraseñas de conexiones entrantes.

Auditorías seguras en Windows

Si la opción “Only use NTLMv2” (Use sólo NTLMv2) está deshabilitada es posible, en teoría, engañar a Nessus para que intente iniciar sesión en un servidor de Windows con credenciales del dominio a través del protocolo NTLM versión 1. Esto proporciona al atacante remoto la capacidad de usar un “hash” que se haya obtenido por medio de Nessus. Es posible que este “hash” pueda descifrarse para revelar el nombre de usuario o la contraseña. También se lo puede usar para iniciar sesión directamente en otros servidores. Obligue a Nessus a usar NTLMv2 habilitando la opción “Only use NTLMv2” (Use sólo NTLMv2) al momento del análisis. Esta acción impide que un servidor de Windows hostil use NTLM y reciba un “hash”.

NTLMv2 puede usar la “SMB Signing” (Firma SMB). Asegúrese de que la “SMB Signing” (Firma SMB) esté habilitada en todos sus servidores de Windows, para impedir que los servidores que reciban un “hash” de un análisis Nessus vuelvan a usarlo. Además, asegúrese de imponer una directiva que exija el uso de contraseñas seguras que no puedan descifrarse con facilidad a través de ataques por diccionario con herramientas como John the Ripper y L0phtCrack.

Tenga en cuenta que ha habido distintos tipos de ataques contra la seguridad de Windows para extraer “hashes” de equipos con el fin de volver a usarlos en servidores hostiles. “SMB Signing" (Firma SMB) añade una capa de seguridad para impedir estos ataques de tipo “Man in the middle” (intermediarios).

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:

- **Nessus 5.2 Installation and Configuration Guide** (Guía de instalación y configuración de Nessus 5.2): instrucciones paso a paso sobre la instalación y la configuración.
- **Nessus 5.2 User Guide** (Guía del usuario de Nessus): instrucciones sobre cómo configurar y operar la interfaz de usuario de 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 archivos Nessus v2): describe la estructura del formato de archivos `.nessus`, que se introdujo a través de Nessus 3.2 y NessusClient 3.2.
- **Nessus 5.0 REST Protocol Specification** (Especificación del protocolo REST en Nessus 5.0): describe la interfaz y el protocolo REST en Nessus.
- **Nessus 5 and Antivirus** (Nessus 5 y los antivirus): describe cómo interactúan con Nessus varios de los paquetes de software de seguridad más utilizados, y ofrece consejos y soluciones para permitir una mejor coexistencia con el software sin comprometer su seguridad u obstaculizar sus tareas de análisis de vulnerabilidades.
- **Nessus 5 and Mobile Device Scanning** (Nessus 5 y el análisis de dispositivos móviles): describe cómo Nessus se integra con el Servidor de Active Directory de Windows y servidores de administración de dispositivos móviles para identificar los dispositivos móviles en uso en la red.
- **Nessus 5.0 and Scanning Virtual Machines** (Nessus 5.0 y el análisis de máquinas virtuales): describe cómo el analizador de vulnerabilidades Nessus de Tenable Network Security puede utilizarse para auditar la configuración de las plataformas virtuales y también el software que se está ejecutando en ellas.
- **Strategic Anti-malware Monitoring with Nessus, PVS, and LCE** (Supervisión estratégica anti-malware con Nessus, PVS y LCE): describe cómo la plataforma USM de Tenable puede detectar una amplia variedad de software malicioso, e identificar y determinar la gravedad de las infecciones de malware.
- **Patch Management Integration** (Integración de administración de revisiones): este documento describe cómo Nessus y SecurityCenter pueden aprovechar credenciales en los sistemas de administración de revisiones IBM TEM, Microsoft WSUS y SCCM, VMware Go y Red Hat Network Satellite para ejecutar auditorías de revisiones en sistemas para los que pueda no haber credenciales disponibles para el analizador 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.
- **Tenable Products Plugin Families** (Familias de plugins de productos de Tenable): ofrece una descripción y un resumen de las familias de plugins para Nessus, el Log Correlation Engine (Motor de correlación de registros de eventos) y el Passive Vulnerability Scanner (Analizador pasivo de vulnerabilidades).

- **SecurityCenter Administration Guide** (Guía de administración de SecurityCenter)

Estos son otros recursos en línea:

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

Puede contactarse con Tenable en support@tenable.com o sales@tenable.com, o visitar nuestro sitio web http://www.tenable.com/.

Acerca de Tenable Network Security

Más de 20 000 organizaciones confían en Tenable Network Security, entre ellas el Departamento de Defensa de EE. UU. en su totalidad y muchas de las compañías más grandes y los gobiernos de todo el mundo, para adelantarse a las vulnerabilidades, amenazas y riesgos de compatibilidad emergentes. Sus soluciones Nessus y SecurityCenter siguen marcando la norma para identificar vulnerabilidades, evitar ataques y cumplir con muchísimos requisitos regulatorios. Para obtener más información, visite www.tenable.com.

SEDE CENTRAL MUNDIAL

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